Security+ CertMaster Study

Uvod u tečaj

CompTIA Security+ certifikacija je globalna certifikacija koja potvrđuje temeljne vještine kibernetičke sigurnosti potrebne za obavljanje osnovnih sigurnosnih funkcija i izgradnju karijere u IT sigurnosti.

- Sažeti temeljne sigurnosne koncepte.
- Usporediti vrste prijetnji.
- Objasniti odgovarajuća kriptografska rješenja.
- Implementirati upravljanje identitetom i pristupom.
- Osigurati arhitekture, mreže i uređaje.
- Objasniti aspekte upravljanja ranjivostima.
- Provoditi postupke sigurnosnih operacija.
- Implementirati kontrole zaštite podataka.

Modul 1

Sažetak temeljnih sigurnosnih koncepata

Pregled modula

Sigurnost je kontinuirani proces koji uključuje procjenu zahtjeva, postavljanje organizacijskih sigurnosnih sustava, očvršćivanje i testiranje sustava, praćenje okoline te odgovor na prijetnje i incidente čim se pojave. Kao sigurnosni stručnjak na početnoj razini, vaš je posao biti u toku sa svim tim procesima.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Sažeti koncepte informacijske sigurnosti.
- Usporediti i suprotstaviti vrste sigurnosnih kontrola.
- Opisati sigurnosne uloge i odgovornosti.

Lekcija 1A

Sigurnosni koncepti

Pregled lekcije

Da biste bili uspješan i vjerodostojan sigurnosni stručnjak, trebate razumjeti sigurnost u poslovanju od samih temelja. To znači razumijevanje konceptualnog okvira sigurnosti i važnosti usklađivanja sigurnosnih mjera s poslovnim ciljevima.

Informacijska sigurnost

Informacijska sigurnost (infosec) odnosi se na zaštitu podatkovnih resursa od neovlaštenog pristupa, napada, krađe ili oštećenja. Zaštita informacijske imovine oslanja se na tri načela koja zajedno tvore trijadu CIA:

- Povjerljivost znači da informacije mogu čitati samo osobe koje su izričito ovlaštene za pristup.
- Integritet znači da su podaci pohranjeni i preneseni onako kako je zamišljeno, a svaka izmjena je neovlaštena osim ako nije izričito odobrena kroz odgovarajuće kanale.
- Dostupnost znači da su informacije lako dostupne onima koji su ovlašteni za pregled ili izmjenu. Trijada se također može nazvati 'AIC' kako bi se izbjegla zbrka s Centralnom obavještajnom agencijom.

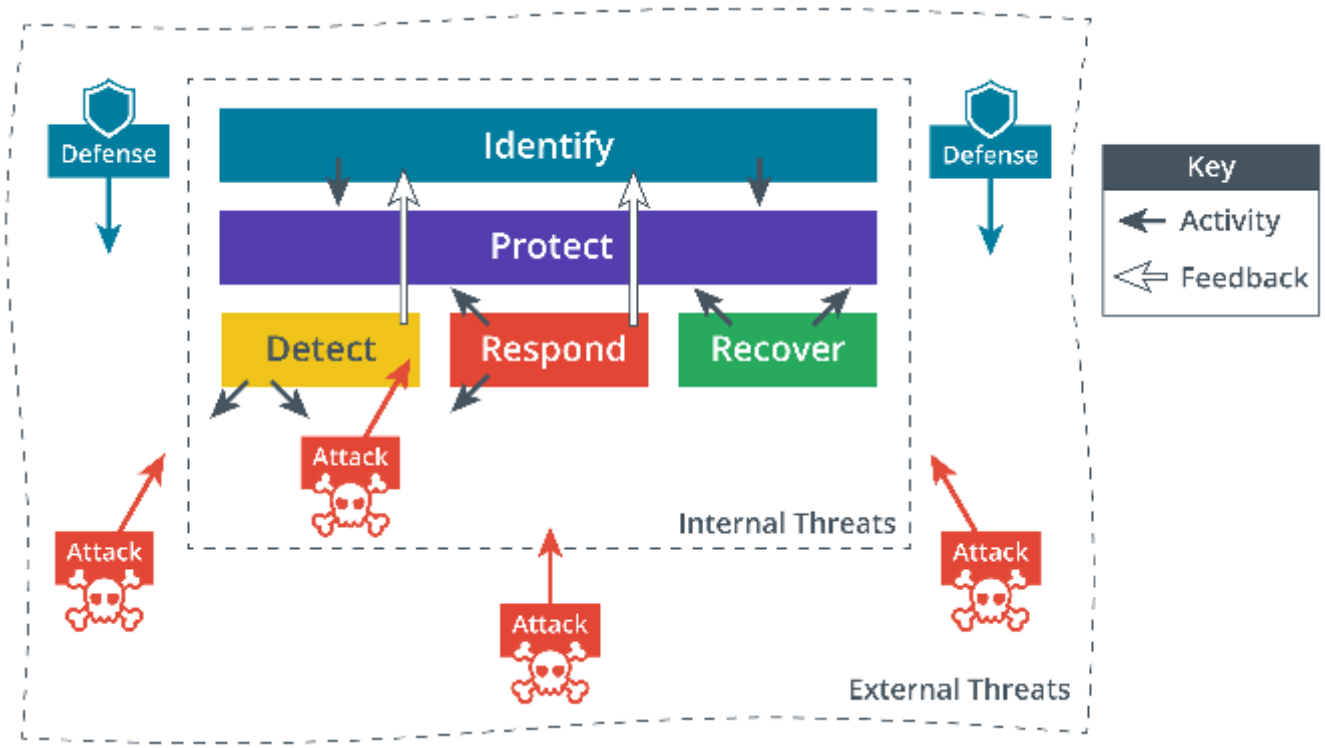
Neki sigurnosni modeli i istraživači identificiraju i druga svojstva sigurnih sustava. Najvažnije od njih je neporecivost (non-repudiation) — subjekt ne može zanijekati da je poduzeo neku radnju.

Okvir kibernetičke sigurnosti

U okviru cilja osiguravanja informacijske sigurnosti, kibernetička sigurnost se konkretno odnosi na pružanje zaštite za sustave i mreže koji pohranjuju i obrađuju podatke u digitalnom obliku. NIST Cybersecurity Framework (CSF) identificira pet stalnih i usporednih funkcija:

- Identificiraj (Identify) — razvijaj sigurnosne politike i sposobnosti. Procijeni rizike, prijetnje i ranjivosti te preporuči sigurnosne kontrole za njihovo ublažavanje.

- Zaštiti (Protect) — nabavi/razvij, instaliraj, upravljaj i povuci IT hardver i softver uz sigurnost kao ugrađeni zahtjev svake faze životnog ciklusa operacije.
- Detektiraj (Detect) — provodi kontinuirano, proaktivno praćenje kako bi se osiguralo da su kontrole učinkovite i sposobne zaštititi od novih vrsta prijetnji.
- Odgovori (Respond) — identificiraj, analiziraj, sadržavaj i iskorijeni prijetnje sigurnosti sustava i podataka.
- Oporavak (Recover) — implementiraj mjere za kibernetičku otpornost te zamijeni ili obnovi sustave koji su pogođeni nakon napada ili drugog incidenta.



NIST-ov okvir je samo jedan primjer. Postoje mnogi drugi okviri za kibernetičku sigurnost (CSF).

Analiza razlika (Gap Analysis)

Svaka sigurnosna funkcija povezana je s određenim ciljevima ili ishodima. Na primjer, jedan ishod funkcije Identificiranja mogao bi biti: 'Fizička imovina organizacije (npr. uređaji i sustavi) inventarizirana su u roku od dva radna dana od nabave.' Organizacija će zatim ocijeniti koliko dobro njena trenutna praksa zadovoljava taj cilj.

Okvir kibernetičke sigurnosti usmjerava odabir i konfiguraciju kontrola. Okviri su važni jer štede od nule osmišljavanja vlastite metodologije. Mnoge organizacije i vladine agencije objavljuju okvire koji mogu biti opći ili specifični za industriju. Na primjer, National Institute of Standards and Technology (NIST) objavljuje okvire i smjernice koji pokrivaju sve aspekte IT operacija i sigurnosti.

Function	Controls (Actual/Required)	CIA Triad Risk Levels	Target Remediation
Identify (10/16)	Asset Management (4/6)	C : 6 I : 6 A : 6	Q4
	Governance (3/4)	C : 6 I : 6 A : 1	Q3
	Risk Assessment (3/6)	C : 6 I : 6 A : 3	Q3
Protect (8/16)	Identity and Access Management (5/8)	C : 9 I : 9 A : 4	Q1
	Data Security (3/8)	C : 9 I : 9 A : 4	Q1

Advanced capability
Intermediate capability
No/basic capability

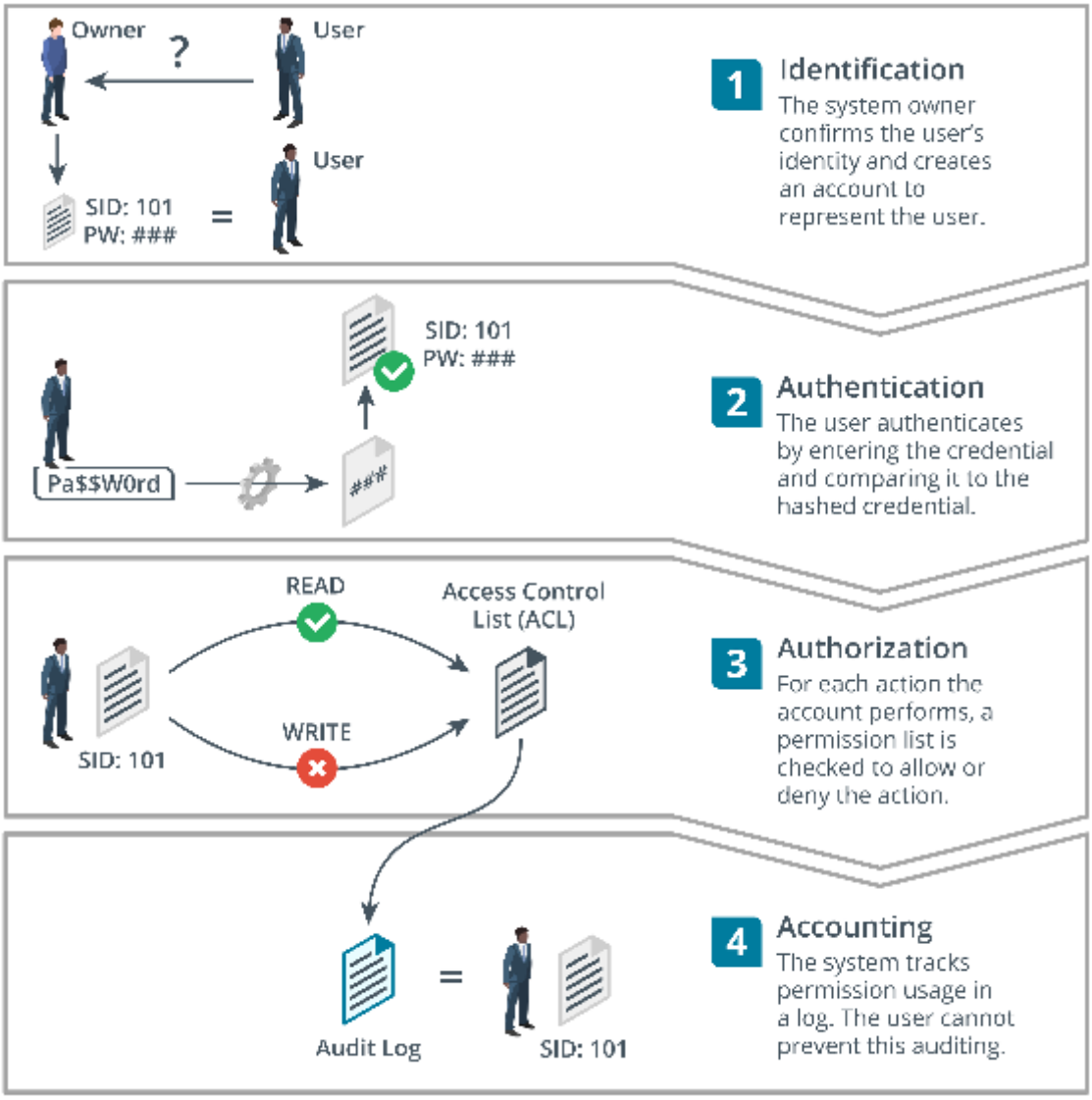
Dok neke ili sve radove uključene u analizu razlika može obaviti interni sigurnosni tim, analiza razlika vjerojatno je i regulatorni zahtjev ili zahtjev za usklađenost, pa zahtijeva neovisnu potvrdu. Stoga bi revizija trebala biti provedena od strane neovisnih stručnjaka treće strane. Ovi stručnjaci mogu biti konzultanti ili organizacija koja obavlja procjenu ispunjavate li zahtjeve odabranog okvira. Pristup temeljen na okviru usmjeren je na razvoj i upravljanje procesom koji osigurava sigurnost. Uspješno pridržavanje okvira dovest će do identificiranja sigurnosnih kontrola koje treba uvesti. Kontrola je sigurnosni mehanizam, politika ili procedura koja može upravljati prijetnjama, smanjiti rizike ili im ublažiti utjecaj. Pristup ili proces, identitet i autentikacija (IAA) implementira sigurnosne kontrole koji upravljaju pristupom sustavima:

- Identifikacija — stvaranje računa ili ID-a koji jedinstveno predstavlja korisnika, uređaj ili proces na mreži.
- Autentikacija — dokazivanje da je subjekt onaj za koga se izdaje kada pokušava pristupiti resursu. Faktor autentikacije određuje vrstu vjerodajnica koju subjekt može koristiti. Na primjer, osobe se mogu autenticirati davanjem lozinke; računalni sustav može se autenticirati korištenjem tokena poput digitalnog certifikata.
- Autorizacija — utvrđivanje koja prava subjekti trebaju imati na svakom resursu i provedba tih prava. Model autorizacije određuje kako se ta prava dodjeljuju. Na primjer, u diskrecijskom modelu, vlasnik objekta može dodijeliti pravo. U obveznom

modelu, prava su unaprijed određena pravilima koja nameće sustav i koja nijedan korisnik unutar sustava ne može mijenjati.

- Računovodstvo (Accounting) — praćenje ovlaštenog korištenja resursa ili korištenja prava od strane subjekta te upozoravanje kada se otkrije ili pokuša neovlašteno korištenje.

Razlike između identifikacije, autentikacije, autorizacije i računovodstva.



Poslužitelji i protokoli koji implementiraju ove funkcije mogu se nazuvati autentikacija, autorizacija i računovodstvo (AAA). Korištenje IAM-a za opisivanje sigurnosnih tijekova rada u poduzeću sve je raširenije jer se važnost procesa identifikacije sve više prepoznaje.

- Identifikacija — osigurajte da su kupci legitimni. Na primjer, možda ćete trebati osigurati da se adrese naplate i dostave podudaraju i da ne pokušavaju koristiti lažne načine plaćanja.
- Autentikacija — osigurajte da kupci imaju jedinstvene račune i da samo oni mogu upravljati svojim narudžbama i podacima o naplati.
- Autorizacija — pravila za osiguranje da kupci mogu naručivati samo kada imaju valjane načine plaćanja. Možete upravljati programima vjernosti ili promocijama koje ovlašćuju određene kupce za pregled neobavljenih artikala.

- Računovodstvo — sustav mora bilježiti radnje koje kupac poduzima (kako bi se, na primjer, osiguralo da ne mogu zanijekati narudžbu). Zapamtite da se ti procesi primjenjuju i na ljude i na sustave. Na primjer, web aplikacija koja pristupa bazi podataka mora se identificirati, autenticirati i autorizirati, a njezine radnje trebaju biti evidentirane.

Lekcija 1B

Sigurnosne kontrole

Pregled lekcije

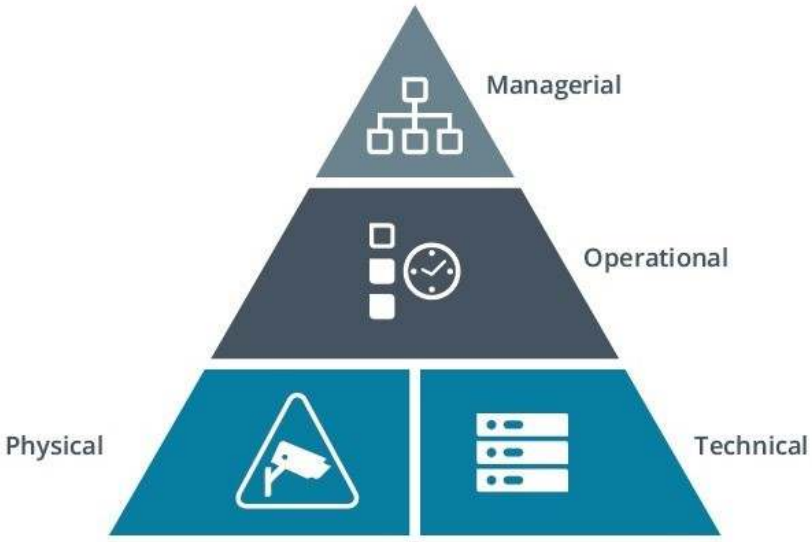
Jamstvo informacijske sigurnosti i kibernetičke sigurnosti postiže se implementacijom sigurnosnih kontrola. Identificiranjem osnovnih kategorija kontrola i tipova funkcija koje kontrole mogu imati, bit ćete u boljem položaju za prepoznavanje praznina u sigurnosnom položaju vaše organizacije.

Kategorije sigurnosnih kontrola

Jamstvo informacijske i kibernetičke sigurnosti obično se odvija unutar općenitog procesa upravljanja poslovnim rizicima. Sigurnosne politike i kontrole identificiraju rizike i trebale bi biti osmišljene da ih ublaže. Kontrola je svaka vrsta zaštitne mjere ili zaštite. Postoje mnogi načini razvrstavanja kontrola. Prema NIST SP 800-53, kontrole se mogu svrstati u tri kategorije:

- Upravljačke (Managerial) — kontrola pruža nadzor nad informacijskim sustavom. Primjeri mogu uključivati identifikaciju rizika ili alat koji omogućuje procjenu i odabir drugih sigurnosnih kontrola.
- Operativne (Operational) — kontrola se implementira primarno od strane ljudi. Na primjer, zaštitari i programi obuke su operativne kontrole.
- Tehničke (Technical) — kontrola je implementirana kao sustav (hardver, softver ili firmware). Na primjer, vatrozidi, antivirusni softver i modeli kontrole pristupa OS-u su tehničke kontrole.
- Fizičke (Physical) — kontrole poput sigurnosnih kamera, alarma, prolaza, brava, rasvjete i zaštitara koje odvraćaju i otkrivaju pristup prostorijama i hardveru često se stavljaju u zasebnu kategoriju od tehničkih kontrola.

Kategorije sigurnosnih kontrola.



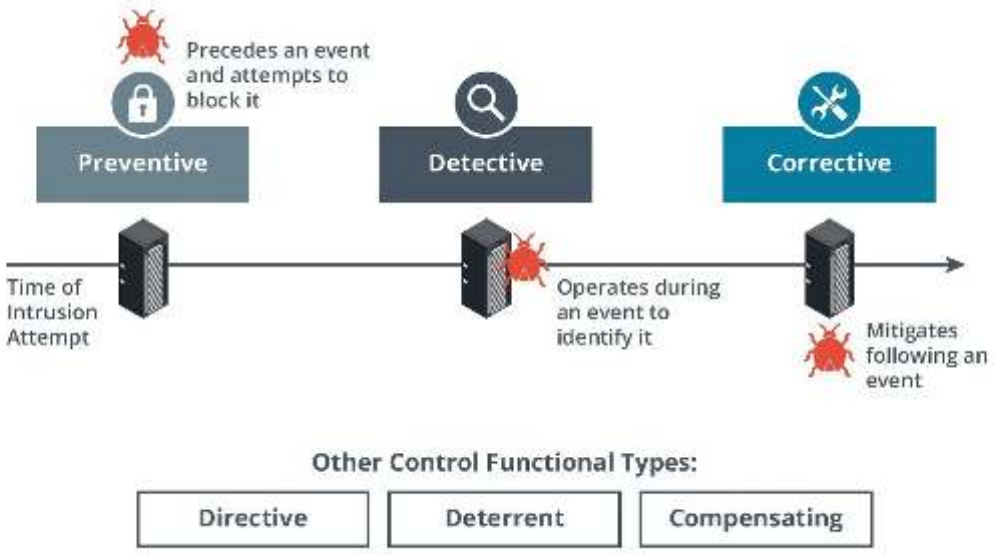
Iako koristi drugačiju shemu, budite svjesni načina na koji National Institute of Standards and Technology (NIST) klasificira kontrole u svom posebnom dokumentu (SP) 800-53. Taj dokument opisuje kontrole kao upravljačke, operativne i tehničke, dok fizičke kontrole uključuje u operativnu kategoriju.

Funkcionalni tipovi sigurnosnih kontrola

Osim kategorije, sigurnosna kontrola može se definirati prema cilju ili funkciji koji pruža:

- Preventivne (Preventive) — kontrola djeluje na uklanjanje ili smanjenje vjerojatnosti uspjeha napada. Preventivna kontrola djeluje prije nego što napad može nastupiti. Liste kontrole pristupa (ACL) konfigurirane na vatrozidima i firewall softveru su preventivna tehničke kontrole.
- Detektivne (Detective) — kontrola možda ne sprečava ili odvraća pristup, ali identificira i bilježi pokušaj ili uspješnu provalu. Detektivna kontrola djeluje za vrijeme napada. Dnevnici su jedan od boljih primjera detektivnih kontrola.
- Korektivne (Corrective) — kontrola uklanja ili smanjuje utjecaj povrede sigurnosne politike. Korektivna kontrola koristi se nakon napada. Dobar primjer je sustav sigurnosnog kopiranja koji obnavlja podatke oštećene napadom.
- Direktivne (Directive) — kontrola nameće pravilo ponašanja, kao što je politika, standard dobre prakse ili standardni operativni postupak (SOP). Na primjer, ugovor zaposlenika navodi disciplinske postupke ili uzroke za raskid ugovora.
- Odvraćajuće (Deterrent) — kontrola možda fizički ili logički ne sprečava pristup, ali psihološki odvraća napadača od pokušaja provale. To može uključivati znakove i upozorenja o pravnim kaznama za neovlašteni pristup.
- Kompenzacijske (Compensating) — kontrola je zamjena za principalnu kontrolu, kako preporučuje sigurnosni standard, i pruža isti (ili bolji) stupanj zaštite, ali koristi drugu

metodologiju ili tehnologiju. To može uključivati korištenje mrežne segmentacije kako bi samo određeni hostovimogli komunicirati jedni s drugima umjesto odvajanja hostovaFizički.



Uloge i odgovornosti u informacijskoj sigurnosti

Sigurnosna politika je formalizirana izjava koja definira kako će se sigurnost provoditi u organizaciji, sukladno poslovnim zahtjevima i ciljevima. Da bi sigurnosna politika bila učinkovita, treba biti razumljiva i primjenjiva na sve zaposlenike. Na primjer, zaposlenicima bez tehničkog znanja mora biti jasno što se od njih očekuje, ako se od njih traži da zaštite podacima s kojima rade.

- Ukupna odgovornost za IT funkciju leži na Chief Information Officer (CIO). Ta uloga može imati i izravnu odgovornost za sigurnost. Neke organizacije imenuju i Chief Technology Officer (CTO) za odgovornost za razvoj i implementaciju konkretnih tehnologija.
- U većim organizacijama, interna odgovornost za sigurnost može biti dodijeljena namjenskom odjelu kojim rukovodi Chief Security Officer (CSO) ili Chief Information Security Officer (CISO).
- Menadžeri mogu imati odgovornost za domenu, poput kontrole zgrada, web usluga ili računovodstva.
- Tehničko i stručno osoblje odgovorno je za implementaciju, održavanje i praćenje politike. Sigurnost može biti osnovna kompetencija sistemskih i mrežnih administratora, ili može postojati namjenski sigurnosni tim.
- Netehnički zaposlenici imaju odgovornost usklađivanja s politikom i relevantnim zakonodavstvom.
- Vanjska odgovornost za sigurnost (dužna pažnja ili odgovornost) leži uglavnom na direktorima ili vlasnicima, iako je važno naglasiti da svi zaposlenici dijele određenu mjeru odgovornosti. NIST-ova National Initiative for Cybersecurity Education (NICE) opisuje standardne kompetencije i uloge za cybersecurity osoblje.

Kompetencije informacijske sigurnosti

IT stručnjaci koji rade u ulozi s odgovornostima za sigurnost moraju biti kompetentni u sljedećem:

- Sudjelovati u procjenama rizika i testiranju sigurnosnih sustava i davati preporuke.
- Specificirati, pribaviti, instalirati i konfigurirati sigurne mrežne sustave.

- Pratiti sustave i istraživati sigurnosne incidente.
- Odgovarati na sigurnosne prijetnje i integrirati intel prijetnji.
- Analizirati sustave i odgovoriti na provedbu ranjivosti sustava.
- Provoditi kriminalistička ispitivanja.

Poslovne jedinice informacijske sigurnosti

Sljedeće jedinice često se koriste za predstavljanje sigurnosne funkcije unutar organizacijske strukture:

Sigurnosni operativni centar (SOC) pruža resurse i osoblje za implementaciju brze detekcije i odgovora na incidente, kao i za proaktivno praćenje i lov na prijetnje. Neki SOC-ovi operiraju 24/7 kao primarna odgovornost za sigurnost i mogu se koristiti za pružanje usluga klijentima ili partnerima. Mnoge manje organizacije ne mogu si priuštiti tim koji radi 24/7, pa umjesto toga koriste usluge upravljanog sigurnosnog pružatelja usluga (MSSP).

DevSecOps

Mrežne operacije i korištenje cloud računarstva sve više koriste automatizaciju kroz softverski kod. Tradicionalni model odvojene razvojne faze i operativne faze sve je više zamijenjen DevOps modelom gdje su razvojni i operativni timovi integrirani. Slično tome, DevSecOps model integrira sigurnosne timove u DevOps procese. Umjesto da sigurnost bude briga samo sigurnosnog tima, sigurnost postaje zajednička odgovornost svih timova.

Sažetak

Trebate moći usporediti i suprotstaviti sigurnosne kontrole koristeći kategorije i funkcionalne tipove. Trebate znati opisati sigurnosne uloge i odgovornosti. Trebate moći navesti poslovne jedinice informacijske sigurnosti, uključujući SOC, CIRT i DevSecOps. Za postizanje ovih ishoda,

razmotrite sljedeće akcije:

- Kreirajte izjavu o sigurnosnoj misiji i prateće politike koje naglašavaju važnost trijade CIA: povjerljivost, integritet, dostupnost.
- Dodijelite uloge kako bi sigurnosni zadaci i odgovornosti bili jasno razumljivi i kako bi utjecaji na sigurnost bili procijenjeni i ublaženi u cijeloj organizaciji.
- Razmotrite stvaranje poslovnih jedinica, odjela ili projekata za podršku sigurnosnoj funkciji, kao što su SOC, CIRT i DevSecOps.
- Identificirajte i procijenite zakone i industrijske propise koji nameću zahtjeve usklađenosti vašem poslovanju.
- Odaberite okvir koji odgovara zahtjevima usklađenosti i poslovnim potrebama vaše organizacije.
- Kreirajte matricu sigurnosnih kontrola koje su trenutno na snazi kako biste identificirali kategorije i funkcije — razmotrite uvođenje dodatnih kontrola za eventualne nepodudarajuće sposobnosti.
- Provedite analizu razlika kako biste procijenili sigurnosne sposobnosti u usporedbi sa zahtjevima okvira i identificirali ciljeve za razvoj dodatnih kompetencija kibernetičke sigurnosti i poboljšanje ukupnog jamstva informacijske sigurnosti.

Modul 2

Usporedba vrsta prijetnji

Pregled modula

Da biste napravili učinkovitu sigurnosnu procjenu, morate moći objasniti strategije i za obranu i za napad. Vaša odgovornost kao sigurnosnog stručnjaka uključuje razumijevanje kako napadači misle i rade, kao i razumijevanje pejzaža prijetnji relevantnog za vašu organizaciju.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Usporediti i suprotstaviti atribute i motivacije vrsta aktera prijetnji.
- Objasniti uobičajene vektore prijetnji i površine napada.
- Objasniti različite vrste ranjivosti.

Lekcija 2A

Akteri prijetnji

Pregled lekcije

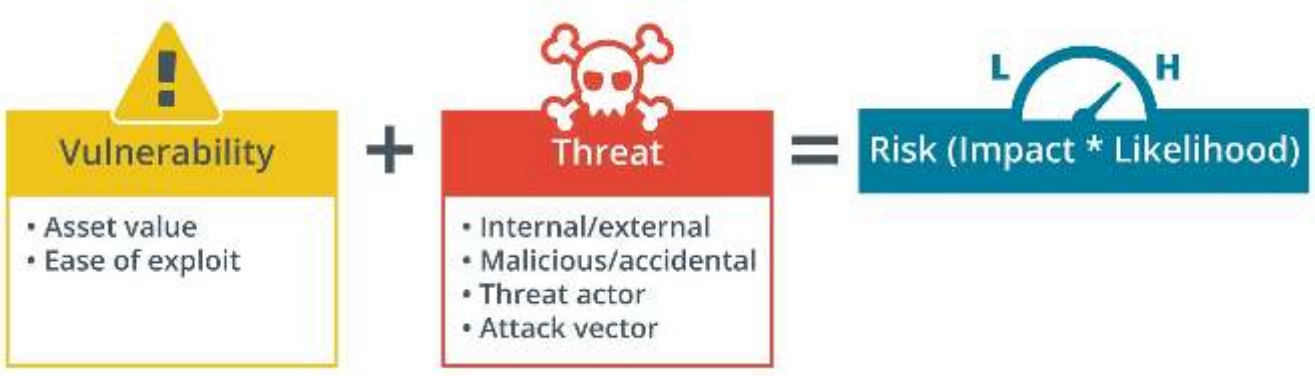
Kada procjenjujete sigurnosni položaj vaše organizacije, morate primijeniti koncepte ranjivosti, prijetnje i rizika. Rizik je ono čemu vaša organizacija pokušava upravljati implementacijom sigurnosnih kontrola. Znanje o tome tko je vjerojatno aktivan prijetnji i zbog čega napada, pomaže vam u izgradnji profila prijetnji za te grupe i identificiranju odgovarajućih kontrola.

Ranjivost, prijetnja i rizik

Sigurnosni timovi moraju identificirati načine na koje bi njihovi sustavi mogli biti napadnuti. Ove procjene obično uzimaju u obzir sljedeće pojmove:

- Ranjivost je slabost koja bi mogla biti slučajno pokrenuta ili namjerno iskorištena kako bi se uzrokovalo kršenje sigurnosti. Primjeri ranjivosti uključuju neispravno konfiguriran ili instaliran hardver ili softver, propuste u poslovnim procesima, ljudsku pogrešku i nesvjesnost.
- Prijetnja je potencijal da neka osoba ili stvar iskoristi ranjivost i naruši sigurnost. Prijetnja može imati namjernu motivaciju ili biti nenamjerna. Osoba ili stvar koja predstavlja prijetnju naziva se akter prijetnje ili prijetnja agent. Prijetnja postaje incident kada je ranjivost aktivno iskorištena od strane aktera prijetnje.
- Rizik je razina opasnosti koju predstavljaju ranjivosti i prijetnje. Kada se identificira ranjivost, rizik se izračunava kao vjerojatnost njenog iskorištavanja od strane aktera prijetnje i utjecaj koji bi uspješan napad imao na organizaciju.

Odnos između ranjivosti, prijetnje i rizika.



Atributi aktera prijetnji

Povijesno gledano, tehnike kibernetičke sigurnosti oslanjale su se na identifikaciju statičnih poznatih prijetnji — npr. poznatih potpisa malwarea ili popisa IP adresa koje treba blokirati. Međutim, ovo je reaktivni pristup koji ne funkcionira dobro protiv prijetnji visokih sposobnosti. Danas se kibernetička sigurnost temelji na konceptu inteligencije prijetnji (Threat Intelligence — TI), koji akter prijetnje s taktikama, tehnikama i procedurama (TTP) koje koriste stavlja u središte analize.

Motivacije aktera prijetnji

Motivacija je razlog aktera prijetnje za izvođenje napada. Zlonamjerni akter prijetnje može biti motiviran nizom ciljeva. Svaki cilj može biti postignut korištenjem jedne ili više strategija:

- Prekid usluge — sprječava organizaciju od normalnog rada. To može uključivati napad na njihovu web stranicu ili korištenje malwarea za blokiranje pristupa poslužiteljima i radnim stanicama zaposlenika. Prekid usluge može biti cilj sam po sebi, koji akter prijetnje može koristiti za ucjenu ili iznudu.
- Eksfiltracija podataka — prenosi kopiju neke vrste vrijednih informacija s računala ili mreže bez odobrenja. Akter prijetnje može izvesti ovu vrstu krađe jer želi podatkovnu imovinu za sebe (npr. poslovne tajne) ili za preprodaju trećoj strani (npr. osobne podatke kupaca koji se mogu upotrijebiti za prijevaru).
- Dezinformacija — krivotvorenje neke vrste pouzdanog resursa, kao što je promjena sadržaja web stranice, manipuliranje tražilicama za ubacivanje lažnih stranica, ili korištenje botova za objavljivanje lažnih informacija na društvenim mrežama.

Kaotične motivacije

U ranim danima Interneta, mnogi napadi prekida usluge i dezinformacija počinjeni su iz kaotičnih razloga. Akter prijetnje motiviran kaosom jednostavno želi remetiti i oštetiti bez specifičnog cilja.

- Ucjena (Blackmail) je zahtjev za plaćanjem kako bi se spriječilo objavljivanje informacija. Akter prijetnje možda je ukrao informacije ili kreirao lažne podatke koji izgledaju kao da je meta počinila zločin.
- Iznuda (Extortion) je zahtjev za plaćanjem kako bi se spriječio ili zaustavio napad. Na primjer, akter prijetnje možda je koristio malware za blokiranje pristupa računalima organizacije i zahtijeva plaćanje za njihovo otključavanje.
- Prijevara (Fraud) je krivotvorenje evidencija. Unutarnja prijevara može uključivati manipulaciju računima radi pronevjere sredstava ili izmišljanje podataka o kupcima

radi pranja novca.

- Zaposlenik koji djeluje kao zviždač zbog etičke zabrinutosti u vezi s ponašanjem organizacije ili koristi nedopušteno ponašanje za prikupljanje informacija radi zviždaštva.
- Kampanjska grupa koja remeti usluge organizacije za koju smatraju da djeluje suprotno njihovim etičkim ili filozofskim uvjerenjima.
- Nacionalna država koja koristi prekid usluge, eksfiltraciju podataka ili dezinformacije protiv vladinih organizacija ili tvrtki u drugoj državi u svrhu ratnih ciljeva. Nacionalne države obično perpetuiraju espionažu.

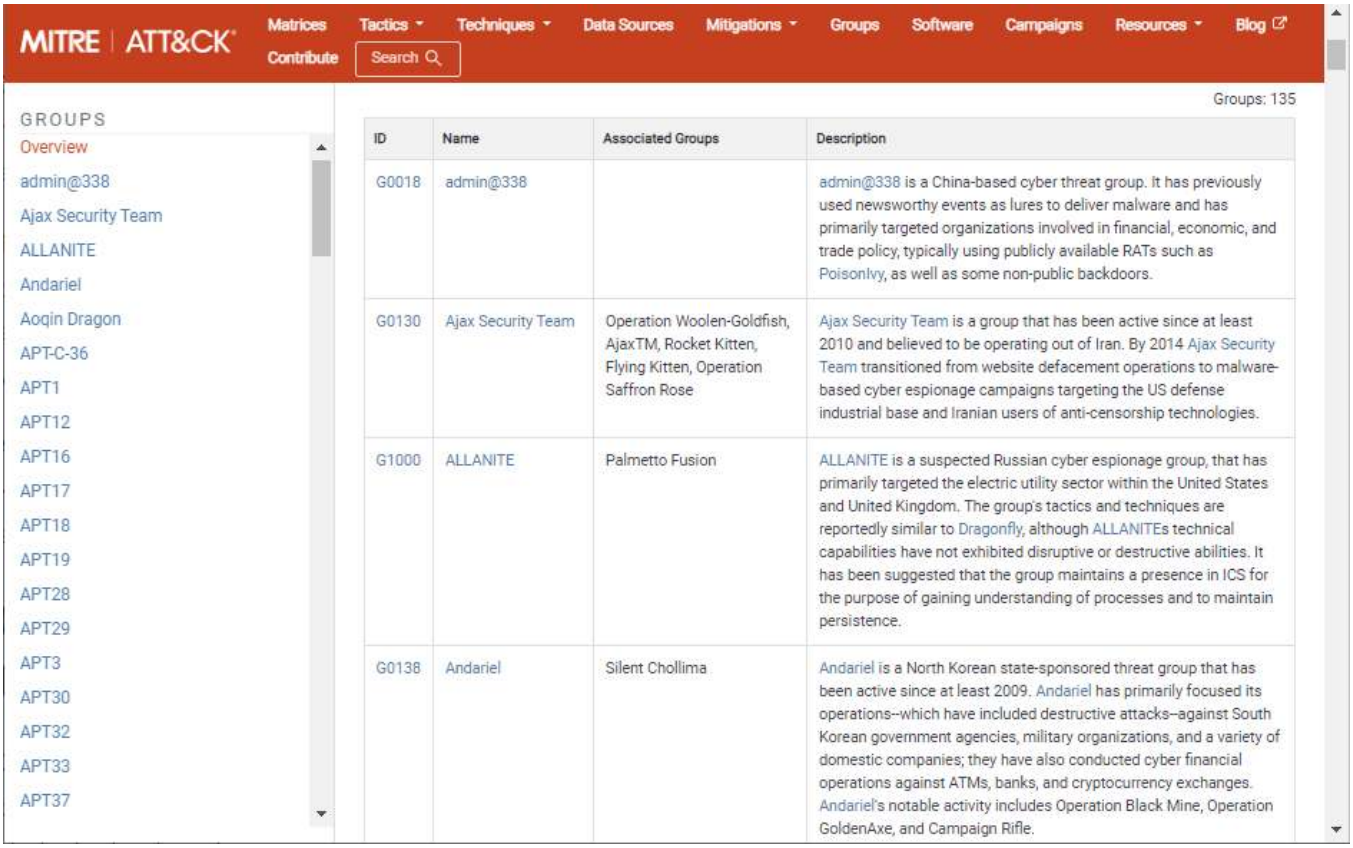
Hakeri i haktivisti

Uz opću svijest o strategijama i motivacijama, može biti korisno procijeniti aktere prijetnji prema profilu ili tipu. Ovaj profil identificira koji tipo napadača bi mogli biti prijetnja organizaciji. Hakeri su akteri prijetnji koji koriste computer i mrežne vještine za izvođenje napada koji ugrožavaju dostupnost, integritet ili povjerljivost podataka.

ali grupe za zagovaranje okoliša i životinja mogu ciljati tvrtke u širokom spektru industrija.

Akteri nacionalnih država

Većina nacionalnih država razvila je stručnost u kibernetičkoj sigurnosti i koristit će kibernetičko oružje za postizanje vojnih i političkih ciljeva. Ove sposobnosti se brzo šire i razvijaju. Nation-state akteri obično su pod pokroviteljstvom obrambenih ili obavještajnih agencija. Mogu djelovati pod krinkom regularnih vojnih i obavještajnih aktivnosti ili mogu sponzorirati neovisne akter prijetnji u kriminalnim skupinama ili haktivističkim skupinama.



Državni akteri radit će po principu duge ruke od nacionalne vlade, vojske ili sigurnosne službe koja ih sponzorira i plaća. Obično će biti registrirani kao privatna tvrtka. Okvir MITRE ATT&CK identificira poznate taktike i tehnike koje koriste različite grupe aktera

prijetnji.

Organizirani kriminal i konkurenti

U mnogim zemljama, kibernetički kriminal premašio je fizički kriminal po broju incidenata, po vrijednosti ukradene imovine i po troškovima koje nameće žrtvama. Ovo je potaknuto organiziranim kriminalnim skupinama koje provode sofisticirane napade koji im donose profit. Organizirane kriminalne grupe mogu provoditi sve poznate vrste kibernetičkih napada.

Interni akteri prijetnji

Mnogi akteri prijetnji djeluju izvana iz mreža koje napadaju. Eksterni akter mora provaliti ili inače zadobiti pristup. Interni akter prijetnje ima pristup (fizički ili logički) imovini organizacije ili ga lako može steći. Interni akteri mogu biti zaposlenici, bivši zaposlenici ili poslovni partneri koji zloupotrebljavaju svoje ovlaštene privilegije. Interni akteri prijetnji mogu raditi iz financijskih razloga, iz neke osobne ljutnje ili nezadovoljstva, ili jer su primorani od strane stranih sila.

Lekcija 2B

Površine napada

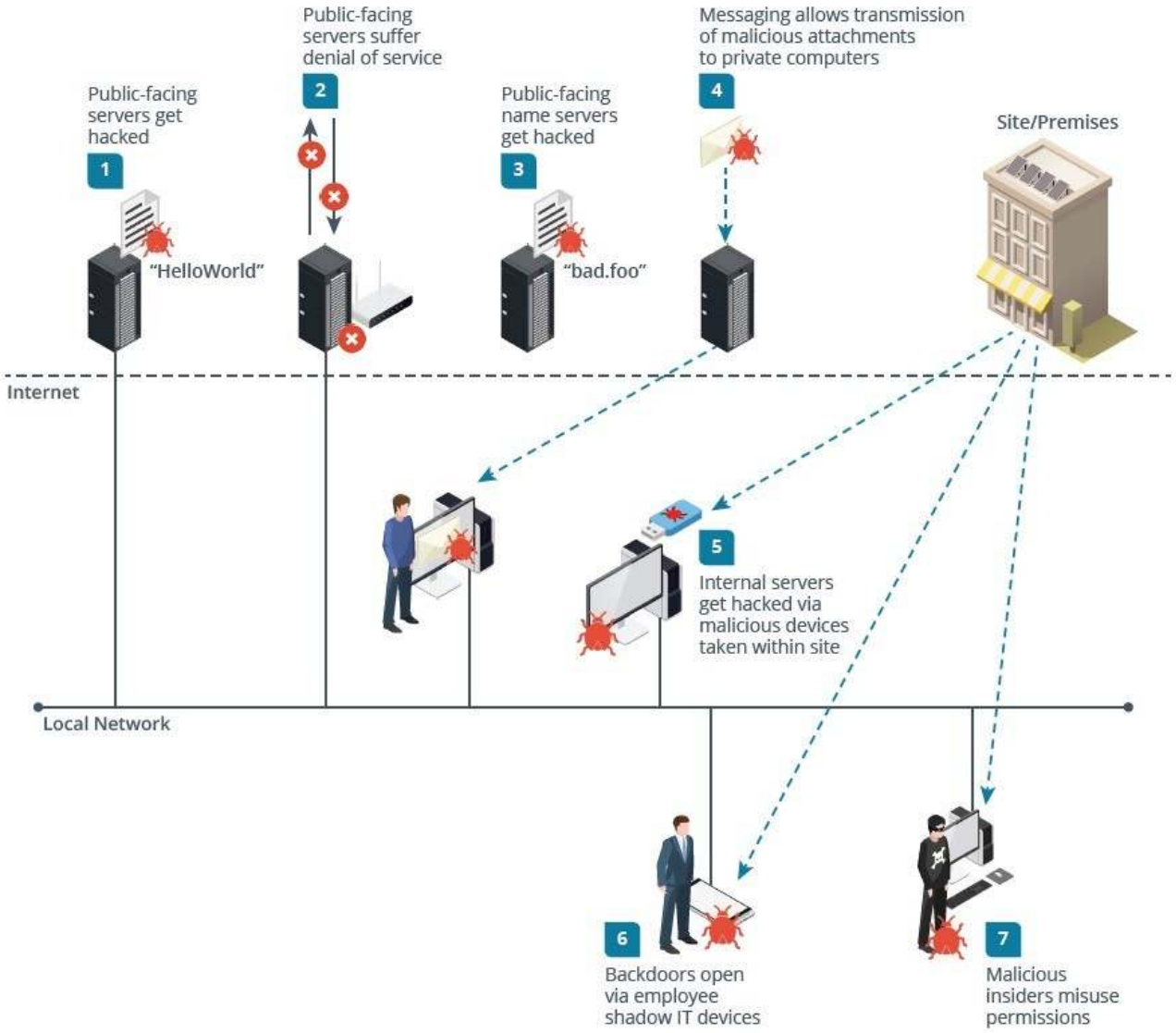
Pregled lekcije

Razumijevanje metoda kojima akteri prijetnji infiltriraju mreže i sustave ključno je za vašu sposobnost procjene površine napada i identificiranja prikladnih sigurnosnih kontrola. U ovoj lekciji istražit ćete koncepte koji vam pomažu u prepoznavanju površina napada i vektora prijetnji.

Površina napada i vektori prijetnji

Površina napada su sve točke u kojima bi zlonamjerni akter prijetnje mogao pokušati iskoristiti ranjivost. Vektor prijetnje (ili vektor napada) je specifična metoda koju akter prijetnje koristi za iskorištavanje ranjivosti na površini napada.

Procjena površine napada.



Organizacija ima ukupnu površinu napada. Možete procjenjivati površine napada i u užim opsegima, poput onog jednog poslužitelja ili računala, web aplikacije, ili identiteta i pristupnih prava zaposlenika. U nastavku su opisane ključne kategorije vektora napada koje treba procijeniti.

Ranjivi softverski vektori

Ranjivi softver sadrži grešku u kodu ili dizajnu koja se može iskoristiti za zaobilaženje kontrole pristupa ili rušenje procesa. Obično se ranjivosti mogu iskoristiti samo u određenim uvjetima koji su napadaču dostupni. Sigurnosna zakrpa (patch) ažurira softverski kod kako bi uklonila ranjivost. Primjena zakrpa naziva se upravljanje zakrpama (patch management).

Mrežni vektori

Ranjivi softver daje akteru prijetnje mogućnost izvođenja zlonamjernog koda na sustavu. Da bi to učinio, akter prijetnje mora biti u mogućnosti pokrenuti exploit kod na sustavu ili putem mreže. Vektori mrežnog eksploatiranja dijele se na udaljene i lokalne:

- Udaljeni (Remote) znači da se ranjivost može iskoristiti slanjem koda meti putem mreže i ne ovisi o autentificiranoj sesiji sa sustavom za izvođenje.

- Lokalni (Local) znači da exploit kod mora biti pokrenut iz autentificirane sesije na računalu. Napad se ipak može odvijati putem mreže, ali akter prijetnje treba koristiti valjane vjerodajnice ili preuzeti postojeću sesiju da bi ga izveo.

Da bi se minimizirali rizici od softverskih ranjivosti, administratori moraju smanjiti površinu napada uklanjanjem nesigurnih mreža. Nesigurna mreža je ona kojoj nedostaju atributi povjerljivosti, integriteta ili dostupnosti:

- Nedostatak povjerljivosti — akteri prijetnje mogu prisluškivati mrežni promet i dohvatiti lozinke ili druge osjetljive informacije. Ovi se napadi nazivaju i napadima prisluškivanja (eavesdropping).
- Nedostatak integriteta — akteri prijetnje mogu priključiti neovlaštene uređaje. To se može koristiti za prisluškivanje prometa ili njegovo presretanje i izmjenu, pokretanje lažnih servisa i aplikacija, ili izvođenje exploit koda protiv drugih mrežnih hostova. Ovi napadi često se opisuju kao napadi na putu (on-path attacks).
- Nedostatak dostupnosti — akteri prijetnje mogu izvoditi napade ometanja usluge.

Ako akter prijetnje ne može steći dovoljan pristup za direktno pokretanje udaljenog ili lokalnog exploita, mamac može prevariti korisnika da olakša napad. Sljedeći mediji se uobičajeno koriste kao mamci:

- Prenosivi uređaj (Removable Device) — napadač skriva malware na USB memorijskom pogonu ili memorijskoj kartici i pokušava prevariti zaposlenike da povežu medij s PC-om, laptopom ili pametnim telefonom. Za neke exploite, samo spajanje medija može biti dovoljno za pokretanje malwarea. Tipičnije, napadač će konstruirati zanimljiv naziv datoteke kako bi naveo korisnika da je otvori.
- Izvršna datoteka (Executable File) — akter prijetnje skriva exploit kod u programskoj datoteci. Jedan primjer je Trojanac (Trojan Horse malware). Trojanac je program koji izgleda kao nešto besplatno, korisno ili zabavno, ali zapravo sadrži proces koji će stvoriti backdoor pristup računalu akteru prijetnje.
- Dokumentne datoteke (Document Files) — akter prijetnje skriva zlonamjerni kod ugrađivanjem u datoteke dokumenata, kao što su PDF ili Office datoteke, koji se pokreće kada korisnik otvori dokument.

Najmoćniji exploiti su zero-click. Većina exploit koda u datotekama mora namjerno otvoriti korisnik. Zero-click znači da samo primanje privitka ili pregled slike na web stranici dovodi do kompromitacije. Ovi exploiti ciljaju ranjivosti u softveru koji prikazuje sadržaj, poput preglednika, media playera ili preglednika dokumenata.

Površina napada lanca opskrbe

Lanac opskrbe (supply chain) je end-to-end proces dizajniranja, proizvodnje i distribucije roba i usluga kupcima. Umjesto direktnog napada na metu, akter prijetnje može ciljati jedan od dobavljača u lancu opskrbe:

- Dobavljač (Supplier) — nabavlja proizvode direktno od proizvođača za prodaju u bulk drugim poduzećima. Ovakav tip trgovine naziva se poslovanjem između tvrtki (B2B).
- Prodavač (Vendor) — nabavlja proizvode od dobavljača za prodaju maloprodajnim poduzećima (B2B) ili direktno kupcima (B2C). Prodavač može dodati određenu razinu prilagodbe i izravnu podršku.

Lekcija 2C

Socijalni inženjering

Pregled lekcije

Ljudi

zaposlenici, ugovaratelji, dobavljači i kupci — predstavljaju dio površine napada svake organizacije. Zajednički se nazivaju ljudskim vektorom. Osoba s dozvolama na mreži predstavlja vektor napada koji akteru prijetnje omogućuje zaobilaženje svih tehničkih sigurnosnih mjera. Napadi koji koriste lažne identitete i obmanu za iskorištavanje ovog vektora zovu se socijalni inženjering (social engineering).

Ljudski vektori

Protivnici mogu koristiti raznolik raspon tehnika za kompromitaciju sigurnosnog sustava. Preduvjet za mnoge vrste napada je pribavljanje informacija o mreži i sigurnosnom sustavu. Te se informacije mogu prikupiti koristeći tehnike socijalnog inženjeringa. Primjeri socijalnog inženjeringa:

- Akter prijetnje kreira izvršnu datoteku koja traži od mrežnog korisnika lozinku i bilježi što korisnik unese. Napadač zatim šalje tu izvršnu datoteku korisniku uz priču da korisnik mora otvoriti datoteku i ponovo se prijaviti na mrežu da razriješi problem s prijavom.
- Akter prijetnje kontaktira help desk pretvarajući se da je udaljeni prodajni predstavnik koji treba hitnu pomoć u pristupu mreži od kuće.

Lažno predstavljanje i pretekstualizacija

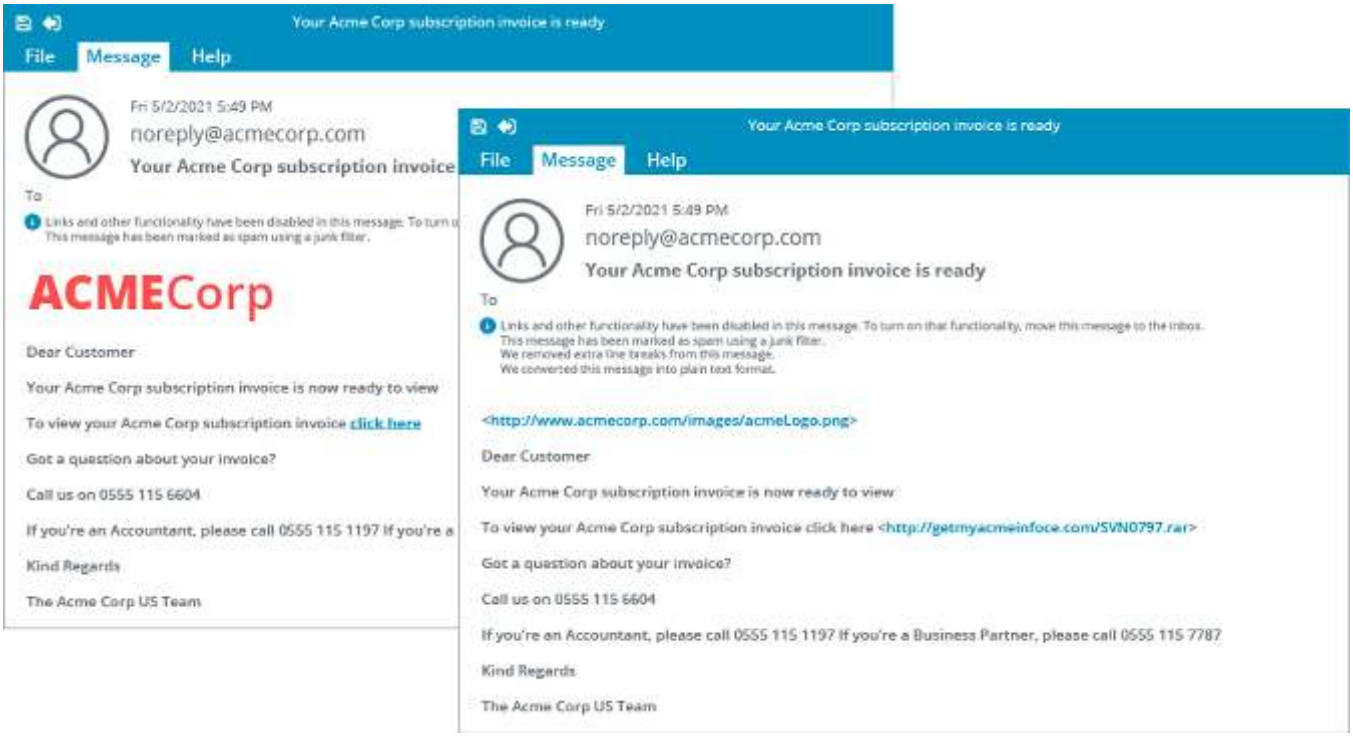
Lažno predstavljanje (impersonation) jednostavno znači pretvaranje da je netko drugi. To je jedna od osnovnih tehnika socijalnog inženjeringa. Lažno predstavljanje je moguće kada meta ne može verificirati pravi identitet napadača. Pretekstualizacija (pretexting) je specifičniji oblik lažnog predstavljanja: akter prijetnje smišlja i prezentira lažni scenarij koji uvjerava metu da su zahtjevi napadača legitimni:

- Uvjerljivo/konsenzus/sviđanje — uvjeriti metu da je zahtjev prirodan i da bi bilo nepristojno ili nekako 'čudno' odbiti ga.

- Prisila/prijetnja/hitnost — zastrašiti metu lažnim pozivanjem na autoritet ili kaznu, poput gubitka posla ili nedovoljno brzog reagiranja kako bi se spriječio neki grozan ishod. Klasični napad lažnog predstavljanja je kada socijalni inženjer nazove odjel, tvrdi da mora nešto prilagoditi i traži od zaposlenika da izvrše neke radnje ili navedu lozinku.

Akt kreiranja krivotvorene verzije web stranice za korisnike originalne web stranice kako bi ih obavijestio da moraju ažurirati račun, ili s lažnom alertom ili uzbuno, pri čemu se nudi prerušena veza koja zapravo vodi na krivotvorenu stranicu. Kada korisnik autenticira na krivotvorenu stranicu, akter prijetnje bilježi detalje.

Phishing se odnosi specifično na e-mail ili tekstualnu poruku kao vektore prijetnje. Ista vrsta napada može se izvoditi i putem drugih vrsta medija:



- Vishing — phishing napad koji se provodi putem glasovnog kanala (telefon ili VoIP). Na primjer, mete mogu biti nazvane od strane nekoga tko se predstavlja kao njihova banka, tražeći da verificiraju nedavnu transakciju i navedu sigurnosne detalje. Teže je

prepoznati sumnjive elemente u glasovnoj komunikaciji.

- SMiShing — phishing napad koji koristi SMS tekstualne poruke kao vektor. Direktne poruke jednom kontaktu imaju veliku vjerojatnost neuspjeha. Drugi tehnike socijalnog inženjeringa i dalje koriste krivotvorene resurse, poput lažnih stranica i stranica za prijavu, ali se oslanjaju na preusmjeravanje korisnika.

Typosquatting

I phishing i pharming ovise o lažnom predstavljanju da bi uspjeli. Lažna poruka ili stranica mora izgledati kao da dolazi iz izvora kojemu meta vjeruje. Akter prijetnje može koristiti različite nedosljednosti u tipkanju ili redoslijedu domene da bi stvorio uvjerljiv, ali krivotvoreni URL. Ova tehnika se naziva typosquatting ili URL hijacking.

Kompromitacija poslovnog e-maila (Business Email Compromise

BEC) — Dok je phishing tipično povezan s masovnim napadima putem e-maila, BEC se odnosi na sofisticiranu kampanju koja cilja određenu osobu u organizaciji, obično u financijama ili upravi. BEC napad može trajati tjednima ili čak i dulje, jer napadač pažljivo istražuje metu, njen uredski tijek rada i poslovne odnose. Napadač će imitirati legitimnog menadžera i koristiti phishing e-mail za preusmjeravanje financijskih transakcija ili pristup osjetljivim informacijama.

Meta napada na zalijevanje rupa (watering hole). Napadač može kompromitirati web stranicu tvrtke za dostavu pizze kako bi pokrenuo exploit kod na posjetiteljima. Na taj način mogu zaraziti računala zaposlenika e-commerce tvrtke i prodrijeti u njihovu mrežu.

Sažetak

Trebate moći objasniti kako procjenjivati vrste vanjskih i unutarnjih aktera prijetnji u smislu namjere i sposobnosti. Trebate biti u mogućnosti sažeti vektore koji čine površinu napada organizacije. Za postizanje ovih ishoda, razmotrite sljedeće akcije:

- Kreirajte profil vrsta aktera prijetnji koji predstavljaju najvjerojatnije prijetnje vašem poslovanju. Zapamtite da možete biti meta kao dobavljač nekom većem poduzeću.
- Koristite analizu poslovnih tijekova rada i inventar imovine za identifikaciju površine napada organizacije.
- Testirajte sigurnost ranjivosti softvera kontinuiranim upravljanjem zakrpama i procjenama ranjivosti.
- Testirajte sigurnost mrežnih vektora segmentacijom mreže, vatrozidima i praćenjem mrežnog prometa.
- Testirajte sigurnost ljudskog vektora kroz programe obuke i simulirane vježbe phishinga.

Modul 3

Objašnjenje kriptografskih rješenja

Pregled modula

Funkcija zaštite kibernetičke sigurnosti ima za cilj izgradnju sigurnih IT sustava za obradu koji pokazuju atribute povjerljivosti, integriteta i dostupnosti. Mnogi od tih sustava u potpunosti ili djelomično ovise o kriptografiji kao temeljnoj tehnologiji. Kriptografija se odnosi na tehnike šifriranja kojima se sačuvava tajnost i integritet informacija.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Usporediti i suprotstaviti kriptografske algoritme.
- Objasniti važnost infrastrukture javnih ključeva i digitalnih certifikata.
- Objasniti važnost korištenja odgovarajućih kriptografskih rješenja za razmjenu podataka.

Lekcija 3A

Kriptografski algoritmi

Pregled lekcije

Kriptografski algoritam su konkretne operacije koje se izvode radi kodiranja ili dekodiranja podataka. Moderni kriptografski sustavi koriste simetrične i asimetrične tipove algoritama za kodiranje i dekodiranje podataka. Uz to, kriptografski algoritmi haširanja (hash) mogu se koristiti za provjeru integriteta podataka.

Kriptografski koncepti

Kriptografija, što doslovno znači 'tajno pisanje', je vještina čuvanja informacija sigurnima kroz kodiranje. To je suprotnost od sigurnosti kroz nejasnost (security through obscurity). Sigurnost kroz nejasnost pokušava zaštititi informacije skrivajući informacije o njihovom postojanju ili lokaciji. Kriptografska terminologija:

- Otvoreni tekst (Plaintext ili Cleartext) — nešifrovana poruka.
- Šifrirani tekst (Ciphertext) — šifrirana poruka.
- Algoritam — postupak koji se koristi za šifriranje i dešifriranje poruke.
- Kriptoanaliza (Cryptanalysis) — vještina razbijanja kriptografskih sustava.
- Ključ (Key) — vrijednost koja se unosi u algoritam zajedno s podacima da bi se generirala i dekriptirala izlazna vrijednost.

Kod rasprave o kriptografiji i napadima na sustave šifriranja, uobičajeno se koristi skup likova za opisivanje različitih aktera:

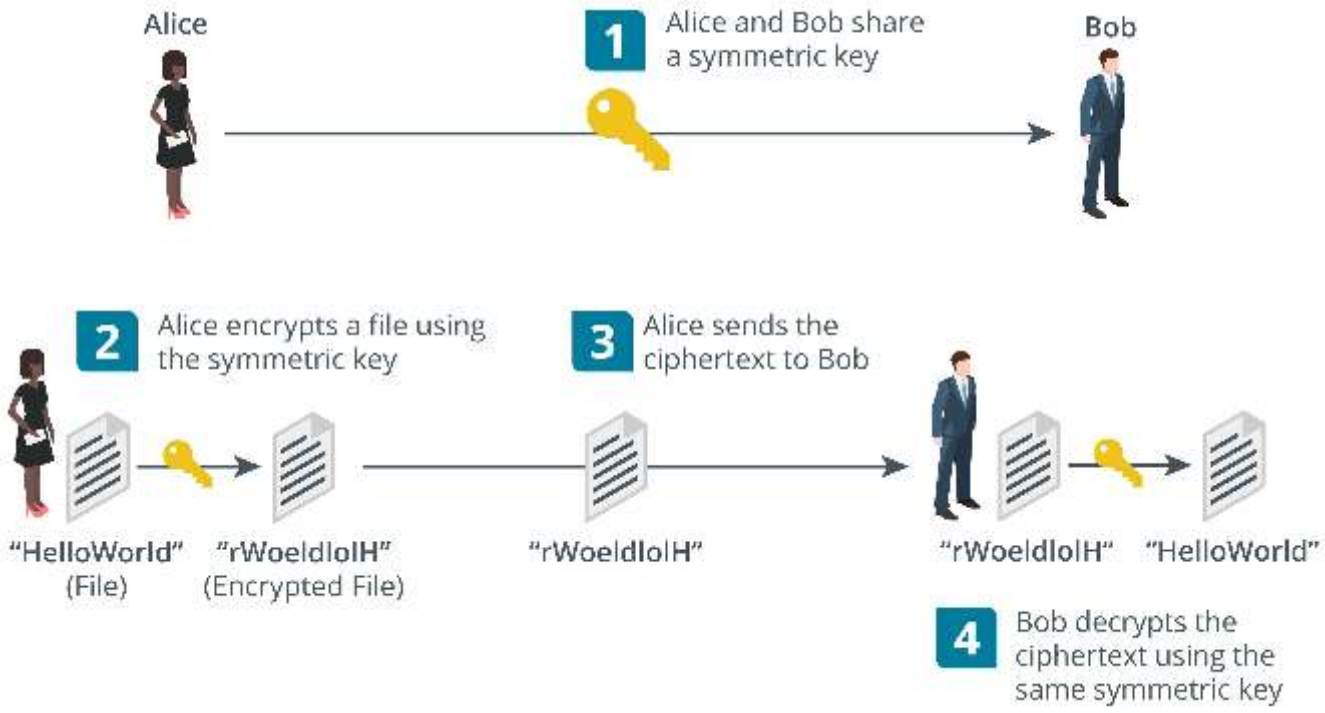
- Alice — pošiljatelj izvorne poruke.
- Bob — namjerni primatelj poruke.
- Mallory — zlonamjerni napadač koji pokušava na neki način ugroziti poruku.

Simetrično šifriranje

Algoritam šifriranja ili šifra je vrsta kriptografskog procesa koji kodira podatke kako bi se mogli pohraniti ili prenijeti sigurno, a potom dekriptirati samo od strane vlasnika ili namjeravanog primatelja. U simetričnoj kriptografiji, isti tajni ključ koristi se i za šifriranje i

za dešifriranje. To znači da isti ključ moraju znati i Alice i Bob. Simetričnog šifriranja ima više primjera, uključujući Triple DES (3DES) i Advanced Encryption Standard (AES). AES je de facto standard za simetričnu enkripciju. Postoje tri varijante: AES-128, AES-192 i AES-256, pri čemu brojevi označavaju duljinu ključa u bitovima.

Operacija simetričnog šifriranja i slabosti.



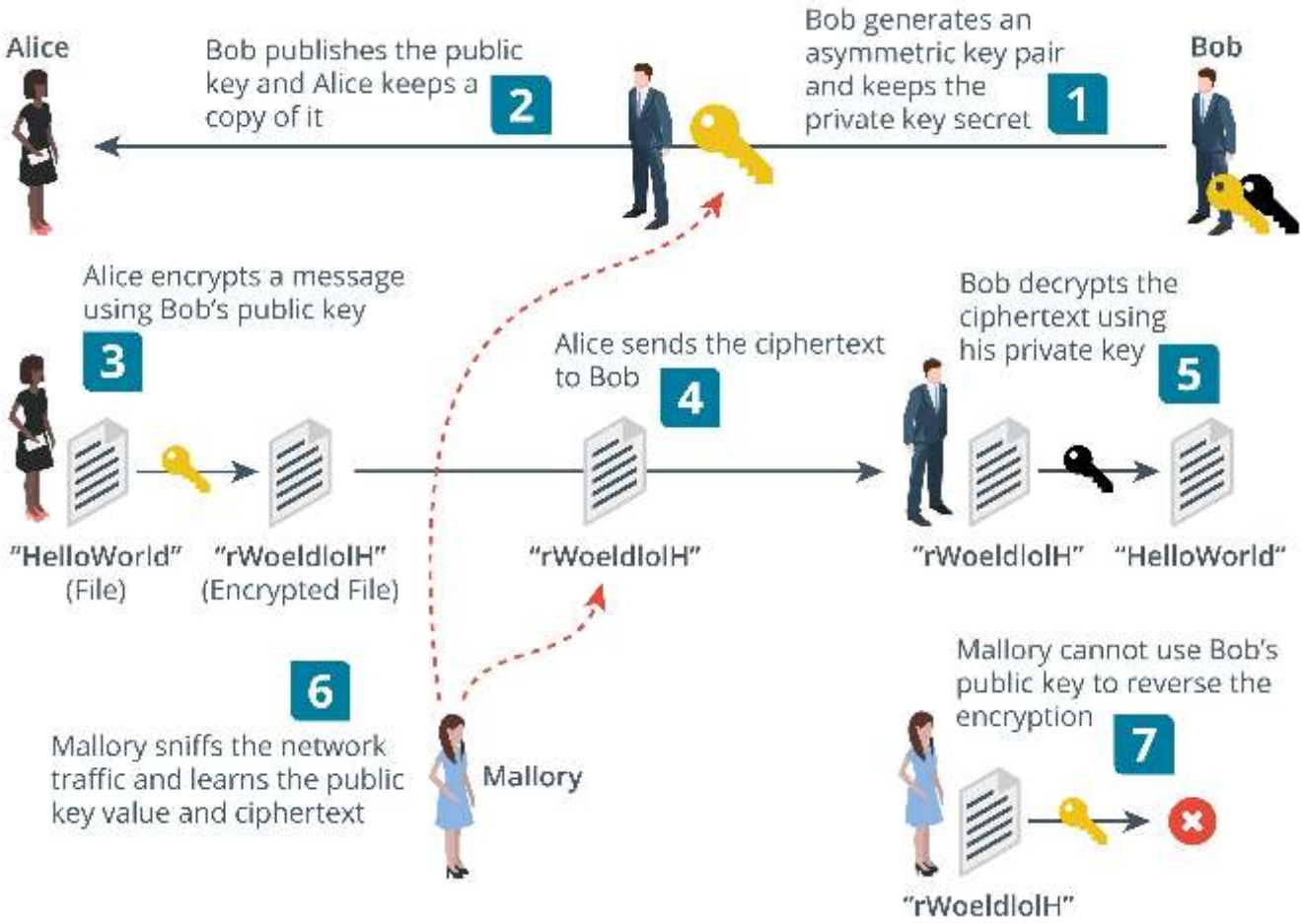
Simetrično šifriranje je vrlo brzo. Koristi se za masovno šifriranje (bulk encryption) velikih količina podataka. Glavni problem je kako Alice i Bob 'se susreću' da bi se dogovorili ili razmijenili ključ. Ako Mallory presretne ključ, može dešifrirati sve poruke koje su si razmijenili ili lažirati poruke.

Duljina ključa

Algoritmi šifriranja koriste ključ za povećanje sigurnosti procesa. Što je duljina ključa veća, to je teže provaliti šifriranje. Duljina ključa mjeri se u bitovima, a prostor ključeva (keyspace) je ukupan broj mogućih vrijednosti ključa. Na primjer, ključ od 8 bita ima prostor od 256 mogućih vrijednosti. Skup mogućih ključnih vrijednosti eksponencijalno raste s duljinom ključa.

AES-256 ima prostor ključeva od 2^256. Taj prostor nije dvaput veći od AES-128; on je mnogo bilijuna puta veći i prema tome je znatno sigurniji. U asimetričnoj enkripciji, javni i privatni ključ su matematički povezani. Asimetrična enkripcija zahtijeva dulje ključeve od simetrične da bi pružila istu razinu sigurnosti. Na primjer, RSA ključ od 2048 bita otprilike je ekvivalentan simetričnom ključu od 112 bita. Kvantna kriptografija može omogućiti rješavanje matematičkih problema koji su temelj asimetričnih kriptosustava. Kvantno sigurna kriptografija (post-kvantna kriptografija) razvija asimetrične algoritme koji su otporni na kvantno računanje.

Asimetrično šifriranje.



Koraci su sljedeći: 1. Bob generira asimetrični par ključeva i drži privatni ključ tajnim. 2. Bob objavljuje javni ključ i Alice zadržava kopiju. 3. Alice šifrira poruku Bobovim javnim ključem i šalje je Bobu. 4. Bob dekriptira poruku koristeći privatni ključ. Mallory može presresti poruku, ali je ne može dešifrirati jer nema privatni ključ. Asimetrična enkripcija rješava problem distribucije ključeva jer nema potrebe za sigurnim kanalom za razmjenu javnog ključa.

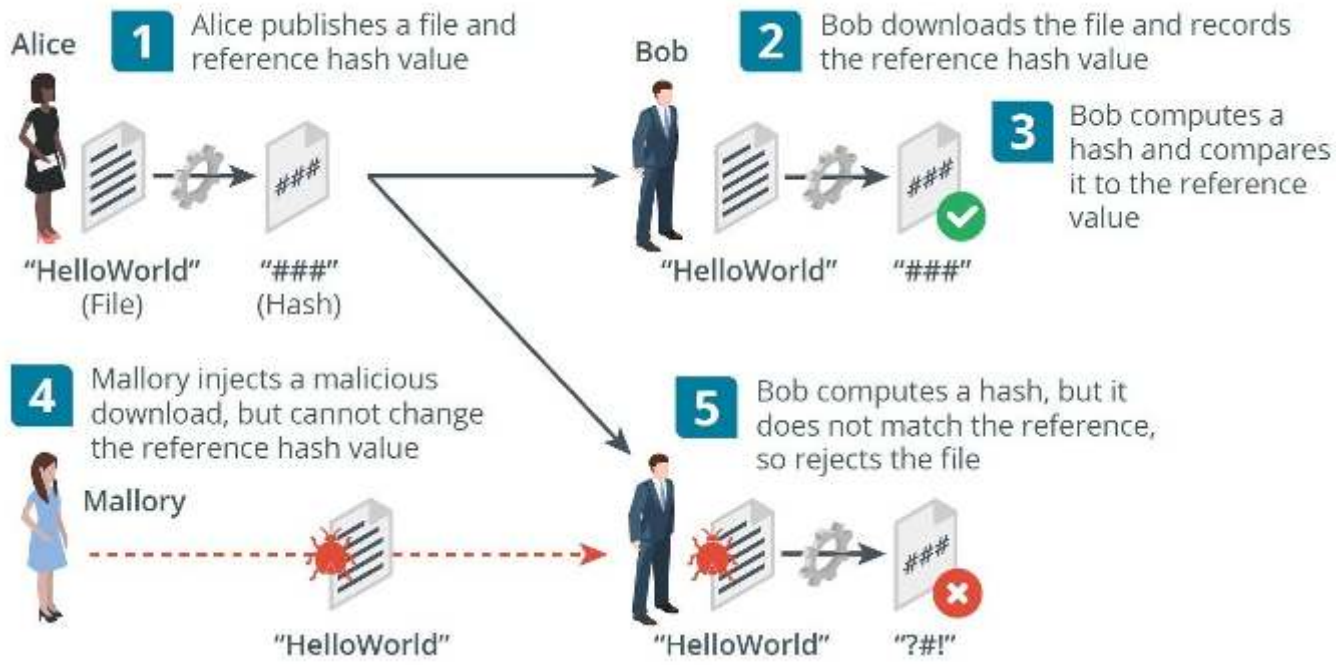
Haširanje

Kriptografski hashing algoritam proizvodi niz bitova fiksne duljine iz ulaznog otvorenog teksta koji može biti bilo koje duljine. Izlaz se može nazvati hash ili sažetak poruke (message digest). Ista ulazna vrijednost uvijek daje isti izlaz, ali izlaz uvijek izgleda nasumično i ne otkriva ništa o ulazu.

Funkcija je dizajnirana tako da je nemoguće oporaviti podatke otvorenog teksta iz sažetka (jednosmjerna) i tako da različiti ulazi vjerojatno neće dati isti izlaz (kolizija). Hashing algoritam verificira integritet poruke — ako dođe do kolizije, moguće je da se netko pokušao nasloniti na sustav i da je poruka modificirana.

Postoje dvije popularne implementacije hash algoritama:

- Sigurni hash algoritam (SHA — Secure Hash Algorithm) — smatra se najjačim algoritmom. Postoje varijante koje daju izlaze različitih veličina, pri čemu se duži sažeci smatraju sigurnijima. Najpopularnija varijanta je SHA-256, koja daje sažetak od 256 bita.

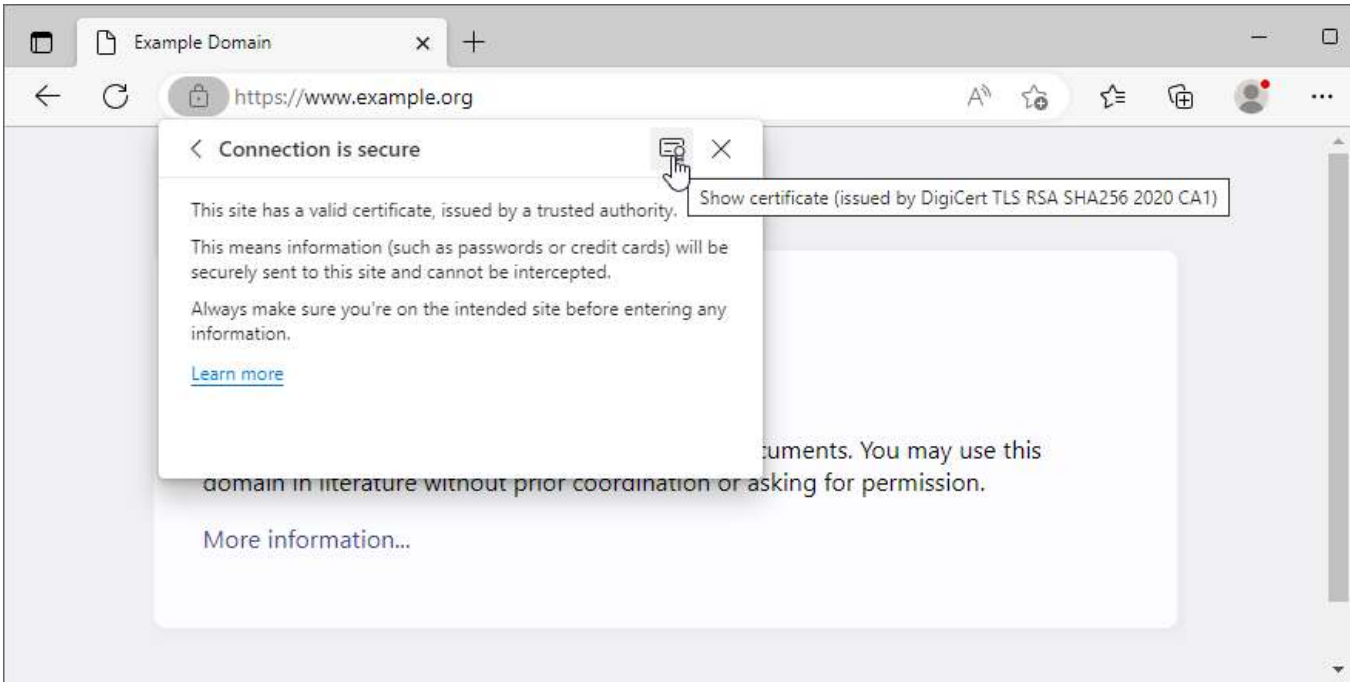


- Message Digest Algorithm #5 (MD5) — daje sažetak od 128 bita. MD5 se ne smatra sasvim sigurnim za korištenje kao SHA-256, ali može biti potreban zbog kompatibilnosti između sigurnosnih proizvoda.

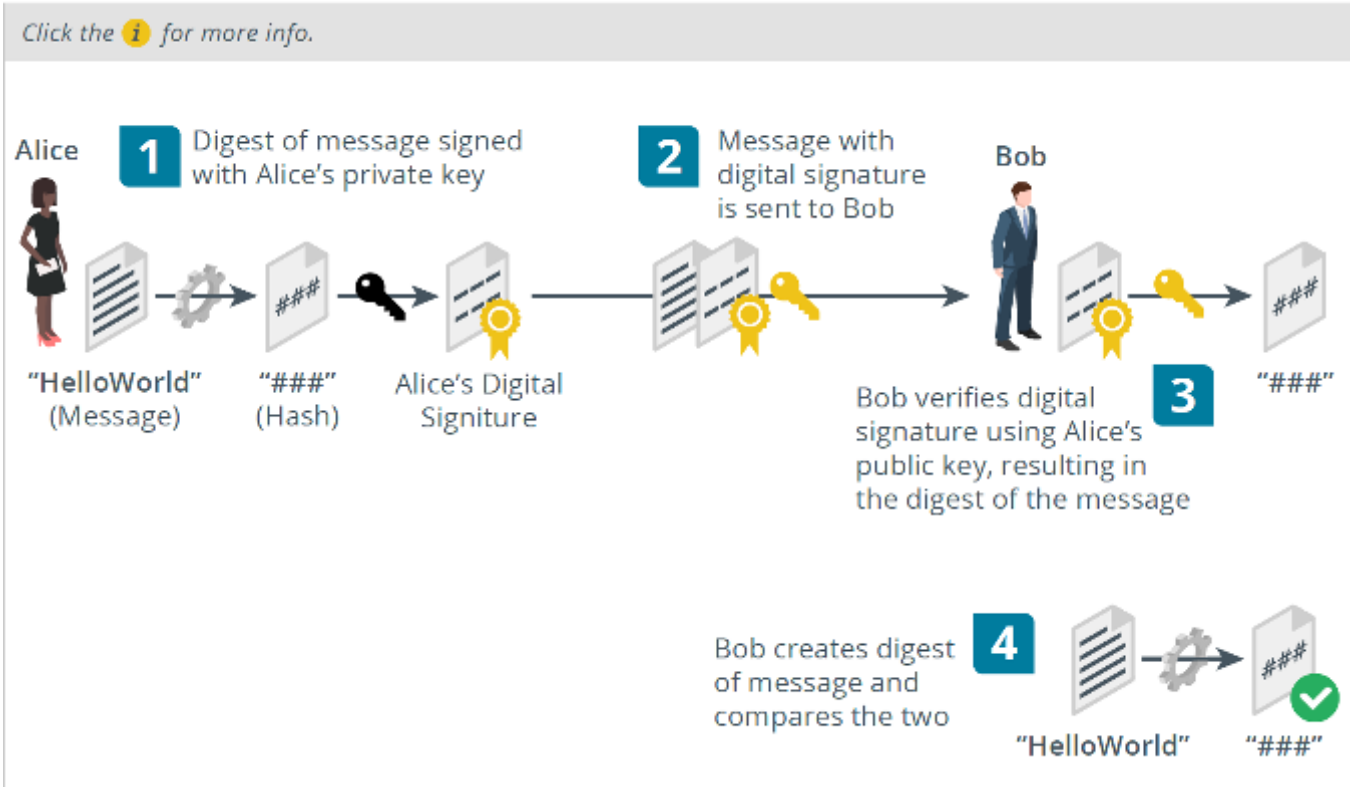
```
C:\Users\James\Downloads>fciv -sha1 "c:\users\james\documents\photo.jpg"
//
// File Checksum Integrity Verifier version 2.05.
//
baa30028bd0cac06b9d200993dda7e613c0af4e6 c:\users\james\documents\photo.jpg

C:\Users\James\Downloads>_
```

Digitalni potpisi

Jedan hash funkcija, simetrična šifra ili asimetrična šifra naziva se kriptografskim primitivom. Kompletan kriptografski sustav ili proizvod vjerojatno koristi više kriptografskih primitiva zajedno u protokolu šifriranja. Primjer je digitalni potpis koji kombinira asimetričnu enkripciju s hashingom. Kriptografija javnih ključeva može autenticirati pošiljatelja, jer oni kontroliraju privatni ključ koji proizvodi poruke na način koji nitko drugi ne može. Haširanje dokazuje integritet izračunavanjem jedinstvene poruke fiksne veličine.



Koraci za kreiranje digitalnog potpisa: 1. Pošiljatelj (Alice) kreira sažetak poruke koristeći unaprijed dogovoreni hash algoritam, kao što je SHA-256, i zatim izvodi operaciju potpisivanja na sažetku koristeći njezin odabrani asimetrični algoritar i privatni ključ. 2. Alice šalje potpisani sažetak i original poruke Bobu (i svim ostalim primateljima). 3. Bob dešifrira potpis koristeći Alicin javni ključ, otkrivajući sažetak poruke. 4. Bob izračunava sažetak primljene poruke i uspoređuje ga s dešifriranim sažetkom. Ako se podudaraju, poruka nije modificirana u prijenosu.



Postoji nekoliko standarda za kreiranje digitalnih potpisa. Public Key Cryptography Standard #1 (PKCS#1) definira korištenje RSA algoritma. Algoritam digitalnog potpisa (DSA) koristi šifru koja se zove ElGamal, a Elliptic Curve DSA (ECDSA) koristi kriptografiju

eliptičnih krivulja.

Lekcija 3B

Infrastruktura javnih ključeva

Pregled lekcije

Infrastruktura javnih ključeva (PKI

Public Key Infrastructure) je okvir koji pomaže uspostaviti povjerenje u korištenje kriptografije javnih ključeva za potpisivanje i šifriranje poruka putem digitalnih certifikata. Digitalni certifikat je paket koji sadrži javni ključ i identificira vlasnika ključa, koji odobrava tijelo za certifikaciju (CA — Certificate Authority).

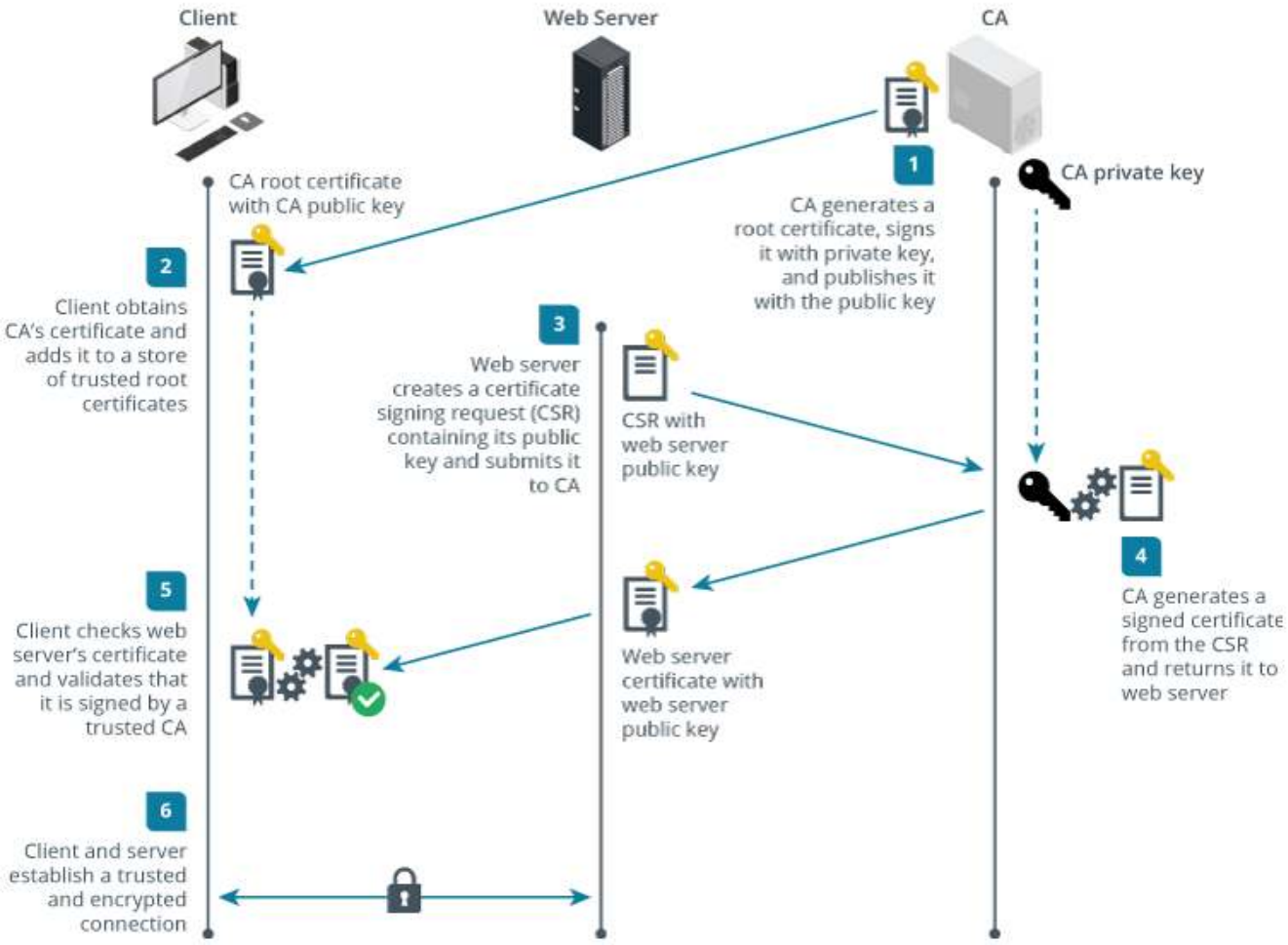
Tijela za certifikaciju

Kriptografija javnih ključeva rješava problem distribucije ključeva šifriranja kada želite sigurno komunicirati s drugima ili autenticirati poruku koju šaljete drugima. Postoje dvije uobičajene upotrebe:

- Kada želite da vam drugi šalju povjerljive poruke, date im vaš javni ključ za šifriranje poruke. Poruka se tada može dešifrirati samo vašim privatnim ključem, koji čuvate poznatim samo sebi.
- Kada se želite autenticirati drugima, potpisujete hash vaše poruke privatnim ključem.

PKI može koristiti privatna ili CA treće strane. Privatni CA se može postaviti unutar organizacije za internu komunikaciju. Certifikati koje izdaje bit će pouzdani samo unutar organizacije. Za javnu komunikaciju, korisnici često trebaju certifikate od javnog CA trećih strana (poput DigiCert, Comodo, Let's Encrypt).

Funkcije javnog CA trećih strana su sljedeće:

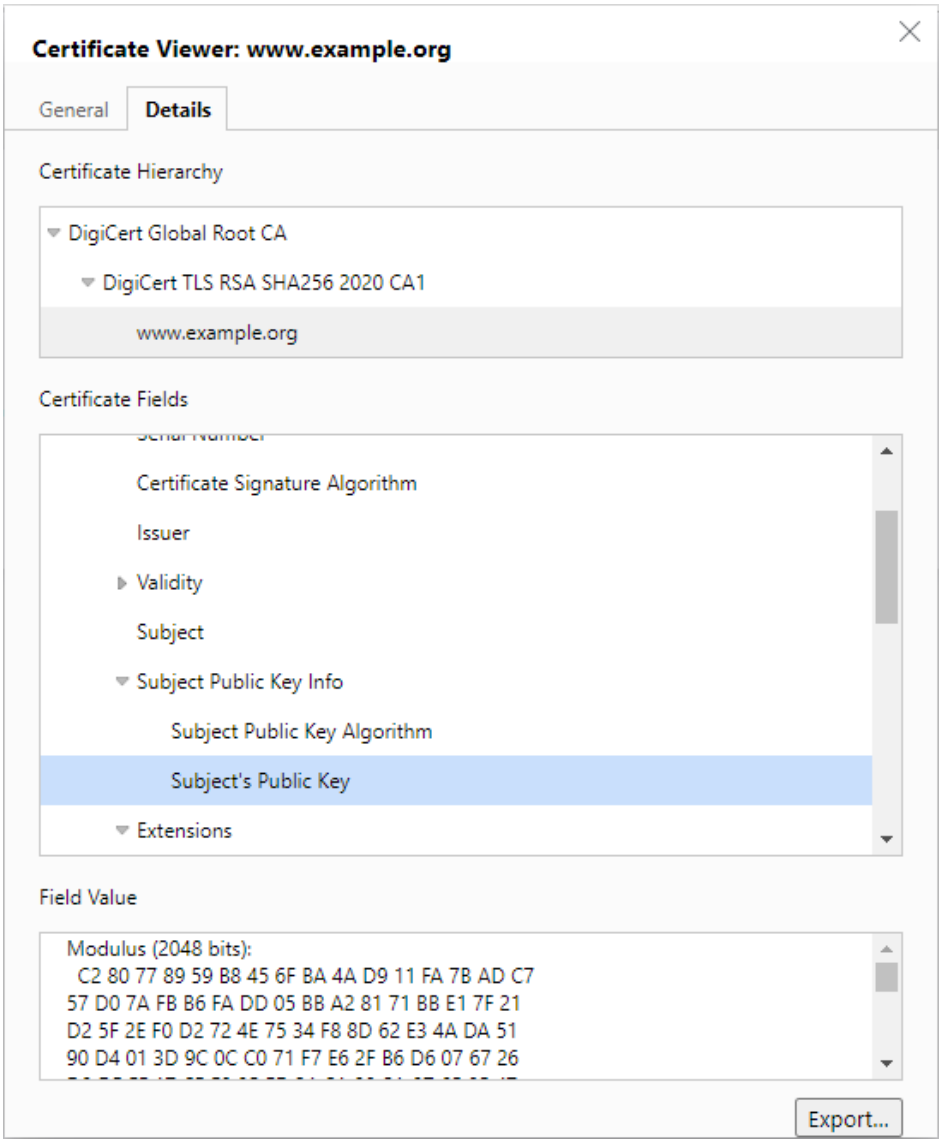


- Pružanje niza certifikacijskih usluga korisnoj zajednici korisnika koje CA opslužuje.
- Osiguravanje valjanosti certifikata i identiteta onih koji se za njih prijavljuju (registracija).
- Uspostavljanje modela povjerenja, posebno između organizacija, poput financijskih institucija.
- Upravljanje poslužiteljima (repozitorijima) koji pohranjuju i administriraju certifikate.
- Provedba upravljanja životnim ciklusom ključeva i certifikata, posebno opozivanje nevažećih certifikata.

Digitalni certifikati

Digitalni certifikat je u osnovi omotnica za javni ključ subjekta. Uz javni ključ, sadrži informacije o subjektu i izdavatelju certifikata. Certifikat potpisuje CA koji ga izdaje.

Detalji digitalnog certifikata koji prikazuju javni ključ subjekta.



Digitalni certifikati temelje se na X.509 standardu koji je odobrila Međunarodna telekomunikacijska unija i standardizirala Internet Engineering Task Force (IETF). RSA je razvio standard Public Key Cryptography Standard #10 (PKCS#10) za zahtjev za potpisivanje certifikata (CSR). Certifikati su obično u DER (Distinguished Encoding Rules) binarnom formatu, no za razmjenu se mogu kodirati u Base64 ASCII format (PEM). Digitalni certifikat sadrži:

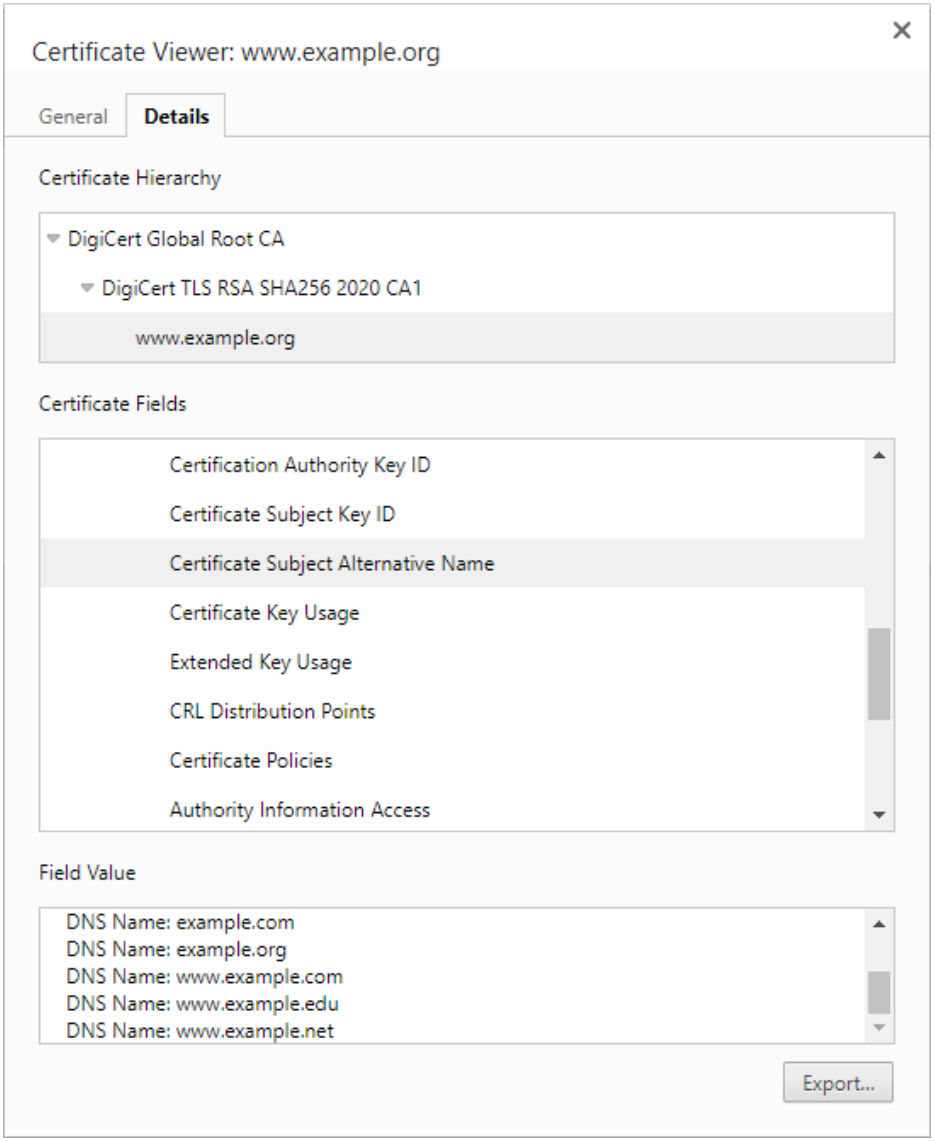
- Serijski broj i verziju X.509 certifikata.
- Informacije o predmetu (Subject) s identifikatorima poput naziva domene i organizacije.
- Rok valjanosti.
- Informacije o izdavatelju.
- Digitalni potpis izdavatelja.

Korijen povjerenja

Model korijena povjerenja (root of trust) definira kako korisnici i različiti CA-ovi mogu vjerovati jedni drugima. Svaki CA sebi izdaje certifikat. To se naziva korijenim certifikatom (root certificate). Korijeni certifikat ima najdulje trajanje od svih certifikata u PKI hijerarhiji i obično je samopotpisan (self-signed). Korijeni CA može potpisivati certifikate za

podređene (intermediate) CA-ove. Svaki podređeni CA može potpisivati certifikate krajnjih entiteta (end-entity certificates). Lanac povjerenja (chain of trust) opisuje niz CA-ova koji su potpisali certifikat sve do korijenog CA. Ovaj lanac mora biti neprekinut i svi certifikati moraju biti valjani.

Web poslužitelj za www.example.org identificira se certifikatom koji je izdao DigiCert TLS CA1 posredni CA. Certifikat posrednog CA potpisan je od strane DigiCertovog Global Root CA.



Samopotpisani certifikati

U nekim okolnostima, korištenje PKI može biti preteško ili skupo za upravljanje. Svako računalo, web poslužitelj ili programski kod može biti raspoređen sa samopotpisanim certifikatom. Na primjer, mrežni uređaji kao što su usmjerivači i preklopnici često dolaze s tvornički instaliranim samopotpisanim certifikatima koji se koriste za sigurno upravljanje uređajima. Samopotpisani certifikati mogu se koristiti i za programiranje testiranja u razvojnim okruženjima.

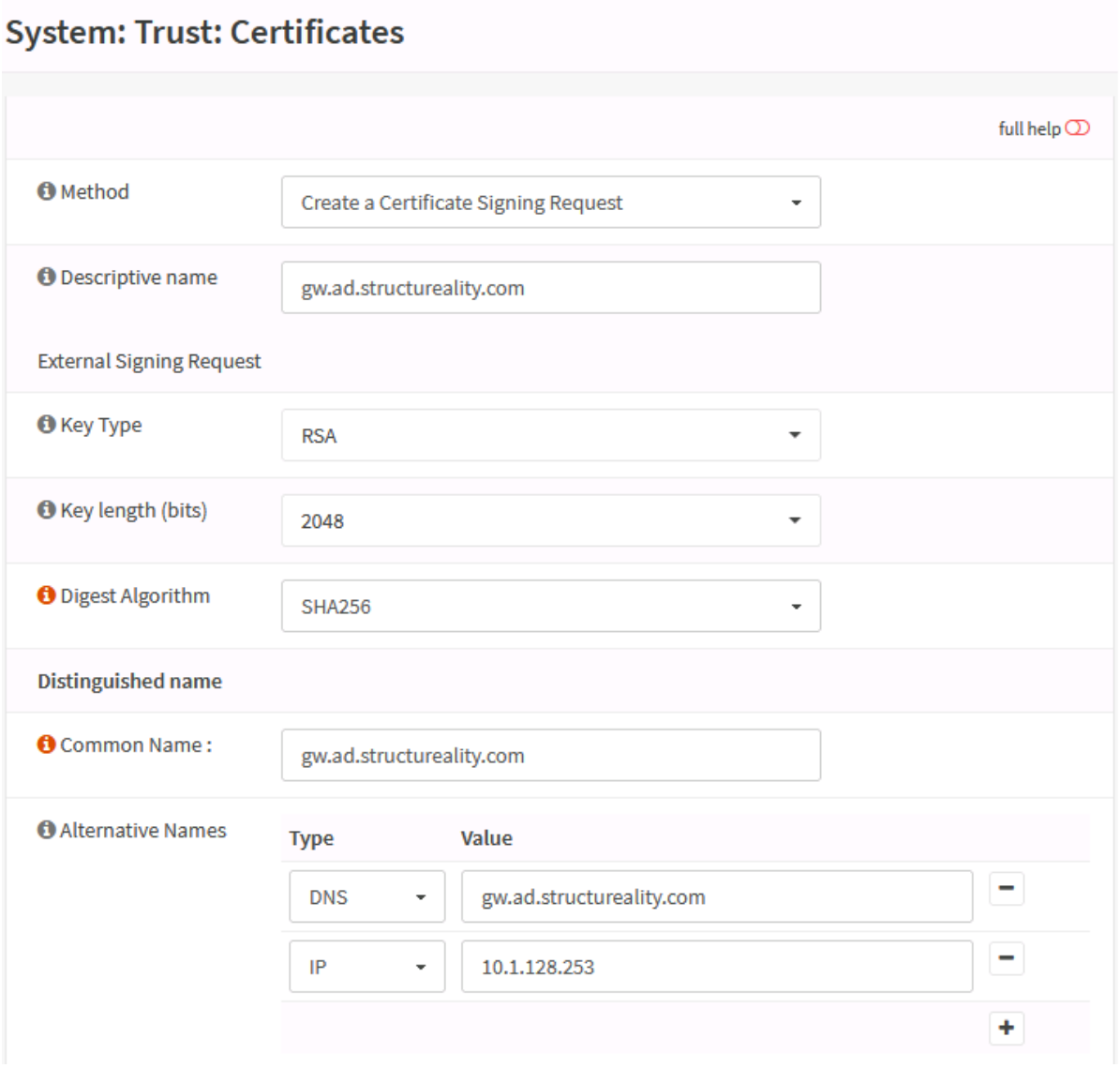
Samopotpisani certifikat. Samopotpisani certifikati mogu biti korisni i u razvojnim i testnim okruženjima. Operativni sustav ili preglednik označit će samopotpisane certifikate kao nepouzdane, ali korisnik može odabrati nastaviti ili ručno instalirati certifikat kao

pouzdan.

Zahtjevi za potpisivanje certifikata

Registracija je proces kojim krajnji korisnici kreiraju račun kod CA i postaju ovlašteni za traženje certifikata. Točni procesi kojima su korisnici ovlašteni za dobivanje certifikata ovise o pravilima CA, ali mogu uključivati registraciju putem web obrasca, osobnu provjeru identiteta ili korištenje RA (Registration Authority). Odobreni korisnik može podnijeti zahtjev za potpisivanje certifikata (CSR), koji CA zatim pregleda i, ako odobri, potpisuje certifikat i vraća ga korisniku.

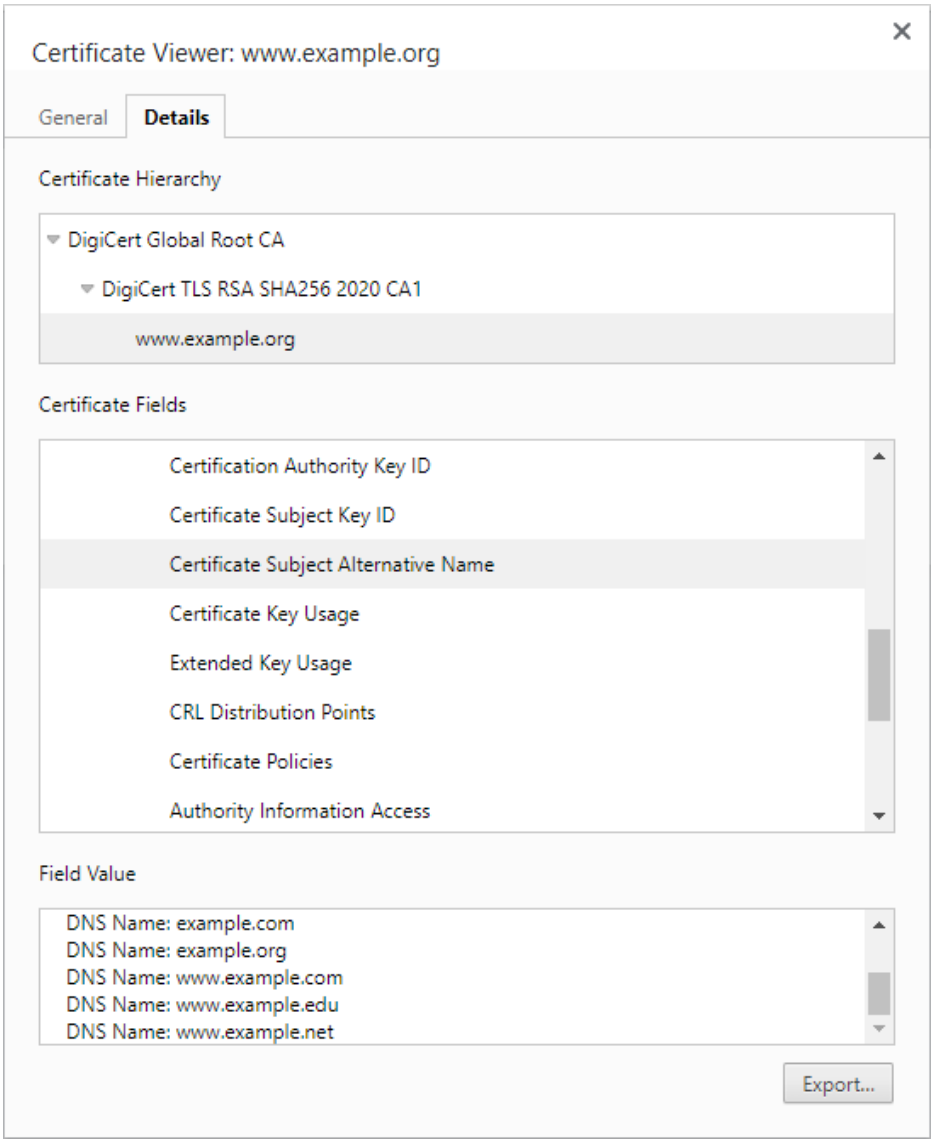
Korištenje web obrasca u vatrozidnom uređaju OPNsense za traženje certifikata. DNS i IP alternativni nazivi moraju odgovarati vrijednostima koje će klijenti koristiti za pristup web stranici.



