Analiza kibernetičkih napada na kritične infrastrukture

Sviben, Tonka

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija - smjer Menadžerska informatika

ANALIZA KIBERNETIČKIH NAPADA NA KRITIČNE INFRASTRUKTURE

Diplomski rad

Tonka Sviben, 1191240015

Zagreb, rujan, 2022.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija - smjer Menadžerska informatika

ANALIZA KIBERNETIČKIH NAPADA NA KRITIČNE INFRASTRUKTURE

ANALYSIS OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURES

Diplomski rad

Student: Tonka Sviben

JMBAG: 1191240015

Mentor: prof. dr. sc. Mario Spremić

Zagreb, rujan, 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad/ seminarski rad / prijava teme diplomskog rada isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada / prijave teme nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada / prijave teme ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada / prijave teme nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Tonka Sviben

(vlastoručni potpis studenta)

Zagreb, 30.08.2022.

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

Tonka Sviben

(personal signature of the student)

Zagreb, 30.08.2022.

(place and date)

SAŽETAK

Tema ovog diplomskog rada nastoji prikazati važnost utjecaja kibernetičkih napada na pojedinca, organizaciju i društvo. Zbog sve veće količine podataka u optjecaju i svakodnevnog korištenja informacijske tehnologije, kibernetički napadi se događaju sve češće te su posljedice sve opasnije za društvo. Kritične infrastrukture su posebno osjetljive mete za napadače te su pod povećanim nadzorom. Sigurnost kritičnih infrastruktura postiže se detaljnim i kontinuiranim analiziranjem napada koji su se dogodili. Uz osnovne principe informacijske sigurnosti, najvažnije je educirati društvo o važnosti kibernetičke sigurnosti, prijetnjama i rizicima koji nastaju zbog intenzivne primjene informacijske tehnologije u poslovanju i svakodnevnom životu. Također, u sklopu diplomskog rada provedeno je istraživanje o informiranosti ispitanika o kibernetičkoj sigurnosti i kibernetičkim napadima.

Ključne riječi: kibernetička sigurnost, kibernetički napad, kibernetički rizik, kritična infrastruktura, informacijski sustav

SUMMARY

The topic of this thesis aims to show the importance of the impact of cyberattacks on the individual, organization and society. Due to the increasing amount of data in circulation and daily use of information technology, cyber attacks occur more often now than ever and the consequences for society are dangerous. Critical infrastructures are particularly vulnerable targets for attackers and are under increased surveillance. Security of critical infrastructures is achieved by detailed and continuous analysis of attacks that have occurred. In addition to the basic principles of information security, it is important to educate society about the importance of cyber security, threats and risks that arise due to the intensive application of information technology in business and everyday life. Also, as part of the thesis, a survey was conducted on respondents' awareness of cyber security and cyber attacks.

Keywords: cyber security, cyber attack, cyber risk, critical infrastructure, information system

SADRŽAJ

1. UVOD

1.1 Predmet i cilj rada

Predmet ovog diplomskog rada je analiza kibernetičkih napada na kritične infrastrukture. Digitalizacijom i razvojem novih tehnologija povećava se vjerojatnost kibernetičkih napada u kritičnim infrastrukturama zbog korištenja informacijskih sustava. Cilj rada je utvrditi i objasniti na koji način su se dogodili odabrani kibernetički napadi te koje su njihove posljedice na kritične infrastrukture. Na svjetskoj razini kontinuirano raste broj kibernetičkih napada koji postaju sve složeniji i imaju sve teže posljedice, stoga je važno shvatiti utjecaj koji kibernetički napadi imaju na kritične infrastrukture te se pravovremeno informirati o kibernetičkoj sigurnosti kako bi se napadi spriječili ili barem ublažile njihove posljedice.

1.2 Metode istraživanja i izvori podataka

Rad se sastoji od teorijskog i empirijskog dijela te su korištene različite metode i izvori. Korištene su znanstvene i stručne publikacije dostupne u elektroničkim bazama podataka, knjige, materijali dostupni u knjižnici Ekonomskog fakulteta u Zagrebu s područja informatike, stranice stručnih časopisa s područja ekonomije te razne internetske stranice. Empirijsko istraživanje provedeno je korištenjem online anketnog upitnika (Google obrazac), a ispitanici su bili studenti Ekonomskog fakulteta u Zagrebu. Svi izvori podataka navedeni su na kraju diplomskog rada u Literaturi.

1.3 Sadržaj i struktura rada

Rad je podijeljen na pet poglavlja, pri čemu je prvi dio uvod u kojem se definiraju predmet i cilj rada, metode istraživanja i izvori podataka u radu. U drugom poglavlju „Objašnjenja pojmova vezanih uz kibernetičke napade ” definirani su kibernetička sigurnost, rizici i napadi i kritične infrastrukture te ključne informacije o njima. U trećem poglavlju analizirani su napadi na kritične infrastrukture koji su se dogodilo diljem svijeta te se nastoje objasniti posljedice napada. Zatim je u četvrtom poglavlju „Istraživanje razine informiranosti o kibernetičkim napadima“ opisan cilj istraživanja, metodologija i rezultati provedenog istraživanja. Na samom kraju, peto poglavlje je zaključak koji donosi sažetak rada i zaključnu misao cjelokupnog rada.

2. OBJAŠNJENJA POJMOVA VEZANIH UZ KIBERNETIČKE NAPADE

2.1 Kibernetička sigurnost

Područje kibernetičke sigurnosti ima sve veći značaj u vremenu digitalizacije i razvoja novih tehnologija te se zbog sve većeg korištenja informacijskih sustava u svijetu bilježi porast kibernetičkih napada. Kako bi se uspješno odgovorilo na napade potrebno je imati svijest o važnosti kibernetičke sigurnosti te poznavati točne definicije pojmova vezanih uz ovo područje. Kako bi se kontinuitet poslovanja održao, nužno je da organizacije shvate važnost kibernetičke sigurnosti te sigurnosne prakse učine dijelom organizacijske kulture.

Razvoj digitalne transformacije doveo je do novih prijetnji kibernetičkoj sigurnosti, a pandemija korona virusa stvorila je nove prilike za kibernetičke kriminalce koji posebno ciljaju organizacije koje rade na daljinu.

Postoji mnogo definicija kibernetičke sigurnosti od kojih su neke:

- Kibernetička sigurnost se uglavnom sastoji od obrambenih metoda koje se koriste za otkrivanje i sprječavanje potencijalnih uljeza (Kemmerer, 2003).
- Kibernetička sigurnost uključuje smanjenje rizika od zlonamjernog napada na softver, računala i mreže. To uključuje alate koji se koriste za otkrivanje provala, zaustavljanje virusa, blokiranje zlonamjernog pristupa, provođenje provjere autentičnosti, omogućavanje šifrirane komunikacije i tako dalje (Amoroso, 2006).
- Kibernetička sigurnost skup je alata, politika, sigurnosnih koncepata, sigurnosnih mjera zaštite, smjernica, pristupa upravljanju rizikom, radnji, obuke, najboljih praksi, jamstava i tehnologija koje se mogu koristiti za zaštitu kibernetičkog okruženja i organizacije te imovine korisnika (ITU, 2009).
- Aktivnost, proces, sposobnost ili stanje prema kojem su informacijski i komunikacijski sustavi i informacije sadržane u njima zaštićeni i/ili obranjeni od oštećenja, neovlaštene uporabe, modifikacije ili iskorištavanja (DHS, 2014).

Kibernetička sigurnost se osigurava kroz strategije i planove koji uključuju obrambenu upotrebu informacijske tehnologije za napad na protivnike. Pomoću strategija i planova za kibernetičku sigurnost definira se pravni okvir za kibernetičke rizike te postupci u slučaju kibernetičkih napada.

Holistički okvir za ocjenjivanje i poboljšanje kulture informacijske sigurnosti predložen je istraživanjem (Arbanas, Spremić, Žajdela Hrustek, 2021) koje je utvrdilo kako se informacijska sigurnost ne treba promatrati samo s tehničkog aspekta, već postoji i ljudski problem. Istraživanje je imalo praktičan i znanstveni doprinos te je utvrđeno kako postoji potreba za proučavanjem informacijske sigurnosti s tehnološkog, organizacijskog, društvenog i upravljačkog aspekta. Predloženi okvir može se promatrati kao uravnotežen alat za prepoznavanje i utjecaj na faktor koji ne pridonosi dovoljno postojećoj kulturi informacijske sigurnosti u organizaciji ili, obrnuto, faktor koji uvelike utječe na postojeću kulturu informacijske sigurnosti i omogućuje stvaranje dodane vrijednosti za organizaciju u cjelini (Arbanas, Spremić, Žajdela Hrustek, 2021).

