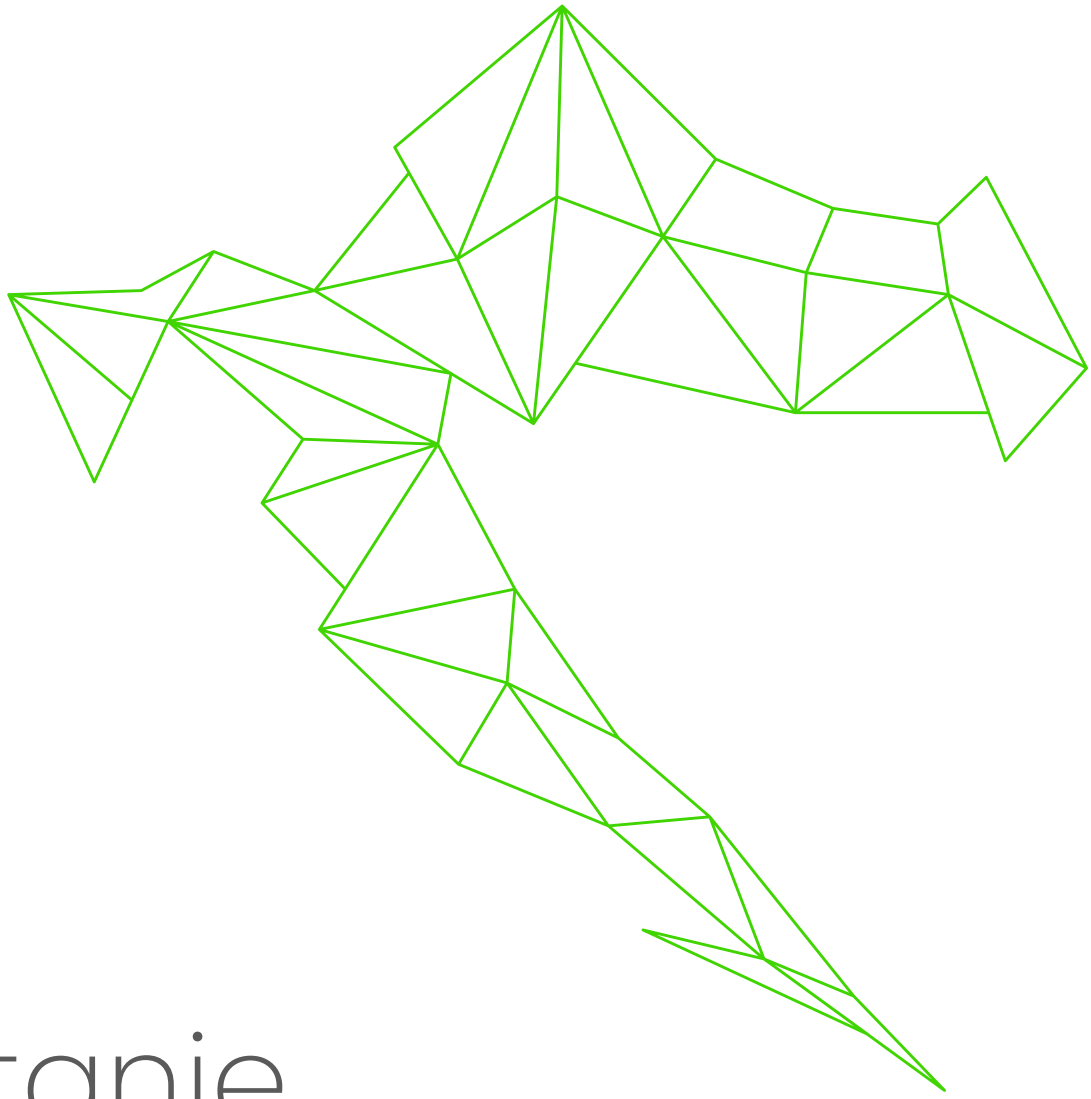
diverto

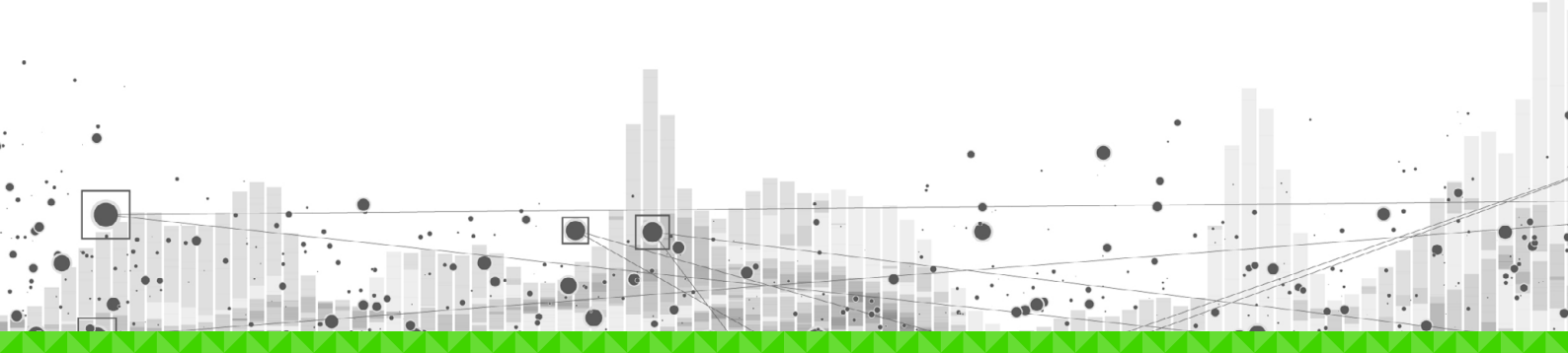


Stanje informacijske sigurnosti

U REPUBLICI HRVATSKOJ

2021.

— INDEX



// UVODNIK

Pred vama je treće izdanje našeg osvrta na informacijsku sigurnost u Republici Hrvatskoj. Ohrabreni vašim interesom, kao i pozitivnim reakcijama koje smo dobili, nastavljamo izdavati ovaj izvještaj. I dalje nastojimo svako izdanje poboljšati kako bi vam bilo od što veće koristi.

Kao i prethodni, i ovaj izvještaj rezultat je zajedničkog rada s našim korisnicima, kojima se ovim putem zahvaljujem. Rezultat je to rada i svih osoba i timova unutar Diverta koji stoje iza gotovo svakog pokazatelja i iznesene brojke. Izvještaj je temeljen na pregledu kroz tri različite perspektive informacijske sigurnosti: upravljačke, napadačke i obrambene, uz osvrte na aktualne situacije na području informacijske sigurnosti u Republici Hrvatskoj.

Ubrzana digitalizacija bez ozbiljnog pristupa sigurnosti nije opcija. Vidjeli smo to i u prethodnoj godini. Svjedoci smo sve izraženije digitalizacije i rada od kuće, ali svjedoci smo i posljedica koje se događaju bez ozbiljnog pristupa sigurnosti.

Ovisnost o dobavljačima sve je izraženija u procesnom (OT) i IT svijetu, a sigurnost lanca dobavljača svima nam je postala izazov. Prošla godina nam je pokazala kako je lanac dobavljača sve veća i poželjnija meta napadača, a vidjeli smo posljedice napada na lanac dobavljača na lokalnoj i na globalnoj razini. Na konkretnim primjerima naših korisnika uvjerili smo se da nije dovoljno vjerovati, već je potrebno tražiti i provjeriti sigurnosnu razinu svakog dobavljača.

Preuzeta e-mail komunikacija i *ransomware* i dalje su najdominantnije kategorije incidenata u Hrvatskoj. Najveći broj incidenata s konkretnim i značajnim posljedicama koje smo zabilježili u 2021. godini upravo su bili te kategorije. Naravno, to ne govori da ostalih kategorija nije bilo, već da su ove kategorije znatno iskočile.

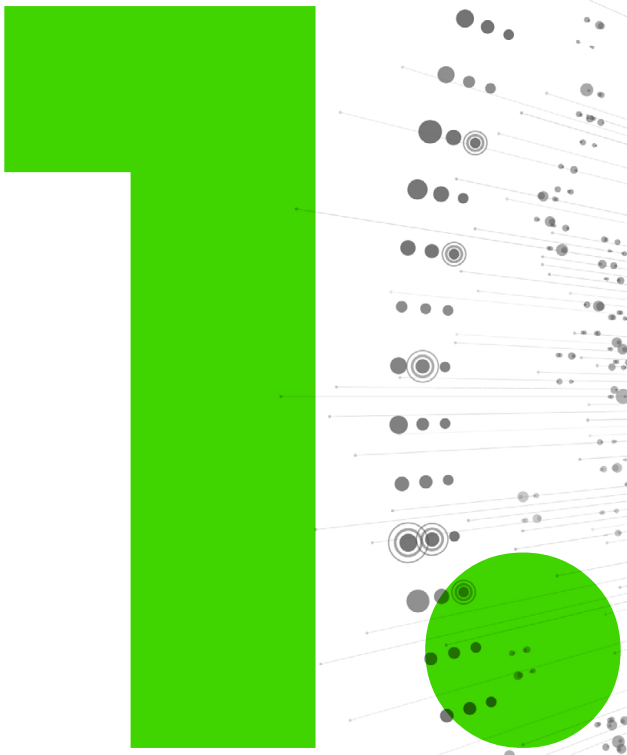
Red i *Purple teaming* postaju sve prihvaćeniji načini testiranja informacijske sigurnosti. Redovno izvođenje takvih testiranja i vježbi postalo je standard, a penetracijski test industrijski minimum. Ne radite li *Red, Blue* i *Purple* vježbe u vašoj organizaciji, znači da gubite korak s drugim organizacijama.

Rad na preventivnim aktivnostima i dalje je važan i najbolji način smanjenja rizika informacijske sigurnosti. Otegotna okolnost je što je uočljiv nedostatak stručnjaka na području informacijske i kibernetičke sigurnosti koji će raditi na takvim aktivnostima, a potražnja za istima će samo rasti u sljedećem periodu. To već danas za većinu organizacija predstavlja rizik kojim se treba pravovremeno pozabaviti.

Izazova je puno i njihovom rješavanju potrebno je pristupiti već danas. Nastavljamo s izradom ovog izvještaja kako bismo Vam pomogli u pregledu trendova i stanja informacijske sigurnosti u Republici Hrvatskoj te unaprijedili naše procjene i razinu informacijske sigurnosti. U nadi da će vam i ovaj izvještaj pomoći u tome.

Vlatko Košturjak, CTO

diverto



Upravljačka perspektiva

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 zaštiti svoju najvrjedniju imovinu.

Ključni pokazatelji u promatranom razdoblju:

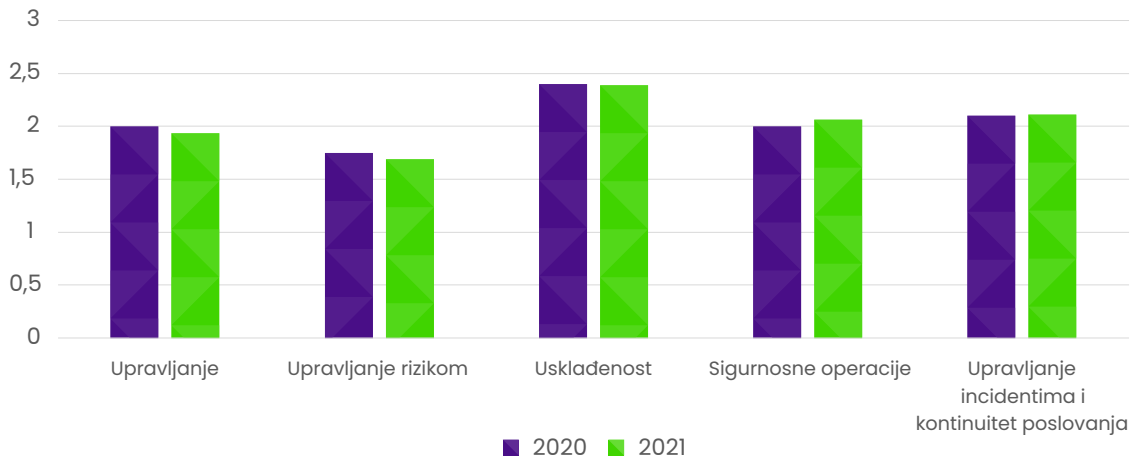
- povećana izloženost kibernetičkim napadima kao posljedica sve izraženije digitalizacije i rada od kuće
- pandemija je povećala svijest o informacijskoj sigurnosti, posebno u segmentu osiguranja kontinuiteta poslovanja
- informacijska sigurnost se i dalje shvaća kao IT sigurnost ili kao područje usklađenosti s regulativom
- *phishing* je i dalje dominantan vektor uspješnih i *„jeftinih"* napada na informacijske resurse organizacija
- *ransomware* napadi su i dalje u porastu, a napadači su prijeteći objavom povjerljivih informacija dodali još jednu polugu u iznudi
- globalni trendovi ukazuju na povećan broj zabilježenih sigurnosnih incidenata, dok organizacije u RH i dalje nerado informiraju zainteresiranu javnost o sigurnosnim incidentima, tako da raspolažemo samo našim podacima i podacima MUP-a[1] na temelju kojih je vidljiv porast u odnosu na prošlu godinu od minimalno 30 %
- napad na lance opskrbe postaje sve češći vektor kompromitacije, posebice kod pružatelja usluga koji ostvaruju udaljeni pristup, pružaju administratorski softver ili gotove softverske komponente.

[1] Poredbeni prikaz kaznenih djela kibernetičkog kriminaliteta 2020./2021.

Informacijska sigurnost pozicionirala se kao obavezna tema o kojoj se raspravlja na upravljačkoj razini i samim time počinje utjecati na strateške odrednice razvoja kompanija. Nedostatak razumijevanja i pozicioniranja uloge informacijske sigurnosti i dalje je prisutan, ali uz kontinuiran dijalog očekuje se jače osvještavanje, razjašnjenje granica između sukladnosti i upravljanja sigurnošću te rad na podizanju zrelosti postojećih mehanizama zaštite.

