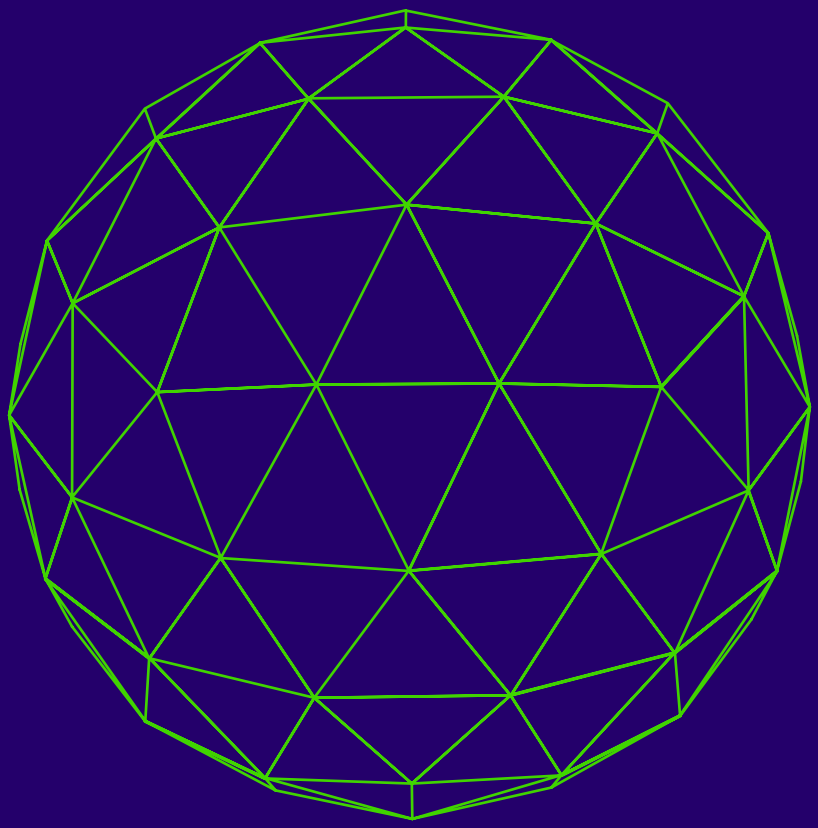
diverto



STANJE INFORMACIJSKE SIGURNOSTI 2020.

TRAVANJ 2021.

Poštovani,

Iza nas je neobična godina. Godina obilježena pandemijom i potresima na zagrebačkom i sisačkom području gdje su organizacije trebale aktivirati svoje planove za kontinuitet poslovanja. To je svakako dobar test za upravljanje kontinuitetom poslovanja i koliko je svaka organizacija spremna u kratkom vremenom odgovoriti na dva različita izazova.

Sve su veći regulatorni i ugovorni zahtjevi za područje informacijske sigurnosti. Posljedice nepridržavanja sve su teže. O tome govore kazne i skupi oporavak od samog incidenta. Potvrda navedenog jest i prva nepravomoćno izrečena GDPR kazna u Hrvatskoj. Jednostavno, svi su prepoznali da je informacija jedan od najvrjednijih resursa ovog doba u kojem živimo i da je treba adekvatno zaštiti.

Treba zaštiti i prilazne puteve informaciji kroz implementaciju sigurnosti lanca opskrbe. Kroz incident u kojem je u središtu bio Solarwinds, pokazalo se kako napadači sve više koriste indirektne puteve kako bi došli do vrijednog cilja. Potvrda je to napadačke upornosti i ustrajnosti.

Svakako bih izdvojio incidente koji su se dogodili kod velikih organizacija u hrvatskome digitalnom prostoru, a koje su same organizacije javno i priznale. Ovakvo izlaženje u javnost svakako treba pohvaliti jer incidenti su se događali i prije. No, priznavanje incidenata i komunikacija s javnosti i relevantnim tijelima su izostajali. Hrabar je to i dobar iskorak u pravom smjeru jer pomaže i u osvješćivanju javnosti kako se incidenti događaju i kako svatko može postati žrtvom.

Sve navedeno govori kako se rad na preventivnim aktivnostima pokazao korisnim te da i dalje treba raditi na njihovim poboljšanjima i ustrajati na uspostavljanju adekvatne sigurnosne razine.

Vjerujem kako će izvještaj pomoći upravo u tome jer daje pregled i trendove informacijske sigurnosti te dijelove na koje bi trebali obratiti pozornost u budućnosti kako bismo poboljšali vlastiti sustav sigurnosti.

Izvještaj je rezultat zajedničkog rada s našim korisnicima kojima ovim putem zahvaljujem. Rezultat je to rada i svih osoba i timova unutar Diverta, a iza svakog pokazatelja i iznesene brojke stoji vrlo detaljna priča i danonoćni rad. Ukratko, trudimo se izvještaj razvijati u smjeru da bude koristan i relevantan za sve koji se bave područjem informacijske sigurnosti.

Vlatko Košturjak
CTO

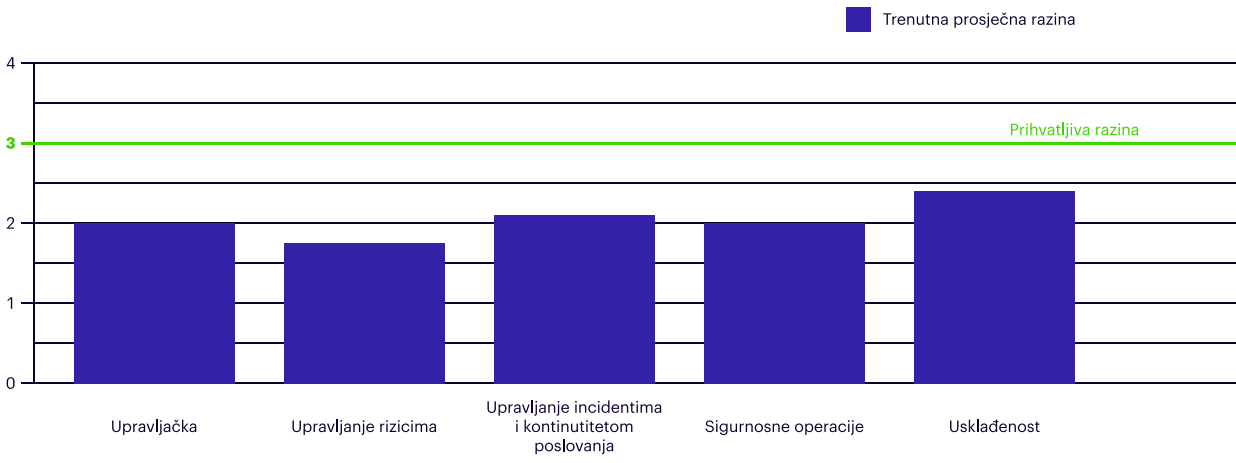
1 Pregled iz tri različite perspektive

1.1 Upravljačka perspektiva

Upravljačka perspektiva daje uvid u to koliko je pojedina organizacija odnosno njezino poslovodstvo svjesno utjecaja informacijske sigurnosti na poslovanje. Upravljačku razina odgovorna je prepoznati rizike koji ozbiljno mogu narušiti kontinuitet poslovanja i otpornost organizacije na sigurnosne prijetnje. S pomoću prikazanih pokazatelja, trendova i procjena kretanja u 2021. godini upravljačka razina može lakše prepoznati prijetnje i donijeti odluke kako zaštiti svoju najvrjedniju imovinu.

Ključni pokazatelji u promatranom razdoblju

- povećana izloženost kibernetičkim napadima kao posljedica rada od kuće
- informacijska sigurnost i dalje dominantno shvaćena kao IT sigurnost
- *phishing* je i dalje predominantan vektor uspješnih i „jeftinih“ napada na informacijsku sigurnost
- prelijevanja posljedica globalnih incidenata *(CitOday)* na područje naše zemlje
- sigurnost lanca opskrbe (najčešće samo na razini ugovornih odnosa i bez konkretnih mjera provjere sigurnosti)
- prva nepravomoćna izrečena GDPR kazna u Hrvatskoj
- *privacy shield* kao osnova prijenosa osobnih podataka u SAD više nije prihvatljiv *(Schrems II)*.