2.2 Kibernetički rizik

Kibernetički rizici nastaju kao posljedica intenzivne primjene digitalnih tehnologija u poslovanju i svakodnevnom životu (Spremić, 2017). Organizacije i pojedinačni korisnici izloženi su rizicima kao što su krađa identiteta, uništavanje reputacija i sudske tužbe itd. Rizik kibernetičke sigurnosti odnosi se na kombinaciju vjerojatnosti prijetnje i gubitka (obično u financijskom smislu) (Muscat, 2019). Kibernetički rizici imaju dvojnu narav jer su neizbježni, stalno su prisutni i njihova pojava i intenzitet stvaraju probleme u poslovanju, a njihovo bolje upravljanje čuva vrijednost informatičkih ulaganja (Spremić, 2017). Kibernetičke prijetnje odnose se na događaje s mogućnošću prouzročenja štete, dok su ranjivosti slabosti u sustavu. Prijetnja je opasnija što više ranjivosti sustava iskoristi. Kibernetičke prijetnje bilježe kontinuirani porast na globalnoj razini, a najveći broj prijetnji u posljednje dvije godine nastao je zbog pandemije korona virusa. Rizik od zaraze prisilio je organizacije na rad od kuće čime su se stvorili dodatni kibernetički rizici. Organizacije su premjestile svoj rad iz ureda te su bile prisiljene koristiti poslovanje u oblaku gdje su zaposlenici stvarali i pohranjivali podatke na daljinu putem aplikacija u oblaku (eng. Cloud) i time su se povećale mogućnosti za napad. Osim rizika koji su nastali zbog rada na daljinu, uvođenje 5G mreže i povećanje korištenja Internet stvari (eng. Internet of Things, dalje u tekstu „IoT“) dovodi do povećanja ranjivosti podataka na kibernetičke napade. Pojam IoT se odnosi na povezivanje brojnih uređaja opremljenih računalnim čipovima koji čine tehnološke i

infrastrukturne digitalne platforme (Spremić, 2017). Razvijanje novih tehnologija dovodi do svakodnevnog povećanja podataka čime se povećava rizik od njihovog oštećenja, gubitka ili manipulacije. Podaci se stvaraju i pohranjuju na privatnim i javnim IT infrastrukturama, na komunalnim infrastrukturama, na privatnim i javnim podatkovnim centrima u oblaku, na osobnim računalnim uređajima i na IoT uređajima. Prema Morganu (2020) do 2025. godine će ukupno biti pohranjeno 100 zetabajta podataka.

Tablica 1 Mjerne jedinice za podatke

Naziv jedinice	Kratica	Decimalni sustav	Binarni sustav
Jotabajt	(YB)	1.000^8	1.024^8
Zetabajt	(ZB)	1.000^7	1.024^7
Eksabajt	(EB)	1.000^6	1.024^6
Petabajt	(PB)	1.000^5	1.024^5
Terabajt	(TB)	1.000^4	1.024^4
Gigabajt	(GB)	1.000^3	1.024^3
Megabajt	(MB)	1.000^2	1.024^2
Kilobajta	(KB)	1.000	1.024
Bajt	(B)	1	1

Izvor: samostalna izrada autorice rada (prema: PC Chip, 2018)

Prema Agenciji Europske unije za kibernetičku sigurnost (2021) postoji devet glavnih skupina prijetnji:

1. Ucjenjivački softver (eng. ransomware) – nakon neovlaštenoga upada u računalo, najčešće djelovanjem računalnoga virusa kojega je pokrenuo neoprezni korisnik, šifriraju se podaci koji su u njemu pohranjeni, a koji su neophodni za nastavak rada ili poslovanja, pri čemu računalni kriminalci traže odštetu (najčešće u bitcoinima) za njihovo dešifriranje (Spremić, 2017).
2. Zlonamjerno rudarenje kriptovalute (eng. cryptojacking) – neovlašteno korištenje tuđih računalnih resursa za rudarenje kriptovalute (Chickowski, 2022).
3. Prijetnje podacima – objavljivanje osjetljivih, povjerljivih ili zaštićenih podataka u nepouzdano okruženje.

4. Zlonamjerni računalni programi (eng. malware) – računalni virusi i ostali zlonamjerni računalni kodovi napisani i distribuirani s namjerom da naprave štetu nad računalnim i ostalim resursima (Spremić, 2017).
5. Dezinformacija – širenje pogrešnih informacija kako bi se smanjilo povjerenje.
6. Nezlonamjerne prijetnje –ljudske pogreške i pogrešne konfiguracije sustava.
7. Prijetnje dostupnosti i integritetu – napadi koji sprječavaju korisnike sustava u pristupu njihovim podacima uzrokujući smanjenje performansi, gubitak podataka i prekide usluga.
8. Prijetnje povezane s e-poštom – cilj je manipulirati ljudima putem e-pošte.
9. Prijetnje lancu opskrbe – npr. napad na pružatelja usluga, kako bi se dobio pristup podacima kupca.

Kibernetički rizici su uvijek prisutni te ih nije moguće otkloniti, no potrebno ih je dobro poznavati i razviti planove odgovora na njih. Kako bi se smanjili kibernetički rizici organizacije redovito moraju održavati svoje sustave te biti u toku s najnovijim tehnologijama. Potrebno je provoditi segmentaciju na mrežama kako bi se smanjio učinak napada, održavati usklađenost sa HIPAA, SOX, ISO 27001 i drugima, te je najvažnije educirati zaposlenike o rizicima kojima su izloženi. Podizanje svijesti organizacije je ključni čimbenik osiguranja kibernetičke sigurnosti.

2.3 Kibernetički napadi

Kibernetički napadi se događaju sve češće i postaju sofisticiraniji te imaju veći utjecaj na svakodnevni život i poslovanje. Napadi se mogu dogoditi bilo kada, osim pojedinaca i poduzeća, kibernetički napadi kao mete imaju i lokalne i državne vlasti, točnije kritične infrastrukture. Svakodnevno se otkrivaju novi malware i virusi. Kibernetički napad bi potencijalno mogao onesposobiti sustave organizacije, grada ili države. Kibernetički napadi su vrlo opasni za organizacije kao i za pojedince. Izdaci za kibernetički kriminal dramatično rastu te je proračun za kibernetičku sigurnost u porastu kako sve više organizacija shvaća vrijednost i važnost ulaganja u kibernetičku sigurnost. Troškovi kibernetičkog napada uključuju oštećenje i uništavanje podataka, ukradeni novac, izgubljenu produktivnost, krađu intelektualnog vlasništva, krađu osobnih i financijskih podataka, pronevjeru, prijevaru, poremećaj kontinuiteta poslovanja, istragu, vraćanje i brisanje podataka te narušavanje ugleda. Pojedinci su također svjesni rizika od kibernetičkih napada jer su naslovi o napadima u medijima sve češći. U današnje vrijeme ne morate biti poslovni

IT stručnjak da biste razumjeli da postoje sigurnosni rizici, ali je teže razumjeti tko, kako, zašto i kada može postati žrtva napada, koliko su napadi rašireni i koje će se vrste prijetnji najvjerojatnije pojaviti.

2.3.1 Vrste kibernetičkih napada

U ovom poglavlju objašnjeni su neki od kibernetičkih napada koji ovisno o razmjeru mogu utjecati na pojedinca ili organizaciju. Kako se svakodnevno u svijetu događaju različite vrste kibernetičkih napada potrebno je raspoznati koje su to vrste i koji su načini zaštite od njih.

A. Napadi zlonamjernih softvera (eng. malware) su jedni od najčešćih vrsta kibernetičkih napada. To su programi koji su najčešće tajno ubačeni u sustav s namjerom ometanja ili počinjenja određene štete odnosno s namjerom ugrožavanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija, operacijskoga sustava ili nekoga drugog dijela računalnoga ili informacijskoga sustava (Spremić, 2017). Zlonamjerni softveri se probijaju u sustave kroz mrežne ranjivosti. Kada korisnik klikne na zaraženu poveznicu ili preuzme privitak iz e-maila on propušta zlonamjerni softver u svojoj sustav. Napadi zlonamjernih softvera se mogu spriječiti antivirusnim softverima (npr. Avast Antivirus, Norton Antivirus i McAfee Antivirus) te korištenjem vatrozida koji filtriraju mrežni promet. U zlonamjerne softvere spadaju:
    - Računalni crvi (eng. worms) koji sami sebe umnožavaju i šire se putem računalne mreže,
    - Špijunski softver (eng. spyware) koji krade povjerljive podatke bez znanja žrtve,
    - Ucjenjivački softver (eng. ransomware) je softver koji blokira pristup ključnim komponentama mreže te je najpoznatiji model monetizacije kibernetičkih napada,
    - Zlonamjerni oglašivački softveri (eng. adware) koji prikazuje reklamni sadržaj na zaslonu korisnika koji sadrži računalni virus,
    - Trojanski virusi koji se prerušavaju u legitimne softvere.

B. Phishing napadi su jedni od najraširenijih kibernetičkih napada. To je vrsta napada koja spada u društveni inženjering. vrsta računalne prijevare s ciljem krađe identiteta. Phishing se odnosi na aktivnosti kojima prevaranti i računalni kriminalci slanjem lažnih elektroničkih poruka, koje izgledaju kao da su ih poslale izvorne institucije, dobiju pristup povjerljivim korisničkim podacima (Spremić, 2017). Kako bi se spriječili ovakvi napadi potrebno je provjeravati e-mail i ne otvarati poštu od sumnjivih izvora te je potrebno redovito ažurirati lozinke u skladu s dobrim praksama.

C. Napadi na lozinke u kojima napadač raznim programima probija lozinku i dobiva pristup podacima. Postoje različite vrste napada na zaporke kao što su napadi grubom silom, napadi rječnikom i keylogger napadi. Kako bi se sprječili ovakvi napadi potrebno je postaviti lozinke u skladu s dobrim praksama.

D. Man-in-the-Middle (MITM) napadi su napadi prisluškivanjem. Napadač koji se nalazi na kanalu između tražitelja resursa i resursa iskorištava ranjivosti mreže i zaobilazi komunikacijske protokole, čime mu je omogućeno nadgledati sadržaj, pohranjivati datoteke i mijenjati sadržaj komunikacije (Spremić, 2017). Ovakvi napadi mogu se spriječiti enkripcijom podataka na mrežnim uređajima i pažljivim korištenjem javnih Wi-Fi mreža.

E. SQL napadi (eng. SQL injection) su napadi u kojima se zlonamjerni kod ubacuje u SQL server kako bi izvršio određenu naredbu (Huremović, 2021). Napadač može pregledavati, uređivati i brisati podatke u bazama podataka. Ovakvu vrstu napada moguće je spriječiti instaliranjem softvera za otkrivanje neovlaštenog pristupa mreži i provjerama valjanosti podataka.

