STANJE INFORMACIJSKE I KIBERNETIČKE SIGURNOSTI U 2023. GODINI S PREPORUKAMA

5. izdanje

UKLJUČENO AKTUALNO OKRUŽENJE PRIJETNJI

UVODNIK

S ponosom predstavljam peto izdanje našeg godišnjeg izvještaja o stanju informacijske i kibernetičke sigurnosti. Nastavljamo tradiciju stalnog praćenja i analize ključnih trendova i izazova u ovom vitalnom području. Svjesni smo važnosti informacijske i kibernetičke sigurnosti u suvremenom poslovanju te vam nastojimo pružiti relevantne uvide i preporuke kako bismo podržali vaše organizacije u održavanju visoke razine sigurnosti svojih sustava.

Geopolitička situacija i sve veća polarizacija u današnjem svijetu podigla je razinu svjesnosti organizacija o važnosti informacijske i kibernetičke sigurnosti. Kibernetička sigurnost postaje važan element u svakoj organizaciji te vrlo česta tema na upravnim odborima organizacija. Vrlo često se pojavljuje i kao tema u javnosti, posebno u svjetlu incidenata koji se događaju u našem okruženju. Sve jače oslanjanje na automatizaciju i digitalizaciju nužno dovodi do toga da potencijalna šteta koju može prouzročiti kibernetički incident postaje sve značajnija.

Svjedoci smo i incidenata koji su pogodili naše okruženje te dospjeli u javnost. Od uspješnih napada na energetski sektor u Srbiji i Sloveniji do uspješnih napada na različite djelatnosti u Hrvatskoj. Zanimljivo je kako najveći incidenti koji dospiju u javnost imaju veze s ucjenom, odnosno ucjenjivačkim softverom (*ransomware*). Napadači su i dalje domišljati, a sada već trostruko ucjenjuju. Osim što već uhodano ukradu podatke i šifriraju ih, sada prijete i prijavom regulatoru ili na osobnoj razini ucjenjuju vodstvo organizacija. Naravno, i dalje ostaje činjenica da većina napada ni ne dospije u javnost.

Zakonodavstvo je prepoznalo izazove kibernetičke sigurnosti te smo svjedoci sve više regulatornih zahtjeva i okvira u tom području. Svakako treba izdvojiti Zakon o kibernetičkoj sigurnosti te novu inačicu direktive *Network and Information Security* (NIS), kao i *The Digital Operational Resilience Act* (DORA) jer će imati širok utjecaj na različite industrije, a posebno na sigurnosnu razinu i njihovo poimanje kibernetičke sigurnosti. Ove inicijative imaju za cilj unaprijediti sigurnosne standarde i osigurati veću otpornost organizacija na kibernetičke prijetnje te ih zato i pozdravljamo.

Unatoč nizu promjena i napretku, sigurnost operativno-tehnoloških (OT) sustava, odnosno industrijskih kontrolnih sustava i dalje ostaje zanemarena tema. Odgovorno poslovodstvo treba se suočiti sa svojom ulogom spram zaštite te investirati, na sličan način kako su to napravili s IT sustavima, i u obranu mnogo kritičnijih (OT) sustava.

Strojno učenje, veliki jezični modeli i umjetna inteligencija već sada su teme čijem se brzom razvoju podjednako raduju i napadačka i obrambena strana te se već standardno upotrebljavaju kao dio njihovih standardnih alata, odnosno mogućnosti. Stoga razumijevanje prijetnji postaje sve veći imperativ za one koji brane IT, ali još više za one koji brane OT sustave.

Kroz naš izvještaj želimo pružiti relevantne informacije i smjernice koje će organizacijama pomoći u suočavanju s izazovima i unapređenju njihove sigurnosne postavke. Uvjeren sam kako će naša analiza i preporuke biti od koristi u ostvarivanju ciljeva sigurnosti i stabilnosti informacijskih i kibernetičkih sustava.

VLATKO KOŠTURJAK,
CTO

POSLOVNI SAŽETAK

Geopolitička situacija i visoke stope inflacije snažno su utjecali na ekonomsku nesigurnost organizacija, što je vidljivo kroz zauzimanje konzervativne pozicije u donošenju poslovnih odluka. Slijedi sažetak ključnih odrednica izvješća za donositelje poslovnih odluka, i to logikom „manje je više".

INVESTICIJA, A NE TROŠAK.

Unatoč rastućim prijetnjama, budžeti za informacijsku/kibernetičku sigurnost ostali su slični ili su malo porasli u organizacijama koje se spremaju na implementaciju novih regulatornih zahtjeva (NIS2, DORA...). **Raste broj organizacija koje troše 10 % i više IT budžeta na informacijsku i kibernetičku sigurnost, ali ne proporcionalno rastućim prijetnjama.**

OD OPĆEG K SPECIFIČNOM.

Ključni zahtjevi regulatora odnose se na upravljanje rizikom, upravljanje incidentima, upravljanje lancem opskrbe, otpornost i upravljanje kontinuitetom poslovanja. **Navedeni zahtjevi predstavljaju temelje kvalitetnog upravljanja sigurnošću.**

SUKLADNOST JE NUŽNA, ALI NE I DOVOLJNA.

Glavni pokretač razvoja informacijske sigurnosti u RH i dalje je sukladnost s regulatornim obavezama koje dolaze s novim Zakonom o kibernetičkoj sigurnosti koji je netom izglasan, Direktivom o kibernetičkoj otpornosti i Uredbom o digitalnoj operativnoj otpornosti za financijski sektor (DORA). Jednom postignuto regulatorno usklađenje se ne smije smatrati konačnim „sigurnim" stanjem. **Postignuta sukladnost ne smije zaustaviti kontinuirano unaprjeđivanje i ulaganje**, jer je to jedini pristup koji vodi prema proaktivnoj informacijskoj i kibernetičkoj sigurnosti koja se može nositi sa stalno evoluirajućim prijetnjama.

OPROSTIVO JE BITI POBIJEĐEN, ALI NE I IZNENAĐEN.

Informacijska i kibernetička sigurnost su i dalje najčešće percipirani kao operativna tema i trošak poslovanja, a ne strateška odrednica ili kompetitivna prednost organizacija. Čak oko 50 % ispitanih organizacija informacijsku sigurnost još uvijek percipira kao „nužno zlo".

NE BITI POBIJEĐEN NITI IZNENAĐEN!

2023. godinu je obilježio značajan porast broja integralnih *Purple teaming* vježbi koje otkrivaju slabosti organizacije na temelju konstruktivne suradnje obrambenih i napadačkih timova.

BOLJE SPRIJEČITI NEGO LIJEČITI.

Penetracijska testiranja i *teaming* vježbe provedene od strane Diverta tijekom 2023. godine u najvećem broju su obuhvaćala procjene sigurnosti aplikacija i infrastruktura, a rezultirala su identifikacijom njihovih ranjivosti. Jednom identificirane kibernetičke ranjivosti moguće je analizirati i utvrditi poslovni utjecaj iskorištavanja istih. Iznimno se korisnim pokazalo analiziranje utjecaja koji bi moglo imati kombinirano iskorištavanje više ranjivosti. **Zaključci ovakvih analiza predstavljaju pouzdan temelj za optimalnu raspodjelu ulaganja u informacijsku i kibernetičku sigurnost.**

A REPUTACIJA?

Hrvatsko nadzorno tijelo za zaštitu osobnih podataka (Agencija za zaštitu osobnih podataka) u prošloj godini je značajno pojačalo svoje aktivnosti što je za posljedicu imalo 7 izrečenih kazni u ukupnom iznosu većem od 8,2 mil. EUR. Uspoređujući sve prethodne godine, navedeno predstavlja 230 % više izrečenih kazni, a prema iznosu, **AZOP je izrekao 2 od 15 najviših kazni izrečenih u 2023. godini na području EU-a.**

PROBLEMI SE RJEŠAVAJU DOK SU „MALI".

Temelj za postizanje otpornosti organizacija u suočavanju s izazovima sve sofisticiranijih kibernetičkih prijetnji je dobra priprema, poznavanje konteksta, krajolika prijetnji i uvježbanost timova. **Sigurnosno-operativni centar (SOC) Divertovim korisnicima omogućuje praćenje i analizu kibernetičkih prijetnji s ciljem osiguravanja najviše razine sigurnosti.** Nadogradnjom SOC-a sustavom ranog upozorenja, kroz koji mogu primati obavijesti o kibernetičkim prijetnjama i ranjivostima „skrojene" specifično za njih naši korisnici postižu značajni napredak u upravljanju i zaštiti poslovanja. Tijekom 2023. godine rješenje za 93% objavljenih ranjivosti bilo je najčešće pravovremena instalacija sigurnosnih zakrpa. ***Threat Hunting*** **operacije vođene stručnim znanjem i kreativnošću naglašavaju važnost „ljudske komponente" SOC-a i dalje su nezamjenjive u otkrivanju sofisticiranih prijetnji kod korisnika koje automatizirani sustavi zaštite najčešće ne uspijevaju registrirati.**

NI JEDNA DRŽAVA NIJE „OTOK".

Primjerice, regionalno, 2023. godinu obilježilo je prelijevanje geopolitičkog stanja prijetnjama Revil/Killnet grupe za izvršenje DDoS napada na financijsko-platežne mreže. **Za očekivati je da će se i u buduće situacije iz stvarnog svijeta odražavati u digitalnom, pa tako i u području informacijsko-kibernetičke sigurnosti.**

OVO NIJE PISAO CHATGPT.

Prepoznati izazovi oko umjetne inteligencije u prethodnom izvješću su se materijalizirali. U ovogodišnjem izvješću posebno poglavlje posvećujemo umjetnoj inteligenciji (AI) i kibernetičkoj sigurnosti. Međuzavisnost AI-ja i kibernetičke sigurnosti je višedimenzionalna. Proučili smo zahtjeve EU Akta o umjetnoj inteligenciji, sistematizirali prijetnje kibernetičkoj sigurnosti koje nastaju korištenjem umjetne inteligencije te potencijal umjetne inteligencije u obrani od kibernetičkih incidenata. **Kako napadi korištenjem AI-a postaju sve sofisticiraniji, tako korištenje AI-a u obrani postaje neophodno.**

PREDVIĐANJA I PREPORUKE.

Razumijevanje tko/što nam prijeti i kako se prijetnjama oduprijeti je ključno za uspješno upravljanje sigurnošću. Koristeći se različitim metodama istraživanja i primjenjujući alate napredne analitike na podacima kojima raspolažemo, donosimo prikaz najznačajnijih kibernetičkih prijetnji s kojima se trenutačno suočavaju zemlje u okruženju s naglaskom na Hrvatsku i Sloveniju te Bosnu i Hercegovinu.

Okruženje prijetnji i Izazovi budućnosti pomoći će vam da se pripremite, ali i promijenite budućnost.

SADRŽAJ

01

UPRAVLJAČKA PERSPEKTIVA

Upravljačka perspektiva pruža uvid u to koliko je pojedina organizacija, odnosno njezino poslovodstvo svjesno utjecaja informacijske sigurnosti na poslovanje i na kojoj su razini zrelosti primijenjene administrativne kontrole informacijske sigurnosti. Poslovodstvo je odgovorno prepoznati i otkloniti rizike informacijske sigurnosti koji mogu ozbiljno narušiti otpornost organizacije i time prouzročiti značajnu financijsku, reputacijsku ili regulatornu štetu.

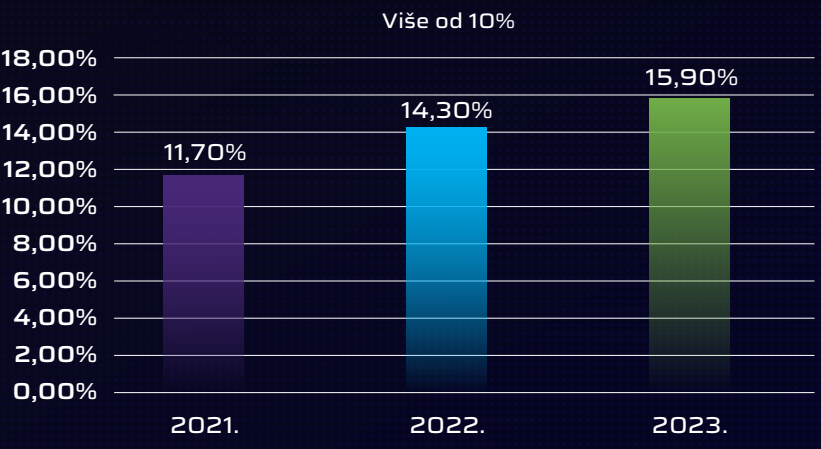
Tradicionalno smo proveli istraživanje o percepciji rizika i spremnosti za buduće izazove te se njime koristimo kao izvorom podataka u ovim, ali i daljnjim dijelovima izvještaja.

U nastavku teksta navodimo relevantne pokazatelje i trendove identificirane u 2023. g. koji mogu pomoći pri donošenju odluka relevantnih za prepoznavanje i rješavanje prijetnji i ranjivosti, a time i povećati otpornost organizacije.

KLJUČNI POKAZATELJI U PROMATRANOM RAZDOBLJU:

Geopolitička situacija, rat u Ukrajini i visoke stope inflacije snažno su utjecali na ekonomsku nesigurnost organizacija, što je vidljivo kroz zauzimanje konzervativne pozicije u donošenju poslovnih odluka.

- Unatoč rastućim prijetnjama, budžeti za informacijsku/kibernetičku sigurnost ostali su slični ili su malo porasli u organizacijama koje se spremaju na implementaciju zahtjeva novih direktiva (NIS2, DORA...). Raste broj organizacija koje troše 10% i više IT budžeta na informacijsku i kibernetičku sigurnost.



SLIKA 1. *Broj organizacija koje izdvajaju više od 10% IT budžeta za sigurnost raste, [Izvor: Diverto]*

- Informacijska i kibernetička sigurnost su i dalje najčešće percipirani kao operativna tema i trošak poslovanja, a ne strateška odrednica ili kompetitivna prednost organizacija, dok oko 50 % ispitanih organizacija informacijsku sigurnost percipira kao „nužno zlo".
- Hrvatsko nadzorno tijelo za zaštitu osobnih podataka (Agencija za zaštitu osobnih podataka) u prošloj godini je značajno pojačalo svoje aktivnosti što je za posljedicu imalo **7 izrečenih kazni u ukupnom iznosu većem od 8,2 mil. EUR**. Uspoređujući sve prethodne godine, navedeno predstavlja **230 % više izrečenih kazni**, a prema iznosu, **AZOP je izrekao 2 od 15 najviših kazni izrečenih u 2023. godini na području EU-a.**
- Trend visoke stope odlaska zaposlenika nakon pandemijskog razdoblja (engl. *big quit*) usporio je u svijetu, a posljedice tog trenda nisu pretjerano vidljive u RH jer se sve organizacije i dalje suočavaju s nedostatkom kvalificirane radne snage.
- **Potražnja za specijaliziranim ulogama (CISO) u 2023. porasla je za 33 %[1] u odnosu na 2022. godinu.** Predviđamo daljnji porast potražnje nakon stupanja na snagu nove regulative.

[1] Diverto CRM

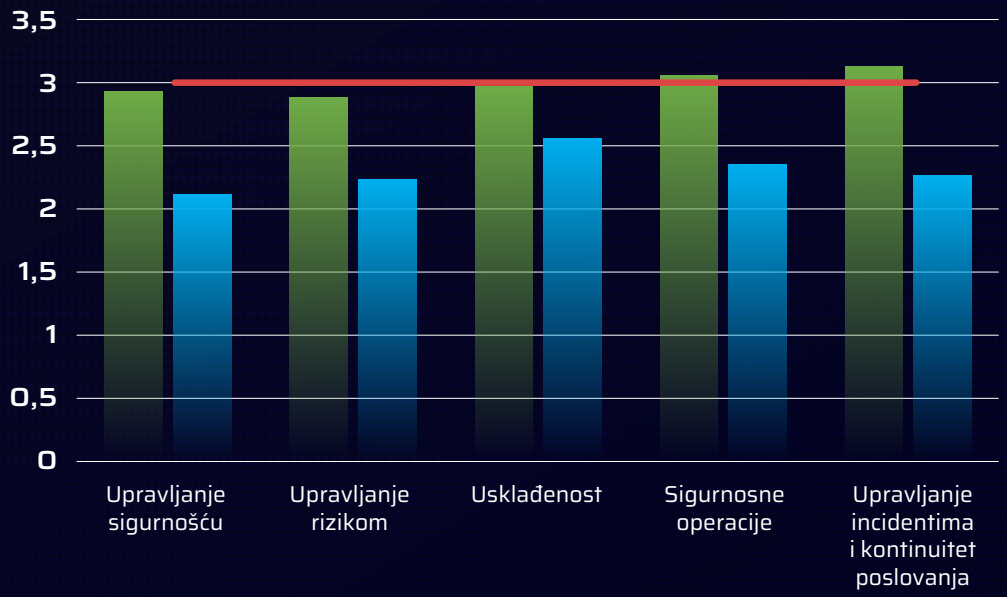
- Alati potpomognuti umjetnom inteligencijom prihvaćeni su rekordnom brzinom, kako od strane IS/KS profesionalaca tako i od strane zlonamjernika. Izazovi zaštite od zlonamjernog korištenja umjetnom inteligencijom dovode do pojačanog opreza i razmatranja kod regulatora te pokušaja normiranja, standardiziranja i reguliranja područja umjetne inteligencije i strojnog učenja.
- **Broj napada ucjenjivačkim softverom (*ransomware*) na svjetskoj razini u 2023. godini je u snažnom porastu, a u odnosu na 2022. godinu porast iznosi čak 68 %,** kao i **broj skupina napadača koji je porastao za više od 30 %**[2]. Prema Divertovim podacima, također je zabilježen porast, ali sa značajnim padom uspješnosti tih napada[3].
- Napadi putem softverskih komponenti, repozitorija otvorenog koda ili općenito, putem aplikacija trećih strana, na svjetskoj razini su u porastu, dok prema Divertovim podacima nisu zabilježeni značajniji incidenti koji bi bili posljedica iskorištavanja ranjivosti u ranjivim softverskim komponentama trećih strana.

„Poslovodstvo snosi odgovornost za prepoznavanje i rješavanje rizika informacijske sigurnosti koji mogu narušiti otpornost organizacije. Njihova uloga uključuje osiguravanje prevencije te umanjenja negativnih utjecaja tako da organizacija ne trpi financijske, reputacijske ili regulatorne gubitke zbog sigurnosnih incidenata. Međutim, često se događa da sigurnosne funkcije unutar organizacije nemaju adekvatan pristup ili utjecaj na odluke poslovodstva, što dovodi do propusta u upravljanju rizicima."

IVAN KALINIĆ
voditelj odjela za strateško upravljanje sigurnosti

STANJE U RH

Razina zrelosti je dobar osnovni pokazatelj kretanja informacijske sigurnosti u organizacijama. Ove godine prvi put uspoređujemo prosječne razine zrelosti u organizacijama s kojima već neko vrijeme surađujemo i pomažemo im u izgradnji učinkovitog programa sigurnosti i razine zrelosti sigurnosnog programa kod organizacija s kojima prvi put surađujemo.



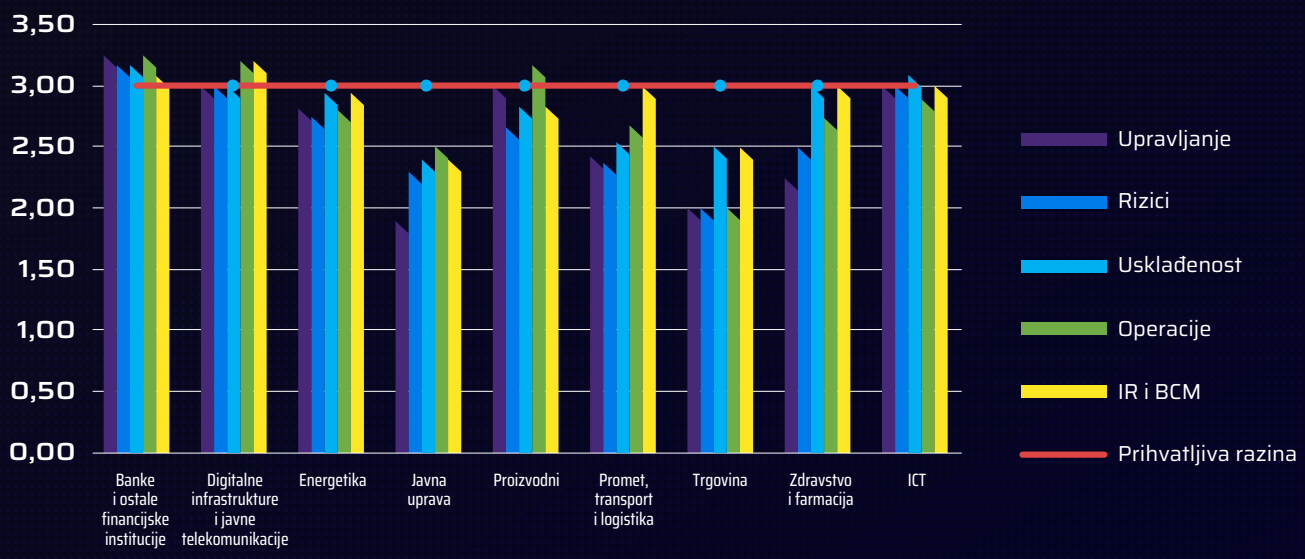
SLIKA 2.
Usporedba razine zrelosti - organizacije u kojima postoji program sigurnosti u odnosu na organizacije koje započinju graditi program sigurnosti, [Izvor: Diverto]

[2] https://www.corvusinsurance.com/blog/q4-ransomware-report
[3] Zlonamjerni kod poglavlje

U većini organizacija s kojima dulje surađujemo, sigurnosne kontrole postaju zrelije i obuhvatnije i u prosjeku se približavaju i prelaze definiranu razinu (3) poznatu kao stanje gdje je većina sigurnosnih kontrola formalizirana, ali se još ne slijede u potpunosti, niti je uvijek moguće izmjeriti njihov učinak. Vidljiv je raskorak između organizacija koje su već započele i grade programe sigurnosti i organizacija koje tek započinju raditi na razvoju takvih programa. Premda se razlika čini malom, potrebno je imati na umu činjenicu da je u prosjeku za podizanje razine za jedan bod potreban vremenski period od tri (3) i više godina te da je razvoj informacijske i kibernetičke sigurnosti u Republici Hrvatskoj intenzivnije potaknut 2018 godine stupanjem na snagu GDPR-a i Zakona o kibernetičkoj sigurnosti.

Dodatno, iz dosadašnjih iskustava, glavni pokretač inicijativa za kibernetičku i informacijsku sigurnost je postizanje sukladnosti. Većina organizacija postizanjem definirane razine najčešće ne želi ili ne može prelaziti na više razine jer to iziskuje dodatne troškove koje najčešće „ne znaju“ opravdati pred poslovodstvom. Navedeni pristup je opasan i ne vodi prema proaktivnoj informacijskoj i kibernetičkoj sigurnosti koja bi se mogla nositi sa stalno evoluirajućim prijetnjama.

Naravno, prosječna razina zrelosti nije ista za sve industrije. Kakva je prosječna razina po industrijama prikazano je u nastavku.

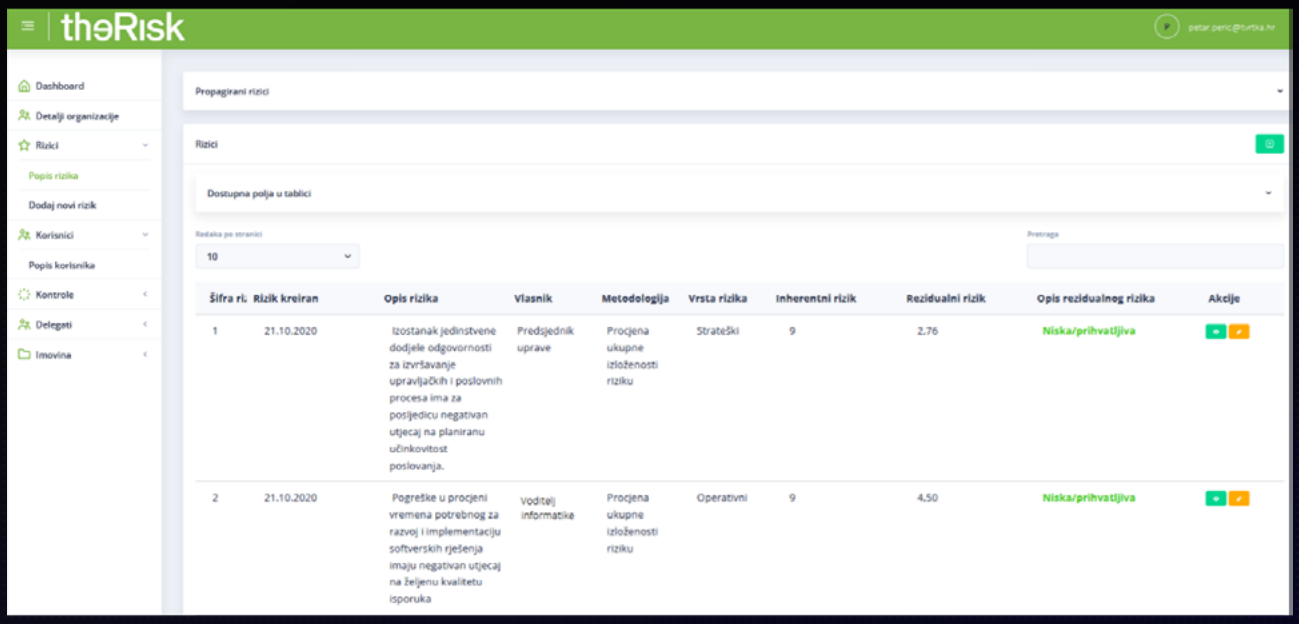


SLIKA 3. *Prosječna razina zrelosti po industrijama, [Izvor: Diverto]*

Po razini zrelosti i dalje vode banke i financijske institucije, što je i razumljivo jer kod njih pojam informacijske i kibernetičke sigurnosti nije nepoznat i postoji već više od 20 godina, Digitalna infrastruktura i javne telekomunikacije također su reguliran sektor koji shvaća vrijednost ispravno postavljenog programa kibernetičke sigurnosti. Iznenađuje relativno visoko pozicioniranje proizvodnog sektora, što nije relevantno na razini cijele RH jer predstavnici proizvodnog sektora u ovom grafikonu nisu tipični predstavnici istog nego korisnici koji su prepoznali dodanu vrijednost kibernetičke sigurnosti.

PROCJENA KRETANJA U 2024.