[Slika 1] Prosječna razina zrelosti područja informacijske sigurnosti [Izvor: Diverto]

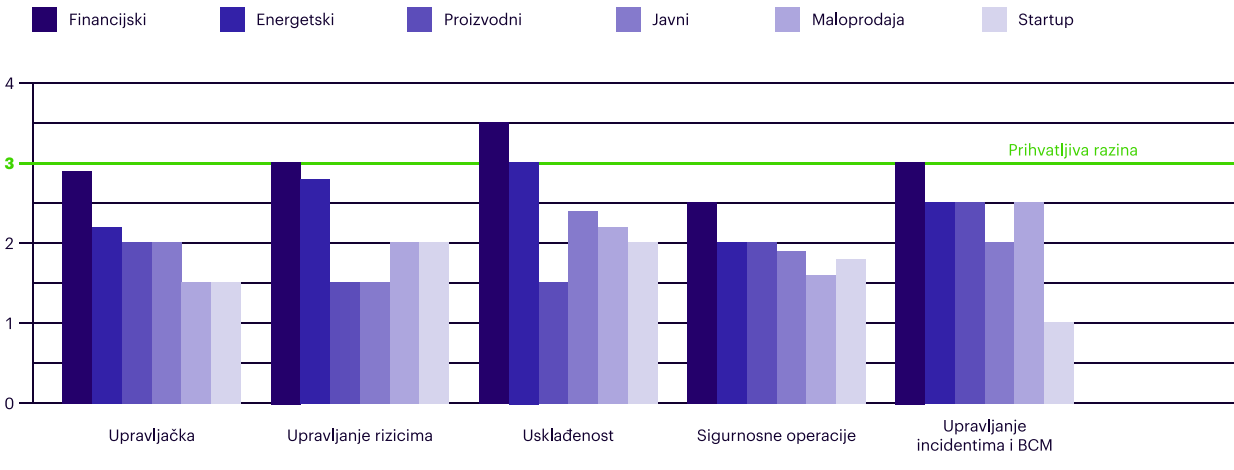
Pozitivni pomaci

U 2020. godini uočavamo pozitivne pomake u razvoju svijesti o važnosti informacijske sigurnosti za poslovanje pojedinih organizacija neovisno o sektoru u kome djeluju. Pravila dobre prakse najviše se prate u reguliranim sektorima kao što su financijski, energetski i telekomunikacijski sektor. Uvođenje NIS direktive pozitivno se odrazilo na svjesnost operatora ključnih usluga o važnosti informacijske sigurnosti koji su pokrenuli brojne projekte za unapređenje.

Identificirani pozitivni pokazatelji

- porast broja organizacija koje žele potvrdu informacijske sigurnosti postići sustavnim pristupom i certifikacijom prema međunarodno priznatim normama
- shvaćanje da su rizici informacijske sigurnosti rizici poslovanja i da ih ne mogu samostalno riješiti IT odjeli
- povećanje ulaganja u osvješćivanje i educiranje zaposlenika
- porast svijesti o potrebi jasne i transparentne komunikacije o incidentima informacijske i kibernetičke sigurnosti

Iako su vidljivi pozitivni pomaci, i dalje postoji 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. Uglavnom se temelje na „nišnom“ pristupu nabave automatiziranih rješenja bez prikladne implementacije i obuke operatera sustava, ali i svih zaposlenika. Ulaganja u informacijsku sigurnost nisu sveobuhvatna i najčešće se percipiraju kao nepotreban trošak kod kojeg ne postoji povrat investicije.



[Slika 2] Razine zrelosti područja informacijske sigurnosti po sektorima [Izvor: Diverto]

Procjena kretanja u 2021.

- nastavak rada od kuće, informacijska sigurnost kao *"business enabler"* u situacijama otežana poslovanja
- sigurnost lanca opskrbe postaje prioritetom u industrijama koje ovise o dobavljačima i trećim stranama
- napuštanje tradicionalnih načina upravljanja udaljenim pristupom organizacijskim resursima i uvođenje *„Zero trust* modela"
- uvježbani i testirani planovi oporavka i krizno komuniciranje kao osnovica osiguranja kontinuiteta poslovanja
- intenzivniji kibernetički napadi na operatore ključnih usluga i ključne infrastrukture
- sve učestalije primjenjivanje proaktivnih načela u informacijskoj sigurnosti korištenjem jedinstvene točke nadzora i upravljanja incidentima u organizacijama
- povećana potražnja za uslugama na području informacijske i kibernetičke sigurnosti
- ciljani *ransomware* napadi preko sofisticiranih *phishing* kampanja
- korištenje umjetne inteligencije i strojnog učenja za manipulaciju uvjerenjima, cijenama dionica...

Iako vrlo izazovna, prošla godina je stavila informacijsku sigurnost u fokus kao nikada prije. Regulatorne promjene poput ZOKS-a, potresi i pandemija, globalni računalni incidenti te ubrzana digitalizacija jasno su definirali poslovne rizike kao sigurnosne i pokazali potrebu za pozicioniranjem informacijske sigurnosti na razini poslovodstva. Cjeloviti razvoj i upravljanje informacijskom sigurnosti već danas predstavlja kompetitivnu prednost koju prepoznaju i klijenti većine organizacija.

Ivan Kalinić
voditelj strateškog razvoja sigurnosti

1.2 Napadačka perspektiva

Napadačka perspektiva daje pregled informacijske sigurnosti iz perspektive napadača. Kako bismo olakšali razumijevanje načina na koji napadači razmišljaju dajemo pregled koji je nastao našim iskustvom testiranja tijekom cijele 2020. godine.

Ključni pokazatelji

- problematično upravljanje nadogradnjama za softver trećih strana, odnosno onih paketa koji se ne održavaju izravno putem centraliziranih rješenja
- zakrpe se uglavnom primjenjuju samo na one ranjivosti pronađene unutar opsega penetracijskih testiranja bez primjene strateških preporuka na razini organizacije
- organizacije koje nemaju zadužene osobe ili odjele za informacijsku sigurnost u pravilu mnogo sporije implementiraju preporuke
- sigurnost aplikacija većim je brojem temeljena na dinamičkoj analizi uz nedostatak statičke analize izvornoga koda aplikacija

Ključni pokazatelji ukazuju nam na to da napadači i dalje mogu računati na to da organizacije nemaju redovite i sustavno provedene primjene politike zakrpa odnosno upravljanja nadogradnjama. Iako je provođenje sigurnosnih testiranja na zasebnim segmentima infrastrukture dobra praksa, i dalje nedostaje provođenje većeg broja naprednih testiranja koja bi testirala organizaciju kao cjelinu.

Pozitivni pomaci

- smanjuje se broj nepotrebno otvorenih mrežnih portova i servisa na vanjskim infrastrukturama
- povećan je broj implementacija sustava za upravljanje privilegiranim računima što dovodi do postupna smanjenja broja računa s administrativnim privilegijima nad cjelokupnom infrastrukturom
- nadogradnja na novije operacijske sustave u pozitivnom je trendu kao i implementacija sustava za nadzor nad infrastrukturama
- pomak u primjeni politika lozinki na one veće duljine i složenosti
- primjena operativnih preporuka za uklanjanje ranjivosti provodi se u kraćem vremenskom razdoblju
- povećan je broj organizacija koje provode testiranja sustava za udaljeni pristup te simulaciju napada trećih strana (*assume breach* scenariji)
- porast broja provođenja naprednih Red teaming testiranja

Procjena kretanja u 2021.

