2022 Stanje informacijske i kibernetičke sigurnosti

diverto

4. izdanje

— SADRŽAJ

// UVODNIK

Zadovoljstvo mi je pozdraviti Vas po četvrti put objavom ovog našeg godišnjeg izvještaja, kojeg sad već možemo nazvati tradicionalnim. Svake godine se trudimo učiniti izvještaj sve boljim i korisnijim za sve one koji se bave sigurnošću kibernetičkih i informacijskih sustava.

U prethodnom razmatranom razdoblju proširili smo bazu korisnika i broj zemalja u kojima izravno i kontinuirano djelujemo. Iako smo od samih početaka redovito i uspješno provodili poslovne aktivnosti na globalnoj razini, uspostavljanjem upravljanih sigurnosno-operativnih centara (SOC) izvan Hrvatske otvorena nam je mogućnost proširenja i obogaćivanja ovog izvještaja. Diverto SOC narastao je za 55 % u odnosu na 2021. godinu, a broj provedenih istraga povećan je za 30 %.

Geopolitička situacija podigla je razinu svjesnosti organizacija o važnosti informacijske i kibernetičke sigurnosti. Informacijska sigurnost postaje važan element u svakoj organizaciji. Prepoznavanje i adresiranje rizika informacijske sigurnosti postali su sve važniji za poslovodstva organizacija jer je šteta koju može prouzročiti sigurnosni incident značajna.

Dva druga najveća motiva za poboljšanje sigurnosne razine u organizacijama su regulatorni zahtjevi i incidenti koji se događaju u našem okruženju. Objava nove inačice direktive *Network and Information Security* (NIS) i *The Digital Operational Resilience Act* (DORA) u službenim glasnicima EU-a, kao i nove inačice standarda ISO 27001 obilježili su 2022. godinu. Predstoje nam izazovi i razdoblje prilagodbe novim okvirima (npr. izazovi transpozicije direktive EU NIS2 u nacionalnom zakonodavstvu), što će svakako doprinijeti povećanim sigurnosnim razinama u organizacijama.

Sigurnosni incidenti su i dalje česta pojava jer redovno budemo pozvani pomoći i izvan našeg sigurnosno-operativnog centra (SOC). Isto tako, vidljivo je kako incidenti samo mijenjaju kategoriju, a posljedice su i dalje prisutne. Nije odmah toliko uočljivo jer je i dalje prisutno prikrivanje informacija o sigurnosnim incidentima, no posebno je vidljivo kod onih koji nemaju sigurnosni nadzor ili uhodane procese otkrivanja i odgovora na incidente. Ukratko, to znači da se napadači i dalje uspješno prilagođavaju i ostvaruju svoje ciljeve. Jedan od razloga zasigurno je i to što se dane preporuke ne primjenjuju.

Kako bi organizacije napredovale upravo u segmentima sigurnosnog nadzora, uhodanih procesa otkrivanja i odgovora na incidente, sve više se upotrebljavaju vježbe *Purple teaming* koje postaju uobičajene i za velike organizacije u Hrvatskoj. To je dobro iskustvo za rad napadačkog (*red*) i obrambenog tima (*blue*), a svrha je unaprijediti otkrivanje i sprječavanje sigurnosnih incidenata te skratiti vrijeme otkrivanja i odgovora na sigurnosne incidente.

Kibernetička sigurnost OT sustava u dijelu organizacija koje su dio kritičnih infrastruktura i kod većine OT sustava u proizvodnim organizacijama i dalje je zasnovana na „pogrešnoj" percepciji *„Air Gapa"* i načelima: „ako radi, ne diraj". Industrijalizacija 4.0 nosi svoje izazove i kod većine organizacija tek se rađa svijest o potrebi za multidisciplinarnim pristupom izazovu osmišljanja, izgradnje i održavanja sustava koji ne samo da su sigurni za ljude i pouzdani, nego su i kibernetički sigurni i otporni na neprestano rastući broj prijetnji takvim sustavima.

Organizacije izrađuju ili upotrebljavaju sve veći broj aplikacija i API sučelja, a ispravna zaštita zahtijeva uključivanje sigurnosti od samog početka te provjeru komponenti kojima se koristi. Ispravan put podrazumijeva postavljanje sigurnosnih kontrola u cijeli životni ciklus proizvoda, što uključuje automatizaciju sigurnosnih provjera u CI-ju/CD-u (eng. *Continuos Improvement / Continuos Delivery*), naravno, uz redovito provođenje sigurnosnih testiranja.

Izazova je i dalje puno, a njihovom rješavanju potrebno je pristupiti odmah. Posebno će biti izazovno sagledati kibernetičke prijetnje i prilike umjetne inteligencije u razdoblju koje slijedi. Kako bi pomogli razmotriti najvažnije izazove, prvi put donosimo i okruženje prijetnji (engl. *Threat landscape*) kojeg smo izradili kako bi pomogli organizacijama u boljem upravljanju rizikom te, u konačnici, poboljšanju razine informacijske sigurnosti .

Sigurni smo da će vam ovaj izvještaj pomoći u tome,

Vlatko Košturjak, CTO

1. Upravljačka perspektiva

diverto

1. UPRAVLJAČKA PERSPEKTIVA

Upravljačka perspektiva pruža uvid u to koliko je pojedina organizacija, odnosno njezino poslovodstvo svjesno utjecaja informacijske sigurnosti na poslovanje. Poslovodstvo je odgovorno prepoznati i adresirati rizike informacijske sigurnosti koji mogu ozbiljno narušiti otpornost organizacije na sigurnosne prijetnje i time prouzročiti značajnu financijsku, reputacijsku ili regulatornu štetu.

U nastavku teksta kroz pokazatelje, trendove i procjene kretanja navodimo informacije za lakše prepoznavanje prijetnji te donošenje odluka o tome kako zaštititi svoju najvrjedniju imovinu.

1.1. Ključni pokazatelji

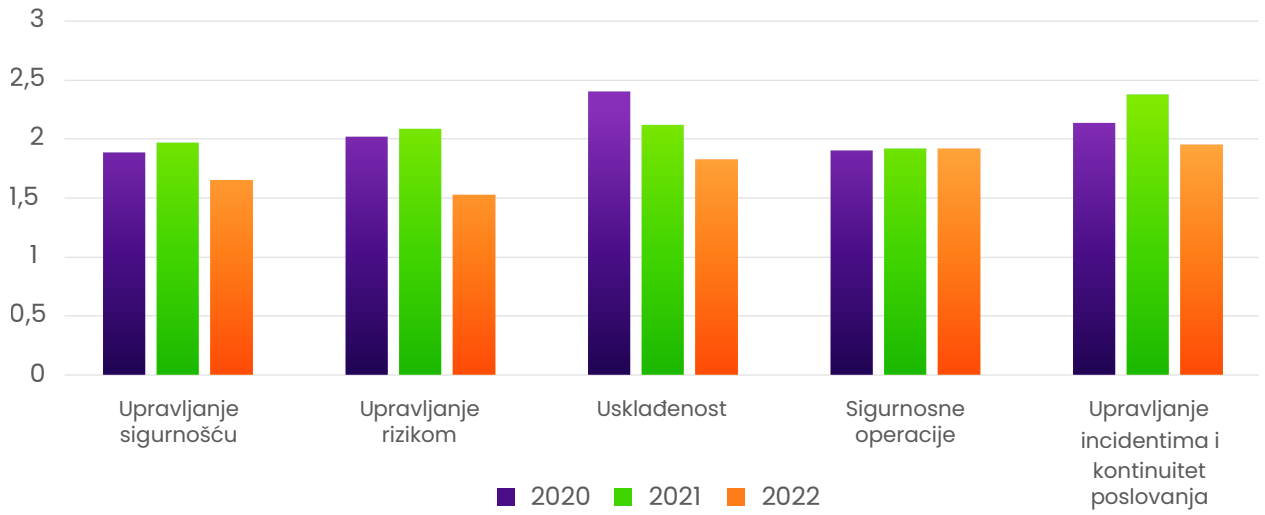
Ključni pokazatelji u promatranom razdoblju:

- nakon snažne digitalizacije i osiguranja preduvjeta udaljenog rada tijekom pandemije, voditelji sigurnosti zamijenili su reaktivni sa strukturiranim načinom rada i time ponovno ovladali programom sigurnosti
- o sigurnosti se govori na upravljačkoj razini te su s većom vidljivošću primjetna i veća očekivanja upravljačke razine, ali kako se sigurnost više ne smatra strateškim, nego operativnim ciljem, upravljačka razina gubi zainteresiranost za tu temu
- primjetan je značajan jaz u percipiranom riziku i razini pripremljenosti na incidente, a voditeljima sigurnosti je teško identificirati sve prijetnje, stoga se okreću poboljšanju otpornosti i jačanju planova kontinuiteta
- udaljenim načinom rada, zaposlenici i njihovi uređaji postali su novi perimetar organizacijskog IT sustava koji je potrebno zaštititi, čime ni ne znajući kolektivno prelazimo u svojevrsnu arhitekturu „nultog povjerenja“ (engl. *zero trust*)
- u postpandemijskom razdoblju IT zaposlenici su željni promjena, što za posljedicu ima visoku stopu odlazaka (engl. *big quit*), a u kombinaciji s nedostatkom kvalificirane radne snage organizacije se okreću pružateljima sigurnosnih usluga
- socijalni inženjering i dalje zauzima prvo mjesto među tehnikama napada, više od 90 % napada započinje phishing porukom e-pošte[1], a pritom su primijećeni uspješni napadi upotrebom isključivo tehnika socijalnog inženjeringa
- broj *ransomware* napada u 2022. godini je u blagom padu, ali zato njihova složenost raste ulančavanjem više ranjivosti u jedan uspješan napad

[1] https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

- dvostrukom iznudom (engl. *double extortion*), osim onemogućavanja pristupa podacima, više od 80 % *ransomware* napada za posljedicu ima i eksfiltraciju podataka iz organizacije[2]
- porast[3] broja incidenata informacijske sigurnosti
- napadi putem softverskih komponenti i repozitorija otvorenog koda u porastu su za više od 600 %
- geopolitička situacija, pandemija i inflacija napravili su značajne poremećaje u opskrbnim lancima, što se osjeti i u području sigurnosti (nedostupna oprema, iznimno visoke cijene opreme i licencija itd.)
- kraj godine obilježila je pojava velikog broja sustava potpomognutih umjetnom inteligencijom koji omogućuju napadačima bez stručnog znanja izradu raznih novih i kreativnih metoda napada, falsificiranje dokumentacije, manipulaciju informacijama i upravljanja javnim mišljenjem (stvaranje i uređivanje *deepfake* videozapisa i zvuka, izrada dokumenata itd.).

Razina zrelosti je dobar osnovni pokazatelj kretanja informacijske sigurnosti u organizacijama. Prosječna razina zrelosti informacijske sigurnosti u 2022. godini jasno pokazuje da treba jačati operativnu otpornost organizacija.



SLIKA 1 *Prosječna razina zrelosti prema industriji - nove procjene, [Izvor: Diverto]*

[2] https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting

[3] Pokazatelj utemeljen na: Statističkom pregledu temeljnih sigurnosnih pokazatelja i rezultata rada MUP-a u 2022. godini, podacima dobivenim kroz redovne operacije blue tima i podacima iz internetske ankete društva Diverto

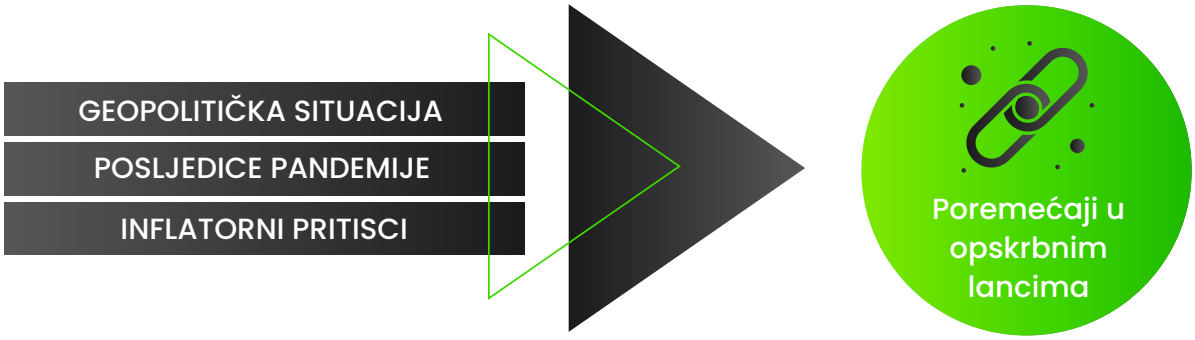
Treba napomenuti kako se utvrđivanje razine zrelosti uobičajeno obavlja prilikom izvršavanja Divertovih usluga, poput snimki stanja informacijske sigurnosti s novim korisnicima, a trenutačno ne prikazujemo rezultate kontinuiranih godišnjih procjena s postojećim korisnicima. Dakle, radi se o korisnicima koji su prethodno samostalno radili na svojem programu informacijske sigurnosti, a u promatranoj godini su odlučili zatražiti pomoć od Diverta kako bi postigli željenu razinu. U budućim izvještajima planiramo obuhvatiti rezultate procjena novih i postojećih korisnika.

1.2. Trendovi

Na globalnoj razini, u 2022. godini uočili smo kako su rizici informacijske sigurnosti, točnije, rizici od IT sigurnosnih incidenata zauzeli čvrsto prvo mjesto po važnosti percipiranog rizika za organizacije[4]. U Republici Hrvatskoj za korisnike Divertovih usluga ne možemo potvrditi taj trend, prvenstveno jer rizici prekida poslovanja i dalje predstavljaju najveću brigu organizacija, bez obzira bili oni posljedica sigurnosnog incidenta ili bilo kojeg drugog makroekonomskog, regulatornog rizika ili više sile. Sveukupno gledajući, situacija je takva da se rizici informacijske sigurnosti ne percipiraju kao rizici koji imaju značajnog utjecaja na poslovanje organizacija.

Primarni fokus u 2022. godini bio je na strukturiranom upravljanju i iskorištavanju svih sigurnosnih poboljšanja ostvarenih u prethodnoj godini, uvedenih kao posljedica odgovora na pandemijsko razdoblje. Općenito, bilježimo blage pozitivne pomake u razvoju svijesti o važnosti informacijske sigurnosti i o utjecaju rizika informacijske sigurnosti na poslovanje pojedinih organizacija.

Razni nepredviđeni događaji, poput geopolitičke situacije, posljedica pandemije te inflatornih pritisaka prouzročili su značajne poremećaje u opskrbnim lancima. Spomenuti poremećaji dodatno su osvijestili upravljačke razine organizacija u Republici Hrvatskoj kako globalni događaji itekako imaju utjecaja na njihovo poslovanje te ih potaknuli na značajnije promišljanje o povezanim rizicima i situacijama koje su unutar i izvan njihove domene djelovanja.



Ovakvo promišljanje potaknulo je organizacije na razmatranje alternativnih tržišta i lanaca opskrbe, što je utjecalo na to da se i tržište Republike Hrvatske dodatno otvori i smanji ovisnost o lokalnim pružateljima usluga. Kada se ista problematika preslika na informacijsku sigurnost, jasno je kako dosadašnji obrasci zaštite sustava postizanjem sigurnosti samo na infrastrukturnoj razini više nisu dovoljni. Arhitekture modernih sustava su decentralizirane, konzumiraju iznimne količine zatvorenih i otvorenih servisa, softverskih komponenti i repozitorija otvorenog koda. Navedeno u fokus postavlja

[4] https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz_Risk_Barometer_2022_FINAL.pdf

upravljanje opskrbnim lancima i povjerenje koje se daje pružateljima tih usluga. Izravna posljedica ovih trendova je povećana potražnja za usklađivanjem poslovanja s do sada manje zastupljenim standardima i atestacijama kod nas, poput *AICPA SOC 2 Type II, TISAX, NIST CSF* i slično.

Na tržištu usluga informacijske sigurnosti u Republici Hrvatskoj primjetan je porast potražnje za:

Potražnja za navedenim uslugama predstavlja direktnu reakciju na nedostatak kvalificirane radne snage.

1.3. Procjena kretanja u 2023.

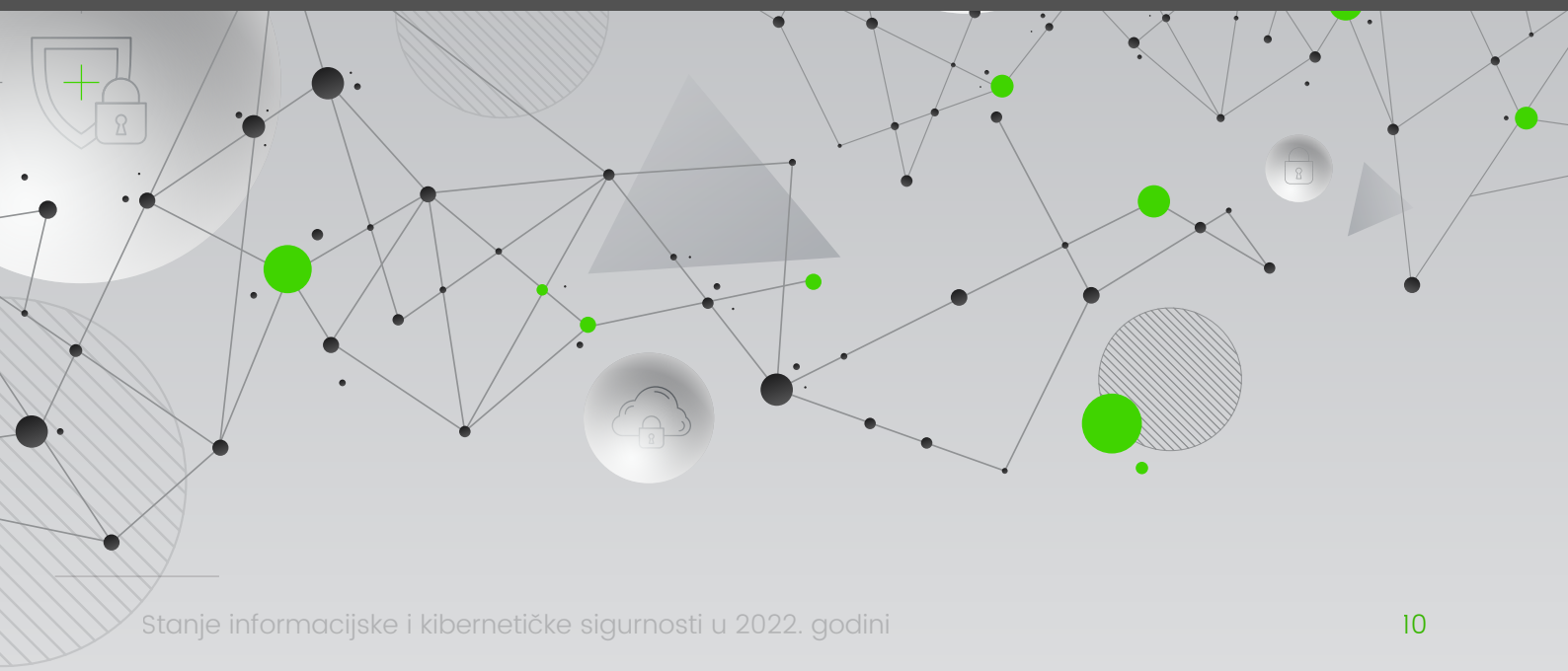
Procjena kretanja u 2023 godini iz upravljačke perspektive je:

- usprkos našim prethodnim procjenama, lokalno tržište i dalje ne prepoznaje rizike informacijske sigurnosti kao posebne rizike, što daje naznake kako će se oni i dalje razmatrati u sklopu „ostalih" rizika koji za posljedicu imaju prekid poslovanja
- glavni pokretač razvoja informacijske sigurnosti u Republici Hrvatskoj i dalje će biti regulatorne obaveze koje dolaze s novim Zakonom o kritičnim infrastrukturama (EU CIP), novom uredbom o elektroničkoj privatnosti (*ePrivacy*), HNB-ovom Odlukom o primjerenom upravljanju informacijskim sustavom, novim Zakonom o digitalnoj operativnoj otpornosti (*DORA*), promjenama koje donosi direktiva *NIS2* i novi prijedlog Zakona o kibernetičkoj sigurnosti
- osim navedenih obaveznih pokretača, svi akteri koji žele uspješno sudjelovati na globalnom tržištu će biti primorani dokazati svoju sigurnost i steći povjerenje putem nekih od dobrovoljnih standarda poput: *TISAX*, nove inačice *ISO/IEC 27001:2022*, ili *SOC2 Type II* atestacije i slično
- dosadašnja načela zaštite sustava na razini infrastrukture više nisu dovoljna, očekuje se snažno fokusiranje na zaštitu programskih sučelja, repozitorija i softverskih komponenti
- geopolitička situacija i inflacija će i dalje snažno utjecati na „kupovnu moć" organizacija pri nabavi sigurnosnih rješenja i usluga

- fokus u osiguranju lanaca opskrbe prijeći će s nedostupnosti ljudi, pružatelja usluga i prirodnih katastrofa na kibernetički podržane sustave, točnije, na obranu od incidenata informacijske sigurnosti i osnaživanju sposobnosti oporavka od istih
- pružatelji IT usluga iz svojih ponuda uklanjanju opcije kupovine rješenja i instalacija „*on-prem*“, snažna inflacija i prebacivanje troška iz kapitalnih investicija u operativne troškove može prouzročiti suzdržanost pri nabavi takvih rješenja i prebaciti fokus na optimizaciju iskorištenosti postojećih tehnologija i rješenja
- umjetna inteligencija i strojno učenje postali su široko dostupni, premda su još nedovoljno zrele i kontrolirane tehnologije. Već sada je primjetna javna dostupnost algoritama i metoda pomoću kojih je moguće zloupotrijebiti kapacitete umjetne inteligencije (izrada uvjerljivih *phishing* poruka e-pošte, plagiranje sadržaja, stvaranje lažnih vijesti, stvaranje polimorfnih zlonamjernih aplikacija i slično)
- komercijalizacija umjetne inteligencije naglo je proširila njezinu dostupnost za sve namjene. Očekujemo porast krađa identiteta korištenjem AI-ja i *deepfake* sintetičkih sadržaja prvenstveno jer dostupna tehnologija omogućuje vrlo jednostavno stvaranje takvih sadržaja
- nedostatak kvalificirane radne snage je i dalje prisutan te se jaz dodatno produbljuje. Obrazovni sustav ne reagira dovoljno brzo, posljedica čega će biti daljnje povećanje velike razlike u ponudi i potražnji za stručnjacima sigurnosti, daljnje jačanje pružatelja usluga i slabljenje organizacije, ali i povećavanje stručnosti samih pružatelja sigurnosnih usluga.