Atributi naziva subjekta

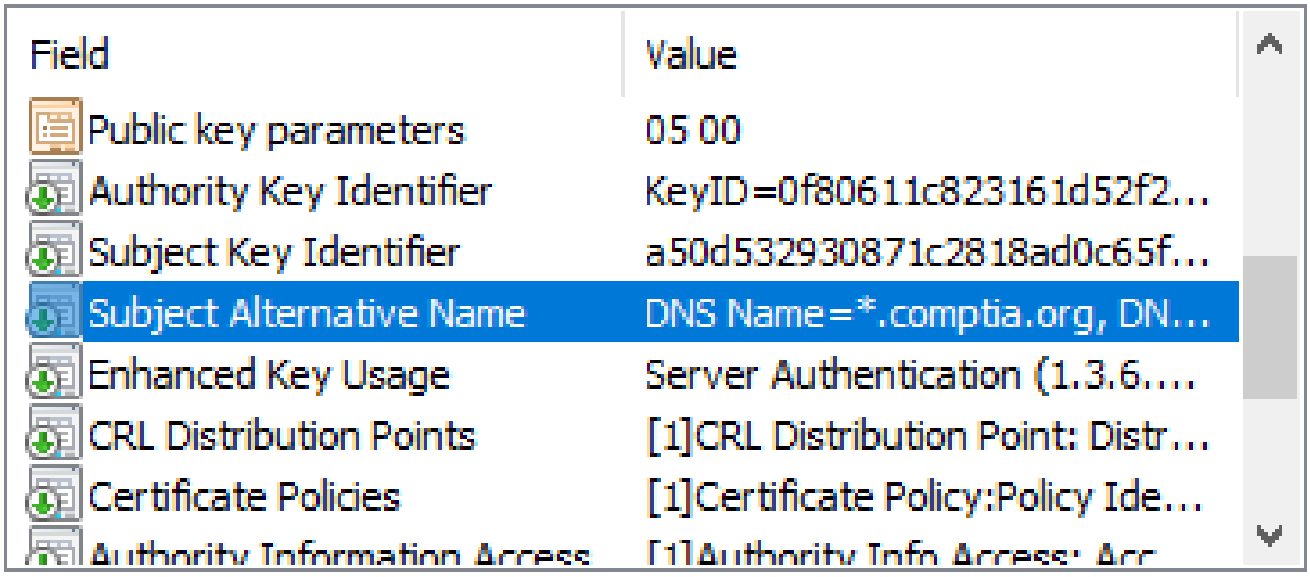
Kada su certifikati prvi put uvedeni, atribut uobičajenog imena (CN — Common Name) koristio se za identifikaciju potpuno kvalificiranog naziva domene (FQDN) kojim se pristupa poslužitelju, poput www.example.com. Trenutni standard zahtijeva korištenje polja Subject Alternative Name (SAN) za navođenje FQDN-ova koje certifikat pokriva, uz CN koji sada identifikira vlasnika certifikata.

Primjerni certifikat domene konfiguriran je s alternativnim imenima subjekta za različite domene najviše razine i poddomene.



Ipak je sigurnije staviti FQDN i u CN, jer nisu svi preglednici i implementacije ažurirani sa standardima. Certifikat koji pokriva više FQDN-ova naziva se certifikat s alternativnim imenima subjekta (SAN certifikat) ili unified communications certificate (UCC) ili multi-domain certifikat.

SAN polje također omogućuje certifikatu da predstavlja različite poddomene, poput www.comptia.org i members.comptia.org. Navođenje specifičnih poddomena je sigurnije, ali ako se doda nova poddomena, mora se izdati novi certifikat. Zamjenski certifikat (wildcard certificate) pokriva sve poddomene jedne domene, npr. *.comptia.org.

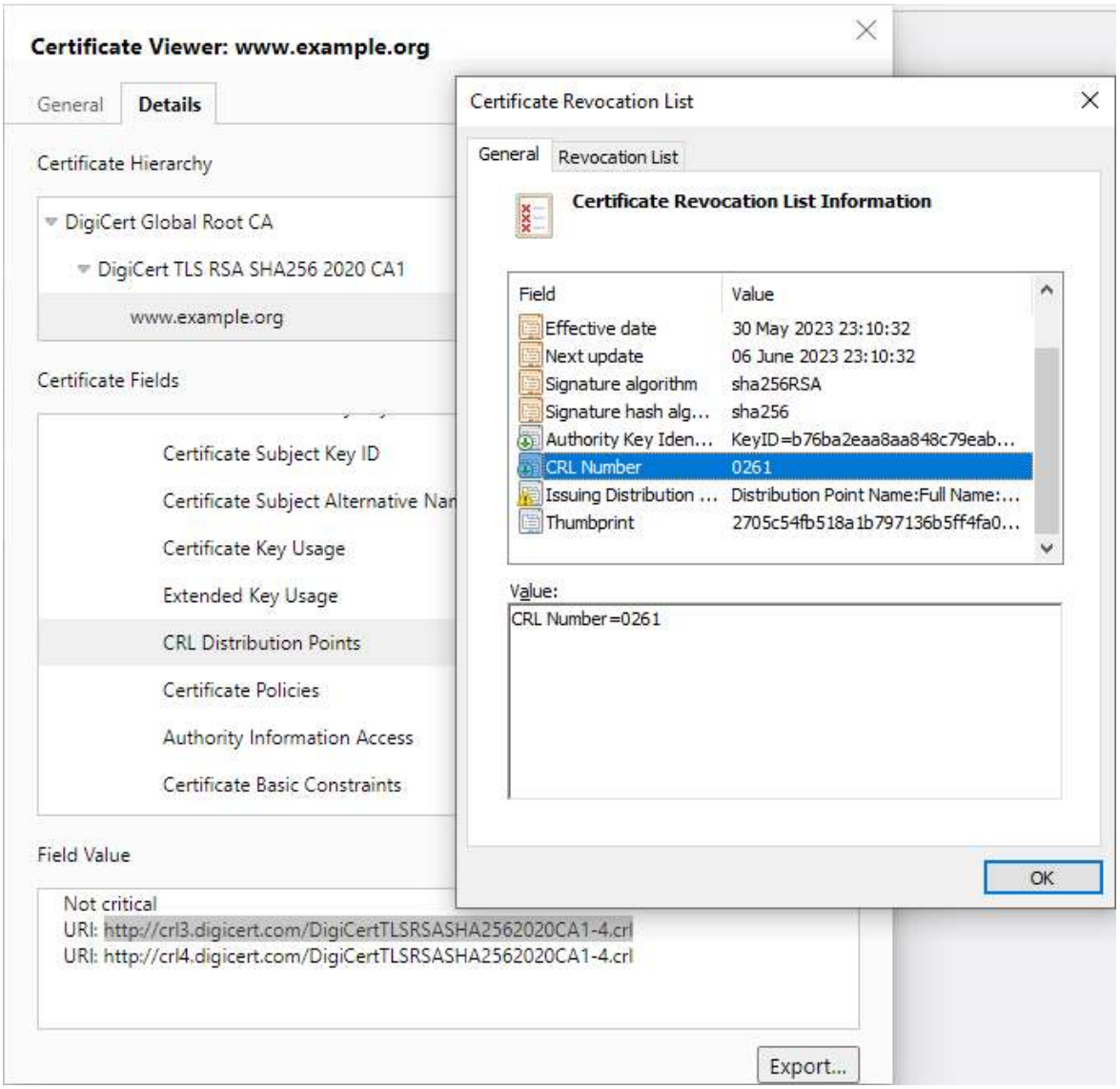


Certifikat se može opozvati ili suspendirati:

- Opoziv (revoked) certifikat više nije valjan i ne može se 'poništiti opoziva' ili vratiti.
- Suspendirani certifikat može biti ponovo omogućen.

Certifikat može biti opozvan ili suspendiran od strane vlasnika ili od CA iz više razloga. Na primjer, privatni ključ može biti kompromitiran, poslovanje može biti zatvoreno, korisnik može napustiti organizaciju ili je certifikat možda pogrešno izdan.

Mora postojati mehanizam koji korisnicima govori je li certifikat valjan, opozvan ili suspendiran. CA mora voditi popis opoziva certifikata (CRL — Certificate Revocation List) od svih opozvanih i suspendiranih certifikata. CRL se potpisuje od strane CA i distribuira korisnicima.



CRL ima sljedeće atribute:

- Razdoblje objavljivanja (Publish Period) — datum i vrijeme kada je CRL objavljen. Većina CA-ova je postavljena za automatsko objavljivanje CRL-a.
- Točka distribucije (Distribution Point) — lokacija/e na kojima je CRL objavljen.
- Razdoblje valjanosti (Validity Period) — razdoblje u kojem se CRL smatra mjerodavnim. Obično je to period između dva uzastopna objavljivanja.
- Potpis — CRL je potpisan od strane CA radi provjere autentičnosti.

Kod CRL sustava postoji rizik da certifikat može biti opozvan, ali ga klijenti ipak prihvaćaju jer ažurirani CRL nije objavljen. Daljnji problem je da preglednik (ili drugi klijent) mora preuzeti i pohraniti CRL lokalno, a mreža mora biti dostupna da bi to izvršila. OCSP (Online Certificate Status Protocol) može ažurirati status certifikata u stvarnom vremenu bez potrebe za preuzimanjem CRL-a.

Upravljanje ključevima

Upravljanje ključevima (key management) odnosi se na operativna razmatranja za različite faze životnog ciklusa ključa. Životni ciklus ključa može uključivati sljedeće faze:

- Generiranje ključa (Key Generation) — kreira asimetrični par ključeva ili simetrični tajni ključ potrebne jačine, koristeći odabranu šifru.

- Pohrana (Storage) — sprječava neovlašteni pristup privatnom ili tajnom ključu i štiti od gubitka ili oštećenja ključa.

Siguran pristup ključu trebao bi biti potpuno revidiran. Idealno, kriptografska pohrana je tamper-evident. To znači da se odmah zna kada je privatni ili tajni ključ kompromitiran i može se opozvati.

```
GnuPG needs to construct a user ID to identify your key.

Real name: James Pengelly
Email address: jpengelly@comptia.org
Comment:
You selected this USER-ID:
    "James Pengelly <jpengelly@comptia.org>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/kali/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/C3E
1D43D17CBCC7C80A3D4889564BC94BD4E1D99.rev'
public and secret key created and signed.

pub   rsa2048 2023-05-31 [SC] [expires: 2025-05-30]
      C3E1D43D17CBCC7C80A3D4889564BC94BD4E1D99
uid                      James Pengelly <jpengelly@comptia.org>
sub   rsa2048 2023-05-31 [E] [expires: 2025-05-30]
```

Ovi nedostaci mogu se riješiti korištenjem kriptoprocesora za generiranje i pohranu ključeva. Budući da je namijenjen jednoj funkciji, kriptoprocesorski hardver ima manju površinu napada od punog računala. Trusted Platform Module (TPM) je specifikacija za siguran kriptoprocesor koji se može ugraditi u uređaj. TPM se može implementirati na više načina:

- Diskretni (Discrete) znači da je TPM implementiran kao namjenski čip. Ovo pruža tamper otpornost i najmanju površinu napada.
- Integrirani (Integrated) znači da je TPM dio skupa čipova ili CPU-a koji obavlja i druge funkcije. Ova implementacija nije tamper otporna i ima širu površinu napada.
- Firmware znači da je TPM implementiran u niskonivojski operativni kod platforme. Ovisi o funkciji sigurne enklave CPU-a ili skupa čipova za zaštitu kriptografskog materijala. Primjeri uključuju Intelovu Platform Trust Technology (PTT) i AMD-ov fTPM.

Hardverski sigurnosni modul

Hardverski sigurnosni modul (HSM — Hardware Security Module) je kriptoprocesorski hardver implementiran u izmjenjivom ili namjenskom obliku, uključujući rack-mount uređaje, PCIe kartice i USB ključeve. Tvrtke mogu certificirati svoje proizvode prema Federal Information Processing Standard 140 Level 2 (FIPS 140-2) radi uspostavljanja povjerenja na tržištu.

Sigurna enklava

Korištenje kriptoprocesora znači da ključevi nisu izravno dostupni putem datotečnog sustava. Kriptoprocesor komunicira s aplikacijama koje trebaju pristupiti ključu putem sučelja programskog programa (API). Sigurna enklava, kao što je Intel Software Guard Extensions, može zaštititi podatke pohranjene u sistemskoj memoriji tako da ih nepouzdan proces ne može čitati.

Sigurna enklava je dizajnirana tako da čak i procesi s root ili sistemskim pristupom ne mogu čitati zaštićenu memoriju. To je posebno korisno za zaštitu kriptografskih ključeva koji su pohranjeni u memoriji.

Pohrana ključeva u escrow

Ako je privatni ili tajni ključ izgubljen ili oštećen, šifrirani tekstovi ne mogu se oporaviti osim ako je napravljena sigurnosna kopija ključa. Pravljenje kopija ključa je problematično jer postaje vjerojatnije da će kopija biti kompromitirana. Korporativna politika može zahtijevati da su ključevi pohranjeni u escrow — tj. da se kopija ključa drži u sigurnom, neovisnom dijelu sustava kojim upravljaju administratori certifikata ili za oporavak od katastrofe.

Lekcija 3C

Kriptografska rješenja

Pregled lekcije

Kao IT sigurnosni stručnjak, morate biti u mogućnosti odabrati kriptografska rješenja koja su primjerena za dani sigurnosni problem. Kriptografsko rješenje koristi šifre i alate, kao što su digitalni certifikati i hash funkcije, za zaštitu podataka u mirovanju (at rest), u prijenosu (in transit) i u korištenju (in use).

Šifriranje za podršku povjerljivosti

Ako su podaci šifrirani, nije važno je li disk koji pohranjuje informacije ukraden ili može biti presretnut prilikom prijenosa putem mreže, jer bez ključa napadač ne može pročitati sadržaj. Podaci mogu biti u jednom od sljedećih stanja:

- Podaci u mirovanju (Data at rest) — stanje kada su podaci u nekoj vrsti trajnog medija za pohranu.
- Podaci u prijenosu (Data in transit ili data in motion) — stanje kada se podaci prenose putem mreže.
- Podaci u korištenju (Data in use ili data in processing) — stanje kada su podaci zauzeti u privremenoj memoriji, kao što su sistemski RAM ili CPU registri i priručna memorija.

Privatni ključ za ovo je šifriran tako da korisnik mora navesti vjerodajnicu svog računa da bi ga koristio. U ovom kontekstu, privatni ključ je Ključ za šifriranje ključeva (KEK — Key Encryption Key). Sustav generira slučajni Ključ za šifriranje podataka (DEK — Data Encryption Key) koji se koristi za šifriranje samih podataka, dok se DEK zatim šifrira s KEK-om.

Šifriranje diska i datoteka

Podaci u mirovanju obuhvaćaju velik broj mehanizama pohrane. O njima možemo razmišljati u smislu razina šifriranja. Niže razine, poput šifriranja cijelog diska, imaju prednost što zaštićuju sve podatke na disku, ali nedostatak je što, jednom kada je disk montiran, podaci su dostupni u šifriranom obliku. Viša razina pohrane, poput šifriranja pojedinih datoteka, zahtijeva složenije upravljanje ključevima, ali je selektivnija.

Ako uređaj ima TPM ili HSM kompatibilan s proizvodom za šifriranje, disk/volumen/datotečni sustav može biti zaključan ključevima pohranjenima u TPM-u ili HSM-u.

Šifriranje baza podataka

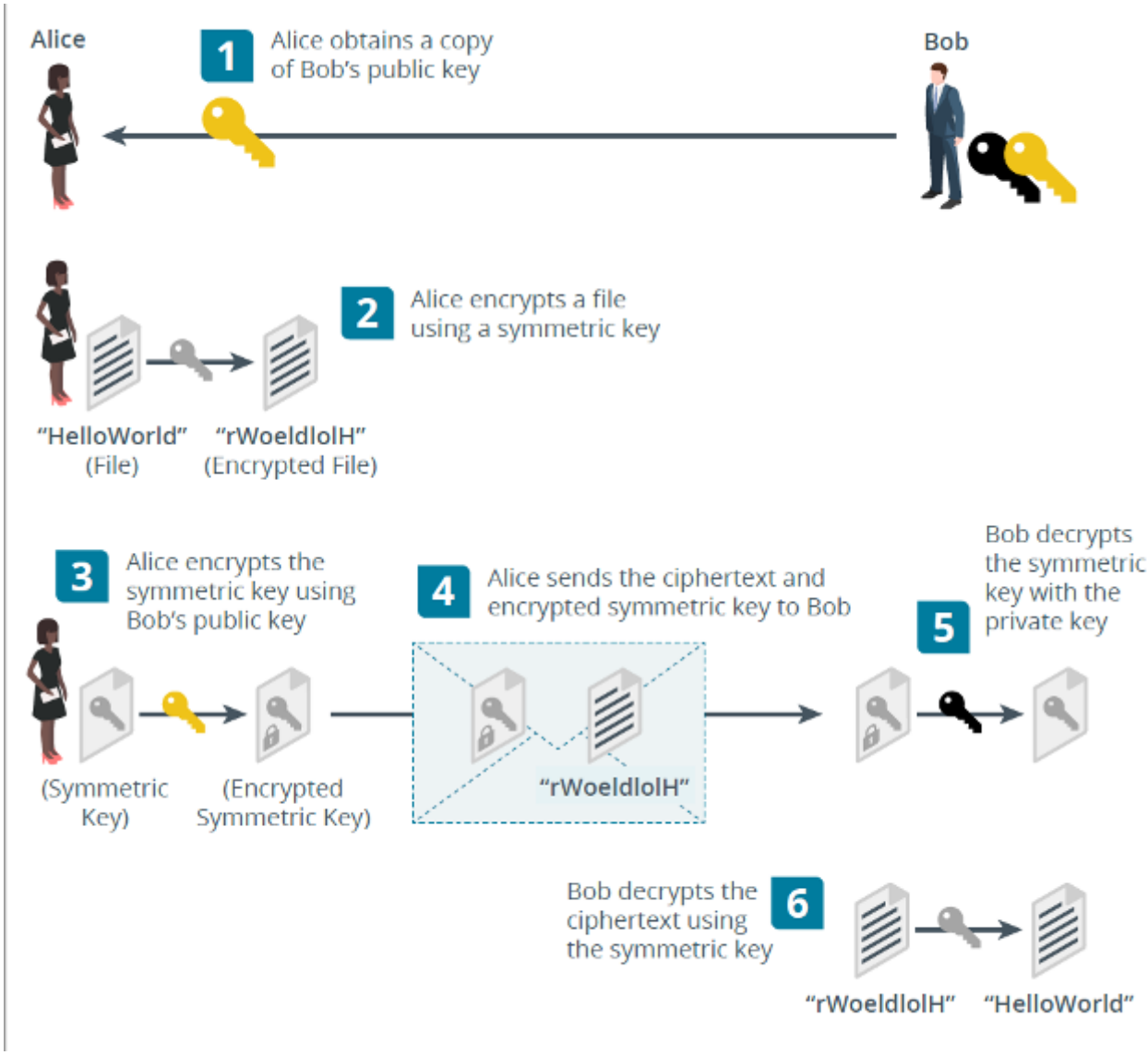
Strukturirana baza podataka pohranjuje podatke u tablicama. Svaka tablica se sastoji od stupaca s određenim tipovima podataka. Zapisi se pohranjuju kao redovi u tablici s vrijednošću unesenom za svako polje. Podaci tablice su na kraju pohranjeni kao datoteke na disku. Baze podataka se mogu šifrirati na razini datoteke, stupca ili polja. Šifriranje na razini polja ili stupca je najfleksibilnije, a šifriranje na razini datoteke je najjednostavnije.

Transportno šifriranje i razmjena ključeva

Transportno/komunikacijsko šifriranje štiti podatke-u-prijenosu. Različiti proizvodi za transportno šifriranje razvijeni su za različita mrežna rješenja. Neki primjeri:

- Wi-Fi Protected Access (WPA) — osigurava promet koji se šalje putem bežične mreže.
- Internet Protocol Security (IPsec) — osigurava promet koji se šalje između dvije krajnje točke putem javne ili nepouzdane transportne mreže. Ovo se naziva virtualnom privatnom mrežom (VPN).
- Transport Layer Security (TLS) — osigurava aplikacijske podatke, kao što su web ili email podaci, koji se šalju putem javne ili nepouzdane mreže.

Kao i kod podataka u mirovanju, asimetrična šifra se tipično ne koristi za izravno šifriranje mrežnih podataka, jer je neučinkovita. Proizvodi za transportno šifriranje koriste sustav razmjene ključeva koji im omogućuje uspostavu simetričnog ključa za šifriranje sesije. Taj simetrični ključ se tada koristi za šifriranje prometa za ostatak sesije. Ova tehnika korištenja asimetričnog šifriranja za zaštitu simetričnog ključa naziva se digitalnim omotnicom (digital envelope).

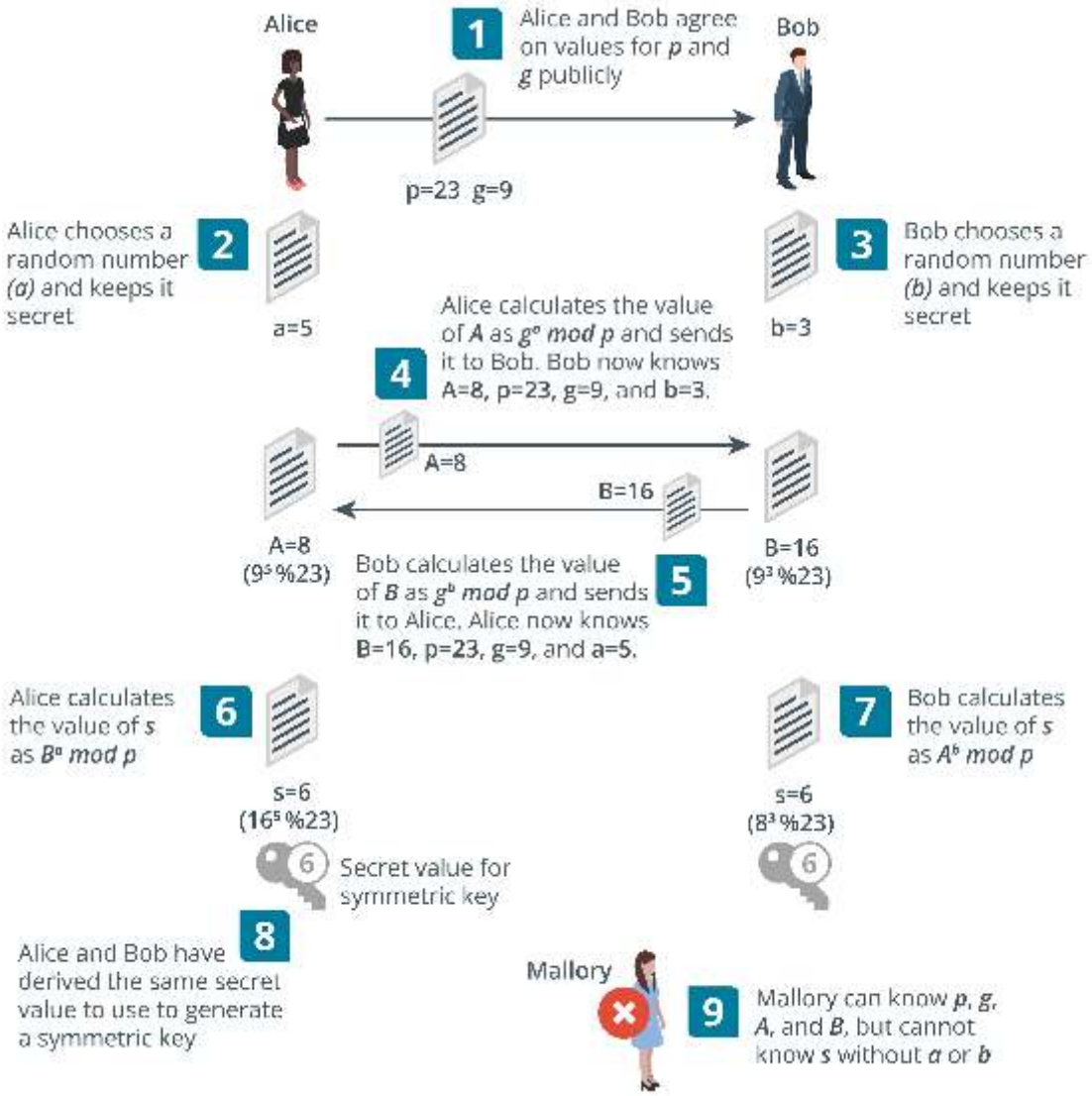


Transportno šifriranje također koristi kriptografiju za osiguravanje integriteta i autentičnosti poruka, tako da primatelj može provjeriti da ih nije modificirao nitko osim pošiljatelja. Provjera integriteta i autentičnosti može koristiti Hash-based Message Authentication Code (HMAC) koji kombinira hash poruke s tajnim ključem.

Savršena forward tajnost

Kod korištenja digitalne omotnice, strane moraju razmijeniti ili dogovoriti tajni ključ za masovno šifriranje, koji se koristi s odabranom simetričnom šifrom. U originalnoj implementaciji digitalnih omotnica, poslužitelj i klijent razmjenjuju simetrični ključ šifriran asimetričnim ključem poslužitelja. Ako privatni ključ poslužitelja bude kompromitiran, napadač koji je snimio prošli promet može dešifrirati prošle sesije. Ova mana potaknula je razvoj savršene forward tajnosti (Perfect Forward Secrecy — PFS).

Korištenje Diffie-Hellman za izvođenje tajne vrijednosti za generiranje zajedničkog simetričnog ključa šifriranja sigurno putem javnog kanala.



Korištenje privremenih (ephemeral) ključeva sesije znači da buduća kompromitacija poslužitelja neće dovesti do napada na snimljene podatke. Čak i ako napadač može dobiti ključ za jednu sesiju, ostale sesije ostaju povjerljive. Ovo masivno smanjuje rizik.

Soljenje i rastezanje ključa

Vrijednosti koje se koriste za privatni ključ ili tajni ključ moraju biti nasumično odabrane. Ako postoji nešto predvidljivo u načinu na koji je vrijednost ključa izvedena, ima manje entropije. Niska entropija posebno je zabrinjavajuća kada god kriptografski sustav koristi podatke koje generira korisnik, poput lozinke.

Niska entropija posebno je zabrinjavajuća kada god kriptografski sustav koristi podatke koje generira korisnik, poput lozinke. Korisnici skloni biraju lozinke niske entropije jer su ih lakše zapamtiti. Ova vrsta podataka je prekratka i preuredna da bi bila sigurna kao kriptografski ključ direktno. Rješenja za ovo uključuju: (1) Soljenje — dodavanje nasumičnog broja (soli) na lozinku prije hashiranja. (2) Rastezanje ključa (key stretching) — korištenje algoritma koji namjerno zahtijeva više računalnih resursa za hash, usporavajući napade grubom silom.

Blockchain

Blockchain je koncept u kojemu se rastuća lista transakcijskih zapisa osigurava korištenjem kriptografije. Svaki zapis se naziva blokom i prolazi kroz hash funkciju. Hash

vrijednost prethodnog bloka u lancu dodaje se svakom novom bloku, što osigurava da se prethodni blok ne može modificirati bez da se to primijeti.

Blockchain tehnologija ima razne potencijalne primjene. Može osigurati integritet i transparentnost financijskih transakcija, pravnih ugovora, zaštite autorskih prava i intelektualnog vlasništva, online sustava glasanja, sustava upravljanja identitetom i lanca opskrbe.

Zamagljivanje

Zamagljivanje (obfuscation) je vještina čineći poruku ili podatke teškim za pronalazak. To je sigurnost kroz nejasnost, što se normalno ne preporuča. Ipak postoji nekoliko upotreba za tehnologije zamagljivanja:

- Steganografija (doslovno 'skriveno pisanje') ugrađuje informacije unutar neočekivanog izvora; na primjer, poruka skrivena u slici. Dokument ili datoteka koja sadrži skrivenu poruku naziva se covertext. Poruka se može šifrirati nekim mehanizmom prije ugrađivanja, osiguravajući povjerljivost.
- Maskiranje podataka može značiti da su svi ili dio sadržaja polja baze podataka zamagljeni zamjenom stvarnih podataka s tokenima ili pseudonimima.

Trebate biti pažljivi da SAN polje navodi domene, poddomene ili wildcard domene kojima se pristupa poslužitelju.

- Kreirajte politike i procedure za korisnike i poslužitelje za podnošenje CSR-ova, plus procese identifikacije, autentikacije i autorizacije kako bi osigurali da se certifikati izdaju samo valjanim subjektima.
- Postavite procedure za upravljanje ključevima i certifikatima, uključujući opoziv i sigurnosno kopiranje/escrow ključeva, idealno korištenjem namjenskih hardverskih kriptoprocesora, kao što su TPM-ovi i HSM-ovi.

Modul 4

Implementacija upravljanja identitetom i pristupom

Pregled modula

Svaki mrežni korisnik i host uređaj mora biti identificiran računom kako biste mogli kontrolirati njihov pristup aplikacijama, podacima i uslugama vaše organizacije. Procesi koji podržavaju ovaj zahtjev nazivaju se upravljanjem identitetom i pristupom (IAM). Točno identificiranje korisnika i uređaja, te pružanje prava pristupa samo onima koji ih trebaju i samo kada ih trebaju, jedna je od temeljnih načela učinkovite sigurnosti.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Implementirati autentikaciju temeljenu na lozinci i višefaktorsku autentikaciju.
- Implementirati politike računa i rješenja za autorizaciju.
- Implementirati rješenja za jednokratnu prijavu i federativni identitet.

Lekcija 4A

Autentikacija

Pregled lekcije

Pretpostavljajući da je račun kreiran sigurno i da je identitet vlasnika računa verificiran, autentikacija verificira da samo vlasnik računa može koristiti račun i da sustav može koristiti samo vlasnik računa. Autentikacija se koristi za provjeru identiteta korisnika, uređaja ili procesa.

Dizajn autentikacije

Autentikacija se izvodi kada podnositelj zahtjeva (supplicant ili claimant) prezentira vjerodajnice autentikacijskom poslužitelju. Poslužitelj uspoređuje što je prezentirano s kopijom vjerodajnica koje ima pohranjene. Ako se podudaraju, račun je autenticiran. Faktor autentikacije je vrsta podataka (vjerodajnice) koje subjekt može prezentirati za dokazivanje svog identiteta:

- Povjerljivost, u smislu autentikacije, je kritična, jer ako vjerodajnice računa procure, akteri prijetnje mogu se lažno predstavljati kao vlasnik računa i djelovati na sustavu s pravima koja vlasnik ima.

Windows zaslon za prijavu.

Osobni identifikacijski broj (PIN) je također nešto što znate. Izvorno su PIN-ovi bili kratki četveroznamenkasti ili šesteroznamenkasti numerički nizovi koji se koriste s bankovnim karticama. U modernim dizajnima autentikacije, glavna karakteristika PIN-a je da je lokalan za određeni uređaj. PIN je pohranje u TPM-u uređaja ili zaštićenom pohranom, umjesto u centralnom direktoriju lozinki.

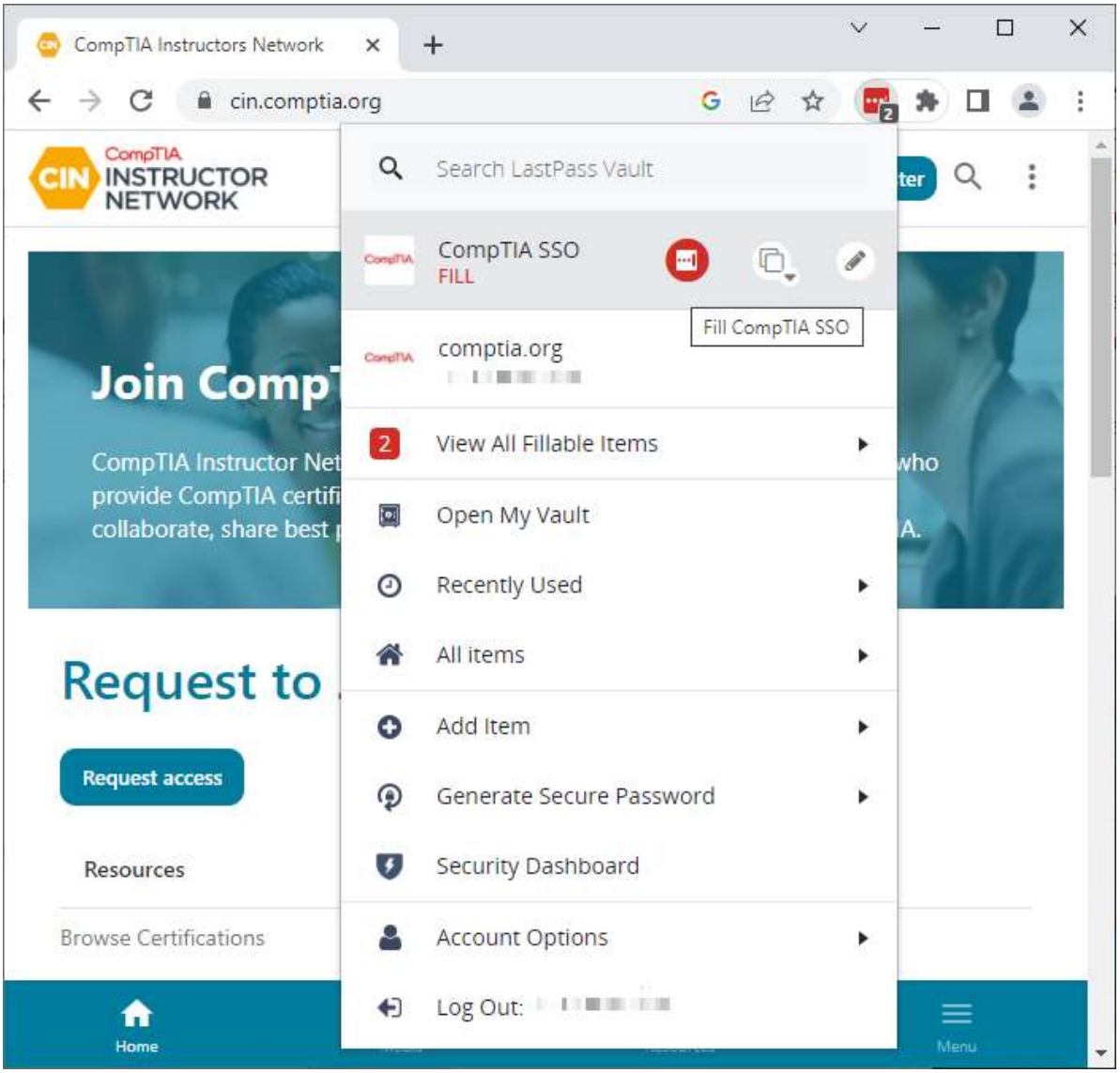
Koncepti lozinki

Nepravilno upravljanje vjerodajnicama nastavlja biti jedan od najprinosnijih vektora za mrežne napade. Ako organizacija mora nastaviti oslanjati se na vjerodajnice temeljene na lozinci, njeno korištenje mora biti upravljano jakim politikama i obukom:

- Duljina lozinke (Password Length) — nameće minimalnu duljinu lozinki. Može postojati i maksimalna duljina.
- Složenost lozinke (Password Complexity) — nameće pravila složenosti lozinke (kao što su zabrana korištenja korisničkog imena unutar lozinke i kombinacija najmanje osam velikih/malih alfanumeričkih i nealfanumeričkih znakova).
- Starost lozinke (Password Age) — prisiljava korisnika da odabere novu lozinku nakon određenog broja dana.
- Ponovna upotreba i povijest lozinki (Password Reuse and History) — sprječava odabir lozinke koja je već bila korištena. Atribut povijesti postavlja koliko prethodnih lozinki je blokirano. Atribut minimalne starosti sprječava korisnika od brzog cikliranja kroz promjene lozinki kako bi se vratio na preferiranu frazu.

Ponovna upotreba lozinke može značiti i korištenje radne lozinke na drugom mjestu (npr. na maloprodajnoj web stranici). Ova vrsta ponašanja može se policirati samo mekim politikama.

Korištenje LastPass upravitelja lozinki za prijavu na CompTIA web stranicu.



Glavni rizici od upravitelja lozinki su odabir slabe master lozinke, kompromitacija cloud pohrane ili sustava vendora i napadi lažnog predstavljanja dizajnirani da prevare upravitelja da unese lozinku na krivotvorenu stranicu.

Višefaktorska autentikacija

Dizajn autentikacije koji koristi samo lozinke ili jedan faktor znanja smatra se slabim. Tajne lozinki su previše sklone kompromitaciji da bi bile pouzdane. Drugi faktori autentikacije mogu se koristiti za dopunu lozinke. Nešto što imate (Something you have) je faktor posjedovanja. To znači da vlasnik računa posjeduje nešto što nitko drugi nema, kao što je pametna kartica, ključ-privjesak ili pametni telefon koji može generirati ili primati kriptografski token.

Nešto što jeste (Something you are) je biometrijski faktor koji koristi fizičke karakteristike poput otiska prsta, uzorka šarenice oka ili prepoznavanja lica. Nešto što radite (Something you do) obuhvaća obrasce unosa, kao što su ritam tipkanja ili uzorci pokreta.

Možete vidjeti i reference na dvofaktorsku autentikaciju (2FA). To samo znači da su uključena točno dva faktora, kao što je vlasničko-bazirana pametna kartica ili biometrijski identifikator s nečim što znate, poput lozinke ili PIN-a.

Biometrijska autentikacija

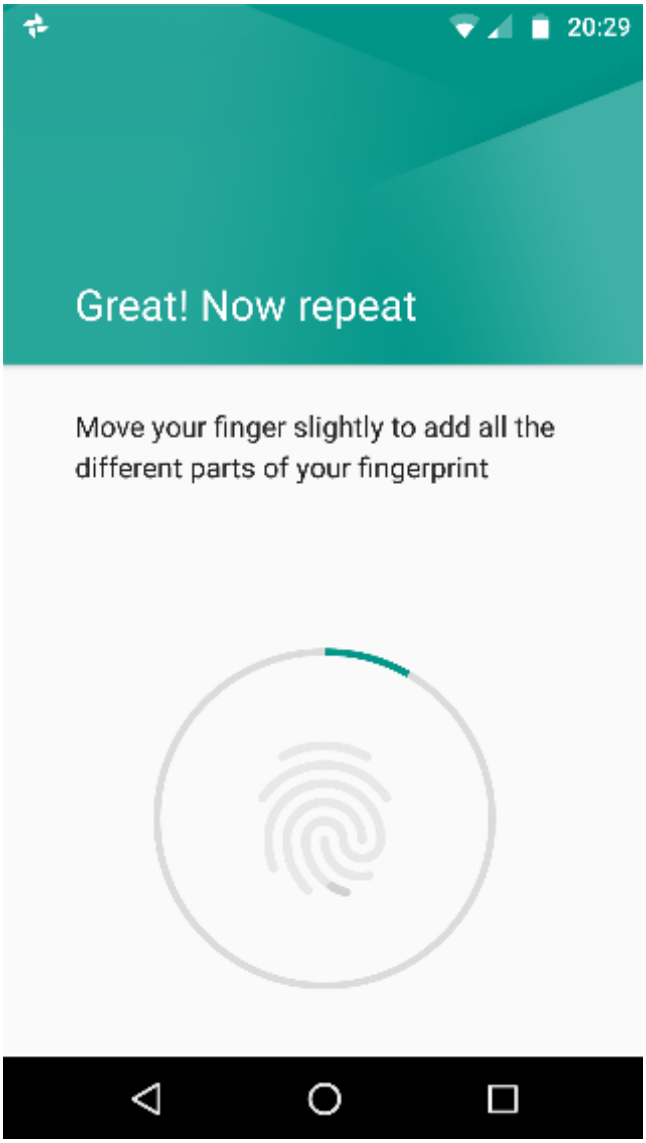
Prvi korak u postavljanju biometrijske autentikacije je upis (enrollment): 1. Senzorski modul prikuplja biometrički uzorak od mete. 2. Modul za ekstrakciju značajki kreira predložak (template). Predložak je matematička reprezentacija biometričke vrijednosti. 3. Predložak se pohranjuje u bazu podataka. Kada korisnik pokušava autentikaciju, sustav uspoređuje novo izmjereni biometrički uzorak s pohranjenim predlošcima:

- Stopa lažnog odbijanja (FRR — False Rejection Rate) — je kada legitimni korisnik nije prepoznat. Ovo se naziva i pogreška tipa I ili stopa lažnih nepodudaranja (FNMR).

Lažno odbijanje uzrokuje neugodnost korisnicima, ali lažno prihvaćanje može dovesti do sigurnosnih propusta, i zato se obično smatra najvažnijim mjerilom.

- Stopa pogreška prijelaza (CER — Crossover Error Rate) — točka na kojoj se FRR i FAR susreću. Što je niža CER, to je tehnologija učinkovitija i pouzdanija.
- Propusnost (Throughput) — je vrijeme potrebno za kreiranje predloška za svakog korisnika i vrijeme potrebno za autentikaciju. Ovo je važno razmatranje za pristupne točke s velikim prometom, poput aerodroma ili željezničkih kolodvora.

Konfiguriranje prepoznavanja otiska prsta na Android pametnom telefonu.



Prepoznavanje lica bilježi višestruke pokazatelje o veličini i obliku lica, poput razmaka između očiju ili širine i duljine nosa. Skeniranje obično koristi optičke i infracrvene kamere ili senzore za sprječavanje pokušaja spoofinga koji koriste slike ili maske.

Hardverski tokeni za autentikaciju

Faktor posjedovanja znači da korisnik posjeduje neku vrstu uređaja koji samo oni mogu koristiti. To se naziva autentikatorom. Autentikator može generirati ili primiti token koji identificira i autenticira korisnika:

- Autentikacija temeljena na certifikatu (Certificate-Based Authentication) — je kada podnositelj zahtjeva kontrolira privatni ključ koji može generirati jedinstveni potpisani token. Pružatelj identiteta može verificirati potpis putem javnog ključa.
- Jednokratna lozinka (OTP — One-Time Password) — je kada se token generira korištenjem neke vrste hash funkcije ili algoritma temeljenog na vremenu ili brojaču.

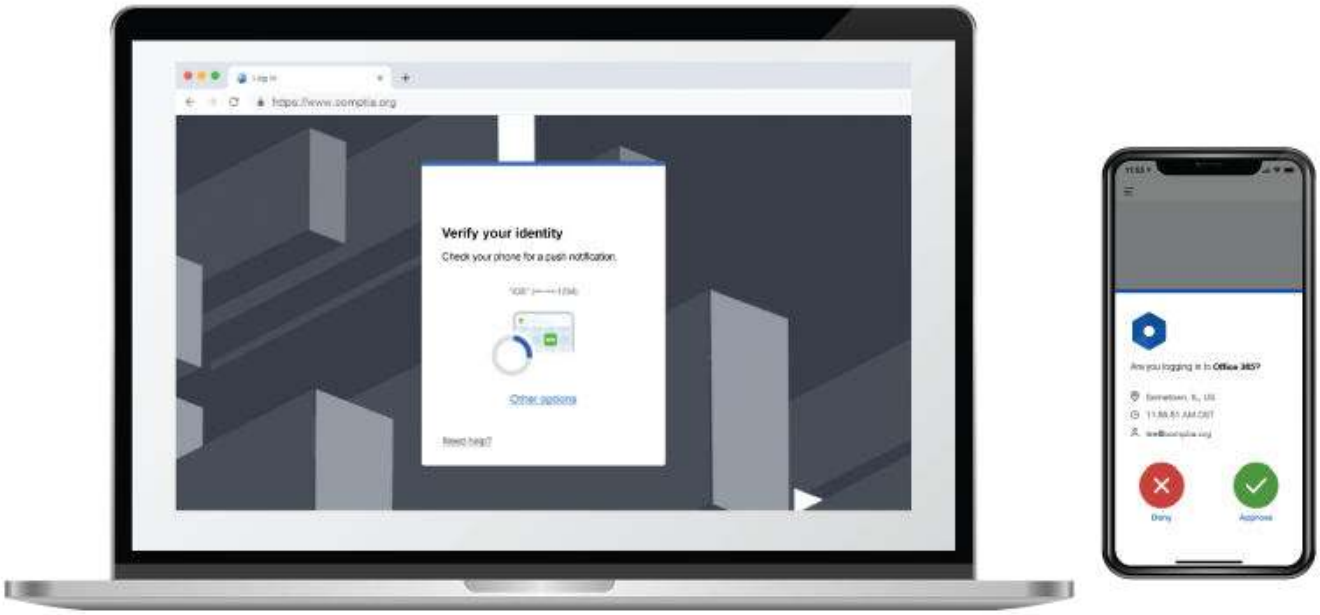
Generator token ključ-privjeska.

Postoje i jednostavnije pametne kartice i privjesci koji jednostavno prenose statički token programiran u uređaj. Na primjer, mnogi sustavi ulaska u zgrade rade na temelju statičnih kodova. Ovi mehanizmi su visoko ranjivi na kloniranje i replay napade.

Meki tokeni za autentikaciju

Meki token za autentikaciju je jednokratna lozinka generirana od strane pružatelja identiteta i prenesena podnositelju zahtjeva. OTP se može poslati na registrirani telefonski broj kao SMS/tekstualna poruka ili poslati na email račun.

Korištenje aplikacije za autentikaciju za prijavu na web stranicu. Nakon što se korisnik prijavi lozinkom, stranica ih traži da autoriziraju prijavu korištenjem aplikacije za autentikaciju instalirane na njihovom pametnom telefonu.



Autentikacija bez lozinke

Kod MFA temeljene na tokenima, korisnički račun je tipično još uvijek konfiguriran s lozinkom. To se može koristiti kao mehanizam sigurnosne kopije ili može postojati dvostupanjski proces verifikacije, gdje korisnik mora unijeti lozinku i autenticirati se tokenom. Alternativno, autentikacija bez lozinke (passwordless) zamjenjuje lozinku

sigurnijim faktorima.

Da bi sustav bez lozinke bio siguran, autentikator mora biti pouzdan i otporan na napade spoofinga ili kloniranja. Atestacija (attestation) je mehanizam za autentikatorski uređaj, kao što je FIDO sigurnosni ključ ili TPM u PC-u ili laptopu, da dokaže da nije modificiran i da je konfiguriran u skladu s pravilima. Standardi kao što su FIDO2 i WebAuthn definiraju mehanizme za autentikaciju bez lozinke koristeći sigurnosne ključeve ili biometriku.

Lekcija 4B

Autorizacija

Pregled lekcije

Autorizacija je dio upravljanja identitetom i pristupom koji upravlja dodjelom privilegija mrežnim korisnicima i uslugama. Implementacija modela kontrole pristupa pomaže organizaciji da upravlja implikacijama dodjela privilegija i odgovori na sigurnosne incidente.

Diskrecijska i obvezna kontrola pristupa

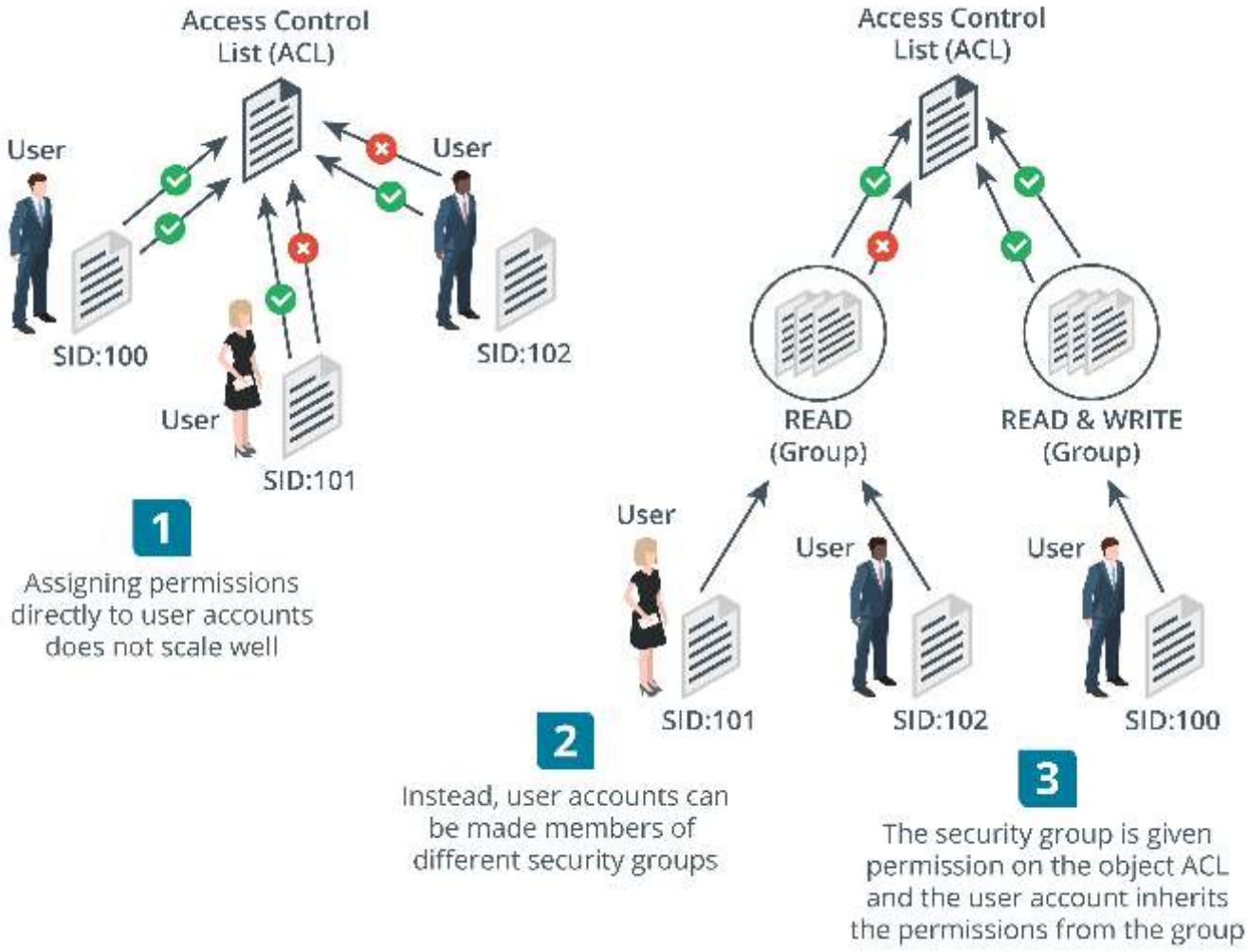
Korisnički račun koji je autenticiran može dobiti prava i dozvole na mrežama, računalima i podacima. Model kontrole pristupa opisuje načela prema kojima korisnici dobivaju prava. Diskrecijska kontrola pristupa (DAC — Discretionary Access Control) je model u kojem vlasnik objekta (korisnik) ima ovlaštenje dodijeliti pristup. U obveznoj kontroli pristupa (MAC — Mandatory Access Control), vlasnik objekta ne može dodijeliti pristup, jer je ovlaštenje određeno sistemski.

Označavanje objekata i davanje dozvola odvija se korištenjem unaprijed uspostavljenih pravila. Ključna točka je da su ta pravila ne-diskrecijska i ne mogu se mijenjati ni jednim korisničkim računom. Budući da je jednostavan sustav klasifikacije nefleksibilan, većina MAC modela koristi višerazinsku klasifikaciju u kojoj korisnici imaju određenu razinu odobrenja (npr. povjerljivo), a objekti imaju određenu razinu klasifikacije. Korisnici mogu pristupiti samo objektima čija je klasifikacija jednaka ili niža od njihovog odobrenja.

Kontrola pristupa temeljena na ulogama i atributima

RBAC (Role-Based Access Control) i ABAC (Attribute-Based Access Control) koriste ne-diskrecijska, pravilo-bazirana dodjeljivanja dozvola s više fleksibilnosti od MAC. RBAC znači da organizacija definira niz uloga i svaka uloga ima odgovarajuće prava. Korisnici se dodaju ulogama na temelju funkcije svog posla.

Korištenje sigurnosnih grupa za dodjelu privilegija.

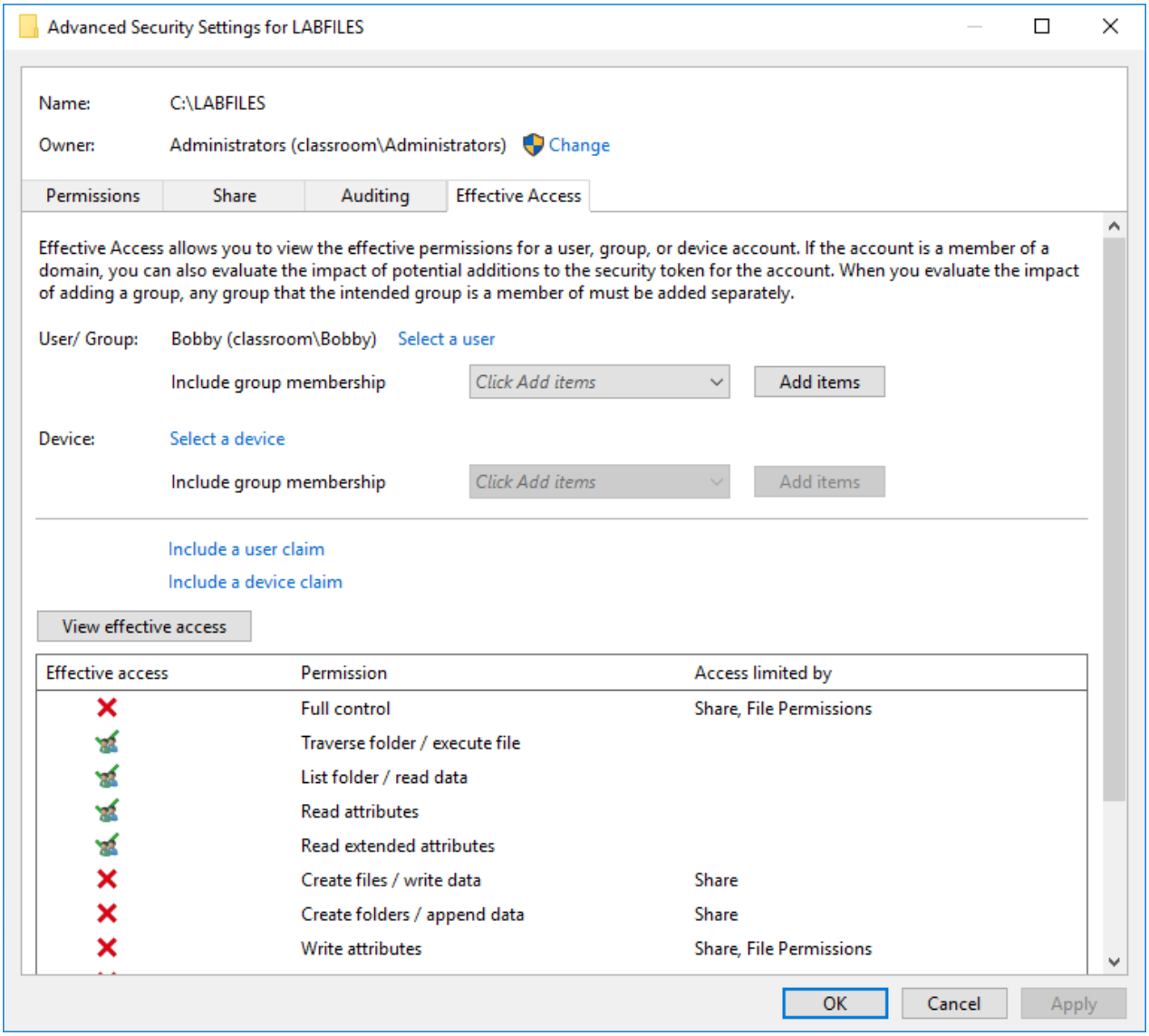


RBAC se može djelomično implementirati mapiranjem sigurnosnih grupa na uloge, ali to nisu identične sheme. Članstvo u sigurnosnim grupama je uglavnom diskrecijsko (dodijeljuje ga administrator, a ne određuje sustav). ABAC ide korak dalje od RBAC definirajući prava i dozvole temeljene na atributima korisnika, resursa i okruženja. Na primjer, pristup može biti dozvoljen samo kada korisnikov odjel odgovara atributu odjela resursa.

Pravilo-bazirana kontrola pristupa

Pravilo-bazirana kontrola pristupa odnosi se na bilo koji model kontrole pristupa u kojemu su politike kontrole pristupa određene pravilima koja nameće sustav, a ne korisnici sustava. Stoga su RBAC, ABAC i MAC primjeri pravilo-baziranih kontrola pristupa. Vatrozidi primjenjuju pravila koja admini konfiguriraju — ovo je primjer kontrole pristupa temeljene na pravilima. Dozvole datotečnog sustava (poput ACL-ova) koje određuju tko može čitati, pisati ili izvršavati datoteke implementacija su diskrecijske kontrole pristupa.

Određivanje efektivnih dozvola za dijeljenu mapu.



Pribavljanje korisničkih računa

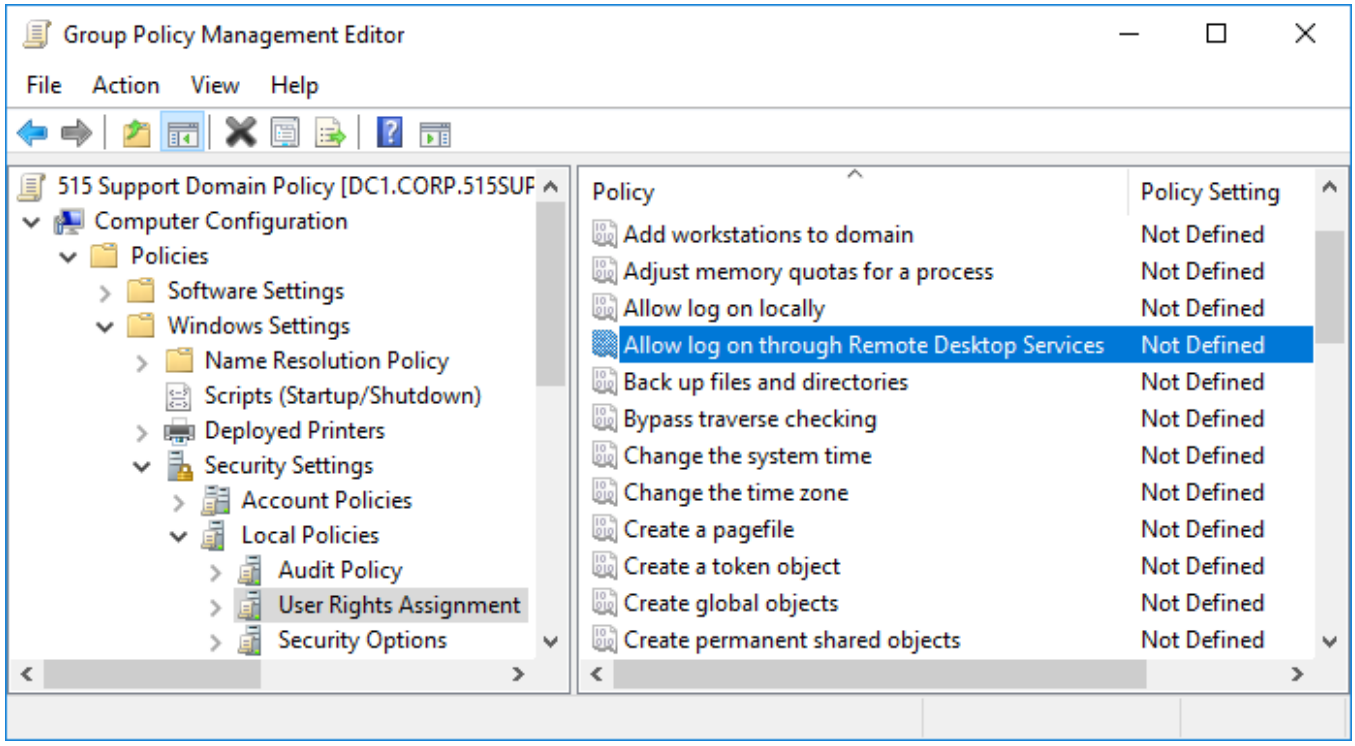
Pribavljanje (provisioning) je proces postavljanja usluge prema standardnoj proceduri ili kontrolnoj listi dobrih praksi. IT odjel mora pratiti sve imovine kojima upravlja, a korisnički računi su vrsta imovine. Pribavljanje korisničkog računa obično uključuje:

- Dokazivanje identiteta (Identity Proofing) — verificira da je osoba ona za koga se predstavlja provjerom službenih dokumenata i evidencija. Okolnosti mogu zahtijevati i provjeru prošlosti, koja verificira trenutne i prošle adrese, obrazovanje ili prethodno zaposlenje i ima li osoba kaznenu evidenciju.

resurse za obavljanje svog posla. Ako su im resursi nedostajni, mogu pokušati nabaviti hardver i softver direktno (Shadow IT).

- Podizanje svijesti o politici (Teaching Policy Awareness) — zakazivanjem obuke i omogućavanjem pristupa resursima za učenje tako da je zaposlenik ili ugovaratelj svjestan sigurnosnih politika i rizika.
- Kreiranje dodjeljivanja dozvola (Creating Permissions Assignment) — identificiranjem radnih uloga koje račun mora podržavati i konfiguriranjem odgovarajućih prava korištenjem modela kontrole pristupa temeljenog na ulogama, obveznog ili atributno-baziranog. Opoređivanje (deprovisioning) je proces uklanjanja pristupa računu kada vlasnik napusti organizaciju.

Konfiguriranje politika pristupa i prava korištenjem Group Policy Objects u Windows Server 2016.



Ograničenja računa

Ograničenja temeljena na politici mogu se koristiti za smanjenje nekih rizika od kompromitacije računa krađom vjerodajnica. Politike temeljene na lokaciji — Korisnik ili uređaj može imati logičnu mrežnu lokaciju, identificiranu IP adresom, podmrežom ili virtualnom lokalnom mrežom (VLAN):

- IP adresa — može biti povezana s mapiranom lokacijom u različitim stupnjevima točnosti temeljenim na informacijama koje je objavio registrant. Registrant je obično pružatelj internetskih usluga (ISP), pa ćete dobiti okvirnu lokaciju hosta temeljenu na ISP-u.
- Politika prijave temeljena na trajanju (duration-based login policy) uspostavlja maksimalni vremenski period u kojemu se račun može koristiti.
- Politika nemoguće vrijeme putovanja / rizičnih prijava (impossible travel time/risky login policy) prati lokaciju događaja prijave kroz vrijeme. Ako ti događaji ne zadovoljavaju prag, račun će biti onemogućen i podiže se upozorenje.
- Politika privremenih dozvola (temporary permissions policy) uklanja račun iz sigurnosne uloge ili grupe nakon određenog vremenskog perioda, zahtijevajući da administrator odobri nastavak dozvola.

Lekcija 4C

Upravljanje identitetom

Pregled lekcije

Dok on-premises mreža može koristiti lokalni direktorij za upravljanje računima i pravima, kako organizacije prelaze na cloud usluge, ove autorizacije moraju biti implementirane korištenjem rješenja za federativno upravljanje identitetom.

Lokalna, mrežna i udaljena autentikacija

Jedna od najvažnijih značajki operativnog sustava je pružatelj autentikacije, koji je softverska arhitektura i kod koji podupire mehanizam kojim je korisnik autenticiran:

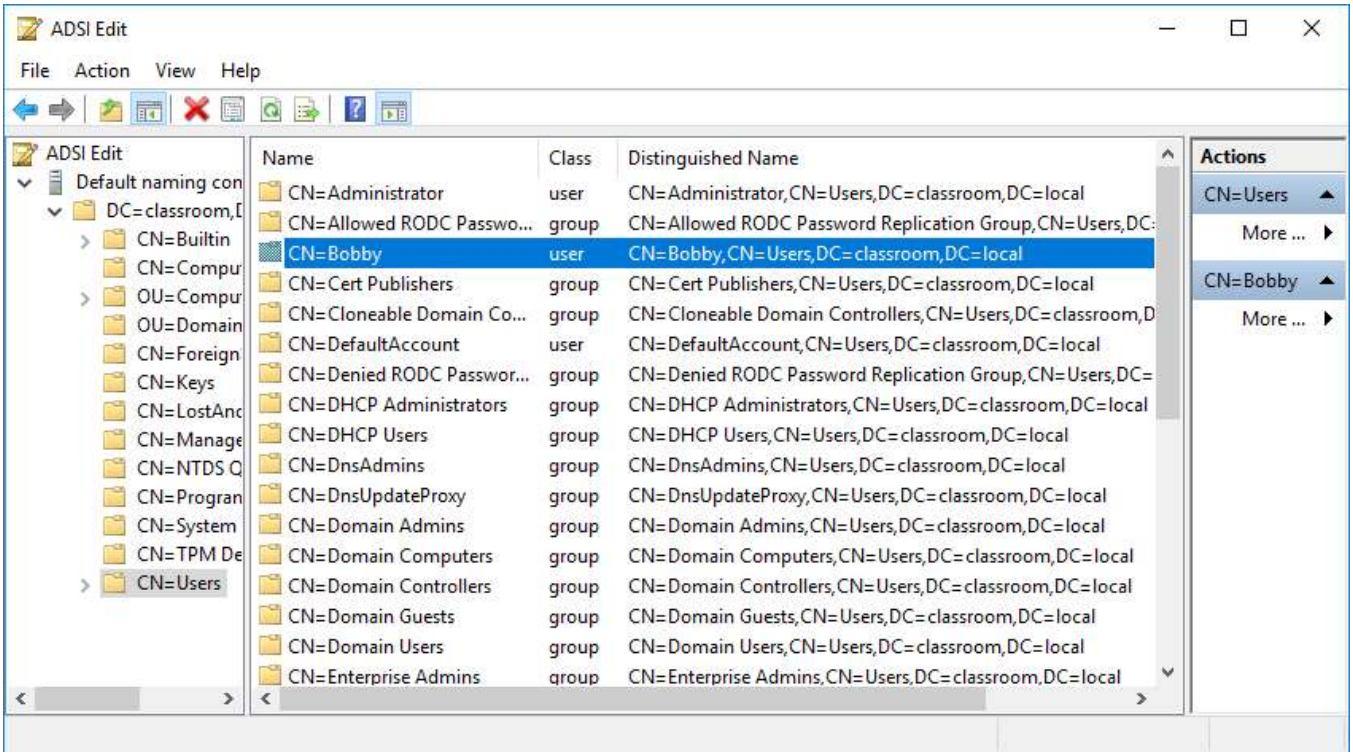
- Windows lokalna prijava (Windows local sign-in) — je Local Security Authority Subsystem Service (LSASS) koji uspoređuje dostavljenu vjerodajnicu s hashom pohranjenim u Security Accounts Manager (SAM) bazi podataka, koja je dio registra.

Linux autentikacija

U Linuxu, lokalna korisnička imena su pohranjena u /etc/passwd. Kada se korisnik prijavi na lokalnu interaktivnu ljusku, lozinka se provjerava prema hashu pohranjenom u /etc/shadow. Interaktivna prijava putem mreže tipično se postiže korištenjem Secure Shell (SSH) protokola.

Direktorijske usluge

Direktorijska usluga pohranjuje informacije o korisnicima, računalima, sigurnosnim grupama/ulogama i uslugama. Svaki objekt u direktoriju ima određeni broj atributa. Shema direktorija opisuje vrste atributa, koje informacije mogu sadržavati i redoslijed kojim su organizirani. Microsoft Active Directory Domain Services (AD DS) je implementacija direktorijske usluge koja se koristi u poduzećima koja koriste Windows Server.

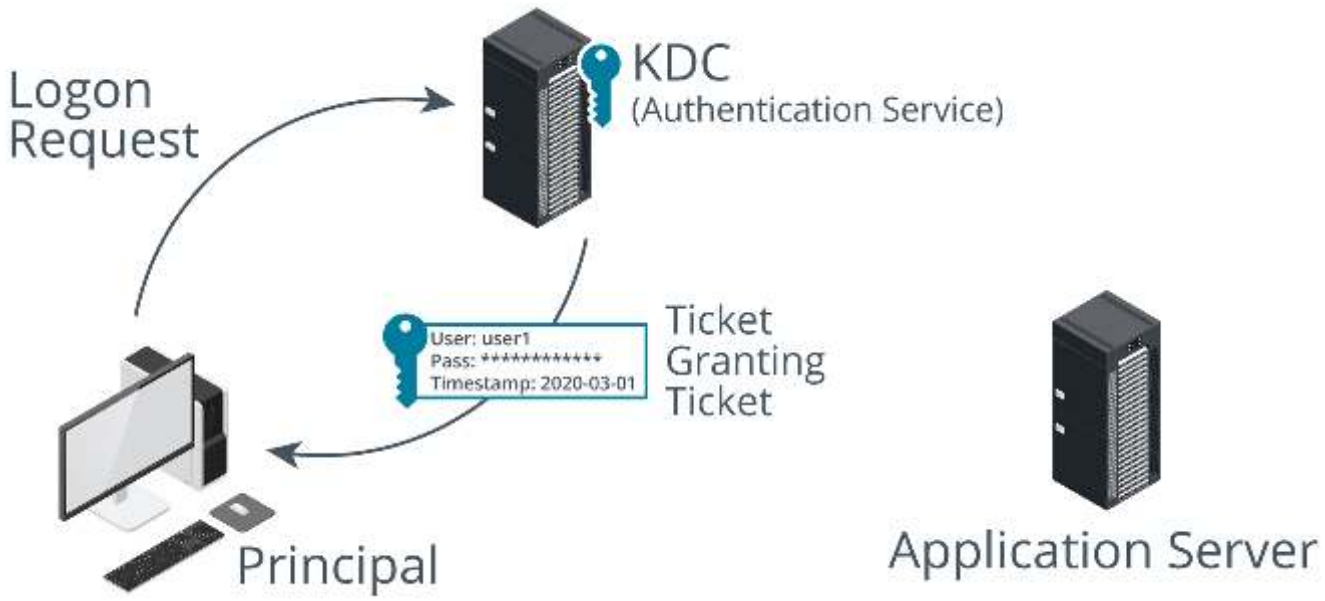


Neki atributi koji se uobičajeno koriste uključuju uobičajeno ime (CN), organizacijsku jedinicu (OU), organizaciju (O), zemlju (C) i domenu (DC).

Na primjer, razlikovno ime web poslužitelja kojim upravlja Widget u UK moglo bi biti sljedeće: CN=WIDGETWEB, OU=Marketing, O=Widget, C=UK, DC=widget, DC=foo

Autentikacija jednokratnom prijavom (SSO)

Sustav jednokratne prijave (SSO — Single Sign-On) omogućuje korisniku autentikaciju u jednom sustavu i primanje autorizacija na integriranim aplikacijskim poslužiteljima bez ponovnog unosa vjerodajnica. Kerberos je protokol za mrežnu autentikaciju jednokratnom prijavom koji se koristi u integriranim okruženjima. Za razliku od lozinke koja ostaje ista u dužem periodu, Kerberos koristi sesijske tokene koji imaju kratko trajanje.



Kerberos može autenticirati i ljude i aplikacijske usluge. Ovi se zajednički nazivaju principalima. Koristeći autentikaciju na Windows domenu kao primjer, prvi korak u Kerberos SSO je autentikacija kod KDC (Key Distribution Center) poslužitelja, implementiranog u Active Directoriju kao Authentication Service (AS). Lozinka ili PIN korisnika koristi se za izračun hasha ključa koji se šalje AS-u.

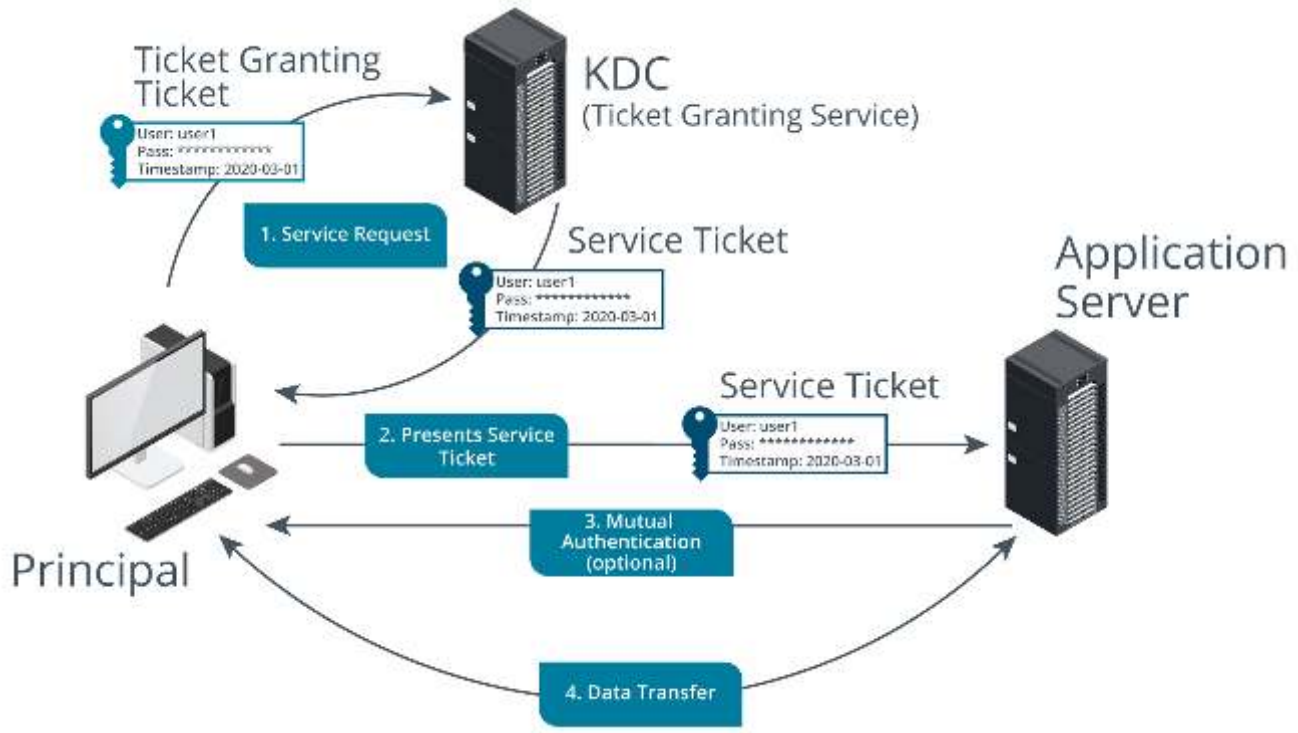
Hash lozinke sam po sebi se ne prenosi putem mreže. Iako se radi jednostavnosti referiramo na lozinke, sustav može koristiti i druge autentikatore, kao što je prijava pametnom karticom.

AS provjerava je li korisnički račun prisutan, može li dekodirati zahtjev podudaranjem hash-a lozinke korisnika s onom u bazi podataka Active Directorija i nije li zahtjev istekao. Ako je zahtjev valjan, AS odgovara s paketom koji sadrži:

- Ulaznica za dodjelu ulaznica (TGT — Ticket Granting Ticket) — sadrži informacije o klijentu (ime i IP adresu) plus vremensku oznaku i period valjanosti. Ovo je šifrirano korištenjem tajnog ključa KDC-a.
- TGS ključ sesije — komunicira između klijenta i Službe za dodjelu ulaznica (TGS — Ticket Granting Service). Ovo je šifrirano korištenjem hasha korisnikove lozinke.

TGT je primjer logičnog tokena. Sve što TGT radi je identificirati tko ste vi i potvrditi da ste autentificirani — ne pruža vam pristup nijednom resursu domene.

Kerberos Služba za dodjelu ulaznica.

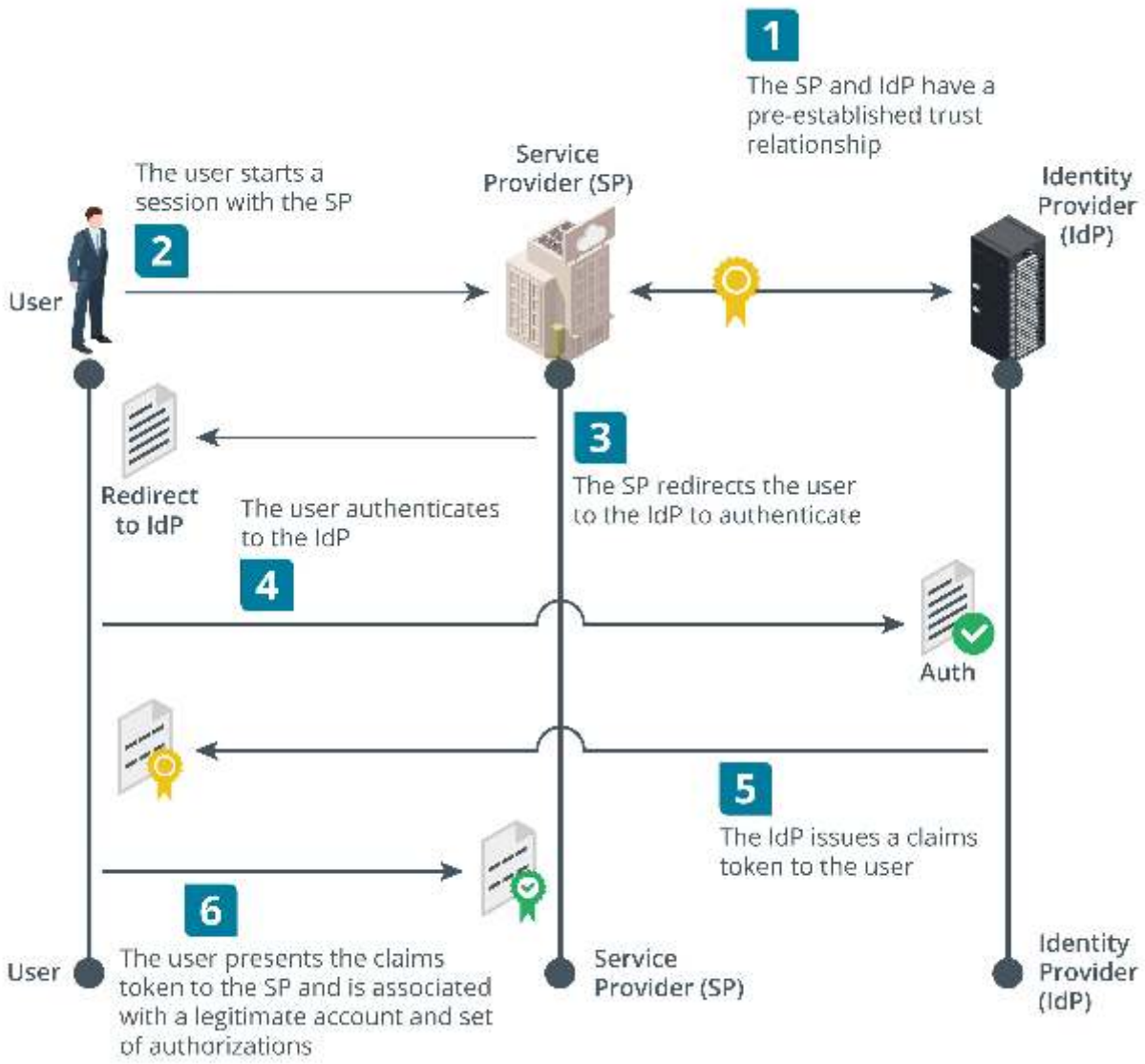


Aplikacijski poslužitelj dekriptira ulaznicu usluge kako bi dobio ključ sesije usluge korištenjem svog tajnog ključa, potvrđujući da mu je principal poslao neizmijenjenu poruku. Zatim dekriptira autentikator korištenjem ključa sesije usluge. Neobavezno, klijent može zahtijevati uzajamnu autentikaciju od poslužitelja i poslužitelj odgovara koristiteljevim vremenskim žigom šifriranim ključem sesije usluge.

Dizajn federativne autorizacije dolazi s više ograničenja i dodatnih zahtjeva za osiguravanje interoperabilnosti između različitih platformi. Web aplikacije možda ne

podržavaju Kerberos, dok mreže trećih strana možda ne podržavaju izravnu federaciju s Active Directoryjem. Federativni sustav upravljanja identitetom (Federated Identity Management — FIM) omogućava organizacijama razmjenu informacija o identitetu i autentikaciji putem raznih standarda i protokola.

Pregled federativnog upravljanja identitetom.



Security Assertion Markup Language (SAML)

Federativna mreža ili cloud trebaju specifične protokole i tehnologije za implementaciju tvrdnji o korisničkom identitetu i prijenos zahtjeva između principala, oslanjajuće strane i pružatelja identiteta. Security Assertion Markup Language (SAML) je XML shema za razmjenu podataka o autentikaciji i autorizaciji između sigurnosnih domena radi implementacije SSO-a.

Primjer SAML odgovora (tvrdnje):

Otvorena autorizacija (OAuth)

Mnogi javni oblaci koriste programska sučelja (API-je) temeljena na Representational State Transfer (REST) arhitekturi umjesto SOAP-a. Ova se zovu RESTful API-ji. Dok je SOAP strogospecificiran protokol, REST je lablja arhitektura. RESTful API-ji koriste JSON (JavaScript Object Notation) za razmjenu podataka i HTTPS za sigurnu komunikaciju.

OAuth (Open Authorization) je protokol koji omogućuje aplikacijama sigurno pristupanje podacima korisnika bez otkrivanja korisnikove lozinke.

Klijentska aplikacija ili usluga mora biti registrirana kod autorizacijskog poslužitelja. Kao dio ovog procesa, klijent registrira URL za preusmjeravanje, koji je krajnja točka koja će obrađivati autorizacijske tokene. Registracija također pruža klijentu ID i tajnu.

Sažetak

Trebate moći procijeniti dizajn i korištenje autentikacijskih proizvoda u smislu zadovoljavanja zahtjeva povjerljivosti, integriteta i dostupnosti. Za postizanje ovih ishoda, razmotrite sljedeće akcije:

- Procijenite zahtjeve dizajna za povjerljivost, integritet i dostupnost ovisno o kontekstu autentikacijskog rješenja (privatna mreža, javni web, VPN gateway ili fizički objekt).
- Odredite je li potrebna višefaktorska autentikacija (MFA) ili autentikacija bez lozinke i koji su faktori autentikacije odgovarajući.

Modul 5

Sigurna arhitektura poslovne mreže

Pregled modula

Upravljanje autentikacijom i autorizacijom korisnika samo je jedan dio izgradnje sigurnih IT usluga. Mrežna infrastruktura mora biti i sama dizajnirana za pokretanje usluga s atributima povjerljivosti, integriteta i dostupnosti. Razumijevanje osnova sigurnosti mreže ključno je za svaku sigurnosnu ulogu.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Usporediti i suprotstaviti sigurnosne implikacije različitih on-premises mrežnih arhitektura.
- Objasniti sigurnosne implikacije rješenja za cloud i virtualizaciju.
- Implementirati sigurne mrežne protokole i usluge.
- Implementirati sigurne mrežne uređaje.

Lekcija 5A

Arhitektura poslovne mreže

Pregled lekcije

Iako možda niste odgovorni za dizajn mreže u svojoj trenutnoj ulozi, važno je da razumijete ranjivosti koje mogu nastati iz slabosti u mrežnoj arhitekturi, i neka opća načela za osiguravanje dobro dizajnirane mreže.

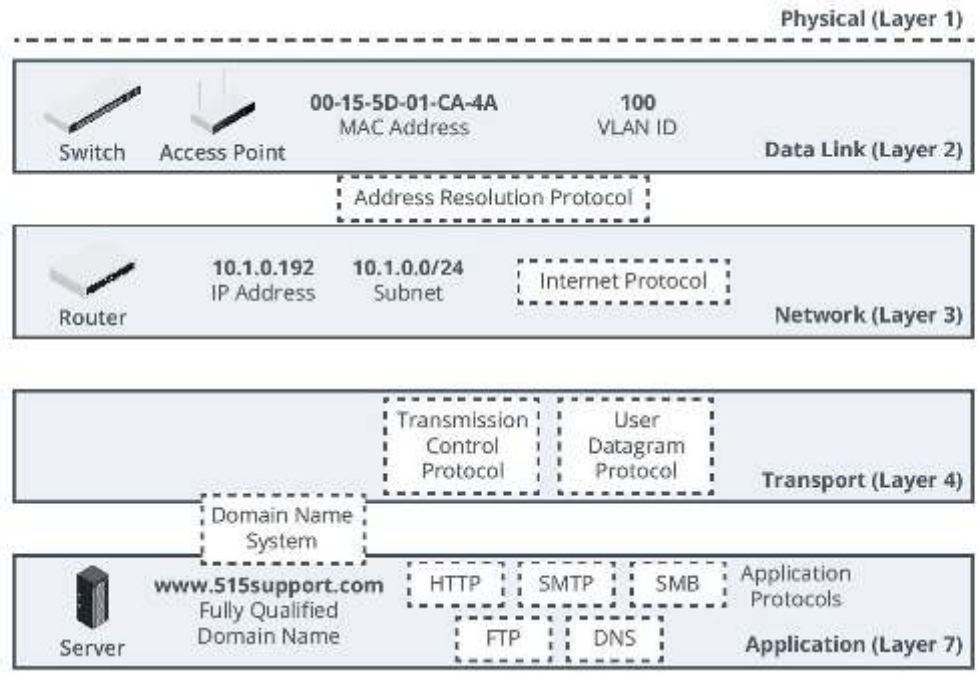
- Mrežna infrastruktura je medij, uređaji i protokoli za adresiranje/prosljeđivanje koji podržavaju osnovnu povezanost.
- Mrežne aplikacije su usluge koje se pokreću na infrastrukturi za podršku poslovnim operacijama.

Ova vrsta poslovnog toka uključivat će sustave s različitim sigurnosnim zahtjevima. Postavljanje klijenta, poštanskog sandučića i poslužitelja za prijenos pošte unutar istog segmenta uvest će mnoge ranjivosti. Razumijevanje i kontrola načina na koji podaci teku između segmenata i usluga bitno je za siguran mrežni dizajn.

Mrežna infrastruktura

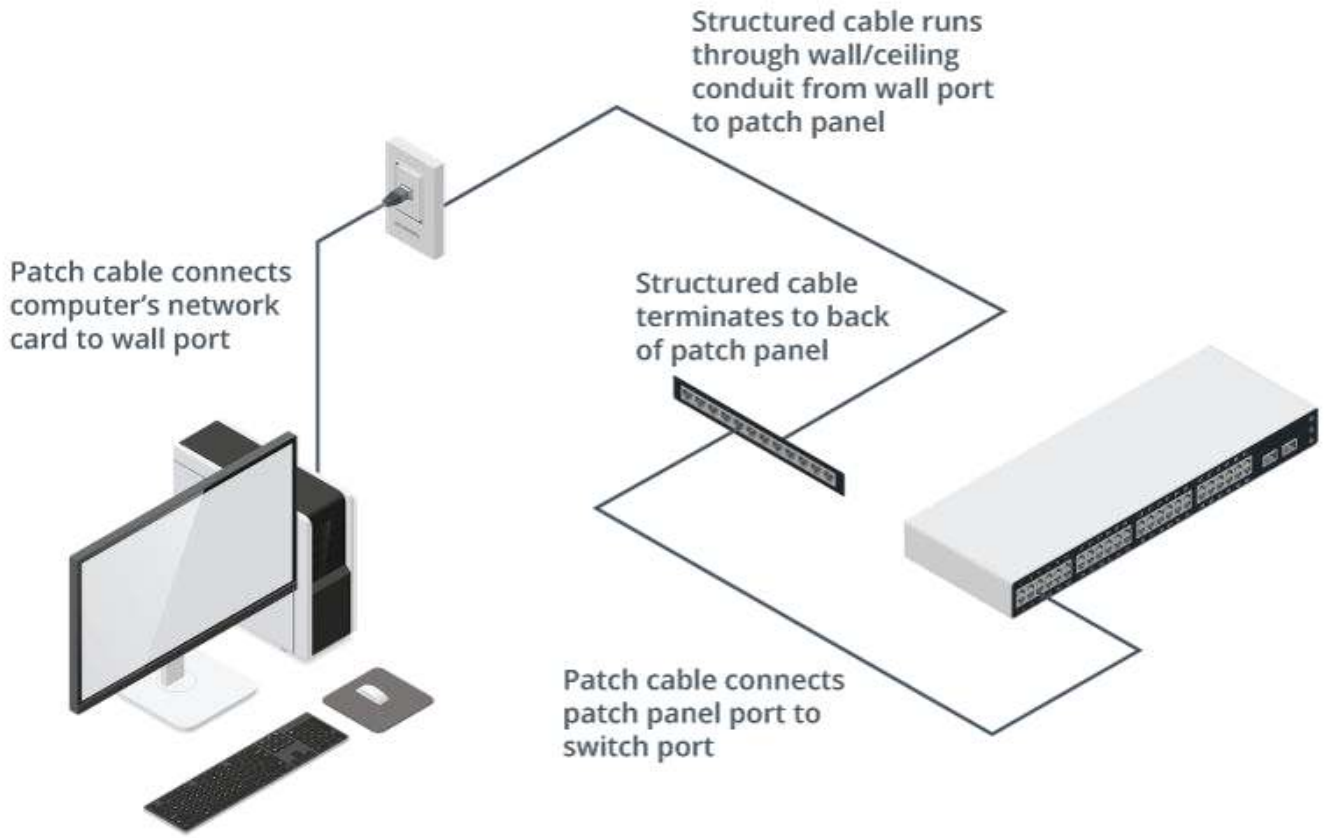
Korisno je koristiti model slojeva za analizu mrežne infrastrukture i usluga. Model Open Systems Interconnection (OSI) je široko citiran primjer kako definirati slojeve mrežnih funkcija. Mreža se sastoji od različitih vrsta uređaja za umrežavanje:

- Preklopnici (Switches) prosljeđuju okvire između čvorova u kabeliranoj mreži. Mrežni adapter u svakom hostu spojen je na port preklopnika putem kabela. Preklopnici rade na sloju 2 OSI modela. Većina LAN-ova koristi mreže temeljene na Ethernet standardu. Ethernet preklopnik donosi odluke prosljeđivanja temeljene na hardverskoj adresi ili MAC adresi.



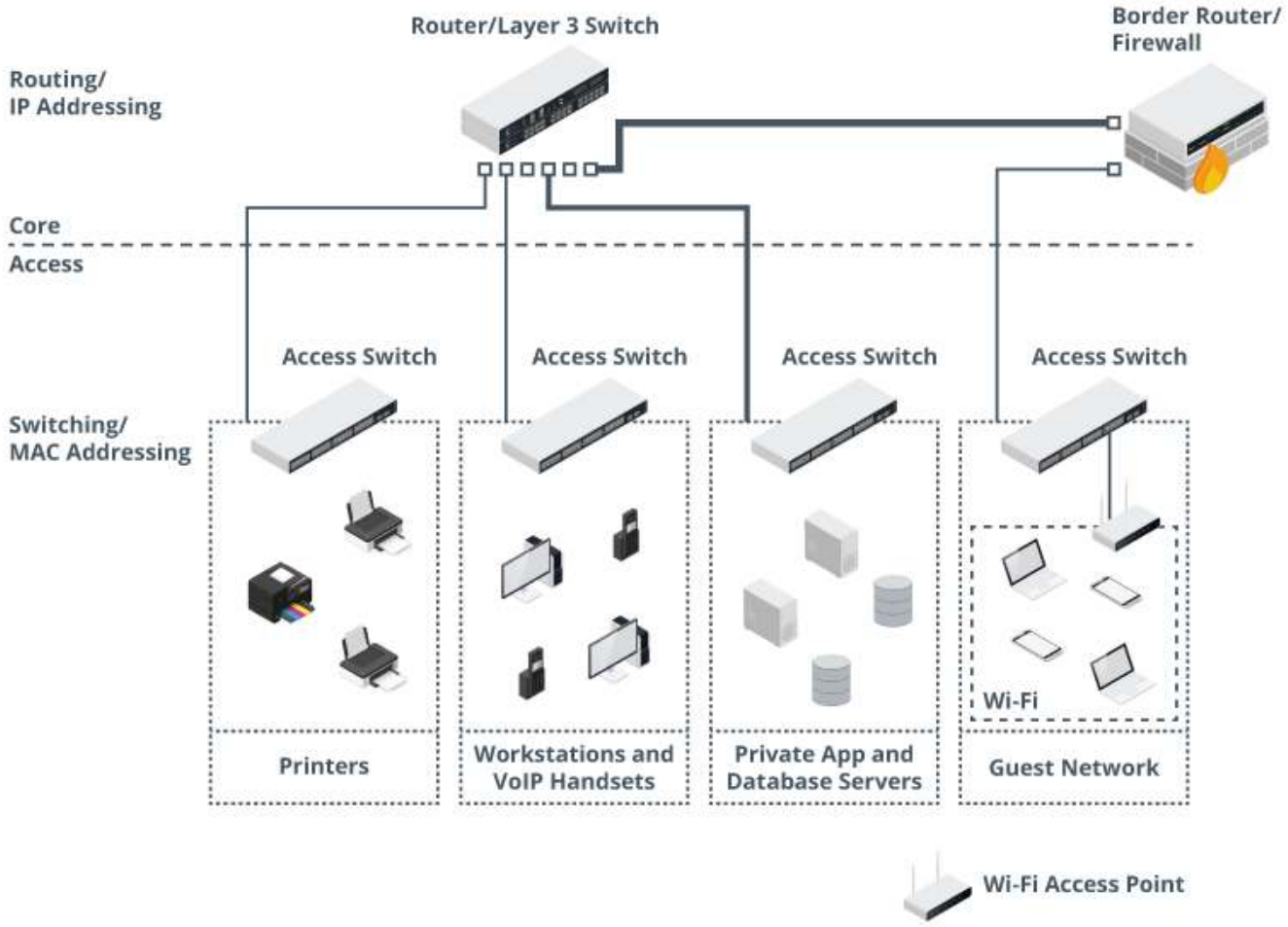
- Bežične pristupne točke (Wireless access points) pružaju most između kabelirane mreže i bežičnih hostova. Pristupne točke rade na sloju 2 OSI modela. Bežični uređaji također koriste MAC adresiranje na sloju 2.
- Usmjerivači (Routers) šalju pakete po međumreži, donoseći odluke prosljeđivanja temeljene na Internet Protocol (IP) adresama. Usmjerivači rade na sloju 3 OSI modela. Svaki lokalni segment obično ima usmjerivač spojen na njega. Usmjerivač djeluje kao zadana pristupna točka za hostove na segmentu za slanje paketa na druge segmente.

Fizička topologija komponenti u strukturiranom kabelskom sustavu.



Ovo se može opisati kao zvjezdasta topologija. Preklopnik sjedi u centru s vezama prema hostovima koji se šire iz njega. Preklopnik može uspostaviti podatkovne veze između bilo koja dva hosta koji su na njega priključeni. Ako host pošalje broadcast svim lokalnim čvorovima, preklopnik osigurava da ga prime svi priključeni hostovi. Ovo se naziva broadcast domenom. Hostovi su svi dio iste lokalne mrežne mreže sloja 2. Ova osnovna zvjezdasta topologija pokazuje određene nedostatke. Broadcast domene s stotinama hostova trpe kazne performansi. Mrežni segment je i 'ravan' u smislu sigurnosti — svaki host može slobodno komunicirati s bilo kojim drugim hostom u istom segmentu. Ovi nedostaci znače da velike mreže koriste hijerarhijalni dizajn s dva ili tri sloja prosljeđivanja. U hijerarhijskom dizajnu postoji niz blokova koje opslužuju pristupni preklopnici, a ti pristupni preklopnici su međusobno povezani usmjerivačima.

preklopnik. Komunikacije između ovih blokova moraju teći putem usmjerivača u jezgrenoj razini i koriste IP adresiranje.

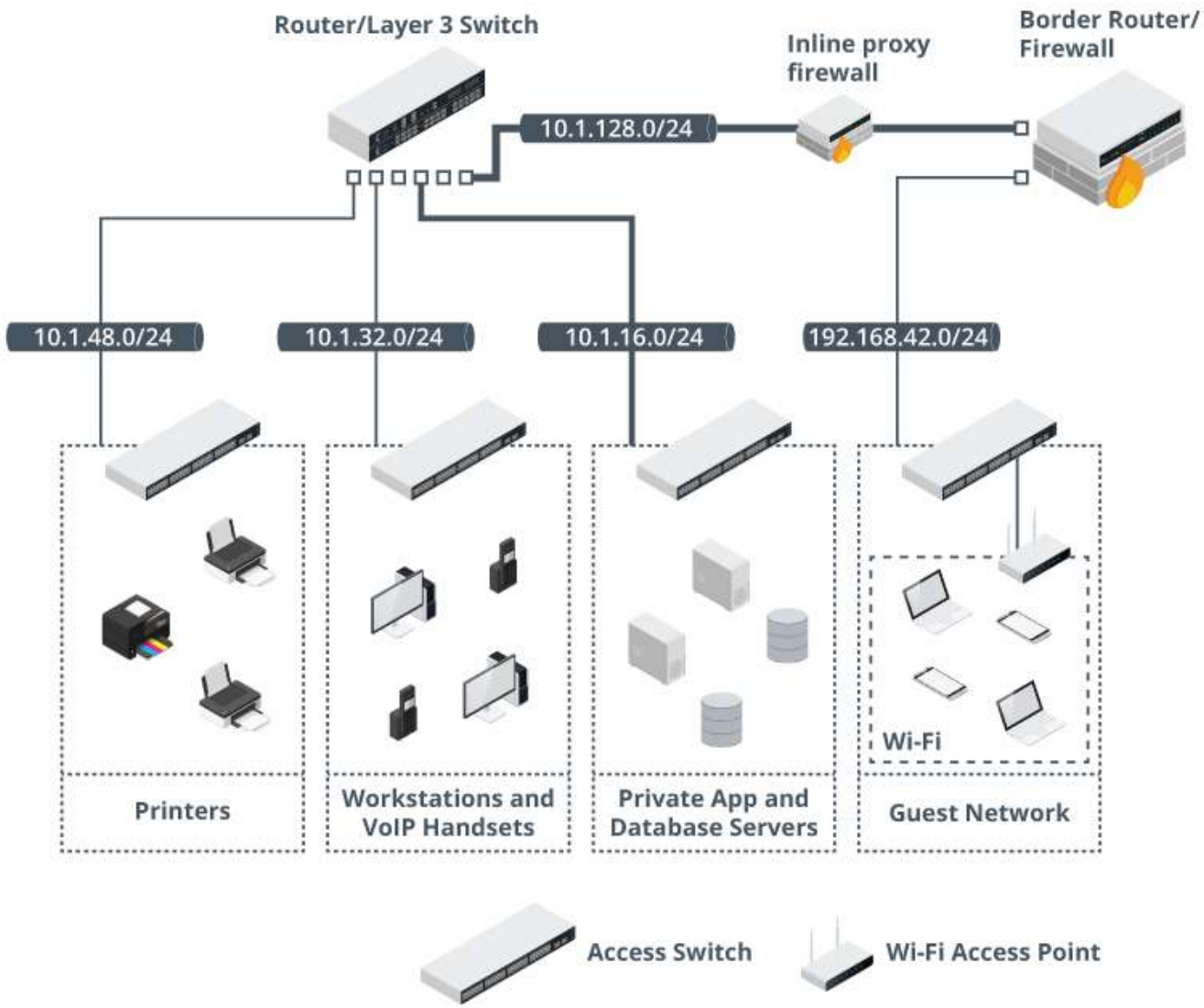


Često ćete vidjeti izraz 'preklopnik sloja 3'. To su uređaji koji implementiraju jezgrenu mrežu. Izvode kombinaciju usmjeravanja i preklapanja. Postoje mnoge vrste preklopnika s različitim ulogama u on-premises i datacenter mrežnim arhitekturama. Dok se klijentske radne stanice priključuju na mrežne preklopnike putem zidnih portova i patch panela, poslužitelji i mrežni uređaji obično su instalirani u zasebnom, sigurnom prostoru koji se naziva sobom za opremu ili serverskom sobom.

Razmatranja usmjeravačke infrastrukture

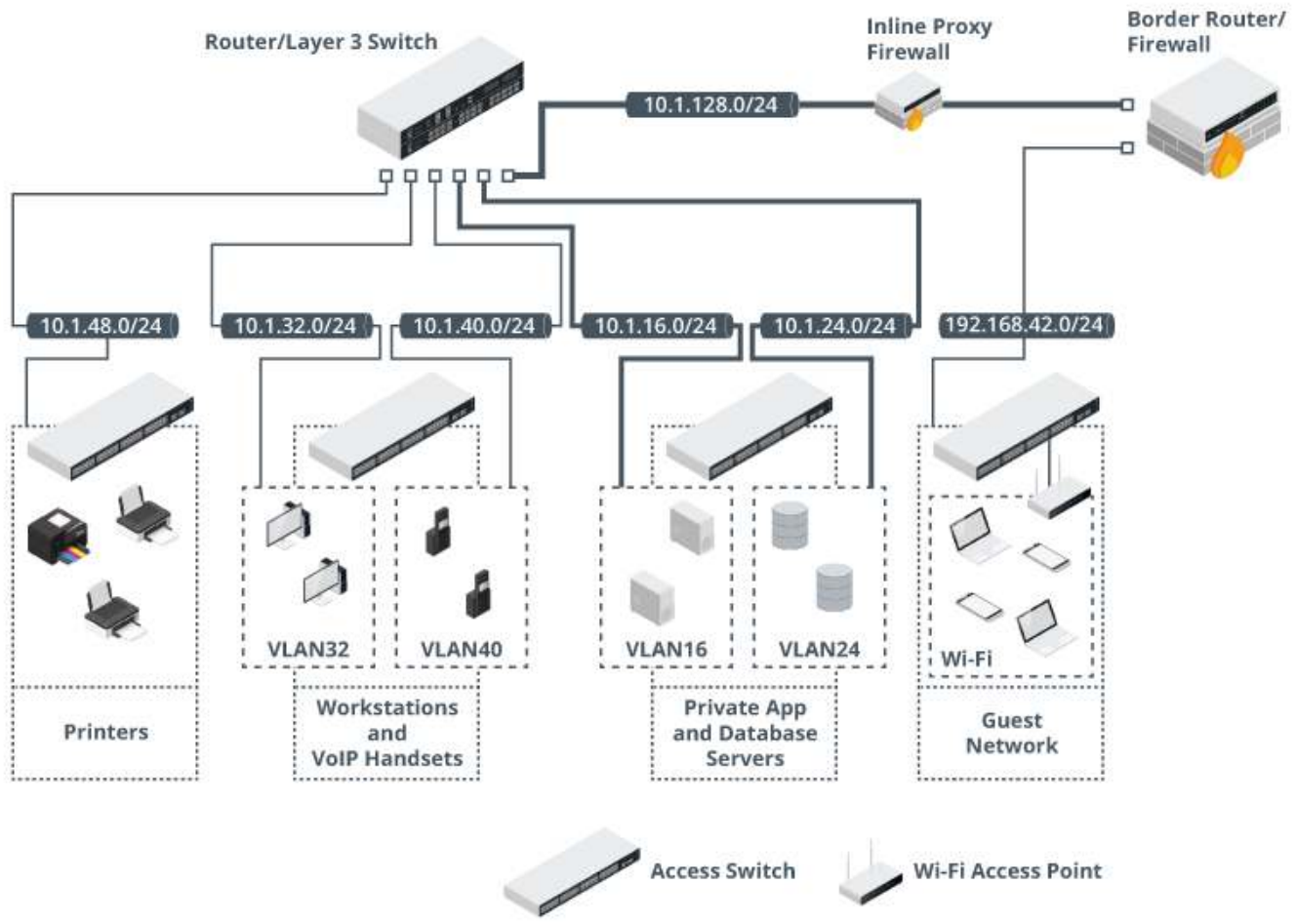
Prosljeđivanje sloja 3, ili usmjeravanje, primjenjuje shemu logičnog adresiranja za identifikaciju svake mreže. Arhitektura sloja 3 predstavlja logičnu segmentaciju mreža i kreiranje mreža unutar mreža, ili podmreža (subnets). Svaka podmreža je zasebna broadcast domena. Internet Protocol (IP) pruža mehanizam adresiranja za logičke mreže i podmreže. 32-bitna IPv4 adresa piše se u decimalnoj notaciji s točkama, s prefiksom mreže ili maskom podmreže.

U hijerarhijskoj mrežnoj arhitekturi, svaki pristupni blok može biti određen kao zasebna IP podmreža. Ovaj sustav logičnog adresiranja sloja 3 olakšava pisanje pravila kontrole pristupa za promet koji je dozvoljen između blokova ili zona. Svaki pristupni blok dobio je podmrežu. Gostujuća mreža je logički odvojena od poslovne LAN i koristi potpuno različitu IP mrežu.



Mreže mogu koristiti i 128-bitno IPv6 adresiranje. IPv6 adrese pišu se u heksadecimalnoj notaciji u općem formatu: 2001:db8::abc:0:def0:1234. U IPv6, zadnjih 64 bita fiksni su kao ID sučelja hosta, a prvih 64 bita sadrže informacije o mreži. Virtualne LAN — Mapiranje logičke IP topologije na fizičke hardverske preklopnike nije uvijek jednostavno. Ovaj problem rješava se virtualnom LAN (VLAN) značajkom koja je podržana kod većine preklopnika. VLAN ID je vrijednost od 2 do 4094. Bilo koji port preklopnika može biti dodijeljen određenom VLAN-u, bez obzira na fizičku lokaciju preklopnika.

dodijeljen određenom VLAN-u, bez obzira na fizičku lokaciju preklopnika. Različiti portovi na istom preklopniku mogu biti dodijeljeni različitim VLAN-ovima. Svaki VLAN je zasebna domena sloja 2. Promet koji se šalje između VLAN-ova koji su spojeni na entitet sloja 3, poput usmjerivača, mora proći kroz uređaj sloja 3 da bi bio proslijeđen. To znači da segmentacija nametnuta VLAN-ovima na sloju 2 može biti mapirana na logičke podjele definirane IP podmrežama na sloju 3.



U dijagramu gore, pristupni blok za klijentske uređaje koristi dva VLAN-a za segmentiranje računalnih radnih stanica (VLAN32) od VoIP uređaja (VLAN40). VLAN-ovi se mapiraju na dvije podmreže: 10.1.32.0/24 i 10.1.40.0/24. VoIP uređaj s IP adresom 10.1.40.100 trebao bi koristiti usmjerivač za kontaktiranje računalnog hosta s IP-om 10.1.32.100. Ova dva hosta možda su spojena na isti preklopnik, ali konfiguracija VLAN-a sprječava ih da izravno međusobno komuniciraju.