- U našem okruženju i dalje po percepciji dominiraju rizici prirodnih katastrofa i makroekonomskih učinaka, ali za razliku od prethodnih godina rizici informacijske i kibernetičke sigurnost zauzeli su visoko mjesto u top 5 poslovnih rizika.
- Glavni pokretač razvoja informacijske sigurnosti u Republici Hrvatskoj i dalje je sukladnost s regulatornim obavezama koje dolaze s novim, netom izglasanim Zakonom o kibernetičkoj sigurnosti, Zakonom o kibernetičkoj otpornosti i novim Zakonom o digitalnoj operativnoj otpornosti (DORA) te sličnim propisima.
- Za očekivati je prelijevanje „trenda" i pojačane napade na proizvodni sektor i na OT sustave koji se sve češće spajaju s poslovnim sustavima unutar inicijativa digitalne transformacije poslovanja.
- Broj izravnih obveznika novog zakona o kibernetičkoj sigurnosti raste i svi će morati primjenjivati mjere kibernetičke sigurnosti na cjelokupno poslovanje, a ne samo ključne sustave kao što je to bilo dosad. Navedeno predstavlja značajan pritisak na obveznike koji će se prelijevati na pružatelje usluga na području kibernetičke sigurnosti.
- Geopolitička situacija i inflacija će i dalje snažno utjecati na „kupovnu moć" organizacija pri nabavi sigurnosnih rješenja i usluga.
- Mogućnost pojave državno ili interesno sponzoriranih napada zbog super izborne godine u našoj zemlji
- Certifikacija pružatelja usluga s područja informacijske i kibernetičke sigurnosti koja će biti posljedica donošenja NIS2 i novog zakona o kibernetičkoj sigurnosti pružit će korisnicima usluga jasne kriterije za nabavu usluga i rješenja te dodatno jamstvo da će pružatelji usluga pružati usluge na prihvatljiv način i s definiranim/predvidivim razinama isporuke koje će biti podložne nadzoru. Takva jamstva do sada nisu postojala i onaj tko je nabavljao usluge iz domene kibernetičke sigurnosti morao je dobro paziti što i od koga nabavlja (*Caveat emptor*).
- Primjena umjetne inteligencije, lažne informacije u naprednim oblicima kao što su slike video materijali (*deepfake*) će biti sve prisutnije i dostupnije za provođenje zlonamjernih radnji poput manipulacije mišljenjem javnosti, pogotovo u ovoj, „super izbornoj godini". Važno je započeti s podizanjem svijesti javnosti o postojanju i potencijalnim rizicima koje ovi materijali nose.
- Nastavak digitalizacije poslovanja i širenje novih tehnologija kao što su autonomna SecOps rješenja, AI i 5G mreže pružit će nove mogućnosti poput poboljšane detekcije prijetnji, neprekidnog učenja i prilagodbe sustava te smanjenje opterećenja operativnog kadra. U isto vrijeme, taj napredak sa sobom donosi ranjivosti i rizike ugrađene u nove tehnologije, kao i mogućnost zloupotrebe novih tehnologija protiv tradicionalnih sustava obrane.
- Upravljanje rizikom postaje sve veći izazov s obzirom na dinamičko okruženje i konstantnu potrebu za kvalitetnom procjenom što je ne moguće raditi bez odgovarajućeg alata, te se očekuje sve veća potreba organizacija za specijaliziranim alatima za procjenu rizika kako bi adekvatno upravljali rizikom.



SLIKA 4. *Prikaz sučelja alata za upravljanje i procjenu rizika, [Izvor: Diverto]*

- Nedostatak kvalificirane radne snage biti će i dalje prisutan, pogotovo u svjetlu novih regulativa. Velika razlika u ponudi i potražnji za stručnjacima sigurnosti jača pružatelje usluga i slabi organizacije, ali i povećava stručnost samih pružatelja sigurnosnih usluga.
- Pojačana potreba za razumijevanjem i informacijama o prijetnjama (*threat inteligence*)
- Proaktivna obrana od ucjenjivačkog softvera (*ransomware*) je obavezna sigurnosna kopija (*backup*), primjena zakrpi, osvještavanje i trening te revizije.

„Analiza utjecaja na poslovanje (Business Impact Analysis - BIA) je nakon pridobivanja podrške poslovodstva i određivanja organizacijske strukture iznimno vrijedan korak u procesu uspostave ili poboljšanja programa upravljanja informacijskom sigurnošću jer omogućuje organizacijama da identificiraju potencijalne štete koje mogu nastati zbog kibernetičkih napada ili ispada u IKT sustavima. Ova analiza pruža ključne informacije o tome koliko je organizacija zapravo ovisna o svojim IKT sustavima i koje su posljedice kada ti sustavi zakažu. BIA je također najbrži način za pribavljanje informacija od poslovne strane, omogućujući integraciju tih informacija u zahtjeve za izgradnju učinkovitog sustava kibernetičke i informacijske sigurnosti."

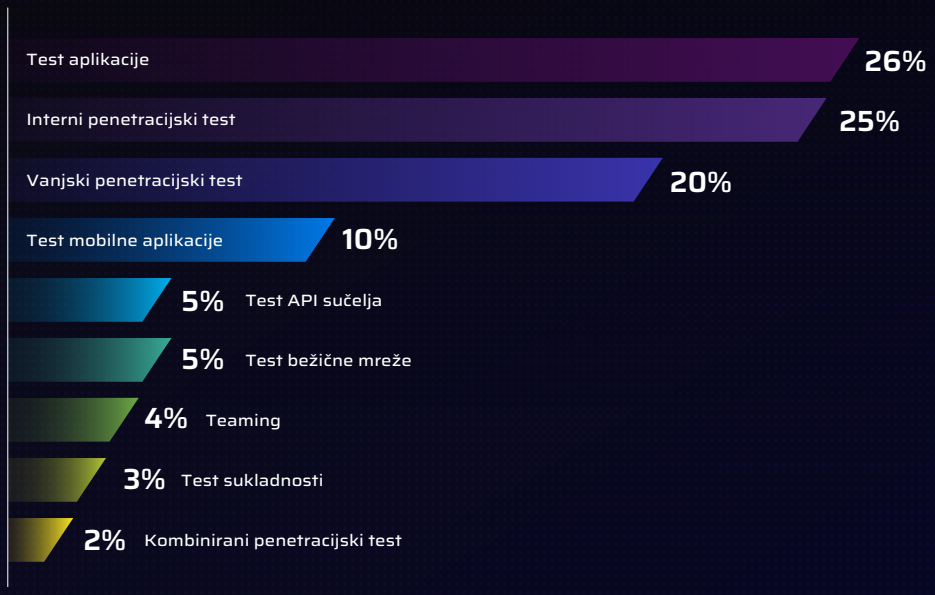
IVAN KALINIĆ
voditelj odjela za strateško upravljanje sigurnosti

02

NAPADAČKA PERSPEKTIVA

Kako bi testirale kibernetičku sigurnost svojih sustava, brojne organizacije provele su različite vrste penetracijskih testova tijekom protekle godine. Primjećujemo kako organizacije koje samostalno upotrebljavaju automatizirane alate za skeniranje ranjivosti ne odustaju od standardnih metoda penetracijskih testiranja te, dapače, idu još i dalje te se koriste naprednim testovima poput *red* i *purple teaming* vježbi sve više i sve slobodnije.

Penetracijska testiranja koje je Diverto proveo tijekom 2023. godine u najvećem broju su obuhvaćala procjene sigurnosti aplikacija i infrastruktura.



SLIKA 5. *Tipovi testova u 2023. godini, [Izvor: Diverto]*

Iako je broj teaming vježbi (npr. *red i purple*) relativno malen u odnosu na broj provedenih drugih oblika testiranja, razlog leži u tome što obično organizacije provode na desetke penetracijskih testova godišnje, dok se *teaming* vježba uobičajeno odradi jednom godišnje.

GLAVNI CILJ PENETRACIJSKIH TESTIRANJA

bio je identificirati i iskoristiti potencijalne ranjivosti kako bi se utvrdio njihov utjecaj na organizaciju. S obzirom na dobivene spoznaje, pružene su odgovarajuće preporuke kako bi se pomoglo u učinkovitom upravljanju otkrivenim rizicima.

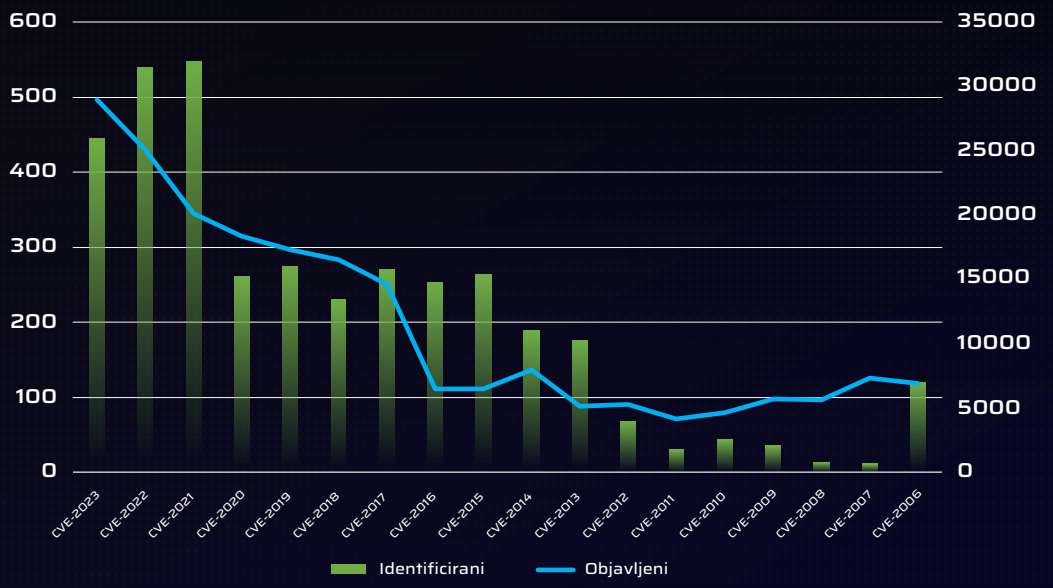
2.1. SIGURNOSNA TESTIRANJA INFRASTRUKTURA

Provedenim infrastrukturnim penetracijskim testovima utvrđeno je kako najveći broj ranjivosti ukazuje na izazove prilikom:

- izdavanja važećih certifikata za web aplikacije i servise
- korištenja slabijim kriptografskim protokola i šiframa (*ciphers*)
- nedostatka aktualnih zakrpa za servise i biblioteke
- upotrebe nepodržanih verzija operacijskih sustava i popratnog softvera
- prisutnost mrežnih autentifikacijskih protokola ranjivih na napade prosljeđivanjem
- spremanja korisničkih vjerodajnica na nezaštićenim i dijeljenim mrežnim lokacijama

U usporedbi s prethodnim godinama, primijećen je smanjen broj ranjivosti koje omogućavaju udaljeno izvršavanje proizvoljnog koda (engl. *remote code execution*).

Ovo ukazuje na brže rješavanje takvih ranjivosti, primjenu preporuka iz provedenih penetracijskih testova te opći trend smanjenja broja ranjivosti ovog tipa. Ova vrsta ranjivosti je prethodnih godina češće iskorištavana za ostvarivanje inicijalnog, neautoriziranog pristupa sustavima, a zatim bi se korištenjem post-eksploatacijskim tehnikama ostvario pristup drugim sustavima i administrativnim sučeljima.



SLIKA 6. *CVE ranjivosti identificirane u testovima u odnosu na broj ukupno objavljenih CVE ranjivosti, [Izvor: Diverto]*

Iz perspektive napadača koji je uspostavio inicijalni pristup organizaciji krađom ili pogađanjem korisničkih vjerodajnica, izvršavanjem zlonamjernog koda u kontekstu korisnika računala ili primjenom različitih taktika/tehnika za ostvarivanje inicijalnog pristupa infrastrukturi, napadačke tehnike prema okviru *MITRE ATT&CK* koje su najčešće omogućavale lateralno kretanje i preuzimanje kontrole nad infrastrukturom bile su:

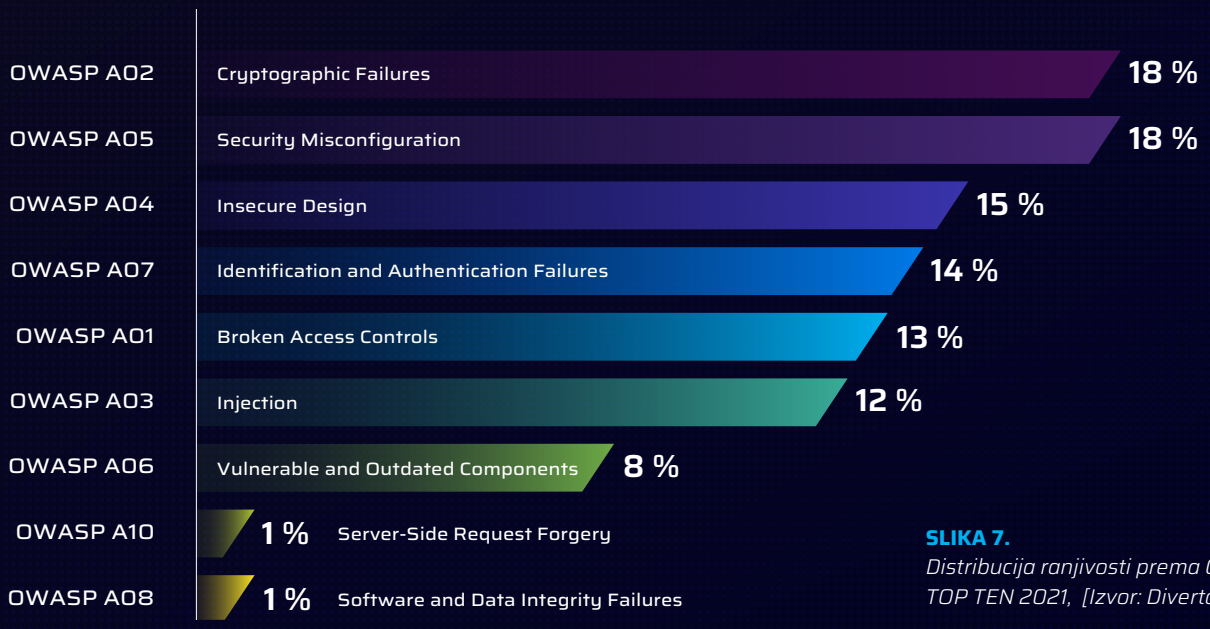
- **T1110:** Brute Force
  https://attack.mitre.org/techniques/T1110/
- **T1552.001:** Unsecured Credentials: Credentials In Files
  https://attack.mitre.org/techniques/T1552/001/
- **T1558.003:** Steal or Forge Kerberos Tickets: Kerberoasting
  https://attack.mitre.org/techniques/T1558/003/
- T1649: Steal or Forge Authentication Certificates
  https://attack.mitre.org/techniques/T1649/
- T1039: Data from Network Shared Drive
  https://attack.mitre.org/techniques/T1039/
- T1003.001: OS Credential Dumping: LSASS Memory
  https://attack.mitre.org/techniques/T1003/001/
- T1190: Exploit Public-Facing Application
  https://attack.mitre.org/techniques/T1190/
- T1210: Exploitation of Remote Services
  https://attack.mitre.org/techniques/T1210/
- T1557.001: Adversary-in-the-Middle LLMNR / NBT-NS Poisoning and SMB Relay
  https://attack.mitre.org/techniques/T1557/001/
- T1550.002: Use Alternate Authentication Material: Pass the Hash
  https://attack.mitre.org/techniques/T1550/002/
- T1550.003: Use Alternate Authentication Material: Pass the Ticket
  https://attack.mitre.org/techniques/T1550/003/
- T1003.003: OS Credential Dumping: NTDS
  https://attack.mitre.org/techniques/T1003/003/
- T1003.006: OS Credential Dumping: DCSync
  https://attack.mitre.org/techniques/T1003/006/
- T1003.002: OS Credential Dumping: Security Account Manager
  https://attack.mitre.org/techniques/T1003/002/

Glavni pozitivni pomaci uočeni kod korisnika su aktivno bavljenje informacijskom sigurnošću, radom na prevenciji tehnika lateralnog kretanja koristeći se modelom „*Admin tiering*“, upotreba privilegiranih radnih stanica prilagođenih za izvođenje administrativnih zadataka, korištenje *jump-box* radnih stanica te poboljšano mrežno segmentiranje. Također, uočen je pozitivan pomak u upravljanju ranjivostima unutarnje i javno dostupne infrastrukture proaktivnim djelovanjem, poput samostalnog provođenja skenirana ranjivosti.

2.2. SIGURNOSNA TESTIRANJA APLIKACIJA

Tijekom 2023. godine provedena su testiranja raznovrsnih web aplikacija i servisa, mobilnih te desktop aplikacija. **Najveći broj pronađenih ranjivosti u aplikacijama odnosi se na upotrebu slabijih kriptografskih algoritama, nedostatak dodatnog očvršćivanja servisa i načela sigurnog dizajna aplikacija te nedostatak nadogradnji za softverske pakete i biblioteke.** Navedeno se može spriječiti već u samom začetku, prvenstveno edukacijom o sigurnom razvoju aplikacija, prilikom podizanja i konfiguracije aplikacijskih poslužitelja uz praćenje najboljih sigurnosnih praksi, te redovitim ažuriranjem softverskih paketa i popratnih biblioteka.

Stanje aplikativne sigurnosti ukazuje na raznolikost u pogledu utjecaja i ozbiljnosti uočenih ranjivosti s više od polovice onih niskog rizika, što ukazuje na poboljšanje u primjeni modela životnog ciklusa razvoja aplikacija. Međutim, ranjivosti srednjeg rizika zahtijevaju posebnu pozornost jer mogu poremetiti funkcionalnost ili izložiti osjetljive podatke. Uspjeh se mjeri dosljednim smanjenjem ranjivosti tijekom vremena. Poduzimanje konkretnih i efektivnih mjera otpornosti igra vitalnu ulogu u ranom otkrivanju ranjivosti. Iako ukupni dojam odaje poboljšanu sliku sigurnosti u odnosu na prethodne godine, preporučuju se kontinuirani ciljani napori za trajnu obranu od kibernetičkih prijetnji.



SLIKA 7.
Distribucija ranjivosti prema OWASP TOP TEN 2021, [Izvor: Diverto]

Analiza ranjivosti aplikacija u skladu s OWASP metodologijom ostaje pouzdano mjerilo za prepoznavanje i rješavanje sigurnosnih slabosti u različitim aplikacijama.

Potrebno je istaknuti značaj robusnih kriptografskih praksi i preciznog upravljanja konfiguracijom u razvoju i implementaciji aplikacija te imperativ uključivanja načela sigurnog dizajna u životni ciklus razvoja softvera kako bi se ublažili potencijalni rizici koji proizlaze iz pogrešnih arhitekturnih odluka zbog njihovog mogućeg utjecaja na integritet podataka i sigurnost na strani poslužitelja.

Dodatno, postoji potreba za strogom provjerom valjanosti korisničkog unosa i sigurnom praksom razvoja aplikacija kako bi se spriječilo umetanje zlonamjernog koda, pažljivo definirala autorizacija i kontrola pristupa, budući da je rješavanje ovih problema najvažnije za sprječavanje neovlaštenog pristupa i jačanje mehanizama kontrole pristupa unutar aplikacija.

> **VAŽNO JE STAVITI NAGLASAK**
> **i na ranjivosti koje se odnose na zastarjele ili ranjive komponente trećih strana, što dodatno potvrđuje nužnost kontinuiranog praćenja i pravovremenih ažuriranja za ublažavanje povezanih rizika.**

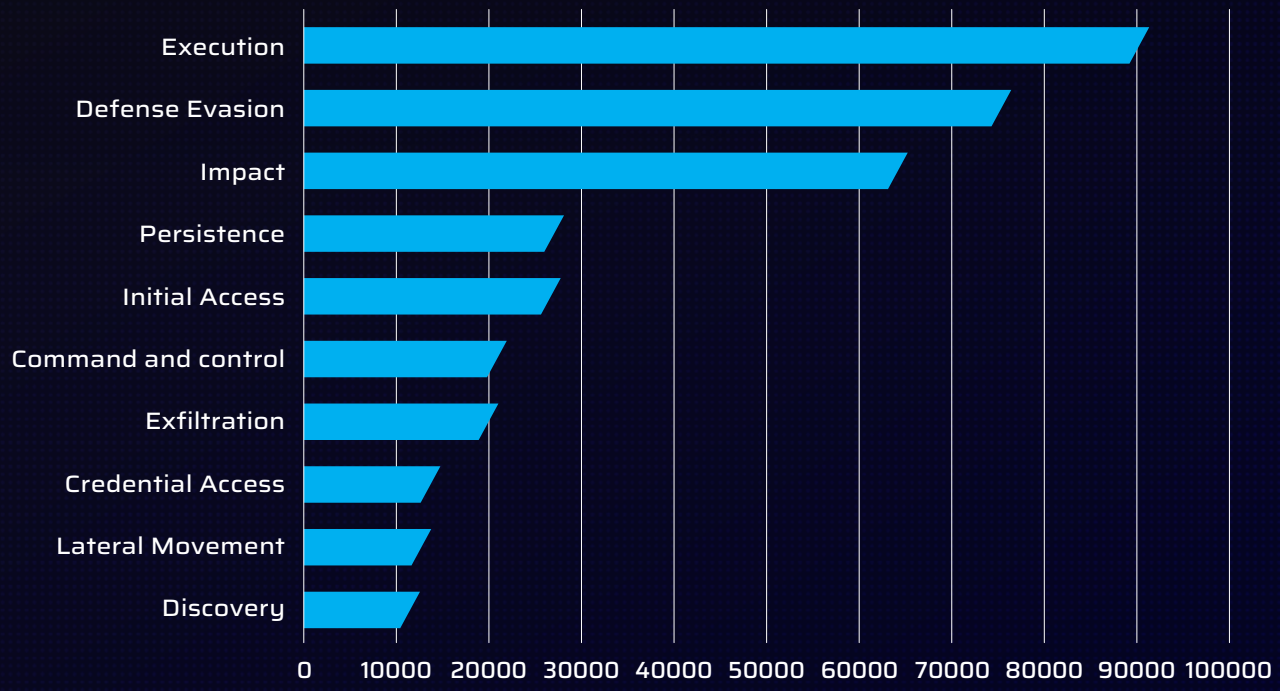
Zaključno, sveobuhvatna analiza OWASP skupa ranjivosti u različitim aplikacijama ističe potrebu za **proaktivnim pristupom sigurnom razvoju softvera.** Davanjem prioriteta **kriptografskim praksama, upravljanju konfiguracijom, načelima sigurnog dizajna i robusnim mehanizmima autentifikacije,** organizacije mogu učinkovito ublažiti raznolik raspon prijetnji i poboljšati ukupnu otpornost svojih aplikacija kao odgovor na aktualne izazove sveukupnog stanja kibernetičke sigurnosti.

OBRAMBENA
PERSPEKTIVA

Obrambena perspektiva uključuje razumijevanje poslovnog okruženja, identificiranje potencijalnih rizika i brzu reakciju na svaki sigurnosni događaj. Tijekom 2023. godine provodili smo proaktivne i reaktivne mjere putem svojih ključnih usluga Sigurnosno-operativni centar (SOC) i *Early Alerting* (Sustav ranih upozorenja).

Ljudska uloga kroz operacije *Threat Hunting*, vođene stručnim znanjem i kreativnošću, imale su nezamjenjivu ulogu u otkrivanju sofisticiranih prijetnji kod korisnika koje tradicionalni sustavi zaštite nisu uspjeli registrirati.

U okviru Sigurnosno-operativnog centra (SOC), posvećeni smo praćenju i analizi kibernetičkih prijetnji kako bismo osigurali najvišu razinu sigurnosti za naše korisnike. U našim operacijama, usredotočili smo se na praćenje sigurnosnih alarma sukladno *MITRE ATT&CK* taktikama koje nam omogućavaju identifikaciju najčešćih prijetnji i sigurnosnih događaja.

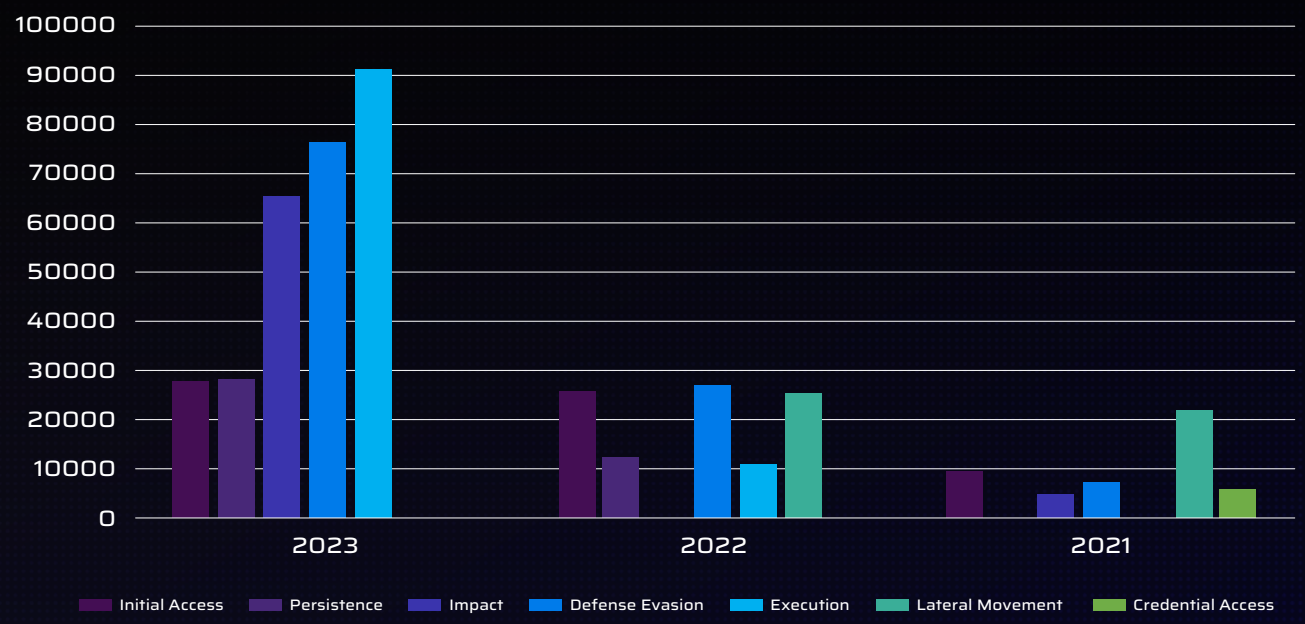


SLIKA 8. *TOP 10 najčešće obrađenih alarma prema MITRE Att&ck taktikama u 2023. godini, [Izvor: Diverto SOC]*

UNAPRJEĐENJE KVALITETE I KAPACITETA

Sigurnosno-operativnog centra (SOC) značajno je proširilo opseg i broj provedenih istraga te obrađenih sigurnosnih događaja tijekom 2023. godine u usporedbi s prijašnjim godinama.