F. Napadi uskraćivanjem usluge (eng. Denial-of-Service) uključuju nedopuštene aktivnosti sprječavanja ili onemogućavanja ovlaštene uporabe računalne mreže, sustava ili programa iskorištavanjem njihovih resursa (Spremić, 2017). Ukoliko u napadu sudjeluje više kompromitiranih sustava tada govorimo o distribuiranom napadu uskraćivanjem usluge (eng. Distributed Denial-of-Service). Da bi se spriječili napadi potrebno je analizirati mrežni promet te definirati planove odgovora na incidente kako bi se vrijeme bez usluge smanjilo.

G. Unutarnji napadi ne uključuju treću stranu već korisnike informacijskog sustava i zaposlenike organizacije te su raširenji u manjim organizacijama jer je segmentacija uloga manja nego u većim organizacijama. U mnogim slučajevima, napadač koristi značajnu količinu resursa, alata i vještina kako bi pokrenuo sofisticirani računalni napad i potencijalno uklonio sve dokaze tog napada (Techopedia, b.d.). Kako bi se spriječili ovakvi napadi organizacije bi trebale imati zdravu organizacijsku kulturu te visoku razinu svijesti o sigurnosti.

H. Napadi zlonamjernog rudarenja kriptovalute (eng. cryptojacking) su usko povezani s kriptovalutama. Napadači pristupaju tuđim računalima radi rudarenja kriptovalute koje se odvija u pozadini te ga žrtve nisu svjesne. Pristup se dobiva zarazom preko web stranice ili poveznice. Napadi se mogu spriječiti redovitim ažuriranjem sustava, instaliranjem softvera za blokiranje oglasa koji su primarni izvor ovakvih zaraza i instaliranjem ekstenzije koje se koriste za prepoznavanje i blokiranje skripta.

I. Eksploatacija nultog dana (eng. Zero-Day Exploit) je ranjivost u sustavu ili uređaju koja je otkrivena, ali još nije zakrpana (Trend Micro, b.d.). Najčešće se o ranjivosti obavještavaju zaposlenici, ali vijest dolazi i do napadača. Ovisno o ranjivosti potrebno je neko vrijeme da se popravi problem dok u međuvremenu, napadači ciljaju otkrivenu ranjivost. Eksploatacije nultog dana mogu se spriječiti automatizacijom i dobrim upravljanjem procesom razvijanja zakrpa kako bi se izbjegla kašnjenja u implementaciji.

J. Napad na pouzdano i posjećeno web mjesto (eng. Watering Hole Attack) cilja na web stranice koje žrtva često koristi kako bi se komprimirali osobni podaci ili omogućio udaljeni pristup računalu žrtve. Cilj je zaraziti računalo ciljanog korisnika i dobiti pristup mreži na radnom mjestu ciljanog korisnika (Wright, Bacon 2021). Napadi ovakve vrste mogu se spriječiti redovitim održavanjem sustava, upotrebom sustava za sprječavanje upada (IPS), prikrivanjem aktivnosti na mreži putem VPN-a koji omogućuje sigurniju vezu.

2.3.2 Kibernetički napadi u brojkama

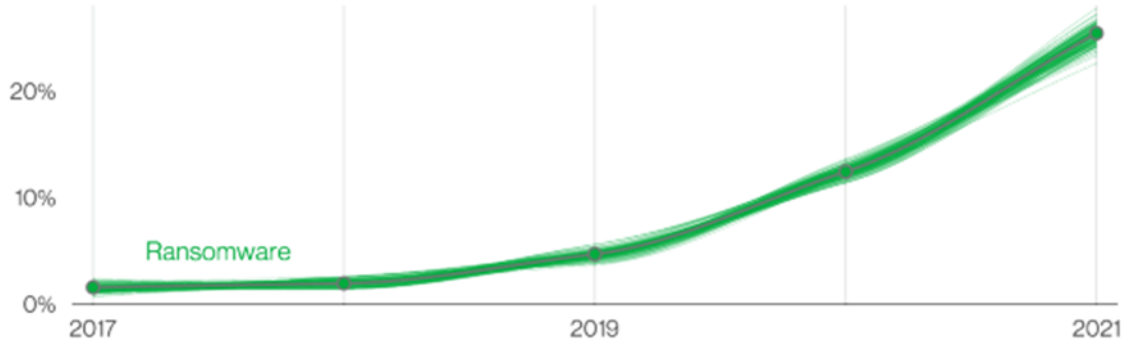
U ovom poglavlju izdvojeni su podaci iz nekoliko istraživanja iz područja kibernetičke sigurnosti koja su provedena u 2021. godini. Kibernetička sigurnost se pomno prati i detaljno analizira kako bi se u budućnosti spriječili napadi i kako bi se kibernetički rizici minimizirali.

- Verizon Data Breach Investigations Report

U Verizon izvješću "Data Breach Investigations Report" (2022) prikazano je kako napadači djeluju i koga ciljaju te koje metode napada imaju najveće posljedice. Verizon je analizirao 23.896 incidenata u otprilike 20 različitih industrija koji su se dogodili tijekom vremenskog razdoblja od 1. studenog 2020. do 31. listopada 2021.

Ransomware napadi su imali porast od skoro 13% u odnosu na 2020. godinu. Istraživanje je otkrilo da je čak 78% organizacija doživjelo napade ransomware-a putem e-pošte u 2021. Autori istraživanja primjećuju da je promjena ljudskog ponašanja ono što je potrebno kako bi se smanjio rizik od napada ransomware-a. Ljudski element je bio ključan za 82% incidenata u 2021. godini te je i dalje glavni uzrok porasta napada.

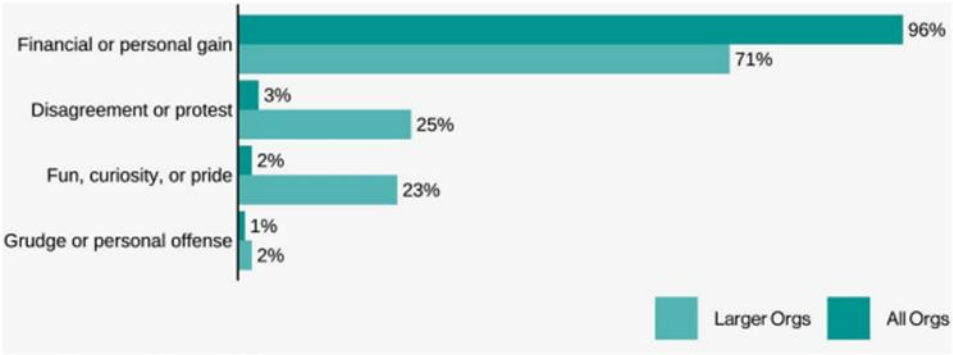
Slika 1 Porast ransomware napada



Izvor: Verizon Data Breach Investigations Report (2021)

Istraživači su smatrali da je važno razumjeti motiv napadača. Financijski motiv je glavni pokretač napada. Nakon toga slijede napadi zbog nezadovoljstva ili protesta, napadi nastali iz zabave. Na posljednjem mjestu su napadi nastali zbog osobnih zamjeraka.

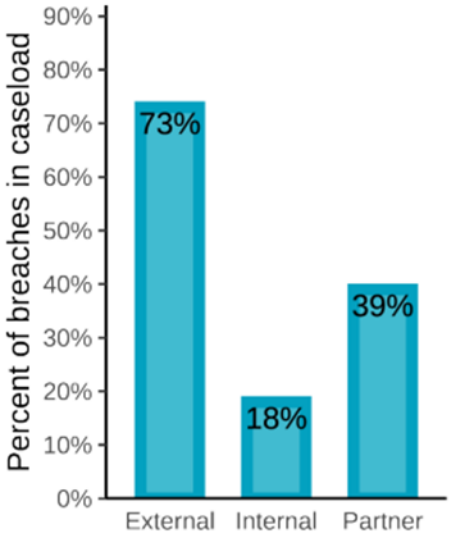
Slika 2 Motivi kibernetičkih napada



Izvor: Verizon Data Breach Investigations Report (2021)

Istraživanje je pokazalo kako je vjerojatnost napada najveća od vanjskih izvora. U skoro tri od četiri slučaja izvori napada su bili izvan organizacije. Poslovni partneri bili su izvori napada u 39% obrađenih povreda podataka. Unutarnji izvori činili su najmanji broj incidenata (18%).

Slika 3 Izvori kibernetičkih napada



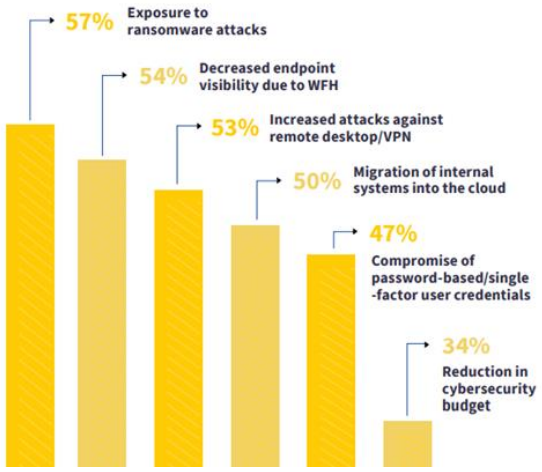
Izvor: Verizon Data Breach Investigations Report (2021)

- The State of Incident Response

Prema VMware-ovom izvješću „The State of Incident Response“ (2021) potreba za detaljnim i dobro uvježbanim planovima odgovora na incidente je veća nego ikada. Pandemija korona virusa pokazala je nedostatke odjela kibernetičke sigurnosti mnogobrojnih organizacija te neučinkovitost njihovih planova odgovora na incidente. Velika većina (93%) organizacija je doživjela kompromitiranje podataka u proteklih 12 mjeseci, a većina voditelja sigurnosti (82%) smatra da je njihova organizacija ranjiva. Također, istraživanje je pokazalo kako gotovo polovica organizacija (49%) nije spremna odgovoriti na izazove kibernetičke sigurnosti, dok druga polovica (54%) gubi vrijeme istražujući upozorenja niske razine i time usporava proces odgovora na važnije incidenta. Gotovo polovica organizacija smatra da nema odgovarajuće resurse (uključujući osoblje i stručnost) za otkrivanje ili odgovaranje na kibernetičke prijetnje.