Kvalificirane stručnjake informacijske sigurnosti obrazovni sustav teško može brzo proizvesti, posebno s trenutačnim kurikulumom i manjkom stručne prakse. Kvalifikacije i iskustvo u području informacijske sigurnosti trenutačno se postižu dugogodišnjim radom u drugim područjima, a informacijska sigurnost je u pravilu druga karijera svakog stručnjaka informacijske sigurnosti.

Ivan Kalinić, voditelj odjela za strateško upravljanje sigurnosti



2. Napadačka perspektiva

diverto

2. NAPADAČKA PERSPEKTIVA

Provedena penetracijska testiranja u 2022. godini obuhvaćala su procjene sigurnosti raznovrsnih aplikacija i infrastruktura - od mobilnih, desktop, web aplikacija te aplikacijsko-programskih sučelja i servisa do unutarnjih, vanjskih i bežičnih infrastruktura, kao i tijekom prethodnih godina. Svrha provedenih penetracijskih testiranja bila je pronaći i iskoristiti ranjivosti kako bi se utvrdio njihov utjecaj na organizaciju te uz adekvatne preporuke pomoći pri upravljanju otkrivenim rizicima.

Penetracijska testiranja su samo dio procesa, no težina upravljanja otkrivenim rizicima odgovornost je organizacija. Organizacije bi trebale kontinuirano ulagati u razvoj sigurnosnih timova i njihovu suradnju s ostalim organizacijskim jedinicama kako bi se osigurali prihvatljivi odgovori na otkrivene rizike.

2.1. Pozitivni pomaci u 2022. godini

Geopolitička situacija utjecala je na povećani volumen i raznovrsnost skeniranja ranjivosti na infrastrukturnoj i aplikativnoj razini od strane zlonamjernih aktera, kao i povećan broj pokušaja ostvarivanja inicijalnog pristupa korištenjem metoda socijalnog inženjeringa. U svijetu su se tijekom 2022. godine dogodili sigurnosni incidenti i kod organizacija s dugogodišnjim ulaganjima u informacijsku sigurnost i osvješćivanje djelatnika, gdje su napadači upravo korištenjem tehnika socijalnog inženjeringa ostvarili inicijalni pristup do informacijskog sustava, a potom procesima enumeracije, iskorištavanjem ranjivosti, lateralnim kretanjem te eskalacijom privilegija preuzeli administrativne ovlasti.

Imajući na umu prethodnu činjenicu, organizacije prepoznaju potrebu za provođenjem kako inicijalnih, tako i dodatnih testiranja. Uz navedeno, organizacije su prihvatile naše sugestije u izmjenama načina provođenja samih penetracijskih testiranja kako bi ista što bolje simulirala aktualne prijetnje i tehnike napadača, što je vrijedno spomena i pohvale. Također, ograničenje pristupa do javno izloženih servisa, kao i osvješćivanje zaposlenika, imalo je dodatnu ulogu u smanjivanju rizika. Novootkrivene ranjivosti u softverskim i hardverskim rješenjima, kao i nove napadačke tehnike, uvijek predstavljaju dodatne izazove

i zahtjeve za implementacijom mjera za smanjenje rizika, pravovremenim instalacijama zakrpi, izmjenama u programskom kodu i konfiguracijama te kontinuiranim nadzorom nad cjelokupnom infrastrukturom.

Napadači rijetko ostvare direktan pristup do nečega što je organizacijama vitalno za poslovanje te moraju provesti niz radnji kako bi ostvarili pristup do ključnih sustava ili informacija. Iskorištavanja ranjivosti na aplikativnoj razini, ako ne govorimo o ranjivostima u samim softverskim komponentama, zahtijevaju od napadača da enumeriraju aplikacije, te pokušaju pronaći ranjivosti u istima. Stoga je, uz redovito samostalno skeniranje ranjivosti, provođenje penetracijskih testiranja i implementaciju slojevitog sigurnosnog modela, nužno da organizacije imaju centralizirano prikupljanje dnevničkih zapisa te uspostavljen proces nadzora, praćenja i analize prikupljenih podataka. U svemu navedenome vidljivi su pozitivni pomaci u usporedbi s 2021. godinom.

2.2. Predviđanje kretanja testiranja sigurnosti za 2023. godinu

Uslijed povećanog broja kibernetičkih napada očekuje se daljnje podizanje svijesti o informacijskoj sigurnosti te više proaktivnog djelovanja - angažmanom vanjskih partnera za informacijsku sigurnost i putem namjenskih timova organizacija orijentiranih isključivo na informacijsku sigurnost.

- daljnje povećanje broja sigurnosnih testiranja kroz scenarije *Assume-Breach*
- nastavak rasta provođenja vježbi *Purple Teaming*
- implementacija usluge upravljanja ranjivostima – *Vulnerability Management as a Service*
- povećanje broja samostalnih i redovitih skeniranja ranjivosti putem automatiziranih alata te pravovremeno uklanjanje otkrivenih ranjivosti.

2.3. Sigurnosna testiranja na infrastrukturnoj razini

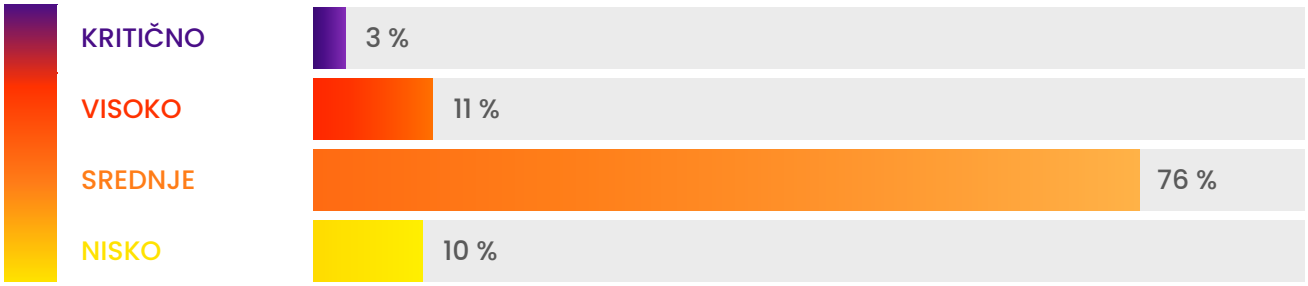
Ranjivosti na infrastrukturnoj razini koje su tijekom 2022. godine omogućile inicijalni pristup do infrastrukture ili pristup do korisničkih računa bile su:

- iskorištavanje mrežnih protokola u svrhu provođenja napada Čovjekom u sredini (MITM) i „*Relay*“ napada
- inicijalno zadane zaporke ili zaporke koje se mogu jednostavno odgonetnuti
- ranjivosti na izloženim servisima čije iskorištavanje omogućava inicijalni pristup sustavu bez prethodne autentifikacije
- neadekvatna politika zaporki i upravljanja korisničkim računima, što napadačima olakšava odgonetanje korisničkih vjerodajnica.

Nakon ostvarivanja inicijalnog pristupa, razne konfiguracijske ranjivosti omogućile su daljnju eskalaciju privilegija i lateralno širenje, poput:

- servisnih računa sa slabim lozinkama i višim privilegijama
- ranjivih predložaka certifikata na servisima *Active Directory Certificate Services*
- iskorištavanja mrežnih autentifikacijskih mehanizama za provođenje napada *relay* i napada preusmjeravanjem prometa
- raznih konfiguracijskih propusta i neadekvatnih privilegija na objekte unutar *Active Directory* domene
- neadekvatnih privilegija na dijeljenim mrežnim direktorijima koji sadrže korisničke vjerodajnice u čistom tekstu, kriptografske sažetke zaporki ili konfiguracijske datoteke s istima
- napada na korisnike s privilegijama čitanja zaporki iz rješenja za upravljanje lozinkama.

UDIO RANJIVOSTI NA INFRASTRUKTURAMA



Najčešće korištene tehnike:

- *Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay* https://attack.mitre.org/techniques/T1557/001/
- *Exploit Public-Facing Application* https://attack.mitre.org/techniques/T1190/
- *Brute Force: Password Guessing* https://attack.mitre.org/techniques/T1110/001/
- *Brute Force: Password Cracking* https://attack.mitre.org/techniques/T1110/002/
- *Exploitation of Remote Services* https://attack.mitre.org/techniques/T1210/
- *Unsecured Credentials: Credentials In Files* https://attack.mitre.org/techniques/T1552/001/
- *Unsecured Credentials: Credentials in Registry* https://attack.mitre.org/techniques/T1552/002/

- *Credentials from Password Stores* https://attack.mitre.org/techniques/T1555/
- *Data from Network Shared Drive* https://attack.mitre.org/techniques/T1039/
- *Valid Accounts: Default Accounts* https://attack.mitre.org/techniques/T1078/001/
- *Valid Accounts: Local Accounts* https://attack.mitre.org/techniques/T1078/003/
- *Use Alternate Authentication Material: Pass the Hash* https://attack.mitre.org/techniques/T1550/002/
- *Use Alternate Authentication Material: Pass the Ticket* https://attack.mitre.org/techniques/T1550/003/
- *Steal or Forge Authentication Certificates* https://attack.mitre.org/techniques/T1649/
- *Steal or Forge Kerberos Tickets: Kerberoasting* https://attack.mitre.org/techniques/T1558/003/
- *Steal or Forge Kerberos Tickets: AS-REP Roasting* https://attack.mitre.org/techniques/T1558/004/
- *OS Credential Dumping: LSASS Memory* https://attack.mitre.org/techniques/T1003/001/
- *OS Credential Dumping: Security Account Manager* https://attack.mitre.org/techniques/T1003/002/
- *OS Credential Dumping: NTDS* https://attack.mitre.org/techniques/T1003/003/
- *OS Credential Dumping: DCSync* https://attack.mitre.org/techniques/T1003/006/
- *Account Manipulation: Service Principal Manipulation* https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-2/

2.4. Sigurnosna testiranja desktop i web aplikacija te servisa

Većina ranjivosti pronađenih tijekom penetracijskih testiranja desktop i web aplikacija te servisa odnose se na pogrešnu ili neadekvatnu konfiguraciju web poslužitelja. Za primjer možemo uzeti HTTP sigurnosna zaglavlja čiji nedostatak smanjuje uspješnost obrane od napada, dok njihovo pravilno postavljanje može biti učinkovit način za jačanje sigurnosti aplikacija.

Također, učestalo je i korištenje slabijih kriptografskih algoritama, što povećava rizik od uspješnog provođenja napada čovjekom u sredini (MITM).

U usporedbi s prethodnim godinama, primjetan je porast ranjivosti koje se odnose na korištenje zastarjelih i ranjivih softverskih komponenti, što ukazuje na nedostatak pravilne i dosljedne implementacije sigurnosnih kontrola kroz životni ciklus razvoja softvera (SDLC) te nedostatak procesa za upravljanje ranjivostima.

Pogrešna ili neadekvatna konfiguracija web poslužitelja te korištenje zastarjelih i ranjivih softverskih komponenata posljedično ukazuje na problem nedostatka stručnjaka za kibernetičku sigurnost, što za organizacije predstavlja jednu od najvećih ranjivosti.

Približno 10 % pronađenih ranjivosti odnosi se na nedovoljne kontrole pristupa kao što su:

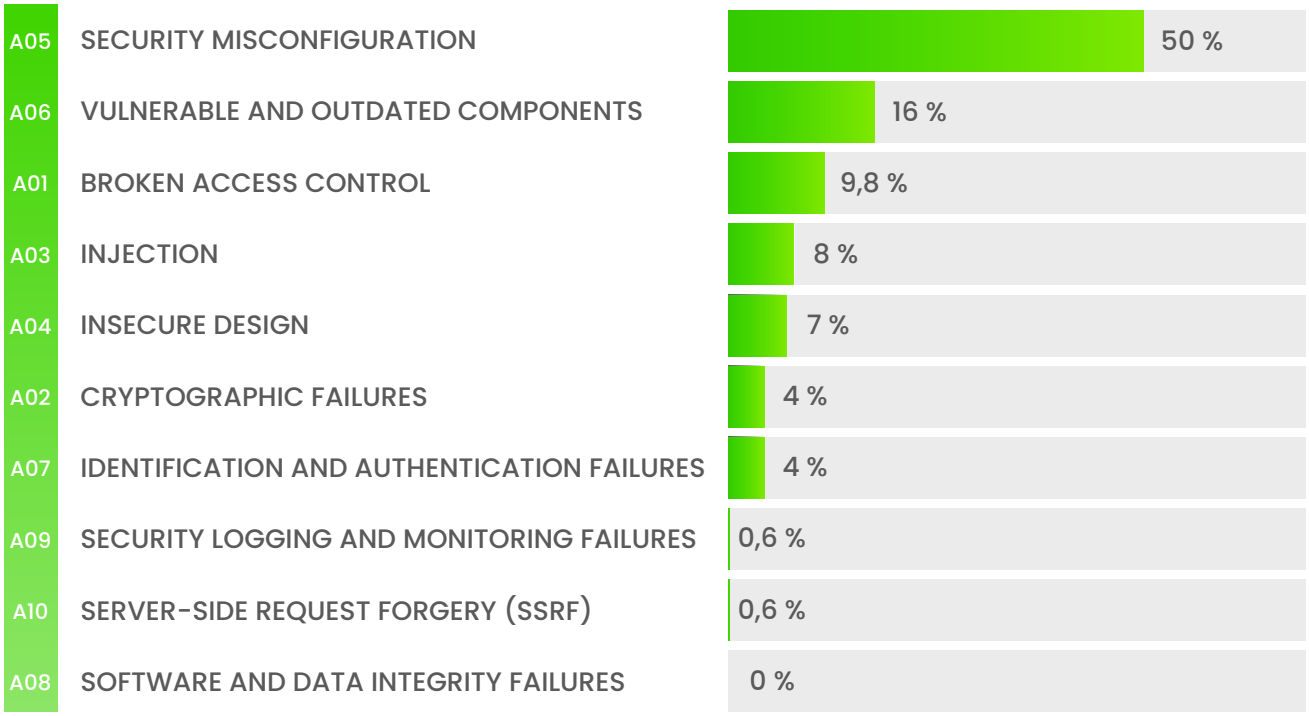
- kršenje pravila najmanjih mogućih privilegija korisnika gdje bi pristup trebao biti dozvoljen samo određenim funkcionalnostima
- zaobilaženje kontrola pristupa promjenom HTTP zahtjeva kako bi se pristupilo osjetljivim podacima kojima korisnik ne bi trebao imati pristup
- pregled ili izmjena tuđeg korisničkog računa
- neautentificiran ili neautoriziran pristup povjerljivim informacijama.

Povećanje broja ranjivosti koje se odnose na nedostatak kontrole pristupa može upućivati na to da se organizacije suočavaju s izazovima rasta i održivosti procesa poslovanja.

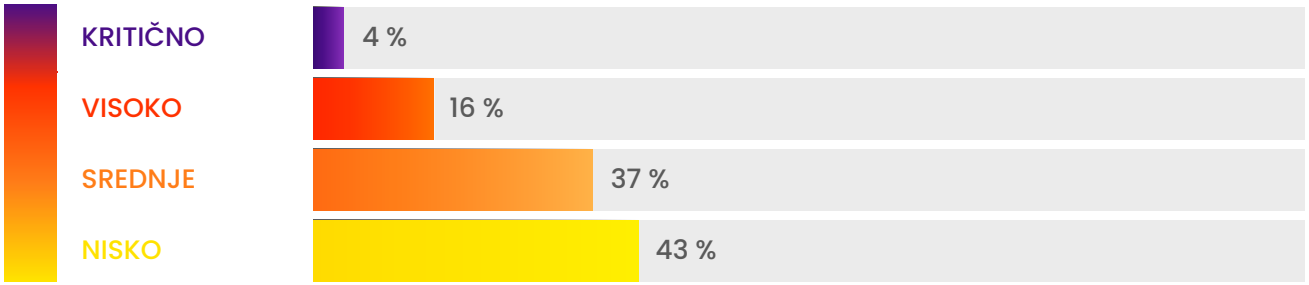
Oko 8 % pronađenih ranjivosti odnosi se na ranjivosti umetanja proizvoljnog koda, gdje korisnikov unos nije adekvatno provjeren, filtriran, odnosno „pročišćen“ od strane aplikacije ili servisa, što je dovelo do:

- pristupa informacijama pohranjenim u bazama podataka
- krađe, odnosno oponašanja tuđe korisničke sjednice
- pristupa operativnom sustavu
- izvršavanja zlonamjernog koda u kontekstu preglednika.

UDIO RANJIVOSTI PO OWASP TOP 10



PREMA KRITIČNOSTI RANJIVOSTI



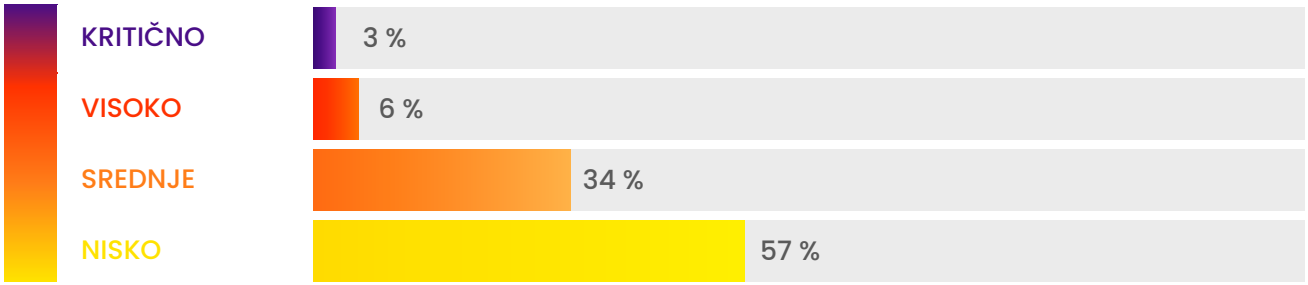
2.5. Mobilne aplikacije

Kod mobilnih aplikacija, najveći broj pronađenih ranjivosti odnosi se na nesigurnu pohranu osjetljivih informacija. Takve informacije uključuju podatke o kreditnim karticama, stanjima računa i osobnim identifikacijskim podacima kao što su OIB ili PIN. Iako se navedeni podaci moraju negdje pohranjivati, preporučuje se provjeriti načine na koji mobilne aplikacije, operativni sustavi te biblioteke koje su u upotrebi upravljaju sljedećim značajkama:

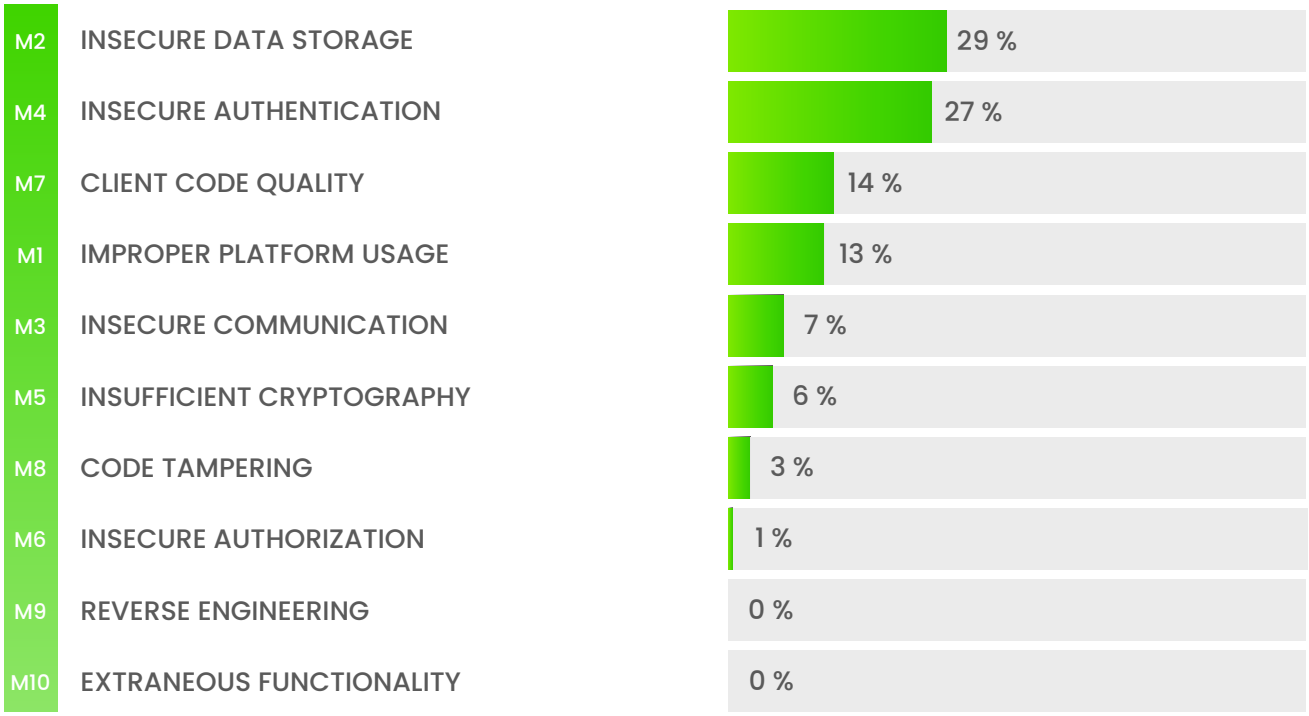
- URL međuspremanje
- međuspremanje podataka tipkovnice
- odlazak aplikacije u pozadinu
- nesigurna pohrana podataka
- analitika podataka koji se šalju trećim stranama.

