PC PRESS

Bezbednost

SPECIJALNI DODATAK ČASOPISA PC PRESS #335

Hakeri ne spavaju: sajberbezbednost danas

Osnovna paradigma se promenila. Više se ne radi o podizanju neprobojnih zidova, već o izgradnji otpornosti. Hakeri ne spavaju: uvek će se naći neko ko će pokušati da napadne baš vašu kompaniju, da ukrade baš vaše podatke. Kako da brzo detektujemo pretnju i napad, da ograničimo štetu i oporavimo se?

Luka Milinković

Globalni izveštaji svetskih IT giganata, kao i konsultantskih i analitičkih kuća potvrđuju ono što vidimo u praksi. S razvojem tehnologije, a posebno veštačke inteligencije, sajberpretnji i novih opasnosti nije manje, već ih je, zapravo, sve više... i sve su opasnije. Stvari ipak nisu crne, jer i bezbednost napreduje, ali samo ako pratimo bezbednosne trendove: standarde, metodologije, tehnologiju, rešenja. Treba da budemo oprezni i spremni na nove izazove! A uz adekvatnu pripremu, i korak ispred napadača. Procena rizika, a zatim prevencija i spremnost na nova dešavanja mnogo su bolji nego čekati da se stvari same dese i iznenaditi se onim što smo mogli da pretpostavimo.

Veštačka inteligencija u službi prevaranata

Napredak tehnologije u svakom smislu, a posebno u pravcu veštačke inteligencije, dovodi do razvoja novih i unapređenja postojećih metoda odbrane i zaštite IT infrastrukture i kritičnih podataka, ali i do razvoja sofisticiranijih pretnji i tehnika napada.

Njeno veličanstvo Veštačka Inteligencija sada je u službi svih. I čuvara i prevaranata. I stvaralaca i uništitelja. I svako pokušava da je iskoristi na najbolji način za svoje interese i (poslovne) potrebe.

Mnoge pretnje su ostale, kao što je *phishing*, ali su evoluirale. Retki su e-*mail*-ovi u kojima zlonamerne osobe samo pozivaju da kliknete na *random* generisan link. Sada u kreiranju *phishing* pretnji aktivno učestvuje AI, stvarajući mnogo bolji sadržaj prilagođen vrsti napada, ciljanoj kompaniji ili čak samom korisniku.

Nova generacija *phishing* napada, pokretana veštačkom inteligencijom, prevazilazi ranije nedostatke, kao što su loš pravopis, generičke poruke i lako uočljivi lažni linkovi. Tako napadači sada uz pomoć sofisticiranih AI alata kreiraju personalizovane, uverljive i teško prepoznatljive prevare, a

EKONOMIJA SAJBERKRIMINALA KAO USLUGE

Specijalizovane kriminalne grupe sada nude svoje „usluge“ na mračnoj strani Interneta kroz *Cybercrime-as-a-Service* – CaaS. Tako da je moguće iznajmiti pristup mrežama, kupiti zlonamerni softver ili unajmiti tim za izvođenje *ransomware* ili *phishing* napada, što značajno smanjuje tehničku barijeru za ulazak u svet sajberkriminala.

Veliki problem za organizacije je hronični nedostatak kvalifikovanih stručnjaka za informacionu bezbednost. Ovaj jaz onemogućava efikasno korišćenje naprednih bezbednosnih tehnologija i pravovremeni odgovor na incidente

sami napadi postaju znatno efikasniji nego ranije.

Koristeći modele za obradu prirodnog jezika (NLP), slične onima koji pokreću napredne *chat* botove, napadači mogu da generišu e-*mail*-ove i poruke koji su gramatički besprekorni i stilski prilagođeni. AI analizira ogromne količine podataka sa društvenih mreža, različitih sajtova i drugih javno dostupnih izvora kako bi se prikupile informacije o meti. Rezultat ovakvih analiza su poruke koje mogu da imitiraju ton komunikacije određene kompanije, pa čak i stil pisanja konkretne osobe, koji za žrtvu može biti kolega ili nadređeni. Ovakav nivo personalizacije čini prevaru znatno težom za otkrivanje. Tako, na primer, e-*mail* može da sadrži informacije o nedavnom poslovnom događaju, projektu na kojem žrtva radi ili druge lične detalje iz privatnog ili poslovnog života, koji su nađeni na Internetu. I sve to kako bi se stvorila iluzija legitimnosti.

Deepfake audio i video prevare

Jedna od najopasnijih primena veštačke inteligencije u *phishing*-u jeste upotreba *deepfake* tehnologije. Na ovaj način napadačima se omogućava da kreiraju veoma realistične audio i video snimke koji imitiraju glas i izgled osobe od poverenja, kao što je direktor kompanije (CEO), kolega ili član porodice.

Ova vrsta napada može biti izuzetno ubedljiva. Da ovo nije samo mašta, pokazuju zabeleženi slučajevi gde su zaposleni u finansijskim odeljenjima primali glasovne poruke ili pozive, navodno od svojih direktora, sa hitnim zahtevom za transfer novca. S obzirom na autentičnost glasa, žrtve često ne posumnjaju u prevaru. Da li treba da budemo sumnjičavi ili da svima i svemu verujemo? Izgleda da je danas najbolja zaštita: sumnjaj u sve što pročitaš, vidiš ili čuješ! Sumnjaj u svaki digitalni sadržaj koji nisi (dobro) proverio.

Tako, po ko zna koji put, dolazimo do *Zero Trust* arhitekture, koja je ključna za svaku kompaniju, za svaki server, za svaki IT ekosistem. Samo sada ona dobija još šire značenje. *Zero Trust* arhitektura nalaže da se nijednom korisniku ili uređaju ne veruje podrazumevano. Svaki zahtev za pristup resursima mora biti strogo proveren, bez obzira na to odakle dolazi. Danas možemo sumnjati i u svaki digitalni sadržaj, jer se lakše nego ikada može generisati sadržaj koji će izgledati stvarno, pa i bolje od toga.

Sve ovo nije samo pitanje obmanjivanja žrtve, već i obmanjivanja svih ostalih. Tako reputacija žrtve može biti ozbiljno narušena ako se napadač okomi na nju. Kreiranje lažnih, kompromitujućih fotografija, videa, audio materijala može se brzinom svetlosti proširiti Internetom bez ikakvog znanja žrtve. Bez očekivanja i mogućnosti da reaguje, nanoseći ogromnu štetu i ružne posledice. Ali kome sve? Da li samo žrtvi? Ili i bližnjima u privatnom i poslovnom životu, a vrlo često i samoj kompaniji.

RANSOMWARE 3.0

Ransomware napadi nisu više samo pitanje enkripcije podataka. Za razliku od tradicionalnih *ransomware* i *ransomware* 2.0 napada, sajberkriminalci su više zainteresovani za podatke koji se čuvaju na uređajima žrtve, pa tako napadi uključuju krađu osetljivih podataka pre šifrovanja, pretnju objavljivanjem, DDoS napade i direktno ucenjivanje klijenata i partnera žrtve.

Automatizacija i optimizacija napada

Veštačka inteligencija omogućava napadačima da automatizuju i skaliraju svoje operacije na do sada neviđenom nivou. AI algoritmi mogu da analiziraju ponašanje mete, kao što su, na primer, radne navike ili vreme odgovaranja na e-*mail* sadržaje, kako bi odredili optimalan trenutak za slanje *phishing* poruke i tako povećali šanse za uspeh.

Da li treba da budemo sumnjičavi ili da svima i svemu verujemo? Izgleda da je danas najbolja zaštita: sumnjaj u sve što pročitaš, vidiš ili čuješ

Pored toga, AI čet-botovi mogu da se koriste za interakciju sa žrtvama u realnom vremenu na lažnim sajtovima ili putem društvenih mreža kroz lažne profile, postepeno gradeći poverenje pre nego što zlonamerne osobe zatraže osetljive informacije.

AI je posebno unapredila ciljane *phishing* (*spear phishing*) napade, koji su usmereni na specifične pojedince ili organizacije. Automatizovanim prikupljanjem podataka, AI omogućava kreiranje visokociljanih i relevantnih poruka koje je gotovo nemoguće razlikovati od legitimne komunikacije.

U kontekstu napada pomoću kompromitovanih poslovnih e-*mail*-ova (*Business* E-*mail Compromise* – BEC), napadači koriste AI da imitiraju internu komunikaciju i ubede zaposlene da izvrše neovlašćene aktivnosti, kao što su transferi novca, otkrivanje poverljivih podataka, slanje poverljive dokumentacije, davanje povišenih privilegija itd.

Tradicionalno više nije dovoljno

Stručnjaci za sajberbezbednost upozoravaju da tradicionalne mere zaštite, poput spam filtera, često nisu dovoljne da zaustave AI generisane pretnje. Zbog toga je od ključne važnosti kontinuirana edukacija zaposlenih, razvijanje kritičkog razmišljanja prilikom provere elektronske komunikacije i primena naprednih bezbednosnih rešenja koja koriste veštačku inteligenciju za detekciju anomalija u komunikaciji.

Važno je da se svaka sumnjiva situacija koja se ispita u kompaniji pažljivo proceni: ako nije suviše poverljiva, treba je preneti svim zaposlenima u kompaniji. Na taj način zaposleni bi se upoznali sa stvarnim pretnjama koje nisu samo predmet mašte sajberinženjera i bezbednosnih edukacija već su se stvarno dogodile. Neki od primera koje bi trebalo predstaviti zaposlenima nakon što se uoče u kompaniji su:

- lažni profili na društvenim mrežama gde se osobe predstavljaju lažnim opisima poslova (nekada čak i u vašoj kompaniji), lažnom biografijom, lažnom fotografijom, vrlo često generisanom AI alatima;
- *phishing* e-*mail*-ovi koje su stigli pojedinim zaposlenima;
- pokušaji prevare preko telefonskih poziva;
- lažno kreirani sajtovi na koje su se usmeravali zaposleni prilikom posete legitimnih sajtova;
- lažni (kompromitujući) video, audio ili foto materijali nekih zaposlenih;
- haking napadi na kompanije s kojima sarađujete bilo da su vaši klijenti, partneri ili vendori.

NAPADI NA LANAC SNABDEVANJA

Napadi na lanac snabdevanja (*Supply Chain Attacks*) su napadi gde kompromitovanjem jednog softverskog vendora ili servis provajdera, napadači mogu istovremeno ugroziti hiljade njegovih korisnika. Napadači ciljaju manje bezbedne karike u lancu snabdevanja kako bi stekli pristup mrežama stotina ili hiljada njihovih klijenata, što ovakve napade čini izuzetno efikasnim i teškim za odbranu.

Veštačka inteligencija omogućava napadačima da automatizuju i skaliraju svoje operacije na do sada neviđenom nivou

Ko je odgovoran za bezbednost podataka?

Još jedan od velikih problema za organizacije jeste i hronični nedostatak kvalifikovanih stručnjaka za informacionu bezbednost. Ovaj jaz onemogućava efikasno korišćenje naprednih bezbednosnih tehnologija i pravovremeni odgovor na incidente. U poslednje vreme je primetno da svest o bezbednosnim rizicima raste, a to dovodi do povećanja budžeta za IT i sajberbezbednost. Takođe, fokus se stavlja na alate i rešenja za sveobuhvatniju zaštitu i bolju integraciju postojećih resursa, kao i na ulaganje u ljudske resurse i sprovođenje zahteva standarda i regulative. Vrlo često se ulazi i u eksternalizaciju sajberservisa kako bi se dobili veća stručnost i brže reagovanje u kritičnim situacijama.

Stručnjaci, ali i kompanije, počinju da shvataju da se nijedna organizacija ne može boriti i odbraniti sama, pa tako raste značaj platformi za razmenu informacija o pretnjama (*Threat Intelligence Sharing*), kako unutar industrijskih sektora, tako i između privatnog i javnog sektora. A sve sa ciljem adekvatne zaštite, jače odbrane i bolje iskorišćenosti novih tehnologija u cilju prevencije i detekcije pretnji, a ne boljeg kreiranja napada. I ono najvažnije. Bezbednost je odgovornost svih nas! Svaki zaposleni, od direktora do praktikanta, ima ulogu u zaštiti informacija.

