OPĆA OPASNOST IOT ĆE DOVESTI DO TOGA DA ĆE USKORO SVAKI AUTOMOBIL POSTATI POTENCIJALNA META IT NAPADA

Renato Telen, voditelj data centra Megatrend poslovnih rješenja, govori o sigurnosti cloud sustava, opasnostima koje donosi internet stvari (IoT) te spremnosti na štete kibernetičkih napada

Na IT sigurnosna rješenja većina tvrtki još uvijek gleda kao na nužno zlo

Ekstremna raširenost mobilnih uređaja te njihova 'informatička' snaga trenutačno predstavljaju gotovo nesavladiv izazov u postizanju IT sigurnosti

Jedan od najvećih privatnih podatkovnih centara u Hrvatskoj, onaj Megatrenda, ima dobar uvid u to koliko je cloud promijenio poimanje ICT sigurnosti. O tome smo razgovarali s voditeljem data centra Megatrend poslovnih rješenja Renatom Telenom.

Kako se danas najefikasnije zaštititi od cyber napada kad je glavna ICT paradigma cloud? Kakva rješenja vi nudite za to?

Samo korištenje clouda nije značajno promijenilo način i metode zaštite od cyber napada. Naročito jer su kvalitetni cloud sustavi u principu puno bolje zaštićeni od cyber napada nego većina korisnika u svojim 'on premise' IT sustavima. Sveobuhvatna zaštita od cyber napada zahtijeva i sveobuhvatno rješenje za zaštitu. Pod rješenjem se ne govori samo o software rješenjima, nego i o postavljanju niza radnih i operativnih procedura te ispravnom i sveobuhvatnom dizajnu IT sustava. Većina korisnika štiti svoj IT sustav od napada izvana, a u potpunosti zanemaruje sigurnosne elemente potrebne za zaštitu sustava iznutra. Takvo ponašanje otvara nekoliko sigurnosnih problema. Ako napadač izvana uspije doći do barem jednog unutarnjeg sustava, vrlo mu je lako proširiti se i na ostale unutarnje sustave.

S druge strane, svi imamo korisnike (zaposlenike tvrtke) koji moraju (i dozvoljeno im je) koristiti unutarnje IT sustave. Vrlo je teško i gotovo nitko to ne radi, uspostaviti nadzor nad korisnicima koji imaju ovlasti koristiti IT sustave. Što ako se dogodi da imamo zlonamjernog unutarnjeg korisnika? Kako možemo dokazati njegovu zlu namjeru ili djelo? Ili još puno jednostavnije - što ako naš korisnik nosi i koristi službeno računalo kod kuće gdje je puno manje zaštićen pa se računalo zarazi nekim malicioznim kodom ili neki haker probije zaštitu i ima mogućnost pokretanja koda na računalu (bez znanja vlasnika, naravno). Kada se onda naš korisnik spoji na mrežu firme, ako ne postoje odgovarajuće zaštite, haker je u stanju nesmetano se koristiti našim unutarnjim sustavima.

Koja su danas najtraženija rješenja iz područja ICT sigurnosti?

Današnja IT sigurnosna rješenja moraju zadovoljiti mnogo raznorodnih zadataka. Od jednostavne inspekcije prometa, analize paketa, otkrivanja malicioznih paketa, otkrivanja i sprječavanja izvršenja malicioznog koda sve do kompletne analize eventualnih ranjivosti, analize rizika, vođenja kompletnog 'asset management' sustava IT-a. Jedna činjenica je zajednička svim IT sigurnosnim sustavima - većini nedostaje kvalitetnih sigurnosnih stručnjaka. Trenutačne analize američkog tržišta, a ostatak svijeta nije puno drugačiji, pokazuju da će do 2020. Americi nedostajati oko tri milijuna ljudi za pogon IT sigurnosnih sustava. Svako rješenje mora osim kvalitetne zaštite, osigurati i mnoge druge elemente ako se želi uspješno primijeniti - jednostavnost korištenja, jednostavnost implementacije, automatsko praćenje novih prijetnji, centralno upravljanje i nadzor, 'pokrivanje' svih IT platformi i produkata te performanse - samo su neki od elemenata koje svako kvalitetno rješenje mora ispuniti.

IT usluge se šire svjetlosnom brzinom na područja koja do sada nisu bila korištena, a nije postojao ni nikakav IT security. Internet stvari (IoT) i njegovo ubrzano širenje će u vrlo kratko vrijeme dovesti do toga da je svaki automobil potencijalna meta IT napada. Ekstremna raširenost mobilnih uređaja te njihova 'informatička' snaga trenutačno predstavljaju gotovo nesavladiv izazov u postizanju IT sigurnosti.