Također, veliki broj pronađenih ranjivosti odnosi se na nesigurnu autentifikaciju, što uključuje ranjivosti poput enumeracije tokena i adresa e-pošte, slanja osjetljivih podataka putem URL-a, omogućenog korištenja jednostavnog PIN-a i slično. Ostale ranjivosti mobilnih aplikacija uključuju korištenje slabijim kriptografskim algoritmima, nedostatak otkrivanja ovlasti te neispravnu provjeru SSL certifikata. Najučestalije ranjivosti mobilnih aplikacija bile su:

PREMA KRITIČNOSTI RANJIVOSTI



RANJIVOSTI PREMA OWASP MOBILE TOP 10



Promatrajući trend ranjivosti mobilnih aplikacija, mogu se uočiti napori u suradnji između sigurnosnih i razvojnih odjela koji prije svega moraju zadovoljiti druge prioritete poput rokova, poslovnih ciljeva, strategija za izlazak na tržište i sl. Skretanjem pozornosti na sigurnosne prakse i kontinuiranom edukacijom zaposlenika moguće je umanjiti rizike koje mobilne aplikacije predstavljaju za poslovanje.

Sigurnosna testiranja, kao i informacijski sustavi organizacija, moraju biti sklona promjenama. Napadači učestalo mijenjaju aktualne taktike i tehnike te je nužno uvoditi promjene u načinu provođenja sigurnosnih testiranja kako bi organizacije na vrijeme mogle nadograditi postojeće ili implementirati dodatne sigurnosne mjere. Od iznimne je važnosti da se sigurnosni incidenti otkriju na vrijeme te da su organizacije u tim trenutcima spremne pravovremeno odgovoriti na iste, a tome su znatno pridonijele provedene Purple Teaming vježbe.

Ivan Račić, voditelj napadačkog tima

3. Obrambena perspektiva

diverto

3. OBRAMBENA PERSPEKTIVA

Vlastito iskustvo nam pokazuje da je 2022. godina bila znatno zahtjevnija od 2021. godine u provođenju obrambenih aktivnosti, i to gotovo kod svih korisnika kojima pružamo usluge Sigurnosno-operativnog centra. Uvođenje novih tehnologija kojima naši korisnici unapređuju vlastito poslovanje, povećani broj prijetnji, a pri tome i kontinuirani rast tehnika napada iziskuju vrlo intenzivnu suradnju Diverta i korisnika.

U 2022. godini, bilježimo rast broja SOC-ova kao i broja nadziranih uređaja u Diverto SOC-ovima od 55 % u odnosu na prethodnu 2021. godinu.

SLIKA 2 *Porast broja uređaja u SOC-u, [Izvor: Diverto]*

3.1. Ključni pokazatelji u promatranom razdoblju

Donosimo najvažnije pokazatelje trenutnog stanja sigurnosti iz obrambene perspektive i izazove s kojima smo se susretali zaključno s 2022. godinom.

- upravljanje ranjivostima je nedostatno. Bilo da su one programske ili konfiguracijske prirode, ranjivosti se moraju provjeravati češće i uklanjati znatno brže od trenutka uočavanja. Uočili smo da je važno primijeniti takav pristup na ključne sustave, ali isto tako i na one, „manje važne" sustave u organizacijama. Uočili smo da vrijeme od trenutka javne objave *exploita* (pod uvjetom da je to poznat podatak) pa do prvog zabilježenog pokušaja iskorištavanja pripadajuće ranjivosti „pada" na svega nekoliko sati. Smatramo da se taj vremenski interval umanjio zahvaljujući sve većem broju napadačkih grupa na internetu, odnosno onih koji znaju iskorištavati ranjivosti

- nepotpun popis imovine je ozbiljan nedostatak kod većine organizacija koje žele sveobuhvatnu zaštitu svojih servisa. Popis imovine se mora sustavno obnavljati i održavati s jasnom definicijom ključnih servisa i njegovih komponenti. Teško je štititi nešto, ako ne znate što sve posjedujete i na što to može utjecati

- sigurnosna ojačanja na radnim stanicama za ulazne periferne jedinice su manjkava. Zlonamjerni kod *Raspberry Robin* kod je u drugoj polovici 2022. godine vrlo učinkovito djelovao čak i na računalima gdje postoji kvalitetna antivirusna zaštita. Širio se po računalnoj mreži korištenjem USB memorije na pojedinim radnim stanicama, uočeno je kontinuirano djelovanje u većem broju štićenih organizacija koje su dio Diverto SOC-a

- sigurnosne komponente sustava kao što su vatrozidi, IPS, Proxy uređaji i slično nisu potpuno iskorišteni sa svim svojim mehanizmima zaštite i često izostaje nužna napredna konfiguracija. Organizacije koje posjeduju takve uređaje redovito ih nadograđuju novim inačicama operativnih sustava i obnavljaju ih novijim modelima, ali to samo po sebi nije dovoljno

- povećane su aktivnosti zlonamjernih zaposlenika (engl. *insider*) u organizacijama, to smo uočili i izlaskom na incidente gdje Diverto nema SOC, kao i u svakodnevnim operacijama SOC-a. Takvi zaposlenici dovoljno dobro poznaju sustav pa tako znaju i koji podaci mogu biti korisni i kako neopaženo djelovati u radnjama neovlaštenog kopiranja. Dodatno, postoje i zaposlenici koji iz vlastitog neznanja ugrožavaju radno okruženje često preuzimajući aplikacije s interneta koje u sebi sadrže neželjeni kod (*PUP/PUA*)

- znatno je manji utjecaj *ransomwarea* na radna okruženja nego u 2021. godini, ali smo i dalje bilježili mnogobrojne pokušaje proboja u kojima su napadači imali namjeru zaključati datoteke

- i dalje je česta praksa nedovoljna zaštita poslužitelja, čak i onda kada se nalaze u odgovarajućim izoliranim okruženjima (*DMZ*). Navodimo tri glavna nedostatka: poslužitelji nemaju antivirusnu zaštitu, imaju pristup internetu iako to nije potrebno za funkcioniranje u internoj mreži i ne upotrebljavaju se vatrozidi na samom poslužitelju koji bi spriječili napadača u lateralnom širenju po drugim sustavima jednom kada napadač uđe u izolirano okruženje.

I dalje vidimo nedovoljnu iskorištenost postojećih sigurnosnih komponenti - korisnik kupi uređaj, ali je konfiguracija sustava nedostatna.

„Prijetnje u okruženju, odnosno izazovi s kojima se organizacije susreću sve manje su rješive kroz tehnološka rješenja, već uspjesi u obrani od napadača uvelike ovise o vidljivosti, kompleksnosti (ili jednostavnosti) sigurnosnih informacija i stručnosti ljudi koji brane organizaciju od napadača. Organizacije koje imaju kompletnu sliku svoje površine napada prikupljaju podatke iz više izvora u jasne i djelotvorne sigurnosne informacije te imaju kombiniranu unutarnju i vanjsku ljudsku stručnost – uvelike su i brže i uspješnije u obrani od današnjih prijetnji.“

Ivan Ivković, voditelj obrambenog tima

3.2. Percepcija usluge SOC-a je pozitivna

Diverto je u 2022. godini značajno pojačao SOC kapacitete u broju ljudi i unapređenju znanja, a isto tako se proširio i na nova radna okruženja. Možemo slobodno reći da postoji želja za unapređenjem sigurnosti i u radnim okruženjima gdje zakonska obveza nije glavni pokretač promjena. To samo pokazuje da svijest o važnosti kibernetičke sigurnosti poslovanja raste.

Postojeći korisnici naših SOC usluga su prepoznali mnogobrojne situacije u kojima je SOC reagirao pravovremeno i spriječio proboje već u prvom koraku.

Broj provedenih istraga je povećan za 30 % u 2022. godini u odnosu na 2021. godinu. To je logičan rast, s obzirom na znatno povećane kapacitete SOC-a u broju uređaja koje pratimo.

SLIKA 3 *Porast broja provedenih istraga, [Izvor: Diverto]*

3.3. Ljudska komponenta je ključna u SOC operacijama

Da SIEM sam po sebi nije zadovoljavajuća tehnologija za zaštitu sustava, pokazuju i rezultati *Threat Hunting* operacija koje provode analitičari Diverta. *Threat Hunting* koji je vođen hipotezama (engl. *hypotesis-driven*), a ne pokazateljima ugroženosti (engl. *IOC-driven*) daje znatno bolje rezultate u pronalasku zlonamjernog djelovanja. Divertovi analitičari su tako u 2022. godini pronašli mnogobrojne ugroze kod korisnika čije djelovanje nisu zabilježili korisnikovi sustavi antivirusne zaštite, vatrozida, IPS-a i slično.

3.4. *DevSecOps*

DevSecOps je iznimno važan pristup za zaštitu informacijske sigurnosti u organizacijama, a posebno za zaštitu aplikativne razine. *DevSecOps* se temelji na konceptu integriranja sigurnosti u cijeli životni ciklus razvoja i isporuke softverskih rješenja, od samog početka do kraja procesa. Ovaj pristup osigurava da se sigurnost ne tretira kao naknadna misao, već kao integralni dio svakog koraka u razvoju softvera, uključujući planiranje, programiranje, testiranje i isporuku. Time se postiže brži i učinkovitiji razvoj softvera, a istovremeno se osigurava sigurnost i sprečavaju ranjivosti i napadi. Uzimajući u obzir stalno rastuće prijetnje kibernetičkih napada te sve složenije napade, *DevSecOps* postaje neophodan za organizacije koje žele osigurati pouzdanost i sigurnost svojih softverskih rješenja.

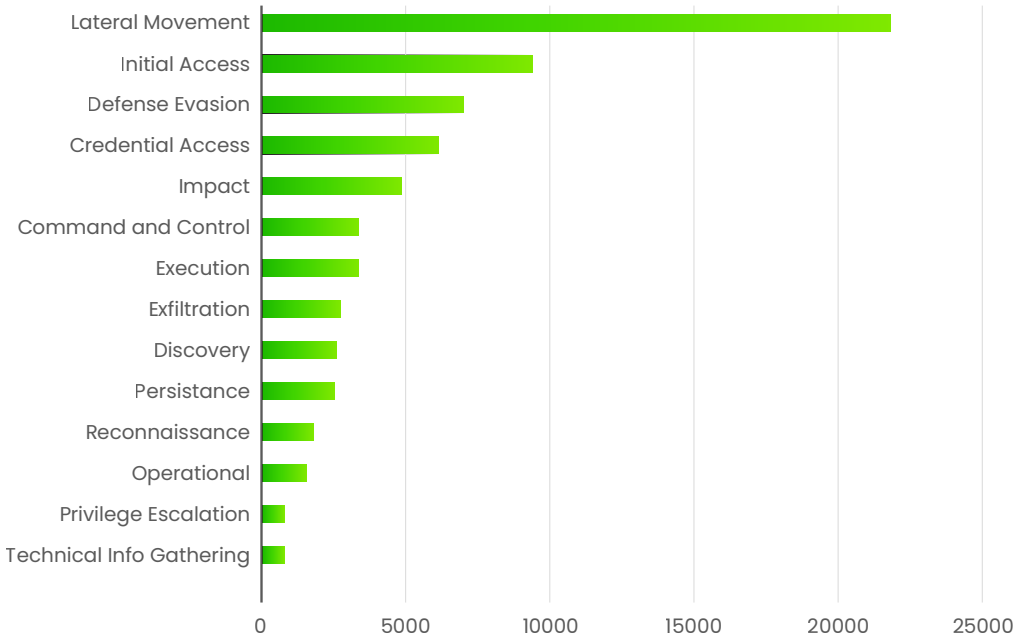
DevSecOps koristi *CI/CD* pristup za integriranje sigurnosti u cijeli proces isporuke softvera. To znači da se sigurnost testira i integrira tijekom cijelog procesa, uključujući automatizirane sigurnosne provjere tijekom faze izgradnje i testiranja. Na ovaj način se osigurava da se ranjivosti i sigurnosni propusti otkriju i rješavaju ranije u procesu razvoja, što za posljedicu ima sigurnija softverska rješenja koja se brže isporučuju korisnicima.

Automatizacija i koncepti IaC-a (engl. Infrastructure as Code) su dio svakodnevnice za DevSecOps timove. Ubrzanje u razvoju i sistematizaciji donosi nove rizike s kojima treba upravljati poput trovanja lanca opskrbe (engl. Supply chain poisoning) i izloženosti vjerodajnica. Stoga se moraju pratiti sigurnosne mjere i preporuke najbolje prakse kroz cijeli životni ciklus DevSecOpsa i biti integralni dio svakog njegovog procesa te svakako iskoristiti alate koji su nam široko dostupni, poput DAST-a, SAST-a i SCA.

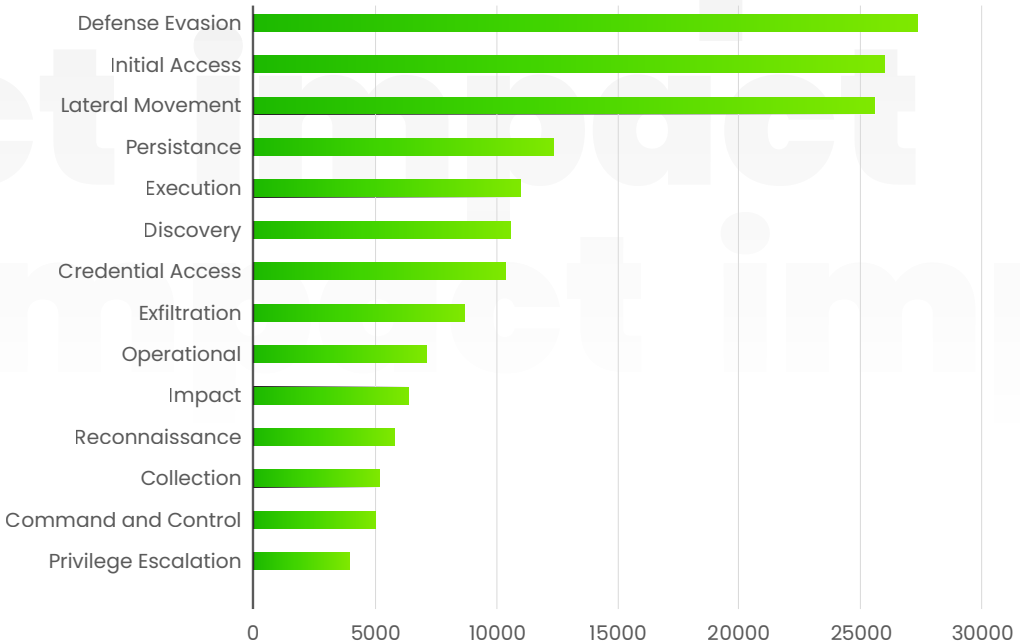
Omar El Tabari, voditelj DevSecOps tima

3.5. Utjecaj na radne procese štićenih organizacija

Važno je napomenuti da nismo imali situacije u kojima je napadač ostvario negativan utjecaj na poslovanje (*Impact*), a da pri tome sustavi otkrivanja u SOC-u nisu ništa zabilježili. Dodatno, značajnim pojačanjem stručnosti i broja ljudi za *Tier 1* operacije u 2022. godini, osjetno smo umanjili vrijeme djelovanja napadača u štićenim organizacijama. Tako je, primjerice, četrnaesta grupa tehnika *Impact* (MITRE Att&ck okvir) bila peta najčešća u 2021. godini po mehanizmu otkrivanja, dok je u 2022. godini tek deseta. To je dobar pokazatelj i za nas kao pružatelja usluga, ali i za naše korisnike.



SLIKA 4 *Najčešći alarmi prema taktikama MITRE att&ck u 2021., [Izvor: Diverto]*



SLIKA 5 *Najčešći alarmi prema taktikama MITRE att&ck u 2022., [Izvor: Diverto]*

4. Integralna perspektiva – *Purple Teaming*

diverto

4. INTEGRALNA PERSPEKTIVA – *PURPLE TEAMING*

U 2022. godini provedene su *Purple Teaming* vježbe za različite organizacije kroz nekoliko različitih scenarija poput:

- simulacije napadača koji je ostvario pristup do unutarnje infrastrukture putem VPN-a
- simulacije napadača koji je ostvario pristup do reprezentativne radne stanice zaposlenika
- simulacije napada treće strane (engl. *Supply chain*) kojoj je omogućen fizički pristup organizaciji
- simulacije napada na imeničke servise *Active Directory*.

Svrha provođenja *Purple Teaming* vježbi je simulirati stvarne taktike i tehnike napadača kako bi se:

- identificirale slijepe točke trenutačne sigurnosne razine
- unaprijedilo otkrivanje i sprječavanje sigurnosnih incidenata
- skratilo vrijeme otkrivanja i odgovora na sigurnosne incidente
- steklo vrijedno iskustvo obrambenih timova u slučaju stvarnih sigurnosnih incidenata.

Purple Teaming vježbe provode se kombinirajući simultani rad Divertovog napadačkog (*Red*) i organizacijskog obrambenog (*Blue*) tima, a aktivnosti koje se provode su relevantne za specifičnu industriju, zemljopisni položaj i veličinu organizacije.

Purple Teaming vježbe provode se koristeći *Assume Breach* način razmišljanja i metodologiju. Ona pomaže kao vodič prilikom usmjeravanja ulaganja u informacijsku sigurnost, donošenju odluka o dizajnu te operativnih sigurnosnih praksi. Također, ograničava povjerenje u aplikacije, usluge, identitete i mreže tretirajući ih sve – i unutarnje i vanjske – kao nesigurne i vjerojatno već ugrožene.

Kroz provedene vježbe, doneseni su sljedeći zaključci:

- iako postoje razna sigurnosna rješenja, nadzorni sustavi, SIEM-i, zaštite krajnjih točaka, mrežni senzori te napredni vatrozidi i *proxy* sustavi, oni često nisu podešeni na adekvatan način te je broj otkrivanja provedenih napadačkih aktivnosti vrlo nizak. Rijetko je problem u samim rješenjima, već u nedostatku adekvatnog podešavanja, testiranja i edukacije djelatnika koji se njima koriste, kao i nedostatak stručne radne snage u organizacijama
- sigurnosni incidenti bi se u većini slučajeva mogli rekonstruirati, ali ih se ne bi primijetilo na vrijeme
- implementirana sigurnosna rješenja mogu se s vremenom zaobići te se ne smije oslanjati isključivo na njih. Sigurnosni timovi su ključan faktor pravovremenog otkrivanja sigurnosnih incidenata
- nedostatak cjelodnevnog nadzora i reakcije ili pravovremene reakcije na temelju slanja obavijesti o sumnjivim aktivnostima napadaču omogućava kompromitaciju sustava izvan radnog vremena organizacije. Nerijetko je potrebno kratko vrijeme da napadač ostvari svoj cilj te je do prvog pregleda nadzornih sustava idućeg radnog dana često već prekasno
- komunikacija prema napadačkim centrima *Command & Control* te eksfiltracija podataka rijetko se primijeti
- zastarjeli uređaji i operativni sustavi često nisu podržani od strane nadzornih rješenja te predstavljaju slijepe točke u organizacijama
- nedostatak obogaćivanja dnevničkih zapisa te ograničena pokrivenost sustava putem nadzornih agenata
- nepostojeća ili nedovoljna ulaganja u sigurnosne timove u vidu dodatnih edukacija te sudjelovanja u *hands-on* vježbama.

Zaključno, implementirana sigurnosna rješenja su kao i pričuvna pohrana – ako nisu testirana, može se smatrati da ne ispunjavaju svrhu. Dodatni izazov je što se otkrivanje u većini slučajeva temelji na poznatome (engl. *Known Bad*). Stoga su ulaganje u sigurnosne timove, samostalno provođenje vježbi od strane organizacije ili u suradnji s vanjskim partnerima te suradnja timova unutar organizacije ključni faktori za podizanje razine sigurnosti, otkrivanje odstupanja od uobičajenih aktivnosti te pravovremeno odgovaranje na incidente.

5. Pokazatelji

diverto

5. POKAZATELJI

U nastavku izdvajamo detaljnije pokazatelje specifične za informacijsku i kibernetičku sigurnost.

5.1. Percepcija rizika

UVOD

U protekloj, 2022. godini, Diverto je započeo s godišnjim provođenjem istraživanja o percepciji informacijske i kibernetičke sigurnosti u Republici Hrvatskoj. Namjera nam je istraživanje provoditi početkom svake godine za prošlu godinu, s ciljem praćenja trendova u informacijskoj i kibernetičkoj sigurnosti Republici Hrvatskoj. S obzirom da je ove, 2023. godine, istraživanje provedeno drugi put, moguće je uočiti neke zanimljive razlike (buduće trendove) u usporedbi 2021. i 2022. godine.

U nastavku možete pročitati zanimljive uvide te proučiti grafičke i slikovne prikaze promjena u percepciji informacijske i kibernetičke sigurnosti u Republici Hrvatskoj za 2021. i 2022. godinu.