Cisco bezbednosna arhitektura kao ključ kontinuiteta i sigurnosti poslovanja kompanija

Kompanija Cisco, kao jedan od globalnih lidera u oblasti mrežnih i bezbednosnih rešenja, već decenijama gradi arhitekture koje imaju za cilj da kompanijama obezbede stabilnost i otpornost na napade. Upravo ideja da poslovanje danas zavisi od brzine i otpornosti u kriznim situacijama stoji iza Cisco bezbednosne arhitekture

Nikola Milovanović, Technical Presales Architect

Danas je gotovo nemoguće zamisliti uspešan biznis bez snažne i pametno postavljene bezbednosne mrežne arhitekture. Pretnje su sve raznovrsnije – od sofisticiranih sajbernapada (npr. *spear phishing* i ransomware) do krađe podataka – a kompanije žive u okruženju gde je poslovni kontinuitet jednako važan kao i sam proizvod ili usluga koju nude. Gubitak podataka danas ne znači samo tehnički problem, već vrlo često gubitak poverenja partnera i klijenata, što u mnogim slučajevima može predstavljati nepovratan udarac za samu kompaniju.

Kompanija *Cisco*, kao jedan od globalnih lidera u oblasti mrežnih i bezbednosnih rešenja, već decenijama gradi arhitekture koje imaju za cilj da kompanijama obezbede stabilnost i otpornost na napade. Važnost takvih rešenja najbolje se vidi kroz realne događaje – podsetimo se samo tragedije rušenja Svetskog trgovinskog centra u Njujorku 2001. godine, kada su mnoge kompanije koje nisu imale adekvatno rešeno čuvanje i zaštitu podataka jednostavno prestale da postoje, dok su one koje su imale dobro osmišljene planove kontinuiteta poslovanja nastavile rad već posle nekoliko dana.

Fazna implementacija Cisco bezbednosne mrežne arhitekture predstavlja optimalno rešenje za većinu kompanija, jer omogućava da se kompleksni projekti sprovode postupno, u skladu sa finansijskim planovima i prioritetima

Napadači vrebaju...

U našem okruženju, na brdovitom Balkanu, do pre pet ili šest godina problem kontinuiteta rada poslovnih IT sistema kompanija bio je uglavnom povezan s dostupnošću napajanja i pouzdanošću rada samih mrežnih uređaja, radnih stanica i servera. Danas, hteli mi to da priznamo ili ne, kompanije i organizacije u Srbiji se sve više suočavaju s problemima koji postoje u ekonomski najrazvijenijim državama sveta, a koji se odnose na sajbernapade. Broj sajbernapada u Srbiji je u stalnom porastu, napadi su sve sofisticiraniji (na primer, broj detekcija *ransomware*-a porastao je za 71,6 odsto u 2024. godini, dok je broj napada na banke i POS terminale šest puta povećan u odnosu na prethodnu godinu), očigledan je nedostatak kadrova u sektoru sajberbezbednosti i nedovoljna je implementacija industrijskih bezbednosnih standarda.

Upravo ta lekcija – da poslovanje danas zavisi od brzine i otpornosti u kriznim situacijama – stoji i iza *Cisco* bezbednosne arhitekture, koja kombinuje savremene tehnologije i inteligentno upravljanje rizicima u jedinstveno rešenje.

Cisco bezbednosna arhitektura *(Cisco Security Architecture)* daje pregled *Cisco* bezbednosnog portfolija, najčešćih scenarija primene i preporučenih mogućnosti u okviru jedinstvene arhitekture. Ovaj referentni model povezuje se i sa oblastima koje prate industrijske bezbednosne okvire, kao što su NIST, CISA i DISA.

Osnovne komponente

Pet osnovnih komponenti *Cisco* bezbednosne referentne arhitekture su:

- lokalne mreže (*on-premises*) i mreže na ivici oblaka (*cloud edge*);
- bezbednost korisnika/zaposlenih i uređaja koje koriste;
- bezbednost opterećenja radnih stanica i aplikacija;

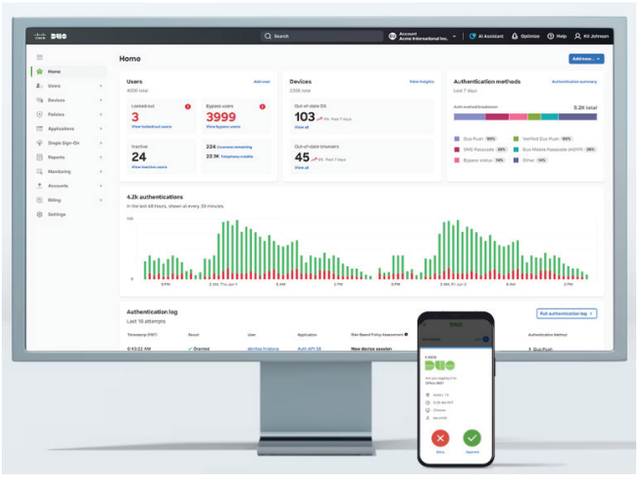
Cisco Security Platform

- centar za bezbednosne operacije, tzv. SOC (*Security Operations Center*) i
- bezbednost platformi u oblaku (*cloud security*).

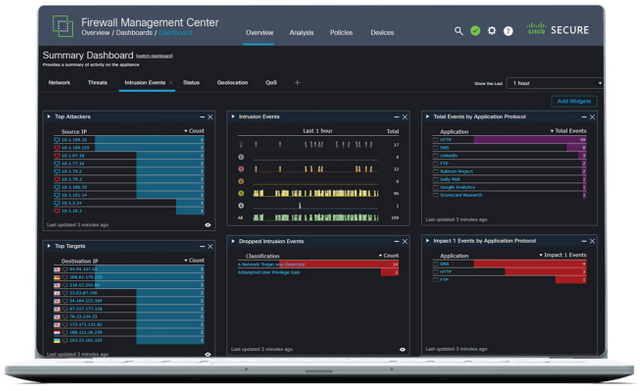
Svaka kompanija ima jedinstveno mrežno okruženje (i lokalno i u oblaku) zasnovano na sopstvenim poslovnim potrebama, tako da nije neophodno odmah primeniti kompletnu *Cisco* bezbednosnu arhitekturu, već je preporuka da se radi fazna implementacija. Iskustvo iz višedecenijske prakse na domaćem IT tržištu, pokazuje da je druga bitna komponenta uspešnog bezbednosnog „koktela" da kompanijski IT i bezbednosni tim razmotri sve bitne parametre bezbednosti poslovnog sistema (kao što su kritične poslovne aplikacije, koji zaposleni ili spoljni saradnici udaljeno pristupaju važnim resursima kompanije) i da zajedno sa *Cisco* ekspertima zajedno mapiraju svoj put bezbednosti.

Fazna implementacija *Cisco* bezbednosne mrežne arhitekture predstavlja optimalno rešenje za većinu kompanija, jer omogućava da se kompleksni projekti sprovode postupno, u skladu sa finansijskim planovima i prioritetima. Istovremeno, ovakav model uvodi mogućnost stalnog usklađivanja sa uvek prisutnim promenama u okruženju sajberbezbednosti.

Duo



FMC



Cisco koktel

Nakon sagledavanja opštih aspekata, vreme je da pređemo na detaljnije predstavljanje sastojaka *Cisco* bezbednosnog „koktela" koji kompanijama omogućava kontinuitet i bezbednost poslovanja, odnosno miran san i nesmetan rad.

Cisco bezbednosna arhitektura sastoji se od funkcionalnih modula i mogućnosti koje pružaju višeslojnu zaštitu, kao što su *Zero Trust* (nulto poverenje za svakog korisnika), SASE (siguran pristup kao servis na ivici mreže) i XDR (prošireno otkrivanje i reagovanje za zaštitu uređaja koje koriste zaposleni i drugi krajnji korisnici) za SOC centar. Krajnji spoljni sloj predstavlja platforma pod nazivom *Security Cloud Control.* Ova platforma u oblaku koristi AI/ML algoritme, otvorena je i proširiva i omogućava jedinstveno upravljanje procenom rizika za sve unutrašnje module arhitekture. *Talos* je sistem globalne bezbednosne inteligencije sa ciljem praćenja pretnji, pružanja akcionih informacija o pretnjama i istraživanje malvera u realnom vremenu, na celoj globalnoj Internet mreži. SOC funkcionalnosti, poput reputacije IP adresa i domena, SNORT potpisa, analize i kontrole malicioznih fajlova, kategorizacije URL-ova i AI odbrane, dostupne su u više tačaka korporativnog sistema – krajnji uređaji, *firewall* uređaji nove generacije (NGFW), e-*mail*, *cloud gateway*-i i radne stanice i serveri.

Firewall sledeće generacije

Cisco NGFW (Next-Generation Firewall) pruža naprednu zaštitu mreže kombinujući tradicionalni firewall sistem sa funkcijama kao što su inspekcija aplikacija, prevencija upada i integrisana zaštita od malvera. Omogućava kompanijama da precizno kontrolišu pristup aplikacijama i resursima, dok AI i analitika pomažu u prepoznavanju i blokiranju sofisticiranih pretnji.

Ispod sloja operacija bezbednosti nalaze se *Zero Trust* i SASE moduli, koji pokrivaju celu arhitekturu – od korisnika i uređaja do radnih opterećenja (radne stanice i serveri) i aplikacija u okruženju više oblaka (*multicloud*). Funkcionalnosti za bezbednost korisnika i uređaja osiguravaju što jednostavnije korisničko iskustvo kroz jedinstveni *Secure Client,* uz visoku zaštitu od pretnji poput *phishing*-a i *ransomware*-a. Put podataka od korisnika/uređaja do radnih stanica i servera, i aplikacija može se ostvariti preko *Cloud Edge* mreže ili lokalnih (*on-premises*) mrežnih modula.

Jedna od osnovnih prednosti sistemski razvijene arhitekture leži u mogućnostima deljenja kontekstualnih informacija i identiteta. Osnovna funkcionalnost počinje sa *Cisco Identity Services Engine* (ISE) i proteže se do *Cloud Edge,* SD-WAN, IoT i radnih opterećenja i aplikacija kako bi se delile informacije o bilo kojem uređaju koji pristupa zaštićenim resursima kompanije. S druge strane, omogućena je integracija s rešenjima trećih strana (drugih proizvođača), tako da postoji dinamička i detaljna kontrola pristupa korisnika i aplikacija.

Krađa identiteta danas čini većinu bezbednosnih propusta. *Cisco Duo* je rešenje za višefaktorsku autentifikaciju (MFA) koje kompanijama omogućava da zaštite pristup svojim aplikacijama i podacima. Korisnici (zaposleni i spoljni saradnici) potvrđuju svoj identitet putem mobilne aplikacije, SMS-a, poziva ili hardverskog tokena, čime se znatno smanjuje rizik od neovlašćenog pristupa. *Duo* prati ponašanje korisnika i uređaja, pružajući uvid u potencijalne pretnje

i sigurnosne propuste. Pored toga, lako se integriše s postojećim aplikacijama i servisima u oblaku, što olakšava primenu u svakoj kompaniji.

Zero Trust arhitektura

Cisco Identity Intelligence je ključni deo *Zero Trust* arhitekture i pruža uvid u ponašanje korisnika preko različitih izvora identiteta koji se obično nalaze u mrežama kompanije. Bezbednosna politika kompanije treba da bude jasno definisana i mora reagovati na promene zasnovane na različitim podacima, kao što su informacije o pretnjama, trendovi logovanja, neuobičajeno ponašanje pri prijavljivanju, nerealna putovanja i slično.

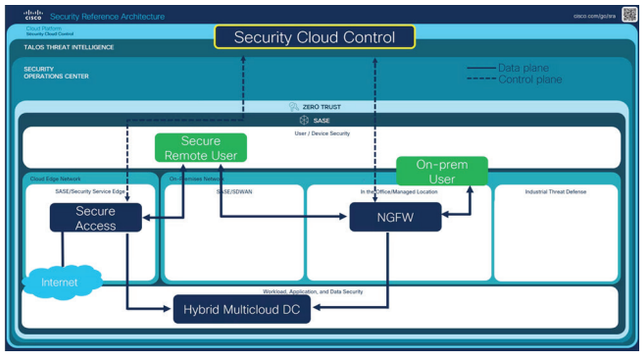
Zato referentna bezbednosna arhitektura omogućava primenu ovakvih politika, uključujući *Identity Threat Detection & Response (ITDR),* kroz *cloud edge* i lokalne mreže, kao i radna opterećenja i aplikacije u *multicloud* okruženju, kako bi SOC analitičari mogli brzo da reaguju na incidente širom mreže.

Cilj platforme *Security Cloud Control* je da omogući ujednačavanje politika i deljenje zajedničkih objekata unutar nje, pružanje integrisane arhitekture, kao što je *Hybrid Mesh Firewall,* gde se *firewall* servisi na cloud edge, lokalnim mrežama i *multicloud data* centrima mogu ujediniti i pojednostaviti, smanjujući mogućnost ljudske greške.