Ovaj prirodni rast rezultat je sustavnog proširenja kapaciteta našeg SOC-a, posebice u povećanju broja SOC korisnika, količini novih uređaja i podržanih tehnologija koje aktivno pratimo, te unaprjeđenju sigurnosnih operacija u sklopu pružanja usluge Sigurnosno-operativnog centra.

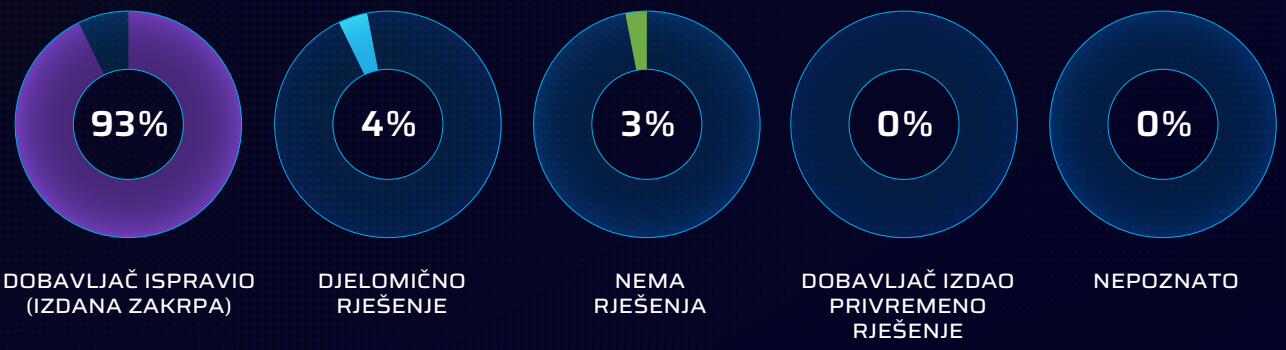


SLIKA 9. *TOP 5 najčešće obrađenih alarma prema MITRE Att&ck taktikama u 2023. , 2022. i 2021. godini [Izvor: Diverto SOC]*

Temelj za preventivno djelovanje organizacija u suočavanju s izazovima sve sofisticiranijih kibernetičkih prijetnji je pravovremeno reagiranje na identificirane prijetnje i ranjivosti. Uz široki spektar različitih servisa koje korisnici upotrebljavaju, praćenje i upravljanje ranjivostima postalo je sve zahtjevnije.

Korisnici se svake godine suočavaju s izazovom u pravovremenom reagiranju i upravljanju prijetnjama i ranjivostima. Ova kompleksnost dovodi do povećanog rizika od iskorištavanja ranjivosti s potencijalno ozbiljnim posljedicama po sigurnost informacija i integritet sustava.

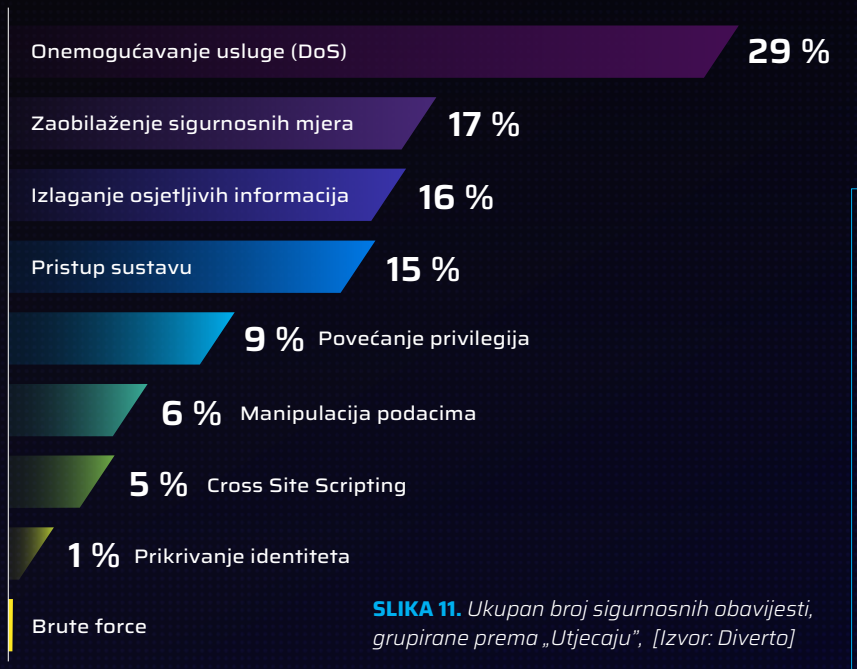
U protekloj godini, Divertovi korisnici su postigli značajan napredak u upravljanju i zaštiti informacijske imovine te su u sklopu usluge Sustava ranog upozorenja primali sigurnosne obavijesti o prijetnjama i ranjivostima u svom sustavu. Rješenje za 93 % objavljenih ranjivosti tijekom 2023. godine bilo je u vidu pravovremene instalacije sigurnosne zakrpe.



SLIKA 10. *Ukupan broj sigurnosnih obavijesti, grupirane prema „Statusu rješenja", [Izvor: Diverto]*

Analiza identificiranih sigurnosnih ranjivosti korisnika tijekom prošle godine jasno ističe najveću prijetnju, odnosno mogući vektor napada iz vanjskog okruženja (eng. *Remote*) koji predstavlja trenutno najveći izazov za sigurnost. **Imperativ i glavna preporuka i dalje je jačanje sigurnosti vanjskih pristupnih točaka kako kako bismo smanjili mogućnost iskorištavanja ranjivosti sustava i osigurali integritet podataka.**

Sigurnosne obavijesti tijekom protekle godine istražene su s naglaskom na njihov utjecaj na moguću vrstu iskorištavanja. **Kao najznačajnije ključne sigurnosne obavijesti izdvojili bismo „Onemogućavanje usluge - DOS“, „Zaobilaženje sigurnosnih mjera“, „Izlaganje osjetljivih informacija“ i „Pristup sustavu“ uzimajući u obzir da predstavljaju značajan izazov za sigurnost sustava te čine 77 % svih identificiranih ranjivosti tijekom 2023. godine.**



SLIKA 11. *Ukupan broj sigurnosnih obavijesti, grupirane prema „Utjecaju“, [Izvor: Diverto]*

PREPORUČUJEMO redovitu identifikaciju i ažuriranje potpunog popisa informacijske imovine. To uključuje sve sustave, mrežne uređaje, podatkovne baze i ostale sigurnosne tehnologije i komponente koje čine vašu infrastrukturu. Precizna definicija informacijske imovine ključna je za pravilno usmjeravanje sigurnosnih napora.

NAGLAŠAVAMO važnost pravovremenog ažuriranja sustava putem instalacije sigurnosnih zakrpi. Aktivno praćenje dostupnih zakrpi i njihova brza implementacija smanjuju rizik od iskorištavanja poznatih ranjivosti.

PREPORUČUJEMO usmjeravanje resursa i procesa prema pravovremenoj analizi sigurnosnih događaja, čime se omogućava brzo otkrivanje neobičnih aktivnosti. Upotreba alata za analizu datotečnih zapisa i implementacija sustava ranog upozorenja pridonose povećanju sposobnosti organizacije za prepoznavanje i reagiranje na potencijalne prijetnje.

IDENTIFICIRANE RANJIVOSTI TREBAJU BITI KLJUČNA TOČKA za daljnje jačanje obrambenih mehanizama. Preporučuje se usmjeriti na implementaciju dodatnih sigurnosnih kontrola, provođenje dodatnih testiranja sigurnosti i educiranje osoblja o novim prijetnjama i ranjivostima.

„Suočeni s izazovima sve složenijih kibernetičkih prijetnji, neprestano ažuriranje strategija obrambene perspektive, uz posebni naglasak na ključnu ulogu SOC-a, osigurava efikasan odgovor na dinamiku kibernetičkog okruženja. Kroz jačanje sigurnosnih kapaciteta i proaktivno praćenje novih prijetnji, postavljamo temelje stabilnosti i pouzdanosti informacijskih resursa organizacije.”

DAVOR SLAVICA,
voditelj obrambenog tima

04

INTEGRALNA PERSPEKTIVA – PURPLE TEAMING

S obzirom na povećani broj provedenih *Purple teaming* vježbi tijekom 2023. godine, radosni smo što smo u mogućosti podijeliti naša iskustva.

Purple teaming predstavlja sigurnosnu vježbu tijekom koje **crveni (napadački) tim** Diverta i **plavi (obrambeni) tim** organizacije odnosno klijenta blisko surađuju kako bi unaprijedili kibernetičku sigurnost organizacije međusobnim dijeljenjem informacija i znanja.

GLAVNI CILJ *PURPLE TEAMING* VJEŽBE

je usavršavanje sposobnosti otkrivanja i reakcije na potencijalne incidente, provođenje procjene sigurnosti kroz autentične simulacije napadačkih scenarija, sustavno testiranje specifičnih napada te razvoj obrambenih strategija radi poboljšanja sigurnosne vidljivosti i preciznog identificiranja potencijalnih ranjivosti sustava.

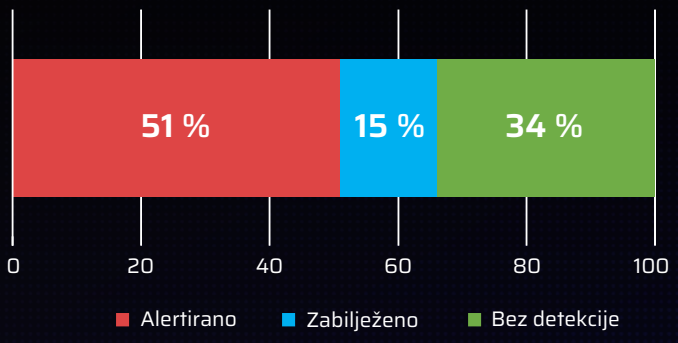
Bitno je naglasiti da **organizacija treba biti na određenoj sigurnosnoj razini pri provođenju Purple teaming vježbe te imati implementirane alate detekcije** kao što je SIEM, sigurnosno-operativni centar i druge sigurnosne sustave. Ti alati omogućuju plavom (obrambenom) timu da sustavno prati, analizira i reagira na potencijalne sigurnosne prijetnje. Uz to, *Purple teaming* vježbe omogućuju organizaciji da identificira nedostatke u detekciji i alarmiranju te ih nakon toga poboljša u komunikaciji s crvenim (napadačkim) timom. Stoga, provođenje *Purple teaming* vježba nije samo testiranje postojećih sustava i procesa, već i prilika za njihovo poboljšanje.

***Purple teaming* vježba zahtijeva snažno uključenje obrambenog tima organizacije.** Iskustvo simulacije napada u kontroliranim uvjetima je, na temelju reakcija naših klijenata, ne samo korisno nego i uzbudljivo. Bitno je naglasiti kako se ove vježbe trebaju shvatiti pozitivno, na način da organizacije kroz njih uče o slabostima primijenjenih sigurnosnih mjera.

Pronalazak takvih slabosti ne predstavlja kritiku samih mjera i sustava, već pruža priliku za poboljšanje razine sigurnosti kroz prijenos znanja između napadačkih i obrambenih timova u sigurnom okruženju.

Bilo bi izuzetno teško pronaći organizaciju u kojoj bi vježba završila bez ikakvih nedostataka u njezinim obrambenim sustavima. Stoga je naša preporuka obrambenim timovima da se usredotoče na identificiranje tih nedostataka i njihovom rješavanju. Na temelju našeg iskustva i međunarodnih spoznaja, jasno je da je gotovo nemoguće predvidjeti sve taktike, tehnike i smjerove napada kojima bi se iskusni napadač mogao koristiti.

Kroz nekoliko različitih scenarija, rezultati otkrivanja ofenzivnih aktivnosti tijekom provedenih *Purple teaming* vježbi su sljedeći:



SLIKA 12. *Rezultati otkrivanja ofenzivnih aktivnosti u Purple teamingu, [Izvor: Diverto]*

Navedeni podaci ukazuju da se u prosjeku preko 50 % ofenzivnih aktivnosti može otkriti na vrijeme kroz korištenje uobičajenim sigurnosnim mehanizmima. Dio napadačkih aktivnosti može se primijetiti pregledom datotečnih zapisa bilo lokalno ili na centraliziranim SIEM rješenjima, dok značajan dio aktivnosti napadači mogu provesti bez da se iste primijete na sigurnosnim sustavima i centraliziranim rješenjima za prikupljanje datotečnih zapisa.

Glavni uočeni nedostaci u organizacijama su:

- SIEM rješenje ne upotrebljava se za jedinstveni, centralizirani nadzor
- nedostatak obogaćivanja datotečnih zapisa (primjerice upotrebom *Sysmon* rješenja)
- nedostatak pravila otkrivanja posebno prilagođenih za organizaciju
- nepotpuna pokrivenost infrastrukture nadzornim agentima
- nedostatak lažnih resursa / informacija na infrastrukturi (*honeypot/honeytoken*)
- nedostatak kvalificiranog kadra posvećenog sigurnosti organizacije
- lažan osjećaj sigurnosti

Iz navedenih podataka vidimo da većina organizacija koje su provele *Purple teaming* vježbu ima SIEM sustav, no uočeno je da njegova svrha nije u potpunosti iskorištena te je potrebna dodatna sigurnosna konfiguracija radnih stanica na kojima datotečni zapisi (engl. *log*) nisu dodatno obogaćeni već se prikupljaju samo standardni događaji (engl. *event*) ili SIEM nije kontinuirano nadograđivan novim pravilima otkrivanja. Također, nerijetko se SIEM rješenje upotrebljava isključivo za centralizirano prikupljanje datotečnih zapisa, zanemarujući mogućnosti ranog upozorenja i otkrivanja prijetnji. Ovo ograničava SIEM na pasivni alat za prikupljanje podataka, umjesto da bude proaktivna centralna konzola za praćenje sigurnosnih incidenata. Stoga je ključno iskoristiti puni potencijal SIEM-a kako bi organizacije bile u mogućnosti brzo identificirati i reagirati na potencijalne prijetnje. *Purple teaming* vježbe su prilika da se ovi nedostaci prepoznaju i adresiraju, omogućavajući organizacijama da unaprijede svoje sustave te educiraju ljude.

Većina organizacija oslanja se na sigurnosne alate i uređaje, no to stvara lažan osjećaj sigurnosti. Smatrajući da su potpuno zaštićene zbog prisutnosti navedenih rješenja, organizacije često zaboravljaju da oni predstavljaju samo jedan važan, ali ipak ograničen aspekt ukupne sigurnosti.

> **BITNO JE OSVIJESTITI ORGANIZACIJE**
> o važnosti ovakvih vježbi te potaknuti konstruktivan pristup koji će omogućiti identifikaciju i rješavanje sigurnosnih slabosti na temelju suradnje i zajedničkog razumijevanja između plavih i crvenih timova.

Tek kroz takav pristup organizacije mogu istinski iskoristiti potencijal *Purple teaming* vježbe za poboljšanje sigurnosti same organizacije.

05

PRIPREMA ZA BUDUĆNOST

Iako se u 2023. ova tema spominjala sporadično, s donošenjem nacionalne legislative u 2024. smatrali smo da ju je potrebno obraditi u ovom izvještaju. Cilj nam je na pregledan način informirati organizacije u našoj zemlji i šire o ovoj temi kako bi prepoznale koliko im je ona relevantna.

5.1. NIS2

NIS2 Direktiva (Direktiva (EU) 2022/2555) – Direktiva o mjerama za visoku zajedničku razinu kibernetičke sigurnosti zamjenjuje NIS Direktivu (Direktiva (EU) 2016/1148) iz 2016. godine. NIS2 direktiva je već transponirana u novi hrvatski Zakon o kibernetičkoj sigurnosti (NN 14/2024). DORA je *lex specialis* u odnosu na NIS2 Direktivu.

CILJ DIREKTIVE

NIS2 Direktiva je zakonodavni okvir uspostavljen od strane Europske unije s ciljem dostizanja visoke zajedničke razine kibernetičke sigurnosti i otpornosti diljem Europske unije.

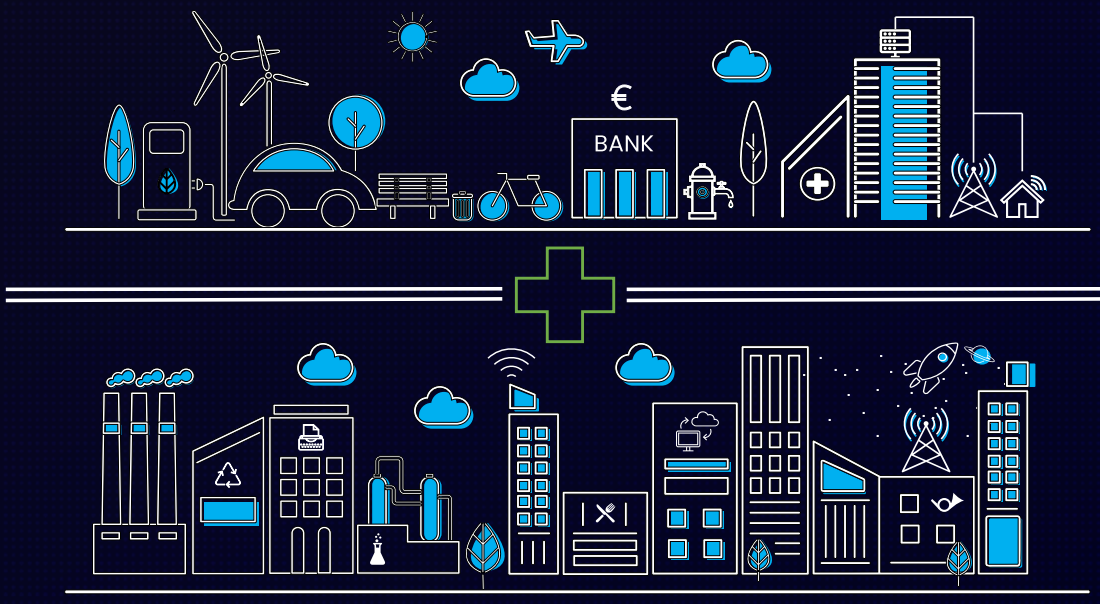
5.1.1. ŠTO NOVO DONOSI NIS2?

NIS2 Direktiva u odnosu na prvotnu NIS Direktivu donosi nekoliko ključnih promjena:

1. **POVEĆANJE OPSEGA** u smislu:
    a. **Sektora** na koje se odnosi

NIS1 SEKTORI

ENERGIJA, TRANSPORT, FINANCIJSKE INFRASTRUKTURE I BANKE, VODA, ZDRAVSTVO, PRUŽATELJI DIGITALNIH USLUGA, DIGITALNA INFRASTRUKTURA.



SLIKA 13. *Prikaz sektora uključenih u NIS1 i NIS2 Direktivu, [Izvor: Diverto]*

NIS2 SEKTORI

JAVNA ADMNISTRACIJA, HRANA, ISTRAŽIVANJE, SVEMIR, RASPOLAGANJE OTPADOM, ICT SERVISI (B2B), POŠTA, PROIZVODNJA KRITIČNIH PRODUKATA, PRUŽATELJI JAVNIH ELEKTRONIČKIH KOMUNIKACIJSKI MREŽA I SERVISA.

Zbog utjecaja globalnih trendova, pandemije i geopolitičke situacije, utvrđeno je da je opseg NIS Direktive bio ograničen s obzirom na potrebe i rizike stoga je broj sektora na koje se odnosi NIS2 znatno veći.

b. **Sustava** koje obuhvaća

SLIKA 14. *Prikaz sustava koje obuhvaća NIS1 I NIS2 direktiva, [Izvor: Diverto]*

Dok je NIS u fokusu imao isključivo sustave koji podržavaju pružanje ključne usluge, NIS2 prepoznaje da i ranjivosti u drugim dijelovima informacijskog sustava mogu imati negativni utjecaj na poslovanje stoga u opseg stavlja sve mrežne i informacijske sustave subjekta obveznika, neovisno o procesima koje podržavaju.

2. ODGOVORNOSTI UPRAVLJAČKIH FUNKCIJA

Poslovodstvo postaje zakonski odgovorno za:

- nadzor i upravljanje kibernetičkom sigurnošću i
- odobravanje mjera upravljanja rizicima.

Navedeno u NIS Direktivi nije bilo adresirano i sada se uvodi kao mjera koja bi trebala utjecati na veću važnost i vidljivost sigurnosti unutar organizacija, a samim time i osigurati pravovremene odluke u svrhu zaštite mrežnih i informacijskih sustava te očuvanja kontinuiteta poslovanja subjekta obveznika.

3. NADZOR SUKLADNOSTI

SLIKA 15. *Prikaz nadzora sukladnosti kojeg propisuje NIS2 Direktiva, [Izvor: Diverto]*

Nadzor sukladnosti je također novost koja je uvedena kroz NIS2, a provodit će se periodički ili na zahtjev kroz revizije sigurnosti i stručne nadzore. Revizije sigurnosti u ključnim subjektima provodit će za to autorizirana tijela, a važni subjekti reviziju mogu provoditi samostalno. Stručni nadzor odgovornost je nadležnih sektorskih tijela.

4. KOREKTIVNE MJERE I SANKCIJE

Nesukladnosti utvrđene kao rezultat revizija i stručnih nadzora mogu za posljedicu imati:

- privremene suspenzije
- zabrane obavljanja djelatnosti ili
- novčane kazne za subjekte obveznike i/ili odgovorne osobe unutar subjekta obveznika.

5.1.2. VREMENSKI OKVIR

SLIKA 16. *Vremenski okvir NIS2 Direktive, [Izvor: Diverto]*

Od dana donošenja novog Zakona o kibernetičkoj sigurnosti:

- Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona imaju **jednu godinu** za kategorizaciju subjekata i dostavu obavijesti o kategorizaciji.
- Subjekti obveznici imaju rok od **trideset dana** od zaprimanja obavijesti o kategorizaciji u kojem moraju početi slati obavijesti o incidentima.
- Rok za usklađivanje, odnosno implementaciju mjera je **godinu dana** od zaprimanja obavijesti o kategorizaciji subjekta.
- Rok za provedbu revizije sigurnosti je **dvije godine** od isteka roka za usklađivanje.

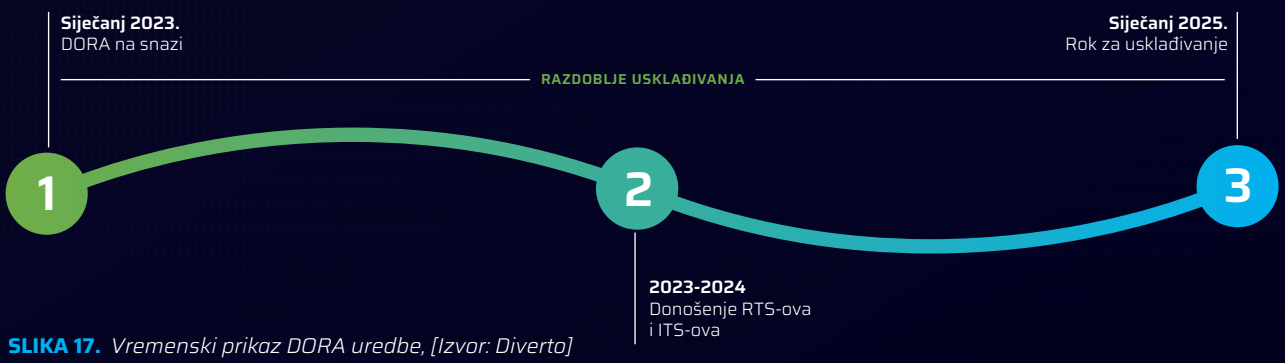
5.2.DORA

DORA (Uredba (EU) 2022/2554) – Uredba o digitalnoj operativnoj otpornosti za financijski sektor je *lex specialis* u odnosu na NIS2 Direktivu i direktno je primjenjiva na zemlje članice Europske unije.

U opsegu DORA-e su:

- financijske institucije na razini EU
- pružatelji IKT usluga.

CILJ
je ojačati informacijsku sigurnost financijskog sektora zbog sve većeg razvoja digitalnih proizvoda i usluga.



SLIKA 17. *Vremenski prikaz DORA uredbe, [Izvor: Diverto]*

U odnosu na NIS2 koji nalaže donošenje mjera usklađenja kroz lokalne uredbe, **DORA ovlašćuje Europska nadzorna tijela (*European Supervisory Authorities – ESA*) da donesu niz standarda koje su subjekti obveznici dužni usvojiti** (*RTS – Regulatory Technical Standards, ITS – Implementing Technical Standards*) iz sljedećih područja upravljanja informacijskom sigurnošću:

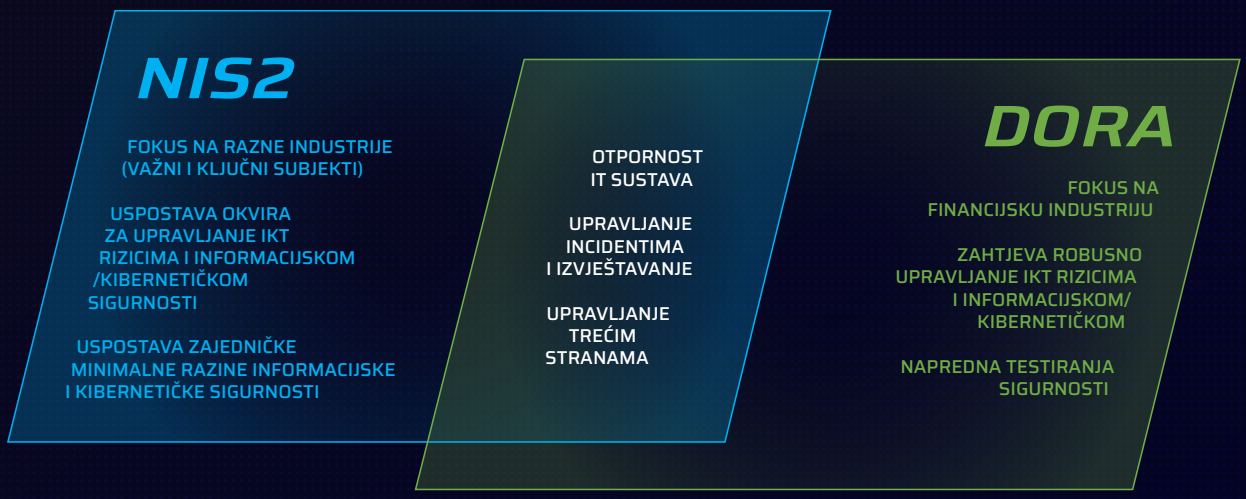
- upravljanje IKT rizicima (uključujući implementaciju tehničkih mjera i kontrola u poslovne procese)
- upravljanje, klasifikacija i izvješćivanje u vezi s IKT incidentima
- testiranje digitalne operativne otpornosti
- upravljanje IKT rizikom povezanim s trećim stranama.