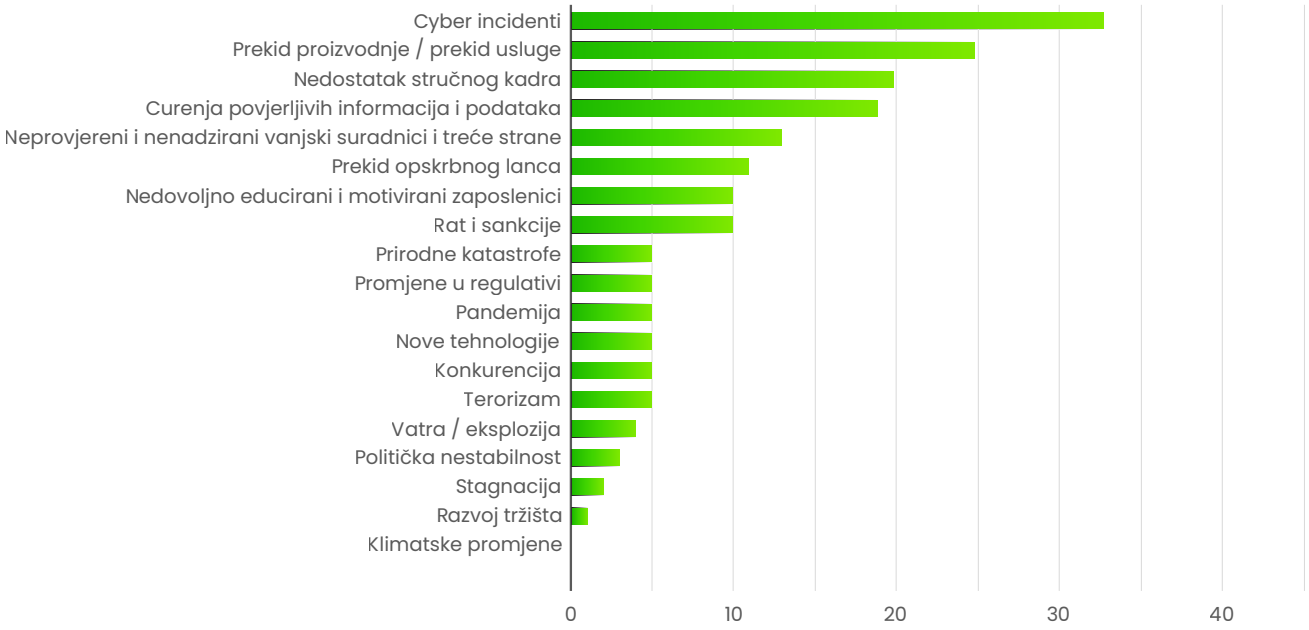
Neke od važnijih promjena odnose se na:

- rangiranje kibernetičkih incidenata (ponovno na prvom mjestu percipiranih rizika)
- porast broja tvrtki koje imaju sustav upravljanja informacijskom/kibernetičkom sigurnošću
- porast udjela IT budžeta koji se troši na informacijsku/kibernetičku sigurnost
- porast broja tvrtki koje testiraju/provjeravaju stanje informacijske sigurnosti
- porast svijesti o sigurnosnim incidentima uz istovremeni porast broja tvrtki koje su imale značajnije incidente
- porast posljedica sigurnosnih incidenata
- porast broja tvrtki koje imaju definiran i uvježban proces odgovora na incidente i drugo.

Treba napomenuti i to da je ove godine istraživanje provedeno i na području Slovenije za 2022. godinu, s obzirom na znatno proširenje poslovnih aktivnosti i na tom području.

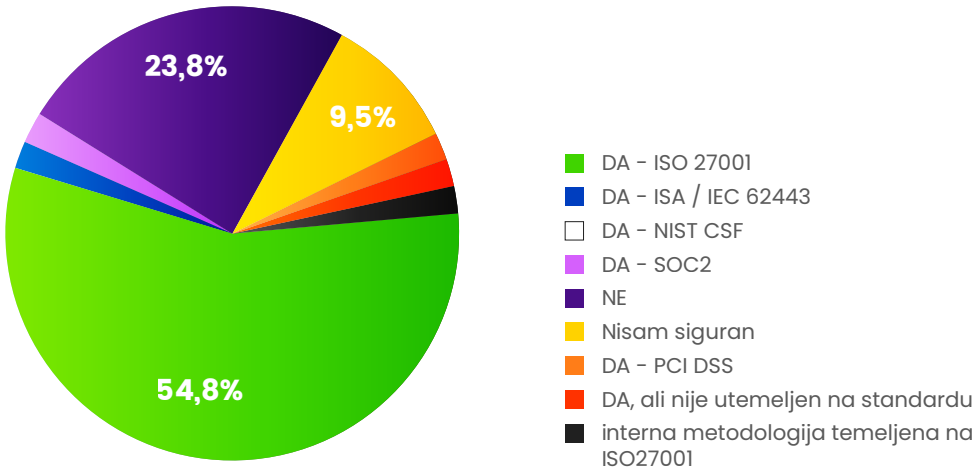
NAJVAŽNIJI UVIDI

Prema Vašem razmišljanju, što predstavlja najveći rizik za Vašu organizaciju? Možete izabrati više odgovora.



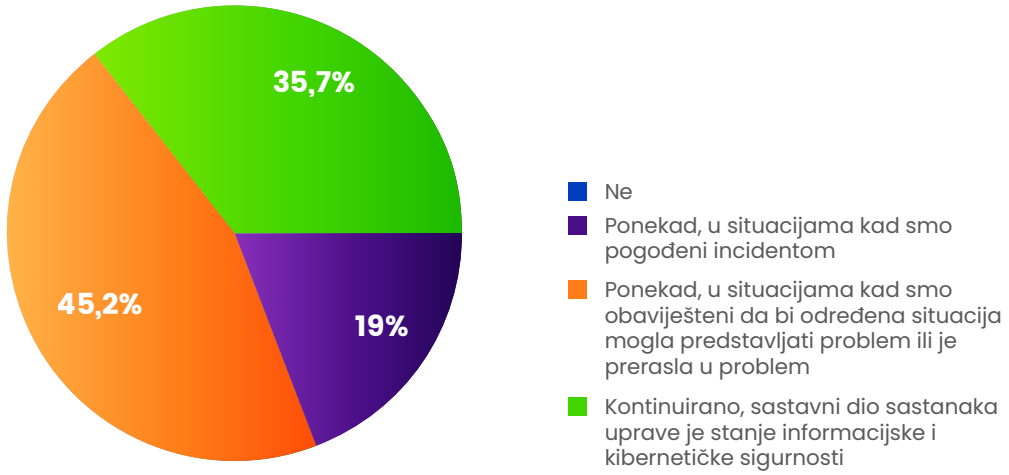
Tvrtke i ove i prošle godine stavljaju kibernetičke incidente na prvo mjesto percipiranih rizika. Osim toga, raste i osviještenost u svezi rizika kibernetičkih incidenata: porast sa 70 % na 78,6 % (2022./2023.).

Imate li uspostavljen sustav upravljanja informacijskom/kibernetičkom sigurnošću (ISMS/CSMS) i ako imate, na čemu je baziran?



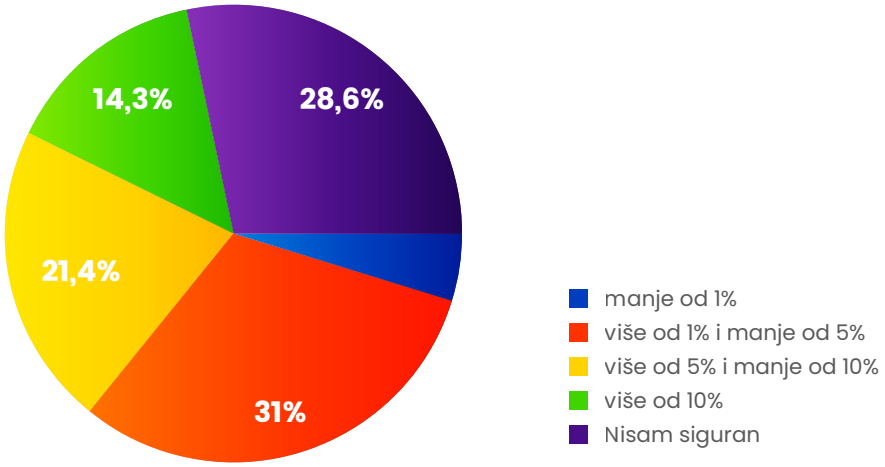
Povećava se broj tvrtki koje imaju sustav upravljanja informacijskom/kibernetičkom sigurnošću. Porast tvrtki s implementiranom standardom ISO 27001 s 51,7 % na 54,8 % (2022./2023.). Istovremeno se smanjuje broj tvrtki koje nemaju sustav upravljanja informacijskom/kibernetičkom sigurnošću: smanjenje s 30 % na 23,8 % (2022./2023.)

Raspravlja li se na sastancima Vaše uprave o pitanjima informacijsko/kibernetičke sigurnosti?



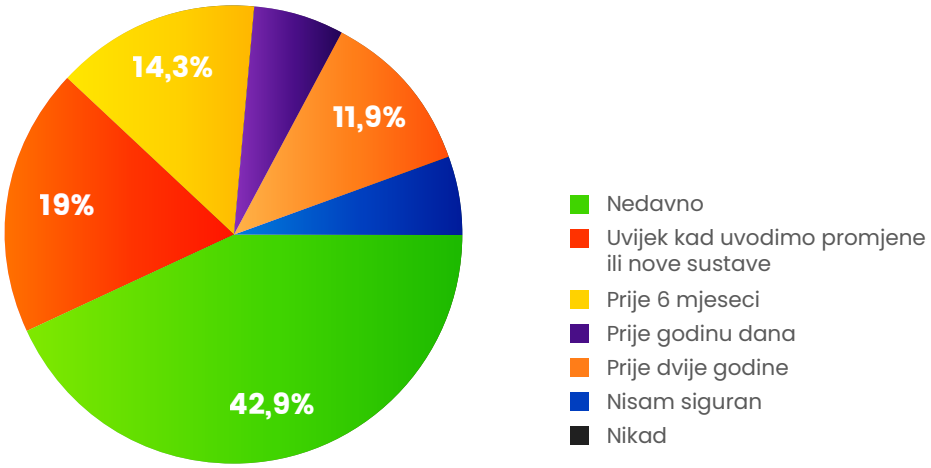
Sve organizacije (100 %) u raznim situacijama (kontinuirano / ponekad / nakon incidenta) na sastancima uprave raspravljaju o pitanjima informacijske/kibernetičke sigurnosti: porast u sva tri segmenta (2022./2023.). Ni jedan ispitanik u anketi (2023.) nije odgovorio „NE“: prošle godine 8,3 % (2022.).

Koji postotak IT budgeta trošite na informacijsko/kibernetičku sigurnost?



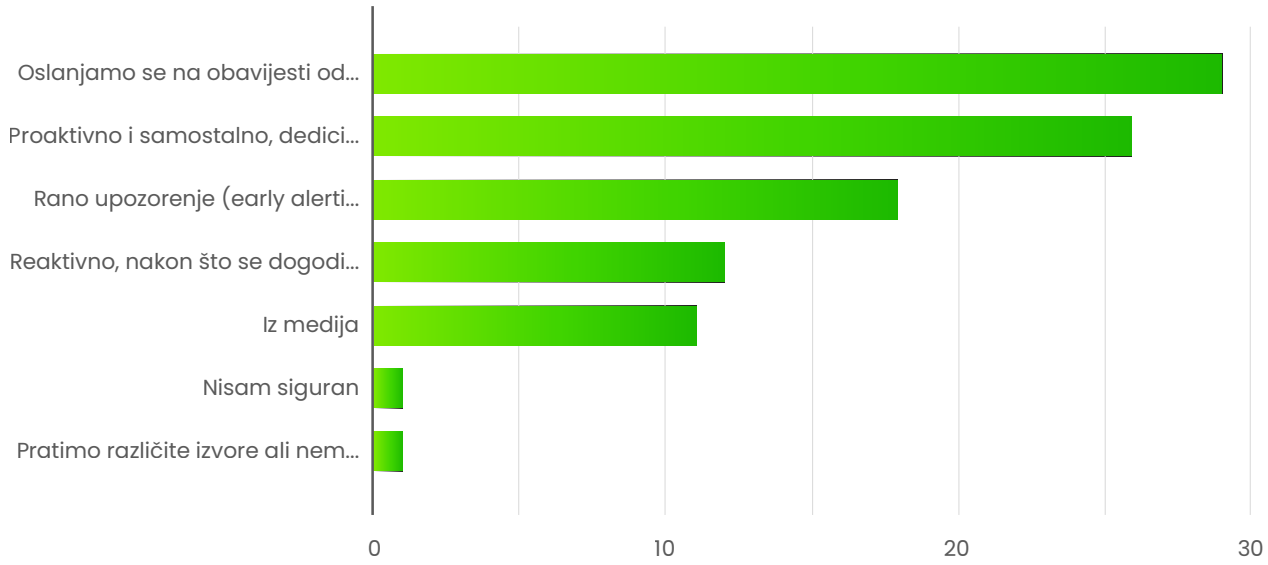
Evidentan je porast IT budžeta koji se troši na informacijsku/kibernetičku sigurnost: više od 10 % budžeta (s 11,7 % na 14,3 % tvrtki); više od 5 % i manje od 10 % budžeta (s 15 % na 21,4 %); više od 1 % i manje od 5 % budžeta (s 26,7 % na 31 % tvrtki). Smanjio se broj tvrtki koje troše manje od 1 % IT budžeta na informacijsku/kibernetičku sigurnost: s 18,3 % na 4,8 % (2022./2023.).

Kada ste zadnji put testirali/provjerili stanje informacijske sigurnosti u Vašoj organizaciji?



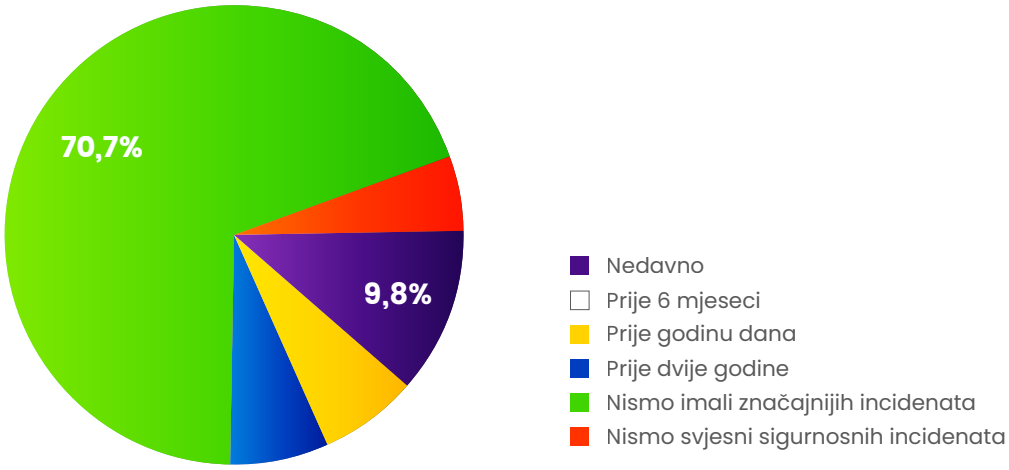
Raste broj organizacija koje uvijek testiraju/provjeravaju stanje informacijske sigurnosti kada uvode promjene ili nove sustave. Porastao je i broj onih koje to čine unazad 6 mjeseci (usporedba 2022./2023.).

Načini kako se informirate o prijetnjama i ranjivostima Vaših sustava?
Možete izabrati više odgovora.



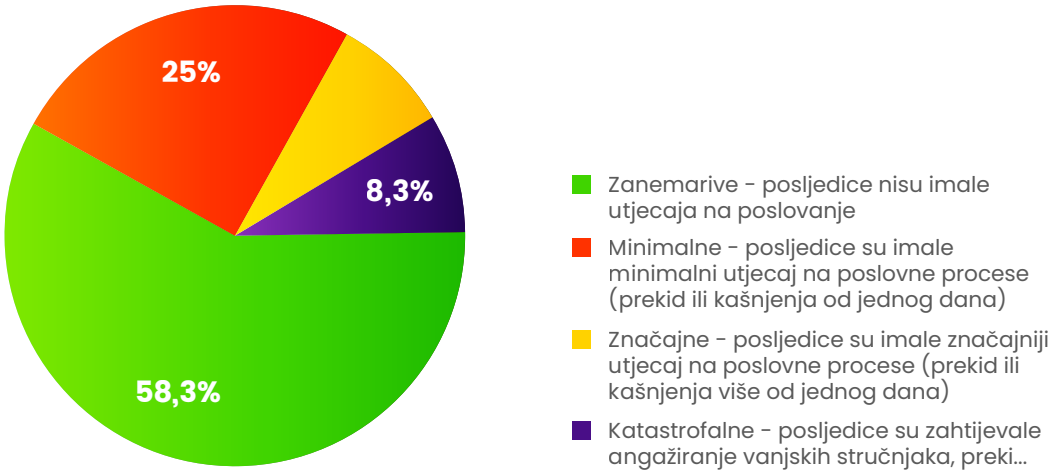
Vidljiv je porast proaktivnih i formalnih načina informiranja o prijetnjama i ranjivostima sustava te smanjenje reaktivnog pristupa i informiranja iz medija (usporedba 2022./2023.).

Jeste li imali značajnijih incidenata informacijske/kibernetičke sigurnosti? (Značajniji incident može biti na primjer: nedostupnost ili gubitak podataka u...nje podataka koje je izazvalo financijske kazne...)



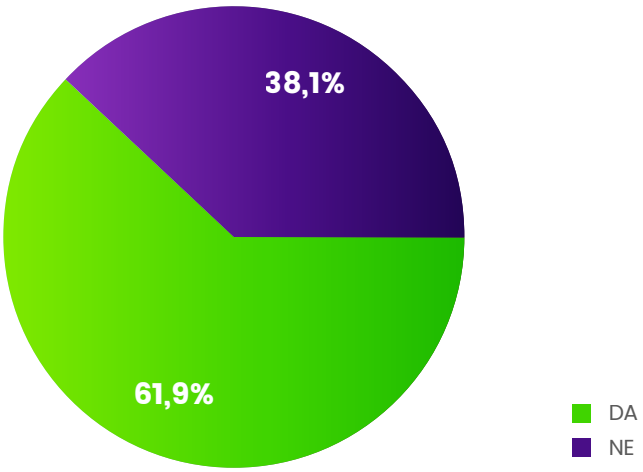
Smanjuje se broj organizacija koje nisu svjesne sigurnosnih incidenata (raste svijest o sigurnosnim incidentima). Smanjuje se broj organizacija koje nisu imale značajnijih incidenata (raste broj organizacija koje su imale značajnije incidente). Raste broj organizacija koje su u zadnjih dvije godine imale značajnije incidente (usporedba 2022./2023.)

Ukoliko ste imali incident, kako biste ocijenili posljedice istog?



Evidentan je porast minimalnih/značajnih/katastrofalnih posljedica sigurnosnih incidenata. Ujedno je zabilježeno smanjenje zanemarivih posljedica (usporedba 2022./2023.).

U vašoj organizaciji postoji definiran i uvježban proces odgovora na incidente?



Raste broj organizacija koje imaju definiran i uvježban proces odgovora na incidente s 33,3 % na 38,1 % (usporedba 2022./2023.).

UMJESTO ZAKLJUČKA

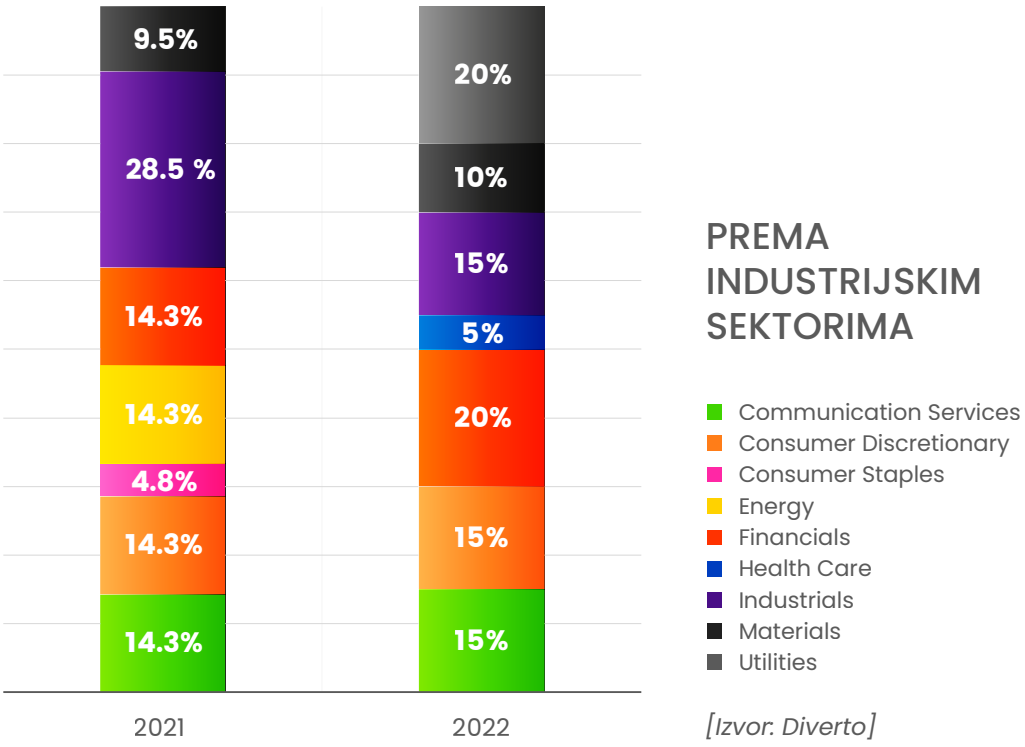
Navedeni rezultati nedvojbeno ukazuju na činjenicu da zabilježeni porast broja incidenata potiče i sve veću osviještenost o informacijskim i kibernetičkim rizicima, što ima za posljedicu i kontinuirani porast ulaganja u informacijsku i kibernetičku sigurnost. Zaključak koji se na temelju navedenih informacija nameće sam po sebi jest da hrvatske tvrtke u sve većem broju prepoznaju prednosti proaktivnog naspram reaktivnog pristupa upravljanju informacijskim i kibernetičkim rizicima.

