STANTON CHASE

Uticaj globalnih trendova na sajber bezbednost i kako se zaštiti

April 2023

STANTON CHASE

Uvodnik

Sajber bezbednost je postala najaktuelnija tema u proteklih nekoliko godina, i čini se kao da sada dostiže svoj vrhunac. Različiti napadi koji ugrožavaju sajber bezbednost su sve češći i samim tim i izazovi da se ona sačuva i očuva. 2.244 sajber napada se dešava svakog dana, što je jedan napad na svakih 39 sekundi. Ransomver napadi su najveća pretnja za sajber bezbednost. Najčešći su jer su laki i relativno jeftini za izvođenje. Ovakav tip napada podrazumeva da hakerski softver uđe u organizacijske računare i blokira pristup sve dok se ne plati otkup. Samo u prvoj polovini 2022. godine se dogodilo 236,1 milion ransomver napada, što je 15 napada u svakoj sekundi. U 2022. godini čak 71% organizacija širom sveta bila je žrtva takvih napada što je za 20% više nego 2018. godine.

Zbog aktuelnosti ove teme i važnosti da se o tome, u svakoj kompaniji, razmišlja na vreme, a ne kada je kasno, obavili smo razgovor sa Duškom Rokvićem, generalnim direktorom kompanije Exclusive Networks.

"Broj sajber napada u stalnom je porastu, kako u regionu, tako i u Srbiji. Iako je najveći broj napada usmeren na preduzeća i javne službe državnih institucija, danas svako može biti meta napadača."

Duško Roković, GM, Exclusive Networks

Više je razloga, odnosno globalnih trendova koji se reflektuju na teritoriji Srbije i podstiču enormni rast sajber pretnji. Za početak, moramo istaći da digitalna transformacija, koja zahteva od kompanija da brzo usvajaju nove poslovne modele, ne donosi samo prednosti kompanijama kao što su produktivnost i smanjenje operativnih troškova.

Ova opšta digitalizacija stvara bezbednosne praznine, a napadači spremno „čekaju u zasedi" da iskoriste nezaštićene sisteme organizacija.

STANTON CHASE

Trendovi koji utiču na sajber bezbednost

U oblasti sajber bezbednosti se izdvaja nekoliko trendova koji utiču na bezbednost organizacija. Važno je razumeti ih kako biste bili korak ispred sajber pretnji kojih je sve više. Evo najvažnijih trendova koji utiču na sajber bezbednost:

1. Nedostatak radne snage

Kompanije se već nekoliko godina suočavaju sa nedostatkom zaposlenih, a to je posebno primetno u IT odeljenjima. Dakle, bezbednost organizacija trpi zbog nedovoljnog broja ljudi. Osim što imaju poteškoća u pronalaženju, kompanije teško mogu da zadrže stručnjake koji su sposobni da se pobrinu za sve složenije pretnje i digitalnu infrastrukturu. Ovaj trend ne pogađa samo velike kompanije, već se dešava i da zaposleni masovno napuštaju posao u SMB sektoru. Neke studije, uključujući (ISC)² 2022 Cybersecurity Workforce Study, pokazuju da svetu nedostaje čak 3,4 miliona stručnjaka za sajber bezbednost. Ako kompanija nema dovoljno zaposlenih, neće imati veštine vezane za zaštitu mreže i mrežne operacije.

2. Ljudski faktor kao glavni razlog sajber napada i proboja sistema

Kada pomislimo na sajber napad, najčešće mislimo na napade malvera i ransomvera. Međutim, najčešći uzrok proboja sistema je ljudska nepažnja, greška ili nedovoljno poznavanje bezbednosti. Drugim rečima, veća je verovatnoća da će do napada doći usled krađe identiteta putem phishing napada, nego da će kompanija biti pogođena napadom ransomvera. Greške u konfiguraciji, neažuriranje sistema i slične ljudske greške dodatno olakšavaju napadačima pristup sistemima i otkrivanje ranjivih podataka.

3. Previše korišćenih alata za sajber bezbednost

Naravno, kompanije postaju sve svesnije pretnji, pa značajno ulažu u rešenja za zaštitu. Danas nije neuobičajeno da jedna kompanija implementira više različitih rešenja, od različitih dobavljača. To mogu biti, na primer, next-generation firewall rešenja, SD-WAN, DLP, ZTNA, itd. Problem je što povećan broj zaštitnih rešenja znači više kontrolnih tačaka. A što je veći broj tačaka, to je veća složenost. Takva složenost komplikuje održavanje i povećava mogućnost sajber napada. Drugim rečima, veća složenost znači manje sigurnosti.