- sve više organizacija provodit će sigurnosna testiranja, od temeljnih skeniranja ranjivosti do naprednih penetracijskih testiranja
- uočen je i trend testiranja pristupa trećih strana kroz razne scenarije koji će se u sljedećim razdobljima još dodatno ojačati
- provjera statičke analize izvornoga koda uvodi se u redovan proces testiranja aplikacija i servisa

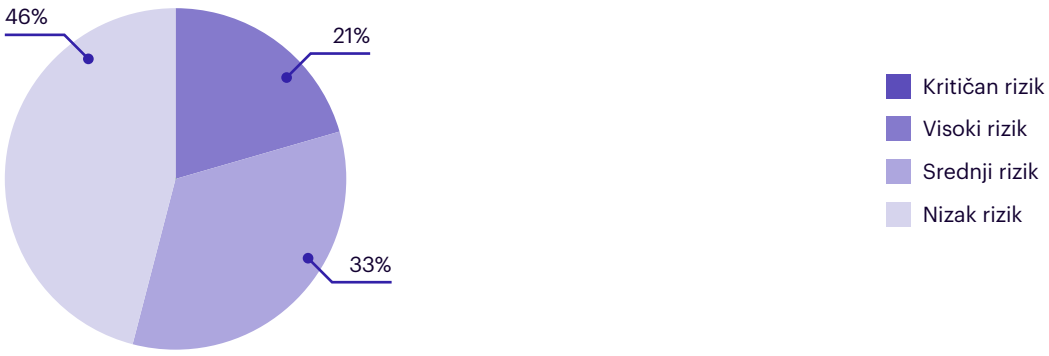
Pregled ranjivosti

U nastavku dajemo pregled najčešćih ranjivosti koje su pronađene tijekom testiranja koja smo proveli kroz cijelu 2020. godinu. Osim penetracijskih testiranja tu su i rezultati *Red teaming* testiranja koji su izdvojeni u posebnu cjelinu.

Najučestalije ranjivosti aplikacija i servisa*

- *Injection*
- *Broken access controls*
- *Cross-site Scripting*
- *Sensitive data exposure*
- *Cross-site Request Forgery*

* Temeljeno na *OWASP Top 10 Web Application Security Risks*



[Slika 3] Raspodjela identificiranih ranjivosti u aplikacijama i servisima po kritičnosti

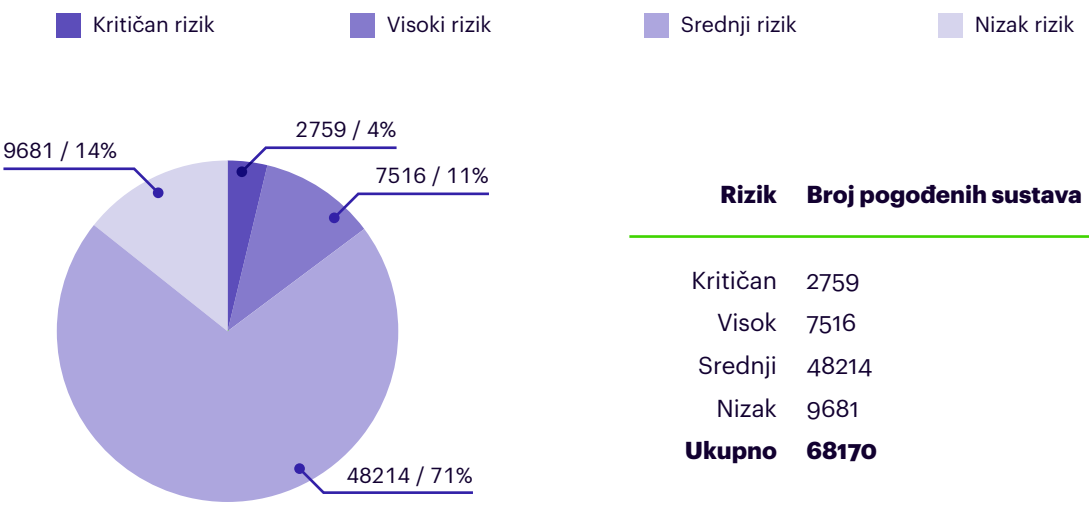
[Izvor: Diverto]

Najučestalije ranjivosti mobilnih aplikacija

- nedostatak *SSL Certificate pinning* mehanizma
- nedostatak mehanizma otkrivanja administrativnih ovlasti na mobilnim uređajima
- pohranjivanje osjetljivih informacija na uređajima
- neobfuscirane aplikacije (nemaskirani aplikacijski kod)
- otkrivanje API ključeva i detaljnih informacija o pozadinskim servisima

Najučestalije ranjivosti infrastruktura

- nedostatak zakrpa za operacijske sustave i popratni softver
- iskorištavanje funkcionalnosti *broadcast* i *multicast* protokola
- neadekvatne dozvole nad grupnim politikama *(Active Directory Group Policy),* dijeljenim mrežnim direktorijima i servisima za udaljeno upravljanje
- značajan broj korisničkih računa koji imaju pristup do administrativnih sučelja
- javno Izloženi Repozitoriji koda, administrativni portali i nadzorna sučelja
- inicijalno postavljene ili jednostavno pogodljive lozinke te njihova ponovna upotreba
- pohranjivanje privatnih ključeva, sigurnosnih kopija i lozinki u čistom tekstu na neadekvatno zaštićenim dijeljenim mrežnim mapama
- neadekvatan nadzor i filtriranje mrežnog prometa prema vanjskim mrežama
- korištenje protokola čistog teksta



Rizik	Broj pogođenih sustava
Kritičan	2759
Visok	7516
Srednji	48214
Nizak	9681
Ukupno	**68170**

[Slika 4] Raspodjela identificiranih ranjivosti na infrastrukturama po kritičnosti

[Izvor: Diverto]

Najučestalije ranjivosti IoT uređaja

- *command injection* ranjivosti
- loša obfuskacija lozinki
- korištenje slabih lozinki čije je kriptografske sažetke jednostavno probiti
- nezaštićen *bootloader*
- ugrađeni kredencijali za bežične pristupne točke sa slabim lozinkama

Zaključci nakon provedenih *Red teaming* testiranja

- neadekvatne kontrole fizičkog pristupa
- nedostatak sustava za videonadzor ili njegova neadekvatna primjena
- iako se treninzi za podizanje svijesti o sigurnosti provode, provedba naučenog u praksi se pokazala nedostatnom
- nedostatak višefaktorske autentikacije za vanjske servise
- neadekvatna zaštita i nedostatak nadzora nad bežičnim mrežama i servisima u oblaku
- nesrazmjeri u provedbi sigurnosnih politika između zaposlenika i vanjskih partnera
- neadekvatno podešeni sustavi za otkrivanje sigurnosnih incidenata
- jednom kada napadači zaobiđu perimetarske zaštite, ofenzivne aktivnosti napadača rjeđe se primijete, a sumnjive aktivnosti većinom se ne prijave obrambenim timovima
- unutar pretinaca elektroničke pošte nalazi se velik broj korisničkih vjerodajnica te ostalih povjerljivih informacija koje bi trebale biti dodatno zaštićene ili pohranjene na centraliziranim sustavima

Red i *Purple teaming* vježbama te analizom izvornog koda aplikacija pronalaze se one ranjivosti koje je teško otkriti zasebnim sigurnosnim testiranjima. Takva naprednija i sveobuhvatnija testiranja pokazala su se kao vrijedan korak u procesu podizanja organizacijske sigurnosti.