Jasno je da DORA za obveznike postavlja robusna pravila za postizanje digitalne operativne otpornosti zbog čega se snažan naglasak stavlja upravo na testiranje digitalne operativne otpornosti naprednim metodama kao što su penetracijska testiranja vođena prijetnjama (TLPT – *Threat Lead Penetration Test*) u jasno definiranim intervalima.

Također, jedno od područja za koje smatramo da bi moglo utjecati na veće promjene je upravljanje rizikom trećih strana koje do sada nisu bile regulirane na ovakvoj razini.

U slučaju nesukladnosti sa zahtjevima, DORA kao i NIS2 propisuje sankcije u obliku novčanih kazni.

5.2.1. ODNOS IZMEĐU NIS2 I DORA-e



5.3. CRA

Cyber Resilience Act (CRA) – Uredba Europskog parlamenta i Vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020 odobrena je 12. ožujka 2024. od strane Europskog parlamenta. Odobreni prijedlog Uredbe dostupan je na poveznici.

CRA je pravni okvir koji opisuje zahtjeve kibernetičke sigurnosti za hardverske i softverske proizvode s digitalnim elementima koji se plasiraju na tržištu Europske unije. Proizvodi s digitalnim elementima u tom smislu su svi softverski ili hardverski proizvodi i njihova rješenja za daljinsku obradu podataka, uključujući softverske ili hardverske komponente koje se zasebno stavljaju na tržište.

CILJ REGULATIVE je osigurati primjereno upravljanje sigurnošću proizvoda s digitalnim elementima od strane proizvođača tijekom cijelog životnog ciklusa.

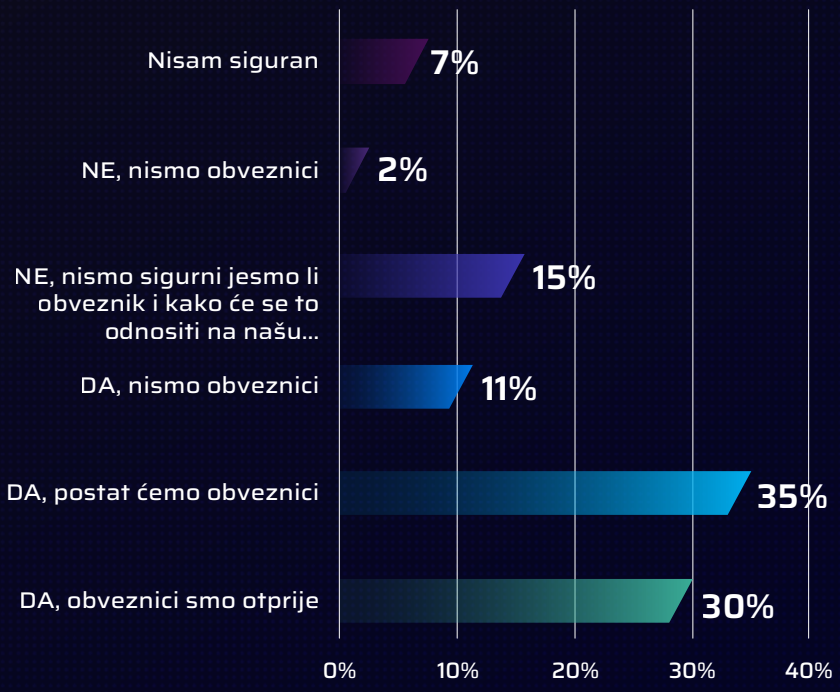
5.4. KLJUČNI IZAZOVI I (NE)SPREMNOST ORGANIZACIJA

U ovom poglavlju obrađeni su rezultati istraživanja koje smo proveli ove godine s većim brojem organizacija vezano za teme NIS/DORA/CRA. Vjerujemo da će vam biti interesantno usporediti situaciju u vašoj organizacij s ovom slikom koju smo dobili kroz naše istraživanje.

RAZINA SVIJESTI

Saznanja do kojih smo došli ukazuju kako poslovodstva organizacija nisu na jednak način informirana o NIS2 Direktivi te novim obvezama i odgovornostima koje iz nje proizlaze. Navedeno se ponajviše odnosi na subjekte koji će biti klasificirani kao važni i koji će tek postati obveznici Zakona. Neki od subjekata iz novih sektora u opsegu (npr.: telekomi, poštanske usluge, proizvodnja) do sada su bili regulirani zakonima specifičnim za njihovu industriju i područje poslovanja, dok zaštita informacijske i kibernetičke sigurnosti najčešće nije bila u fokusu.

S druge strane, očekivano, financijska industrija koja je navikla na visoke zahtjeve informacijske i kibernetičke sigurnosti prednjači u aktivnostima koje se poduzimaju kako bi se osigurala zahtijevana razina sukladnosti s DORA-om.



S druge strane,

35 %

organizacija svjesno je da će postati novi obveznici jedne od navedenih regulativa te znaju što to za njih znači.

22 %

organizacija nije sigurno što će za njih značiti nove regulative niti odnosi li se neka od regulativa na njih.

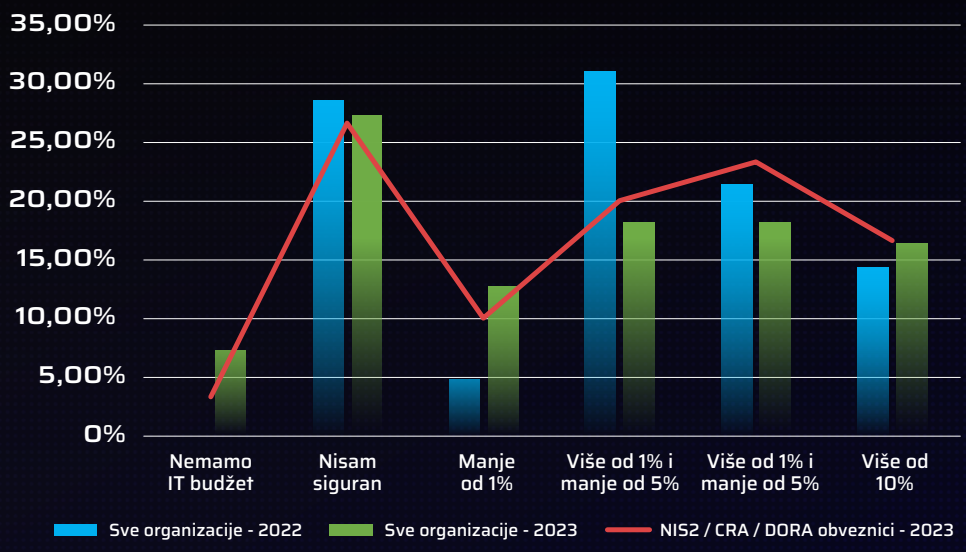
SLIKA 18. *Znate li što za vašu organizaciju znači donošenje regulativa NIS2 / CRA / DORA?, [Izvor: Diverto]*

BUDŽET

Za implementaciju zahtjeva koji proizlaze iz novih regulativa, potrebno je pravovremeno izdvojiti i prikladan budžet.

Temeljem podataka koje smo prikupili, organizacije koje su svjesne i sigurne da će biti obveznici NIS2/CRA/DORA regulativa izdvajaju veći postotak IT budžeta u odnosu na sve ispitane organizacije u 2022. i 2023. godini.

To se najviše prepoznaje iz činjenice da 23 % obveznika regulativa izdvaja više od 5% i manje od 10 % IT budžeta za informacijsku/kibernetičku sigurnost u odnosu na 18 % svih ispitanih organizacija u 2023., odnosno 21 % organizacija u 2022. godini.



SLIKA 19.
Alokacija budžeta za informacijsku /kibernetičku sigurnost kod organizacija koje su svjesne i sigurne da će biti obveznici NIS2/CRA/DORA regulativa u odnosu na sve ispitane organizacije u ovoj i prošloj godini, [Izvor: Diverto]

Organizacije obveznice regulativa koje nisu izdvojile sredstva za usklađivanje najčešće:

- nisu svjesne zahtjeva regulativa vezanih uz informacijsku i kibernetičku sigurnost niti hoće li se oni odnositi na njih
- svjesne su regulativa, ali smatraju da postoji dovoljno vremena za usklađivanje
- svjesne su regulativa, ali smatraju da regulative, posebno NIS2, neće zaživjeti na način kako su definirane zbog čega nemaju ni strah od sankcija.

OGRANIČENI RESURSI

Uz nove regulatorne zahtjeve i činjenicu da u području informacijske i kibernetičke sigurnosti općenito postoji značajan manjak ljudskih resursa, za očekivati je da će navedeno u narednim godinama predstavljati još veći izazov nego što je to bilo do sada. Na veliki porast potražnje za resursima utjecat će organizacije koje do sada nisu upravljale informacijskom i kibernetičkom sigurnošću na primjeren ili ni na koji način.

S obzirom na ograničenu ponudu resursa na tržištu i nemogućnost izgradnje kapaciteta za upravljanje informacijskom i kibernetičkom sigurnošću „iznutra“, organizacije sve više prepoznaju praktičnost i dodanu vrijednost eksternaliziranih usluga kao što su *Cyber Threat Intelligence*, vCISO, Sigurnosni Operativni Centar.

70 % ispitanih organizacija koje su svjesne i sigurne da će biti obveznice NIS2/CRA/DORA regulativa je alociralo budžet u svrhu usklađivanja,

40 % istih je zaključilo da aktivnosti usklađivanja neće biti u mogućnosti samostalno provesti.

50 %
organizacija koje nisu sigurne što će za njih značiti nove regulative niti odnosi li se neka od regulativa na njih nemaju IT budžete ili nisu sigurne koliki postotak IT budžeta imaju na raspolaganju za potrebe informacijske/ kibernetičke sigurnosti.

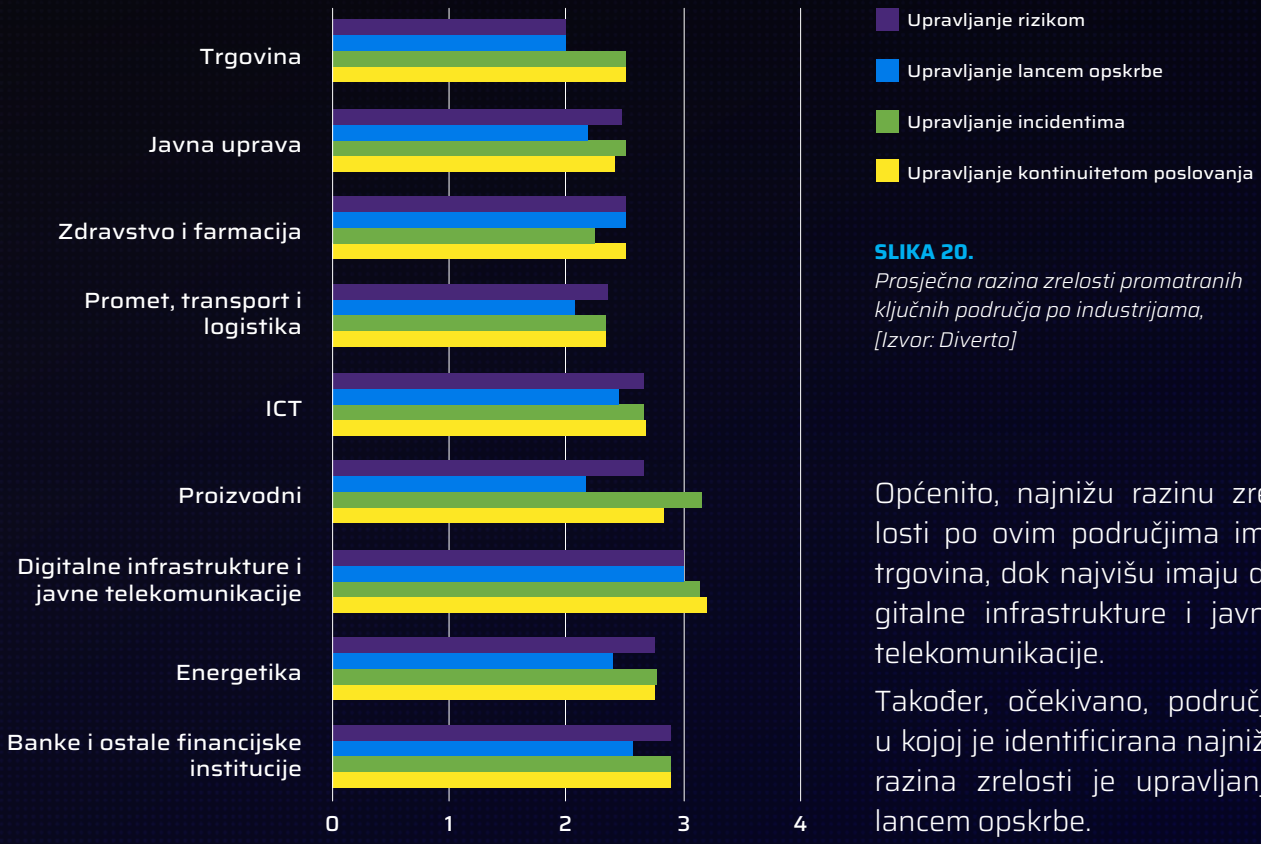
Međutim, prema rezultatima naših ispitivanja,

80 %
organizacija koje su svjesne i sigurne da će biti obveznici NIS2/CRA/DORA regulativa, smatra da ulaganja u informacijsku/ kibernetičku sigurnost omogućavaju sigurno poslovanje i otpornost na kibernetičke napade.

5.3.2. IZAZOVI VEZANI UZ ZAHTJEVE REGULATIVA

Ukoliko bismo izdvojili ključne zahtjeve koji proizlaze iz regulativa, s naglaskom na NIS2, to bi bili zahtjevi vezani uz upravljanje rizikom, lancem opreme, incidentima i kontinuitetom poslovanja.

Usporedili smo razine zrelosti navedenih procesa kod organizacija s kojima Diverto surađuje, i to po industrijama:



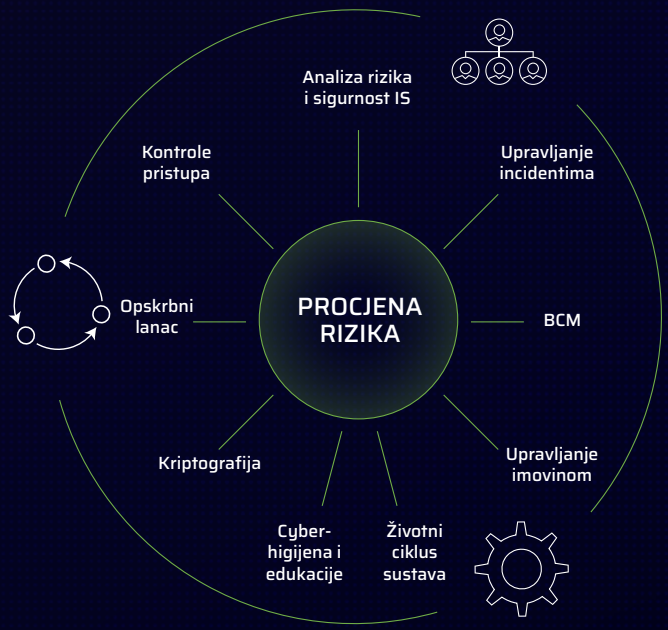
SLIKA 20.
Prosječna razina zrelosti promatranih ključnih područja po industrijama, [Izvor: Diverto]

Općenito, najnižu razinu zrelosti po ovim područjima ima trgovina, dok najvišu imaju digitalne infrastrukture i javne telekomunikacije.

Također, očekivano, područje u kojoj je identificirana najniža razina zrelosti je upravljanje lancem opskrbe.

1. UPRAVLJANJE RIZIKOM

NIS2 definira područja informacijske sigurnosti koja moraju minimalno biti obuhvaćena procjenom rizika i na koja se moraju primijeniti tehničke, operativne i organizacijske mjere. Cilj primjene mjera je osiguranje prevencije ili svođenje utjecaja incidenta na minimum.



SLIKA 21.
Prikaz uspostave procesa upravljanja neplaniranim situacijama, [Izvor: Diverto]

SLIKA 22.
Prikaz uspostavljanja procesa izvještavanja, [Izvor: Diverto]

2. UPRAVLJANJE INCIDENTIMA

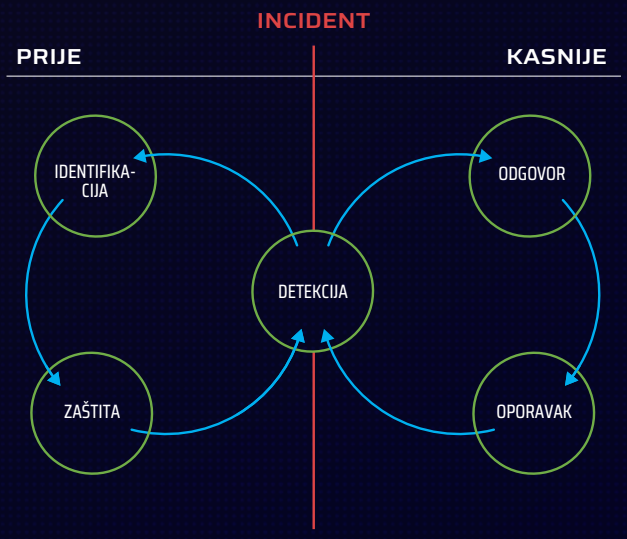
Uspostava procesa koji obuhvaća praćenje, evidentiranje i prijavljivanje incidenata. Ključni i važni subjekti moraju imati uspostavljene procese za brzo izvješćivanje o sigurnosnim incidentima sa znatnim utjecajem na pružanje njihove usluge ili primatelje. NIS2 postavlja posebne rokove obavijesti, kao što je 24-satno „rano upozorenje".

3. UPRAVLJANJE LANCEM OPSKRBE

Najviše bojazni oko postizanja sukladnosti vezano je uz upravljanje lancem opskrbe. Naime, kroz proces upravljanja lancem opskrbe na način kako to zahtijevaju regulative, potrebno je identificirati cjelokupni lanac odgovornosti i nadležnosti. Provjereno i sigurno partnerstvo između pružatelja upravljanih usluga, dobavljača softvera, hardvera i drugih obveznika zakona postaje važnije no ikad.

Osim već poznatih zahtjeva koji su vezani uz upravljanje lancem opskrbe, u obzir će biti potrebno uzeti i:

- specifične ranjivosti
- sveukupnu kvalitetu proizvoda
- razinu informacijske/kibernetičke sigurnosti dobavljača do kraja opskrbnog lanca
- procedure sigurnog razvoja proizvoda/usluge



SLIKA 23.
Prikaz uspostave procesa upravljanja neplaniranim situacijama, [Izvor: Diverto]

4. OTPORNOST I UPRAVLJANJE KONTINUITETOM POSLOVANJA

Uz osnovnu **higijenu informacijske/kibernetičke sigurnosti** koja se odnosi na razinu dobrih navika koje su korisnici informacijskih i kibernetičkih sustava usvojili, kojih se svakodnevno pridržavaju i koje u konačnici pomažu u ublažavanju posljedica potencijalnih incidenata, neizbježno je ne spomenuti upravljanje kontinuitetom poslovanja. Da bi organizacija osigurala otpornost i kontinuitet poslovanja u slučaju nastanka neželjenih događaja, važno je uspostaviti proces upravljanja neplaniranim situacijama prije i nakon nastanka incidenta.

Proveli smo istraživanje u kojem smo ispitali spremnost organizacija na nadolazeće regulative.

PROMOTRIVŠI ORGANIZACIJE KOJE SU SVJESNE I SIGURNE DA ĆE BITI OBVEZNICI NIS2/CRA/ DORA REGULATIVA:

67 % **Na sastancima uprave NE raspravlja o pitanjima informacijske/kibernetičke sigurnosti ili raspravlja samo u slučaju incidenta ili drugog (potencijalnog) problema** vezanog uz informacijsku/ kibernetičku sigurnost

83 % **Smatra da će uspjeti na vrijeme postići sukladnost** sa zahtjevima navedenih regulativa.

43 % **Nema ili ne zna ima li uspostavljen sustav upravljanja** informacijskom/kibernetičkom sigurnošću (ISMS/CSMS)

63 % **Smatra da je ZKS dobar** i da pokriva ključna područja kibernetičke sigurnosti nužna za funkcioniranje države

30 % **Nema definirane i uvježbane načine odgovora na incidente.**

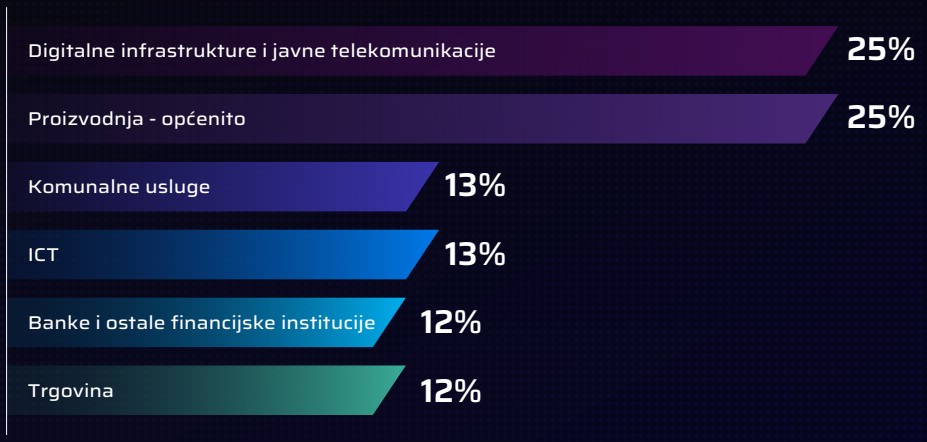
06

POKAZATELJI

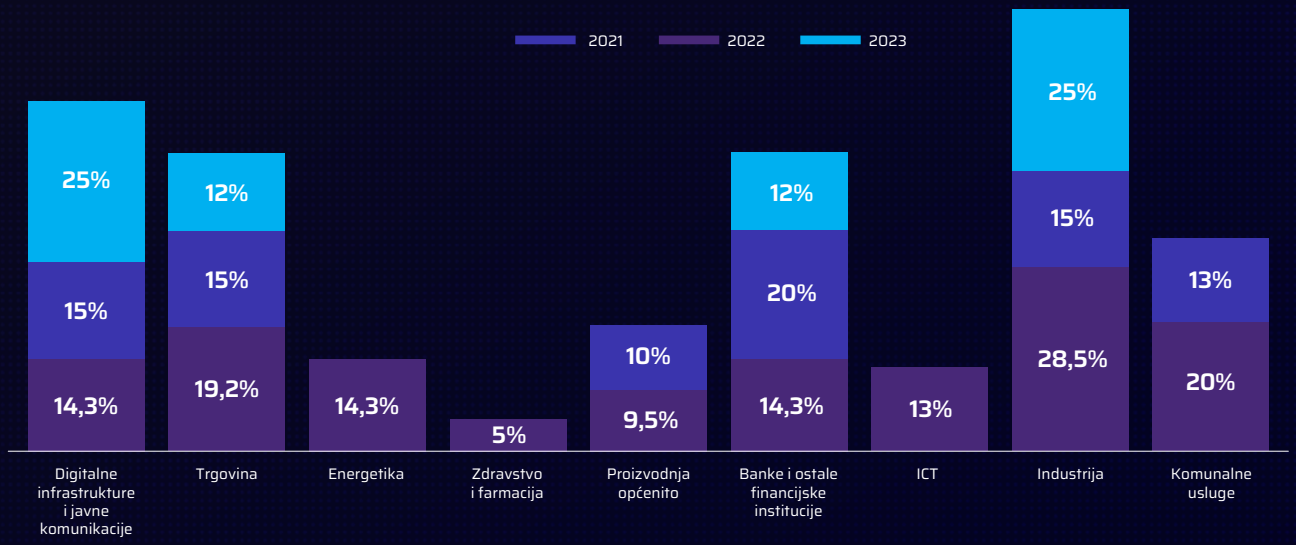
6.1. INCIDENTI

Diverto posjeduje dugogodišnje iskustvo u upravljanju incidentima u području informacijske i kibernetičke sigurnosti. Značajne incidente definiramo kao događaje u kojima je napadač svojim djelovanjem značajno utjecao na povjerljivost, integritet ili dostupnost informacija, kao i na poslovne procese, financije i ugled organizacije. Organizacije obično samostalno razvijaju kriterije kako bi odredile što smatraju značajnim, uzimajući u obzir svoje specifične potrebe i rizike ovisno o industriji.

NAPOMENA: tijekom 2023 godine za klasifikaciju sigurnosnih incidenata prema industrijskom sektoru korišten je GICS® (*The Global Industry Classification Standard*)

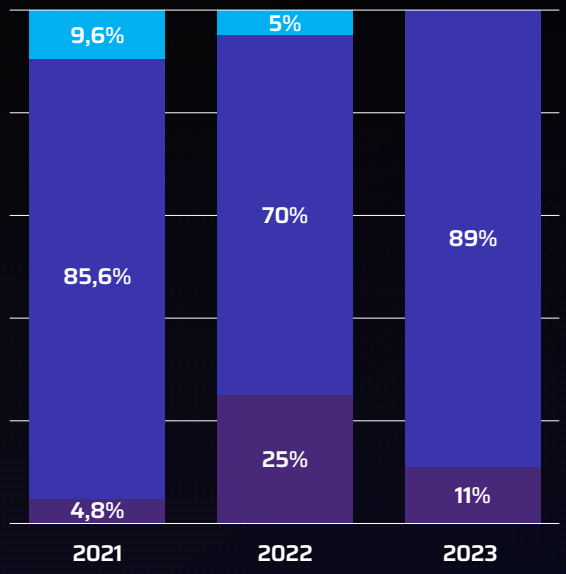


SLIKA 24. *Klasifikacija incidenata tijekom 2023 godine prema industrijskim sektorima, [Izvor: Diverto]*



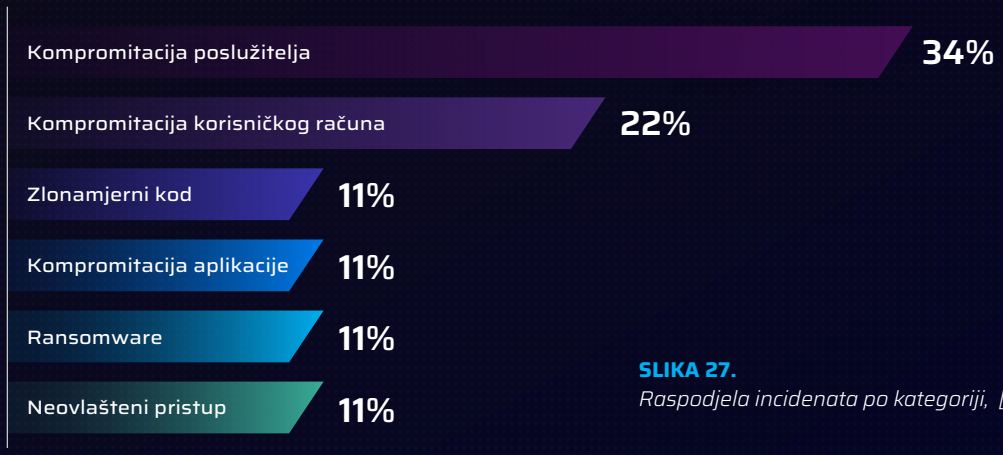
SLIKA 25. *Klasifikacija incidenata tijekom zadnje tri godine prema industrijskim sektorima, [Izvor: Diverto]*

U usporedbi s prethodnom godinom, primijetili smo porast utjecaja vanjskih napadačkih aktivnosti. Vanjski napadi, koji uključuju različite tehnike, alate i strategije, postaju sve izazovniji i donose dodatne izazove u očuvanju sigurnosti informacija i kibernetičke stabilnosti organizacije. Dinamika utjecaja vanjskih napadača naglašava potrebu za stalnim praćenjem i poboljšanjem sigurnosnih postupaka koji pomažu u smanjenju rizika od sigurnosnih incidenata i pravovremenih otkrivanja incidenata.