5.2. Incidenti

Diverto ima višegodišnje iskustvo u upravljanju i odgovoru na incidente informacijske i kibernetičke sigurnosti. Incidentom smatramo one događaje u kojima je napadač ostvario značajni utjecaj na organizaciju kroz neovlašteno kopiranje podataka, zaključavanje podataka, obustave rada IT servisa, umanjio očekivanu kvalitetu poslovanja i/ili narušio ugled organizacije. Godišnje obrađujemo oko dvadesetak[5] značajnih incidenata u Republici Hrvatskoj. Iz toga smo izuzeli pokušaje napadača da ostvari ulazak u organizaciju jer takve događaje bilježimo svakodnevno u Sigurnosno-operativnom centru Diverta.

Možemo reći da su u zadnjih pet godina naši korisnici podjednako organizacije iz privatnog i javnog sektora. Tako imamo iskustvo u radu u energetskom, financijskom, proizvodnom, zdravstvenom i drugim sektorima. Iz priloženog grafa je vidljivo da usluge upravljanja incidentima koriste tvrtke iz raznovrsnih sektora. Graf prikazuje usporedbu 2022. godine u odnosu na prethodnu godinu.

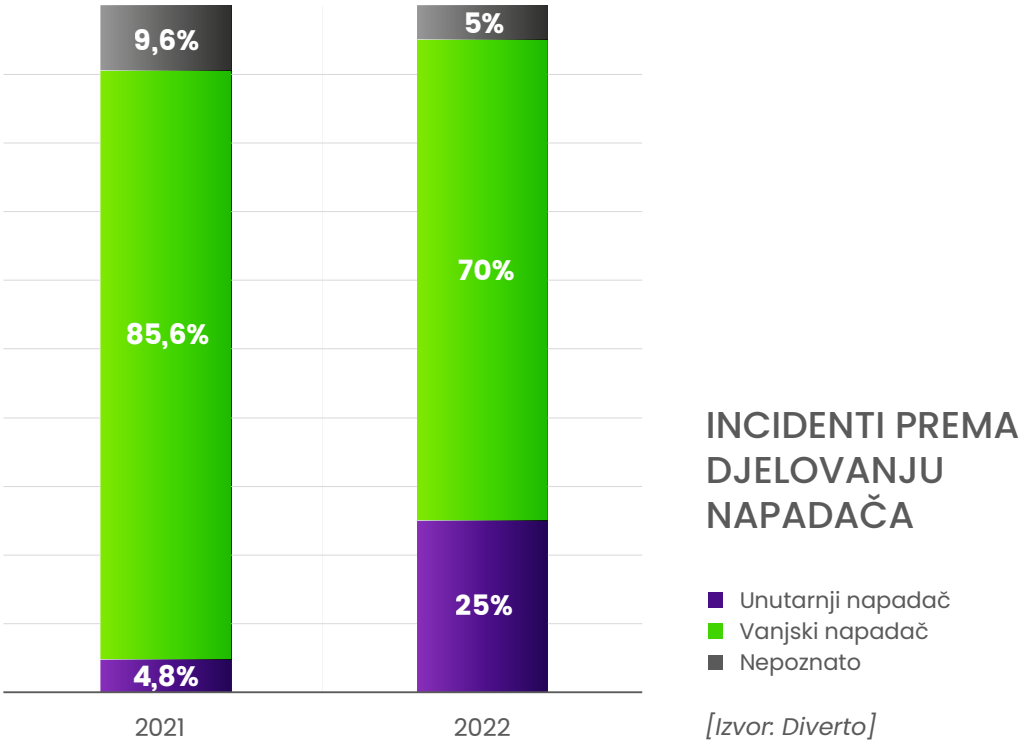
[5] Naglasak je na značajne, kroz redovno poslovanj



[Izvor: Diverto]

NAPOMENA: *Za klasifikaciju industrijskih sektora korišten je GICS® (The Global Industry Classification Standard)*

U 2022. godini smo uočili povećanje incidenata u kojima su unutarnji akteri ostvarili negativan utjecaj na organizaciju u kojoj rade. To su najčešće incidenti povezani s curenjem povjerljivih podataka te javna objava, neovlašteno čitanje elektroničke pošte i slično. Graf prikazuje incidente prema izvoru djelovanja.



[Izvor: Diverto]

I dalje je prisutan trend prikrivanja informacija o sigurnosnim incidentima, vjerojatno radi izbjegavanja reputacijske štete i izloženosti kaznama. Takvom praksom se, nažalost, propušta prilika za učenje i podizanje svijesti o informacijskoj sigurnosti kod tvrtki u kojima je ona na niskim razinama. Stoga ovaj izvještaj predstavlja jedan reprezentativniji prikaz stanja u odnosu na „sivu zonu" incidenata.

5

NAUČENE LEKCIJE

Upravljanjem i sudjelujući u odgovoru na kibernetičke incidente u 2022. godini, uočili smo mnogobrojne nedostatke u organizacijama gdje je napadač ostvario djelovanje. Izdvajamo pet najvažnijih naučenih lekcija. Njihovom primjenom moguće je značajno unaprijediti kibernetičku sigurnost organizacije.

#1 Redovito provoditi podizanje svijesti zaposlenika o najčešćim prijetnjama

Phishing napadi su postali uobičajeni, ali smo primijetili napredak napadača u formiranju i osmišljavanju samog sadržaja poruka koje se šalju žrtvama. Napadači ulažu više truda pa tako uobičajene gramatičke pogreške koje su nastale korištenjem javno dostupnim alatima za prevođenje na hrvatski jezik više nisu tako učestale i lako primjetne. U organizacijama i dalje rade zaposlenici koji nemaju dovoljnu razinu znanja da bi prepoznali *phishing* napade, a upravo taj vektor i dalje bilježimo kao ulaznu točku napadača i u 2023. godini.

#2 Implementirati višefaktorsku autentifikaciju za sve ključne servise tvrtke

Vanjski i unutarnji IT servisi poput VPN-a, elektroničke pošte, pohrane kopija podataka i imeničkih servisa su najčešće prvi cilj napadača. U 2022. godini smo zabilježili incidente u kojima su se napadači koristili spomenutim servisima da ostvare negativan utjecaj na organizaciju kopiranjem ili brisanjem podataka. I dalje samo mali broj organizacija primjenjuje višefaktorsku atutentifikaciju za ključne servise. Primjerice, implementacijom višefaktorske autentifikacije za VPN servis znatno je otežano kontinuirano spajanje napadača. Implementacijom višefaktorske autentifikacije za sustav za pohranu kopija podataka i imenički servis kao što je *MS Active Directory*, značajno se može ograničiti, pa čak i onemogućiti djelovanje napadača čiji je cilj zaključavanje podataka i ucjena.

#3 Ograničiti pristup internim podacima (POLP)

Prekomjerna i neprovjerena prava zaposlenika koji može čitati, kopirati ili mijenjati povjerljivu dokumentaciju mogu imati negativan utjecaj na povjerljivost, cjelovitost i raspoloživost podataka. U 2022. godini broj incidenata u kojima su sudjelovali unutarnji napadači se povećao. Zlonamjerni zaposlenici jako dobro poznaju vlastito radno okruženje i lako mogu prepoznati kritične sustave ili podatke kojima se mogu okoristiti. Važno je svakom djelatniku omogućiti neometan rad samo s podacima i servisima koji su nužni za njegov opseg posla, ništa više od toga. Takav princip konfiguracije korisničkih prava se još naziva i POLP (*Principle of Least Privilege*).

#4 Provoditi redovita penetracijska testiranja

Ranjive web aplikacije i drugi vanjski servisi organizacija su i dalje dobar

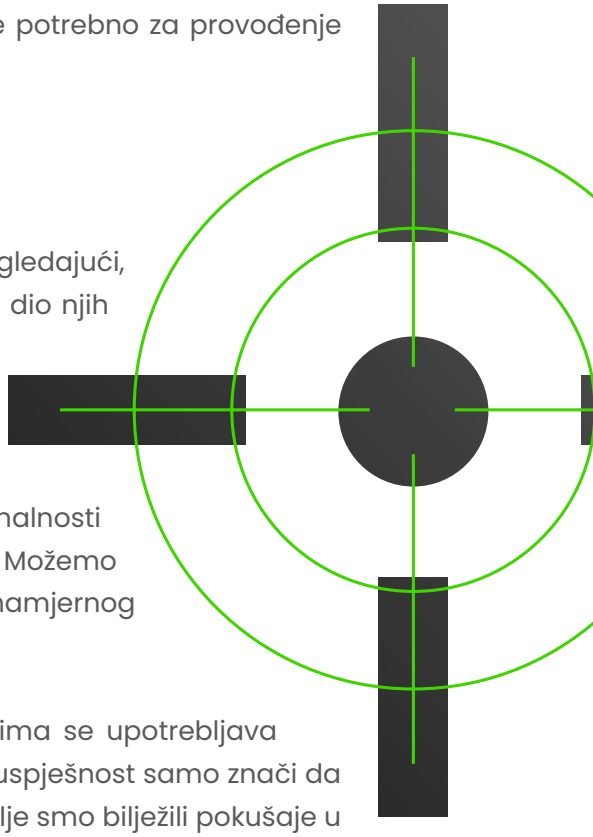
mamac za napadača. Napadači su i u 2022. godini iskorištavali nezakrpane ranjivosti za neovlašteni ulaz u računalnu mrežu organizacija. Naše iskustvo pokazuje da se redovita penetracijska testiranja i dalje ne provode kod većine organizacija koje su bile obuhvaćene zlonamjernim djelovanjem napadača. Bilo da se radi o programskoj ili konfiguracijskoj ranjivosti, ona je prilika za napadača. Penetracijskim testom vlasnik sustava može uočiti i tretirati ranjivosti prije nego ih uoči i iskoristi napadač.

#5 Izraditi plan odgovora na kibernetičke incidente i prije nego se oni dogode

U većini radnih okruženja u kojima smo vodili i upravljali incidentom, vlasnik sustava nije imao prethodno pripremljenu definiranu proceduru i postupanje u slučaju proboja kibernetičke sigurnosti. Naša iskustva su pokazala da je znatno teže upravljati incidentom u takvim okruženjima jer najčešće vlasnik sustava odrađuje pojedinačne korake oporavka po vlastitom nahođenju i iskustvu, nehotično čineći mnogobrojne pogreške koje u konačnici značajno usporavaju povratak sustava u normalno funkcioniranje i ne sprječavaju napadača pravovremeno, a napadač i dalje nakon prvog uočavanja djeluje u sustavu. Diverto SOC i Diverto *Honeypot*, uz tehničku komponentu, uspostavljaju i procese kojima se organizacijama omogućava provođenje sustavnog i prikladnog odgovora na incidente te umanjuju ukupno vrijeme potrebno za provođenje istražnih radnji i vrijeme potrebno za ponovni oporavak sustava.

5.3. Zlonamjerni kod

Glavni motiv napadača je i ove godine bio financijski. Ukupno gledajući, od svih obrađenih zlonamjernih uzoraka u 2022. godini, najveći dio njih možemo kategorizirati kao *Infostealer*. To je kod programiran da prikuplja aktivnosti korisnika na računalu i to na način da bilježi upisane znakove na tipkovnici, uzima izvode ekrana, pretražuje i kopira konfiguracijske datoteke na računalu koje sadrže pristupne parametre i slično. Češće smo uočavali funkcionalnosti za krađu novčanika kriptovaluta u 2022. godini nego u godini prije. Možemo slobodno reći da je to postala uobičajena funkcionalnost zlonamjernog koda koji spada u kategoriju *Infostealer*.



Zabilježili smo manju uspješnost napada u 2022. godini u kojima se upotrebljava *Ransomware*, kod za zaključavanje i kodiranje datoteka. Manja uspješnost samo znači da napadač nije ostvario negativan utjecaj na organizaciju, no i dalje smo bilježili pokušaje u kojima su napadači imali namjeru upotrijebiti *Ransomware*.

Izdvajamo nekoliko uzoraka s detaljima. *AgentTesla* kao najzastupljeniji uzorak u Sigurnosno-operativnom centru, a *Raspberry Robin, Vidar* i *GuLoader* kao uzorke koji su u većoj mjeri ostvarivali proboj u organizacijama gdje se tradicionalno ulaže u sigurnu infrastrukturu.

AgentTesla

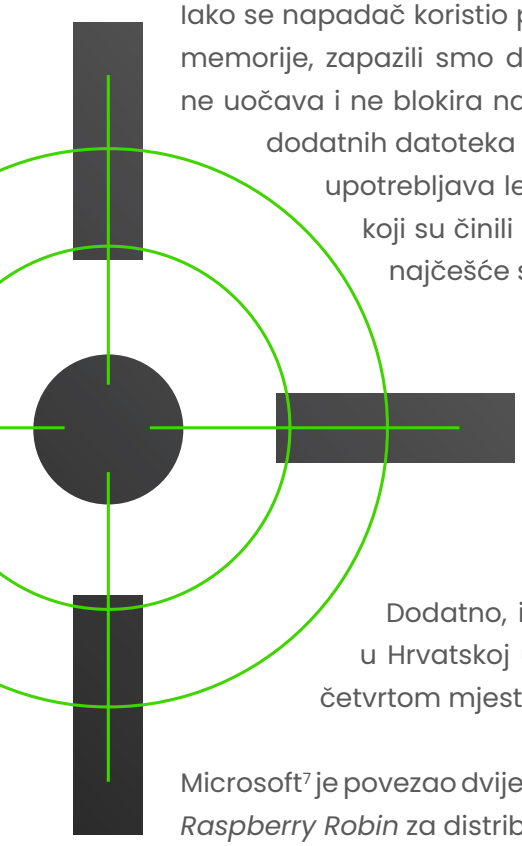
AgentTesla je najzastupljeniji zlonamjerni kod kojeg smo zabilježili u 2022. godini u Divertovom Sigurnosno-operativnom centru. Njegova popularnost je prije svega rezultat modela MaaS (*Malware-as-a-Service*), točnije svatko tko želi pokrenuti napade može naručiti svoju inačicu koda koja je prilagođena, platiti za to, pa čak dobiti i službenu podršku u slučaju poteškoća. Kako

se *AgentTesla* ne pripisuje samo jednoj grupi napadača, uočili smo različite tehnike isporuke, instalacije i početnog izvršavanja koda s ciljem trajnog postavljanja spomenutog alata na računalo. Kao i obično, isporučuje se u *Phishing* pošti sa zaraženim prilogom, a nismo uočili zavidnu razinu sofisticiranosti napadača.

Uobičajeno, *AgentTesla* za slanje prikupljenih podataka izvan organizacije koristi FTP ili SMTP servis – ovisno o konfiguraciji. Pravilnim podešavanjem vatrozida za kontrolu FTP i SMTP prometa, na jednostavan je način moguće spriječiti curenje podataka izvan organizacije, čak i u slučaju zaraženog računala.

Rasberry Robin

U drugoj polovini 2022. godine zabilježili smo prisutnost zlonamjernog koda *Raspberry Robin* u više organizacija. Početni vektor ulaska je zaražena USB memorija, najčešće *flash* ili vanjski USB disk. Iako se napadač koristio prilično jednostavnim tehnikama za izvršavanje koda nakon spajanja memorije, zapazili smo da nekoliko različitih komercijalnih rješenja za zaštitu radnih stanica ne uočava i ne blokira napad. Nakon što se izvrši kod s USB memorije, započinje preuzimanje dodatnih datoteka s interneta i instalacija na računalo. Za spomenute funkcije napadač upotrebljava legitimni servis *Microsoft Windows Installer* (MsiExec). Internetski izvori koji su činili mrežu zlonamjernog koda *Raspberry Robin* za preuzimanje datoteka najčešće su HTTP servisi na QNAP uređajima.



Bez obzira na to što je napadač ukomponirao nekoliko jednostavnih, a već pomalo zastarjelih tehnika za realizaciju napada, reakcija komercijalnih rješenja za zaštitu radnih stanica u nekim radnim organizacijama je potpuno izostala te je napadač u nekim situacijama izvršio kod.

Dodatno, i *TrendMicro*[6] je u svom sustavu zabilježio značajnu prisutnost RR-a u Hrvatskoj u listopadu i studenom prošle godine. Hrvatska se tada nalazila na četvrtom mjestu u odnosu na cijeli svijet.

Microsoft[7] je povezao dvije ruske skupine, DEV-0243 i DEV-0950, koje su se koristile infrastrukturom *Raspberry Robin* za distribuciju *Ransomwarea*.

Vidar

Slično kao i *AgentTesla*, *Vidar* je *Infostealer* i moguće ga je kupiti po modelu *MaaS*-a. U 2022. godini smo zabilježili povećanu prisutnost ovog uzorka u Sigurnosno-operativnom centru. Najčešće je bio distribuiran putem *Phishinga* uz priložene poveznice za preuzimanje sa interneta. U nekim situacijama smo zabilježili da napadači upotrebljavaju *Discord* kao distribucijski kanal (poveznicu u *Phishingu*), a nakon instalacije zlonamjernog koda na računalo, *Vidar* upotrebljava Telegram kanale i *Steam Community* (komunikacijska platforma za ljubitelje videoigara) za dohvat i preuzimanje dodatnog sadržaja.

[6] https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html
[7] https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

GuLoader

GuLoader je Trojan dizajniran za distribuciju drugih uzoraka na zaražena računala. Zabilježili smo situacije u kojima je napadač uspješno zaobišao važne sustave zaštite koristeći *GuLoader*. Detaljnijom analizom uzoraka uočili smo da *GuLoader* upotrebljava mnogobrojne tehnike za otkrivanje virtualnog okruženja i otkrivanje tehnologije *Sandbox* za dinamičku analizu koda. Distribuiran putem *Phishinga*, u pojedinim situacijama je uspješno „prošao" do radnih stanica zaposlenika.

Uočili smo i značajnu prisutnost drugih tipova zlonamjernog koda: *IceID, Formbook, NanoCore*; ali bez značajnijeg uspjeha po napadača.

RANJIVOSTI I KODOVI ZA ISKORIŠTAVANJE

Kao dio zlonamjernog koda, a prvenstveno kao okidač za njegovo izvršavanje, zabilježili smo veći broj pokušaja iskorištavanja programskih ranjivosti. Izdvajamo tri najzastupljenija koje smo bilježili u Sigurnosno-operativnom centru, a svi oni obuhvaćaju proizvode tvrtke *Microsoft*.

CVE-2022-30190 - Follina

Zabilježili smo *Phishing* poruke e-pošte s prilogom, najčešće u nekom od *Word* formata koji su u sebi imali ugrađen spomenuti kod za iskorištavanje ranjivosti. Iskorištena ranjivost kroz *Microsoft Word* dokument kao potproces aktivira ranjivu komponentu MSDT (*Microsoft Support Diagnostic Tool*), najčešće preuzimajući dodatni sadržaj s interneta u kojem se nalazi zlonamjerni kod.

CVE-2022-41040, CVE-2022-41082 - ProxyNotShell

Iskorištavanje dviju ranjivosti, SSFR-a (*Server-Side Request Forgery*) i RCE-a (*Remote Code Execution*), u kombinaciji na servisu *Microsoft Exchange* napadačima omogućuju pokretanje koda s proširenim pravima. Tako zbog nedostatne kontrole ulaznih parametara na mehanizmu *Autodiscover* napadač može izvršavati *PowerShell* skripte. Kako je *Microsoft Exchange* raširena tehnologija za razmjenu elektroničke pošte i nalazi se u mnogobrojnim organizacijama, zabilježili smo velik broj pokušaja iskorištavanja spomenutih ranjivosti.

5.4. Phishing

Dobro poznati trend rasta incidenata u kojima je korišten socijalni inženjering nastavlja se u 2022. godini. *Phishing* napada je očekivano sve više, a podaci pokazuju kako je rast veći nego ikada. U 2022. godini je zabilježeno 34% više slučajeva uspješno izvedenih *phishing* napada u odnosu na 2021. godinu[8] što jasno pokazuje kako doba *phishinga* tek slijedi.

Imajući na umu povećanje broja *phishing* napada i njihovu sve veću složenost, u 2022. godini smo razvili novu metodologiju testiranja otpornosti organizacija na napade koji koriste socijalni inženjering. Poslali smo preko 8000 *phishing* poruka na više od 4000 jedinstvenih adresa organizacija javnog i privatnog sektora te ustanovili da čak 21,22% korisnika nije prepoznalo barem jednu *phishing* poruku.

[8] Phishing Scams & Attacks: What To Expect in 2023, Splunk

U odnosu na prošlu godinu kada smo ustanovili da 23% korisnika ne može prepoznati *phishing* poruku, napredak je jasan uzmemo li u obzir kako je *phishing* poruka značajno više, a broj korisnika koji ne mogu prepoznati *phishing* poruku manji.

Ovaj postotak odstupa od globalnog prosjeka prema kojem je čak trećina promatranih pojedinaca učinila nešto što je dovelo u rizik njih ili organizaciju[9]. Razlika se može tumačiti razlikom između zrelosti promatranih organizacija. Podaci kojima Diverto raspolaže prikupljeni su mahom analizirajući organizacije koje imaju uspostavljene programe podizanja svijesti i koje su već provodile *phishing* testiranja. Također, usporedimo li porast broja phishing napada s relevantnim podacima za **Republiku Hrvatsku**, gdje je **broj prijavljenih računalnih prijevara MUP-u porastao za 23%**[10], jasno je vidljivo da još uvijek ne spadamo u kategoriju najpoželjnijih meta.