Ivan Račić
voditelj ofenzivnog tima

1.3 Obrambena perspektiva

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

Ključni pokazatelji u promatranom razdoblju

- upornost napadača raste i ne odustaju nakon višestrukih pokušaja
- napadi su fokusiraniji i sve više napada cilja točno određenu organizaciju
- najzastupljeniji zlonamjerni kod koji se uspješno izvrši na radnim stanicama jest *Purple Fox* i *Emotet*
- vidljiva su redovita mjesečna inkrementalna poboljšanja već znanoga zlonamjernog koda
- porast *ransomware* incidenta

Pozitivni pomaci

- sve više organizacija odlučuje se na cjeloviti pristup informacijskoj sigurnosti uvođenjem SOC-a, umjesto dosadašnjeg ulaganja u SIEM sustave, čime se unapređuje sigurnost aktivnim praćenjem sigurnosnih događaja. Uglavnom se radi o naprednim organizacijama koje su visoko podignule razinu informacijske sigurnosti
- manje organizacije, često pritisnute negativnim iskustvima, odlučuju se na vanjsku potporu uslugama dediciranog tima za odgovor na incidente s definiranim vremenom odgovora
- u energetskom sektoru, kao i u djelatnosti proizvodnje, shvaća se važnost uvođenja SOC-a kao holističkog rješenja koje povezuje IT/OT/IoT
- dio organizacija primjenjuje i dobre prakse aktivnog praćenja sigurnosnih događaja, za razliku od dosadašnjeg reaktivnog pristupa

Preporuke za ispravan odgovor na incidente

- imati unaprijed razrađene procese i raspisane procedure u slučaju incidenta
- imati ažuran popis informacijske imovine i tokova podataka
- imati prikladno bilježenje dnevničkih zapisa i njihovo prikupljanje na centralni sustav
- koristiti višefaktorsku autentikaciju minimalno na servisima izloženima prema internetu
- pravilno konfigurirati i optimizirati postojeće tehnologije
- ograničiti prava pristupa na potreban minimum
- pozvati stručnjake za odaziv na incident odmah po uočavanju incidenta

2020. godina donijela nam je velik broj incidenata što je potaklo organizacije da počnu više razmišljati o kontinuiranom nadzoru i o tome da se nije dovoljno osloniti samo na prevenciju. Fokus treba biti i na detekciji incidenta u ranim fazama.

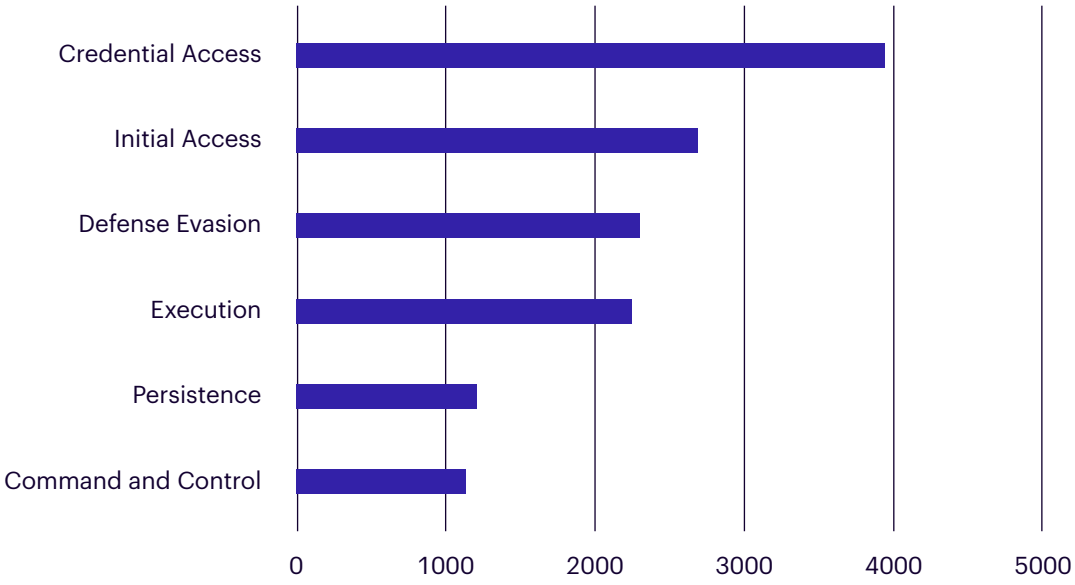
Vladimir Ožura
voditelj SOC-a

2 Stanje u Hrvatskoj

2.1 Incidenti

Spoznaje do kojih smo došli kroz Diverto SOC (Sigurnosni operativni centar) u 2020. 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.

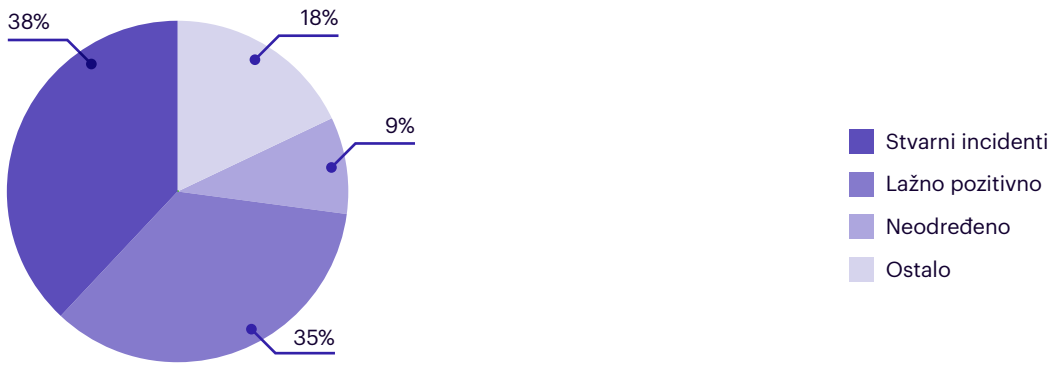
Unutar Diverto SOC-a pratimo alarme sukladno MITRE Att&ck taktikama te smo izdvojili one najčešće.



[Slika 5] Najčešći alarmi prema MITRE Att&ck taktikama u 2020. godini* [Izvor: Diverto SOC]

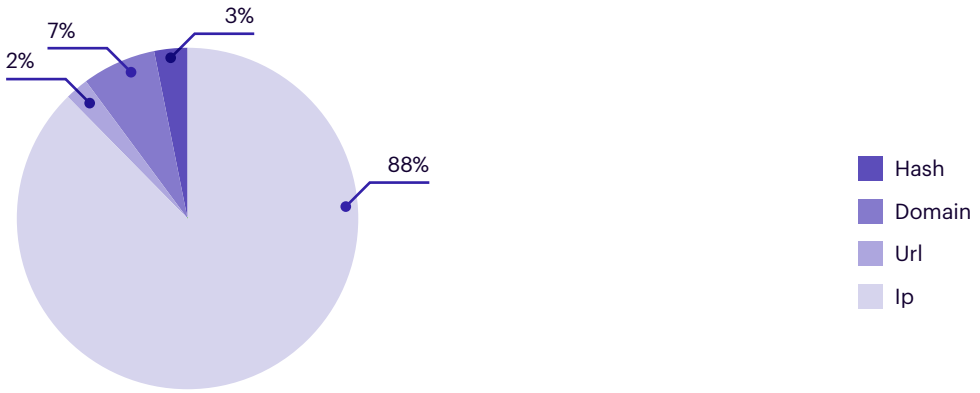
* temeljeno na preko 21 000 obrađenih alarma i preko 1000 istraga od Diverto SOC tima u 2020. godini

Prateći 2020. godinu možemo sumirati kako je unutar Diverto SOC-a 38 % svih istraga bilo okarakterizirano kao stvarni incidenti, dok je 35 % 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.



[Slika 6] Pregled istraga u 2020. godini [Izvor: Diverto SOC]

Naša baza prikupljenih indikatora znatno je povećana kroz redovne analize, *phishing* poruke, zlonamjerne datoteke i incidente. Ručno smo analizirali više od 300 zlonamjernih datoteka, među njima *Purple Fox, Emotet, AgentTesla i NanoCore*.