SLIKA 26.
Incidenti prema djelovanju napadača, [Izvor: Diverto]

Tijekom protekle godine, u sklopu pružanja usluge SOC-a i upravljanja incidentima, naša organizacija suočila se s raznolikim sigurnosnim izazovima koji su se odrazili kroz više kategorija sigurnosnih incidenata. Ističemo kategoriju incidenata „Kompromitacija poslužitelja“ koja se posebno istaknula zbog iskorištavanja sigurnosnih propusta u javno dostupnim servisima.



SLIKA 27.
Raspodjela incidenata po kategoriji, [Izvor: Diverto]

Svjesni globalne prirode sigurnosnih prijetnji, u ovom godišnjem izvještaju želimo skrenuti pažnju na značaj sigurnosti informacija i istaknuti nekoliko primjera javno dostupnih informacija o sigurnosnim incidentima u Hrvatskoj i našem susjedstvu tijekom 2023 godine, uključujući i one u kojima Diverto nije bio aktivno uključen u rješavanje incidenta.

- Travanj 2023. - Hakiran instagram profil Grada Dubrovnika i nije postojala kontrola nad objavama na profilu.
- Lipanj 2023. - Hrvatski autoklub pretrpio je hakerski napad na svoje računalne poslužitelje, što je imalo utjecaj na rad mrežnih stranica i odvijanje internetskih usluga, poput informiranja o stanju u cestovnom prometu.
- Rujan 2023. - Hakiran Facebook profil kultne splitske slastičarnice, obrisane stare objave, postavljene lažne objave.
- Listopad 2023. - Hakerski napad blokirao rad državne tvrtke Hrvatske vode.
- Studeni 2023. - Problemi u radu *WhatsApp* aplikacije na mobitelima povezani sa sigurnosnim sustavom operatera koji kontrolira dolazne SMS kodove.
- Studeni 2023. - Holding Slovenske Elektrane pretrpio najveći kibernetički napad u povijesti Slovenije.
- Prosinac 2023. - Hakeri napali Elektroprivredu Srbije.

Aktivnim sudjelovanjem na kibernetičkim incidentima tijekom 2023. godine, identificirali smo nekoliko nedostataka u organizacijama koje su postale mete napadača. Temeljem naučenih lekcija iz prošle, ali i prethodnih godina, izdvajamo preporuke kojima je moguće značajno ojačati obrambene mehanizme i smanjiti rizik od budućih kibernetičkih napada.

- **Redovito ažuriranje sustava i aplikacija**

  Održavajte redovito ažuriranje operativnih sustava, softvera i aplikacija kako biste ispravili sigurnosne propuste i smanjili rizik od iskorištavanja ranjivosti.
- **Edukacija zaposlenika o sigurnosnim prijetnjama i rizicima**

  Organizirajte edukacije za zaposlenike o kibernetičkim prijetnjama, socijalnom inženjeringu te pravilima sigurnosti na internetu kako biste podigli svijest i smanjili rizik od ljudskih pogrešaka.
- **Implementacija više faktorske autentifikacije (MFA/2FA)**

  Aktivirajte višefaktorsku autentifikaciju za pristup važnim sustavima i računima, čime ćete povećati sloj zaštite, čak i u slučaju krađe lozinki.
- **Uspostava SOC/SIEM sustava**

  Implementirajte SOC/SIEM sustav kako biste povezali događaje iz različitih izvora, non-stop pratili sve sigurnosne događaje, otkrili nepravilnosti u stvarnom vremenu i unaprijedili brzinu otkrivanja incidenta.
- **Kvalitetno upravljanje incidentima**

  Razvijte plan brzog odgovora na incidente koji uključuje precizne korake za identifikaciju, izolaciju i rješavanje kibernetičkih prijetnji.

  Implementirajte napredne sustave praćenja i detekcije kako biste brzo identificirali neobične aktivnosti i odgovorili na potencijalne prijetnje prije nego što prouzroče ozbiljnu štetu.
- **Implementirajte Deception sustav**

  Kako bi otežali napadačima razlikovati stvarne sustave od lažnih te im smanjili šansu za uspjeh napada i pravovremeno ih otkrili, postavite lažne resurse i mamce (npr. *Honeypot*) kao dodatni sloj obrane i integrirajte ih u SOC/SIEM.
- **Redovite sigurnosne provjere i testiranja**

  Periodički provodite sigurnosne provjere i testiranja kako biste identificirali slabosti u sustavima i aplikacijama te ih ojačali prije nego što postanu meta napadača.

6.2. ZLONAMJERNI KOD

„Napadači su u 2023. godini zlonamjerni kôd upotrebljavali primarno u financijske svrhe. Zlonamjerni kôd razvijen prije nekoliko godina i dalje se uspješno upotrebljava, ali jasno je vidljivo da se napadači konstantno pokušavaju prilagoditi novim trendovima i tehnologijama s ciljem što težeg otkrivanja i veće uspješnosti napada."

IGOR KRAMARIĆ
Analitičar kibernetičkih prijetnji

GLAVNE PRIJETNJE:

1. **INFOSTEALERI:**

- prema zapažanjima Diverta infostealeri su najčešća vrsta zlonamjernog programa na našim prostorima,no naglašavamo kako je to i u skladu sa zapažanjima globalnih trendova
- cilj infostealera je krađa osjetljivih informacija, a najčešće upotrijebljeni infostealeri prema našim zapažanjima uključuju ***RedLine, Amadey, Raccoon, ViperSoftX*** i daleko najpopularniji ***AgentTesla***
- način zaraze: *phishing* poruke s priloženim dokumentima (primarni su vektor zaraze) i *drive-by-download* (lažno ažuriranje Internetskog pretraživača s ciljem preuzimanja zlonamjernog programa)
- zanimljivo je da smo uočili da se određene poveznice skidaju s lanca blokova, što ukazuje na konstantnu evoluciju napadača i njihovu potragu za novim načinima distribucije zlonamjernog koda kako bi povećali uspjeh napada i otežali otkrivanje.

2. **COINMINERI:**

zlonamjerni program koji se koristi resursima zaraženih računala za rudarenje kriptovaluta za korist napadača.

3. **RASPBERRY ROBIN:**

uzlazna prijetnja u Hrvatskoj, a i globalno, koja se najčešće širi putem USB memorije i služi za dostavljanje ostalih zlonamjernih datoteka poput *Clop* i *LockBit* ucjenjivačkog softvera (*ransomware*). Ovaj zlonamjerni program povezuje se s napadačkim skupinama kao što su *Evil Corp* i *Whisper Spider*.

GLAVNI MOTIV NAPADAČA:

I u 2023. nastavlja se trend glavnog motiva napadača: FINANCIJSKI.

NAJČEŠĆE METE PODATAKA ZA INFOSTEALERE:


upisani znakovi na tipkovnici


uzimanje snimaka zaslona


podaci o kreditnim karticama


vjerodajnice različitih aplikacija


kolačići i povijest pretraživanja internetskih pretraživača


elektronička pošta i kontakti {pošta, omotnica}


novčanik kriptovaluta

4. **UCJENJIVAČKI SOFTVER (*RANSOMWARE*):**

- **dok se broj pokušaja i uspješnih napada ucjenjivačkim softverom (*ransomware*) povećao na globalnoj razini, Diverto je zabilježio značajan pad uspješnih šifriranja podataka u Hrvatskoj u 2023. godini**
- pad se pripisuje povećanoj svijesti korisnika i organizacija o prijetnjama ucjenjivačkog softvera (*ransomware*) te poboljšanim mjerama sigurnosti
- veliki broj napada rezultat je javnog otkrivanja kôda nekih ucjenjivačkih softvera (*ransomwarea)*, što je dovelo do povećanja varijanti i činjenice da sada i manje tehnički napadači mogu izvoditi napade
- ističu se trendovi povećanja iskorištavanja ranjivosti nultog dana (*0-day*) (*MOVEit* napad koji je *Clop Ransomware* iskoristio da zarazi veliki broj računala) i taktike „višestruke iznude" (krađa podataka uz šifriranje).

SLIKA 28.
Prikaz vrsta iznuda, [Izvor: Diverto]

ZAKLJUČAK:

Zlonamjerni kôd iz godine u godinu je u porastu, a tako se nastavilo i u 2023. godini. Napadači se i dalje aktivno koriste starim i provjerenim tehnikama koje su uspješne, ali se i konstantno prilagođavaju novim tehnologijama i trendovima s ciljem veće uspješnosti napada. Sve to ukazuje na potrebu za stalnom budnošću i proaktivnim mjerama zaštite od sve sofisticiranijih i raznolikijih prijetnji.

ISKORIŠTAVANJE SLABOSTI:

Broj otkrivenih ranjivosti svake je godine sve veći i iako je u ovoj godini bilo nekoliko globalno velikih incidenata vezanih uz napade nultog dana (*0-day*) napade, Diverto je na svojem skupu podataka identificirao da su stare ranjivosti i dalje najpopularnije: *Log4Shell* (CVE-2021-44228), *ProxyNotShell* (CVE-2022-41040, CVE-2022-41082) i *Equation Editor* (CVE-2017-11882).

6.3. PHISHING

Malo toga se teško sa sigurnošću može potvrditi, ali rast broja *phishing* poruka iz godine u godinu zaista polako ulazi u tu kategoriju. Iz godine u godinu govorimo o rekordima, i 2023. godina nas, nažalost, nije iznenadila.

U 2023. godini smo poslali

9824

phishing poruka prema

4683

jedinstvena korisnika.

Od 2018. godine pa sve do 2022. godine imali smo konstantan trend pada postotka korisnika koji nisu prepoznali *phishing* poruku.

Međutim, u 2023. godini taj je broj značajno porastao za 9 % u odnosu na 2022. godinu i iznosi

30 %

Prvotno zabrinjavajuća, ova razlika izvire iz činjenice kako je u 2023. godini čak

73 %

korisnika po prvi put testirano.

Ohrabrujuće je da sve više organizacija prepoznaje potrebu provjere i edukacije zaposlenih o ovoj temi.

SLIKA 29.
Postotak korisnika koji nisu prepoznali phishing poruku u odnosu na broj poslanih poruka, [Izvor: Diverto]

SIGURNOST JE PROCES, A NE STANJE!

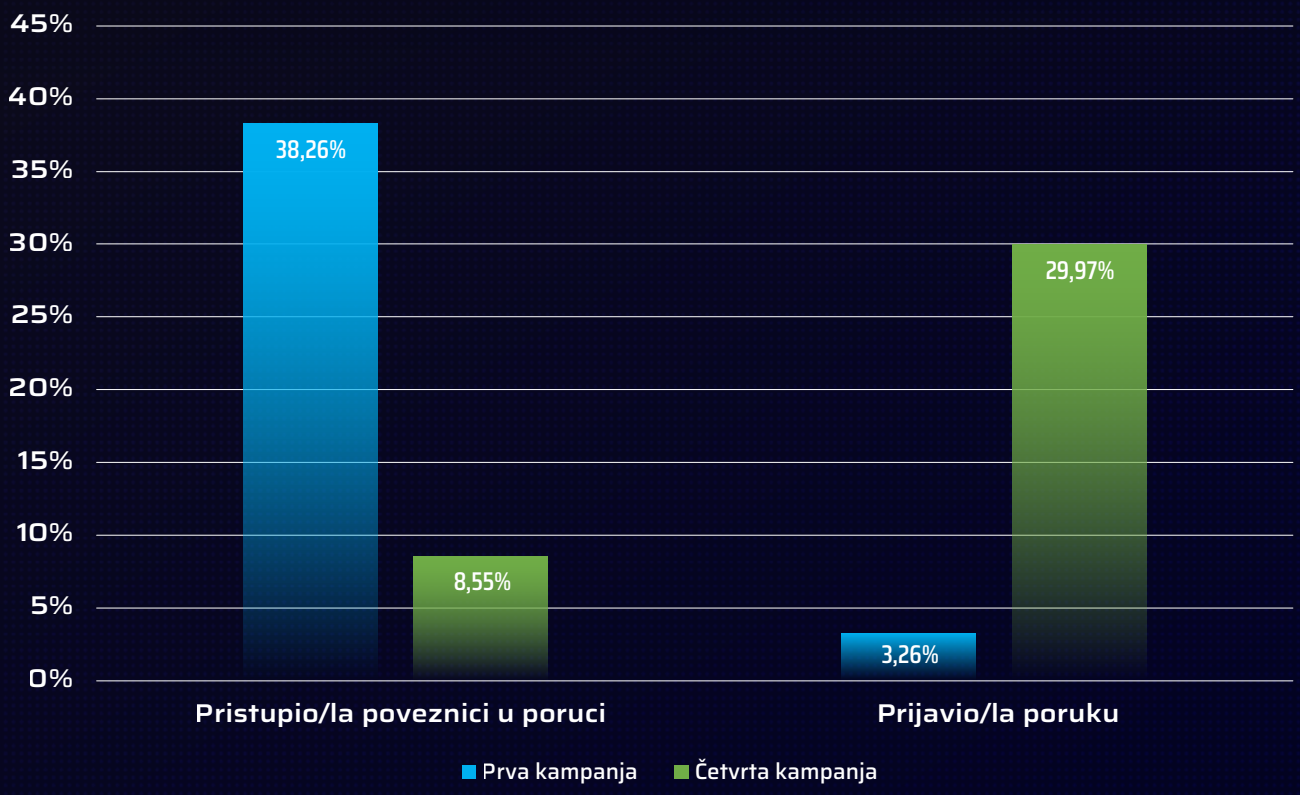
Od više organizacija koje smo na različite načine testirali na otpornost na napade koji koriste socijalni inženjering, kao primjer dobre prakse izdvajamo jednu s kojom smo provodili cjelogodišnji program testiranja i edukacija zaposlenih.

Phish'd studija slučaja:

Metodologija: 1 organizacija s više od tisuću zaposlenika s uredima diljem Hrvatske, 4 kampanje *phishing* testiranja tijekom perioda od 1 godine, svi zaposlenici i predlošci lake težine prepoznavanja. Svi zaposlenici organizacije su educirani o opasnostima i načinima prepoznavanja phishing poruka.

REZULTATI:

- od 1. do 4. kampanje postotak korisnika koji ne prepoznaju *phishing* poruku pao je s 38 % na 9 %,
- od 1. do 4. kampanje postotak korisnika koji su ispravno prepoznali i prijavili *phishing* poruku narastao je s 3 % do 30 %

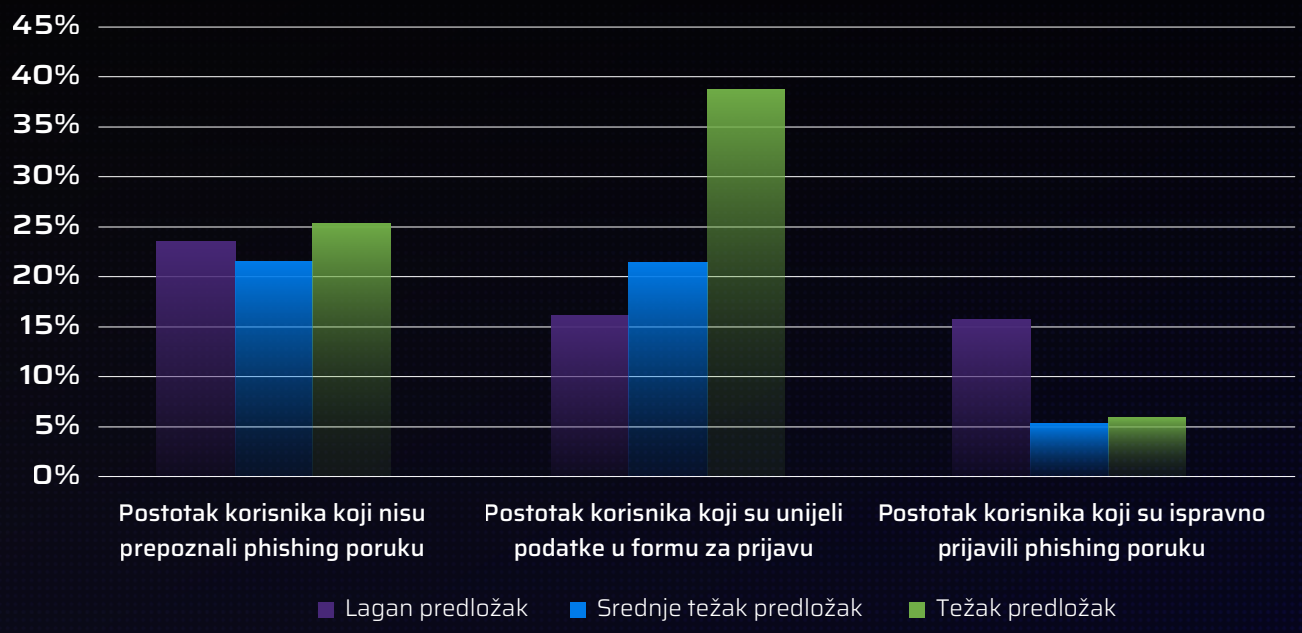


SLIKA 30. *Prikaz phishing studije/kampanje, [Izvor: Diverto]*

ŠTO NAM DODATNO GOVORE KONKRETNI PODACI IZ 2023. GODINE

Phishing testiranje: utjecaj složenosti poruke

Sagledamo li podatke na cjelokupnoj testiranoj populaciji te podijelimo li ih na temelju težine upotrebljenog predloška (lažne poruke), rezultati traže dodatno pojašnjenje.



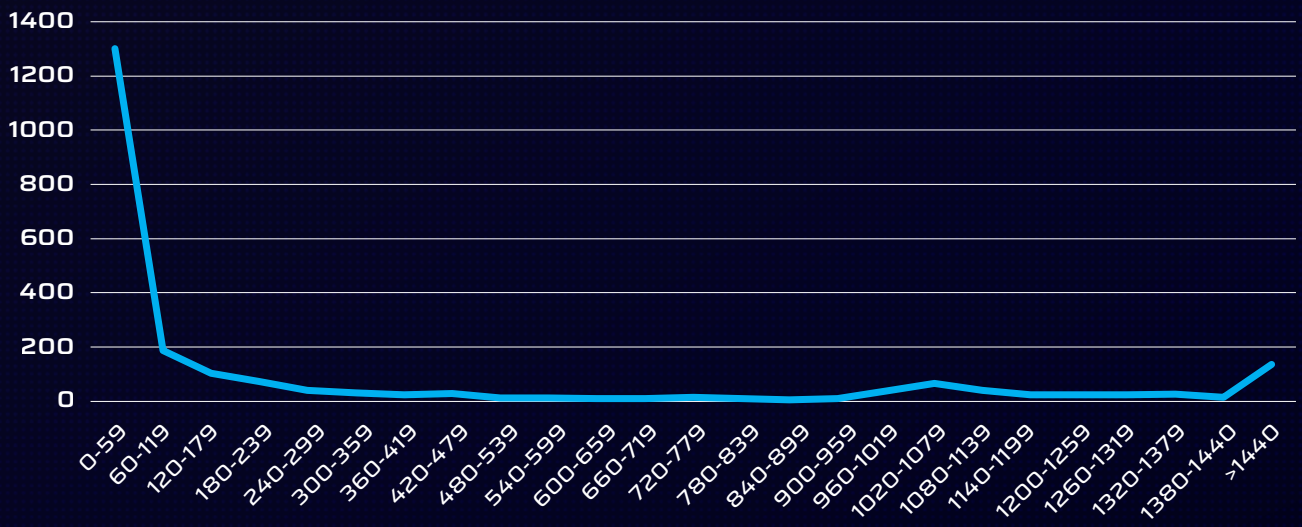
SLIKA 31. *Rezultati testiranja u 2023. godini s obzirom na težinu prepoznavanja upotrebljenog predloška, [Izvor: Diverto]*

Podaci pokazuju da složenost *phishing* poruke ne utječe značajno na broj korisnika koji je nisu prepoznali. Međutim, postoje neke nijanse koje valja uzeti u obzir:

- **organizacije koje tek kreću s testiranjem *phishinga:*** preporučuje se korištenje jednostavnih predložaka koji se lako prepoznaju
- **organizacije s iskustvom u testiranju *phishinga:*** traže se složeniji predlošci koji se što više približavaju onima koje koriste zlonamjerni akteri
- **zrele organizacije s uspostavljenim programima edukacije:** imaju veći postotak korisnika koji ispravno prijavljuju *phishing* poruke, čak i one složenije. To je rezultat kontinuiranog rada na osvješćivanju korisnika i kombiniranja testiranja s kvalitetnim edukacijama.

Kontinuirana edukacija i usmjereno testiranje korištenjem krojenim *phishing* porukama ključni su faktori u jačanju otpornosti na napade. Zrele organizacije kombiniraju složene simulacije napada s edukacijama kako bi bile spremne za najsofisticiranije napade.

Sagledamo li ponašanje korisnika koji ne uspijevaju prepoznati *phishing* poruke, ogromna većina njih poruci pristupa **unutar sat vremena od primitka.**



SLIKA 32 . *Podaci o prepoznavanju phishing poruke prema broju minuta koje su prošle od inicijalnog primitka poruke, [Izvor: Diverto]*

- **Prikupljanje podataka dulje od 48 sati ne daje značajne dodatne rezultate.**
- **Najvažnije aktivnosti se odvijaju u „zlatnom satu“ nakon testiranja.**
- **Analiza i edukacija moraju biti brze i usklađene s rezultatima testiranja.**

CILJ
iskoristiti „pomutnju" i formirati dobre navike kod korisnika.

BRZA I JASNA REAKCIJA NA *PHISHING* PORUKE KLJUČNA JE ZA POBOLJŠANJE OTPORNOSTI NA NAPADE!

Razlog tome je što postoji značajan broj korisnika koji ponavljaju iste greške u testiranjima.

Od
4683
jedinstvena korisnika testirana 2023. godine,

2089
je bilo metom napada dva ili više puta.

Štoviše,
11,15 %
tih korisnika u više od

50 %
slučajeva nije moglo prepoznati *phishing* poruku.

Dakle, više od 10 % korisnika ponavlja greške, a kampanje s jednostavnim predlošcima rijetko postižu dobre rezultate, čak i u organizacijama s visokom razinom zrelosti.

Na temelju ovih zaključaka, prag ispod kojeg rijetko koja kampanja ide je 10 % ponavljača.

PAMETNA EDUKACIJA ZA BOLJU ZAŠTITU OD PHISHINGA

Jesmo li možda u pokušaju da podignemo razinu otpornosti organizacija na napade koji se koriste socijalnim inženjeringom bili skloniji upotrijebiti batinu nego mrkvu?

Korištenje straha bila je i ostala omiljena alternativa dugim i zamornim prezentacijama, nagrađivanje prijava umjesto kažnjavanja onih koji su se „upecali“ djeluje kao utopija, a mnogima od nas ponekad i nije jasno što i kako napraviti u trenutku kada korisnik ne prepozna da je riječ o phishing poruci čak i kada ona dolazi s adrese *fraud@whytrustme.net*.

Ne možemo prestati testirati, ali svaki test mora dati neku dodanu vrijednost pored temeljnih postotaka koji ne otkrivaju potpunu sliku otpornosti organizacije. Bilo da se jasno definiraju bolne točke ili otkriju navike korisnika u interakciji s *phishing* porukom, rezultat svakog testiranja mora biti iskorišten da smanji prirodni jaz između djelatnika zaduženih za sigurnost i korisnika.

Kako bismo to postigli u testiranjima koje provodimo, u suradnji s klijentom prikupljamo što više informacija kako bi nam pomogle dati jasniju sliku zrelosti organizacije. Naša metodologija omogućava nam usporedbu kampanja različitih težina, a u sklopu testiranja prikupljamo podatke o prijavama, segmentiramo predloške prema različitim kategorijama korisnika te uspostavljamo programe testiranja kroz dulji period. Također, razvili smo i sustav edukacija koji obrađuje specifične scenarije koje smo upotrijebili u testiranju kako bismo korisniku na pristupačan način ukazali na pogreške.

Izazovi u 2024. godini

- tradicionalne metode edukacije ne prate složenost i broj *phishing* poruka
- generativni modeli (AI) olakšavaju i automatiziraju pisanje naprednih poruka uvelike čineći jezičnu barijeru lako premostivom zaprekom
- multi vektorski napadi koji upotrebljavaju više metoda socijalnog inženjeringa sve su rasprostranjeniji
- porast broja različitih metoda napada koje do sada nisu bile u velikoj mjeri zastupljene – *smishing, vishing, QRishing*

Rješenje

- intenzivnije testiranje korisnika u svrhu podizanja svijesti i razvoja kritičkog razmišljanja
- razvijanje odnosa povjerenja između zaposlenika i službe koja skrbi o sigurnosti
- intenzivnija suradnja službe koja skrbi o sigurnosti sa službama upravljanja ljudskim potencijalima
- ugradnja vrijednosti kibernetičke higijene u organizacijsku kulturu
- pozitivno isticanje pojedinaca koji prijavljuju *phishing* poruke uz uspostavu sustava nagrađivanja
- automatizirano označavanje poruka poput onih koje dolaze van domene ili poruka pošiljatelja s kojima se prije nije komuniciralo
- implementacija sigurnosnih mehanizama kao što je digitalni potpis i šifriranje poruka te uvođenje obaveznog korištenja višefaktorskom autentifikacijom
- upotreba generativnih modela (AI) za pripremu personaliziranih edukacijskih programa krojenih prema potrebama svakog zaposlenika.