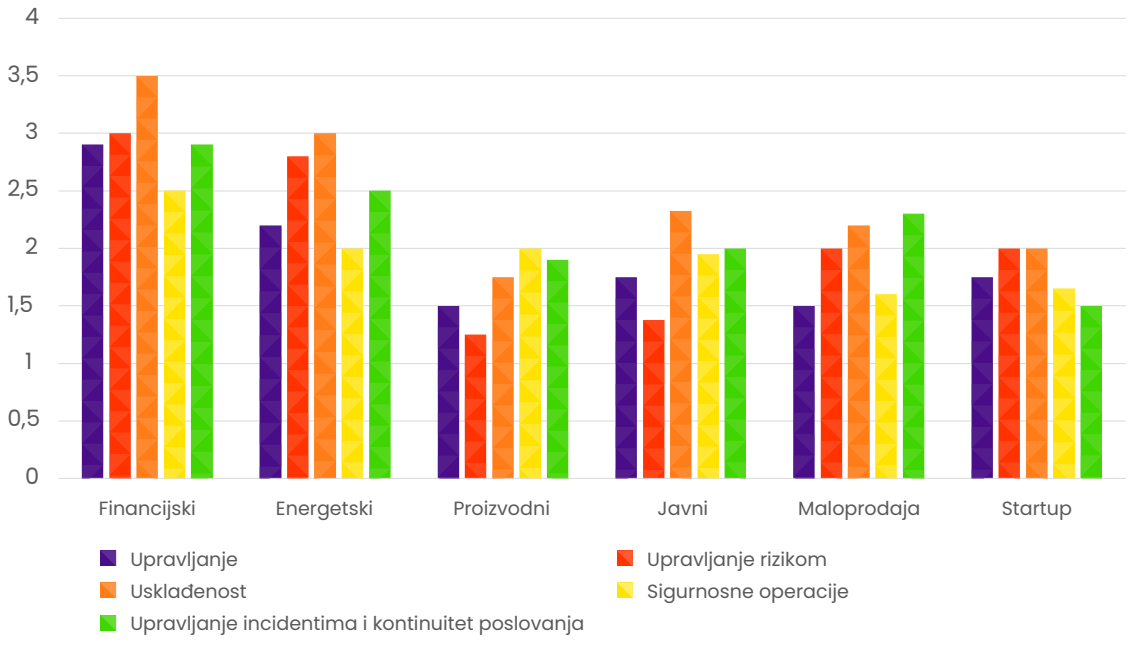
Ivan Kalinić, voditelj strateškog razvoja sigurnosti

Razina zrelosti je dobar osnovni pokazatelj kretanja informacijske sigurnosti u organizacijama. Prosječna razina zrelosti informacijske sigurnosti u 2021. ne donosi značajne promjene po područjima u odnosu na 2020. godinu.



SLIKA 1 *Prosječna razina zrelosti područja informacijske sigurnosti u 2021. naspram 2020. [Izvor: Diverto]*

Kako je razina zrelosti informacijske sigurnosti različita od industrije do industrije, napravljen je i usporedni pregled po industrijama. Naravno, financijski i dalje predvodi po svojoj zrelosti.



SLIKA 2 *Prosječna razina zrelosti područja informacijske sigurnosti 2021. [Izvor: Diverto]*

1.1. Trendovi

Na globalnoj razini, u 2021. godini uočili smo kako su rizici informacijske sigurnosti „pali“ s drugog na treće mjesto po važnosti percipiranog rizika za organizacije, ustupajući mjesto globalnoj pandemiji. U Republici Hrvatskoj za korisnike Divertovih usluga možemo potvrditi taj trend, dok sveukupno gledajući, situacija je takva da se rizici informacijske sigurnosti ne percipiraju[2] kao rizici koji imaju značajnog utjecaja na poslovanje organizacija.

Registrirani su pozitivni pomaci u razvoju svijesti o važnosti informacijske sigurnosti i o utjecaju rizika informacijske sigurnosti na poslovanje pojedinih organizacija, neovisno o sektoru. Bez obzira na pomake, kod većine organizacija je i dalje izražen nedostatak razumijevanja uloge informacijske sigurnosti, kao i njezine implementacije po načelima dobrih praksi unutar organizacija. Strategije razvoja informacijske sigurnosti, kao i vizije uloge informacijske sigurnosti u organizacijama vrlo su raznolike. Bez prethodnog usklađenja s ciljevima organizacije, provedene analize rizika i isplativosti, uglavnom se temelje na „nišnom“ pristupu nabave automatiziranih rješenja bez prikladne implementacije i obuke operatera sustava, ali i svih zaposlenika.

Na tržištu usluga informacijske sigurnosti u Republici Hrvatskoj primjetan je porast potražnje i ponude za raznim tehničkim rješenjima i uslugama testiranja IT i OT infrastrukture, kao i aplikativnih rješenja. Uslijed velike potražnje, tržište bilježi veći broj pružatelja upravljanih usluga informacijske sigurnosti, ali bez standardizacije razine usluge u skladu s dobrim praksama. Ulaganja u informacijsku sigurnost nisu sveobuhvatna i najčešće se smatraju nepotrebnim troškom bez povrata ulaganja.

Pravila dobre prakse najviše se prate u reguliranim sektorima kao što su financijski, energetski i telekomunikacijski sektor. Provođenje Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, kao i sukladno Zakonu započeti procesi nadzora od strane nadležnih sektorskih tijela, pozitivno su se odrazili na razinu svijesti poslovodstva o važnosti informacijske sigurnosti, što je posljedično dovelo do povećanja ulaganja u informacijsku sigurnost. Primjećujemo pomak prilikom definiranja projektnih zadataka implementacije sustava upravljanja informacijskom sigurnošću (ISMS), pri kojem se uz implementaciju ISO27000 baziranih ISMS-ova počinju primjenjivati i specijalizirani standardi poput ISA/IEC 62443, NIST CSF, SOC2 i slični.

[2] Izvor, Svjetski ekonomski forum: https://widgets.weforum.org/regionalrisks2020/home.html

1.2. Procjena kretanja u 2022.

- prethodno spomenuti „pad“ percepcije rizika informacijske sigurnosti je privremen i u 2022. godini očekujemo da će rizici informacijske sigurnosti biti prvi rizici koje će razmatrati sve organizacije
- financijska industrija u Republici Hrvatskoj će i dalje snažno investirati u informacijsku sigurnost zbog nadzora Europske banke
- sigurnost lanaca opskrbe već je postala prioritet u industrijama koje ovise o dobavljačima i trećim stranama, a očekuje se jača regulacija ili stroža kontrola mehanizama sigurnosti i povezanih rizika uz eksternalizaciju
- hibridni način rada postaje svakodnevica, informacijska sigurnost će se sve više shvaćati kao „*business enabler*“ u situacijama otežanog poslovanja, ali i „*cost saver*“ ako se promatraju troškovi radnih mjesta
- potreba za postizanjem prihvatljive zrelosti informacijske sigurnosti i dokazivanjem kontinuirane usklađenosti korištenjem specijaliziranih standarda, poput standarda TISAX, SOC2 i IEC 62443 biti će izraženija za organizacije koje nude svoje usluge na međunarodnom tržištu
- jačanje ideoloških i „*haktivističkih*“ napada te napada sponzoriranih od strane države iznjedrit će veliki broj do sada nepoznatih tehnika i taktika napada koji će se upotrebljavati u svakodnevnim napadima

- neselektivni i vrlo intenzivni kibernetički napadi na sve organizacije koje su povezane na Internet
- sve učestalija primjena proaktivnih načela u informacijskoj sigurnosti korištenjem jedinstvenih točaka nadzora i upravljanja incidentima u organizacijama
- nedostatak stručnjaka informacijske i kibernetičke sigurnosti već predstavlja rizik za većinu organizacija, a očekuje se povećana potražnja za kompetencijama na području informacijske i kibernetičke sigurnosti
- daljnje orijentiranje k upotrebi *cloud* usluga i pomak prema „*Zero trust modelima*“
- sve intenzivnija i uspješnija upotreba umjetne inteligencije i strojnog učenja u svrhe falsificiranja dokumentacije, manipulacija informacijama i upravljanja javnim mišljenjem.

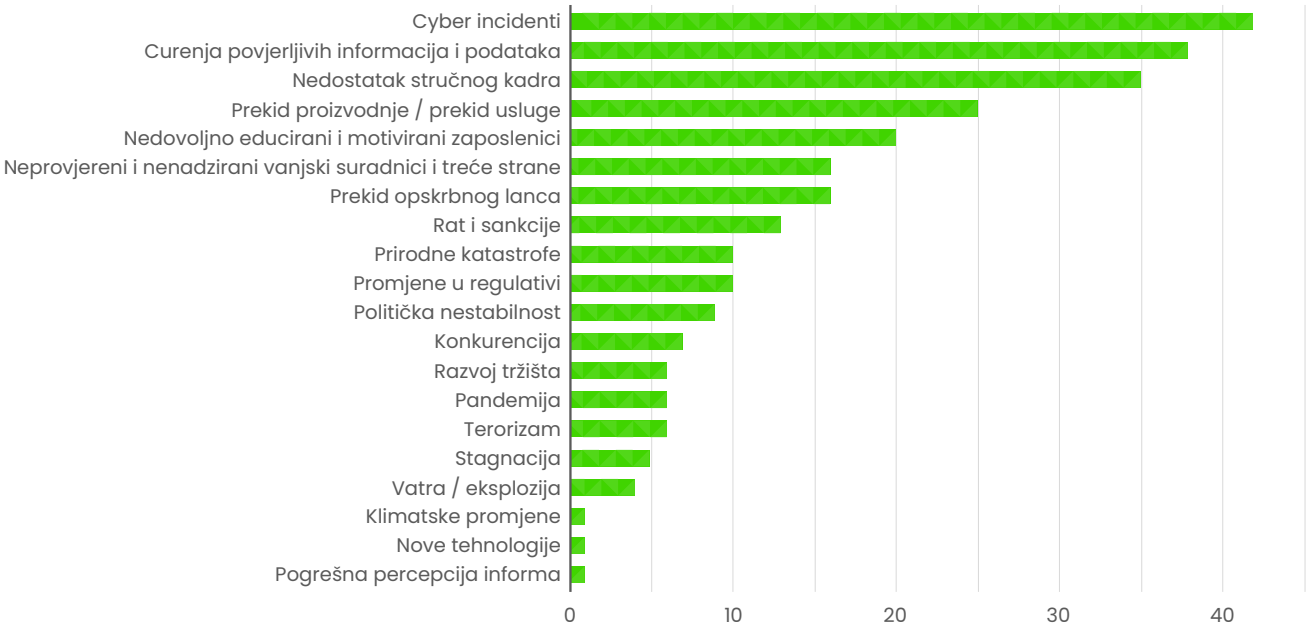
1.3. Istraživanje Diverta o percepciji rizika

Na svjetskoj razini provode se razna općenita i sektorska istraživanja o stanju informacijske / kibernetičke sigurnosti i percepciji informacijske sigurnosti u organizacijama. Navedena istraživanja daju vrlo vrijedne informacije organizacijama koje žele uspostaviti ili postići određenu razinu zrelosti informacijske / kibernetičke sigurnosti. Takav je način dijeljenja informacija posebno vrijedan osobama koje su u organizacijama i tvrtkama zadužene za informacijsku sigurnost. Na razini Republike Hrvatske nismo uspjeli pronaći relevantne informacije i istraživanja koja bi obuhvatila tematiku percepcije osoba zaduženih za informacijsku sigurnost. Imajući to u vidu, samostalno smo proveli inicijativu istraživanja i prikupljanja podataka o stanju informacijske sigurnosti u RH. Početkom ove godine izradili smo *online* anketu i poslali je na ispunjavanje ograničenom skupu organizacija na području RH. Osobe koje su davale odgovore na pitanja iz ankete bile su najmanje razine Voditelj IT odjela, CISO, CSO, COO, CFO i slične razine. Svim našim ispitanicima zajedničko je postojanje svijesti o rizicima informacijske sigurnosti, iako ta razina nije jednaka kod svih.

Svjesni smo ograničenja provedbe *online* ankete kao i pripadajućih pristranosti koje mogu utjecati na rezultate. Također, sa sviješću o ograničenjima provođenja takve ankete na ograničenom uzorku ispitanika, željeli bismo potaknuti organizacije na sudjelovanje u anketi šireg opsega koja bi se provodila periodički, a rezultati tih istraživanja bi uvijek bili dostupni zainteresiranoj javnosti. U nastavku Vam predstavljamo par zaključaka koji bi bez obzira na ograničenja trenutnog istraživanja mogli biti relevantni za većinu organizacija.