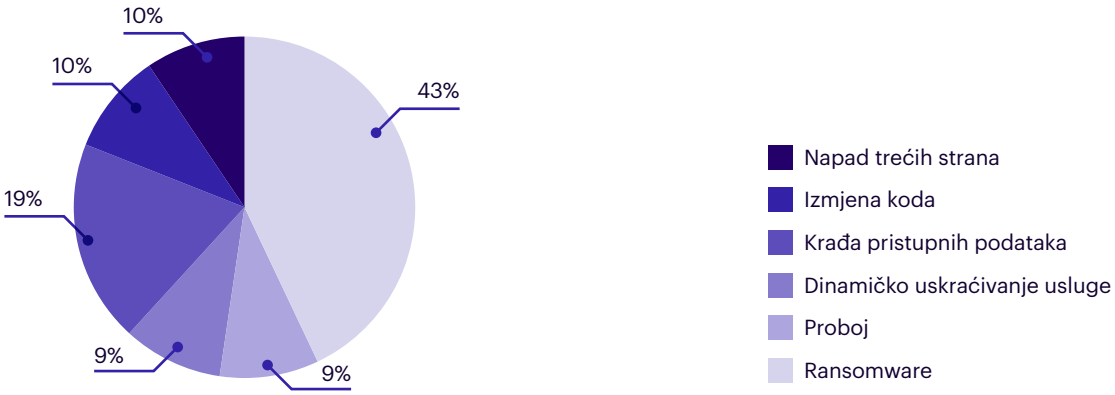
[Slika 7] Prikaz prikupljenih indikatora po vrsti [Izvor: Diverto SOC]

Incidenti van SOCa

Kako se moglo i očekivati 2020. godinu obilježio je veliki broj incidenata koje smo obradili za klijente koji ne koriste SOC usluge. Naš tim bio je prisutan u rješavanju više desetaka takvih incidenata što je u odnosu na prošlu godinu porast od čak 400 %.

Godinu 2020. pamtit ćemo po velikom broju *ransomware* incidenata, čak 43 % svih incidenata spadaju u tu kategoriju. Krađa pristupnih podataka i dalje je pri vrhu, dok smo viđali i incidente poput izmjene koda i napad trećih strana. Incidenti poput dinamičkog uskraćivanja usluge i proboja, iako u najmanjem postotku, nisu nimalo beznačajni.

Godina je završila incidentom koji smo klasificirali kao proboj, a uočen je korištenjem Diverto *Honeypota* u ranoj fazi napada . Da nije uočen na vrijeme pitanje je bi li incident završio samo probojem ili bi rezultirao ozbiljnijim posljedicama.



[Slika 7] Raspodjela incidenata po kategoriji [Izvor: Diverto SOC]

Nemoguće je spominjati incidente u 2020. godini bez nužnog osvrta na pandemiju koja nas je sve pogodila i to u kontekstu prelaska na rad od kuće. To je za sobom povuklo novi niz sigurnosnih problema koje su napadači itekako dobro iskoristili čemu u prilog govore i brojke incidenata kojima smo svjedočili.

Najbolji su primjeri toga *phishing* kampanje koje su napadači koristili kako bi socijalnim inženjeringom došli do pristupnih podataka. Novonastali vektori ulaska u interne mreže organizacija koji su se pojavili u pokušaju omogućavanja obavljanja radnih zadataka radnicima od kuće:

- izloženi RDP/SSH servisi prema internetu
- VPN pristup s jednostavnim lozinkama uz nedostatak višefaktorske autentikacije
- nedostatak korporativne zaštite izvan organizacije

Svjedoci smo vremena u kojem incidenti postaju svakodnevicom. Od javno poznatih informacija o incidentima u Hrvatskoj svakako treba spomenuti tri organizacije koje su javno priznale da su imale problema u 2020. godini, i to iz različitih industrija. INA, Overseas Express i Pevex hrabro su odlučile priznati napade i izići u javnost. Iako su incidenti okarakterizirani kao *ransomware,* organizacije su smetnje otklonile i uspješno se oporavile. Ovakvo izlaženje u javnost svakako treba pohvaliti i nadamo se da će postati trendom u budućnosti.

2.2 Phishing

Tijekom 2020. godine u suradnji s različitim organizacijama u našoj zemlji proveli smo istraživanje otpornosti zaposlenika organizacija javnog i privatnog sektora na zlonamjerne *phishing* napade. Cilj nam je bio utvrđivanje svijesti i spremnosti hrvatskih korisnika na obranu od takvih napada.

Rezultati pokazuju kako ukupno 27% primatelja nije prepoznalo lažne poruke elektroničke pošte, pri čemu su bile uključene poruke različite težine prepoznavanja. Prateći trendove, iz ovog postotka vidljiv je pozitivan pomak u razini svijesti radnika u odnosu na prethodne godine.

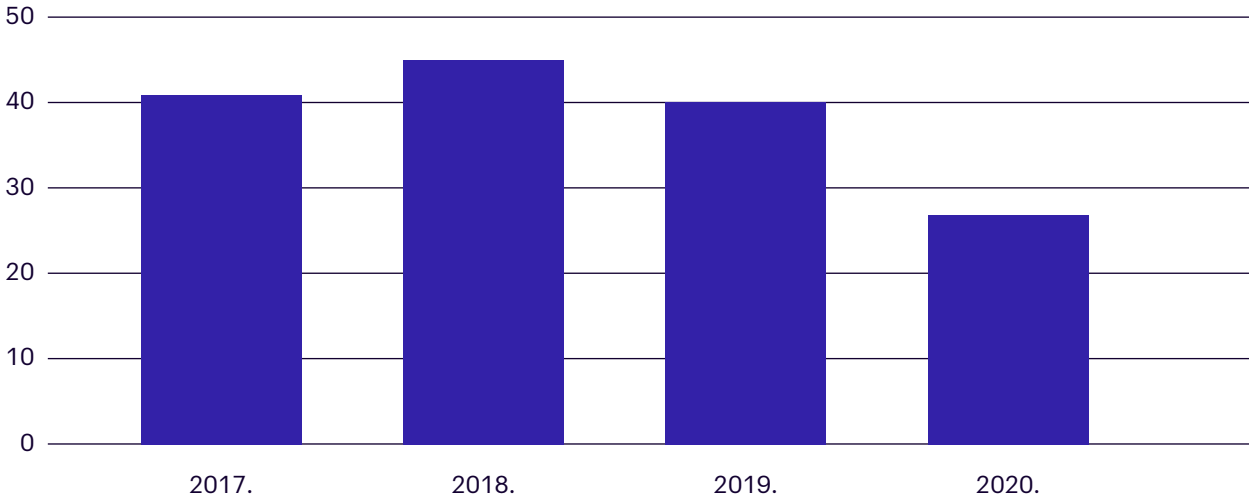
Kada od ukupnog broja poruka promatramo samo one koje su svojim sadržajem bile vezane za okolnosti nastale uslijed pandemije, tada postotak primatelja koji nisu prepoznali lažne poruke izrazito raste. Poruke s takvim sadržajem imale su uspješnosti i preko 47%. Hrvatska, izgleda, u ovome prati svjetske trendove, jer i na globalnoj razini broj napada upravo putem poruka sadržaja vezanih za pandemiju također raste i iznosi oko 40%.

Najbolja zaštita od napada metodama socijalnog inženjeringa, koji uključuju i *phishing* poruke, edukacija je korisnika računalnih sustava te pravodobno dijeljenje informacija o aktualnim napadima.

Primjena samo tehničkih mjera zaštite od *phishing* napada nije dovoljna. Uz tehničke mjere zaštite, najefikasnija mjera obrane od *phishing* napada i dalje je kontinuirano provođenje edukacija zaposlenika.