Percepcija *phishinga* se mijenja i on iz tradicionalno podcijenjene metode napada postaje metoda koju sve ozbiljnije shvaćamo. Prema izvještaju *Cost of a Data Breach Report 2022.*[11], *phishing* je najštetnija i druga najčešća točka ulaza kod incidenata curenja podataka. Uzmemo li kao relevantne podatke dostupne putem *Google Trends* alata, razvidno je da se o *phishingu* u svijetu i Hrvatskoj sve više progovara, ali i da je u Hrvatskoj rast interesa za temom *phishinga* značajno sporiji.

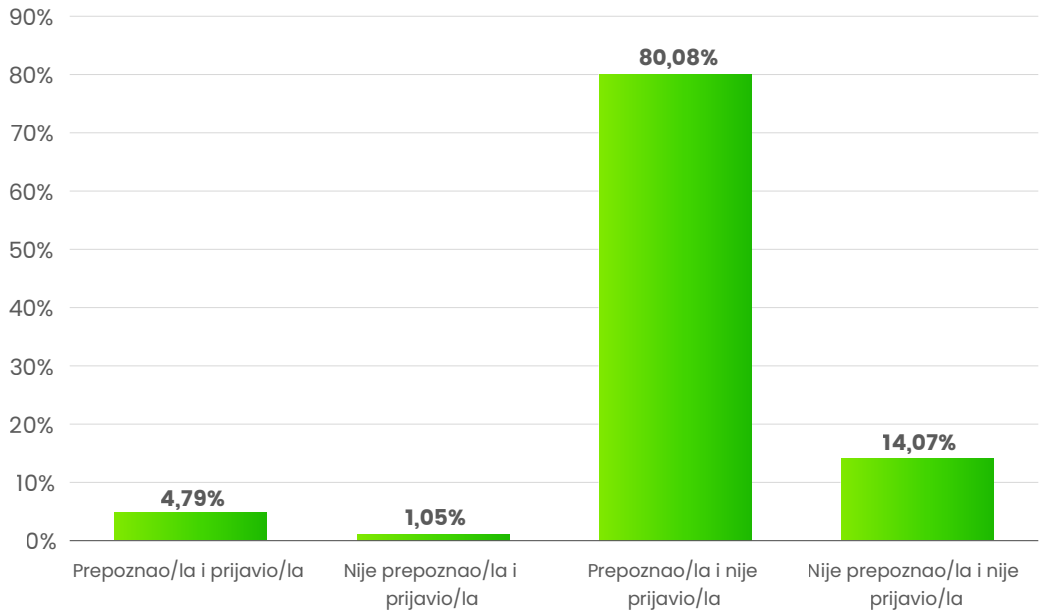
Razlika u odnosu na globalne trendove ponovno je prisutna, međutim, promjenom metodologije te načina provođenja *phishing* testiranja, u 2022. godini smo stekli dublji uvid u otpornost pojedinih organizacija. Gdje je to bilo moguće, pratili smo ponašanje pojedinačnih korisnika, način na koji reagiraju na *phishing* poruke te bilježili prijave *phishing* poruka kako bismo dobili što potpuniju sliku.

Na temelju podataka prikupljenih na populaciji od 1898 jedinstvenih korisnika (u 3 odvojena nezavisna istraživanja) pokazalo se da:

- 94% korisnika phishing poruke ne prijavljuje nadležnoj organizacijskoj jedinici
  - 80% korisnika poruku ili ne pročita ili ju prepozna kao zlonamjernu, ali ju ne prijavi nadležnoj organizacijskoj jedinici
  - 14% korisnika poveznici u poruci pristupi i ne prijavi potencijalni incident nadležnoj organizacijskoj jedinici
- 5% korisnika svaku od dobivenih phishing poruka ispravno prepozna i prijavi
- 1% korisnika prijavi phishing poruku nakon što shvate da su pogriješili

Ukratko, u velikoj smo mjeri naučili korisnike prepoznavati phishing poruke i ne uspostavljati interakciju s napadačem, ali je ostalo mnogo posla u podizanju svijesti korisnika o važnosti i korisnosti prijave. Na umu treba imati kako promatrana populacija dolazi iz zrelih organizacija u kojima postotak korisnika koji nisu uspjeli prepoznati barem jednu phishing poruku pozitivno odstupa od prosjeka.

[9] 2023 State of the Phish, Proofpoint
[10] Poredbeni prikaz kaznenih djela kibernetičkog kriminaliteta 2021./2022., MUP RH
[11] Cost of a Data Breach Report 2022., Ponemon Institute/IBM Security



SLIKA 6 *Prikaz ponašanja korisnika prilikom prepoznavanja i prijavljivanja phishing poruka, [Izvor: Diverto]*

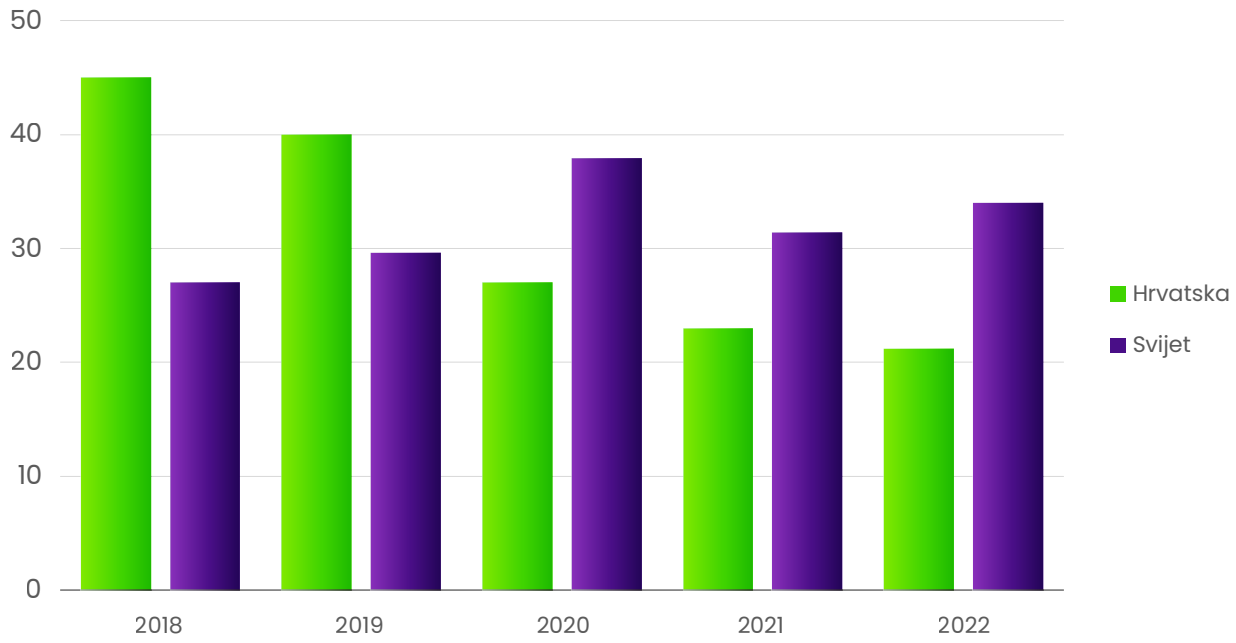
Pri određivanju težine prepoznavanja poruka korištenih u testiranju, koristili smo se nizom kvantitativnih i kvalitativnih pokazatelja kako bismo stekli što bolji uvid u otpornost organizacije na različite vrste napada.

Korištenje složenijim porukama značajno umanjuje broj korisnika koji poruku prepoznaju, što je samo po sebi očekivano i prema našem istraživanju čak 33 % korisnika ne može prepoznati *phishing* teške razine prepoznavanja.

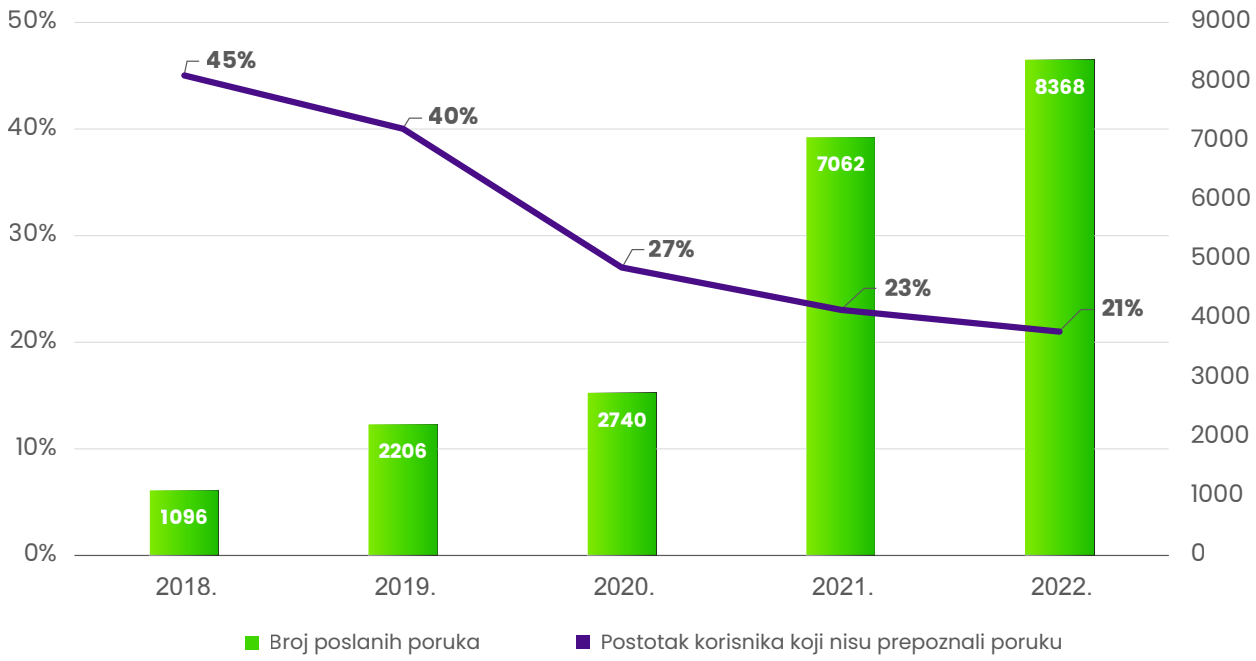
Razina težine prepoznavanja *phishing* poruke sigurno će rasti, pogotovo uzmemo li u obzir razvoj na polju umjetne inteligencije koja će napadaču značajno olakšati pripremu uvjerljive poruke. Veoma je važno na vrijeme prepoznati i odgovoriti na složenije napade sustavnim programom edukacije, periodičkim testiranjem te razvijanjem odnosa povjerenja i osvještavanjem važnosti prijave.

I ove je godine sasvim jasno da borba s *phishing* porukama nikada neće prestati i da nikada neće postojati idealna organizacija u kojoj će svi korisnici prepoznati sve *phishing* poruke te ih ispravno prijaviti nadležnoj organizacijskoj jedinici baš svaki put. Međutim, dubljim uvidom u ponašanje svakog korisnika i detaljnijom analizom, moguće je identificirati pogreške u pristupu koji trenutačno prevladava, a to je pristup u kojem iz godine u godinu koristimo iste metode kako bismo podigli otpornost organizacije očekujući drugačije rezultate.

Pogrešno je od svakog korisnika očekivati da prepozna baš svaku *phishing* poruku. I najbolje educiranim korisnicima se može u žurbi i pod pritiskom dogoditi trenutak nepažnje. Međutim, samo ispravnim prepoznavanjem i pravilnom prijavom korisnik zauzima aktivan stav u obrani cijele organizacije. Upravo je zato od iznimne važnosti usmjeriti naša nastojanja prema kvalitetnim programima edukacije koji, s jedne strane, korisniku daju alate koji će mu pomoći u prepoznavanju napada koji se koriste socijalnim inženjeringom, a s druge strane, u njemu razvijaju odgovornost prema sigurnosti organizacije i njegovoj ulozi u lancu sigurnosti.



SLIKA 7 *Postotak korisnika koji nisu prepoznali phishing poruku, [Izvor: Diverto] (podaci za Hrvatsku); 2023 State of the Phish, [Izvor: Proofpoint] (globalni podaci)*



SLIKA 8 *Postotak korisnika koji nisu prepoznali phishing poruku u odnosu na broj poslanih poruka, [Izvor: Diverto]*

Preduvjet za uspješnu obranu od phishing napada nije samo prepoznavanje zlonamjerne phishing poruke, već i pravovremena i pravilna prijava. Korisnici moraju od pasivnog sudionika u procesu sigurnosti postati aktivni element koji uči, proaktivno reagira i u odnosu povjerenja surađuje s nadležnim službama zaduženim za sigurnost.

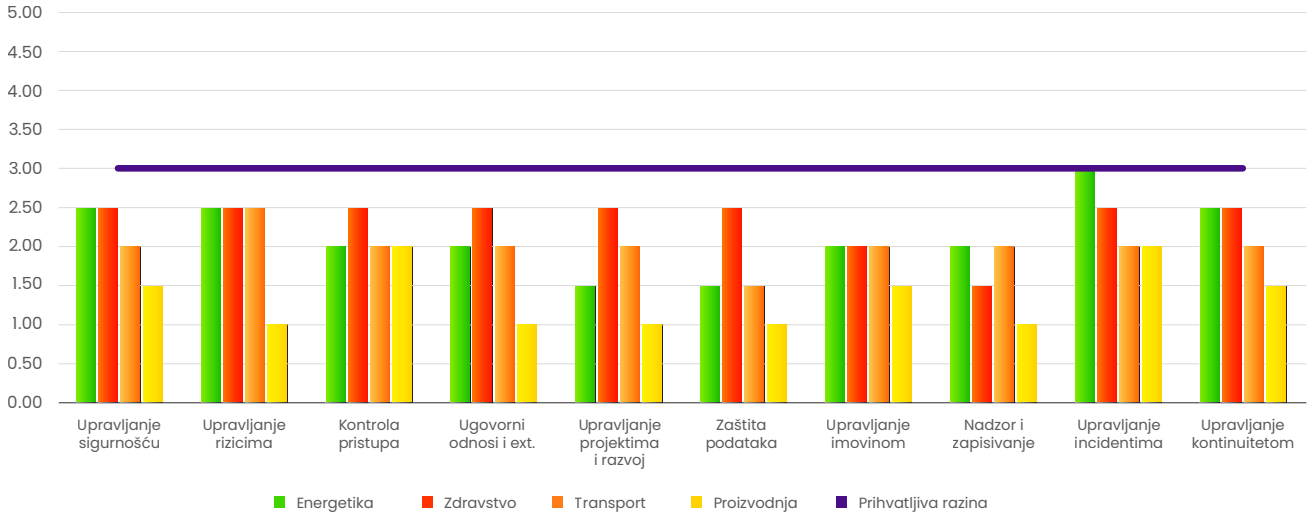
Svan Hlača, voditelj usluga socijalnog inženjeringa

5.5. Kibernetička sigurnost i OT/IIoT trendovi

Kibernetička sigurnost industrijskih kontrolnih sustava (OT sustava) je postala „vruća tema" u vrlo kratkom vremenu. Kibernetički napadi, premda započinju u „virtualnom svijetu", ne utječu više samo na podatke organizacija i eventualne novčane gubitke izazivane štetom na podacima. Današnji kibernetički napadi na OT sustave mogu imati ozbiljne posljedice u „stvarnom svijetu", poput posljedica po nacionalnu sigurnost, zdravlje i sigurnost ljudi, okoliš te, općenito, ekonomiju koja ovisi o kritičnim infrastrukturama i industrijama svake države. Dodatno, aktualna geopolitička situacija i postizanje ratnih ciljeva kroz kibernetičku domenu naglašava važnost kibernetičke sigurnosti OT sustava.

U posljednjih nekoliko godina, Republika Hrvatska postigla je značajne pomake u usklađivanju s EU NIS Direktivom i lokalnim transpozicijama direktive kroz Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Međutim, i dalje postoji mnogo izazova za zaštitu kritične infrastrukture u OT sustavima. Nije nepoznanica da kritična infrastruktura često koristi starije sustave dizajnirane tako da budu pouzdani, ali zbog svoje starosti, inherentno kibernetički nesigurni. Ta činjenica, u današnje vrijeme integracija, takve OT sustave čini privlačnim metama napadača. Dodatni izazov sigurnosti OT sustava predstavlja razvoj novih tehnologija jer nove tehnologije poput IoT-a (*Internet of Things*) i 5G mreža dodatno povećavaju rizik od napada. Spomenuti sigurnosni izazovi dodatno će biti naglašeni i regulatornim zahtjevima nedavno donesene NIS 2 direktive koja značajno širi svoj opseg primjene.

Diverto je kroz 2022. godinu intenzivno surađivao i nastavlja suradnju s organizacijama i industrijama koje sve više ovise o OT sustavima. Prvi put donosimo vam ocjenu zrelosti relevantnih područja kibernetičke sigurnosti OT sustava prilikom inicijalnih procjena sigurnosti:



SLIKA 9 *Razina zrelosti kibernetičke sigurnosti kritičnih sustava po područjima u različitim industrijama, [Izvor: Diverto]*

Napominjemo kako su ulazni podaci za ovaj izvještaj rezultati usluga koje je Diverto izvršio tijekom 2022. godine. Konkretnije, radi se o procjenama razine kibernetičke sigurnosti i/ili procjenama usklađenosti sa Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (ZKS). Dodatno, naglašavamo kako su svi ulazni podaci za ovaj izvještaj proizašli iz usluga

utvrđivanja razine zrelosti kod organizacija koje su Divertovi „novi korisnici“, točnije, radi se o korisnicima koji su prethodno samostalno radili na svojem programu informacijske sigurnosti, a u promatranoj godini su odlučili zatražiti pomoć od Diverta kako bi odredili razinu kibernetičke sigurnosti i/ili razinu usklađenosti sa ZKS-om te kako bi dobili i preporuke kako doseći željenu/zahtijevanu razinu.

SIGURNOSNI IZAZOVI/PROPUSTI U KONFIGURACIJI OT SUSTAVA

Uz sumarnu ocjenu zrelosti, donosimo vam kratki osvrt na najčešće izazove/propuste na razini mrežnih komunikacija, računalne opreme, terenskih uređaja (PLC, RTU, HMI) s kojima smo se sreli u prethodnom razdoblju.

Mrežna oprema

- **nepostojanje mrežne segmentacije.** Najčešće ne postoje zasebni mrežni segmenti koji bi onemogućavali potencijalno širenje zlonamjernog aktera nakon inicijalnog proboja u OT mrežu
- **pouzdanje isključivo u fizičku sigurnost izdvojenih lokacija** bez primjene dodatnih kontrola poput segmentacije i ograničavanja tokova podataka
- **korištenje „univerzalnim“ mrežnim uređajima** na koje su fizički priključeni uređaji IT i OT sustava
- **neprimjenjivanje kritičnih zakrpa** na upravljive mrežne uređaje
- **usvajanje pravila sa starih mrežnih uređaja** bez dokumentiranja i verifikacije kontradikcija u pravilima
- **ograničene mogućnosti bilježenja i nadzora.** Događaji na mrežnim uređajima zadržavaju se ograničeno i kratko vrijeme, najčešće zbog nepostojanja namjenskih rješenja *Syslog* ili *SIEM*, što uvelike otežava istražne aktivnosti i analitiku.

Računalna oprema

- **neprimjenjivanje kritičnih zakrpa na operativne sustave i SCADA softver.** Na svim računalima svojstveno je da ne posjeduju kritične sigurnosne zakrpe i da je iznimno zahtjevno pravovremeno primijeniti ih, bez obzira postoji li ili ne postoji proces primjene i prioritizacije zakrpa
- **zaporke koje se mogu lako odgonetnuti ili nepostojeće zaporke za pristup sustavima.** U kontroliranim pokušajima probijanja zaporki (neovisno je li korisnički ili privilegirani račun), kod više od 70 % slučajeva uspješno smo probili zaporke zbog jednostavnosti i neprimjene politika kompleksnosti. U 10 % sustava nisu uopće postojale zaporke
- **nepostojanje provjere integriteta programske podrške.** Događaji na računalima OT mreže ne prate se sustavno, najčešće zbog nepostojanja namjenskih rješenja *Syslog* ili *SIEM*. Bez postavljene osnovice (*baseline*) i dodatnih sigurnosnih mehanizama, poput digitalnog potpisivanja SCADA softvera teško je utvrditi neovlaštene izmjene na sustavima

- **korištenje nesigurnim ili nepotrebnim protokolima.** Upotrebljavaju se nesigurni protokoli poput *Telneta* i FTP-a, dodatno je na dosta računala bio omogućen *IPv6* protokol koji je najčešće nepotreban/opasan u OT mrežama
- **korištenje manje sigurnim konfiguracijskim postavkama.** Upotrebljavaju se postavke koje mogu dodatno narušiti integritet i sigurnost sustava, poput onemogućenog *LUA*, pogrešno konfiguriranog IP *multicasta*, omogućenog *NETBIOS-a*, onemogućenog *LMHASH-a*, velikog broja međuspremljenih vjerodajnica i slično.

PLC, RTU i ostali uređaji

- **nemogućnost praćenja integriteta firmvera i softvera** na udaljenom uređaju kroz SCADA-u i DCS
- **nepostojanje ili neprimjena autentikacijskih mehanizama** međusobno između L1 uređaja, L1 i SCADA-e ili DCS sustava, pogotovo u situacijama kad su uređaji udaljeni od lokacije na kojoj se nalazi SCADA i DCS
- **korištenje zastarjelim uređajima i sustavima.** Takve uređaje nije moguće održavati niti integrirati u SCADA-u ili DCS. Navedeno u kombinaciji s otežanom dobavljivošću novih sustava može prouzročiti značajne zastoje u provođenju kritičnih aktivnosti u slučaju napada koji oštećuje sustav.