1.3.1. Percepcija rizika – što organizacije u RH smatraju najvećim rizikom za njihovo poslovanje

Prema Vašem razmišljanju, što predstavlja najveći rizik za Vašu organizaciju?
Možete izabrati više odgovora. 60 odgovora



SLIKA 3 *Rizici koje prepoznaju organizacije koje su sudjelovale u ispitivanju. [Izvor: Diverto]*

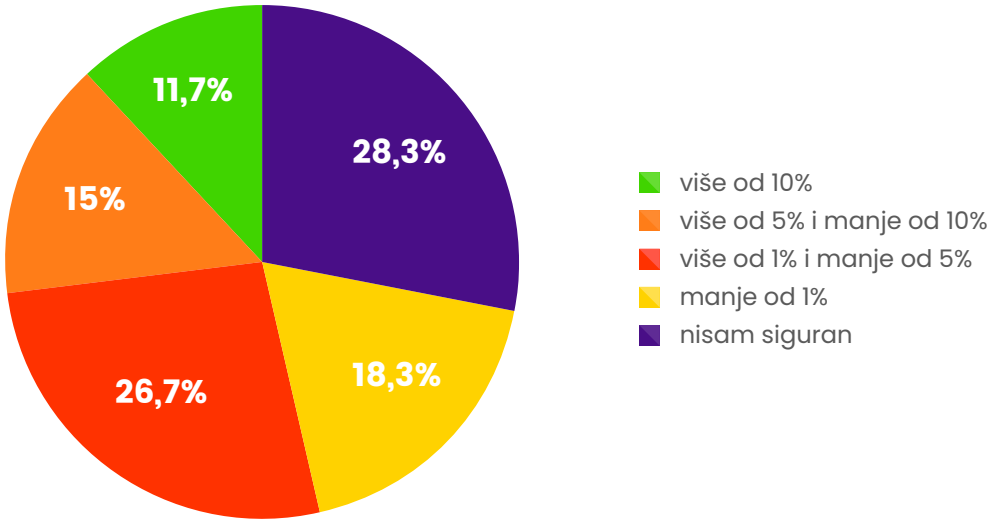
S obzirom da je uzorak bio ograničen (60 organizacija) i s obzirom da većina tih organizacija već ima određena saznanja o rizicima koje nosi nenadzirana upotreba ICT tehnologija, te imajući u vidu „nedavno" donošenje Opće Uredbe, najviše prepoznati rizici vežu se uz *cyber* incidente, curenja podataka i nedostatak stručnog kadra. Međutim, zanimljivo je da su prekid proizvodnje i prekid u lancu opskrbe tek na 4. i 5. mjestu po percepciji ispitanih organizacija, dok je na globalnoj razini prema ACGS[3]-u i WEF[4]-u to rizik broj 1 u prošloj godini.

1.3.2. Shvaćanje uloge informacijske i kibernetičke sigurnosti u organizaciji

Želja nam je bila ispitati poziciju informacijske sigurnosti unutar organizacije i koliki utjecaj ta osoba/funkcija ili organizacijska jedinica ima na organizaciju. Pozitivan trend je da sve više organizacija ima zasebni organizacijski dio zadužen za informacijsku sigurnost, čak 43 % ispitanih organizacija, dok trećina organizacija i dalje smatra da je to, formalno ili neformalno, posao IT odjela. Primjetan je trend angažiranja eksternalizirane CISO uloge kod 7 % organizacija. Dodatno, preko 70 % ispitanih organizacija na sastancima uprave raspravlja o pitanjima informacijske sigurnosti (40 % redovno i 33 % u situacijama kad procjena rizika pokaže da bi određeni događaj mogao prouzročiti štetu za organizaciju).

1.3.3. Udio IT budgeta koji se izdvaja za informacijsku/ kibernetičku sigurnost i na što se najviše troši sigurnosni budžet

Koji postotak IT budgeta trošite na informacijsku / kibernetičku sigurnost?
60 odgovora



SLIKA 4 *Udio IT Budgeta koji se izdvaja za informacijsku sigurnost. [Izvor: Diverto]*

[3] https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
[4] https://www.weforum.org/reports/the-global-risks-report-2021

Pokušali smo dobiti informacije koje daju uvid u udio IT budžeta koji se troši na IS i na što se najviše troši:

Okvirno, s obzirom da dio ispitanika nije bio siguran u budžet koji se upotrebljava, distribucija budžeta za IS izgleda ovako:

Naravno, kod odgovora na incidente nismo dobili odgovore organizacija koje su imale značajne incidente u razdoblju od protekle dvije godine, tako da bi ovi rezultati mogli postati značajno drugačiji u slučaju šireg istraživanja.

1.3.4. Testiranje sigurnosti i upravljanje incidentima

Preko ¾ ispitanih organizacija je provelo ispitivanja informacijske sigurnosti u zadnjih godinu dana, pored toga je pozitivno da 73 % organizacija nije imalo značajnih incidenata i da su samo dvije organizacije imale značajne incidente. 66 % organizacija ima uspostavljen i funkcionirajući postupak odgovora na incidente.

1.3.5. Načini pribavljanja informacija o aktualnim zbivanjima u svijetu i ranjivostima sustava

Velika većina, odnosno 5/6 organizacija oslanja se na informacije od dobavljača i proizvođača sustava, što uz trenutna stanja uređenosti ugovornih odnosa iz aspekta informacijske sigurnosti može predstavljati veliki rizik jer, govoreći iz iskustva, obavještavanje od strane dobavljača ili proizvođača je najčešće na dobrovoljnoj bazi i nije formalizirano ugovorom.

73%

ORGANIZACIJA NIJE IMALO ZNAČAJNIH INCIDENATA

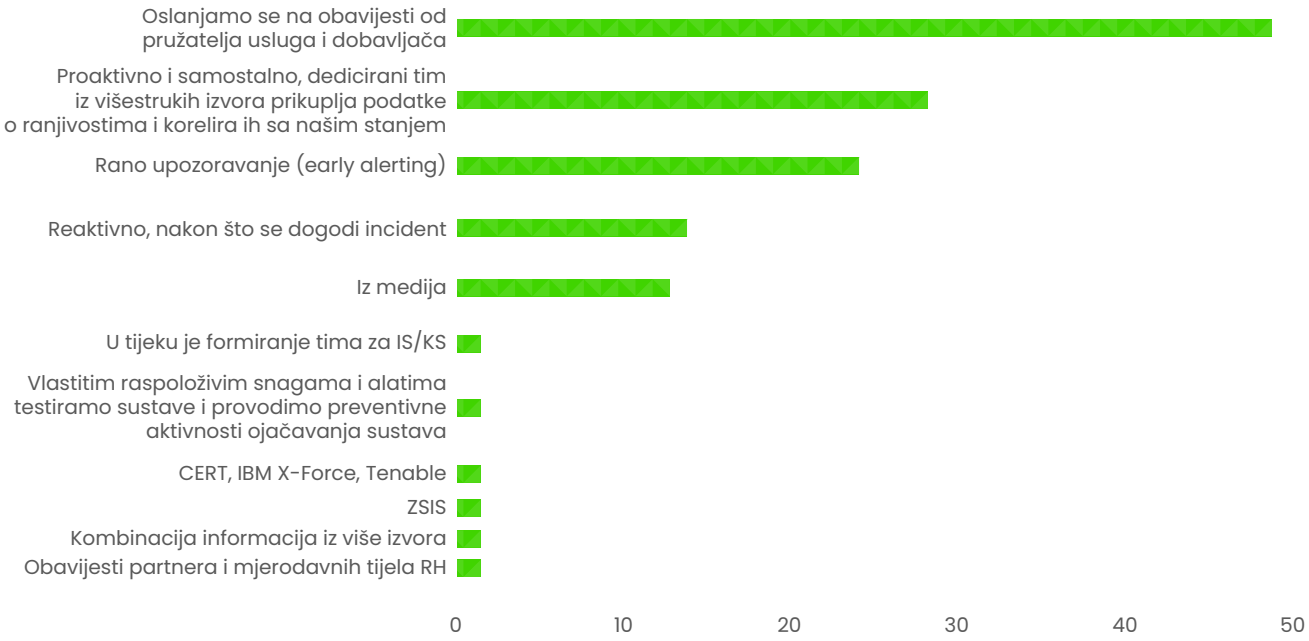
27%

ORGANIZACIJA JE IMALO INCIDENT MANJEG ILI VEĆEG OPSEGA

66%

ORGANIZACIJA IMA USPOSTAVLJEN I FUNKCIONIRAJUĆI POSTUPAK ODGOVORA NA INCIDENT

Načini kako se informirate o prijetnjama i ranjivostima Vaših sustava?
Možete izabrati više odgovora. 60 odgovora



SLIKA 5 *Najčešći načini pribavljanja informacija o novim prijetnjama i ranjivostima sustava. [Izvor: Diverto]*

1.3.6. IT i OT, koja je razlika?

Donošenje NIS direktive i stupanjem na snagu ZOKS-a, aktualizira se tematika korištenja ICT tehnologija u industrijskim kontrolnim sustavima. Gartner je to 2005. godine nazvao OT tehnologijama (OT sustavima). OT sustavi i tehnologije upotrebljavaju se u 33 % ispitanih organizacija, dok daljnjih 25 % nije upoznato s terminom OT/procesni sustavi, stoga postoji mogućnost da takvih sustava ima i više.

diverto

Napadačka perspektiva

2. NAPADAČKA PERSPEKTIVA

Pregledom provedenih penetracijskih testiranja tijekom 2021. godine prikazat ćemo stanje informacijske sigurnosti iz perspektive napadača. Vjerujemo da smo provedenim testiranjima otkrili i pomogli pri otklanjanju značajnog broja ranjivosti kojima napadači mogu prouzročiti financijsku i reputacijsku štetu organizacijama te zajedno s Vama sudjelovali u smanjivanju rizika i podizanju razine sigurnosti informacijskih sustava.

Sigurnosna testiranja u najvećem broju su provedena nad vanjskim, unutarnjim i bežičnim infrastrukturama te mobilnim, desktop, web aplikacijama i servisima.

2.1. Pozitivni pomaci i procjena kretanja

Procjena kretanja za 2021. godinu iz izvještaja stanja informacijske sigurnosti za 2020. godinu u većem je dijelu točno predviđena. Zaista se sve više organizacija koje prethodno nisu provodile sigurnosna testiranja odlučilo na provođenje istih. Također, sigurnosna testiranja pristupa trećih strana kroz *assume-breach* scenarije bila su u porastu i tijekom 2021. godine.

Pozitivan pomak je uočen i pravovremenim testiranjima sustava prethodno puštanja u produkciju. Sigurnosna testiranja sve su manje iz aspekta „moramo napraviti", već su iz aspekta „želimo napraviti".

Nažalost, povremeno se kod organizacija bez uspostavljenog procesa upravljanja informacijskom sigurnošću sigurnosna testiranja počinju provoditi nakon sigurnosnih incidenata, no ubrzo postaju dijelom redovite prakse.

Predviđanje povećanja provjere statičke analize izvornog koda pokazala se preuranjenom, no s druge strane postoji pozitivan pomak prilikom integracije *CI/CD pipeline-a* te sve veće prisutnosti *container* servisa kod organizacija, gdje smo revizijom konfiguracija, provedenim testiranjima te sugestijama u skladu s najboljim praksama pomogli pri dodatnom očvršćivanju takvih rješenja.

U prosincu 2021. godine javno je objavljen kod za iskorištavanje ranjivosti u Log4j dodatku, koji je izrazito rasprostranjen i integriran u raznim rješenjima. U tim kaotičnim trenutcima primijećen je pozitivan pomak u spremnosti organizacija za pravovremenu reakciju na potencijalne ugroze. Vjerujemo da smo Vam u tim trenutcima pomogli, što provođenjem izvanrednih testiranja što razvojem dodatnih alata za otkrivanje navedene ranjivosti (https://github.com/Diverto/nse-log4shell).

2.2. Predviđanje kretanja testiranja sigurnosti za 2022. godinu

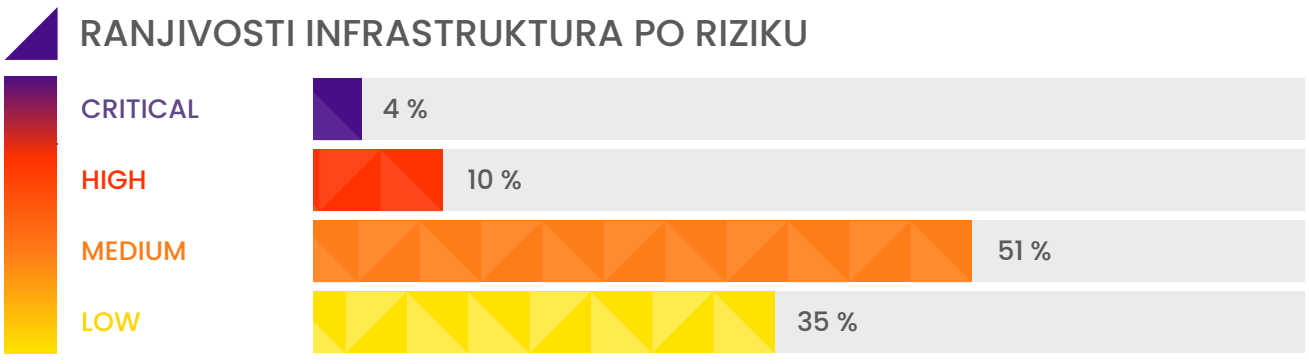
- Sigurnosni timovi u organizacijama će i dalje rasti
- Organizacije će sve više samostalno provoditi redovita skeniranja ranjivosti putem automatiziranih alata
- Očekuje se daljnje povećanje broja penetracijskih testiranja te daljnji rast *Red* i *Purple teaming* vježbi.

2.3. Sigurnosna testiranja na infrastrukturnoj razini

Od „standardnih" ranjivosti na infrastrukturama izdvojili bismo nedostatak upravljanja zakrpama za softver trećih strana, čiji udio daleko premašuje sve ostale tipove ranjivosti, kao i tijekom prethodnih godina. Također, u manjem broju se popravljaju ranjivosti koje nije bilo moguće iskoristiti, već je primaran fokus na otklanjanju onih ranjivosti koje su iskorištene tijekom sigurnosnih testiranja.

Poznata i istrošena fraza da je lanac jak koliko i njegova najslabija karika i dalje dobiva na težini upravo kod penetracijskih testiranja infrastruktura, gdje izloženi servis prema Internetu koji ima jednostavnu lozinku, nedostatak kritične zakrpe za softver ili ranjiva web aplikacija omogućava preuzimanje kontrole nad poslužiteljem, a nerijetko i nad cjelokupnom infrastrukturom.

Prilagodbom na udaljeni pristup rada korisnicima se morao omogućiti alternativni pristup aplikacijama i servisima kojima se inače koriste, ali su takve promjene otvorile i nove vektore napada te su se konfiguracijske pogreške uvedene takvim promjenama uspješno iskorištavale. Korištenje bežičnih pristupnih točaka bez prethodne provjere njihove autentičnosti, uz slabe lozinke, omogućilo je iskorištavanje takvih konfiguracijskih propusta, što je rezultiralo ostvarivanjem pristupa do unutarnjeg dijela infrastrukture te osjetljivih informacija.