Telen napominje kako se često implementiraju rješenja koja ne pružaju adekvatnu zaštitu

DANIJEL BERKOVIĆ/ PIXSELL

Kad pogledate pet godina unazad i to usporedite sa stanjem danas, vidite li napredak u prepoznavanju važnosti ICT sigurnosti među domaćim tvrtkama?

Neki napredak postoji i vidljiv je no niti blizu ne odgovara realnim potrebama i očekivanjima. Tvrtke u principu reagiraju reaktivno - kada se nešto dogodi, onda se ide u istraživanje rješenja i nažalost se implementira rješenje koje je financijski 'primamljivo', ali zapravo ne i dovoljno dobro. Tvrtke koje su u svom poslovanju vezane na neke regulatorne ili slične obaveze ulažu nešto više u sigurnosna rješenja, ali vrlo su rijetke tvrtke koje imaju sveobuhvatno i kvalitetno rješenje. Razloga za to ima mnogo - sigurnosna rješenja su u principu skupa, zahtijevaju dodatne visoko stručne kadrove kao i značajan operativni pogon i trošak.

Na IT sigurnosna rješenja se još uvijek gleda kao na nužno zlo. Vrlo je malo tvrtki koje su realno izračunale koliki gubitak u poslovanju, direktan ili indirektan, predstavlja šteta nanesena cyber napadom - gubitak podataka, nedostupnost servisa, objavljivanje tajnih podataka i slično.

> JEDNA ČINJENICA JE ZAJEDNIČKA **SVIM IT SIGURNOSNIM SUSTAVIMA - VEĆINI NEDOSTAJE KVALITETNIH SIGURNOSNIH STRUČNJAKA**. ANALIZE KAŽU DA ĆE DO 2020. AMERICI NEDOSTAJATI OKO TRI MILIJUNA LJUDI ZA POGON IT SIGURNOSNIH SUSTAVA

Koja vi rješenja nudite u području cyber sigurnosti?

Megatrend nudi rješenja u svim segmentima IT sigurnosti: QRadar kao sveobuhvatno IT sigurnosno rješenje, MaaS360 rješenje za sigurnost mobilnih uređaja i prijenosnih računala, StoredIQ rješenje za kontrolu pristupa te organiziranje ne strukturiranih podataka (fileovi, mailovi itd.) i Guardium rješenje za kontrolu pristupa bazama podataka. Zajednička svim rješenjima je mogućnost instalacije kod korisnika (osim MaaS360), ali i korištenje kao cloud usluge iz Megatrend data centra. Korištenje IT sigurnosnih sustava kao cloud usluge donosi nekoliko značajnih prednosti u odnosu na instalaciju na vlastitoj lokaciji. Cloud usluga ne zahtijeva kapitalni trošak (nema nabavke opreme, licencija), usluga se implementira u vrlo malo vremena te se proširuje i optimizira prema potrebama, a korisnik ima pristup portalu sa svim informacijama i akcijama. Svi korisnici su striktno izolirani u vlastita okruženja.

QRadar je SIEM (Security Information Management System) koji pokriva sva područja nadzora svih IT segmenata (mrežni promet, sva računala, svi OS, kontrole pristupa, distribuciju SW-a itd.). Qradar je izravno povezan sa svjetskom bazom poznatih IT security napada - XForce s koje automatski dobiva sve informacije o napadima, ali i o rješenjima. On je prvi komercijalno dobavljivi IT sigurnosni sustav koji koristi Watson Advisor - sustav umjetne inteligencije za analizu i sprječavanje sigurnosnih IT događaja.

MaaS360 je cloud usluga upravljanja mobilnim uređajima (uključivo i mobilna računala) koji podržava sve OS-ove (iOS, Android, WinMobile...) i pokriva sve segmente nadzora i upravljanja - kontrolu uređaja, siguran email, sigurnu distribuciju dokumenata, antimalware te siguran pristup u korporativnu mrežu.StoredIQ je sustav koji nadzire pristup ali i lokaciju nestrukturiranih podataka. Po potrebi može seliti podatke na dopuštene (zaštićene) lokacije ako su isti pronađeni na nedopuštenim (neosiguranim) lokacijama. StoredIQ se pokazao kao vrhunski učinkovit alat u 'discovery' fazi implementacije GDPR projekata. Gaurdium je alat koji kontrolira i bilježi pristup bazama podataka bez obzira na koji način se pristupa. Izuzetno je učinkovit za auditing svrhe - praćenje i izvještavanje o pristupima. ***pd***