Security
Operations
Center

ODBRANA DIGITALNOG

Security Operation Center - fleksibilni outsourcing u domenu IT bezbednosti

IT Security ili *Cyber Security* u današnje vreme nije samo jedna od funkcija IT-a, već predstavlja ključni element za celokupno poslovanje kompanije. Pretnje i izazovi u ovoj oblasti postaju sve složenije i zahtevaju „svesnost" i stalna ulaganja u vidu ljudskih i tehničkih resursa. Zato *outsourcing IT security* usluga predstavlja optimalan odgovor na ove izazove, jer pored smanjenja rizika u poslovanju smanjuje i kapitalna i operativna ulaganja.

Zašto je bitan IT security?

U digitalnoj ekonomiji informacija je najvažniji, a nekad i jedini resurs. Ti resursi mogu „na klik" da budu dostupni čitavom svetu, bez fizičkih i teritorijalnih ograničenja, što ih čini ranjivim i podložnim čak i većem broju napada *cyber* napada istovremeno.

Procenjuje se da je *cyber* kriminal danas „vredniji" i „unosniji" čak i od tržišta narkotika. Dodatnu težinu ovom problemu daje činjenica da praktično svaki podatak ima neku rednost. To dokazuje i učestala pojava *ransomware* napada (maliciozni softver koji kriptuje podatke na računaru, uz traženje otkupnine za njihovo otključavanje).

Zašto SOC?

Pre nekoliko godina *IT security* bio je sveden na *firewall* i na antivirusna rešenja, ali tada je i to bilo uglavnom dovoljna zaštita. U to vreme cyber kriminal nije bio toliko razvijen i pretnje su bile manje sofisticirane. To potvrđuje i činjenica da je u poslednje dve godine detektovano više različitih vrsta malicioznih programa i virusa nego u prethodnoj deceniji.

Zato danas *IT security* zahteva, ne samo velika ulaganja u ljudske i tehničke resurse, već i konstantno praćenje i prilagođavanje trendovima. Zbog navedenih razloga kapitalni i operativni *IT security* troškovi postaju sve veći i sve teže se uklapaju u dostupne budžete.

Sagin Security Operations Center, kao delimični ili potpuni *security outsourcing*, predstavlja optimalan, efikasan i jeftin odgovor na ove izazove.

SAGA
new frontier group

Usluge SOC-a

Namensko angažovanje eksperata za bezbednost

Jedna od najvažnijih prednosti je angažovanje **posvećenog tima *security* eksperata**. Veće kompanije verovatno imaju sopstvene timove i ekspertizu u ovoj oblasti, ali čak i u tom slučaju Sagin SOC tim predstavlja efikasnu dopunu internom timu u oblastima koje oni ne pokrivaju. Ekspertski tim SOC-a pokriva bezbednosna rešenja velikog broja različitih proizvođača i sarađuje sa brojnim institucijama u domenu IT bezbednosti. Široko polje delovanja ovog tima zato predstavlja značajnu prednost u borbi protiv svih vrsta *cyber* pretnji.

Niži troškovi i skalabilnost

Sagin SOC obezbeđuje **24/7 monitoring** i minimizovanje efekata incidenata. U većini kompanija ne postoje resursi za angažovanje internog tima koji će biti dostupan u tri smene. Sagin SOC pruža non-stop monitoring bez potrebe za proširenjem internih timova. Ovakav pristup je skalabilan: infrastruktura i procesi obezbeđeni su od starta u sklopu usluge, a resursi se prilagođavaju klijentu i rastu bez potrebe za dodatnim kapitalnim investicijama.

Svesnost i fokusiranost

Iskustvo koje je Sagin SOC tim stekao na velikoj bazi klijenata pruža mnogo širi pogled nego što ga imaju interni resursi. Slične, ili čak iste pretnje mogu da se jave kod više klijenata, pa stečeno specifično iskustvo kod jednog klijenta može da se primeni za bržu i efikasniju detekciju i uklanjanje pretnji kod drugih klijenata. IT i *security* rešenja u kompanijama često predstavljaju izolovana ostrva, kako u smislu tehničke integracije tako i u smislu jurisdikcije različitih timova i osoba. Sagin SOC je u mogućnosti da prati celokupan IT sistem uz efikasnu korelaciju događaja i realno prepoznatih incidenata, na osnovu kojih se preduzimaju odgovarajuće akcije za minimizaciju njihovih efekata.

Šta donosi SOC?

Osnovni operativni korak u povećanju bezbednosti sistema, a samim tim i smanjenju rizika u poslovanju jeste postizanje visokog stepena „vidljivosti" nad celim sistemom. To je ključni faktor u svim fazama potencijalnog incidenta i njegovoj prevenciji, detekciji i odgovoru na njega. To nije samo praćenje rada sistema, već filtriranje, korelacija i fokusiranje na prave incidente. U praksi, to je kao traženje igle u plastu sena.

Sagina SOC usluga prilagođava se specifičnostima svakog okruženja i svake organizacije. U mogućnosti je da prati sisteme koji su sastavljeni od rešenja različitih proizvođača, a pre faze implementacije Sagin tim eksperata za bezbednost aktivno radi sa korisnikom u cilju analize zahteva i potpunog pokrivanja svih sigurnosnih aspekata sistema.

Do 2020. godine 75% budžeta velikih kompanija za IT security trošiće se na brzu detekciju i odgovore na cyber napade, dok je 2012. godine na to trošeno manje od 10% budžeta.

„Five Golden Rules for Creating Effective Security Policy", Gartner security report, septembar 2014.

SAGA
new frontier group

Saga d.o.o. Beograd
64a Zorana Djindjica Blvd.
11070 Belgrade, Serbia
www.saga.rs

Više od polovine organizacija će do 2018. godine koristiti usluge kompanija koje su specijalizovane za zaštitu podataka, upravljanje sigurnosnim rizicima i sigurnosnom IT infrastrukturom u cilju podizanja nivoa IT bezbednosti.

Gartner's 2014 Security and Risk Management Summit, London, septembar 2014.