SLIKA 6 *Ranjivosti infrastruktura po riziku. [Izvor: Diverto]*

Kontinuiranim osvještavanjem o značaju informacijske sigurnosti prepoznata je potreba za naprednijim sigurnosnim testiranjima, bržem uklanjanju ranjivosti te pravovremenim reakcijama na nove rizike koje se svakodnevno pronalaze. Purple teaming vježbe, ispitivanja sigurnosti lanca opskrbe te testiranja aplikacija prije puštanja u produkciju postaju dio redovitog procesa upravljanja sigurnošću organizacija.

Ivan Račić, *voditelj ofenzivnog tima*

Izdvojene ranjivosti koje su omogućile preuzimanje kontrola nad dijelom ili cjelokupnom infrastrukturom:

- Slabe i inicijalno zadane lozinke
- Servisni računi s visokim privilegijama i slabim lozinkama
- Grupne politike s minimalnom duljinom lozinki od osam znakova
- Nedostatak segregacije prava ili njena neadekvatna primjena
- Stariji operacijski sustavi bez adekvatnih zakrpi i dodatnih zaštitnih mehanizama
- Javno dostupne sigurnosne pohrane baza podataka s kriptografskim sažetcima lozinki
- *SQL* i *command injection* ranjivosti na aplikacijama dostupnim s Interneta
- Dostupni repozitoriji koda, poput *Subversion-a* i *GIT-a* te servisi za pohranu podataka koji ne zahtijevaju autentifikaciju.

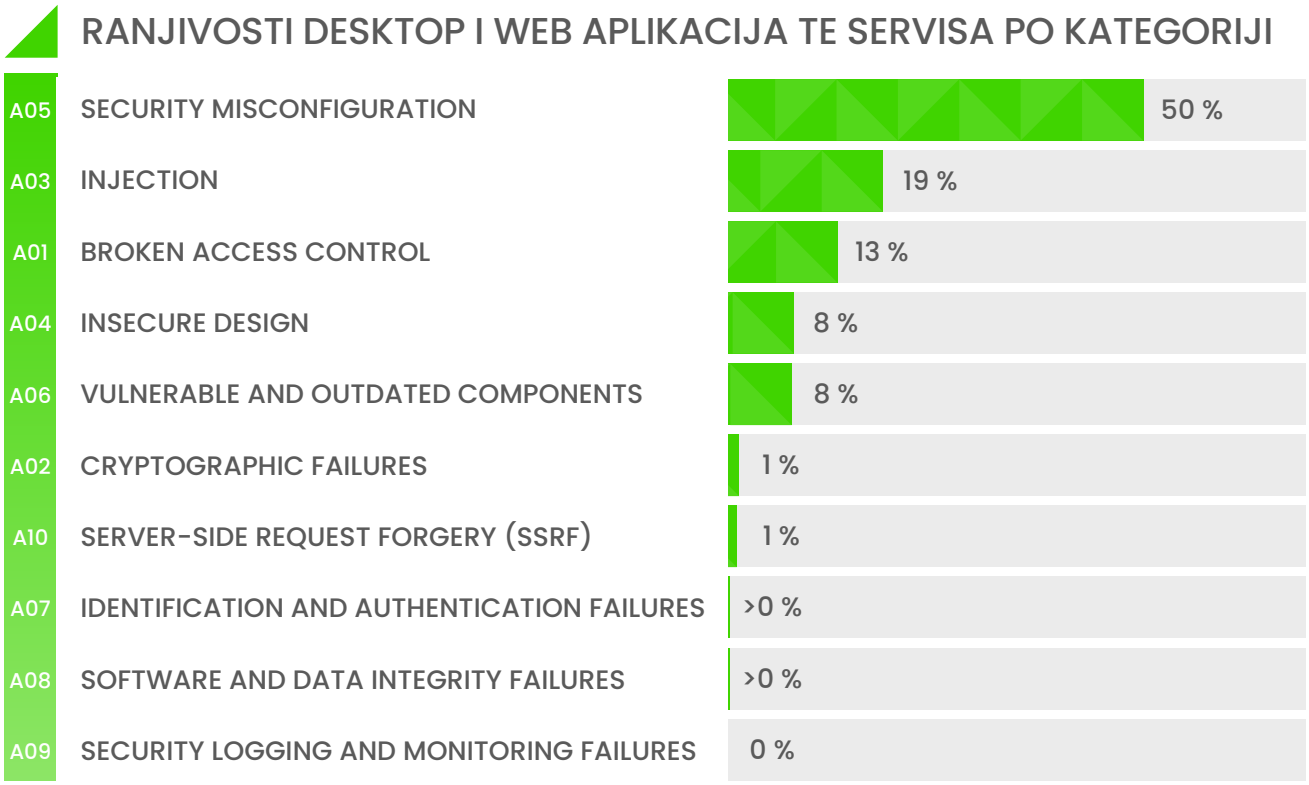
2.4. Sigurnosna testiranja web-servisa, desktop i web aplikacija

Uz uobičajene ranjivosti, gdje se prilikom konfiguracije poslužitelja na razini web-servisa ne upotrebljavaju dodatna sigurnosna HTTP zaglavlja i atributi kolačića, zatim upotreba slabijih kriptografskih algoritama i protokola te ranjivih softverskih komponenti, ranjivosti koje su imale najveći utjecaj na sigurnost aplikacija omogućile su:

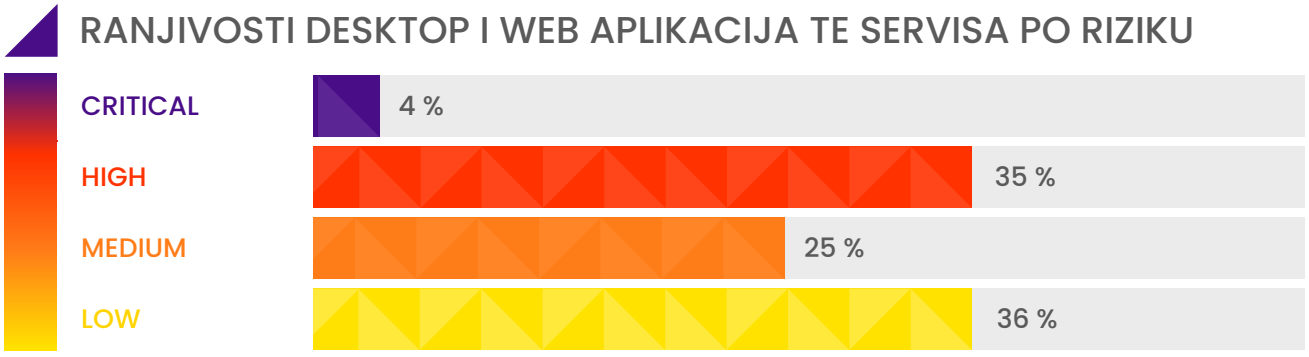
- umetanje proizvoljnog *JavaScript*, *SQL* koda te sistemskih naredbi
- krađa korisničkih sjednica

- izvršavanje dodatnog koda u kontekstu pretraživača
- pristup do baze podataka
- pristup do operacijskog sustava.

- zaobilaženje horizontalne, vertikalne te kontekstualne kontrole pristupa
  - pristup do povjerljivih informacija tuđih korisničkih računa s i bez prethodne autentifikacije
  - izvršavanje administrativnih funkcija iskorištavanjem ranjivosti u procesu autorizacije.



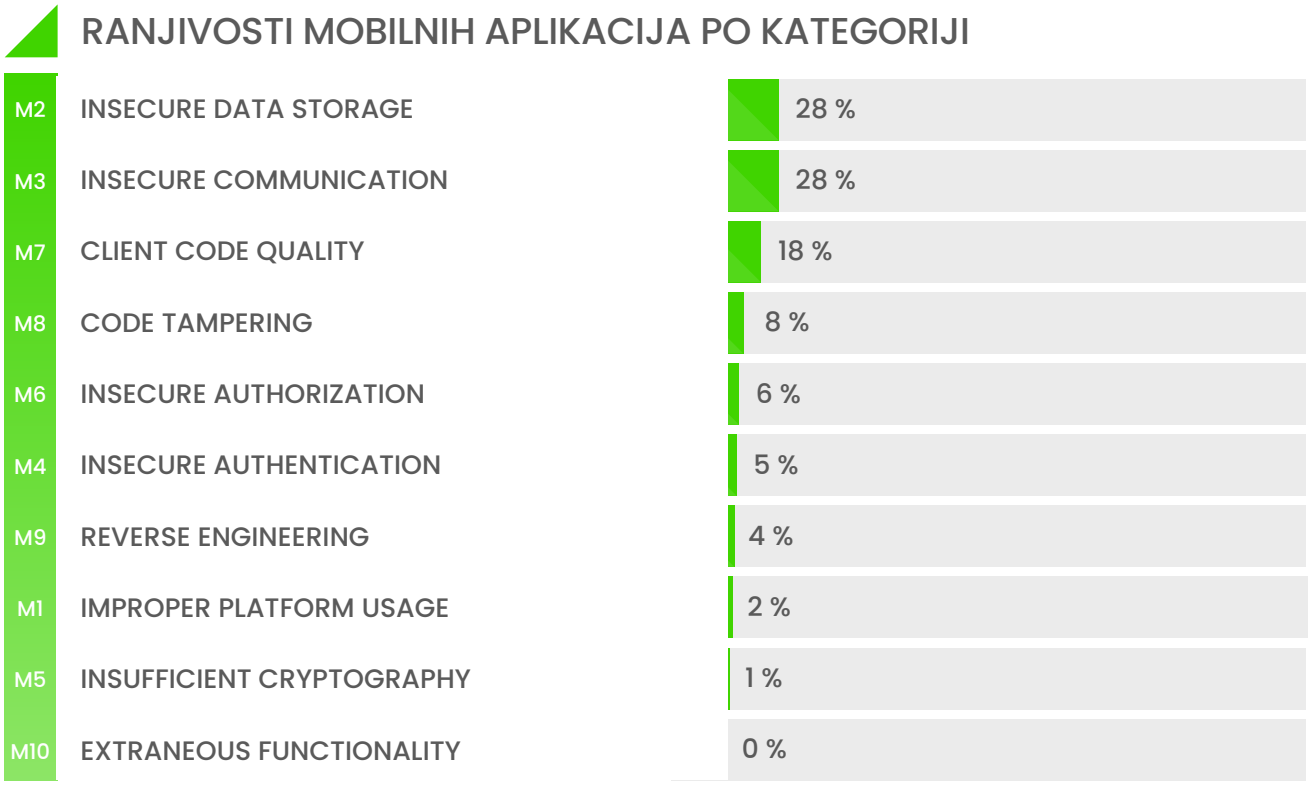
SLIKA 7 *Ranjivosti desktop i web aplikacija te servisa po kategoriji. [Izvor: Diverto]*



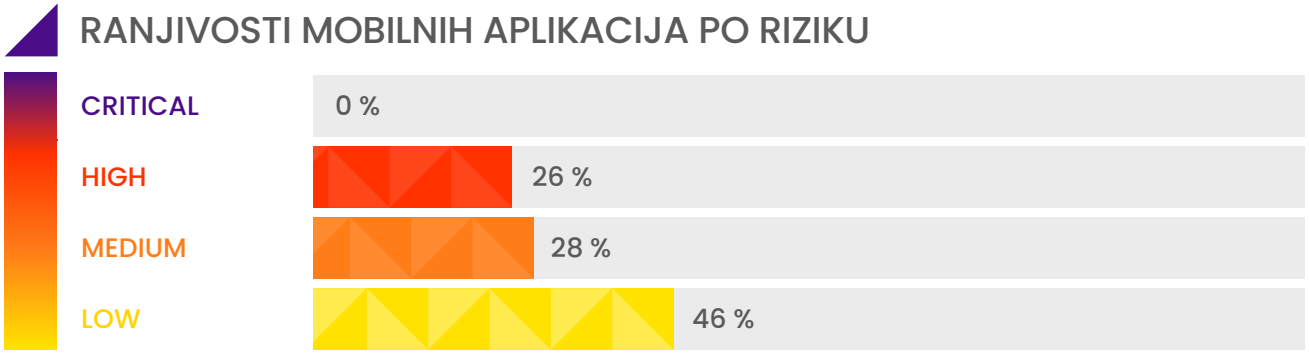
SLIKA 8 *Ranjivosti desktop i web aplikacija te servisa po riziku. [Izvor: Diverto]*

2.5. Mobilne aplikacije

Sigurna pohrana osjetljivih informacija, poput autentifikacijskih tokena i ostalih povjerljivih informacija, vrlo je bitna kod mobilnih aplikacija. Iako se osjetljive informacije moraju pohranjivati na samim mobilnim uređajima, preporučuje se upotrebljavati enkripcijske mehanizme samog mobilnog operacijskog sustava za sigurnu pohranu takvih podataka. Korištenje zaštitnih mehanizama poput *root/jailbreak* detekcije i *SSL pinning-a* svakako su poželjne dodatne sigurnosne kontrole, no u većini slučajeva nije potrebno dugo vremensko razdoblje kako bi se isti zaobišli. Najučestalije ranjivosti mobilnih aplikacija bile su:



SLIKA 9 *Ranjivosti mobilnih aplikacija po kategoriji. [Izvor: Diverto]*



SLIKA 10 *Ranjivosti mobilnih aplikacija po riziku. [Izvor: Diverto]*

diverto

Obrambena perspektiva

3. OBRAMBENA PERSPEKTIVA

Obrambena perspektiva daje uvid u spremnost određene organizacije za prevenciju incidenata informacijske sigurnosti. To je ujedno i najzastupljenija perspektiva te nažalost i jedina perspektiva koju organizacije u Hrvatskoj uzimaju kao relevantnu.

