



Varnost pod nadzorom



Miro Faganel, vodja oddelka varnost in komunikacije, S&T Slovenija.

Informacijska varnost je v 21. stoletju ključnega pomena za poslovanje podjetij. Podatki in informacije predstavljajo namreč vrednost in kapital, ki ju velja hraniti in varovati. Podjetja se v zadnjih letih soočajo z vse več digitalnimi napadi in krajam podatkov, zato v svoja okolja nameščajo vse več varnostnih rešitev. Področje varnosti postaja posledično vse bolj kompleksno in težje obvladljivo, a k sreči obstajajo rešitve, ki obvladajo tudi nadzor varnostnih in ostalih naprav, procesov, sistemov in aplikacij.

Varnostni profesionalci in administratorji IT za nadzor in upravljanje varnostnih naprav in aplikacij vse pogosteje uporabljajo rešitve za upravljanje varnostnih informacij in dogodkov, znane pod kratico SIEM (Security Information and Event Management). Navadno gre za sklop orodij, ki znajo komunicirati z različnimi varnostnimi aplikacijami in napravami ter se znajo samodejno odzvati v primerih varnostnih incidentov in le-te tudi odpraviti. Orodja SIEM, ki delujejo v realnem času, upravljavcu na enem mestu nudijo celovit pregled nad stanjem varnosti informacijskega

in povezanih sistemov.

Največji izziv varnostnih in IT-strokovnjakov v podjetjih je obvladovanje velikega števila različnih sistemov in ogromnih količin podatkov, ki jih s svojim delom ustvarijo uporabniki. Marsikje je stanje že postalo neobvladljivo, preprosto zato, ker posameznik bodisi zaradi pomanjkanja znanja in/ali pomanjkanja časa ne more ugotoviti skupnega imenovalca posameznih dogodkov na različnih sistemih. Zato pa IT-upravitelji potrebujejo natančno orodje, ki zna komunicirati z več varnostnimi sistemi in napravami ter njihove podatke prevesti na skupni imenovalec. Orodja za upravljanje varnostnih informacij in dogodkov z zbiranjem in analiziranjem vseh podatkov iz strežnikov, mrežnih in ostalih naprav ter sistemov omogočajo učinkovito upravljanje varnostnih tveganj.

Najsodobnejše rešitve SIEM odlikuje visoka stopnja integracije, saj znajo zajeti in obdelati podatke o uporabnikih in njihovih aktivnostih od sistema vhodnih vrat do delovnega namizja na računalniku. Dnevniki aktivnosti vseh naprav in aplikacij so tako zbrani na enem mestu. To nadzorniku ponuja sledljivost dogodkov do samega izvora, posledično pa je tudi rekonstrukcija dogodkov bistveno hitrejša, zato se podjetje lahko hitreje odzove na morebitne varnostne incidente. Ker je čas denar, se naložba v rešitev za upravljanje varnostnih informacij in dogodkov lahko povrne zelo hitro, saj ta omogoča hitro zaznavanje ter odpravljanje napak in omejevanje ter preprečevanje poslovne škode.

Skladnost in revizijska poročila

Poslovna praksa narekuje vpeljavo re-

šitev SIEM predvsem na področjih, ki so podvržena regulativi in pogostim revizijam poslovanja. Z vidika občutljivosti in varnosti podatkov so na prvem mestu tako banke in zavarovalnice, sledijo pa jim različne državne organizacije (policija, vojska ...) in napredna podjetja, ki se zavedajo, kako kritične so poslovne informacije za njihovo poslovanje (varnostne službe, telekomunikacijska podjetja ...). Podjetja in organizacije z orodji SIEM bistveno lažje dokazujejo skladnost poslovanja z najrazličnejšimi standardi in predpisi (Basel II, GLBA, HIPAA, ISO 27001, PCI, SOX ...). Orodja SIEM tudi znatno olajšajo pripravo revizijskih poročil za različne nadzornike sistemov. Večina teh orodij ima že vgrajene in tudi prednastavljene predloge poročil in obrazcev, ki služijo za dokazovanje skladnosti z različnimi regulativami in standardi.

Napredne rešitve za nadzor varnostnih naprav in mehanizmov

Analitično podjetje IDC podrobno spremlja tudi razvoj varnostnih IT-rešitev. Na področju orodij SIEM v segment najnaprednejših ponudnikov uvršča predvsem ameriško podjetje ArcSight, katerega prednost se skriva v vgrajenih pametnih rešitvah, zadolženih za iskanje korelacij med podatki. ArcSightova orodja, kakršno je Enterprise Security Manager (ESM), znajo namreč zbrati, prevesti in analizirati podatke iz več deset različnih sistemov hkrati ter iz njih izluščiti informacije, ki varnostnemu strokovnjaku ali IT-upravitelju ponujajo dodano vrednost.

Dotatna prednost specializiranega

ponudnika ArcSight je tudi način delovanja njegovih SIEM-rešitev. Te za zajem podatkov uporabljajo zbrane sistemske dnevnike, ki jih posamezni sistemi in naprave oddajajo pri svojem delu. Posledično od upravitelja IT-okolja ne zahtevajo nameščanja različnih odjemalcev in aplikacij na strežnike in naprave, ki bi dodatno obremenjevali ali celo destabilizirali sistem/napravo.

Z globljim razumevanjem varnostnih pravil, dela uporabnikov ter tokov podatkov po omrežju ArcSight ESM omogoča edinstveno razumevanje trenutnega in preteklega stanja.