Security Cloud Control koristi AI mogućnosti kako bi primenio zajedničku politiku (na primer: „Zabrani Petru da koristi finansijsku aplikaciju na mobilnom uređaju nakon 17 h“) na različitim tačkama primene – fizičkim, virtuelnim ili *cloud* sigurnosnim grupama – kroz celu *multicloud* mrežu.

Univerzalni ZTNA (pristup mreži sa nultom tolerancijom) koristi *Cisco Secure Client* i omogućava korisnicima i njihovim uređajima jednostavan i siguran pristup bilo kojoj aplikaciji, bez potrebe za aktiviranjem punog VPN-a ili razmišljanjem o tome kako bezbedno pristupiti željenoj aplikaciji.

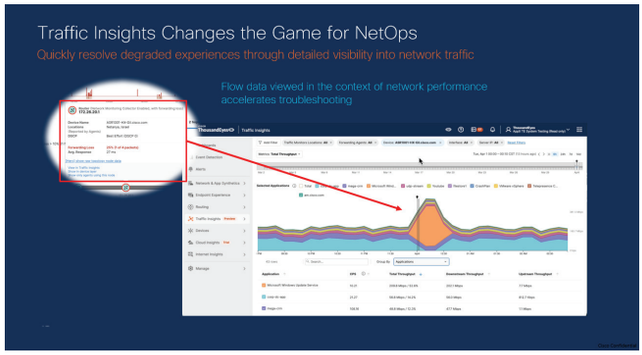
Cilj *Zero Trust* pristupa je da korisnicima bude dodeljen minimalan potreban nivo pristupa kako bi se



Universal ZTNA

sprečio neovlašćen ili prekomeran pristup. *Universal* ZTNA omogućava VPN po aplikaciji kada je moguće i definiše pravi put podataka u skladu s politikom aplikacije. Na primer, finansijska kompanija koja ne želi da koristi oblak (*cloud*), može povezivati korisnike s kritičnim aplikacijama preko lokalnih mreža, dok se nekritične aplikacije mogu koristiti preko *cloud edge* mreže.

Thousand Eyes v2



Cisco je ponudio bezbednosnu arhitekturu sa svim potrebnim sistemima koja predstavlja most između bezbednog IT okruženja i kontinuiteta poslovanja

Procena performansi

Cisco ThousandEyes pruža detaljan uvid u performanse mreže, Interneta i servisa u oblaku, omogućavajući kompanijama da prate dostupnost i brzinu svojih aplikacija. Ovaj sistem detektuje probleme u realnom vremenu, od lokalnih mreža do globalnog Interneta, i pomaže timovima da brzo identifikuju uzrok problema. *ThousandEyes* kombinuje merenja s vizuelizacijom podataka, čineći složene mrežne performanse jednostavnijim za praćenje i razumevanje. *Cisco AppDynamics* je platforma za praćenje performansi aplikacija, a omogućava identifikaciju i rešavanje problema pre nego što utiču na krajnje korisnike, optimizujući performanse i stabilnost sistema. *AppDynamics* prati sve slojeve aplikacije, od baze podataka do korisničkog interfejsa, i povezuje metrike s poslovnim rezultatima. Korišćenjem navedena dva *Cisco* sistema, koji nude vizuelizaciju i detaljne analize, timovi za IT i razvoj kompanije mogu brže donositi odluke i poboljšati efikasnost poslovnih procesa.

Danas nijedna kompanija ne može da zanemari sajberbezbednost – gubitak podataka znači gubitak poverenja i često ozbiljne poslovne posledice. *Cisco* bezbednosna arhitektura pokazuje kako se modernim alatima, kao što su *Security Cloud Control*, *Universal* ZTNA i *Identity Intelligence*, može obezbediti višeslojna zaštita i inteligentno upravljanje pristupom korporativnoj mreži. Kroz integrisane module i AI podršku, kompanije mogu da pojednostave bezbednosne politike, smanje ljudske greške i brzo reaguju na pretnje. Ukratko, *Cisco* je ponudio bezbednosnu arhitekturu sa svim potrebnim sistemima koja predstavlja most između bezbednog IT okruženja i kontinuiteta poslovanja, čineći mreže otpornijim i korisničko iskustvo jednostavnijim.

comtradedistribution.com

Cisco Secure Wins

Brz oporavak poslovnog sistema i posle najtežih kibernapada

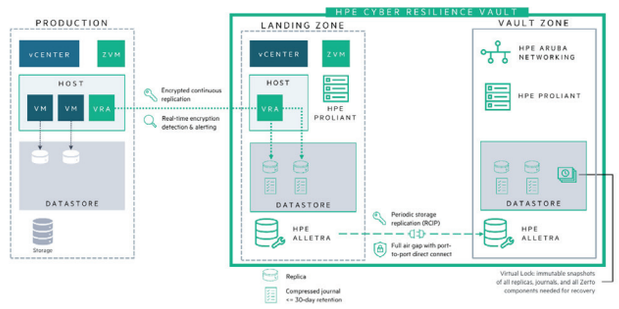
Sve je jasnije da se ransomware i hakerskim napadima jako teško odupreti, stoga treba ozbiljno razmišljati o brzom oporavku posle eventualnog napada. HPE Cyber Resilience Vault omogućava brz oporavak poslovanja uz najviši nivo zaštite podataka

Pretnje od *ransomware* i drugih kibernapada nastavljaju da rastu, kako po učestalosti tako i u tehnikama i sofistikaciji. Napadi postaju sve jeftiniji otkako su se pojavile kriminalne mreže koje nude *ransomware* napade kao uslugu, a uspešne ucene motivišu i finansiraju razvoj sve novijih *malware* programa.

Da bi se nosile u koštac sa ovakvim izazovima, kompanije sve više ulažu u razne tehnologije zaštite, u pokušaju da preduprede upad i umanje načinjenu štetu. Apsolutnu zaštitu je nemoguće garantovati, pa su od jednake važnosti i tehnologije oporavka. To su rešenja koja omogućavaju da se posle napada poslovanje oporavi i nastavi sa ispravnim podacima, makar i s nekim gubitkom vremena.

HPE *Cyber Resilience Vault* nudi najviši nivo zaštite podataka, uz veoma brz oporavak (nizak RTO). Čak i ako je sva oprema u produkcionom računskom centru ispravna, povraćaj velike količine podataka sa *backup* uređaja niskih performansi može produžiti oporavak za više dana ili čak sedmica. Pretraga i utvrđivanje koja verzija *backup*-a nije inficirana dodatno produžava proces.

Ukoliko zakonodavni organi ili interna služba bezbednosti vrše uviđaj na produkcionoj opremi, može biti neophodno da se poslovne aplikacije privremeno izvršavaju na odvojenoj lokaciji – što nije nešto što namenski



HPE Cyber Resilience Vault u potpuno virtualiziranom okruženju

backup uređaji ili arhivski *storage* u *cloud*-u omogućavaju. Imperativ je što pre nastaviti s poslovanjem, što tradicionalna *backup* i arhivska rešenja ne omogućavaju, jer nisu ni dizajnirana s takvim ciljem na umu.

HPE Cyber Resilience Vault

HPE *Cyber Resilience Vault* je rešenje dizajnirano da odgovori ovakvim izazovima, zasnovano na HPE *Alletra storage*-u, HPE *ProLiant* serverima, HPE *Aruba* mreži i HPE *Zerto* softveru. Predstavlja integrisan sistem za zaštitu podataka uz primenu svih najviših standarda zaštite, i s tri osnove:

Replikacija i detekcija – stalna kvazisinhrona replikacija podataka štiti svaki upis u realnom vremenu, istovremeno detektujući bilo kakve anomalije, o kojima obaveštava nadzorni sistem.

ŠTA JE HPE ZERTO?

HPE *Zerto* je softversko rešenje za oporavak od otkaza *(disaster recovery),* uz kontinuiranu zaštitu podataka (CDP). U trenutku kada se pokrene, HPE *Zerto* će iskopirati virtuelnu mašinu na lokaciju koju odredi korisnik. U HPE *Cyber Resilience Vault*-u, to je *Landing* zona. Od trenutka kada se mašina iskopira, HPE *Zerto* će nastaviti da je „prati“ u produkcijskom okruženju i svakih nekoliko sekundi beleži njihove upise u žurnal transakcija.

U žurnalu će ostati zabeležene inkrementalne promene mašine na svakih nekoliko sekundi, a maksimalno u trajanju do 30 dana. To omogućava da u slučaju bilo koje vrste otkaza virtuelne mašine vratimo celu virtuelnu mašinu ili samo pojedinačne fajlove na bilo koje izabrano stanje iz žurnala.

Zerto nudi mogućnost testiranja *disaster recovery* plana. U tom slučaju, HPE *Zerto* će podići virtuelne mašine na lokaciji koju korisnik odredi, uz mogućnost da se to uradi uz promenu mrežnih parametara tih mašina. Ova operacija je izuzetno brza – za virtuelne mašine srednje veličine (stotinak gigabajta) ona traje svega nekoliko desetina sekundi. Upravo po ovoj osobini, softver je i dobio ime: *Zerto* dolazi od *Zero RTO* (*Recovery Time Objective*).

Izolacija i bezbednost – izdvojena *Vault* zona je *offline,* mrežno izdvojena i čuva nepromenljive kopije na bezbednom HPE hardveru visokih performansi.

Testiranje i oporavak – jednostavno identifikujte tačke za oporavak pre infekcije i potom brzo oporavite aplikacije sačinjene od višestrukih VM, čak i u okruženjima sa hiljadama VM.

Kako HPE Cyber Resilience Vault radi?

Landing zona je uparena s produkcionim okruženjem, bazirana na *VMware vSphere* i može predstavljati tradicionalni DR ako je locirana na izdvojenoj lokaciji. Na *Landing* zonu se pomoću HPE *Zerto* softvera kontinuirano i kvazisinhrono repliciraju zaštićene VM s produkcionog okruženja. HPE *Zerto* CDP replikacija nema nikakve agente, tako da ne postoji mogućnost da *malware* zaobiđe ili isključi HPE *Zerto* zaštitu unutar VM. Svaki upis sa štićene VM se kompresuje, enkriptuje i prenosi u *Landing* zonu. Tu se upisuje u CDP žurnal – tekući zapis sa stotinama ili hiljadama *restore* tačaka, s konzistencijom između različitih VM i sačuvanim redosledom upisa *(write-order fidelity)*. Žurnal čuva od jednog sata do 30 dana podataka i predstavlja prvu i najbolju opciju za oporavak kod *ransomware* napada.

Vault zona je fizički kolocirana s *Landing* zonom, fizički izolovana *(Clean room* – čista soba), bez aktivnih mrežnih konekcija *(air-gapped)* i nema pristupa ni Internetu ni produkcionim mrežama. Pošto nema centralne upravljačke ravni, *Vault* zona nema izložene ni *management* portove i nema nijednu tačku kompromisa. HPE *Alletra* u *Landing* zoni i *Vault* zoni koriste direktno povezane IP portove za *Remote copy over IP* (RCIP) replikaciju. Repliciraju se svi podaci iz *Landing* zone, uključujući HPE *Zerto* žurnale i replike. Ovaj pristup kombinuje najbolje aspekte sinhrone replikacije (hiperniski RPO i visoke performanse) i tradicionalne asinhrone replikacije: veća dopuštena latencija, bez uticaja na performanse produkcije, i sa smanjenim zauzećem *storage*-a.

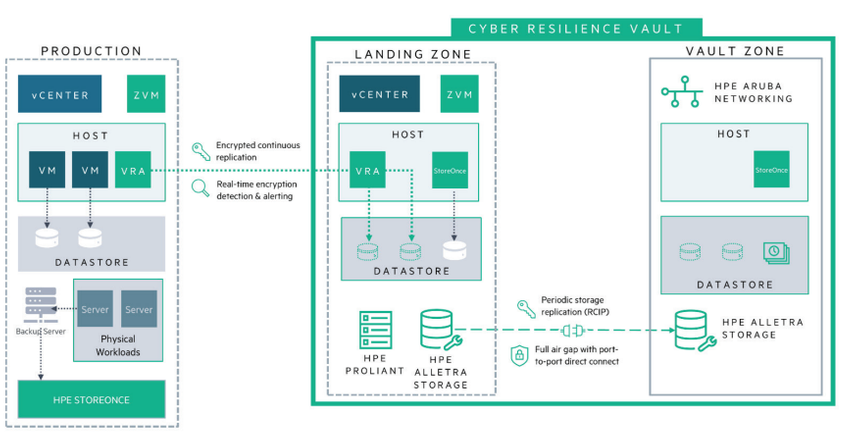
Proces oporavka

Proces oporavka je predviđen za različite scenarije infekcije, uključujući sledeće:

Zaraza pojedinih fajlova / direktorijuma / VM: ako je zona udara *ransomware*-a ograničena na pojedine fajlove i direktorijume unutar VM, pogođeni resursi se mogu gotovo trenutno oporaviti iz HPE *Zerto* žurnala na stanje iz 5-15 sekundi pre infekcije.