TRENDOVI

OT sustavi su primarna meta u kibernetičkom ratovanju

OT sustavi su ključni za funkcioniranje kritičnih infrastruktura u industriji, energetici i državnim institucijama, stoga su sve češće cilj kibernetičkog ratovanja. Ovi sustavi kontroliraju procese u stvarnom vremenu, stoga je ugrožavanje tih sustava potencijalno opasno po sigurnost i funkcioniranje cijele nacije. Ugroza takvih sustava može prouzročiti jednaki učinak kao kinetičko ratovanje uz značajno manja ulaganja i izloženost napadača. Navedeno u kombinaciji s izazovima pripisivanja takvih napada postaje izuzetno privlačan način ratovanja gdje se uz relativno „skromna" ulaganja postižu učinci jednaki klasičnom „kinetičkom" ratovanju.

Ransomware na OT Level 1 uređajima

Ransomware dokazano ima negativne učinke na IT sustave te može utjecati i na OT sustave bez da ih direktno zarazi, čemu smo svjedočili kod incidenata poput *Colonial Pipeline*. Uzevši u obzir trenutno stanje i pad prihoda *ransomware* skupina na području IT sustava, nedostatnu segmentaciju OT sustava, niske ili nepostojeće sigurnosne kapacitete postojeće opreme te u svjetlu prvih uspješnih plasiranja *ransomwarea* na L1 uređaje u OT mrežama, za očekivati je pojačani broj *ransomware* napada na OT sustave.

Nastavak na povezivanju IT i OT sustava

- konvergencija i sve manje razlike u načinima funkcioniranja OT i IT mreža
- problemi integracije stare (*legacy*) opreme i nove opreme
- uporaba *virtual PLC-ova*
- implementacija jeftinijih (*IIoT*) rješenja (npr. uz korištenje *Raspberry* Pi).

Dodatno će utjecati na uvođenja/otkrivanja novih ranjivosti OT sustava i aktivna iskorištavanja istih.

NAČINI ZA POBOLJŠANJE KIBERNETIČKE SIGURNOSTI

Iako su izazovi kibernetičke sigurnosti za operatore ključnih usluga i kritične infrastrukture u Republici Hrvatskoj ozbiljni, ne zaostajemo za svjetskim trendovima primjene sigurnosnih mehanizama u kibernetičkom prostoru.

Važno je neprekidno raditi na poboljšanju sigurnosti kroz kontinuirano razmatranje i uključenje OT sustava u postojeće sigurnosne mehanizme organizacija kako bi se spriječili napadi i zaštitile kritične infrastrukture. Donosimo Vam nekoliko generalnih preporuka za poboljšanje:

- uključivanje kibernetičke sigurnosti u projekte izgradnje OT sustava u najranijim fazama projekta
- provjera identiteta i prava pristupa za sve osobe i uređaje koji imaju pristup kritičnim sustavima
- stalno praćenje i analiziranje mrežnih aktivnosti kako bi otkrili moguće napade
- uspostava procesa i mehanizama sigurnog upravljanja dobavljačima i kontrole opskrbnog lanca
- implementacija sigurnosnih standarda poput ISA 62443 i ISO 27001
- izgradnja, testiranje i kontinuirano poboljšavanje plana odgovora na incidente i planova kriznog upravljanja u svrhu podizanja otpornosti.
- kontrolirano praćenje ranjivosti i ažuriranje softvera i hardvera kako bi se spriječili sigurnosni propusti.

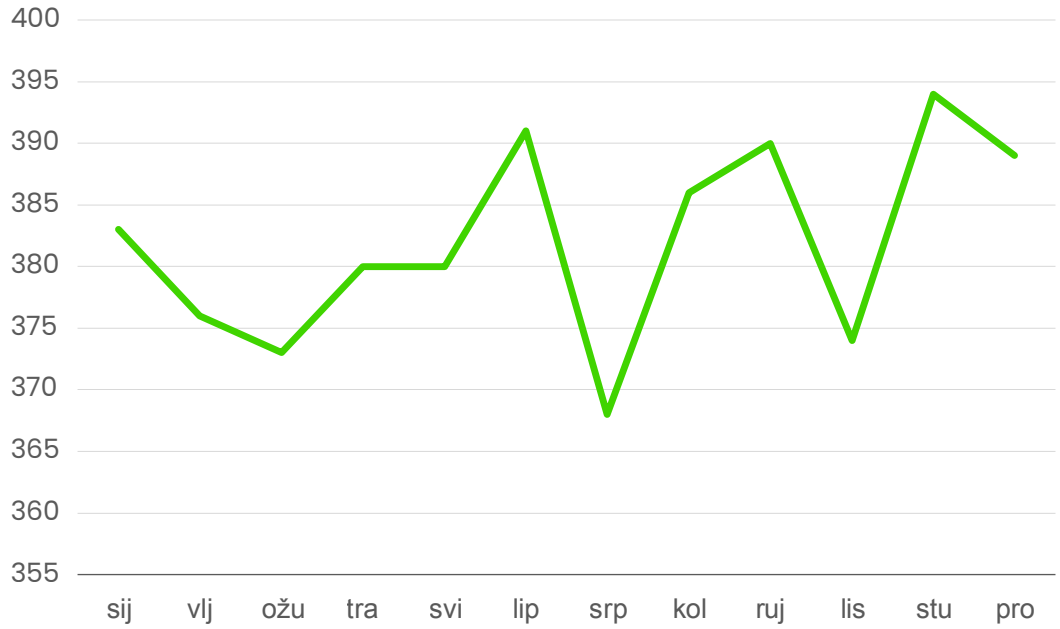
Nedostatak podrške poslovodstva, preveliko oslanjanje na izolaciju procesne mreže i proizvođača, odnosno integratora često je razlog nepostojanja/neuspjeha programa kibernetičke sigurnosti. Ključno je uključiti sve relevantne strane, uključujući procesno osoblje, proizvođače i integratore, IT osoblje, osoblje zaduženo za informacijsku sigurnost, osoblje zaduženo za fizičku sigurnost, ljudske resurse, pravnu službu i poslovodstvo u proces uspostave funkcionalnog programa kibernetičke sigurnosti kojim se kasnije osigurava najbolja moguća zaštita od kibernetičkih prijetnji.

Mario Blažević, voditelj OT usluga

5.6. Distribuirani napadi uskraćivanjem usluge (DDoS)

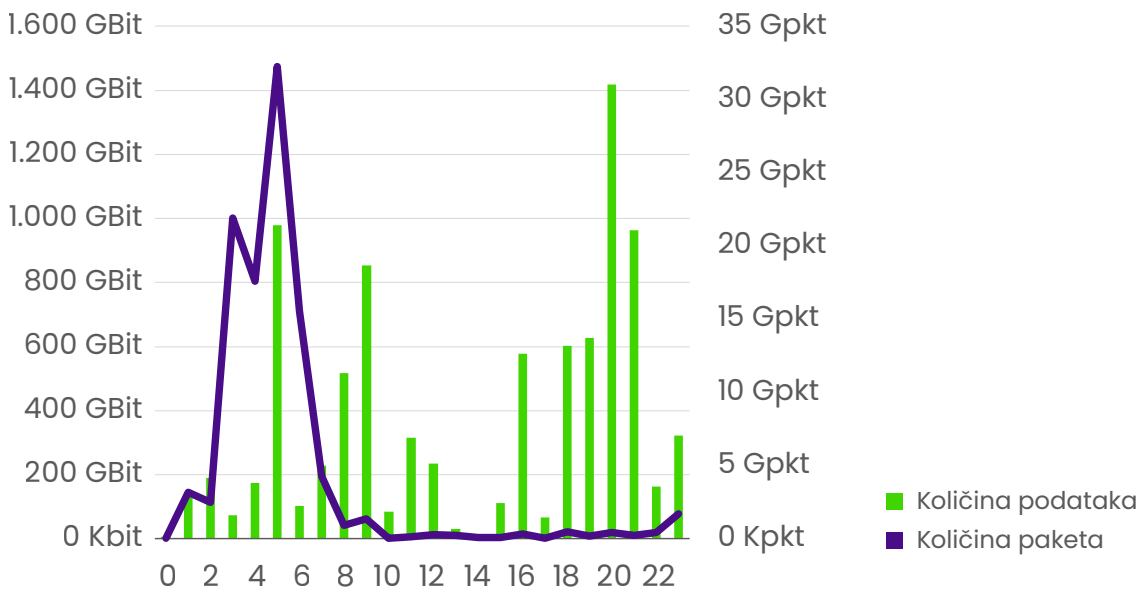
Distribuirani napad uskraćivanja usluge je jedan od najjednostavnijih i najosnovnijih, ali i dalje najučestalijih napada u internetskom prostoru. Stoga vam donosimo više detalja o DDoS napadima tijekom 2022. godine u Hrvatskoj.

Pogleda li se broj napada po mjesecima, u hrvatskom internetskom prostoru takvi su napadi učestali te nema određenog perioda kada takvi napadi nisu izraženi u promatranoj godini. Srpanj ima nešto manji broj napada, a najizraženiji je mjesec studeni. Međutim, same razlike između navedenih vršnih vrijednosti nisu značajne.



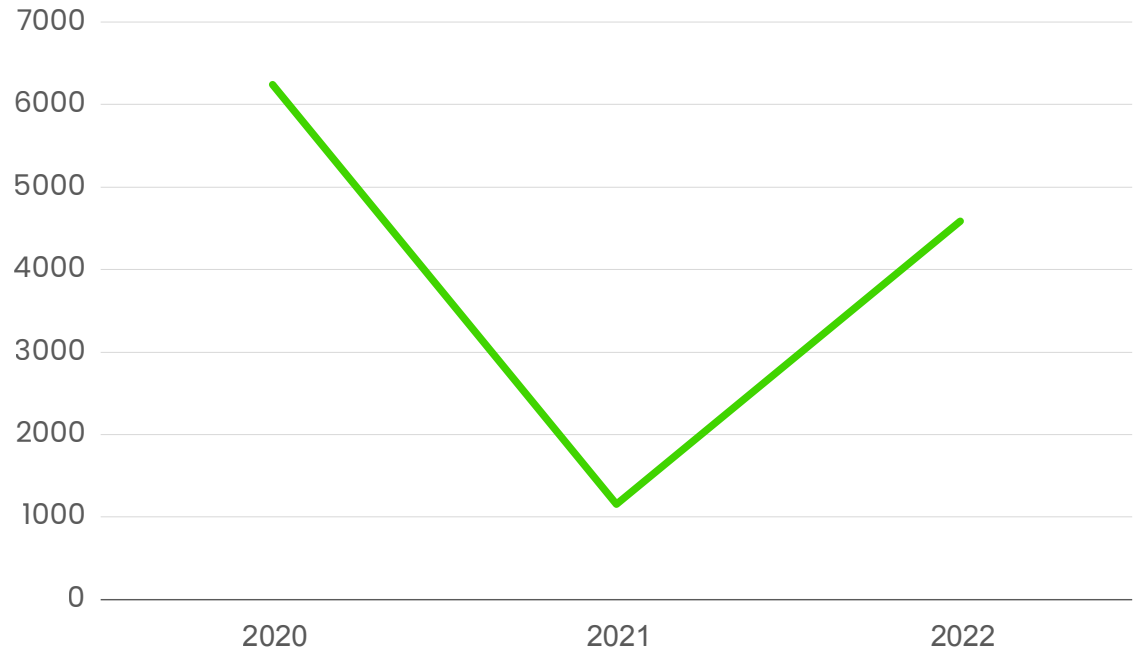
SLIKA 10 *Broj napada prema mjesecima u 2022. godini, [Izvor: Diverto]*

Interesantno je pogledati kada napadači najčešće započinju svoje napade u 2022. godini. Prema veličini napada, to su očigledno večernji i jutarnji sati. Navedeno nameće zaključak kako napadači počinju napad dok je uobičajeno manji broj ljudi raspoloživ za nadzor sustava ili su napadači iz drugih vremenskih zona.

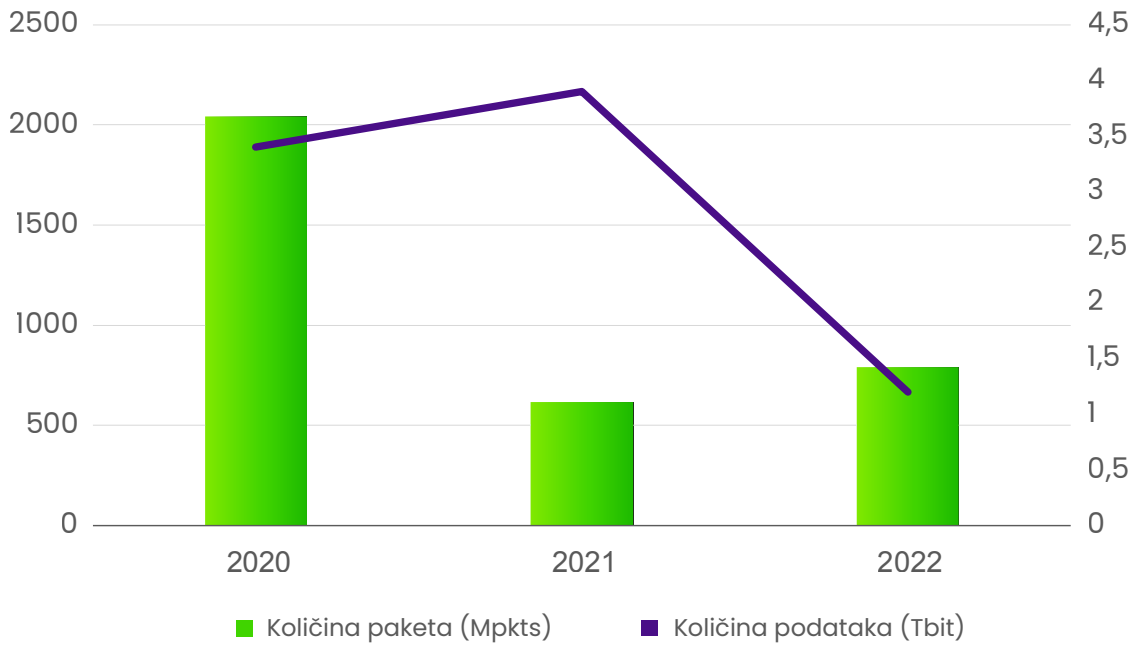


SLIKA 11 *Veličine napada prema početnom satu (UTC) napada u 2022. godini, [Izvor: Diverto]*

Ako usporedimo proteklu godinu s prethodnim godinama, 2022. godina nije bila rekordna godina ni po broju napada ni veličini napada. Ono što je svakako bilo zapaženo jest povratak broja napada nakon znatnog smanjenja u 2021. godini.



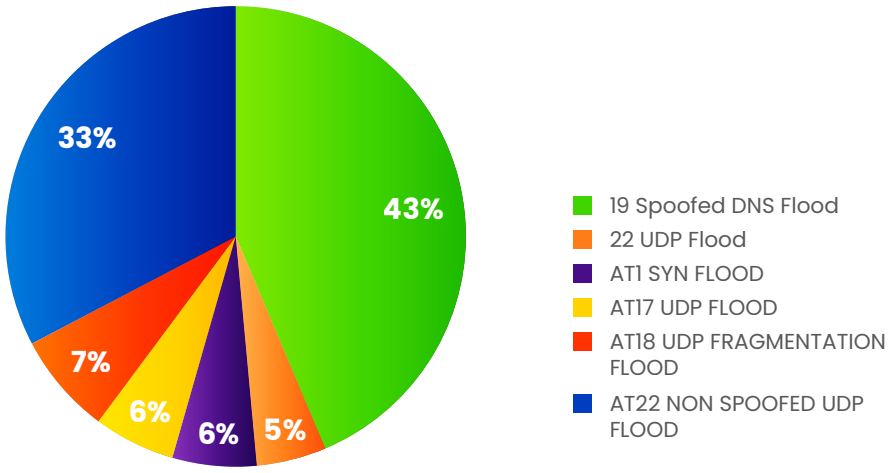
SLIKA 12 *Broj napada po godinama, [Izvor: Diverto]*



SLIKA 13 *Najveći napadi prema godinama, [Izvor: Diverto]*

U 2022. godini izraženija je uporaba UDP protokola za napade, pogotovo ako gledamo prema broju zaprimljenih podataka. Ukratko, napadači su poslali više podataka UDP protokolima nego drugima (primjerice: TCP).

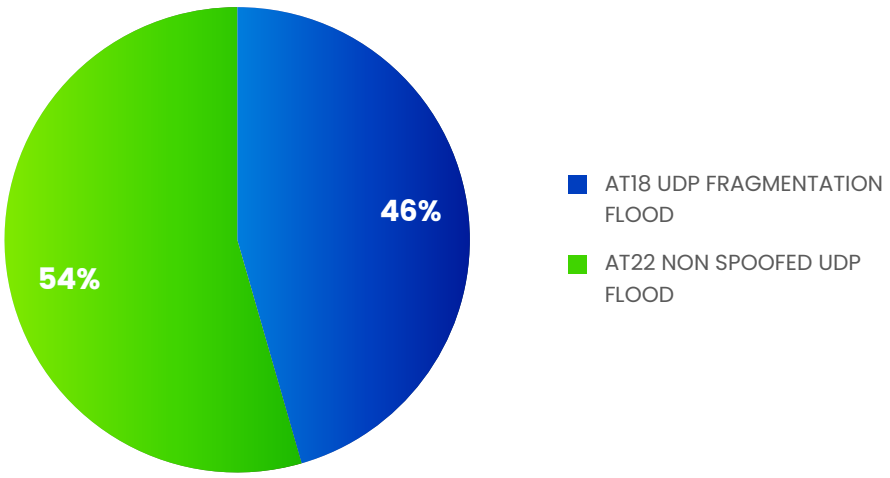
Poredak	Tip napada	Količina paketa
1	19 Spoofed DNS Flood	789 Mpkts
2	AT22 NON SPOOFED UDP FLOOD	298,3 Mpkts
3	AT22 NON SPOOFED UDP FLOOD	113,0 Mpkts
4	AT1 SYN FLOOD	106,8 Mpkts
5	AT22 NON SPOOFED UDP FLOOD	105,7 Mpkts
6	AT17 UDP FLOOD	103,3 Mpkts
7	22 UDP Flood	88,8 Mpkts
8	AT22 NON SPOOFED UDP FLOOD	74,4 Mpkts
9	AT18 UDP FRAGMENTATION FLOOD	71,1 Mpkts
10	AT18 UDP FRAGMENTATION FLOOD	58,0 Mpkts



SLIKA 14 *Raspodjela tipova napada u 10 najvećih napada prema broju pristiglih paketa, [Izvor: Diverto]*

Poredak po količini podataka

Poredak	Tip napada	Količina paketa	Količina podataka
1	AT22 NON SPOOFED UDP FLOOD	298,3 Mpkts	1,2 Tbits
2	AT18 UDP FRAGMENTATION FLOOD	58,0 Mpkts	689,9 Gbits
3	AT18 UDP FRAGMENTATION FLOOD	71,1 Mpkts	602,0 Gbits
4	AT22 NON SPOOFED UDP FLOOD	113,0 Mpkts	442,9 Gbits
5	AT18 UDP FRAGMENTATION FLOOD	37,1 Mpkts	428,0 Gbits
6	AT22 NON SPOOFED UDP FLOOD	105,7 Mpkts	414,3 Gbits
7	AT22 NON SPOOFED UDP FLOOD	74,4 Mpkts	290,2 Gbits
8	AT18 UDP FRAGMENTATION FLOOD	21,6 Mpkts	229,6 Gbits
9	AT22 NON SPOOFED UDP FLOOD	22,5 Mpkts	189,0 Gbits
10	AT18 UDP FRAGMENTATION FLOOD	15,9 Mpkts	171,4 Gbits



SLIKA 15 *Raspodjela najvećih 10 napada prema količini zaprimljenih podataka, [Izvor: Diverto]*

Posljedice DDoS napada obično traju mnogo duže nego sami napad. Trajanje napada odnosi se na prepoznatu mrežnu razinu na uređajima koji služe za zaštitu. Iako prepoznato vrijeme trajanja napada na mrežnom uređaju može izgledati kao kratak napad, posljedica samog napada je često mnogo duža jer je potrebno određeno vrijeme da se uređaji, infrastruktura i aplikacije dovedu u normalni režim rada, pogotovo u slučaju kada sustav zaštite i sam sustav nisu adekvatno implementirani i dimenzionirani.

NAJDUŽI NAPAD TRAJAO JE PREKO 14 SATI (877 MINUTA).

TOP 5 DDOS TEHNIKA PREMA BROJU PRISTIGLIH PAKETA

- 19 Spoofed DNS Flood
- AT22 NON SPOOFED UDP FLOOD
- AT1 SYN FLOOD
- AT17 UDP FLOOD
- AT18 UDP FRAGMENTATION FLOOD

TOP 5 DDOS TEHNIKA PREMA KOLIČINI PRISTIGLIH PAKETA

- AT22 NON SPOOFED UDP FLOOD
- AT18 UDP FRAGMENTATION FLOOD
- AT3 ACK FLOOD
- AT17 UDP FLOOD
- AT1 SYN FLOOD

Kako su DDoS napadi i dalje prisutni, preporuka je provjeriti svoju DDoS zaštitu, a posebno izvan uobičajenog radnog vremena. I dalje je preporuka obratiti pažnju na točke spajanja udaljenih radnika, poput VPN koncentratora te kritične aplikacije izložene internetu i otpornost na eDDoS napade.