Varnostni nadzornik lahko v vsakem trenutku preveri, kdo je prijavljen v omrežje, do katerih podatkov dostopa in kaj z njimi počne ter kakšno varnostno tveganje je s to aktivnostjo povezano. ArcSight ESM v svojih modelih ne pozna le omrežja, sisteme in naprave, temveč lahko spremlja uporabnike, zaposlene, stranke in partnerje ter vse skupaj poveže z naprednimi analitičnimi aktivnostmi. Tako podjetju temeljiteje predstavi poslovna tveganja, s katerimi se sooča pri svojem poslovanju.

Avtomatizacija močno olajša delo

Ob prepoznavi tveganj ArcSight ESM z upravljanjem identitet in varnostnih politik poskrbi, da se odpravijo varnostni incidenti in prepreči dodatna škoda. Pravilno implementirana rešitev skrbi za sprotno alarmiranje odgovornih, ob avtomatiziranih varnostnih postopkih pa v realnem času tudi ustrezno ukrepa ob varnostnih kršitvah.

Povezave med različnimi sistemi, varnostnimi politikami ter sezname uporabnikov omogočajo hitro ugotavljanje neskladij, pa naj gre za kršenje pravil ali varnostne incidente. Rešitve SIEM tako budno spremljajo tudi navade uporabnikov in sprožijo alarm, če uporabnik nenadno poveča kvote

prenesenih podatkov, dostopa do aplikacij ali podatkovnih baz, veliko časa uporablja sicer manj pogosto uporabljane vire, ob vstopu/izstopu v/iz podjetja še vedno brska po aplikaciji ali podatkovni bazi ...

ArcSight ESM omogoča tudi določanje prioriteten sistemov, saj v praksi velja, da dogodki, ki so si sicer enaki, pomenijo drugačno varnostno prioriteto za posamezen sistem. Skladno z dogodki se oblikujejo tudi poročila, saj rešitev oblikuje različna poročila o varnostnih incidentih, trendih, izjemah ...

Uprava za, informatiki proti

Zanimiv precedens ponudniki rešitev SIEM doživljajo tudi pri prodaji le-teh poslovnim okoljem. Uprave podjetij so nad možnostmi in funkcionalnostmi navdušene, manj pa informatiki in sistemski administratorji. Ti so imeli v preteklosti dostop do vseh virov in podatkov v podjetju, v praksi je večina teh ljudi upravljala tudi z varnostnimi rešitvami in je lahko zakrila sledove svojih dejanj. Varnostne rešitve SIEM skrbijo za pregled nad aktivnostmi vseh uporabnikov, varno shranjevanje dnevnikov sistemov in naprav pa pomeni, da jih informatik ne more brisati, potvarjati ali kakorkoli drugače spreminjati. Lukenj v sistemih tako ni več, strokovnjaki pa podjetjem svetujejo tudi novo razmejitve vlog zaposlenih, in sicer na administratorje ter nadzornike/varnostne kontrolorje.

Pri implementaciji mora sodelovati tudi naročnik

Naročnikova vloga pri implementaciji rešitve za upravljanje varnostnih informacij in dogodkov temelji na sodelovanju s ponudnikom rešitve. Naročnik mora namreč imeti jasno sliko, kaj od rešitve želi in kakšen bo namen njene implementacije. Podjetja imajo različne razloge za

implementacijo rešitev SIEM, med najpogostejšimi pa so zaznavanje in odpravljanje varnostnih incidentov, zmanjšanje odzivnega časa ob neljubem dogodku, skladnost poslovanja z regulativo ... Naročnik med implementacijo varnostne rešitve uredi tudi pošiljanje podatkov iz ciljnih sistemov, kar je enkratni poseg.

Čas implementacije rešitve ArcSight ESM je odvisen od obsega sistemov, ki jih želi podjetje vključiti v spremljanje in upravljanje. Zahtevnejša implementacija, ki obsega rešitve za spremljanje in upravljanje do 10 različnih sistemov (spletni strežniki, podatkovni strežniki, aplikacijski strežniki, kontrola dostopa, identifikacijski strežnik ...) in »obvladuje« do tisoč naprav, od kakovostnega ponudnika navadno zahteva do tri mesece. Cena takšne implementacije je povezana tudi z obsegom storitev, začne pa se pri 50 evrskih tisočakah. »Družba S&T je edini certificiran partner ArcSight v Sloveniji, poleg tega pa imajo S&T-jevi strokovnjaki bogate izkušnje tako s področja informacijske varnosti kot tudi povezovanja različnih sistemov. Velika in pogosto težko premostljiva težava slovenskih podjetij je upravljanje heterogenih okolij, številna podjetja pa se niti ne zavedajo, kako kompleksno je v zadnjih letih postalo področje varnosti,« je povedal vodja oddelka varnost in komunikacije v podjetju S&T Slovenija Miro Faganel.

Svojevrstni izziv sistemskih so tudi poslovne aplikacije, ki jih podjetje razvije samo ali pa jih zanj razvije kakšen manjši ponudnik. Te navadno oddajajo manj informacij o svojem delovanju, zato v družbi S&T Slovenija pri vsaki stranki najprej opravijo tudi preizkus delovanja rešitev SIEM z »nestandardnimi« aplikacijami ter poskrbijo za ustrezno prilagoditev.

Consulting. Integration. Outsourcing.