STANTON CHASE

Najveći izazovi za kompanije u kontekstu sajber zaštite

Navedeni trendovi dovode do mnogih izazova za kompanije i njihove bezbednosne timove. Pored pomenutog nedostatka veština potrebnih za borbu protiv sofisticiranih pretnji, problem su i izolovani silosi informacija, oprema i sistemi koji nisu adekvatno održavani, površina napada koja je svakim danom sve veća, prevelika količina upozorenja o potencijalnim pretnjama, itd.

Kako kompanije mogu da se zaštite

Evidentno je da će se opšta digitalna transformacija, koja uključuje usvajanje novih modela kao što je hibridni rad, nastaviti i u budućnosti. Takođe se može očekivati da će se kompanije još neko vreme boriti sa nedostatkom zaposlenih. Upravo zbog toga je važno razmišljati o objedinjavanju rešenja koja se koriste, odnosno usvajanju rešenja koja kombinuju više različitih rešenja u jedan alat.

Pod uslovom da ih imaju, bezbednosni timovi kompanija su malobrojni, imaju ograničene mogućnosti otkrivanja i reagovanja i potrebno im je rešenje koje će im pomoći sa upravljanjem i rastereti ih manje važnih zadataka. Danas na tržištu imamo nekoliko proizvođača i tehnologija koje mogu efikasno da odgovore na širok spektar bezbednosnih izazova.

Fortinet je izgradio svoju poziciju kao vodeći proizvođač rešenja za sajber bezbednost na portfelju koji objedinjuje više od 50 bezbednosnih mrežnih rešenja, čime je nadogradio tradicionalni koncept bezbednosti i olakšao timovima da se nose sa pretnjama. Ovaj širok spektar rešenja obuhvata sve, od rešenja za zaštitu krajnjih tačaka, preko firewall rešenja, switch-eva i access point rešenja do SD-VAN rešenja. Konsolidacija je ovde ključna.

Pomenimo i XDR tehnologiju, koja postaje standard u odbrani od sofisticiranih napada. To je tehnologija koja funkcioniše na način koji objedinjuje analizu cloud sistema, krajnjih tačaka i e-pošte i na taj način korisnicima pruža jasan uvid u potencijalne pretnje. Ukratko, XDR kombinuje brojna rešenja u jednom alatu. Automatizacijom i eliminisanjem nepotrebnih upozorenja koja ne predstavljaju stvarnu pretnju za organizacije, IT timovi su rasterećeni.

Kao što smo pomenuli, većina napada počinje krađom identiteta, tako da je neophodno da se kompanije fokusiraju na bezbedno prijavljivanje na sisteme. Naime, prijavljivanje u sistem je prvi korak ka kompaniji, a ako taj prvi korak nije dovoljno zaštićen, veća je šansa da će kompanija biti napadnuta. Svi već znaju da lozinke više ne pružaju dovoljan nivo zaštite, tako da industrija već neko vreme govori o metodama zaštite. U poslednjih godinu dana, višefaktorska autentifikacija je takođe postala ranjiva na phishing i napadači su počeli rutinski da zaobilaze takve prakse, pa se preporučuje upotreba MFA tehnika otpornih na phishing. Pre svega, ovde moramo da pomenemo Fido, standard koji ne zavisi toliko od lozinki, a olakšava administraciju i upravljanje.

STANTON CHASE

U Srbiji je prošle godine zabeležen rekordan broj napada na domaća preduzeća i državne institucije. Kao globalno priznati stručnjak za sajber bezbednost i digitalnu infrastrukturu, Exclusive Networks će nastaviti da podržava partnere i klijente u prevazilaženju ovih izazova.