Na slici 4 prikazani su rizici za koje voditelji sigurnosti smatraju da su njihove organizacije bile izložene tijekom 2021. godine. Najveću izloženost imali su ransomware napadima, nakon toga slijede rizici koji su nastali zbog rada od kuće koji uključuju i rad u oblaku, te smanjenje budžeta za kibernetičku sigurnost unutar organizacije.

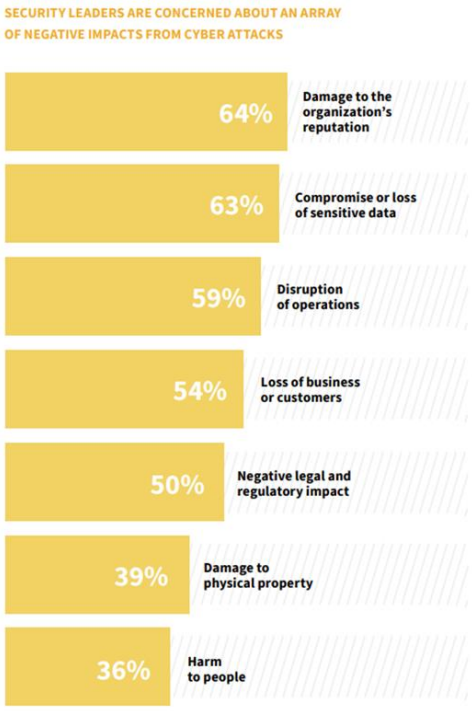
Slika 4 Rizici kojima su organizacije izložene



Izvor: The State of Incident Response (2021)

Istraživanje je pokazalo kako voditelje sigurnosti zabrinjavaju negativne posljedice kibernetičkih napada koje su redom negativna reputacija, gubitak ili oštećenje podataka, prekid poslovanja, gubitak klijenata, pravni sporovi, fizičko oštećenje imovine i povrede zaposlenika.

Slika 5 Negativne posljedice kibernetičkih napada



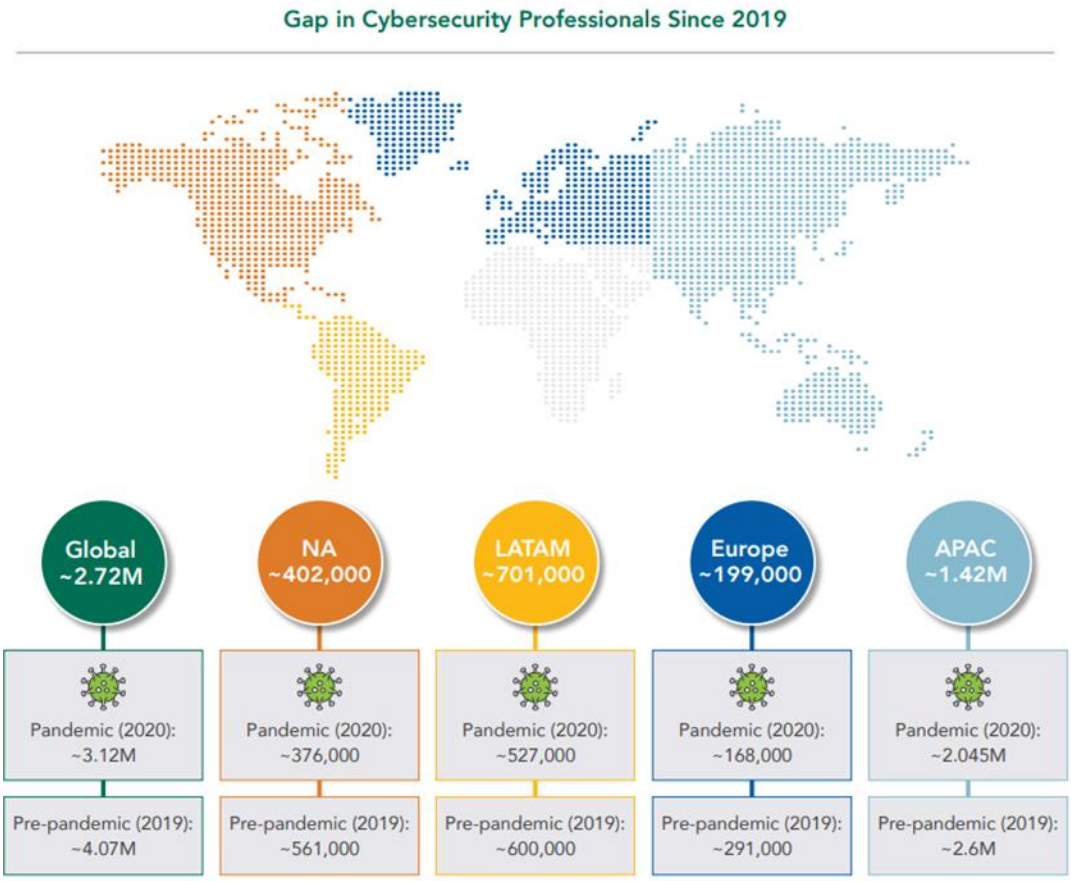
Izvor: The State of Incident Response (2021)

- Cybersecurity Workforce Study

Studija pod nazivom „Cybersecurity Workforce Study“ (2021) prikupila je podatke od 4753 stručnjaka za kibernetičku sigurnost koji rade s malim, srednjim i velikim organizacijama diljem Sjeverne Amerike, Europe, Latinske Amerike i Azije i Pacifika.

Za 2021. studija procjenjuje da postoji 4,19 milijuna stručnjaka za kibernetičku sigurnost diljem svijeta, što je povećanje od više od 700.000 u odnosu na prošlu godinu. Drugu godinu zaredom, nedostatak radne snage u kibernetičkoj sigurnosti smanjio se na 2,72 milijuna u usporedbi s 3,12 milijuna prošle godine. No, procjena radne snage za kibernetičku sigurnost i nedostatak radne snage za kibernetičku sigurnost sugeriraju da globalna radna snaga za kibernetičku sigurnost treba porasti za 65% da bi se učinkovito branila kritična sredstva organizacije.

Slika 6 Jaz radne snage u kibernetičkoj sigurnosti



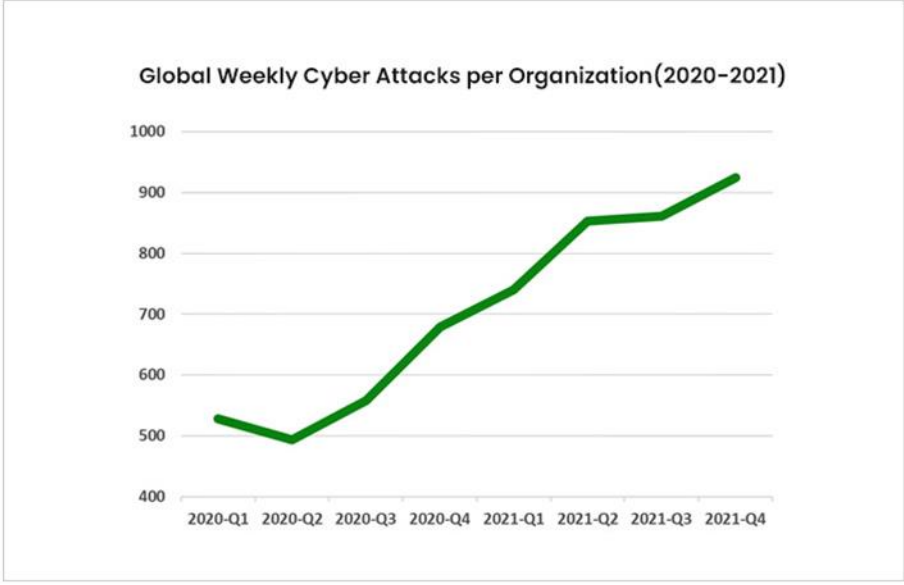
Izvor: Cybersecurity Workforce Study (2021)

Jaz u radnoj snazi za kibernetičku sigurnost razlikuje se od regije do regije. Jaz radne snage se povećava u Sjevernoj Americi, Europi i Latinskoj Americi. Međutim, zemlje APAC pokazuju kontinuirano smanjenje jaza u radnoj snazi za kibernetičku sigurnost te je taj pad dovoljno značajan da nadoknadi potražnju u ostatku svijeta.

- Check Point Research

Statistika i podaci korišteni u izvješću pod nazivom „Check Point Research“ (2022) prikazuju podatke koje je otkrila tehnologija Threat Prevention tvrtke Check Point, pohranjene i analizirane u ThreatCloudu. ThreatCloud pruža obavještavanje o prijetnjama u stvarnom vremenu koje proizlazi iz stotina milijuna senzora diljem svijeta, preko mreža, krajnjih točaka i mobilnih telefona. Prema izvješću, od sredine 2020. do 2021. porastao je broj kibernetičkih napada te je dostigao vrhunac od 925 kibernetičkih napada tjedno po organizaciji, na globalnoj razini. Na Slici 7 vidljiv je rast broja napada po kvartalima u razdoblju od drugog kvartala 2020. do zadnjeg kvartala 2021. godine.