Ako je više VM zaraženo, HPE *Zerto* ih može skoro trenutno oporaviti u produkcijsko okruženje bez međukoraka poput *Storage vMotion*-a.

Zaraza celokupne produkcije: ukoliko su sve VM na produkcionoj/primarnoj lokaciji inficirane, ali *Landing* zona nije, kompletan *failover* omogućava da se produkcija restartuje u vremenu merenom minutima.



Zaštita fizičkih servera putem standardnog backup i HPE *StoreOnce*

RPO i RTO?

RPO i RTO su dva osnovna parametra koja opisuju očekivanja za koja je dizajniran sistem zaštite podataka, što je najčešće *backup* sistem.

Recovery Point Objective – RPO je parametar koji procenjuje koliki je najveći gubitak podataka, mereno vremenski. Ukoliko se *backup* nekog sistema vrši svakog dana, onda je njegov RPO 24 časa. Skraćivanje RPO-a se postiže češćim *backup*-om, što obično ima negativan uticaj na performanse produkcionih sistema.

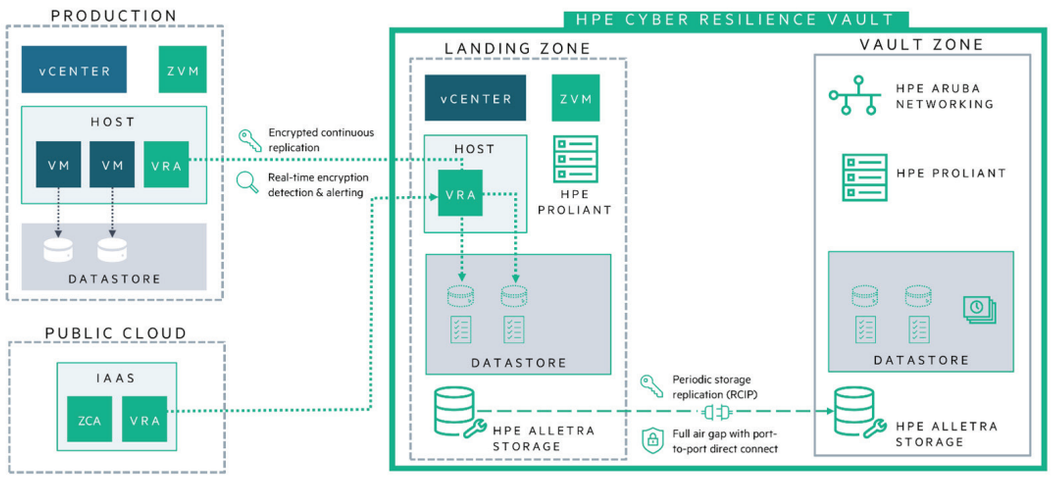
Recovery Time Objective – RTO je parametar koji procenjuje koliko je vremena potrebno da se sistem oporavi iz zaštitnih kopija posle katastrofe. RTO je teško proceniti unapred, jer veoma zavisi od obima nastale štete, performansi sistema na kojima se čuvaju zaštitne kopije, stanja i performansi primarnih *storage*-a i slično. U manje katastrofalnim situacijama, RTO se obično kreće u opsegu od nekoliko sati do nekoliko dana.

Apsolutnu zaštitu od ransomware napada je nemoguće garantovati, pa su veoma važne i tehnologije oporavka, rešenja koja omogućavaju da se poslovanje u najkraćem roku oporavi

HPE *Alletra* je all-NVMe *storage* visokih performansi i visoke pouzdanosti i omogućava da se produkcija na *Landing* zoni izvršava bez gubitka performansi i potrebe za dodatnim sekundarnim *storage*-om.

Zaraza više lokacija: ako se dogodi da su i produkciona i sekundarna lokacija zaražene (recimo, enkriptovani hostovi i brzo širenje infekcije uprkos mrežnoj segmentaciji), HPE *Cyber Resilience Vault* postaje najbezbednija čista soba u kojoj se radi oporavak. Evo kratkog sižea procesa oporavka:

- Ponovo napraviti lokaciju za oporavak: unutar *Vault* zone iskoristiti *immutable snapshot* da bi se oporavili VMFS i sačuvali UUID potpisi resursa.
- Oporaviti HPE *Zerto*: pošto je HPE *Zerto* visoko otporan i automatizovan, virtuelni menadžeri i *data mover*-i će se vratiti *online* i nastaviti rad bez ručne rekonfiguracije ili *setup*-a.
- Oporaviti podatke: koristeći HPE *Zerto* žurnale, odaberite jedan od hiljada dostupnih trenutaka za



Zaštita hibridnog cloud okruženja

oporavak da biste podigli sve VM u proizvoljnom redosledu. Orkestracija koja je deo HPE *Zerto* i visoke performanse HPE *Alletra storage*-a daju RTO u minutima i satima, umesto danima i nedeljama. Aplikacije sastavljene od više VM se brzo oporavljaju iz snimka u istom vremenskom trenutku, minimizujući potrebu za ručnom rekonfiguracijom posle oporavka.

Zaštita kompleksnih okruženja

Premda je zaštita VM pomoću HPE *Zerto* svakako tehnološki najnapredniji aspekt, arhitekte HPE *Cyber Resilience Vault*-a nisu zaboravili ni zaštitu složenih okruženja.

Za okruženja s kritičnim servisima na fizičkim serverima, omogućena je replikacija podataka iz *backup*-a putem HPE *StoreOnce*. Sam softver za *backup* mora da podržava HPE *StoreOnce* kao *backup* uređaj, koji će automatski preneti podatke u virtuelni server u *Landing* zoni.

I tu se fleksibilnost ne završava – postojanje HPE *Zerto Cloud Appliance*-a omogućava zaštitu podataka iz javnog *cloud* okruženja u vašem HPE *Cyber Resilience Vault*-u.

HPE *Zerto Cloud Appliance* je dostupan u većini vodećih javnih *cloud* provajdera, kao što su *Amazon*, *Google*, *Microsoft*, *Oracle* ili IBM.

Ako je zona udara ransomware-a ograničena na pojedine fajlove i direktorijume unutar VM, pogođeni resursi se mogu gotovo trenutno oporaviti iz HPE Zerto žurnala na stanje iz 5-15 sekundi pre infekcije

Projektovan za bezbednost i performanse

HPE *Cyber Resilience Vault* u sebi objedinjuje vrhunsku bezbednost i najviše performanse, ispunjavajući i najstrože standarde, nudeći:

- potpuni *air gap* sa izolovanim *Vault*-om,

ALI JA IMAM OPREMU RAZLIČITIH PROIZVOĐAČA!

HPE *Zerto* je potpuno nezavisan od hardvera na kome se izvršava. Najvažniji zahtevi su da je štićeno okruženje virtualizirano, i da je virtuelizacija izvršena na jednoj od podržanih platformi: *VMware vSphere* ili *HyperV*.

Uskoro će se ovoj listi virtuelizacionih platformi pridružiti i HPE *Morpheus VM Essentials* – najnovija alternativa na tržištu. Fizički (ne-virtuelizovani) serveri se mogu štititi pomoću HPE *StoreOnce* koji replicira standardne *backup*-e podataka.

Uz HPE Cyber Resilience Vault sada je dostupno rešenje najviše bezbednosti i performansi, koje će se suprotstaviti pretnji ransomware-a

- *Zero Trust* arhitekturu,
- ojačane aplikativne VM bazirane na *Linux*-u,
- decentralizovano upravljanje bez jedinstvene tačke za kompromitaciju,
- nepromenljive *offsite* i *offline* kopije podataka,
- zaštićeni *Tamper-proof* NTP,
- detekciju enkripcije podataka u realnom vremenu,
- proširivost na 10.000+ VM po vCentru,
- All-NVMe *storage* najnovije generacije za privremeno izvršavanje bilo koje aplikacije pri oporavku,
- *storage* sa garancijom 100% dostupnosti u *Landing* zoni,
- sav hardver zaštićen *Silicon Root Of Trust* bezbednosnim procesorima.

Stvarna kiberotpornost

Uz HPE *Cyber Resilience Vault* sada je dostupno rešenje najviše bezbednosti i performansi da se suprotstavi pretnji *ransomware*-a. Jedinstvena decentralizovana arhitektura HPE *Zerto* omogućava brz oporavak u *air-gap* okruženju čak i posle najtežih napada.

- Drastično smanjen *downtime* nakon napada.
- Izbegava se direktan ili indirektan gubitak prihoda.
- Pomaže pri dostizanju regulatornih zahteva poput HIPAA, DORA, GDPR, SOX, ili FISMA/NIST SP 800-34.

Sva kompleksnost sakrivena iza jedinstvenog rešenja od jednog vendora i s najboljim proizvodima u svakom koraku oporavka posle kibernapada.

Za upite u vezi sa HPE rešenjima za *disaster recovery* i *ransomware* zaštitu obratite se našem lokalnom stručnjaku Milanu Avramoviću na *m.avramovic@selectium.com*.

hpe.com

Čovek i AI: partnerstvo za sigurniju budućnost

Na prvi pogled, mejl je izgledao bezazleno: standardni dopis s logotipom partnera i priloženim dokumentom

Zaposleni ga otvara rutinski, kao što je uradio stotinu puta ranije. Samo nekoliko minuta kasnije, mreža je već kompromitovana - u pozadini se nevidljivo širi malver, brišući granicu između obavljanja svakodnevnog zadatka i katastrofe.

Tada počinje prava trka s vremenom: svaki naredni minut odlučuje da li će podaci ostati zaštićeni ili će završiti na crnom tržištu. Brzina je presudna. To potvrđuje i statistika, s obzirom na to da se u skoro polovini slučajeva eksfiltracija podataka dogodi brže od jednog dana, a u petini njih i za manje od jednog sata. To znači da organizacija koja nema plan odgovora na incidente praktično sama sebi uskraćuje šansu za opstanak.

Ovo iskustvo nije izmišljeno, već jedan od scenarija s kojim se *Incident Response* timovi sve češće suočavaju. Šta raditi kada vas ugrozi ovakva greška? Upravo o tome će se govoriti na predavanju „Moć brze reakcije“ koje će na konferenciji *Pulse360*, posvećenoj sajberbezbednosti, održati Jovan Milosavljević, *Delivery Lead* kompanije PULSEC.

„Prema našem iskustvu, napadi postaju sve sofisticiraniji, a ako se sajbernapad i dogodi - nema mesta panici i reakcija mora biti brza i odlučna. Naš tim imao je priliku da učestvuje u neutralisanju brojnih napada, u ublažavanju njihovih posledica i oporavku sistema - stičući tako iskustvo koje nam omogućuje da brzo i adekvatno reagujemo“, ističe Milosavljević.

Odgovor na incidente samo je jedna od tema koju će pokrenuti *Pulse360*.

Konferencija će se održati 9. oktobra u *Sava centru*, a u njenom fokusu biće uticaj veštačke inteligencije na oblast sajberbezbednosti. Učesnici konferencije će, u skladu sa ovogodišnjim sloganom konferencije - *AI & Security Puzzle*, razgovarati o tome kako se AI i ljudska ekspertiza uklapaju u jednu kompleksnu, ali nužnu celinu.

Posetioci konferencije saznaće i na koji način AI menja lice OT bezbednosti i koliko nas oslanjanje na automatizaciju s jedne strane osnažuje, a s druge ostavlja ranjivijima. Biće pokrenut i novi format „sajberdijalog“ tokom koga ćemo razgovarati o uticaju veštačke inteligencije na organizaciju i servise bezbednosno-operativnih centara. Među istaknutim temama je i pitanje upravljanja identitetima: kako pomoću veštačke inteligencije prepoznati ko zaista treba da ima određena prava, kako otkriti privilegije koje više nisu u upotrebi i kako zaštititi organizaciju od unutrašnjih rizika.

Sve ove priče spajaju se u jednu zajedničku poruku: sajberbezbednost danas nije pitanje „da li ćete se susresti sa bezbednosnim izazovima“, već „kako se za njih pripremiti, kako biti proaktivan i kako iskoristiti i znanje eksperata i mogućnosti veštačke inteligencije“. *Pulse360* upravo zato nije samo prilika da se čuju zanimljiva predavanja već i da se iz prve ruke doživi kako izgleda kada tehnologija i ljudi zajedno odgovaraju na najveće izazove digitalnog doba.