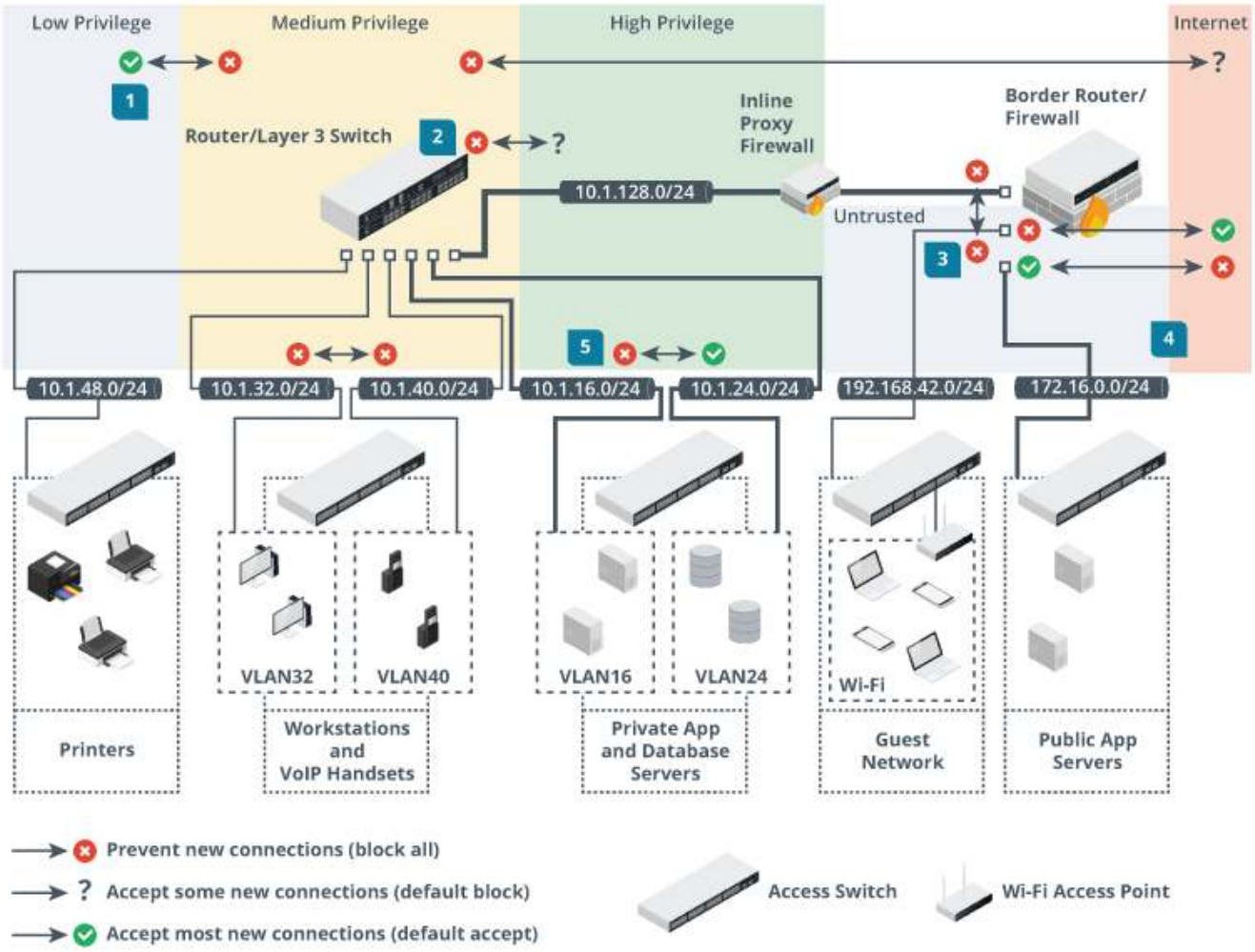
Sigurnosne zone

Mrežne arhitekturne značajke koje kreiraju segmente mapirane na podmreže omogućuju kreiranje sigurnosne topologije temeljene na zonama. On-premises mreže imaju jasnu organizacijsku granicu na mrežnom opsegu (perimetru). Hostovi izvan perimetra nalaze se u zoni javnog Interneta i nisu pouzdani. Hostovi unutar perimetra imat će različite razine povjerenja i zahtjeve kontrole pristupa. Da biste mapirali internu sigurnosnu topologiju, analizirajte sustave i imovinu podataka koji podržavaju tijekove rada i identificirajte one koji imaju slične zahtjeve kontrole pristupa:

- Baze podataka i datotečni sustavi koji pohranjuju podatke tvrtke i osobne podatke trebaju dati prioritet povjerljivosti i integritetu. Podaci obično ne bi trebali biti pohranjeni unutar jedne zone — razmatranje o utjecaju kada je zona kompromitirana važno je za ograničavanje štete.
- Klijentski uređaji trebaju dati prioritet integritetu i dostupnosti. Ovi uređaji ne bi trebali pohraniti podatke i stoga imaju niži zahtjev povjerljivosti.
- Javno dostupni aplikacijski poslužitelji (web, e-mail, udaljeni pristup itd.) trebaju dati prioritet integritetu i dostupnosti. Ne bi trebali pohraniti osjetljive podatke.

- Aplikacijski poslužitelji koji podržavaju mrežnu infrastrukturu (autentikacija, direktorij, praćenje/bilježenje) moraju pokazivati visoke razine povjerljivosti, integriteta i dostupnosti.

Mrežni dijagram koji prikazuje razine privilegija sigurnosnih zona i pojednostavljena pravila pristupa.



Dijagram ilustrira kako promet između hostova u zonama s različitim razinama privilegija može biti podvrgnut kontrolama pristupa: 1. Zona s niskim privilegijama koja sadrži hostove teške za osiguravanje (npr. pisači) može prihvatiti veze, ali ne može inicirati zahtjeve na bilo koje druge hostove. 2. Klijentski uređaji na poslovnoj LAN-u mogu upućivati ovlaštene zahtjeve u različitim zonama, ali ne mogu prihvatiti nove zahtjeve za vezom. 3. Hostovi u gostujućoj zoni mogu pristupiti Internetu, ali im nije dopušten pristup poslovnoj LAN-u. 4. Javno dostupni poslužitelji mogu prihvatiti zahtjeve s Interneta, ali ne mogu inicirati zahtjeve prema poslovnoj LAN-u.

Površina napada

Mrežna površina napada su sve točke u kojima bi akter prijetnje mogao dobiti pristup hostovima i uslugama. Korisno je koristiti model slojeva za analizu potencijalne površine napada:

- Sloj 1/2 — omogućuje neovlaštenim hostovima da se priključe na zidne portove ili bežične mreže i komuniciraju s hostovima unutar iste broadcast domene.

- Sloj 3 — omogućuje neovlaštenim hostovima da dobiju valjanu mrežnu adresu, možda lažiranjem, i komuniciraju s hostovima u drugim zonama.
- Sloj 4/7 — omogućuje neovlaštenim hostovima da uspostave veze na TCP ili UDP portove i komuniciraju s protokolima i uslugama aplikacijskog sloja.

Pored toga, trebate razmatrati vanjsku/javnu površinu napada zasebno od interne/privatne površine napada. Svaki sloj zahtijeva vlastitu vrstu sigurnosnih kontrola za sprječavanje, otkrivanje i ispravljanje napada. Raspoređivanje višestrukih kategorija i funkcija kontrola za provedbu višestrukih slojeva zaštite naziva se obranom u dubinu (defense in depth). Tipične slabosti u mrežnoj arhitekturi uključuju:

- Pojedinačne točke kvara — 'usko grlo' koje ovisi o jednom hardverskom poslužitelju ili uređaju ili mrežnom kanalu.
- Složene ovisnosti — usluge koje zahtijevaju dostupnost mnogih različitih sustava.
- Dostupnost iznad povjerljivosti i integriteta — često je primamljivo uzimati 'prečice' za brzo pokretanje usluge. Kompromitiranje sigurnosti može predstavljati brzi popravak, ali dugoročno stvara rizike.
- Nedostatak dokumentacije i kontrole promjena — mrežni segmenti, uređaji i usluge mogu biti dodani bez odgovarajućih procedura kontrole promjena.
- Previše oslanjanje na sigurnost perimetra — ako je privatna mrežna arhitektura 'ravna' (svaki host može kontaktirati svaki drugi host), prodiranjem u mrežni rub napadaču se daje sloboda kretanja.

Sigurnost portova

Svaki zidni port i port preklopnika predstavlja prilikuza aktere prijetnje da priključe uređaj na mrežu. Pristup fizičkim portovima preklopnika i hardveru preklopnika treba biti ograničen na ovlašteno osoblje. MAC filtriranje i MAC ograničavanje — Konfiguriranje MAC filtriranja znači da port preklopnika dopušta samo određenim MAC adresama da se povežu.

preklopnik će zabilježiti prvih dva MAC-a koji se povežu na taj port, a zatim odbaciti promet s uređaja s različitim MAC adresama. Konfiguriranje ARP inspekcije na Cisco preklopniku.

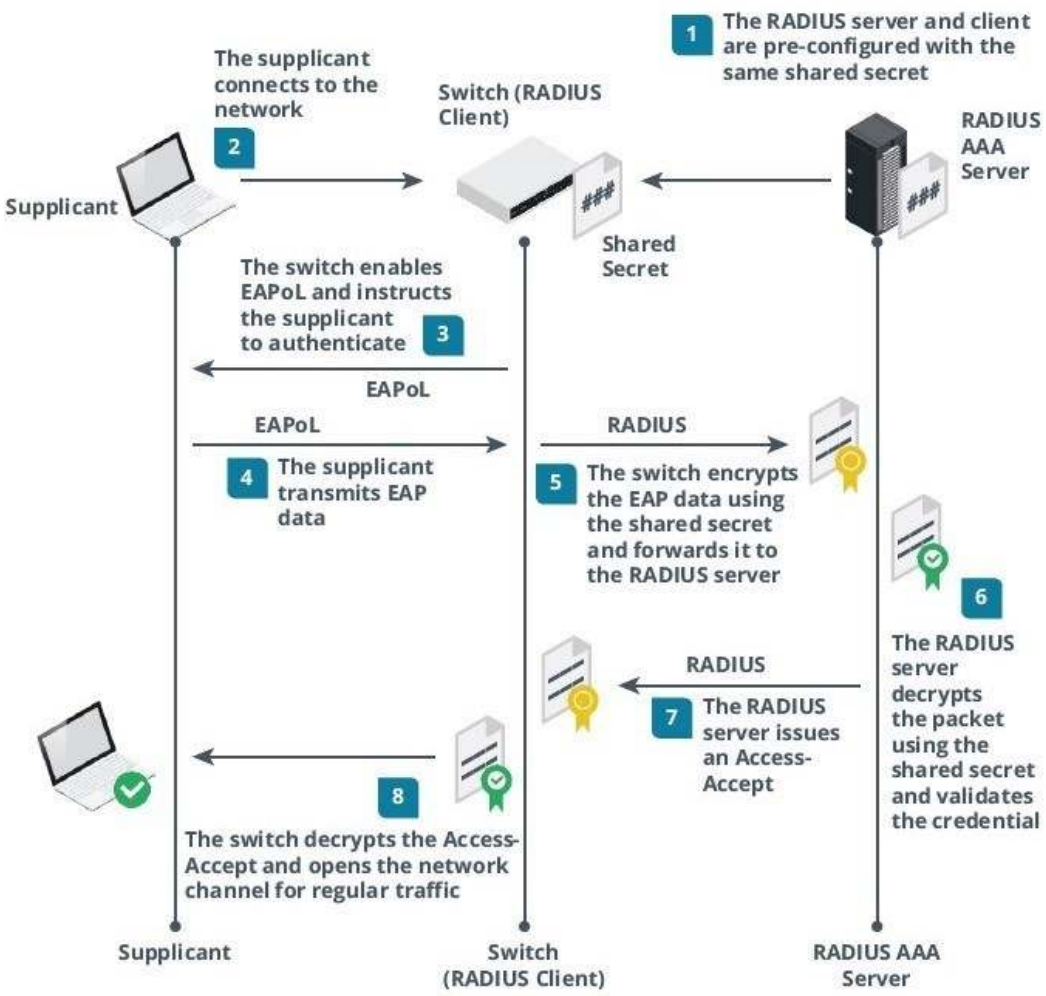
```
NYCORE1>
NYCORE1#
*Mar  1 00:02:27.991: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:02:46.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
NYCORE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NYCORE1(config)#ip arp inspection vlan 1,999
NYCORE1(config)#
*Mar  1 00:07:20.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/23, vlan 1.([0023.049
0.0000/192.168.16.21/00:07:20 UTC Mon Mar 1 1993])
```

802.1X i Extensible Authentication Protocol — Bolja sigurnost dobiva se prisiljavanjem računala i/ili korisnika na autentikaciju prije nego što se odobri potpuni mrežni pristup. IEEE 802.1X Port-based Network Access Control (PNAC) standard omogućuje preklopniku da zahtijeva autentikaciju kada se host priključi na jedan od njegovih portova. 802.1X koristi arhitekturu autentikacije, autorizacije i računovodstva (AAA):

- Podnositelj zahtjeva (Supplicant) — je uređaj koji traži pristup, poput korisnikovog PC-a.

- Autentikator (Authenticator) — je mrežni uređaj koji ne provjerava zahtjeve za autentikacijom direktno, već djeluje kao kanal za autentikacijske podatke.
- Autentikacijski poslužitelj (Authentication server) — poslužitelj koji drži ili može kontaktirati direktorij mrežnih objekata i koji može provjerditi zahtjeve za autentikacijom.
- Extensible Authentication Protocol (EAP) — pruža okvir za implementaciju višestrukih vrsta metoda autentikacije. Često se koristi s digitalnim certifikatima.
- Remote Authentication Dial-In User Service (RADIUS) — omogućuje autentikatoru i autentikacijskom poslužitelju da komuniciraju odluke o autentikaciji i autorizaciji.

IEEE 802.1X Port-based Network Access Control s RADIUS i EAP autentikacijom.



Fizička izolacija

Neki hostovi su toliko sigurnosno kritični da ih je nesigurno priključiti na bilo koju vrstu mreže. Jedan primjer je korijeni CA u PKI. Drugi primjer je host koji se koristi za analizu izvođenja malwarea. Host koji nije fizički spojen ni na jednu mrežu naziva se air-gapped. Fizičko izoliranje hosta ili grupe hostova poboljšava sigurnost, ali donosi i značajne izazove upravljanja. Upravljanje uređajima mora se obavljati na lokalnom terminalu. Sva ažuriranja ili instalacije moraju se obavljati putem USB-a ili optičkih medija, koji su potencijalni vektori napada i moraju se skenirati.

Razmatranja arhitekture

Kada procjenjujete upotrebu određene arhitekture i odabir učinkovitih kontrola, razmatrajte niz čimbenika: troškovi, računalna snaga i responsivnost, skalabilnost, dostupnost, otpornost, potrošnja energije, dostupnost zakrpa i prijenos rizika.

- Troškovi — arhitekturne promjene i nabava uređaja i softvera zahtijevaju početno kapitalano ulaganje. Vrijednost ulaganja u sigurnosnu arhitekturu i kontrole može se izračunati na temelju koliko smanjuju gubitke od incidenata.
- Računalna snaga i responsivnost — minimizacija vremena obrade za radna opterećenja. Svaki mrežni uređaj zahtijeva dovoljno resursa CPU-a, sistemske memorije, pohrane i mrežne propusnosti.
- Skalabilnost i jednostavnost implementacije — minimizacija troškova kada se radna opterećenja povećavaju ili smanjuju. Skalabilan sustav može brzo ili automatski dodavati ili uklanjati računalne resurse bez prekomjernih troškova.
- Dostupnost — minimizira zastoj ili maksimizira radni vijek. Zastoj može biti zbog planiranog održavanja ili neplaniranih kvarova i sigurnosnih incidenata.
- Otpornost i jednostavnost oporavka — smanjuje vrijeme oporavka od kvara. Sustav koji se oporavlja od kvara bez ručne intervencije otporniji je od onog koji zahtijeva pokretanje od strane administratora.
- Energija — značajka koja osigurava da objekt može zadovoljiti energetske zahtjeve svojih uređaja i radnih opterećenja.
- Dostupnost zakrpa — osigurava da je firmware i softverski kod zaštićen od exploita za poznate ranjivosti.
- Prijenos rizika — ugovor koji koristi treću stranu za upravljanje mrežnom infrastrukturom. Ugovor o razini usluge (SLA) može biti definiran s kaznama ako se metrike za responsivnost, skalabilnost, dostupnost i otpornost ne maintainaju.

Lekcija 5B

Mrežni sigurnosni uređaji

Pregled lekcije

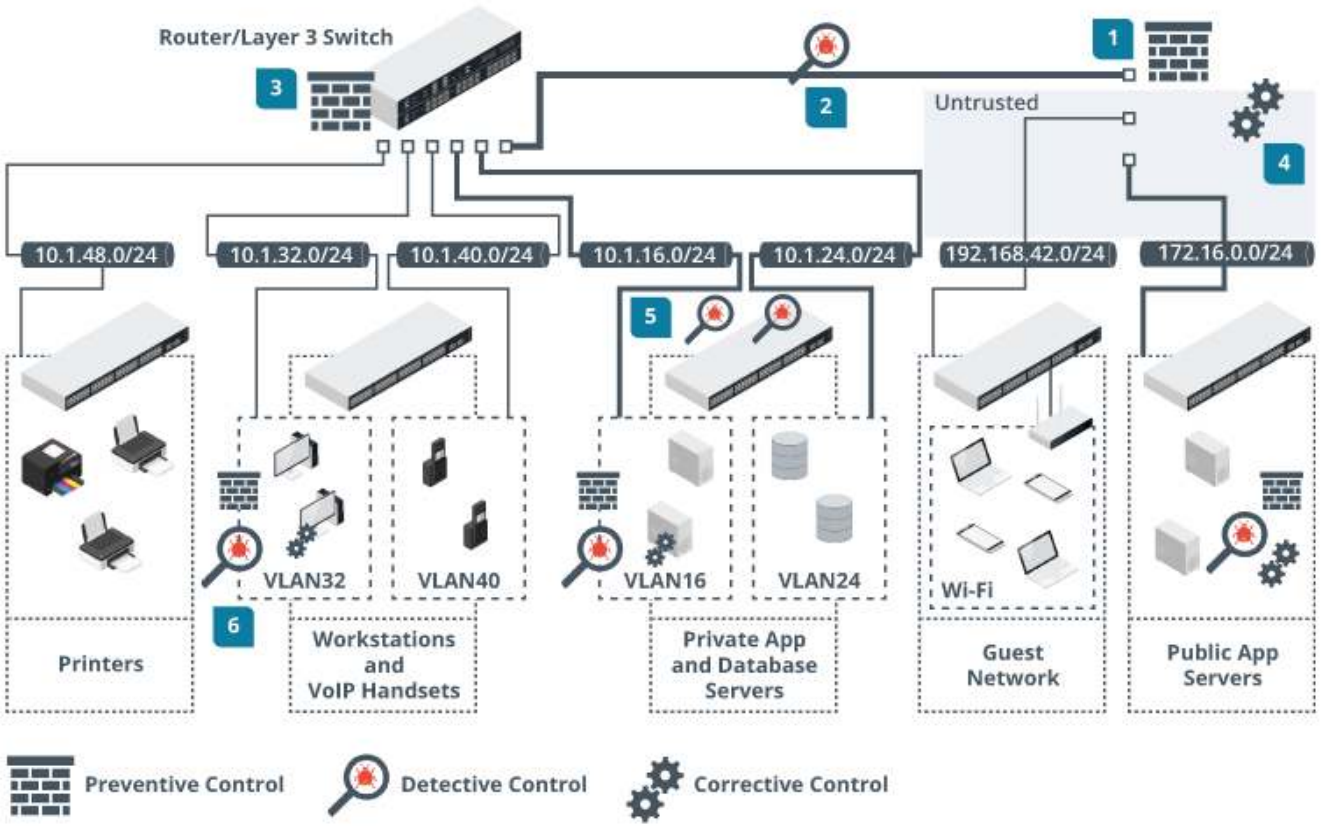
Uz sigurnosnu arhitekturu temeljenu na zonama, mrežni sigurnosni uređaji osiguravaju da promet koji teče između zona i unutar zona zadovoljava politike kontrole pristupa. Odabir kontrola na temelju njihovih funkcija i atributa te njihovo odgovarajuće postavljanje unutar topologije ključno je za osiguranje učinkovite mrežne sigurnosti.

Postavljanje uređaja

Odabir učinkovitih kontrola za mrežnu infrastrukturu je proces odabira vrste i postavljanja sigurnosnih uređaja i softvera. Cilj je provedba segmentacije, primjena kontrola pristupa i praćenje prometa zbog kršenja politike. Postoje tri opcije postavljanja:

- Preventivne kontrole — često se postavljaju na granicu mrežnog segmenta ili zone. Preventivne kontrole poput vatrozida provode sigurnosne politike na promet koji ulazi i izlazi iz segmenta.
- Detektivne kontrole — mogu biti postavljene unutar perimetra za praćenje prometa koji se razmjenjuje između hostova unutar segmenta. Pruža upozorenja o zlonamjernom prometu koji je izbjegao perimeterske kontrole.
- Korektivne kontrole — mogu biti postavljene unutar prometa za ispravljanje otkrivenih grešaka ili nepravilnosti.
- Preventivne, detektivne i korektivne kontrole — mogu biti instalirane na hostovima kao sloj zaštite krajnjih točaka, uz kontrole mrežne infrastrukture.

Postavljanje sigurnosnih kontrola za osiguravanje raznovrsnosti i obrane u dubinu.



Dijagram prikazuje kako različite vrste kontrola mogu biti postavljene unutar mreže za osiguravanje obrane u dubinu: 1. Na mrežnoj granici, preventivna kontrola poput vatrozida provodi pravila pristupa za ulazni i izlazni promet. 2. Senzor postavljen inline iza graničnog vatrozida prenosi promet na sustav za otkrivanje upada za implementaciju detektivne kontrole. 3. Liste kontrole pristupa konfigurirane na internim usmjerivačima provode pravila za promet koji se prosljeđuje između internih zona. 4. Dolazni promet za javno dostupne poslužitelje može biti posredovan load balancerom. 5. Senzori priključeni na zrcalne portove preklopnika omogućuju otkrivanje upada za hostove ili zone s višim privilegijama. 6. Na svakom hostu, softver za zaštitu krajnjih točaka primjenjuje niz preventivnih, detektivnih i korektivnih kontrola.

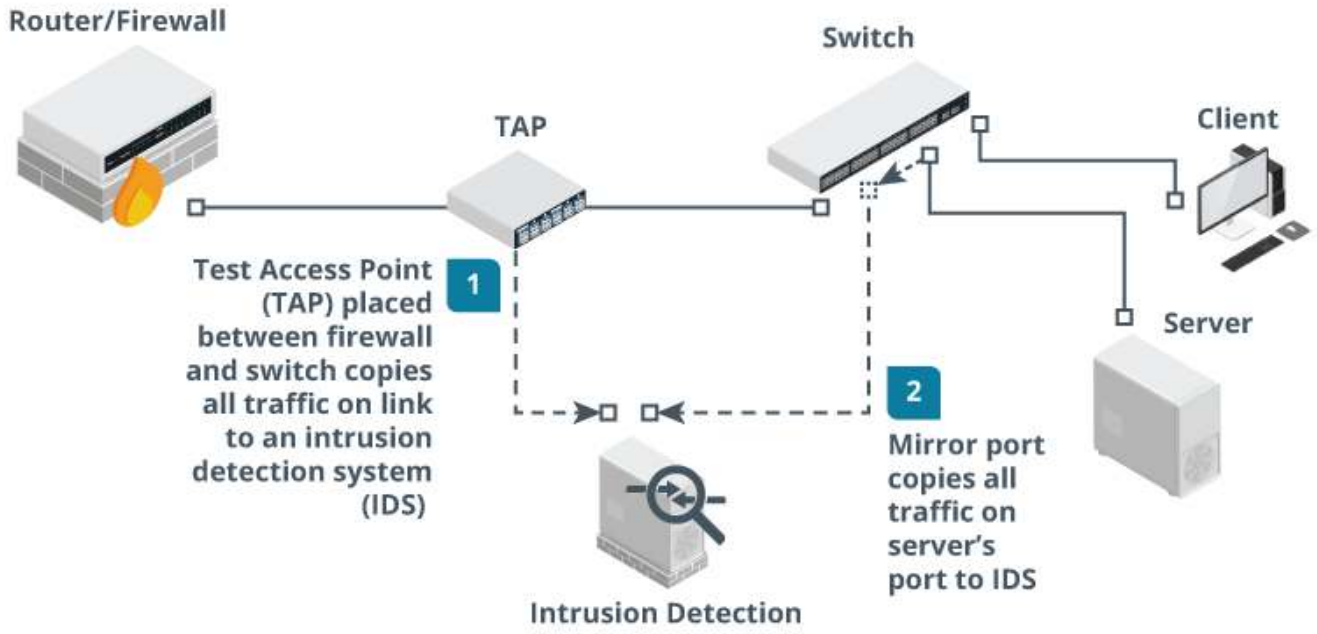
Atributi uređaja

Atributi određuju precizan način na koji uređaj može biti postavljen unutar mrežne topologije. Pasivna sigurnosna kontrola je ona koja ne zahtijeva nikakvu konfiguraciju klijenta za rad. Aktivna sigurnosna kontrola koja izvodi skeniranje mora biti konfigurirana s vjerodajnicama i dozvolama pristupa.

Aktivna kontrola koja izvodi filtriranje zahtijeva da hostovi budu izričito konfigurirani za korištenje kontrole. Inline uređaji i metode praćenja — Uređaj koji je raspoređen inline postaje dio kabelskog puta. Inline uređaj može kopirati mrežni promet na monitor ili senzor. Senzor može biti konfiguriran za primanje prometa na dva različita načina:

- Test access point (TAP) — inline je uređaj s portovima za dolazno i odlazno mrežno kabliranje i induktor ili optički splitter koji fizički kopira signal iz kabliranja na monitor port. Kao hardversko rješenje fizičkog sloja, ne donose se logičke odluke pa monitor port prima svaki okvir.
- SPAN (switched port analyzer)/ogledalo port — senzor je priključen na posebno konfiguriran ogledalo port na preklopniku koji prima kopije okvira upućenih određenim

pristupnim portovima. Ova metoda nije potpuno pouzdana — okviri s pogreškama neće biti zrcaljeni i okviri mogu biti odbačeni pod velikim opterećenjem.



Fail-Open nasuprot Fail-Closed

Sigurnosni uređaj može ući u stanje kvara iz više razloga: kvar napajanja ili hardvera, nezagodiva povreda politike ili greška konfiguracije. Kada zakaže, uređaj može biti dizajniran ili konfiguriran za fail-open ili fail-closed.

Kada zakaže, uređaj može biti dizajniran ili konfiguriran za fail-open ili fail-closed:

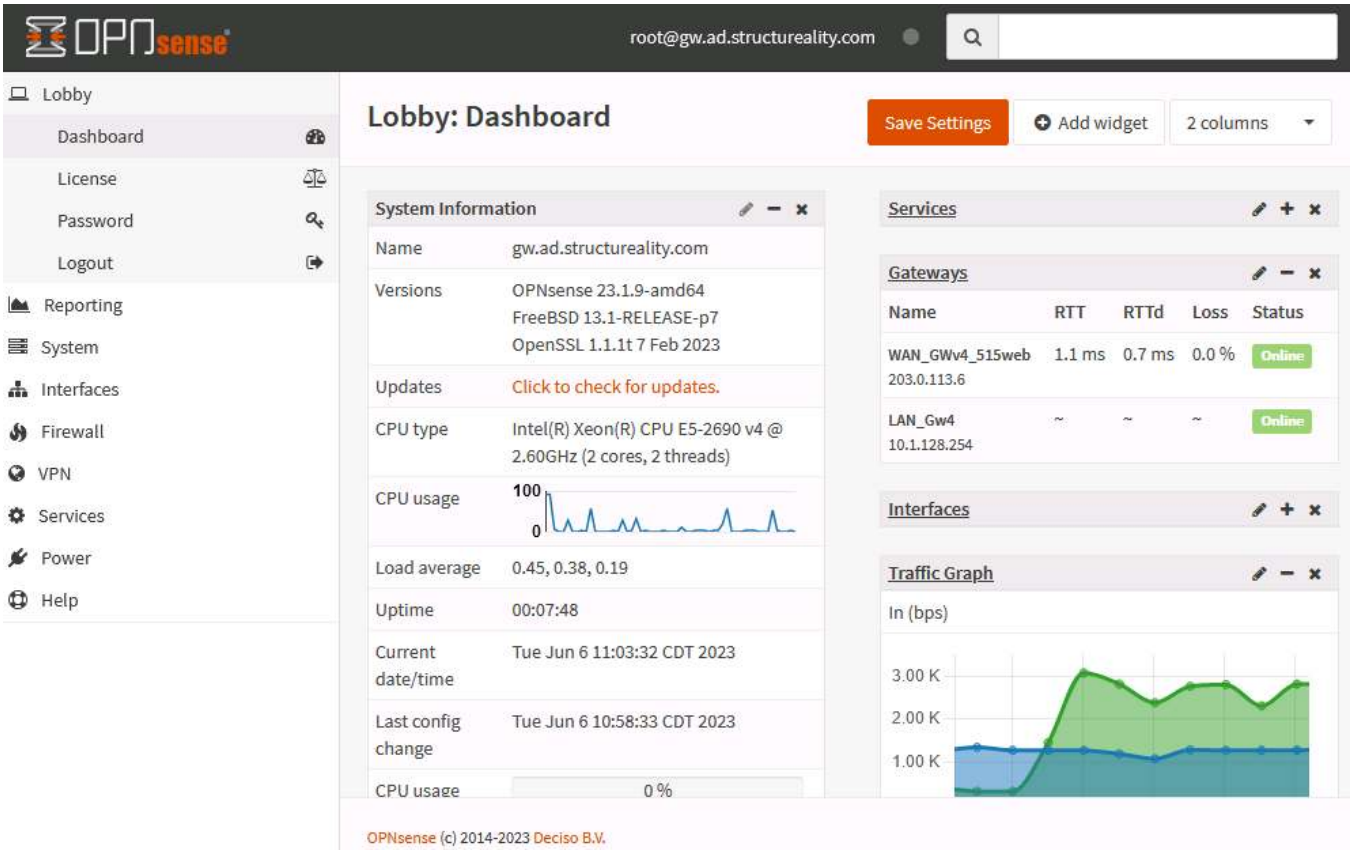
- Fail-open znači da se pristup mreži ili hostu čuva, ako je moguće. Ovaj način daje prednost dostupnosti nad povjerljivosti i integritetom. Rizik fail-open kontrole je da akter prijetnje može osmisliti stanje kvara da bi porazio kontrolu.
- Fail-closed znači da je pristup blokiran ili da sustav ulazi u najsigurnije dostupno stanje, s obzirom na kvar koji je nastao. Ovaj način daje prednost povjerljivosti i integritetu nad dostupnosti. Rizik fail-closed kontrole je zastoj sustava.

Vatrozidi

Vatrozid je preventivna kontrola dizajnirana za provedbu politika na promet koji ulazi i izlazi iz mrežne zone. Filtriranje paketa — Vatrozid za filtriranje paketa konfiguriran je specificiranjem grupe pravila nazvane popis kontrole pristupa (ACL). Svako pravilo definira specifičnu vrstu paketa podataka i radnju koju treba poduzeti kada paket odgovara pravilu. Vatrozid za filtriranje paketa može pregledati zaglavlja IP paketa. Pravila se temelje na informacijama pronađenim u tim zaglavljima:

- IP filtriranje — prihvaća ili odbija promet na temelju izvorišnih i/ili odredišnih IP adresa.
- ID/vrsta protokola — IP paket koji nosi identificirani protokol, najčešće TCP ili UDP.
- Filtriranje porta/sigurnost — prihvaća ili odbija paket na temelju izvorišnih i odredišnih TCP/UDP brojeva portova.
- Usmjereni (sloj 3) — vatrozid izvodi prosljeđivanje između podmreža. Svako sučelje na vatrozidu spaja se na različitu podmrežu i predstavlja različitu sigurnosnu zonu.

- Premošćeni (sloj 2) — vatrozid pregledava promet koji prolazi između dva čvora, kao što su usmjerivač i preklopnik.
- Inline (sloj 1) — vatrozid djeluje kao kabelski segment. Dva sučelja nemaju MAC ni IP adrese. Promet primljen na jednom sučelju ili se blokira ili prosljeđuje na drugo. Ovo se naziva i virtualnom žicom (virtual wire) ili bump-in-the-wire.

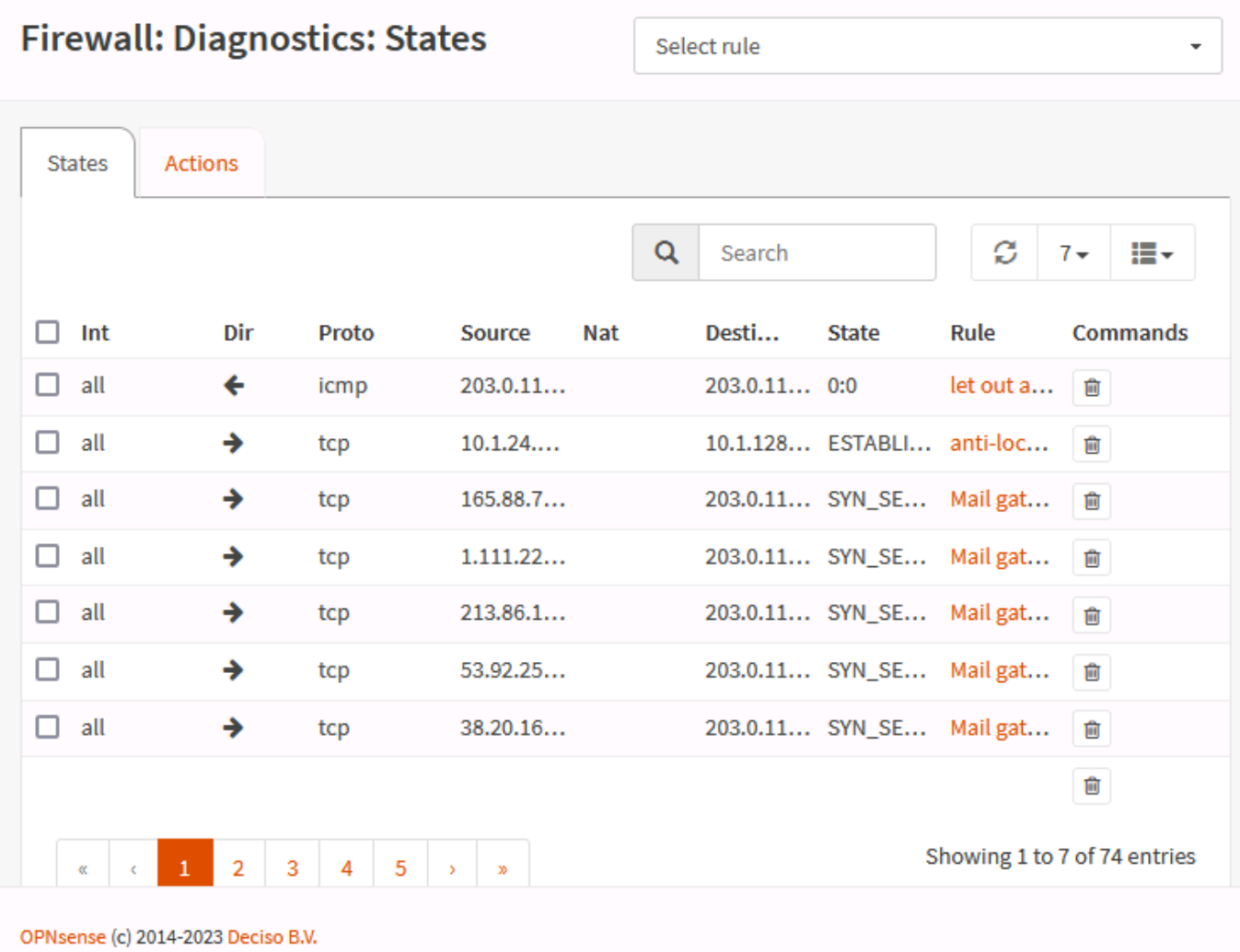


Usmjerivački vatrozid ili vatrozid-usmjerivač implementira funkcionalnost filtriranja kao dio firmware-a usmjerivača. SOHO (Small Office/Home Office) Internet usmjerivači dolaze s ugrađenim vatrozidom.

Vatrozidi sloja 4 i sloja 7

Osnovno filtriranje paketa je bez stanja (stateless). To znači da ne čuva informacije o mrežnim sesijama. Svaki paket analizira se neovisno, bez zapisa o prethodno obrađenim paketima. Vatrozid s inspekcijom stanja (stateful inspection) prati informacije o sesiji uspostavljenoj između dva hosta. Svi vatrozidi sada uključuju određenu razinu sposobnosti inspekcije stanja. Podaci sesije pohranjuju se u tablici stanja.

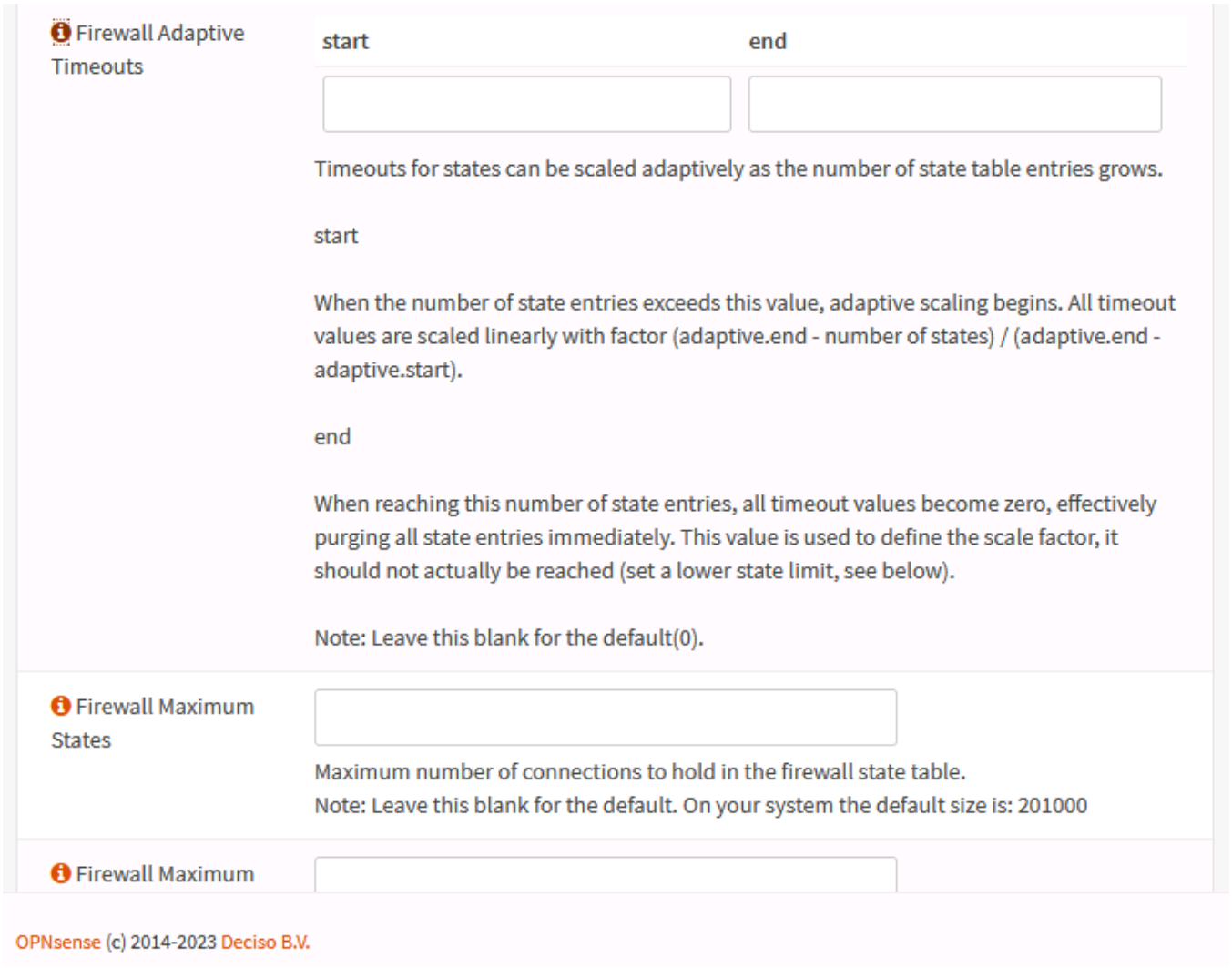
Vatrozid s inspekcijom stanja prati informacije o sesiji uspostavljenoj između dva hosta. Svi vatrozidi sada uključuju određenu razinu sposobnosti inspekcije stanja. Podaci sesije pohranjuju se u tablici stanja. Kada paket pristigne, vatrozid ga provjerava kako bi potvrdio pripada li postojećoj vezi. Tablica stanja u vatrozidnom uređaju OPNsense.



Inspekcija stanja može se odvijati na sloju 4 i sloju 7. Vatrozid sloja 4 pregledava TCP trosmjerni rukovanje (handshake) kako bi razlikovao nove od uspostavljenih veza. Legitimna TCP veza treba slijediti SYN > SYN/ACK > ACK redoslijed za uspostavljanje sesije. Odstupanja od ovoga, poput SYN-a bez ACK-a ili anomalija rednih brojeva, mogu biti odbačena kao zlonamjerni napadi poplavljanja ili preotimanja sesije.

Konfiguracija pravila vatrozida OPNsense

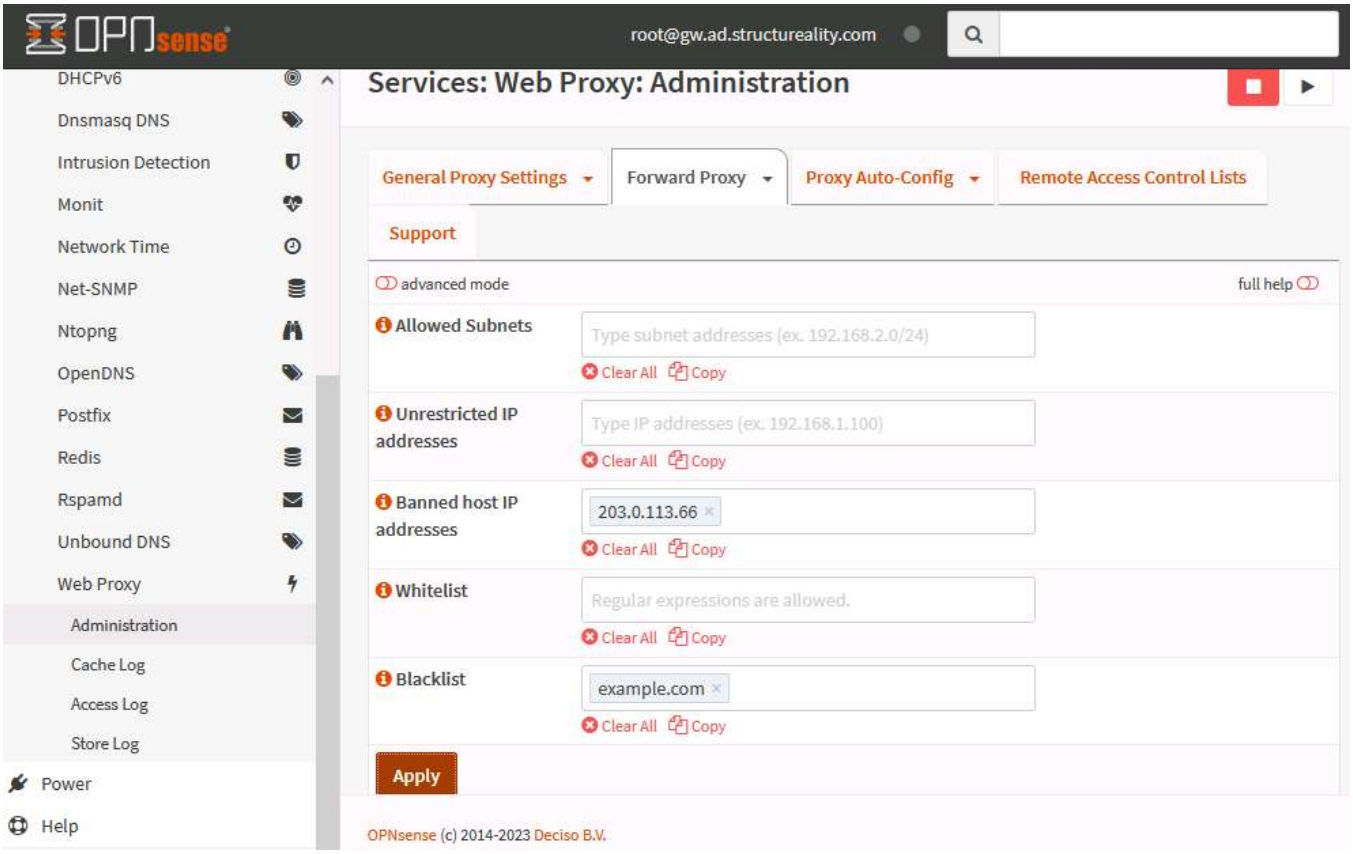
Napredne postavke omogućuju primjenu maksimalnih vrijednosti za stanja i veze.



Vatrozid sloja 7 može pregledati zaglavlja i sadržaj paketa aplikacijskog sloja. Jedna ključna značajka je provjera odgovara li aplikacijski protokol portu, jer malware može pokušati slati sirove TCP podatke putem porta 80 samo zato što je port 80 otvoren. Proxy poslužitelji — Vatrozid koji izvodi filtriranje aplikacijskog sloja vjerojatno je implementiran kao proxy. Gdje mrežni vatrozid samo prihvaća ili blokira promet, proxy poslužitelj radi na modelu pohrani-i-proslijedi. Proxy dekonstruira svaki paket, izvodi analizu, zatim rekonstruira paket i prosljeđuje ga.

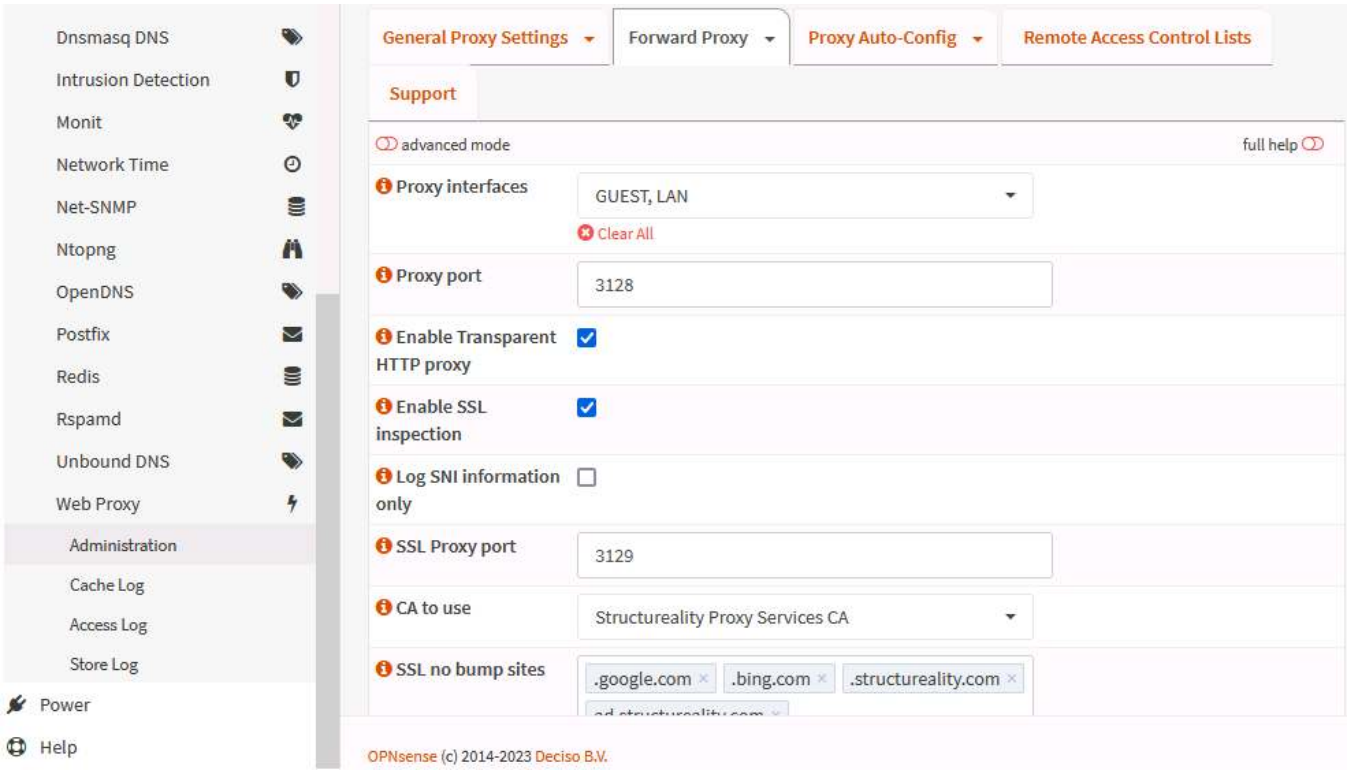
Proxy poslužitelji prema naprijed (Forward Proxy Servers)

Forward proxy pruža protokol-specifičan odlazni promet. Na primjer, web proxy omogućuje klijentskim računalima na lokalnoj mreži da se povežu na web stranice na Internetu. Ovo je forward proxy koji opslužuje TCP portove 80 i 443 za odlazni promet. Konfiguriranje postavki filtra za proxy poslužitelj s predmemoriranjem koji radi na OPNsense.



Glavna prednost proxyja je da se klijentska računala povezuju na specificiranu točku na perimetarnoj mreži za web pristup. Ovo pruža određenu mjeru upravljanja prometom i sigurnosti. Proxy poslužitelji također pružaju mehanizme predmemoriranja, pri čemu se često zatražene web stranice zadržavaju na proxyu, eliminiranjem potrebe za ponovnim dohvaćanjem tih stranica za naknadne zahtjeve.

- Ne-transparentni proxy znači da klijent mora biti konfiguriran s adresom proxy poslužitelja i brojem porta za njegovo korištenje.
- Transparentni (ili prisilni ili presrećajući) proxy presreće klijentski promet bez potrebe da klijent bude rekonfiguriran. Transparentni proxy mora biti implementiran kao usmjerivač ili inline mrežni uređaj.



Oba tipa proxyja mogu biti konfigurirana da zahtijevaju autentikaciju korisnika prije dopuštanja pristupa. Proxy vjerojatno može koristiti jednokratnu prijavu (SSO) da to učini bez traženja lozinke od korisnika.

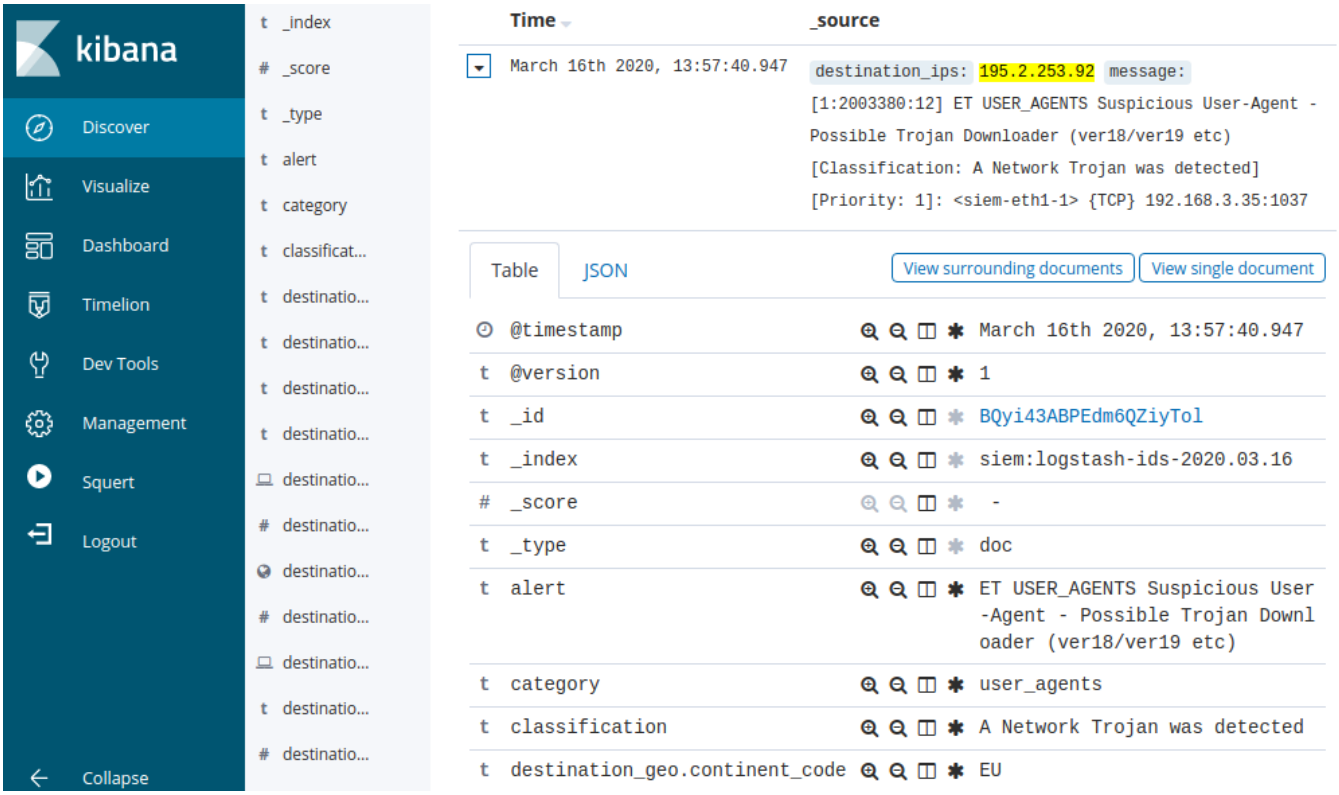
Proxy poslužitelji prema natrag (Reverse Proxy Servers)

Reverse proxy poslužitelj pruža protokol-specifičan dolazni promet. Reverse proxy je tipično raspoređen na mrežnom rubu i konfiguriran za slušanje zahtjeva klijenata s javne mreže (Interneta). Proxy primjenjuje pravila filtriranja i, ako su prihvaćena, kreira odgovarajući zahtjev i prosljeđuje ga na aplikacijski poslužitelj unutar sigurno zaštićene screened subnet zone na lokalnoj mreži.

Sustavi za otkrivanje upada

Sustav za otkrivanje upada (IDS) je kontrola koja izvodi analizu u stvarnom vremenu mrežnog prometa ili zapisnika sustava i aplikacija. Senzori — Mrežni IDS bilježi promet putem packet sniffera koji se naziva senzor. Senzor može koristiti SPAN/ogledalo port ili inline TAP.

može zabilježiti veliku količinu podataka o prometu pa ne možete postaviti višestruke senzore svugdje u mreži bez osiguravanja resursa za njihovo pravilno upravljanje. Ovisno o veličini mreže i resursima, jedan ili nekoliko senzora raspoređuje se za praćenje ključnih resursa ili mrežnih putova.



Sustavi za otkrivanje upada

Promet zabilježen od strane svakog senzora prenosi se na host ili uređaj koji pokreće IDS, poput Snorta, Suricata ili Zeek/Bro. Kada promet odgovara potpisu za otkrivanje ili heurističnom uzorku, IDS podiže upozorenje ili generira unos zapisnika, ali ne blokira izvorišni host. Ovaj tip pasivnog senzora ne usporava promet i neotkriven je od strane napadača.

Sustavi za sprječavanje upada

Sustav za sprječavanje upada (IPS) je uređaj ili softver sposoban za aktivni odgovor. IPS skenira promet za usklađivanje s potpisima za otkrivanje i može biti konfiguriran za automatsko djelovanje u zaustavljanju napada. Tipični odgovori:

- Blokiranje izvora nesukladnog prometa, privremeno ili trajno. Ovo se naziva shunning.
- Resetiranje veze bez blokiranja izvorišne adrese.
- Preusmjeravanje prometa na honeypot ili honeynet za dodatnu analizu prijetnji.

Napomena: I Snort i Suricata mogu biti konfigurirani kao sustavi za sprječavanje upada.

Vatrozidi sljedeće generacije i unificiranog upravljanja prijetnjama — Vatrozid sljedeće generacije (NGFW) kombinira tradicionalne funkcionalnosti vatrozida s naprednim mogućnostima, kao što su duboka inspekcija paketa, sprječavanje upada i svijest o aplikacijama. Tipične značajke uključuju:

- Filtriranje svjesno aplikacija sloja 7, uključujući inspekciju TLS šifriranog prometa.
- Integracija s mrežnim direktorijima, olakšavajući politike filtriranja po korisniku ili ulozi.
- Funkcionalnost IPS-a.
- Integracija s cloud umrežavanjem.

Unificiranom upravljanje prijetnjama (UTM) odnosi se na sigurnosni proizvod koji centralizira mnoge vrste sigurnosnih kontrola — vatrozid, antimalware, mrežno

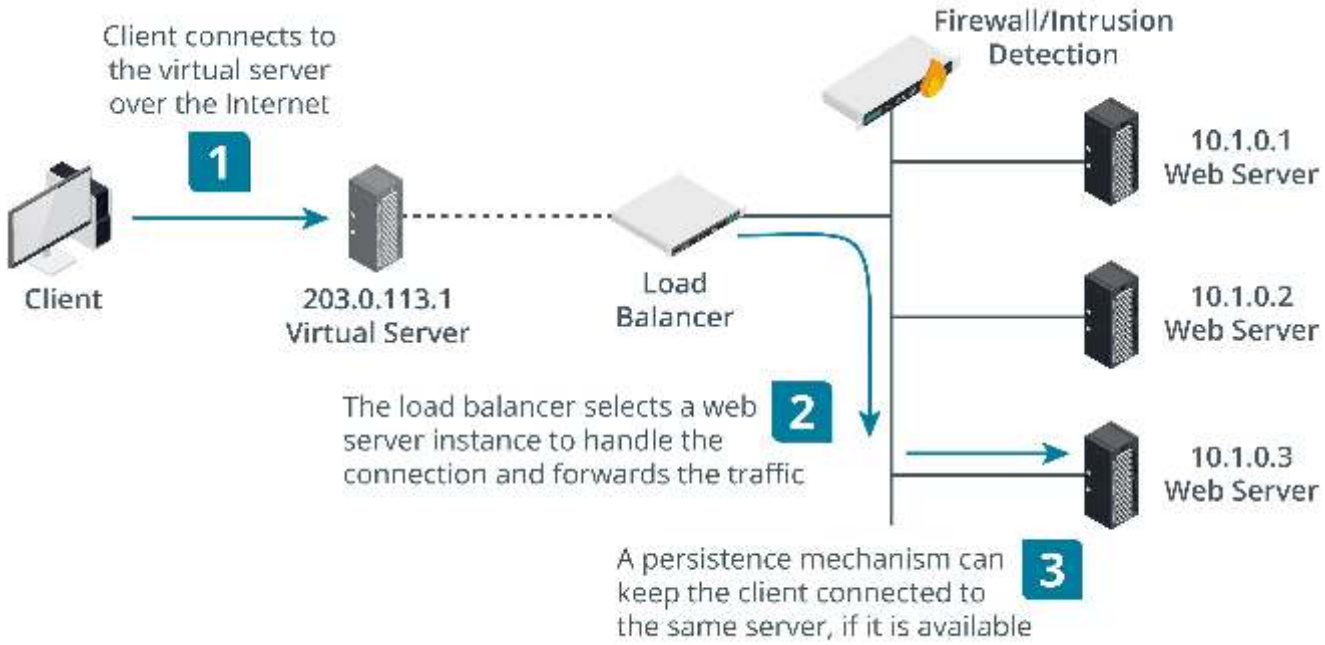
sprječavanje upada, filtriranje spam-a, filtriranje sadržaja, sprječavanje gubitka podataka, VPN — u jedan uređaj.

Load balanceri

Load balancer distribuira zahtjeve klijenata po dostupnim serverskim čvorovima u farmi ili skupu. Koristi se za provisioning usluga koje mogu skalirati od lakih do teških opterećenja i za ublažavanje napada uskraćivanja usluge. Load balancer se može rasporediti u bilo kojoj situaciji gdje postoji više poslužitelja koji pružaju istu funkciju.

- Load balancer sloja 4 — osnov load balanceri donose odluke prosljeđivanja na temelju IP adrese i vrijednosti TCP/UDP porta.
- Load balancer sloja 7 (content switch) — moderni load balanceri trebaju biti u stanju donositi odluke prosljeđivanja na temelju podataka na razini aplikacije.

ili vrsta podataka poput video ili audio streaminga. Ovo zahtijeva složeniju logiku, ali je procesna snaga modernih uređaja dovoljna za rješavanje ovoga. Topologija osnovne arhitekture load balanciranja.



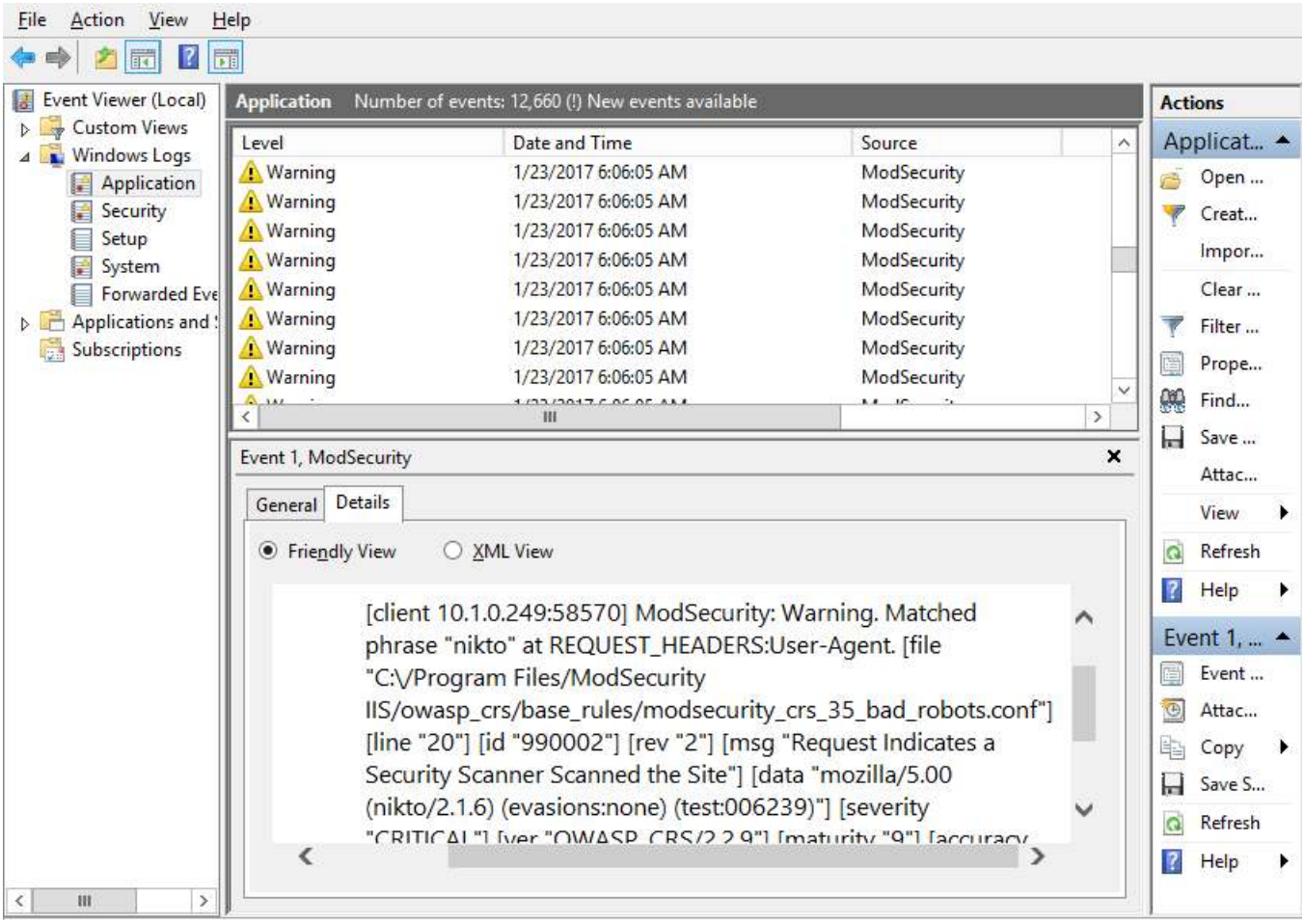
Raspoređivanje

Algoritam raspoređivanja je kod i metrike koje određuju koji čvor je odabran za obradu svakog dolaznog zahtjeva. Najjednostavnija vrsta raspoređivanja zove se round robin. Drugi metodiuključuju odabir čvora s najmanje veza ili s najboljim vremenom odgovora. Load balancer mora koristiti heartbeat ili provjeru zdravlja (health check) za provjeru dostupnosti svakog čvora.

Web aplikacijski vatrozidi (WAF)

WAF je dizajniran za zaštitu softvera koji se pokreće na web poslužiteljima i njihovim back-end bazama podataka od napada ubrizgavanja koda i napada uskraćivanja usluge. WAF-ovi koriste pravila svjesna aplikacija za filtriranje prometa i izvođenje inspekcije upada specifičnih za aplikaciju.

WAF može biti programiran s potpisima poznatih napada i koristiti podudaranje uzoraka za blokiranje zahtjeva koji sadrže sumnjivi kod. Izlaz iz WAF-a bit će zapisan u zapisnik, koji može otkriti potencijalne prijetnje web aplikaciji. WAF može biti raspoređen kao uređaj koji štiti zonu u kojoj je web poslužitelj smješten ili kao plug-in softver za web poslužiteljsku platformu.



Lekcija 5C

Sigurna komunikacija

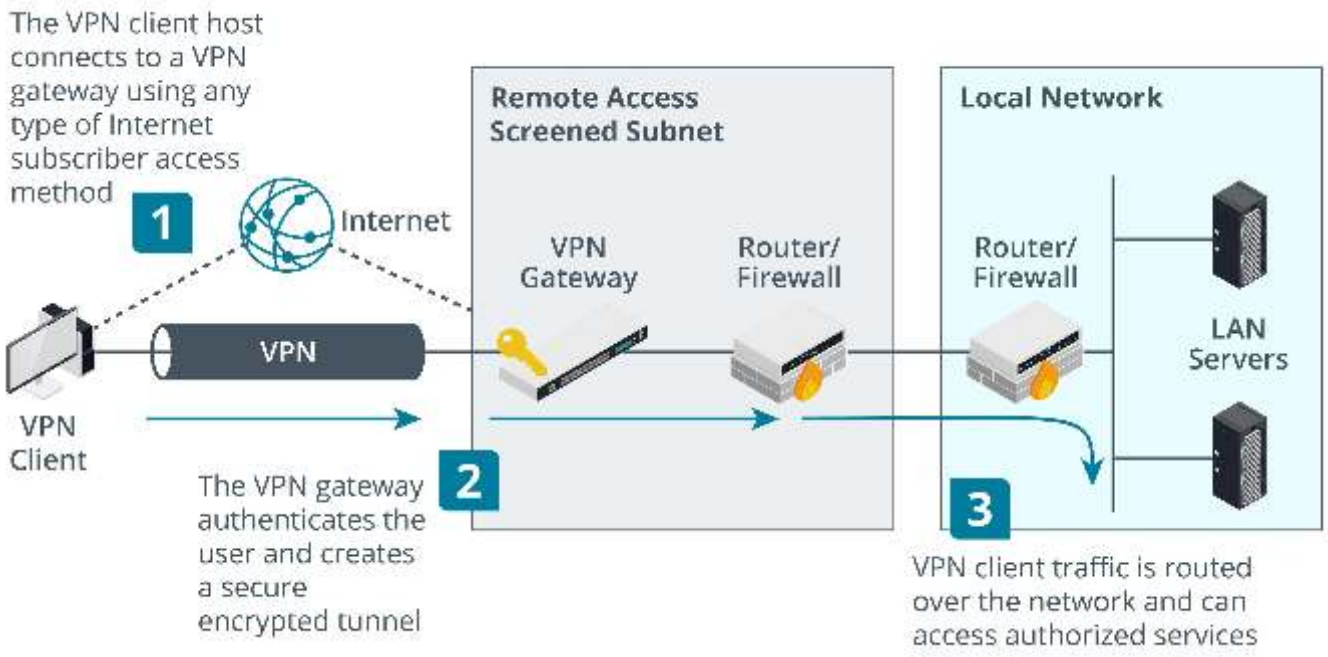
Pregled lekcije

S današnjom mobilnom radnom snagom, većina mreža mora podržavati veze udaljenih zaposlenika, ugovaratelja i kupaca. Ove veze često koriste nepouzdane javne mreže poput Interneta. Shodno tome, razumijevanje kako implementirati sigurne komunikacijske protokole za virtualno umrežavanje bit će veliki dio vašeg posla kao informatičkog sigurnosnog stručnjaka.

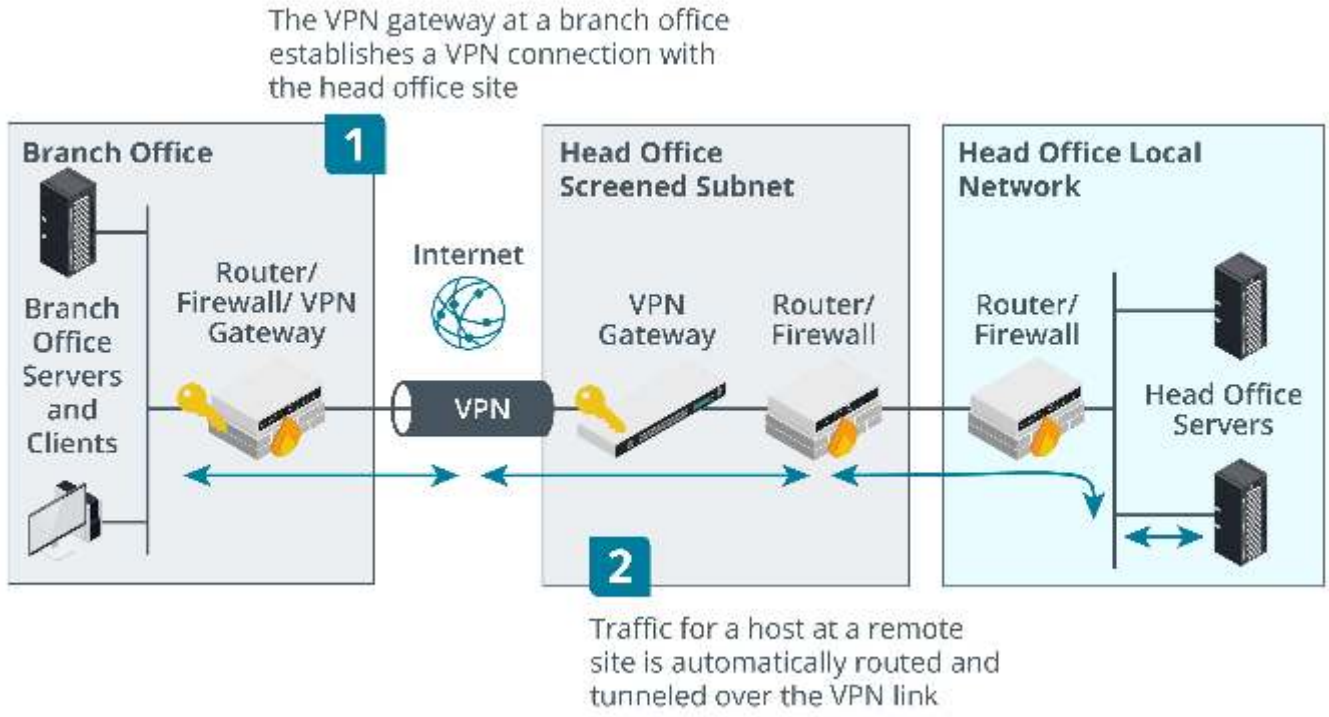
Arhitektura udaljenog pristupa

Umrežavanje udaljenim pristupom znači da se korisnikov uređaj ne priključuje izravno kabelski ili bežično na mrežu. Veza se odvija putem ili kroz posrednu mrežu. Većina udaljenog pristupa implementirana je kao virtualna privatna mreža (VPN) koja radi putem mreža pružatelja internetskih usluga. VPN protokol uspostavlja sigurni tunel za čuvanje privatnosti sadržaja, čak i kada paketi prolaze kroz ISP-ove usmjerivače.

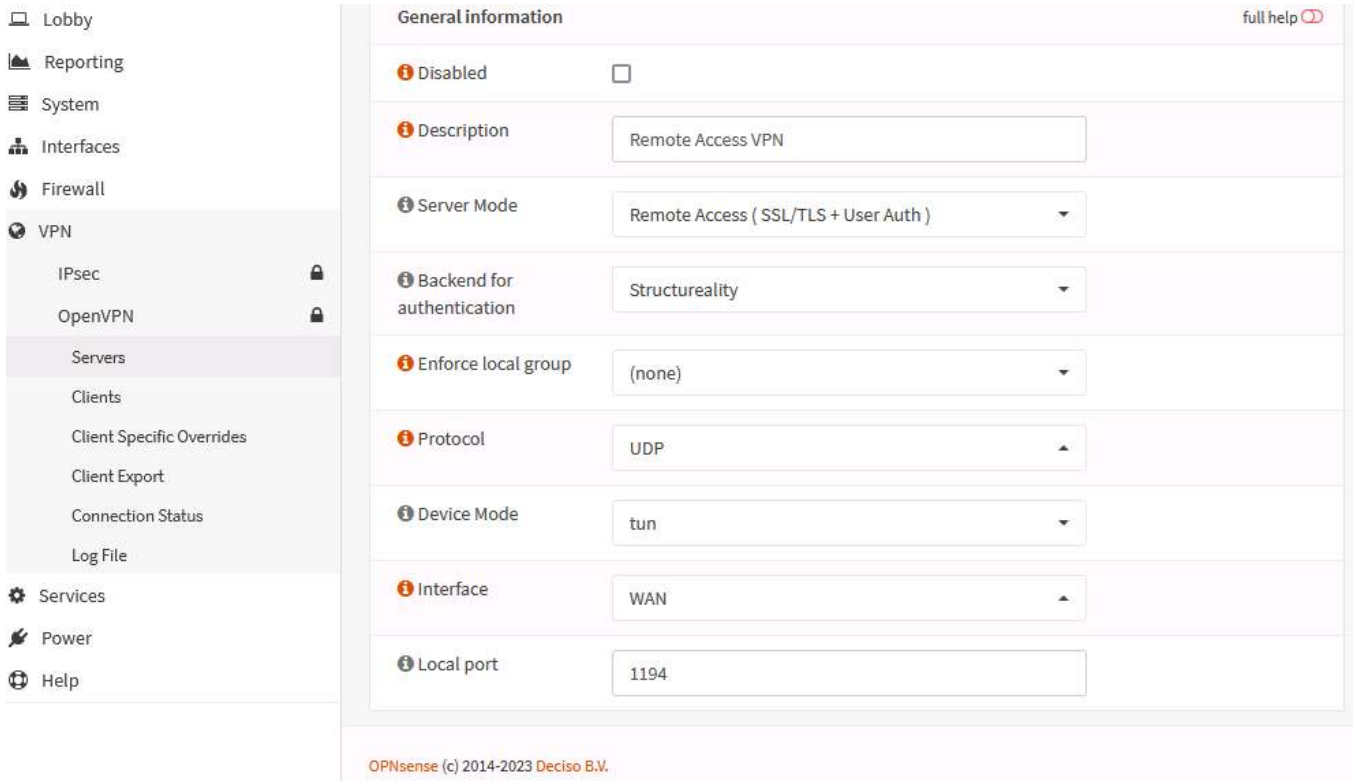
VPN za udaljeni pristup.



VPN se može rasporediti i u modelu site-to-site za spajanje dvije ili više privatnih mreža. Dok se veze VPN-a za udaljeni pristup tipično iniciraju od strane klijenta, site-to-site VPN konfiguriran je za automatski rad. Pristupnici razmjenjuju sigurnosne informacije koristeći protokol na kojem se VPN temelji. Hostovi na svakom site-u ne moraju biti konfigurirani s bilo kojim informacijama o VPN-u.



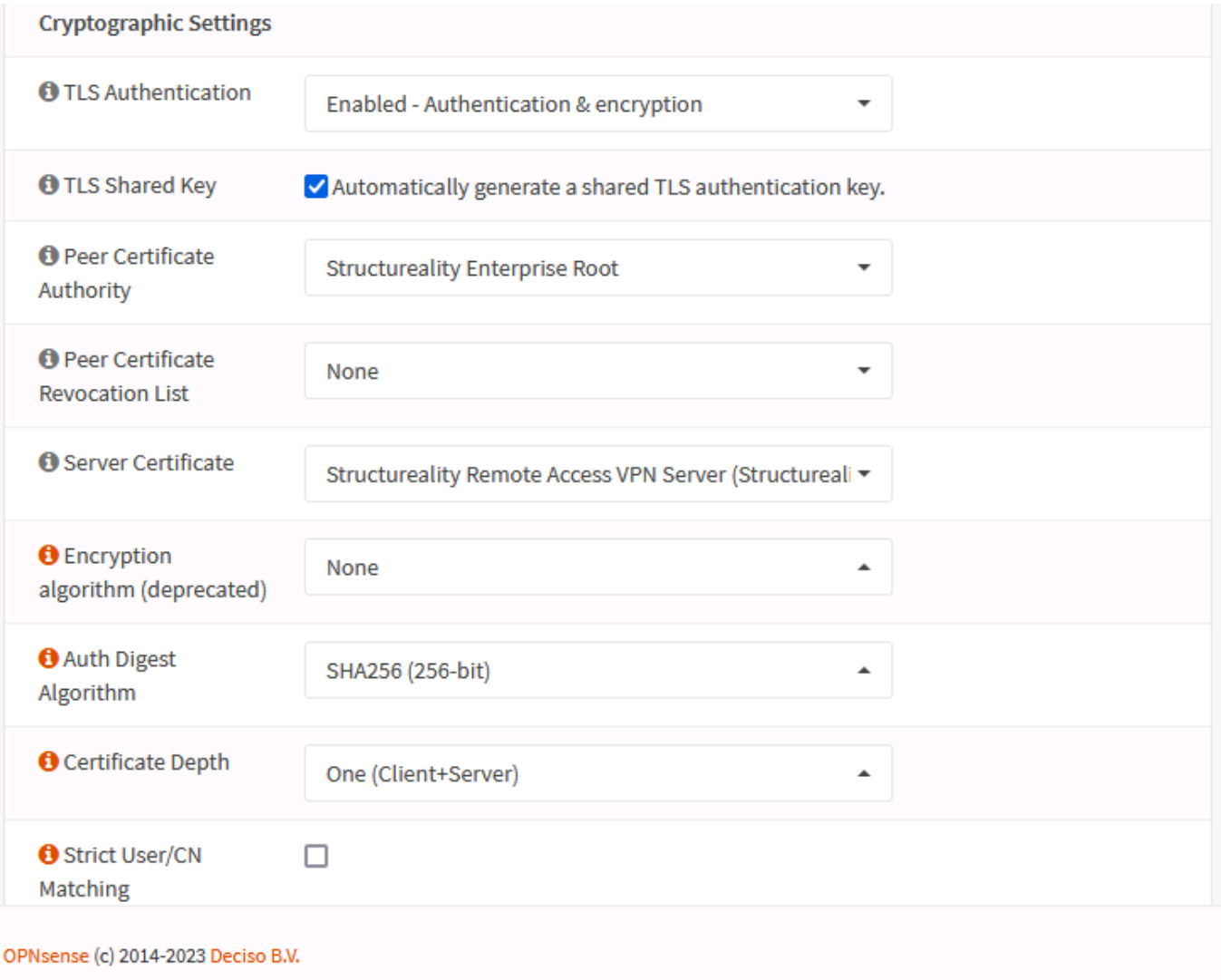
Treća topologija je host-to-host tunel. Ovo je sredstvo osiguravanja prometa između dva računala gdje privatna mreža nije pouzdana. Nekoliko VPN protokola korišteno je kroz godine. Naslijeđeni protokoli poput PPTP-a su zastarjeli jer ne nude adekvatnu sigurnost. TLS i IPsec su sada preferirane opcije za konfiguriranje VPN pristupa.



TLS tuneliranje

TLS VPN znači da se klijent povezuje na poslužitelj za udaljeni pristup koristeći digitalne certifikate. Certifikat poslužitelja identificira VPN pristupnik klijentu. TLS kreira šifrirani tunel za korisnika za podnošenje vjerodajnica za autentikaciju, koje se normalno obrađuju RADIUS poslužiteljem.

Konfiguriranje certifikata poslužitelja za OpenVPN u sigurnosnom uređaju OPNsense.



TLS VPN može koristiti TCP ili UDP. UDP se može odabrati zbog marginalno superiornijih performansi, posebno kada se tunelira promet osjetljiv na kašnjenje poput glasa ili videa. Važno je koristiti sigurnu verziju TLS-a. Najnovija verzija je TLS 1.3. TLS 1.2 je i dalje podržan. Verzije starije od TLS 1.2 su zastarjele.

IPsec tuneliranje

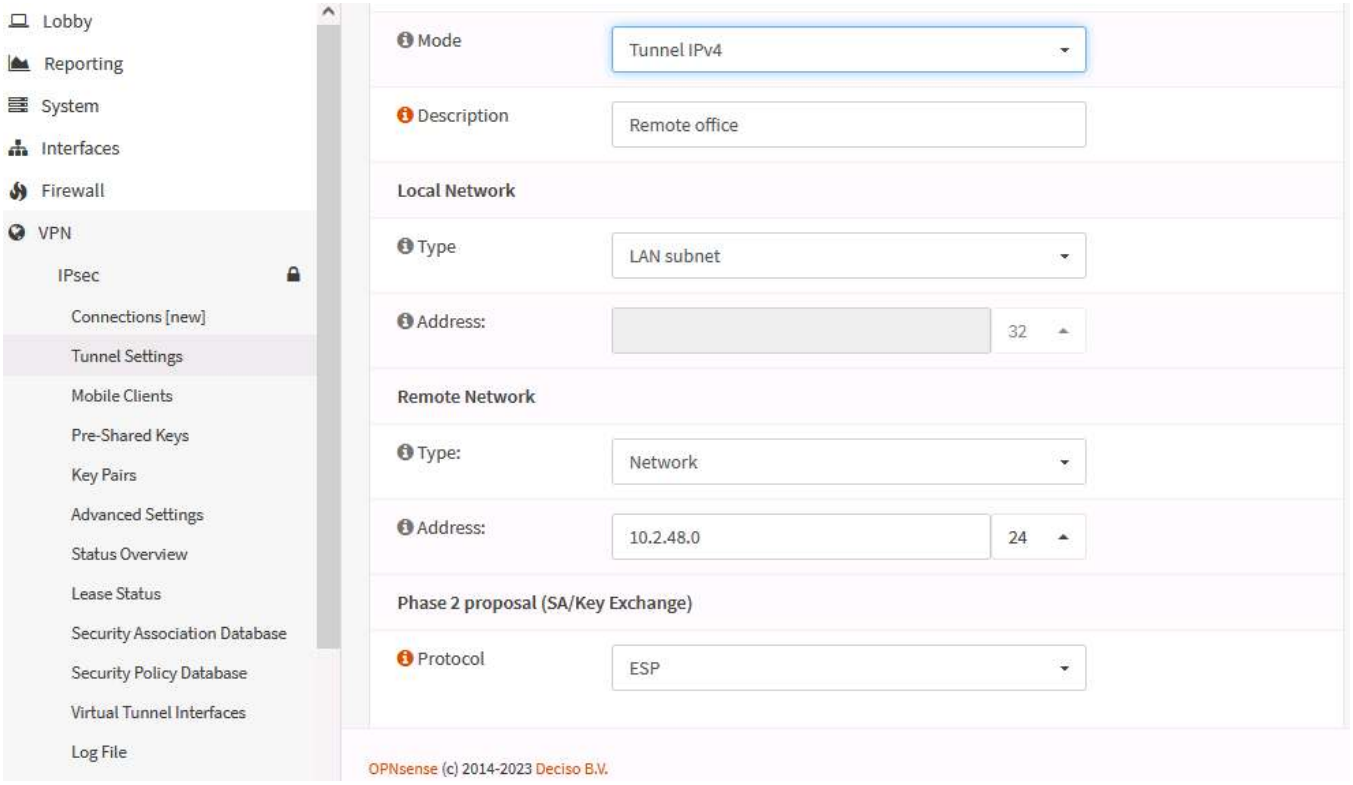
TLS se primjenjuje na razini aplikacije. Internet Protocol Security (IPsec) radi na mrežnom sloju OSI modela (sloj 3). To znači da može biti implementiran bez konfiguriranja specifičnih aplikacija. Postoje dva osnovna protokola u IPsec-u:

- Autentikacijsko zaglavlje (AH — Authentication Header) — izvodi kriptografski hash na cijelom paketu, uključujući IP zaglavlje, plus dijeljeni tajni ključ i dodaje ovu vrijednost u svojem zaglavlju kao Integrity Check Value (ICV).

nije modificiran. Sadržaj nije šifriran pa ovaj protokol ne pruža povjerljivost.

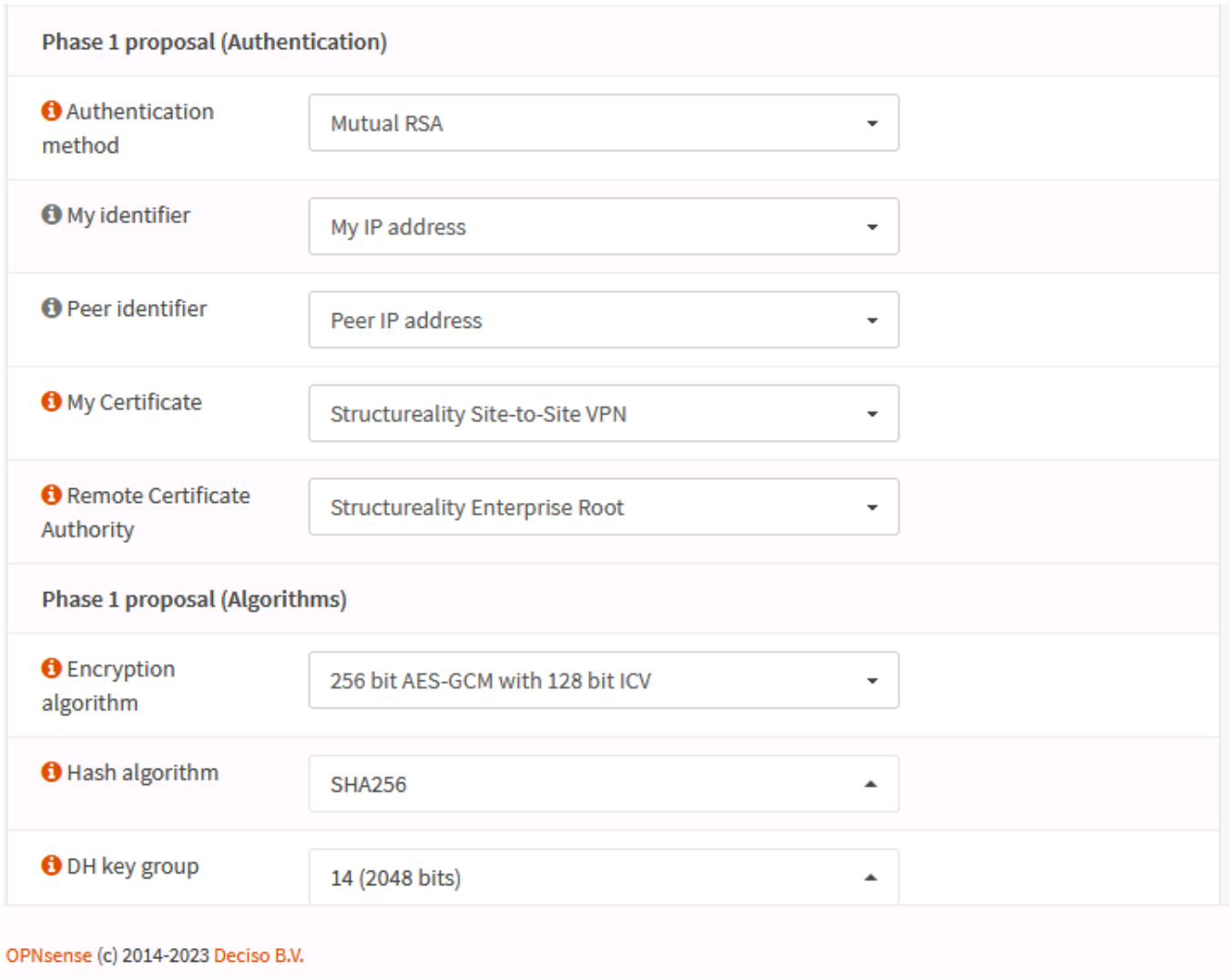
- Enkapsulacijski sigurnosni sadržaj (ESP — Encapsulating Security Payload) — može se koristiti za šifriranje paketa umjesto jednostavnog računanja ICV-a. ESP isključuje IP zaglavlje kada računa ICV.
- Transportni način — koristi se za sigurnu komunikaciju između hostova na privatnoj mreži. Kada se ESP primijeni u transportnom načinu, IP zaglavlje za svaki paket nije šifrirano, samo sadržaj podataka.

- Tunel način — koristi se za komunikacije između VPN site-ova putem nesigurne mreže. S ESP-om, cijeli IP paket (zaglavlje i sadržaj) je šifriran i enkapsuliran kao datagram s novim IP zaglavljem.



Internet Key Exchange

Svaki host ili usmjerivač koji koristi IPsec mora biti dodijeljen politici. Politika IPsec-a postavlja mehanizam autentikacije i korištenje AH/ESP i transportnog ili tunel načina za vezu između dva peera. Protokol Internet Key Exchange (IKE) implementira metodu autentikacije, odabire koje kriptografske šifre su uzajamno podržane od oba peera i izvodi razmjenu ključeva. Skup svojstava naziva se security association (SA).



IKE pregovori odvijaju se u dvije faze: 1. Faza I uspostavlja identitet dvaju peerova i izvodi dogovor o ključu koristeći Diffie-Hellman algoritam za kreiranje sigurnog kanala. Dvije metode autentikacije peerova su uobičajene:

- Digitalni certifikati — izdaju se svakom peeru od strane uzajamno povjerljivog CA za identifikaciju jednih s drugima.
- Unaprijed dijeljeni ključ (group authentication) — kada je isti pristupni kod konfiguriran na oba peera.

Faza II koristi sigurni kanal kreiran u Fazi I za uspostavljanje kojih šifri i veličina ključeva bit će korišteno s AH i/ili ESP u IPsec sesiji. IKEv2 ima neke dodatne značajke koje su protokol učinile popularnim za korištenje kao samostalno VPN rješenje za udaljeni pristup:

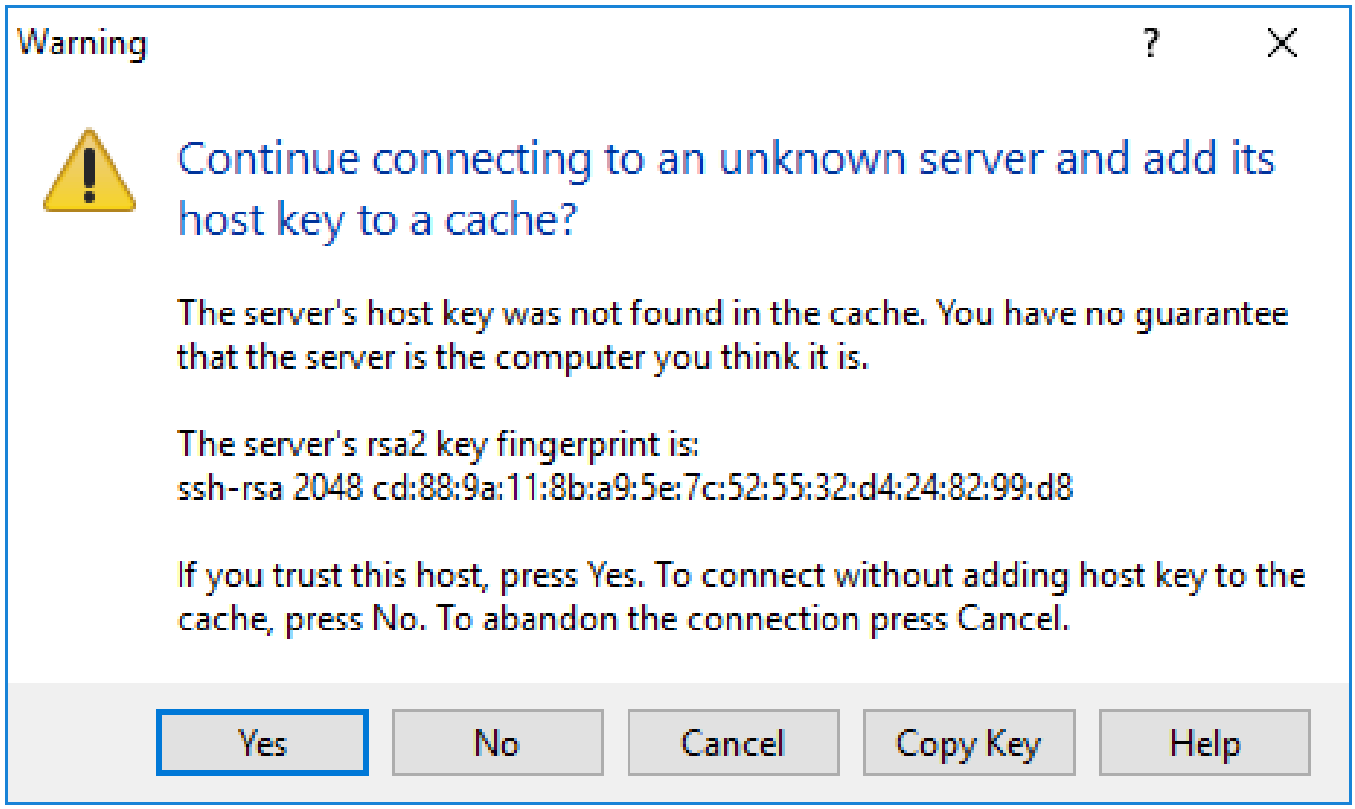
- Podržava EAP metode autentikacije, dopuštajući autentikaciju korisnika na RADIUS poslužitelju.
- Pruža jednostavan način postavljanja.
- Dopušta NAT traversal i MOBIKE multihoming.

Udaljeni desktop

Udaljeni pristup može biti i sredstvo za spajanje na određeno računalo putem mreže. Microsoft-ov Remote Desktop Protocol (RDP) može se koristiti za pristup fizičkom računalu jedan-na-jedan. RDP veze su šifrirane po defaultu. SSH — Secure Shell (SSH) je glavno sredstvo za dobivanje sigurnog udaljenog pristupa komandnoj liniji. Główne Koristi SSH-a

su udaljeno upravljanje i sigurni prijenos datoteka (SFTP).

Potvrđivanje host ključa SSH poslužitelja koristeći PuTTY SSH klijent.



Host ključ mora biti promijenjen ako se posumnja u bilo kakav kompromis hosta. SSH dopušta razne metode za autentikaciju klijenta na poslužitelju:

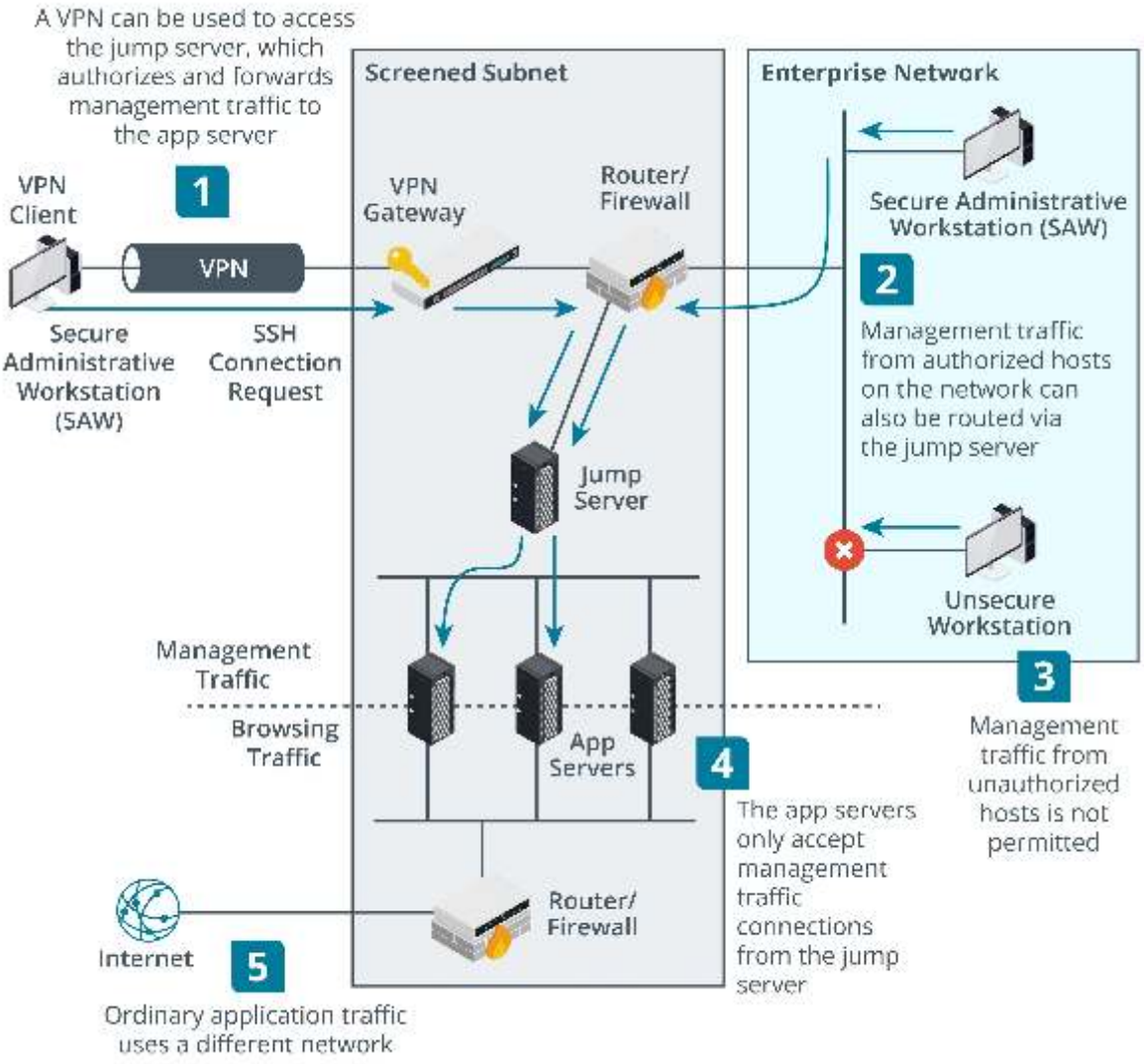
- Korisničko ime/lozinka — klijent podnosi vjerodajnice koje SSH poslužitelj verificira bilo u lokalnoj bazi podataka korisnika ili korištenjem RADIUS poslužitelja.
- Autentikacija javnim ključem — javni ključ svakog udaljenog korisnika dodaje se na popis ključeva ovlaštenih za svaki lokalni račun na SSH poslužitelju.
- Kerberos — klijent podnosi Kerberos vjerodajnice (TGT) dobivene pri prijavi na radnu stanicu poslužitelju koristeći GSSAPI.

Za spajanje na SSH poslužitelj na 10.1.0.10 koristeći račun 'bobby' i autentikaciju lozinkom: ssh bobby@10.1.0.10. Sljedeće naredbe kreiraju novi par ključeva i kopiraju ga na račun na udaljenom poslužitelju: ssh-keygen -t rsa; ssh-copy-id bobby@10.1.0.10. Za kopiranje datoteke s udaljenog poslužitelja na lokalni host: scp bobby@10.1.0.10:/logs/audit.log audit.log

Out-of-Band upravljanje i Jump poslužitelji

Remote access management channel odnosi se na specifičan slučaj korištenja sigurne mreže i shell aplikacije za administriranje mrežnog preklopnika, usmjerivača, vatrozida ili poslužitelja. Sigurne administrativne radne stanice (SAW) moraju biti strogo zaštićene, idealno s instaliranim samo softverom potrebnim za pristup administrativnom kanalu. Jump server je rješenje za problem upravljanja hostovima izloženima Internetu. Administratori se povezuju na jump server i zatim koriste jump server za spajanje na admin sučelje na aplikacijskom poslužitelju. Admin sučelje poslužitelja ima jedan unos u svom ACL-u (jump server) i odbija pokušaje veze s bilo kojih drugih hostova.

Osiguravanje upravljačkog prometa korištenjem jump poslužitelja.



Sažetak

Trebate razumjeti korištenje segmentacije za implementaciju sigurnosnih topologija temeljenih na zonama i biti u mogućnosti odabrati odgovarajuće vrste kontrola i lokacije implementacije za zaštitu mreža i hostova u danim scenarijima. Smjernice za implementaciju:

- Identificirajte poslovne tijekove rada i poslužitelje, klijente, protokole i imovinu podataka koji ih podržavaju. Dizajnirajte segmentirane mrežne zone ili blokove koji podržavaju sigurnosne zahtjeve, koristeći VLAN-ove, podmreže i politike vatrozida za implementaciju dizajna.
- Rasporedite preklapanje i usmjeravačke uređaje i protokole za podržavanje svakog bloka, uzimajući u obzir sigurnost portova ili 802.1X mrežnu kontrolu pristupa (NAC).
- Analizirajte površinu napada i odaberite učinkovite kontrole raspoređene na odgovarajuće mrežne lokacije.
- Rasporedite sigurnost portova ili 802.1X NAC za ublažavanje rizika od lažnih uređaja priključenih na fizičke mrežne portove.

- Rasporedite usmjerivačke vatrozide za provedbu kontrole pristupa i sprječavanja upada na perimetru zona.
- Rasporedite senzore za otkrivanje upada iza vatrozida ili na zrcaljenom portu preklopnika.
- Razmatrajte upotrebu proxy poslužitelja, NGFW i WAF za napredno filtriranje svjesno aplikacija i korisnika.
- Dizajnirajte usluge uravnoteženog opterećenja za provisioning visoke dostupnosti i tolerancije kvarova. Smjestite zahtjeve sigurnih komunikacija s TLS i IPsec VPN protokolima.
- Implementirajte sigurne komunikacije za desktop/shell udaljeni pristup s RDP i SSH. Razmatrajte korištenje jump poslužitelja za konsolidaciju upravljanja grupom poslužitelja u zaštićenoj zoni.

Modul 6

Sigurna cloud mrežna arhitektura

Pregled modula

Cloud mrežna arhitektura obuhvaća niz koncepata i tehnologija dizajniranih za osiguravanje povjerljivosti, integriteta i dostupnosti podataka i aplikacija unutar cloud-baziranih okruženja. Cloud arhitektura i moderne prakse implementacije softvera omogućuju besprijekorne integracije, upravljanje i optimizaciju resursa unutar cloud-baziranih okruženja. Ključne značajke uključuju provisioning na zahtjev, elastičnost i skalabilnost, koji dopuštaju brzu implementaciju i dinamičke prilagodbe računalnih, pohranbrenih i mrežnih resursa po potrebi.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Sažeti sigurne cloud i virtualizacijske usluge.
- Primijeniti cloud sigurnosna rješenja.
- Sažeti koncepte infrastrukture kao koda.
- Istražiti Internet of Things.
- Pregledati koncepte zero trust arhitekture.

Lekcija 6A

Cloud infrastruktura

Pregled lekcije

Razumijevanje koncepata cloud platforme ključno je za sigurnosne stručnjake radi učinkovite zaštite digitalnih resursa, osiguranja usklađenosti i upravljanja rizicima u modernim IT okruženjima. Kako organizacije sve više usvajaju cloud tehnologije, postaje neophodno imati čvrsto razumijevanje cloud modela i usluga.

- Javni (ili višekorisničko dijeljeni) — je usluga koja se nudi putem Interneta od strane pružatelja usluga oblaka (CSP) potrošačima oblaka. Ovim modelom poduzeća mogu nuditi pretplate ili plaćanje prema korištenju, a istovremeno pružati usluge nižih razina besplatno.
- Hosting privatni — hostiran je od strane treće strane za isključivu upotrebu organizacije. Ovo je sigurnije i može garantirati bolje performanse, ali je skuplje. Privatni — cloud infrastruktura koja je potpuno privatna i u vlasništvu organizacije. U ovom slučaju ne postoji dijeljenje resursa s vanjskim korisnicima.

Privatni cloud može biti on-premises ili off-site u odnosu na ostale poslovne jedinice. Lokalna veza očito može pružiti bolje performanse i manje je podložna prekidima (gubitak internetske veze ne utječe na lokalnu mrežu). Off-site rješenje pruža bolju elastičnost i skalabilnost.

- Zajednički (Community) — je kada nekoliko organizacija dijeli troškove privatnog ili potpuno privatnog clouda. To se obično radi kako bi se udružili resursi za zajednički cilj, poput standardizacije i sigurnosnih politika.
- Arhitektura jednog stanara (Single-tenant) — pruža namjensku infrastrukturu jednom kupcu, osiguravajući da samo taj kupac može pristupiti infrastrukturi. Ovaj model nudi najvišu razinu sigurnosti jer kupac ima potpunu kontrolu. Međutim, može biti skuplji od alternativa.
- Višekorisničke arhitektura (Multi-tenant) — je kada više kupaca dijeli istu infrastrukturu, s podacima i aplikacijama svakog kupca logički odvojenima od ostalih. Ovaj model je isplativ, ali može povećati rizik od neovlaštenog pristupa ili curenja podataka ako nije pravilno osiguran.

- Hibridna arhitektura — koristi javnu i privatnu cloud infrastrukturu. Ovaj model pruža veću fleksibilnost i kontrolu nad osjetljivim podacima i aplikacijama dopuštajući korisnicima pohranu osjetljivih podataka na privatnoj infrastrukturi uz korištenje javne za manje osjetljive svrhe.
- Arhitektura bez poslužitelja (Serverless) — je kada pružatelj clouda upravlja infrastrukturom i automatski skalira resurse prema zahtjevu. Ovaj model može biti sigurniji od tradicionalnih arhitektura jer pružatelj clouda upravlja infrastrukturom i osigurava je.