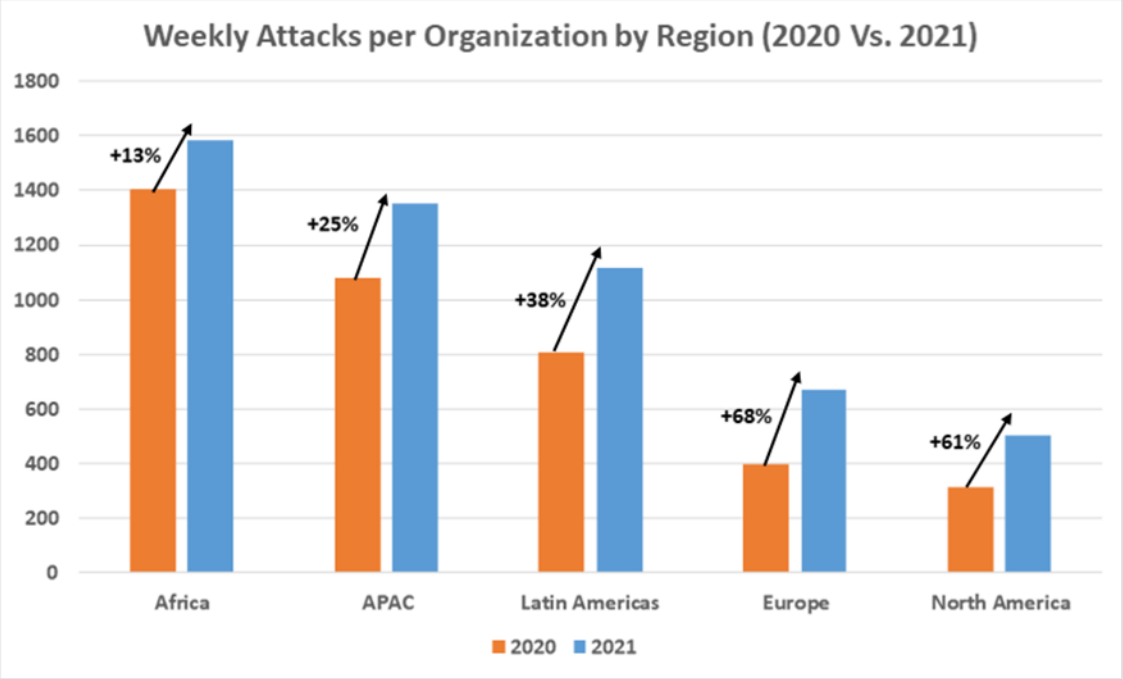
Slika 7 Globalni tjedni napadi na organizacije



Izvor: Check Point Research (2022)

Prema podacima koje je prikupio Check Point, 2021. godina je bila rekordna godina u pogledu kibernetičke sigurnosti s porastom napada od čak 50% na globalnoj razini u usporedbi s 2020. godinom, pri čemu je 1 od 61 organizacije u svijetu svaki tjedan pogođena ransomwareom.

Slika 8 Tjedni napadi na organizacije prema regijama

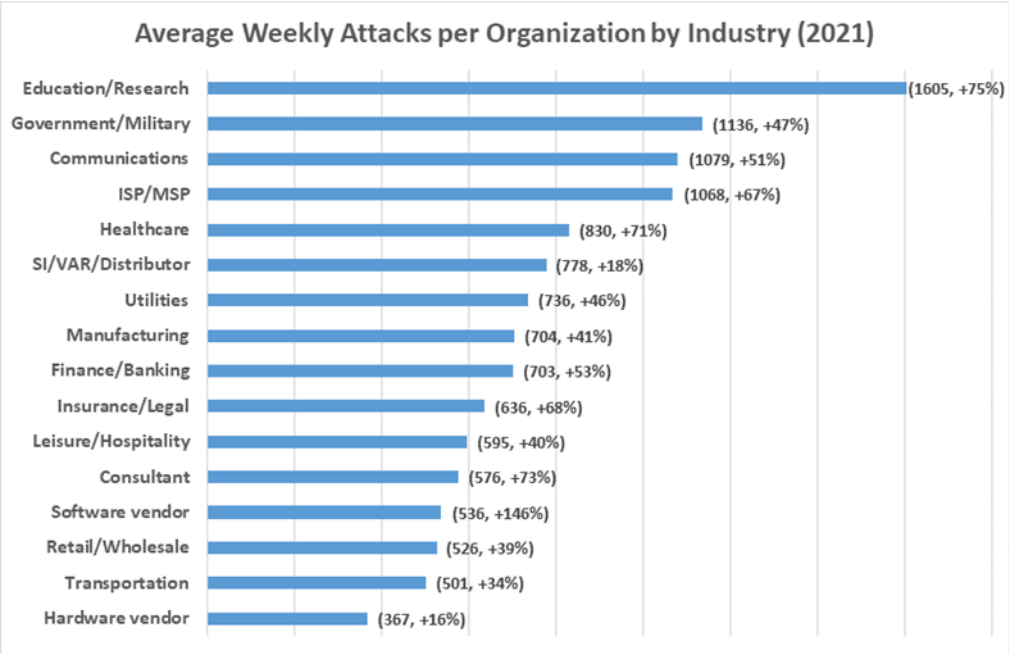


Izvor: Check Point Research (2022)

Podaci dobiveni istraživanjem grupirali su se i analizirali prema regijama. Istraživanje je pokazalo kako je Afrika je doživjela najveći broj napada u 2021. s čak 1582 tjedna napada po organizaciji te ima povećanje od 13% u odnosu na 2020. godinu. Regija APAC (Azija-Pacifik) je druga je prosjekom od 1353 tjedna napada po organizaciji 2021., što je povećanje od 25% u odnosu na 2020. Nakon toga slijedi Latinska Amerika s tjednim prosjekom od 1118 napada i Europa sa 670 tjednih napada. Iako je Sjeverna Amerika zadnja sa samo 503 napada po organizaciji tjedno, ona je imala najveći porast broja kibernetičkih napada u 2021. godini, čak 61% u odnosu na 2020. godinu.

Dodatno, podaci dobiveni istraživanjem grupirali su se prema industrijskim sektorima. U 2021. godini obrazovanje/istraživanje je bio sektor koji je doživio najveći broj napada, s prosječno 1605 napada po organizaciji svaki tjedan. To je bilo povećanje od 75% u odnosu na 2020. Slijedi vladin/vojni sektor, koji je imao 1136 napada tjedno (povećanje od 47%) i komunikacijska industrija koja je imala 1079 napada tjedno po organizaciji (povećanje od 51%).

Slika 9 Prosječni tjedni napadi na organizacije po industrijama



Izvor: Check Point Research (2022)

Check Point je utvrdio kako je jedan od najvećih izazova s kojima se suočavaju stručnjaci za sigurnost napadi Gen V koji kombiniraju širok raspon prijetnji, napada velikih razmjera i široke površine napada.

- ENISA Threat Landscape Report

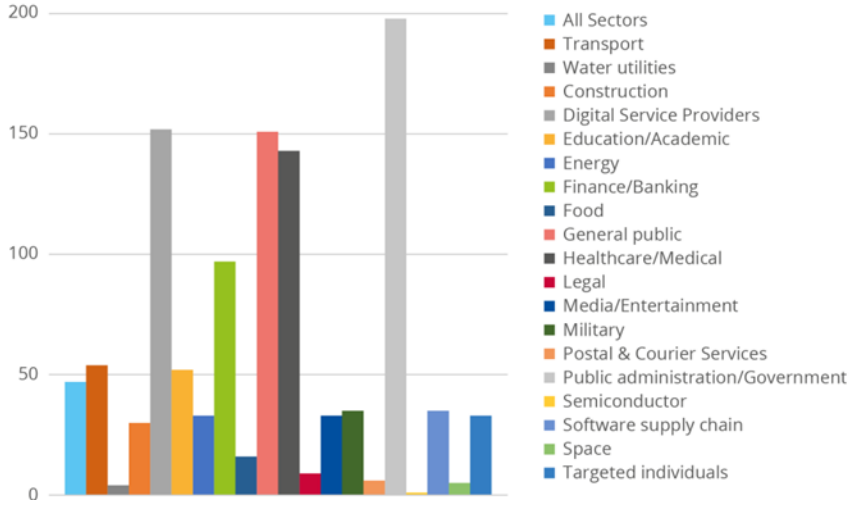
Izvješće Agencije Europske unije za kibernetičku sigurnost pod nazivom „ENISA Threat Landscape Report“ (2021) godišnje je izvješće o statusu kibernetičkih prijetnji koje identificira glavne prijetnje, trendove, tehnike napada, a također opisuje relevantne mjere ublažavanja negativnih učinaka. Vremenski raspon izvješća je od travnja 2020. do srpnja 2021. godine, a neka od najvažnijih saznanja su sljedeća:

- Primijećeni su pojačani napori vlada da ometaju i poduzimaju pravne radnje protiv prijetnji koje sponzorira država.
- Kibernetički napadi sve više ciljaju i utječu na kritične infrastrukture.
- Pojavile su se nove vrste zlonamjernog softvera poput zlonamjernog softvera bez datoteke koji se izvršava iz memorije.

- Količina napada zlonamjernog rudarenja kriptovaluta dosegla je rekordnu razinu u prvom kvartalu 2021.
- Kibernetički kriminalci su sve više motivirani monetizacijom svojih aktivnosti, a kriptovaluta je najčešći način isplate otkupnina.
- Poslovni model Phishing-as-a-Service (PhaaS) postaje sve raširenij.
- Došlo je do porasta napada povezanih sa zdravstvenim sektorom zbog pandemije i porastom potražnje za informacijama o cjepivu.. Poslovni model dezinformacije kao usluge (DaaS) znatno je porastao. Dezinformacije su omogućene umjetnom inteligencijom (AI).
- Tradicionalni DDoS (Distributed Denial of Service) napadi se fokusiraju na mobilne mreže i IoT (Internet stvari). Dijeljenje resursa u virtualnim okruženjima povećava DDoS napade.
- Tijekom 2020. i 2021. porastao je broj nezlonamjernih incidentima. Naime, zbog povećanog korištenja tehnologija tijekom rada na daljinu, broj ljudskih pogrešaka i pogrešnih konfiguracija sustava se povećao. Također, došlo je do naglog porasta nezlonamjernih sigurnosnih incidenata u oblaku.
- Ransomware se trenutno smatra najzabrinjavajućom prijetnjom. Podaci pokazuju da se prosječna otkupnina udvostručila se sa 71 000 eura na 150 000 eura u razdoblju od 2019. do 2021. godine.
- Prosječno vrijeme prekida rada napadnutih organizacija bilo je 23 dana, a napad ransomwareom dogodio se otprilike svakih 11 sekundi.
- 76% Europljana vjeruje da su suočeni sa sve većim rizikom da postanu žrtve kibernetičkog napada.