Ivona Loparić
voditeljica usluga socijalnog inženjeringa

Postotak primatelja koji nisu prepoznali Phishing poruku



[Slika 9] Postotak primatelja koji nisu prepoznali *Phishing* poruku [Izvor: Diverto]

Godina	Postotak primatelja	Broj poslanih poruka	
2017	42	1235	
2018	45	1096	
2019	40	2206	
2020	27	2740	
		7277	Ukupno poslano poruka

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

2.3 Zlonamjerni kod

Financijska korist jest dominantan motiv u gotovo svim napadima tijekom 2020. godine u Hrvatskoj. Napadači su se koristili dvjema poznatim tehnikama za ostvarenje svojih ciljeva:

- prikupljanje upisanih znakova na tipkovnici
- zaključavanje datoteka od poslovne važnosti

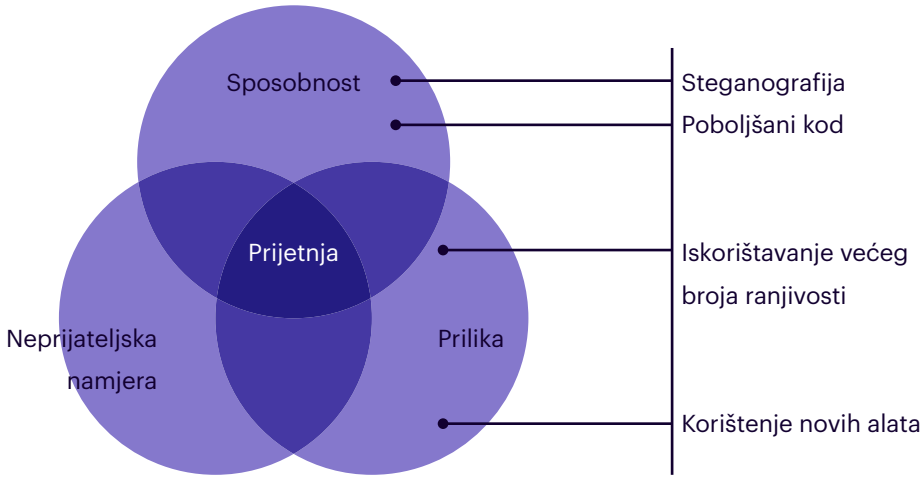
Ransomware je učinkovitije zaključavao datoteke. Nove verzije češće su sadržavale funkcionalnosti poput *Wake-On-LAN* mehanizma. *Ransomware* time djeluje lateralno u mreži, pali ugašena računala i zaključava datoteke na njima.

Veću opasnost predstavljaju i proširenja za preglednike (engl. *browser extension*). Proširenja s ugrađenim zlonamjernim kodom manipuliraju i preusmjeravaju podatke unutar preglednika i komuniciraju s napadačem. Neučinkovitost sigurnosnih rješenja da detektiraju zlonamjerna proširenja predstavlja ozbiljan problem organizacijama.

Napadači kontinuirano unapređuju tehnike napada. Primjer je zlonamjerni kod *Purple Fox*. Zabilježili smo tri bitne nadogradnje u 2020.:

- uvođenje steganografske tehnike
- uvođenje alata za kompromitaciju *broadcast* protokola
- iskorištavanje većeg broja ranjivosti u Windows okruženju

Napadači su unaprijedili sposobnosti i povećali prilike pa je primjerice *Purple Fox* postao veća prijetnja u drugoj polovini 2020. godine.



[Slika 10] Poboljšanja *Purple Foxa* tijekom 2020. godine

Intenzivnije djelovanje *Emoteta* uočeno je drugom polovinom 2020. godine i u Hrvatskoj. Krajem kolovoza povećan je broj *phishing* poruka e-pošte koje su ga distribuirale, trend se protezao do sredine studenoga. Veliki *botnet* omogućio je napadačima lakše upravljanje i prikupljanje podataka na zaraženim računalima.

Zlonamjerni kod je i dalje uspješan alat proboja, unatoč tome što sve velike organizacije posjeduju napredne sustave prevencije.

Bojan Alikavazović
voditelj analize zlonamjernog koda

2.4 Distribuirani napadi uskraćivanjem usluge (DDoS)

Donosimo vam detalje o DDoS napadima tijekom 2020. u Hrvatskoj. Distribuirani napad uskraćivanja usluge jedan je od najjednostavnijih i najosnovnijih, ali i dalje najučestalijih napada u internet prostoru. U Hrvatskom mrežnom prostoru takvi su napadi jednako tako učestali te nema određenog razdoblja kada takvi napadi nisu izraženi.

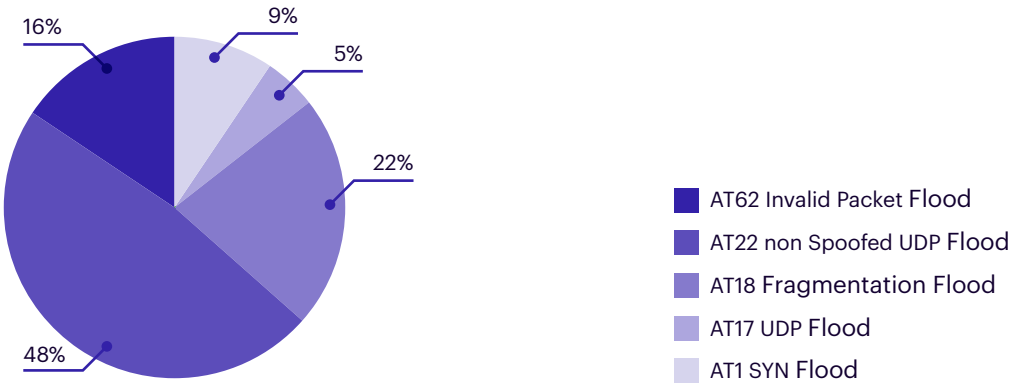
Posljedice DDoS napada obično traju mnogo duže nego sam napad. Trajanje napada odnosi se na prepoznatu mrežnu razinu na uređajima koji služe za zaštitu. Iako prepoznato vrijeme trajanja napada na mrežnom uređaju može izgledati kao kratak napad, posljedica samog napada često je mnogo duža jer je potrebno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

Tip napada	Broj paketa	Trajanje u min.
AT22 non Spoofed UDP Flood	2.43 Gpkts	875
AT62 Invalid Packet Flood	1.1 Gpkts	38
AT22 non Spoofed UDP Flood	891 Mpkts	624
AT1 SYN Flood	655.5 Mpkts	9
AT18 UDP FRAGMENTATION Flood	442 Mpkts	61
AT17 UDP Flood	353 Mpkts	7
AT18 UDP Fragmentation Flood	303.2 Mpkts	11
AT18 UDP Fragmentation Flood	293.4 Mpkts	16
AT18 UDP Fragmentation Flood	280.5 Mpkts	8
AT18 UDP Fragmentation Flood	223 Mpkts	62

[Tablica 2] Najveći napadi po ukupnoj količini paketa u 2020. godini [Izvor: Diverto]

TOP 5 DDoS tehnika po broju pristiglih paketa

1. AT22 non Spoofed UDP Flood
2. AT62 Invalid Packet Flood
3. AT1 SYN Flood
4. AT18 UDP Fragmentation Flood
5. AT17 UDP Flood



[Slika 11] Raspodjela najvećih napada po kategoriji [Izvor: Diverto]

Tip napada	Kol. podataka	Broj paketa	Trajanje u min.
AT18 UDP Fragmentation Flood	3.4 Tbits	303.2 Mpkts	11
AT18 UDP Fragmentation Flood	3.3 Tbits	293.4 Mpkts	16
AT18 UDP Fragmentation Flood	3.0 Tbits	280.5 Mpkts	8
AT3 ACK Flood	1.6 Tbits	149.0 Mpkts	460
AT3 ACK Flood	1.6 Tbits	148.5 Mpkts	461
AT3 ACK Flood	1.3 Tbits	122.2 Mpkts	360
AT18 UDP Fragmentation Flood	1.2 Tbits	118.2 Mpkts	8
AT3 ACK Flood	1.0 Tbits	99.0 Mpkts	701
AT3 ACK Flood	1.0 Tbits	98.3 Mpkts	682
AT3 ACK Flood	964.5 Gbits	91.8 Mpkts	431

[Tablica 3] Najveći napadi po ukupnoj količini podataka u 2020. godini [Izvor: Diverto]

TOP 5 DDoS tehnika po količini podataka

1. AT18 UDP Fragmentation Flood
2. AT3 ACK Flood
3. AT62 Invalid Packet Flood
4. AT2 SYN ACK Flood
5. AT1 SYN Flood

S obzirom na povećaniji rad izvan ureda, preporučujemo obratiti pozornost na točku spajanja udaljenih zaposlenika poput VPN koncentratora te kritične aplikacije izložene internetu.