Informacije su pohranjene u javnom oblaku. Često dolazi do grešaka uzrokovanih zbunjenošću oko granice između on-premises i javne cloud infrastrukture. Uz to, korištenjem više pružatelja clouda mogu nastati kompleksnosti u upravljanju i integraciji.

Modeli cloud usluga

Pored modela vlasništva (javni, privatni, hibridni ili zajednički), modeli cloud usluga razlikuju se po razini složenosti i količini unaprijed konfigurirane infrastrukture: Softver kao usluga (SaaS) pruža gotov softver kojim upravlja pružatelj usluge. Platforma kao usluga (PaaS) pruža okruženje za razvoj i implementaciju softvera. Infrastruktura kao usluga (IaaS) pruža virtualizirane računalne resurse putem interneta.

komponente i internetske veze koje zahtijevaju, iznajmljujete ih po potrebi iz datacentra pružatelja usluge. Primjeri uključuju Amazon Elastic Compute Cloud (aws.amazon.com/ec2), Microsoft Azure Virtual Machines i Google Compute Engine. S IaaS-om, kupac je odgovoran za konfiguriranje i upravljanje virtualnim strojevima, pohranom, mrežom i operativnim sustavima. Pružatelj oblaka odgovoran je za osiguravanje fizičke infrastrukture, virtualnih hypervisora i osnovnih mrežnih usluga.

Matrica odgovornosti

Kada koristite cloud infrastrukturu, sigurnosni rizici se ne prenose, već se dijele između pružatelja clouda i korisnika. Pružatelj clouda odgovoran je za osiguravanje temeljne infrastrukture, dok je korisnik odgovoran za sigurnost onoga što implementira na toj infrastrukturi. Precizna podjela odgovornosti ovisi o modelu usluge koji se koristi.

Model odgovornosti

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	●	●	●	●	●	✓	✓
Client and end-point protection	●	●	●	◐	◐	✓	✓
Identity and access management	●	●	◐	◐	◐	✓	✓
Application-level controls	●	●	◐	◐	◐	✓	✓
Network controls	●	◐	○	○	○	✓	✓
Host infrastructure	●	◐	○	○	○	✓	
Physical security	●	○	○	○	○		

● Cloud Customer ○ Cloud Provider

Funkcija kao usluga (FaaS) povezana je s računarstvom bez poslužitelja. Omogućuje programerima izvršavanje pojedinih dijelova koda (ili funkcija) kao odgovor na različite okidače, poput HTTP zahtjeva, promjena baze podataka ili zakazanih zadataka.
Odgovornosti pružatelja clouda:

- Fizička sigurnost infrastrukture
- Osiguravanje računalne, pohranbrene i mrežne opreme
- Osiguravanje temeljnih elemenata umrežavanja, poput DDoS zaštite
- Sigurnosna kopija pohrane u oblaku i oporavak
- Sigurnost i dostupnost hypervisora

Odgovornosti korisnika cloud usluge:

- Upravljanje korisničkim identitetima
- Konfiguriranje geografske lokacije za pohranu podataka i pokretanje usluga
- Kontrola pristupa korisnika i usluga cloud resursima
- Konfiguracija sigurnosti podataka i aplikacija
- Usklađenost i zakonodavne zahtjeve

Kako je prethodno navedeno, podjela odgovornosti postaje više/manje složena ovisno o korištenom modelu usluge. Na primjer, u SaaS modelu, konfiguraciju i kontrolu umrežavanja obavlja pružatelj oblaka, dok u IaaS modelu tu kontrolu obavlja korisnik.

Identificiranje granice između odgovornosti korisnika i pružatelja clouda, u smislu sigurnosti, imperativ je za smanjenje rizika od uvođenja ranjivosti u vaše okruženje.

Centralizirana i decentralizirana računarstvo

Centralizirana računarska arhitektura odnosi se na model u kojem se sva obrada podataka i pohrana obavljaju na jednom mjestu, obično na centralnom poslužitelju. Svi korisnici se spajaju na ovaj centralni poslužitelj radi pristupa resursima. Decentralizirane arhitekture distribuiraju obradu i pohranu podataka između višestrukih čvorova. Primjeri decentraliziranih arhitektura:

- Blockchain je distribuirana tehnologija knjige koja omogućuje sigurne, transparentne i decentralizirane transakcije.
- Peer-to-peer (P2P) mreže su mreže dizajnirane za distribuciju obrade i pohrane podataka između sudjelujućih čvorova, umjesto oslanjanja na centralni poslužitelj.
- Mreže za isporuku sadržaja (CDN) distribuiraju sadržaj na višestrukim poslužiteljima radi poboljšanja performansi, pouzdanosti i skalabilnosti.
- IoT uređaji mogu biti spojeni u decentraliziranu mrežu za dijeljenje podataka i procesorske snage.
- Distribuirane baze podataka distribuiraju podatke na višestrukim poslužiteljima, osiguravajući da su podaci uvijek dostupni, čak i ako jedan poslužitelj prestane raditi.
- Tor (The Onion Router) je mreža koja omogućuje anonimnu komunikaciju i pregledavanje. Tor preusmjerava promet kroz mrežu dobrovoljno upravljanih poslužitelja kako bi sakrio lokaciju i internetsku aktivnost korisnika.

Koncepti otporne arhitekture

Jedna od prednosti clouda je mogućnost implementacije visoko dostupnih i otpornih arhitektura za ublažavanje fizičkih ili logičkih kvarova.

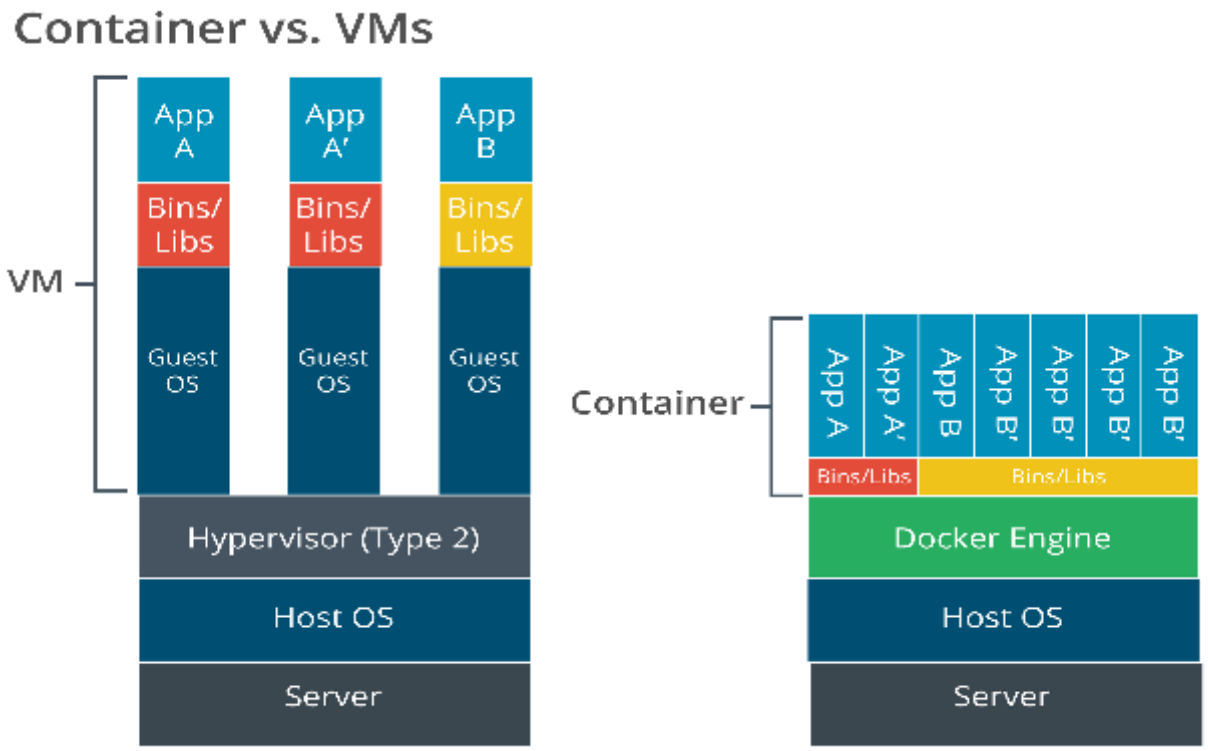
Replikacija podataka omogućuje poduzećima kopiranje podataka tamo gdje se može najučinkovitije koristiti. Cloud se može koristiti kao centralno mjesto pohrane, čineći podatke dostupnima svim poslovnim jedinicama. Replikacija podataka može se odvijati na različitim razinama:

- Lokalna replikacija — replicira vaše podatke unutar jednog datacentra u regiji gdje ste kreirali račun za pohranu. Replike se često nalaze u odvojenim domenama kvara i domenama nadogradnje.
- Regionalna replikacija (poznata i kao zona-redundantna pohrana) — replicira vaše podatke na višestrukim datacentrima unutar jedne ili dvije regije. Štiti podatke i pristup u slučaju uništenja ili prestanka rada jednog datacentra.
- Geo-redundantna pohrana (GRS) — replicira vaše podatke u sekundarnu regiju koja je udaljena od primarne regije. Štiti podatke u slučaju regionalnog kvara ili katastrofe.

Virtualizacija aplikacija i virtualizacija kontejnera

Virtualizacija aplikacija je ograničeniji tip infrastrukture virtualnog desktopa (VDI). Umjesto pokretanja cijelog klijentskog desktopa kao virtualnog stroja, samo se aplikacijska logika virtualizira. Kontejneri su lagana, prenosiva okruženja koja sadrže sve što aplikacija treba za pokretanje, uključujući kod, runtime, sistemske alate i biblioteke.

konfiguracija ima različite verzije softvera i biblioteke potrebne za nove komponente. 'Noćna mora ovisnosti' često se manifestira kao frustrirajući ciklus pokušaja rješavanja sukoba ažuriranjem jedne ovisnosti koja uzrokuje sukobe s drugima. Docker je popularna platforma za kontejnerizaciju koja rješava ovaj problem pružanjem standardiziranog okruženja za razvoj i implementaciju aplikacija.



Cloud arhitektura i serverless računarstvo

Serverless računarstvo je model cloud računarstva u kojemu pružatelj clouda upravlja infrastrukturom i automatski alocira resurse prema potrebi, naplaćujući samo za stvarno korišteno računanje. U ovom modelu programeri mogu fokusirati resurse na pisanje koda umjesto na upravljanje poslužiteljima i infrastrukturom.

koristiti ovu tehnologiju. Serverless računarstvo pruža skalabilnu, isplativu i laku za upravljanje infrastrukturu za eventom-pokretane i zadatke obrade podataka. Sa serverlessom, sva arhitektura se apstrahira, što znači da programeri ne trebaju brinuti o skaliranju, dostupnosti ili infrastrukturnom održavanju. Platforma automatski skalira resurse gore ili dolje prema zahtjevu, plaćate samo ono što koristite, a infrastruktura je uvijek dostupna i otporna.

Uz to, cloud platforme pružaju napredne mreže za isporuku sadržaja (CDN) koje optimiziraju web promet predmemoriranjem sadržaja, a pohrana objekata pruža masivne, nestrukturirane usluge pohrane podataka koje mogu rasti prema potrebi. Cloud arhitektura uključuje niz alata i tehnika za izgradnju otpornih, skalabilnih i dostupnih aplikacija:

- Balansiranje opterećenja (Load Balancing) — Distribuira mrežni promet na višestruke poslužitelje ili usluge radi poboljšanja performansi i osiguravanja visoke dostupnosti. U oblaku, load balanceri su posrednici (proxiji) između korisnika i pozadinskih resursa poput virtualnih strojeva ili kontejnera. Distribuiraju dolazni promet između skupnog pozadinskih resursa.
- Edge računarstvo (Edge Computing) — Optimizira geografsku lokaciju resursa i usluga za omogućavanje brže obrade i smanjenog kašnjenja. Umjesto preusmjeravanja svih podataka u centralizirani cloud datacenter, edge računarstvo koristi distribuirane računalne resurse za minimiziranje udaljenosti koju podaci moraju prijeći.
- Automatsko skaliranje (Auto-Scaling) — Je automatizirani proces koji prilagođava računalne resurse alocirana aplikaciji na temelju zahtjeva. Automatsko skaliranje dopušta cloud infrastrukturi da dinamički

skalira resurse gore ili dolje kako bi odgovarala zahtjevima stvarnog opterećenja u stvarnom vremenu. Na primjer, za perioda velikog zahtjeva, automatski se provisioniraju dodatni resursi za obradu povećanog opterećenja, osiguravajući da aplikacija ostaje odzivna i dostupna.

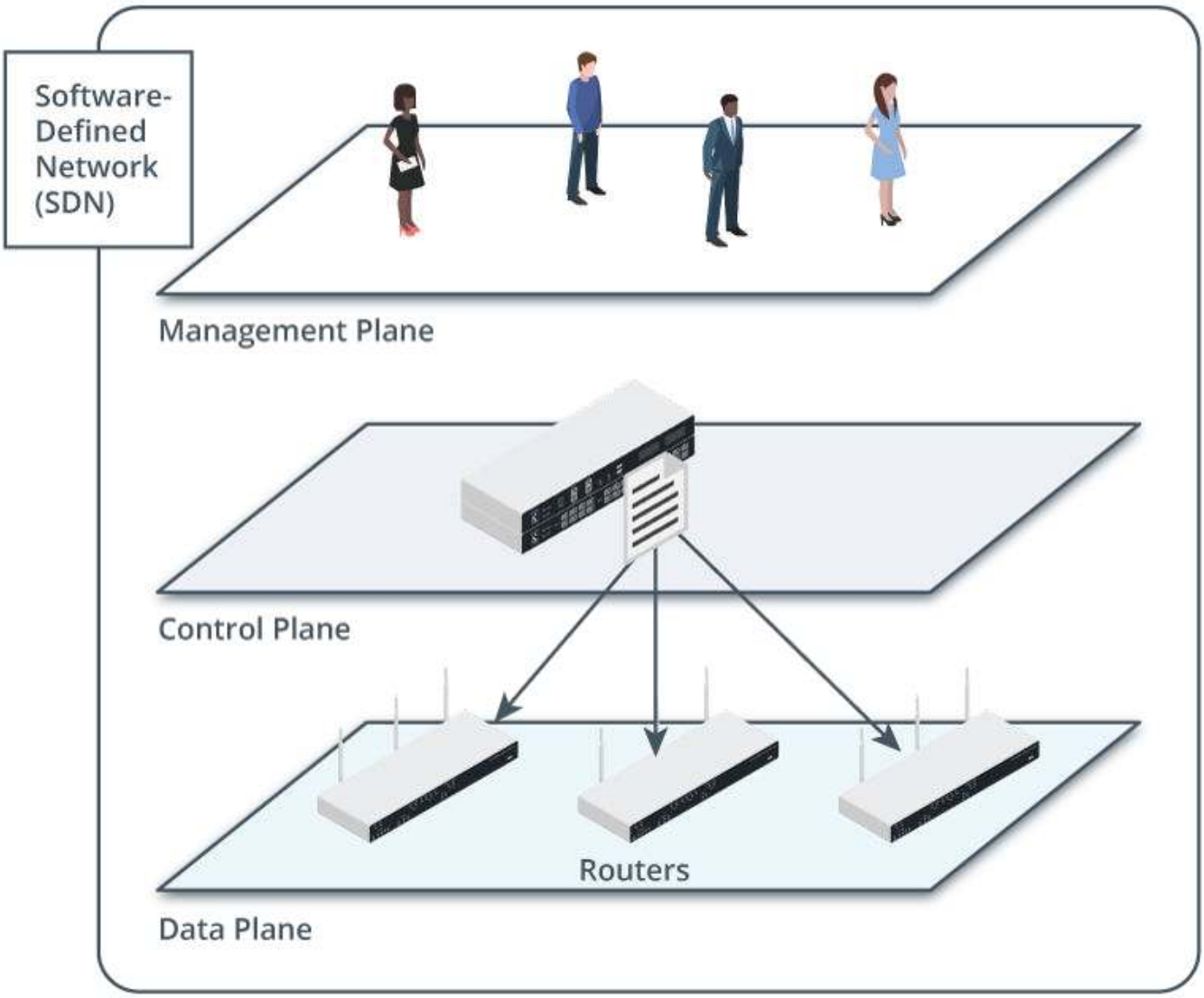
Softverski definirana mreža

IaC je dijelom olakšan fizičkim i virtualnim mrežnim uređajima koji su u potpunosti konfigurabilni putem skriptiranja i API-ja. Kako mreže postaju složenije — možda uključujući višestruke cloud platforme, on-premises implementacije i zaposlene koji rade na daljinu — složenost upravljanja njima raste. Softverski definirana umrežavanja (SDN) bavi se ovim problemom razdvajanjem slojeva mreže na:

- Upravljački sloj (Management plane) — prati uvjete prometa i status mreže.
- Kontrolni sloj (Control plane) — donosi odluke o tome kako promet treba biti prioritiziran, osiguran i kuda treba biti prebačen.
- Podatkovni sloj (Data plane) — obrađuje prebacivanje i usmjeravanje prometa i primjenu sigurnosnih kontrola pristupa. SDN aplikacija može se koristiti za definiranje odluka politike na kontrolnom sloju. Te se odluke zatim implementiraju na

podatkovnom sloju pomoću aplikacije mrežnog kontrolera.

Uređaji podatkovnog sloja kojima upravlja uređaj kontrolnog sloja i koje prati upravljački sloj.



Značajke cloud arhitekture

Infrastruktura javnog clouda pruža širok raspon dostupnih značajki za osiguravanje visoke dostupnosti i minimalnih prekida za kupce. Replikacija podataka i redundancija su među ključnim mehanizmima. Cloud pružatelji redovito repliciraju podatke između višestrukih datacentara, čak i preko geografskih regija, kako bi se zaštitili od regionalnih katastrofa.

migriranjem postojećih radnih opterećenja s on-premises u cloud. Korištenje cloud usluga uključuje pomak od kapitalnih troškova (CapEx) na operativne troškove (OpEx). CapEx uključuje početne troškove za nabavu hardvera i softvera, dok OpEx uključuje tekuće troškove poput pretplata.

- Automatiziranje implementacije i upravljanja cloud resursima smanjuje potrebu za ručnom intervencijom i često se postiže korištenjem upravljanja konfiguracijom, orkestracije kontejnera i infrastrukture kao koda.
- Standardizirane konfiguracije, predlošci i slike pojednostavljuju implementaciju i osiguravaju dosljednost.

- Prenosivost osigurava da se aplikacije i usluge mogu lako premjestiti između različitih cloud infrastruktura, izbjegavajući zavisnost o jednom dobavljaču i pružajući veću fleksibilnost. Jednostavnost oporavka — Pružatelji clouda tipično nude funkcionalnost sigurnosne kopije i oporavka kako bi organizacijama omogućili zakazivanje i automatiziranje sigurnosnih kopija za brz oporavak od katastrofa ili kvarova.

tekuće usklađenosti. Uz to, ISA treba razmatrati korištenje podugovaratelja i jasno definirati sigurnosne odgovornosti i zahtjeve za njihov odabir te proces obavještavanja u slučaju sigurnosnog incidenta. Ugovor o razini usluge (SLA) trebao bi specificirati mjerljive metrike poput dostupnosti sustava, vremena odgovora i performansi.

infrastrukture. Ovaj nedostatak kontrole može otežati ili čak onemogućiti primjenu zakrpa prema zakonskim i regulatornim zahtjevima ili vremenskim okvirima. Sigurna komunikacija i pristup — Softverski definirana perimetralna mreža (SDP) je sigurnosni okvir koji stvara sigurne, šifrirane veze između korisnika i resursa kojima pristupaju, bez obzira na lokaciju. Za razliku od tradicionalnih perimetralnih mrežnih pristupa, SDP verificira korisnika i uređaj prije nego što odobri pristup specifičnim resursima, smanjujući površinu napada.

Lekcija 6B

Ugrađeni sustavi i Zero Trust arhitektura

Pregled lekcije

Kao sigurnosni stručnjaci, bitno je razumjeti koncepte vezane uz ugrađene sustave, Internet stvari (IoT), industrijske kontrole i zero trust arhitekturu. Kako raste usvajanje ugrađenih sustava i IoT-a, tako raste i potencijalna površina napada. Ugrađeni sustavi su specijalizirani računalni sustavi dizajnirani za određene zadatke ili funkcije unutar većeg sustava.

- Kućanski uređaji — poput hladnjaka, perilica rublja i aparata za kavu, sadrže ugrađene sustave koji kontroliraju njihove funkcije i operacije.
- Pametni telefoni i tableti — sadrže niz ugrađenih sustava, uključujući procesore, senzore i komunikacijske module.
- Automobilski sustavi — poput modernih automobila sadrže ugrađene sustave uključujući jedinice za upravljanje motorom, sustave zabave i sigurnosne sustave poput airbagas i anti-blok kočenja.
- Industrijska automatizacija — Ugrađeni sustavi postoje u kontrolnim sustavima i strojevima, poput robota, montažnih linija i senzora.
- Medicinski uređaji — poput elektrostimulatora srca, inzulinskih pumpi i monitora glukoze u krvi, sadrže ugrađene sustave koji kontroliraju njihove funkcije i pružaju podatke zdravstvenim radnicima.
- Zrakoplovstvo i obrana — Zrakoplovi, sateliti i vojna oprema koriste ugrađene sustave za navigaciju, komunikaciju i kontrolu. Operativni sustavi u stvarnom vremenu — RTOS (Real-Time Operating System) je vrsta operativnog sustava dizajniranog za aplikacije koje zahtijevaju obradu u stvarnom vremenu s minimalnim kašnjenjem.

Primjeri RTOS-a

Operativni sustav VxWorks uobičajeno se koristi u zrakoplovnim i obrambenim sustavima. VxWorks pruža performanse u stvarnom vremenu i pouzdanost, te je stoga dobro prikladan za upotrebu u zrakoplovima, svemirskim letjelicama i vojnoj opremi. QNX je još jedan RTOS koji se koristi u automobilskim sustavima, medicinskim uređajima i

industrijskim kontrolnim sustavima. QNX pruža mikrokernelsku arhitekturu koja ga čini pouzdanim i sigurnim.

Industrijski kontrolni sustavi

Sustavi za automatizaciju tijeka rada i procesa — Industrijski kontrolni sustavi (ICS) pružaju mehanizme za automatizaciju tijeka rada i procesa. Ovi sustavi kontroliraju strojeve koji se koriste u kritičnoj infrastrukturi kao što su energija, voda, prijevoz i industrijska proizvodnja. Tri primarne vrste su: SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System) i PLC (Programmable Logic Controller).

Ove vrste sustava koriste se u mnogim sektorima industrije:

- Energetika se odnosi na generiranje i distribuciju energije. Šire gledano, komunalne usluge uključuju vodu/kanalizaciju i transportne mreže.
- Industrijska može se posebno odnositi na rudarstvo i preradu sirovina, uključujući opasne visokotlačne peći, preše, centrifuge, pumpe i slično.
- Proizvodnja i montaža odnose se na stvaranje komponenti i njihovo sastavljanje u proizvode. Ugrađeni sustavi koriste se za kontrolu automatiziranih proizvodnih sustava, poput kovina, mlinova i montažnih linija.
- Logistika se odnosi na premještanje stvari s mjesta gdje su napravljene ili sastavljene do mjesta gdje trebaju biti. Ugrađena tehnologija koristi se u kontroli automatiziranih transportnih i dizaličnih sustava plus senzora za praćenje komponenti.
- Objekti se odnose na sustave upravljanja gradilištem i zgradama, koji tipično automatiziraju grijanje, ventilaciju i klimatizaciju (HVAC), rasvjetu i sigurnosne sustave. ICS/SCADA su se povijesno gradili bez obzira na IT sigurnost, iako sada postoji visoka svjesnost o nužnosti sigurnosti.

Internet stvari

Internet stvari (IoT) odnosi se na mrežu fizičkih uređaja, vozila, uređaja i drugih objekata opremljenih senzorima, softverom i povezivanjem, što im omogućuje prikupljanje i razmjenu podataka. IoT uređaji mogu biti jednostavni poput senzora temperature ili složeni poput autonomnih vozila.

Danas je u upotrebi mnogo IoT uređaja i aplikacija. Na primjer, pametni domovi često koriste IoT senzore i aktuatore za kontrolu rasvjete, temperature i sigurnosnih sustava, dopuštajući vlasnicima da daljinski nadziru i kontroliraju svoja doma. U industrijskom okruženju, IoT senzori prate performanse strojeva u stvarnom vremenu, predviđaju kvarove i optimiziraju operacije.

IoT uređaji često imaju loše sigurnosne karakteristike iz nekoliko razloga. IoT uređaji su tipično dizajnirani s fokusom na funkcionalnost, a ne sigurnost, i imaju ograničenu procesorsku snagu i memoriju. Ovo čini implementaciju robustnih sigurnosnih mjera izazovnijim.

njihov proces dizajna i razvoja. Mnogi IoT uređaji su ubrzano stavljeni na tržište bez odgovarajućeg sigurnosnog testiranja, što rezultira ranjivostima koje kibernetički kriminalci mogu iskoristiti. Uz to, potrošači i organizacije često zanemaruju ažuriranje firmware-a IoT uređaja, ostavljajući ih ranjivima na poznate exploite.

- Zaklada za sigurnost Interneta stvari (IoTSF) - https://iotsecurityfoundation.org
- Industrial Internet Consortium (IIC) Okvir sigurnosti - https://www.iiconsortium.org/iisf/

- Cloud Security Alliance (CSA) IoT okvir kontrola sigurnosti - https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework
- Europski institut za telekomunikacijske norme (ETSI) IoT sigurnosni standardi

Deperimeterizacija i Zero Trust

Rastuća potreba za Zero Trust arhitekturama (ZTA) — Povećana ovisnost organizacija o informacijskim tehnologijama potaknula je zahtjeve da usluge budu uvijek dostupne i dostupne s bilo koje lokacije. Ove potrebe znače da modeli mrežne sigurnosti temeljeni na perimetru postaju manje učinkoviti. Principi Zero Trust uključeni su u okvir sigurnosti koji se fokusira na osiguravanje svakog zahtjeva za pristupom bez obzira na lokaciju ili korisnika.

- NIST SP 800-207 https://csrc.nist.gov/publications/detail/sp/800-207/final.
- CISA-in Zero Trust model zrelosti https://www.cisa.gov/zero-trust-maturity-model

Deperimeterizacija

Deperimeterizacija se odnosi na sigurnosni pristup koji pomiče fokus od obrane granica mreže na zaštitu pojedinih resursa i podataka unutar mreže. Kako organizacije postaju sve više distribuirane i ne mogu oslanjati na jasan mrežni perimetar, sigurnosni modeli temeljeni na perimetru postaju manje učinkoviti.

sigurnosni modeli temeljeni na perimetru postaju manje učinkoviti u adresiranju modernih prijetnji. Koncepti deperimeterizacije zagovaraju implementaciju višestrukih sigurnosnih mjera oko pojedinačnih resursa, kao što su podaci, aplikacije i uređaji, umjesto samo oslanjanja na perimetarsku obranu. Ključni čimbenici koji utječu na deperimeterizaciju:

- Cloud — Poslovne infrastrukture su tipično raspoređene između on-premises i cloud platformi. Uz to, cloud platforme mogu se koristiti za distribuciju računalnih resursa globalno.
- Rad na daljinu — Sve više organizacija usvojilo je djelomično ili potpuno udaljene radne snage. Ova udaljena radna snaga dramatično proširuje trag poduzeća. Uz to, zaposlenici koji rade od kuće podložniji su sigurnosnim propustima kada se spajaju iz nesigurnih domova ili javnih mreža.
- Mobilni — Moderni pametni telefoni i tableti često se koriste kao primarni računalni uređaji jer imaju dovoljno procesora, memorije i kapaciteta pohrane. Sve više korporativnih podataka pristupa se putem ovih uređaja kako se njihove mogućnosti šire.
- Outsourcing i ugovaranje — Dogovori o podršci često pružaju udaljeni pristup vanjskim entitetima, a taj pristup često znači da mreža vanjskog pružatelja služi kao ulazna točka u organizacije koje podržavaju.
- Bežične mreže (Wi-Fi) — Bežične mreže podložne su sve većem broju eksploatacija, ali često su bežične mreže otvorene i nesigurne ili je mrežni sigurnosni ključ opće poznat.
- Veća sigurnost — Zahtijeva autentikaciju i provjeru svih korisnika, uređaja i aplikacija prije mrežnog pristupa.
- Bolje kontrole pristupa — Uključuju strože ograničenja o tome tko ili što može pristupiti resursima i s kojih lokacija.
- Poboljšano upravljanje i usklađenost — Ograničavaju pristup podacima i pružaju veću operativnu vidljivost aktivnosti korisnika i uređaja.

- Povećana granularnost — Korisniku daje pristup onome što treba kada to treba.

Zero Trust arhitektura zahtijeva temeljito razumijevanje mnogih komponenti i tehnologija korištenih unutar mreže organizacije. Sljedeći popis opisuje bitne komponente Zero Trust arhitekture:

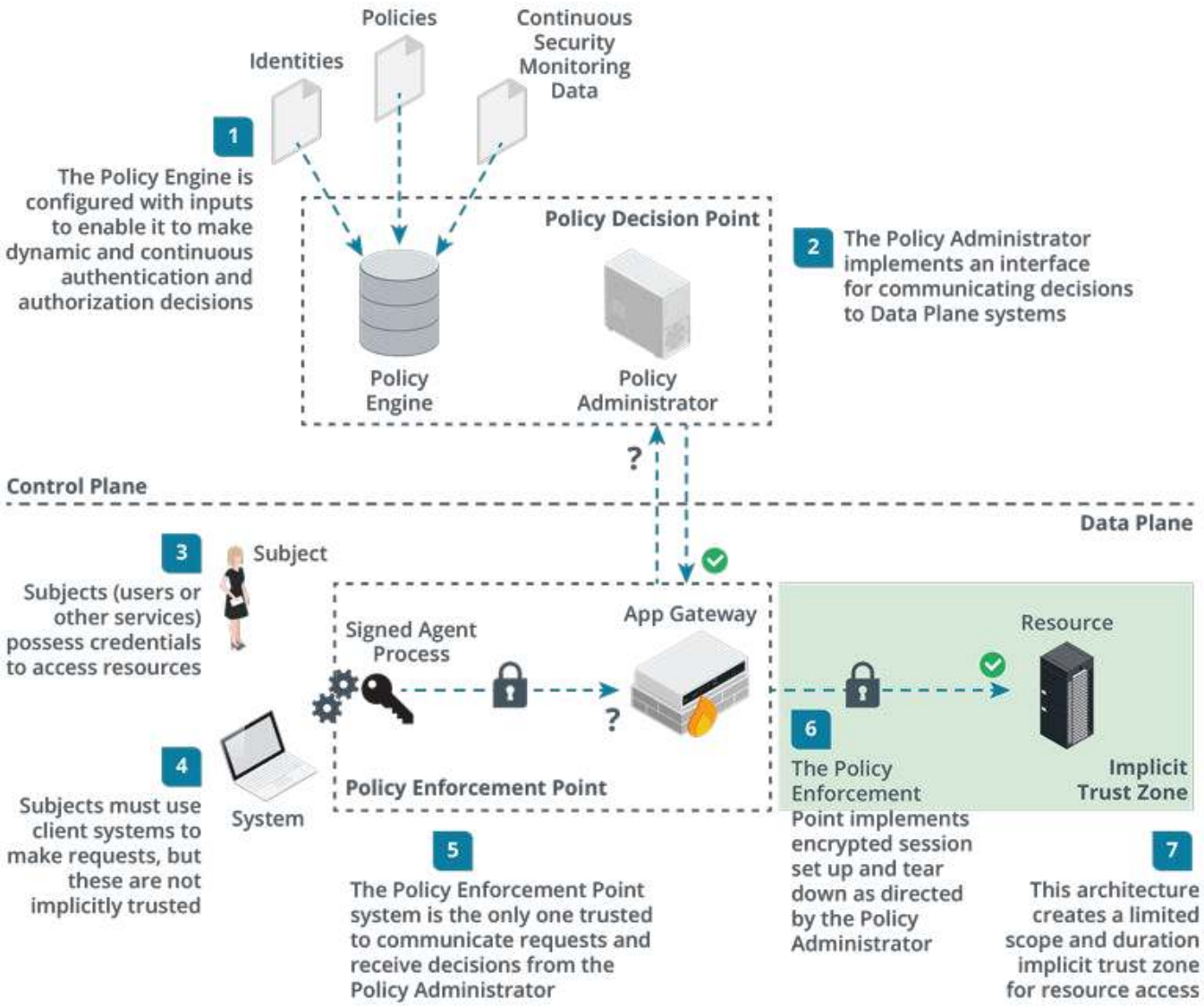
- Mrežna i sigurnost krajnjih točaka — Kontrolira pristup aplikacijama, podacima i mrežama.
- Upravljanje identitetom i pristupom (IAM) — Osigurava da samo verificirani korisnici mogu pristupiti sustavima i podacima.
- Primjena na temelju politike — Ograničava mrežni promet samo na legitimne zahtjeve.
- Sigurnost clouda — Upravlja pristupom cloud aplikacijama, uslugama i podacima.
- Vidljivost mreže — Analizira mrežni promet i aktivnosti lokacija.
- Zaštita podataka — Kontrolira i osigurava pristup osjetljivim podacima, uključujući enkripciju i reviziju.
- Otkrivanje i sprječavanje prijetnji — Identificira i sprječava napade na mrežu i sustave spojene na nju.

Sigurnosni koncepti Zero Trust

Zero trust je sigurnosni model koji pretpostavlja da svi uređaji, korisnici i usluge nisu inherentno pouzdani, bez obzira jesu li unutar ili izvan mrežnog perimetra. Tri glavna principa: nikada ne vjeruj, uvijek verificiraj; koristiti pristup s najnižim privilegijama; pretpostaviti povredu (assume breach).

- Adaptivni identitet prepoznaje da korisnički identiteti nisu statični i da provjera identiteta mora biti kontinuirana i temeljena na trenutnom kontekstu korisnika i resursima kojima pokušavaju pristupiti.
- Smanjenje opsega prijetnji znači da se pristup mrežnim resursima dodjeljuje samo na temelju potrebe da se zna, i pristup je ograničen samo na one resurse koji su potrebni za dovršetak određenog zadatka. Ovaj koncept smanjuje površinu napada mreže i ograničava štetu koju uspješni napad može uzrokovati.
- Kontrola pristupa temeljena na politici opisuje kako se politike kontrole pristupa koriste za provedbu ograničenja pristupa na temelju korisničkog identiteta, postave uređaja i mrežnog konteksta. Postava uređaja odnosi se na sigurnosni status uređaja, uključujući njegove sigurnosne konfiguracije, verzije softvera i usklađenost s organizacijskim politikama.

Komponente u NIST-ovom okviru zero trust arhitekture.



Kontrolni sloj upravlja politikama koje diktiraju kako su korisnici i uređaji ovlašteni za pristup mrežnim resursima. Implementiran je kroz centraliziranu točku odluke o politici. Točka odluke o politici se sastoji od:

- Motor politike konfiguriran je s identitetima i vjerodajnicama subjekata i hostova, politikama kontrole pristupa, ažuriranom obavještajnom prijetnjom, analitikom ponašanja i drugim rezultatima sigurnosnog skeniranja i praćenja hosta i mreže. Ovi sveobuhvatni podaci o stanju omogućuju mu definiranje algoritma za odluke o pristupu.
- Administrator politike odgovoran je za upravljanje procesom izdavanja tokena pristupa i uspostavljanja ili ukidanja sesija, na temelju odluka koje donosi motor politike. Administrator politike implementira sučelje između kontrolnog sloja i podatkovnog sloja.

implementiran kao softverski agent koji radi na klijentskom hostu i koji komunicira s app pristupnikom. Točka primjene politike sučeljava se s administratorom politike za postavljanje sigurnog podatkovnog puta između klijenta i resursa. Svaka veza mora biti ovlaštena i autentificirana. Ako veza nije ovlaštena, pristupnik je blokira.

Sažetak

Trebate biti u mogućnosti sažeti koncepte virtualizacije i cloud računarstva i razumjeti uobičajene cloud sigurnosne koncepte vezane uz računalne, pohranbrene i mrežne funkcije. Smjernice za implementaciju:

- Procijenite zahtjeve za dostupnost i povjerljivost koji će odrediti odgovarajući model cloud implementacije (javni, hostiran privatni, privatni, zajednički ili hibridni).
- Identificirajte model provisioniranja usluge (softver, platforma ili infrastruktura) koji najbolje odgovara zahtjevu aplikacije, s obzirom na dostupne razvojne resurse i stupanj potrebne prilagodbe.
- Razmotrite mogu li se usluga ili poslovne potrebe bolje podržati naprednim konceptima:
- Mikrousluge, serverless i orkestracija fokusiraju se na zahtjeve tijeka rada, a ne na administraciju poslužitelja.
- Prednosti i uobičajeni scenariji korištenja softverski definiranih mreža.
- Ako koristite CSP, kreirajte SLA i matricu sigurnosnih odgovornosti kako biste identificirali tko će obavljati sigurnosno kritične zadatke. Osigurajte da je izvještavanje i praćenje cloud sigurnosnih podataka integrirano s on-premises nadzorom i reakcijom na incidente.
- Procijenite sigurnosne značajke ugrađenih uređaja i izolirajte ih od ostalih mrežnih uređaja.
- Implementirajte koncepte zero trust arhitekture za validaciju veza i uređaja umjesto oslanjanja na koncepte granice 'unutra' i 'van'.

Modul 7

Objasni koncepte otpornosti i sigurnosti lokacije

Pregled modula

Upravljanje imovinom, otpornost sigurnosne arhitekture i fizička sigurnost ključni su koncepti koji čine temelj učinkovitih kibernetičkih sigurnosnih operacija. Upravljanje imovinom uključuje identificiranje, praćenje i zaštitu organizacijskih resursa, što je temeljno za osiguravanje njihove sigurnosti i dostupnosti. Otpornost sigurnosne arhitekture bavi se planiranjem i implementacijom sustava koji mogu nastaviti funkcionirati čak i za sigurnosnih incidenata.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Pregledati važne koncepte sigurnosnih kopija podataka.
- Razumjeti prakse upravljanja imovinom.
- Istražiti strategije visoke dostupnosti i otpornosti.
- Pregledati važne koncepte fizičke sigurnosti.

Lekcija 7A

Upravljanje imovinom

Pregled lekcije

Upravljanje imovinom kritična je komponenta učinkovitih operacija kibernetičke sigurnosti. Uključuje identificiranje, klasificiranje i popis IT imovine organizacije, uključujući hardver, softver, podatke i osoblje. Učinkovito upravljanje imovinom pruža osnovu za sigurnosne operacije pružanjem sveobuhvatnog pregleda resursa organizacije.

Praćenje imovine

Proces upravljanja imovinom prati sve kritične sustave, komponente, uređaje i druge vrijedne objekte organizacije u inventaru. Uključuje i prikupljanje i analiziranje informacija o tim resursima, kao što su lokacija, stanje i vlasništvo.

Dodjeljivanje/računovodstvo i nadzor/praćenje imovine

Dodjeljivanje vlasništva imovine i klasifikacija su bitne komponente dobro strukturiranog procesa upravljanja imovinom, osiguravajući da organizacije učinkovito upravljaju i zaštite svoju imovinu.

sigurnost imovine, održavanje i tekuće upravljanje. Klasifikacija imovine uključuje organiziranje imovine na temelju njihove vrijednosti, osjetljivosti ili kritičnosti za organizaciju. Ovo omogućuje konzistentnu i ponovljivu primjenu sigurnosnih kontrola. Metode inventarizacije imovine:

- Ručni inventar — U manjim organizacijama ili za određene vrste imovine, ručno kreiranje i održavanje inventara može biti izvedivo. Ovaj postupak uključuje fizičku inspekciju imovine i bilježenje relevantnih informacija.
- Mrežno skeniranje — Alati za mrežno skeniranje, poput Nmapa, Nessusa ili OpenVAS-a, mogu automatski otkriti i numerirati mrežne uređaje, uključujući poslužitelje, preklopnike, usmjerivače i radne stanice. Ovi alati mogu identificirati otvorene portove, usluge, pa čak i operativne sustave.
- Softver za upravljanje imovinom — Softverska rješenja za upravljanje imovinom, poput Lansweepera, ManageEngine ili SolarWindsa, mogu automatski otkriti, pratiti i katalogizirati razne vrste imovine. Ovi alati često pružaju centralizirani upravljački

ekran.

- Baza podataka upravljanja konfiguracijom (CMDB) — CMDB je centralizirano repozitorij informacija o IT infrastrukturi organizacije, uključujući imovinu, konfiguracije i odnose.
- Rješenja za upravljanje mobilnim uređajima (MDM) — Za organizacije sa značajnim brojem mobilnih uređaja, MDM rješenja poput Microsoft Intunea mogu pomoći u upravljanju i osiguravanju pametnih telefona, tableta i druge mobilne imovine.
- Otkrivanje cloud imovine — S organizacijama koje sve više usvajaju cloud usluge, cloud-native alati, poput AWS Configa ili Azure Resource Grapha, ili rješenja trećih strana mogu pomoći u otkrivanju i katalogiziranju imovine raspoređene u cloudu.

Štoviše, organizacije trebaju procijeniti ukupni trošak vlasništva (TCO) imovine, uzimajući u obzir početnu nabavnu cijenu zajedno s tekućim troškovima održavanja, ažuriranja i potencijalnih sigurnosnih incidenata. Prioritizacija nabave imovine na temelju TCO i sigurnosnih razmatranja može pomoći organizacijama u raspoređivanju resursa učinkovitije.

Koncepti zaštite imovine

S perspektive operacija kibernetičke sigurnosti, imovina opisuje kritične resurse, informacije i infrastrukturne komponente koje moraju biti zaštićene od potencijalnih prijetnji i neovlaštenog pristupa. Koncepti zaštite imovine:

- Imovina usluga su stvari, procesi ili ljudi koji doprinose pružanju IT usluge.
- Konfiguracijska stavka (CI) je imovina koja zahtijeva specifične postupke upravljanja za pružanje usluge. Svaka CI mora biti označena, idealno koristeći standardnu konvenciju imenovanja. CI-ovi su definirani njihovim atributima i odnosima pohranjenima u bazi podataka upravljanja konfiguracijom (CMDB).
- Osnovna konfiguracija je popis postavki kojima imovina, poput poslužitelja ili aplikacije, mora se pridržavati. Sigurnosne osnove opisuju minimalni skup sigurnosnih konfiguracionih postavki koje uređaj ili softver mora održavati da bi se smatrao adekvatno zaštićenim.
- Sustav upravljanja konfiguracijom (CMS) opisuje alate i baze podataka koji se koriste za prikupljanje, pohranu, upravljanje, ažuriranje i izvješćivanje o informacijama o CI-ovima.

snimiti ove informacije u proračunskim tablicama i dijagramima, dok velika organizacija može uložiti u namjenske aplikacije dizajnirane za korporativna okruženja. Dijagrami su najbolji način za snimanje složenih odnosa između elemenata infrastrukture.

Sigurnosne kopije podataka

Sigurnosne kopije igraju bitnu ulogu u zaštiti imovine osiguravanjem dostupnosti i integriteta kritičnih podataka i sustava organizacije. Kreiranjem kopija važnih informacija i pohranjivanjem na sigurnim lokacijama, organizacije mogu brzo oporaviti podatke u slučaju kvara sustava, prirodnih katastrofa ili kibernetičkih napada. Ključne značajke softvera za sigurnosne kopije:

- Podrška za razna okruženja (virtualna, fizička i cloud)
- Deduplikacija podataka i kompresija za optimizaciju prostora pohrane
- Trenutni oporavak i replikacija za brzo prebacivanje (failover)
- Zaštita od ransomwarea i enkripcija za osiguravanje podataka

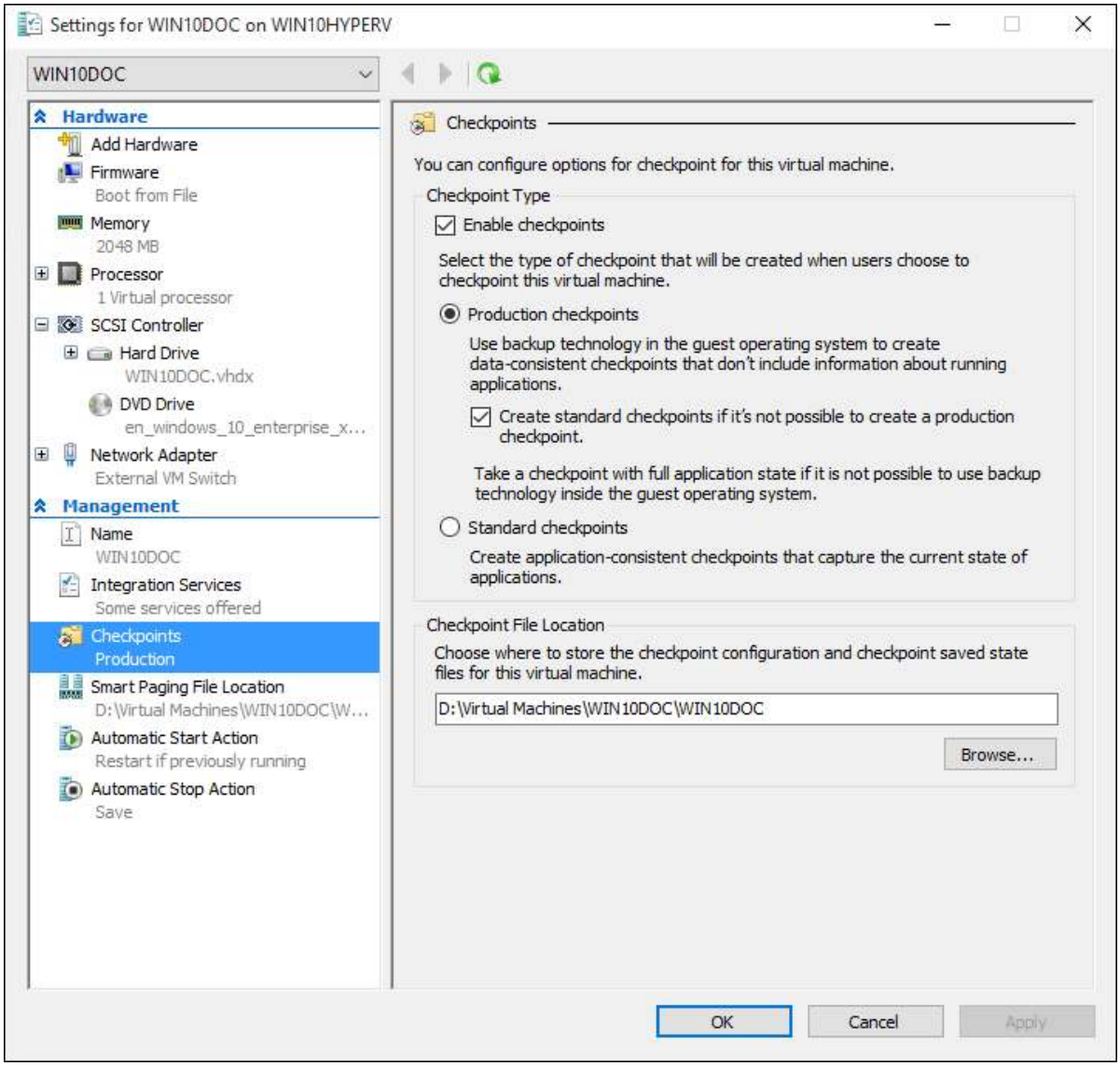
Deduplikacija podataka opisuje tehniku kompresije podataka koja optimizira prostor pohrane identificiranjem i eliminiranjem redundantnih podataka. Funkcionira analiziranjem blokova podataka unutar skupa podataka i usporedbom za pronalaženje identičnih sadržaja, pri čemu se duplicirani podaci zamjenjuju pokazivačima na jedan originalni primjerak.

poduzeća s relativno stabilnim podacima ili manje strogim regulatornim nadzorom mogu odabrati manje česte sigurnosne kopije, balansirajući zaštitu podataka, troškove sigurnosnih kopija i troškove održavanja. Na kraju krajeva, optimalna frekvencija sigurnosnih kopija ovisi o zahtjevima specifičnim za organizaciju i usklađenosti s industrijskim standardima i propisima.

Napredna zaštita podataka

Snimke (Snapshots) — Snimke igraju vitalnu ulogu u zaštiti podataka i oporavku, hvatajući stanje sustava u određenom trenutku. Snimke virtualnih strojeva (VM), datotečnih sustava i mreže pohrane (SAN) svaka ima svoju namjenu:

- VM snimke, poput onih kreiranih u VMware vSphere ili Microsoft Hyper-V, hvataju stanje virtualnog stroja, uključujući njegovu memoriju, pohranu i konfiguracijske postavke. To omogućuje administratorima vraćanje VM-a na prethodno stanje u slučaju kvarova ili oštećenja podataka.
- Snimke datotečnog sustava, poput onih koje pruža ZFS ili Btrfs, hvataju stanje datotečnog sustava u danom trenutku, omogućujući korisnicima oporavak slučajno izbrisanih datoteka ili vraćanje prethodnih verzija datoteka.
- SAN snimke se uzimaju na razini blokovne pohrane unutar mreže pohrane. Primjeri uključuju snimke u NetApp ili Dell EMC sustavima pohrane, koje hvataju stanje cijelog volumena pohrane, omogućujući brzi oporavak velikih skupova podataka i aplikacija.



Replikacija i vođenje dnevnika (journaling)

Replikacija i vođenje dnevnika su metode zaštite podataka koje osiguravaju dostupnost i integritet podataka održavanjem višestrukih kopija i praćenjem promjena podataka. Replikacija uključuje kreiranje i održavanje kopija podataka na više lokacija, što osigurava da su podaci dostupni čak i ako jedna lokacija postane nedostupna.

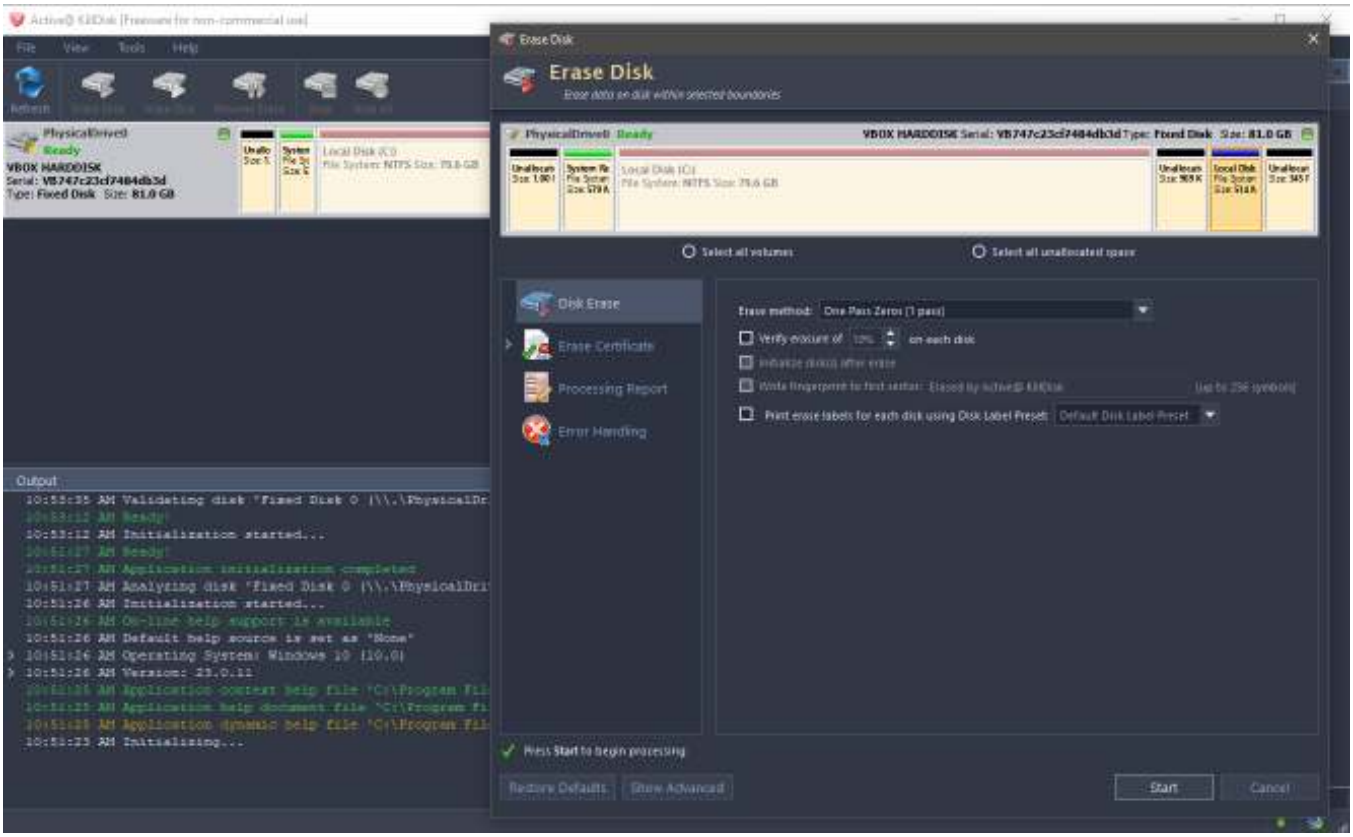
greška ili zlonamjernih napada posjedovanjem redundantnih kopija podataka. U slučaju kvara, replicirani podaci mogu se koristiti za vraćanje sustava u prvobitno stanje. Praktičan primjer replikacije je replikacija baze podataka, gdje se iste informacije pohranjuju na više poslužitelja. Vođenje dnevnika je tehnika pohrane koja bilježi svaku transakciju ili operaciju promjene u zasebnu datoteku dnevnika. Ovo omogućuje oporavak podataka do specifične točke u vremenu.

Sigurno uništavanje podataka

Nekoliko uobičajenih okolnosti može zahtijevati uništavanje podataka unutar organizacije radi osiguravanja sigurnosti, usklađenosti i pravilnog upravljanja resursima. Na kraju perioda zadržavanja podataka, organizacije moraju osigurati da se podaci sigurno unište kako bi spriječile neovlašteni pristup ili povredu podataka. Metode sigurnog brisanja uključuju prepisivanje, demagnetizaciju i fizičko uništavanje.

podataka kada više nije potrebno ili ako to zatraži subjekt podataka. Povremeno uništavanje zastarjelih ili zastarnih podataka može pomoći u održavanju učinkovitog iskorištavanja pohrane i smanjenju rizika od povreda podataka. Uz to, u nekim industrijama, propisi zahtijevaju sigurno uništavanje podataka kao dio usklađenosti. Organizacije moraju imati jasne politike i postupke za uništavanje podataka koji su u skladu s tim regulatornim zahtjevima.

Softver za brisanje podataka Active KillDisk.



Datoteke izbrisane s magnetnog tvrdog diska nisu potpuno obrisane. Umjesto toga, sektori koji sadrže podatke označeni su kao dostupni za pisanje, a podaci koje sadrže uklanjaju se tek kada se dodaju nove datoteke. Slično tome, SSD-ovi koriste različite tehnike za upravljanje podacima i čak mogu premjestiti podatke u drugi sektor kako bi se izbjeglo habanje sektora, čineći brisanje podataka složenijim. Sigurno brisanje zahtijeva posebne metode kao što su višestruko prepisivanje, demagnetizacija (za magnetne medije) ili fizičko uništavanje.

Lekcija 7B

Strategije redundancije

Pregled lekcije

Strategije redundancije bitne su za planiranje oporavka od katastrofe i kontinuiteta poslovanja organizacije. Ove strategije uključuju planiranje kontinuiteta operacija (COOP), koje uključuje razvoj procesa i postupaka koji osiguravaju da organizacija može nastaviti svoje kritične operacije čak i za katastrofe ili ometajućih događaja.

osiguravanje da organizacije mogu nastaviti pružati bitne usluge i minimizirati utjecaj nepredviđenih događaja na njihove operacije. Sigurnosne kopije — Sigurnosne kopije igraju kritičnu ulogu u planovima kontinuiteta operacija (COOP) osiguravajući da su kritični podaci i sustavi dostupni čak i za ometajućih događaja. Zahtjevi sigurnosnih kopija za COOP uključuju: učestalost sigurnosnih kopija, testiranje sigurnosnih kopija, sigurno pohranjivanje van lokacije i postupke oporavka.

Organizacije moraju osigurati da imaju prave tehnološke resurse za upravljanje povećanim radnim opterećenjima i podršku novim aplikacijama ili uslugama. Kada se radi o infrastrukturi, planiranje kapaciteta uključuje procjenu postojećih resursa, predviđanje budućih zahtjeva i planiranje za skaliranje resursa prema potrebi.

Rizici planiranja kapaciteta

Rizici za ljude vezani uz planiranje kapaciteta — Rizici za ljude vezani uz planiranje kapaciteta mogu uključivati nedovoljno osoblje ili jaz u vještinama, što dovodi do neadekvatne raspodjele resursa. Strategije za ublažavanje ovih rizika:

- Unakrsno osposobljavanje (Cross-Training) — Zahtijeva da zaposlenici razviju vještine i znanje izvan svojih primarnih uloga kako bi ublažili rizik od previše oslanjanja na specifične pojedince ili timove.
- Planovi za rad na daljinu — Opisuju strategije za učinkovit rad zaposlenika izvan tradicionalnog uredskog okruženja. Planovi za rad na daljinu definiraju komunikacijske kanale, tehnološke zahtjeve i očekivanja.
- Alternativne strukture izvještavanja — Opisuju privremene odnose izvještavanja za smanjenje rizika vezanog uz pojedinačne točke kvara u upravljanju ili donošenju

odluka.

- Virtualna privatna mreža (VPN) — Pruža siguran pristup internoj mreži i resursima organizacije.
- Softver za udaljenu radnu površinu — Dopušta udaljeni pristup računalima ili virtualnim radnim površinama u uredu.
- Alati temeljeni na cloudu — Platforme poput Microsoft 365, Google Workspacea, Dropboxa i Slacka omogućuju suradnju udaljenih timova, dijeljenje dokumenata i komunikaciju.
- Softver za video konferencije — Aplikacije poput Zooma, Microsoft Teamsa ili Webex olakšavaju virtualne sastanke i dijeljenje ekrana.
- Alati za trenutne poruke i chat — Aplikacije poput Slacka, Microsoft Teamsa ili Discorda omogućuju komunikaciju u stvarnom vremenu i brzu suradnju.
- Virtualni telefonski sustavi — Telefonski sustavi temeljeni na cloudu dopuštaju zaposlenicima upućivanje i primanje poziva na daljinu koristeći računala ili mobilne uređaje.
- Alati za upravljanje projektima — Platforme poput Trella, Asane ili Jire pomažu u upravljanju zadacima i praćenju projekata. Promjene u kapacitetu radne snage — Otkazi mogu uvesti niz kibernetičkih sigurnosnih i fizičkih rizika u organizaciju, što je ključno razmatrati unutar planiranja kapaciteta.

Nasuprot tome, precjenjivanje kapacitetnih potreba za planiranje kapaciteta može negativno utjecati na organizaciju. Povećani troškovi od nepotrebnih troškova za tehnologiju, infrastrukturu i osoblje opterećuju proračune i odvraćaju sredstva od bitnih inicijativa. Potpora za sustave ili resurse koji se ne koriste može biti složena i zahtijeva značajno osoblje i stručnost, što dovodi do povećanog opterećenja administracije.

Dostupnost i mjerne vrijednosti zastoja

Dostupnost sustava obično se mjeri kao postotak vremena rada: dvije devetke (99%) znači 87 sati i 36 minuta zastoja godišnje; tri devetke (99,9%) = 8h 45min; četiri devetke (99,99%) = 52min; pet devetki (99,999%) = 5min i 15s. Zastoj se izračunava iz zbroja zakazanih servisnih intervala plus neplanirani kvarovi.

Skalabilnost i elastičnost

Visoka dostupnost znači i da sustav može podnijeti brzi rast zahtjeva. Ova svojstva se nazivaju skalabilnošću i elastičnošću. Skalabilnost je sposobnost povećanja resursa za podršku povećanom opterećenju. Postoje dvije metode skaliranja:

- Horizontalno skaliranje (scale out) znači dodavanje više resursa paralelno s postojećim resursima.
- Vertikalno skaliranje (scale up) znači povećanje snage postojećih resursa.

Elastičnost se odnosi na sposobnost sustava da obradi ove promjene prema zahtjevu u stvarnom vremenu. Tolerancija kvarova — Oporavak od katastrofe može zahtijevati korištenje alternativnog mjesta obrade:

- Vruće web-mjesto (Hot site) može preuzeti gotovo odmah. Obično znači da je lokacija u vlasništvu organizacije i spremna za implementaciju s aktivnim skupom podataka.
- Toplo web-mjesto (Warm site) slično je, ali zahtijeva da se učita najnoviji skup podataka.

- Hladno web-mjesto (Cold site) treba duže za postavljanje. Može biti prazna zgrada s ugovorom o najmu za instalaciju potrebne opreme.

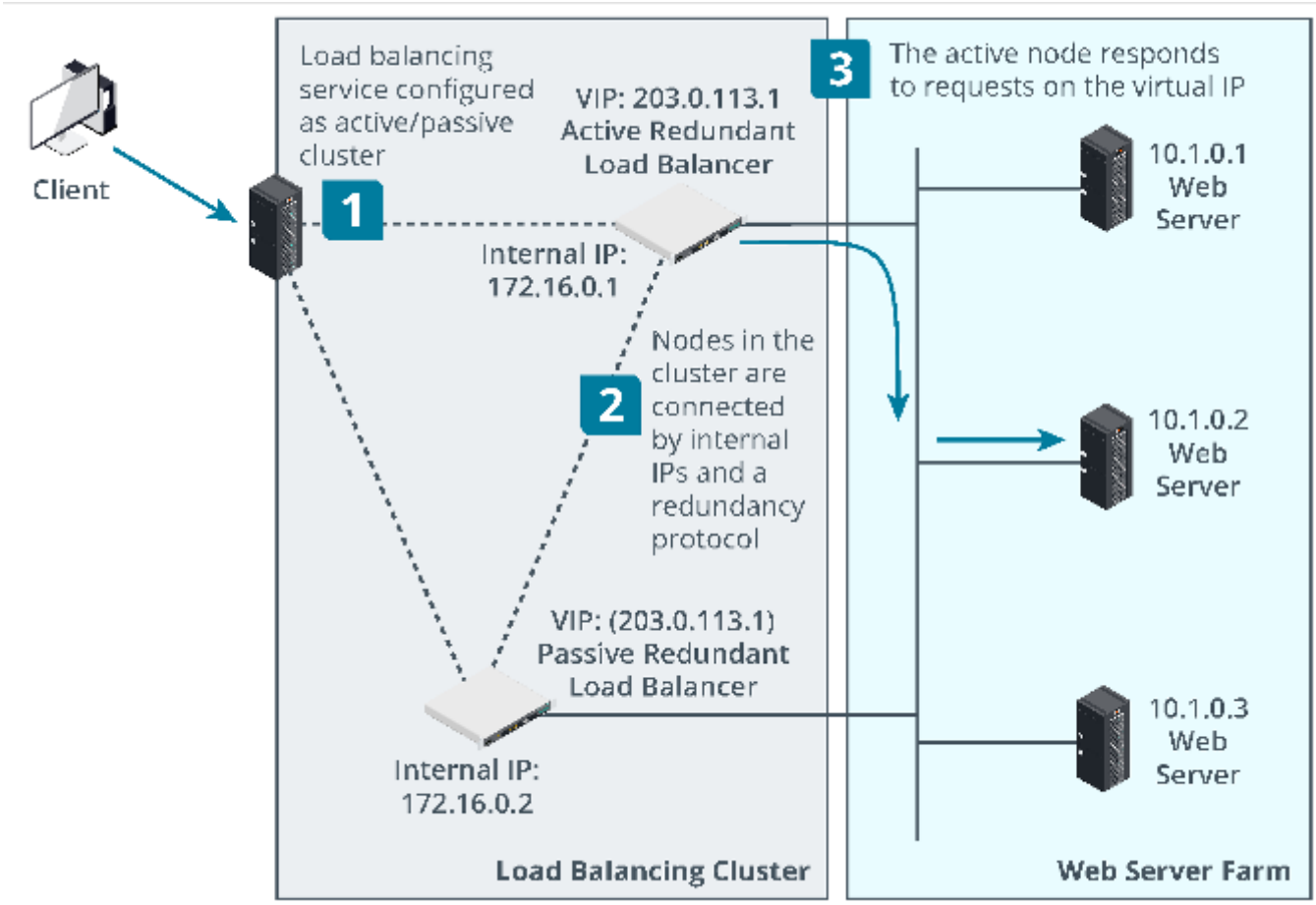
resursa. Isti sigurnosni postupci moraju se primjenjivati na redundantnim web-mjestima, rezervnim sustavima i sigurnosnim kopijama podataka kao i na glavnoj kopiji. Geografska disperzija odnosi se na distribuciju oporavilišnih web-mjesta na različitim geografskim lokacijama. Ovo osigurava da regionalna katastrofa ne pogodi istovremeno primarno i sekundarno web-mjesto. Vrste testiranja:

- Testiranje opterećenja uključuje specijalizirane softverske alate za validaciju performansi sustava pod očekivanim ili vršnim opterećenjima i identificiranje uskih grla ili problema skalabilnosti.
- Testiranje prebacivanja (failover) fokusira se na validaciju procesa prebacivanja kako bi osigurao besprijekoran prijelaz između primarne i sekundarne infrastrukture.
- Testiranje sustava nadzora validira učinkovito otkrivanje i odgovor na kvarove i probleme s performansama. Robusne prakse testiranja omogućuju organizacijama da osiguraju da tehnologije visoke dostupnosti, balansiranja opterećenja i prebacivanja učinkovito ispunjavaju svoju svrhu.

Klasteriranje

Dok balansiranje opterećenja distribuira promet između neovisnih čvorova obrade, klasteriranje dopušta višestrukim redundantnim čvorovima obrade koji međusobno dijele podatke da prihvataju veze. Ovo pruža redundanciju i visoku dostupnost za kritične sustave.

i uglavnom je povezano s upravljanjem web prometom, dok se klasteri koriste za pružanje redundancije i visoke dostupnosti za sustave poput baza podataka, datotečnih poslužitelja i ostalih. Virtualna IP adresa (VIP) — Na primjer, organizacija može koristiti virtualnu IP adresu za klaster baze podataka. Klijenti komuniciraju s VIP-om, a klasternii upravljač usmjerava zahtjeve na aktivni čvor. Ako aktivni čvor zakaže, VIP se automatski premješta na drugi čvor.



Aktivno/pasivno (A/P) i aktivno/aktivno (A/A) klasteriranje

U aktivno/pasivnoj konfiguraciji, jedan čvor je aktivan, a drugi je pasivan. Aktivni čvor obrađuje sve zahtjeve, dok je pasivni čvor u stanju čekanja spreman za preuzimanje ako aktivni čvor zakaže. U aktivno/aktivnoj konfiguraciji, svi čvorovi obrađuju zahtjeve istovremeno, što pruža bolje performanse i redundanciju.

N+1 i N+M konfiguracije: U standardnoj aktivno/pasivnoj konfiguraciji, svaki aktivni čvor mora biti usklađen s pasivnim čvorom. Kako bi se smanjili troškovi vezani uz pasivne čvorove, koriste se N+1 i N+M konfiguracije:

- N+1 konfiguracija: Ovdje se jedan pasivni čvor dijeli između višestrukih aktivnih čvorova. Na primjer, s pet aktivnih čvorova, umjesto pet pasivnih čvorova, provisioniran je samo jedan pasivni čvor koji može preuzeti za bilo koji aktivni čvor koji zakaže.
- N+M konfiguracija: U ovoj postavci, višestruki pasivni čvorovi dijele se između višestrukih aktivnih čvorova. Na primjer, s deset aktivnih čvorova, mogu biti dostupna dva ili tri pasivna čvora. Ovi pasivni čvorovi mogu preuzeti u slučaju kvarova, nudeći ravnotežu između redundancije i ekonomičnosti. Redundancija aplikacija — Redundancija aplikacija može se postići klasteriranjem, repliciranjem ili load balancingom.

UPS dopušta dovoljno vremena za prebacivanje na alternativni izvor napajanja, poput rezervnog generatora. Ako nema sekundarnog izvora napajanja, UPS će omogućiti administratoru da barem ugasi poslužitelj ili uređaj na prikladan način. Fizički sigurnosni kontrolnici poput UPS-a, PDU-ova i generatora osiguravaju redundanciju napajanja za

kritičnu infrastrukturu.

strategiji obrane u dubinu, pomažući u minimiziranju ljudske greške i osiguravanju brzog odgovora na sigurnosne incidente. Raznolikost dobavljača — Raznolikost dobavljača bitna je iz nekoliko razloga, nudeći prednosti ne samo u smislu kibernetičke sigurnosti, već i poslovne otpornosti i inovacija:

- Kibernetička sigurnost — Oslanjanje na jednog dobavljača za sva softverska i hardverska rješenja može stvoriti jednu točku kvara. Raznolikost dobavljača uvodi višestruke tehnologije, smanjujući utjecaj jedne ranjivosti.
- Poslovna otpornost — Raznolikost dobavljača ublažava rizik vezan uz zavisnost o jednom dobavljaču i osigurava da operacije organizacije nisu u potpunosti ovisne o proizvodima ili uslugama jednog dobavljača.
- Inovacija — Raznolikost dobavljača donosi različite perspektive, ideje i tehnologije, što može dovesti do inovativnije i agilne IT infrastrukture.
- Natjecanje — Raznolikost dobavljača promiče zdravo tržišno natjecanje, što može dovesti do boljih cijena, poboljšanih značajki proizvoda i kvalitetnije korisničke podrške.
- Prilagodba i fleksibilnost — Različiti dobavljači nude jedinstvena rješenja koja zadovoljavaju specifične potrebe, a raznolik ekosustav dobavljača dopušta organizacijama odabir najboljeg rješenja za njihove zahtjeve.
- Upravljanje rizicima — Raznolikost dobavljača pomaže u raspoređivanju rizika vezanog uz potencijalne kvarove proizvoda ili usluga, sigurnosne povrede i ostale probleme.
- Usklađenost — U nekim industrijama, propisi ili industrijski standardi mogu zahtijevati od organizacija održavanje raznolikosti dobavljača radi osiguravanja usklađenosti.

sigurnost podataka, optimizaciju performansi i ekonomičnost. Hostiranjem primarne aplikacijske infrastrukture kod jednog pružatelja clouda i korištenjem drugog za sigurnosne kopije i oporavak od katastrofe, tvrtka osigurava kontinuiranu dostupnost i raznolikost dobavljača. Tehnike dezinformacija i privlačenja pozornosti:

- Korištenjem lažnih DNS unosa za navođenje višestrukih hostova koji ne postoje.
- Konfiguriranjem web poslužitelja s višestrukim mamac direktorijima ili dinamički generiranim stranicama za usporavanje skeniranja.
- Korištenjem okidanja porta ili lažiranja za vraćanje lažnih telemetrijskih podataka kada host detektira aktivnost skeniranja portova. Ovo će rezultirati lažnim izvješćivanjem o višestrukim portovima kao otvorenima i usporavanjem skeniranja.
- Korištenjem DNS ponora (sinkhole) za preusmjeravanje sumnjivog prometa na drugu mrežu, poput honeyneta, gdje se može analizirati.

Testiranje otpornosti

Metode testiranja — Testiranje otpornosti sustava i učinkovitosti odgovora na incidente ključno je za organizacije da se oporave od ometanja i održe kontinuitet poslovanja. Provođenjem raznih testova, organizacije mogu identificirati slabosti i prilike za poboljšanje.

- Vježbe na okruglom stolu (Tabletop Exercises) uključuju timove koji raspravljaju i rade kroz hipotetske scenarije za procjenu njihovih planova odgovora i procesa donošenja odluka.

identificiraju jaz u znanju, komunikaciji i koordinaciji, što u konačnici jača sposobnosti organizacije za odgovor na incidente. Na primjer, vježba na okruglom stolu može simulirati napad ransomwarea kako bi testirala koliko dobro tim odgovora na incidente koordinira komunikaciju i eskalira problem.

- Testovi prebacivanja (Failover Tests) uključuju namjerno uzrokovanje kvara primarnog sustava ili komponente za procjenu automatskog prijenosa operacija na sekundarni, redundantni sustav. Ovi testovi osiguravaju da rezervni sustavi mogu besprijekorno preuzeti za stvarnog incidenta, minimizirajući zastoj i gubitak podataka.
- Simulacije su kontrolirani eksperimenti koji repliciraju scenarije iz stvarnog svijeta, dopuštajući organizacijama da procijene svoje procese odgovora na incidente i otpornost sustava pod realnim uvjetima.
- Testovi paralelne obrade uključuju istovremeno pokretanje primarnih i rezervnih sustava za validaciju funkcionalnosti i performansi rezervnih sustava bez ometanja normalnih operacija.

Lekcija 7C

Fizička sigurnost

Pregled lekcije

Koncepti fizičke sigurnosti kritična su komponenta kibernetičke sigurnosti. Mjere fizičke sigurnosti, poput kontrole pristupa, videonadzora i kontrola okoliša, pomažu u zaštiti fizičke imovine organizacije, uključujući infrastrukturu i opremu, od fizičkih prijetnji i neovlaštenog pristupa.

Kontrole fizičke sigurnosti

Fizička sigurnost kritična je za operacije kibernetičke sigurnosti jer pruža prvu liniju obrane od fizičkog pristupa kritičnoj imovini organizacije. Kibernetička sigurnost je o osiguravanju podataka i sustava, a fizička sigurnost je o osiguravanju fizičke opreme i prostora koji podržavaju te sustave.

- Autentikacija — Kreira popise pristupa i identificira mehanizme koji dopuštaju odobrenim osobama prolaz kroz barijere.
- Autorizacija — Kreira barijere oko resursa za kontrolu pristupa putem definiranih ulaznih i izlaznih točaka.
- Računovodstvo — Bilježi kada se koriste ulazne/izlazne točke i otkriva sigurnosne povrede.

Fizička sigurnost često se implementira ugradnjom zona. Svaka zona je odvojena vlastitim barijerama. Jedan ili više sigurnosnih mehanizama kontroliraju ulazne i izlazne točke kroz barijere.

Raspored lokacije, ograde i osvjetljenje

Fizička sigurnost kroz dizajn okoliša — Fizička sigurnost kroz dizajn okoliša je pristup sigurnosti koji koristi izgrađeni okoliš za poboljšanje sigurnosti i sprječavanje kriminala. Ovaj pristup uključuje pažljivo planiranje i dizajn fizičke lokacije za maksimiziranje vidljivosti, smanjenje skrovišta i stvaranje osjećaja reda.

Ograde

Vanjski dio zgrade može biti zaštićen ogradama. Sigurnosne ograde trebaju biti transparentne (kako bi čuvari mogli vidjeti svaki pokušaj proboja), robusne (kako bi ih bilo teško prerezati) i sigurne protiv penjanja (visine najmanje 2,5 metra, a idealno s bodljikavom žicom na vrhu).

Stupci (Bollards) koji se koriste za zaštitu ulaza željezničke stanice Reading u Britaniji.

Postojeće strukture

Može biti malo opcija za prilagodbu rasporeda lokacije u postojećim prostorijama. Suočeni s troškovnim ograničenjima i potrebom za ponovnim korištenjem postojeće infrastrukture, ugradnja sljedećih principa može poboljšati sigurnost:

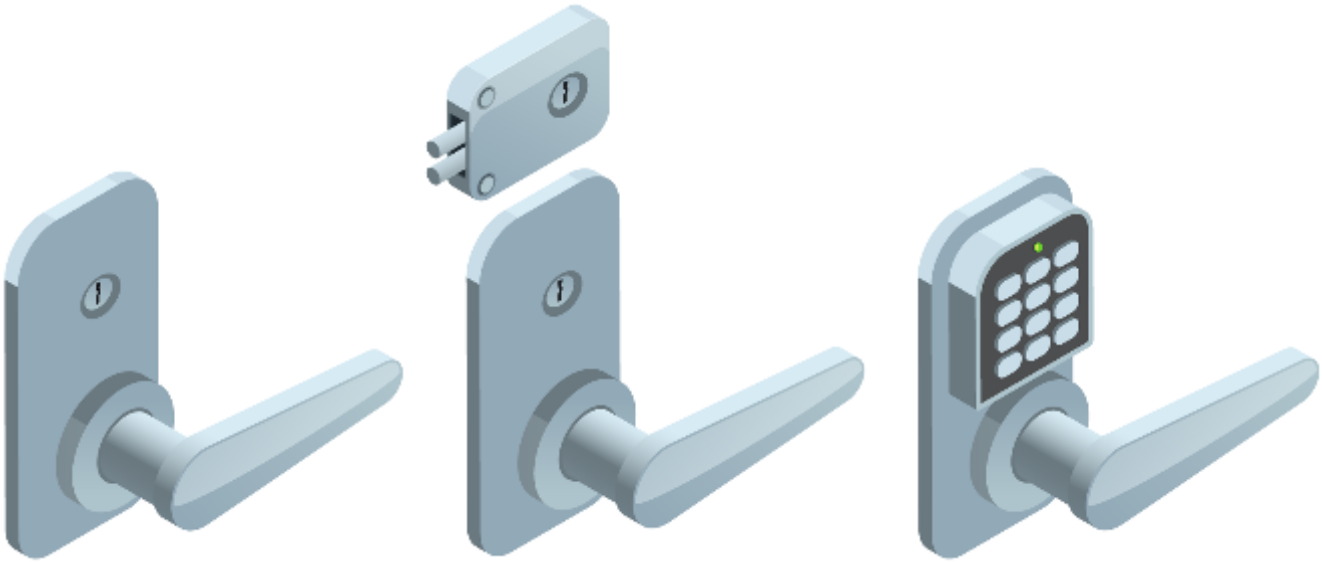
- Smjestite sigurne zone, poput prostorija s opremom, što dublje unutar zgrade, izbjegavajući vanjske zidove, vrata i prozore.
- Koristite demilitariziranu zonu za fizički prostor. Pozicionirajte javne pristupne zone tako da gosti ne prolaze pored sigurnih zona.
- Koristite oznake i upozorenja za jačanje ideje da je sigurnost strogo kontrolirana. Osim osnovnih znakova 'zabranjen ulaz', neka doma i uredi prikazuju i znakove sigurnosnih tvrtki čije usluge koriste.
- Nasuprot tome, ulazne točke u sigurne zone trebaju biti diskretne. Ne dopustite uljez da ima priliku pregledati sigurnosne mehanizme koji štite takve zone.
- Nastojte minimizirati promet koji prolazi između zona. Tok ljudi treba biti 'unutra i van', a ne 'kroz i između'.

- Dajte visokoprommetnim javnim područjima visoku vidljivost kako biste otežali prikriveno korištenje pristupnika, mrežnih portova i računalne opreme.
- U sigurnim zonama, pozicionirajte zaslone ili uređaje za unos dalje od prolaza ili prozora. Koristite jednosmjerno staklo vidljivo samo iznutra prema van.

Pristupnici i brave

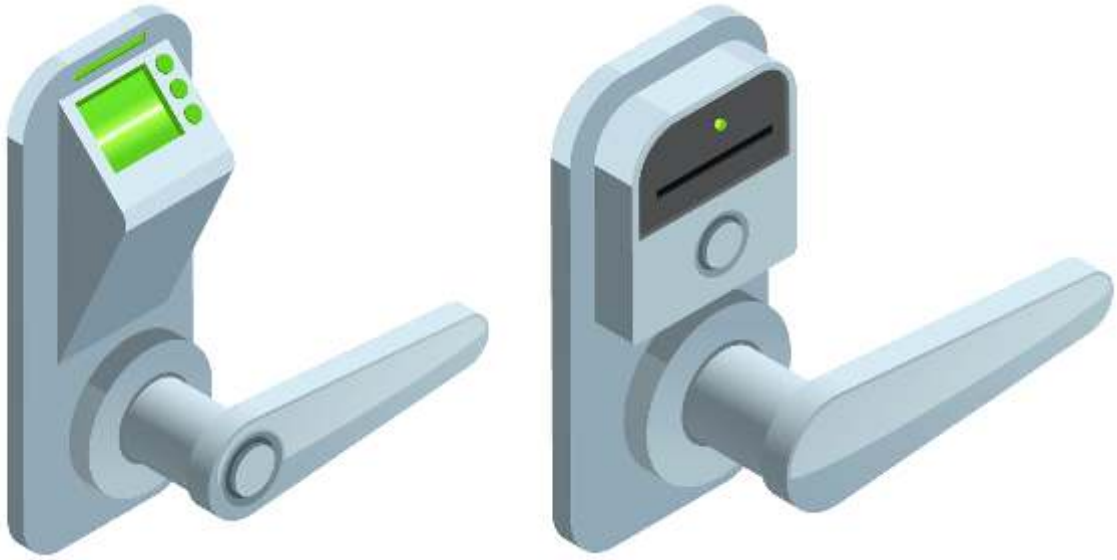
Za osiguravanje pristupnika mora biti opremljen bravicom. Siguran pristupnik normalno će biti samozatvarajući i samobravajući, a ne ovisan o korisniku da ga zatvori i zaključa. Vrste brava:

- Fizičke — su konvencionalne brave koje sprječavaju rukovanje kvaki vrata bez korištenja ključa. Skuplje vrste nude veću otpornost na biranje brave.
- Elektroničke — su brave koje umjesto ključa rade unosom PIN-a na elektroničku tipkovnicu. Ova vrsta brave se naziva i šifarskom, kombiniranom ili bravom bez ključa. Pametna brava može biti otvorena magnetskom karticom ili može imati čitač blizine za otkrivanje prisutnosti fizičkog tokena.



- Biometrijske — je brava integrirana s biometrijskim skenerom.

Generički primjeri biometrijskog skenera za otisak palca i brave temeljene na kartici s tokenom.



Pristupna kontrolna čekaonica (Mantrap)

Pristupna kontrolna čekaonica, poznata i kao mantrap, sigurnosna je mjera koja regulira ulaz u sigurno područje. Uključuje dvoja vrata ili kapije koja su međusobno zaključana i dopuštaju samo jednoj osobi prolaz odjednom. Prva vrata moraju biti zatvorena i zaključana prije nego što se druga vrata mogu otvoriti, sprječavajući neovlašteni pristup i osiguravajući da svaka osoba može biti verificirana zasebno.

Zaštitari i kamere

Nadzor je tipično drugi sloj sigurnosti dizajniran za poboljšanje otpornosti perimetarskih pristupnika. Nadzor se može fokusirati na perimetarna područja ili unutar sigurnosnih zona. Zaštitari mogu biti trenirani za prepoznavanje i odgovor na sigurnosne prijetnje u stvarnom vremenu.

učinkovit mehanizam za otkrivanje i odvraćanje od upada, ali je razmjerno skup. Može biti nemoguće postaviti zaštitare unutar određenih zona jer im ne može biti dodijeljena odgovarajuća sigurnosna dozvola.

Kamere u CCTV mreži tipično su spojene na multiplekser koristeći koaksijalne kablove. Multiplekser može prikazivati slike s kamera na jednom ili više ekrana, dozvoliti operateru upravljanje funkcijama kamere i pohraniti slike na medij poput video kasete ili tvrdog diska.

- Prepoznavanje kretanja — Pojavljuje se kada je sustav kamere konfiguriran s tehnologijom identifikacije hoda. To znači da sustav može generirati upozorenje kada se itko u vidnom polju kamere kreće u obrascu koji ne odgovara poznatoj i ovlaštenoj osobi.
- Detekcija objekata — Pojavljuje se kada sustav kamere može detektirati promjene u okolini, poput nestajanja poslužitelja ili nepoznatog uređaja spojenog na zidni port.
- Dronovi/UAV — kamere montirane na dronovima mogu pokriti šira područja nego zemaljske patrole.

Alarmni sustavi i senzori

Alarmi igraju vitalnu ulogu u fizičkoj sigurnosti nadopunjujući ostale sigurnosne kontrole. Alarmi upozoravaju osoblje zaštite i stanare zgrade o potencijalnim prijetnjama ili povredama. Oni su i kontrole otkrivanja i odvraćanja.

- Krug (Circuit) — Koristi alarm temeljen na strujnom krugu koji se oglašava kada se krug otvori ili zatvori, ovisno o vrsti alarma. Na primjer, to bi moglo biti otvaranje vrata ili prozora ili rezanje ograde.
- Detekcija kretanja (Motion Detection) — Koristi alarm temeljen na kretanju vezan za detektor koji se aktivira bilo kojim kretanjem unutar područja. Senzori u ovim detektorima su ili mikrovalovi radiosignali ili pasivni infracrveni (PIR) koji otkrivaju toplinu tijela.

- Detekcija buke (Noise Detection) — Koristi alarm koji aktiviraju zvukovi koje prima mikrofon. Moderna AI analiza može identificirati specifične vrste zvuka, čineći ovaj tip sustava manje sklonim lažnim pozitivima.
- Blizina (Proximity) — Koristi RFID tagove i čitače za praćenje kretanja označenih objekata unutar područja. To omogućuje alarmnom sustavu otkrivanje pokušava li netko ukloniti opremu.
- Prisila (Duress) — Koristi alarm koji ručno aktivira osoblje ako dođe pod prijetnju. Postoje mnogi načini implementacije ove vrste alarma, uključujući bežične privjeske, skrivene senzore ili okidače i pametne telefone.
- Infracrveni senzori uobičajeno se koriste u sustavima za otkrivanje kretanja. Detektiraju promjene toplinskih uzoraka uzrokovane pokretnim objektima, poput ljudskog uljeza. Ovi se često koriste u stambenim i poslovnim sigurnosnim sustavima, aktivirajući alarme ili sigurnosna svjetla kada otkriju kretanje.
- Senzori tlaka tipično su instalirani unutar podova ili prostirki i aktiviraju se težinom. Mogu se koristiti u visoko sigurnim područjima za otkrivanje neovlaštenog pristupa ili čak u prodajnim okruženjima za brojanje posjetitelja.
- Mikrovalovi senzori emitiraju mikrovalove i mjere odraz od pokretnog objekta. Često su kombinirani s infracrvenim detektorima u dvojnim tehnološkim senzorima kretanja.
- Ultrazvučni senzori emitiraju zvučne valove na frekvencijama iznad raspona ljudskog sluha i mjere vrijeme koje valovi trebaju da se vrate nakon udara o objekt. Često se koriste u automatiziranim sustavima rasvjete.

Sažetak

Trebate biti u mogućnosti objasniti važnost upravljanja imovinom, koncepata otpornosti i fizičkih sigurnosnih kontrola u potpori operacija kibernetičke sigurnosti. Smjernice za upravljanje imovinom i kontrole otpornosti:

- Identificirajte imovinu: katalogizirati svu imovinu, fizičku i nematerijalnu; uključiti ključne informacije poput vrste, lokacije, vrijednosti i vlasništva; implementirati upravljanje životnim ciklusom imovine.
- Pratite imovinu: pratite lokaciju i status imovine, posebno mobilnih ili imovine sklone krađi.
- Razumijte zahtjeve regulatorne usklađenosti: imovina vezana uz zdravlje i sigurnost, zaštitu podataka mora biti upravljana usklađeno s propisima.
- Provedite planiranje oporavka od katastrofe i kontinuiteta poslovanja.
- Sigurno zbrinite imovinu koristeći zakonski usklađene i sigurne metode.

Osigurajte adekvatno planiranje kapaciteta za ljude, tehnologiju i infrastrukturu:

- Implementirajte strategije visoke dostupnosti uključujući: skalabilnost i elastičnost, toleranciju kvarova i redundanciju, klasteriranje, otpornost web-mjesta.
- Koristite procjene rizika za identificiranje imovine s visokim zahtjevima dostupnosti.
- Provisionirajte redundanciju radi ispunjavanja zahtjeva visoke dostupnosti.
- Vruće, toplo ili hladno web-mjesto za oporavak od katastrofe.

- Koristite dvostruko napajanje, PDU-ove, UPS-ove i generatore za otpornost sustava napajanja.
- Koristite NIC udruživanje, višestruke putove i balansiranje opterećenja za otpornost mreže.

Slijedite ove smjernice za implementaciju ili nadogradnju fizičkih sigurnosnih kontrola:

- Ako je moguće, dizajnirajte lokacije kao zone za maksimiziranje kontrola pristupa i nadzora za najsigurnija područja, koristeći industrijsku kamuflaž, perimetarsku mrežu, air gapove, sefove i trezore gdje je primjenjivo.
- Osigurajte perimetar lokacije i pristupne točke koristeći ograde, barijere/stupce i brave (fizičke, elektroničke i biometrijske). Ako koristite pametne kartice, koristite vrstu otpornu na kloniranje/skimming.
- Nadzirite lokaciju koristeći zaštitare, CCTV i dronove/UAV, te koristite učinkovito osvjetljenje za maksimiziranje nadzora.
- Implementirajte alarmni sustav (krug, temeljen na kretanju, blizini i/ili prisilni) za otkrivanje upada.
- Koristite ID bedževe za autorizaciju pristupa.

Modul 8

Objasni upravljanje ranjivostima

Pregled modula

Upravljanje ranjivostima kritično je za kibernetičku strategiju svake organizacije, obuhvaćajući identificiranje, procjenu, liječenje i izvještavanje o sigurnosnim ranjivostima u operativnim sustavima, aplikacijama i ostalim komponentama. Proaktivno upravljanje ranjivostima pomaže organizacijama u smanjenju površine napada i ublažavanju rizika od kompromitiranja sigurnosti.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Opisati važnost upravljanja ranjivostima.
- Objasniti sigurnosne brige vezane uz opće i ranjivosti specifične za aplikacije.
- Sažeti tehnike skeniranja ranjivosti.
- Objasniti analizu ranjivosti i mjere sanacije.

Lekcija 8A

Ranjivosti uređaja i OS-a

Pregled lekcije

Operativni sustavi, uključujući mobilne, česta su meta kibernetičkih napada. Upravljanje ranjivostima u ovim sustavima igra centralnu ulogu u operacijama kibernetičke sigurnosti. Ranjivosti se uvode iz različitih izvora, uključujući neispravno kodiranje, pogrešnu konfiguraciju i upotrebu zastarjelog softvera.

Ranjivosti operativnog sustava

Operativni sustavi (OS) jedna su od najkritičnijih komponenti svake infrastrukture, pa ranjivosti u OS-u mogu dovesti do značajnih problema kada su uspješno iskorištene. Microsoft Windows, macOS, Linux i mobilni OS poput Androida i iOS-a su svi podložni ranjivostima koje trebaju biti pažljivo upravljane.

Široko usvajanje mobilnih OS-ova poput Androida i iOS-a i njihova sve veća upotreba kao primarnih računalnih platformi umjesto tradicionalnih računala čini ih vrijednim metama za napad i eksploataciju. Android je otvorenog koda, što ga čini podložnim fragmentaciji i neravnomjernoj primjeni ažuriranja.

- Microsoft Windows — Jedna od najozloglašenijih ranjivosti u povijesti Windowsa bila je MS08-067 ranjivost u Windows Server Serviceu. Ova ranjivost je dopuštala izvršavanje udaljenog koda ako je posebno izrađen paket poslan Windows poslužitelju. Ovu ranjivost je iskoristio crv Conficker.
- macOS — 2014. godine značajna ranjivost nazvana 'Shellshock' pogodila je sve sustave temeljene na Unixu, uključujući macOS. Dopuštala je napadačima da potencijalno preuzmu kontrolu nad sustavom zbog greške u Bash shellu.
- Android — Ranjivost Stagefright otkrivena 2015. prominentan je primjer za Android. Dopuštala je napadačima izvršavanje zlonamjernog koda na Android uređaju slanjem posebno izrađene MMS poruke.
- iOS — 2019. godine tim Project Zero tvrtke Google otkrio je niz ranjivosti u iOS-u koje su napadači vezani uz nacije zloupotrebljavali. Ovi 'napad na pojilištu' iskoristili su nekoliko ranjivosti za dobivanje potpunog pristupa uređaju.

- Linux — Buba Heartbleed 2014. bila je ozbiljna ranjivost u OpenSSL kriptografskoj softverskoj biblioteci u mnogim Linux sustavima. Ranjivost je dopuštala napadačima čitanje memorije sustava koji pokreće ranjive verzije OpenSSL softvera, kompromitujući tajne ključeve.

Vrste ranjivosti

Naslijeđeni i sustavi na kraju životnog vijeka (EOL) — Hardverske ranjivosti, posebno one vezane uz sustave na kraju životnog vijeka i naslijeđene sustave, predstavljaju značajne sigurnosne izazove za mnoge organizacije.

dijele zajedničku karakteristiku: oba su zastarjela. EOL sustavi mogu biti naslijeđeni sustavi, a neki naslijeđeni sustavi su i EOL. Proizvođač ili dobavljač više ne podržava EOL sustave, pa ne primaju ažuriranja, ispravke ili sigurnosne zakrpe. To ih čini ranjivima na iskorištavanje poznatih ranjivosti koje neće biti zakrpane. Organizacije koje rade s EOL sustavima suočavaju se s povećanim rizicima sigurnosnih povreda jer napadači mogu koristiti poznate ranjivosti bez straha od buduće zakrpe.

Takva ranjivost mogla bi omogućiti napadaču da preuzme kontrolu nad svim virtualnim strojevima koji se pokreću na jednom fizičkom poslužitelju, dovodeći do potencijalno razornog sigurnosnog proboja. Poznati primjer je ranjivost 'Cloudburst', koja je pogodila VMware Workstation i dopustila izvršavanje koda u gostu koji bi mogao izaći iz virtualnog stroja i kompromitirati host sustav.

Ranjivosti nultog dana (Zero-Day)

Ranjivosti nultog dana odnose se na prethodno nepoznate greške softvera ili hardvera koje napadači mogu iskoristiti prije nego što programeri ili dobavljači postanu svjesni njih ili imaju priliku ih popraviti. Naziv 'zero-day' odnosi se na broj dana od kada je prodavač softvera saznao za ranjivost — nula dana znači da su upravo otkriveni i nema dostupne zakrpe.

Ranjivosti nultog dana imaju značajnu financijsku vrijednost. Zero-day exploit za mobilni OS može vrijediti milijune dolara. Sukladno tome, protivnik će koristiti ranjivost nultog dana samo za napade visoke vrijednosti. Stoga se ranjivosti nultog dana pažljivo čuvaju u tajnosti dok se ne iskoriste.

Ranjivosti pogrešne konfiguracije

Pogrešna konfiguracija sustava, mreža ili aplikacija uobičajen je uzrok sigurnosnih ranjivosti. To može dovesti do neovlaštenog pristupa, curenja podataka ili čak potpunog kompromisa sustava. Tipične pogrešne konfiguracije uključuju: nepromijenjena zadana lozinka, nepotrebne otvorene portove i usluge, previše permisivne kontrole pristupa i nedostatak enkripcije.

Kriptografske ranjivosti

Kriptografske ranjivosti odnose se na slabosti u kriptografskim sustavima, protokolima ili algoritmima koje se mogu iskoristiti za kompromitiranje podataka. Značaj takvih ranjivosti je proporcionalan osjetljivosti podataka koje štite — greška u kriptografiji može razotkriti osjetljive financijske podatke, tajne vlade ili osobne identifikacijske informacije.

u WPA2 protokolu koji štiti Wi-Fi promet. Ova ranjivost dopušta napadaču u dometu žrtve da presretne i dekriptira neke vrste osjetljivog mrežnog prometa. Simetrični i asimetrični algoritmi šifriranja mogu biti ranjivi zbog slabih ključeva, zastarjelih algoritama ili implementacijskih grešaka.

Generiranje kriptografskog ključa opisuje proces stvaranja kriptografskih ključeva za šifriranje, dešifriranje, autentikaciju ili druge svrhe. Važno je koristiti industrijske preporučene pristupe pri generiranju kriptografskih ključeva, osiguravanju ključeva, izvođenju rotacije i upravljanju životnim ciklusom ključeva.

kontrole i mehanizme autentikacije, te redovito praćenje i revizija korištenja ključeva. Uz to, organizacije moraju povremeno mijenjati kriptografske ključeve (što se naziva i rotacijom ključeva) kako bi ojačale sigurnost sustava i ublažile rizik od kompromisa ključeva.

Bočno učitavanje (Sideloading), Rootanje i Jailbreaking

Mobilni uređaji uvode jedinstvene sigurnosne ranjivosti vezane uz njihov rad i specijalizirani softver:

- Rootanje — Uključuje dobivanje root pristupa ili administrativnih privilegija na Android uređaju za modificiranje sistemskih datoteka, instaliranje prilagođenih ROM-ova i pristup značajkama koje nisu dostupne regularnim korisnicima.
- Jailbreaking — Dok se ovaj pojam može primijeniti na bilo koji uređaj, primarno se koristi za opisivanje dobivanja potpunog pristupa iOS uređaju (iPhoneu ili iPadu) uklanjanjem ograničenja koja nameće Appleov iOS. Jailbreaking dopušta korisnicima instaliranje neovlaštenih aplikacija i prilagodbu uređaja.

Aplikacijska trgovina F-Droid za Android.

Rootanje, bočno učitavanje i jailbreaking nude korisnicima veću kontrolu i fleksibilnost nad njihovim uređajima, ali uvode i mnoge rizike za organizacije. Rootanje, bočno učitavanje i jailbreaking mogu oslabiti sigurnosne mehanizme uređaja, čineći ga ranjivijim na napade. Na primjer, uklanjanjem Appleovog Gatekeepera zaštite od jailbreakinga, iOS uređaj može instalirati i pokrenuti nepotpisani kod i aplikacije koje nisu prošle Appleov sigurnosni pregled.

Organizacije koje djeluju u reguliranim industrijama poput zdravstva ili financija trebaju implementirati stroge politike koje zabranjuju rootanje, bočno učitavanje i jailbreaking zbog povećanog rizika od povreda podataka i neusklađenosti.

Lekcija 8B

Ranjivosti aplikacija i clouda

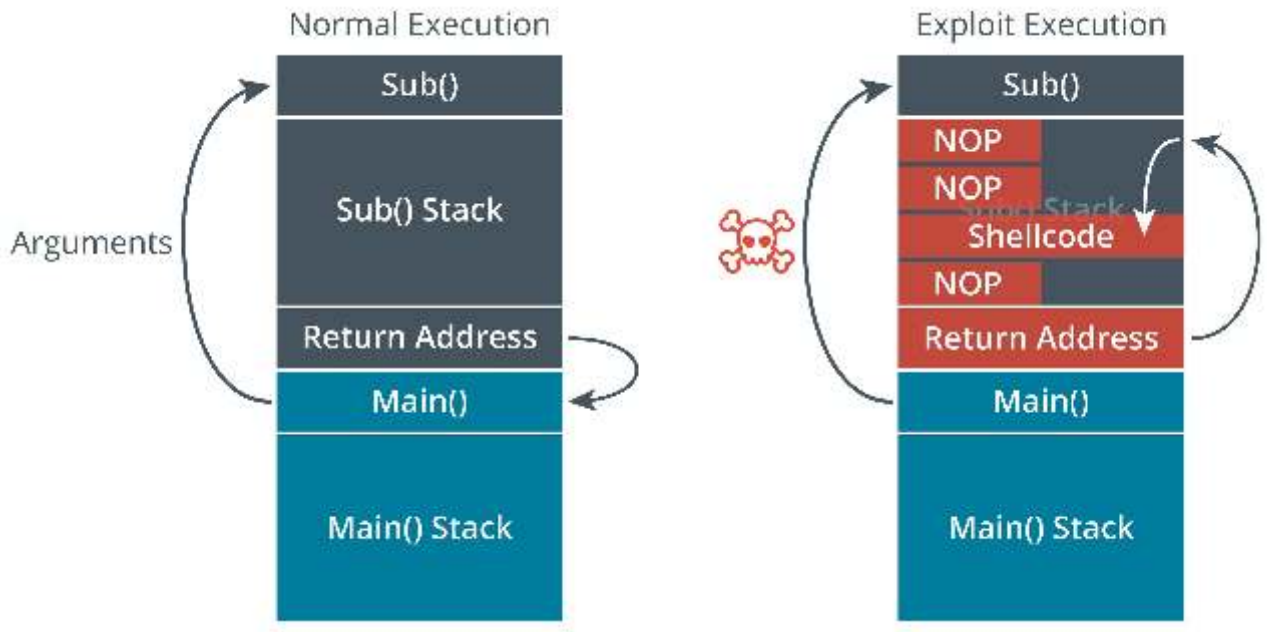
Pregled lekcije

Web i cloud aplikacije uvode jedinstvene sigurnosne brige koje proizlaze iz različitih izvora, poput pogrešnih konfiguracija, nesigurnih praksi kodiranja i upotrebe komponenti trećih strana s poznatim ranjivostima.

Ranjivosti aplikacija

Stanje utrke (Race Condition) i TOCTOU — Ranjivosti aplikacija uvjetovane stanjem utrke odnose se na greške softvera vezane uz vremenski redoslijed događaja unutar softverskog programa, koje se mogu manipulirati i dovesti do neočekivanog i potencijalno opasnog ponašanja. TOCTOU (Time of Check to Time of Use) je vrsta ranjivosti stanja utrke.

korisniku da dobije privilegirani pristup, i Microsoft Windows ranjivost povećanja privilegija (CVE-2020-0796), koja je ranjivost stanja utrke vezana uz protokol Microsoft Server Message Block 3.1.1 (SMBv3). Upravljanje zakrpama je ključno za adresiranje ranjivosti stanja utrke čim ih dobavljači otkriju.



Zlonamjerno ažuriranje (Malicious Update)

Zlonamjerno ažuriranje odnosi se na ažuriranje koje izgleda legitimno, ali sadrži štetni kod, koji kibernetički kriminalci često koriste za distribuciju malwarea ili izvršavanje kibernetičkog napada. Ažuriranje može tvrditi da ispravlja greške softvera ili nudi nove značajke, ali u stvarnosti kompromitira sustav ili podatke korisnika.

Opseg evaluacije

Meta ili opseg evaluacije odnosi se na proizvod, sustav ili uslugu koja se analizira za potencijalne sigurnosne ranjivosti. To može biti softverska aplikacija, mreža, sigurnosna usluga ili čak organizacijsko okruženje. Prakse opsega evaluacije uključuju: kriptografsku analizu, procjenu kontrole pristupa, pregled konfiguracije i testiranje penetracije.

Prakse opsega evaluacije

Kriptografska analiza: Procjenjivanje kriptografskih mehanizama, uključujući algoritme enkripcije, upravljanje ključevima i sigurnu pohranu ključeva. Procjena kontrole pristupa: Procjenjivanje pristupnih kontrolnih mehanizama, uključujući autentikaciju, autorizaciju i reviziju. Pregled konfiguracije: Pregled konfiguracije sustava, uređaja i aplikacija za identificiranje potencijalnih sigurnosnih slabosti. Testiranje penetracije: Pokušaj iskorištavanja ranjivosti unutar definiranog opsega za procjenu sigurnosnog položaja sustava.

(XSS). Ovi napadi iskorištavaju inherentno povjerenje weba u zahtjeve ili skripte koje izgledaju kao da dolaze od valjanih korisnika ili pouzdanih stranica. CSRF je opširnije raspravljen u Lekciji 13.

Skriptiranje na više stranica (Cross-Site Scripting

XSS) — Web aplikacije ovise o skriptiranju, a većina web stranica danas su web aplikacije, a ne statičke stranice. XSS ranjivosti dopuštaju napadaču da ubaci zlonamjerni kod u web stranicu koja se prikazuje u korisnikovom pregledaču. Postoje dvije primarne vrste XSS napada: pohranjeni (persistent) XSS i odraženi (reflected) XSS.

3. Poslužitelj vraća stranicu s legitimnom DOM skriptom ugrađenom, ali koja sadrži parametar: James 4. Preglednik prikazuje stranicu koristeći DOM skriptu, dodajući

zlonamjernu skriptu na stranicu. 5. Preglednik izvršava skriptu, koja šalje žrtvin kolačić sesije na badsite.foo.

Napadi na cloud aplikacije

Napadi na cloud aplikacije ciljaju aplikacije hostirane na cloud platformama i iskorištavaju potencijalne ranjivosti unutar tih aplikacija ili cloud infrastrukture na kojoj rade.

Visoko dostupna i skalabilna priroda clouda može učiniti cloud aplikacije atraktivnim metama za napadače. Na primjer, napadač može iskoristiti ranjivost u cloud aplikaciji, što rezultira neovlaštenim pristupom osjetljivim podacima pohranjenim u cloudu.

Cloud kao platforma za napad

Napadači mogu koristiti cloud platforme i za phishing i distribuciju malwarea. Mogu lako postaviti lažne web stranice koje oponašaju legitimne na cloud uslugama i koristiti ove stranice za trikiranje korisnika da otkriju osjetljive informacije. Posrednik za sigurnost pristupa cloudu (CASB) je sigurnosna usluga koja djeluje kao posrednik između korisnika i pružatelja cloud usluge. CASB može:

- Omogućiti autentikaciju s jednom prijavom i provoditi kontrole pristupa od poslovne mreže do pružatelja clouda.
- Skenirati za malware i lažan ili nesukladan pristup uređaja.
- Nadzirati i revidirati aktivnost korisnika i resursa.
- Ublažiti eksfiltraciju podataka sprječavanjem pristupa neovlaštenim cloud uslugama s upravljanih uređaja.
- Forward proxy — je sigurnosni uređaj ili host pozicioniran na rubu klijentske mreže koji prosljeđuje korisnički promet na cloud mrežu ako sadržaj tog prometa udovoljava politici.
- Reverse proxy — je pozicioniran na rubu cloud mreže i usmjerava promet na cloud usluge ako sadržaj tog prometa udovoljava politici. Ne zahtijeva konfiguraciju korisničkih uređaja.
- Sučelje za programiranje aplikacija (API) — posreduje veze između cloud usluge i cloud potrošača umjesto postavljanja CASB uređaja ili hosta inline. Na primjer, ako je korisnički račun onemogućen ili autorizacija opozvana na lokalnoj mreži, API može komunicirati ovu promjenu cloud pružatelju.