Tijekom 2022. godine analizirali smo ukupno 4584 napada koje su prepoznali uređaji za zaštitu od DDoS napada smješteni u javnom i privatnom sektoru u Hrvatskoj. Podaci o napadima su preuzeti s uređaja koji mogu identificirati DDoS napade te ne uključuju nezaštićena odredišta i napade koji nisu prepoznati. Napadi su kategorizirani prema taksonomiji DDoS napada tvrtke RioRey, raspoloživoj na sljedećoj poveznici:

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

6. Okruženje prijetnji – *Threat Landscape* 2023.

diverto

6. OKRUŽENJE PRIJETNJI – *THREAT LANDSCAPE* 2023.

Primjenjujući analitičke metode i podatke s kojima raspolažemo, donosimo najznačajnije prijetnje s kojima se trenutno suočavaju Hrvatska, Slovenija te Bosna i Hercegovina u području kibernetičke sigurnosti.

RAZLIKA IZMEĐU PRIJETNJE I RANJIVOSTI

Prijetnja (eng. threat) je mogućnost napada ili zlonamjerna aktivnost koja bi mogla ugroziti informacijski sustav, dok je ranjivost (eng. vulnerability) propust ili manjkavost u informacijskom sustavu koja može omogućiti napadaču da iskoristi neki sigurnosni propust i ostvari neovlašten pristup ili provede druge zlonamjerne aktivnosti. Prijetnje mogu iskoristiti postojeće ranjivosti kako bi izvršile napade. Prijetnje i ranjivosti su međusobno povezane jer se prijetnje često oslanjaju na ranjivosti kako bi ostvarile svoje ciljeve.

ZNAČAJNIJE PRELIJEVANJE GEOPOLITIČKE SITUACIJE

Trenutna geopolitička situacija je prijetnja informacijskoj sigurnosti u Republici Hrvatskoj:

- Hrvatska se nalazi na križanju nekoliko geopolitičkih sila, što znači da su napadi izvana mogući od strane državnih aktera koji žele ugroziti stabilnost i sigurnost države
- kao članica EU-a, Hrvatska dijeli različite vrste podataka sa svojim partnerima u EU-u, što znači da postoji rizik od kibernetičkih napada usmjerenih prema tim podacima
- Hrvatska je geografski pozicionirana između istoka i zapada, što znači da je izložena različitim vrstama napada koji se mogu dogoditi u susjednim zemljama, a zatim se prenijeti u Hrvatsku.
- Većina zapaženih/obrađenih incidenata dogodila se zbog „prelijevanja" aktivnosti iz susjedstva.

Kompromitirani lanac opskrbe/ napadačke grupe izuzetne sposobnosti

Ugroza opskrbnog lanca može imati značajan utjecaj na informacijsku sigurnost, posebno kod organizacija koje ovise o dobavljačima: IT tvrtke, banke, energetika, državne agencije i slično. Napadačke grupe (APT) izuzetne sposobnosti su vrlo vješte u izvođenju naprednih kibernetičkih napada i često ciljaju opskrbni lanac i „manje" sigurne elemente opskrbnog lanca većih organizacija. Kibernetički napadi koji su izvedeni putem ugroženog opskrbnog lanca obično su sofisticirani i teško ih je otkriti. Ugroženi opskrbni lanac je teško otkriti, a može utjecati na učinkovitost organizacije i dovesti do gubitka povjerenja korisnika. Neki od zapaženih/obrađenih incidenata dogodili su se zbog ugrožavanja opskrbnog lanca.

Malware i Ransomware / Fluktuacija/ Rebranding / Copycat ransomware grupa / Disk wipers

Malware je zlonamjerni softver koji se obično upotrebljava za krađu ili uništavanje podataka. On može uzrokovati oštećenje sustava, krađu zaporki, krađu identiteta i slično. *Ransomware* je vrsta *malwarea* koji blokira pristup računalu ili podacima dok žrtva ne plati otkupninu. *Ransomware* napadi mogu biti vrlo štetni za organizaciju, a mogu dovesti do gubitka osjetljivih podataka, smanjenja produktivnosti i gubitka novca. *Disk wipers* kao vrsta zlonamjernog softvera koji se upotrebljava za uništavanje podataka su vrlo opasni jer trajno uništavaju podatke i sustav, čime organizacije dovode u velike probleme. Upotrebljavaju se obično kod ciljanih napada i vrlo su teški za otkrivanje i uklanjanje. Dodatni problem pripisivanja napada jest da se *ransomware* grupe transformiraju i „rebrandiraju" pa se obično ponovno pojavljuju pod drugim imenom i nastavljaju s napadima. Čak i ako se neke grupe raspuste, druge mogu preuzeti njihove metode i nastaviti s napadima na organizacije. Neki od zapaženih/obrađenih incidenata dogodili su se zbog zlonamjernog softvera.

Poslovni model Hacker as a service i značajni porast DDoS napada

Hacker as a service i porast dostupnosti DDoS napada predstavljaju nove izazove u borbi protiv kibernetičkog kriminala. Model *Hacker as a service* je način angažiranja hakera za izvođenje napada. To je postalo moguće jer je sve više hakera i kibernetičkih kriminalaca usmjereno na zaradu, a ne samo na ideološke motive. Model omogućuje čak i manje iskusnim kriminalcima izvršavanje napada na organizacije jer mogu unajmiti „profesionalne" hakere koji će ih voditi kroz proces. Porast dostupnosti DDoS napada je dodatni problem za organizacije koji proizlazi iz navedenog modela. Ovi napadi ciljaju na preopterećenje web poslužitelja organizacije, što dovodi do prekida u radu. Napadi su sada intenzivniji i sofisticiraniji nego prije, a sve češće se upotrebljavaju i kao diverzija kako bi se skrenula pozornost sigurnosnih timova dok drugi napadi prolaze neprimijećeno. Iako se broj napada na organizacije možda smanjio, njihov intenzitet i ciljanost su porasli. Neki od zapaženih/obrađenih incidenata vrlo vjerojatno su posljedica korištenja modelom.

Kompromitacija internetske veze i oblaka (engl. cloud) te njihova (ne)raspoloživost

Ugroza same internetske veze, odnosno servisa u oblaku koji su postali kritični elementi za mnoge usluge koje koristimo postaje značajan problem za veliki broj organizacija. Prijetnja je to koja se već danas realizira (srećom kratkotrajno kroz kraće ispade) kako bi nas podsjetila o sve većoj zavisnosti o telekomunikacijskim vezama i uslugama u oblaku.
Tipični primjer takvog, još uvijek mogućeg napada je preotimanje BGP-a te nedostupnost globalnog pružatelja usluge u oblaku poput Amazona, Azurea ili Googlea.

Kombiniranje tipova socijalnog inženjeringa

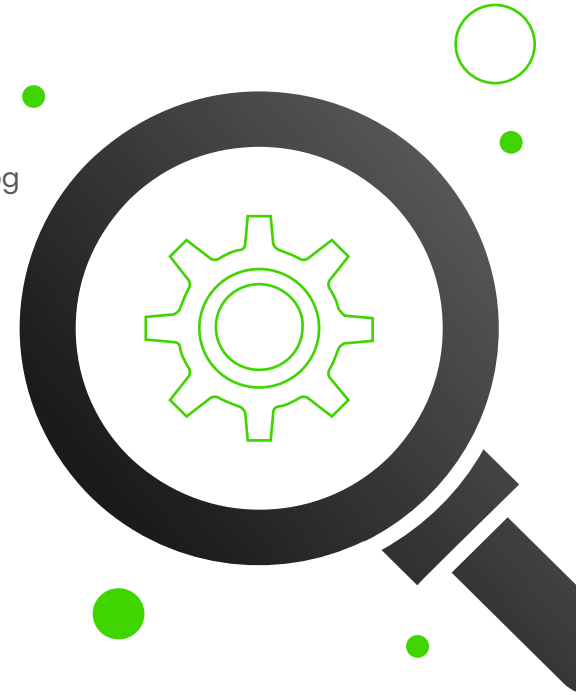
Napadači se sve više orijentiraju na iskorištavanje slabosti ljudske strane kako bi povećali vjerojatnost uspješnog napada. Osim već standardnih *phishing* napada, uočljiva je povećana uporaba vishinga te ispreplitanje različitih kanala za napade gdje napadač, primjerice, kombinira *vishing* zajedno s *phishing* napadom. Ova pojava posebno je naglašena u tzv. TOAD (engl. *Telephone-Oriented Attack Delivery*) napadima, ali i u sve češćim pokušajima da se zaobiđe mehanizam zaštite koji pruža multifaktorska autentifikacija. Takav model se učestalo upotrebljava

kako bi se pribavio neovlašteni pristup sustavima ili kompromitirala poslovna komunikacija (engl. *Business E-mail Compromise*).

Povećano iskorištavanje pogreški u dizajnu, konfiguraciji ili planiranju

Vidljivo je povećano iskorištavanje dizajna, konfiguracijskih pogreški i neispravnog planiranja. Kako se smanjuje površina napada i postoje već brojne sigurnosne kontrole u operativnim sustavima kojima se svakodnevno koristimo, napadači su se orijentirali više na ovakav tip napada gdje još uvijek postoji velika mogućnost pogreške. Napadači navedeno iskoriste kako bi izveli napade poput krađe podataka, *ransomwarea*, *phishinga* ili napada usmjerenih na povećanje pristupa računalnim resursima.

Kibernetičko ratovanje i dezinformiranje



Kibernetičko ratovanje (engl. *Cyber warfare*) je postala svakodnevnica na globalnoj razini kao dio konvencionalnog ratovanja te okosnica hibridnog ratovanja. Trenutačna geopolitička situacija ne pomaže ni Hrvatskoj. Sasvim je uobičajeno upregnuti „kibernetičke ratnike" za ostvarivanje prevlasti u virtualnom svijetu i tijekom samog konvencionalnog, „kinetičkog" ratovanja. Jedan od elemenata koji se često upotrebljava je dezinformiranje koje ne mora biti dio samog ratovanja.

Dezinformacije su postale snažan alat za manipulaciju u digitalnom dobu, i to ne samo javnim mnijenjem. S ciljem obmane, osim dezinformacija, upotrebljava se i širenje lažnih vijesti u cilju utjecanja na mišljenje ili poticanje žrtava manipulacije na određenu akciju.

Zamke za sustave i podatke

Napadači su shvatili kako mogu postaviti „digitalne zamke" za sustave i podatke. Za razliku od aktivnog napada koji isto tako mogu aktivno izvoditi, u mogućnosti su uspostaviti domene i druge digitalne objekte kako bi izgledali što sličniji pravima. Na navedenim mjestima bi žrtve najčešće mogle pogriješiti u pisanju ili prepisivanju s obrasca ili zvučne komunikacije te čekaju da žrtva pogriješi i pošalje podatke na krivu adresu e-pošte, domenu ili odredište (npr. dvrto.hr umjesto diverto.hr) te konfiguriraju svoje sustave tako da sva odredišta budu prihvaćena i spreme sve što je poslano. Još opasniji slučaj je dohvaćanje komponenti ili izvršnog koda iz takvih izvora.

Nedostatak ljudi i znanja: nedostatak stručnjaka za kibernetičku sigurnost i nedostatak operativnog osoblja

Na tržištu rada vlada nedostatak stručnjaka koji su sposobni pratiti razvoj tehnologije i prepoznati nove prijetnje i ranjivosti kako bi pravovremeno mogli poduzeti zaštitne mjere. Postojeći stručnjaci na području kibernetičke sigurnosti su već sada preopterećeni velikim brojem zadataka i odgovornosti, što znači da su organizacije podložnije greškama i propustima koji mogu rezultirati sigurnosnim ranjivostima. Kibernetički stručnjaci i operativno osoblje su rijetki resursi, a plaće i uvjeti rada su obično visoki. Organizacije s ograničenim proračunima mogu se naći u situaciji da si ne mogu priuštiti potrebne resurse za prikladno upravljanje sigurnošću informacijskih sustava. To dovodi do daljnjeg povećanja rizika od sigurnosnih incidenata i potencijalnih šteta. U RH je ovaj problem dodatno naglašen ulaskom u EU i otvaranjem mogućnosti rada izvan RH. Većina zapaženih/obrađenih incidenata događa se zbog nedovoljnog broja ljudi koji mogu pratiti događanja u organizaciji.

7. Izazovi budućnosti

diverto

7. IZAZOVI BUDUĆNOSTI

Slijedi prikaz izazova koji nas očekuju u bliskoj budućnosti i srednje ročno.

Upotreba umjetne inteligencije

Umjetna inteligencija će imati veći utjecaj na svakodnevne odluke u poslovnom, ali i u privatnom svijetu. Uz mnoge nedostatke, a prvenstveno one u kojima UI i dalje ne može potpuno zamijeniti čovjeka, ipak će nastaviti svoj razvojni put i povećat će utjecaj u budućnosti odlučivanja. Strah od njenog negativnog utjecaja na život ljudi je opravdan. Čovjek je tvorac UI i prenio je vlastite obrasce razmišljanja u njene "algoritme". Predrasude i pristranosti već sada pokazuju zabrinjavajući utjecaj na rezultate u odlučivanju koje donosi UI.

Izlaskom ChatGPT-a u javnu domenu korištenja, umjetna inteligencija postaje dio arsenala koje će koristiti napadači. Olakšava i ubrzava stvaranje alata i drugih elemenata za ofenzivno djelovanje u kibernetičkom prostoru. Primjerice, stvaranje koda u željenom programskom jeziku za točno određene operacije nikada nije bilo lakše. Osim sintakse, napadač dobiva i detaljan opisni sadržaj pojedinačnih blokova naredbi. Izrada tekstualnog sadržaja za *Phishing* mailove umanjuje potrebu za vlastitom kreativnošću napadača. Sve što napadač treba uraditi je postaviti pitanje, a rezultat dolazi od sada uz znatno manje napora.

Povećana potreba za obavještajnom analitikom

Biti u prednosti, znači pobijediti. Nažalost, spomenuta rečenica ide često u korist napadača. No da bi smo povećali prednost pred napadačima, sve češće ćemo posezati za provjerenim disciplinama obavještajne analitike u kibernetičkom prostoru. Znanja i vještine obavještajne analitike se razvijaju desetljećima i to nije novo područje, ali se intenzivno širi i na digitalnu razinu. Taj će porast u vremenu ispred nas biti značajan.

Aktivno praćenje grupa napadača kroz dulji vremenski period, definiranje načina djelovanja, uočavanje promjena u taktikama i tehnikama olakšava izgradnju profila napadača te pravovremenu pripremu zaštite organizacija. Time će disciplina prikupljanja podataka te njihova eksploatacija rezultirati stvaranjem obavještajnih informacija čija će važnost biti sve veća.

Porast prijetnji u kritičnoj infrastrukturi

Značajnim ulaganjima u modernizaciju sustava automatizacije te povezivanjem na Internet, kritična infrastruktura će biti izloženija vanjskim prijetnjama. Iz Divertovog iskustva možemo potvrditi da vlasnici kritičnih infrastruktura imaju priliku shvatiti da je iznimno važno provjeriti i razumjeti sigurnosne postavke svojih sustava. Zahvaljujući tome, mogu se izbjeći česte pogreške u vjerovanju da su sustavi potpuno odvojeni od interneta ili poslovnog dijela mreže organizacije. Ovo je ključno kako bi se osigurala sigurnost i zaštitili važni sustavi od kibernetičkih prijetnji. Porast broja komponenti, a posebno IIoT uređaja poboljšati će automatizaciju te će odvesti industrijske kontrolne sustave i u oblak (engl. *Cloud*).

Zbog direktnog utjecaja na okruženje u kojem živimo, a posebno utjecaja na živote, kritična infrastruktura će i dalje biti zanimljiva napadačima. Kako kriminalnim skupinama koje imaju financijske motive, tako i državno-sponzoriranim grupama s političkim motivima.

Izraženije hibridno ratovanje

Prethodna godina je pokazala svu moć hibridnog ratovanja na relaciji Rusije i Ukrajine. Iako su oružani sukobi počeli u veljači, dezinformiranje javnosti i širenje lažnih vijesti, te kibernetičko djelovanje prema Ukrajini seže godinama unazad.

Sinkroniziranjem medija, oružanih snaga i kibernetičke vojske moguće je destabilizirati funkcioniranje države djelujući iz više pravaca istovremeno. U budućnosti će se još više koristiti mediji, prije svega za utjecaj na javno mnijenje stanovništva šireći lažne vijesti u eter putem interneta, televizije, radija i drugih kanala informiranja. Kao i mediji, i kibernetička vojska će se još više koristiti, ali za napade na kritičnu infrastrukturu i špijunažu. Za razliku od konvencionalne vojske, ratovanje u stvarnom svijetu je ograničeno teritorijalnim djelovanjem, dok kibernetička vojska nema takva ograničenja.

Mnogobrojne sankcije uvedene Rusiji mogle bi pojačati njeno kibernetičko djelovanje s ciljem industrijske špijunaže. Treba imati na umu da je Rusija godinama uvozila tehnologiju koju i dalje mora održavati ili zamijeniti nečim adekvatnim. Najjeftiniji način da odgovori na "*How to*" je krađa intelektualnog vlasništva.

Porast broja aplikacija i API sučelja, te kompleksnosti

Daljnji rast digitalizacije i automatizacije ima za posljedicu sve veći broj aplikacija, API sučelja i mikroservisa gdje je veliki udio navedenih izložen na Internetu ili su raspoloživi kroz druge aplikacije i API sučelja. Navedene aplikacije i API sučelja su nužna kako bi pristupali funkcionalnostima, ali i uspješno automatizirali procese.

Sve veća kompleksnost i zavisnost između sučelja, automatizirane razmjene podataka i komunikacije među sučeljima, podiže i razinu izloženosti odnosno rizika. Primjenom agilnih principa i razvoja temeljenog na isporuci malih i inkrementalnih isporuka, tradicionalno modeliranje prijetnji i primjena sigurnog dizajna predstavlja izazov pri razvoju, što dodatno podiže nesigurnost u aplikacije i sučelja. Svjesni smo kako je u sučelja i njihove zavisnosti potrebno implementirati adekvatne sigurnosne kontrole i redovno testirati kako bi se spriječila kompromitacije podataka i same infrastrukture, ali za sada ne postoji industrijska praksa kako pomiriti učinkovitost, visoku razinu kohezije i sigurnost. Izazov će svakako biti u osiguravanju navedenih aplikacija i sučelja kao i njihovih komponenti, te redovno održavanje razine sigurnosti.

Upravljanje sigurnosti dinamičke infrastrukture

Sve veća automatizacija infrastrukture bilo u javnom ili privatnom oblaku na mrežnoj razini i razini operativnog sustava je očekivana i u trenutnom zamahu. Svakodnevno podizanje i zaustavljanje podmreža, pravila vatrozida, računala i pripadajućih operativnih sustava su prednosti koje organizacije prepoznaju i kapitaliziraju. Međutim, pojavljuje se sve veći izazovi u upravljanju sigurnošću. Primjerice, kako napraviti ispravan odgovor na incidente na aplikacijskoj kontejneru koji se pojavio i nestao uz dinamička mrežna pravila i sučelja koja su se u međuvremenu promijenila?

Izazova u takvom okruženju je mnogo. Znati u svakom trenutku površinu napada, te kako efikasno upravljati imovinom što uključuje i upravljanje ranjivostima i upravljanje incidentima samo je početak avanture osiguravanja dinamičke infrastrukture.

Nedostatak stručnjaka za kibernetičku sigurnost

Jedan od najvećih izazova je svakako nedostatak stručnjaka za kibernetičku sigurnost. Među 10 najvećih prijetnji kibernetičkoj sigurnosti (za razdoblje do 2030. godine) ENISA navodi i nedostatak stručnjaka za kibernetičku sigurnost. *World Economic Forum* navodi i sljedeće: sektoru kibernetičke sigurnosti nedostajati će 3,4 milijuna stručnjaka. Da problem postaje sve izazovniji potvrđuje i istraživanje prema kojem se jaz (u nedostatku stručnjaka za kibernetičku sigurnost) u 2022. godini povećao za 26,2% u odnosu na 2021.

Jedna od posljedica nedostatka stručnjaka za kibernetičku sigurnost postala je razvidna u WEF-ovom istraživanju prema kojemu će 59% tvrtki imati poteškoće u području kibernetičke sigurnosti. Nažalost, ni to nije sve. Problem postaje još veći kada se pogleda rezultat istraživanja provedenog na postojećim (zaposlenim) stručnjacima za kibernetičku sigurnost: 30% njih planira primijeniti posao u sljedeće dvije godine.

5G tehnologija i sigurnosni rizici

Glavni rizici 5G tehnologije mogu se kategorizirati na sljedeće kategorije: rizici za privatnost, prijetnje nacionalnoj sigurnosti, ovisnost lanca opskrbe, kibernetički napadi, negativni učinci na zdravlje i gubitak radnih mjesta zbog povećanja učinkovitosti.[12]

Dodatno, poseban sigurnosni izazov predstavlja virtualizacija mrežnih funkcija (engl. *Network Function Virtualization*, NFV - koncept koji definira arhitekturu mreže temeljenu na virtualnim mrežnim funkcijama).

S obzirom na navedeno te nezaobilaznu i široku implementaciju 5G tehnologije, posebnu pozornost potrebno je posvetiti ranjivostima i prijetnjama 5G tehnologije, a s ciljem ovladavanja rizicima 5G tehnologije.

[12] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

diverto

Diverto pruža visokospecijalizirani spektar usluga iz područja informacijske i kibernetičke sigurnosti. Usluge prilagođavamo kako bismo zadovoljili specifične potrebe naših klijenata s ciljem unapređenja njihove sigurnosti uz najbolji omjer cijene i kvalitete.

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

Izvještaj je rezultat zajedničkog rada s našim korisnicima, kojima se 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.