Pulse360 je prilika da se iz prve ruke doživi zajednički odgovor ljudi i tehnologije na najveće izazove digitalnog doba

Da podsetimo, konferenciju *Pulse360* organizuje kompanija PULSEC, regionalni lider u oblasti sajberbezbednosti i strateški partner *Telekom Srbija Grupe*, dok se među partnerima konferencije nalaze: *Co.Next, Exclusive Networks, Clico, Ingram Micro, Trend Micro, Check Point, CyberArk, Palo Alto Networks*, F5, *Thales, Symantec, Huawei, Proofpoint, Tenable, Verimatrix, Hive, Reputeo* i poslovna mreža RU4M? koja je ujedno i zvanična aplikacija konferencije.

Konferencija je otvorena za IT menadžere, inženjere, analitičare, kao i poslovne korisnike zainteresovane za najnovije trendove u digitalnoj bezbednosti. Učešće je besplatno, uz prethodnu prijavu na sajtu kompanije.

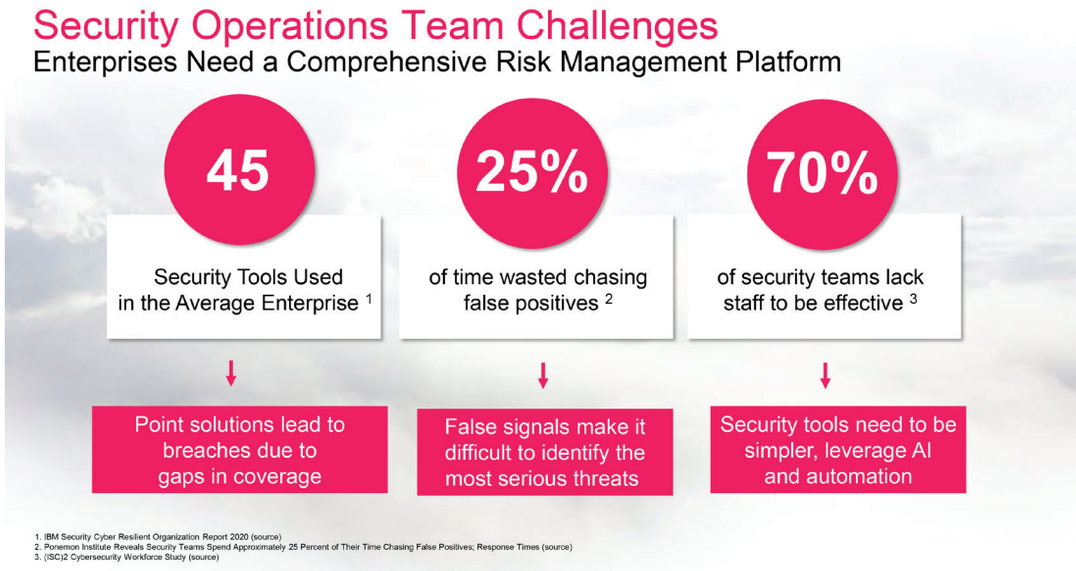
pulsec.com

PULSEC je regionalni lider u oblasti sajberbezbednosti, sa centrima u Srbiji, BiH i Švajcarskoj. PULSEC pruža kompletan spektar usluga sajberbezbednosti, uključujući kontinuirani 24/7 SOC nadzor, napredna penetraciona testiranja, detekciju pretnji zasnovanu na veštačkoj inteligenciji, sveobuhvatnu podršku za usklađenost sa bezbednosnim propisima, specijalizovane usluge *Incident Response*-a, kao i *Security Awareness* obuke krajnjih korisnika.

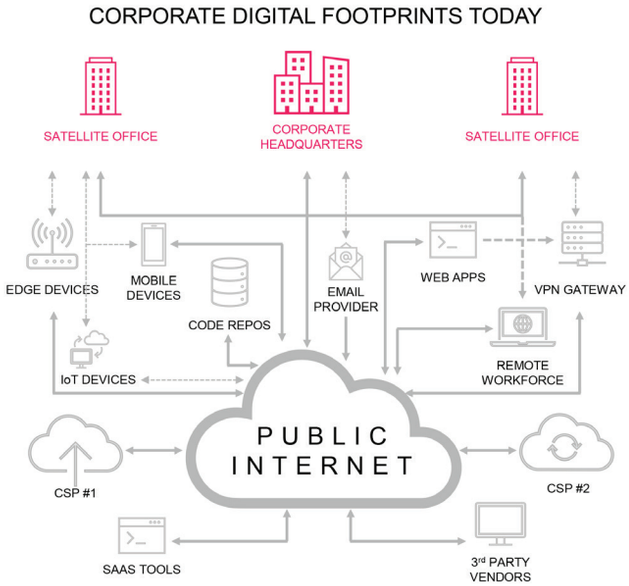
Inteligencija koja pravi razliku: Check Point Infinity ERM

U svetu u kojem se granica između poslovnih i tehničkih rizika gotovo potpuno izgubila, pitanje sajber bezbednosti više nije u nadležnosti samo IT odeljenja. Danas je to strateški izazov svake kompanije, direktno vezan za reputaciju, poverenje korisnika i finansijsku stabilnost. Upravo iz tog razloga Check Point je razvio Infinity External Risk Management (ERM) – objedinjeno rešenje za praćenje, otkrivanje i ublažavanje eksternih sajber pretnji.

Nekada se pod površinom napada podrazumevao relativno mali broj spoljnih sistema – veb serveri, mejl servisi, javne aplikacije. Međutim, digitalna transformacija i migracija u oblak značajno su proširili tu sliku. Danas napadači tragaju za slabostima ne samo u javnim servisima, već i u repozitorijumima izvornog koda, društvenim mrežama, partnerskim sistemima, pa čak i u raznim privatnim komunikacionim kanalima.



Ova proširena površina napada podrazumeva desetine potencijalnih ulaza u mrežu jedne organizacije – od kompromitovanih lozinki i fišing sajtova do lažnih profila na društvenim mrežama. Upravo tu na scenu stupa Infinity ERM, nudeći kontinuirano praćenje i pravovremenu reakciju.



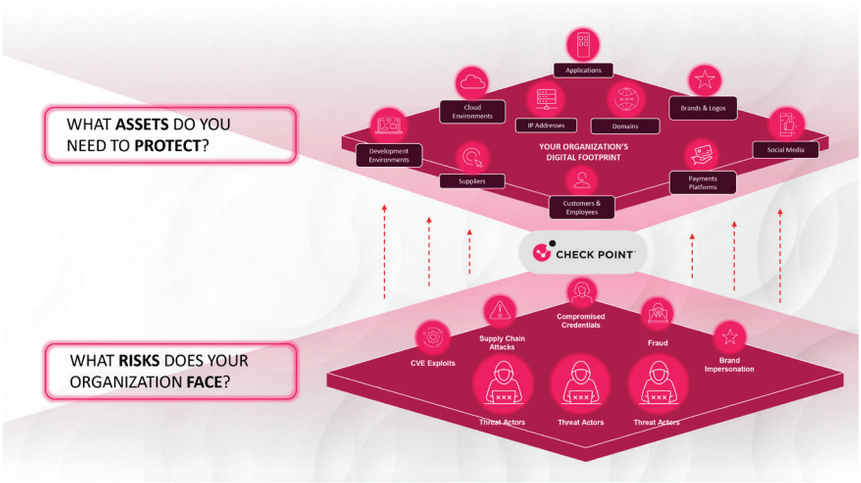
Jedinstvena platforma

Infinity ERM nije samo još jedan alat u nizu specijalizovanih servisa. Radi se o objedinjenoj SaaS platformi, koja povezuje više ključnih funkcionalnosti:

- Praćenje spoljne površine napada i otkrivanje ranjivosti.
- Monitoring *deep & dark Web*-a, uključujući forume i *chat* grupe gde se planiraju napadi.
- Zaštitu brenda i domena od imitacija, fišing kampanja i lažnih aplikacija.
- Upravljanje rizicima trećih strana, uključujući dobavljače i partnere.
- Integrisano obaveštavanje i izveštavanje, sa mogućnošću povezivanja sa postojećim bezbednosnim sistemima i SIEM alatima.

Sve to može da se pokrene veoma brzo – za nekoliko minuta vide se prvi rezultati.

> **Danas napadači tragaju za slabostima ne samo u javnim servisima, već i u repozitorijumima izvornog koda, društvenim mrežama, partnerskim sistemima, pa čak i u privatnim komunikacionim kanalima**



Deep and Dark Web kao izvor informacija

Jedan od najsnažnijih aduta Infinity ERM-a je sposobnost da dopre do mesta gde se najčešće kriju pretnje – duboki i mračni Web. Reč je o zatvorenim forumima, kripto-marketima i šifrovanim komunikacionim kanalima u kojima kriminalne grupe razmenjuju podatke i planiraju napade.

Check Point automatizuje proces infiltracije u te zajednice i beleži više od 55 miliona obaveštajnih stavki mesečno, uključujući kompromitovane akreditive, ukradene kreditne kartice i malver logove. Na taj način organizacije mogu da reaguju još u ranoj fazi, pre nego što incident eskalira.

Konkretne koristi:

- Detekcija kompromitovanih lozinki i poverljivih podataka.
- Brza identifikacija malvera na korporativnim uređajima.
- Praćenje kada su brendovi, proizvodi ili domeni pomenuti u hakerskim grupama.
- Ciljana upozorenja koja pomažu bezbednosnim timovima da se fokusiraju na ono što je zaista važno.

Ljudski faktor i stručna podrška

Pored tehnologije, važan deo rešenja je i globalni tim stručnjaka koji rade rame uz rame sa korisnicima. *Check Point* analitičari nude:

- Trijažu i pravovremena upozorenja, kako bi se izdvojile prave pretnje.
- Posebna istraživanja i analize prema potrebama organizacije.
- Servise uklanjanja lažnih sadržaja, sa stopom uspeha od čak 96% u gašenju fišing sajtova i lažnih profila.

Za male timove to znači ogromnu uštedu resursa – u praksi, *Check Point* analitičari postaju produžena ruka internih bezbednosnih odeljenja.

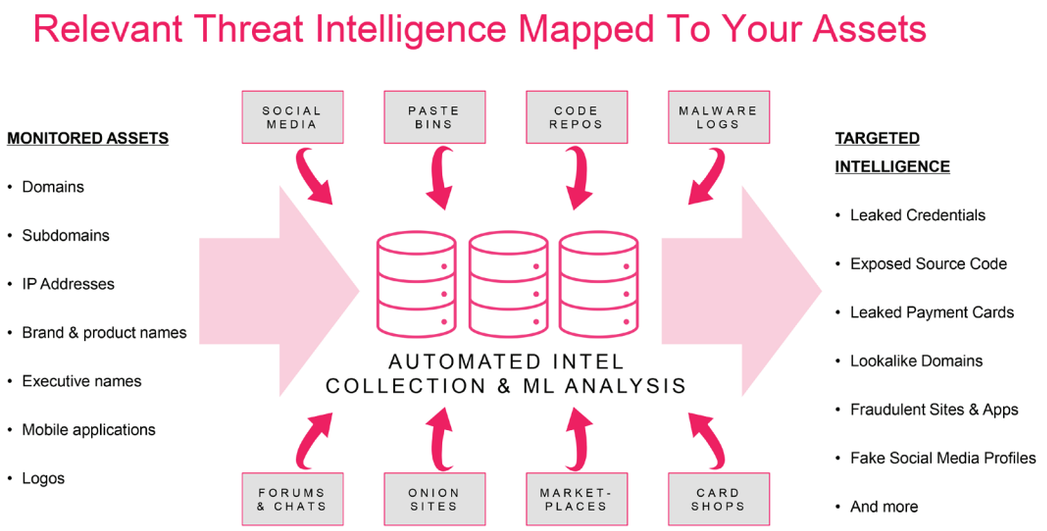
Adut Infinity ERM-a je sposobnost da dopre do mesta gde se najčešće kriju pretnje – duboki i mračni Web. Reč je o zatvorenim forumima, kripto-marketima i šifrovanim komunikacionim kanalima u kojima kriminalne grupe razmenjuju podatke i planiraju napade

Dokazana vrednost

Statistika jasno pokazuje značaj *Infinity* ERM-a:

- 92% svih upozorenja odnosi se na stvarne i relevantne pretnje.
- Više od 55 miliona obaveštajnih unosa mesečno omogućava široku pokrivenost.
- 96% uspeha u uklanjanju malicioznih sadržaja tokom poslednjih deset kvartala.

Zahvaljujući ovim rezultatima, rešenje je prepoznato od strane analitičkih kuća i lidera industrije. Među korisnicima su globalne kompanije koje se oslanjaju na brzu detekciju, istraživanje i neutralizaciju pretnji.