Lanac opskrbe

Ranjivosti lanca opskrbe softvera odnose se na potencijalne rizike i slabosti uvedene u softverske proizvode tijekom njihovog razvoja, distribucije i održavanja životnog ciklusa. Ovaj lanac opskrbe opisuje putovanje softvera od koncepcije do korisnika. Svaka karika u lancu može biti potencijalna točka ulaska za napadače koji žele kompromitirati softver.

kao biblioteke, frameworki i druge komponente trećih strana. SBOM (Software Bill of Materials) uključuje detalje poput naziva komponente, verzija i informacija o dobavljačima. SBOM ima za cilj pružiti transparentnost i vidljivost u softversku arhitekturu, pomažući organizacijama u upravljanju rizicima vezanim uz ranjivosti lanca opskrbe. Pored SBOMa, organizacije trebaju provoditi skeniranje ranjivosti lanaca opskrbe i koristiti alate za analizu sastava softvera (SCA).

Lekcija 8C

Metode identifikacije ranjivosti

Pregled lekcije

Skeniranje ranjivosti temeljni je zadatak unutar programa upravljanja ranjivostima i koristi automatizirane procese skeniranja za identificiranje i procjenu potencijalnih problema. Skenovi ranjivosti fokusiraju se na mreže, operativne sustave, aplikacije i uređaje, tražeći poznate ranjivosti, pogrešne konfiguracije i slabosti.

Skeniranje ranjivosti

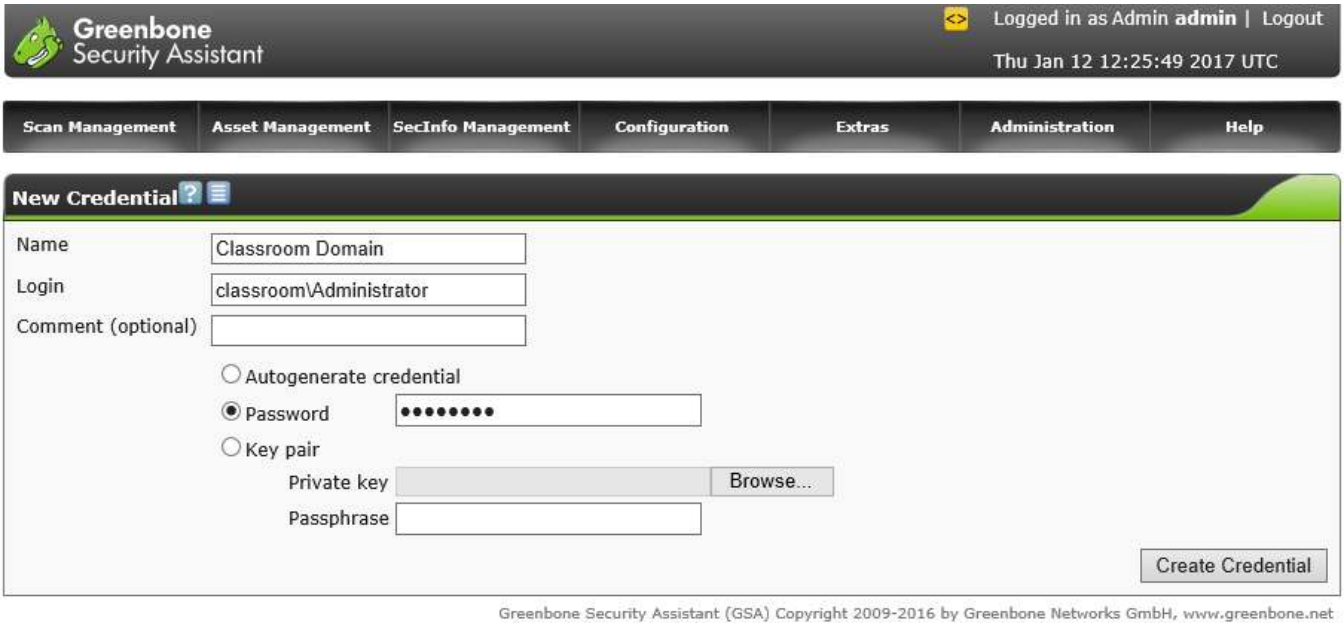
Upravljanje ranjivostima je kamen temeljac modernih praksi kibernetičke sigurnosti usmjerenih na identificiranje, klasificiranje, saniranje i ublažavanje ranjivosti unutar sustava ili mreže. Jedan ključni aspekt je automatizirana procjena ranjivosti korištenjem alata kao što su Nessus, OpenVAS ili Qualys za sistematično skeniranje sustava i mreža za poznate ranjivosti.

alati postoje za dublje analiziranje načina na koji su aplikacije dizajnirane za rad i mogu locirati ranjivosti koje se tipično ne identificiraju pomoću generaliziranih pristupa skeniranju. Mrežni skener ranjivosti — Mrežni skener ranjivosti je alat koji skenira mrežne uređaje i hostove za poznate ranjivosti, pogrešne konfiguracije i slabosti.

Skeneri ovise o bazi podataka poznatih softverskih i konfiguracijskih ranjivosti. Alat kompajlira izvješće o svakoj ranjivosti u svojoj bazi podataka koja je pronađena na svakom hostu. Svaka identificirana ranjivost dobiva ocjenu kritičnosti koja se koristi za prioritizaciju mjera sanacije.

Skenirani bez vjerodajnica i s vjerodajnicama

Sken bez vjerodajnica je onaj koji napreduje usmjeravanjem testnih paketa prema hostu bez prijave u OS ili aplikaciju. Pogled je onaj koji host izlaže nepovlaštenom korisnika ili anonimnom klisnetu na Internetu. Sken s vjerodajnicama je onaj gdje je skener osiguran s vjerodajnicama korisničkog računa, dopuštajući mnogo detaljniji pregled stanja hosta.



Skeneri aplikacija i web aplikacija

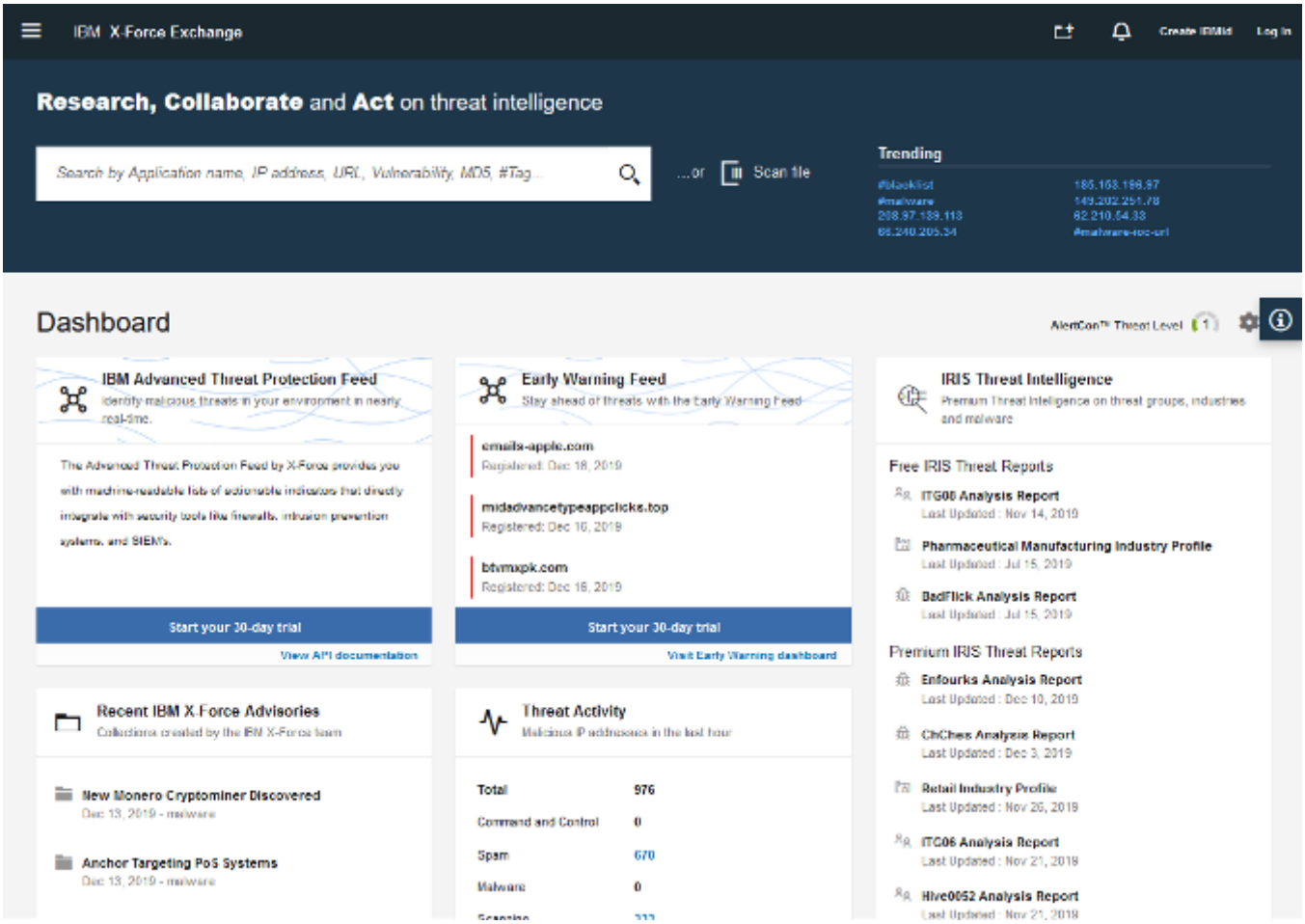
Slično tome, skeniranje ranjivosti aplikacija opisuje specijaliziranu metodu skeniranja ranjivosti za identificiranje slabosti softverskih aplikacija. Ovo uključuje statičku analizu koda, dinamičko testiranje i analizu interaktivne aplikacijske sigurnosti.

imaju vlastite cikluse izdavanja i ažuriranja, odvojene od ostatka okruženja, zahtijevajući ciljani proces upravljanja ranjivostima. Praćenje paketa — Još jedna važna mogućnost u skeniranju ranjivosti aplikacija je praćenje paketa i ovisnosti. Ovo uključuje praćenje verzija svih softverskih komponenti korištenih u aplikaciji i praćenje poznatih ranjivosti u tim komponentama.

Prijenosnici prijetnji

Još jedan važan element upravljanja ranjivostima je upotreba prijenosnika prijetnji (threat feeds). To su izvori informacija u stvarnom vremenu koji se neprestano ažuriraju o potencijalnim prijetnjama i ranjivostima, koji se često prikupljaju iz različitih izvora uključujući vladine agencije, sigurnosne istraživačke organizacije i privatne tvrtke.

mogu biti integrirani u sigurnosnu infrastrukturu organizacije, pridonoseći proaktivnoj strategiji kibernetičke sigurnosti. Izbor između prijenosnika prijetnji otvorenog koda i vlasničkih često se svodi na nekoliko važnih atributa: pokrivenost, točnost, pravovremenost i troškovi.



Rezultati primarnog istraživanja koji se poduzimaju od strane pružatelja podatkovnih prijenosnika prijetnji i akademika mogu imati tri glavna oblika:

- Istraživanje bihevioralnih prijetnji — je narativni komentar koji opisuje primjere napada i taktike, tehnike i procedure (TTP) prikupljene kroz primarne istraživačke izvore.
- Reputacijska obavještajna prijetnja — su popisi IP adresa i domena vezanih uz zlonamjerno ponašanje, plus potpisi poznatog malwarea temeljenog na datotekama.
- Podaci prijetnji — su računalni podaci koji mogu korelirati događaje promatrane na mrežama i zapisnicima kupaca s poznatim TTP-ovima i pokazateljima aktera prijetnji. Podaci prijetnji mogu biti pakirani kao prijenosnici koji se integriraju s platformom SIEM.

(CTI) podaci. Podaci sami po sebi nisu potpuno sigurnosno rješenje. Za proizvodnju djelotvornih obavještajnih podataka, podaci prijetnji moraju biti korelirani s promatranim podacima iz klijentskih mreža. Ova vrsta analize često je pokretana AI platformama. Primjeri komercijalnih prijenosnika prijetnji:

- IBM X-Force Exchange (exchange.xforce.ibmcloud.com)
- Mandiant's FireEye (mandiant.com/advantage/threat-intelligence)
- Recorded Future (recordedfuture.com/platform/threat-intelligence)

Organizacije za dijeljenje informacija

Organizacije za dijeljenje informacija o prijetnjama su suradničke grupe koje razmjenjuju podatke o novim kibernetičkim prijetnjama i ranjivostima. Ove organizacije prikupljaju, analiziraju i distribuiraju informacije vezane uz prijetnje, pomažući organizacijama da

ostanu informirane o najnovijim prijetnjama.

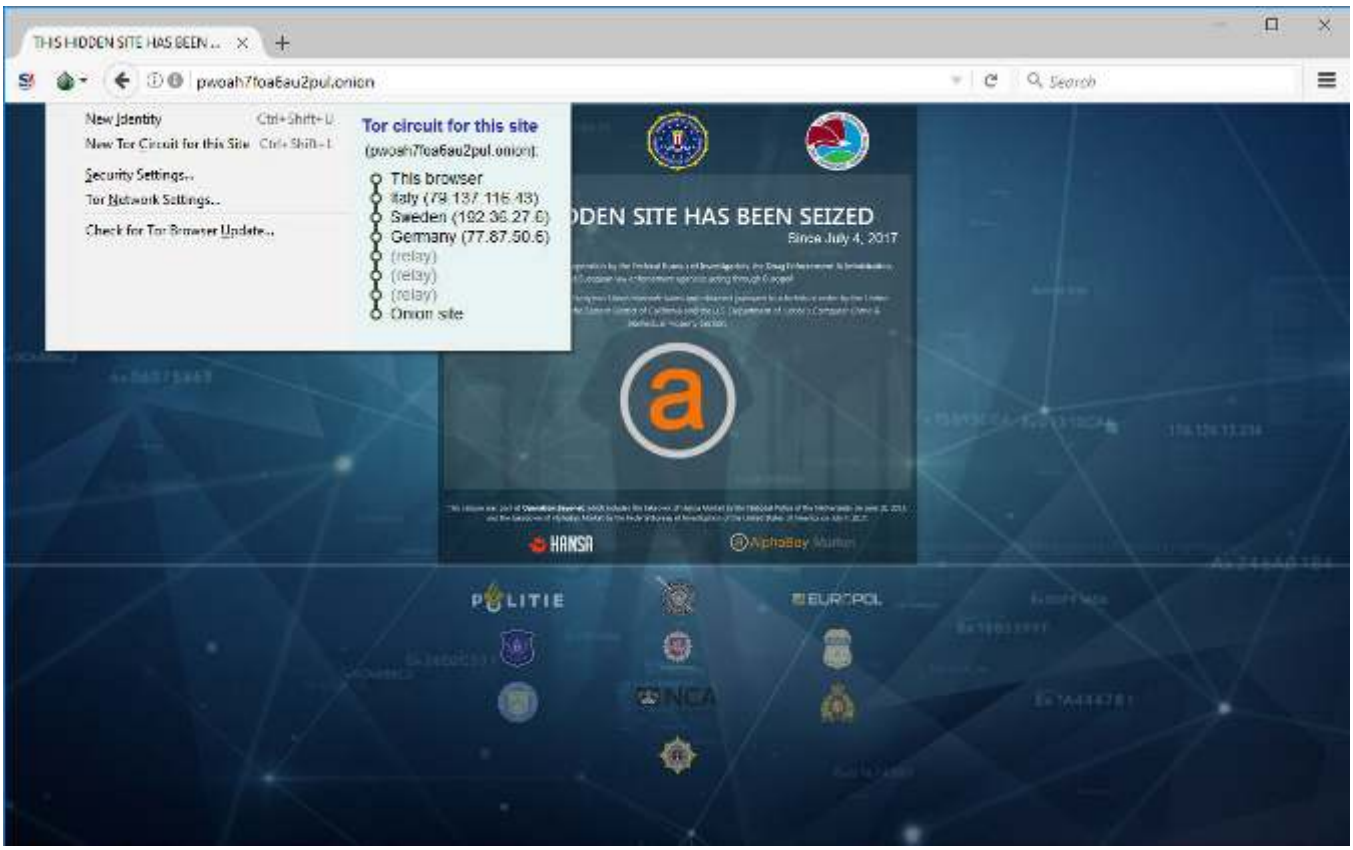
OSINT može pružiti vrijedan kontekst za procjenu razina rizika vezanih uz specifičnu ranjivost. Na primjer, novotkrivene ranjivosti koje se aktivno iskorištavaju ili raspravlja na hakerskim forumima.

Duboki i mračni web

Istraživanje prijetnji je napor kontraobavještajnog prikupljanja u kojemu sigurnosne tvrtke i istraživači pokušavaju otkriti taktike, tehnike i procedure (TTP) modernih kibernetičkih protivnika.

kibernetičkih protivnika. Postoji mnogo tvrtki i akademskih institucija angažiranih u primarnom istraživanju kibernetičke sigurnosti. Pružatelji sigurnosnih rješenja s vatrozidima i platformama za antimalware izvode puno podataka iz vlastitih baza korisnika.

- Mračna mreža (Dark Net) — je mreža uspostavljena kao prekrivač Internet infrastrukture softverom poput The Onion Routera (TOR), Freeneta ili I2P, koji djeluje za anonimiziranje upotrebe i sprječavanje treće strane da zna o postojanju mreže.
- Mračni web (Dark Web) — su stranice, sadržaj i usluge dostupne samo putem mračne mreže. Dok postoje tražilice mračnog weba, mnoge su stranice skrivene od njih. Pristup web stranici mračnog weba putem njezinog URL-a često je dostupan samo putem usmene predaje.



Istraživanje ovih web stranica i oglasnih ploča mračnog weba vrijedan je izvor kontraobavještajnih podataka. Anonimnost usluga mračnog weba olakšala je istražiteljima infiltraciju u forume i web-trgovine gdje napadači kupuju i prodaju eksploate i ukradene podatke.

Napominjemo da je sudjelovanje u nezakonitim aktivnostima na mračnom webu strogo zabranjeno. Radi sigurnosti, važno je biti oprezan i slijediti zakonske i etičke smjernice pri istraživanju mračnog weba. Mračni web ima neke legitimne svrhe:

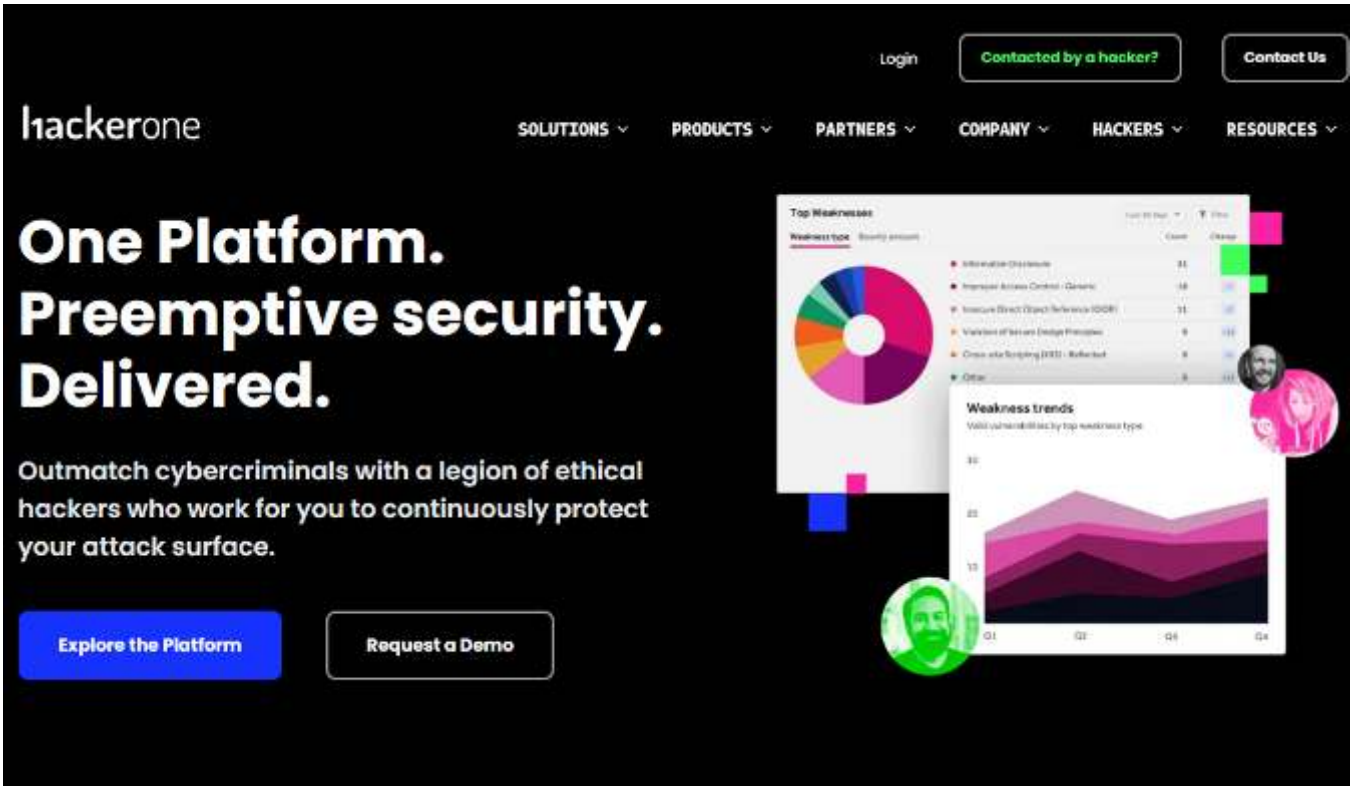
- Privatnost i anonimnost — Mračni web pruža platformu za poboljšanu privatnost i anonimnost. Dopušta korisnicima komunikaciju i pregledavanje Interneta bez otkrivanja svog identiteta ili lokacije, što može biti vrijedno za zviždače, novinare, aktiviste ili pojedince koji žive pod represivnim vladama.
- Pristup cenzuriranim informacijama — U zemljama sa strogom Internet cenzurom, mračni web može biti put za pristup informacijama koje su inače blokirane ili ograničene.
- Istraživanje i dijeljenje informacija — Neki akademski istraživači ili stručnjaci za kibernetičku sigurnost mogu istraživati mračni web radi stjecanja uvida u kriminalne aktivnosti i analize novih prijetnji.

Ostale metode procjene ranjivosti

Testiranje penetracije — Testiranje penetracije, ili pen testing, agresivniji je pristup upravljanju ranjivostima. Etički hakeri pokušavaju probiti sigurnost organizacije na isti način kao pravi napadač.

- Testiranje u nepoznatom okruženju (crna kutija) — je kada konzultant/napadač nema privilegiranih informacija o mreži i njezinim sigurnosnim sustavima. Ovaj tip testa zahtijeva opsežnu fazu izviđanja.
- Testiranje u poznatom okruženju (bijela kutija) — je kada konzultant/napadač ima potpuni pristup informacijama o mreži. Ovi testovi su korisni za simuliranje ponašanja privilegirane interne prijetnje.
- Testiranje u djelomično poznatom okruženju (siva kutija) — je kada konzultant/napadač ima neke informacije. Ovaj tip testa zahtijeva djelomično izviđanje. Nagrade za pronalaženje grešaka (Bug Bounties) — Programi bug bounty opisuju kada organizacije nagrađuju vanjske istraživače sigurnosti za otkrivanje ranjivosti u njihovim sustavima.

istraživači ili 'bijeli hat' hakeri. I testiranje penetracije i programi bug bounty su proaktivne prakse kibernetičke sigurnosti za identifikaciju i ublažavanje ranjivosti u sustavu ili aplikaciji. Oboje uključuju iskorištavanje ranjivosti u kontroliranom okruženju, ali s različitim opsegom, strukturom i nagradama.



Programi odgovornog otkrivanja (responsible disclosure) uspostavljeni su od strane organizacija kako bi potaknuli pojedince da prijave sigurnosne ranjivosti u softveru ili sustavima, dopuštajući organizaciji da adresira i popravi ove ranjivosti prije nego što postanu javno poznate.

i kibernetičke sigurnosti. Sigurnosne revizije procjenjuju sigurnosne kontrole, politike i procedure organizacije, često koristeći standarde poput ISO 27001 ili NIST Okvira kibernetičke sigurnosti kao mjerila. Ove revizije mogu identificirati nedostatke u konfiguraciji sigurnosnih kontrola i pomoći organizacijama u usklađivanju s industrijskim standardima i propisima.

Lekcija 8D

Analiza i sanacija ranjivosti

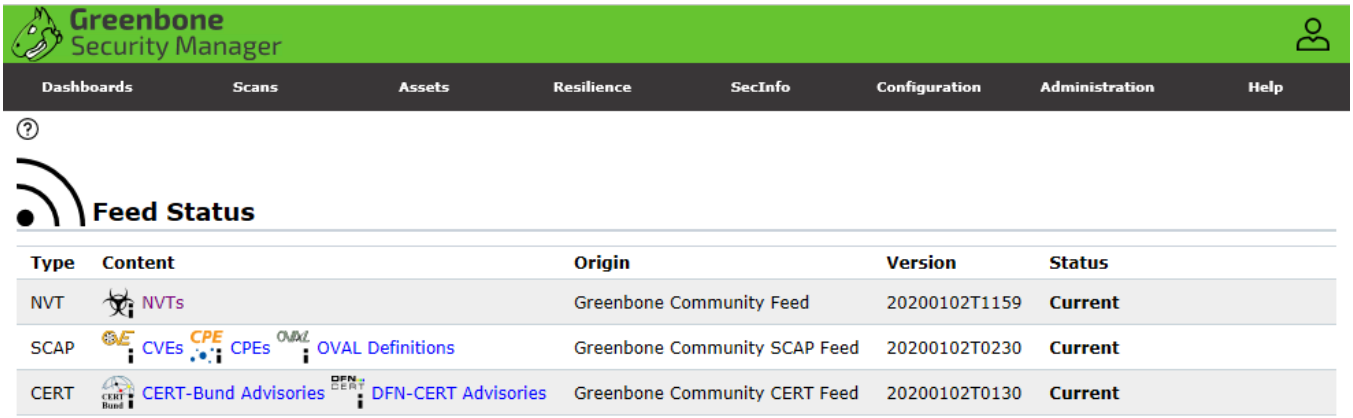
Pregled lekcije

Analiza i sanacija ranjivosti su kritične faze upravljanja ranjivostima. Analiza ranjivosti uključuje procjenu ranjivosti za njihov potencijalni utjecaj i iskoristivost. Ovaj proces može uzeti u obzir faktore poput kritičnosti sustava, osjetljivosti podataka i potencijalnog finansijskog utjecaja.

Uobičajene ranjivosti i izloženosti

Automatizirani skener mora biti ažuriran s informacijama o poznatim ranjivostima. Ove informacije se često opisuju kao prijenosnik ranjivosti. Sustav Common Vulnerabilities and Exposures (CVE) pruža standardizirani identifikator za svaku poznatu ranjivost i izloženost.

Provjera statusa prijenosnika u Greenbone Community Edition upravitelju ranjivosti.



Nacionalna baza podataka ranjivosti (NVD) je repozitorij koji održava Nacionalni institut za standarde i tehnologiju (NIST) koji pruža detaljne informacije o poznatim softverskim ranjivostima, uključujući podatke o ranjivostima iz CVE sustava. Svaki CVE unos sadrži:

- Identifikator u formatu: CVE-GGGG-####, gdje je GGGG godina u kojoj je ranjivost otkrivena, a #### je najmanje četiri znamenke koje označavaju redoslijed u kojemu je

ranjivost otkrivena.

- Kratki opis ranjivosti.
- Referentni popis URL-ova koji pružaju više informacija o ranjivosti.
- Datum kada je unos ranjivosti kreiran.

CVE rječnik pruža glavni doprinos NIST-ovoj Nacionalnoj bazi podataka ranjivosti (nvd.nist.gov). NVD dopunjuje CVE opise s dodatnom analizom, metricom kritičnosti izračunatom koristeći Common Vulnerability Scoring System (CVSS) i popise poznatih softverskih konfiguracija pogođenih ranjivošću.

Lažni pozitivi, lažni negativi i pregled zapisnika

Nakon završetka skeniranja ranjivosti, alat generira sažeto izvješće svih otkrića. Izvješće kodira ranjivosti bojama prema njihovoj kritičnosti, s crvenim za kritične i narančastim za visoke ranjivosti. Svaka pronađena ranjivost treba biti pregledana i prioritizirana za sanaciju.

Information | Results (135 of 1148) | Hosts (1 of 254) | Ports (17 of 30) | Applications (19 of 44) | Operating Systems (1 of 6) | CVEs (48 of 48) | Closed CVEs (56 of 56) | TLS Certificates (3 of 5) | Error Messages (2 of 2) | User Tags (0)

1 - 10 of 135

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Microsoft Windows Multiple Vulnerabilities (KB4457131)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 9:58 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4467691)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:20 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4471321)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:40 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4512517)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:27 PM UTC
Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities	9.3 (High)	97 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:19 PM UTC
Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities	9.3 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:09 PM UTC

Aktivno ili intruzivno skeniranje generalno je vještije u otkrivanju šire palete ranjivosti u host sustavima i može značajno smanjiti lažne pozitive. Lažni pozitiv odnosi se na slučaj gdje skener ili drugi sigurnosni alat pogrešno identificira bezopasnu aktivnost ili entitet kao zlonamjeran ili ranjiv.

naknadni kvar nekoliko drugih povezanih procesa. U ovom slučaju, korišten je relevantan izvor podataka za potvrdu valjanosti upozorenja ranjivosti.

Analiza ranjivosti

Analiza ranjivosti kritična je za podršku nekoliko ključnih aspekata strategije kibernetičke sigurnosti organizacije, uključujući prioritizaciju, klasifikaciju ranjivosti, razmatranja izloženosti i razmatranja okoline. Analiza ranjivosti uključuje procjenu ozbiljnosti svake

ranjivosti koristeći metrike poput CVSS-a, razmatranje potencijalnog utjecaja na organizaciju i kontekst prijetnji.

može utjecati i na analizu ranjivosti. Određene operativne prakse povećavaju izloženost specifičnim ranjivostima ili utječu na potencijalni utjecaj uspješnog iskorištavanja. Primjeri uključuju loše prakse upravljanja zakrpama, nedostatke u kontrolama pristupa i neadekvatne prakse fizičke sigurnosti.

Odgovor na ranjivosti i sanacija

Prakse odgovora i sanacije ranjivosti obuhvaćaju razne strategije i taktike, uključujući zakrpanje, osiguranje, segmentaciju, kompenzacijske kontrole, iznimke i izuzeća:

- Zakrpanje (Patching) je jedna od najizravnijih i najučinkovitijih praksi sanacije. Uključuje primjenu ažuriranja i zakrpa na softver ili sustave za ispravljanje poznatih ranjivosti.
- Kibernetičko osiguranje može pružiti financijsku zaštitu u slučaju sigurnosnog proboja koji rezultira iz ranjivosti. Dok osiguranje izravno ne ublažava ranjivosti, važno je u sveobuhvatnoj strategiji upravljanja rizicima.
- Segmentacija uključuje dijeljenje mreže na zasebne segmente radi sadržavanja potencijalnih sigurnosnih proboja. Ako napadač iskoristi ranjivost i dobije pristup jednom segmentu, ograničen je na taj segment.
- Kompenzacijske kontrole odnose se na mjere postavljene za ublažavanje rizika ranjivosti kada sigurnosni timovi ne mogu izravno eliminirati ranjivost ili kada izravna sanacija nije odmah moguća.
- Iznimke i izuzeća opisuju scenarije gdje specifične ranjivosti ne mogu biti sanirane zbog poslovne kritičnosti, tehničkih ograničenja ili troškovnih ograničenja. U tim slučajevima, viši rukovodstveni timovi prihvaćaju rizik i dokumentiraju obrazloženje.

nepotpuna ili neispravna implementacija ispravaka. Ovi problemi prolaze nezamijećeno bez validacije, izlažući organizaciju istoj ranjivosti koju je prvobitno nastojala adresirati. Validacija pomaže potvrditi da se mjere sanacije implementiraju ispravno.

- Ponovni pregled (Re-scanning) uključuje izvođenje dodatnih skenova ranjivosti nakon implementacije mjera sanacije. Ponovni pregled ima za cilj odrediti jesu li ranjivosti identificirane u inicijalnom pregledu riješene.
- Revizija (Auditing) uključuje temeljiti pregled procesa sanacije pregledavanjem koraka poduzetih za adresiranje ranjivosti i osiguravanjem da su usklađeni s politikama i najboljim praksama organizacije.
- Verifikacija je proces potvrđivanja rezultata mjera sanacije i uključuje razne metode, uključujući ručne provjere, automatsko testiranje ili pregled sistemskih zapisnika ili drugih zapisa.

Sažetak

Trebate biti u mogućnosti sažeti vrste sigurnosnih procjena, poput lovljenja ranjivosti, prijetnji i testiranja penetracije. Trebate i moći objasniti opće procedure za provođenje ovih procjena.

Smjernice za provođenje procjena ranjivosti

Slijedite ove smjernice kada razmatrate upotrebu sigurnosnih procjena:

- Identificirajte procedure i alate koji su potrebni za skeniranje ranjivosti. To može značiti provisioniranje pasivnih mrežnih skenera, aktivnih udaljenih ili mrežnih skenera temeljenih na agentima i skenera aplikacija ili web aplikacija.
- Razvijte plan konfiguracije i održavanja za osiguravanje ažuriranja prijenosnika ranjivosti i prijetnji.
- Redovito pokretajte preglede i pregledavajte rezultate za identificiranje lažnih pozitiva i lažnih negativa, koristeći pregled zapisnika i dodatne CVE informacije za validaciju rezultata prema potrebi.
- Zakazujte preglede konfiguracije i planove sanacije, koristeći kritičnost ranjivosti CVSS za prioritizaciju akcija.
- Razmotrite implementaciju platformi analize prijetnji, praćenje savjeta i biltena za nove izvore prijetnji.
- Razmotrite implementaciju vježbi testiranja penetracije, osiguravajući da su postavljene s jasnim opsegom projekta.

Modul 9

Procijeni mrežne sigurnosne sposobnosti

Pregled modula

Sigurne osnove (secure baselines), učvršćivanje (hardening), bežična sigurnost i kontrola mrežnog pristupa temeljni su koncepti kibernetičke sigurnosti. Sigurne osnove uspostavljaju skup standardiziranih sigurnosnih konfiguracija za različite vrste IT imovine, dok tehike učvršćivanja smanjuju površinu napada minimiziranjem nepotrebnih usluga i povećanjem sigurnosnih kontrola.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Opisati važnost sigurnih osnova.
- Istražiti koncepte učvršćivanja uređaja.
- Sažeti razmatranja dizajna bežičnih mreža.
- Objasniti postavke bežične sigurnosti.
- Razumjeti mogućnosti kontrole mrežnog pristupa (NAC).

Lekcija 9A

Osnove mrežne sigurnosti

Pregled lekcije

Osnove mrežne sigurnosti opisuju skup minimalnih sigurnosnih kontrola i konfiguracija za mrežu. Osnove tipično pokrivaju područja poput konfiguracija vatrozida, sigurnosnih postavki usmjerivača i preklopnika i protokola autentikacije. Pridržavanje sigurnih osnova ključno je za upravljanje ranjivostima i smanjenje površine napada.

usklađenosti, alati usklađeni s SCAP-om (Security Content Automation Protocol), poput OpenSCAP-a, mogu procijeniti i verificirati pridržavanje sustava osnovi. Nadalje, CIS pruža alat CIS-CAT Pro za automatiziranu procjenu konfiguracije sustava prema CIS benchmarkovima. Preporuke za učvršćivanje mrežnih uređaja:

- Promijenite zadane vjerodajnice koje su dobro dokumentirane i predstavljaju značajan sigurnosni rizik.
- Onemogućite nepotrebne usluge i sučelja na preklopniku ili usmjerivaču. Nisu sve usluge ili sučelja potrebna. Na primjer, usluge poput HTTP-a ili Telneta treba izbjegavati.
- Koristite sigurne protokole upravljanja poput SSH umjesto Telneta ili HTTPS umjesto HTTP-a.
- Implementirajte liste kontrole pristupa (ACL) za ograničavanje pristupa usmjerivaču ili preklopniku samo na potrebne uređaje i mreže.
- Omogućite bilježenje i nadzor za identificiranje problema poput ponovljenih neuspjela prijava i promjena konfiguracije.
- Konfiguriranje sigurnosti portova pomaže ograničiti uređaje koji se mogu spojiti na port preklopnika radi sprječavanja neovlaštenog pristupa.
- Snažne politike lozinki pomažu smanjiti rizik od napada lozinki.
- Fizički osigurajte opremu pohranjivanjem uređaja u zaključanoj prostoriji radi sprječavanja neovlaštenog fizičkog pristupa. Hardver i operativni sustavi poslužitelja:

- Promijenite zadane vjerodajnice za sprječavanje neovlaštenog pristupa, slično mrežnim uređajima.
- Onemogućite nepotrebne usluge za smanjenje površine napada poslužitelja. Svaka usluga koja se pokreće na poslužitelju predstavlja potencijalnu ulaznu točku.
- Redovito primjenjujte softverske sigurnosne zakrpe i ažuriranja za ispravljanje poznatih ranjivosti.
- Načelo najnižih privilegija ograničava svakog korisnika na minimalni iznos privilegija potrebnih za obavljanje funkcije radi smanjenja utjecaja kompromitiranog računa.
- Koristite vatrozide i sustave za otkrivanje upada (IDS) za blokiranje ili upozoravanje na zlonamjernu aktivnost.
- Sigurna konfiguracija poslužitelja trebala bi koristiti konfiguracije osnove poput onih koje pružaju CIS ili STIG-ovi.
- Snažne kontrole pristupa uključuju snažne politike lozinki, višefaktornu autentikaciju (MFA) i upravljanje privilegiranim pristupom (PAM).
- Omogućite bilježenje i nadzor za identificiranje problema poput ponovljenih neuspjelih prijava i promjena konfiguracije, slično prednostima za mrežnu opremu.
- Koristite antivirusna i antimalware rješenja za automatsko otkrivanje i karantenu malwarea.
- Fizička sigurnost ormara za poslužitelje, serverskih soba ili datacentara sprječava neovlašteni pristup.

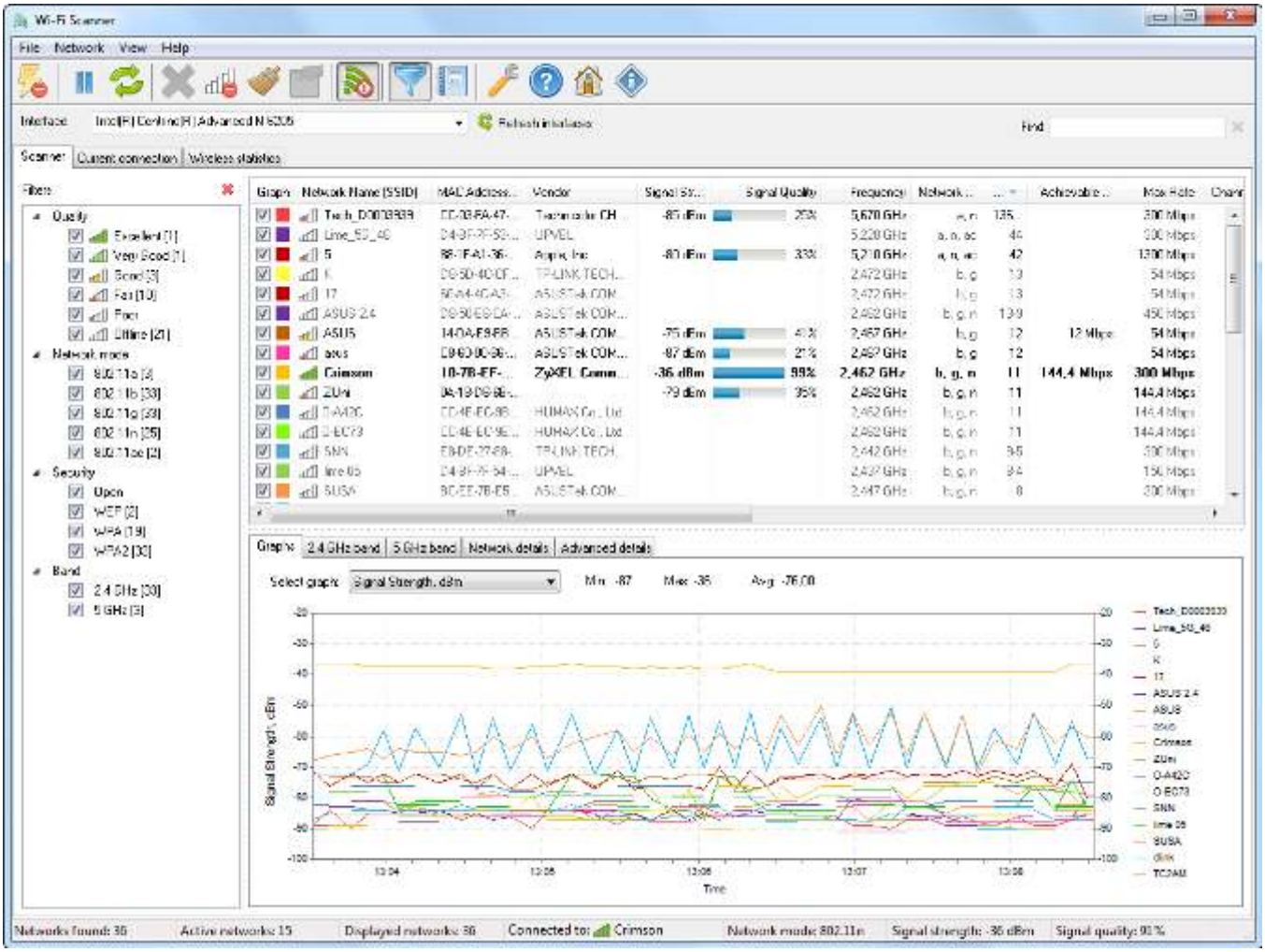
Razmatranja instalacije bežične mreže

Razmatranja instalacije bežične mreže odnose se na faktore koji osiguravaju dobru dostupnost ovlaštenih Wi-Fi pristupnih točaka. Mreža s neravnomjernim pokrivenosti signala ili koja podliježe elektromagnetskim interferencijama oslabljuje dostupnost.

Postavljanje bežičnih pristupnih točaka (WAP)

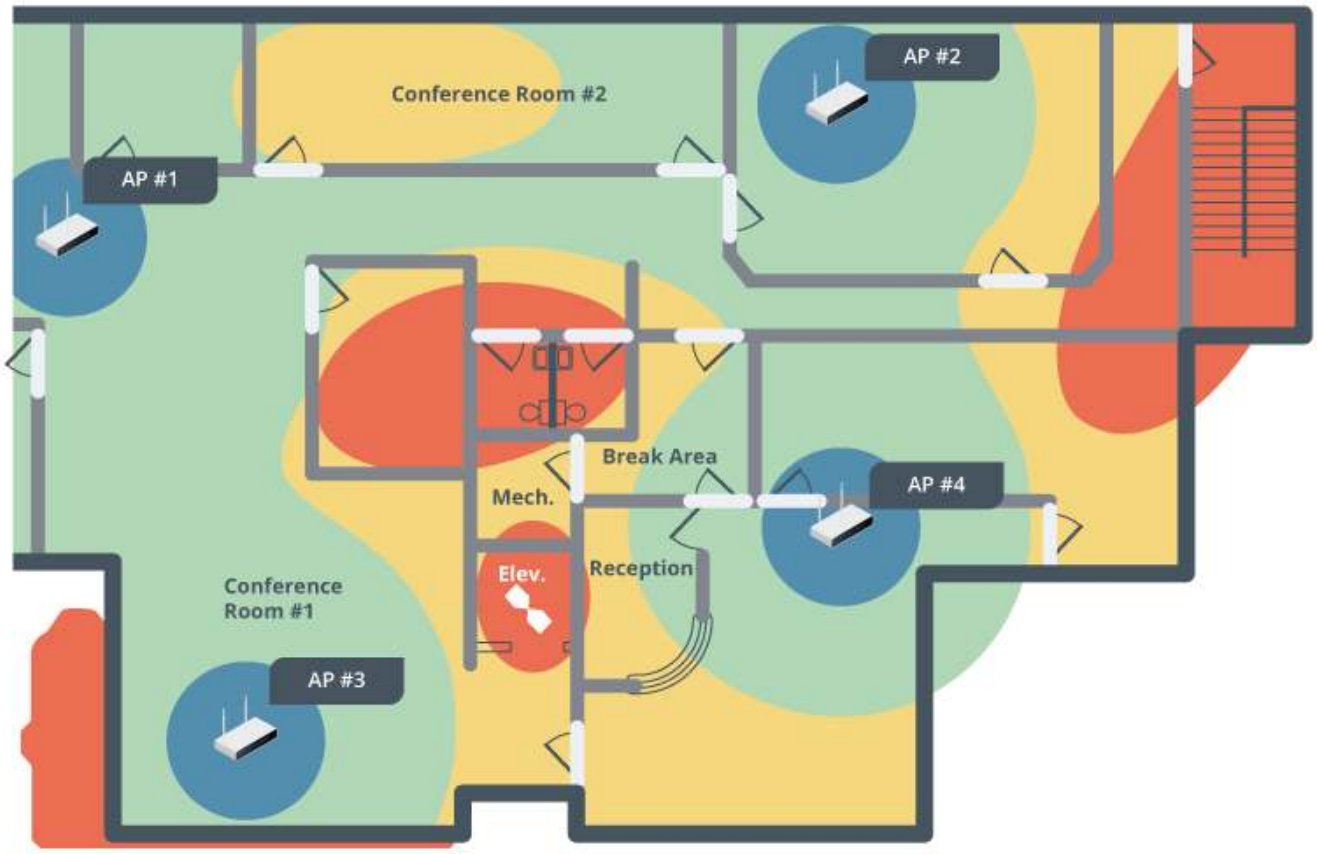
Infrastrukturna bežična mreža sastoji se od jedne ili više bežičnih pristupnih točaka, svake spojene na žičanu mrežu. Pristupne točke prosljeđuju promet između bežičnih klijenata i ostatka mreže.

Primjer izlaza alata za Wi-Fi skeniranje Lizard Systems.



Ova mjerenja se kombiniraju i analiziraju za proizvodnju toplinskih karta (heat map), prikazujući gdje je signal jak (zelena/plava) ili slab (crvena), i koji kanal se koristi i kako se preklapaju. Ovi podaci se zatim koriste za optimiziranje postavljanja pristupnih točaka radi maksimiziranja pokrivenosti i minimiziranja interferencija.

Ilustracija toplinske karte (heat map)

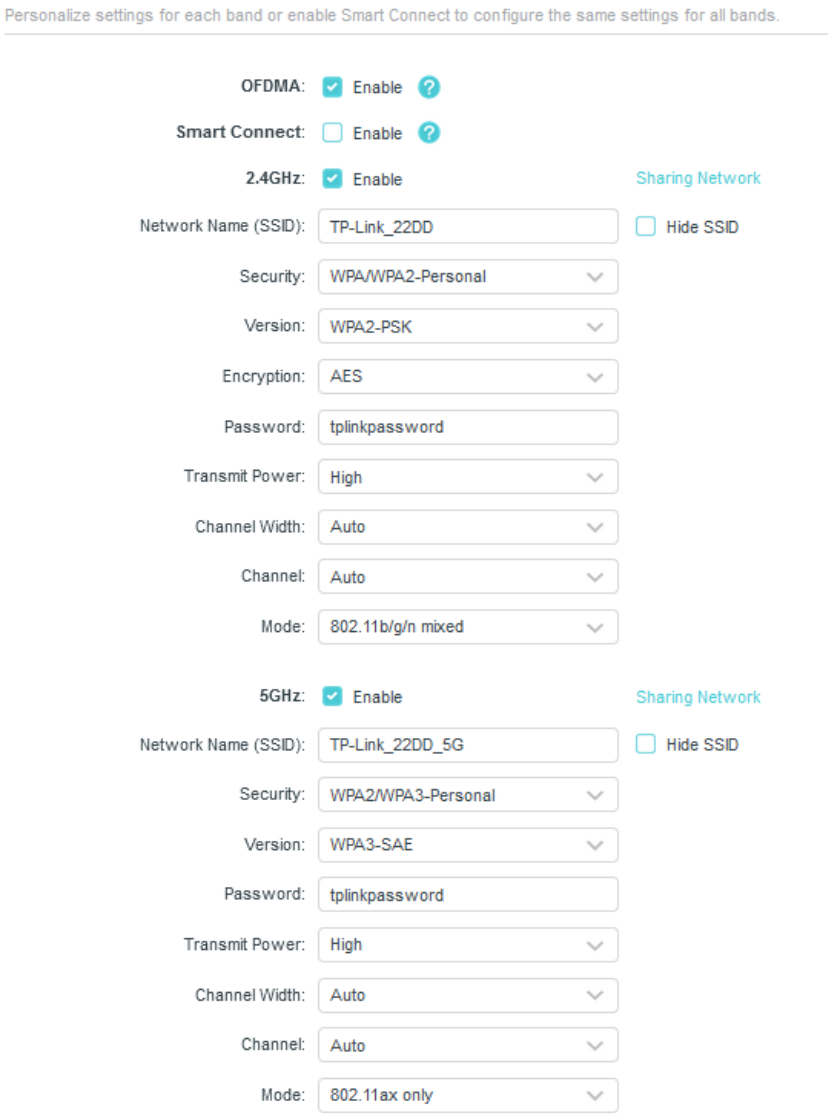


Primjer toplinske karte uredskog prostora s četiri pristupne točke. Boje se koriste za prikaz snage signala iz pristupnih točaka: plava pokazuje jaku snagu signala, zelena pokazuje dobru pokrivenost, žuta pokazuje slabu pokrivenost, a crvena pokazuje nikakvo ili zanemarivo pokriće.

Bežična enkripcija

Pored dizajna lokacije, bežična mreža mora biti konfigurirana sa sigurnosnim postavkama. Bez enkripcije, bilo tko unutar dometa može presresti i pročitati pakete koji prolaze po bežičnoj mreži. WPA3 je trenutna preporuka za bežičnu enkripciju.

sigurnost, dok je 5 GHz mreža za uređaje sposobne za 802.11ax (Wi-Fi 6) koji koriste WPA3-SAE autentikaciju.



Wi-Fi zaštićeno postavljanje (WPS)

Budući da je postavljanje pristupne točke sigurno relativno složeno za stambene potrošače, dobavljači su razvili sustav za automatizaciju procesa nazvan Wi-Fi Protected Setup (WPS). Međutim, WPS ima poznate ranjivosti i treba biti onemogućen ako nije potreban. WPA3 donosi neka poboljšanja nad WPA2:

- Simultana autentikacija jednakih (SAE) — zamjenjuje protokol razmjene unaprijed dijeljenog ključa (PSK) u WPA2, osiguravajući da napadač ne može presresti Wi-Fi lozinku čak i kada bilježi podatke od uspješne prijave.
- Poboljšano otvoreno (Enhanced Open) — šifrira promet između uređaja i pristupne točke, čak i bez lozinke, što povećava privatnost i sigurnost na otvorenim mrežama.
- Ažurirani kriptografski protokoli — zamjenjuje AES CCM s AES Galois Counter Mode (GCM) načinom rada. Galois Counter Mode ima više razine performansi od CCM-a.
- Wi-Fi jednostavno povezivanje (Easy Connect) — dopušta povezivanje uređaja skeniranjem QR koda, smanjujući potrebu za složenim konfiguracijama uz održavanje sigurnih veza.

Wi-Fi performanse ovise i o podršci uređaja za najnovije 802.11 standarde. Najnovija generacija (802.11ax) se reklamira kao Wi-Fi 6. Raniji standardi su retroaktivno nazvani

Wi-Fi 4 (802.11n) i Wi-Fi 5 (802.11ac).

Metode Wi-Fi autentikacije

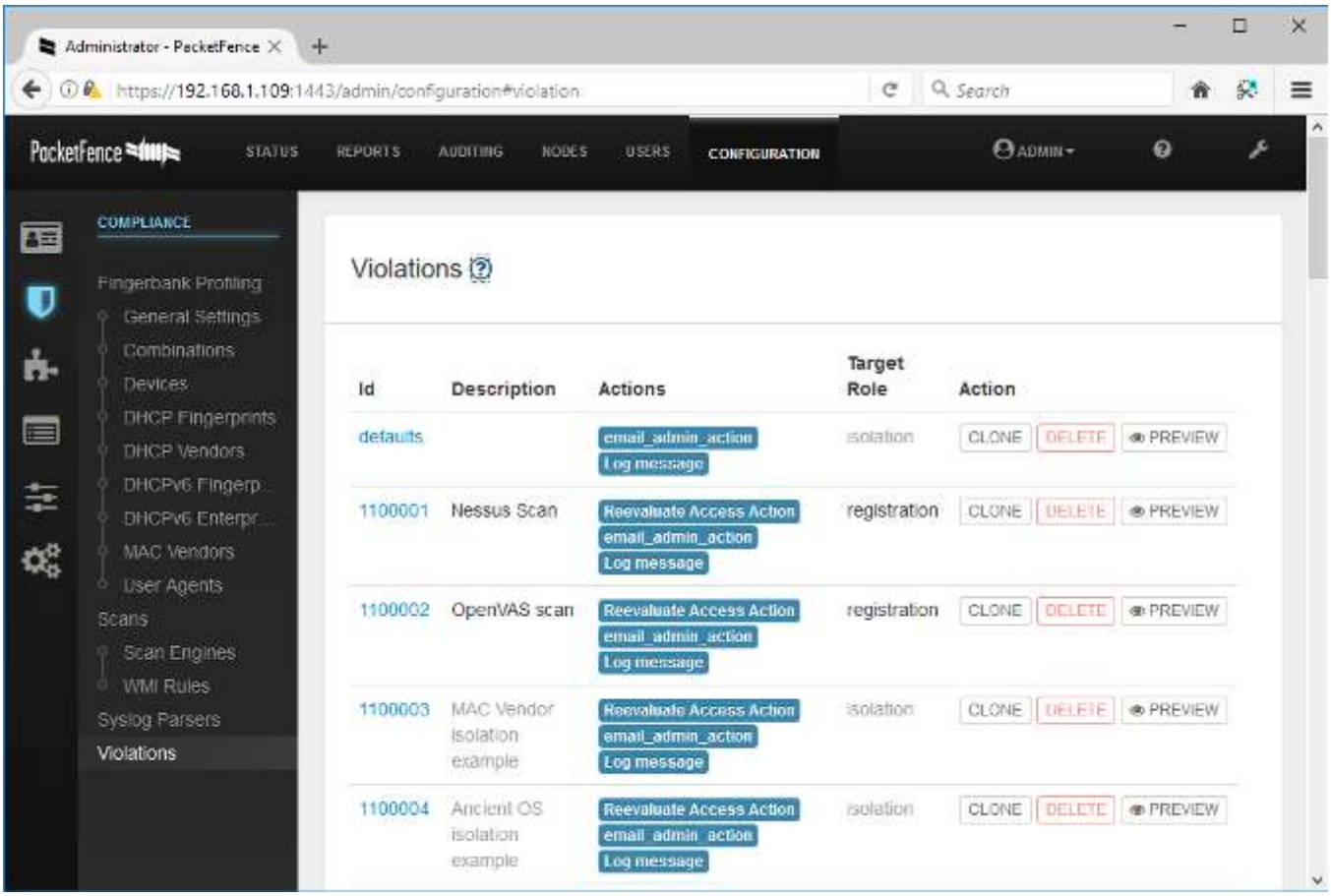
Kako biste osigurali mrežu, morate potvrditi da se samo valjani korisnici spajaju na nju. Wi-Fi autentikacija dolazi u tri vrste: osobna, otvorena i korporativna. Osobna autentikacija koristi unaprijed dijeljeni ključ (PSK) za autentikaciju. Korporativna autentikacija koristi 802.1X i RADIUS za autentikaciju korisnika na korporativnoj mreži.

autentikacija koristeći jedinstvene vjerodajnice dopušta mrežnim administratorima praćenje mrežne upotrebe na granularnoj razini. Protokol podržava i višestruke tipove Extensible Authentication Protocola (EAP), poput EAP-TLS koji koristi digitalne certifikate za autentikaciju klijenta i poslužitelja.

Kontrola mrežnog pristupa (NAC)

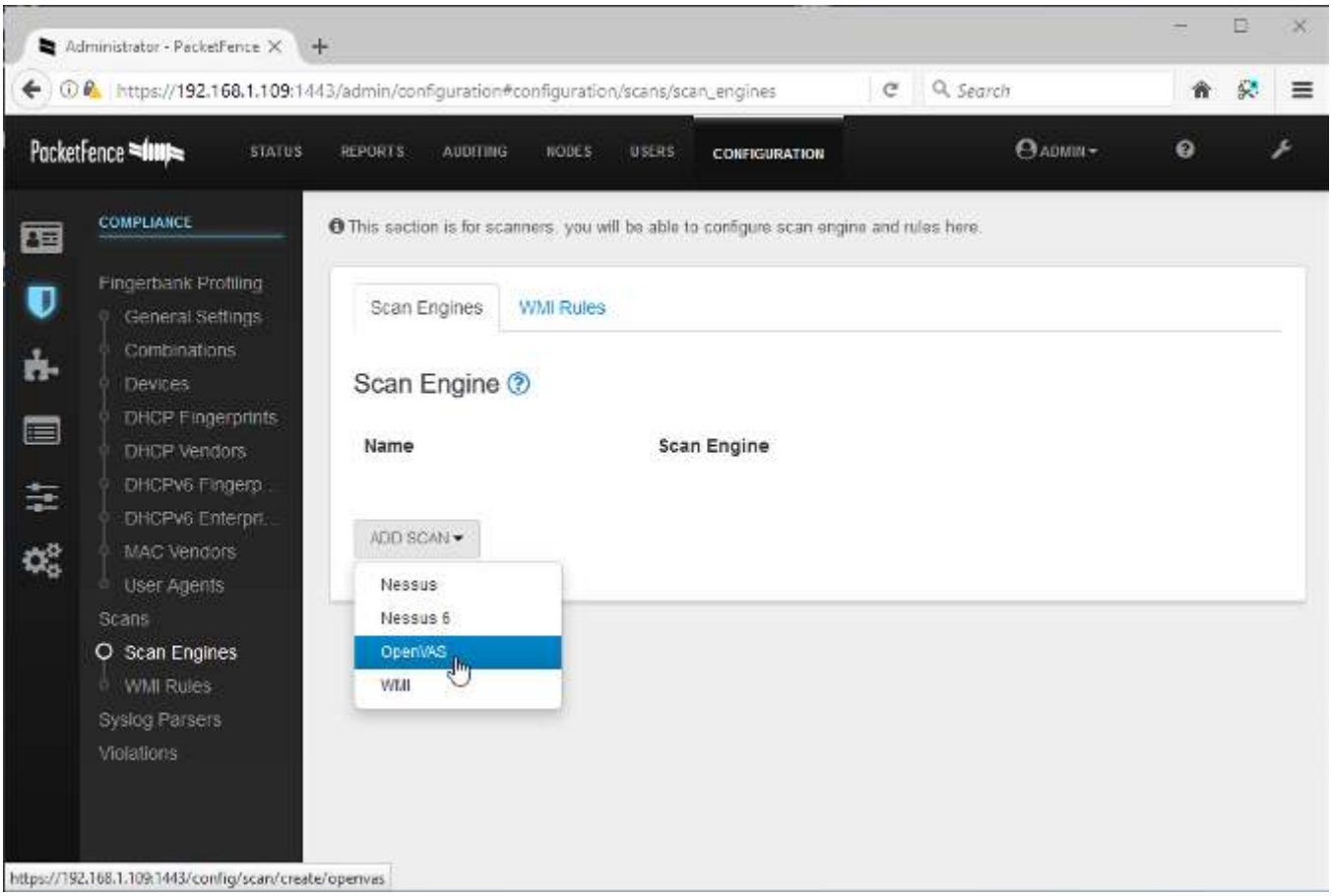
Kontrola mrežnog pristupa (NAC) ne samo da autentificira korisnike i uređaje prije dopuštanja pristupa mreži, već i provjerava i provodi usklađenost s uspostavljenim sigurnosnim politikama.

dodjela VLAN-a. Dinamička dodjela VLAN-a je NAC značajka koja dodjeljuje VLAN uređaju na temelju atributa korisničkog identiteta, vrste uređaja, lokacije uređaja ili rezultata provjere zdravlja. Na primjer, kompromitiranom uređaju može biti dodijeljen karantinski VLAN koji ima ograničeni pristup mreži.



Agent može biti persistentan, u kom slučaju je instaliran kao softverska aplikacija na klijentu, ili nepersistentan. Nepersistentan (ili topivi) agent se učitava u memoriju durante procjene stanja i briše se kada je sesija završena. Stalni agent uvijek nadzire klijentski uređaj dok se uređaj koristi, dok privremeni agent samo provodi provjere kada se uređaj

pokušava spojiti na mrežu.



Lekcija 9B

Poboljšanje mrežnih sigurnosnih sposobnosti

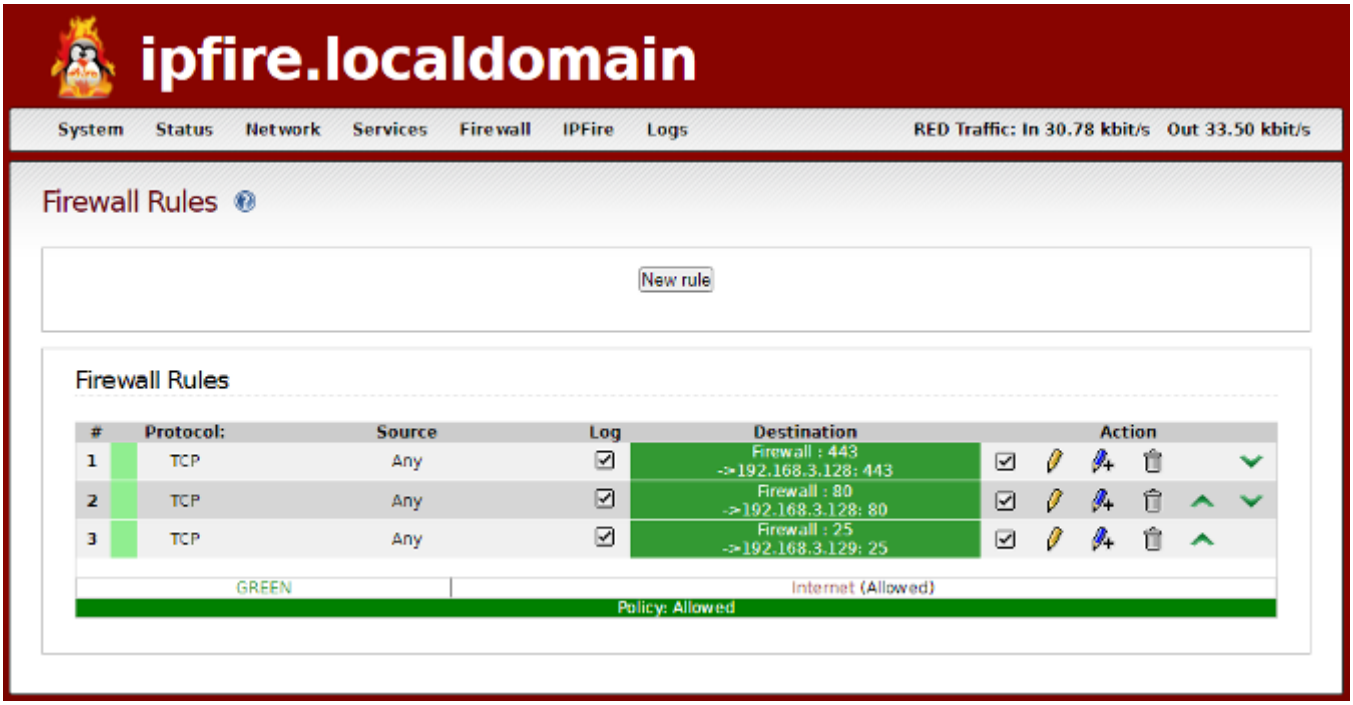
Pregled lekcije

Vatrozidi, sustavi za otkrivanje upada (IDS), sustavi za sprječavanje upada (IPS) i web filteri temeljne su komponente u infrastrukturi kibernetičke sigurnosti dizajniranoj za zaštitu umreženih sustava. Ovi alati rade zajedno za filtriranje i analizu mrežnog prometa, otkrivanje i sprječavanje zlonamjernih aktivnosti.

Liste kontrole pristupa (ACL)

Lista kontrole pristupa (ACL) je popis dozvola vezanih uz mrežni uređaj, poput usmjerivača ili preklopnika, koji kontrolira promet na razini mrežnog sučelja. ACL-ovi tipično definiraju koji promet je dozvoljen ili zabranjen na temelju izvorišne i odredišne IP adrese, protokola i informacija o portu.

Ako vatrozid nema zadano implicitno pravilo odbijanja, eksplicitno pravilo odbijanja svega može se ručno dodati na kraj ACL-a. Primjer pravila vatrozida konfiguriranih na IPFire. Ovaj skup pravila dopušta svaki HTTP i HTTPS promet izlaziti iz interne mreže.



Svako pravilo može specificirati blokirati ili dozvoliti promet na temelju nekoliko parametara, koji se često nazivaju n-torkama (tuples). Ako svako pravilo zamislite kao redak u bazi podataka, n-torke su stupci. Opće preporuke za konfiguriranje vatrozida:

- Blokirajte dolazne zahtjeve s internih ili privatnih IP adresa (koje su očito lažirane).
- Blokirajte dolazne zahtjeve od protokola koji bi trebali funkcionirati samo na razini lokalne mreže, poput ICMP-a, DHCP-a ili protokola usmjeravanja.
- Koristite testiranje penetracije za potvrdu sigurne konfiguracije. Bilježite pokušaje pristupa i nadzirite zapisnike za sumnjive aktivnosti.
- Poduzmite uobičajene korake za osiguravanje hardvera na kojemu radi vatrozid i koristite upravljačko sučelje.

```
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  10.1.0.192          0.0.0.0/0
2    ACCEPT     tcp  --  10.1.0.0/24         0.0.0.0/0           tcp dpt:22
3    ACCEPT     udp  --  0.0.0.0/0           0.0.0.0/0           udp dpt:53
4    ACCEPT     tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:53
5    ACCEPT     tcp  --  10.1.0.0/24         0.0.0.0/0           tcp dpt:80
6    ACCEPT     tcp  --  10.1.0.0/24         0.0.0.0/0           tcp dpt:443
7    ACCEPT     all  --  0.0.0.0/0           0.0.0.0/0           ctstate RELATED,ESTABLISHED
```

Na primjer, pravilo vatrozida može biti specifično dizajnirano za dopuštanje ili odbijanje prometa na temelju TCP ili UDP brojeva portova na kojima usluga radi. Ako web poslužitelj

na mreži treba dozvoliti samo dolazni HTTP i HTTPS promet, vatrozid može biti konfiguriran s odgovarajućim pravilima.

Sustavi za otkrivanje i sprječavanje upada

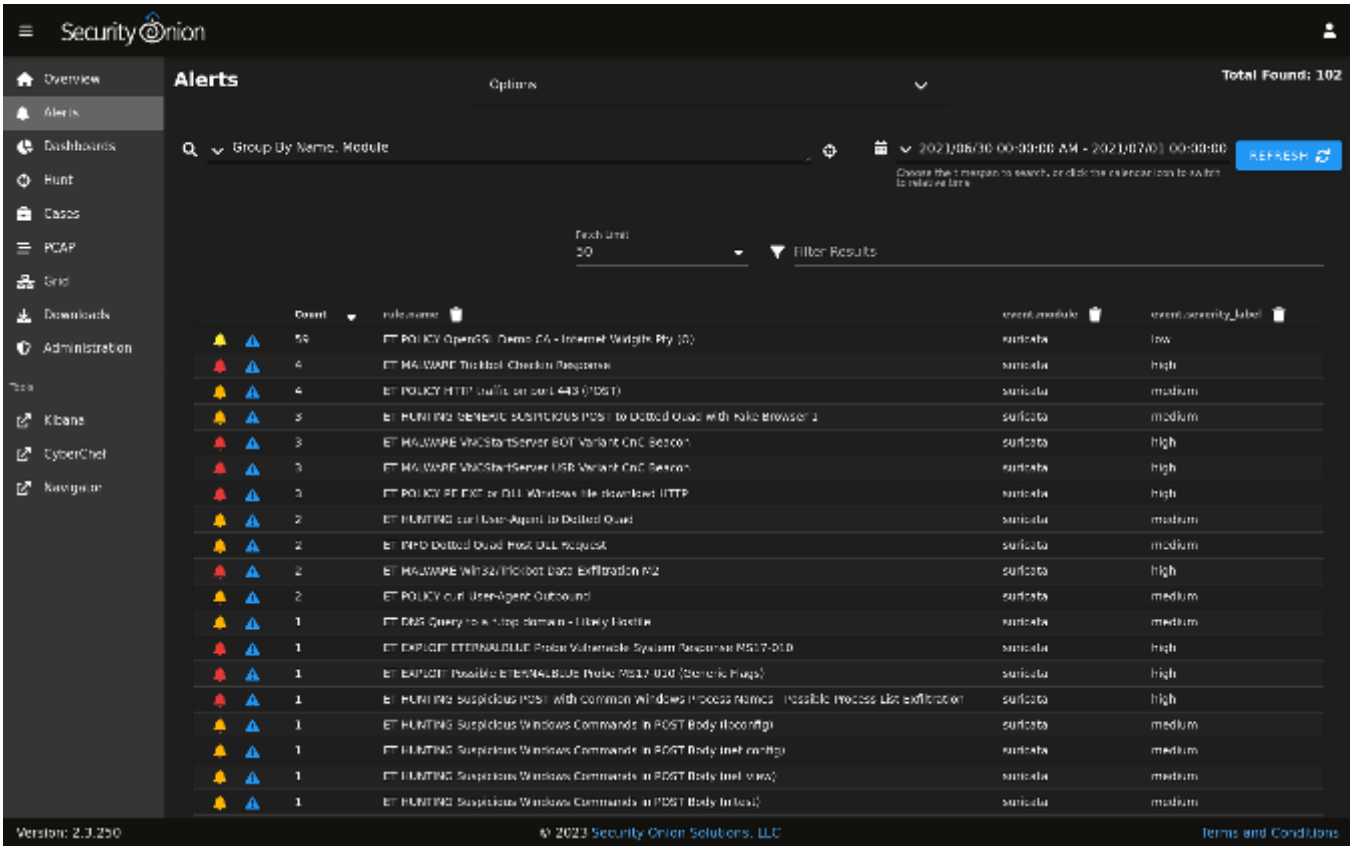
Sustavi za otkrivanje upada (IDS) i sustavi za sprječavanje upada (IPS) igraju kritičnu ulogu u sigurnosnim operacijama. Oba sustava nadziru mrežni promet, zapisnike i aktivnosti sustava za znakove zlonamjernih aktivnosti, ali se razlikuju u načinu odgovora na identificirane prijetnje.

Host-based i mrežni sustavi za otkrivanje upada (IDS) i sustavi za sprječavanje upada (IPS) svaki nude jedinstvene prednosti u osiguravanju mreže, a korištenje obaju u kombinaciji često dovodi do sveobuhvatnijeg sigurnosnog položaja.

Nasuprot tome, sustavi za sprječavanje upada (IPS), poput Suricata, proaktivni su sigurnosni alati koji otkrivaju potencijalne prijetnje i poduzimaju akcije za sprječavanje ili ublažavanje njih. IPS identificira prijetnju i može automatski blokirati, resetirati veze ili poduzeti druge zaštitne akcije.

- Snort je jedan od najpoznatijih IDS/IPS alata. Koristi jezik temeljen na pravilima koji kombinira prednosti metoda inspekcije temeljenih na potpisu, protokolu i anomaliji.
- Suricata je visoko-performansni open source IDS/IPS/NSM motor. Suricata je dizajniran da u potpunosti iskoristi moderni hardver i pruža više performansi i skalabilnost od Snorta.
- Security Onion je Linux distribucija dizajnirana za otkrivanje upada, nadzor mrežne sigurnosti i upravljanje zapisnicima. Uključuje i Snort i Suricata, zajedno s nizom drugih alata.

Upravljački panel Security Onion Alerts prikazuje nekoliko upozorenja zabilježenih koristeći Emerging Threats (ET) skup pravila i Suricata.



Metode otkrivanja IDS-a i IPS-a

U IDS-u, motor analize je komponenta koja skenira i interpretira promet zabilježen senzorom s ciljem identificiranja sumnjivih prometa. Motor analize koristi jednu ili više metoda otkrivanja: detekcija temeljena na potpisu, detekcija temeljena na anomaliji i detekcija temeljena na politici.

Datoteka pravila Snort dobivena od open source prijenosnika zajednice Emerging Threats.

```
  GNU nano 2.5.3                    File: downloaded.rules

# ----- Begin ET-emerging-activex Rules Category ----- #

# -- Begin GID:1 Based Rules -- #

#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Internet Explorer Plugin.ocx Heap Overfl$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 1$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 2$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 3$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX MciWndx ActiveX Control"; flow:from_serv$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object Instantiation Memory Corrupti$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Danim.dll and Dxtmsft.dll COM Objects"; $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX JuniperSetup Control Buffer Overflow"; f$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Wmm2fxa.dll COM Object Instantiation Mem$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft WMIScriptUtils.WMIObjectBroker$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsmIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft DExplore.AppObj.8.0 object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VisualStudio.DTE.8.0 object ca$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Microsoft.DbgClr.DTE.8.0 objec$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsaIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Business Object Factory object$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook Data Object object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook.Application object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Install En$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Install Engine Ins$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Shell.Application $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Shell.Appl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX NCTAudioFile2 ActiveX SetFormatLikeSampl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft Internet Explorer ADO$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Sony ImageStation (SonyISUpload.cab 1.0.$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Citrix Presentation Server Client WFICA.$
                        [ Read 27185 lines (Warning: No write permission) ]
```

Potpisi i pravila (koji se često nazivaju dodacima ili prijenosnicima) koji pokreću otkrivanje upada moraju se redovito ažurirati za pružanje zaštite od najnovijih vrsta prijetnji. Komercijalni softver zahtijeva pretplatu. Open source softver, poput Snorta, podržan je aktivnom zajednicom.

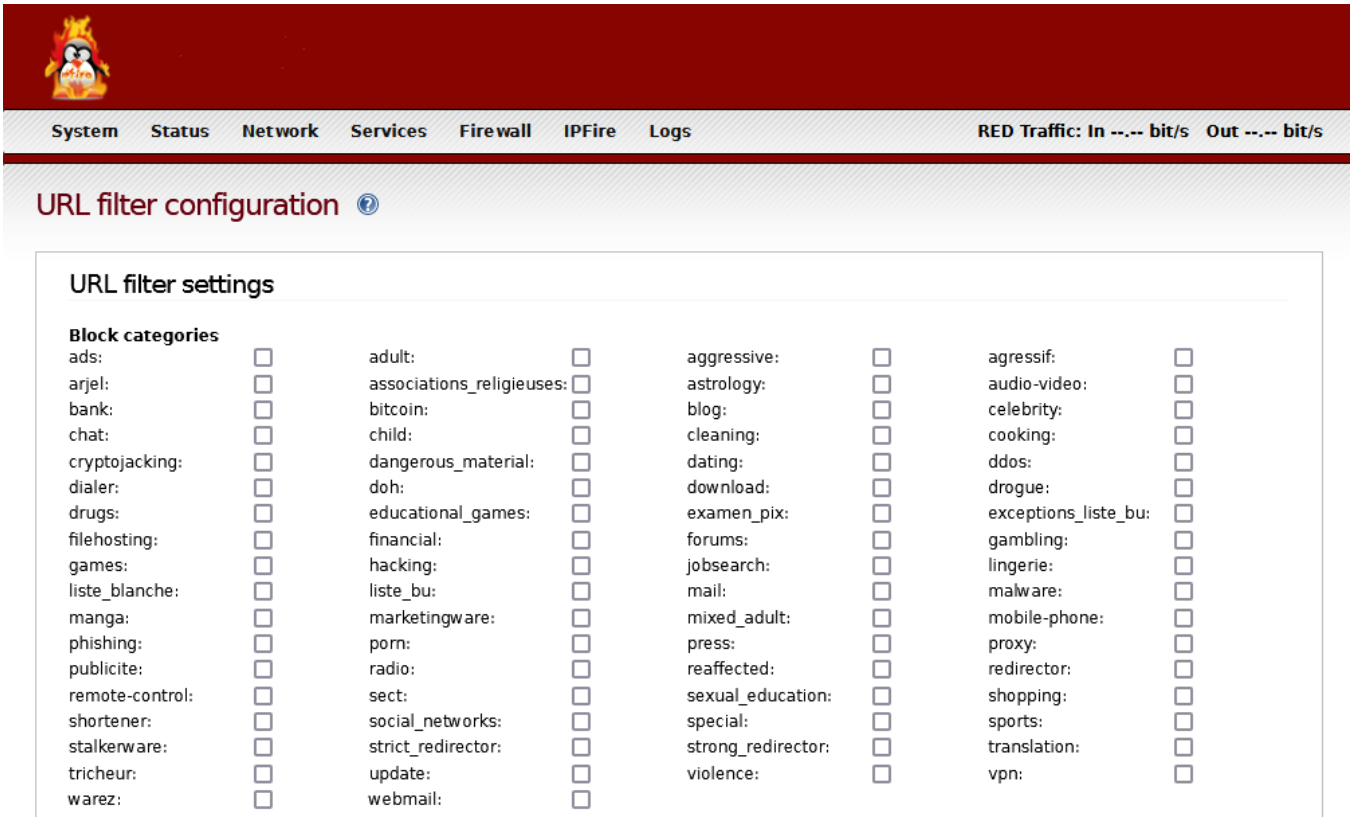
- Analitika ponašanja korisnika i entiteta (UEBA) — su proizvodi koji skeniraju pokazatelje iz višestrukih izvora otkrivanja upada i zapisnika za identificiranje anomalija. Često su integrirani s platformama za upravljanje sigurnosnim informacijama i događajima (SIEM).
- Analiza mrežnog prometa (NTA) — su proizvodi slični IDS-u i NBAD-u u tome što primjenjuju tehnike analize samo na mrežne tokove, a ne na višestruke mrežne i izvore podataka zapisnika.

Ponekad se bihevioralna i anomalijska detekcija uzimaju kao ista stvar (u smislu da motor otkriva anomalično ponašanje). Ovo možda nije uvijek slučaj. Anomalijska detekcija može se više specifično odnositi na statističko modeliranje mrežnog prometa, gdje se uspostavlja osnova normalne aktivnosti i otkrivaju značajna odstupanja.

putem centraliziranog proxy poslužitelja, može učinkovito kontrolirati i nadzirati sav dolazni i odlazni web sadržaj. Primarna uloga proxyja u filtriranju web sadržaja je analizirati web zahtjeve korisnika i odgovarajuće odgovore. Metode filtriranja web

sadržaja:

- Skeniranje URL-ova — gdje proxy poslužitelj ispituje URL-ove koje zahtijevaju korisnici. Može blokirati pristup specifičnim URL-ovima za koje se zna da hostiraju zlonamjerni sadržaj, neprikladni su ili krše politiku korištenja Interneta u tvrtki.
- Kategorizacija sadržaja — klasificira web stranice u razne kategorije, poput društvenih mreža, kockanja, sadržaja za odrasle, web maila i mnogih drugih. Organizacije mogu definirati pravila za dopuštanje ili odbijanje pristupa na temelju ovih kategorija.
- Pravila blokiranja — koriste proxy poslužitelj za implementaciju pravila blokiranja na temelju raznih faktora poput URL-a web stranice, domene, IP adrese, kategorije sadržaja ili specifičnih ključnih riječi.
- Filtriranje na temelju reputacije — koriste proxy poslužitelje za ugradnju filtriranja na temelju reputacije, koje koristi neprestano ažurirane baze podataka koje ocjenjuju web stranice na temelju njihovog promatranog ponašanja i povijest.



Problemi vezani uz filtriranje weba

Filtriranje sadržaja nije bez potencijalnih problema i izazova. Jedan uobičajeni problem je preblokiranje ili potblokiranje. Preblokiranje se pojavljuje kada je filtar previše ograničavajući, blokirajući legitimne i korisne stranice. Potblokiranje se pojavljuje kada filtar propušta neke neprikladne ili štetne stranice.

Sažetak

Poboljšanje mrežnih sigurnosnih sposobnosti bitno je za zaštitu osjetljivih podataka, održavanje integriteta i dostupnosti IT sustava i nadopunjavanje sposobnosti sigurnosnih operacija. Smjernice:

- Odaberite sigurnu osnovu na temelju pažljive analize profila rizika organizacije.

- Automatizirajte primjenu i upravljanje sigurnim osnovama koristeći alate poput Active Directory Group Policy, Ansiblea, Puppeta ili Chefa.
- Kontinuirano revidirajte bežične mreže za osiguravanje pravilne konfiguracije i validaciju pristupnih točaka.
- Implementirajte korporativne metode mrežne autentikacije za obogaćivanje bilježenja, poboljšanje zaštite podataka i pružanje granularne kontrole.
- Provedite zahtjeve mrežne sigurnosti implementacijom NAC 'čuvara pristupa'.
- Koristite vatrozide, IDS/IPS i filtriranje weba za nadzor i kontrolu mrežnog prometa i blokiranje pristupa zlonamjernom ili neprikladnom sadržaju.

Modul 10

Procijeni sigurnosne sposobnosti krajnjih točaka

Pregled modula

Sigurnost krajnjih točaka ima za cilj osigurati svaku krajnju točku spojenu na mrežu, od prijenosnih računala do pametnih telefona, tableta i drugih IoT uređaja, radi sprječavanja da budu ulazna točka napada. Učinkovita sigurnost krajnjih točaka zahtijeva kombinirani pristup koji uključuje hardver, softver i prakse korisnika.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Istražiti važnost učvršćivanja krajnjih točaka.
- Razumjeti tehnike učvršćivanja.
- Istražiti jedinstvene izazove vezane uz učvršćivanje ugrađenih uređaja.
- Naučiti o učvršćivanju mobilnih uređaja.
- Objasniti važnost i strategije upravljanja mobilnim uređajima.

Lekcija 10A

Implementacija sigurnosti krajnjih točaka

Pregled lekcije

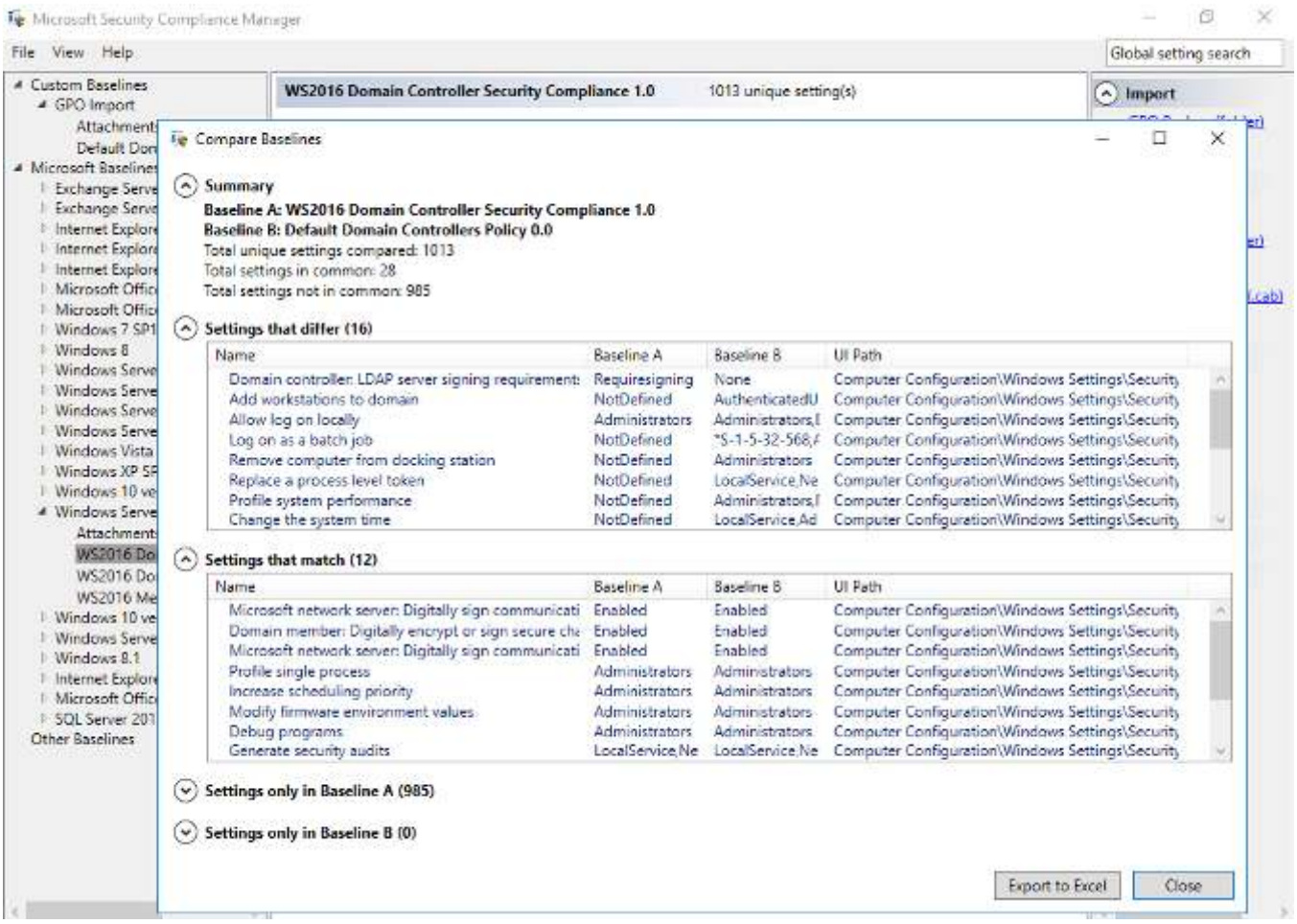
Učvršćivanje uređaja opisuje praksu promjene konfiguracija za zaštitu sustava od prijetnji smanjenjem ranjivosti pripisanih zadanim konfiguracijama. Standardne tehnike uključuju redovito ažuriranje i zakrpanje operativnih sustava i aplikacija, onemogućavanje nepotrebnih usluga i portova i implementaciju snažnih politika autentikacije.

- Sučelja pružaju vezu s mrežom. Neka računala mogu imati više od jednog sučelja. Na primjer, mogu postojati žičana i bežična sučelja ili sučelje modema.

Neka računala mogu dolaziti s mrežnom karticom za upravljanje. Ako bilo koje od ovih sučelja nije potrebno, trebaju biti izričito onemogućena, a ne samo ostavljena neupotrebljenima.

- Usluge pružaju biblioteku funkcija za različite vrste aplikacija. Neke usluge podržavaju lokalne značajke OS-a i instaliranih aplikacija. Ostale usluge podržavaju udaljene veze od klijenata do poslužiteljskih aplikacija. Neuporabljene usluge trebaju biti onemogućene.
- Portovi aplikacijskih usluga dopuštaju klijentskom softveru spajanje na aplikacije putem mreže. Ovi trebaju biti onemogućeni ili blokirani na vatrozidu ako udaljeni pristup nije potreban.
- Trajna pohrana drži korisničke podatke generirane aplikacijama, plus predmemorirane vjerodajnice. Enkripcija diska bitna je za sigurnost podataka. Samo-enkriptirajući diskovi mogu se koristiti tako da su svi podaci u mirovanju uvijek sigurno pohranjeni.

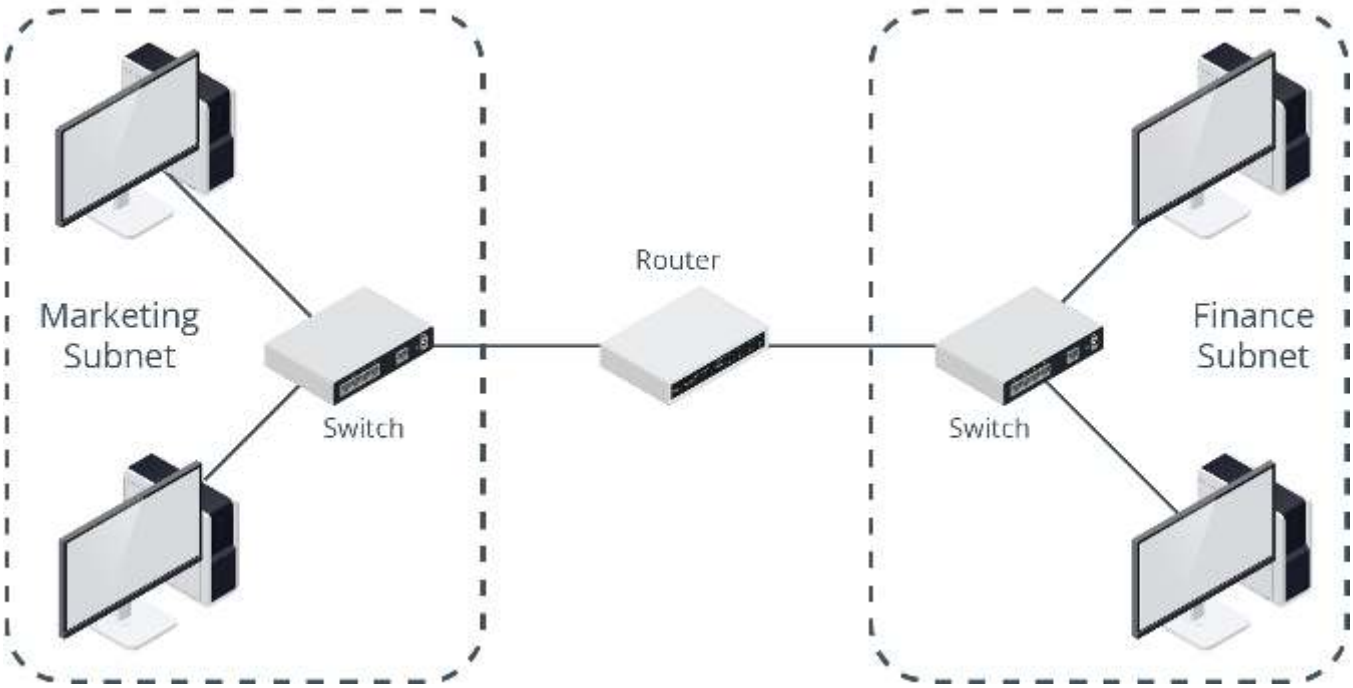
Security Compliance Toolkit (docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10). Korištenje Security Compliance Managera za usporedbu postavki u produkcijskom GPO-u s preporučenom baznom konfiguracijom.



Zaštita krajnjih točaka

Svrha učvršćivanja uređaja je poboljšati sigurnost sustava minimiziranjem potencijalnih ranjivosti koje bi zlonamjerni entitet mogao iskoristiti. Ovo se postiže konfiguriranjem mrežnih, softverskih i hardverskih komponenti u skladu s najboljim praksama. Segmentacija i izolacija su ključne strategije u zaštiti krajnjih točaka.

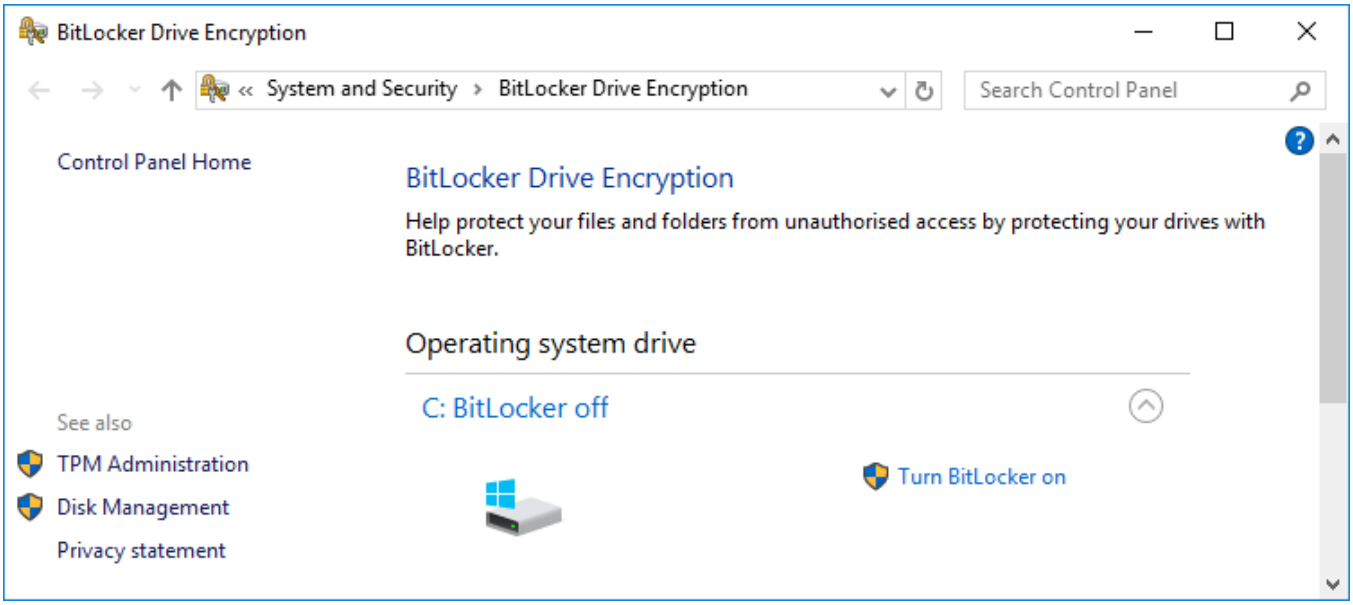
Segmentirana mreža koja prikazuje Marketing i Finance podmreže i postavljanje mrežnih uređaja. Promet između dvije mreže kontrolira usmjerivač.



Izolacija uređaja

Izolacija uređaja odnosi se na odvajanje pojedinih uređaja unutar mreže radi ograničavanja njihove interakcije s ostalim uređajima i sustavima. Ovo ima za cilj poboljšanje zaštite krajnjih točaka sprječavanjem širenja prijetnji unutar mreže.

kreirati lozinku ili ključ za oporavak. To se može koristiti ako se disk premjesti na drugo računalo ili TPM bude oštećen. Aktivacija BitLocker enkripcije diska.



Jedan od nedostataka FDE-a je da, budući da OS izvodi kriptografske operacije, performanse su smanjene. Ovaj problem se ublažava samo-enkriptirajućim diskovima (SED), gdje se kriptografske operacije izvode u hardveru, ne utječući na performanse sustava.

uređaja/firmwarea. Skeniranje je korisno samo ako su uspostavljeni učinkoviti postupci za primjenu nedostajućih zakrpa. U stambenim i malim mrežama, hostovi su tipično konfigurirani za automatsko ažuriranje, što znači da se zakrpe preuzimaju i primjenjuju

bez korisničke intervencije.

Napredna zaštita krajnjih točaka

EDR i XDR — Proizvod za otkrivanje i odgovor na krajnjim točkama (EDR) ima za cilj pružiti stvarnovremensku i povijesnu vidljivost kompromitiranja krajnjih točaka. EDR sakuplja i analizira podatke s krajnjih točaka za otkrivanje prijetnji i odgovor na sigurnosne incidente.

Napomena da je upravljano otkrivanje i odgovor (MDR) klasa hostirane sigurnosne usluge. EDR se fokusira na krajnje točke, dok XDR (Extended Detection and Response) proširuje tu sposobnost na višestruke sigurnosne slojeve poput mrežnih, oblaka i krajnjih točaka, pružajući integrirani pogled prijetnji i mogućnosti odgovora.

iznenada se počne prijavljivati iz strane zemlje. Ove aktivnosti mogle bi ukazivati na potencijalnu povredu podataka ili kompromis računa i pokrenuti upozorenje UEBA sustava. Neki komercijalni UEBA proizvodi dostupni na tržištu:

- Splunk User Behavior Analytics
- IBM QRadar User Behavior Analytics
- Rapid7 InsightIDR
- Forcepoint Insider Threat

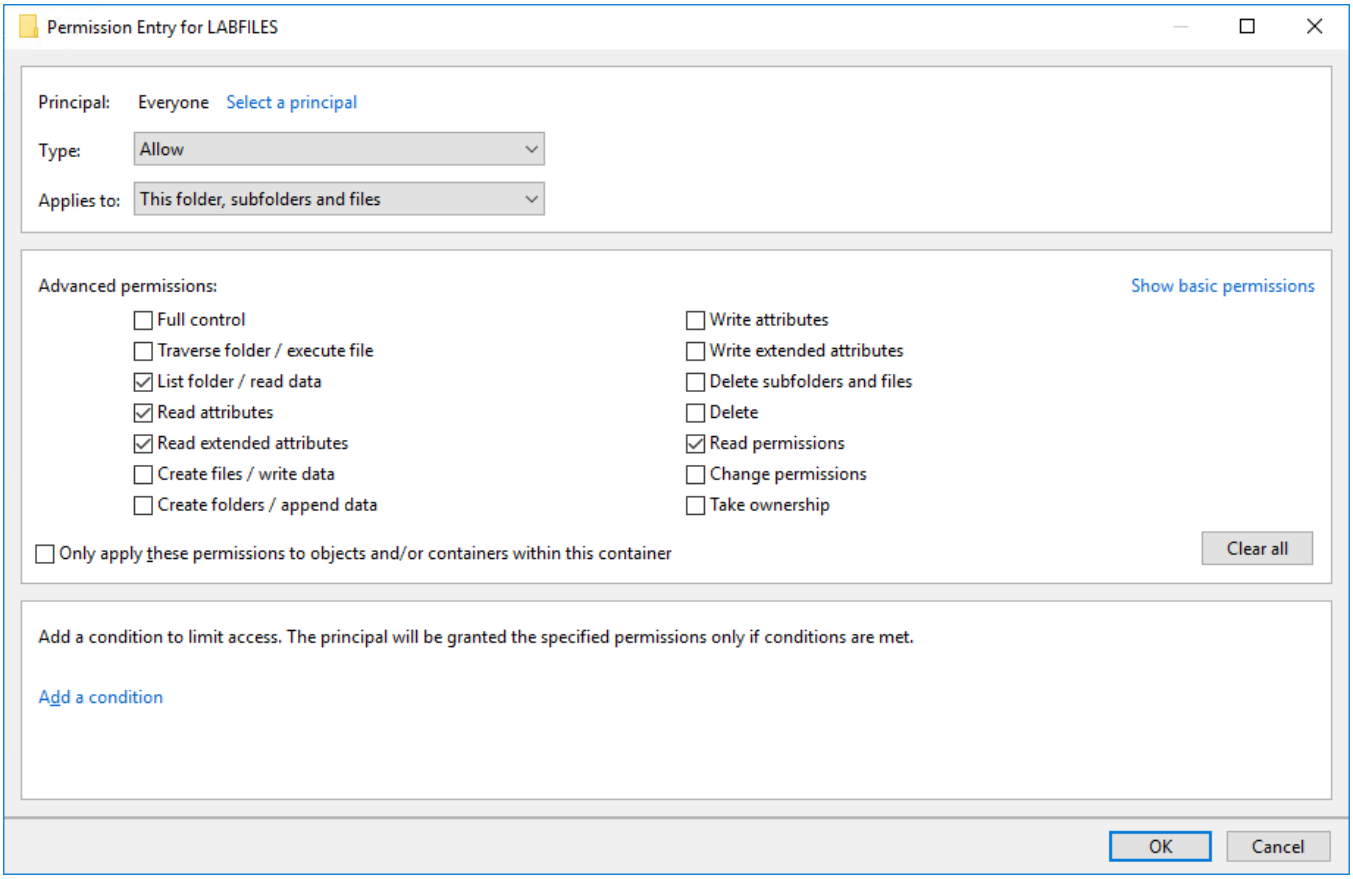
Konfiguracija krajnjih točaka

Ako je sigurnost krajnje točke probijena, postoji nekoliko klasa vektora za razmatranje:

- Socijalni inženjering — ako je malware izvršio korisnik, koristite sigurnosno obrazovanje i osvješćivanje za smanjenje rizika od budućih napada.
- Ranjivosti — ako je malware iskoristio softversku grešku, instalirajte zakrpu ili izolirajte sustav dok se zakrpa ne razvije.
- Nedostatak sigurnosnih kontrola — ako je napad mogao biti spriječen zaštitom krajnje točke/AV, host vatrozidom, filtriranjem sadržaja, DLP-om ili MDM-om, istražite mogućnost njihove implementacije.
- Konfiguracijsko pomicanje (Configuration Drift) — ako je malware iskoristio nedokumentiranu promjenu konfiguracije, primijenite konfiguraciju osnove i istražite postupke upravljanja konfiguracijom.
- Slaba konfiguracija — ako je konfiguracija bila ispravno primijenjena, ali je ipak bila iskorištena, pregledajte predložak za osmišljavanje sigurnijih postavki. Kontrola pristupa — Kontrola pristupa odnosi se na reguliranje i upravljanje dozvolama dodijeljenim pojedincima ili procesima koji pristupaju sistemskim resursima.

Drugi praktičan pristup ograničavanju pristupa je korištenje kontrole pristupa temeljene na ulogama (RBAC). RBAC dodjeljuje prava pristupa sustavu na temelju unaprijed definiranih uloga, a svaka uloga ima pažljivo definiran skup dozvola. Ovo pojednostavljuje upravljanje pristupom i osigurava da korisnici imaju pristup samo resursima koji su relevantni za njihove poslovne odgovornosti.

Konfiguriranje unosa kontrole pristupa za mapu.



Na primjer, u Linuxu postoje tri osnovna prava:

- Čitanje (r) — je mogućnost pristupa i pregledavanja sadržaja datoteke ili listanje sadržaja direktorija.
- Pisanje (w) — je mogućnost spremanja promjena u datoteku ili kreiranje, preimenovanje i brisanje datoteka u direktoriju.
- Izvođenje (x) — je mogućnost pokretanja skripte, programa ili drugog softverskog fajla, ili mogućnost pristupa direktoriju, izvođenja datoteke iz tog direktorija ili obavljanja zadatka na tom direktoriju. Ove dozvole mogu se primijeniti u kontekstu korisnika vlasnika, grupnog računa ili svih ostalih.

U apsolutnom načinu, dozvole se dodjeljuju koristeći oktalnu notaciju, gdje je r=4, w=2 i x=1. Na primjer, sljedeća naredba ima isti učinak: chmod 755 home. U ovom primjeru, 755 odgovara: vlasnik = 7 (čitanje + pisanje + izvođenje), grupa = 5 (čitanje + izvođenje), ostali = 5 (čitanje + izvođenje).

- Lista dopuštenih (allow list) odbija izvođenje osim ako je proces izričito ovlašten.
- Lista blokiranih (block list) generalno dopušta izvođenje, ali izričito zabranjuje navedene procese.

Sadržaj lista dopuštenih i lista blokiranih mora se ažurirati kao odgovor na incidente i tekuće lovljenje i praćenje prijetnji.

- Standardizirane konfiguracijskie osnove definiraju organizacije poput NIST-a, CIS-a ili sama organizacija i koriste se kao mjerilo za način konfiguriranja sustava i uređaja.
- Automatizirani alati za upravljanje konfiguracijom koriste se za automatsku primjenu i održavanje standardiziranih konfiguracionih osnova u cijelom okruženju.

- Kontinuirano praćenje i provjere usklađenosti ključni su za otkrivanje odstupanja od obveznih konfiguracija.
- Procesi upravljanja promjenama osiguravaju da su promjene konfiguracije pravilno pregledane, testirane i odobrene prije implementacije.

Tehnike učvršćivanja

Za zaštitu krajnjih točaka od raznih i stalno razvijajućih prijetnji kibernetičke sigurnosti potrebni su različiti pristupi učvršćivanja. Ove prijetnje zahtijevaju slojevit i sveobuhvatan pristup, poput primjene zakrpa, upravljanja korisničkim računima i kontrole hardvera i softvera.

ne služi poslovnoj svrsi. Time se pomaže sprječavanje neovlaštenog prijenosa podataka, instaliranja zlonamjernog softvera ili izravnog pristupa sustavu. Softver za kontrolu portova pruža dodatnu zaštitu nadzorom i upravljanjem USB i ostalim portovima.

- Enkripcija cijelog diska (FDE) šifrira cijeli tvrdi disk uređaja. Osigurava da su svi podaci, uključujući operativni sustav i korisničke datoteke, zaštićeni čak i kada operativni sustav ne radi. Alati poput BitLockera za Windows i FileVault za macOS pružaju mogućnosti enkripcije cijelog diska.
- Enkripcija prijenosnih medija osigurava da podaci ostaju zaštićeni čak i kada su fizički uklonjeni s uređaja poput SD kartica ili USB masovnih uređaja pohrane.
- Virtualne privatne mreže (VPN) nadopunjuju enkripciju krajnje točke pružanjem sigurnog tunela za prijenos podataka koji štiti od prisluškivanja i napada na putu.
- Enkripcija e-pošte štiti osjetljive informacije pohranjene u e-porukama koristeći protokole poput PGP (Pretty Good Privacy) ili S/MIME. Host-based vatrozidi i IPS — Host-based vatrozidi i sustavi za sprječavanje upada (IPS) vitalni su elementi zaštite krajnjih točaka koji filtriraju dolazni i odlazni mrežni promet.
- Kreirajte plan implementacije s razmatranjima poput redoslijeda implementacije, vremenskih okvira i korištenja faza za ograničavanje potencijalnih ometanja uzrokovanih postavkama zaštite krajnjih točaka.
- Standardizirajte konfiguracije zaštite krajnjih točaka na svim uređajima za osiguravanje dosljednosti u razinama zaštite.
- Automatizirajte implementacije koristeći alate poput SCCM-a, Group Policy ili rješenja trećih strana.
- Ažuriranja i zakrpe softvera agenta zaštite krajnjih točaka i definicija potrebne su za osiguravanje najviših razina zaštite.
- Nadzirite agente zaštite krajnjih točaka za provjeru upozorenja ili znakova potencijalnih sigurnosnih incidenata.
- Centralizirajte upravljanje za pružanje sveobuhvatnog pogleda na konfiguracije, ažuriranja i status krajnjih točaka.

posebno ranjivi na neovlašteni pristup. Stoga je mijenjanje ovih lozinki u snažne, jedinstvene vjerodajnice ključno kao dio početnog procesa postavljanja za svaki uređaj ili sustav. Uklanjanje nepotrebnog softvera smanjuje površinu napada i opterećenje upravljanja zakrpama, budući da svaki komad softvera potencijalno uvodi ranjivosti.