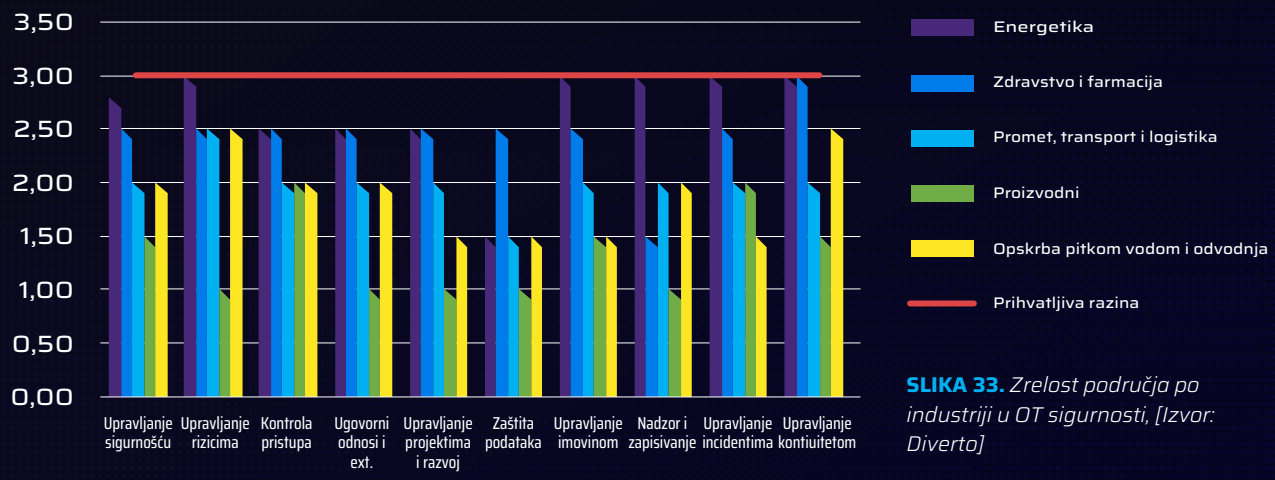
KLJUČ ZA POBOLJŠANJE OTPORNOSTI
na *phishing* napade je neophodna suradnja odjela za sigurnost i ostalih korisnika, uz brzu i jasnu edukaciju temeljenu na rezultatima testiranja.

6.4. OT TRENDOVI

Nedavni napadi na operatore kritičnih infrastruktura u susjednim zemljama brutalno su nas podsjetili na ranjivost i potencijalne posljedice koje kibernetički incidenti mogu imati na takve infrastrukture. U svjetlu tih događanja i toga da je u 2023. godini izrađen prijedlog novog Zakona o kibernetičkoj sigurnosti (ZKS), kibernetička sigurnost postaje još značajniji izazov za većinu vlasnika OT sustava. Novi ZKS je izglasan početkom 2024. godine, a NIS2 i novi ZKS otvaraju put predviđanju kojeg je prije nekoliko godina dao Gartner[4], odnosno da će se do 2024. godine 75 % najvišeg poslovodstva suočiti s osobnom odgovornošću za kibernetičke incidente.

OCJENA ZRELOSTI KIBERNETIČKE SIGURNOSTI OT SUSTAVA U 2023. GODINI:

Diverto je i kroz 2023. godinu nastavio suradnju s organizacijama i industrijama koje sve više ovise o kibernetički povezanim OT sustavima. U nastavku vam donosimo ocjenu zrelosti relevantnih područja kibernetičke sigurnosti OT sustava po industrijama:



SLIKA 33. *Zrelost područja po industriji u OT sigurnosti, [Izvor: Diverto]*

U odnosu na 2022. godinu, sektor energetike podigao je razinu zrelosti svih područja za 0,5 što je veliki uspjeh i posljedica uspješne implementacije prvih upravljanih OT SOC usluga u Republici Hrvatskoj.

> **Preko 50 % inicijalno pregledanih sustava ne primjenjuje dobre prakse mrežne segmentacije i implementacije zona i vodova koji bi značajno ograničili posljedice potencijalnog napada.**

Posljedice su to dugogodišnje nedovoljne suradnje i razumijevanja šire slike od strane IT i OT osoblja. Za učinkovitu i djelotvornu obranu od napada osim porasta potražnje za konzultantskim uslugama provođenja Gap analiza naspram ZKS-a i dobrih praksi poput IEC 62443 2-1, 3-2 i 3-3, procjena rizika, te uslugama upravljanog OT SOC-a, predviđamo pojačanu potražnju za sigurnosnim uslugama poput: **testiranja ranjivosti, penetracijskih testiranja i testiranja segmentacije mreže.**

TRENDOVI I AKTUALNOSTI

UTRKA S VREMENOM: ZKS i OT sustavi

- Novi ZKS - izazov za vlasnike i operatere OT sustava kod određivanja prikladnih protumjera za otklanjanje kibernetičkih rizika.

[4] Gartner: cyber-physical systems,
https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

- Četvrtina ispitanih smatra da je novi ZKS preopširan i neće biti u mogućnosti riješiti sve zahtjeve.
- „Tradicionalna nesklonost“ vlasnika i operatera OT sustava prihvaćanju tehnoloških rješenja i procesa koji nisu direktno vezani uz upravljanje fizičkim procesom - prethodna primjena sigurnosnih rješenja u OT okruženjima često je za posljedicu imala probleme.

SLIKA 34. *Percepcija složenosti novog ZKS-a, [Izvor: Diverto]*

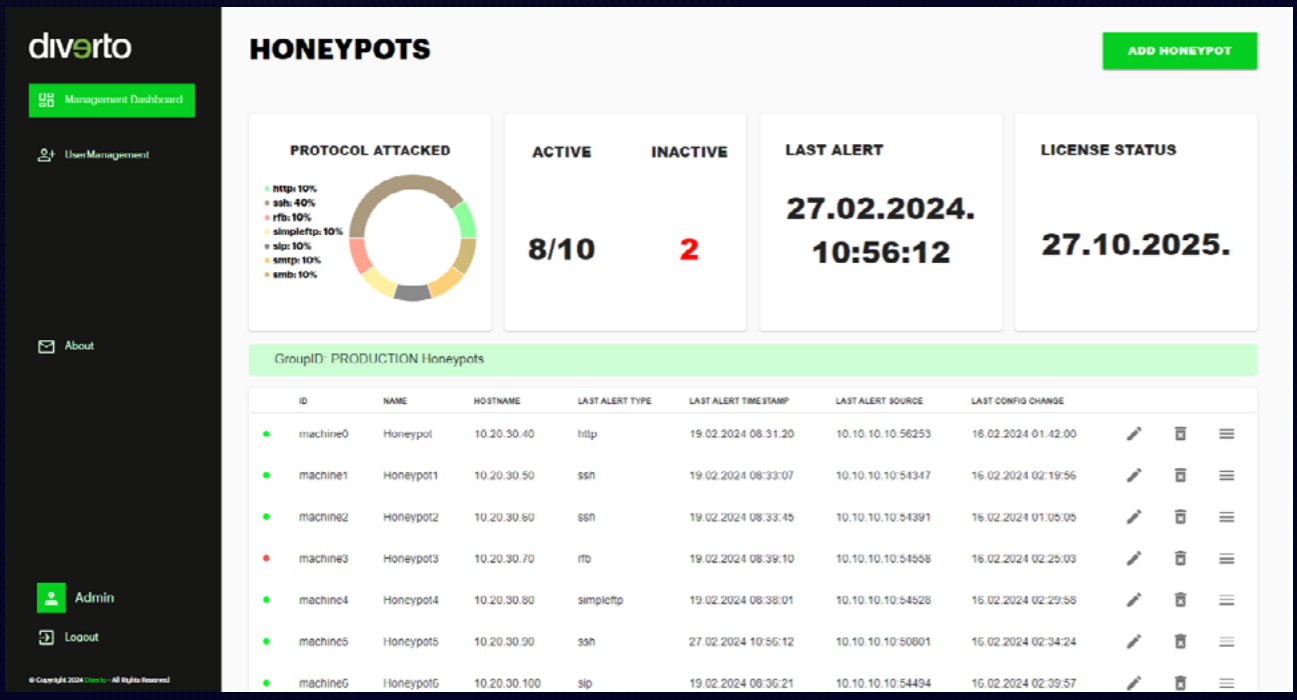
- Danas na tržištu postoji značajan broj proizvođača rješenja specifičnih za OT, a nesklonost je i dalje prisutna.
- Vrijeme za implementaciju protumjera kibernetičke sigurnosti u OT sustave kod kojih je visoka raspoloživost imperativ iznimno je ograničeno i dragocjeno.
- Propust pri implementaciji protumjera može značiti čekanje do sljedeće planirane neaktivnosti, što može biti i do godinu dana kasnije.

ODGOVORNOST POSLOVODSTVA: KIBERNETIČKI RIZICI

- Poslovodstva se suočavaju s novim obvezama i potencijalnim sankcijama.
- Nedostatak svijesti o rizicima kod poslovodstva – NIS2 regulativa naglašava odgovornost poslovodstva za upravljanje kibernetičkim rizicima.
- **Poslovodstvo mora preuzeti odgovornost** za kibernetičku sigurnost OT sustava i proaktivno pristupiti implementaciji prikladnih mjera zaštite.

OBMANA KAO OBRANA: ZAVARAJ NAPADAČA, ZAŠTITI OT

- Sustavi utemeljeni na tehnologijama za obmanjivanje/zavaravanje (engl. *deception technology*) napadača u OT sustavima pružaju niz prednosti.



SLIKA 35. *Izgled upravljačke strane tipične tehnologije zavaravanja, [Izvor: Diverto]*

- Pravilno postavljen sustav otkriva napade i „kupuje" obrambenom timu vrijeme za zaštitu važnijih dijelova OT infrastrukture te „troši“ vrijeme napadaču.
- Služi i kao dodatna detekcijska sigurnosna kontrola ukoliko drugi sustavi i kontrole zakažu.
- Uspješnost implementacije sustava zavisi od pozicioniranja unutar procesne mreže, uzimajući u obzir particioniranje na zone i vodove te prepoznavanje zona i komunikacijskih puteva s najvišim rizikom od napada.
- Više od 90 % alarma primljenih sa sustava za obmanjivanje/zavaravanje u OT SOC-u dovelo je do istraga koje su ukazale na nedopuštene i nenajavljene aktivnosti na OT sustavima korisnika.

Koristeći se tehnologijama za obmanjivanje/zavaravanje, znatno smo unaprijedili OT SOC, uspostavljajući slojevitu obranu ključnu za sučeljavanje s kibernetičkim prijetnjama u složenom digitalnom okruženju. Instalacija više od 30 takvih sustava prošle godine u različitim okruženjima pokazala je lakoću implementacije i minimalne zahtjeve za održavanje, te predviđamo njihovu rastuću popularnost.

SPOSOBNOST REAKCIJE NA INCIDENTE

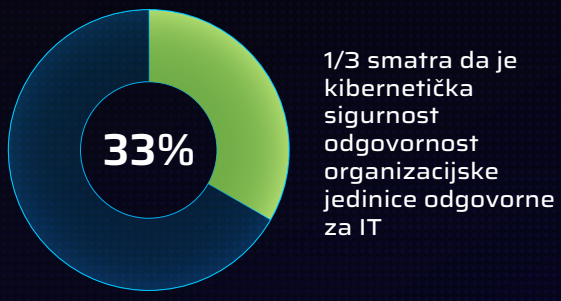
- Sposobnost brzog i učinkovitog odgovora na kibernetičke incidente ključna je za održavanje sigurnosti i stabilnosti OT sustava.
- U OT svijetu još uvijek nedostaje specifičnih znanja i iskustava u prepoznavanju i odgovoru na kibernetičke incidente.
- Manje od četvrtine organizacija posjeduje uvježbane i sposobne timove za odgovor na incidente.
- Neophodno je graditi kapacitete kod vlasnika OT sustava, ali i formirati multidisciplinarne timove za odgovor na incidente, sastavljene od stručnjaka iz industrijske automatizacije, smjenskog osoblja, IKT stručnjaka, dobavljača i ostalog relevantnog osoblja kako bi se ispravno odgovorilo na kibernetičke incidente.

„Iako većina vlasnika i operatora OT sustava smatra da su spremni za prikladan odgovor na kibernetičke incidente (preko 80 %), simulacije i uvježbavanja često otkrivaju složenost i neprimjenjivost njihovih postojećih planova u realnim situacijama. Stoga je ključno razvijati i redovito uvježbavati jednostavne i jasne procedure za reagiranje na incidente i oporavak, kako bi se osigurala efikasna zaštita i brz povratak u normalno stanje.”

MARIO BLAŽEVIĆ
Voditelj OT usluga

NEDOSTATAK OSOBLJA ZA KIBERNETIČKU SIGURNOST U OT-u

- Kao i na globalnom tržištu, osoblja za kibernetičku sigurnost u OT-u nedostaje, a sve više vlasnika i operatora OT sustava traže pomoć vanjskih suradnika kroz konzultantske i /ili upravljane sigurnosne usluge.
- Javne tvrtke sa striktno hijerarhijskim ustrojem imaju izazov kod prepoznavanja ključne važnosti upravljanja kibernetičkom sigurnosti za cjelokupno poslovanje i, posljedično, teško mogu privući prikladnu radnu snagu.
- ZKS donosi zahtjeve za standardizacijom, akreditacijom i nadzorom pružatelja upravljanih usluga kibernetičke sigurnosti, što će vlasnicima i operatorima OT sustava pružiti veće povjerenje u eksternalizaciju tih usluga - olakšavanje suradnje i osiguranje bolje zaštite kritične infrastrukture.
- Više od jedne trećine ispitanih organizacija smatra da je kibernetička sigurnost odgovornost organizacijskih jedinica odgovornih za IT.



SLIKA 36. *Percepcija odgovornosti za kibernetičku sigurnost, [Izvor: Diverto]*

OT IMOVINA: IZAZOVI „VIDLJIVOSTI“

- Iscrpljujući procesi i postupci ručne gradnje „inventara“ OT sustava (početci upravljanja imovinom) s upitnim rezultatima.
- Automatizacija procesa upravljanja OT imovinom –„vidljivost“ OT imovine u tehničkim rješenjima najčešće nije zadovoljavajuća (u početku otkriva oko 30 % „ručno“ identificirane imovine).
- Poboljšanja „vidljivosti“ imovine mogu se postići optimizacijom mrežne infrastrukture i omogućavanjem zrcaljenja prometa na prikladnim lokacijama (često nije izvedivo zbog zastarjele opreme).
- Za svu imovinu koju nije moguće imati pod automatskim nadzorom potrebno je razviti i implementirati odgovarajuće kompenzacijske sigurnosne mjere.

OBAVJEŠTAJNI PODACI O PRIJETNJAMA (*THREAT INTELLIGENCE*) U OT-u

- Obavještajni podaci o kibernetičkim prijetnjama (*cyber threat intelligence*) ključni su za proaktivnu reakciju na prijetnje i zaštitu organizacija od kibernetičkih napada
- Uspostava programa obavještajnih podataka o prijetnjama (*threat intelligence*) za OT sustave je izazov zbog specifičnih ranjivosti i potrebe za detaljnim znanjem za iskorištavanje tih ranjivosti
- 75 % ispitanih organizacija oslanja se na informacije proizvođača/integratora koje često ne mogu ispravno interpretirati.
- Nedostatak stručnjaka za primjenu obavještajnih podataka o prijetnjama (*threat intelligence*) otežava proaktivnu i na stvarnim prijetnjama utemeljenu zaštitu kritične infrastrukture.

ŽIVOTNI CIKLUS OBAVJEŠTAJNIH PODATAKA O CYBER PRIJETNJAMA

SLIKA 37. *Životni ciklus obavještajnih podataka o kibernetičkim prijetnjama, [Izvor: Diverto]*

INTEGRATORI OT RJEŠENJA SVE ČEŠĆE NUDE I RJEŠENJA ZA KIBERNETIČKU SIGURNOST

- Partnerstva između proizvođača OT sustava i proizvođača rješenja za kibernetičku sigurnost za posljedicu imaju sve širu ponudu „ekskluzivnih, *all in one*" rješenja - rješenja koja pasivno analiziraju mrežni promet i otkrivaju anomalije i nedozvoljene aktivnosti.
- „Lažni" osjećaj sigurnosti kod vlasnika i operatora OT sustava oslanjanjem samo na tehnološke sustave bez sveobuhvatnog pristupa i prikladne edukacije osoblja koje nadzire sigurnosna rješenja.
- Zbog nedostatka osoblja i potrebe za automatizacijom, rješenja s aktivnim komponentama koje će preventivno djelovati i upravljati sigurnosnim aktivnostima unutar procesnih mreža su logičan sljedeći korak, a napredak tehnologije umjetne inteligencije (AI) mogao bi dodatno ubrzati ovaj proces, pružajući napredniju analizu i odgovor na prijetnje, ali i rizik od neprikladne implementacije i reakcije automatiziranih sustava.

„Iako se čini najjednostavnije i najbrže, oslanjanje isključivo na tehnološka rješenja bez sustavnog pristupa i odgovarajuće edukacije pogonskih stručnjaka može biti zavaravajuće. Sveobuhvatan pristup kibernetičkoj sigurnosti koji kombinira tehnološka rješenja, edukaciju, redovito praćenje i odgovor na incidente ključan je za pravilno upravljanje kibernetičkim rizicima u OT sustavima."

ANDRIJA GRGIĆ
Voditelj OT rješenja

6.5. DevSecOps

Razvoj sigurnog softvera postaje sve važnija tema s obzirom na dinamično okruženje tehnološkog razvoja koje obuhvaća mnogobrojne tehnologije i često pati od nedostatka standardizacije.

Evolucija razvojnih timova i prelazak na *DevOps* filozofiju dovela je do ubrzanja razvojnog ciklusa softvera i poboljšanja efikasnosti timova. Međutim, *DevOps* timovi se suočavaju s izazovima poput nerazumnih rokova isporuke, „impedancije" između *Developmenta* i *Operationsa* kao i nedovoljne svijesti o sigurnosnim ranjivostima. Neprikladno svladavanje tih izazova dovodi do softvera koji nije razvijen prema principima „*security by design*" i „*security by default*". Okviri dobrih praksi, a sve češće i regulatori (koji se pozivaju na dobre prakse) naglašavaju da integracija sigurnosti u životni ciklus razvoja softvera omogućava ranu identifikaciju i ublažavanje ranjivosti i prijetnji. Tragom dobrih praksi, *DevSecOps* proširuje *DevOps* filozofiju uključivanjem sigurnosnih praksi direktno u ciklus razvoja softvera, osiguravajući da sigurnost postane integralni dio razvoja od samog početka, umjesto da se dodaje kao naknadna provjera.

Tranzicija s tradicionalne *DevOps* filozofije na *DevSecOps* praksu zahtijeva značajne napore i promjene u kulturi timova. Ova tranzicija nije samo tehnička promjena, već zahtijeva cjelovitu posvećenost sigurnosti svih članova tima kao neodvojivom dijelu procesa razvoja.

Kako bi premostili navedene izazove, razvijeni su različiti modeli zrelosti. Model zrelosti predstavlja okvir koji mjeri zrelost procesa ili poslovne funkcije. Zrelost se definira kroz pouzdanost, učinkovitost, stabilnost i sigurnost poslovnog procesa razvoja softvera tijekom životnog ciklusa. Primjenom prikladnog modela zrelosti u razvoju softvera moguće je značajno smanjiti rizik od razvoja ranjivog softvera jer isti pruža način za kvalitativnu evaluaciju trenutne razine zrelosti procesa razvoja i planiranje dugoročnih ciljeva za poboljšanje performansi.

Nedovoljna pažnja prema najboljim praksama sigurnosti tijekom razvojnog ciklusa glavni je uzrok ranjivosti softvera. Stoga su razvijeni modeli zrelosti kako bi organizacijama pomogli definirati trenutnu razinu zrelosti i planirati unapređenje praksi na višu razinu.

MoveIT incident i njemu slični tijekom 2023. godine, zajedno sa sve većim pritiscima regulatora potaknuli su intenzivnije upite i zahtjeve korisnika za analizom postojećih *DevOps* procesa i za implementacijom *DevSecOps* procesa. Kao osnova za procjenu i građenje *DevSecOps* procesa najčešće se upotrebljava *OWASP SAMM* koji kroz 5 poslovnih funkcija daje okvir za izradu sigurnijeg softvera. Usvajanje *SAMM-a* je dugotrajan proces i najbolje je primijeniti fazni pristup kako bi se postigla visoka razina zrelosti u sigurnosti softvera.

Modeli kao što su *OWASP DevSecOps Maturity Model (DSOMM)* i *OWASP Software Assurance Maturity Model (SAMM)* pomažu razvojnim timovima, pružajući strategije i akcijske elemente za mjerenje trenutne razine zrelosti i planiranje njezina poboljšanja.

6.6. USPOREDBA EDR/XDR, MDR I SOC

Kroz dugogodišnji rad s klijentima identificirali smo izazov u uspoređivanju tehnoloških sposobnosti različitih proizvođača i pružatelja usluga koji svoje proizvode i usluge opisuju specifičnim terminologijama, otežavajući objektivnu procjenu prikladnosti pojedinog rješenja. Pri tome se sugerira kako tehnologija sama može u potpunosti zamijeniti potrebu za ljudskim intervencijama u upravljanju sigurnosnim incidentima. Stoga je ključno usvajanje holističkog pristupa koji obuhvaća i tehnologiju i ljudski faktor te poticanje transparentnosti kod proizvođača i podizanja svijesti organizacija o važnosti integracije tehnoloških i ljudskih resursa za visoku razinu sigurnosti. Sljedeći evolutivni korak je kibernetički obrambeni centar (engl. *Cyber Defence Center*), u kojem se sve više stavlja naglasak na proaktivnu obranu. U nastavku vam pružamo tabelarni prikaz koji usporedno prikazuje sposobnosti prethodno navedenih sustava i rješenja. Iako je nezahvalno uspoređivati, prikaz pomaže da jasnije vidite svoje opcije i lakše odaberete najbolje rješenje koje odgovara vašim potrebama. Odluka je uvijek na vama, ovisi o vašim potrebama i mogućnostima, no nikako ne bi smjela biti donešena bez razumijevanja dometa različitih rješenja.

Zabrinjavajući je trend kako neki predstavljaju svoja tehnološka rješenja, poput sustava Endpoint detection and response (EDR) /Extended detection and response (XDR), kao potpune zamjene za Sigurnosno-operativni centar (SOC).

		EDR/XDR	MDR	SOC	CDC
TEHNOLOGIJA	Prikupljanje zapisa s krajnjih točki	●	●	●	●
	Prikupljanje zapisa s poslovnih i mrežnih sustava neovisno o lokaciji sustava – lokalno ili u oblaku (npr.: mail, ERP, mrežni uređaji)	○	●	●	●
	Prikupljanje zapisa iz sigurnosnih alata (DLP, DAM, IPS, UEBA i sl.)	-	○	●	●
	Prikupljanje zapisa iz specifično razvijenih (*custom*) aplikacija	-	-	●	●
	Dugoročna pohrana dnevničkih zapisa	○	○	●	●
	Prosljeđivanje dnevničkih zapisa u treće sustave (SIEM)	○	○	●	●
	Implementacija u oblaku (*cloud*)	●	●	●	●
	Implementacija na lokaciji (*on-premise*)	○	○	●	●
	Neovisna platforma	-	-	●	●
LJUDI	Non-stop nadzor i trijaža	-	●	●	●
	Upravljanje otkrivanjima (ljudski vođeno)	-	○	●	●
	Upravljanje odgovorima (ljudski vođeno)	-	○	●	●
	Upravljanje istragama i incidentima (ljudski vođeno)	-	○	●	●
	Lov na prijetnje (ljudski vođen i *hypothesis-driven*)	-	○	●	●
PROCESI	Osnovne tehničke upute (*Investigation Guide*)	●	●	●	●
	Osnovni procesi suradnje (*workflow*)	-	○	●	●
	Osnovni procesi (*playbook*)	-	○	●	●
	Procesi upravljanja incidentima	-	○	●	●
	Procesi forenzike	-	-	●	●
NAPREDNE USLUGE	Upravljanje izloženošću (*Exposure management*)	○	○	○	●
	Kontinuirano podizanje svijesti o sigurnosti (*Security awareness*)	-	○	○	●
	Upravljanje ranjivostima (VMaaS)	-	○	○	●
	Simulacija napadača (***Purple Teaming***)	-	-	○	●
	Upravljani sustavi zavaravanja (*Managed Deception systems*)	-	-	○	●

- Nije Uključeno / Nema značajku ○ Djelomično podržano ILI dostupno kako add-on tj. dodatna usluga/licenca
● Uključeno / ima značajku

SLIKA 38. *Usporedba EDR/XDR, MDR I SOC [Izvor: Diverto]*

EDR i XDR tehnička rješenja su jedna od komplementarnih tehnologija unutar SOC-a koje povećavaju mogućnosti otkrivanja i olakšavaju rad sigurnosnim analitičarima. *Managed Detection and Response* (MDR) je usluga temeljena na EDR ili XDR tehnologijama koja može organizacijama pomoći da na brz i jednostavan način poboljšaju svoje sigurnosno-operativne sposobnosti u području otkrivanja i odgovora na incident. MDR je posebno koristan organizacijama koje nemaju resurse ili stručnost za vlastiti SOC.

Tehnologije i usluge poput EDR/XDR/MDR pokrivaju samo dio funkcionalnosti SOC-a i zbog svojih ograničenja nisu zamjena za punu SOC uslugu temeljenu na SIEM rješenju sa širim spektrom ljudski vođenih usluga.

„Svjedoci smo porasta broja napada čiji potencijalni utjecaj može dovesti do potpunog zaustavljanja poslovanja zahvaćene organizacije, posebice u slučaju onih koje pružaju kritične usluge. To neizbježno za posljedicu ima ozbiljan poremećaj cijelog poslovanja, a ponekad i poremećaj normalnog života korisnika kritičnih usluga. Smatram kako se ne bi smjelo štedjeti ili pristajati na značajne kompromise prilikom ulaganja u napredne sigurnosne alate i usluge. Iako su EDR/XDR kvalitetni alati, a MDR može biti dobra opcija za manje organizacije koje tek razvijaju svoje sigurnosne kapacitete, ključna i dugoročna investicija na koju bi većina organizacija trebala usredotočiti svoju pažnju i sredstva jest implementacija Sigurnosno-operativnog centra (SOC).”

IVAN IVKOVIĆ
voditelj SOC usluge

6.7. DISTRIBUIRANI NAPADI USKRAĆIVANJEM USLUGE (DDOS)

Napadi distribuiranog uskraćivanja usluge (DDoS) predstavljaju jednu od najjednostavnijih i najčešćih prijetnji u svijetu internetskog prostora. S obzirom na njihovu stalnu prisutnost, želimo podijeliti dodatne pojedinosti o DDoS napadima tijekom 2023. godine.