Najveći napad po broju paketa jest 2,43 milijarde paketa i trajao je 875 minuta.

Najveći napad po količini podataka jest 3,4 Tbit i trajao je 11 minuta.

Analizirano na uzorku od ukupno 6247 napada koje su prepoznali uređaji za zaštitu od DDoS napada smješteni kod javnog i privatnog sektora u našoj zemlji. Analizirani napadi uzeti su 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 raspoložive na sljedećoj poveznici:

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

3 NIS direktiva i izazovi pred operatorima ključnih usluga

Kibernetička sigurnost industrijskih kontrolnih sustava (OT sustavi) kao predmet NIS direktive potaknula je pružatelje ključnih usluga na promjenu paradigme po kojoj OT sustavi, za razliku od IT sustava, nisu izloženi prijetnjama u kibernetičkom prostoru. Sigurnost OT Sustava postizala se strogim fizičkim i komunikacijskim razdvajanjem od svih ostalih sustava. OT sustavi bili su „sigurni" od kibernetičkih napada jer je njihova sigurnost ovisila o tome koliko su dobro primijenjene fizičke mjere zaštite i kontrole fizičkog pristupa do sustava. No s NIS direktivom sve se promijenilo te su danas operatori ključnih usluga, ali i sve organizacije koje su u vlasništvu ovih sustava stavljene pred nove izazove.

1. **Interni resursi i raskorak u vještinama u IT i OT sustavima (skill gap)**
   Sve je češća pojava spajanja starih, visoko pouzdanih, ali i inherentno kibernetički nesigurnih industrijskih kontrolnih sustava u kibernetički prostor. U kombinaciji s nedostatkom internih resursa koji bi mogli identificirati i ispravno umanjiti rizike može rezultirati prekomjernim izlaganjem OT sustava i posljedično napadima koji mogu prouzročiti posljedice po samog operatora, ali i po sve ostale ključne sustave koji ovise o usluzi operatora.

2. **Mogućnost detekcije incidenta kibernetičke sigurnosti**
   Sustavno prepoznavanje incidenata kibernetičke sigurnosti u OT sustavima zahtjevan je zadatak zbog već prethodno spomenutih nedostatnih internih resursa, starih sustava, neažurne dokumentacije tokova podatka, visoke ovisnosti o pružateljima usluga i zbog visokog rizika od utjecaja na procese podržane od sustava. Prepoznavanje djelovanja zlonamjernih aktivnosti bez sustavnog i automatiziranog pristupa praktički je nemoguće.

3. **Mijenjajući Threat landscape**
   Potreba za uvođenjem novih tehnologija u pružanje ključnih usluga kod operatora uvodi nove varijable s kojima operatori moraju računati na drukčije načine nego s prijašnjim „statičnim" statističkim prijetnjama. Vjerojatnost ostvarenja neke kibernetičke prijetnje ne smije i ne može biti temeljena na statistici jer ono što je dosad i danas nemogu-

će i nije zabilježen takav slučaj, zbog napretka tehnologije može već sutra biti ostvarivo i nanijeti operatoru značajne gubitke.

4. **Svijest operatora o situaciji**
   Primijetili smo kako je većina operatora, osim nekoliko reguliranih sektora, dosad vrlo malo pozornosti posvećivala kibernetičkoj sigurnosti svojih sustava ili je bila u uvjerenju da je kibernetička sigurnosti tih sustava pod kontrolom IT odjela. Stupanjem na snagu Zakona o kibernetičkoj sigurnosti, operatori su dobili dodatni poticaj da procijene kibernetičke rizike svojih usluga i da primijene prikladne tehničke, fizičke i administrativne mjere zaštite istih. Zakonske obveze polako podižu svijest operatora, ali prethodno navedeni izazovi vezani uz manjak internih resursa, nemogućnost prepoznavanja incidenata kao i stalno mijenjajući threat landscape i dalje su velik izazov.

5. **Kontinuitet poslovanja i ažurnost planova oporavka**
   Kontinuitet poslovanja sve više ovisi o OT sustavima o kojima, najčešće zbog manjka resursa, postoje ograničena znanja unutar operatora. U slučajevima neplaniranih situacija operatori se većinom pouzdaju na vanjske dobavljače koji posjeduju potrebna znanja i vještine. Bez obzira na navedeno, operatori su obvezni definirati strategije kontinuiteta poslovanja i redovno uvježbavati planove odgovora na nepogode izazvane kibernetičkim putem.

6. **Industrijski kontrolni sustavi nemaju odgovarajuću sigurnosnu zaštitu**
   Procesne *Ethernet* mreže nisu potpuno odvojene od poslovnih *Ethernet* mreža u organizacijama kritične infrastrukture. Nedovoljno razumijevanje metodologije odvajanja ostavlja česte sigurnosne nedostatke:
   - procesna mreža koristi DNS i NTP servise iz poslovne mreže
   - procesnoj mreži pristupa se VPN spajanjem kroz infrastrukturu poslovne mreže
   - vatrozidom, koji dijeli procesnu i poslovnu mrežu, upravlja osoblje iz poslovne mreže

   Zastarjeli i nepodržani operacijski sustavi čine većinu platformi koje su u upotrebi u procesnim mrežama. Očuvanje procesa proizvodnje ne dopušta česte izmjene komponenata u industrijskim kontrolnim sustavima, a alternativne metode, poput sigurnoga konfiguracijskog ojačanja, najčešće nisu provedene.

   Ipak, tijekom 2020. godine zabilježeni su pozitivni pomaci. Mnogobrojne organizacije koje upravljaju kritičnom infrastrukturom počele su s procjenom stanja sigurnosti te uklanjanjem nedostataka.

NIS 2

NIS je prva direktiva o kibernetičkoj sigurnosti na razini cijelog EU-a koja je stupila na snagu 2016. godine i pomogla postići višu i ujednačeniju razinu sigurnosti mrežnih i informacijskih sustava. Izrađen je prijedlog "NIS 2" direktive koji bi sa sobom trebao donijeti daljnja poboljšanja kao i nove sektore koje će pokrivati:

Podizanje kapaciteta za kibernetičku sigurnost

- strože provođenje i nadzor mjera
- uspostava administrativnih sankcija, uključujući kazne za povrede pri upravljanju rizicima i upravljanju kibernetičkom sigurnošću

Suradnja među zemljama članicama EU-a

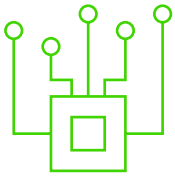
- uspostava EU CyCLONe *(Establishment of European Cyber Crises Liaison Organisation Network),* mreže za upravljanje velikim incidentima Kibernetičke sigurnosti
- naglasak na dijeljenja informacija i suradnju među zemljama članicama
- koordinirana otkrivanja ranjivosti

Upravljanje rizicima

- fokusiranije mjere za odgovor na incidente, upravljanje kriznim situacijama upravljanje i otkrivanje ranjivosti, testiranje i enkripciju
- ojačavanje upravljanja dobavljačima (engl. *supply chain*)
- jasnije obaveze prijave incidenta (definiraniji proces i vremenska crta)

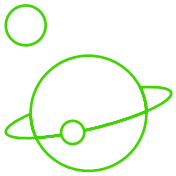
Dodatni sektori koje pokriva NIS2

Telekomunikacijske kompanije

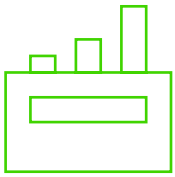


Digitalne usluge (usluge podatkovnih centara...)