Tijekom izvještajnog razdoblja, pet sektora s najviše incidenata kibernetičke sigurnosti bili su javna uprava i vlada (198 incidenata), pružatelji digitalnih usluga (152 incidenta), opća javnost (151 incident), zdravstvo i financije (143 incidenata). Također, značajan broj incidenata bio je usmjeren na krajnje korisnike, a ne na neki određeni sektor.

Slika 10 Kibernetički napadi po sektorima



Izvor: ENISA Threat Landscape Report (2021)

2.4 Kritične infrastrukture

Osim napada na pojedince, sve su češći napadi na kritične infrastrukture jer su napadači prepoznali vrijednost ometanja njihovih sigurnosnih sustava. Kritična infrastruktura opći je izraz za fizičke i računalne sustave koji su ključni za funkcioniranje vlade i gospodarstva (Encyclopedia.com, b.d.). Napadi na kritične infrastrukture pokazali su koliko su gradovi, državne institucije i velike organizacije ranjivi te da je potrebno podizanje svijesti o rizicima.

U Republici Hrvatskoj je od 18. svibnja 2013. godine na snazi Zakon o kritičnim infrastrukturama (NN 56/13). Zakonom je definirano što se smatra kritičnom infrastrukturom te kako se njima upravlja. Dodatno, Sigurnosno-obavještajna agencija je 2019. godine uspostavila Centar za kibernetičku sigurnost s ciljem zaštite nacionalnog kibernetičkog prostora te zajedno sa Zavodom za sigurnost informacijskih sustava i razvila središnji sustav za državno sponzorirane kibernetičke napada pod nazivom SK@UT.

Prema podjeli koja je općeprihvaćena postoji 10 kritičnih infrastruktura:

1. Energetika,
2. Komunikacijska i informacijska tehnologija,
3. Promet,

4. Zdravstvo,
5. Vodno gospodarstvo,
6. Hrana,
7. Financije,
8. Proizvodnja, skladištenje i prijevoz opasnih tvari,
9. Javne službe,
10. Nacionalni spomenici i vrijednosti.

Provedeno je preliminarno istraživanje (Spremić, Šimunic, 2018) o tome kako velika poduzeća u Hrvatskoj, koja su povezane s važnom ili kritičnom nacionalnom infrastrukturom upravljaju kibernetičkom sigurnošću. Rezultati istraživanja pokazali su kako poduzeća imaju vrlo učinkovite osnovne organizacijske i tehničke kontrole, ali da svijest o kibernetičkoj sigurnosti još uvijek nije ključni dio poslovne strategije i kulture. Također, istraživanje je pokazalo kako najviši rukovoditelji i dalje pretpostavljaju da je kibernetička sigurnost isključivo odgovornost IT odjela. Poduzeća bi trebala davati više značaja kibernetičkoj sigurnosti kako bi što učinkovitije djelovala u svrhu zaštite kontinuiteta poslovanja.

3. ANALIZA KIBERNETIČKIH NAPADA NA KRITIČNE INFRASTRUKTURE

Svakodnevno se bilježi porast kibernetičkih napada na kritične infrastrukture. Prethodno se smatralo da je rizik kibernetičkih napada na kritične infrastrukture nizak zbog potrebe za specijalističkim znanjem i zbog nepostojanja odgovarajućih internetskih veza. Međusobna povezanost mnogih digitalnih tehnologija i važnih ili kritičnih infrastrukturnih sustava dovela je do stvaranja novih ranjivosti s dalekosežnim implikacijama (Spremić, Šimunic, 2018). U odlomku su analizirani kibernetički napadi na kritične infrastrukture. Gašenje kritične infrastrukture zbog kibernetičkog napada može imati značajan društveni učinak. Stoga je važno analizirati napade koji ciljaju na upravljačke sustave.

3.1 Energetika

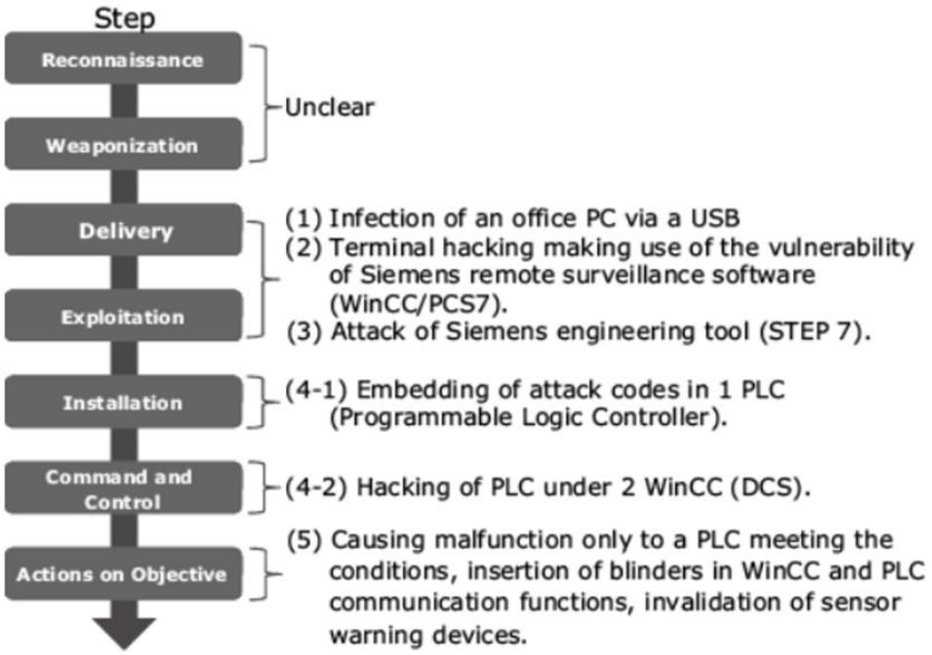
Kibernetički napadi na energetski sektor postaju sve ciljaniji i sofisticiraniji, a utjecaj kibernetičkog napada može biti razoran. Glavni čimbenici koji povećavaju ranjivost energetskog sektora su sljedeći:

- Brzi tempo tehnoloških inovacija
- Sve veća sofisticiranost kibernetičkih napada
- Privlačnost sektora kao kibernetičke mete.

Stuxnet je računalni crv, otkriven u lipnju 2010., koji je posebno stvoren za preuzimanje određenih programibilnih industrijskih kontrolnih sustava i prouzrokuje kvar opreme koju ti sustavi pokreću, cijelo vrijeme unoseći lažne podatke u monitore sustava koji pokazuju da oprema radi kako je predviđeno (Britannica, b.d.).

U siječnju 2010. godine inspektori koji su posjetili tvornicu za obogaćivanje urana primijetili su da se centrifuge kvare neviđenom brzinom. U to vrijeme nisu mogli otkriti uzrok. Nakon pet mjeseci, istraživači su pronašli zlonamjerne datoteke u jednom od sustava. 15. srpnja 2010. dogodio se DDoS napad na mailing listu za sigurnost industrijskih sustava. Ovaj napad je prekinuo bitan izvor informacija za tvornice i elektrane. Stuxnet se širio u dva vala. Prvi val bio je manje vidljiv i ciljaniji od drugog. Stuxnet je javnosti postao poznat tijekom drugog vala, koji je bio agresivniji i raširenij. Crv je uspio zaraziti više od 20.000 uređaja u 14 iranskih nuklearnih postrojenja i uništiti oko 900 centrifuga (Fruhlinger, 2017).

Slika 11 Tijek događaja napada Stuxnet-om



Izvor: NEC (2017)

Slika prikazuje faze napada uspoređujući aktivnosti napadača s vojnim akcijama. Iako metode "izviđanja" i "naoružavanja" nisu jasne, pretpostavlja se da su Sjedinjene Države bile te koje su unaprijed prikupile informacije i stvorile Stuxnet koristeći opremu nuklearnog postrojenja koja je zaplijenjena u Libiji. Karakteristike ovog napada uključuju iskorištavanje ranjivosti univerzalne kontrolne opreme i "zataškavanje komunikacije za skrivanje napada i onesposobljavanje uređaja za upozorenje" (Noguchi, Ueda, 2017).

Iako nijedna država nije službeno priznala stvaranje Stuxneta, vjeruje se da su SAD i Izrael zajednički razvili crv. Stuxnet je bio prvi virus koji je izazvao fizičko uništenje zaraženih uređaja. To je ozbiljno naštetilo iranskom nuklearnom programu.

Stuxnet je najvjerojatnije prenijet preko USB stickova koje su agenti nosili unutar objekata. Nakon prodiranja u Windows sustave, Stuxnet inficira datoteke koje pripadaju Siemensovim industrijskim softverskim aplikacijama i prekida njihovu komunikaciju. Kada zarazi računalo, provjerava je li to računalo spojeno na određene modele programibilnih logičkih kontrolera (PLC) koje proizvodi Siemens. PLC-ovi su način na koji računala komuniciraju s industrijskim strojevima kao što su centrifuge za uran i upravljaju njima (Fruhlinger, 2017). Crv zatim mijenja programiranje PLC-a,

što dovodi do toga da se centrifuge okreću prebrzo i predugo, oštećujući ili uništavajući osjetljivu opremu u procesu. Dok se to događa, PLC-ovi govore upravljačkom računalu da sve radi dobro, što otežava otkrivanje ili dijagnosticiranje što nije u redu dok ne bude prekasno. Stuxnet također sadrži rootkit koji sakriva crva od nadzornih sustava.