Zaključak

U vremenu kada sajber napadi postaju sofisticiraniji, a poslovni modeli sve zavisniji od digitalne infrastrukture, kompanije ne mogu sebi da priušte čekanje da incident nastupi. Potrebna je proaktivna strategija – a *Infinity External Risk Management* predstavlja upravo to: inteligentnu, objedinjenu i isplativu platformu koja spaja automatizovanu tehnologiju i ljudsku ekspertizu.

Na kraju, kako kaže jedan od korisnika: *"Check Point* nije samo još jedno EASM rešenje – donosi vrednost sa visoko relevantnom inteligencijom iz dubokog i mračnog *Web*-a." Upravo ta kombinacija dubine uvida, brzine reakcije i stručne podrške čini *Infinity* ERM alatom koji menja pravila igre u oblasti sajber bezbednosti.

checkpoint.com

Cisco ponovo osvaja tržište firewall uređaja

Cisco donosi novu generaciju uređaja – Cisco Secure Firewall, CSF200 i CSF1200 – osmišljene da odgovore na savremene izazove mrežne zaštite. U tekstu koji sledi upoznaćemo njihove glavne adute i mogućnost da i oni, poput svojih prethodnika, steknu kultni status među firewall rešenjima

Nikola Milovanović, Technical Presales Architect, Comtrade Distribution

Sećate li se vremena kada se reč *firewall* najčešće prevodila u jednu oznaku – PIX? A zatim je ASA nastavila da nosi taj status i dugo bila najpoznatije ime u *Cisco* porodici bezbednosnih rešenja. Sada, u 2025. godini, *Cisco* donosi novu generaciju uređaja – **Cisco Secure Firewall**, CSF200 i CSF1200 – osmišljene da odgovore na savremene izazove mrežne zaštite.

Prva barijera

Definicija kaže da je *firewall* uređaj temelj mrežne bezbednosti i prva barijera protiv sajbernapada na mrežnu i IT infrastrukturu kompanija. Njegova uloga je da pregleda mrežni saobraćaj i blokira zlonamerne sadržaje ili pokušaje neovlašćenog pristupa, čuvajući time podatke i IT sisteme. Današnja rešenja, poznata kao *Next-Generation FireWall* (NGFW), idu korak dalje – otkrivaju upade, analiziraju aplikacije i u realnom vremenu reaguju na napredne pretnje. Na taj način organizacije dobijaju mnogo jači štit protiv sve sofisticiranijih napada. Može li *Cisco* da ponudi više od navedenog?

U vremenu kada kompanije ubrzavaju digitalizaciju svog poslovanja i prilagođavaju se zahtevima veštačke inteligencije, tradicionalni sistemi zaštite više nisu dovoljni. *Cisco* sa svojim inovativnim **Hybrid Mesh Firewall** pristupom donosi bezbednost koja se pruža kroz svaki deo mreže – od *data* centra i *cloud*-a, do IoT uređaja i udaljenih lokacija kompanija. Oslanjajući se na veštačku inteligenciju (AI) i mašinsko učenje (ML), **Cisco Secure Firewall** omogućava pametnije otkrivanje i zaustavljanje pretnji, dok istovremeno pojednostavljuje svakodnevno upravljanje *firewall* uređajem. Na taj način korisnici dobijaju rešenje koje spaja modernizaciju i bezbednost, pružajući pouzdan oslonac u digitalnom poslovanju.

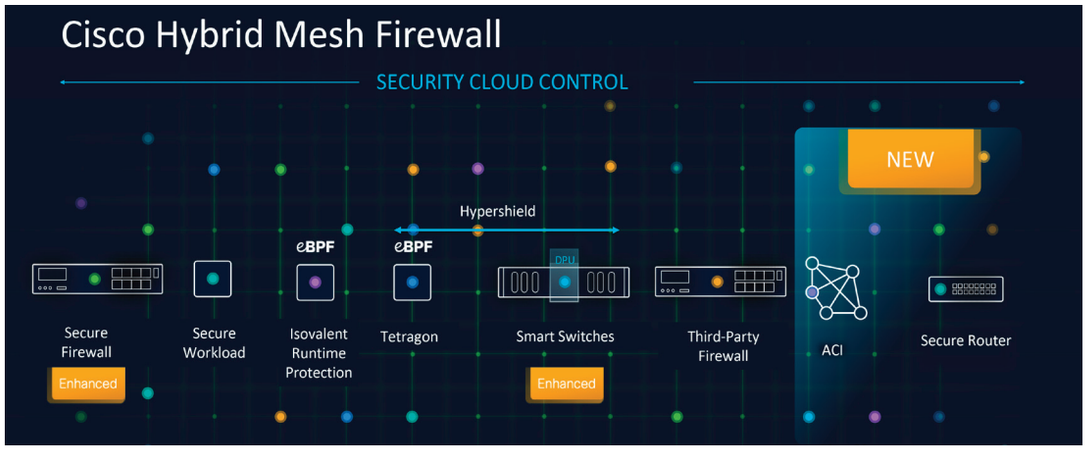
Napredni AI/ML mehanizmi omogućavaju firewall uređajima da uče iz globalnih bezbednosnih događaja i reaguju na nove vrste napada u realnom vremenu

Pre nego što predstavimo serije *Cisco Secure Firewall* uređaja – CSF200 i CSF1200 – važno je osvrnuti se na to kako veštačka inteligencija i mašinsko učenje menjaju način na koji funkcioniše mrežna bezbednost. Napredni AI/ML mehanizmi omogućavaju *firewall* uređajima da aktivno uče iz globalnih bezbednosnih događaja i reaguju na nove vrste napada u realnom vremenu. *Cisco* na ovom polju ima snažan oslonac kroz *Cisco* **Talos** tim, koji dnevno analizira čak 900 milijardi bezbednosnih događaja, pretvarajući te podatke u efikasne zaštitne servise. Uz to, ugrađeni agent **Cisco AI Assistant** pomaže administratorima oko konfiguracije, primene preporučenih procedura iz prakse i automatizacije radnih procesa, dok set funkcionalnosti na bazi veštačke inteligencije **AIOps** pojednostavljuje upravljanje *firewall*-ovima i ubrzava reakciju na bezbednosne pretnje.

Poseban značaj ima i **Encrypted Visibility Engine (EVE)**, koji koristi AI/ML da prepozna i blokira mali-

ciozne aktivnosti čak i u šifrovanom saobraćaju, bez potrebe za njegovim dešifrovanjem. Na kraju, tu je i **Snort ML**, tehnologija koja analizira mrežni saobraćaj u realnom vremenu i otkriva nove, *zero-day* ranjivosti, čime se organizacijama pruža dodatni nivo sigurnosti.

Sve ove inovacije čine osnovu na kojoj su izgrađene nove serije *Cisco Secure Firewall* uređaja – CSF200 i CSF1200 – spremne da odgovore na izazove digitalnog doba i pruže korisnicima pouzdanu zaštitu zasnovanu na veštačkoj inteligenciji. Pored svega toga, *Cisco Secure Firewall* uređaji donose odličan odnos cene i performansi.



Za centralne lokacije

Cisco Secure Firewall 1200 serija namenjena je za centralne lokacije kompanija manje i srednje veličine i obuhvata šest modela uređaja – od CSF1210CE do CSF1250 – koji pružaju potpune *firewall* servise uz performanse od 6 Gb/s do 18 Gb/s. Zahvaljujući podršci za širok spektar interfejsa (1G, 2.5G i 10G, u RJ-45 ili SFP+ varijanti), ovi modeli se lako uklapaju u različite mrežne topologije i omogućavaju pouzdano povezivanje s korporativnim ili javnim Internet okruženjem.

Cisco Secure Firewall 200 serija predstavlja više bezbednosnih uređaja namenjenih povezivanju i zaštiti distribuiranih kompanija, tako da ni udaljene poslovnice više nisu slaba karika u bezbednosnom lancu. Ona proširuje primenu *Cisco* bezbednosne politike i inspekcije pretnji na korisnike i uređaje u poslovnicama i manjim lokacijama.

CSF200 je najmlađi član porodice *Cisco Secure Firewall*, ali donosi napredne NGFW funkcionalnosti kombinovane sa **SD-WAN** tehnologijom (softverski definisan WAN). Prvi model iz ove serije koji će biti dostupan na tržištu je **CSF220**, najavljen za decembar 2025. godine. Sa *firewall* performansama od 1 Gb/s, CSF220 postavlja temelj za veće modele ove serije, otvarajući put ka proširenju i skalabilnoj zaštiti mreže.

CSF *firewall* uređaji podržavaju i jednostavnije upravljanje mrežnom bezbednošću centralizovano kroz sistem **Cisco Security Cloud Control**, tako da se može primeniti jedinstvena politika zaštite kroz sve delove mreže – od poslovnica i kampusa, preko *data* centara, pa sve do *cloud* servisa. Uz *Cisco Security Cloud Control*, kompanije dobijaju uvid u mrežne bezbednosne aspekte u realnom vremenu, pojednostavljene radne procese i unapređenu zaštitu zahvaljujući centralizovanom upravljanju i AI analizama podataka sa svih *Cisco* bezbednosnih uređaja. Na taj način administratorima je olakšano donošenje odluka i brža reakcija na pretnje.

Za upravljanje CSF *firewall* uređajima dostupni su i tradicionalni načini upravljanja – ugrađeni menadžment klijent na samom *firewall*-u (FDM) i namenski centralni menadžment uređaj (fizički i virtuelni) u mreži korisnika (FMC).

Ako su PIX i ASA nekada važili za legende mrežne bezbednosti, CSF200 i CSF1200 deluju kao njihovi moderni naslednici spremni za digitalno doba

Za kompanije koje ne žele da prave kompromis po pitanju dostupnosti Internet servisa ili distribuirane korporativne mreže, CSF *firewall* uređaji podržavaju rad u konfiguraciji visoke dostupnosti (model *active-standby*).

U Cisco okruženju

Korišćenje **Cisco CSF firewall uređaja** donosi brojne prednosti, posebno u okruženjima koja već koriste *Cisco* mrežnu infrastrukturu, jer omogućava jednostavnu integraciju i koordinaciju svih komponenti. *Cisco* je globalno priznat brend u oblasti mrežnih rešenja i sajberbezbednosti, sa širokom bazom sertifikovanih stručnjaka koji olakšavaju implementaciju i podršku. *Cisco* se svojim modelima serija 3100 (*firewall* performanse od 10 Gb/s do 45 Gb/s) i 4200 (*firewall* performanse od 65 Gb/s do 140 Gb/s) već ranije pobrinuo za kompanije koje imaju velike zahteve po pitanju performansi mrežnog saobraćaja (kao što su *data* centri, provajderi Internet servisa i velike korporacije). Za kompanije koje imaju najveće zahteve, *Cisco* je najavio model CSF6100 (do 400 Gb/s *firewall* performanse).

Ako su PIX i ASA nekada važili za legende mrežne bezbednosti, CSF200 i CSF1200 deluju kao njihovi moderni naslednici spremni za digitalno doba. Uz balans između performansi, jednostavnog upravljanja i naprednih sigurnosnih funkcija, oni ne donose samo zaštitu već i mirniji san administratorima koji znaju da će mreža funkcionisati bezbedno i pouzdano.

comtradedistribution.com.

InSight softver u praksi

InSight softver mogao bi se uporediti s rendgenom, samo za nadzor Internet mreže, ili pak s termovizijskim kamerama. U oba slučaja, akcenat je upravo na otkrivanju elemenata i događaja koji su inače potpuno nevidljivi. Ovi nevidljivi mrežni podaci do sada su promicali usled nepostojanja adekvatnog alata za njihovu identifikaciju, analizu, ekstrapolaciju i vizuelizaciju

Lena Perović, founder and CGO at Developico

InSight je softversko rešenje za telemetriju IKT mreža, bazirano na *sFlow* podacima, a firma *Serbian Open eXchange* (SOX), kao kritična IKT infrastruktura Republike Srbije, kontinuirano ulaže napore u prevenciju bezbednosnih pretnji, smetnji i otkaza i kao takva bila je idealna za ulogu saveznika u razvoju i prvog testera.

Rendgen ili FLIR – termovizijska kamera

Korišćenjem *InSight* alata u potpunosti je promenjen način na koji je SOX posmatrao Internet saobraćaj. Na osnovu neprocenjivih *sFlow* informacija o količini i raspodeli Internet saobraćaja, iz korena je promenjen celokupan dizajn SOX mreže uz direktan i ključan uticaj na bezbednost i skalabilnost.

Ušavši još dalje u svet telemetrije, otvorila su se nova polja za istraživanje, a sve bez narušavanja privatnosti, s obzirom na to da se pristupa analizi metapodataka iz zaglavlja IP paketa i *Ethernet frame*-ova.