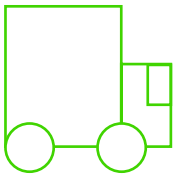
Upravljanje otpadnim vodama i otpadom



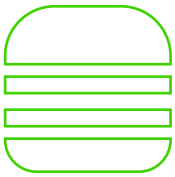
Svemir



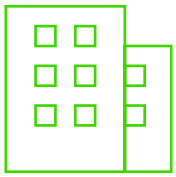
Proizvodnja kritičnih proizvoda (kemikalije, lijekovi)



Poštanske i kurirske službe



Hrana



Javna uprava

Sastavni dio upravljanja kibernetičkom sigurnošću ključnih usluga je sposobnost operatora da pravovremeno prepozna incident koji može imati utjecaja na pružanje ključne usluge, sposobnost ispravne reakcije na incident kao i sposobnost oporavka od posljedica incidenta uz čim manje posljedice po ključne usluge za koje su proglašeni operatorima.

Mario Blažević
voditelj OT usluga

4 Preporuke

Digitalizacija
Proteklo razdoblje obilježila je hiperprodukcija aplikativnih rješenja pri čemu su mnogi ignorirali potrebu analize rizika vezanih za ranjivosti takvih rješenja. To je dovelo do pojave dijela ranjivih aplikacija koje ne štite poslovne i osobne podatke na prihvatljiv način. Ponajviše se takve ranjivosti odnose na aplikacije koje zahtijevaju prijenos dokumentacije korisnika prema pružateljima usluga. Pozitivno je što su neki, prateći standardni proces rada i dobre prakse, promjenama upravljali na način koji uzima u obzir prethodno sagledavanje ranjivosti i postupke cjelovitog testiranja rješenja što i mi preporučujemo.

Kontinuitet poslovanja
Zbog intenzivnih seizmoloških aktivnosti na području okolice Zagreba i Siska potrebno je reevaluirati procjene utjecaja i posljedica potresa, a posebice njihovu vjerojatnost pojave. Svjedoci smo povećanja vjerojatnosti ostvarenja povezanih događaja poput požara, poplava ili urušavanja građevinskih objekata. Tradicionalna strategija odgovora na rizike potresa jest djelomičan prijenos rizika na treću stranu (osiguravatelja), to jest, ugovaranje polica osiguranja od požara i povezanih rizika. Potres je, uz situaciju vezano uz pandemiju virusa COVID-19, samo podsjetnik na važnost sustavnog održavanja i testiranja realnih planova kontinuiteta poslovanja.

Lanac opskrbe
Sve veća kompleksnost sustava te povećano korištenje trećih strana i *cloud* usluga povećava ovisnost organizacija o svom lancu opskrbe. Već neko vrijeme tema sigurnosti lanca opskrbe česta je u informacijskoj sigurnosti, a potvrdu o njezinoj važnosti dobila je *SolarWinds* incidentom koji je identificiran krajem 2020. godine. 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 cjelokupne infrastrukture.

DevSecOps
Implementacijom *Continuos Delivery* (CD) i *Continuos Integration* (CI) alata u razvojni ciklus omogućio je 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 na to da generički alati za kvalitetu koda obič-

no ne provjeravaju sve potrebne sigurnosne zahtjeve i nisu dostatni za kvalitetnu provjeru sigurnosti. Naša je preporuka to napraviti specijaliziranim SAST i DAST alatima koji provjeravaju veći skup sigurnosnih kontrola i zahtjeva te su u mogućnosti prepoznati kompleksnije sintakse i pozive.

Preporuke po sektorima

Financijski

Kao reguliran i nadziran sektor kojem upravljanje rizicima nije nepoznanica već svakodnevica treba:

- educirati zaposlenike o phishing napadima i posljedicama takvih napada
- automatizirati sigurnosne provjere odmah u početku kroz *DevSecOps*
- uvesti sigurnosne provjere softverskih i hardverskih komponenata
- redovno provoditi napredne napadačke vježbe (*purple* i *red* testiranja)
- nadograditi postojeće nadzorne mehanizme rješenjima poput sigurnosnog operativnog centra

Energetski

Energetski sektor u današnje vrijeme uvelike ovisi o industrijskim kontrolnim sustavima (OT sustava) te sve više uviđa važnost informacijske sigurnosti. Stupanjem na snagu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, između ostalog, naglašavaju se:

- procjena rizika kibernetičke sigurnosti
- obveze detekcije i prijave incidenta sa značajnim utjecajem
- ispravno izoliranje IT i OT sigurnosnih zona
- uvođenje sigurnosne provjere softverskih i hardverskih komponenata
- nadogradnja postojećih nadzornih mehanizama rješenjima poput sigurnosnog operativnog centra s integralnim pristupom nadzora poslovne i procesne mreže.

Proizvodnja

Uvođenjem automatizacije i međusobne povezanosti sustava putem računalnih mreža u organizacije se uvode novi, dosad neprepoznati rizici. Ti rizici nisu samo rizici IT-a, nego rizici organizacije pa je potrebno:

- prepoznati i tretirati rizike informacijske sigurnosti
- uključiti OT sustave u procjenu rizika
- alocirati dovoljne resurse (ljudske i tehničke) za informacijsku sigurnost
- izdvojiti informacijsku sigurnost izvan IT odjela
- ispravno izolirati IT i OT sigurnosne zone.

Javni sektor

Prelazak na povećani opseg rada od kuće za većinu javnih institucija naglasio je potrebu osiguranja zadovoljavajuće razine usluga i servisa građanima na siguran način. Kako bismo to postigli potrebno je:

- osigurati sigurno spajanje na mrežu institucije korištenjem provjerenih računala i sigurnih protokola spajanja
- obučiti zaposlenike o rizicima rada od kuće i načinima kako te rizike minimizirati
- provjeravati ranjivosti i penetracijski testirati izradu novih rješenja koja digitaliziraju usluge.

Maloprodaja

Ušli smo u vrijeme internetske trgovine, a kako bi internetska trgovina bila sigurna potrebno je da:

- vođenje projekta izrade ili nadogradnje internetske trgovine uključuje komponentu informacijske sigurnosti kroz životni ciklus
- treća strana koja pruža usluge izrade programskih rješenja primjenjuje dobre prakse informacijske sigurnosti i zaštite podataka o transakcijama
- redovito provodite kontrole nad trećim stranama

Start Up

Informacijsku sigurnost najlakše je implementirati prilikom pokretanja poduzetničkog pothvata. Dakle:

- primijenite razumne tehničke i organizacijske mjere koje će umanjiti rizike i koje će vašim korisnicima dati sigurnost i povjerenje prilikom korištenja proizvoda ili usluga
- automatizirajte sigurnosne provjere odmah u početku
- uvedite sigurnosne provjere softverskih i hardverskih komponenti koje ugrađujete
- educirajte osoblje o osnovama informacijske sigurnosti
- provodite redovna testiranja *IoT* i *cloud* rješenja ako ih razvijate

5 O izvještaju

Diverto d.o.o., jedno od vodećih društava na području primjene informacijske sigurnosti, donosi osvrt na stanje informacijske sigurnosti u Hrvatskoj za cijelu 2020. godinu. Prethodni osvrt i povratne informacije koje smo dobili pokazuju da postoji interes za takvim izvještajima i Diverto aktivnostima izdavanja izvještaja podiže svijest o informacijskoj sigurnosti kod šire poslovne zajednice u Republici Hrvatskoj kao i u regiji.

Osvrt i preporuke donose se kroz tri različite, ali međusobno povezane perspektive informacijske sigurnosti korištenjem *top-down* pristupa:

- upravljačke *(governance)*
- napadačke *(offensive)* i
- obrambene *(defensive)* perspektive

Osvrt temeljimo na:

- procjenama stanja informacijske sigurnosti u organizacijama javnog i privatnog sektora u našoj zemlji koje su u domeni našeg GRC *(Governance Risk and Compliance)* tima
- podacima prikupljenima iz aktivnosti Diverto Sigurnosnog operativnog centra i aktivnostima našeg obrambenog tima
- rezultatima provjere ranjivosti, penetracijskih testiranja i drugih tipova sigurnosnih testiranja koje provodi naš napadački tim

Osim osvrta obradili smo i, po nama najznačajnije, teme od interesa u području primjene informacijske sigurnosti za koje vjerujemo da će obilježiti i godinu koja je pred nama.