Stuxnet se nikad nije namjeravao proširiti izvan iranskog nuklearnog postrojenja u Natanzu. Objekt je bio prozračen i nije bio spojen na internet. Međutim, zlonamjerni softver završio je na računalima povezanim s internetom i počeo se širiti u divljini zbog svoje izuzetno sofisticirane i agresivne prirode, iako je napravio malu štetu vanjskim računalima koja je zarazio.

Kako bi se poduzeća zaštitila od Stuxneta preporuča se korištenje vatrozida i popisa dopuštenih aplikacija za filtriranje mreže od zlonamjernih aktera, pažljivo nadziranje aktivnosti na mreži i održavanje strogih pravila za prijenosne medije.

3.2 Komunikacijska i informacijska tehnologija

15. srpnja 2020. godine napadnuta je društvena mreža Twitter. Napad je trajao 24 sata, a napadač je bio 17-godišnjak i njegovi suučesnici te su preuzeli kontrolu nad računima korisnika od visoke važnosti (računi političara, slavnih osoba i poduzetnika, kompanija za kriptovalute). U izvješću Ministarstva financijskih usluga države New York (2020) detaljno je opisan tijek napada i njegove posljedice.

Značajno je da napad nije uključivalo niti jednu od visokotehnoloških ili sofisticiranih tehnika koje se često koriste u kibernetičkim napadima – bez zlonamjernog softvera, bez eksploatacija i bez stražnjih vrata. Hakeri su se prilikom telefonskih poziva pretvarali da su iz Twitterovog odjela za informacijsku tehnologiju. Ova vrsta napada naziva se vhishing i spada u društveni inženjering. Društveni inženjering (engl. social engineering) se odnosi na navođenje ili manipuliranje osobama kako bi otkrili što je moguće više podataka o sebi (Spremić, 2017).

Napad se dogodio u tri faze:

1. napadi društvenog inženjeringa za dobivanje pristupa Twitterovoj mreži
2. preuzimanje računa s poželjnim korisničkim imenima i prodaja pristupa
3. preuzimanje desetaka Twitter računa visokog profila i pokušaj prevare ljudi da hakerima pošalju bitcoin.

Prema izvješću Ministarstva financijskih usluga države New York (2020), u novčanoj vrijednosti, hakeri su ukrali bitcoine u vrijednosti od preko 118.000 USD. Ukupno je 130 korisničkih računa ugroženo , a od toga je 45 računa korišteno za objavljivanje tweetova. Za sedam neverificiranih Twitter računa, hakeri su također preuzeli informacije o računu putem Twitterovog alata "Vaši podaci s Twittera" ("YTD"), koji daje sažetak detalja i aktivnosti Twitter računa (Department of Financial Services, 2020). Nakon što su hakeri preuzeli kontrolu nad Twitter računima kompanija za kriptovalute, kompanije su reagirale u roku od nekoliko minuta i blokirale transakcije između bitcoin adresa kupaca i hakera.

Twitter je prvi put postao svjestan ovog napada kada je nekoliko zaposlenika prijavilo sumnjive prijave i telefonske pozive ujutro 15. srpnja 2020. godine nakon čega je objavio kako je pod napadom i da poduzimaju korake kako bi se sustavi oporavili. Stavili su zabranu objava mnogim verificiranim računima, te im je bilo onemogućeno mijenjanje lozinki ili im se čak korisnički račun zaključao. Zaposlenicima je bio zabranjen pristup svim sustavima kako se napad ne bi proširio. Također je pokrenuo proces verifikacije tijekom kojeg je svaki zaposlenik Twittera morao prisustvovati videokonferenciji s nadređenim i promijeniti svoje lozinke pred nadređenim (Thompson, Barrett, 2020).

Uspjeh hakera u velikoj je mjeri bio rezultat slabosti u kibernetičkoj sigurnosti. Twitter nije imao glavnog službenika za informacijsku sigurnost (CISO) od prosinca 2019., a zbog pandemije je prešao na rad na daljinu što je stvorilo još više ranjivosti. Iako je Twitter imao određene kontrole pristupa, one nisu bile dovoljne da spriječe napad. Zaposlenici su prva linija obrane te je potrebno osigurati da budu svjesni prijetnji i rizika rada na daljinu. Također, napad se mogao izbjeći da su se pratile mrežne aktivnosti. Sigurnosni timovi trebaju koristiti sustav za praćenje mrežnih aktivnosti i praćenje upozorenja o prijetnjama i razviti procese za prikupljanje i analizu sigurnosnih informacija. Kibernetički napad na Twitteru pokazuje potrebu za snažnom kibernetičkom sigurnošću svih društvenih medija jer pogreške u kibernetičkoj sigurnosti mogu imati ozbiljne posljedice.

3.3 Promet

Ministarstvo prometa u Coloradu (CDOT) bilo je žrtva dvaju napada 2018. godine. U veljači je izveden prvi napad SamSam ransomware-om na Ministarstvo prometa u Coloradu (CDOT) koji je zahvatio otprilike polovicu računala u CDOT-u. Iako je Ministarstvo zajedno s Uredom guvernera za internetsku tehnologiju odmah odgovorilo na napad, u ožujku iste godine napadači su izveli još jedan napad koji je bio rizičan i za druge državne resurse. Nakon navedenih napada osnovana je Ujedinjena zapovjedna skupina (UCG) za definiranje smjernica i kontrola prilikom incidenata koja je imala važnu ulogu u rješavanju problema.

SamSam ransomware korišten u ovom incidentu prvi put se pojavio 2016. godine i korišten je samo u ciljanim napadima te se u prošlosti širio putem protokola udaljene radne površine (eng. Remote Desktop Protocol, dalje u tekstu „RDP“). RDP je siguran mrežni komunikacijski protokol koji omogućuje mrežnim administratorima da daljinski dijagnosticiraju probleme s kojima se pojedinačni korisnici susreću i daje korisnicima daljinski pristup njihovim fizičkim radnim stolnim računalima (Chai, Posey, 2022). Napadači skeniraju Internet u potrazi za računalima s otvorenim RDP vezama i probijaju se u velike mreže i šire na još više računala. Nakon što imaju dovoljno jaku prisutnost na mreži, napadači postavljaju ransomware SamSam i čekaju da napadnuta organizacija plati otkupninu ili im brišu podatke. Kao što je objašnjeno u poglavlju 2.2 Kibernetički rizik, glavni cilj napada ransomware-om je dobiti otkupninu za napadnute podatke i sustave, te je najčešća valuta plaćanja bitcoin

Colorado je bio prisiljen proglasiti prvo izvanredno stanje u povijesti zbog kibernetičkog incidenta. Debbi Blyth (2020), državna službenica za informacijsku sigurnost, rekla je kako je bilo bitno proglasiti izvanredno stanje kako bi se omogućilo surađivanje s Državnim uredom za upravljanje hitnim situacijama i Nacionalnom gardom Colorada. Kako bi se pronašlo rješenje, sastanci su se održavali dva puta puta dnevno te su na njima sudjelovali Ured za hitne slučajeve, državni fuzijski centar Colorada, Guvernerov ured za informacijsku tehnologiju, US-CERT, Ministarstvo domovinske sigurnosti, Savezna agencija za upravljanje hitnim situacijama i FBI, zajedno s četiri neimenovana dobavljača sigurnosnih usluga i tvrtka za odgovor na incidente. Više od 130 ljudi bilo je uključeno u intervenciju i oporavak, a mnogi od njih radili su 18 sati dnevno. Sigurnosni službenici ugasili su više od 2000 računala zaposlenika dok su istraživali napad, a u međuvremenu, zaposlenicima je zabranjen pristup internetu dok se problem ne riješi. Dva tjedna utrošena su na

uklanjanje svih prijetnji i uklanjanje zlonamjernog softvera, a još dva tjedna na vraćanje sustava i usluga, što je koštalo ukupno 1,7 milijuna dolara (Wright, 2020). Manje od devet mjeseci nakon incidenta, Ministarstvo pravosuđa optužilo je dvojicu osumnjičenika povezanih s napadima.

Utvrđeno je kako je glavni uzrok bila ranjivost nastala zbog novog internetskog virtualnog poslužiteljem s izravnom vezom izravno na mrežu koji je bio pogrešno konfiguriran te administrativne privilegije za koje nisu postojale odgovarajuće kontrole. Sustav je trebao biti poslužitelj za kratkoročno testiranje, ali kako standardne sigurnosne kontrole nisu primijenjene poslužitelj je bio ugrožen u roku od dva dana od stvaranja. SamSam ransomware je pogodio Windows OS računala iako su bila zaštićena McAfee antivirusom.

Iako je ovaj napad imao vrlo jak utjecaj na poslovanje Ministarstva prometa u Coloradu neke preventivne aktivnosti koje su se provodile spriječile su nastanak veće štete. Naime, Ministarstvo prometa je redovito pohranjivalo podatke i stvaralo sigurnosne kopije te je zahvaljujući tome izbjeglo plaćanje otkupnine. Osim redovitih sigurnosnih kopija CDOT - ova mrežna segmentacija ograničila je sposobnost napadača šire ransomware na kritična područja poput sustava za kontrolu prometa (Chuang, 2020). Mrežna segmentacija omogućila je izolaciju zlonamjernog softvera unutar jednog odjela. Iako su učinci na CDOT bili značajni, ova je segmentacija izravno pridonijela obuzdavanju zlonamjernog softvera i spriječila širenje kroz Colorado State Network (CSN). Dok su sustavi CDOT-a bili pod napadom, operativni poslovi su se nastavili izvršavati zbog definiranog Plana kontinuiteta poslovanja. Međutim, plan nije bio operativan koliko je mogao biti i nije se uvježbavao dovoljno često da bi se omogućila pouzdana primjena plana. Kao rezultat toga, nije postojao sustavan pristup eskalirajućem incidentu. Napad se mogao spriječiti pravovremenom implementacijom alata i softvera za sigurnosnu analitiku i otkrivanje koji je bio kupljen. Da je skup alata bio u potpunosti implementiran, ranije bi upozorio na napad i možda ga u potpunosti spriječio.