Mi pak najradije pravimo analogiju između rezultata koje daje *InSight* softver i rezultata analize krvi. Poput rezultata analize krvi, na osnovu uzorkovanja mrežnih podataka iz *InSight* softvera, dolazimo do jasnih indikacija o zdravlju mreže, zajedno sa uputom šta da pregledamo ili testiramo sledeće.

Slika 1. Početni ekran Internet Security modula softvera InSight

Kao i u slučaju opšteg zdravstvenog stanja, i za analizu uzorkovanih mrežnih podataka potreban je ekspert i njegovo stručno mišljenje. Upravo zato u alat smo integrisali svoje znanje i iskustvo u oblasti mreže, uz dodatak ML/AI (mašinskog učenja i veštačke inteligencije), dodajući podacima značenje, svrhu i prošlost. Sveobuhvatan pregled i analiza podataka koju smo ovim putem postigli, van domašaja je svakog pojedinca, koliko god iskusnog u ovoj oblasti. Upravo zato je upotreba ML/AI bila pravo rešenje.

Korišćenjem InSight alata u potpunosti je promenjen način na koji je SOX posmatrao Internet saobraćaj. Na osnovu neprocenjivih sFlow informacija o količini i raspodeli Internet saobraćaja, iz korena je promenjen celokupan dizajn SOX mreže uz direktan i ključan uticaj na bezbednost i skalabilnost

Širom otvorenih očiju

U današnje doba jasno je da u Internet mreži makar i treptaj oka može dovesti do previda neke *cyber* pretnje, pokušaja prodora ili krađe podataka. Ono što je tom prilikom svakako ukradeno, jeste naš mir.

Korišćenjem *InSight* alata, postiže se:

- osećaj sigurnosti i kontrole,
- produbljivanje znanja o sopstvenoj Internet mreži,
- razumevanje normalnih i bezbednih *pattern*-a saobraćaja,
- bezbednost ključnih elemenata sistema,
- dodatna tačnost zbog korišćenja ML/AI i manji *false positive i*
- optimizacija i jednostavnost planiranja budućeg širenja mreže.

U daljem tekstu predstavili smo dva primera upotrebe *InSight* alata. Prvi

primer je nešto jednostavniji, ali veoma izražen u svakodnevnom radu SOC/NOC timova – napad velikom količinom saobraćaja s različitih polaznih adresa – DDoS. Drugi primer je studija slučaja na primeru našeg partnera i korisnika, firme SOX, koja ukazuje na vrednosti analitike i na veoma konkretne korake i rezultate koji su iz korišćenja *InSight* softvera proistekli.

Primer 1: Detekcija i rešavanje DDoS napada u mreži ISP

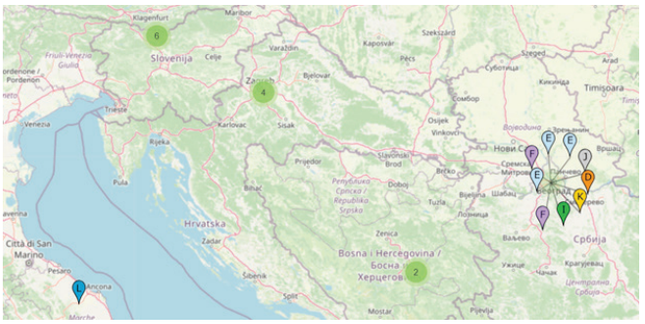
U mreži jednog od korisnika *InSight* softvera došlo je do DDoS napada. Iako je mreža bila zaštićena raznim sistemima za detekciju i prevenciju napada (IDS/IPS), kako od natprovajdera, tako i unutar same mreže, DDoS napad „se provukao" i preopteretio linkove i centralne procesore. Pristup mreži i mogućnost konfigurisanja bili su izuzetno ograničeni, a administratori bez alata kojima bi mogli da analiziraju izvor problema.

InSight u SaaS opciji rešio je problem kroz iterativni postupak i omogućio brzu i konkretnu reakciju administratorima na rešavanju problema.

- *InSight* Saas instanca se *host*-uje van mreže ISP, pa samim tim nije bila ugrožena DDoS napadom.
- Na prvoj strani modula za *Internet Security* softvera *InSight*, vidi se značajan porast broja alarma, s jasnom vremenskom korelacijom.
- Na prikazu aktivnih alarma se lako mogu uočiti MAC adrese s najvećim dolaznim saobraćajem, kao i značajna promena u raspodeli *destination* ASN-ova.

Korelacija MAC adrese sa AS brojem ugrožene mreže dovela je do identifikacije mreže ugroženog korisnika, za kojeg se ispostavilo da je novi korisnik u mreži ISP, bez istorije ponašanja i bez sumnje da bi mogao biti predmet DDoS napada. *InSight* alat je, među ostalim podacima, istakao i oznaku uređaja i porta i omogućio administratorima brzu reakciju.

InSight softver je bio tajni sastojak uspeha SOX-a u prethodnih 15 godina postojanja, koji je sada dostupan i drugima



Slika 2. Broj root-DNS servera u SEE

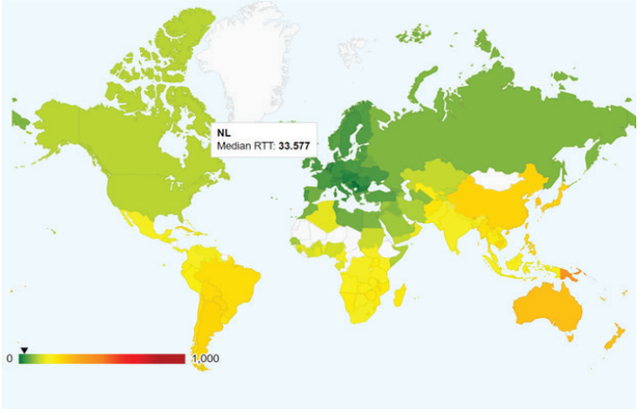
Odmah po identifikaciji pokrenuta je akcija čišćenja saobraćaja od DDoS napada, kako kod natprovajdera, koji su sada imali detalje napada i mogli da sprovedu brze akcije, tako i aktiviranje *blackholing*-a i *remote blackholing*-a kroz partnerske mreže.

Urađena je *root-cause* analiza i digitalna forenzika od ISP-a, ali i *InSight* tima kako bi se ovakve situacije izbegle u budućnosti, a najbolje prakse su ugrađene u sam *InSight* alat.

Primer 2: InSight analitika u službi unapređenja bezbednosti, kvaliteta i stabilnosti srpskog Interneta

SOX, nacionalna tačka za razmenu Internet saobraćaja i kritična infrastruktura po mnogim kriterijumima, već godinama je zadovoljni korisnik *InSight* alata u tri scenarija:

- *SOC/Security* – praćenje naglih promena i korelacija, kao i iskakanje iz parametara sezonalnosti i raspodele saobraćaja u vremenu.

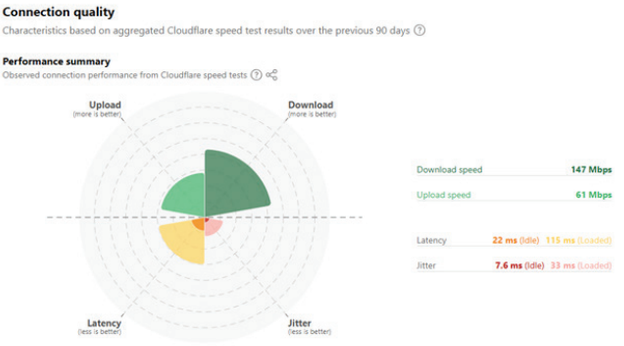


Slika 3. RTT kašnjenje iz Srbije

Korišćenjem sva tri raspoloživa InSight programska modula (BI/NOC/SOC), SOX je postigao rezultate vidljive na celom IKT tržištu Srbije

- BI/Poslovna analitika – s kojom mrežom se povezati, kada, gde i zašto?
- NOC/Bezbednost i kontinuitet poslovanja – praćenje zauzetosti kapaciteta mreže, izbegavanje uskih grla i proaktivno ugovaranje kapaciteta za koje je po pravilu potrebno tri do šest meseci, pa je pravovremena reakcija neophodna.

InSight analitika ugrađena je u samu arhitekturu SOX mreže, ali i u operativne i bezbednosne procedure u nadzoru i upravljanju SOX mrežom i SOX uslugama.



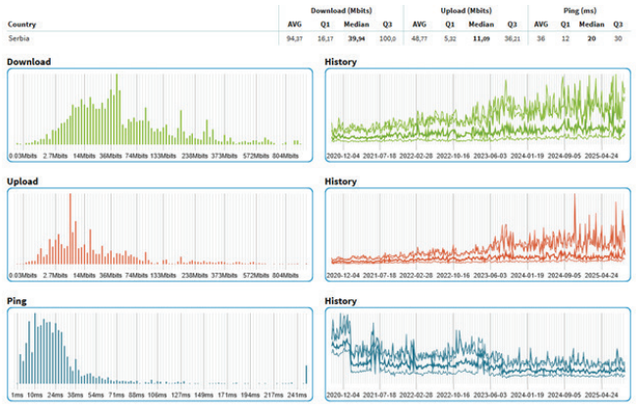
Slika 4. Kvalitet Interneta u Srbiji

Korišćenjem sva tri raspoloživa *InSight* programska modula (BI/NOC/SOC), SOX je postigao rezultate vidljive na celom IKT tržištu Srbije:

- Prepoznata je važnost bezbednog i brzog pristupa javnim DNS *resolver*-ima i uspostavljena je najdirektnija moguća saradnja sa 1.1.1.1, 9.9.9.9, 8.8.8.8, a što se može proveriti sa *lg.sox.rs*.
- Prepoznata je potreba za bezbednim, direktnim vezama 100G kapaciteta s najvećim svetskim CDN (*Content Delivery Networks*), kao što su *Google*, *Akamai*, *ByteDance*, *Meta*, M247, CDN77, *Valve* (*Steam*), *Hetzner*, *Netflix* i drugima. Veze su realizovane u prethodnom periodu.
- Prepoznata je potreba za širom regionalnom saradnjom s drugim operaterima mreža za razmenu Internet saobraćaja iz Austrije, Češke, Mađarske, Rumunije,

Bugarske, Severne Makedonije, Ukrajine, Poljske, što je donelo bezbedniju komunikaciju visokih performansi. Veze su realizovane u prethodnom periodu.

- Prepoznata je potreba za zaštitom od DDoS napada s javnog Interneta i uspostavljena je saradnja s globalnim *cloud* provajderom DDoS zaštite *Voxility* pre više od sedam godina.
- Prepoznata je potreba za dovođenjem *root-DNS* servera u Srbiju, što je povećalo brzinu otvaranja sajtova za sve korisnike u Srbiji, povećalo je otpornost na kratke i duže prekide međunarodnih linkova i postavilo Srbiju na mapu *root-servers.org*.
- Prepoznata je potreba za konstantnim praćenjem kvaliteta Interneta u Srbiji kroz uvođenje 10+ sistema za merenje kvaliteta Interneta *testmyspeed.sox.rs*.
- Prepoznata je potreba za *host*-ovanjem lokalnih *Linux* repozitorijuma i napravljena najveća *mirror Linux* distribucija u ovom delu SEE *regiona mirror1.sox.rs*.



Slika 5. Trenutna raspodela brzine Interneta + Trend poboljšanja kvaliteta Interneta u Srbiji

- Prepoznata je potreba za praćenjem kvaliteta globalne vidljivosti SOX mreže iz sveta i uspostavljena saradnja s: *ris.ripe.net/peerlist/all.shtml, www.routeviews.org/routeviews/collectors/, www.caida.org/projects/ark/statistics/monitor/beg-rs/map_rtts.html,* a natprovajderi su testirani i menjani na osnovu kvaliteta, raspoloživosti i bezbednosti usluge i *InSight* analitike saobraćaja. HE, RETN, GTT, NTT, *Arelion*, *Cogent*, *Zayo*, ZET-NET, samo su neki od globalnih provajdera koji su izabrani upravo na osnovu *InSight* analitika.

Rezultat je vidljiv apsolutno svim korisnicima Interneta u Srbiji, jer saobraćaj umesto preko javnog (nebezbednog i nestabilnog) Interneta dolazi bezbednim i najkraćim mogućim putem od servera u zemlji i regionu do računara, laptopa, telefona, IoT uređaja, bez bespotrebnog kruženja po Evropi i svetu. Internet stranice se otvaraju munjevito, a otkazi pojedinačnih linkova i kablova prilikom grubih građevinskih radova u SEE regionu nemaju direktnog uticaja na korišćenje Internet usluga u Srbiji.