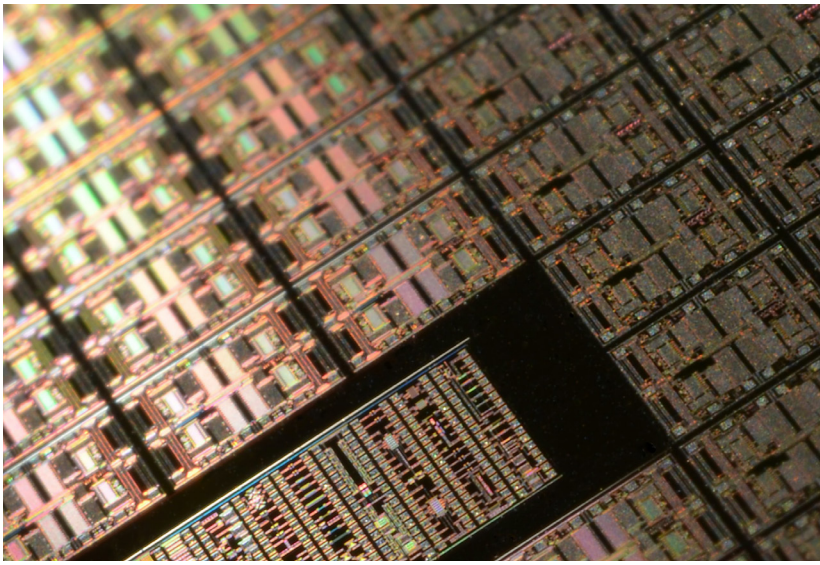
Exclusive Networks u svom portfoliju ima najširi spektar rešenja za zaštitu od sajber napada, zaštitu podataka, izgradnju data centara, zaštitu IoT uređaja i slično. Između ostalog, kompanija olakšava partnerima rešavanje problema vezanih za daljinski rad, skladištenje podataka, zaštitu ICS infrastrukture i zaštitu identiteta.

Zaključak

Skoro svi napadi su finansijski motivisani. Krađe podataka su najveći savremeni korporativni problem, jer pored etičkog aspekta, kompanije koštaju milione dolara. Predviđa se da će globalni troškovi štete od sajber kriminala za 2023. godinu biti 8 triliona dolara, što je čak 253.679 dolara po sekundi. Industrija sajber bezbednosti vredela je preko 156,30 milijardi dolara 2022. Predviđa se da će do 2027. godine dostići neverovatnih 403 milijarde dolara. Skoro 70% preduzeća se suočilo sa najmanje jednim napadom ransomvera, a 60% tog iznosa je moralo i da plati – neretko i više puta. Uz to, sve organizacije u kojima je ugrožena bezbednost mogu se suočiti sa velikim novčanim kaznama usled nepreduzimanja adekvatnih mera. U proseku, potrebno je oko 287 dana za otkrivanje i sprečavanje sajber napada. Sajber napadi postaju sve sofisticiraniji i teži za suočavanje. Kompanije koje ovaj savremeni izazov shvate ozbiljno, mogu da uštede stotine hiljada dolara.

“Podaci predstavljaju problem zagađenja informacionog doba, a zaštita privatnosti ekološki izazov.”

Bruce Schneier



STANTON CHASE

Izvori

- https://interestingengineering.com/cyber-attacks-more-likely-to-bring-down-f-35-jets-than-missiles
- https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide
- https://www.statista.com/outlook/tmo/cybersecurity/worldwide
- https://cybersecurityventures.com/stats
- https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022
- https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-vol-3-report.pdf
- https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/
- https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
- https://venturebeat.com/security/report-ransomware-attack-frequency-and-amount-demanded-down-in-h1-2022
- https://identitytheft.org/statistics/
- https://www.websiterating.com/sr/research/cybersecurity-statistics-facts/
- https://www.verizon.com/business/resources/reports/dbir/2020/results-and-analysis/
- https://blog.checkpoint.com/2022/02/02/the-2022-workforce-security-report/

STANTON CHASE

Asia/Pacific
Auckland · Bangalore · Beijing · Chennai
Hong Kong · Kuala Lumpur · Mumbai · New Delhi
Perth · Seoul · Shanghai · Singapore · Sydney · Tokyo

Europe, Middle East, Africa
Amsterdam · Athens · Belgrade · Brussels · Bucharest
Budapest · Copenhagen · Dubai · Düsseldorf · Frankfurt
Helsinki · Istanbul · Johannesburg · Lagos · Lisbon
London · Lyon · Madrid · Milan · Oslo
Paris · Porto · Prague · San Sebastian · Sofia
Stockholm · Stuttgart · Vienna · Warsaw · Zurich

Latin America
Bogotá · Buenos Aires · Lima · Mexico City
Montevideo · Panama City · Santiago · São Paulo

North America
Atlanta · Austin · Baltimore · Birmingham
Boston · Calgary · Chicago · Dallas · Detroit · Houston
Los Angeles · Miami · Nashville · New York
Philadelphia · Raleigh · San Francisco
Toronto · Washington, D.C.

Your Leadership Partner