3.1. Tehnički pokazatelji u promatranom razdoblju

- porast uspješno preuzete e-mail komunikacije (engl. *Business email compromise - BEC*)
- nakon inicijalne kompromitacije sustava, napadači su spremni ostati prikriveni duže vremensko razdoblje, tj. sve dok se ne otvori prilika za što uspješniji napad
- veliki porast sigurnosnih propusta u raznim javno dostupnim servisima, mrežnim uređajima i aplikacijama. Organizacije često nemaju informaciju koju svu imovinu i softver imaju u sustavu
- kod *Ransomware* napada, napadači paralelno s ucjenom za otključavanje dokumenata traže i plaćanje otkupnine za neobjavljivanje dokumenata koji su ukradeni prije samog šifriranja sustava
- iako većina organizacija ulaže u sigurnosne tehnologije novije generacije, primijećeno je kako se alarmi koji ti sustavi generiraju ne nadziru aktivno. Prilikom istraga značajnih incidenata često je uočeno da su postojali alarmi iz rane faze napada na koje nije reagirano, a mogli su omogućiti organizaciji da spriječi napad prije nego što je on imao značajan utjecaj na sustav ili podatke.

U 2021. godini elektronska pošta je i dalje značajna ulazna točka napadača u mrežu, a ransomware je glavna briga velikih i malih organizacija. Sve više napora se ulaže i u upravljanje rizikom napada na lanac opskrbe koji mogu indirektno negativno utjecati na organizacije.

Ivan Ivković, *voditelj obrambenog i SOC tima*

3.2. Pozitivni pomaci

- odluku o cjelovitom pristupu informacijskoj sigurnosti uvođenjem sigurnosno-operativnog centra (SOC) više ne donose samo velike organizacije, već i one koje su karakteriziraju kao manje i srednje (SMB)
- sve više organizacija implementira tehnologije koje se bave zaštitom i upravljanjem privilegiranim računima
- svjesnost o važnosti uvođenja SOC-a kao holističkog rješenja koje povezuje IT/OT/IoT proširuje se iz sektora energetike i proizvodnje u druge sektore kao što su transport, kemijska industrija, opskrba vodom, gospodarenje otpadom
- povećava se broj organizacija koje primjenjuju i dobre prakse aktivnog praćenja sigurnosnih događaja, za razliku od dosadašnjeg reaktivnog pristupa.

3.3. Preporuke za pripremljenost za obranu od najčešćih vektora kibernetičkih napada

- za obranu od napada preuzimanja e-mail komunikacije uz implementaciju tehničkih rješenja zaštite (npr. *MFA*, digitalni potpisi, *SPF/DKIM/DMARC* zapisi, nadzor *forwarding* pravila), potrebna je i edukacija krajnjih korisnika na temu *Phishing* napada te implementacija poslovnih procesa kao što su sekundarna odobrenja za sva veća plaćanja ili telefonske potvrde zahtjeva za prijenos sredstava
- aktivno upravljati popisom informacijske imovine i svim softverom koji se upotrebljavaju unutar IT sustava. Razviti program kontinuirane procjene i upravljanja ranjivostima za svu imovinu i softver unutar infrastrukture organizacije kako bi se sanirale prilike za napadače i svele na minimalnu razinu. Jedan od primjera iz prakse je da se nakon svakog redovnog termina za instalaciju zakrpa provedu interna skeniranja sustava „*vulnerability management*“ alatom kako bi se potvrdilo da su ranjivosti otklonjene
- implementacija „*cold*“ ili „*offline*“ sigurnosnih kopija (*backup*). Ova vrsta kopija može biti ključna za oporavak IT sustava u slučaju *Ransomware* napada. Izvedba *offline* kopija se može bazirati na trakama, NAS sustavu koji nije stalno spojen na mrežu, *cloud* pohrani podataka, namjenskim uređajima s funkcionalnošću „*Retention Lock*“ (RL). *Offline backup* mora sadržavati najvažnije poslovne sustave i podatke koji su identificirani kroz procjenu rizika i analizu utjecaja na poslovanje
- implementacija „Information rights management“ sustava koji će zaštititi podatke koji slučajno ili krađom izađu izvan IT sustava organizacije
- osim prikladnog bilježenja dnevničkih zapisa i njihovog prikupljanja u centralni sustav, potrebno je vršiti aktivni nadzor svih sigurnosnih događaja
- imati unaprijed razrađene procese i propisane procedure u slučaju incidenta.

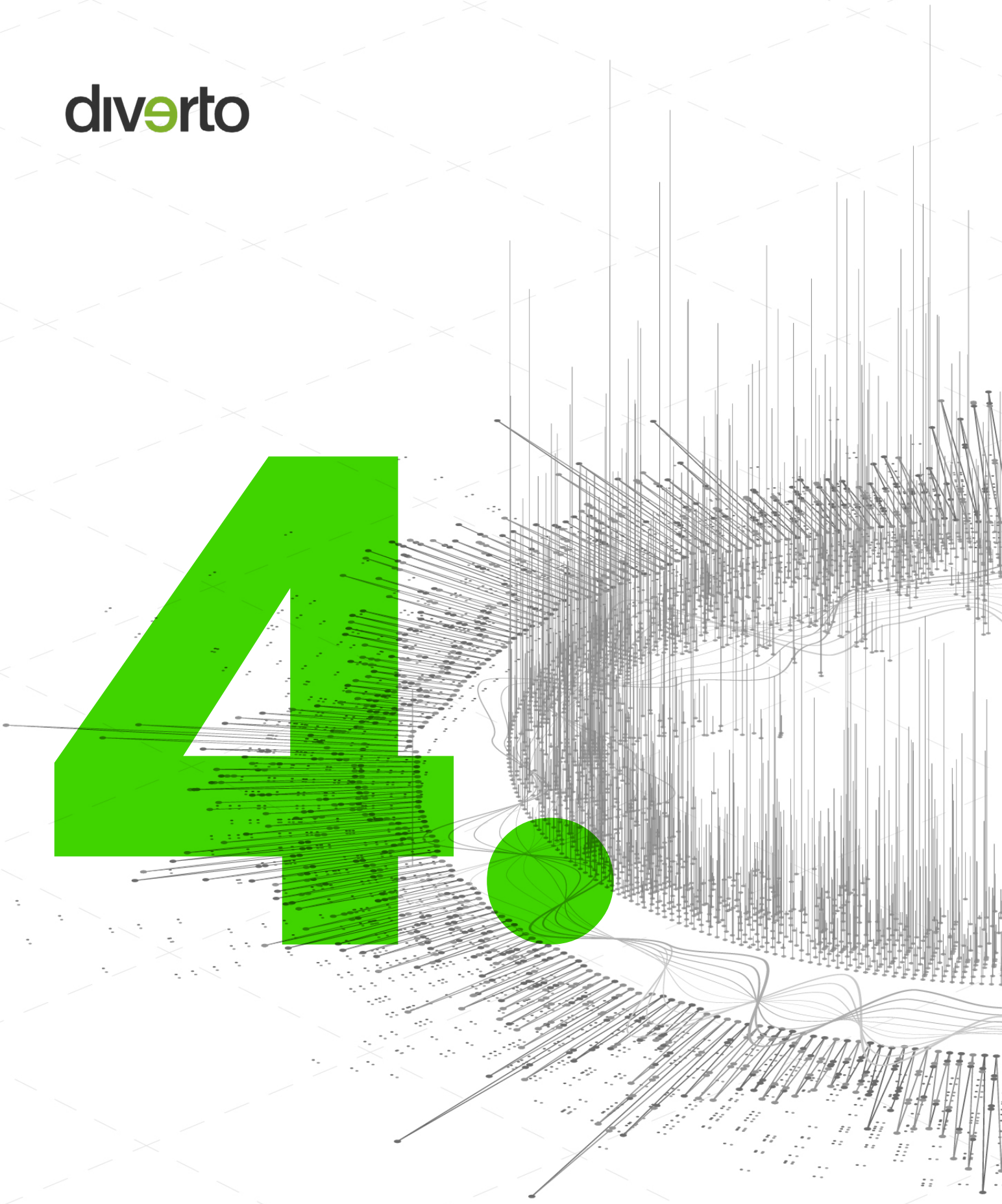
3.4. Zlonamjerni kod

Ransomware je i dalje dominantan tip zlonamjernog koda koji napadači koriste u svrhu stjecanja financijskih sredstava. Većina incidenata u 2021. godini koji su uključivali zlonamjerni kod u Republici Hrvatskoj, a obradio ih je Diverto, sadržavali su upravo kod za zaključavanje i šifriranje datoteka.

Zabilježili smo i brojne napade u kojima se napadači koriste naizgled legitimnim softverom za ugradnju zlonamjernog koda. Tako je, primjerice, softver za uređivanje PDF datoteka ili obradu i reprodukciju glazbenih zapisa i neke druge namjene predstavljen kao „besplatan" na lažnim stranicama nepostojeće tvrtke. Najčešće se u takvim situacijama radi o zlonamjernom kodu koji prikuplja korisničke parametre za spajanje na različite servise - *Keylogger.*

U nekoliko obrađenih uzoraka koji su upotrijebljeni u dobro pripremljenim napadima na tvrtke u Hrvatskoj uočene su mnogobrojne, pa čak i jednostavne tehnike ubacivanja koda u postojeće legitimne aplikacije operacijskog sustava Windows. Suvremena i ažurirana antivirusna zaštita u pojedinim situacijama nije bila u mogućnosti detektirati zlonamjerni kod. To samo ukazuje da „tradicionalni" zaštitni mehanizmi poput antivirusa i dalje nisu dovoljni te je potrebno učiniti korak dalje i ići k naprednijim rješenjima za radne stanice.

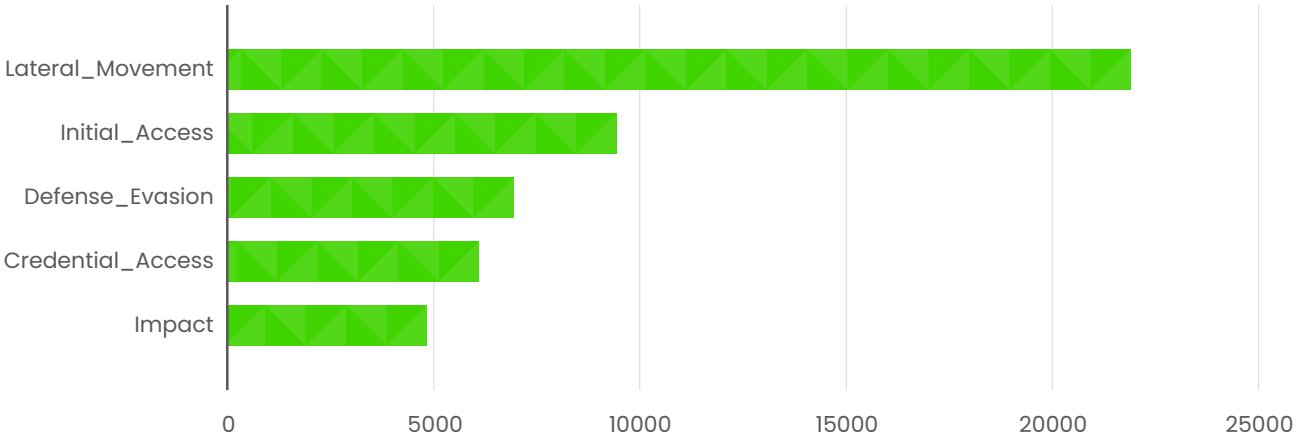
diverto



Incidenti

4. INCIDENTI

Spoznaje do kojih smo došli kroz Diverto SOC u 2021. godini dijelimo kako bismo podignuli svjesnost o tome da se incidenti događaju svakodnevno te da se mogu dogoditi bilo kojoj organizaciji, bez obzira na veličinu i sektor. Unutar Diverto SOC-a pratimo alarme sukladno MITRE Att&ck taktikama te smo izdvojili one najčešće.

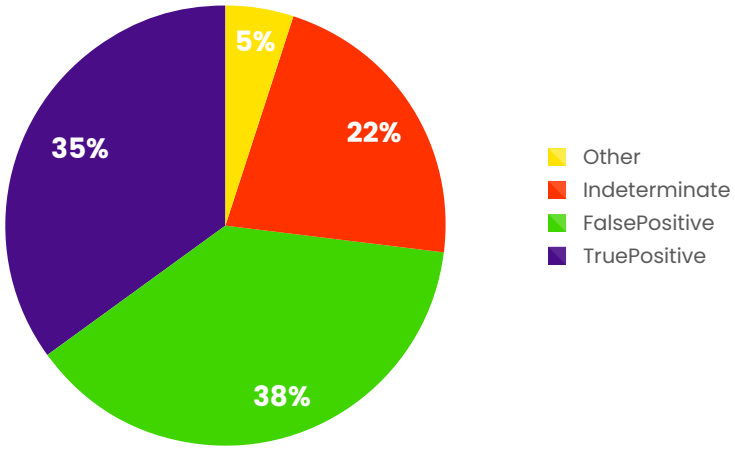


SLIKA 11 *TOP 5 najčešćih alarma prema MITRE Att&ck taktikama u 2021. godini* [Izvor: Diverto SOC]*

**temeljeno na preko 69 000 obrađenih alarma i preko 1000 istraga Diverto SOC tima u 2021. godini*

Prateći 2021. godinu, možemo sažeto iznijeti kako je unutar Diverto SOC-a 35 % svih istraga bilo okarakterizirano kao stvarni incidenti, dok je 38 % istraga bilo lažno pozitivnih. Dakako, ostatak su neodređene istrage za koje se nije moglo odrediti jesu li stvarni incidenti ili lažno pozitivni zbog nedostatka dokaza. Za nas je ovaj postotak neodređenih istraga bio prilika za unapređenje prikupljanja i filtriranja događaja kako bi takvih istraga bilo što manje.