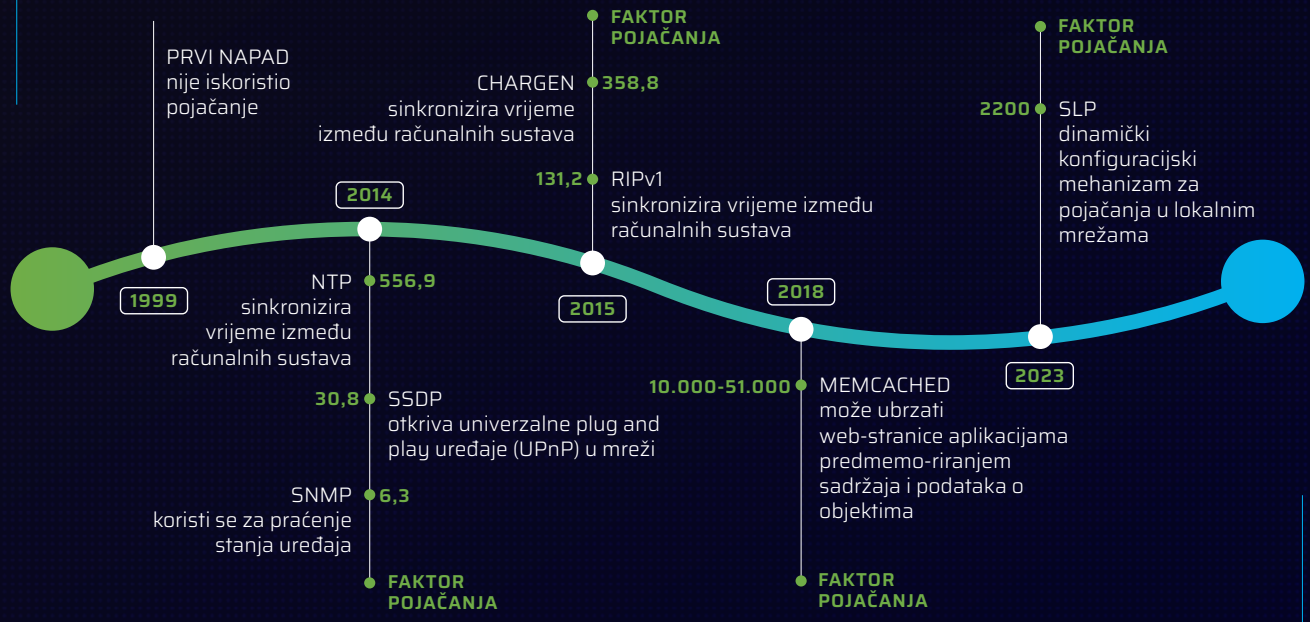
GLOBALNO

2023. godina obilježila je objava novog protokola koji se može upotrijebiti za povećanje DDoS napada sa značajnim faktorom povećanja (i do 2200 puta).

REGIONALNO

2023. godinu obilježilo je prelijevanje geopolitičkog stanja prijetnjama Revil/Killnet grupe za izvršenje DDoS napada na financijsko-platežne mreže.

DDOS VEKTORI POJAČANJA TIJEKOM VREMENA



SLIKA 39. *Značajnije amplifikacijske metode kroz godine, [Izvor: Diverto]*

Porastu napada na aplikacijskoj razini pomogao je i *HTTP/2 Rapid Reset Attack* koji je prouzročio velike DDoS napade tijekom ljeta.

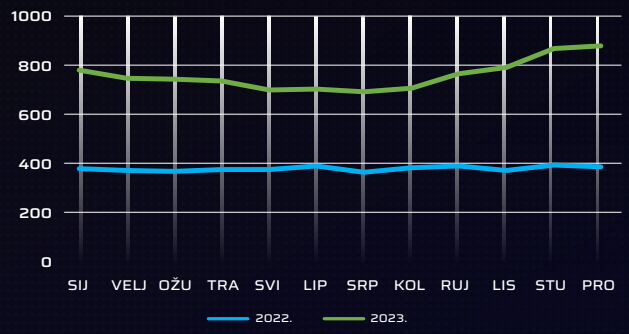
HTTP/2 RAPID RESET NAPAD

SLIKA 40. *Izgled HTTP/2 Rapid Reset napada, [Izvor: Diverto]*

Analizirajući broj napada po mjesecima, primjećuje se da su takvi incidenti u hrvatskom internetskom prostoru učestali tijekom cijele godine, bez jasno definiranog razdoblja kada nisu izraženi. Važno je napomenuti da unatoč navedenim vrhunskim vrijednostima, razlike među njima nisu značajne

Jednako su napadane usluge smještene kod samih korisnika i u oblaku, gdje je oblak pogodan i za izvođenje ekonomski distribuiranih napada uskraćivanja usluge (engl. *Economic Distributed Denial of Service*).

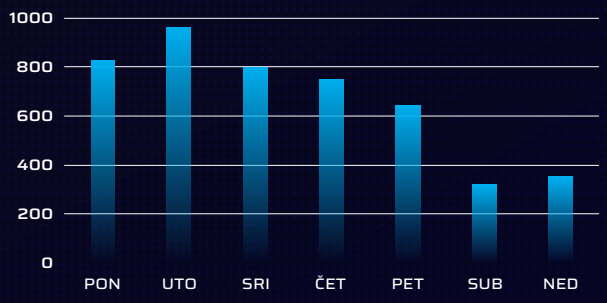
Iako se bilježi nešto manji broj napada u srpnju, najviše izraženi mjesec je prosinac.



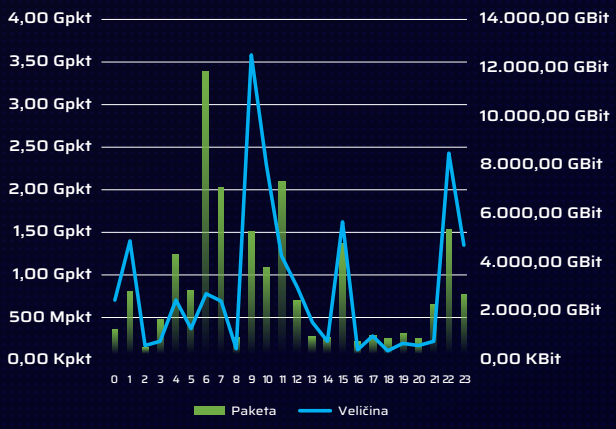
SLIKA 41. *Broj napada prema mjesecima u 2023 i 2022. godini, [Izvor: Diverto]*

SLIKA 42. *Veličina napada prema mjesecima u 2023. godini, [Izvor: Diverto]*

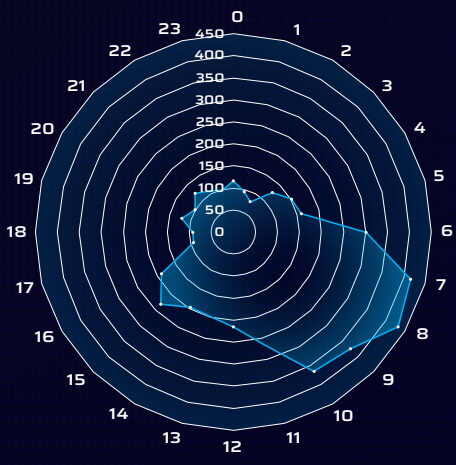
Interesantno je pogledati kada napadači najčešće započinju svoje napade u 2023. godini. **Po broju napada, to su očigledno ponedjeljak i utorak u jutarnjim satima. Navedeno nameće zaključak kako napadači biraju vrijeme kada je posljedica na poslovanje najveća.**



SLIKA 43. *Broj napada po danima u tjednu, [Izvor: Diverto]*

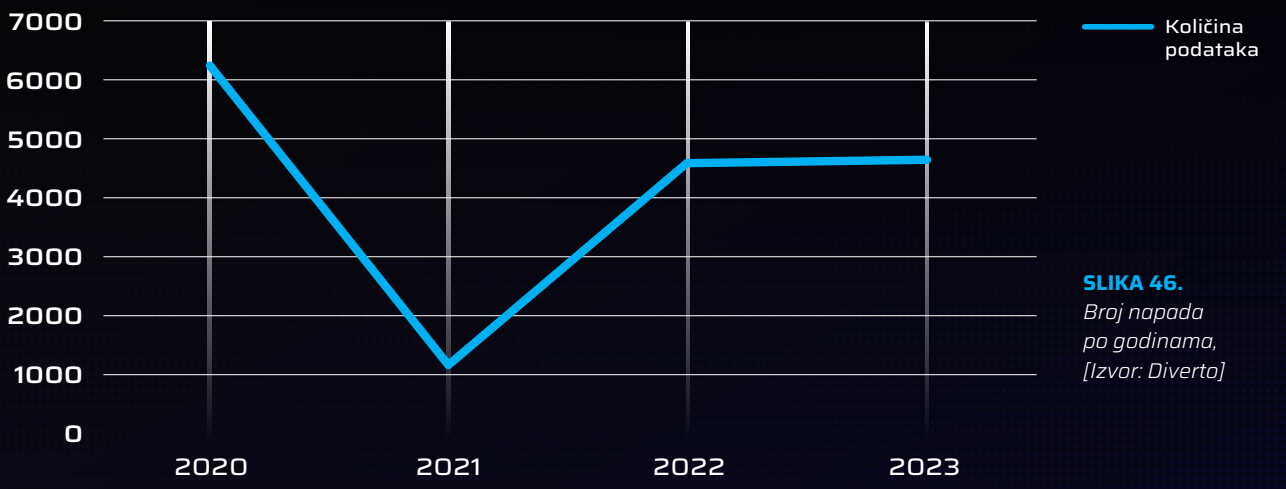


SLIKA 44. *Veličine napada prema početnom satu napada, [Izvor: Diverto]*

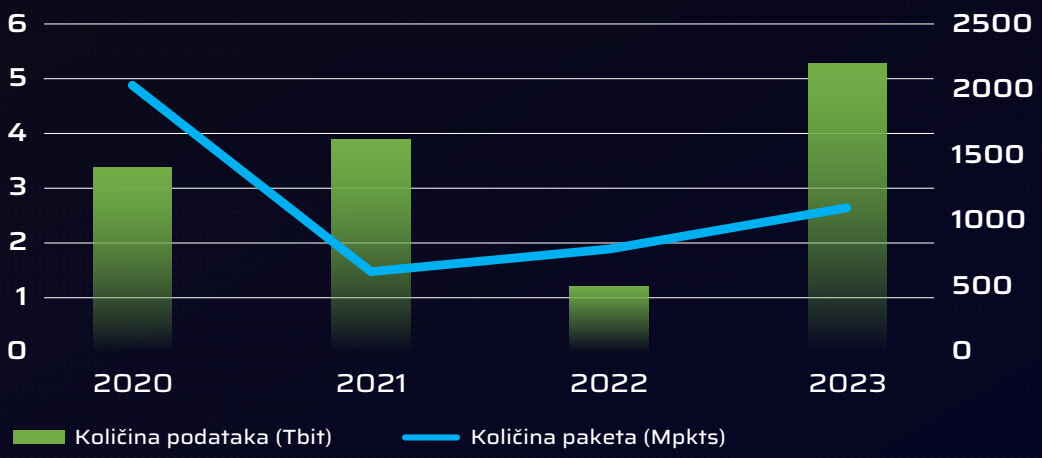


SLIKA 45. *Broj DDoS napada prema početnom satu (CET) napada, [Izvor: Diverto]*

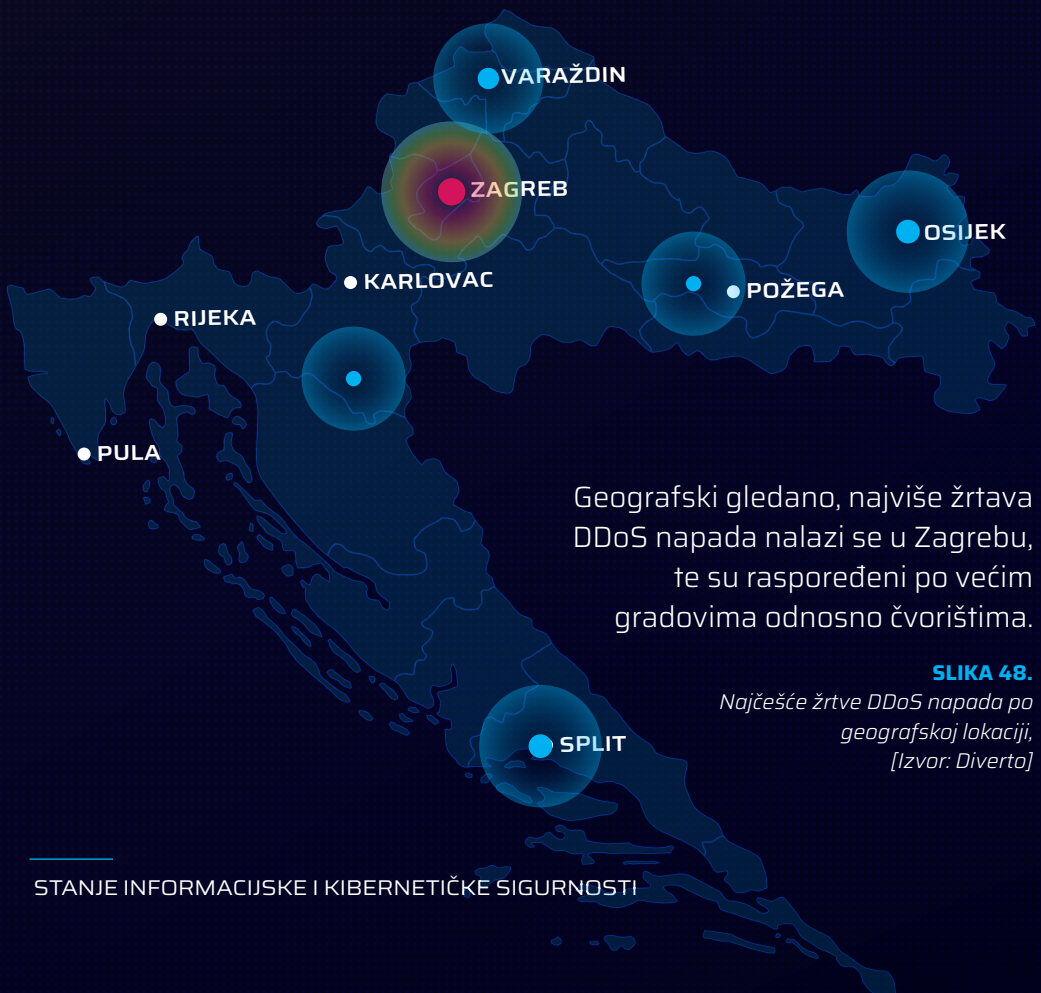
U usporedbi s prethodnim godinama, 2023. godina je bila rekordna što se tiče uočenog najvećeg napada po količini podataka. Radi se o napadu od 5,3 Tb primarno korištenjem UDP protokolom.



SLIKA 46.
Broj napada po godinama, [Izvor: Diverto]



SLIKA 47.
Najveći napadi prema godinama, [Izvor: Diverto]

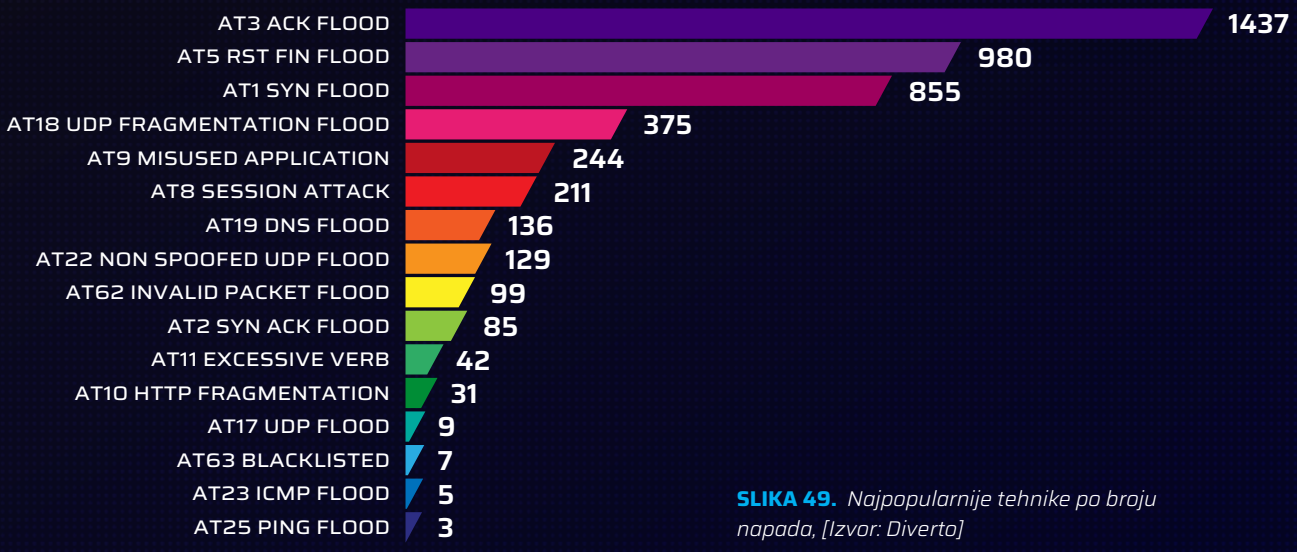


Geografski gledano, najviše žrtava DDoS napada nalazi se u Zagrebu, te su raspoređeni po većim gradovima odnosno čvorištima.

SLIKA 48.
Najčešće žrtve DDoS napada po geografskoj lokaciji, [Izvor: Diverto]

U 2023. godini i dalje je izraženija uporaba UDP protokola za napade, pogotovo ako gledamo prema broju zaprimljenih podataka. Međutim, TCP protokol je isto tako prisutan ako gledamo broj zaprimljenih paketa.

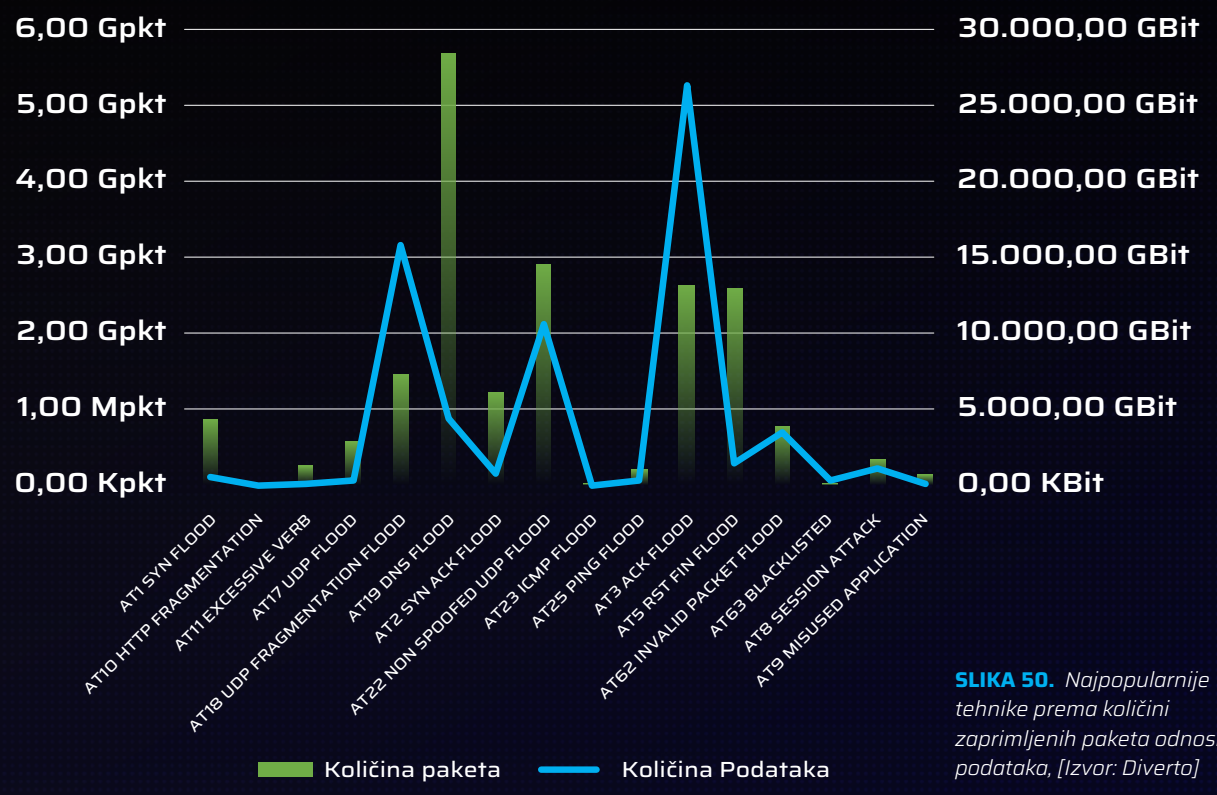
POREDAK	TIP NAPADA	KOLIČINA PAKETA	KOLIČINA PODATAKA
1	AT2 SYN ACK FLOOD	1,10 Gpkt	723,90 Gb
2	AT22 NON SPOOFED UDP FLOOD	1,10 Gpkt	4.100,00 Gb
3	AT18 UDP FRAGMENTATION FLOOD	498,60 Mpkt	5.300,00 Gb
4	AT22 NON SPOOFED UDP FLOOD	433.20 Mpkt	1.700,00 Gb
5	AT22 NON SPOOFED UDP FLOOD	374,60 Mpkt	1.400,00 Gb
6	AT22 NON SPOOFED UDP FLOOD	302,70 Mpkt	1.200,00 Gb
7	AT18 UDP FRAGMENTATION FLOOD	301,10 Mpkt	3.300,00 Gb
8	AT3 ACK FLOOD	274,50 Mpkt	3.200,00 Gb
9	AT11 EXCESSIVE VERB	229,40 Mpkt	124,80 Gb
10	AT62 INVALID PACKET FLOOD	227,00 Mpkt	1.400,00 Gb



SLIKA 49. *Najpopularnije tehnike po broju napada, [Izvor: Diverto]*

POREDAK PO KOLIČINI PODATAKA

POREDAK	TIP NAPADA	KOLIČINA PAKETA	KOLIČINA PODATAKA
1	AT18 UDP FRAGMENTATION FLOOD	498,60 Mpkt	5.300,00 Gb
2	AT22 NON SPOOFED UDP FLOOD	1,10 Gpkt	4.100,00 Gb
3	AT18 UDP FRAGMENTATION FLOOD	301,10 Mpkt	3.300,00 Gb
4	AT3 ACK FLOOD	274,50 Mpkt	3.200,00 Gb
5	AT18 UDP FRAGMENTATION FLOOD	222,70 Mpkt	2.500,00 Gb
6	AT3 ACK FLOOD	166,00 Mpkt	2.000,00 Gb
7	AT3 ACK FLOOD	168,30 Mpkt	1.900,00 Gb
8	AT3 ACK FLOOD	162,00 Mpkt	1.900,00 Gb
9	AT22 NON SPOOFED UDP FLOOD	433,20 Mpkt	1.700,00 Gb
10	AT3 ACK FLOOD	145,20 Mpkt	1.700,00 Gb



SLIKA 50. *Najpopularnije tehnike prema količini zaprimljenih paketa odnosno podataka, [Izvor: Diverto]*

Kako su DDoS napadi i dalje prisutni, preporuka je implementirati i provjeriti svoju DoS odnosno DDoS zaštitu. Provjera može uključivati kontakte i postupke u slučaju napada, pa sve do provođenja samog testiranja zaštite. I dalje je preporuka obratiti pažnju na točke spajanja udaljenih radnika, poput VPN koncentratora te kritične aplikacije izložene internetu.

Napadi su kategorizirani prema taksonomiji DDoS napada tvrtke RioRey, raspoloživoj na sljedećoj poveznici:

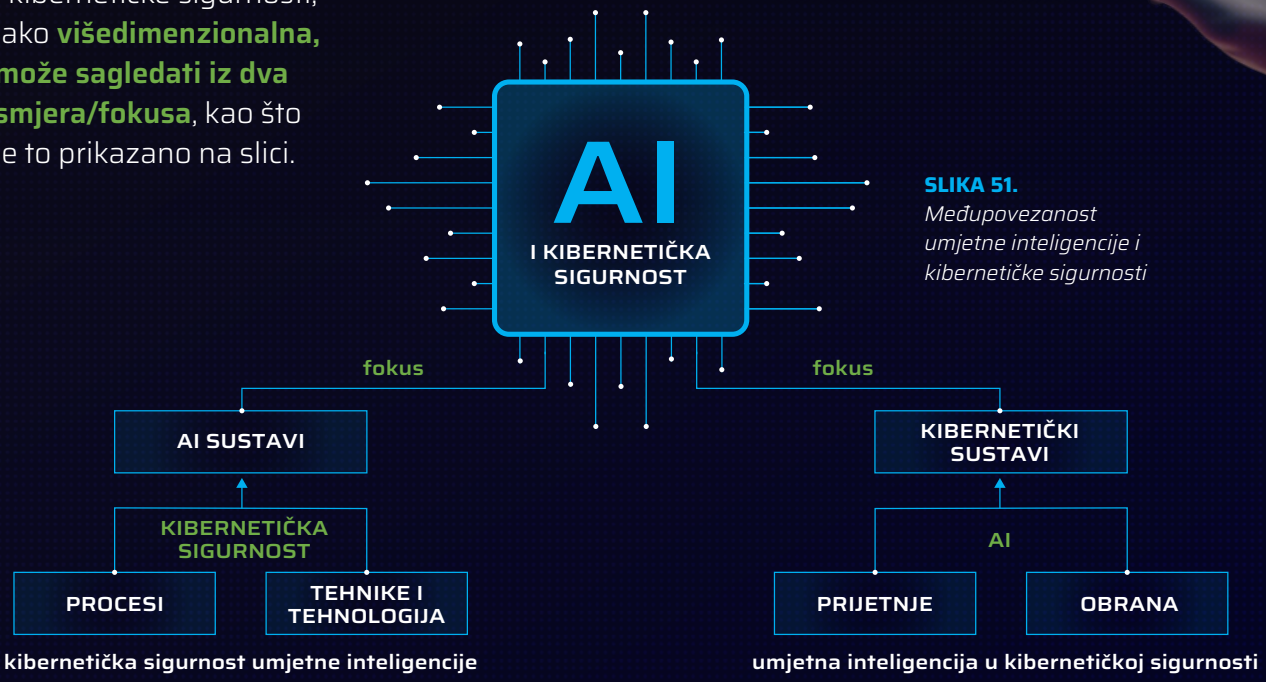
https://www.riorey.com/types-of-ddos-attacks

POSEBNU PAŽNJU TREBA OBRATITI na HTTP/2 implementaciju i SLP protokol koji ne bi smio biti izložen na internetu.

6.8. KIBERNETIČKA SIGURNOSTI I AI

Prepoznati izazovi oko umjetne inteligencije u prethodnom izvješću su se materijalizirali. Stoga, u ovogodišnjem izvješću posvećujemo posebno poglavlje umjetnoj inteligenciji (AI) i kibernetičkoj sigurnosti.

Treba napomenuti da se međuzavisnost AI-ja i kibernetičke sigurnosti, iako **višedimenzionalna, može sagledati iz dva smjera/fokusa**, kao što je to prikazano na slici.