Učvršćivanje specijaliziranih uređaja

Industrijski kontrolni sustavi (ICS), uključujući sustave za nadzornu kontrolu i akviziciju podataka (SCADA), ugrađeni sustavi, operativni sustavi u stvarnom vremenu (RTOS) i Internet stvari (IoT) uređaji svaki predstavljaju jedinstvene sigurnosne izazove koji zahtijevaju specijalizirane pristupe učvršćivanja. Ove arhitekture su podložne raznim ranjivostima jer su dizajnirane za rad, a ne sigurnost.

Lekcija 10B

Učvršćivanje mobilnih uređaja

Pregled lekcije

Učvršćivanje mobilnih uređaja kritično je za kibernetičku sigurnost i uključuje nekoliko bitnih praksi dizajniranih za zaštitu uređaja od prijetnji i ranjivosti, uključujući (kao minimum) kontrole poput redovitih ažuriranja OS-a, enkripciju uređaja i snažne politike lozinki.

Tehnike učvršćivanja mobilnih uređaja

Postoji mnogo sličnosti između učvršćivanja mobilnih uređaja ili tradicionalnih stolnih računala. Obje zahtijevaju zakrpe operativnog sustava, snažne jedinstvene lozinke, zaštitu krajnjih točaka i kriptografske kontrole. Modeli implementacije mobilnih uređaja:

- Donesi vlastiti uređaj (BYOD) — znači da je mobilni uređaj u vlasništvu zaposlenika. Uređaj mora udovoljavati zahtjevima koje je razvila organizacija, a zaposlenik mora pristati na instaliranje korporativnih aplikacija.
- Korporativno vlasništvo, samo za poslovnu upotrebu (COBO) — znači da je uređaj vlasništvo organizacije i može se koristiti samo za poslovne svrhe.
- Korporativno vlasništvo, osobno omogućeno (COPE) — znači da organizacija bira i nabavlja uređaj, koji ostaje u njenom vlasništvu. Zaposlenik ga može koristiti za pristup osobnoj e-pošti i profilima društvenih mreža i osobno pregledavanje weba.
- Izaberi vlastiti uređaj (CYOD) — sličan je COPE-u, osim što zaposlenik dobiva izbor uređaja s unaprijed utvrđenog popisa.

Enkripcija cijelog uređaja i vanjski mediji

Gotovo sve verzije mobilnog OS-a za pametne telefone i tablete pružaju enkripciju cijelog uređaja. U iOS-u postoje različite razine enkripcije.

- Svi korisnički podaci na uređaju uvijek su enkriptirani, ali ključ je pohranjen na uređaju. Ovo se primarno koristi kao sredstvo brisanja uređaja — OS samo treba izbrisati ključ da podatke učini nedostupnima.

- Podaci e-pošte i sve aplikacije koje koriste opciju 'Zaštita podataka' podliježu drugoj rundi enkripcije koristeći ključ koji je izveden i zaštićen korisničkim vjerodajnicama.

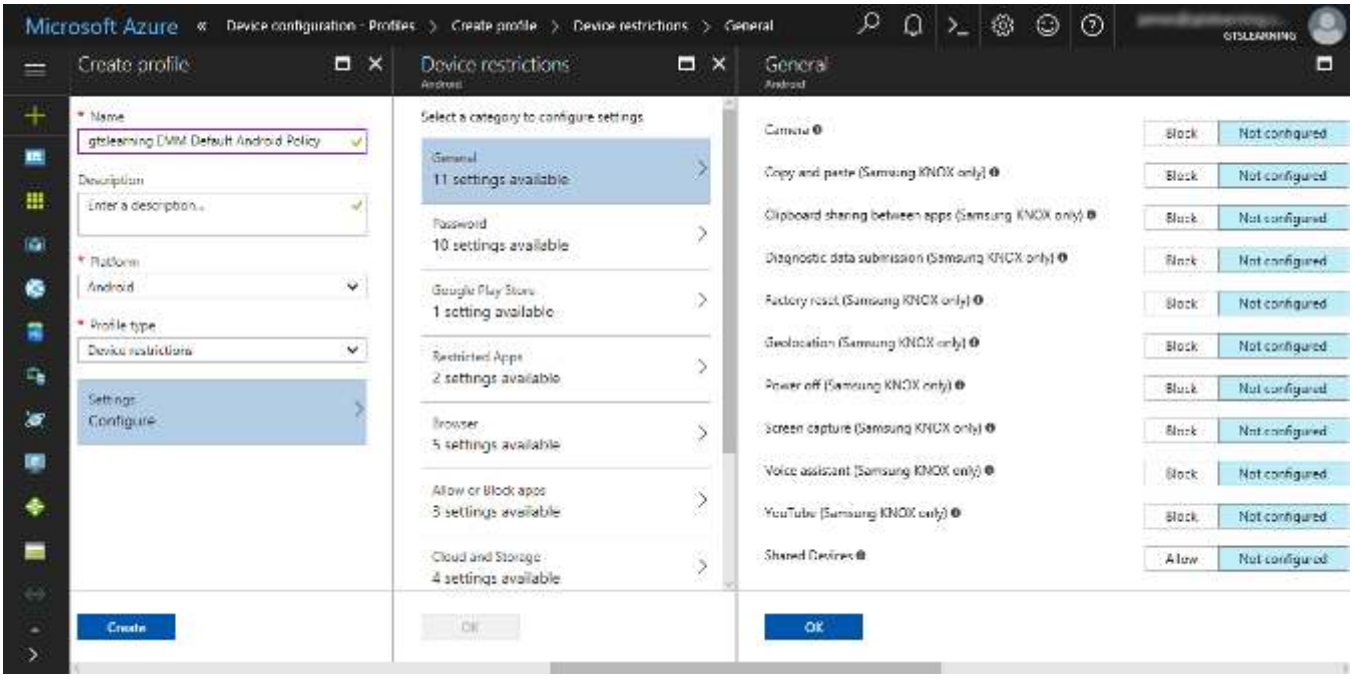
sigurnost za podatke u slučaju krađe uređaja. Nisu svi korisnički podaci enkriptirani koristeći opciju 'Zaštita podataka'; kontakti, SMS poruke i slike na primjer nisu. U iOS-u, Zaštita podataka je zadano omogućena za aplikacije trećih strana koje koriste iOS enkripcijsko API.

Lokacijske usluge

Geolokacija je upotreba mrežnih atributa za identificiranje (ili procjenu) fizičke pozicije uređaja. Uređaj koristi lokacijske usluge za određivanje svoje trenutne pozicije. Lokacijske usluge se određuju korištenjem:

- Globalnog pozicioniranog sustava (GPS) — je sredstvo određivanja geografske širine i dužine uređaja na temelju informacija primljenih od satelita putem GPS senzora.
- Unutarnjeg pozicioniranog sustava (IPS) — određuje lokaciju uređaja trianguliranjem njegove blizine ostalim radio izvorima, poput ćelijskih tornjeva, Wi-Fi pristupnih točaka i Bluetooth/RFID odašiljača.

Ograničavanje dozvola uređaja poput kamere i snimke zaslona koristeći Intune.



GPS označavanje

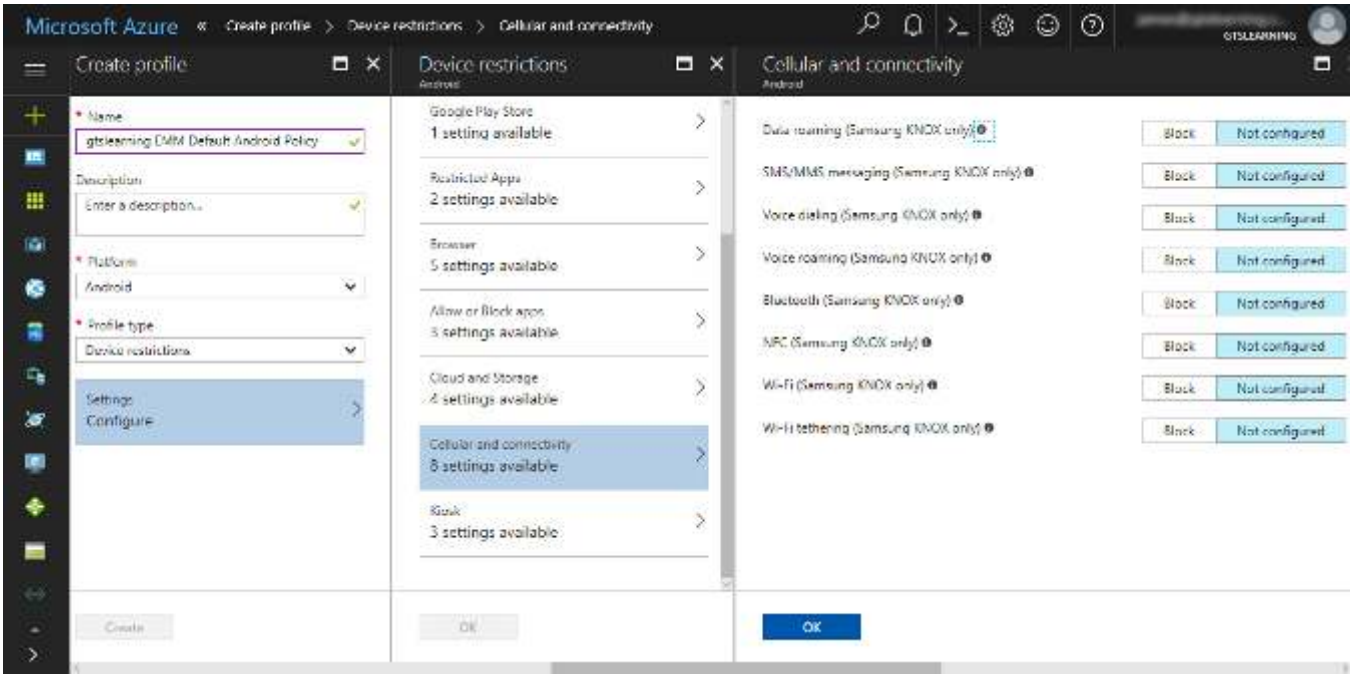
GPS označavanje je proces dodavanja metapodataka geografske identifikacije, poput geografske širine i dužine gdje je uređaj bio lociran u to vrijeme, medijima poput fotografija, SMS poruka i video zapisa. GPS označavanje može biti korisno za dokazivanje lokacije u pravnim situacijama ili za organiziranje fotografija prema lokaciji.

Metode mobilnih i GPS veza

Mobilni uređaji koriste razne metode veza za uspostavljanje komunikacija u lokalnim i osobnim mrežama i za pristup Internet podacima putem pružatelja usluge.

Zaključavanje Android metoda povezivosti s Intuneom

imajte na umu da se većina postavki može primijeniti samo na Samsung KNOX-sposobne uređaje.



Mobilne/ćelijske podatkovne veze

Pametni telefoni, tableti i prijenosna računala koriste mobilne podatkovne mreže za komunikaciju podataka. Mobilne podatkovne veze malo su vjerojatno predmet nadzora i filtriranja. Zaštita podataka koji prolaze po mobilnim mrežama zahtijeva enkripciju aplikacijskog sloja, poput VPN-a.

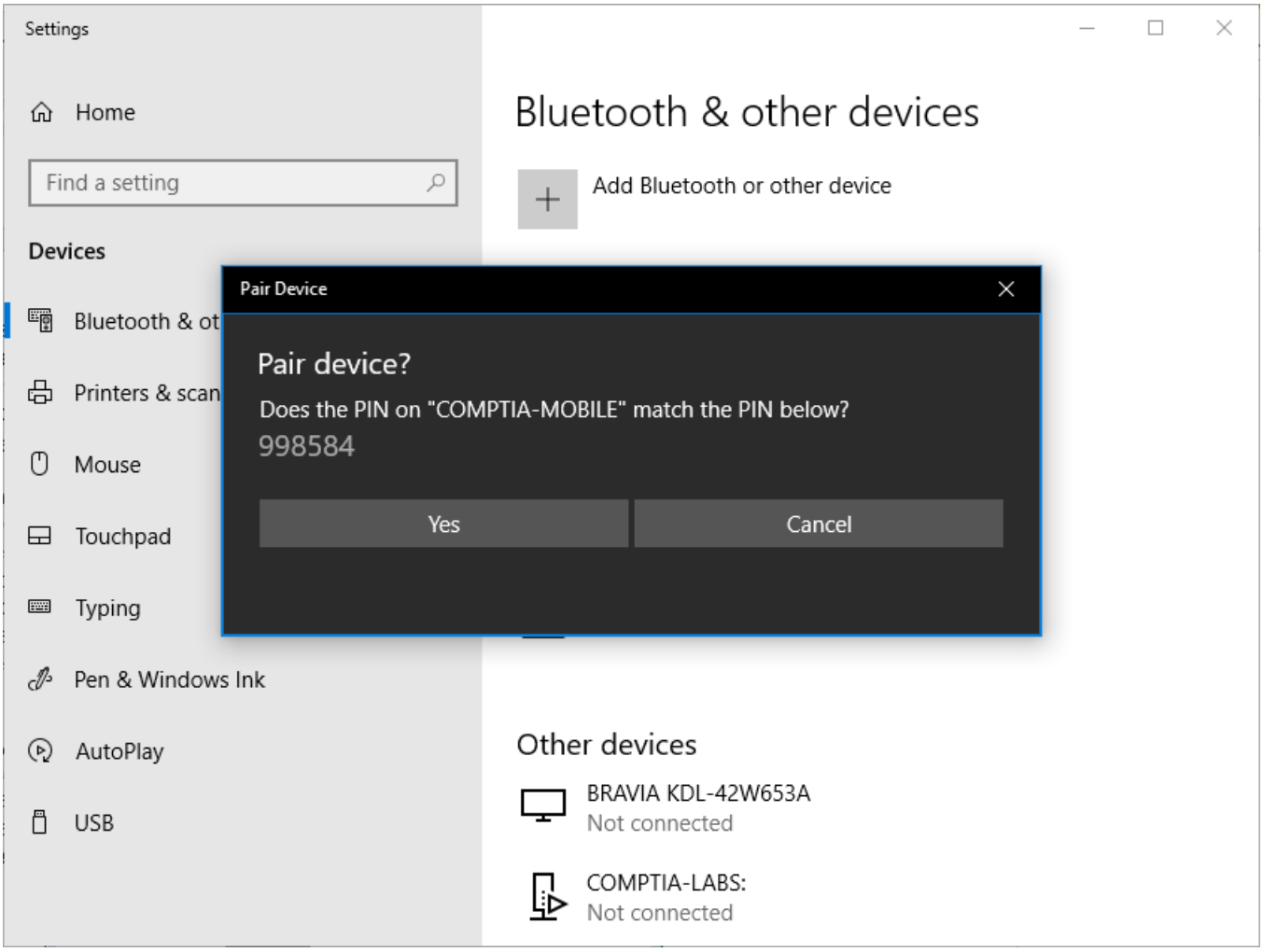
Osobne mrežne mreže (PAN) omogućuju povezivanje između mobilnog uređaja i perifernih uređaja. Ad hoc (ili peer-to-peer) mreže između mobilnih uređaja ili između mobilnih uređaja i drugih računalnih uređaja mogu se uspostaviti koristeći Wi-Fi, Bluetooth ili NFC.

Metode Bluetooth veza

Bluetooth je bežična tehnologija temeljena na radijskim valovima dizajnirana za implementaciju umrežavanja kratkog dometa osobnih mreža. Neka sigurnosna pitanja vezana uz Bluetooth:

- Otkrivanje uređaja — je kada se uređaj može staviti u otkrivajući način, što znači da će se spojiti na bilo koji drugi Bluetooth uređaj u blizini. Nažalost, čak i uređaj koji nije u otkrivajućem načinu i dalje može biti detektiran.
- Autentikacija i autorizacija — je kada se uređaji autentificiraju ('uparuju') koristeći jednostavnu pristupnu šifru konfiguriranu na oba uređaja. Ovo uvijek treba biti promijenjeno u sigurnu frazu i nikada ne ostavljati kao zadano.
- Malware — je kada postoje proof-of-concept Bluetooth crvi i aplikacijski exploiti, posebno exploit BlueBorne, koji može kompromitirati bilo koji aktivan i nezakrpan sustav bez obzira je li otkrivanje omogućeno i bez zahtijevanja korisničke intervencije.

Uparivanje računala s pametnim telefonom.



Korištenjem preklopnika kontrolnog centra možda zapravo ne isključuje Bluetooth radio na mobilnom uređaju. Ako postoji bilo kakva sumnja u status zakrpa ili izloženost ranjivostima, Bluetooth treba biti potpuno onemogućen u postavkama uređaja.

Uparivanje i autentikacija: Tijekom uparivanja, uređaji razmjenjuju kriptografske ključeve za autentikaciju identiteta jednih s drugima i uspostavljanje sigurnog komunikacijskog kanala. NFC (Near Field Communication) je kratko-rasponska radio komunikacijska tehnologija koja omogućuje jednostavno postavljanje veze dodirom uređaja ili njihovim spajanjem na kratkoj udaljenosti. NFC može biti iskorišten za presretanje podataka ako dva uređaja komuniciraju, ali zahtijeva da napadač bude u neposrednoj blizini.

putem metode slične DoS napadu — preplavljivanjem područja prekomjernom količinom RF signala za ometanje prijenosa. Skimming kreditne ili bankovne kartice dati će napadaču dugi broj kartice i datum isteka.

Sažetak

Trebate biti u mogućnosti primijeniti politike i tehnologije učvršćivanja hosta i procijeniti rizike od lanaca opskrbe trećih strana i ugrađenih/IoT sustava. Smjernice za implementaciju rješenja sigurnosti hosta:

- Uspostavite konfiguracijske osnove za svaku vrstu hosta. Osigurajte da su hostovi implementirani prema konfiguracionoj osnovi i postavite praćenje za osiguravanje usklađenosti.
- Konfiguriranje enkripcije cijelog diska.

- Implementirajte rješenje zaštite krajnje točke koje zadovoljava sigurnosne zahtjeve za funkcije poput antimalwarea, vatrozida, IDS-a, EDR-a i DLP-a.
- Uspostavite postupke upravljanja zakrpama za testiranje ažuriranja za različite grupe hostova i osigurajte upravljanje OS-om i softverom trećih strana.
- Kreirajte plan upravljanja za sve IoT uređaje koji se koriste na radnom mjestu.
- Procijenite sigurnosne zahtjeve za ICS i/ili SCADA ugrađene sustave.

Modul 11

Poboljšaj sposobnosti sigurnosti aplikacija

Pregled modula

Koncepti sigurnih protokola i razvoja aplikacija bitni su stupovi robusne kibernetičke sigurnosti. Protokoli poput HTTPS-a, SMTPS-a i SFTP-a pružaju šifrirane komunikacijske kanale, osiguravajući povjerljivost i integritet podataka u prijenosu.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Razumjeti koncepte sigurnih protokola.
- Istražiti mogućnosti DNS filtriranja.
- Pregledati protokole sigurnosti e-pošte.
- Istražiti tehnike sigurnosti aplikacija.
- Pregledati koncepte sandboxinga.

Lekcija 11A

Sigurnosne osnove protokola aplikacija

Pregled lekcije

Sigurni protokoli temeljni su za održavanje sigurnosti podataka. Sigurni protokoli uključuju HTTPS (Hypertext Transfer Protocol Secure) za sigurni web promet, SMTPS i IMAPS za zaštitu tradicionalnih usluga e-pošte, LDAPS za zaštitu imeničkih usluga, FTPS i SFTP za sigurni prijenos datoteka, SNMPv3 za sigurno mrežno upravljanje te SSH za sigurni udaljeni pristup. Svaki od ovih protokola koristi enkripciju i autentifikaciju za zaštitu podataka u prijenosu.

Sigurni protokoli

Mnogi protokoli koji se danas koriste na računalnim mrežama razvijeni su prije nekoliko desetljeća, kada je funkcionalnost bila na prvom mjestu, pouzdanost se pretpostavljala umjesto da se zarađuje, a mrežna sigurnost bila je zanemaren problem. Ovi protokoli i dalje su u upotrebi, no uz dodatak sigurnih verzija koje pružaju enkripciju i autentifikaciju kako bi se kompenzirali nedostaci originala.

Sigurni protokoli koriste enkripciju i dekripciju koje zahtijevaju pravilno upravljanje kriptografskim ključevima, uključujući procese koji se odnose na njihovo kreiranje, pohranjivanje, distribuciju i opoziv. Uz to, sigurni protokoli zahtijevaju digitalne certifikate za autentifikaciju i verifikaciju identiteta. Upravljanje certifikatima uključuje proces koji se odnosi na kreiranje, distribuciju, pohrani, opozivu i validaciju certifikata. Infrastruktura javnih ključeva (PKI) pruža okvir za upravljanje digitalnim certifikatima i kriptografskim ključevima.

Transport Layer Security

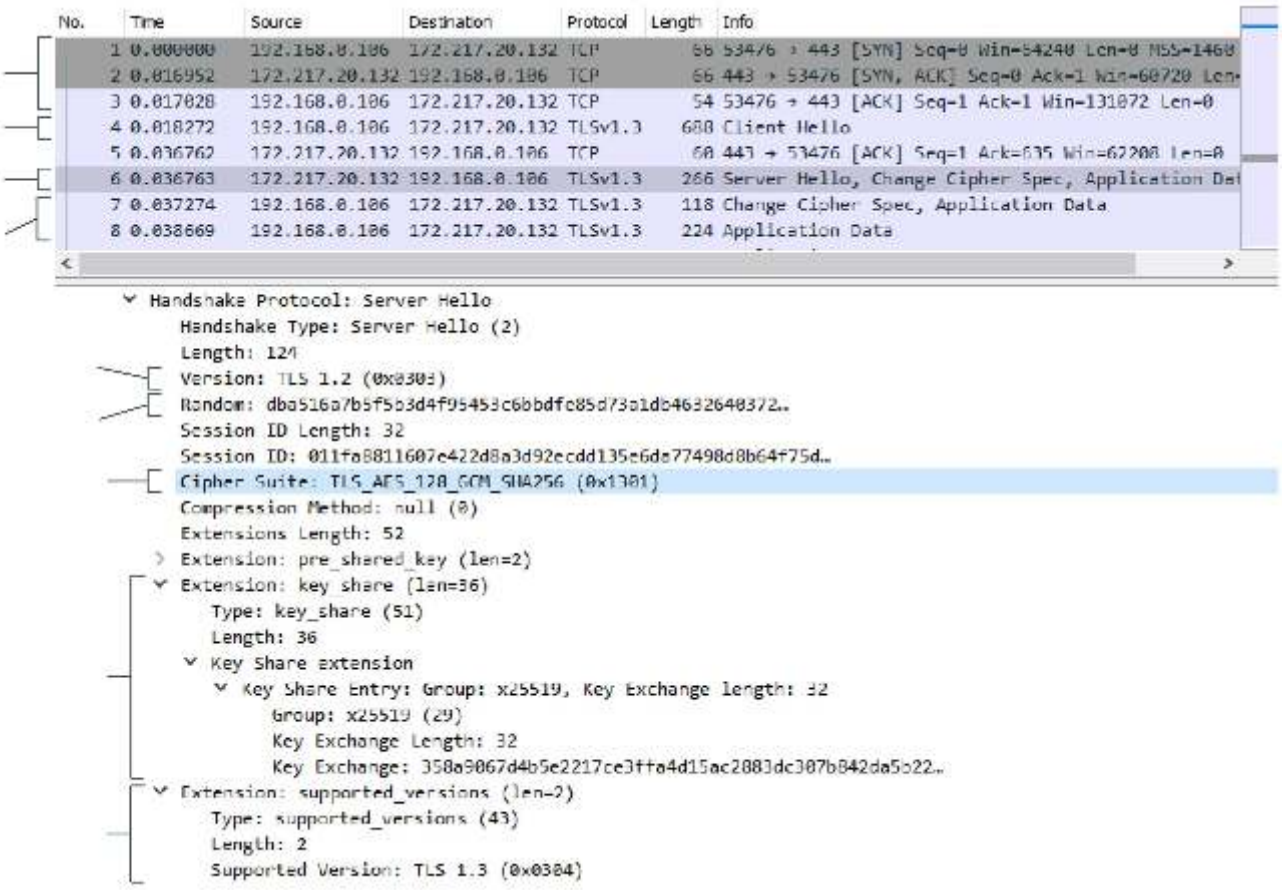
Kao i kod ostalih ranih TCP/IP aplikacijskih protokola, HTTP komunikacije nisu zaštićene. Netscape je devedesetih godina razvio Secure Sockets Layer (SSL) kako bi riješio nedostatak sigurnosti na webu. SSL je na kraju zamijenjen standardom Transport Layer Security (TLS). TLS osigurava povjerljivost i integritet podataka u prijenosu između klijentskih i poslužiteljskih aplikacija. TLS koristi asimetričnu enkripciju za razmjenu ključeva te simetričnu enkripciju za zaštitu podataka u prijenosu.

protokolu da se dogovori o međusobno podržanim šiframa s klijentom i pregovara o enkriptiranoj komunikacijskoj sesiji. HTTPS prema zadanim postavkama radi na portu 443. HTTPS operacija označena je korištenjem https:// u URL-u preglednika. Certifikat koji je koristio server vidljiv je klikom na ikonu lokota u pregledniku.

Također je moguće instalirati certifikat na klijenta kako bi server mogao vjerovati klijentu. To se ne koristi često na webu, ali je značajka VPN-ova i poslovnih mreža koje zahtijevaju međusobnu autentifikaciju. Ovo je poznato kao uzajamna TLS (mTLS) autentifikacija.

TLS verzija 1.3 odobrena je 2018. godine. Jedna od glavnih značajki TLS 1.3 je uklanjanje mogućnosti izvođenja napada degradacije sprečavanjem korištenja nesigurnih značajki i algoritama iz prethodnih verzija. TLS 1.3 također skraćuje rukovanje, što rezultira bržim postavljanjem veze. TLS 1.2 i dalje je u širokoj upotrebi, ali TLS 1.0 i TLS 1.1 smatraju se zastarjelim i trebali bi biti onemogućeni.

Pregledavanje TLS rukovanja u Wireshark snimci paketa. Imajte na umu da veza koristi TLS 1.3 i jedan od skraćenih skupova šifri (TLS_AES_128_GCM_SHA256).



Sigurne imeničke usluge

Mrežni imenik popisuje subjekte (uglavnom korisnike, računala i usluge) i objekte (poput direktorija i datoteka) dostupnih na mreži, zajedno s dodijeljenim dozvolama i privilegijama. Protokol lakog pristupa imeniku (LDAP) standardni je protokol za pristup i upravljanje imeničkim uslugama. LDAP ne pruža nikakvu enkripciju prema zadanim postavkama. LDAP autentifikacija može biti konfigurirana na tri načina:

- Bez autentifikacije — znači da je anonimni pristup imeniku odobren.

• Jednostavno vezanje — znači da klijent mora dostaviti svoje razlikovano ime (DN) i lozinku, ali

• Simple Authentication and Security Layer (SASL) — znači da klijent i server pregovaraju o

upotrebi podržanog mehanizma autentifikacije, poput Kerberosa. Naredba STARTTLS može se koristiti za zahtijevanje enkripcije (pečaćenja) i integriteta poruka (potpisivanja). Ovo je preferirani mehanizam za Microsoft Active Directory.

• LDAP Secure (LDAPS) — znači da je server instaliran s digitalnim certifikatom, koji koristi

za postavljanje sigurnog tunela za razmjenu korisničkih vjerodajnica. LDAPS koristi port 636. Ako je potreban siguran pristup, anonimni i jednostavni načini autentifikacije trebaju biti onemogućeni na serveru. Opće

ali točan mehanizam je specifičan za pojedinog prodavatelja i nije specificiran u LDAP standardnoj dokumentaciji. Osim ako ne hostiraju javnu uslugu, LDAP imenički server trebao bi biti dostupan samo iz privatne mreže organizacije.

Sigurnost Simple Network Management Protocola

Simple Network Management Protocol (SNMP) široko je korišten okvir za upravljanje i nadzor. SNMP se sastoji od SNMP monitora i agenata.

• Agent je proces (softver ili firmware) koji se izvodi na preklopniku, usmjerniku, serveru ili drugom

SNMP kompatibilnom mrežnom uređaju.

• Ovaj agent održava bazu podataka zvanu baza upravljačkih informacija (MIB) koja sadrži

statistike vezane uz aktivnost uređaja (na primjer, broj okvira u sekundi koje obrađuje preklopnik). Agent je također sposoban pokrenuti operaciju zamke gdje obavještava upravljački sustav o specifičnom događaju.

• SNMP monitor (softverski program) pruža lokaciju s koje se može nadzirati mrežna aktivnost.

Nadzire sve agente redovitim ispitivanjem za informacije iz njihovih MIB-ova i prikazuje informacije za pregled. Također prikazuje sve operacije zamki kao upozorenja za administratore.

• SNMP nazivi zajednice šalju se kao čisti tekst i stoga ne bi trebali biti preneseni preko

mreže ako postoji ikakav rizik da bi mogli biti presretnuti.

• Koristite teško pogodive nazive zajednice; nikada ne ostavljajte naziv zajednice prazan ili postavljen na

zadanu vrijednost.

• Koristite liste kontrole pristupa za ograničavanje upravljačkih operacija na poznate hostove (tj. ograničite na

jednu ili dvije IP adrese hosta).

• Koristite SNMP v3 gdje god je moguće i onemogućite starije verzije SNMP-a. SNMP v3 podržava

enkripciju i jaku autentifikaciju temeljenu na korisnicima. Umjesto naziva zajednica, agenti su konfigurirani s popisom korisničkih imena i dozvola za pristup. Kada je potrebna autentifikacija, SNMP poruke su potpisane.

Usluge prijenosa datoteka

Postoji mnogo načina prijenosa datoteka preko mreža. Mrežni operativni sustav može hostirati dijeljene mape i datoteke, omogućujući njihovo kopiranje ili pristup putem lokalne mreže.

web servera. FTP je učinkovitiji od privitaka e-pošte ili HTTP prijenosa datoteka, ali nema sigurnosnih mehanizama. Sva autentifikacija i prijenos podataka komuniciraju se kao čisti tekst, što znači da vjerodajnice i podaci mogu biti presretnuti.

- Eksplicitni TLS (FTPES) — koristi naredbu AUTH TLS za nadogradnju nesigurne veze

uspostavljene na portu 21 na sigurnu. Ovo štiti vjerodajnice autentifikacije. Podatkovna veza za prijenos datoteka također može biti enkriptirana (korištenjem naredbe PROT).

- Implicitni TLS (FTPS) — pregovara o SSL/TLS tunelu prije razmjene bilo kakvih FTP

naredbi. Ovaj način koristi sigurni port 990 za upravljačku vezu. FTPS je teško konfigurirati kada postoje vatrozidovi između klijenta i servera. Posljedično, FTPES je obično preferirani standard.

Usluge e-pošte

Usluge e-pošte koriste dvije vrste protokola:

- Simple Mail Transfer Protocol (SMTP) specificira kako se pošta šalje s jednog sustava na

drugi.

- Protokol poštanskog sandučića pohranjuje poruke za korisnike i omogućuje im preuzimanje na klijentska

računala ili upravljanje njima na serveru. Sigurni SMTP (SMTPS) — Za dostavu poruke, SMTP server pošiljatelja otkriva IP adresu SMTP servera primatelja koristeći dio domene adrese e-pošte primatelja u DNS-u.

- STARTTLS — je naredba koja nadograđuje postojeću nesigurnu vezu na korištenje TLS-a. To se

naziva i eksplicitni TLS ili oportunistički TLS.

- SMTPS — uspostavlja sigurnu vezu prije razmjene bilo kakvih SMTP naredbi (HELO,

na primjer). Ovo se naziva i implicitni TLS. Metoda STARTTLS je općenito šire implementirana od SMTPS-a. Tipične SMTP konfiguracije koriste sljedeće portove i sigurne postavke:

- Port 25 — koristi se za prosljeđivanje poruka (između SMTP servera ili agenata za prijenos poruka

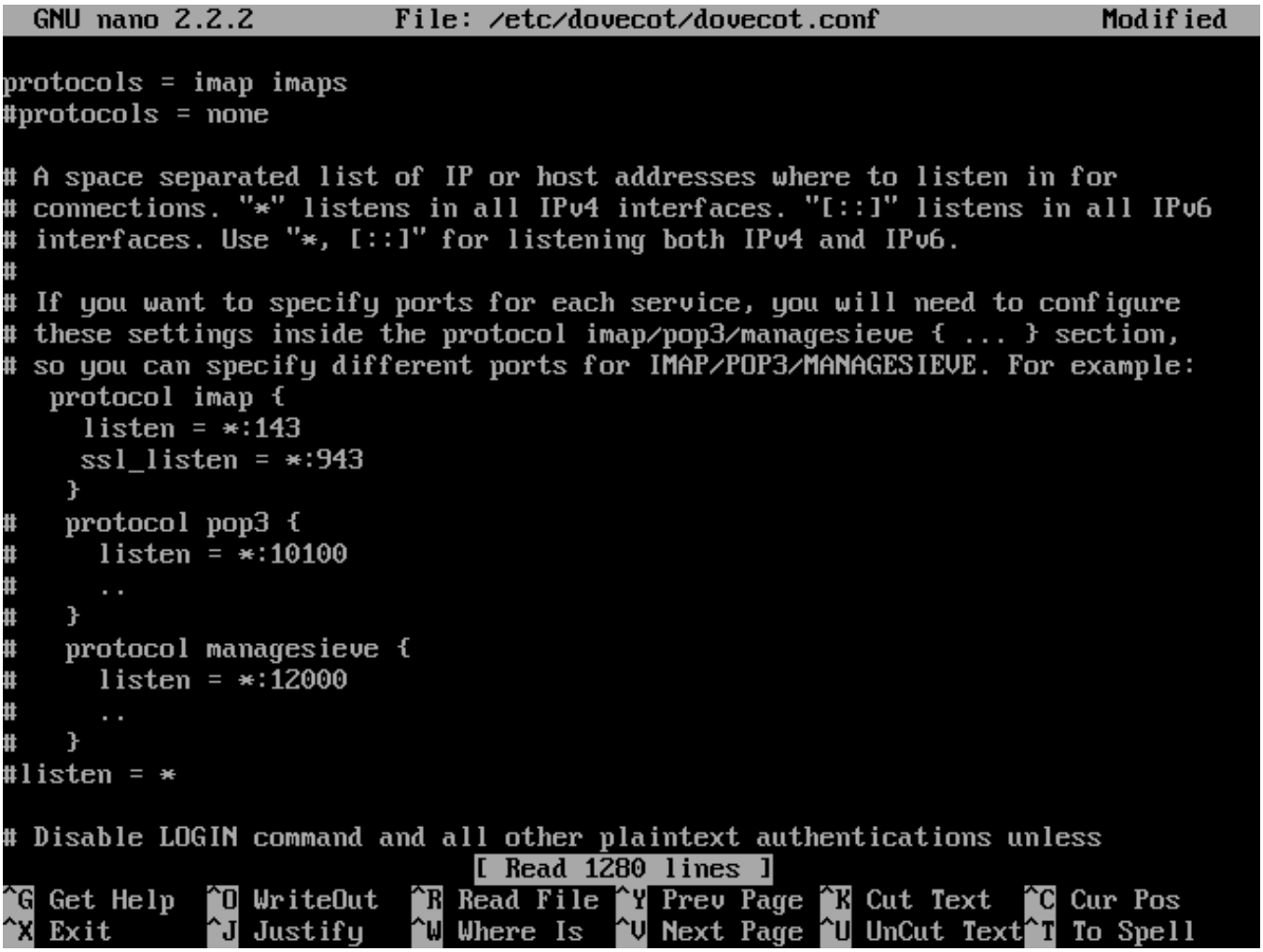
[MTA]). Ako je sigurnost potrebna i podržana od oba servera, naredba STARTTLS može se koristiti za postavljanje sigurne veze.

- Port 587 — koriste ga mail klijenti (agenti za slanje poruka [MSA]) za slanje poruka

za dostavu putem SMTP servera. Serveri konfigurirani za podržavanje porta 587 trebali bi koristiti STARTTLS i zahtijevati autentifikaciju prije slanja poruka.

- Port 465 — koriste ga neki davatelji usluga i mail klijenti za slanje poruka putem implicitnog

TLS (SMTPS), iako je ova upotreba sada zastarjela prema standardnoj dokumentaciji. Sigurni POP (POP3S) — Post Office Protocol v3 (POP3) je protokol poštanskog sandučića dizajniran za pohranu poruka dostavljenih putem SMTP-a. Klijentska aplikacija POP3, poput Microsoft Outlooka ili Mozilla Thunderbirda, uspostavlja TCP vezu s POP3 serverom na portu 110. Korisnik je autentificiran (korisničkim imenom i lozinkom), a poruke su preuzete na lokalni sustav i uobičajeno obrisane s servera. POP3S enkriptira komunikaciju korištenjem TLS-a i koristi port 995.



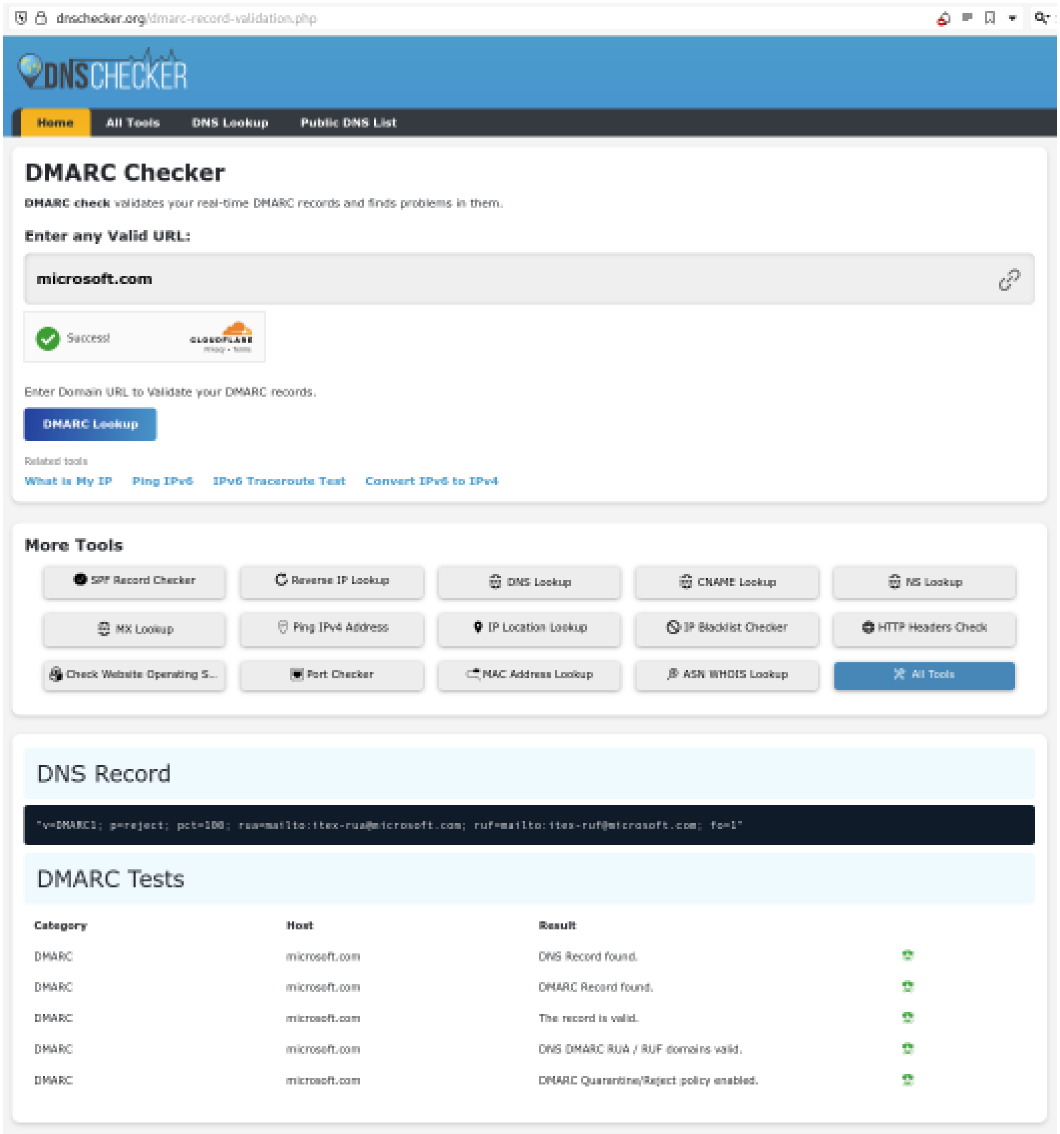
Sigurnost e-pošte

Tri tehnologije pojavile su se kao ključne za verifikaciju autentičnosti e-pošte i sprečavanje phishinga i spama: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) i Domain-based Message Authentication, Reporting and Conformance (DMARC). SPF je DNS zapis koji specificira koji mail serveri su ovlašteni slati e-poštu za određenu domenu. Kada mail server primi poruku, može provjeriti SPF zapis domene pošiljatelja kako bi potvrdio je li server koji šalje ovlašten za slanje e-pošte za tu domenu. SPF pomaže spriječiti lažiranje e-pošte i poboljšava isporuku e-pošte sprječavanjem označavanja legitimnih e-poruka kao spam.

Snimak zaslona korišten uz dopuštenje Microsofta.

DomainKeys Identified Mail (DKIM) koristi značajke enkripcije za omogućavanje verifikacije e-pošte dopuštajući pošiljatelju da potpiše e-poštu digitalnim potpisom. Primajući mail server koristi DKIM zapis domene pošiljatelja za provjeru potpisa i potvrdu da e-pošta nije bila izmijenjena u prijenosu.

Izvođenje DMARC pretrage korištenjem DNSChecker web stranice https://dnschecker.org.



Kombinirana upotreba SPF-a, DKIM-a i DMARC-a značajno poboljšava sigurnost e-pošte čineći mnogo težim napadačima da lažno predstavljaju pouzdane domene, što je jedna od najčešćih taktika koje se koriste u phishing napadima. DMARC gradi na SPF-u i DKIM-u dodavanjem politike koja nalaže primajućim mail serverima što učiniti s e-poštom koja ne prođe provjere SPF-a ili DKIM-a.

i štetnih privitaka. Email pristupnici koriste DMARC, SPF i DKIM za automatizaciju autentifikacije i validacije pošiljatelja e-pošte, smanjujući vjerojatnost da će lažirane ili lažno predstavljene e-poruke biti dostavljene korisnicima. Email pristupnici mogu biti implementirani kao hardverski ili softverski uređaji i mogu biti implementirani lokalno ili u oblaku.

Sprječavanje gubitka podataka putem e-pošte

E-pošta je jedan od najčešće korištenih komunikacijskih kanala unutar organizacija. Služi kao kanal za osjetljive podatke poput financijskih informacija, intelektualnog vlasništva i osobnih podataka zaposlenika i klijenata. Rješenja za sprječavanje gubitka podataka (DLP) pomažu sprječavanju slučajnog ili namjernog slanja osjetljivih podataka neovlaštenim primateljima putem e-pošte. DLP rješenja mogu pratiti odlaznu e-poštu i blokirati ili staviti u karantenu e-poruke koje sadrže osjetljive podatke, poput brojeva kreditnih kartica, socijalnih osiguranja ili intelektualnog vlasništva.

DNS filtriranje

DNS (Domain Name System) filtriranje je tehnika koja blokira ili dopušta pristup određenim web stranicama kontroliranjem razrješavanja naziva domena u IP adrese. Radi na principu interceptiranja DNS upita i provjeravanja traženih naziva domena u odnosu na popis dopuštenih ili zabranjenih stranica. DNS filtriranje nudi nekoliko prednosti:

- Pruža proaktivni obrambeni mehanizam, blokirajući pristup poznatim phishing stranicama,

stranicama za distribuciju zlonamjernog softvera i drugim zlonamjernim mrežnim odredištima.

- Može pomoći u provedbi politika prihvatljive upotrebe (AUP) organizacije blokiranjem pristupa

neprikladnim ili ometajućim web stranicama i osiguravanjem odgovornog i produktivnog korištenja interneta.

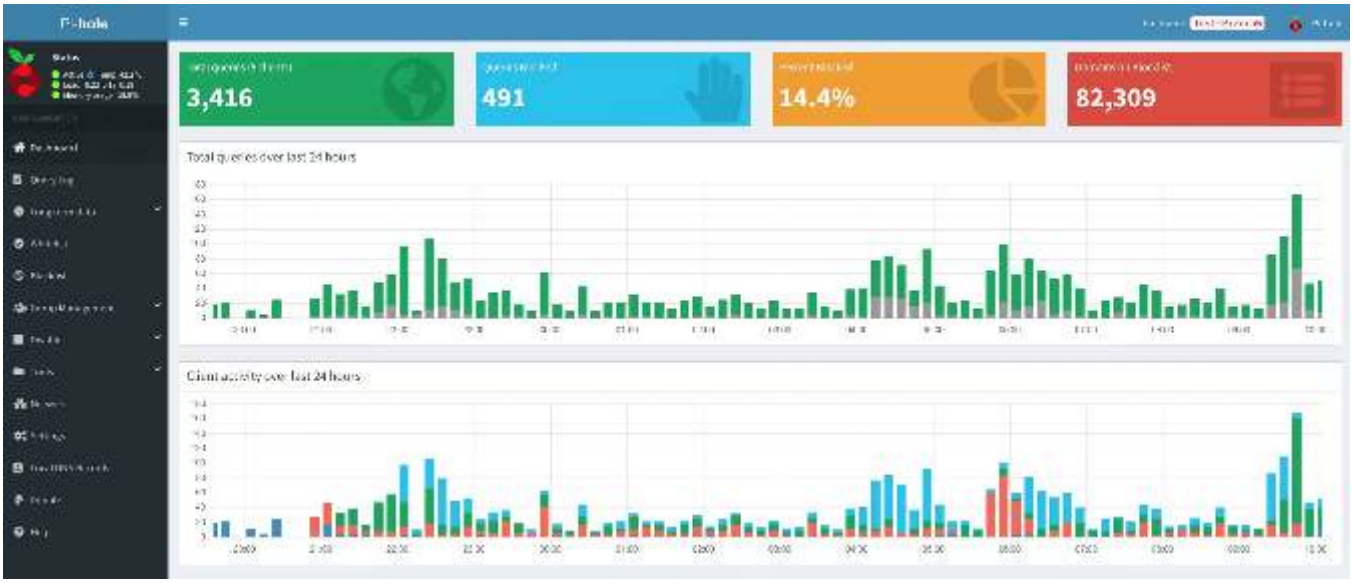
- Može zaštititi sve uređaje spojene na mrežu, uključujući IoT uređaje, pružajući dodatni

sloj sigurnosti.

- Jednostavno je rješenje koje je lako implementirati i predstavlja minimalni rizik, čineći ga

isplativom sigurnosnom kontrolom pogodnom za mreže bilo koje veličine. Iako je DNS filtriranje vrlo učinkovito, mora biti kombinirano s drugim sigurnosnim mjerama za sveobuhvatnu zaštitu. Implementacija DNS filtriranja bez odgovarajuće konfiguracije i održavanja može rezultirati lažnim pozitivima, što blokira pristup legitimnim web stranicama.

Administrativna nadzorna ploča Pi-hole koja prikazuje statistiku DNS razrješavanja.

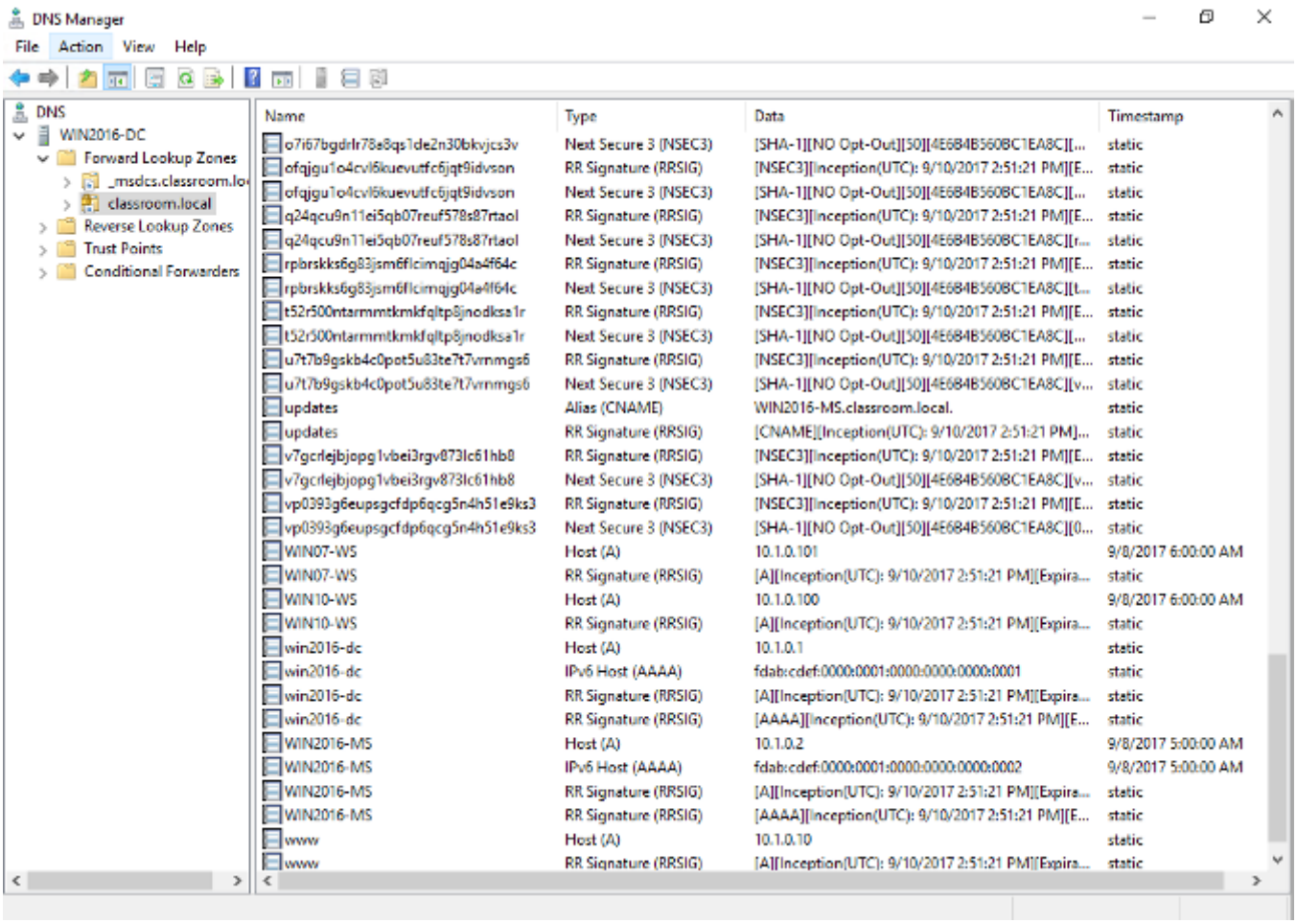


Snimak zaslona ljubaznošću Pi-hole.

DNS sigurnost

DNS je kritična usluga koja bi trebala biti konfigurirana da bude tolerantna na greške. DoS napadi su teško izvedivi protiv servera koji obavljaju razrješavanje internet naziva, ali ako napadač može kompromitirati ili lažirati DNS odgovore, može preusmjeriti korisnike na zlonamjerne web stranice. DNSSEC (Domain Name System Security Extensions) je skup proširenja za DNS protokol koji pruža autentifikaciju DNS podataka. DNSSEC koristi digitalne potpise za verifikaciju autentičnosti DNS zapisa, sprečavajući napade trovanja DNS predmemorije i lažiranja DNS-a.

Windows Server DNS usluge s omogućenim DNSSEC-om.



Snimak zaslona korišten uz dopuštenje Microsofta.

Ključ za potpisivanje ključeva za određenu domenu validira se od strane nadređene domene ili ISP-a hosta. Pouzdanost domene najviše razine validiraju regionalni internetski registri, a DNS root servere osiguravaju organizacije kao što je IANA. Ova hijerarhija povjerenja naziva se lanac povjerenja. DNSSEC sprečava napade čovjeka u sredini gdje bi napadač mogao lažirati DNS odgovore i preusmjeriti korisnike na zlonamjerne web stranice.

Lekcija 11B

Sigurnost u oblaku i koncepti sigurnosti web aplikacija

Pregled lekcije

Sigurnost oblaka i web aplikacija uključuje ojačavanje oblaka, koje jača infrastrukturu oblaka i smanjuje njezinu površinu napada, te sigurnost aplikacija, koja osigurava sigurno dizajniranje, razvoj i implementaciju softvera. Ovo uključuje zaštitu od čestih ranjivosti web aplikacija poput SQL injekcije, cross-site scriptinga (XSS) i nesigurnih izravnih referenci objekata. Sigurnost oblaka uključuje i implementaciju odgovarajuće kontrole pristupa, enkripcije i nadzora za zaštitu podataka i aplikacija u oblaku.

Tehnike sigurnog kodiranja

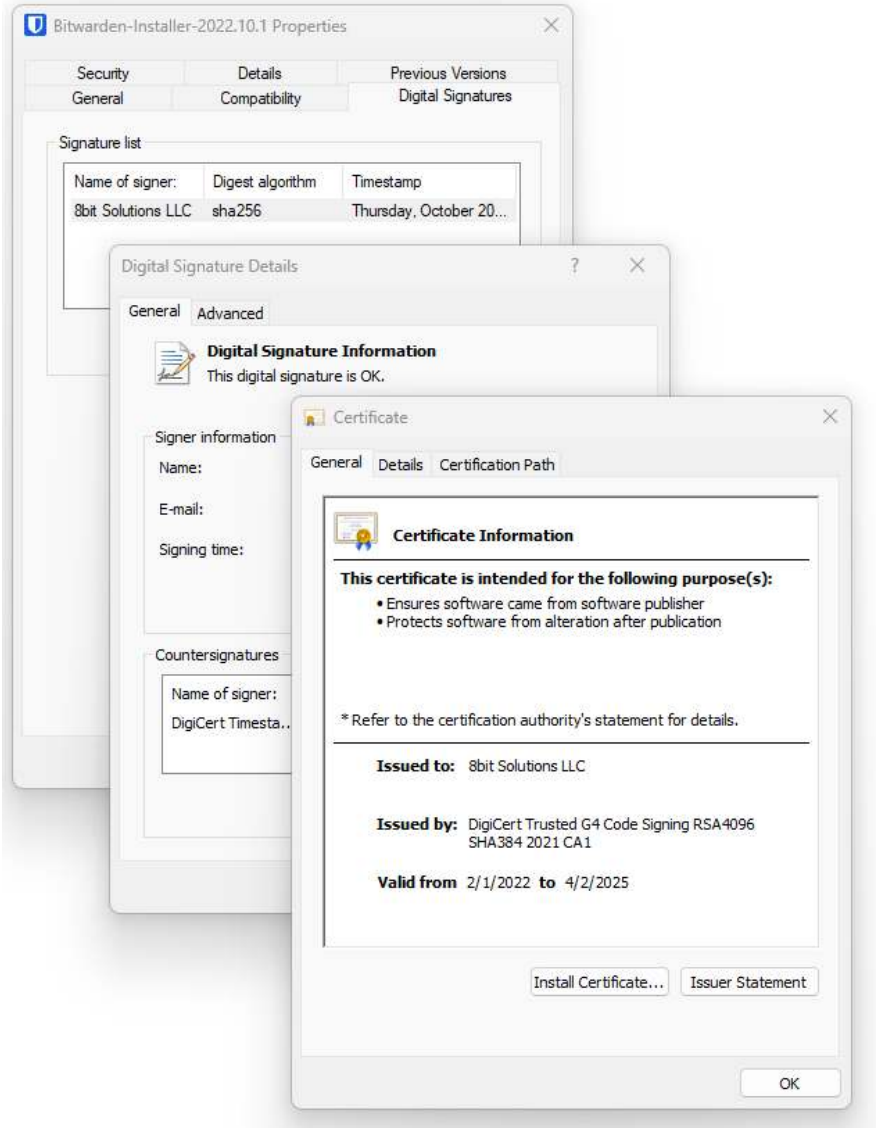
Sigurnosna razmatranja za nove programske tehnologije trebala bi biti dobro razumljena i testirana prije implementacije. Jedan od izazova razvoja aplikacija je taj da programeri koji rade na funkcionalnosti mogu izgubiti iz vida sigurnosne aspekte svog koda. Trening za sigurno kodiranje daje programerima znanje potrebno za pisanje sigurnog koda i razumijevanje uobičajenih ranjivosti web aplikacija. Validacija unosa, kodiranje izlaza, pravilno rukovanje greškama i izbjegavanje izlaganja podataka ključne su prakse sigurnog kodiranja.

OWASP pruža odličan pregled validacije unosa.

Bez učinkovite validacije unosa, aplikacije su ranjive na mnoge različite klase napada injekcijom, poput SQL injekcije, injekcije koda, cross-site scriptinga (XSS) i mnoge druge. Validacija unosa je proces provjere je li unos koji je dostavio korisnik prihvatljiv prije nego što se obradi od strane aplikacije. To uključuje provjeru vrste, duljine, formata i raspona unosa. Kodiranje izlaza je process pretvaranja podataka u format koji nije izvršiv kako bi se spriječili napadi injekcijom.

sigurnosno testiranje (DAST). Prakse kodiranja dizajnirane za podržavanje redovitih zakrpa i ažuriranja ključne su za podršku brzom rješavanju novootkrivenih ranjivosti. Analiza statičkog koda podržava identifikaciju potencijalnih ranjivosti u kodu bez izvršavanja koda. Analiza dinamičkog koda testira aplikacije u izvršnom okruženju, što može otkriti ranjivosti koje statička analiza može propustiti. Kombinacija statičkih i dinamičkih testova pruža sveobuhvatniji pregled sigurnosnog stanja aplikacije.

Pregled digitalnog potpisa sadržanog unutar instalera aplikacije Bitwarden za upravljanje lozinkama.



Zaštite aplikacija

Izlaganje podataka je greška koja dopušta čitanje privilegiranih informacija (poput tokena, lozinke ili osobnih podataka) bez podvrgavanja odgovarajućim kontrolama pristupa. Aplikacije trebaju implementirati principe minimalnih privilegija i potrebe za znanjem kako bi se ograničio pristup osjetljivim podacima samo onima kojima je to potrebno. Enkriptiranje osjetljivih podataka u mirovanju i u prijenosu ključna je mjera zaštite podataka. Aplikacije također trebaju implementirati odgovarajuće rukovanje greškama kako bi se spriječilo otkrivanje osjetljivih informacija o sustavu u porukama o greškama.

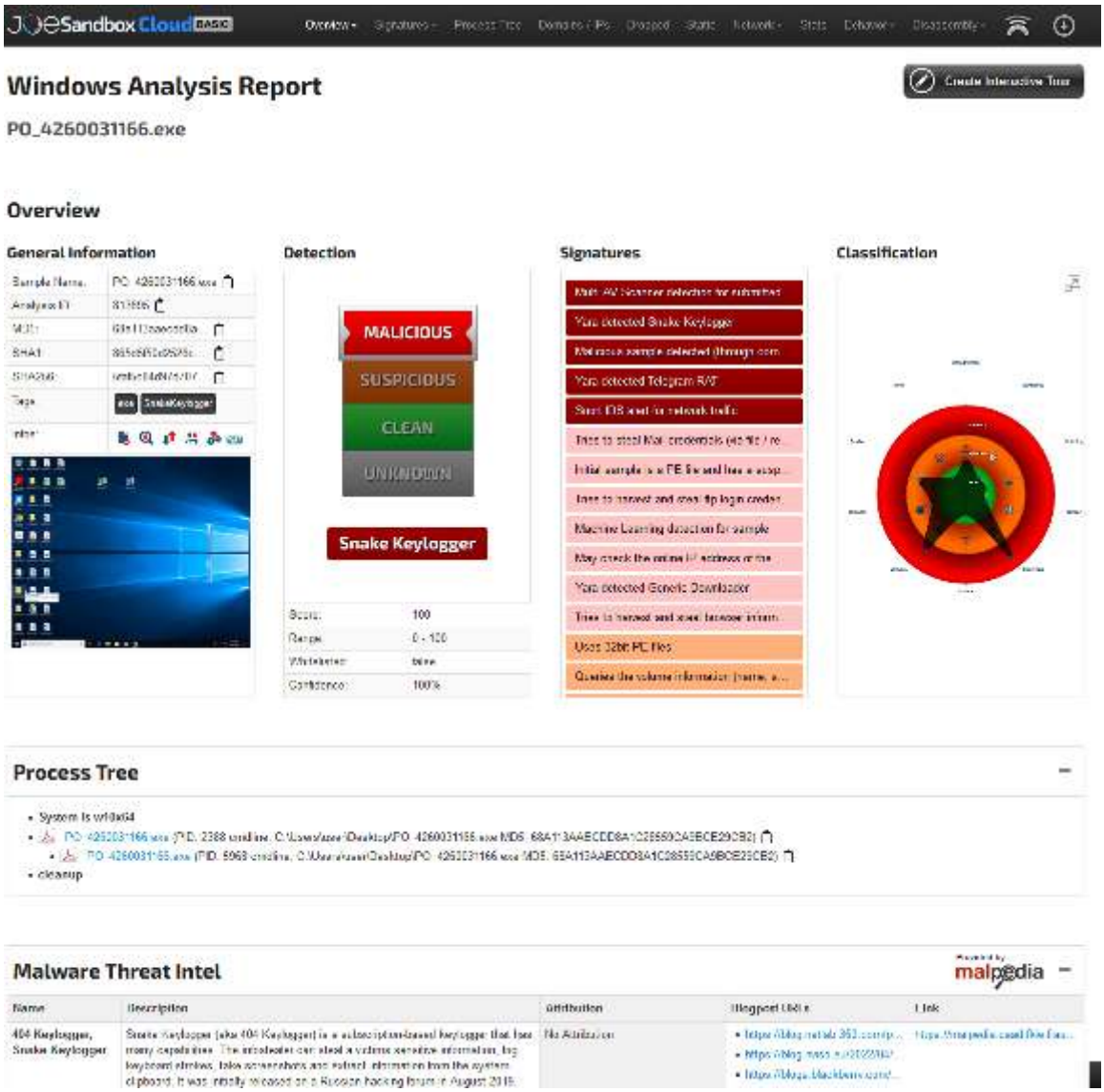
odgovorni za zaštitu infrastrukture, a kupci su odgovorni za zaštitu svojih podataka i aplikacija. Prakse ojačavanja oblaka jačaju infrastrukturu oblaka, smanjujući njezinu površinu napada i poboljšavajući njenu sigurnost. To uključuje implementaciju odgovarajuće kontrole pristupa, enkripcije i nadzora, kao i redovito ocjenjivanje i ažuriranje sigurnosnih konfiguracija oblaka.

Sandboxing softvera

Sandboxing je sigurnosni mehanizam koji se koristi u razvoju i radu softvera za izoliranje procesa koji se izvode jednih od drugih ili sprečavanje pristupa sustavu na kojem se izvode. Sandbox je izolirano okruženje koje ograničava radnje koje program može izvesti i resurse kojima može pristupiti. Sandboxing se može implementirati na razini operativnog sustava, pretraživača ili virtualizacije.

Sandboxing u sigurnosnim operacijama

Alati za sandboxing ključni su u sigurnosnim operacijama i analizi, posebno u otkrivanju i razumijevanju aktivnosti zlonamjernog softvera putem forenzičke inspekcije. Alati za sandboxing mogu izvršiti zlonamjerni kod u izoliranom okruženju i analizirati njegovo ponašanje bez rizika od kompromitiranja produkcijskog sustava. Ovo omogućuje analitičarima sigurnosti identifikaciju zlonamjernih aktivnosti i razvoj učinkovitih odgovora.



Snimak zaslona ljubaznošću Joe Security, LLC.

Sažetak

Trebali biste biti u mogućnosti konfigurirati sigurne protokole za pristup lokalnoj mreži i upravljanje, aplikacijske usluge te udaljeni pristup i upravljanje. Smjernice za poboljšanje sigurnosti aplikacija:

- Procijenite zahtjeve za zaštitu protokola aplikacija, poput potrebe za certifikatima

ili ključevima za autentifikaciju i upotrebu TCP/UDP portova:

- Implementirajte certifikate na web servere za korištenje s HTTPS-om.
- Implementirajte certifikate na mail servere za korištenje sa sigurnim SMTP, POP3 i IMAP.
- Implementirajte certifikate ili host ključeve na datotečne servere za korištenje s FTPS ili SFTP.

Slijedite ove smjernice za poboljšanje projekata razvoja aplikacija:

- Obučite programere o tehnikama sigurnog kodiranja za pružanje specifične zaštite od napada:
- Razumijte različite kategorije napada na web aplikacije koji iskorištavaju ranjivi kod.
- Identificirajte napade injekcijom i mehanizme validacije unosa.

mehanizama.

- Pregledajte i testirajte kod koristeći statičku i dinamičku analizu, obraćajući posebnu pažnju na validaciju

unosa, kodiranje izlaza, rukovanje greškama i izlaganje podataka.

Modul 12

Objasnite koncepte odgovora na incidente i nadzora

Pregled modula

Iz svakodnevne perspektive, odgovor na incidente znači istraživanje upozorenja koja proizvode sustavi za nadzor i problema koje prijavljuju korisnici. Ova aktivnost vodi se politikama i procedurama i podržana je od strane tima za odgovor na incidente koji razumije kako prikupiti i analizirati digitalne dokaze, sadržavati i iskorjenjivati prijetnje te provesti pregled lekcija naučenih.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Sažmite procedure odgovora na incidente i digitalne forenzike.
- Koristite odgovarajuće izvore podataka za istrage incidenata.
- Objasnite koncepte i alate za upozoravanje i nadzor sigurnosti.

Lekcija 12A

Odgovor na incidente

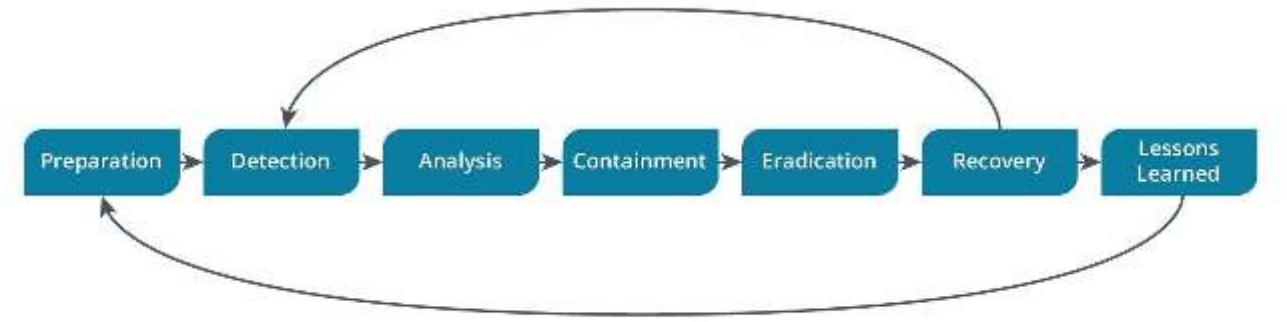
Pregled lekcije

Učinkovit odgovor na incidente vodi se formalnim politikama i procedurama, postavljajući uloge i odgovornosti za tim za odgovor na incidente. Morate razumjeti važnost praćenja ovih procedura i poznavati alate i tehnike koji se koriste za otkrivanje, analizu, sadržavanje i iskorjenjivanje sigurnosnih incidenata.

Procesi odgovora na incidente

Kibernetički sigurnosni incident odnosi se na uspješno ili pokušano kršenje sigurnosnih svojstava imovine, kompromitiranje njezine povjerljivosti, integriteta ili dostupnosti. Odgovor na incidente (IR) je strukturirani pristup upravljanju i ograničavanju posljedica sigurnosnog incidenta. IR proces uobičajeno uključuje sljedeće faze: pripremu, otkrivanje, analizu, sadržavanje, iskorjenjivanje, oporavak i lekcije naučene.

napada. Proces odgovora može morati prolaziti kroz više faza identifikacije, sadržavanja, iskorjenjivanja i oporavka kako bi se postiglo potpuno rješenje. 7. Lekcije naučene — analizira incident kako bi se razumio temeljni uzrok, jesu li primijenjene kontrole bile učinkovite i kako spriječiti slične incidente u budućnosti.



IR proces fokusiran je na kibernetičke sigurnosne incidente. Postoje i veliki incidenti koji predstavljaju egzistencijalnu prijetnju operacijama cijele tvrtke. Ovi veliki incidenti

obrađuju se planom za oporavak od katastrofe (DRP) i planom kontinuiteta poslovanja (BCP). Alati koji se koriste u IR-u uključuju:

- Alati za otkrivanje incidenata pružaju vidljivost u okruženje potpunom ili djelomičnom automatizacijom

prikupljanja i analize mrežnog prometa, nadzora stanja sustava i podataka dnevnika.

- Alati digitalne forenzike olakšavaju prikupljanje i validaciju podataka iz memorije sustava i datotečnih

sustava. To se može izvesti samo za pomoć u odgovoru na incidente ili za kazneni progon prijetnje.

- Alati za upravljanje slučajevima pružaju bazu podataka za bilježenje detalja incidenta i koordiniranje

aktivnosti odgovora u timu respondenata. Ova funkcionalnost često je implementirana kao jedinstveni paket proizvoda. Alati poput upravljanja sigurnosnim informacijama i događajima (SIEM) i sigurnosne orkestracije, automatizacije i odgovora (SOAR) su primjeri alata za upravljanje slučajevima.

postaviti, tim mora voditi viši izvršni donositelj odluka koji može odobriti akcije nakon najozbiljnijih incidenata. Menadžeri osiguravaju svakodnevno funkcioniranje CIRT-a i koordiniraju responze. Ostali stručnjaci koji bi mogli biti potrebni uključuju:

- Pravni — procjenjuje odgovor na incidente s perspektive usklađenosti sa zakonima i

industrijskim propisima. Također može biti potrebno usko surađivati s profesionalcima za provedbu zakona, što može biti zastrašujuće bez stručnog pravnog savjeta.

- Ljudski resursi (HR) — bavi se učincima na ugovore zaposlenika, radno pravo itd.

HR može pomoći u rješavanju temeljnih organizacijskih ili personalnih pitanja koja doprinose incidentu, poput nezadovoljstva zaposlenika, sukoba na radnom mjestu ili neadekvatne obuke.

- Odnosi s javnošću — upravlja negativnim tiskom i/ili reakcijama i komentarima na društvenim mrežama

od ozbiljnog incidenta. Neke organizacije mogu preferirati outsourcing nekih funkcija CIRT-a trećim agencijama zadržavanjem pružatelja odgovora na incidente. Vanjski agenti sposobni su se učinkovitije nositi s određenim vrstama incidenata.

Otkrivanje

Otkrivanje je proces koreliranja događaja iz mrežnih i sistemskih izvora podataka i utvrđivanja jesu li pokazatelji incidenta. Postoje višestruki kanali kojima se pokazatelji mogu identificirati:

- Usklađivanje događaja u datotekama dnevnika, porukama o greškama, upozorenjima IDS-a, upozorenjima vatrozida i drugim izvorima

podataka s uzorkom poznatog ponašanja prijetnji.

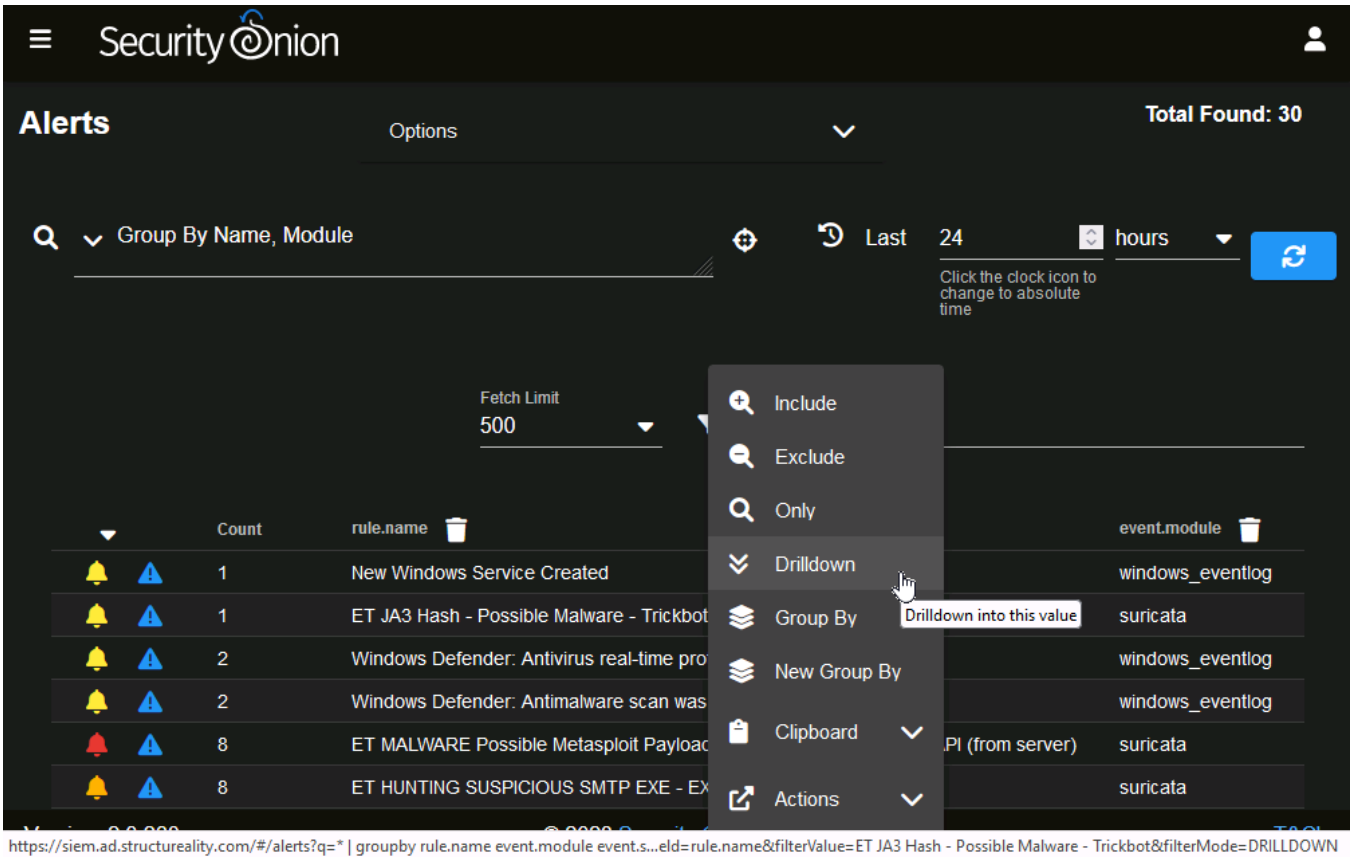
- Identifikacija odstupanja od metrika referentnog sustava.
- Ručno ili fizičko inspekciranje lokacije, prostora, mreža i hostova. Pokretanje

proaktivne pretrage za znakovima upada naziva se lovom na prijetnje.

- Obavještavanje od strane zaposlenika, kupca ili dobavljača.

- Javno izvješćivanje novih ranjivosti ili prijetnji od strane prodavatelja sustava, regulatora, medija ili

druge vanjske strane. Mudro je pružiti mogućnost povjerljivog izvješćivanja kako zaposlenici ne bi bojali prijaviti unutarnje prijetnje poput prijevare ili nepravilnog ponašanja. Kada se otkrije sumnjivi događaj, treba ga prijaviti timu za odgovor na incidente.



Snimak zaslona ljubaznošću Security Onion securityonion.net.

Analiza

Nakon što proces otkrivanja prijavi jedan ili više pokazatelja, u procesu analize, prvi responder istražuje podatke kako bi utvrdio je li identificiran pravi incident i prirodu te ozbiljnost incidenta.

Kada je incident verificiran kao istiniti pozitiv, sljedeći cilj je identificirati vrstu incidenta i zahvaćene podatke ili resurse. To uspostavlja kategoriju incidenta i utjecaj te omogućuje timu za odgovor da prioritizira odgovor. Čimbenici koji utječu na prioritizaciju incidenta uključuju:

- Integritet podataka — najvažniji čimbenik u prioritiziranju incidenata često će biti vrijednost

podataka koji su u opasnosti.

- Zastoj — je mjera u kojoj incident ometa poslovne procese, drugi

vrlo važan čimbenik. Incident može ili degradirati (smanjiti performanse) ili prekinuti (potpuno zaustaviti) dostupnost imovine, sustava ili poslovnog procesa.

- Ekonomski/publicitarni — i integritet podataka i zastoj imaju važne ekonomske učinke

kratkoročno i dugoročno. Kratkoročni troškovi uključuju odgovor na incidente i izgubljene poslovne prilike. Dugoročni ekonomski troškovi mogu uključivati štetu reputaciji i tržišnom položaju.

- Opseg — (općenito broj zahvaćenih sustava) nije izravni pokazatelj prioriteta. Velik

broj sustava može biti zaražen vrstom zlonamjernog softvera koji degradira performanse, ali nije rizik kršenja podataka. Ovo može čak biti i maskirajući napad dok protivnik nastoji kompromitirati podatke na određenom sustavu.

- Vrijeme otkrivanja — istraživanja su pokazala da više od polovice kršenja podataka nije otkriveno

tjednima ili mjesecima nakon što se upd dogodio, dok se u uspješnom upadu podaci obično krše u minutama. Sustavi koji se koriste za pretraživanje upada moraju biti temeljiti, a odgovor na otkrivanje brz.

- Vrijeme oporavka — neki incidenti zahtijevaju dugotrajno saniranje jer su potrebne promjene sustava

složene za implementaciju. Ovaj produljeni period oporavka trebao bi pokrenuti pojačanu budnost za kontinuirane ili nove napade. Kategorija — Kategorije incidenata i definicije osiguravaju da svi članovi tima za odgovor

Faze u lancu ubojstava (kill chain).

Knjige pravila (Playbooks)

CIRT bi trebao razviti profile ili scenarije tipičnih incidenata, poput DDoS napada, epidemija virusa/crva, exfiltracije podataka od strane vanjskog protivnika, izmjene podataka od strane internog protivnika i tako dalje. Tim zatim može razviti plan odgovora na incidente (IRP) i knjige pravila za svaki scenarij. Knjiga pravila dokumentira korake za otkrivanje, analizu, sadržavanje i iskorjenjivanje za određeni tip incidenta.

Sadržavanje

Nakon otkrivanja i analize, baza podataka upravljanja incidentima trebala bi imati zapis o pokazateljima događaja, prirodi incidenta, njegovom utjecaju i istražitelju odgovornom za

Jednostavna mogućnost je odspajanje hosta s mreže izvlačenjem mrežnog kabela (stvaranjem zračnog razmaka) ili onemogućavanjem jego switcha. Ovo je opcija s najmanje prikrivanja i smanjit će prilike za forenzičku analizu live sustava. Segmentacija je alternativna strategija koja ograničava sposobnost napadača da se lateralno kreće unutar mreže izoliranjem zahvaćenih segmenata od ostatka mreže.

Iskorjenjivanje i oporavak

Nakon što je incident sadržan, proces iskorjenjivanja primjenjuje tehnike smanjenja i kontrole za uklanjanje alata za upade i neovlaštenih promjena konfiguracije iz zahvaćenih sustava. Cilj je vraćanje sustava u poznato dobro stanje. Oporavak uključuje vraćanje zahvaćenih sustava u normalnu operaciju.

Ako reinstalirate iz referentnih konfiguracija predložaka ili slika, provjerite nema li u referentnom stanju ništa što je dopustilo nastanak incidenta! Ako da, ažurirajte predložak prije nego ga ponovo implementirate.

Ako je organizacija podvrgnuta ciljanom napadu, imajte na umu da jedan incident može biti praćen brzim sljedećim.

3. Osigurajte da zahvaćene strane budu obaviještene i opremljene sredstvima za saniranje vlastitih sustava. Na primjer, ako su ukradene lozinke kupaca, trebaju biti savjetovani da promijene vjerodajnice.

Lekcije naučene

Proces lekcija naučenih pregledava ozbiljne sigurnosne incidente kako bi odredio njihov temeljni uzrok, jesu li bili izbjegljivi i kako ih izbjeći u budućnosti. Aktivnosti lekcija naučenih trebale bi biti provedene što je moguće brže nakon rješenja incidenta dok je iskustvo još svježe. Primjer analize lekcija naučenih:

- Zašto je baza podataka o sigurnosti pacijenata pronađena na tamnoj mreži? Jer je prijetnja bila u mogućnosti

kopirati je na USB i izaći iz zgrade s njom.

- Zašto je prijetnja bila u mogućnosti kopirati bazu podataka na USB ili to učiniti bez generiranja

upozorenja? Jer su bili u mogućnosti onemogućiti sustav za sprječavanje gubitka podataka.

- Zašto su bili u mogućnosti onemogućiti sustav za sprječavanje gubitka podataka? Jer su imali

povjerene privilegije za to.

- Zašto su im dodijeljene ove privilegije? Nitko ne zna... svim administratorskim

računima su dodjeljene.

- Zašto akt onemogućavanja sustava za sprječavanje gubitka podataka nije generirao upozorenje? Bio je

zabilježen, ali upozorenja za tu kategoriju su bila onemogućena zbog previše lažnih pozitiva. Ovo identificira dva temeljna uzroka kao neispravna dodjela ovlasti i neispravna konfiguracija zapisivanja/upozoravanja.

- Tko je bio protivnik? Je li incident bio vođen iznutra, izvana ili kombinacijom?
- Zašto je incident počinjen? Raspravite motive protivnika i imovinu podataka

na koji su mogli ciljati.

- Kada se incident dogodio, kada je otkriven i koliko je trebalo da se sadrži i

iskorijeni?

- Gdje se incident dogodio (zahvaćeni sustavi hosta i mrežni segmenti)?
- Kako se incident dogodio? Koje taktike, tehnike i procedure (TTPs) su

koristio protivnik? Jesu li TTPs bili poznati i dokumentirani u bazi znanja poput ATT&CK, ili su bili jedinstveni?

- Koje bi sigurnosne kontrole pružile bolju zaštitu ili poboljšale odgovor?

Drugi pristup mogao bi biti prolazak kroz vremensku liniju incidenta kako bi se razumjelo što je bilo poznato, razmišljanje za svaku odluku i koje opcije ili kontrole mogle biti korisnije za tim za odgovor.

Testiranje i obuka

Testiranje i obuka validiraju proces pripreme i pokazuju da je organizacija u cjelini spremna izvesti odgovor na incidente. Nasuprot tome, lekcije naučene mogu pokazati da je obuka bila neadekvatna. Razne vrste testiranja i obuke su dostupne:

- Stolna vježba — ovo je najmanje skup tip testiranja. Voditelj predstavlja scenarij,

a respondenti objašnjavaju kakvu bi akciju poduzeli za identifikaciju, sadržavanje i iskorjenjivanje prijetnje. Obuka ne koristi računalne sustave. Podaci scenarija prezentiraju se kao flash kartice.

- Propust — u ovom modelu voditelj predstavlja scenarij kao za stolnu vježbu,

ali respondenti demonstriraju koje bi akcije poduzeli kao odgovor. Za razliku od stolne vježbe, respondenti izvode radnje poput pokretanja skeniranja i analize uzornih datoteka, obično u laboratorijskom okruženju.

- Simulacije — simulacija je timska vježba gdje crveni tim pokušava

upad, plavi tim upravlja kontrolama odgovora i oporavka, a bijeli tim moderira i procjenjuje vježbu. Ova vrsta obuke zahtijeva znatno ulaganje i planiranje. Članovi

Fotografija Kentucky National Guard Maj. Carle Raisler.

Obuka

Akcije osoblja neposredno nakon otkrivanja incidenta mogu imati kritičan utjecaj na uspješne ishode. Učinkovita obuka o postupcima otkrivanja i izvješćivanja incidenata oprema osoblje da prepozna potencijalne incidente i odgovori na odgovarajući način. Obuka bi trebala pokriti kako prepoznati znakove kompromitiranja, kako prijaviti sumnjive aktivnosti i koje su odgovornosti svakog tima.

Lov na prijetnje

Lov na prijetnje koristi uvide dobivene iz obavještajnih podataka o prijetnjama za proaktivno otkrivanje ima li dokaza da su TTPs već prisutni unutar mreže ili sustava. Ovo je za razliku od pasivnog nadzora koji čeka na upozorenja. Lov na prijetnje može biti vođen:

- Savjetima i biltenima koji upozoravaju na nove vrste prijetnji — lov na prijetnje je radno intenzivna

aktivnost i stoga treba biti provedena s jasnim ciljevima i resursima. Lov na prijetnje obično napreduje prema nekoj hipotezi moguće prijetnje. Sigurnosni bilteni i savjetnici prodavatelja i agencija za obavještajne podatke o prijetnjama pružaju polazišnu točku.

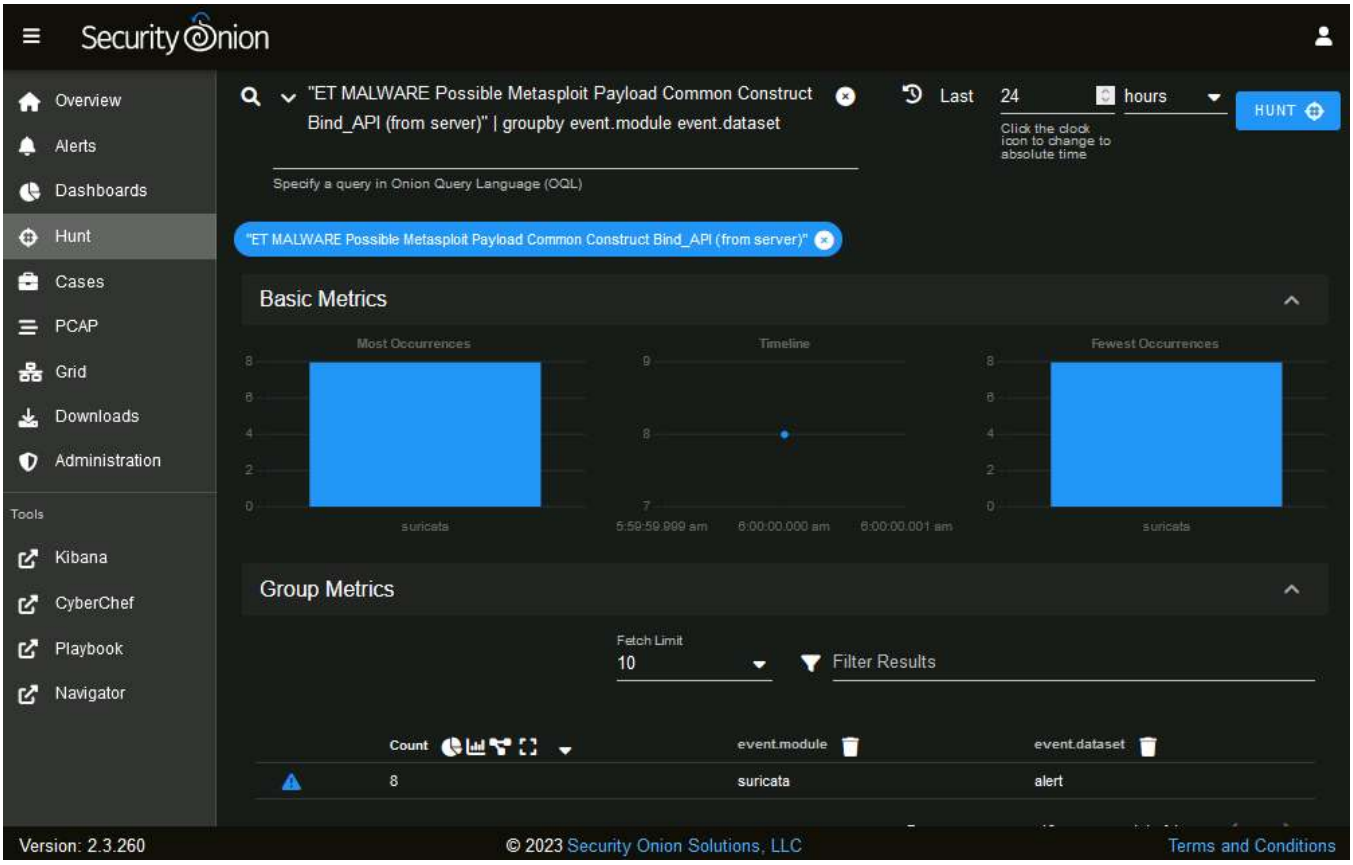
- Fuzija obavještajnih podataka i podaci o prijetnjama — lov na prijetnje može biti proveden ručnom analizom

mrežnih i log podataka, ali ovo je vrlo dugotrajan proces. Organizacija sa SIEM-om i platformom za analitiku prijetnji može primijeniti tehnike fuzije obavještajnih podataka za automatizaciju aspekta lova na prijetnje.

- Manevar — kada istražujete sumnjivo aktivnu prijetnju, morate se sjetiti protivničke

prirode hakiranja. Sposoban prijetnja vjerojatno je anticipirao vjerojatnost lova na prijetnje i pokušao implementirati protumjere za frustriranje otkrivanja. Na primjer, napadač može koristiti legalne alate i usluge za maskiranje zlonamjernih aktivnosti.

Hunt nadzorne ploče u Security Onion mogu pomoći u utvrđivanju utječe li određeno upozorenje samo na jedan sustav (kao ovdje) ili je rasprostranjenije po mreži.



Snimak zaslona ljubaznošću Security Onion securityonion.net.

Lekcija 12B

Digitalna forenzika

Pregled lekcije

Digitalna forenzička analiza uključuje ispitivanje dokaza prikupljenih s računalnih sustava i mreža kako bi se otkrile relevantne informacije, poput izbrisanih datoteka, vremenskih oznaka, korisničke aktivnosti i neovlaštenih transakcija. Forenzički analitičari moraju slijediti stroge procedure kako bi osigurali da su dokazi prikupljeni, sačuvani i analizirani na način koji je prihvatljiv na sudu.

Pravni postupak i pravno zadržavanje

Digitalna forenzika je praksa prikupljanja dokaza s računalnih sustava na standard koji će biti prihvaćen na sudu. Forenzičke istrage su najčešće provedene kada postoji sumnja na kriminalne aktivnosti, kao što su korporativna špijunaža, prijevara ili povrede podataka. Pravni postupak zahtijeva da se dokazi prikupe, sačuvaju i analiziraju na način koji je prihvatljiv na sudu. To znači da analitičar mora biti u mogućnosti pokazati da su dokazi autentični i da nisu bili neovlašteno izmijenjeni.

Pravno zadržavanje odnosi se na činjenicu da informacije koje mogu biti relevantne za sudski slučaj moraju biti sačuvane. Informacije podložne pravnom zadržavanju mogu biti definirane regulatorima ili industrijom, ili nalogom suda. Informacije podložne pravnom zadržavanju trebaju biti identificirane, zaštićene od izmjena i dostupne za pregled.

Prikupljanje

Prikupljanje je proces dobivanja forenzički čiste kopije podataka s uređaja zaplijenjenog kao dokaz. Ako računalni sustav ili uređaj nije u vlasništvu organizacije, postoji pravno pitanje ima li organizacija ovlast za preuzimanje podataka. Redoslijed hlapljivosti opisuje koji su podaci najprije podložni gubitku ako se uređaj isključi ili isklopi:

- Particije i blokovi datotečnog sustava, slobodan prostor.
- Predmemorije sistemske memorije, poput swap prostora/virtualne memorije i hibernacijskih datoteka.
- Privremene predmemorije datoteka, poput predmemorije preglednika.

- Korisnički

4. Podaci udaljenog zapisivanja i nadzora. 5. Fizička konfiguracija i mrežna topologija. 6. Arhivski mediji i tiskani dokumenti. Windows registar je uglavnom pohranjen na disku, ali postoje ključevi — posebno HKLM\SYSTEM i HKLM\SOFTWARE — koji su također dostupni u memoriji.

Prikupljanje sistemske memorije

Sistemska memorija su hlapljivi podaci koji se drže u modulima Random Access Memory (RAM). Hlapljiv znači da se podaci gube kada se ukloni napajanje. Ispis sistemske memorije stvara sliku sadržaja RAM-a.

Pregledavanje popisa procesa u ispisu memorije korištenjem Volatility frameworka.

```
c:\Users\James\Downloads>volatility_2.6_win64_standalone.exe -f c:\dumps\memory.dmp --profile=Win7SP1x64_23418 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----
0xfffffa83020a7040 System                    4      0    106      632 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa8303d6d1d0 smss.exe                308      4      2       29 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa83035f26a0 csrss.exe               396    388      8      370      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83034fe060 wininit.exe             432    388      3       75      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036295e0 csrss.exe               444    424      8      293      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303716b30 winlogon.exe            492    424      3      109      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83035fab30 services.exe            528    432     10      276      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303732b30 lsass.exe               536    432      8      636      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa830373db30 lsm.exe                 544    432     10      142      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037436a0 svchost.exe             652    528     10      349      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037e66a0 svchost.exe             716    528      7      235      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036566a0 svchost.exe             772    528     18      445      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83038bb060 svchost.exe             892    528     18      417      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83038fcb30 svchost.exe             936    528     32      940      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa830393c060 svchost.exe             324    528     17      385      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303960060 svchost.exe             744    528     15      379      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039b7060 spoolsv.exe            1060    528     12      271      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039dd060 svchost.exe            1096    528     19      316      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a58960 vmicsvc.exe            1192    528      5      126      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a70b30 vmicsvc.exe            1216    528      7      217      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a8c060 vmicsvc.exe            1264    528      4       78      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303accb30 vmicsvc.exe            1296    528      5       92      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303b32920 vmicsvc.exe            1340    528      3       82      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8302ab3210 svchost.exe            1436    528     10      179      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8303bcf800 svchost.exe            1528    528      3       43      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303c963a0 svchost.exe            1816    528      5       99      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303ac5b30 svchost.exe            1976    528     14      323      0      0 2020-01-09 21:20:10 UTC+0000
0xfffffa8303155b30 taskhost.exe           1964    528      9      157      1      0 2020-01-09 21:20:14 UTC+0000
0xfffffa83031c3830 sppsvc.exe             2072    528      7      158      0      0 2020-01-09 21:20:14 UTC+0000
0xfffffa8303262060 dwm.exe                2352    892      3       70      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa8303238060 explorer.exe           2376   2344     24      784      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa83033a2b30 jusched.exe            2520   2456      8      233      1      1 2020-01-09 21:20:18 UTC+0000
0xfffffa8303ba0b30 SearchIndexer.         2568    528     11      656      0      0 2020-01-09 21:20:24 UTC+0000
0xfffffa830326a060 procexp64.exe          2900   2376      8      382      1      0 2020-01-09 21:20:45 UTC+0000
0xfffffa83036406a0 WmiPrvSE.exe           3024    652      7      118      0      0 2020-01-09 21:20:51 UTC+0000
0xfffffa8303703190 Tcpview.exe             916   2376      6      139      1      1 2020-01-09 21:21:27 UTC+0000
0xfffffa8302839b30 salter.exe             1808   2376      6      134      1      1 2020-01-09 21:23:49 UTC+0000
0xfffffa8303818230 WMIADAP.exe             380    936      5       85      0      0 2020-01-09 21:24:08 UTC+0000
```

Snimak zaslona Volatility framework volatilityfoundation.org.

Specijalizirani hardverski ili softverski alat može snimiti sadržaj memorije dok host radi. Nažalost, ova vrsta alata mora biti unaprijed instalirana jer zahtijeva upravljački program u kernel modu za izravno kopiranje memorije. Hvatanje memorijskog ispisa nakon incidenta otežano je ako alati nisu bili prethodno postavljeni.

Prikupljanje disk slike

Prikupljanje disk slike odnosi se na prikupljanje podataka iz nehlapljive pohrane. Nehlapljiva pohrana uključuje hard disk pogone (HDD), solid state pogone (SSD), firmware i druge vrste medija koji zadržavaju podatke nakon isključivanja napajanja. Postoje dva pristupa:

- Živuće prikupljanje — ovo znači kopiranje podataka dok host još radi. To može

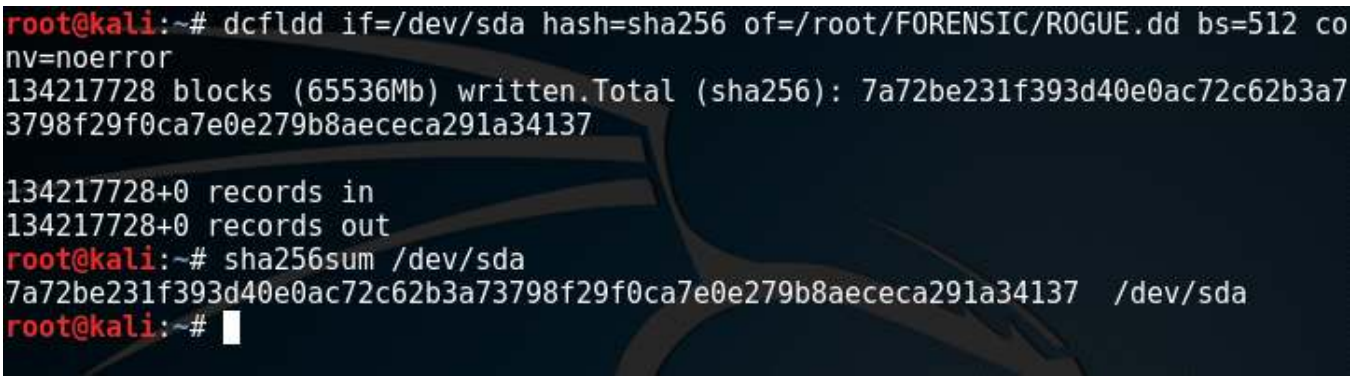
snimiti više dokaza ili više podataka za analizu i smanjiti utjecaj na ukupne usluge, ali podaci na stvarnim diskovima su se promijenili, pa ova metoda možda neće proizvesti pravno prihvatljive dokaze.

- Statičko prikupljanje isključivanjem hosta — ovo nosi rizik da će zlonamjerni softver otkriti

proces isključivanja i izvesti anti-forenziku pokušavajući ukloniti tragove o sebi.

- Statičko prikupljanje izvlačenjem napajanja — ovo znači isključivanje napajanja na zidnoj utičnici

(ne gumb za isključivanje hardvera). Ovo je najvjerojatnije da će sačuvati uređaje za pohranu u forenzički čistom stanju, ali postoji rizik od oštećenja podataka. S dovoljno vremena na licu mjesta, analitičar može koristiti specijalizirani forenzički softver za stvaranje točne bit-po-bit kopije medija pohrane.



Čuvanje

Ključno je da dokazi prikupljeni na mjestu zločina odgovaraju valjanoj vremenskoj liniji. Digitalne informacije podložne su neovlaštenim izmjenama, pa stoga pristup dokazima mora biti strogo kontroliran. Lanac skrbništva dokumentira tko je imao pristup dokazima i kada. Forenzički analitičari trebaju koristiti hash vrijednosti za verifikaciju integriteta digitalnih dokaza i osigurati da nisu bili neovlašteno izmijenjeni.

Ovaj dokaz integriteta osigurava neporicanje. Ako je podrijetlo dokaza sigurno, prijetnja identificirana analizom dokaza ne može zanijekati svoja djelovanja. Hash vrijednosti dokazuju da dokazi nisu bili neovlašteno izmijenjeni od prikupljanja.

Izvješćivanje

Digitalno forenzičko izvješćivanje sažima značajne sadržaje digitalnih podataka i zaključke iz analize istražitelja. Važno je napomenuti da jaki etički principi upravljaju digitalnom forenzičkom praksom:

- Analiza mora biti provedena bez pristranosti. Zaključci i mišljenja trebaju se formirati samo

iz izravnih dokaza koji se analiziraju.

- Metode analize moraju biti ponovljive od strane trećih strana s pristupom istim dokazima.
- Idealno, dokazi ne smiju biti mijenjani ili manipulirani. Ako uređaj korišten kao dokaz

mora biti manipuliran radi olakšavanja analize (onemogućavanje funkcije zaključavanja mobilnog telefona ili sprečavanje udaljenog brisanja, na primjer), razlozi za to moraju biti

valjani i proces mora biti dokumentiran.

- Identificirajte i deduplicirajte datoteke i metapodatke — mnoge datoteke na računalnom sustavu su

"standardne" instalirane datoteke ili kopije iste datoteke. E-otkrivanje filtrira ove vrste datoteka, smanjujući količinu podataka koje se moraju analizirati.

- Pretraživanje — omogućava istražiteljima lociranje datoteka od interesa za slučaj. Uz ključne

riječi, softver može podržavati semantičko pretraživanje. Semantičko pretraživanje poklapa ključne riječi ako odgovaraju određenom kontekstu.

- Oznake — primjenjuju standardizirane ključne riječi ili naljepnice na datoteke i metapodatke za organiziranje

dokaza. Oznake bi se mogle koristiti za označavanje relevantnosti slučaju ili dijelu slučaja ili za prikaz povjerljivosti.

- Sigurnost — u svim točkama, mora se pokazati da su dokazi pohranjeni, prenijeti i

analizirani bez neovlaštenih izmjena.

- Otkrivanje — važan dio sudskog postupka je da isti dokazi budu dostupni

i tužitelju i tuženiku. E-otkrivanje može ispuniti ovaj zahtjev. Nedavni sudski slučajevi zahtijevali su da strane u sudskom slučaju dostave pretražive elektronički pohraniti informacije (ESI) umjesto papirnate dokumentacije.

Lekcija 12C

Izvori podataka

Pregled lekcije

Mreže, hostovi i aplikacije proizvode veliku količinu podataka putem različitih mehanizama. Identificiranje svih ovih izvora podataka, a zatim pretraživanje indikatora prijetnji u njima, značajan je izazov. Alati poput SIEM-a pomažu u automatizaciji ovog procesa agregiranjem i koreliranjem podataka iz više izvora.

Izvori podataka, nadzorne ploče i izvješća

U kontekstu slučaja odgovora na incidente ili istrage digitalne forenzike, izvor podataka je nešto što može biti podvrgnuto analizi za otkrivanje indikatora kompromitiranja ili prijetnje. Primjeri uključuju:

- Podaci i metapodaci datotečnog sustava sistemske memorije i medijskog uređaja.
- Datoteke dnevnika koje generiraju mrežni uređaji (preklopnici, usmjernici i vatrozidi/UTM).
- Mrežni promet snimljen senzorima i/ili sva upozorenja koja generiraju

sustavi za otkrivanje upada.

- Datoteke dnevnika i upozorenja koja generiraju mrežni skeneri ranjivosti.
- Datoteke dnevnika koje generiraju OS komponente klijentskih i serverskih računala.
- Datoteke dnevnika koje generiraju aplikacije i usluge,

uključujući sigurnosni softver baziran na hostu kao što su otkrivanje upada, skeniranje ranjivosti, antivirus i sigurnosni softver vatrozida. Ogromna raznolikost i veličina izvora podataka značajan je problem za istrage. Organizacije trebaju implementirati rješenja za upravljanje tim podatkovnim tokovima.

Nadzorne ploče

Nadzorna ploča događaja pruža konzolu za svakodnevni odgovor na incidente. Pruža sažetak informacija izvučenih iz temeljnih izvora podataka za podržavanje nekog radnog zadatka. Zasebne nadzorne ploče mogu biti konfigurirane za različite uloge i funkcije.

Snimak zaslona ljubaznošću Security Onion securityonion.net.

Automatska izvješća

SIEM se može koristiti za dvije vrste izvješćivanja:

- Upozorenja i alarmi otkrivaju prisutnost indikatora prijetnji u podacima i mogu se koristiti za

pokretanje slučajeva incidenta. Svakodnevno upravljanje izvješćivanjem o upozorenjima čini velik dio radnog opterećenja analitičara.

- Izvješća o statusu komuniciraju podatke o razini prijetnje ili broju incidenata koji se

pokrenuti i učinkovitost sigurnosnih kontrola i procedura odgovora. Ova vrsta izvješćivanja može se koristiti za informiranje upravljačkih odluka. Može biti potrebna i za usklađenost izvješćivanja. SIEM može planirati automatsko generiranje i dostavu ovih izvješća.

Log podaci

Podaci dnevnika kritični su resurs za istraživanje sigurnosnih incidenata. Osim formata dnevnika, morate razmotriti i raspon izvora za datoteke dnevnika te znati kako odrediti kakvu vrstu informacija svaki izvor pruža. Svaki zapis dnevnika obično ima dvije komponente:

- Podaci poruke događaja su specifična obavijest ili upozorenje koje pokreće proces, poput "Neuspjeh prijave"

ili "Vatrozid je odbio promet".

- Metapodaci događaja su izvor i vrijeme događaja. Izvor može uključivati host ili

mrežnu adresu, naziv procesa te polja kategorizacije/prioriteta. Točno zapisivanje zahtijeva da svaki host bude sinkroniziran na isti datum i vrijednost i format vremena. Idealno, svaki host bi trebao referencirati isti izvor vremena.

- PRI kod se izračunava iz objekta i razine ozbiljnosti.
- Zaglavlje sadrži vremensku oznaku, naziv hosta, naziv aplikacije, ID procesa i polja ID-a poruke.
- Dio poruke sadrži oznaku koja prikazuje

sadržaja koji ovisi o aplikaciji. Može koristiti polja odvojena razmacima ili zarezima ili parove ime/vrijednost. Log podaci mogu biti sačuvani i analizirani na svakom hostu pojedinačno, ali većina organizacija zahtijeva centralizaciju.

Log operativnog sustava hosta

Operativni sustav (OS) vodi razne dnevnike za bilježenje događaja dok korisnici i softver komuniciraju sa sustavom. Različite datoteke dnevnika predstavljaju različite aspekte funkcije sustava:

- Događaji autentifikacije bilježe kada korisnici pokušavaju prijaviti se i odjaviti. Događaj je vjerojatno i biti

generiran kada korisnik pokuša dobiti posebne ili administratorske privilegije.