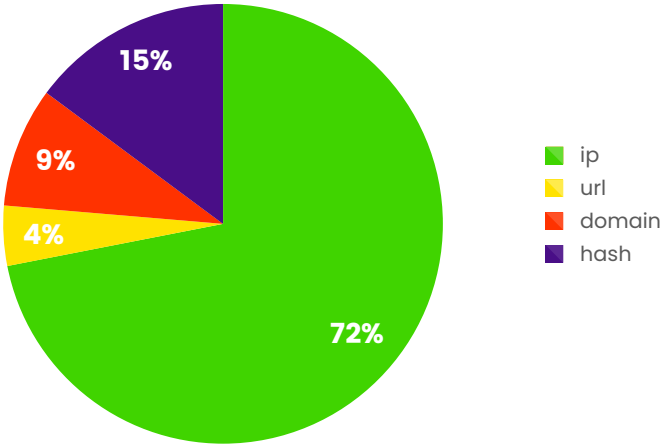
Pregled istraga u 2021. godini



SLIKA 12 *Pregled istraga u 2021. godini [Izvor: Diverto SOC]*

Naša baza prikupljenih indikatora znatno je povećana kroz redovne analize, *phishing* poruke, zlonamjerne datoteke i incidente. Ručno smo analizirali mnogobrojne nove zlonamjerne datoteke, među njima i *Conti, Egregor, LimeRAT* i druge.

Prikaz prikupljenih indikatora po vrsti u 2021. godini



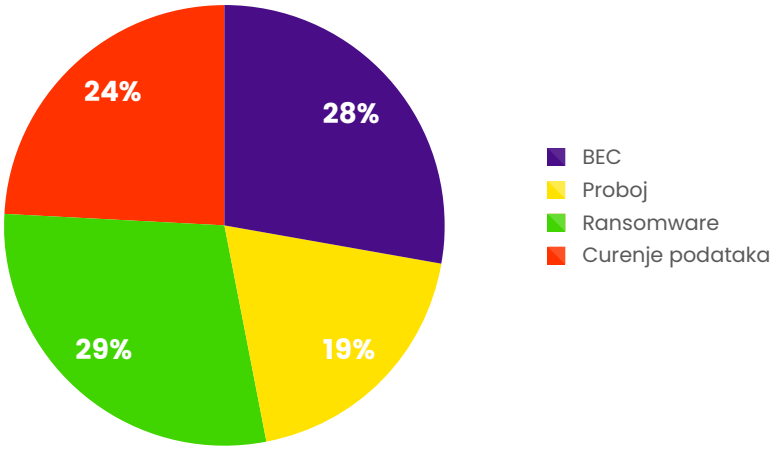
SLIKA 13 *Prikaz prikupljenih indikatora po vrsti [Izvor: Diverto SOC]*

4.1. Značajni incidenti

Kako se moglo i očekivati, 2021. godinu obilježio je porast broja značajnih incidenata koji su imali veliki utjecaj na povjerljivost, integritet i dostupnost korisnikova sustava ili podataka. Naš tim bio je prisutan u rješavanju više desetaka takvih incidenata.

Godinu 2021. pamtit ćemo po velikom rastu incidenata koji su se praktički izjednačili s brojem *ransomware* incidenata. Krađa podataka i dalje je pri vrhu posljedica napada, dok smo vidjeli i značajan porast proboja u korisničke sustave korištenjem ranjivosti za koje nisu pravovremeno implementirane sigurnosne zakrpe proizvođača.

Značajni incidenti



SLIKA 14 *Raspodjela incidenata po kategoriji [Izvor: Diverto SOC]*

Kada govorimo o napadima preuzimanja e-mail komunikacije, svjedočili smo trendu napadača da su nakon inicijalne kompromitacije pristupnih podataka spremni ostati prikriveni duže vremensko razdoblje, tj. sve dok se ne otvori prilika za što uspješniji napad. Kada se ta prilika ukaže, (npr. kompromitirani korisnik ode na godišnji odmor) napadač krene kontrolirati komunikaciju koristeći podatke prikupljene *OSINT* metodama, a preko pravila sandučića elektronske pošte prikriva svoje tragove.

Kod proboja u sustav od strane vanjskih napadača iskorišteni su sigurnosni propusti javno dostupnih servisa, a najčešće se radilo o ranjivostima *Exchange Server mail* sustava, tj. *„ProxyLogon"* i posljedično *„ProxyShell"*. Ovi napadi potvrđuju važnost pravovremene implementacije i validacije sigurnosnih ažuriranja sustava, pogotovo ako je riječ o sustavima koji su javno dostupni.

Iako je broj značajnih incidenata u 2021. godini u Hrvatskoj porastao, većina organizacija koje su bile žrtve napada nisu izlazile u javnost s informacijama o incidentima.

diverto

Phishing

5. PHISHING

U 2021. godini nastavili su se trendovi kojima smo svjedočili u 2020. godini. Pandemija i rad od kuće uvelike su oblikovali svakodnevne poslovne aktivnosti i procese, a zlonamjerni akteri su, kao i do sada, znali nove okolnosti iskoristiti u napadima.

Na globalnoj razini, **broj napada koji se koriste *phishing* porukama** kao početnim mjestom ulaza **ove godine je u porastu za 12 %**[5] u odnosu na prethodnu 2020. godinu.

Uzmemo li u razmatranje relevantne podatke za **Republiku Hrvatsku**, primjećujemo **porast broja prijavljenih računalnih prijevara za 20 %**. Razliku u odnosu na globalne trendove nije lako jednoznačno odrediti, ali neke od razloga možemo pronaći u povećanju svijesti o važnosti informacijske sigurnosti te sve više govora o napadima ovog tipa.

Naši podaci, dobiveni temeljem istraživanja otpornosti zaposlenika organizacija javnog i privatnog sektora na zlonamjerne phishing napade, pokazuju kako prosječno **21 % primatelja nije prepoznalo lažne poruke elektroničke pošte**. Promjena je pozitivna u odnosu na prošlogodišnjih 27 %, no još uvijek je preblizu globalnom pragu **trećine**[6] zaposlenika koji prilikom prvog testiranja nisu prepoznali lažne poruke elektroničke pošte.

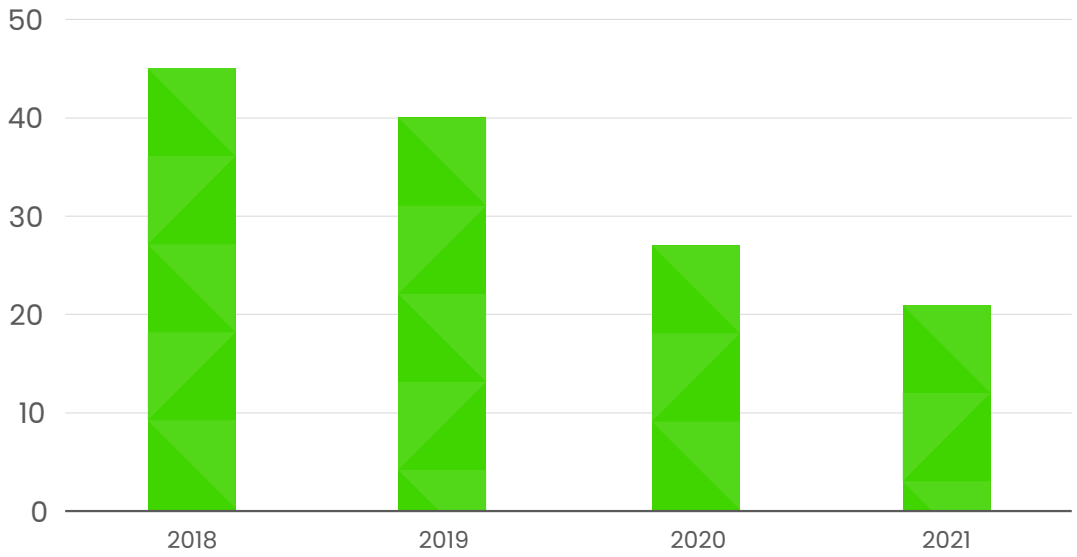
Međutim, u postotak od 27 % primatelja koji nisu prepoznali lažne poruke elektroničke pošte poslane u sklopu testiranja koje smo provodili u 2021. godini ulaze podaci iz kampanja **različitih težina prepoznavanja**. Promotrimo li raspodjelu rezultata prema težini prepoznavanja poruke, jasno se pokazalo kako **postotak prepoznavanja ovisi o složenosti kampanje**. Naime, što je više vremena utrošeno u pripremu kampanje i što je više truda uloženo u prikupljanje javno dostupnih podataka na temelju kojih se sastavljaju usmjerene poruke, to je snažniji rast postotka primatelja koji nisu prepoznali lažne poruke elektroničke pošte. Uzmemo li u obzir globalne trendove koji ukazuju na povećani rast upravo takvih poruka u odnosu na standardne phishing poruke, dolazimo do zaključka kako je potrebno **prilagoditi edukacijske programe** te ih **usmjeriti prema prepoznavanju složenijih *phishing* poruka**.

Iako je trend pada prisutan, daleko je od idealnog i, naposljetku, prihvatljivog. Kao i do sada, najbolja zaštita od napada metodama socijalnog inženjeringa, koje uključuju i phishing poruke, je **kontinuirana, sustavna i aktivna edukacija** koja se prilagođava trendovima i korisniku omogućava da samostalno proaktivno prikuplja informacije, pravovremeno prepozna i primjereno prijavi *phishing* poruke.

[5] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[6] https://www.knowbe4.com/hubfs/2021-Phishing-by-Industry-Benchmarking-Report.pdf?hsCtaTracking=5545cbd3-4d37-4ec2-a812-0b2830feefbb%7C753ae012-a008-46ca-ade5-5035e74f6667

Postotak primatelja koji nisu prepoznali Phishing poruku

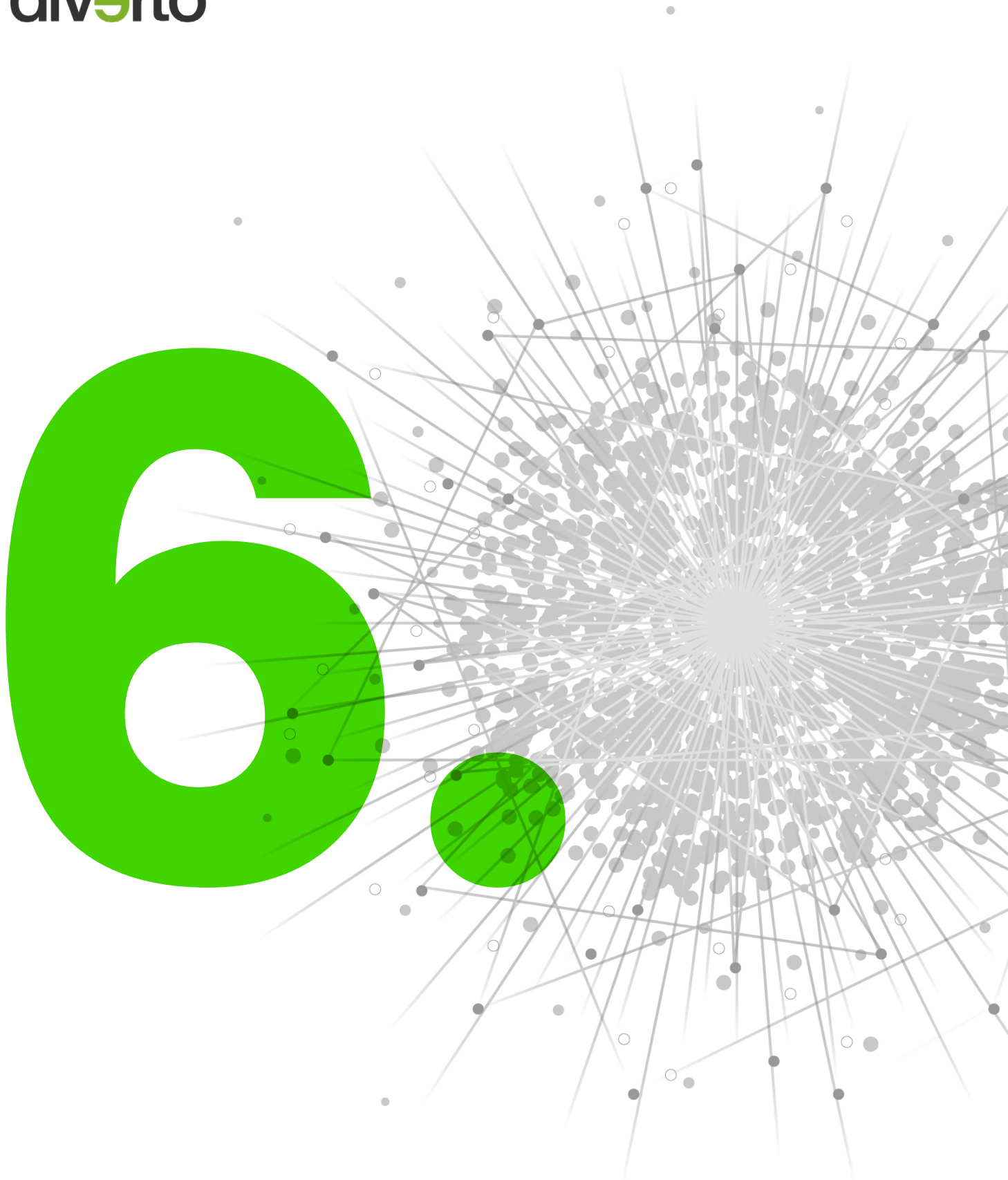


SLIKA 15 *Postotak primatelja koji nisu prepoznali Phishing poruku [Izvor: Diverto]*

Godina	Postotak primatelja	Broj poslanih poruka	
2018	45	1096	
2019	40	2206	
2020	27	2740	
2021	21	7062	
		13104	**Ukupno poslanih poruka**

TABLICA 1 *Postotak primatelja koji nisu prepoznali Phishing poruku u odnosu na broj poslanih poruka [Izvor: Diverto]*

diverto



6.

OT trendovi

6. OT TRENDOVI

Specijalizirani IT sustavi koji upravljaju i nadziru razne proizvodne procese u raznim industrijama (poznatiji kao ICS - industrijski kontrolni sustavi, procesni sustavi ili OT sustavi) kroz svoju povijest bili su fizički izdvojeni i odvojeni od ostalih IT sustava.