SLIKA 51. *Međupovezanost umjetne inteligencije i kibernetičke sigurnosti*

6.8.1. KIBERNETIČKA SIGURNOST UMJETNE INTELIGENCIJE

Ovdje se primarno osvrće na zahtjeve EU Akta o umjetnoj inteligenciji u pogledu kibernetičke sigurnosti. Dobavljači visokorizičnih AI sustava morati će postići određenu usklađenost propisanu zahtjevima iz Akta, a jednu od ključnih uloga imat će standardi kibernetičke sigurnosti. U članku 15. navodi se sljedeće: „visokorizični AI sustavi projektiraju se i razvijaju tako da imaju odgovarajuću razinu točnosti, otpornosti i kibernetičke sigurnosti". Dodatno, u uvodnoj izjavi 51. navodi se da je kibernetička sigurnost ključna za otpornost AI sustava na pokušaje zlonamjernih trećih strana koje iskorištavaju slabe točke sustava da bi im izmijenili način uporabe, ponašanje, sposobnost ili da bi ugrozili njihove sigurnosne mehanizme. Kibernetičkim napadima na AI sustave moguće je iskoristiti resurse svojstvene umjetnoj inteligenciji, kao što su skupovi podataka za učenje (npr. trovanje podataka) ili poučeni modeli (npr. neprijateljski napadi) ili iskoristiti slabe točke digitalnih resursa AI sustava ili osnovne IKT infrastrukture. Kako bi se osigurala razina kibernetičke sigurnosti koja odgovara rizicima, dobavljači visokorizičnih AI sustava trebali bi poduzeti odgovarajuće mjere, prema potrebi uzimajući u obzir i osnovnu infrastrukturu IKT-a.

Dakle, visokorizični AI sustavi morat će ispuniti zahtjev kibernetičke sigurnosti prije upotrebe na tržištu EU-a, a dobavljači AI sustava moraju jamčiti kibernetičku sigurnost i njegovo ažuriranje tijekom cijelog životnog vijeka AI sustava. Izvješće „Kibernetička sigurnost umjetne inteligencije u Aktu o umjetnoj inteligenciji" usredotočuje se na zahtjeve kibernetičke sigurnosti za visokorizične AI sustave, kako je to navedeno u članku 15. Akta. Pritom se definira pojam „kibernetička sigurnost AI-ja" kao polje proučavanja u nastajanju koje prikuplja i kombinira znanja i pristupe iz različitih područja kao što su istraživanja umjetne inteligencije, suparničko/neprijateljsko strojno učenje i opća kibernetička sigurnost.

Izazovi kibernetičke sigurnosti umjetne inteligencije mogu se podijeliti u dvije kategorije:

(1) organizacijski izazovi vezani uz procese i

(2) izazovi istraživanja i razvoja vezani uz tehnike i tehnologiju.

Četiri su glavna načela za **rješavanje zahtjeva Akta o umjetnoj inteligenciji** u pogledu kibernetičke sigurnosti:

Fokus Akta o umjetnoj inteligenciji je na **AI sustavima**;

Usklađenost sa Aktom nužno zahtijeva **procjenu sigurnosnog rizika**;

Zaštita AI sustava zahtijeva integrirani i kontinuirani pristup korištenjem **dokazanim praksama i kontrolama specifičnim za AI**;

Postoje **ograničenja** najsuvremenijih tehnologija pri zaštiti AI modela.

Zaključno, u godinama ispred nas, kibernetička sigurnost umjetne inteligencije postajat će sve važnije, a moglo bi se reći i kritično područje. Tvrtke koje se bave kibernetičkom sigurnošću imat će povećane zahtjeve za implementacijom svojih usluga, standarda i rješenja u primarno visokorizičnim AI sustavima.

6.8.2. UMJETNA INTELIGENCIJA U KIBERNETIČKOJ SIGURNOSTI

Ovdje se osvrće na prijetnje kibernetičkoj sigurnosti korištenjem umjetnom inteligencijom, ali i potencijal umjetne inteligencije u obrani od kibernetičkih incidenata. Neke od ključnih prednosti korištenja umjetnom inteligencijom u kibernetičkoj sigurnosti (obrana) jesu[5]:

ZAŠTITA PODATAKA U HIBRIDNIM OKRUŽENJIMA (*CLOUD*).

AI rješenja mogu identificirati „podatke u sjeni", pratiti abnormalnosti/anomalije u pristupu podacima i upozoriti stručnjake za kibernetičku sigurnost na potencijalne prijetnje od bilo koga tko pristupa podacima ili osjetljivim informacijama štede dragocjeno vrijeme u otkrivanju i rješavanju problema u stvarnom vremenu.

GENERIRANJE PRECIZNIJIH I PRIORITIZIRANIH PRIJETNJI.

Analiza rizika koju pokreće AI može proizvesti sažetke incidenata za upozorenja visoke točnosti i automatizirati odgovore na incidente, ubrzavajući istrage upozorenja i trijažu za prosječno 55 %. AI tehnologija također pomaže u prepoznavanju ranjivosti i obrani od kibernetičkih kriminalaca i kibernetičkog kriminala.

USKLAĐIVANJE POTREBA KORISNIČKOG PRISTUPA I SIGURNOSTI.

AI modeli mogu pomoći u pronalaženju ravnoteže između sigurnosti i korisničkog iskustva analizom rizika svakog pokušaja prijave i provjerom korisnika putem podataka o ponašanju (bihevioralna analiza), pojednostavljujući pristup za provjerene korisnike i smanjujući troškove prijevare do 90 %. AI sustavi pomažu i u sprječavanju krađe identiteta, zlonamjernog softvera i drugih zlonamjernih aktivnosti, osiguravajući visoku razinu sigurnosti.

IZDVOJENA STATISTIKA:

organizacije s potpuno implementiranim AI sigurnosnim sustavima prosječno su smanjile troškove povrede podataka (*data breach*) za 3 milijuna USD. Te sposobnosti doprinose i uštedi vremena. Tako, primjerice, potrebno vrijeme od 230 dana (za otkrivanje, reakciju i oporavak) smanjuju na 99 dana, a organizacije s najzrelijim AI sustavima te sposobnostima automatizacije ostvaruju 40 % veći ROSI (povrat na sigurnosna ulaganja)[6].

Tablica prikazuje AI metode u funkciji/ama kibernetičke sigurnosti[7]

	Stabla odlučivanja	Algoritam potpornih vektora	Naivni Bayesov klasifikator	Algoritam K-srednjih vrijednosti	Skriveni Markovljevi modeli	Genetski algoritmi	Umjetne neuronske mreže	Konvolucijske neuronske mreže	Povratne neuronske mreže	Autoenkoderi	Sijamska neuronska mreža
Otkrivanje upada	■	■	■	■	■	■	■	■	■		■
Otkrivanje zlonamjernog koda	■	■	■	■				■	■		
Provjera ranjivosti	■										
Filtriranje neželjene pošte			■								
Detekcija anomalija					■					■	
Klasifikacija zlonamjernog kôda						■	■				■
Otkrivanje *phishinga*							■				
Analiza prometa								■	■		
Kompresiranje podataka										■	
Izdvajanje značajki										■	

[5] https://www.ibm.com/ai-cybersecurity

[6] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-security-automation

[7] ARTIFICIAL INTELLIGENCE AND CYBERSECURITY RESEARCH; ENISA Research and Innovation Brief; JUNE 2023

Zaključno, primjena generativne umjetne inteligencije za potrebe kibernetičke sigurnosti je u velikom porastu te će nastaviti rasti. Tvrtke će pri odabiru sustava kibernetičke sigurnosti (npr. SOC, SIEM i dr.) sve više uzimati u obzir AI mogućnosti sustava.

Prijetnje kibernetičkoj sigurnosti korištenjem umjetnom inteligencijom izazivaju sve veću zabrinutost organizacija i pojedinaca, s obzirom da mogu izbjeći tradicionalne sigurnosne mjere i uzrokovati značajnu štetu.

Neke od prijetnji na koje treba posebno obratiti pozornost jesu (sažeti popis):

1. upotreba umjetne inteligencije od strane APT-ova kako bi se izbjeglo otkrivanje pri napadima na određene organizacije ili pojedince;
2. zlonamjerni kôd koji se koristi umjetnom inteligencijom (*AI powered malware*)
3. upotreba LLM i ML modela u *phishing* napadima – npr. *WormGPT*;
4. upotreba umjetne inteligencije u napadima dubokom varkom (*deepfake*) i generiranju informacijskih poremećaja;
5. automatizirano iskorištavanje ranjivosti;
6. *credential stuffing* napadi i
7. automatizirani botneti.

01

OKRUŽENJE PRIJETNJI

Koristeći se različitim metodama istraživanja i primjenjujući alate napredne analitike na podatke s kojima raspolažemo, donosimo prikaz najznačajnijih prijetnji s kojima se u području kibernetičke sigurnosti trenutačno suočavaju zemlje EU-a, s naglaskom na Hrvatsku i Sloveniju te Bosnu i Hercegovinu.

ZNAČAJNIJE PRELIJEVANJE GEOPOLITIČKE SITUACIJE I POLARIZACIJA

Geopolitičke tenzije i zatezanja za posljedicu imaju povećano ciljanje određenih zemalja i sektora te potencijalne eskalacije kibernetičkih napada kao instrumenta geopolitičkog pritiska.

KOMPROMITIRANI LANAC OPSKRBE

Napadači sve više ciljaju ranjivosti kod dobavljača (posebno softvera i hardvera) kako bi šire ubacili zlonamjerni kôd i preuzeli kontrolu nad sustavima korisnika.

KIBERNETIČKO RATOVANJE I DEZINFORMIRANJE

Dezinformacije, videozapisi duboke varke (*deepfake*), fotografske manipulacije i slične tehnike se upotrebljavaju za uznemiravanje javnosti, utjecanje na političke procese i slabljenje nacionalne sigurnosti.

PORAST BROJA „USLUŽNIH HAKERA" (HaaS) I NAPADAČKIH GRUPA IZUZETNIH SPOSOBNOSTI (APT)

Laki pristup sofisticiranim alatima i tehnikama napada kroz model *Hacking-as-a-service* (HaaS) omogućava širi krug napadača, dok ciljane operacije APT grupa predstavljaju značajnu prijetnju nacionalnoj infrastrukturi i osjetljivim podacima.

PORAST KVALITETE I KVANTITETE ZLONAMJERNOG KODA, UKLJUČUJUĆI UCJENJIVAČKI SOFTVER (*RANSOMWARE*)

Ucjenjivački softver (*ransomware*) i programi za brisanje diskova ostaju učinkovite metode za ometanje poslovanja, iznuđivanje i uništavanje podataka. Međutim, to je samo podskup cijelog arsenala zlonamjernog kôda.

KOMBINIRANJE VRSTA SOCIJALNOG INŽENJERINGA

Napadači sve više kombiniraju razne vrste socijalnog inženjeringa, poput *phishinga, vishinga* i *smishinga* kako bi prevarili korisnike da otkriju osjetljive informacije ili instaliraju zlonamjerni kôd.

KOMPROMITACIJA INTERNETSKE VEZE I OBLAKA, TE NJIHOVA (NE)RASPOLOŽIVOST

Napadači ciljaju na internetsku infrastrukturu i servise u oblaku (*cloud*) kako bi prekinuli ili ograničili pristup važnim resursima i podacima.

ZNAČAJNI PORAST DoS/DDoS NAPADA

DoS i DDoS napadi su u porastu, a ciljaju preopterećenje poslužitelja i onemogućavanje pružanja usluga korisnicima bilo da su oni smješteni u vašem podatkovnom centru ili oblaku.

PORAST ZAMKI ZA SUSTAVE I PODATKE

Vješto postavljene zamke za sustave i podatke, koristeći se sličnim imenima domena, oglašavanjem i strateškim pozicioniranjem zlonamjernog sadržaja postale su svakodnevnica. Naravno, sve s namjerom kako bi napadači zadobili ovlasti na sustavima i neovlašteno pristupili podacima, odnosno pribavili financijsku korist.

NEDOSTATAK LJUDI, ZNANJA I VJEŠTINA

Nedostatak kvalificiranih stručnjaka za kibernetičku sigurnost i osposobljenog osoblja za upravljanje sigurnošću predstavlja značajnu prepreku za učinkovitu obranu od kibernetičkih prijetnji.

POVEĆANA AUTOMATIZACIJA NAPADA

Napadači sve više upotrebljavaju automatizirane alate i skripte za iskorištavanje ranjivosti, poboljšanje efikasnosti i obima napada.

08

IZAZOVI BUDUĆNOSTI

Organizacija koja radi istraživanje i prati ekonomiju kibernetičke sigurnosti, *Cybersecurity Ventures*, procjenjuje da će do kraja 2024. godine trošak kibernetičkih napada za globalno gospodarstvo premašiti 10,5 milijardi dolara, što dodatno naglašava rastuću nužnost razmatranja kibernetičke sigurnosti kao strateškog prioriteta na razini pojedinca, organizacije i države.

S hitrim razvojem tehnologije, razvija se i napreduje i područje kibernetičkih prijetnji. Najveći, i to transformacijski utjecaj i na ofenzivnu i defenzivnu stranu imat će umjetna inteligencija, koja se provlači i kroz mnoge druge vrste izazova[8] koje ćemo izložiti u nastavku ovoga poglavlja.

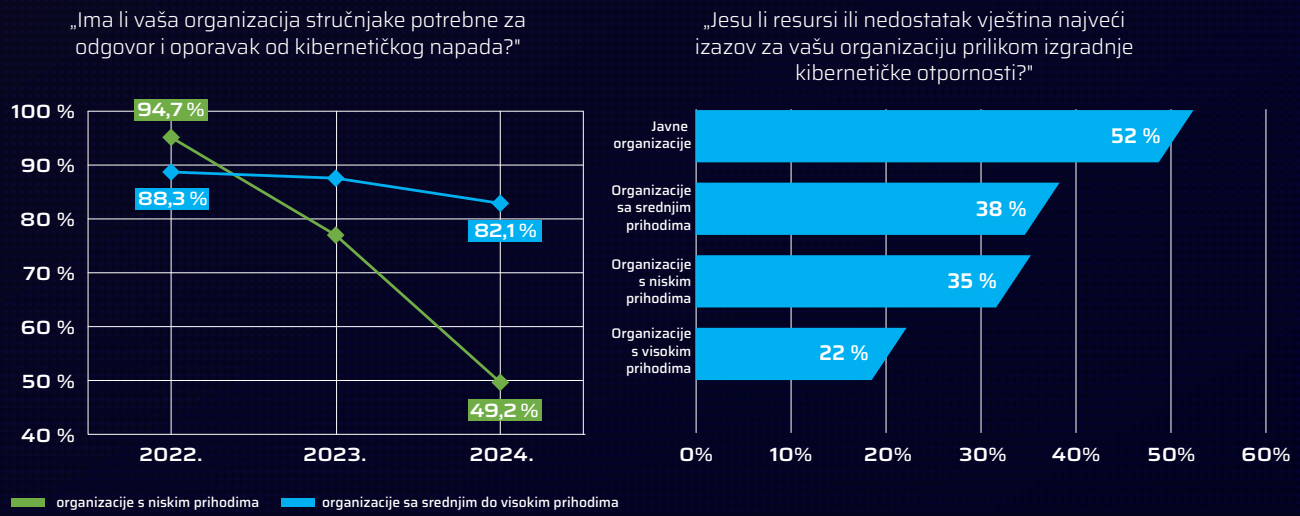
GENERATIVNU UMJETNU INTELIGENCIJU KORISTE OBJE STRANE

Sve sofisticiraniji i pametniji napadi potpomognuti umjetnom inteligencijom obuhvaćat će raspon od dubokih varki (*deepfake*) u području socijalnog inženjeringa do automatiziranog zlonamjernog kôda koji inteligentnom prilagodbom odolijeva otkrivanju. S druge, defenzivne strane, umjetna inteligencija pomagat će u otkrivanju, izbjegavanju ili neutraliziranju prijetnji, zahvaljujući otkrivanju anomalija, pametnoj autentifikaciji i automatiziranom odgovoru na incidente, i to u stvarnom vremenu.

NEDOSTATAK VJEŠTINA U DOMENI KIBERNETIČKE SIGURNOSTI

Sukladno predviđanjima prošlogodišnjeg izvješća, i tijekom 2024. godine očekuje se nestašica stručnjaka s vještinama potrebnim za zaštitu organizacija od kibernetičkih napada. Situacija je zapravo i lošija nego proteklih godina – istraživanja govore da je broj ljudi zaposlenih u kibernetičkoj sigurnosti porastao za 9 % u odnosu na 2022. godinu i sada iznosi 5,5 milijuna. Međutim, potreba za stručnjacima tog profila raste brže od toga: taj se jaz povećao za 13 % u odnosu na 2022., što znači da je trenutačni manjak stručnjaka u tom području u svijetu oko 4 milijuna te da se brojka treba udvostručiti kako bi se popunili kapaciteti. U globalnom istraživanju ISC2[9], 67 % ispitanika izjavilo je da njihova organizacija ima manjak kibernetičkih stručnjaka za prevenciju i rješavanje sigurnosnih problema, dok čak 92 % navodi nedostatak relevantnih vještina vezanih uz kibernetičku sigurnost u svojim organizacijama, ponajprije sigurnost računalstva u oblaku, vještine vezane uz umjetnu inteligenciju i strojno učenje te implementacija *Zero Trust* modela.

Kibernetičke vještine i nedostatak stručnjaka povećavaju se alarmantnom brzinom



SLIKA 52. *Izvor: WEF, Global Cybersecurity Outlook 2024.*

[8] Izvor: https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/

[9] Izvor: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

„MEKE" VJEŠTINE POSTAJU KLJUČNE ZA STRUČNJAKE KIBERNETIČKE SIGURNOSTI

Od stručnjaka za kibernetičku sigurnost sve će se više tražiti preuzimanje složenijih radnih opterećenja jer će krajolik prijetnji u 2024. postati sofisticiraniji. To ne znači samo u tehničkom smislu - oni koji su odgovorni za suzbijanje kibernetičkih prijetnji suočavat će se i sa složenijim društvenim i kulturološkim aspektima ublažavanja prijetnji. To će dovesti do sve većeg oslanjanja na meke vještine kao što su interpersonalna komunikacija, izgradnja odnosa i rješavanje problema.

KIBERNETIČKO RATOVANJE I DRŽAVNO SPONZORIRANI KIBERNETIČKI NAPADI

Rat u Ukrajini razotkrio je do koje su mjere države spremne i sposobne izvesti kibernetičke napade na vojnu i civilnu infrastrukturu u 2024. Sigurno je da će u budućnosti vojne operacije, gdje god se odvijale diljem svijeta, ići zajedno s operacijama kibernetičkog ratovanja, čije najčešće taktike uključuju *phishing* napade osmišljene za dobivanje pristupa sustavima u svrhu ometanja i špijunaže te DDoS napade u svrhu ometanja komunikacija, javnih usluga, transporta i sigurnosne infrastrukture. Osim ratovanja, u 2024. se održavaju i veliki izbori u mnogim državama, uključujući SAD, Ujedinjeno Kraljevstvo i Indiju, gdje također možemo očekivati povećan broj kibernetičkih napada čiji je cilj ometanje demokratskog procesa.

GEOPOLITIKA, AI I INFORMACIJSKI POREMEĆAJI[10]

Kao primjer sjecišta geopolitičkih sukoba i umjetne inteligencije, duboke varke i *phishing* kampanje mogu se pretvoriti u oružje u svrhu remećenja demokratskih izbornih procesa. Iako informacijsko ratovanje nije novi koncept, decentralizacija izvora informiranja i hitri razvoj tehnologije čini obranu od ovih vrsta zlonamjernih prijetnji ključnim izvorom zabrinutosti u nadolazećim godinama. U 2024. godini, ovi će se rizici sjediniti i zauzeti središnju pozornost s obzirom na činjenicu da je to godina u kojoj će izbori održati u preko 45 država koje čine više od 50 % svjetskog BDP-a. S rastućim širenjem novih tehnologija, poput generativnog AI-ja, i njihovom sve širom upotrebom u zlonamjerne kibernetičke svrhe, od presudne je važnosti očuvanje integriteta i pravednosti izbornih procesa. Izazovi informacijskih poremećaja potpomognutih umjetnom inteligencijom mogu se svrstati u 6 područja: 1) lažne informacije i dezinformacije; 2) duboke varke; 3) automatizirane dezinformacije; 4) ciljano oglašavanje; 5) privatnost podataka; 6) algoritamska manipulacija društvenim medijima.

PHISHING NAPADI VIŠE RAZINE

Puno napredniji postat će i napadi iz domene socijalnog inženjeringa. Alati generativne umjetne inteligencije (kao što je *ChatGPT*) omogućuju većem broju napadača pametnije i više personalizirane pristupe, a duboke varke postat će sve prisutnije. Odgovor na to uvelike će se vrtjeti oko osviještenosti i educiranosti u cijeloj organizaciji, iako će AI i *Zero Trust* također igrati sve veću ulogu.

KIBERNETIČKA SIGURNOST U NAJVIŠIM RAZINAMA UPRAVLJANJA

U 2024. kibernetička sigurnost bit će strateški prioritet koji neće više moći ostati na razini IT odjela. Gartner predviđa da će do 2026. godine 70 % uprava tvrtki sadržavati barem jednog člana koji posjeduje stručno znanje iz ovog područja, što će osigurati proaktivan umjesto reaktivnog pristupa obrani od kibernetičkih napada.

ZAŠTITA KIBERNETIČKO-FIZIČKIH SUSTAVA

Konvergencija IT, IoT i OT sustava te primjena COTS uređaja stvaraju kompleksne izazove za sigurnost. Nedostatak testiranja i modeliranja prijetnji može za posljedicu imati širenje površine napada, zahtijevajući napredne pristupe odgovora na prijetnje.

[10] Izvor: WEF, Global Cybersecurity Outlook 2024, https://www.weforum.org/publications/global-cybersecurity-outlook-2024/?_gl=1*13a76o3*_up*MQ..&gclid=CjOKCQiAwbitBhDIARIsABfFYIJbOMGOCLOuLvwNqqoZcDLWwuJ3PiuBgaDGUnpW2J3udzVPADCo4aEaAspNEALw_wcB

KIBERNETIČKA OTPORNOST KAO UNAPRIJEĐENA KIBERNETIČKA SIGURNOST

S obzirom na to da ni najbolje sigurnosne mjere ne osiguravaju 100%-tnu zaštitu, razumijevanje razlike između kibernetičke sigurnosti i otpornosti postat će sve važnije u narednom razdoblju. Naime, fokus kibernetičke sigurnosti jest na prevenciji napada, dok mjere otpornosti osiguravaju kontinuitet operacija i u slučajevima uspješne povrede. Stoga će strateški prioritet u 2024. biti razvoj sposobnosti agilnog oporavka, pritom svodeći gubitke podataka i vrijeme zastoja na minimum.

POTPUNA IMPLEMENTACIJA *ZERO TRUST* NAČELA

Organizacije se suočavaju s izazovima u potpunoj implementaciji *Zero Trust* načela zbog zastarjelih sustava i kompleksnosti okruženja. Implementacija zahtijeva reviziju postojećih arhitektura i temeljito promišljanje pristupa sigurnosti.

REGULATIVA U PODRUČJU KIBERNETIČKE SIGURNOSTI

Vlade i organizacije postaju sve svjesnije rizika koji kibernetičke prijetnje predstavljaju za nacionalnu sigurnost i gospodarski rast. Potencijalne društvene i političke posljedice povrede podataka velikih razmjera jedan su od glavnih čimbenika nastanka nove regulative o pitanjima kibernetičke sigurnosti.

Države članice morat će osigurati koordiniranu provedbu već spomenutih akata[11].

KVANTNO RAČUNALSTVO I POST-KVANTNA KRIPTOGRAFIJA

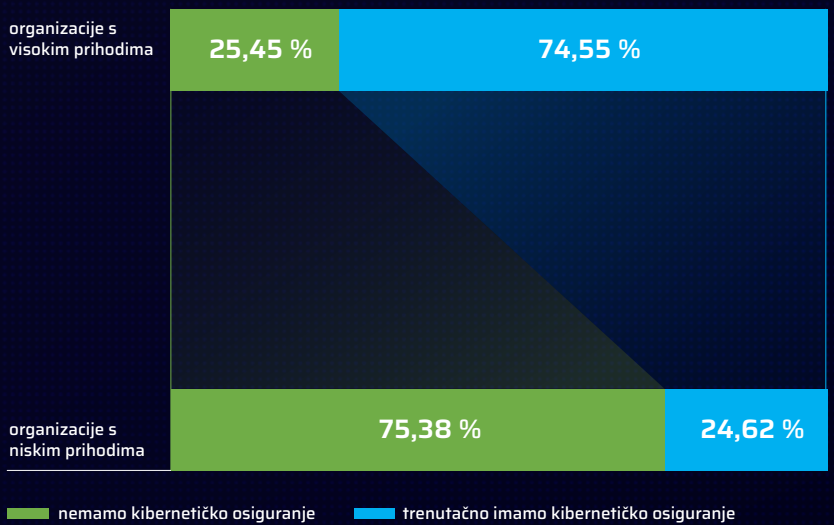
Izazovi kvantnog računalstva su već pred nama i naglašavaju potrebu za zaštitom od kvantnih napada, a poseban dio odnosit će se na zaštitu istoga te otpornost trenutnih kriptografskih zaštita u odnosu na kvantno računalstvo.

OSIGURANJE OD KIBERNETIČKIH NAPADA

Uz regulatorna tijela, i osiguravateljska industrija je iznimno važna za ublažavanje i suzbijanje rizika diljem ekosustava. Kibernetičko osiguranje vrijedan je alat za pokrivanje troška financijske štete neizbježne u svakoj strategiji kibernetičke otpornosti, a u mnogim slučajevima pruža ključnu potporu osiguravanju dovoljnih i učinkovitih ulaganja u kibernetičku sigurnost. Međutim, broj organizacija s policom kibernetičkog osiguranja pao je za 24 % u odnosu na 2022. godinu jer čak ni za velike organizacije osiguranje ponekad nije ekonomski održivo, a sigurnosni budžeti „mogu biti bolje utrošeni negdje drugdje". Uzrok ovog nesklada postaje očigledan kada se promatra kroz prizmu prihoda.

Isto tako treba napomenuti kako osiguranje ne rješava odgovornost.

Organizacije koje su prijavile da posjeduju policu kibernetičke sigurnosti, razvrstane prema visini prihoda



SLIKA 53. *Izvor: WEF, Global Cybersecurity Outlook 2024.*

[11] https://www.cert.hr/zajedno-za-kiberneticku-otpornost-europske-unije/

Web: www.diverto.hr
E: diverto@diverto.hr

Izvještaj je rezultat zajedničkog rada s našim korisnicima kojima ovim putem zahvaljujemo. Rezultat je to rada i svih osoba i timova unutar Diverta, a iza svakog pokazatelja i iznesene brojke stoji vrlo detaljna priča i predani danonoćni rad.