InSight softver je bio tajni sastojak uspeha SOX-a u prethodnih 15 godina postojanja, koji je sada dostupan i drugima, a najbolja iskustva upravljanja SOX mrežom koja se prostire u četiri zemlje, devet gradova, 20 *data* centara ugrađena su u *InSight* softver i dostupna kroz upotrebu sva tri *InSight* programska modula.

https://insight.rs/

Synology jača sajber bezbednost i kontinuitet poslovanja

Svako preduzeće danas se suočava sa dva izazova: zaštitom podataka od neumornih sajber napada i osiguravanjem da operacije nikada ne prestaju, čak i kada hardver otkaže. Synology rešava oba problema kroz platformu na kojoj su skladištenje, bezbednost i podrška čvrsto integrisani – dizajnirani da besprekorno rade zajedno od prvog dana

Počnimo od sajber bezbednosti i koraka koje Synology preduzima da bi je obezbedio.

Brza zaštita od pretnji – Bezbednosna ažuriranja i zakrpe se isporučuju na celu platformu bez odlaganja, zatvarajući ranjivosti pre nego što ih napadači mogu iskoristiti.

Otporan po dizajnu – Ugrađene zaštite od *ransomware*-a, enkripcija od početka do kraja i napredne opcije rezervnih kopija dolaze standardno, pomažući preduzećima da obezbede kritične podatke bez oslanjanja na dodatke trećih strana.

Ujedinjena kontrola – IT timovi upravljaju svime sa jednog interfejsa, smanjujući složenost i eliminišući slepe tačke koje napadači često ciljaju u fragmentiranim okruženjima.

Obezbeđivanje kontinuiteta poslovanja

Optimizovane performanse – Pošto su hardver i softver napravljeni da se dopunjuju, sistemi rade pouzdanije, sa manje prekida.

Ekspresna zamena za Plus seriju – Ukoliko uređaj otkaže, *Synology* obezbeđuje brzu zamenu za sve Plus modele zasnovane na HDD-u, minimizirajući vreme zastoja i održavajući podatke dostupnim kada su najpotrebniji.

Predvidljiv životni ciklus – Preduzeća mogu dugoročno planirati sa poverenjem, znajući da je njihova infrastruktura podržana, bezbedna i spremna za budućnost.

Zašto je to važno za svako preduzeće

Male kompanije – Isti moćni DSM operativni sistem radi na uređajima početnog nivoa kao i na poslovnim modelima. To znači da čak i najmanja preduzeća dobijaju pristup alatima poslovnog nivoa kao što su šifrovane rezervne kopije, centralizovano upravljanje i bezbedno deljenje datoteka – sve bez opterećenja IT odeljenja.

Srednja preduzeća – Kako radno opterećenje raste, *Synology* se lako skalira. Skladištenje, SSD keširanje i jedinice za proširenje omogućavaju kompanijama da podrže više korisnika, zahtevnije aplikacije i veće skupove podataka bez ugrožavanja brzine ili pouzdanosti. Bezbednosne politike i praćenje ostaju centralizovani, održavajući složenost niskom, dok performanse ostaju visoke.

Velike organizacije – Preduzeća sa globalnim poslovanjem dobijaju doslednost i otpornost. Rešenja poput *ActiveProtect*-a proširuju *Synology* zaštitu na udaljene kancelarije i centre podataka, pokrivajući ogromna radna opterećenja i obezbeđujući jedinstvene strategije oporavka širom sveta. Svaka filijala radi na istoj ojačanoj DSM platformi, što čini usklađenost, praćenje i reagovanje na pretnje bržim i efikasnijim.

Uz *Synology*, preduzeća ne samo da čuvaju podatke – oni ih štite od pretnji i garantuju pristup, bez obzira na sve. To su sajber bezbednost i kontinuitet poslovanja, ugrađeni u temelj njihove infrastrukture.

sy.to/dndf9

ELASTIC SIEM: vaš elastičan odgovor na sutrašnje sajberpretnje

Sajberbezbednost je za dobar broj poslovnih ljudi pomalo ono što je zdravstvena ustanova za običnog čoveka

Autor: Bojan Miljković, direktor, Extreme d.o.o.

Plaćamo osiguranje, verujemo da smo zdravi, retko tamo idemo jer uvek imamo važnijih stvari, a ako prečesto budemo išli, mogli bismo nešto i da pronađemo što bi nas dosta koštalo u stresu, vremenu i novcu, pa je lakše da živimo u, neko bi rekao, blaženom *status quo mod*-u.

Za IT menadžere međutim, te „privilegije“ ne važe. Dok se vozite ujutro kroz gradsku gužvu do posla i razmišljate o vašim planovima i zadacima za danas, zovu vas kolege da vam kažu da je na 10 servera i 40 računara, od ukupno 250 koliko imate, od jutros detektovan neki generički trojanac, koji se uporno vraća nakon što ga vaša *endpoint* zaštita obriše. Ne, niko nije zvao niti pisao da traži nikakav novac. Još uvek.

SIEM rešenja postoje oko dvadesetak godina i može se reći da su s promenljivim uspehom bila prihvaćena u svetu sajberbezbednosti

Od planova naravno više nema ništa, stomak vam se već steže, a u glavi roji 1.000 pitanja. Imamo *firewall*, ažuriramo *Windows*-e i endpoint zaštitu. Kako su ušli? Kada? Kuda? Šta su već izneli? Šta je sve kompromitovano a mi još ne znamo? Ugasićemo Internet, za početak, to je najlakše. Uh, a klijenti? A zaposleni? A tek menadžment? Braniću se da mi nisu dali budžet koji sam tražio. Već znam, reći će mi da je trebalo da im pomognem da unapred sagledaju posledice i da su mislili da smo bezbedniji, da već plaćamo *endpoint* zaštitu itd.

Dok razmišljam o tome da ću im reći da još ne postoji bezbednost „na dugme“, bez obzira na sredstva, setim se izreke da trenutak u kom ste napadnuti nije baš najbolji da smišljate odbrambenu strategiju. Nek računaju štetu za firmu i nove budžete, moj prioritet je da isteramo uljeze i vratimo mrežu u mirnodopsko stanje. Samo još da smislim odakle da krenemo…

Kao što nema dve jednake firme, tako nema ni dve firme s jednakim rizicima i potrebama po pitanju sajberbezbednosti. Ako odgovarate za sajberbezbednost u vašoj firmi, a već znate da vaša reputacija kao firme ili gubitak prihoda u slučaju da firma ne radi nekoliko dana ili čak nedelja vredi mnogostruko više nego što ste do sada investirali u sajberbezbednost, ovaj tekst je prvenstveno namenjen vama.

SIEM rešenja postoje oko dvadesetak godina i može se reći da su s promenljivim uspehom bila prihvaćena u svetu sajberbezbednosti. Vredno su sakupljala logove, služila bi dobro za forenziku nakon što nas nešto-neko napadne, obaveštavala uredno admine kad se neki napad uklapao u pravila koja smo napisali, smirivala eksterne proverivače za ISO 27001, PCI DSS i slične standarde bezbednosti, ali nisu uspevala da urade mnogo više od toga.

Šta se od tada promenilo? I okruženje i mi i naši napadači. Dakle, sve. Postalo je kompleksnije. Hibridno. Veliko. A kompleksnost je stari neprijatelj sigurnosti.

Našeg IT menadžera iz uvoda sada čeka mukotrpna i spora borba s ruč-

nim prikupljanjem i analizom logova iz brojnih *cloud* i *onprem* sistema, aplikacija, mrežnih uređaja, u nadi da će pomoći da se razume situacija i očisti mreža, a sve pod priličnim vremenskim pritiskom da se nastavi s normalnim poslovanjem i umanji šteta. Uvek se može reinstalirati radna stanica, ali sa serverima je to često drugi par rukava.

Šta bi, nakon što se izbore s napadom, na pitanje o tome šta predlaže kako da se nešto slično ne ponovi, naš IT menadžer verovatno preporučio svom menadžmentu? Da nabave neki moderan SIEM sistem, koji upošljava statističke modele (da ne kažem *Machine Learning* (ML) ili, još gore, da pomenem AI), da upoznaju vašu mrežu, pronalaze anomalije i igle u plastu sena, pale alarme i automatski preduzimaju akcije tamo gde je automatizacija moguća (npr. u slučajevima gde je dozvoljeno da se prvo puca u žbun pa se onda kroz dim proverava šta je pogođeno ili s e otkrije da se žbun mrdao samo od vetra).

A kako bismo našem menadžmentu odgovorili na zdravorazumsko pitanje: „Koja bi bila suštinska razlika sa SIEM-om u odnosu na sadašnji pristup koji smo imali“? Zamislimo na trenutak kako bi izgledao TV prenos uživo velikog sportskog događaja pokrivenog kamerama, bez centralne sobe u kojoj režiser prenosa vidi šta svaka od kamera trenutno snima. Režiser bi kroz jedan ekran mogao da se poveže na svaku pojedinačnu kameru, ali kroz jedan ekran ni sam ne bi mogao da shvati šta se događa ni gde je potreban fokus, a kamoli da to omogući gledaocima kraj malih ekrana. Tako ugrubo izgleda *cyber security* bez SIEM sistema.

Šta treba da ima jedno savremeno SIEM rešenje kakvo je, na primer, danas holandski *Elastic*? Mora da ima agente (ili drugi mehanizam) za sakupljanje i uniformisanje logova sa radnih stanica, servera, mrežnih uređaja, aplikacija za upravljanje identitetom i autentifikacijom korisnika, *Web* servera i drugih nama bitnih sistema. Šta još? Mora da ima sistem za indeksiranje i analizu logova bitnih

za vašu bezbednost, kako bi brzo bili dostupni kad i gde su potrebni. Potreban je i interfejs, pomoću kojeg se iz kontrolnih tabli, prikaza i alarma na jednostavan način razumeva šta se dešava u našoj mreži. Ovo sve smo imali i pre 20 godina. A danas?

Elastic može biti dobar ulaz u SIEM svet. Vrlo je fleksibilan, ima veliku bazu korisnika i konektora, dobru podršku i viziju i stvarno pruža odličnu vrednost za investirani novac

Danas praktično u realnom vremenu odabrani ML algoritmi detektuju anomalije u odnosu na redovno stanje u našoj mreži i privlače nam pažnju na događaje koje naša *endpoint* zaštita jednostavno nije dizajnirana da uoči. Koje događaje? Na primer, neobičan obim saobraćaja kroz DNS protokol, što liči na izvlačenje podataka, zatim uspešna logovanja s neuobičajenih lokacija, što liči na kompromitovan nalog korisnika, povećani obim saobraćaja ka nekoj zemlji ili detekcija prebacivanja neuobičajeno velikog obima fajlova između dve radne stanice u mreži. Ovo su samo primeri, a ovde nam, kao što rekoh, retko koja *endpoint* zaštita može pomoći jer ovo nisu pretnje u tradicionalnom smislu, već pretpostavke izvedene iz korelacija, koje pružaju priliku da sami preventivno izrežiramo odgovor umesto da budemo statisti u tuđoj režiji.

Osim prevencije, ušteda vremena kada smo pod napadom lako se pretvara u uštedu novca, jer nešto za šta bi nam bili potrebni dani i nedelje da shvatimo, možemo saznati za jedan sat, ukloniti pretnju i nastaviti s normalnim radom. Postoji i AI (zar ste sumnjali?) asistent, koji vam može pomoći da rastumačite neki alert skoro kao da imate stručnjaka za sajberbezbednost u kući.

Elastic može biti dobar ulaz u SIEM svet. Vrlo je fleksibilan, ima veliku bazu korisnika i konektora, dobru podršku i viziju i stvarno pruža odličnu vrednost za investirani novac.

Budućnost u sajberbezbednosti izgleda nije u zasebnim alatima, već u dobro primenjenoj fleksibilnoj platformi koja bi se približno ponašala kao čovek koji razume okruženje, zna šta je važno, razume uzroke i brzo preduzima akciju. Nismo još uvek tu, ali zaista je sasvim jasno gde sajberbezbednost mora da ide da bismo sačuvali naše sajberzdravlje.

Mada, od nekih hakera prosto ni tada neće biti mnogo spasa. Ali kako kaže stara izreka: „Ono što ne možemo da uradimo, ne treba da nas sprečava da uradimo ono što možemo.“

extreme.rs

Tehnologija, ljudi i vizije

Ljudi koji su stvarali PC i njihovi doživljaji u računarskom svetu

Rast i razvoj domaćeg računarskog tržišta kroz vizuru vodećeg IT časopisa

25 priča sa tehnološke ivice

Monografija na 480 strana štampana u vrhunskoj tehnici ukrasiće vašu biblioteku.

U prodaji
pcpress.rs