VISOKA ŠKOLA STURUKOVNIH STUDIJA ZA INFORMACIONE I KOMUNIKACIONE TEHNOLOGIJE

MANAGED SECURITY SERVICE PROVIDERS

SEMINARSKI RAD

Profesor: Natalija Vugdelija

Predmet: Bezbednost informacionih sistema

Student: Lenka Živković

Broj indeksa: 62/17

Beograd, oktobar 2019.

SADRŽAJ

UVOD

Cyber kriminal

Kako tehnologija napreduje iz dana u dan, dolazi i do izuzetno brzog razvoja cyber kriminala. U avgustu 2016. godine jedan od vodećih svetskih istraživača cyber ekonomije, Cybersecurity Ventures[1], je predvideo da će cyber kriminal na godišnjem nivou koštati svet oko 6 triliona dolara do 2021. godine, dok je taj broj u 2015. godini iznosio 3 triliona dolara. Ovo predstavlja najveći transver ekonomskog bogatstva u istoriji i biće isplativije od globalne trgovine svih ilegalnih narkotika zajedno.

Iako nijedan pojedinac nije siguran od napada cyber kriminalaca, preduzeća svih razmera su na najvećem udaru. Kako cyber kriminalci svakodnevno traže najslabije tačke u bezbednosnim sistemima, napadi su sve češći i prelaze na nove tehnike koje preduzeća nekada ne mogu da predvide.

Napadi cyber kriminalaca mogu značajno da utiču na finansijsko stanje jednog preduzeća. Neretko se dešava da preuzeća, posle napada, moraju da menjaju postojeće servere, računare i povrate ogromnu količinu vlasničkih podataka. U ovakvim slučajevima, mala i srednja preuzeća najviše stradaju zbog nemogućnosti da finansijski podrže sve gubitke.
Dodatno, potrošači ređe prihvataju usluge i proizvode od preduzeća koje su doživele napad.

Čuvanje podataka ne samo da iziskuje veliki deo finansijskih sredstava, već zahteva i konstantan rad i poboljšavanje sistema što onemogućava da se firme fokusiraju na svoje glavne poslove.
Iz tih razloga mnoga preduzeća traže alternativne načine zaštite. Jedan od načina na koji preduzeća mogu da odgovore na pretenje cyber kriminala je kroz usluge koje pružaju Managed Security Service Providers (MSSP).

[1] https://cybersecurityventures.com/our-company/

TEORIJSKI DEO

Šta je MSSP?

Managed security service provajderi (MSSP) pružaju širok spektar bezbednosnih usluga, koje mogu da uključuju blokiranje virusa i neželjene pošte (virus and spam blocking), detekciju upada (intrusion detection), upravljanje firewall-ovima i privatnim virtualnim mrežama (VPN).
Njihov posao je da spreče, otkriju i efikasno odreaguju na bilo kakav cyber napad.
Mogu da vrše usluge in-house ili na daljinu, obično preko cloud servisa.

Raspoređivanje i implementacija MSSP usluga

Managed security service provajderi obezbeđuju Security Expert tim koji u koordinaciji sa IT timom kompanije analizira i kreira bezbednosni plan sa odgovarajućim MSSP uslugama.
Security Expert tim će se baviti instalacijama i upravljanjem promenama.

Instalacija podrazumeva:

- Definiciju tehničke konfiguracije
- Definisanje administrativnih kontakata i procedure izvršavanja
- Kreiranje dijagrama topologije mreže
- Pre-konfiguraciju, isporuku i funkcionalne provere testiranja usluga sa svim potrebnim hardverskim i softverskim komponentama

Upravljanje promenama:

- Upravljanje promenama preko samouslužnog framework-a
- Prisilni procesi upravljanja promenama pomoću sveobuhvatnog tiketnog sistema
- Pregled zahteva za promene, pojašnjenja i povratne informacije u slučaju skrivenih rizika
- Snažna autentifikacija korisnika sa revizionim tragom

Monitoring, troubleshoot-ovanje i održavanje

Security Operation Center (SOC) timovi su zaduženi da monitorišu i održavaju sigurnosnu postavku i uređaje. Ovi timovi se obično sastoje iz analitičara, inžinjera kao i rukovodioca koji nadgleda sve sigurnosne operacije.
SOC timovi su karakteristični po tome što pružaju usluge monitoringa, troubleshoot-ovanja i održavanja sistema 24/7, 365 dana u godini. Ova karakteristika daje kompaniji prednost za odbranu od incidenata i upada, bez obzira na izvor, doba dana ili vrstu napada.