- Događaji datotečnog sustava bilježe je li upotreba dozvola za čitanje ili izmjenu datoteke bila dopuštena ili

odbijena. Budući da bi ovo generiralo ogromnu količinu podataka ako je omogućeno za sve objekte datotečnog sustava prema zadanim postavkama, revizija datotečnog sustava obično treba biti eksplicitno konfigurirana. Windows dnevnici — Tri glavna Windows

- Aplikacija — događaji koje generiraju procesi aplikacija, poput pada ili

kada je aplikacija instalirana ili uklonjena.

- Sigurnost — revizijski događaji, poput neuspjele prijave ili uskraćenog pristupa datoteci.
- Sustav — događaji koje generiraju kernel procesi i usluge operativnog sustava, poput

kada usluga ili upravljački program ne može pokrenuti, kada je promijenjen tip pokretanja usluge ili kada se računalo isključuje. Linux dnevnici — Zapisivanje u Linuxu može biti implementirano različito za svaku distribuciju. Neke distribucije koriste sustavni daemon za bilježenje, a neke koriste stariji syslog daemon.

- /var/log/syslog ili /var/log/messages pohranjuje sve događaje koje generira sustav.

Neki od njih kopiraju se u pojedinačne datoteke dnevnika. /var/log/auth.log/var/log/secure

- (Debian/Ubuntu) ili (RedHat/CentOS/Fedora)

bilježi pokušaje prijave, upotrebu sudo privilegija i druge podatke o autentifikaciji i autorizaciji. Osim toga, faillog posebno prati neuspjele događaje prijave. Neke distribucije koriste wtmp, utmp, btmp i who datoteke za bilježenje aktivnosti korisnika.

- Dnevnik upravitelja paketa (apt, yum ili dnf, ovisno o distribuciji) pohranjuje informacije

o tome koji je softver instaliran i ažuriran. Linux dnevnik autentifikacije koji prikazuje da je SSH udaljeni pristup omogućen, neuspjeli pokušaji autentifikacije za korisnika root i uspješna prijava korisnika lamp.

```
00:01:57 lamp sshd[453]: Server listening on 0.0.0.0 port 22.
00:01:57 lamp sshd[453]: Server listening on :: port 22.
00:17:01 lamp CRON[744]: pam_unix(cron:session): session opened for user root(uid=0) by (ui
00:17:01 lamp CRON[744]: pam_unix(cron:session): session closed for user root
00:26:47 lamp login[415]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0
00:26:51 lamp login[415]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failur
00:26:59 lamp login[415]: FAILED LOGIN (2) on '/dev/tty1' FOR 'root', Authentication failur
00:27:05 lamp login[415]: FAILED LOGIN (3) on '/dev/tty1' FOR 'root', Authentication failur
00:27:11 lamp login[415]: pam_unix(login:session): session opened for user lamp(uid=1000) b
00:27:11 lamp systemd-logind[396]: New session 3 of user lamp.
00:27:11 lamp systemd: pam_unix(systemd-user:session): session opened for user lamp(uid=100
00:29:26 lamp sudo:     lamp : TTY=tty1 ; PWD=/home/lamp ; USER=root ; COMMAND=/usr/bin/cat
00:29:26 lamp sudo: pam_unix(sudo:session): session opened for user root(uid=0) by lamp(uid
```

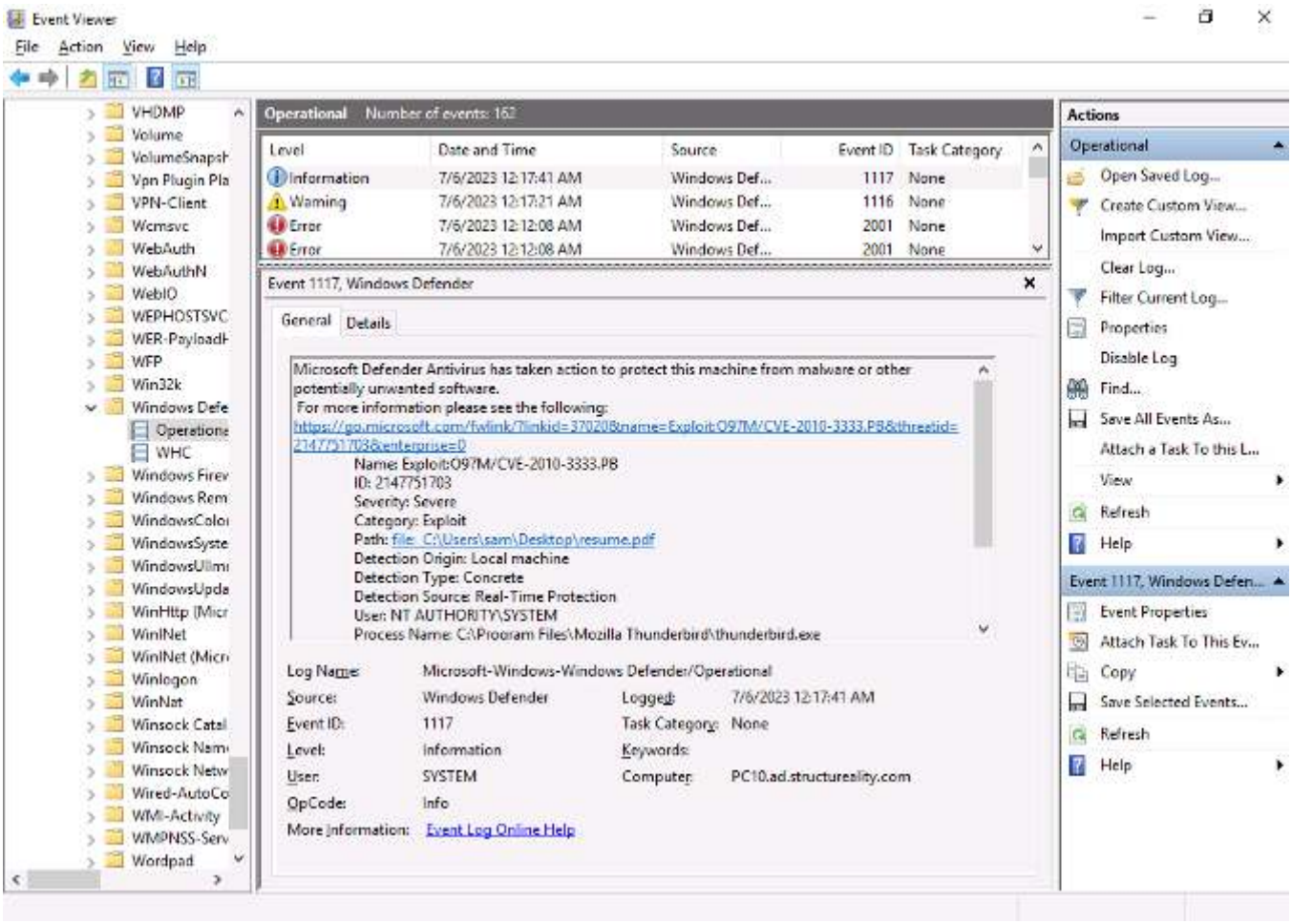
macOS dnevnici — macOS koristi jedinstveni sustav za bilježenje koji može biti pristupan putem grafičke aplikacije Console ili naredbe log. Naredba log može se koristiti s filtrima za pregled sigurnosnih događaja, poput pokušaja autentifikacije i neuspjeha.

Dnevnici aplikacija i krajnjih točaka

Osim događaja koje bilježi operativni sustav, hostovi će vjerojatno generirati i dnevnike aplikacija, uključujući dnevnike sigurnosnog softvera baziranog na hostu.

Dnevnici aplikacija

Datoteka dnevnika aplikacije je ona kojom upravljala aplikacija umjesto OS-a. Aplikacija može koristiti Preglednik događaja ili syslog za pisanje podataka događaja u standardnom formatu, ili može pisati u vlastitu datoteku dnevnika u vlasničkom formatu.



Snimak zaslona korišten uz dopuštenje Microsofta.

Skeniranje ranjivosti

Iako postoji obično sažetno izvješće, skener ranjivosti može biti konfiguriran za bilježenje svake otkrivene ranjivosti u SIEM. Ranjivosti mogu uključivati nedostajuće zakrpe i nekonfigurirani sigurni protokoli.

Mrežni izvori podataka

Mrežni uređaji generiraju vlastite sistemske i sigurnosne/revizijske dnevnike, ali postoje i drugi izvori mrežnih sigurnosnih podataka koji mogu biti korisni za istragu. Mrežni dnevnici — Mrežni uređaji poput preklopnika, usmjernika, vatrozida i pristupnih točaka generiraju dnevnike koji mogu biti korisni za istrage:

- Dnevnik preklopnika može otkriti krajnju točku koja pokušava koristiti više MAC adresa za izvođenje

on-path napada.

- Dnevnik vatrozida može identificirati aktivnost skeniranja na blokiranom portu.
- Dnevnik pristupne točke može zabilježiti događaje disasocijacije koji ukazuju na prijetnju koja pokušava

napasti bežičnu mrežu. Odlomci tipičnog SOHO router dnevnika dok se ponovo pokreće. Događaji prikazuju router koji uspostavlja Internet/WAN vezu i ažurira datum i vrijeme sustava koristeći NTP.

```
May  5 05:05:15 kernel: klogd started: BusyBox v1.24.1 (2023-05-06 13:28:52 CST)
May  5 05:05:27 pppd[1754]: Connected to c6:09:b7:f2:ac:8b via interface eth0
May  5 05:05:27 pppd[1754]: Connect: ppp0 <--> eth0
May  5 05:05:28 pppd[1754]: CHAP authentication succeeded
May  5 05:05:28 pppd[1754]: local  IP address 203.0.113.1
May  5 05:05:28 pppd[1754]: remote IP address 198.51.100.137
May  5 05:05:28 pppd[1754]: primary   DNS address 203.0.113.254
May  5 05:05:31 WAN Connection: WAN was restored.
May  5 05:05:31 ntp: start NTP update
Aug  2 09:38:46 rc_service: ntp 1945:notify_rc restart
Aug  2 09:40:33 WATCHDOG: [FAUPGRADE][auto_firmware_check:(7781)]periodic_check
Aug  2 10:13:23 wlceventd: Deauth_ind 00:15:5D:60:AA:0B, status: 0, reason: Previous authentication no longer valid (2), rssi:-75
Aug  2 10:13:23 wlceventd: Deauth_ind 00:15:5D:60:AA:0B, status: 0, reason: Previous authentication no longer valid (2), rssi:-75
Aug  2 10:13:46 wlceventd: Auth 00:15:5D:60:AA:0B, status: Successful (0), rssi:0
Aug  2 10:13:46 wlceventd: Assoc 00:15:5D:60:AA:0B, status: Successful (0), rssi:-73
```

Dnevnici vatrozida

Svako pravilo vatrozida može biti konfigurirano za generiranje događaja svaki put kada se aktivira. Kao i kod većine vrsta sigurnosnih podataka, ovo može brzo generirati ogromni broj događaja. Potrebno je selektivno konfiguriranje pravila vatrozida za bilježenje.

može potvrditi je li veza bila dopuštena ili odbijena i identificirati koje pravilo potencijalno treba prilagoditi. Dnevnik vatrozida koji prikazuje koja su pravila prolaza i blokade bila pokrenuta, s izvornim i odredišnim

```
1  T09:21:38-05    Info    hn1,pass,in,59897,0,DF,6,tcp,52,10.1.24.101,172.16.0.201,11545,22,0,S
2  T09:21:04-05    Info    hn0,block,in,46700,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,41250,22,0
3  T09:20:40-05    Info    hn0,pass,in,6808,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,49992,80,0,S
4  T09:20:40-05    Info    hn0,pass,in,52605,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,49988,80,0,
5  T09:20:40-05    Info    hn0,pass,in,55459,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,49978,80,0,
6  T09:20:40-05    Info    hn0,pass,in,62368,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,49962,80,0,
7  T09:20:40-05    Info    hn0,pass,in,37408,0,DF,6,tcp,60,203.0.113.66,172.16.0.201,49954,80,0,
```

Budući da je akcija dnevnika konfigurirana po pravilu, moguće je da jedan paket pokrene više događaja.

IPS/IDS dnevnici

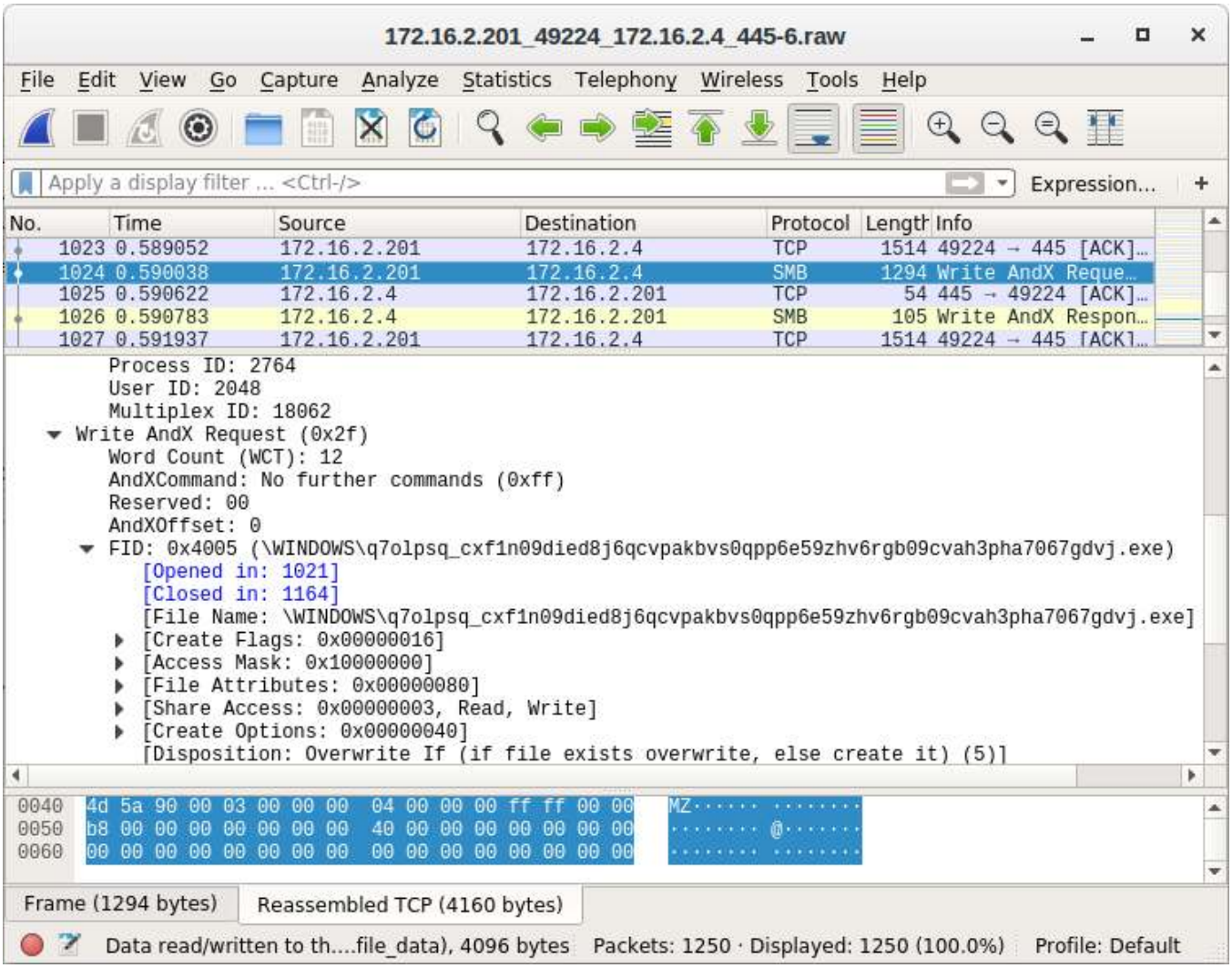
IPS/IDS dnevnik je događaj kada se uzorak prometa poklopi s pravilom. Budući da ovo može generirati visoki broj događaja, može biti primjereno bilježiti samo pravila visoke osjetljivosti/utjecaja.

Pregledavanje poruke neobrađenog dnevnika generirane upozorenjem Suricata IDS u Security Onion SIEM-u.

Snimanje paketa

Mrežni promet može pružiti dragocjene uvide u potencijalna kršenja. Mrežni promet se tipično analizira u detalje na razini pojedinačnih okvira ili korištenjem sažetih statistika. Snimanje paketa (pcap) je metoda hvatanja mrežnog prometa za forenzičku analizu.

može pomoći u otkrivanju alata korištenih u napadu. Također je moguće izvući binarne datoteke poput potencijalnog zlonamjernog softvera za analizu. Korištenje Wireshark analizatora paketa za identifikaciju zlonamjernih izvršnih datoteka.



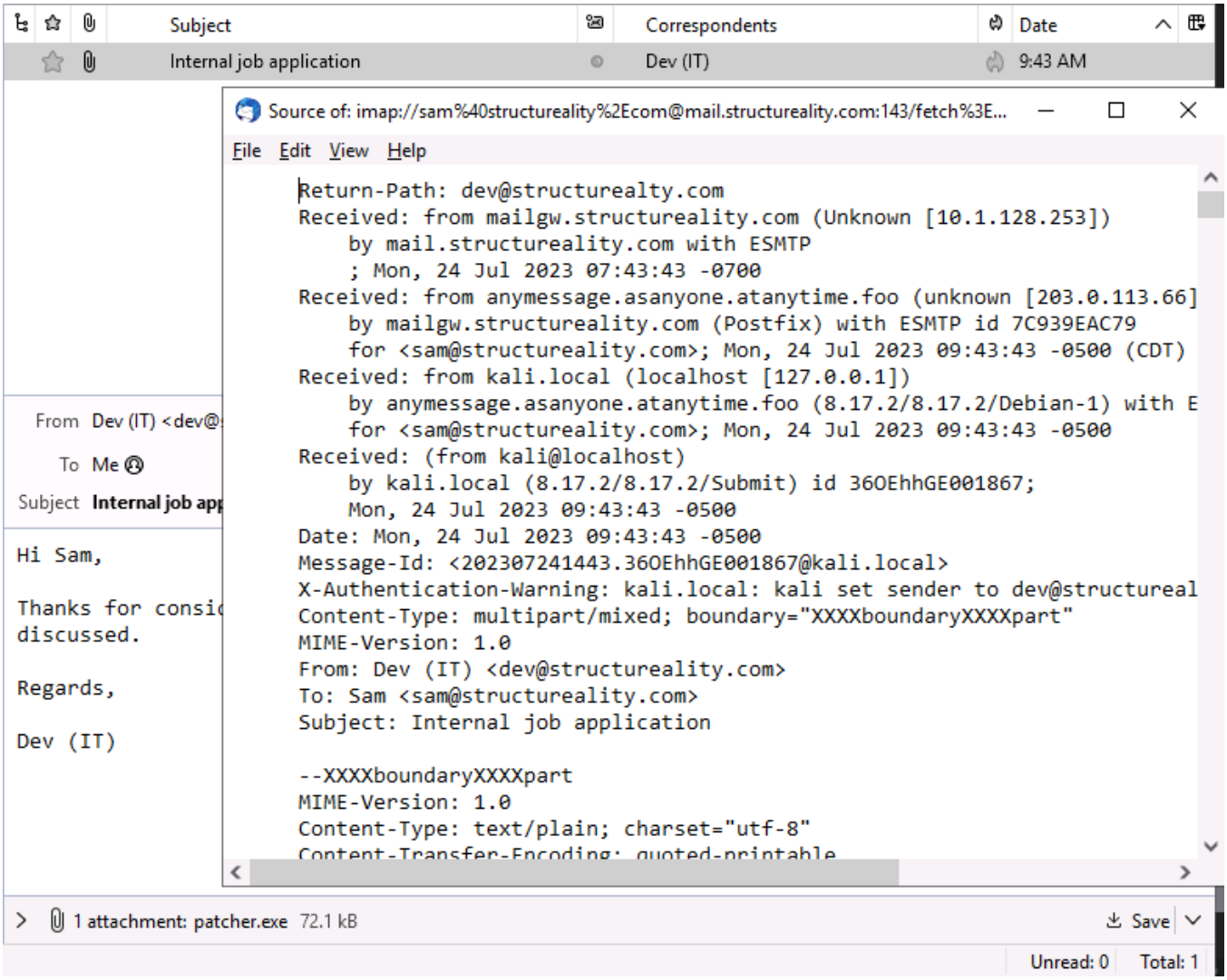
Snimak zaslona Wireshark wireshark.org.

Metapodaci

Metapodaci su svojstva podataka dok ih stvara aplikacija, pohranjuje na medij ili prenosi preko mreže. Svaki zabilježeni događaj ima metapodatke, ali niz drugih izvora metapodataka može biti dragocjen za istrage.

Kako se metapodaci prenose na stranice društvenih medija, mogu otkriti više informacija nego što je korisnik namjeravao. Metapodaci mogu uključivati trenutnu lokaciju i vrijeme, koji se dodaju medijima poput fotografija i videa snimljenih na pametnim telefonima.

Analiza zaglavlja u phishing poruci: pošiljatelj koristi typosquatting u nadi da će primatelj zbuniti structurealty.com s pravom domenom structureality.com.



Snimak zaslona ljubaznošću Mozille.

Lekcija 12D

Alati za upozoravanje i nadzor

Pregled lekcije

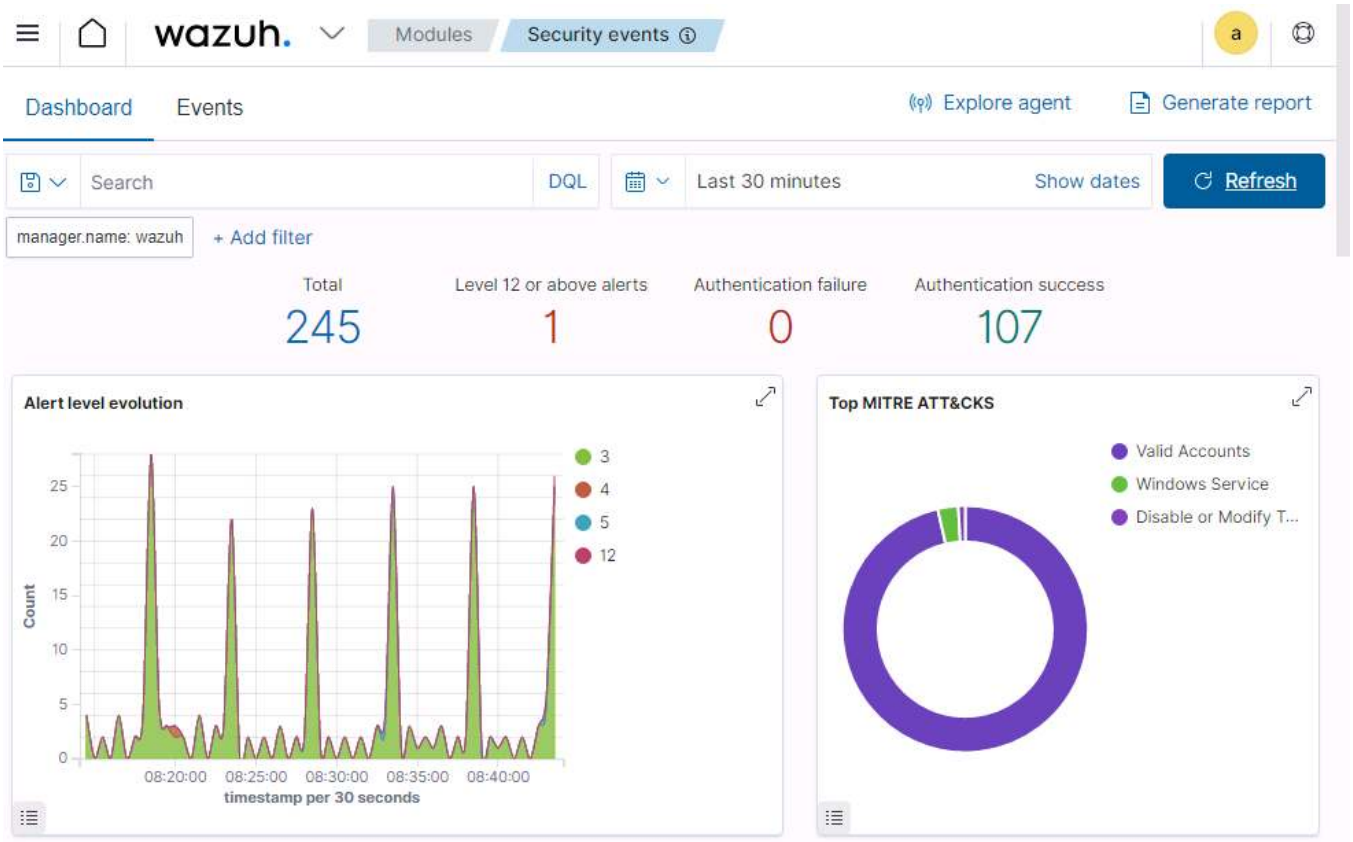
Postoje mnoge vrste sigurnosnih kontrola koje se mogu implementirati za zaštitu mreža, hostova i podataka. Jedna stvar koja je zajednička svim ovim kontrolama jest da generiraju log podatke i upozorenja. Prikupljanje, agregiranje i analiza ovih podataka kritičan je dio upravljanja sigurnošću. Alati za upravljanje sigurnosnim informacijama i događajima (SIEM) osmišljeni su za pomoć organizacijama u upravljanju i analizi ovih podataka.

Softver za upravljanje sigurnosnim informacijama i događajima

Softver osmišljen za pomoć u upravljanju sigurnosnim podatkovnim ulazima i pružanju izvješćivanja i upozoravanja često se opisuje kao upravljanje sigurnosnim informacijama i događajima (SIEM). SIEM kombinira funkcije upravljanja sigurnosnim informacijama (SIM) i upravljanja sigurnosnim događajima (SEM) u jednu platformu.

Wazuh SIEM nadzorna ploča

Konfigurirane nadzorne ploče pružaju pregled stanja mrežnih sigurnosnih metrika na visokoj razini.



Snimak zaslona korišten uz dopuštenje Wazuh Inc.

Prikupljanje temeljeno na agentima i bez agenata

Prikupljanje je način na koji SIEM unosi podatke o sigurnosnim događajima iz različitih izvora. Postoje tri glavne vrste prikupljanja sigurnosnih podataka:

- Temeljeno na agentima — ovaj pristup znači instalaciju usluge agenta na svaki host. Kako se događaji

odvijaju na hostu, podaci za bilježenje se filtriraju, agregiraju i normaliziraju na hostu, a zatim šalju SIEM serveru za analizu i pohranu. Prikupljanje s Windows/Linux/macOS računala obično koristi ovaj pristup.

- Osluškivač/kolektor — umjesto instaliranja agenta, hostovi se mogu konfigurirati za slanje log

Konfiguracijska datoteka agenta za izvore događaja koji se šalju Wazuh SIEM-u.

```
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>
```

Agregacija dnevnika

Za razliku od prikupljanja, agregacija dnevnika odnosi se na normaliziranje podataka iz različitih izvora tako da budu konzistentni i pretraživi. SIEM softver sadrži konektore ili priključke za razumijevanje različitih formata dnevnika koji se upotrebljavaju u infrastrukturi i transformiranje ulaznih zapisa u standardizirani format.

Aktivnosti upozoravanja i nadzora

Kada se podaci prikupe i agregiraju, SIEM se može koristiti za implementaciju aktivnosti upozoravanja, izvješćivanja i arhiviranja.

Napomena: ove aktivnosti mogu biti provedene ručno ili automatizirane korištenjem diskretnih alata za svaki sigurnosni uređaj. Prednost SIEM-a je konsolidacija aktivnosti na jedno sučelje za upravljanje. SIEM može implementirati korelacijska pravila koja uspoređuju podatke iz više izvora i automatski generiraju upozorenja kada se poklopite s uzorcima koji ukazuju na prijetnju.

- Validacija tijekom procesa analize je način na koji analitičar odlučuje je li upozorenje istiniti pozitiv i treba li se tretirati kao incident. Lažni pozitiv je situacija kada se generira upozorenje, ali nema stvarne prijetnje.
- Karantena je korak izoliranja izvora indikatora, poput mrežne adrese, hosta

računala ili datoteke. Koraci odgovora i saniranja upozorenja često se vode knjigom pravila koja pomaže analitičaru u primjeni svih procesa odgovora na incidente za određeni scenarij. Jedna od prednosti SIEM-a je mogućnost automatiziranja odgovora pomoću SOAR (sigurnosna orkestracija, automatizacija i odgovor).

- Izvješća za rukovodstvo pružaju sažetak na visokoj razini za donositelje odluka. Ovo vodi planiranje

i investicijsku aktivnost.

- Izvješća menadžera pružaju čelnicima kibernetičke sigurnosti i odjelima detaljne informacije.

Ovo vodi svakodnevno operativno donošenje odluka.

- Izvješća o usklađenosti pružaju sve informacije koje zahtijeva regulator.

Određivanje koji su metrikama najkorisnije u smislu izvješćivanja uvijek je izazov. Sljedeće vrste ilustriraju neke uobičajene slučajeve upotrebe za izvješćivanje:

- Podaci autentifikacije, poput neuspjelih pokušaja prijave, i kritični podaci revizije datoteka.
- Hostovi s nedostajućim zakrpama i/ili ranjivostima konfiguracije.
- Anomalije privilegiranog korisničkog računa, poput upotrebe izvan radnog vremena ili prekomjernih zahtjeva za

povećanim ovlastima.

- Statistike upravljanja slučajevima incidenata, poput ukupnog volumena, otvorenih slučajeva, vremena rješavanja,

itd.

- Trendovsko izvješćivanje za prikaz promjena ključnih metrika tijekom vremena.

Arhiviranje

SIEM može provesti politiku zadržavanja kako bi se povijesni podaci dnevnika i mrežnog prometa čuvali za definirani period. Ovo omogućava retrospektivno istraživanje incidenata i lov na prijetnje i može biti vrijedan resurs za forenzičke istrage.

Podešavanje upozorenja

Korelacijska pravila vjerojatno dodjeljuju razinu kritičnosti svakom podudaranju. Primjeri uključuju sljedeće:

- Samo bilježenje — događaj se proizvodi i dodaje u bazu podataka SIEM-a, ali nije automatski

kategoriziran.

- Upozorenje — događaj je naveden na nadzornoj ploči ili sustavu za rješavanje incidenata da agent procijeni.

Agent analizira podatke događaja i ili ga odbacuje u dnevnik ili ga validira i pokreće slučaj incidenta.

- Alarm — događaj je automatski klasificiran kao kritičan i podignut je prioritetni alarm. To

može značiti slanje e-pošte rukovatelju incidentima ili slanje SMS poruke. Podešavanje upozorenja je nužno za smanjenje pojavnosti lažnih pozitiva. Lažna upozorenja i alarmi

gube analytičarima vrijeme i smanjuju pouzdanost sustava.

- Usavršavanje pravila otkrivanja i utišavanje razina upozorenja — Ako određeno pravilo generira više

obavijesti nadzorne ploče, parametri pravila mogu biti prilagođeni da smanje ovo, možda dodavanjem više faktora korelacije. Alternativno, upozorenje može biti utišano na status samo bilježenja ili konfigurirano samo za generiranje upozorenja ako su ispunjeni određeni uvjeti.

- Preusmjeravanje iznenadnih 'poplava' upozorenja u posvećenu grupu — Promjene u mreži mogu uzrokovati

da pravilo počne proizvesti daleko više upozorenja nego što bi trebalo. Kada se potvrdi da je ovo lažni pozitiv, umjesto 'spamiranja' nadzorne ploče svakog analitičara, može se dodijeliti posvećenom agentu ili grupi.

- Preusmjeravanje upozorenja vezanih uz infrastrukturu u posvećenu grupu — Pogrešne konfiguracije, poput

odstupanja od referentnog stanja, mogu uzrokovati kontinuirano visoke volumene upozorenja. Dok su ovo važno popraviti, to nije zadatak tima za odgovor na incidente i bolje se njime upravlja infrastrukturnim timom.

- Kontinuirani nadzor volumena upozorenja i povratnih informacija analitičara — Menadžeri bi trebali zadržati

nadzor nad sustavom i biti svjesni rizika od umora od upozorenja. Iskustvo pojedinih analitičara može se iskoristiti za smanjenje osjetljivosti upozorenja ili promjenu parametara određenog pravila ili automatizaciju odgovora.

- Implementacija analize strojnog učenja (ML) — ML može brzo analizirati vrste skupa podataka koje

generira SIEM. Može se koristiti za praćenje kako analitičari odgovaraju na upozorenja i pokušati automatski podesiti skup pravila na način koji smanjuje lažne negative bez utjecaja na istinite pozitivne.

Nadzor infrastrukture

Upravljačka izvješća mogu se koristiti za svakodnevni nadzor računalnih resursa i mrežne infrastrukture. Nisu svi problemi prepoznatljivi iz upozorenja i alarma. Pokretanje redovitih izvješća i mjerenja ključnih metrika performansi može pomoći u proaktivnoj identifikaciji potencijalnih problema. NetFlow i IPFIX su protokoli koji se koriste za izvoz informacija o mrežnom prometu s mrežnih uređaja na sustave za nadzor:

- Isticanje trendova i uzoraka u prometu koji generiraju određene aplikacije, hostovi i

portovi.

- Upozoravanje temeljeno na otkrivanju anomalija, uzorcima analize toka ili prilagođenim okidačima.
- Alati vizualizacije koji prikazuju mapu mrežnih veza i olakšavaju interpretaciju

uzoraka prometa i podataka o toku.

- Identifikacija uzoraka prometa koji otkrivaju nedolično ponašanje korisnika, zlonamjerni softver u prijenosu, tuneliranje,

ili aplikacije koje premašuju dodijeljenu propusnost.

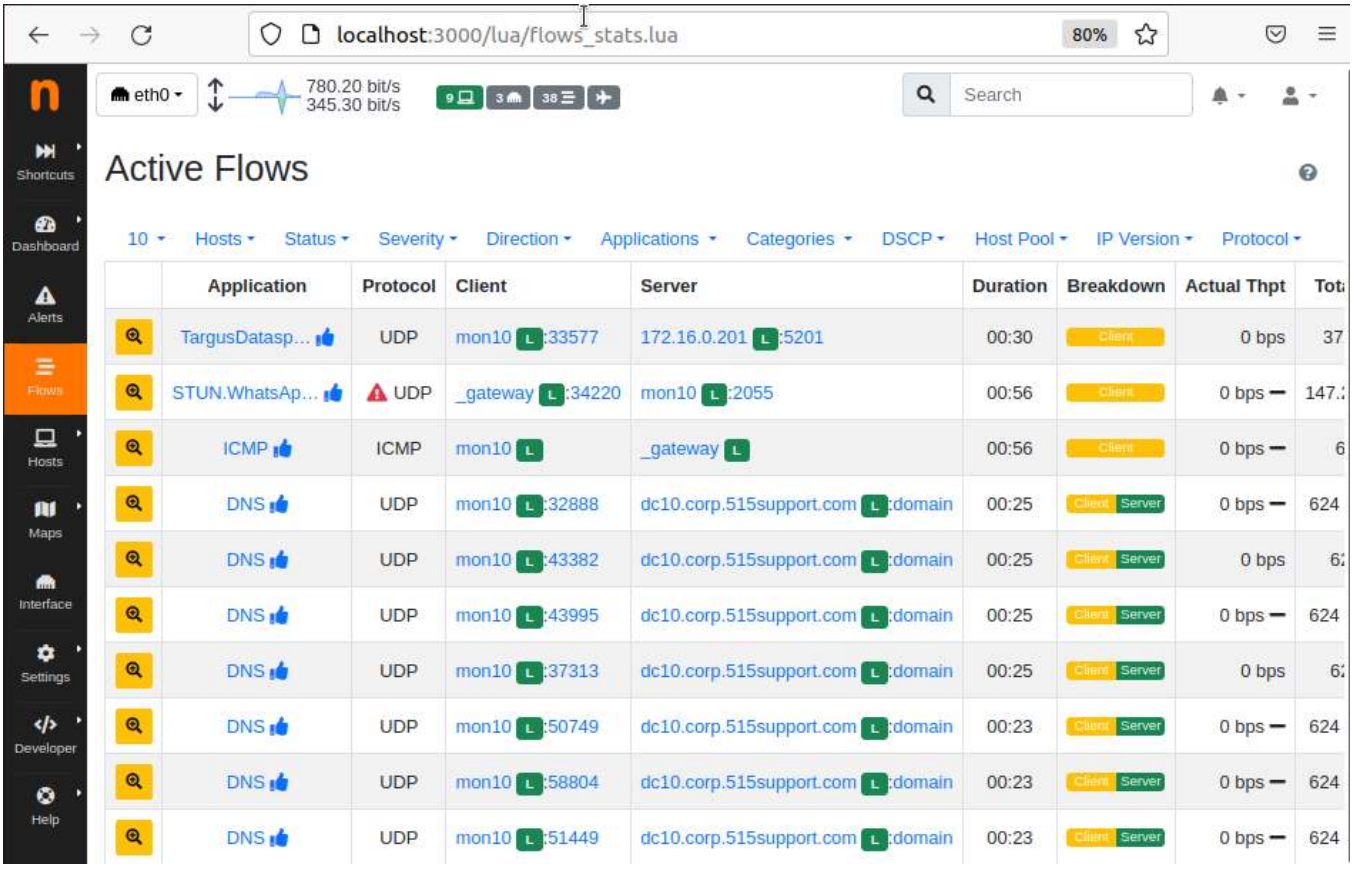
- Identifikacija pokušaja zlonamjernog softvera da kontaktira rukovatelja ili kanal za naredbe i kontrolu (C&C).

NetFlow je Cisco-razvijeno sredstvo za izvješćivanje informacija o mrežnom toku u strukturiranu bazu podataka. NetFlow je prerađen kao IPFIX IETF standard (alati.

iste ključne karakteristike, poput IP izvornih i odredišnih adresa i vrste protokola. Ovih pet dijelova informacija naziva se 5-torka. 5-torka se sastoji od:

- Izvorna adresa
- Odredišna adresa
- Protokol
- Izvorni port
- Odredišni port

7-torka dodaje ulazno sučelje i podatke o tipu usluge IP-a. Svaki izvoznik kešira podatke za novo viđene tokove i postavlja mjerač vremena za određivanje isteka toka. Kada tok istekne ili postane neaktivan, podaci se izvoze u bazu podataka za nadzor.



Snimak zaslona ljubaznošću ntop.

Nadzor sustava i aplikacija

Nadzorne ploče i izvješća pomažu i u praćenju sustava hosta i statusa aplikacija/usluga u stvarnom vremenu. Nadzori sustava i dnevnici — Monitor sustava implementira

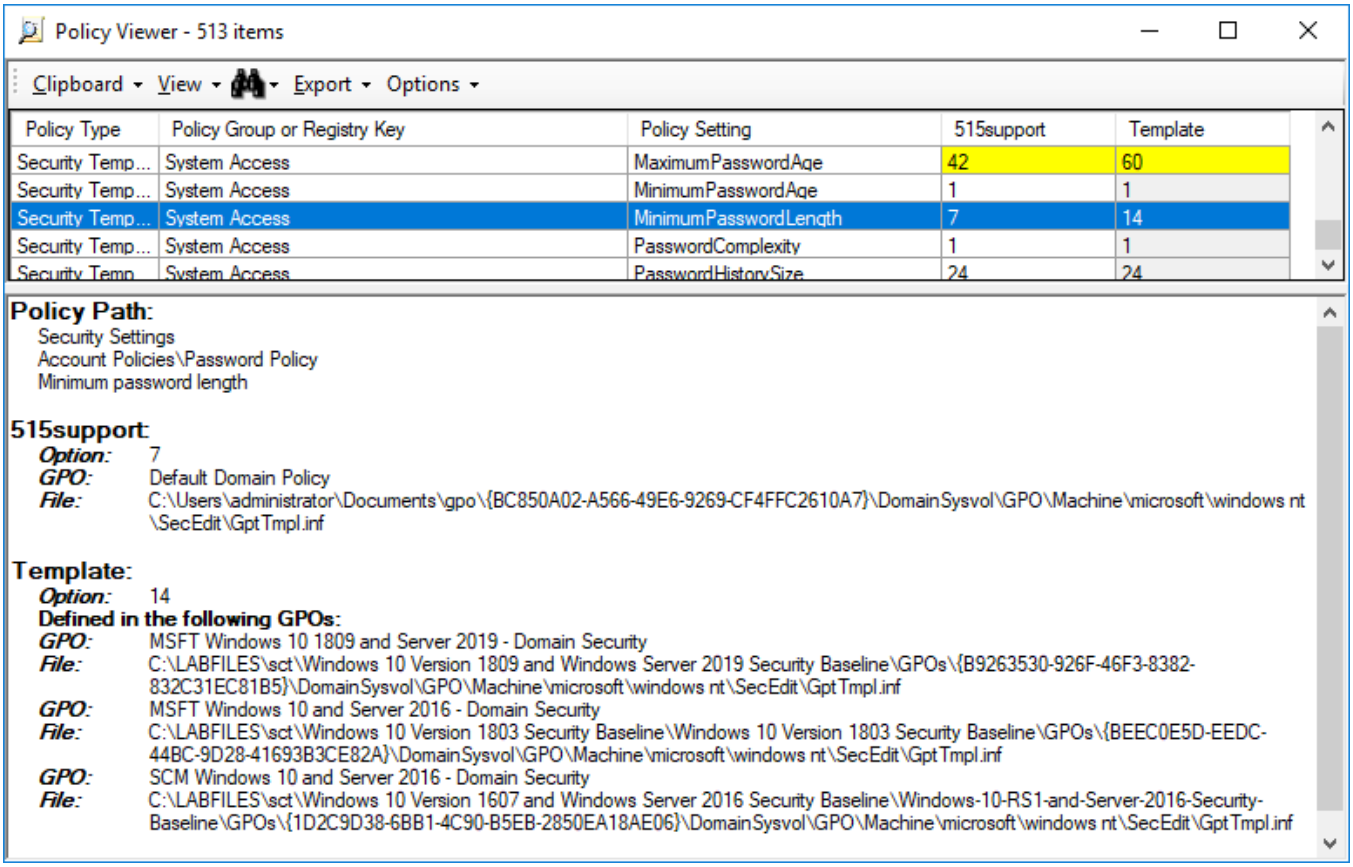
Dnevnici obično povezuju akciju s određenim korisnikom. To je jedan od razloga zašto je ključno da korisnici ne dijele podatke za prijavu. Ako je korisnički račun kompromitiran, nema načina za povezivanje akcija s određenim pojedincem. SCAP (Security Content Automation Protocol) je standard koji se koristi za automatizaciju upravljanja ranjivostima

i mjerenje usklađenosti. SCAP sadrži nekoliko shema i specifikacija:

• Open Vulnerability and Assessment Language (OVAL) — XML shema za opisivanje sigurnosnog stanja sustava i pretraživanje izvješća o ranjivostima i informacija.

• Extensible Configuration Checklist Description Format (XCCDF) — XML shema za razvoj i reviziju kontrolnih listi i pravila za konfiguraciju prema najboljim praksama. Ranije su vodiči za dobre prakse mogli biti pisani u prozi za sistemske administratore.

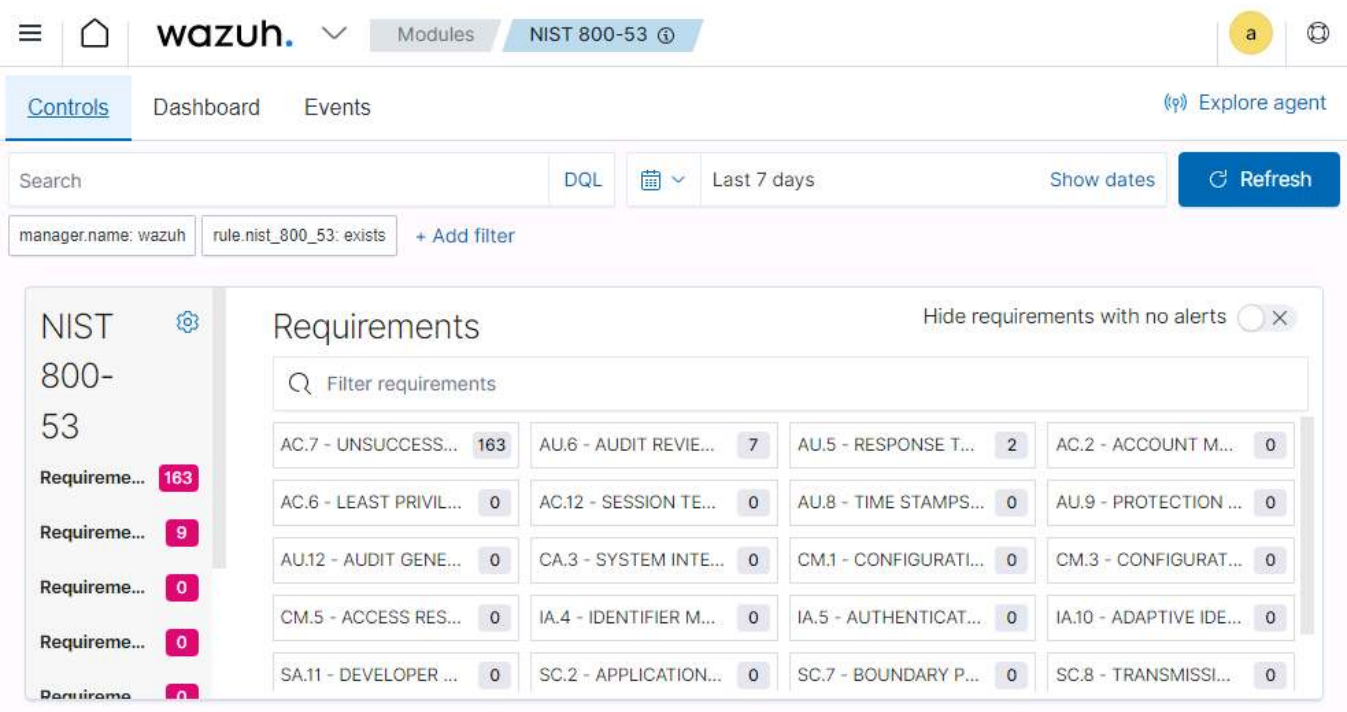
ručno. XCCDF pruža format čitljiv računalom koji se može primijeniti i validirati korištenjem kompatibilnog softvera. Usporedba lokalnih sigurnosnih politika mreže s predloškom. Minimalna duljina lozinke postavljena je na 14 znakova, ispunjavajući sigurnosni zahtjev.



Snimak zaslona korišten uz dopuštenje Microsofta.

Neki skeneri mjere sustave i postavke konfiguracije u odnosu na okvire najboljih praksi. Ovo se naziva skeniranjem usklađenosti. To može biti potrebno za regulatornu usklađenost, ili to možete voljno usporediti sa standardom poput CIS Benchmarks-a.

Predložak za nadzor usklađen sa zahtjevima okvira NIST 800-53.



Sažetak

Trebali biste biti u mogućnosti objasniti procese i procedure uključene u učinkovit odgovor na incidente i digitalnu forenziku, uključujući izvore podataka i alate za upravljanje događajima potrebne za istragu.
Smjernice za provođenje IR-a:

- Identificirajte ciljeve za implementaciju strukturiranog odgovora na incidente, slijedeći procese pripreme,

otkrivanja, analize, sadržavanja, iskorjenjivanja, oporavka i lekcija naučenih.

- Pripremite se za učinkovit odgovor na incidente stvaranjem CIRT/CERT/CSIRT-a s odgovarajućim politikama

i komunikacijama te alatima za upravljanje incidentima.

- Razvijte sustav klasifikacije incidenata i pripremite IRP-e i knjige pravila za različite

scenarije incidenata.

- Koristite stolne vježbe i simulacije za testiranje planova odgovora na incidente.
- Konfigurirajte SIEM za agregiranje odgovarajućih izvora podataka i razvijte korelacijska pravila za prikaz

upozorenja, statusnih indikatora i analize trendova putem nadzornih ploča:

- Izvori podataka datoteka dnevnika hosta (mreža, sustav, sigurnost, izlaz skeniranja ranjivosti).
- Izvori podataka datoteka dnevnika aplikacija (DNS, web, VoIP).
- Podaci o mrežnim paketima i otkrivanju upada.
- Podaci o mrežnom prometu

procedure za karantenu, prikupljanje forenzičkih dokaza, analizu temeljnog uzroka, skeniranje ranjivosti temeljeno na referenci/SCAP i lov na prijetnje.

- Identificirajte standardne strategije za sadržavanje putem izolacije i segmentacije.
- Razvijte ili usvojite konzistentan proces za istraživače incidenata za prikupljanje i sačuvanje

forenzičkih i e-otkrivanje podataka:

- Razmotrite redoslijed hlapljivosti i potencijalni gubitak dokaza ako se host isključi ili napajanje ugasi.
- Zabilježite prikupljanje dokaza videom i intervjuirajte svjedoke za izjave.
- Implementirajte forenzičke alate koji mogu snimiti i validirati dokaze s trajnih i nepersistentnih medija.
- Dokumentirajte pohranu i rukovanje dokazima korištenjem lanca skrbništva.
- Identificirajte dostupne izvore podataka za podršku istragama:
- Log događaje i metapodatke s vatrozida, aplikacija, antivirusa krajnjih točaka specifičnih sigurnosnih događaja, IDS/IPS, mrežnih uređaja, SNMP i skeniranja ranjivosti.
- Izlaz iz snimanja paketa i nadzora mrežnog prometa NetFlow.
- Razmotrite implementaciju SIEM-a za agregiranje i koreliranje izvora podataka radi pokretanja upozorenja i

nadzornih ploča praćenja i automatiziranih izvješća. Koristite podešavanje upozorenja za smanjenje lažnih pozitiva, bez povećanja lažnih negativnih.

Modul 13

Analiza indikatora zlonamjerne aktivnosti

Pregled modula

Faza pripreme odgovora na incidente identificira izvore podataka koji mogu podržati istrage. Također provizira alate za agregiranje i koreliranje ovih podataka i djelomičnu automatizaciju njihove analize kako bi se identificirali indikatori kompromitiranja. Ovaj modul proširuje to razmatranjem vrsta napada koji mogu biti identificirani ovim indikatorima.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Analizirajte indikatore zlonamjerne aktivnosti u zlonamjernom softveru, fizičkim, mrežnim i aplikacijskim

napadima.

Lekcija 13A

Indikatori napada zlonamjernog softvera

Pregled lekcije

Klasificiranjem različitih vrsta zlonamjernog softvera i identificiranjem znakova infekcije, sigurnosni timovi bolje su pripremljeni za saniranje kompromitiranih sustava ili sprečavanje izvršavanja zlonamjernog softvera. Razumijevanje taktika, tehnika i procedura (TTPs) koje koriste napadači ključno je za učinkovit odgovor na incidente i lov na prijetnje.

Klasifikacija zlonamjernog softvera

Mnogi od pokušaja upada koji se izvode protiv računalnih mreža ovise o upotrebi zlonamjernog softvera, ili malware-a. Zlonamjerni softver je jednostavno definiran kao softver koji čini nešto što korisnik nije ovlastio i koje je obično štetno. Zlonamjerni softver može se klasificirati prema načinu na koji se širi i instalira ili prema svojoj svrsi:

- Virusi i crvi predstavljaju neke od prvih vrsta zlonamjernog softvera i šire se bez ikakve

autorizacije korisnika skrivanjem unutar izvršnog koda drugog procesa. Za ove procese se kaže da su zaraženi zlonamjernim softverom.

- Trojanac se odnosi na zlonamjerni softver skriven unutar paketa instalatora za softver koji izgleda

legitimno. Ova vrsta zlonamjernog softvera ne traži nikakav pristanak za instalaciju i aktivno je dizajnirana za tajno djelovanje.

- Potencijalno neželjeni programi (PUP) / Potencijalno neželjene aplikacije (PUA) su

softver instaliran uz paket koji je korisnik odabrao ili možda isporučen s novim računalnim sustavom. Za razliku od Trojanca, prisutnost PUP-a se ne smatra automatski zlonamjernom. Može imati legitimnu namjenu, ali se instalira bez potpunog informiranog pristanka korisnika.

Klasifikacija zlonamjernog softvera prema vektoru.

Ostale klasifikacije temelje se na korisnom teretu koji isporučuje zlonamjerni softver. Korisni teret je akcija koju izvodi zlonamjerni softver osim jednostavnog repliciranja ili trajanja na hostu. Primjeri uključuju brisanje datoteka, enkripciju podataka ili eksfiltraciju povjerljivih informacija.

Računalni virusi

Računalni virus vrsta je zlonamjernog softvera dizajniranog za repliciranje i širenje s računala na računalo, obično 'zarazom' izvršnih aplikacija ili programskog koda. Virusi se mogu klasificirati prema načinu na koji se repliciraju:

- Ne-rezidentni/inficirač datoteka — virus je sadržan unutar izvršne datoteke hosta i izvodi se s

procesom hosta. Virus će pokušati zaraziti druge slike procesa na trajnoj pohrani i izvršiti druge akcije korisnog tereta. Zatim vraća kontrolu programu hosta.

- Memorijsko-rezidentni — kada se izvšrna datoteka hosta izvrši, virus stvara novi proces za

sebe u memoriji. Zlonamjerni proces ostaje u memoriji, čak i ako je proces hosta prekinut.

- Boot — kod virusa upisan je u sektor diska za pokretanje ili tablicu particija fiksnog diska ili

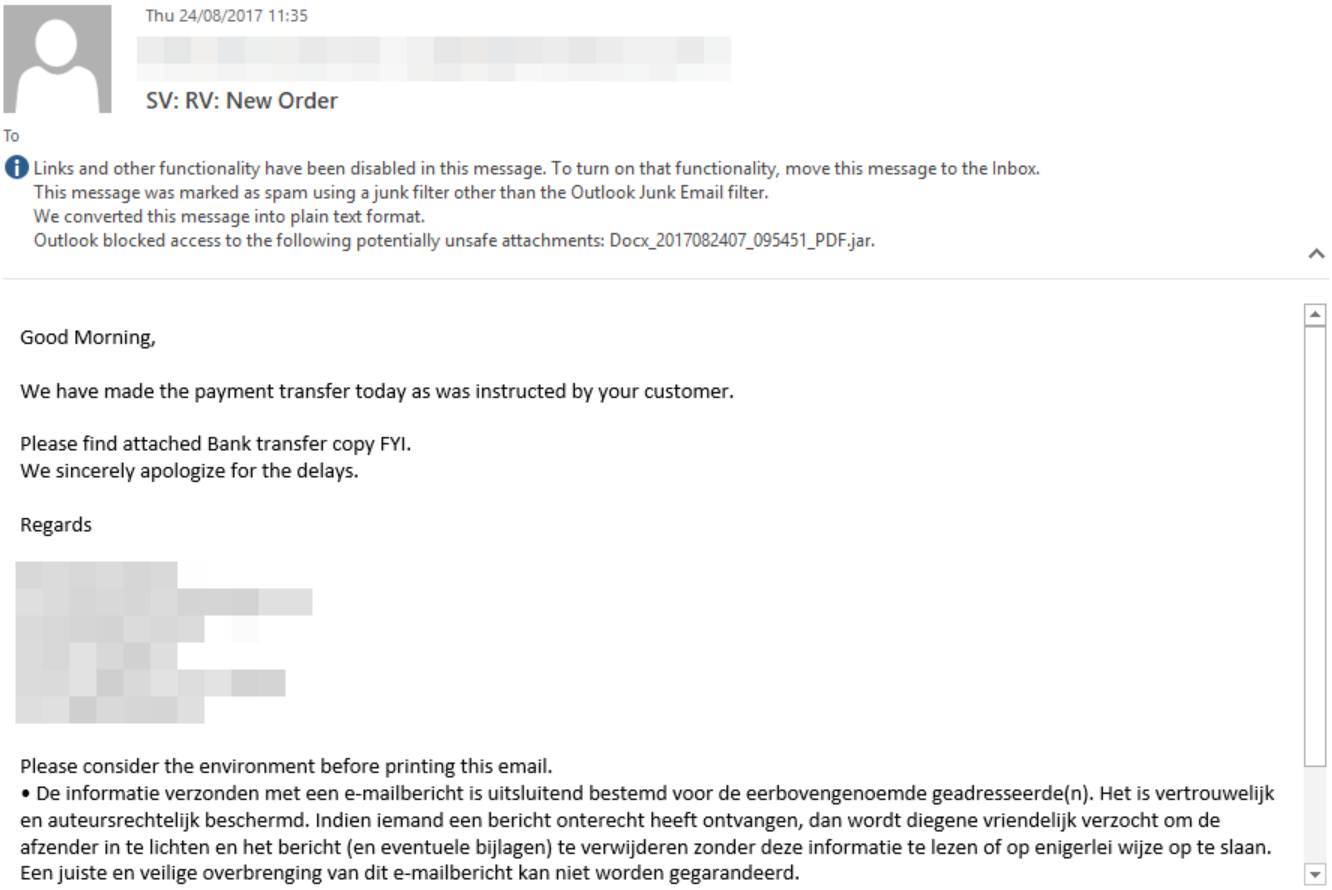
USB medija i izvodi se kao memorijsko-rezidentni proces kada se OS pokrene ili kada se medij pričvrsti na računalo.

- Skriptni i makro virusi — zlonamjerni softver koristi programske značajke dostupne u lokalnim

skriptnim pokretačima za OS i/ili preglednik, poput PowerShella, Windows Management Instrumentation (WMI), JavaScripta, Microsoft Office dokumenata s Visual Basic for Applications (VBA) i sličnih tehnologija.

Nesigurni privitak otkriven Outlookovim mail filterom

'dvostruka' ekstenzija datoteke je nerafinirani pokušaj zavaravanja korisnika koji možda nije upozoren na upotrebu engleskog i holandskog u istom nazivu datoteke.



Thu 24/08/2017 11:35

SV: RV: New Order

To

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk Email filter.
We converted this message into plain text format.
Outlook blocked access to the following potentially unsafe attachments: Docx_2017082407_095451_PDF.jar.

Good Morning,

We have made the payment transfer today as was instructed by your customer.

Please find attached Bank transfer copy FYI.
We sincerely apologize for the delays.

Regards

Please consider the environment before printing this email.
• De informatie verzonden met een e-mailbericht is uitsluitend bestemd voor de eerbovengenoemde geadresseerde(n). Het is vertrouwelijk en auteursrechtelijk beschermd. Indien iemand een bericht onterecht heeft ontvangen, dan wordt diegene vriendelijk verzocht om de afzender in te lichten en het bericht (en eventuele bijlagen) te verwijderen zonder deze informatie te lezen of op enigerlei wijze op te slaan. Een juiste en veilige overbrenging van dit e-mailbericht kan niet worden gegarandeerd.

Snimak zaslona korišten uz dopuštenje Microsofta.

Računalni crvi i beznačajni zlonamjerni softver

Računalni crv je memorijsko-rezidentni zlonamjerni softver koji se može pokrenuti bez intervencije korisnika i replicira se putem mrežnih resursa. Virus se izvodi samo kada korisnik pokrene zaraženi proces. Crv, nasuprot tome, može se samostalno širiti čim dobije pristup mreži. Beznačajni (fileless) zlonamjerni softver vrsta je koja ne upisuje kod na disk, umjesto toga koristiti memorijsko-rezidentne tehnike.

- Beznačajni zlonamjerni softver ne upisuje kod na disk. Zlonamjerni softver koristi memorijsko-rezidentne

tehnike za izvođenje u vlastitom procesu, unutar procesa hosta ili dinamički povezane knjižnice (DLL), ili unutar skriptnog hosta. To ne znači da nema nikakve aktivnosti na disku.

- Beznačajni zlonamjerni softver koristi lagani shellcode za postizanje mehanizma backdoor-a na hostu.

Shellcode je lako rekompilirati u opfusciranom obliku za izbjegavanje otkrivanja skenerima. Zatim je u mogućnosti preuzeti dodatne pakete ili korisne terete za postizanje ciljeva prijetnje.

- Beznačajni zlonamjerni softver može koristiti 'living off the land' tehnike umjesto kompiliranih izvršnih datoteka za

izbjegavanje otkrivanja. To znači da kod zlonamjernog softvera koristi legitimne alate za sistemsko skriptiranje, posebno PowerShell i WMI, za izvođenje akcija korisnog tereta.

Špijunski softver i keyloggeri

Prvi virusi i crvi fokusirali su se na destruktivni potencijal repliciranja. Kako su postale jasne profitabilne upotrebe ovog softvera, programeri zlonamjernog softvera počeli su pisati alate koji mogu prikupljati podatke s kompromitiranih sustava:

- Kolačići za praćenje — kolačić je datoteka u čistom tekstu, nije zlonamjerni softver, ali ako je dopušteno postavkama preglednika,

kolačići treće strane mogu se koristiti za bilježenje web aktivnosti, praćenje IP adrese korisnika i skupljanje raznih metapodataka.

- Superkolačići i oznake — kako softver preglednika daje korisniku određenu kontrolu nad tim koji

kolačići su prihvaćeni, web marketinške tvrtke osmislile su alternativne načine implementacije praćenja koje je teško onemogućiti. Superkolačić je sredstvo pohrane podataka za praćenje u memoriji preglednika umjesto na disku.

- Adware — ovo je klasa PUP/bloatware koji izvodi rekonfiguracije preglednika, poput

dopuštanja kolačića za praćenje, mijenjanja zadanih davatelja pretraživanja, otvaranja stranica sponzora pri pokretanju, dodavanja oznaka i tako dalje.

- Špijunski softver — ovo je zlonamjerni softver koji može obavljati praćenje slično adwareu, ali i nadzirati lokalnu

aktivnost aplikacije, snimati zaslone i aktivirati uređaje za snimanje, poput mikrofona ili web kamere. Druga tehnika špijunskog softvera je preusmjeravanje DNS-a na pharming stranice.

- Keylogger — ovo je špijunski softver koji aktivno pokušava krasti povjerljive informacije

bilježenjem pritisaka tipki. Napadač obično nada da će otkriti lozinke ili podatke kreditne kartice.

Korištenje Metasploit Meterpreter alata za udaljeni pristup za ispis pritisaka tipki s žrtvine mašine, otkrivajući lozinku koja se koristi za pristup web aplikaciji.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
https<Right Shift>://tickets.structureality.com/scp<CR>
jaime<Tab><Right Shift>Pa<Right Shift>$$w0rd

meterpreter >
```

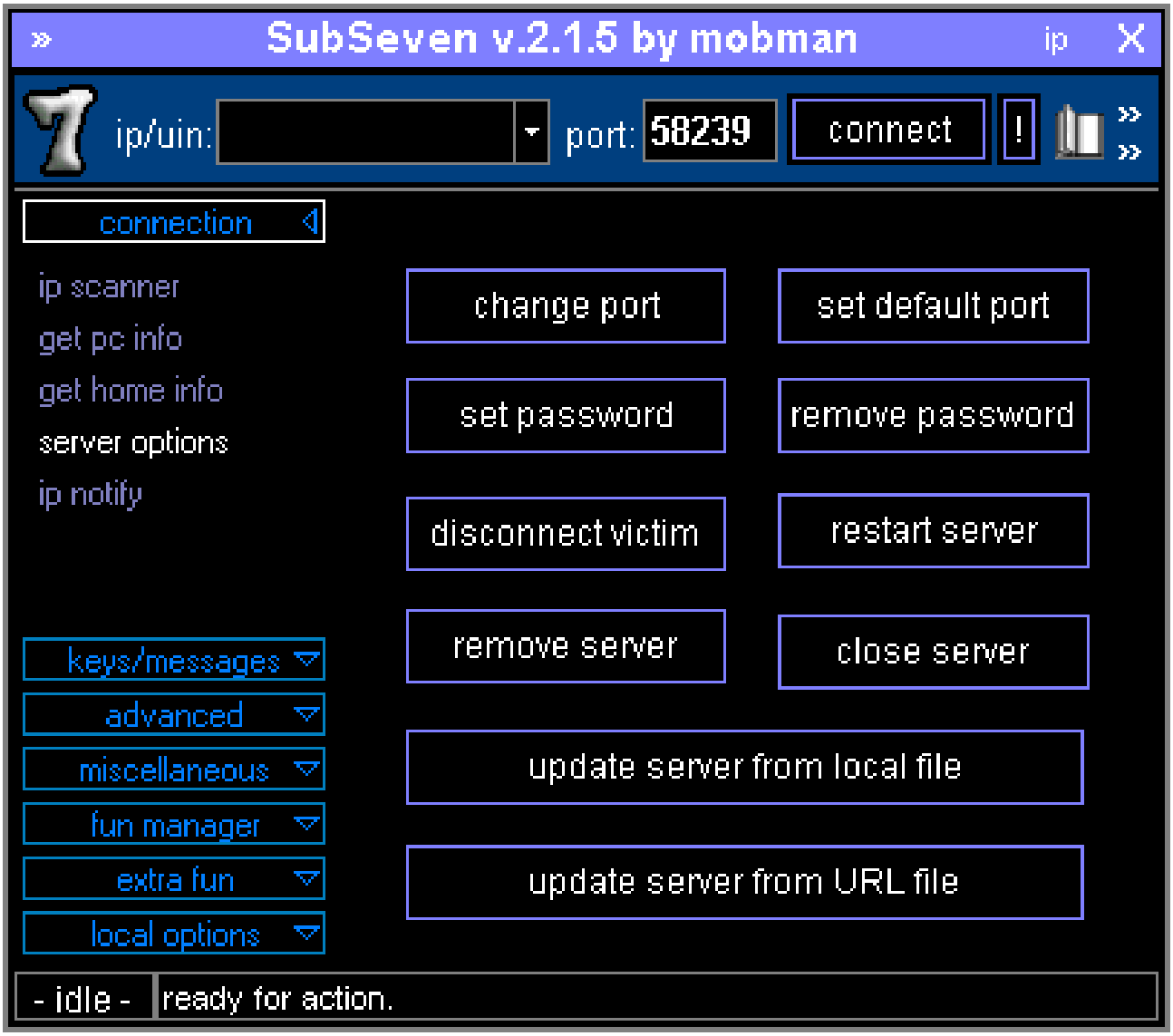
Keyloggeri nisu implementirani samo kao softver. Zlonamjerna skripta može prenositi pritiske tipki na web stranicu treće strane. Postoje i hardverski uređaji koji snimaju pritiske tipki na memorijsku karticu.

Backdoori i trojanci udaljenog pristupa

Svaka vrsta metode pristupa hostu koja zaobilazi uobičajenu metodu autentifikacije i daje udaljenom korisniku administrativnu kontrolu može se nazvati backdoor. Trojanac udaljenog pristupa (RAT) je vrsta backdoor-a koji se instalira kao korisna aplikacija, ali tajno pružaju napadaču udaljenu kontrolu nad hostom.

Kompromitirani host može biti instaliran s jednim ili više botova. Bot je automatizirana skripta ili alat koji izvodi neku zlonamjernu aktivnost. Skupina botova koji su svi pod kontrolom jednog rukovatelja nazivaju se botnet.

SubSeven RAT alat za udaljeni pristup.



Snimak zaslona korišten uz dopuštenje Wikimedia Commons CCAS4.0 International.

Bez obzira koristi li se backdoor kao samostalni mehanizam upada ili za upravljanje botovima, prijetnja mora uspostaviti vezu s kompromitiranog hosta na kanal za naredbe i kontrolu (C2 ili C&C). C2 kanal može biti implementiran korištenjem raznih metoda, uključujući IRC, HTTP/HTTPS, DNS i društvene medije.

Rootkitovi

U Windowsima, trojanski zlonamjerni softver koji ovisi o ručnom izvođenju od strane prijavljenog korisnika nasljeđuje privilegije tog korisničkog računa. Ako račun ima samo standardne dozvole, sposobnost zlonamjernog softvera da našteti sustavu je ograničena.

Ako zlonamjerni softver pokušava promijeniti sistemski šire datoteke ili postavke, zahtijeva privilegije lokalnog administratora. Za dobivanje tih putem ručne instalacije ili izvođenja, korisnik mora biti prijavljen kao administrator ili mora biti prisutna ranjivost eskalacije privilegija. Rootkit je vrsta zlonamjernog softvera koji modificira niske razine

operativnog sustava kako bi sakrio svoju prisutnost i aktivnosti.

Ransomware, kripto-zlonamjerni softver i logičke bombe

Ransomware je vrsta zlonamjernog softvera koji pokušava iznuditi novac od žrtve čineći računalo i/ili datoteke žrtve nedostupnima. Obično enkriptira datoteke korisnika i zahtijeva plaćanje otkupnine u zamjenu za ključ za dekripciju.

WannaCry ransomware

jedan od najpoznatijih primjera ransomwarea koji je 2017. zahvatio stotisućke sustava po cijelom svijetu.

Slika od Wikimedia Commons.

Scareware se odnosi na zlonamjerni softver koji prikazuje alarmantne poruke, često maskirane da izgledaju kao prave OS dijaloške kutije. Scareware pokušava uznemiriti korisnika sugeriranjem da je računalo zaraženo ili da postoji drugi problem koji se može riješiti kupnjom softverskog alata.

Neke vrste zlonamjernog softvera ne okidaju automatski. Zarazivši sustav, čekaju unaprijed konfigurirano vrijeme ili datum (vremenska bomba) ili sistemski ili korisnički događaj (logička bomba). Logičke bombe mogu biti podmetnute od strane nezadovoljnih zaposlenika ili napadača koji su dobili pristup sustavima.

TTPs i IoC

Antivirusni (A-V) skeneri rade na osnovi prepoznavanja poznatog koda zlonamjernog softvera. Kod zlonamjernog softvera pohranjen je kao potpis u bazi podataka antivirusnog skenera. Međutim, oslanjanje isključivo na otkrivanje temeljeno na potpisu nije dovoljno. Taktike, tehnike i procedure (TTPs) pružaju okvir za razumijevanje ponašanja prijetnje, a Indikatori kompromitiranja (IoC) su specifični dokazi da je napad bio izveden. MITRE ATT&CK je okvir koji katalogizira TTPs koje koriste napadači:

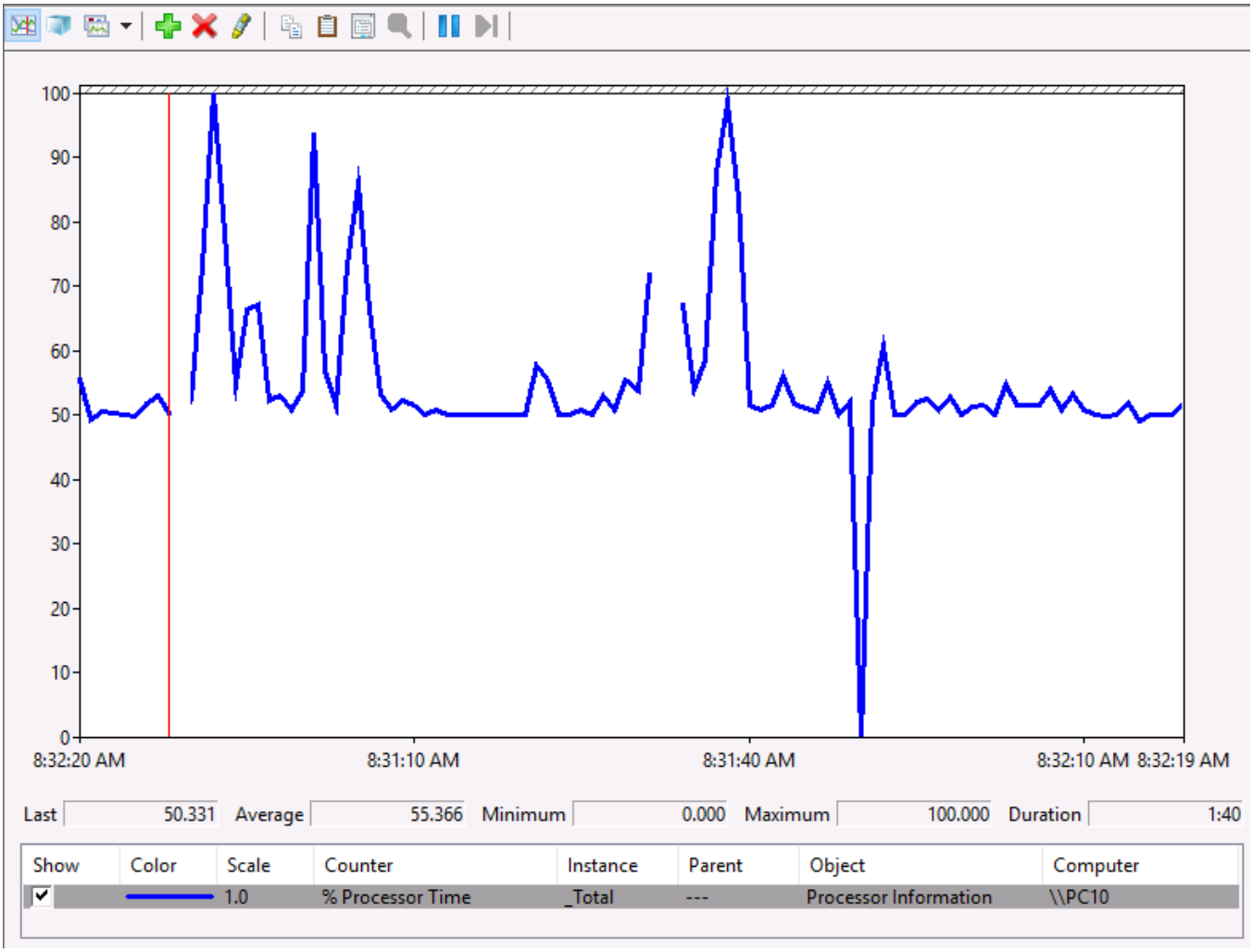
- Taktika — opis visokog nivoa ponašanja prijetnje. Ponašanja poput izviđanja, ustrajnosti i eskalacije privilegija primjeri su taktika.
- Tehnika — opis srednje razine kako prijetnja napreduje taktiku. Na primjer, izviđanje se može postići tehnikama poput aktivnog mrežnog skeniranja, skeniranja ranjivosti i prikupljanja e-pošte.
- Procedura — detaljan opis kako se tehnika izvodi. Na primjer, određena prijetnja može koristiti određeni alat na prepoznatljiv način za izvođenje skeniranja ranjivosti. Kao primjer TTP analize, razmotrite scenarij gdje kriminalna banda nastoji

platforme koriste sustave umjetne inteligencije (AI) za izvođenje automatiziranih analiza. Ovi sustavi podupiru značajke otkrivanja i odgovora modernih paketa za zaštitu od prijetnji. Strojno učenje (ML) može se trenirati na skupovima podataka o prijetnjama za prepoznavanje uzoraka koji ukazuju na zlonamjernu aktivnost.

Indikatori zlonamjerne aktivnosti

S obzirom na raspon vrsta zlonamjernog softvera, postoje mnogi potencijalni indikatori zlonamjerne aktivnosti. Neke vrste zlonamjernog softvera prikazuju očite promjene, poput poruka o ransomwareu ili pop-up prozora adwarea. Ostale vrste zlonamjernog softvera dizajnirane su za tajno djelovanje i mogu biti identificirane samo kroz pažljivo nadziranje sustava i analizu log podataka. Indikatori resursa poput neobično visokog korištenja CPU-a, memorije ili mreže mogu ukazivati na infekciju.

Windows Performance Monitor koji bilježi korištenje CPU-a na klijentskom računalu. Anomalna aktivnost je teško dijagnosticirati, ali ovaj grafikon pokazuje opterećenje koje rijetko pada ispod 50%. Kontinuirano visoko opterećenje procesora može biti indikator infekcije zlonamjernim softverom.



Snimak zaslona korišten uz dopuštenje Microsofta.

Datotečni sustav

Zlonamjerni kod možda se ne izvodi iz slike procesa pohranjene na lokalnom disku, ali će vjerojatno i dalje komunicirati s datotečnim sustavom i registrom, otkrivajući svoju prisutnost. Indikatori datotečnog sustava uključuju neočekivane izmjene datoteka, neočekivane nove datoteke i neuobičajene dozvole datoteka.

Prijetnja će često pokušati iskoristiti postojeći račun za postizanje ciljeva. Sljedeći indikatori mogu otkriti sumnjivo ponašanje računa:

- Blokada računa — sustav je spriječio pristup računu jer je napravljeno previše neuspjelih

pokušaja autentifikacije. Blokada bi također mogla značiti da lozinka korisnika više ne radi jer ju je prijetnja promijenila.

- Istovremeno korištenje sesije — ovo ukazuje da je prijetnja pribavila vjerodajnice računa

i prijavila se na drugoj radnoj stanici ili putem veze za udaljeni pristup.

- Nemoguće putovanje — ovo ukazuje da prijetnja pokušava koristiti udaljeni pristup za

prijavu na račun s geografske lokacije na koju fizički nisu mogli doputovati u vremenu od njihove posljednje prijave. Zapisivanje — Prijetnja će često pokušati pokriti svoje tragove manipuliranjem log datotekama:

- Nedostajući log podaci — ovo bi moglo značiti da je log datoteka izbrisana. Budući da je ovo lako otkriti,

sofisticiranija prijetnja uklonit će log unose. To bi moglo biti naznačeno neobičnim prazninama između vremena log unosa. Najsofisticiranija vrsta napada krivotvorit će log unose da sakrije zlonamjernu aktivnost.

- Zapisivanje izvan ciklusa — prijetnja također može manipulirati sistemskim vremenom ili promijeniti

vremenske oznake log unosa kao sredstvo skrivanja aktivnosti.

Lekcija 13B

Indikatori fizičkih i mrežnih napada

Pregled lekcije

Lokacije i uredi tvrtki i njihove mreže pružaju široku površinu napada za prijetnje. Razumijevanje kako napadi uskraćivanjem usluge, on-path i napadi temeljeni na vjerodajnicama funkcioniraju i koji su indikatori tih napada ključno je za učinkovit odgovor na incidente.

Fizički napadi

Fizički napad je onaj usmjeren prema infrastrukturi kabela, hardverskim uređajima ili okruženju lokacije objekata koji hostiraju mrežu. Gruba sila — Grubi fizički napadi uključuju:

- Razbijanje hardverskog uređaja za izvođenje fizičkog uskraćivanja usluge (DoS).
- Ulazak u prostorije ili ormarima prisiljavanjem brave ili prolaza. Ovo je vjerojatno

indikator krađe ili neovlaštene izmjene. Sprečavanje krađe je često nemoguće garantirati, pa je znanje da je nešto ukradeno važno za stvari poput izvješćivanja o kršenju podataka i poništavanja pristupnih kartica.

Radio Frequency ID (RFID) je sredstvo kodiranja informacija u pasivne oznake. Kada je čitač u dometu oznake, proizvodi elektromagnetski val koji napaja oznaku i prenosi kodirane podatke. RFID se koristi u pristupnim karticama, naljepnicama za praćenje imovine i nekim platnim sustavima. Napadi na RFID sustave uključuju:

- Kloniranje kartice — ovo se odnosi na izradu jedne ili više kopija postojeće kartice. Izgubljena ili ukradena

kartica bez kriptografskih zaštita može biti fizički duplicirana. Gubitak kartice treba odmah prijaviti kako bi se mogla opozvati i izdana nova.

- Skimming — ovo se odnosi na korištenje lažnog čitača za snimanje detalja kartice ili značke, koji

se zatim koriste za programiranje duplikata. Neke vrste kartica blizine mogu biti dosta lako natjerane na emitiranje vjerodajnica na prijenosni RFID čitač koji prijetnja može

sakriti.

Mrežni napadi

Mrežni napad je opća kategorija za niz strategija i tehnika koje prijetnje koriste za ometanje ili dobivanje pristupa sustavima putem mrežnog vektora. Uobičajene faze mrežnog napada uključuju:

- Izviđanje je mjesto gdje prijetnja koristi alate za skeniranje kako bi saznala o mreži.

Otkrivanje hosta identificira koje su IP adrese u upotrebi. Otkrivanje usluge identificira koji TCP ili UDP portovi su otvoreni na određenom hostu. Uzimanje otisaka identificira vrstu aplikacije ili operativnog sustava koji se koriste.

- Prikupljanje vjerodajnica je vrsta izviđanja gdje prijetnja pokušava saznati

lozinke ili kriptografske tajne koje će im omogućiti dobivanje autentificiranog pristupa mrežnim sustavima.

- Uskraćivanje usluge (DoS) u mrežnom kontekstu odnosi se na napade koji uzrokuju da hostovi i usluge

postanu nedostupni. Ova vrsta napada može biti otkrivena alatima za nadzor koji izvješćuju kada host ili usluga ne odgovaraju ili pate od abnormalno visokih volumena prometa.

- Naoružavanje, isporuka i kršenje odnose se na tehnike koje omogućavaju prijetnji da dobije

pristup bez autentifikacije. To obično uključuje različite vrste zlonamjernog koda usmjerene na ranjivu aplikaciju hosta ili uslugu putem mreže.

- Naredbe i kontrola (C2 ili C&C), odašiljanje i ustrajnost odnose se na tehnike i

zlonamjerni kod koji omogućava prijetnji udaljeno upravljanje kompromitiranim hostom i održavanje pristupa u dužem vremenskom periodu.

korištenjem enkriptiranih HTTPS veza. Otkrivanje ove vrste aktivnosti obično ovisi o identifikaciji anomalnih krajnjih točaka veze, poput veza s IP adresama u zemljama ili regijama s kojima organizacija normalno ne komunicira.

- Lateralno kretanje, pivoting i eskalacija privilegija odnose se na tehnike koje omogućavaju prijetnji

kretanje s hosta na host unutar mreže ili iz jednog mrežnog segmenta u drugi, te dobivanje šire i više razine dozvola za sustave i usluge po cijeloj mreži.

- Eksfiltracija podataka odnosi se na dobivanje informacijske imovine i kopiranje na napadačevo

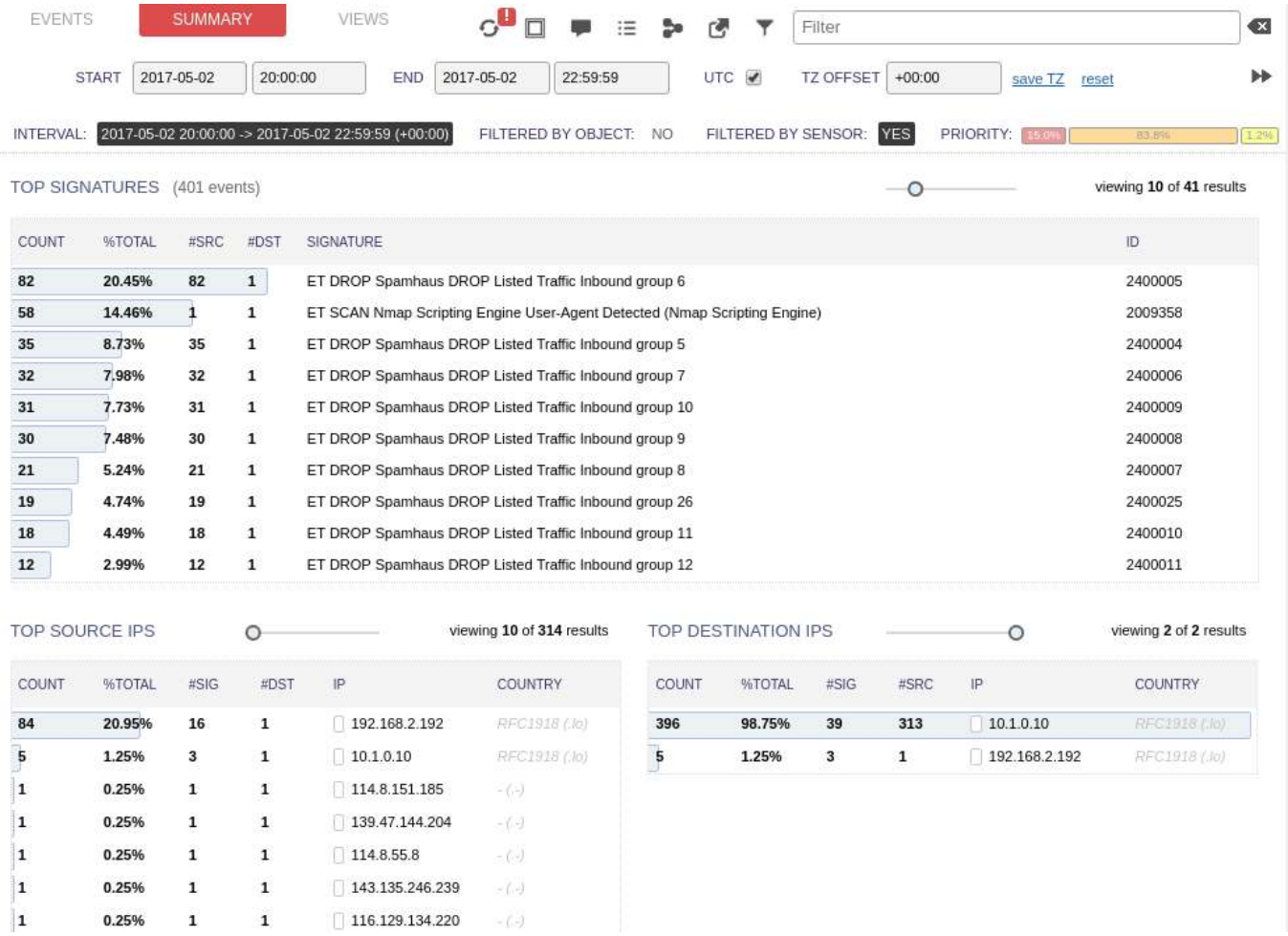
udaljeno računalo. Anomalni veliki prijenosi podataka mogli bi biti indikator eksfiltracije, ali prijetnja može izvesti napad tajno, pomičući samo male količine podataka odjednom.

Distribuirani napadi uskraćivanjem usluge

Napad uskraćivanjem usluge (DoS) je sve što smanjuje dostupnost resursa. DoS napadi mogu ciljati fizički hardver i infrastrukturu, ali su češće usmjereni prema računalnim sustavima i mrežnim uslugama. Distribuirani DoS (DDoS) napad je gdje se napad provodi od strane botnet-a s više strojeva.

Pojačani napadi

Napad pojačanjem vrsta je reflektiranog napada koji cilja slabosti u specifičnim protokolima aplikacija kako bi napad bio učinkovitiji u trošenju ciljnih resursa. DNS pojačanje i NTP pojačanje su uobičajeni primjeri.

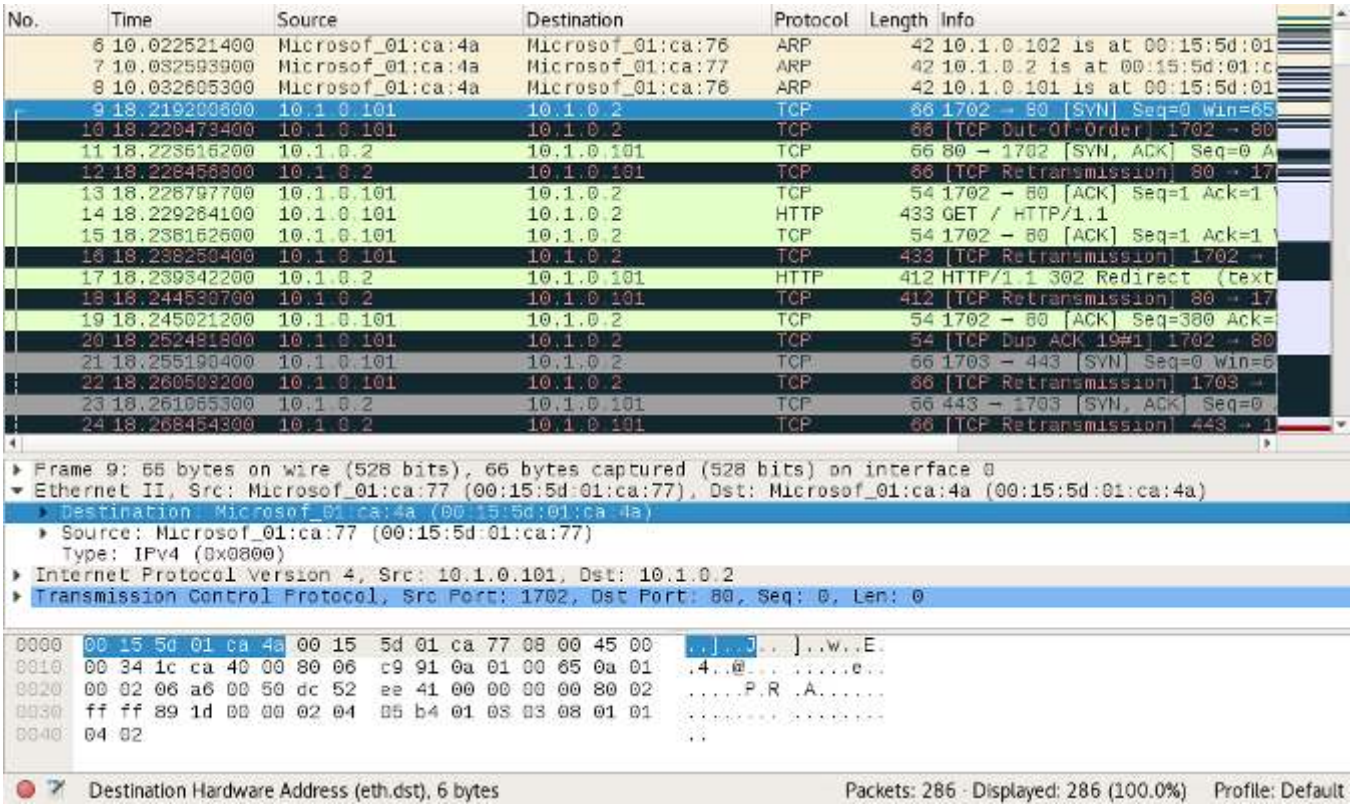


Snimak zaslona korišten uz dopuštenje Security Onion.

On-path napadi

On-path napad je situacija gdje prijetnja zauzima poziciju između dva hosta i transparentno hvata, nadzire i prosljeđuje svu komunikaciju između njih. Budući da je on-path napadač u poziciji da vidi sav promet između dva hosta, može prikupljati vjerodajnice i podatke.

Na primjer, on-path host može prezentirati radnoj stanici lažiranu web formu kako bi pokušao snimiti korisničku vjerodajnicu. Ovaj napad se naziva i adversary-in-the-middle (AiTM) napad ili man-in-the-middle (MitM) napad.



Snimak zaslona korišten uz dopuštenje wireshark.org.

Ovaj snimak zaslona prikazuje pakete snimljene tijekom tipičnog ARP trovanja napadačkog napada:

- U okvirima 6-8, napadačev stroj (s MAC adresom koja završava na :4a) usmjerava gratuitne ARP

odgovore prema ostalim hostovima (:76 i :77), tvrdeći da ima IP adrese .2 i .102. Ovaj obrazac gratuitnog ARP prometa indikator je napada.

- U okviru 9, .101/:77 host pokušava poslati paket prema .2 hostu, ali ga prima

napadačev host (s odredišnom MAC :4a).

- U okviru 10, napadačev host retransmitira okvir 9 prema stvarnom .2 hostu. Wireshark boji

okvir crno i crveno kako bi istaknuo retransmisiju.

- U okvirima 11 i 12, vidljiv je odgovor od .2, primljen od strane napadačevog hosta u okviru 11

i retransmitiran legitimnom hostu u okviru 12. Uobičajeni cilj bit će zadani prolaz podmreže (usmjernik koji pristupa ostalim mrežama). Ako ARP napad trovanja uspije

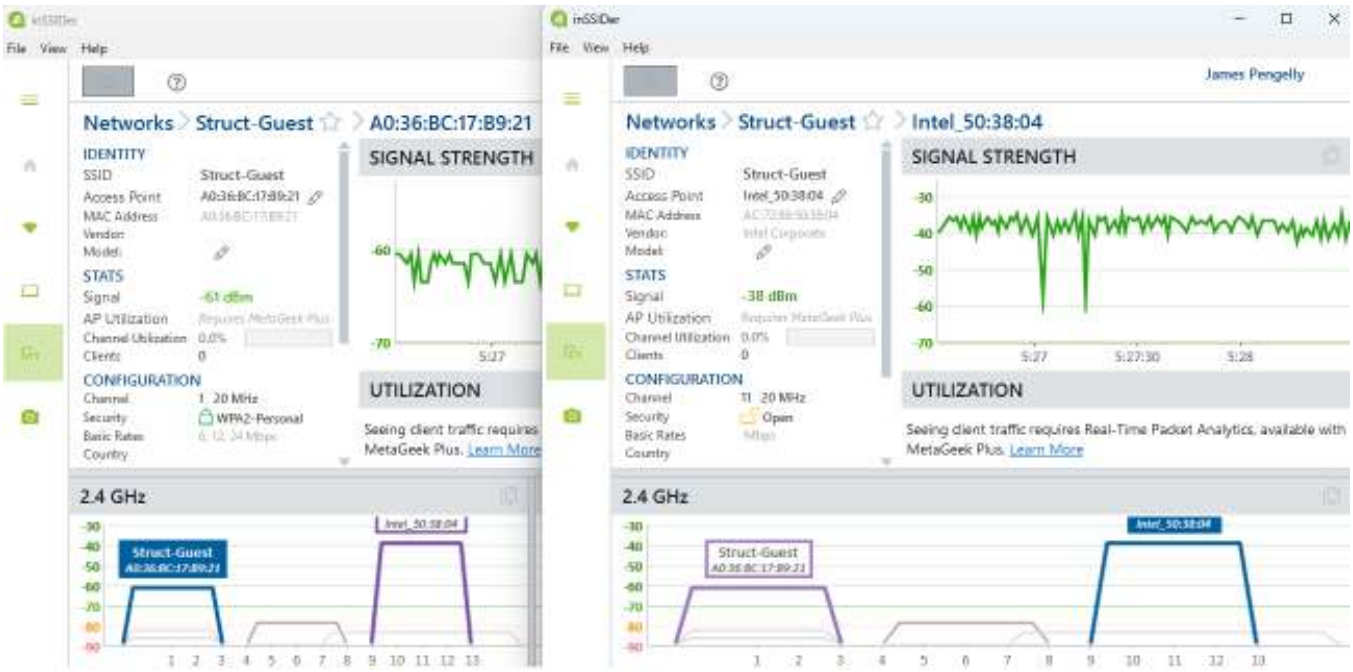
Napadi na Domain Name System

DNS (sustav naziva domena) rješava zahtjeve za nazvanim hostovima i uslugama u IP adrese. Razrješavanje naziva je kritična metoda adresiranja na Internetu i u privatnim mrežama. Napadi na DNS mogu biti identificirani nadzorom DNS log podataka i prometa radi anomalija:

- Vrste upita koje je host uputio DNS-u.
- Hostovi koji komuniciraju sa sumnjivim rasponima IP adresa ili domenama.

- Statistički anomalije poput naglih skokova ili konzistentno velikih brojeva neuspjelih DNS pretraga,

što može ukazivati na računala zaražena zlonamjernim softverom, pogrešno konfigurirana ili pokretanje zastarjelih ili neispravnih aplikacija. DNS je također popularan izbor za implementaciju naredbi i kontrole (C2).



Bežični napadi

Bežične mreže predstavljaju posebne sigurnosne izazove i često su vektor za različite vrste napada. Lažne pristupne točke — Lažna pristupna točka je ona koja je instalirana na mreži bez znanja administratora. Može ju instalirati zaposlenik koji želi bolji Wi-Fi signal, ili je instalira napadač. U svakom slučaju, lažna pristupna točka može biti koristite za presretanje ili manipulaciju mrežnim prometom.

Lažna hardverska pristupna točka može biti identificirana kroz fizičke preglede. Postoje i različiti Wi-Fi analizatori i bežični sustavi za zaštitu od upada koji mogu otkriti lažne

pristupne točke. Mogu bilježiti upotrebu SSID-ova s typosquattingom i nepoznate i duplikate (lažirane) MAC adrese. U poslovnoj mreži, pristupne točke su obično spojene na preklopnike koji mogu biti konfigurirani za otkrivanje neovlaštenih pristupnih točaka.

Napadi lozinkama

Kada korisnik odabere lozinku, vrijednost u čistom tekstu pretvara se u kriptografski hash. To znači da u teoriji nitko osim korisnika (čak ni administratori sustava) ne bi trebao znati lozinku u čistom tekstu. Međutim, napadači mogu pokušati otkriti lozinke koristeći različite tehnike napada:

Offline napadi

Offline napad znači da je napadač uspio pribaviti bazu podataka hash lozinki, poput %SystemRoot%\System32\config\SAM ili %SystemRoot%\NTDS\NTDS.DIT datoteka na Windows sustavima.

revizijski log sustava koji bilježi zlonamjerni pristup računa jednoj od ovih datoteka. Prijetnje također mogu čitati vjerodajnice iz memorije hosta, u kom slučaju jedini pouzdani indikator je anomalna aktivnost procesa.

Napadi ponavljanjem vjerodajnica

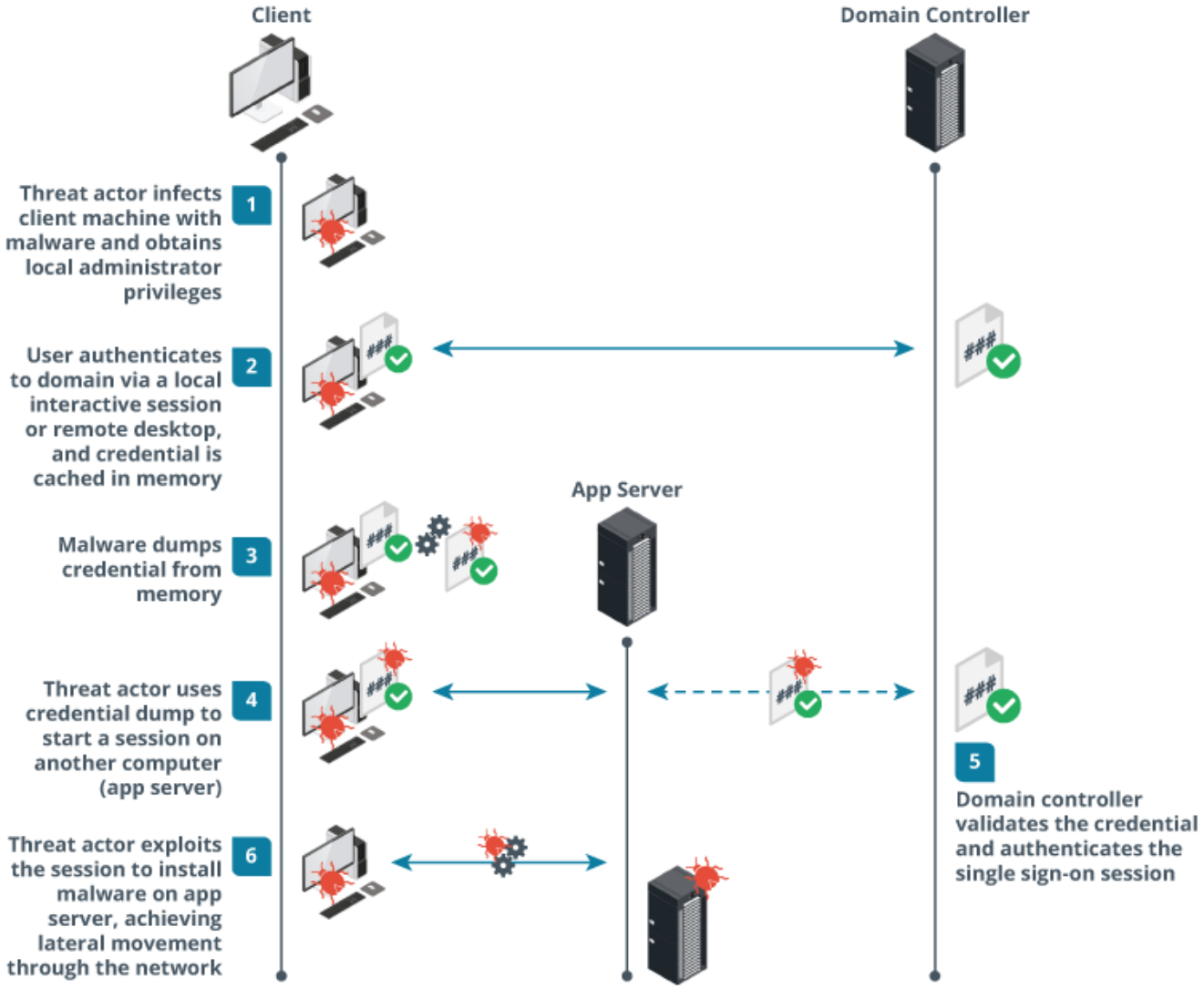
Prijetnja može uspostaviti oslonac na mreži kompromitiranjem jedne radne stanice putem zlonamjernog softvera ili napada lozinkom. Jednom kada je uspostavljen početni oslonac, prijetnja može koristiti tehnike ponavljanja vjerodajnica za lateralno kretanje unutar mreže. Tehnike ponavljanja uključuju krađom sesijskih tokena, hash vrijednosti i Kerberos karata:

- Kerberos Ticket Granting Ticket (TGT) i ključ sesije. Ovo omogućava hostu traženje

ulaznica za usluge za pristup aplikacijama.

- Ulaznice za usluge za aplikacije gdje je korisnik pokrenuo sesiju.
- NT hash lokalnih i domenskih korisničkih i servisnih računa koji su trenutno prijavljeni, bilo

interaktivno ili daljinski putem mreže. Rane Windows poslovne mreže koristile su NT LAN Manager (NTLM) izazov i odgovor autentifikaciju. Dok je NTLM protokol zastario, i dalje se nalazi u različitim mrežnim postavkama.



Naslijeđena NTLM autentifikacija često je onemogućena jer predstavlja visoki sigurnosni rizik. Ostale vrste ponavljanja vjerodajnica usmjerene su prema Kerberos autentifikaciji i autorizaciji. Na primjer, napad pass-the-ticket koristi ukradene Kerberos karte za pristup resursima bez poznavanja izvorne lozinke.

jedan uspješan je postignut. Napad je nazvan po Birthday paradoksu. Ovaj paradoks pokazuje da bi računalno vrijeme potrebno za grubom silom kolizije moglo biti manje od

mehanizmom koji može generirati 264 varijacija. Izračun 264 varijacija zahtijevat će mnogo manje

vremena od izračunavanja 2128 varijacija. Napadi koji iskorištavaju kolizije su teško izvedivi, ali princip iza napada informira o potrebi korištenja metoda autentifikacije s dovoljno dugim hash vrijednostima.

- Shellcode — ovo je kompaktni komad koda koji se koristi kao korisni teret dizajniran za iskorištavanje

ranjivosti u OS-u ili legitimnoj aplikaciji za dobivanje neovlaštenih privilegija, ili stvaranje backdoor-a na hostu ako se pokrene kao trojanac.

- Istovarivanje vjerodajnica — zlonamjerni softver može pokušati pristupiti datoteci vjerodajnica (SAM na lokalnoj

Windows radnoj stanici) ili njuškati vjerodajnice koje drži u memoriji sistemski proces lsass.exe. Osim toga, DCSync napad pokušava prevariti domenski kontroler da replicira svoje podatke korisnika napadaču.

- Pivoting/lateralno kretanje/napad iznutra — opća procedura je korištenje oslonca za

udaljeno izvođenje procesa, koristeći alat kao što su PsExec ili PowerShell. Napadač može tražiti podatkovne imovine ili može pokušati proširiti pristup mijenjanjem sigurnosne konfiguracije sustava.

- Ustrajnost — ovo je mehanizam koji omogućava backdoor-u prijetnje da se ponovo pokrene ako se

host ponovo pokrene ili se korisnik odjavi. Tipične metode su korištenje AutoRun ključeva u registru, dodavanje planiranog zadatka, ili korištenje WMI pretplate na događaje.

Lekcija 13C

Indikatori napada na aplikacije

Pregled lekcije

Web aplikacija izlaže mnoga sučelja javnim mrežama. Napadači mogu iskorištavati ranjivosti u softveru servera i sigurnosti klijentskog preglednika za izvođenje injekcije i napada na sesiju. Razumijevanje ovih vrsta napada i kako ih identificirati ključno je za zaštitu web aplikacija.

Napadi na aplikacije

Napad na aplikaciju cilja ranjivost u OS-u ili softveru aplikacije. Ranjivost aplikacije je dizajnerska greška koja može uzrokovati da sigurnosni model aplikacije bude kompromitiran. Napadi na aplikacije mogu biti:

- Kompromitiranje operativnog sustava ili aplikacija trećih strana na mrežnom hostu iskorištavanjem

trojanaca, zlonamjernih privitaka ili ranjivosti preglednika. To omogućava prijetnji dobivanje oslonca na lokalnoj mreži.

- Kompromitiranje sigurnosti web stranice ili web aplikacije. To prijetnji omogućava dobivanje

kontrole nad web hostom i ili krađe podataka s njega ili korištenja za daljnje prodiranje u mrežu. Povećan broj rušenja i grešaka aplikacija može pružiti opći pokazatelj aktivnosti napada.

Aplikacija ili proces mora imati privilegije za čitanje i pisanje podataka i izvođenje funkcija. Ovisno o tome kako je softver napisan, proces može se izvoditi koristeći sistemski račun, korisnički račun ili poseban servisni račun. Eskalacija privilegija je napad koji nastoji povećati razinu privilegija napadača:

- Vertikalna eskalacija privilegija (ili elevacija) je situacija kada korisnik ili aplikacija može pristupiti

funkcionalnosti ili podacima koji im ne bi trebali biti dostupni. Na primjer, proces može se izvoditi s privilegijama lokalnog administratora, ali ranjivost dopušta proizvoljnom kodu da

se izvrši s privilegijama System.

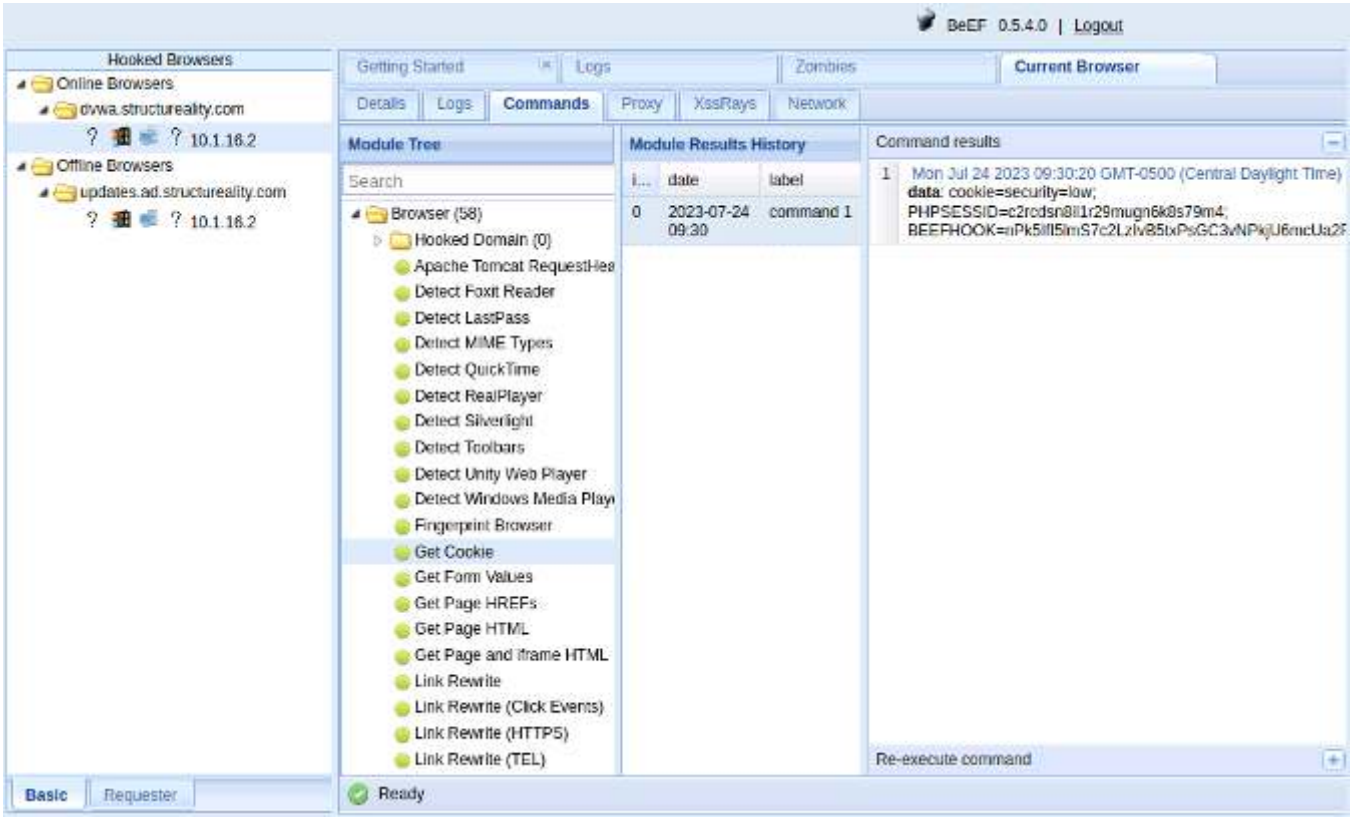
- Horizontalna eskalacija privilegija je situacija kada korisnik pristupa funkcionalnosti ili podacima namijenjenim

drugom korisniku. Na primjer, putem procesa koji se izvodi s privilegijama lokalnog administratora na klijentskoj radnoj stanici, proizvoljni kod je u mogućnosti izvesti se kao domenski račun na drugom hostu.

Napadi ponavljanjem

U kontekstu web aplikacije, napad ponavljanjem najčešće znači iskorištavanje sesija temeljenih na kolačićima. HTTP je nominalno protokol bez stanja, što znači da server ne može lako razlikovati zahtjeve od istog korisnika. Za upravljanje stanjem sesije, aplikacija može koristiti kolačiće za pohranu identifikatora sesije.

Korištenje Browser Exploitation Framework (BeEF) za dobivanje kolačića sesije iz preglednika.



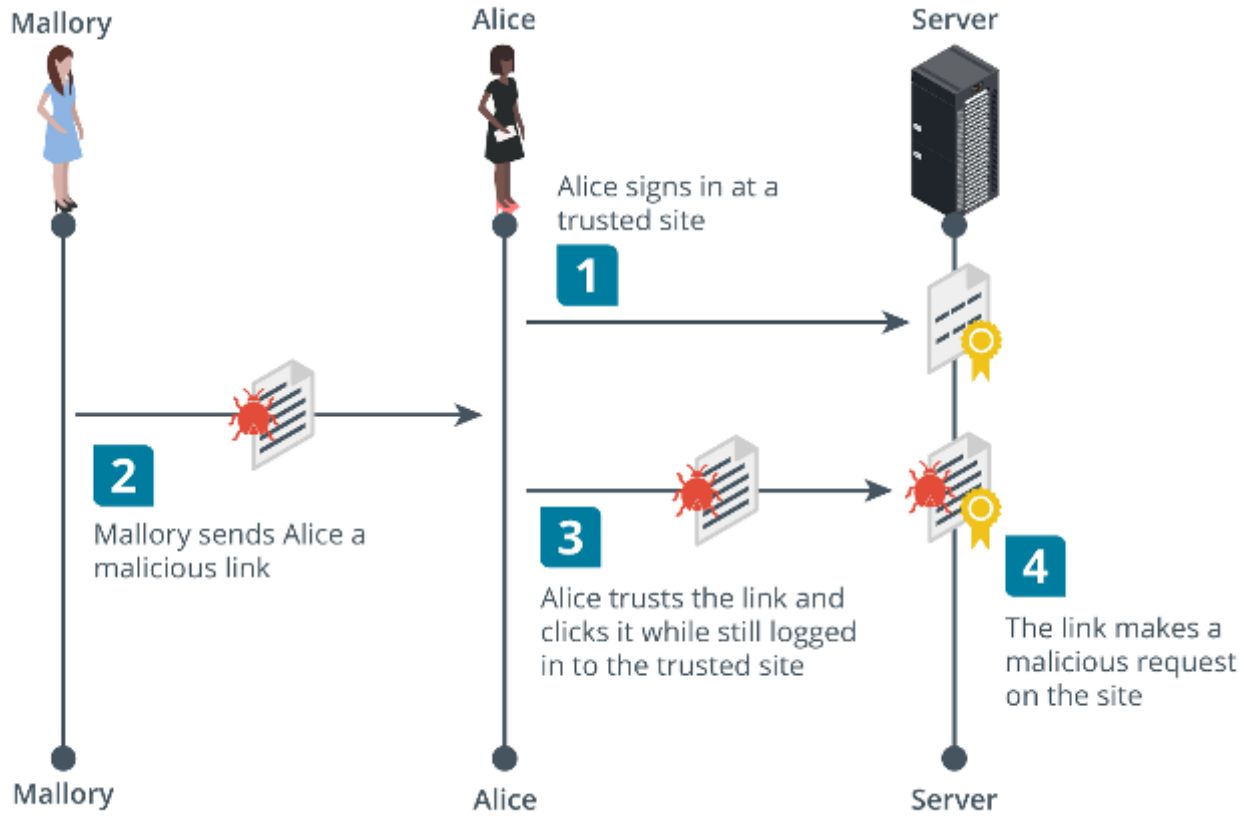
Napadači mogu hvatati kolačiće njuškanjem mrežnog prometa putem on-path napada ili kada se šalju putem nezaštićene mreže, poput javnog Wi-Fi hotspota. Zlonamjerni softver koji zarazi host također može krasti kolačiće iz datoteka ili memorije preglednika.

Napadi predviđanja sesije fokusiraju se na identifikaciju mogućih slabosti u generiranju tokena koji će napadaču omogućiti predviđanje vrijednosti koje će uspostaviti sesije u budućnosti.

Napadi krivotvorenjem

Za razliku od napada ponavljanjem, napad krivotvorenjem otima autentificiranu sesiju za izvođenje neke akcije bez pristanka korisnika. Cross-Site Request Forgery — CSRF napad je gdje zlonamjerna web stranica, e-pošta ili skript uzrokuje da preglednik korisnika izvede radnju na drugoj stranici koja je trenutno autentificirana.

Primjer cross-site request forgery napada.

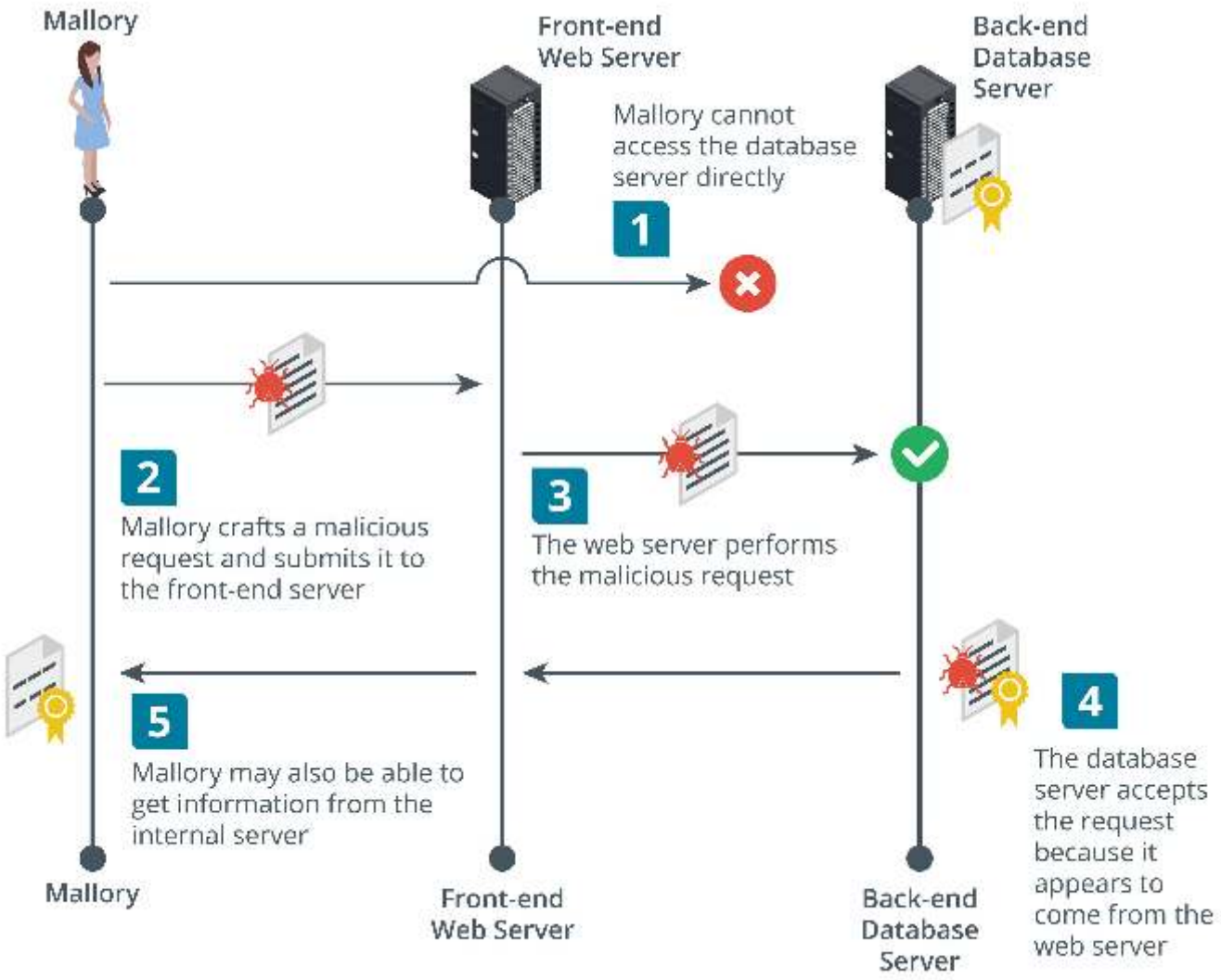


© Slike 123RF.com.

Server-Side Request Forgery

SSRF napad uzrokuje da serverska aplikacija obradi proizvoljni zahtjev koji cilja drugu uslugu. Ciljna usluga mogla bi biti na internoj mreži, što bi napadaču omogućilo pristup internim resursima koji inače ne bi bili dostupni s interneta.

Primjer server-side request forgery napada.



© Slike 123RF.com.

Napadi injekcijom

Napadi poput ponavljanja sesije, CSRF-a i većina vrsta XSS-a su napadi na strani klijenta. To znači da izvode proizvoljni kod u pregledniku. Napad na strani servera izvodi se na samom serveru. SQL injekcija je uobičajeni napad na strani servera koji iskorištava nesigurni kôd baze podataka.

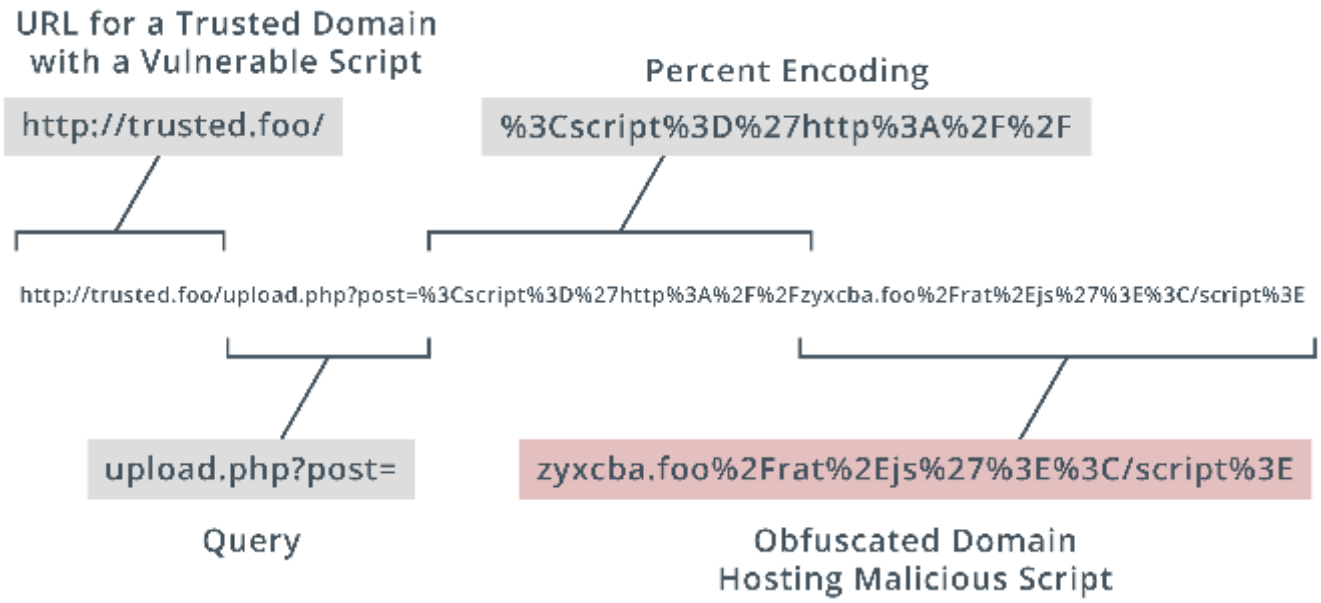
ili validacija unosa ranjiva je na lažiranje, krivotvorenje zahtjeva i injekciju proizvoljnih podataka ili koda. Na primjer, XML External Entity (XXE) napad ugrađuje zahtjev za lokalnom datotekom u XML dokument koji server zatim obradi, što napadaču omogućuje čitanje lokalnih datoteka s poslužitelja.

Napadi prelaženjem direktorija i injekcijom naredbi

Prelazak direktorija je još jedna vrsta napada injekcijom koji se izvodi protiv web servera. Prijetnja podnosi zahtjev za datotekom koja koristi relativne staze (../../../) za izlazak iz korijenskog direktorija weba i pristup datotekama izvan weba. Injekcija naredbi pokušava uzrokovati da server izvede OS shell naredbe.

Napad injekcijom naredbi pokušava uzrokovati da server izvede OS shell naredbe i vrati izlaz pregledniku. Kao i kod prelaska direktorija, web server bi normalno trebao biti konfiguriran za sprečavanje ove vrste napada, ali ranjivosti u kodu aplikacije ili njena

konfiguracija mogu to dopustiti.



Kao dio analize URL-a, važno je razumjeti kako HTTP funkcionira. HTTP sesija počinje s klijentom (user-agent, poput web preglednika) koji upućuje zahtjev HTTP serveru. Server odgovara statusnim kodom i tijelom odgovora. Uobičajene HTTP metode zahtjeva uključuju:

- GET — dohvat resursa.
- POST — slanje podataka serveru za obradu od strane traženog resursa.
- PUT — kreiranje ili zamjena resursa.

Podaci se mogu predati serveru ili korištenjem POST ili PUT metode i HTTP zaglavlja i tijela, ili kodiranjem podataka unutar URL-a koji se koristi za pristup resursu.

Procentno kodiranje

URL može sadržavati samo rezervirane i nerezervirane znakove iz standardnog skupa. Rezervirani znakovi koriste se kao razdjelnici unutar URL sintakse i trebaju biti kodirani ako se koriste kao dio podataka. Procentno kodiranje (URL kodiranje) zamjenjuje nesigurne znakove s % praćenim heksadecimalnim ASCII kodom znaka.

Dnevnici web servera

Web serveri su obično konfigurirani za bilježenje HTTP prometa koji nailazi na grešku ili promet koji odgovara nekom unaprijed definiranom skupu pravila. Ovo može sačuvati indikatore napada, poput pokušaja prelaška direktorija ili SQL injekcije.