Kibernetička sigurnost OT sustava počivala je na *„air-gap"* načelima i ovisila je isključivo o nadzoru fizičke sigurnosti i mogućnosti fizičkog pristupa do računala i uređaja koji podržavaju/omogućavaju nadzor i upravljanje. Održavanje takvih sustava bilo je izdvojeno od održavanja tradicionalnih IT sustava koji su podržavali uredsko poslovanje i poslove poput računovodstva, naplate i upravljanja klijentima.

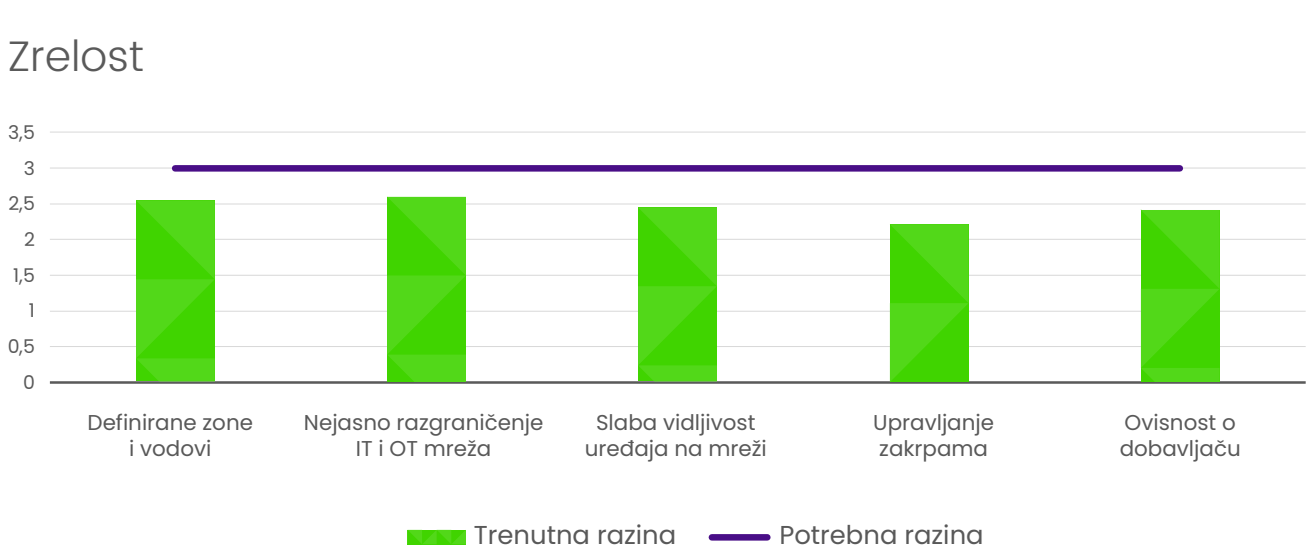
Zbog tradicionalne razdvojenosti i međusobnog „nerazumijevanja" principa rada IT i OT sustava i tehnologija, implementacije novih tehnologija u postojeće „stare" sustave bez razmatrana aspekata kibernetičke sigurnosti, kao i kroničnog nedostatka radne snage koja razumije problematiku OT sustava, izgradnja sigurnih i pouzdanih sustava otpornih na kibernetičke napade je izazov za svakog operatora OT sustava.

Današnje poslovanje u procesnoj i proizvodnoj industriji sve češće traži povezivanje postojećih OT sustava prema vanjskim mrežama poput prethodno spomenutih poslovnih IT sustava i prema Internetu. Razlozi povezivanja variraju od prikupljanja podataka za unos u sustave planiranja proizvodnje te sustave naplate i obračuna, udaljenog nadzora i pregleda nad odvijanjem dijela ili svih procesa, pa sve do potpune mogućnosti udaljenog upravljanja fizičkim procesima preko udaljene veze do SCADA i DCS sustava. Često ta povezivanja nisu popraćena prikladnim sigurnosnim mjerama i nije uzeto u obzir da većina postojećih OT sustava nije primarno dizajnirana kako bi bila zaštićena od modernih kibernetičkih napada, nego je dizajnirana tako da omogućava neometano te sigurno odvijanje procesa za ljude i okoliš.

Stoga današnji OT sustavi postaju sve dostupnija i zanimljivija meta *cyber* napadačima. Ako uzmemo u obzir da kritične infrastrukture država sve više ovise o nekom obliku OT sustava, isti postaju od posebnog značaja za svaku modernu državu. Kroz angažmane za neke od naših klijenata, koji su ujedno i operatori ključnih OT sustava i stupanjem na snagu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, intenzivno smo se angažirali i unijeli u problematiku kibernetičke sigurnosti takvih sustava te vam u nastavku navodimo područja u kojima operatori moraju kontinuirano podizati svoju razinu zrelosti.

Danas nije dovoljno imati fizičku odvojenu OT mrežu, već treba raditi na očvršćavanju kroz slojeve s obzirom na posljedice u fizičkom svijetu i utjecaj na širok lanac dionika. Najveća prepreka provođenju tih aktivnosti je nedostatak radne snage na području kibernetičke sigurnosti.

Mario Blažević, *voditelj OT usluga*



SLIKA 16 *Razina zrelosti područja kod operatora, zrelost bazirana na modificiranom CMM modelu [Izvor: Diverto]*

6.1. Potreba za definiranjem komunikacijsko-upravljačkih sigurnosnih zona i vodova i razgraničenjem IT i OT mreža

Kao što je ranijeobjašnjeno, većina operatora vjeruje da su im OT sustavi razdvojeni od ostalih IT sustava i interneta *„air-gapom"* i da do takvih sustava nije moguće doći preko konvencionalnih komunikacijskih kanala. Takvo vjerovanje je potencirano tvrdnjama dobavljača/trećih strana koji održavaju OT opremu. Međutim, jako malo operatora i dobavljača provodi testiranja mogućnosti proboja iz poslovne IT mreže u OT mrežu. Prilikom provođenja procjena i testiranja nailazili smo na formalne barijere (npr.: vatrozidi) između pojedinih sigurnosnih zona u obliku koji često nije imao dovoljno dobro definiran set pravila te je bilo moguće širenje iz zone u zonu. Dodatno, tokovi podataka između zona, a posebno između OT i IT sustava najčešće nisu dokumentirani niti održavani. Problem sigurnosnih zona potencira i fizička sigurnost pojedine lokacije koja počiva na perimetarskim zaštitama poput ograda, čuvara, video nadzora i sličnih preventivnih, odvraćajućih i detektivnih mjera. Potencijalni zlonamjerni napadač, jednom kada prođe perimetarske mjere zaštite, može relativno lako se širiti unutarnjim perimetrom i utjecati na imovinu koja često nije adekvatno zaštićena.

Preporučamo implementaciju mrežne segmentacije korištenjem *PERA* modela.

6.2. Potreba za vidljivosti uređaja i događaja na ethernetu

Većina postojećih OT sustava sadrži uređaje koji mogu biti stari i preko 20 godina. Iz IT perspektive, u kojoj su periodi zanavljanja IT opreme izuzetno brzi (svakih 3 do 5 godina), takvi uređaji zbog zastarjelosti ili specifičnih komunikacijskih protokola često ne mogu biti prepoznati/registrirani na mreži pomoću konvencionalnih IT sustava za upravljanje imovinom. Operatori OT sustava jako dobro znaju iz aspekta proizvođača i namjene opreme OT sustava s kojom imovinom raspolažu, ali najčešće nisu svjesni ranjivosti takvih sustava. Dodatno, mogućnosti registriranja promjene konfiguracije na OT uređaju su eventualno reaktivne, uvidom u sam uređaj nakon nekontroliranog ponovnog pokretanja uređaja. Nekontrolirano mijenjanje konfiguracije na uređajima i upravljačkim sustavima predstavlja iznimno visok rizik za svakog operatora OT sustava. Događaji koji bi indicirali zlonamjerne aktivnosti na OT mreži najčešće nisu vidljivi jer ne postoje sustavi koji bi bilježili takve događaje i eventualno upozoravali na zlonamjerne aktivnosti. Kao što smo naveli na početku, sustavi su predviđeni za pouzdan rad, ali bez razmišljanja o kibernetičkoj sigurnosti.

Preporučujemo upotrebu Specijaliziranih *asset management* sustava i implementaciju SOC-a za OT.

6.3. Potreba za upravljanje zakrpama

Upravljanje zakrpama u IT sustavima je jednostavno i poprilično pravolinijsko. Izađe nova zakrpa, IT odjel je eventualno testira te nakon toga primjeni zakrpu i sustav je zakrpan bez puno utjecaja na poslovanje. Primjena zakrpa u procesnim sustavima koji osiguravaju proizvodnju ili opskrbu energentima, opskrbu vodom za piće ili proizvodne procese koji ne smiju prestati je izuzetno zahtjevna i u većini situacija se ne odradi zbog toga jer proces ne smije stati, a u trenutcima kada proces stane, primjena zakrpa je nešto što ima najmanji prioritet jer je prioritet da se proces nastavi odvijati u što kraćem roku. Kao rezultat svega navedenoga, većina nezakrpanih ranjivosti OT sustava, ukoliko ne postoji *air-gap*, mogu biti iskorištene od potencijalnih zlonamjernih aktera.

Preporučujemo uspostaviti proces i dodijeliti odgovornosti za provođenje procesa upravljanja zakrpama, uspostaviti proces testiranja ranjivosti te definirati izvore iz kojih prikupljate informacije o ranjivostima sustava.

6.4. Sve veća ovisnost operatera o dobavljačima

Većina OT sustava su visokospecijalizirani sustavi koji upravljaju specifičnim procesima u specifičnim industrijama. Takve sustave i elemente tih sustava tradicionalno razvijaju specijalizirane tvrtke s dugogodišnjim prisustvom na tržištu i zrelim partnerskim odnosima s operatorima. Odnosi s operatorima temelje se na povjerenju i dugogodišnjoj suradnji, ali kad se uzme u obzir činjenica da se sve više sustava umrežava i povezuje te da je na tržištu sve manje raspoložive radne snage na području OT tehnologija, postavlja se pitanje u kojem trenutku dobavljači više neće moći ispunjavati svoje obaveze ili će iste biti ozbiljno degradirane.

Preporučujemo uspostaviti procese upravljanja kibernetičkom sigurnošću dobavljača koji su bazirani na procjeni rizika dobavljača i rizika opskrbnog lanca. Sve situacije koje mogu rezultirati neprihvatljivim rizikom poželjno je adresirati već pri ugovaranju kroz jasno definiranje ugovornih obaveza i očekivane razine usluge. Dodatno, rizike dobavljača i opskrbnog lanca moguće je umanjiti korištenjem pristupa za dokumentiranje ugrađenih komponenti sustava (npr. *Software bill of materials*).

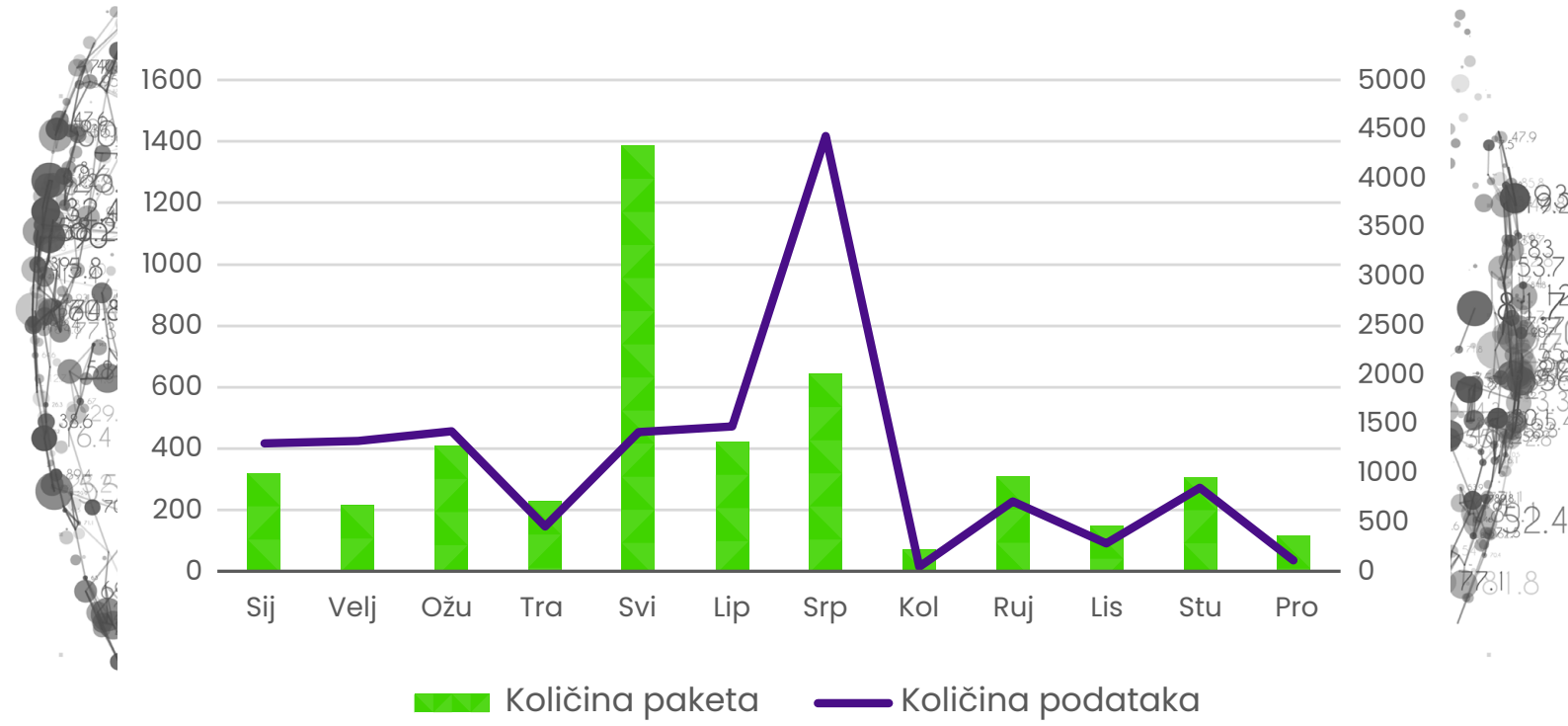
diverto

Distribuirani napadi uskraćivanjem usluge (DDoS)

7. DISTRIBUIRANI NAPADI USKRAĆIVANJEM USLUGE (DDOS)

Distribuirani napad uskraćivanja usluge je jedan od najjednostavnijih i najosnovnijih, ali i dalje najučestalijih napada u internetskom prostoru. U Hrvatskom internetskom prostoru takvi su napadi također učestali te nema određenog perioda kada takvi napadi nisu izraženi. Donosimo vam više detalja o DDoS napadima tijekom 2020 u Hrvatskoj.