24/7 monitoring podrzumeva:

- 24/7 proaktivan nadzor, obaveštenje o događajima
- Efikasan odgovor na otkrivene kritične događaje
- Neograničen broj eskalacija, tiketa i poziva za podršku
- Direktna podrška od strane Security Expert tima

Troubleshoot-ovanje i održavanje podrazumeva:

- Verodostojnost u realnom vremenu sa integrisanim sistemom za izdavanje tiketa
- Otklanjanje incidenata u periodu definisanim u SLA
- Zamena neispravnog ili zastarelog hardvera i vraćanje funkcionalnosti
- Analiza, testiranje i instalacija softverskih zakrpa i ažuriranje

Izveštavanje i prijavljivanje:

- Upotreba mreže u realnom vremenu i statistika opterećenja sistema
- Izveštavanje u realnom vremenu o konfiguracionim postavkama i evidencijama

Service Delivery

Service Delivery je način na koji korporacija pruža pristup IT uslugama, koje uključuju aplikacije, skladištenje podataka i druge poslovne resurse. Sve MSSP usluge se isporučuju na namenskom hardveru. Odluka od fizičkoj lokaciji Platforme za Service Delivery je fleksibilna. Zavisi od toga šta kompaniji najviše odgovara za njihove poslovne potrebe. Hardver se može nalaziti u prostorijama kompanije ili u data centru MSSP-a.

Platforme za Service Delivery su obično zasnovane na operativnom sistemu Linux. Aktiviraju se suštinski alati i uslužni programi kako ne bi dolazilo do neočekivanih nestabilnosti ili kompromitovanih sistema. SOC tim je zadužen za održavanje sistema kako bi se osigurala sigurna i pouzdana usluga. Pored toga, SOC vodi računa o životnom ciklusu hardvera i proaktivno nadograđuje hardver ako je određena generacija hardvera zastarela.

Bez obzira gde se nalazi Platforma za Service Delivery, SOC obezbeđuje da su sva odgovarajuća podešavanja vezana za bezbednost ažurirana i pravilno kofigurisana. Ako je potrebno, SOC prati efikasan proces oporavka od katastrofe i može generisati i ponovo instalirati identičnu konfiguraciju po prethodno definisanom sporazumu o nivou servisa (SLA).

Procesi i komunikacija

Tiketing sistem je jedan od najvažnijih softvera koji koriste svi vodeći service provajderi. Ovi sistemi omogućavaju timovima da organizuju, upravljaju i prate stanje problema klijenata na izuzetno organizovan način. Tiketing sistem funkcioniše tako što se prvo pravi dokument ili tiket u kojem se beleži konkretan problem koji je klijent prijavio. Tiketu imaju pristup i SOC tim i sam klijent. Ako postoji bilo kakav problem ili ako se predvidi neki detalj, obe strane mogu da se upute na tiket da pregledaju prethodne informacije. Kada se problem konačno reši ili SOC tim ili klijent mogu da zatvore taj tiket, koji ostaje logovan u sistemu u slučaju da je potrebno ponovo otvoriti ga.