```
203.0.113.100 [18:52:38] "GET / HTTP/1.1" 200 1352 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
203.0.113.100 [18:52:38] "GET /images/icon-email.png HTTP/1.1" 200 747 "http://www.structureality.com/" "Mozilla/5.0..."
203.0.113.100 [18:52:38] "GET /images/icon-receiver.png HTTP/1.1" 200 1383 "http://www.structureality.com/" "Mozilla/5.0..."
203.0.113.100 [18:52:38] "GET /images/structureality-logo-banner.png HTTP/1.1" 200 151731 "http://www.structureality.com/" "Mozilla/5.0..."
203.0.113.100 [18:52:38] "GET /images/icon-post.png HTTP/1.1" 200 1021 "http://www.structureality.com/" "Mozilla/5.0..."
203.0.113.100 [18:52:38] "GET /favicon.ico HTTP/1.1" 200 1450 "http://www.structureality.com/" "Mozilla/5.0..."
203.0.113.66 [10:53:04] "GET / HTTP/1.1" 200 2965 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:Port Check)"
203.0.113.66 [10:53:05] "GET /cgi.cgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
203.0.113.66 [10:53:05] "GET /webcgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
203.0.113.66 [10:53:05] "GET /bin/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
203.0.113.66 [10:53:05] "GET /cgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
203.0.113.66 [10:53:05] "GET /robots.txt HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:robots)"
203.0.113.66 [10:53:05] "GET /crossdomain.xml HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:crossdomain)"
203.0.113.66 [10:53:05] "GET / HTTP/1.1" 200 2964 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:origin_reflection)"
```

Sažetak

Trebali biste biti u mogućnosti identificirati indikatore zlonamjernog softvera, fizičkih, mrežnih, kriptografskih, lozinki i vrsta napada na aplikacije.

Smjernice za implementaciju analize indikatora

Slijedite ove smjernice za podršku analize različitih vrsta napada:

- Razmotrite implementaciju paketa za zaštitu krajnjih točaka temeljenih na ponašanju koji mogu obaviti učinkovitije

otkrivanje beznačajnog zlonamjernog softvera.

- Razmotrite postavljanje sandboxa s alatima za analizu za istraživanje sumnjivog ponašanja procesa.
- Razmotrite korištenje podatkovnih izvora o prijetnjama za pomoć s identifikacijom dokumentiranih i objavljenih

indikatora.

- Implementirajte revizijske preglede i zapisivanje stranice za identifikaciju grube sile, ekoloških i RFID

kloniranja fizičkih napada.

- Pripremite knjige pravila i obavještajne podatke o prijetnjama za pomoć s analizom napada:
- Potrošnja resursa, anomalije datotečnog sustava, nedostupnost resursa i nedostajuće/izvan-

ciklusni indikatori zapisivanja kompromitiranja sustava.

- Blokada, istovremena sesija i indikatori nemogućeg putovanja kompromitiranja računa.
- Karakteristike bloatwarea, virusa, crva, trojanca, špijunskog softvera, keyloggera, ransomwarea i

vrsta zlonamjernog softvera logičke bombe.

- Indikatori potrošnje resursa mrežnih uređaja DDoS napada, uključujući reflektirane i

pojačane vrste.

- Mrežni nadzor i log indikatori on-path, DNS, bežičnih, ponavljanja vjerodajnica,

kriptografskog degradiranja, raspršivanja lozinki i napada grubom silom lozinki.

- Indikatori nadzora hosta i zapisivanja injekcije, prekoračenja međuspremnika, ponavljanja, eskalacije privilegija,

krivotvorenja i napada prelazenjem direktorija na aplikacije.

Modul 14

Sažmite koncepte sigurnosnog upravljanja

Pregled modula

Sigurnosno upravljanje je kritičan aspekt ukupnog sigurnosnog položaja organizacije, pružajući okvir koji vodi upravljanje kibernetičkim sigurnosnim rizicima. Uključuje razvijanje i implementaciju sigurnosnih politika, standarda i procedura, kao i osiguravanje usklađenosti s relevantnim zakonima i propisima. Učinkovito upravljanje sigurnošću pomaže organizacijama u zaštiti imovine, upravljanju rizicima i postizanju sigurnosnih ciljeva.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Identificirajte razliku između politika, procedura, standarda i smjernica.
- Saznajte o složenostima pravnog okruženja koje utječe na sigurnosne operacije.
- Istražite prakse upravljanja i odgovornosti.

Lekcija 14A

Politike, standardi i procedure

Pregled lekcije

Politike, standardi i procedure tri su ključne komponente koje čine temelj sigurnosnog programa organizacije. Politike su dokumenti visoke razine koji definiraju opće smjerove i principe sigurnosti. Standardi specificiraju tehničke zahtjeve i konfiguracije. Procedure pružaju korak-po-korak upute za implementaciju politika i standarda.

Politike

Organizacijske politike su vitalne u uspostavljanju učinkovitog upravljanja i osiguravanju organizacijske usklađenosti. One čine okvir za operacije, donošenje odluka i ponašanje unutar organizacije. Razne politike relevantne za sigurnost uključuju:

- Politika prihvatljive upotrebe (AUP) — Ova politika opisuje prihvatljive načine korištenja mreže

i računalnih sustava definirajući što predstavlja prihvatljivo ponašanje

korisnika. AUP-ovi obično adresiraju ponašanje pregledavanja, prikladni sadržaj, preuzimanje softvera i rukovanje osjetljivim informacijama. Cilj AUP-a je osigurati da korisnici ne sudjeluju u aktivnostima koje bi mogle ugroziti sigurnost mreže ili izložiti organizaciju pravnoj odgovornosti.

- Politike informacijske sigurnosti — To su politike koje organizacija kreira kako bi osigurala da

svi korisnici informacijske tehnologije poštuju pravila i smjernice vezane uz sigurnost informacija pohranjenih unutar okruženja ili sfere vlasti organizacije.

- Planovi poslovnog kontinuiteta i kontinuiteta operacija (COOP) — Politike poslovnog kontinuiteta i

COOP fokusiraju se na kritične procese koji moraju ostati operativni tijekom i nakon značajnog poremećaja poput prirodne katastrofe ili kibernetičkog napada.

- Oporavak od katastrofe — Ove politike detaljno opisuju korake potrebne za oporavak od katastrofičnog

događaja poput prirodne katastrofe, kvarova glavnog hardvera ili značajnog sigurnosnog kršenja. Cilj je što brže i učinkovitije obnavljanje operacija.

- Odgovor na incidente — Ova politika opisuje procese koje treba slijediti nakon sigurnosnog

kršenja ili kibernetičkog napada. Detaljno opisuje korake za identifikaciju, istraživanje, kontrolu i smanjenje utjecaja incidenata.

- Životni ciklus razvoja softvera (SDLC) — SDLC politike uređuju razvoj softvera

unutar organizacije. Ove politike pružaju strukturirani plan koji detaljno opisuje faze razvoja od početne analize zahtjeva do održavanja nakon implementacije.

- Upravljanje promjenama — Politike upravljanja promjenama opisuju kako se promjene IT sustavima i

softveru zahtijevaju, pregledaju, odobravaju i implementiraju, uključujući sve zahtjeve za dokumentacijom. Smjernice — Smjernice opisuju preporuke koje usmjeravaju akcije u određenom smjeru.

Procedure

Politike i smjernice postavljaju okvir za ponašanje. Procedure definiraju korak-po-korak upute i kontrolne liste za osiguravanje da je zadatak obavljen na način koji ispunjava politiku i standarde organizacije.

- Zapošljavanje — lociranje i odabir osoba za rad na posebnim radnim mjestima. Sigurnost

ovdje uključuje provjeru kandidata i provjeru pozadine.

- Operacije (rad) — često je odjel HR koji upravlja komunikacijom

politike i obuke zaposlenicima. Stoga je ključno da HR menadžeri razumiju politike organizacije i mogu ih učinkovito komunicirati.

- Prekid rada ili razdvajanje (otpuštanje ili umirovljenje) — bez obzira napušta li zaposlenik volonterski ili

nevolonterski, prekid rada je složen proces s brojnim sigurnosnim implikacijama. Provjera pozadine utvrđuje da je osoba tko kaže da jest i

- Sigurni prijenos vjerodajnica — kreiranje i sigurno slanje početne lozinke ili izdavanje

pametne kartice. Proces treba zaštitu od nepoštenih administratorskih zaposlenika. Novokreirani računi s jednostavnim ili zadanim lozinkama lako iskoristivi su backdoor.

- Dodjela imovine — opremanje računala ili mobilnih uređaja korisniku ili dogovor o korištenju

uređaja koje donose sami (BYOD).

- Obuka/politike — raspoređivanje odgovarajuće podizanje sigurnosne svijesti i obuku relevantnu za ulogu i

certifikaciju. IAM automatizacija može ubrzati postupak uvođenja automatizacijom zadataka provizioniranja i upravljanja pristupom povezanih s novim zaposlenicima.

i poboljšanje problematičnih područja. Korištenjem knjiga pravila, organizacije mogu pratiti upotrebu i učinkovitost procedura tijekom vremena i modificirati ih po potrebi za poticanje okruženja kontinuiranog poboljšanja.

- Upravljanje računom — onemogućite korisnički račun i privilegije. Osigurajte da je svaka informacijska

imovina kreirana ili kojom upravlja zaposlenik ali je u vlasništvu tvrtke dostupna (u smislu enkripcijskih ključeva ili datoteka zaštićenih lozinkom).

- Imovina tvrtke — povrat mobilnih uređaja, ključeva, pametnih kartica, USB medija itd. Zaposlenik

treba potvrditi (a u nekim slučajevima i dokazati) da nije zadržao kopije nijedne informacijske imovine.

- Osobna imovina — brisanje korporativnih podataka i aplikacija s uređaja zaposlenika. Zaposlenik

može biti dozvoljena zadržati neke informacijske imovine (poput osobnih e-pošta ili kontakt informacija), ovisno o politikama na snazi.

Standardi

Standardi definiraju očekivani ishod zadatka, poput određenog stanja konfiguracije za server ili referentnih performansi za uslugu. Odabir i primjena standarda pomažu organizacijama u postizanju konzistentnih i provjerivih rezultata.

propisi o zaštiti podataka. Ovi zahtjevi često zahtijevaju implementaciju specifičnih standarda ili korištenje smjernica za postizanje usklađenosti. Industrija zdravstvene zaštite u Sjedinjenim Državama mora se pridržavati HIPAA, dok organizacije koje obrađuju platne kartice moraju biti usklađene s PCI DSS-om.

- ISO/IEC 27001 — Međunarodni standard koji pruža okvir sustava upravljanja informacijskom sigurnošću

(ISMS) kako bi osigurao da su na snazi odgovarajuće i proporcionalne sigurnosne kontrole.

- ISO/IEC 27002 — Ovo je prateći standard ISO 27001 i pruža detaljne smjernice

o specifičnim kontrolama koje treba uključiti u ISMS.

- ISO/IEC 27017 — Proširenje ISO 27001 i specifično za usluge u oblaku.
- ISO/IEC 27018 — Drugi dodatak ISO 27001, i specifičan za zaštitu osobnih

podataka koji mogu identificirati osobu (PII) u javnim oblacima.

- NIST (Nacionalni institut za standarde i tehnologiju) Posebna publikacija 800-63 — Američki

vladini standard za smjernice digitalnog identiteta, uključujući zahtjeve za lozinku i kontrolu pristupa.

- PCI DSS (Payment Card Industry Data Security Standard) — Standard za organizacije

koje rukuju kreditnim karticama od glavnih kartičnih davatelja, uključujući zahtjeve za zaštitu podataka vlasnika kartice.

- FIPS (Federal Information Processing Standards) — FIPS su standardi i smjernice

koje je razvio NIST za federalne računalne sustave u Sjedinjenim Državama koji specificiraju zahtjeve za kriptografiju.

ovi standardi pomažu organizacijama u procjeni njihovog pridržavanja najboljim praksama, identifikaciji nedostataka ili ranjivosti i demonstriranju predanosti održavanju sigurnog i usklađenog okruženja.

- Algoritmi hashiranja — Definira zahtjeve za hash funkcije koje se koriste za pohranu lozinki.
- Soljenje lozinke — Definira metode koje se koriste za zaštitu hash vrijednosti lozinki od rainbow

table napada.

- Sigurni prijenos lozinke — Definira metode za sigurni prijenos lozinke,

uključujući pojedinosti o odgovarajućim skupovima šifri.

- Resetiranje lozinke — Definira odgovarajuće metode provjere identiteta za zaštitu zahtjeva za resetiranje lozinke

od iskorištavanja.

- Upravitelji lozinkama — Definira zahtjeve za upravitelje lozinkama koje organizacije

mogu odabrati ugraditi. Standardi kontrole pristupa osiguravaju da samo ovlaštene osobe mogu pristupiti sustavima i podacima koji su im potrebni za obavljanje poslova.

- Modeli kontrole pristupa — Definira odgovarajuće modele pristupa za različite slučajeve upotrebe.

Primjeri uključuju kontrolu pristupa temeljena na ulogama (RBAC), diskrecijsku kontrolu pristupa (DAC) i mandatornu kontrolu pristupa (MAC).

- Provjera identiteta korisnika — Definira prihvatljive metode za provjeru identiteta prije dodjele

pristupa. Primjeri uključuju jednostavne lozinke, sigurnosne tokene, biometrijske podatke i druge metode.

- Upravljanje privilegijama — Definira metode za upravljanje korisničkim privilegijama kako bi se osiguralo

da imaju minimalni potrebni pristup.

- Protokoli autentifikacije — Definira specifične prihvatljive protokole autentifikacije, poput

Kerberosa, OAuth ili SAML.

- Upravljanje sesijama — Definira dopuštene prakse upravljanja sesijama, uključujući

zahtjeve za isteke sesija, sigurno generiranje i prijenos kolačića sesija i slične zahtjeve.

- Revizijski tragovi — Definira obavezne revizijske sposobnosti dizajnirane za pomoć u identifikaciji i

istraživanju sigurnosnih incidenata. Standardi fizičke sigurnosti štite podatkovne centre, serverske sobe, kabelske ormareve, kabliranje, hardver i infrastrukturu.

- Sigurnost zgrade — Metode za zaštitu objekata, uključujući sustave pristupa karticama, CCTV

nadzor i zaštitarsko osoblje.

- Sigurnost radne stanice — Standardi za fizičku zaštitu prijenosnih računala ili drugih prijenosnih uređaja.
- Sigurnost podatkovnog centra i serverske sobe — Definira zahtjeve za pristup karticama, biometriku

skeniranje, dnevnike prijave/odjave i escorted pristup za posjetitelje.

- Odlaganje opreme — Definira zahtjeve za sigurno odlaganje (ili ponovnu upotrebu)

opreme kako bi se osiguralo da su osjetljivi podaci nepovrativni.

- Upravljanje posjetiteljima — Definira zahtjeve za upravljanje posjetiteljima, poput postupaka prijave/odjave,

posjetiteljskih značka i zahtjeva za escorted pristup. Enkripcija štiti podatke od neovlaštenog pristupa i vitalna je za zaštitu podataka u mirovanju i u prijenosu.

- Algoritmi enkripcije — Definira dopuštene algoritme enkripcije, poput AES (Advanced

Encryption Standard) za simetričnu ili ECC za asimetričnu enkripciju.

- Duljina ključa — Definira minimalno dopuštene duljine ključeva za različite vrste enkripcije.
- Upravljanje ključevima — Definira kako se ključevi generiraju, distribuiraju, pohranjuju i mijenjaju.

Često uključuje zahtjeve za korištenjem sigurnih sustava za upravljanje ključevima, procedure za redovitu promjenu ključeva i procedure za njihov opoziv ako su kompromitirani.

Pravno okruženje

Odbori za upravljanje osiguravaju da se njihove organizacije pridržavaju svih primjenjivih zakona i propisa o kibernetičkoj sigurnosti kako bi ih zaštitili od pravne odgovornosti. Odbor za upravljanje mora biti svjestan pravnog okruženja koje se odnosi na sigurnost.

koncept i zahtijeva da prikupljanje i obrada osobnih informacija budu i sigurni i pošteni. Pravičnost i pravo na privatnost, kako je uspostavljeno propisima poput europske Opće uredbe o zaštiti podataka (GDPR) i Zakona o zaštiti potrošača Kalifornije (CCPA), ključna su razmatranja u upravljanju podacima.

Propisi i nacionalni, lokalni, regionalni i industrijski zakoni — Mnoge zemlje imaju zakone na nacionalnoj razini za podršku učinkovitim praksama kibernetičke sigurnosti i zaštitu podataka građana. Opseg ovih zakona varira, ali obično pokrivaju zahtjeve za zaštitu podataka, prijavljivanje kršenja podataka i standarde kibernetičke sigurnosti. Primjeri relevantnih propisa uključuju:

- Health Insurance Portability and Accountability Act (HIPAA) (Sjedinjene Države)
- The General Data Protection Regulation (GDPR) (Europska unija)

Financijske usluge

- Gramm-Leach-Bliley Act (GLBA) (Sjedinjene Države)
- Payment Card Industry Data Security Standard (PCI DSS) (Ugovorna obveza)

Telekomunikacije

- Communications Assistance for Law Enforcement Act (CALEA) (Sjedinjene Države)

Energetika

- North American Electric Reliability Corporation (NERC) (SAD, Kanada i Baja

California Norte, Meksiko) Obrazovanje i djeca

- Family Educational Rights and Privacy Act (FERPA) (SAD)

- Children's Internet Protection Act (CIPA) (SAD)
- Children's Online Privacy Protection Act (COPPA) (SAD)

Vlada

- Federal Information Security Modernization Act (FISMA) (SAD)
- Criminal Justice Information Services (CJIS) Security Policy (SAD)
- The Government Security Classifications (GSC) (Ujedinjena Kraljevina)

Propisi o kibernetičkoj sigurnosti su pravna pravila i smjernice koje formuliraju vlade i regulatorna tijela za zaštitu digitalnih informacija i sustava od kibernetičkih prijetnji. Postavljaju standarde, zahtjeve i prakse za organizacije. Neki od najutjecajnijih propisa o kibernetičkoj sigurnosti uključuju:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Modernization Act (FISMA)

Upravljanje i odgovornost

Prakse upravljanja osiguravaju da se organizacije pridržavaju svih primjenjivih zakona i propisa o kibernetičkoj sigurnosti kako bi ih zaštitili od pravne odgovornosti. Upravljanje

Krajolik kibernetičke sigurnosti stalno se razvija. Posljedično, organizacije moraju osigurati da su njihove politike, procedure, standardi i prakse pravne usklađenosti u skladu s tim razvojem. To zahtijeva redovitu reviziju i ažuriranje ovih dokumenata i praksi.

ovlast za donošenje odluka i odgovoran je za postavljanje strateškog smjera i politika organizacije. Ova odgovornost često zahtijeva od rukovoditelja donošenje kritičnih odluka o kibernetičkim rizicima, balansiranje sigurnosnih briga s poslovnim potrebama i osiguravanju da su na raspolaganju dovoljni resursi za kibernetičku sigurnost. Odbori za upravljanje mogu uključivati odbor za reviziju, odbor za upravljanje rizicima ili posebne odbore za kibernetičku sigurnost, ovisno o veličini i strukturi organizacije.

Vlasnik

Visokopozicionirani zaposlenik, poput direktora ili potpredsjednika, obično ima ulogu vlasnika i u konačnici je odgovoran za osiguravanje da su podaci na odgovarajući način zaštićeni. Vlasnik podataka ima konačnu odgovornost za odluke o zaštiti podataka i mora biti svjestan klasifikacije podataka i odgovarajućih kontrola.

Lekcija 14B

Upravljanje promjenama

Pregled lekcije

Upravljanje promjenama je sustavni pristup upravljanju svim promjenama napravljenim unutar IT infrastrukture. Njegov primarni cilj je minimiziranje rizika i poremećaja uz maksimiziranje vrijednosti i pogodnosti. Učinkovito upravljanje promjenama osigurava da se promjene uvode kontroliranim, sustavnim načinom koji minimizira potencijalne negativne učinke.

Programi upravljanja promjenama

Upravljanje promjenama igra vitalnu ulogu u sigurnosnim operacijama organizacije. Odnosi se na sustavni pristup koji upravlja svim promjenama na produkcijskom okruženju. Vrste promjena koje se upravljaju uključuju:

- Implementacije softvera
- Ažuriranja sustava
- Zakrpavanja softvera
- Zamjena ili nadogradnja hardvera
- Mrežne izmjene
- Promjene konfiguracije sustava
- Implementacije novih proizvoda
- Novi

Ako se njime ne upravlja pravilno, ove promjene mogu uvesti nove ranjivosti u sustav, poremetiti usluge ili negativno utjecati na status usklađenosti organizacije. Robusni program upravljanja promjenama uključuje procese za zahtijevanje, pregled, odobravanje, testiranje i implementaciju promjena, zajedno s dokumentiranjem i komunikacijom svih promjena zainteresiranim stranama.

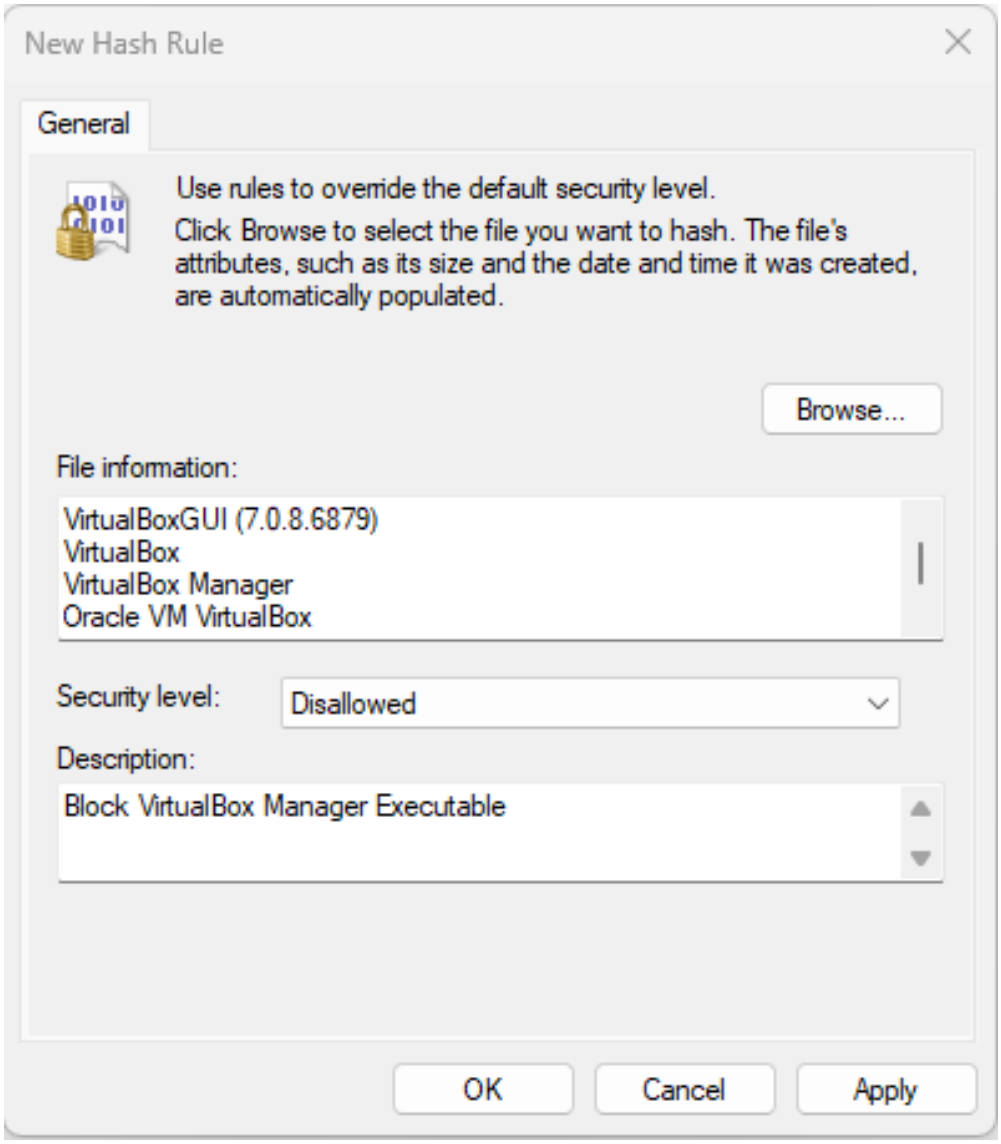
Opis koncepta - Rezultati testiranja: Prije implementacije, promjene prvo moraju biti procijenjene u testnom okruženju kako bi se osiguralo da rade kako je namjeravano i ne uzrokuju probleme. Rezultati testiranja pružaju dokumentirane dokaze o učincima

promjene.

Dopuštene i blokirane promjene

Liste dopuštenih i zabranjenih prikazuju se u praksama upravljanja promjenama. Lista dopuštenih (allowlist) specificira što je dozvoljeno, dok lista zabranjenih (denylist ili blocklist) specificira što je zabranjeno ili zahtijeva posebno odobrenje.

Politike ograničenja softvera (lista zabranjenih) mogu se temeljiti na hash vrijednostima datoteka.



Snimak zaslona korišten uz dopuštenje Microsofta.

Ograničene aktivnosti odnose se na akcije ili promjene koje zahtijevaju dodatni nadzor, stroge kontrole ili više razine odobrenja/autorizacije zbog njihovog potencijalnog utjecaja na kritične sustave ili operacije.

Ponovni pokreti, ovisnosti i zastoji

Ponovni pokreti usluga i aplikacija, kao i zastoji, kritična su razmatranja jer obično imaju izravni utjecaj na poslovne operacije.

promjene zakrpavanja često zahtijevaju ponovni pokret usluga ili aplikacija, što dovodi do zastoja. Jedan od primarnih ciljeva upravljanja promjenama je minimizirati ove poremećaje planiranjem promjena u terminima koji minimiziraju utjecaj na poslovne

operacije.

Zastoj se odnosi na planirano vrijeme namijenjeno implementaciji promjena (planirani zastoj) ili količinu vremena kada usluga ili aplikacija nije dostupna (neplanirani zastoj).

Naslijeđeni sustavi i aplikacije

Naslijeđene aplikacije postavljaju jedinstvene izazove u pogledu upravljanja promjenama jer su ovi sustavi često kritični za poslovne operacije i teško ih je ažurirati bez rizika od prekida. Upravljanje promjenama na naslijeđenim sustavima zahtijeva pažljivo planiranje i testiranje.

Dokumentacija i kontrola verzija

Kontrola verzija odnosi se na praćenje i kontrolu promjena dokumenata, koda ili drugih važnih podataka. Organizacije mogu koristiti kontrolu verzija za praćenje promjena u konfiguracijama, skriptama i dokumentaciji.

Opis stavke - Politike i procedure: Promjene mogu utjecati na postojeće politike i procedure. Kao rezultat toga, ove dokumente treba pregledati i ažurirati kako bi se uskladile s promjenama. Upravljanje verzijama ove dokumentacije osigurava da su sve zainteresirane strane svjesne trenutnih politika i procedura.

Lekcija 14C

Automatizacija i orkestracija

Pregled lekcije

Automatizacija i orkestracija su moćni alati za upravljanje sigurnosnim operacijama. Automatizacija koristi softver za izvođenje repetitivnih, na pravilima temeljenih zadataka, poput nadziranja prijetnji, provjere usklađenosti i provizioniranja korisnika. Orkestracija koordinira te automatizacijske zadatke i integrira različite alate i procese za postizanje složenijih ciljeva.

Automatizacija i skriptiranje

Automatizacija i skriptiranje pojavili su se kao kritični alati u modernim IT operacijama, pomažući organizacijama u optimiziranju procesa, poboljšanju sigurnosti i poboljšanju ukupne učinkovitosti. Ove tehnologije omogućuju IT timovima automatizaciju repetitivnih, vremenski intenzivnih zadataka, smanjujući vjerojatnost ljudske greške i oslobađajući dragocjene resurse za strateškije aktivnosti.

Opis sposobnosti - Provizioniranje: Provizioniranje korisnika i resursa su temeljni IT zadaci koji uvelike imaju koristi od automatizacije i skriptiranja. Provizioniranje korisnika opisuje kreiranje, konfiguriranje, ažuriranje i brisanje korisničkih računa i dozvola na svim sustavima i aplikacijama u organizaciji.

Automatizacija i orkestracija nude i mnoge važne pogodnosti za sigurnosne operacije. Primarno, poboljšavaju učinkovitost omogućavanjem brzog i dosljednog obavljanja repetitivnih zadataka. To oslobađa sigurnosne profesionalce za fokusiranje na složenije i strateške sigurnosne zadatke.

Važna razmatranja

Dok automatizacija i orkestracija pružaju brojne pogodnosti, također predstavljaju neke značajne izazove:

- Složenost — Implementacija automatizacije i orkestracije zahtijeva duboko razumijevanje

sustava, procesa i međuovisnosti organizacije. Loše planirana ili izvršena strategija automatizacije može dodati složenosti, čineći sustave težim za upravljanje i održavanje.

- Trošak — Početni trošak implementacije automatizacije i orkestracije može biti visok, uključujući

troškove vezane uz nabavu i razvoj odgovarajućih alata, integriranje u postojeće sustave i osposobljavanje zaposlenika za njihovu učinkovitu upotrebu.

- Jedinstvena točka kvara — Ako kritični automatizirani sustav ili proces ne uspije, mogao bi utjecati

na više područja organizacije, uzrokujući raširene probleme.

- Tehnički dug — Organizacije mogu gomilati tehnički dug ako se alati automatizacije i orkestracije

implementiraju naprečac, što rezultira loše dokumentiranim kodom, krhkim integracijama sustava ili lošim održavanjem.

složenosti i povećanim troškovima, ironično slično problemima koji su uglavnom vezani uz naslijeđene sustave.

- Trajna podrška — Sustavi automatizacije i orkestracije zahtijevaju trajnu podršku za ostanak

učinkovitim i sigurnim, uključujući ažuriranja i zakrpe, pregled i poboljšanje automatiziranih procesa i kontinuiranu edukaciju.

Sažetak

Trebali biste biti u mogućnosti identificirati važnost upravljanja i njegovu ulogu u oblikovanju sposobnosti sigurnosnog programa. Smjernice za implementaciju upravljanja:

- Implementirajte strukturu upravljanja koja najbolje podržava ciljeve organizacije.
- Iskoristite stručnost kroz odbore za podršku donošenju odluka.
- Uspostavite sveobuhvatnu listu

Modul 15

Objasnite procese upravljanja rizicima

Pregled modula

Učinkovite prakse upravljanja rizicima uključuju sustavnu identifikaciju, procjenu, ublažavanje i nadzor organizacijskih rizika. Revizije pružaju neovisnu i objektivnu procjenu sigurnosnih kontrola i usklađenosti organizacije. Upravljanje rizicima pomaže organizacijama u donošenju informiranih odluka o tome kako dodijeliti resurse za zaštitu imovine i smanjenje ranjivosti.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Objasnite procese i koncepte upravljanja rizicima.
- Objasnite koncepte analize poslovnog utjecaja.
- Razumijte različite odgovore na rizike.
- Saznajte o praksama procjene i upravljanja dobavljačima.

Lekcija 15A

Procesi i koncepti upravljanja rizicima

Pregled lekcije

Upravljanje rizicima uključuje identifikaciju potencijalnih problema, procjenu njihovog potencijalnog utjecaja na organizaciju i implementaciju kontrola za njihovo ublažavanje. Ključni koncepti uključuju identifikaciju rizika, kvalitativnu i kvantitativnu procjenu rizika, odgovore na rizike i procese upravljanja rizicima.

Identifikacija i procjena rizika

Identifikacija rizika temeljna je za upravljanje rizicima kibernetičke sigurnosti. Uključuje prepoznavanje rizika poput napada zlonamjernog softvera, phishing pokušaja, insajderskih prijetnji, povreda podataka i prirodnih katastrofa. Kvalitativna procjena rizika temelji se na subjektivnim faktorima za procjenu i klasifikaciju rizika, dok kvantitativna procjena pokušava dodijeliti konkretne vrijednosti svakom faktoru rizika.

Kvantitativna procjena rizika nastoji dodijeliti konkretne vrijednosti svakom faktoru rizika.

© Slika 123RF.com.

Analiza rizika vs. procjena rizika

Analiza rizika opisuje proces identifikacije i evaluacije potencijalnih rizika i karakteristika koje ih definiraju. Analiza rizika nastoji razumjeti prirodu, uzroke i moguće učinke rizika. Procjena rizika je širiri proces koji uključuje analizu rizika kao sastavnu komponentu, ali se proteže dalje na evaluaciju tolerancije organizacije na rizike.

- Očekivani gubitak od jednog događaja (SLE) — iznos koji bi bio izgubljen u jednom javljanju

faktora rizika. Ovo se određuje množenjem vrijednosti imovine s faktorom izloženosti (EF). EF je postotak vrijednosti imovine koji bi bio izgubljen. Na primjer, može biti 50% za određeni napad.

- Godišnji očekivani gubitak (ALE) — iznos koji bi bio izgubljen u toku

godine. Ovo se određuje množenjem SLE s godišnjom stopom pojavnosti (ARO). ARO opisuje koliko puta godišnje se događa određeni događaj.

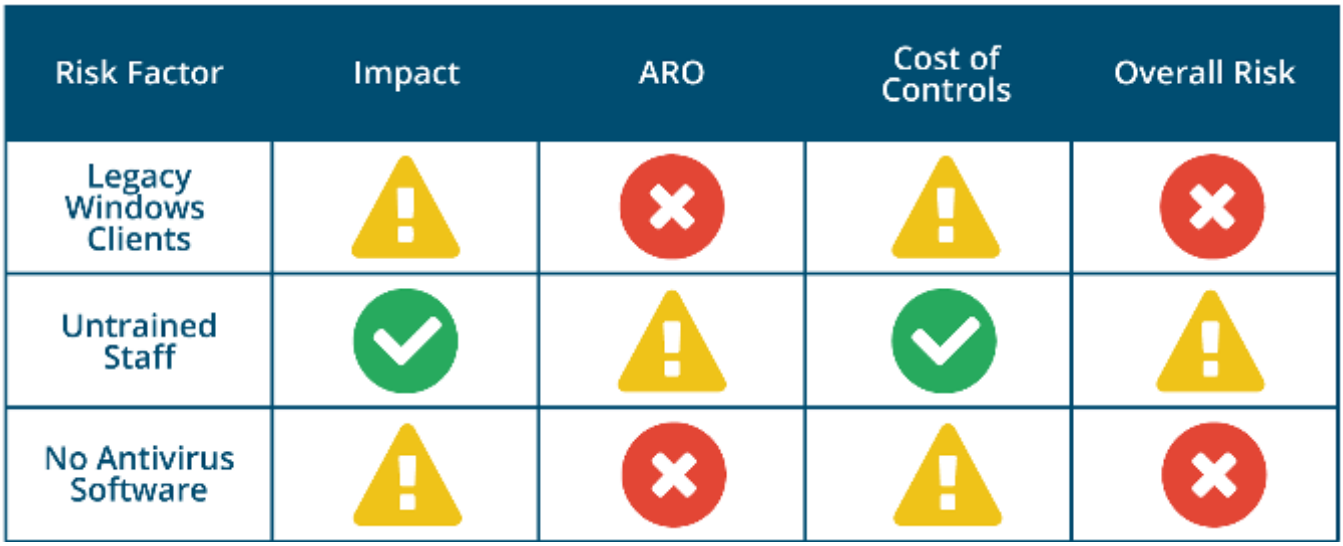
prosječnih troškova 160.000 USD godišnje, tada se ovaj broj može koristiti kao usporedba pri razmatranju troška različitih zaštita. Važno je shvatiti da se vrijednost imovine može procjenjivati na temelju zamjenskog troška, ali i na temelju potencijalnog utjecaja na prihode ili reputaciju organizacije.

- Regulatorni zahtjevi za implementaciju sigurnosnih kontrola i demonstriranje napora za

smanjenje rizika. Primjeri zakonodavstva i propisa koji nalažu sigurnosne kontrole uključuju SOX, HIPAA, Gramm-Leach-Bliley, Zakon o domovinskoj sigurnosti, PCI DSS propise i razne propise zaštite osobnih podataka.

- Visoko vrijedna imovina, bez obzira na vjerojatnost prijetnji.
- Prijetnje s visokom vjerojatnošću (to jest, visoki ARO).
- Procedure, oprema ili softver koji povećavaju vjerojatnost

naslijeđene aplikacije, nedostatak obuke korisnika, stare verzije softvera, nezakrpani softver, pokretanje nepotrebnih usluga, nepostojanje revizijskih procedura itd.). Toplinska mapa — vizualni alat koji pomaže u identifikaciji i prioritiziranju rizika.



FIPS 199 raspravlja o tome kako primijeniti sigurnosne kategorizacije (SC) na informacijske sustave na temelju utjecaja koji bi kršenje povjerljivosti, integriteta ili dostupnosti imalo na misiju organizacije. Razine utjecaja su:

- Nizak — manja šteta ili gubitak imovine ili gubitak performansi (dok bitne funkcije ostaju operativne).
- Umjeren — značajna šteta ili gubitak imovine ili performansi.
- Visok — ozbiljna šteta ili gubitak ili nemogućnost obavljanja jedne ili više bitnih funkcija.

Strategije upravljanja rizicima

Strategije upravljanja rizicima opisuju proaktivne i sustavne pristupe koji se koriste za identifikaciju, procjenu, prioritizaciju i ublažavanje rizika kako bi se minimizirali njihovi negativni učinci na organizaciju.

Izbjegavanje znači prestanak aktivnosti koja uzrokuje rizik. Na primjer, tvrtka može razviti interno razvijenu aplikaciju za upravljanje zalihama, a zatim pokušati je prodavati. Ako se utvrdi da sigurnosni rizici premašuju potencijalne prihode, tvrtka može odlučiti odustati od prodaje aplikacije. Prihvaćanje rizika znači prihvaćanje potencijalnih gubitaka bez poduzimanja specifičnih mjera za smanjenje rizika. Prijenos rizika znači prebacivanje potencijalnih financijskih gubitaka od rizika na treću stranu, poput osiguravatelja ili dobavljača. Ublažavanje rizika znači implementaciju kontrola za smanjenje vjerojatnosti ili utjecaja rizika.

Četiri odgovora na rizik su izbjegavanje, prihvaćanje, ublažavanje i prijenos.

Rezidualni rizik i apetit za rizik

Dok je inherentni rizik rizik prije ublažavanja, rezidualni rizik je vjerojatnost i utjecaj nakon specifičnog ublažavanja, prijenosa ili prihvaćanja mjera. Apetit za rizik opisuje razinu rizika koja je prihvatljiva za organizaciju. Tolerancija na rizik opisuje precizne razine variranja koje su prihvatljive.

Procesi upravljanja rizicima

Upravljanje rizicima je proces identifikacije, procjene i ublažavanja ranjivosti i prijetnji prema bitnim funkcijama koje poduzeće mora obavljati. Formalni procesi upravljanja rizicima obično uključuju sljedeće korake: identifikaciju imovine, identifikaciju prijetnji, analizu ranjivosti, procjenu rizika i identificiranje odgovora na rizike.

za procjenu rizika. Postoje kvantitativne i kvalitativne metode analize utjecaja i vjerojatnosti. 5. Identificirajte odgovor na rizik — za svaki rizik identificirajte moguće protumjere i procijenite cost-benefit analizu svake. Ključni pojmovi u procjeni rizika uključuju:

- Vjerojatnost se često koristi u kvalitativnoj analizi za opisivanje šanse da se dogodi rizični događaj

subjektivno. Vjerojatnost se obično izražava korištenjem 'niska', 'srednja' i 'visoka' ili bodovanjem na skali od 1 do 5.

- Vjerojatnost je kvantitativna mjera koja se obično izražava kao numerička vrijednost između 0 i

1 ili postotak. Vjerojatnost nastoji precizno izmjeriti šansu nastanka rizičnog događaja na temelju statističkih metoda.

- Utjecaj je ozbiljnost rizika ako se realizira kao sigurnosni incident. To može biti određeno

faktorima poput vrijednosti imovine ili troška poremećaja ako je imovina kompromitirana. Upravljanje rizicima je složeno i tretira se dosta različito u tvrtkama i institucijama.

u različitim područjima organizacije. Ključni indikatori rizika (KRI) procjenjuju potencijalni utjecaj i vjerojatnost različitih rizika kako bi vodstveni timovi mogli poduzeti proaktivne korake za učinkovito upravljanje njima. Korištenjem KRI-ova, organizacije mogu identificirati i ublažiti rizike prije nego što eskaliraju u ozbiljne incidente.

Operativna izvješća o rizicima moraju uključivati specifične detalje o faktorima koji doprinose riziku i prikladna su za menadžere ili tehničke zaposlenike. Izvješća o rizicima moraju biti jasna, sažeta i relevantna za ciljnu publiku.

Analiza poslovnog utjecaja

Identifikacija kritičnih sustava — Za podršku otpornosti misijski esencijalnih i primarnih poslovnih funkcija, ključno je provesti identifikaciju i inventar imovine. Ovo treba pokriti sljedeće kategorije imovine:

- Ljudi (zaposlenici, posjetitelji i dobavljači).
- Opipljiva imovina (zgrade, namještaj, oprema i strojevi, ICT oprema,

elektroničke podatkovne datoteke i papirnati dokumenti).

- Neopipljiva imovina (ideje, komercijalna reputacija, brand itd.).
- Procedure (lanci opskrbe, kritične procedure, standardne operativne procedure).

Za misijski esencijalne funkcije važno je smanjiti broj ovisnosti između komponenti. Ovisnosti se identificiraju provođenjem analize poslovnih procesa (BPA). BPA dokumentira ulaze, hardver, omogućivače i izlaze za svaku poslovnu funkciju:

- Ulazi — izvori informacija za izvođenje funkcije (uključujući utjecaj ako se oni

kasne ili nisu u ispravnom redoslijedu).

- Hardver — posebni server ili podatkovni centar koji izvodi obradu.
- Omogućivači — Osoblje i drugi resursi koji podržavaju funkciju.
- Izlazi — podaci ili resursi koje funkcija proizvodi.

Analiza poslovnog utjecaja (BIA) je proces koji pomaže poduzećima razumjeti potencijalne učinke poremećaja na njihove operacije. Uključuje identifikaciju i procjenu utjecaja različitih scenarija poremećaja na kritične poslovne procese, sustave i resurse.

Analiza misijski esencijalnih funkcija generalno je vođena četirima glavnim metrikama:

- Maksimalni tolerirani zastoj (MTD) je najdulje vremensko razdoblje koje prekid poslovne funkcije

može trajati bez uzrokovanja nepopravljivog poslovnog neuspjeha. Svaki poslovni proces može imati vlastiti MTD, poput raspona od minuta do sati za kritične funkcije.

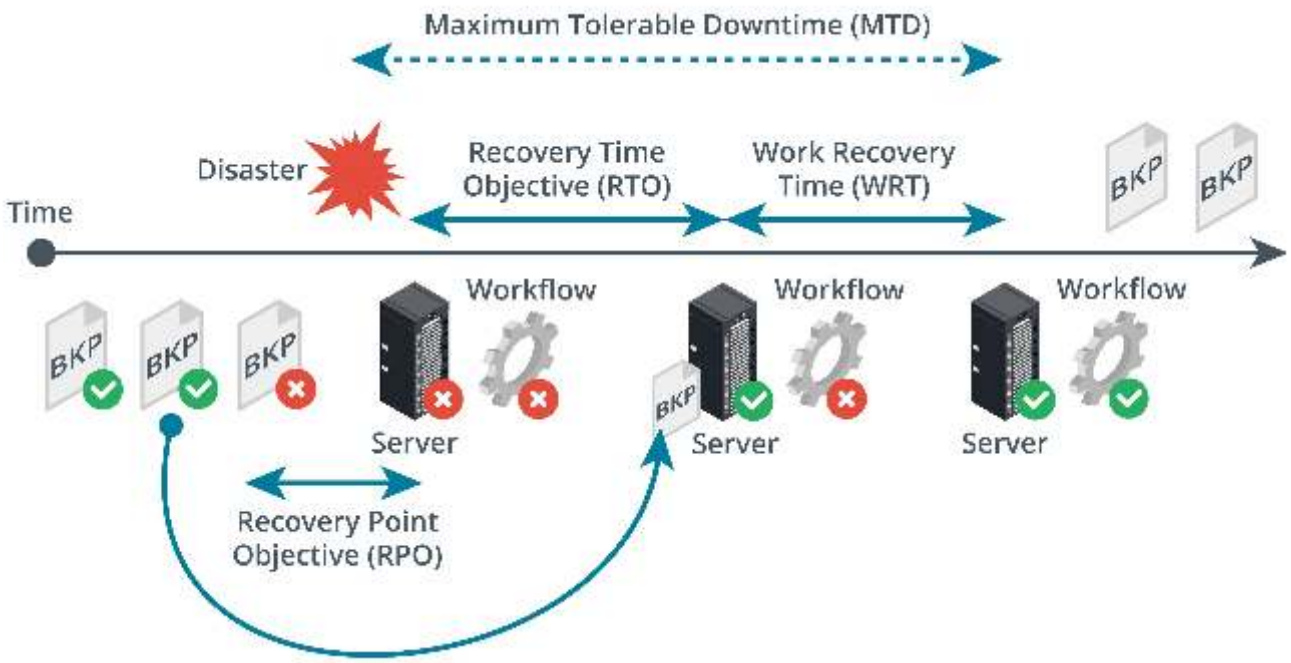
i događaj. Svaku funkciju može podržavati više sustava i imovina. MTD postavlja gornju granicu vremena oporavka koje vlasnici sustava i imovine imaju za nastavak operacija.

- Cilj vremena oporavka (RTO) je period nakon katastrofe za koji pojedinačni IT sustav

može ostati izvan mreže. Ovo predstavlja vrijeme potrebno za identifikaciju problema i zatim provođenje oporavka (obnova iz sigurnosne kopije ili prebacivanje na alternativni sustav).

- Vrijeme radnog oporavka (WRT). Nakon oporavka sustava, može biti potreban dodatni rad

za reintegraciju različitih sustava, testiranje ukupne funkcionalnosti i upoznavanje korisnika sustava s eventualnim promjenama ili različitim radnim praksama kako bi poslovna funkcija bila opet u potpunosti podržana.



- Cilj točke oporavka (RPO) je količina gubitka podataka koji sustav može podnijeti,

izmjerena u vremenu. To jest, ako je baza podataka uništena virusom, RPO od 24 sata znači da se podaci mogu oporaviti (iz sigurnosne kopije) do točke ne više od 24 sata prije incidenta.

© Slike 123RF.com.

Na primjer, baza podataka za upravljanje odnosima s kupcima može podnijeti gubitak nekoliko sati ili dana podataka jer zaposlenici generalno mogu zapamtiti s kime su razgovarali.

nemoguće ih je nanovo snimiti ili srodni procesi pokrenuti sustavima za obradu narudžbi, poput računovodstvenih i podataka o ispunjenju narudžbi. MTD i RPO pomažu u određivanju koje poslovne funkcije imaju prioritet za oporavak. Ostale metrike uključuju:

- Srednje vrijeme između kvarova (MTBF) predstavlja očekivani životni vijek proizvoda.

Izračun MTBF-a je ukupno operativno vrijeme podijeljeno s brojem kvarova. Na primjer, ako imate 10 uređaja koji rade 50 sati i dva se pokvare, MTBF je 250 sati.

- Srednje vrijeme do popravka (MTTR) je mjera vremena potrebnog za ispravljanje kvara kako bi

sustav bio vraćen u puno funkcioniranje. Ovo se može opisati i kao srednje vrijeme za zamjenu ili oporavak. MTTR se izračunava kao ukupan broj sati neplanipanog održavanja podijeljen s brojem kvarova.

Lekcija 15B

Koncepti upravljanja dobavljačima

Pregled lekcije

Procjena rizika treće strane uključuje nekoliko važnih procesa koji su sastavni dio učinkovitih praksi upravljanja rizicima. Ovi procesi uključuju dubinsku provjeru dobavljača, identifikaciju rizika i procjenu te upravljanje ugovorima. Pravilna procjena dobavljača i kontinuirani nadzor osiguravaju da dobavljači trećih strana poštuju sigurnosne standarde organizacije.

Odabir dobavljača

Prakse odabira dobavljača moraju sustavno procjenjivati i evaluirati potencijalne dobavljače kako bi se minimizirali rizici vezani uz outsourcing ili nabavu. Tipično uključuje dubinsku provjeru, procjenu sigurnosnih praksi dobavljača i evaluaciju usklađenosti s relevantnim standardima.

potencijalne rizike jer mogu imati pristup osjetljivim podacima, infrastrukturi ili kritičnim procesima. Pravilna procjena dobavljača i kontinuirani nadzor osiguravaju da dobavljači trećih strana poštuju sigurnosne standarde organizacije. Studije o rizicima trećih strana pokazuju:

- Tvrtke u prosjeku dopuštaju 89 dobavljača pristup njihovim mrežama tjedno.
- 69% organizacija doživjelo je povredu podataka zbog sigurnosnih nedostataka dobavljača.
- 65% ispitanika

strana dobavljača.

- 64% ispitanika reklo je da njihova organizacija stavlja veći naglasak na troškove nego na sigurnost pri

outsourcingu. Evaluacija dobavljača vitalna je za poduzeća kako bi se pridržavala propisa koji često propisuju rigorozno upravljanje trećim stranama.

- Financijski interesi — Dobavljač može imati financijski interes u preporuci specifičnih

proizvoda ili usluga zbog partnerstva, provizija ili financijskih poticaja koji pristrano usmjeravaju njihove preporuke prema opcijama koje možda ne odgovaraju potrebama organizacije.

- Osobni odnosi — Ako dobavljač ima osobne odnose ili bliske veze s donositeljem odluka unutar organizacije, to može utjecati na donošenje odluka i kompromitirati objektivnu evaluaciju ostalih dobavljača.
- Konkurentski odnosi — Dobavljač može imati poslovni odnos ili konkurentski interes s drugim dobavljačem koji se razmatra, što može navesti dobavljača da prioritizira vlastite interese ili partnerstvo nad najboljim interesima organizacije.
- Insajderske informacije — U slučajevima gdje dobavljač ima pristup povjerljivim ili vlasničkim informacijama o ostalim dobavljačima ili strateškim planovima organizacije, dobavljač može koristiti ove informacije za stjecanje nepoštene prednosti ili manipulaciju procesom odabira.

Metode procjene dobavljača

Dubinska provjera, u kontekstu procjene i odabira dobavljača, odnosi se na sveobuhvatni i sustavni proces prikupljanja i analiziranja informacija o potencijalnom dobavljaču. Ovo uključuje pregled financijskog stanja, sigurnosnih praksi i prošlih incidenata dobavljača.

Ove procjene pružaju objektivnu i nepristranu evaluaciju sposobnosti dobavljača. Korištenjem neovisnih procjena, organizacije mogu imati koristi od specijaliziranog znanja i iskustva vanjskih stručnjaka.

Pravni sporazumi

Pravni sporazumi igraju vitalnu ulogu u podržavanju odnosa s dobavljačima uspostavljanjem prava, odgovornosti i očekivanja obiju strana. Pravni sporazumi služe za formaliziranje i zaštitu poslovnih odnosa između organizacija i njihovih dobavljača:

- Memorandum o razumijevanju (MOU) — neobavezujući sporazum koji opisuje namjere, zajednički ciljeve i opće uvjete suradnje između strana. MOU-ovi služe kao preliminarni korak za uspostavljanje zajedničkog razumijevanja prije nastavka s formalnim sporazumom.
- Sporazum o tajnosti (NDA) — osigurava povjerljivost i zaštitu osjetljivih informacija dijeljenih tijekom odnosa. NDA je obvezujući sporazum i vjerojatno će se potpisati zajedno s MOU-om.
- Memorandum o sporazumu (MOA) — formalni sporazum koji definira specifičnih uvjete, odredbe i odgovornosti strana. MOA-i uspostavljaju pravno obvezujući odnos koji pokriva ciljeve, uloge, resurse i obveze.
- Sporazum o poslovnom partnerstvu (BPA) — uređuje dugoročna strateška partnerstva između organizacija. BPA-i obuhvaćaju razne ciljeve, uključujući financijske aranžmane, procese donošenja odluka, prava intelektualnog vlasništva, povjerljivost i mehanizme rješavanja sporova.
- Okvirni ugovor o uslugama (MSA) — opisuje opće uvjete i odredbe specifičnog

ugovora, poput provizioniranja cloud resursa ili podrške za tiketing/help desk. MSA uključuje opseg, cijene, isporuke i prava intelektualnog vlasništva.

- Ugovor o razini usluge (SLA) — definira specifične metrike performansi, standarde kvalitete

i razine usluge koje se očekuju od dobavljača.

- Izjava o radu (SOW)/Radni nalog (WO) — detaljno opisuje opseg projekta ili angažmana dobavljača,

isporuke, rokove i odgovornosti. SOW-ovi pojašnjavaju zadatke dobavljača, očekivanja organizacije i dogovorene isporuke.

- Uloge i odgovornosti — Jasno definirajte uloge i odgovornosti dobavljača i

klijenta u upravljanju rizicima, uključujući specificiranje tko je odgovoran za identifikaciju, procjenu i ublažavanje različitih vrsta rizika.

- Sigurnosni zahtjevi — Opišite sigurnosne standarde, prakse i kontrole kojih se dobavljač

mora pridržavati, uključujući odredbe vezane uz zaštitu podataka, kontrole pristupa, enkripciju, odgovor na incidente i redovite sigurnosne procjene.

- Obveze usklađenosti — Navedite regulatorne i obveze usklađenosti kojih se dobavljač mora

pridržavati, osiguravajući da se usklađuju s industrijskim zahtjevima klijenta, uključujući privatnost, sigurnost podataka i sve ostale primjenjive pravne ili industrijske propise.

- Izvješćivanje i komunikacija — Uspostavite protokole za pravovremeno izvješćivanje o sigurnosnim incidentima,

kršenjima ili potencijalnim rizicima, uključujući definiranje kanala izvješćivanja, učestalosti i razine detalja potrebnih za učinkovitu komunikaciju i upravljanje rizicima.

- Upravljanje promjenama — Opišite procedure za upravljanje promjenama ili ažuriranjima sustava,

procesa ili usluga koje bi mogle utjecati na sigurnost i uvesti nove rizike, uključujući procese odobravanja promjena, zahtjeve za testiranje i prakse dokumentiranja.

- Ugovorne odredbe — Uključite odredbe vezane uz naknadu štete, odgovornost, osiguranje

i prava raskida u slučaju sigurnosnih kršenja ili neispunjavanja obveza upravljanja rizicima. Ove odredbe pomažu u raspodjeli odgovornosti i pružaju pravno rješenje u slučaju sporova.

Lekcija 15C

Revizije i procjene

Pregled lekcije

Revizije i procjene ključne su za održavanje pouzdanih operacija. Revizije uključuju sustavnu evaluaciju procesa, kontrola i usklađenosti s uspostavljenim standardima, politikama i propisima. Procjene procjenjuju učinkovitost sigurnosnih kontrola i identificiraju potencijalne ranjivosti.

Atestacija i procjene

Atestacija se odnosi na verifikaciju i validaciju točnosti, pouzdanosti i učinkovitosti sigurnosnih kontrola, sustava i procesa implementiranih unutar organizacije. Interne revizije provode se od strane internih revizorskih timova koji su dobro upoznati s operacijama organizacije. Interne revizije pružaju vrijedan uvid u sigurnosne prakse i usklađenost organizacije, ali mogu biti predrasudne.

Vanjske revizije prenose nepristranu i objektivnu evaluaciju poslovnih praksi koja je nemoguće dobiti korištenjem internih timova. Vanjske revizije osiguravaju da organizacije ispunjavaju zakonske zahtjeve i industrijske standarde, a mogu biti potrebne za regulatornu usklađenost ili certifikacije poput ISO 27001.

Interne procjene zahtijevaju se za vladine agencije prema NIST RMF-u, PCI-DSS-u i drugima.

Pristup vanjskim procjenama

Regulatorna procjena: Regulatorna tijela ili agencije provode procjene kako bi osigurale usklađenost s specifičnim zakonima, propisima ili industrijskim standardima.

Penetracijsko testiranje

Penetracijsko testiranje (pen test) koristi ovlaštene tehnike hakiranja za otkrivanje iskoristivih slabosti u sigurnosnim sustavima cilja. Pen testovi imaju sljedeće ciljeve:

- Verificirajte da prijetnja postoji — U kibernetičkoj sigurnosti, prijetnja, poput ranjivosti sustava ili mreže,

može uključivati sve što pruža negativnu akciju ili događaj sustava, mreže ili aplikacije. Korištenjem nadzora, socijalnog inženjeringa, mrežnih skenera i skenera ranjivosti možete potvrditi postojanje prijetnje.

- Zaobiđite sigurnosne kontrole — potražite jednostavne načine napada na sustav. Na primjer, ako je

mreža snažno zaštićena vatrozidom, je li moguće dobiti fizički pristup računalu u zgradi i pokrenuti zlonamjerni softver s USB sticka?

- Aktivno testirajte sigurnosne kontrole — istražite slabosti konfiguracije i greške,

poput slabih lozinki ili ranjivosti softvera.

- Iskoristite ranjivosti — dokažite da je ranjivost visokorizična iskorištavanjem za dobivanje pristupa

podacima ili instalacijom backdoor-a. Ključna razlika od pasivne procjene ranjivosti je da se aktivno pokušava testirati sigurnosne kontrole.

- Skeniranje portova — Skeniranje ciljne mreže za identifikaciju otvorenih portova i usluga koje se izvode

na njima.

- Enumeracija usluga — Interakcija s identificiranim uslugama za prikupljanje informacija o njihovim

verzijama, konfiguracijama i potencijalnim ranjivostima.

- Uzimanje otisaka OS-a — Pokušaj identifikacije operativnog sustava koji se izvodi na ciljnim strojevima

analizom mrežnih odgovora i ponašanja.

- DNS enumeracija — Prikupljanje informacija o DNS infrastrukturi cilja, poput

naziva domena, poddomena i IP adresa.

- Pretraživanje web aplikacija — Istraživanje web aplikacija za identifikaciju stranica, direktorija i

potencijalnih ranjivosti. Pasivno izviđanje uključuje prikupljanje informacija o ciljnim sustavima i mrežama bez izravne interakcije s njima fokusiranjem na prikupljanje javno dostupnih informacija.

- Prikupljanje OSINT-a (Open-Source Intelligence) — Prikupljanje javno dostupnih informacija iz

raznih izvora poput tražilica, društvenih medija, javnih baza podataka i web stranica.

- Analiza mrežnog prometa — Nadzor mrežnog prometa za identifikaciju uzoraka, uređaja, IP

adresa i potencijalnih ranjivosti bez aktivnog generiranja prometa. Pasivno izviđanje pomaže testerima penetracije u prikupljanju početnih informacija o digitalnom otisku cilja.

Vrste vježbi

Penetracijsko testiranje je ključna komponenta procjena kibernetičke sigurnosti koja uključuje simuliranje stvarnih napada na računalne sustave, mreže ili aplikacije kako bi se identificirale ranjivosti i procijenila učinkovitost sigurnosnih kontrola. Postoje tri glavne vrste timova koji sudjeluju u vježbama: crveni tim (napadači), plavi tim (branitelji) i

ljubičasti tim (kombinacija oba).

Sažetak

Trebali biste biti u mogućnosti objasniti upravljanje rizicima, analizu poslovnog utjecaja i procese i metrike planiranja oporavka od katastrofe. Smjernice za upravljanje rizicima:

- Identificirajte i procjenjujte rizike kontinuirano kako biste išli u korak s promjenjivim poslovnim

praksama.

- Analizirajte rizik koristeći kvalitativne i kvantitativne metode za pomoć pri prioritiziranju napora saniranja

i alokaciji resursa.

- Izradite registar rizika za pomoć pri upravljanju i praćenju rizika uključujući osoblje zaduženo za rješavanje

njih.

- Uključite poslovne prakse dobavljača u upravljanje rizicima i procjenu.
- Identificirajte i analizirajte dobavljače uključene u lanac opskrbe i osigurajte da imaju

odgovarajuće sigurnosne operacije.

- Koristite višestruke metode revizije i procjene za mjerenje učinkovitosti sigurnosnih

kontrola i usklađenosti organizacije sa zakonskim i regulatornim zahtjevima usklađenosti.

Modul 16

Sažmite koncepte zaštite podataka i usklađenosti

Pregled modula

Zaštita podataka i usklađenost obuhvaćaju niz praksi i principa usmjerenih na zaštitu osjetljivih informacija, osiguravanje privatnosti i pridržavanje primjenjivih zakona i propisa. To uključuje klasifikaciju podataka, upravljanje podacima, implementaciju kontrola zaštite podataka i osiguravanje organizacijske usklađenosti s relevantnim standardima.

Sažetak modula

U ovoj lekciji radit ćete sljedeće:

- Objasnite koncepte privatnosti i osjetljivosti podataka.
- Objasnite kontrole privatnosti i zaštite podataka.

Lekcija 16A

Klasifikacija podataka i usklađenost

Pregled lekcije

Klasifikacija podataka i usklađenost ključni su aspekti upravljanja podacima i kibernetičke sigurnosti. Klasifikacija podataka kategorije su informacija prema razini osjetljivosti i potencijalnom utjecaju ako su kompromitirani. Usklađenost se odnosi na pridržavanje primjenjivih zakona, propisa, standarda i politika vezanih uz zaštitu podataka.

Klasifikacije podataka

Sheme klasifikacije podataka identificiraju osjetljive podatke za prikladnu zaštitu podatkovnih imovina. Vladine i vojne organizacije definiraju klasifikacijske razine za informacije ovisno o utjecaju koji bi njihovo neovlašteno otkrivanje imalo na nacionalnu sigurnost.

Vladine klasifikacijske razine za informacije su:

- Javne informacije — Javne informacije su besplatno dostupne i mogu biti legalno objavljene

i slobodno distribuirane.

- Povjerljivo — Informacije koje, ako su neovlašteno otkrivene, mogu prouzrokovati određenu štetu

nacionalnoj sigurnosti.

- Tajno — Informacije koje, ako su neovlašteno otkrivene, mogu prouzrokovati ozbiljnu štetu

nacionalnoj sigurnosti.

- Strogo povjerljivo — Informacije koje, ako su neovlašteno otkrivene, mogu prouzrokovati iznimno ozbiljnu

štetu nacionalnoj sigurnosti. Klasifikacijske razine privatnog sektora:

- Vlasničko — Vlasničke informacije su zaštićene jer se razumno smatra da tvrtkama pružaju

konkurentsku prednost ili predmet su regulatornih zahtjeva kao što su poslovne tajne, zaštićeni sadržaj ili postoje u obliku koji je skup i zahtjevan za razvoj ili izgradnju.

- Privatno — Privatne informacije su zaštićene jer sadrže osobne identifikacijske informacije (PII) ili

informacije o zdravlju (PHI). Privatne informacije trebaju se zaštititi kako bi se minimizirali rizici od krađe identiteta i povreda privatnosti.

- Osjetljivo — Osjetljive informacije trebaju zaštitu jer, ako su otkrivene, mogu oštetiti

reputaciju organizacije ili otkriti slabosti u njenim obrambenim politikama.

- Ograničeno — Ograničene informacije imaju striktne kontrole pristupa namijenjene maloj skupini ili

pojedincu i ograničene su na one kojima su prijeko potrebne za obavljanje zadataka (pristup na temelju potrebe za znanjem).

Regulatorne sheme

Suverenitet podataka odnosi se na ideju da digitalni podaci podliježu zakonima i propisima države ili regije u kojoj se nalaze.

Razmatranja o suverenitetu podataka uključuju: Lokalizacija podataka: Suverenitet podataka često uključuje zahtjeve lokalizacije podataka koji nalažu da određene vrste podataka moraju biti pohranjene i obrađivane unutar određenih geografskih granica. Na primjer, General Data Protection Regulation (GDPR) Europske unije obvezuje organizacije na pridržavanje zakona o zaštiti podataka EU-a za osobne podatke EU-a.

Usklađenost s lokalnim zakonima: Organizacije moraju uskladiti upravljanje podacima s lokalnim zakonima koji variraju po jurisdikciji. To može biti izazovno za multinacionalne organizacije.

Geo-rezidualni zahtjevi: Neke industrije (npr. zdravstvo, financije, vlada) imaju specifične zahtjeve za pohranu podataka u određenim regijama ili državama.

Zaštita podataka pri pohrani (at rest)

Zaštita podataka pri pohrani (at rest) odnosi se na zaštitu podataka koji se aktivno ne prenose između uređaja ili mreža i koji se pohranjuju na nekom mediju, poput tvrdog diska, baze podataka, flashdog diska ili arhivskih sustava pohrane.

- Enkripcija — Korištenjem enkripcijskog algoritma i ključeva za šifriranje osjetljivih podataka,

tako da je originalnom sadržaju moguće pristupiti samo s ispravnim ključevima za dešifriranje. Enkripcija diska, enkripcija baze podataka i enkripcija datoteke ključni su slojevi zaštite.

- Fizička sigurnost — Upotreba mjera fizičke sigurnosti poput zaključanih soba za poslužitelje, sefova

i ograničenih zona pristupa za zaštitu fizičkih medija pohrane od neovlaštenog fizičkog pristupa.

- Kontrole pristupa — Implementacija strogih kontrola pristupa i autentifikacijskih mehanizama za ograničavanje

tko može pristupiti, izmijeniti ili brisati podatke u mirovanju.

- Sigurnosne kopije i oporavak — Redovito izrađivanje sigurnosnih kopija podataka i primjena robusnih planova

oporavka od katastrofe za zaštitu od gubitka ili korupcije podataka.

- Tokenizacija/Maskiranje podataka — Zamjena osjetljivih podataka ne-osjetljivim nadomjestcima (tokenima)

koji ne sadrže izvorne vrijednosti ili maskiranje podataka za smanjenje izloženosti osjetljivih informacija.

Zaštita podataka pri prijenosu (in transit)

Zaštita podataka pri prijenosu (in transit) fokusira se na zaštitu podataka koji se kreću između lokacija, poput putovanja kroz internet ili privatnu mrežu, posebno od neovlaštenog pristupa i prisluškivanja.

- Enkripcija — Korištenjem protokola poput TLS (Transport Layer Security), SSL (Secure Sockets Layer)

i sigurnih VPN tunela koji šifriraju podatke za prijenos, osiguravajući da je sadržaj čitljiv samo namijenjenim primateljem.

- Autentifikacija — Implementacija mehanizama autentifikacije za osiguravanje da se samo ovlašteni sustavi

i korisnici mogu komunikacijom međusobno, smanjujući rizik od napada čovjeka u sredini ili prisluškivanja.

- Zaštita integriteta podataka — Osiguravanje da podaci nisu izmijenjeni za vrijeme prijenosa korištenjem

kriptografskih provjera (npr. HMAC - Hash-Based Message Authentication Code).

- Sigurni protokoli — Upotreba sigurnih protokola komunikacije ili sigurnih verzija protokola koji

pružaju ugrađenu enkripciju, autentifikaciju i zaštitu integriteta.

Zaštita podataka u upotrebi (in use)

Zaštita podataka u upotrebi (in use) fokusira se na zaštitu podataka koji se aktivno obrađuju ili koriste unutar računalnog sustava. Primjeri zaštite podataka u upotrebi uključuju:

- Enkripcija u upotrebi — Korištenjem tehnika enkripcije za zaštitu podataka dok se obrađuju u

memoriji CPU-a ili unutar sigurnih enklava, sprječavajući neovlašteni pristup osjetljivim informacijama čak i ako je sustav kompromitiran.

- Sigurno izvođenje — Pokretanje osjetljivog koda u izoliranom ili povjerljivom okruženju izvođenja

(Trusted Execution Environment - TEE), poput Intel SGX ili ARM TrustZone, koji pruža zaštitu od neovlaštenog pristupa ili neovlaštene izmjene podataka za vrijeme obrade.

- Homomorfna enkripcija — Napredna kriptografska tehnika koja omogućuje izvođenje izračuna

na šifriranim podacima bez dešifriranja, osiguravajući povjerljivost podataka dok su u upotrebi.

- Upravljanje pravima na digitalne sadržaje (DRM) — Upotreba DRM tehnologije za kontrolu kako se

digitalni sadržaj može koristiti ili distribuirati.

- Maskiranje podataka — Korištenjem tehnika maskiranja ili anonimizacije podataka za zaštitu

osjetljivih informacija za vrijeme obrade, osiguravajući da se stvarni podaci ne izlažu nepotrebno.

Tokeni se mogu čuvati u bazama podataka ili aplikacijama umjesto originalnih vrijednosti. Tokenizacija se razlikuje od enkripcije jer je token potpuno nova vrijednost, a ne šifrirana verzija izvornih podataka. Primjeri tokenizacije uključuju zamjenu broja kreditne kartice nasumičnim šesnaestoznamenkastim brojem koji se zove token plaćanja.

Sprječavanje gubitka podataka (DLP)

Sprječavanje gubitka podataka (DLP) je sigurnosna strategija koja štiti osjetljive podatke od neovlaštenog pristupa, otkrivanja ili eksfiltracije, bilo namjerne ili nenamjerne. DLP sustavi identificiraju, nadziru i kontroliraju kretanje osjetljivih podataka izvan organizacije.

- Otkrivanje — DLP rješenja prolaze kroz podatke u potrazi za osjetljivim informacijama,

uključujući ne samo strukturirane podatke, poput baza podataka, već i nestrukturirane podatke, poput e-pošte i Office dokumenata.

- Klasifikacija — DLP rješenja klasificiraju podatke prema unaprijed definiranim politikama koje određuju

što se smatra osjetljivim podacima. Ovo može uključivati PII, financijske podatke, intelektualno vlasništvo itd.

- Nadzor — DLP rješenja kontinuirano prate pokrete podataka unutar mreže organizacije i

identificiraju potencijalna kršenja politike.

- Zaštita — Kada se otkrije potencijalno kršenje, DLP rješenje može poduzeti razne akcije,

uključujući upozorenja, blokiranje prijenosa, enkripciju podataka ili pokretanje istraga.

- Izvješćivanje — DLP rješenja generiraju detaljna izvješća o kretanjima podataka i kršenjima

politike, pružajući vrijedne uvide za poboljšanje politika i procesa zaštite podataka.

DLP rješenja mogu biti implementirana na raznim točkama unutar IT infrastrukture organizacije:

- Mrežni DLP — ovo se instalira na mrežnom perimetru između interne mreže i

interneta ili između internih mreža i provjerava sadržaj mrežnih paketa za osjetljive podatke.

- Krajnji DLP — ovo se instalira na korisničkim uređajima i provjerava datoteke i podatke

koji se čuvaju ili pristupa na tim uređajima.

- Pohrana u oblaku/DLP za e-poštu — ovo štiti podatke pohranjene u uslugama oblaka ili

poslane putem e-pošte, pružajući vidljivost i kontrolu nad kretanjem osjetljivih podataka.

Sanacija

Sanacija je ključni korak u ciklusu upravljanja podacima gdje se osjetljivi podaci uklanjaju, zaštićuju ili transformiraju kako bi se smanjila izloženost ili poštivali zahtjevi usklađenosti. Procesi sanacije variraju ovisno o specifičnom kontekstu i zahtjevima, ali obično uključuju jednu ili više sljedećih tehnika:

- Brisanje podataka — Uklanjanje podataka s medija pohrane na način koji onemogućuje

oporavak korištenjem standardnih alata. Ovo može uključivati brisanje podataka, uništavanje ili fizičko uništenje medija pohrane.

- Anonimizacija podataka — Modifikacija osjetljivih podataka na način koji onemogućuje

identifikaciju originalnih informacija. Ovo može uključivati generalizaciju, zamjenu ili miješanje podataka.

- Maskiranje podataka — Zamjena originalnih osjetljivih podataka ne-osjetljivim alternativama

ili zamjenskim znakovima koji zadržavaju strukturu podataka ali sakrivaju osjetljivi sadržaj.

- Enkripcija — Šifriranje podataka na način koji je čitljiv samo onima koji imaju odgovarajuće

ključeve za dešifriranje, smanjujući rizik od otkrivanja ako su podaci kompromitrani.

- Tokenizacija — Zamjena originalnih osjetljivih podataka (npr. broja kreditne kartice) nasumičnim

nadomjestcima (tokenima) koji ne sadrže izvorne vrijednosti.

Tehnike sanacije mogu uključivati fizičko uništenje, brisanje ili prepisivanje na licu mjesta, kriptografsko brisanje (crypto-erase) i uništavanje podataka putem specijaliziranog softvera.

Za provjeru brisanja medija pohrane koriste se različite tehnike poput NIST SP 800-88 revizije, certifikacije treće strane i forenzičke provjere. Rješenja za upravljanje podacima i usklađenost trebaju uzeti u obzir zakonodavne zahtjeve, regulatorne zahtjeve i zahtjeve privatnosti pri odabiru prikladnih metoda sanacije.

Razmatranja o suverenitetu podataka pri pohrani u oblaku uključuju:

- Izbjegavajte pohranu osjetljivih podataka koji podliježu specifičnoj jurisdikciji u javnom oblaku

koji nije u toj jurisdikciji.

- Koristite privatni oblak ili implementaciju na licu mjesta za visoko regulirane podatke.
- Odaberite pružatelje oblaka koji nude geo-rezidenciju i jurisdikcijske opcije pohrane.
- Implementirajte kontrole za sprječavanje slučajnog prijenosa podataka u regije koje ne zadovoljavaju

zahtjeve suvereniteta.

- Obavite dubinsku provjeru kako biste razumjeli politike suvereniteta podataka pružatelja oblaka

i osigurali usklađenost sa zahtjevima vaše organizacije.

Definiranje uloga u upravljanju podacima

Uloge u upravljanju podacima definiraju tko ima određene odgovornosti za upravljanje podacima i osiguranje njihove ispravnosti, integriteta i sigurnosti unutar organizacije.

- Vlasnik podataka je odgovoran za osiguranje dostupnosti podataka osobama kojima su oni potrebni,

običnо poslovni rukovodilac, a ne IT osoblje.

- Čuvar/skrbnik podataka je IT ili drugi stručnjak koji implementira upute od vlasnika podataka o tome kako zaštititi

i kontrolirati pristup podacima.

- Upravitelj privatnosti razvija i provodi politike zaštite osobnih podataka (i osoblja i kupaca).
- DPO (Službenik za zaštitu podataka) odgovoran je za nadzor strategije zaštite podataka i

implementacije kako bi osigurali usklađenost s propisima o zaštiti podataka.

Sporazumi i regulatorni okviri usklađenosti

Organizacije moraju identificirati koji regulatorni okviri upravljaju njihovim poslovanjem i implementirati prikladne politike, procedure i kontrole kako bi ispunile te zahtjeve. Uobičajeni regulatorni okviri i standardi uključuju:

- PCI DSS (Standard sigurnosti podataka platne industrije) — Standard za industriju platnih kartica koji

uspostavlja sigurnosne zahtjeve za organizacije koje obrađuju, pohranjuju ili prenose informacije o kreditnim karticama.

- HIPAA (Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja) — Američki zakon koji

uspostavlja nacionalne standarde za zaštitu medicinskih evidencija i drugih osobnih zdravstvenih informacija.

- GDPR (Opća uredba o zaštiti podataka) — Propis Europske unije koji propisuje stroge

zahtjeve o načinu na koji organizacije sakupljaju, pohranjuju i koriste osobne podatke.

- SOX (Sarbanes-Oxley zakon) — Američki savezni zakon koji regulira financijsku reviziju i

nadzor za javna poduzeća, uključujući IT sigurnost i zaštitu podataka.

- FISMA (Savezni zakon o upravljanju informacijskom sigurnošću) — Američki zakon koji nameće zahtjeve

sigurnosti informacijskih sustava koji se koriste ili kojima upravljaju savezne agencije.

- ISO/IEC 27001 — Međunarodni standard koji određuje zahtjeve za sustav upravljanja informacijskom

sigurnošću (ISMS).

- NIST okvir kibernetičke sigurnosti — Dobrovoljni okvir koji pruža smjernice za poboljšanje

upravljanja rizicima kibernetičke sigurnosti i praksama.

Organizacije moraju kontinuirano pratiti promjene zakonodavnog i regulatornog okruženja, prilagođavati politike i procedure prema potrebi i dokumentirati usklađenost kako bi demonstrirale pridržavanje zahtjeva.

Primjer procjene rizika privatnosti

Organizacija koja obrađuje zdravstvene informacije pacijenata mora razmotriti: pohranu osobnih i zdravstvenih podataka u skladu sa HIPAA-om, implementaciju kontrola pristupa i enkripcije, provedbu redovitih sigurnosnih procjena i revizija, osiguranje da dobavljači i poslovni partneri poštuju zahtjeve zaštite podataka, implementaciju politika sigurnog upravljanja podacima i politika pohrane podataka.

Organizacije trebaju razumjeti koje vrste osobnih podataka prikupljaju i obrađuju, svrhu obrade, zakonski temelj obrade, prava subjekata podataka, mehanizme prijenosa podataka i zahtjeve pohrane podataka.

Lekcija 16B

Politike osoblja

Pregled lekcije

Politike osoblja koje se odnose na kibernetičku sigurnost obuhvaćaju niz smjernica, postupaka i protokola koje organizacija uspostavlja za reguliranje ponašanja zaposlenika, upravljanje pristupom osjetljivim informacijama i ublažavanje potencijalnih sigurnosnih rizika unutar radne snage.

Politike ponašanja

Politike ponašanja važan su aspekt upravljanja zaposlenicima u organizacijama. Odnose se na skup pisanih ili neformalnih pravila i standarda koji reguliraju ponašanje zaposlenika na radnom mjestu. Ove politike namjeravaju stvoriti pozitivno, produktivno i sigurno radno okruženje, uz promicanje etičnog ponašanja i usklađenosti s pravnim i regulatornim zahtjevima.

Uobičajene politike ponašanja relevantne za kibernetičku sigurnost uključuju:

- Prihvatljiva politika korištenja (AUP) — AUP opisuje primjerenu upotrebu IT resursa,

uključujući internet, e-poštu i ostale tehnologije. Ova politika obično zabranjuje nezakonitu aktivnost i može zabraniti seksualnu, diskriminatornu, kriminalna ili uvredljiva sadržaj.

- Politika e-pošte — Politika e-pošte opisuje kakva je upotreba e-pošte za poslovne svrhe dopuštena

i ograničenja vezana uz osobnu upotrebu ili otkrivanje osjetljivih podataka.

- Politika lozinki — Politika lozinki opisuje zahtjeve za snagu lozinki, rokove isteka

i procedure upravljanja lozinkama.

- Politika čistog stola/ekrana — Politika čistog stola osigurava da se povjerljive i osjetljive

informacije ne ostavljaju neunaprijed zabilježene ili nezaštićene na radnim površinama. Politika čistog ekrana nalaže da se zaključa računalni zaslon ili odjavite se sa sesija pri napuštanju radnog mjesta.

- Politika upravljanja resursima — Ova politika opisuje zadatke potrebne za izlaz osoblja, što je

posebno relevantno za IT osoblje s povišenim pristupnim privilegijama. Postupci odlaska trebaju biti kodirani kako bi se osiguralo brisanje pristupnih vjerodajnica, revokacija certifikata i povrat korporativnih uređaja.

- Politika rada na daljinu — Politika rada na daljinu opisuje smjernice i sigurnosne zahtjeve

za zaposlenike koji rade od kuće ili s udaljenih lokacija.

Obuka za sigurnosnu svjesnost

Obuka za sigurnosnu svjesnost je organizirani program namijenjen obrazovanju i informiranju zaposlenika o različitim sigurnosnim prijetnjama, praksama i politikama. Cilj je potaknuti zaposlenike da prepoznaju i reagiraju na sigurnosne incidente i ublažiti rizike koji se mogu pojaviti zbog ljudske pogreške ili nenamjernih sigurnosnih propusta.

- Prepoznavanje phishinga — Obuka zaposlenika da prepoznaju pokušaje phishinga, uključujući

sumnjive e-poruke, veze ili zahtjeve za osjetljivim informacijama, i kako ih prijaviti.

- Sigurna upotreba e-pošte — Edukacija zaposlenika o sigurnoj upotrebi e-pošte, uključujući

izbjegavanje klikanja na sumnjive veze ili preuzimanja privitaka iz nepoznatih izvora.

- Upravljanje lozinkama — Podučavanje zaposlenika o važnosti jakih lozinki, kako ih stvoriti i

upravljati njima sigurno.

- Regulatorna usklađenost — Osiguravanje da zaposlenici razumiju i pridržavaju se relevantnih

propisa i standarda industrije.

- Fizička sigurnost — Edukacija zaposlenika o važnosti zaštite fizičke imovine, poput kontrola pristupa,

zaštite ID oznaka i politike čistog stola.

- Sigurnost na društvenim mrežama — Upozoravanje zaposlenika na rizike dijeljenja osjetljivih

informacija na platformama društvenih medija.

- Prevencija i otkrivanje insajderskih prijetnji — Podučavanje zaposlenika o prepoznavanju

potencijalnih znakova insajderske prijetnje i kako ih prijaviti.

Phishing kampanje

Phishing kampanje su simulirani napadi koji oponašaju stvarne phishing e-poruke. Ove kampanje testiraju koliko dobro zaposlenici prepoznaju phishing pokušaje i reakciju na njih. Učinkovita kampanja za simulaciju phishinga trebala bi:

- Biti realna — Phishing e-poruke trebaju biti dovoljno realistične da zaposlenici

zapravo mogu biti prevareni u klikanju na veze ili pružanju osjetljivih informacija.

- Pokrivati razne napade — Koristite razne taktike napadača, kao što su spear phishing, whaling, vishing i smishing, kako bi se testirala sposobnost zaposlenika da prepoznaju razne vrste phishing napada.
- Biti u odgovarajućoj frekvenciji — Kampanje trebaju biti redovite, ali ne toliko česte da se zaposlenici počnu osjećati previše pod nadzorom.
- Uključivati mjerenje — Praćenje stope klikanja zaposlenika, stope izvješćivanja i ostale metrike za procjenu napretka.
- Biti praćena obukom — Koristite rezultate kampanje za prilagodbu i poboljšanje programa obuke za sigurnosnu svjesnost.

Životni ciklus obuke

Životni ciklus obuke za sigurnosnu svjesnost je kontinuirani krug evaluacije, razvoja, isporuke i mjerenja programa obuke. Koraci u životnom ciklusu obuke uključuju:

- Procjena potreba — Identificirajte sigurnosne potrebe obuke organizacije evaluacijom sigurnosnih rizika, propisa industrije i zahtjeva uloga.
- Razvoj programa — Razvijte plan obuke i gradivo koji se bave identificiranim potrebama, prilagođavajući sadržaj različitim ulogama ili odjelima.
- Isporuka obuke — Provedite obuku korištenjem odgovarajućeg pristupa, poput e-učenja, učionice ili kombiniranja.
- Procjena i mjerenje — Procijenite učinkovitost programa obuke korištenjem kvizova, testova ili ocjenjivanja temeljenih na ponašanju.
- Kontinuirano poboljšanje — Ažurirajte program obuke na temelju povratnih informacija i promjena u sigurnosnom pejzažu.

Učinkovita obuka o sigurnosnoj svjesnosti uvodi zaposlenike u tipove napada socijalnog inženjeringa, objašnjava relevantne zakone i propise, demonstrira učinkovite sigurnosne prakse, osigurava da zaposlenici znaju kako prijaviti sigurnosne incidente i osigurava da zaposlenici razumiju što se od njih očekuje s obzirom na provođenje sigurnosnih politika.

Obuka može biti namijenjena posebno korisniku, ulozi ili sektoru. Obuka prilagođena ulozi prilagođava programe posebnim potrebama zaposlenika uzimajući u obzir razne faktore kao što su organizacijska uloga, razina iskustva, tip korištenih uređaja, radno okruženje i geografska lokacija.

Obuka za korisnike koji imaju privilegirani pristup

Ovaj tip obuke ključan je za zaposlenike kojima je povjerena povišena razina pristupa radi njihovog zvanja ili uloge unutar organizacije. Korisnici s privilegiranim pristupom česti su ciljevi za phishing napade jer imaju visoke razine ovlasti nad sustavima, mrežama i osjetljivim informacijama.

Obuka za izvršne korisnike

Izvršno osoblje, poput direktora, menadžera i rukovoditelja, često ima visoku razinu povjerenja unutar organizacije i može imati pristup osjetljivim poslovnim informacijama. Ova vrsta obuke naglašava potrebu za visokom razinom sigurnosne svjesnosti u svim tipovima interakcija, uključujući poslovnu komunikaciju i susrete s klijentima.

Specifična obuka za zaposlenike i odjele

Osim obuke za sve zaposlenike i obuke za privilegirane korisnike i izvršne korisnike, važno je pruži posebnu obuku ili sektore koji su posebno izloženi određenim sigurnosnim prijetnjama. Na primjer, zaposlenici IT-a trebaju se educirati o naprednim tehnikama hakera, dok zaposlenici prodaje trebaju naučiti kako zaštititi podatke o kupcima.

Kontinuirani nadzor i poboljšanje

Obuka za sigurnosnu svjesnost mora biti prikladna i ažurna kako bi odgovorila na najnovije sigurnosne prijetnje. To uključuje redovite ažuracije i revizije sadržaja obuke kako bi se uključili najnoviji sigurnosni trendovi i prijetnje. Organizacije trebaju procjenjivati i mjeriti učinkovitost svojih programa obuke na temelju metrika ponašanja, kao što je smanjena stopa klikanja phishinga i poboljšani odgovori na sigurnosne incidente.

Resursi za sigurnosnu svjesnost uključuju e-učenje i online tečajeve, live radionice i seminare, simulirane phishing kampanje, sigurnosne blogove i newslettere, videozapise i webinare te igrificirane platforme učenja. Simulirani phishing napadi često se koriste za testiranje i poboljšanje pripremljenosti zaposlenika.

Odgovornost i kultura

Stvaranje kulture odgovornosti je ključno za učinkovite programe sigurnosne svjesnosti. To uključuje:

- Demonstriranje predanosti upravljanja — Vodstvo mora demonstrirati predanost sigurnosti

i sigurnosnoj obuke kroz aktivno sudjelovanje i zagovaranje.

- Uspostavljanje jasnih očekivanja — Zaposlenici trebaju razumjeti svoja sigurnosna

odgovornosti i kako se uklapaju u opći plan sigurnosti organizacije.

- Nagrađivanje pozitivnog ponašanja — Nagrađivanje i prepoznavanje zaposlenika koji se

izvrsno ponašaju u sigurnosnoj svjesnosti pomaže stvoriti kulturu odgovornosti.

- Poduzimanje korektivnih mjera — Kada zaposlenici krše sigurnosne politike ili proceduru, odgovarajuće

korektivne mjere trebaju biti poduzete za poboljšanje ponašanja i naglasiti ozbiljnost sigurnosti.

Sažetak

U ovoj lekciji istražili smo ključne komponente sigurnosti informacija vezane uz politike osoblja i upravljanje podacima.

- Politike ponašanja uspostavljaju standarde za odgovorno korištenje IT resursa i ponašanje na radnom

mjestu, tvoreći temelj za sigurnu i produktivnu radnu okolinu.

- Klasifikacija podataka i suverenitet podataka ključni su za upravljanje osjetljivim informacijama.

Identificiranje i kategorizacija podataka prema stupnju osjetljivosti pomaže organizacijama implementirati prikladne kontrole zaštite.

- Zaštita podataka pri pohrani, prijenosu i upotrebi od ključne je važnosti. Organizacije trebaju

implementirati odgovarajuće enkripcije, enkripcijske protokole i provjere integriteta kako bi osigurale sigurnost podataka u svim stanjima.

- Rješenja za sprječavanje gubitka podataka (DLP) mogu automatski sprječavati neovlašteni prijenos

osjetljivih podataka.

- Programi obuke za sigurnosnu svjesnost osiguravaju da su zaposlenici opremljeni znanjem

i vještinama za prepoznavanje i reagiranje na sigurnosne prijetnje.

- Phishing kampanje testiraju pripremljenost zaposlenika i pomažu organizacijama identificirati

područja gdje je potrebna dodatna obuka.

- Kontinuirani nadzor i poboljšanje programa obuke ključni su za praćenje s promjenjivim

sigurnosnim pejzažom.

Zaključak

Ovaj priručnik pokrio je ključne teme iz CompTIA Security+ certifikacije, pružajući sveobuhvatni pregled konceptualnih i tehničkih aspekata kibernetičke sigurnosti. Od temeljnih sigurnosnih koncepta i arhitekture mreže do naprednih tema poput kriptografije, upravljanja identitetima i privilegiranim pristupom, odgovora na incidente i upravljanja rizicima, ovaj materijal priprema kandidate za položiti Security+ ispit i primijeniti stečena znanja u stvarnim scenariima zaštite informacija.

Sigurnosni stručnjaci moraju kontinuirano ažurirati svoja znanja kako bi pratili stalno promjenjivi pejzaž kibernetičkih prijetnji. Primjena principa opisanih u ovim lekcijama pomoći će u zaštiti organizacijskih resursa, zaštiti povjerljivih informacija i osiguravanju usklađenosti s regulatornim zahtjevima.

Uspješan sigurnosni stručnjak kombinira tehničku stručnost s jakim poslovnim razumijevanjem, učinkovitom komunikacijom i predanosti etičkim praksama. Ovladavanjem materijalima u ovom priručniku, bit ćete dobro opremljeni za napredovanje u svojoj kibernetičkoj karijeri i doprinos sigurnosnom posturanju vaše organizacije.