DDoS napadači postaju efikasniji i efektivniji u 2021. godini. U odnosu na 2020. Godinu, broj napada se znatno smanjio. Međutim, pojedinačni napadi su postali veći u pogledu količine paketa i podataka te se produžilo i samo trajanje. U 2021. godini su podjednako zastupljeni napadi putem TCP i UDP protokola.



SLIKA 17 *DDoS napadi po mjesecima u 2021. godini [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, te aplikacije dovedu u normalni režim rada. Pogotovo u slučaju kada sustav zaštite i sam sustav nije adekvatno implementiran i dimenzioniran.

NAJVEĆI NAPAD PO BROJU PAKETA JE 617,6 MILIJARDI PAKETA I TRAJAO JE 1824 MINUTE.

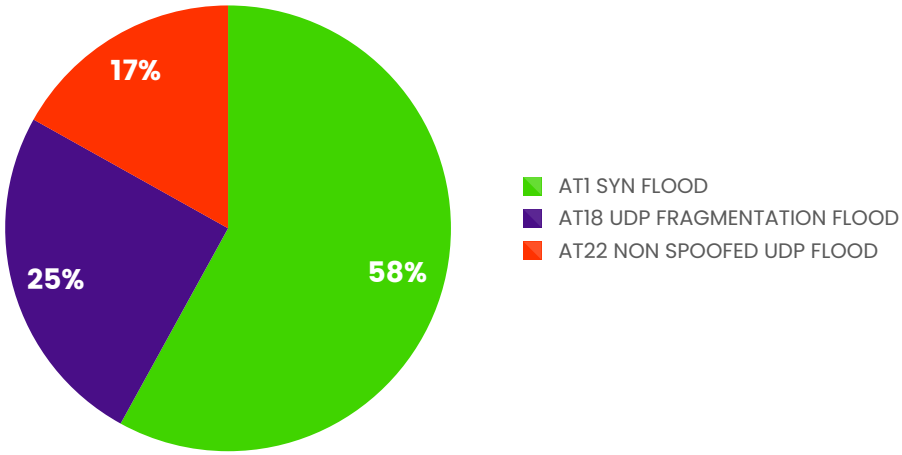
Tip napada	Broj paketa	Trajanje u min.
AT1 SYN FLOOD	70.0 Mpkts	2379
AT18 UDP FRAGMENTATION FLOOD	469.6 Mpkts	937
AT1 SYN FLOOD	51.3 Mpkts	712
AT1 SYN FLOOD	36.0 Mpkts	623
AT1 SYN FLOOD	24.8 Mpkts	993
AT22 NON SPOOFED UDP FLOOD	126.0 Mpkts	442
AT22 NON SPOOFED UDP FLOOD	155.4 Mpkts	1490
AT18 UDP FRAGMENTATION FLOOD	62.1 Mpkts	57880
AT1 SYN FLOOD	18.2 Mpkts	19380
AT18 UDP FRAGMENTATION FLOOD	21.5 Mpkts	18603

TABLICA 2 *Najveći napadi po omjeru količine paketa i trajanja u 2021. godini [Izvor: Diverto]*

TOP 5 DDoS tehnika po broju pristiglih paketa

1. AT1 SYN FLOOD
2. AT18 UDP FRAGMENTATION FLOOD
3. AT22 NON SPOOFED UDP FLOOD
4. AT3 ACK FLOOD
5. AT25 PING FLOO

Raspodjela najvećih napada po kategoriji



SLIKA 18 *Raspodjela najvećih napada po kategoriji [Izvor: Diverto]*

Tip napada	Količina podataka	Broj paketa	Trajanje u min.
AT18 UDP FRAGMENTATION FLOOD	3.9 Tbits	469.6 Mpkts	62
AT18 UDP FRAGMENTATION FLOOD	611.6 Gbits	62.1 Mpkts	14
AT18 UDP FRAGMENTATION FLOOD	155.0 Gbits	13.8 Mpkts	4
AT18 UDP FRAGMENTATION FLOOD	258.7 Gbits	24.1 Mpkts	7
AT18 UDP FRAGMENTATION FLOOD	236.9 Gbits	23.2 Mpkts	7
AT18 UDP FRAGMENTATION FLOOD	222.9 Gbits	21.9 Mpkts	7
AT18 UDP FRAGMENTATION FLOOD	108.8 Gbits	10.0 Mpkts	4
AT18 UDP FRAGMENTATION FLOOD	143.7 Gbits	21.5 Mpkts	6
AT18 UDP FRAGMENTATION FLOOD	246.0 Gbits	24.0 Mpkts	11
AT18 UDP FRAGMENTATION FLOOD	154.2 Gbits	16.2 Mpkts	7

TABLICA 3 *Najveći napadi po omjeru količine podataka i trajanja u 2021. godini [Izvor: Diverto]*

NAJVEĆI NAPAD PO KOLIČINI PODATAKA JE 3,9 TBIT I TRAJAO JE 62 MINUTE.

TOP 5 DDOS TEHNIKA PO KOLIČINI PODATAKA

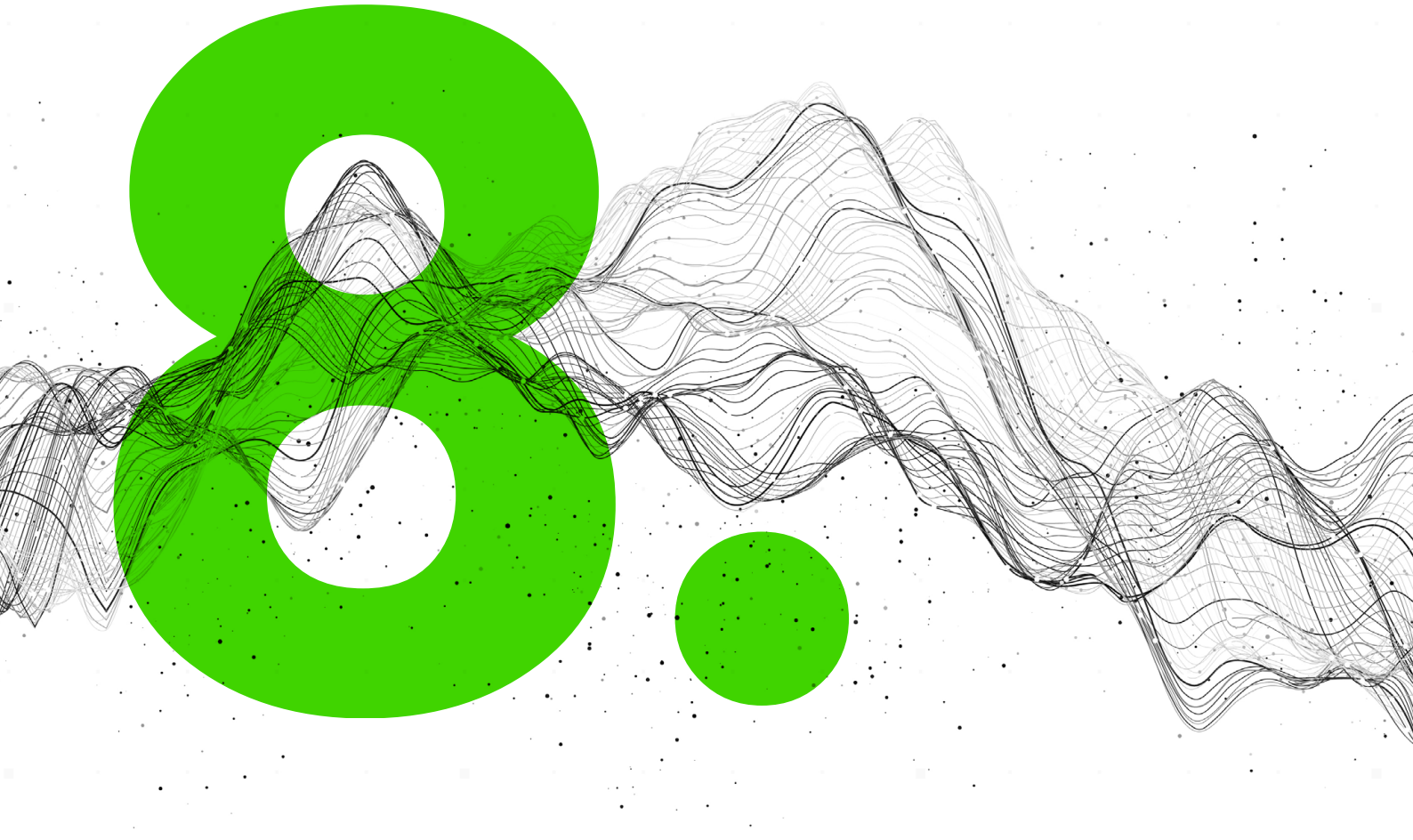
1. AT18 UDP FRAGMENTATION FLOOD
2. AT22 NON SPOOFED UDP FLOOD
3. AT3 ACK FLOOD
4. AT1 SYN FLOOD
5. AT62 INVALID PACKET FLOOD

I dalje je preporuka obratiti pažnju na točku spajanja udaljenih radnika, poput VPN koncentratora te kritične aplikacije izložene Internetu.

NAJDUŽI NAPAD TRAJAO JE PREKO 47 SATI (2872 MINUTE).

Analizirano na uzorku od ukupno 1155 napada koje su prepoznali uređaji za zaštitu od DDoS napada smješteni kod javnog i privatnog sektora u našoj zemlji. Analizirani napadi su preuzeti s uređaja koji mogu identificirati DDoS napade te ne uključuju nezaštićena odredišta i napade koji nisu prepoznati. Napadi su kategorizirani po taksonomiji DDoS napada tvrtke RioRey, raspoloživoj na sljedećoj poveznici:
https://www.riorey.com/types-of-ddos-attacks

diverto



Preporuke

8. PREPORUKE

LANAC OPSKRBE

Sve veća kompleksnost sustava u IT i OT svijetu te povećano korištenje trećih strana i *cloud* usluga povećava ovisnost organizacija o svom lancu opskrbe. Već neko vrijeme tema sigurnosti lanca opskrbe je česta tema u informacijskoj sigurnosti, a potvrdu o važnosti ova teme dobila je kroz razne incidente u Hrvatskoj i na globalnoj razini. Stoga preporučujemo uspostavu procesa upravljanja lanca opskrbe, poput sigurnosnih zahtjeva dobavljačima te provjere postupanja dobavljača, bilo da se radi o besplatnim komponentama u vašem aplikacijskom softveru ili upravljanjem vaše kompletne infrastrukture. Isto tako, ukoliko ste dobavljač drugima, preporuka je provjeriti i očvrsnuti svoj lanac opskrbe te vlastiti proizvod.

OT/PROCESNI SUSTAVI

OT i procesni sustavi zanimljivi su napadačima jer su vrlo često ranjiviji zbog ograničene mogućnosti redovite dogradnje i očvršćivanja te velikih posljedica koje kompromitacije mogu uzrokovati. Stoga je preporuka započeti s aktivnostima proaktivne zaštite i sigurnosnog nadzora takvih sustava. Uvijek je dobar početak napraviti snimku stanja i odrediti željeno stanje te korake kako doći do željenog stanja. Preporuka je posebnu pažnju obratiti na spojne točke između OT sustava i drugih sustava te definirane sigurnosne LAN zone unutar OT sustava. Čest je slučaj da se identificiraju dodatne spojne točke i nedostatak zaštite istih. Kako bilo kakav proces u ovakvim sustavima zna uzeti vremena, preporuka je krenuti bez odgađanja.

DEVSECOPS

Implementacijom *Continuos Delivery* i *Continuos Integration* alata u razvojni ciklus, isti je omogućio i provjeru sigurnosti zahtjeva uz uobičajeno funkcionalno testiranje. Sada je već moguće veliki broj sigurnosnih provjera napraviti automatski u samom razvoju. Svakako treba obratiti pozornost, budući da generički alati za kvalitetu koda obično ne provjeravaju sve potrebne sigurnosne zahtjeve i nisu dostatni za kvalitetnu provjeru sigurnosti. Naša preporuka je to napraviti specijaliziranim SAST, DAST i IAST alatima koji provjeravaju veći skup sigurnosnih kontrola i zahtjeva te su u mogućnosti prepoznati kompleksnije sintakse i pozive. Naravno, kombinirajte navedene alate s alatima za provjeru ranjivosti samih komponenti (SCA). Izrada softverskog popisa komponenti koji se ugrađuje u pojedini sustav ili aplikaciju postaje sve češće zahtjev i praksa (engl. *Software Bill of Materials* – SBOM).

RIZICI

Današnje vrijeme je zaista izazovno za bilo koje poslovno okruženje. Rizici se mijenjaju u kratkom vremenskom razdoblju, kao i mogućnosti rukovanja rizikom. Intenzivne seizmološke aktivnosti i COVID-19 samo su jedni od primjera zajedno s posljedicama koje nose. Izazov je postao znati svoje najveće rizike i upravljati samim rizicima. U prošlosti je to bilo moguće raditi ručno uz povremeno ažuriranje, ali sve bliže smo sve većoj automatizaciji ovog područja. Preporuka je svakako iskoristiti mogućnosti specijaliziranog softvera i olakšati proces upravljanja rizikom.

Diverto pruža visokospecijalizirani spektar usluga iz područja informacijske 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