Tiketi se kreiraju na osnovu sledećih procesa:

- Incident

  Bilo koji dogadjaj koji uzrokuje ili može uzrokovati prekid ili smanjenje kvaliteta usluge
- Izmena

  Promena u podešavanjima koje se mogu izvršiti bez promene same instalacije hardvera/softvera
- Održavanje

  Ovo uključuje zakrpe, nadogradnje ili promene koje izvršava klijent
- Drugi zahtevi

  Namenjen za opšta pitanja. Ako je takav tiket ustvari o incidentu, promeni ili problemu, tip tiketa se menja u skladu sa tim

Komunikacija između SOC tima i klijenata može da se izvede na dva načina, bilo proaktivno od strane SOC tima ili kada ga klijent inicira.
U slučaju proaktivne intervencije od strane SOC tima, na osnovu analiza sistemske aktivnosti i njenog bezbednosnog uticaja, SOC deluje pre nego što problem ima šansu da se razvije:

- Inženjer SOC tima kontaktira IT predstavnika na klijentskoj lokaciji kako bi diskutovao o najnovijim nalazima
- Ako je potrebno, SOC tim otvara tiket i označava tip tiketa, tj zahtev, održavanje, incident ili izmena
- SOC obrađuje tikete i rešava incidente, održavanje i druge zahteve. Ako je izmena, prosleđuje Security Expert timu koji koordinira i implementira izmene i popravke konfiguracije za lokaciju klijenta.

U slučaju interakcije sa SOC timom, koju inicira klijent:

- Klijenti, korisnici i partneri preciziraju svoje bezbednosne zahteve svojim IT administratorima
- Klijentov IT administrator, kontaktira SOC tim koji otvara tiket i označava tip tiketa, tj. zahtev, održavanje, incident ili promenu
- SOC tim obrađuje tikete i rešava incidente, održavanje i druge zahteve. Ako je izmena, prosleđuje Security Expert timu koji koordinira i implementira izmene i popravke konfiguracije za lokaciju korisnika.

ZAKLJUČAK

Važnost cyber bezbednosti će nastaviti da raste kako se tehnologija bude razvijala i kako se budu pojavljivale nove pretnje za preduzeća svih razmera. Potražnja za Cloud-based uslugama ima poseban značaj u povećanju ranjivosti za preduzeća bez uspostavljene bezbednosne mreže. Ulaganje u strategiju za pomoć u odbrani od bezbednosnih napada sada je važnije nego ikada.

Bez obzira da li preduzeću nedostaje bezbednosni program ili jednostavo žele da prošire svoje bezbednosne mere, Managed Security Service Provajderi su dragocena opcija. Vrhunska zaštita, ušteda troškova, fokus poslovanja, sigurnosni stručnjaci i vrhunska tehnologija su samo neke od prednosti koje preduzeće mogu da očekuju kada traže podršku bezbednosti izvan svoje organizacije. Rukovodioci imaju fleksibilnost da se obrate stručnjacima kako bi osnažili svoje bezbednosne timove kako bi posao i njihovi kupci mogli da ostanu u fokusu organizacije.

LITERATURA

[1] Global Cybercrime damages predicted to reach $6 trillion annually by 2021, Cybercrime magazin, dostpuno na: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] Benefits of a managed security service provider, YouTube kanal Hitachi system security, dostupno na: https://www.youtube.com/watch?v=yNRWBeaP1uA

[3] Managed security service providers (MSSP), TechTarget, dostpuno na: https://searchitchannel.techtarget.com/definition/MSSP?fbclid=IwAR3SbY3lyXQOpgQw_IFCU8Nqm7i6DOTtm9drzWdeI0_hylWvOnK4gg54bDU

[4] What are Managed security service providers? Why organizations hire Managed security service providers, DATAINSIDER Digital Guardians Blog, dostpuno na: https://digitalguardian.com/blog/what-are-managed-security-services-why-organizations-hire-managed-security-service-providers

[5] What's a ticketing system?, HubSpot, dostupno na: https://blog.hubspot.com/service/ticketing-system

[6] Why a Managed security service provider is good for your bussiness, Impact, dostpuno na: https://www.impactmybiz.com/blog-why-a-managed-security-service-provider-mssp-is-good-for-your-business/

[7] The 5 Benefits of a Managed Security Service Provider, Hitachi, dostpuno na: https://www.hitachi-systems-security.com/blog/benefits-managed-security-service-provider/

[8] 10 Managed Security Services Benefits To Know, Cipher, dostpuno na: http://blog.cipher.com/10-managed-security-services-benefits

[9] Managed security service, Wikipedia, dostupno na: https://en.wikipedia.org/wiki/Managed_security_service