Napad ransomware-a SamSam na Ministarstvo prometa Colorada u konačnici je ojačao državni program kibernetičke sigurnosti uključujući zatvaranje instanci Microsoftovog protokola za udaljenu radnu površinu koje su bile otvorene za internet i uvođenje dvofaktorske autentifikacije za sve privilegirane račune, te je vjerojatno spriječio ponovne napade.

3.4 Zdravstvo

U rujnu 2020. godine u Njemačkoj je zabilježena prva smrt koja je izravno povezana s kibernetičkim napadom. Žena je umrla tijekom ransomware napada na Sveučilišnu bolnicu u Düsseldorfu. Ransomware je napao 30 poslužitelja u Sveučilišnoj bolnici u Düsseldorfu, srušivši sustave te je prisilio bolnicu da odbije hitne pacijente. Kao rezultat toga žena u životnoj opasnosti poslana je u bolnicu udaljenu 32 km u Wuppertalu i umrla je zbog kašnjenja u liječenju (Ralston, 2020). Naime, napad nije bio namijenjen bolnici već je otkupnina upućena na obližnje sveučilište. Policija u Düsseldorfu kontaktirala je napadače putem poruke za otkupninu kako bi objasnila da je pogođena bolnica, a ne sveučilište, te da dovode u opasnost zdravlje pacijenata. Napadači su zaustavili napad i otključali podatke. Nije jasno jesu li kibernetički kriminalci namjeravali uzeti sustave Sveučilišne bolnice Düsseldorf za taoce ili je bolnica bila kolateralna šteta u napadu na sveučilište. Zahtjev za otkupninom je upućen Sveučilištu Heinrich Heine, koje je povezano s bolnicom, a ne samoj bolnici.

Napadači su provalili u bolnicu koristeći rupu u softveru Citrix. Budući da bolnica nije uspjela ažurirati svoj softver, kibernetički kriminalci su mogli iskoristiti nedostatak za provalu i šifriranje podataka.

Njemačke vlasti još uvijek istražuju smrt ove žene. Ako se utvrdi da je njezino preusmjeravanje u drugu bolnicu odgovorno za njezinu smrt, policija bi taj kibernetički napad mogao tretirati kao ubojstvo. Tužitelji spremaju tužbu pod pretpostavkom da se napad može identificirati kao ubojstvo iz nehaja koje se definira kao ubojstvo druge osobe iz nemara ili bez zlobe. Kako bi uspjeli u tome, trebali bi utvrditi pravnu uzročnost tj. da su napad i odgoda u liječenju koje je izazvana, dovoljno pridonijeli smrtnosti (Ralston, 2020).

Stručnjaci za kibernetičku sigurnost se nadaju da će smrt od napada na ransomware biti poziv na buđenje regulatorima i IT administratorima da je potrebno učiniti više kako bi spriječili i odvratili kibernetičke napade.

3.5 Vodno gospodarstvo

Izraelski vodovodni sustav pod stalnim je kibernetičkim napadima te je izraelska uprava za vodu potpisala ugovor o zaštiti vodne infrastrukture s poduzećem za kibernetičku sigurnost SIGA OT Solutions da zaštiti svoju infrastrukturu nakon napada.

U travnju 2020. godine je šest objekata Uprave za vodu bilo meta kibernetičkog napada. Napadači su pokušali povećati količinu klora u opskrbi vodom koja teče u stambena područja te bi stotine ljudi bile u opasnosti da se razbole. Također, postojala je šansa da bi napad aktivirao sigurnosni sustav, isključio crpke i ostavio tisuće bez vode tijekom ozbiljnog toplinskog vala (Staff, 2020). Da je uspjelo, to bi izazvalo velike zdravstvene probleme svima koji su pili vodu, kao i ozbiljno naštetilo poljoprivrednoj industriji. Ovaj napad dogodio se jer su napadači provalili u programibilne logičke kontrolere (PLC) i preuzeli kontrolu nad opskrbom vodom. Zaposlenici u postrojenju za vodu otkrili su promjenu u razinama klora u vodi i brzo su upozorili izraelsku agenciju za kibernetičku sigurnost. Nakon upada, Izraelska nacionalna kibernetička uprava i Uprava za vodu poslali su upozorenje u kojem pozivaju postrojenja za pročišćavanje vode da promijene lozinke svoje opreme povezane s internetom s naglaskom na operativne sustave i uređaje za kontrolu klora.

Izraelski dužnosnici nikada nisu pripisali napad u travnju, ali Washington Post objavio je da je upad bio povezan s Iranom pozivajući se na strane obavještajne službe (Warrick, Nakashima, 2020).

U lipnju 2020. godine dogodila su se dva napada koja nisu nanijela ozbiljnu štetu vodovodnom sustavu. Prvi napad pogodio je pumpe za poljoprivrednu vodu u gornjoj Galileji, dok je drugi napad pogodio pumpe za vodu u središnjoj pokrajini Mateh Yehuda. Radilo se o specifičnim, malim instalacijama odvodnje u poljoprivrednom sektoru koje su mještani odmah sanirali, bez ikakvih šteta ili bilo kakvih stvarnih posljedica (Staff, 2020). Napadači su hakirali softver koji pokreće crpke nakon usmjeravanja preko američkih i europskih poslužitelja kako bi sakrili izvor.

1.prosinca 2020. iranski napadač je objavio video proboja u HMI sustav izraelskog rezervoara za otpadnu vodu. HMI sustav rezervoara bio je povezan izravno s internetom, bez ikakvog sigurnosnog uređaja koji bi ga branio ili ograničavao pristup, a u vrijeme objave sustav nije koristio niti jednu metodu autentifikacije prilikom pristupa. To je napadačima dalo jednostavan pristup sustavu i mogućnost izmjene bilo koje vrijednosti u sustavu. Sve što je protivnicima bilo potrebno

bila je veza sa mrežom i web preglednik. Kao odgovor na napad, od 2. prosinca 2020. HMI web aplikacija zahtijeva autentifikaciju za pristup sustavu. Međutim, sustav je i dalje dostupan putem interneta bez ikakvih prepreka. Također, sustav još uvijek dopušta komunikaciju za koju se koristi za Modbus/TCP protokol koji ne zahtijeva nikakvu provjeru autentičnosti/šifriranje. Glavni razlog zbog kojeg je rezervoar bio meta to što je omogućio lak, nezaštićen pristup.

Ovi slučajevi naglašavaju potrebu za odgovarajućom kibernetičkom zaštitom na infrastrukturi u područjima koja su u sukobima jer su stalno na meti.

3.6 Prehrana

U ožujku 2021. američko poduzeće za proizvodnju pića, Molson Coors, pretrpjelo je napad ransomwareom koji je prouzročio značajne poremećaje u njegovom poslovanju, uključujući poslovanje, proizvodnju i otpremu. Napadači ransomwareom traže ranjivosti sustava kako bi ušli u mrežu i onda se šire, stoga je poduzeće isključilo svoje sustave kako bi spriječili daljnje širenje zlonamjernog softvera, izravno utječući na zaposlenike koji nisu mogli pristupiti određenim sustavima. Napad je doveo do kašnjenja i prekida u radu, proizvodnji i isporuci.

Nakon što su otkrili prijetnju, aktivirali su plan odgovora na incidente i komunicirali sa zaposlenicima i poslovnim partnerima o problemu. Također, angažirali su vodeće forenzičke IT stručnjake i pravne savjetnike kako bi identificirali glavni uzrok. Otvorena je i policijska istraga te su obaviještena sva relevantna osiguravajuća društva (Hope, 2021). Međutim, nijedna ransomware skupina nije preuzela odgovornost za kibernetički napad niti je zatražila otkupninu. Napadači često šute odmah nakon napada kako bi povećali vjerojatnost suradnje žrtve. Tišina im također donosi veću moć jer mnoge žrtve pokušavaju prikriti incident kako bi izbjegle štetu reputaciji povezanu s napadima ransomwarea. Nakon obmanjivanja vlasti i javnosti, organizacije bi mogle pretrpjeti daljnju štetu po ugledu i moguće pravne posljedice ako odbiju platiti otkupninu.

Ovo je primjer kako napadači ciljaju organizacije visokog profila kako bi prekinuli ključne operacije poslovanja. Za proizvodne organizacije, ransomware predstavlja veliku prijetnju podacima i dostupnosti sustava. Kao što je navedeno u poglavlju 2.2. Kibernetički rizik, ovakvim napadom gubi se pristup podacima, ali se i sustavi koji upravljaju proizvodnim procesom mogu zaustaviti, sprječavajući uspješnu proizvodnju, pa čak i isporuku proizvoda. Ransomware napadi na proizvodne tvrtke mogli bi biti razorni jer bi mali prekid u proizvodnji mogao biti katastrofalan

za druge tvrtke u opskrbnom lancu. Prema Edgardu Capdevielleu (2021), izvršnom direktoru tvrtke Nozomi Networks, napadi visokog profila postaju prečesti jer su napadači shvatili da su neizmjerno profitabilniji kada ciljaju velike organizacije i ometaju njihove kritične poslovne operacije.

Glavni cilj oporavka je bio što prije početi sa ponovnom proizvodnjom te su u ostvarili značajan napredak u obnavljanju sustava i sve pivovare su mogle ponovno proizvoditi i isporučivati proizvode.

Kako bi se poduzeće oporavilo od napada i smanjilo mogućnost ponovnih incidenata uvelo je promjene kao što su snažna segmentacija, obuka korisnika, proaktivni programi kibernetičke higijene, multi faktorska provjera autentičnosti i upotreba stalno ažuriranih podataka o prijetnjama za zaštitu IT i operativnih okruženja od ransomwarea i drugih kibernetičkih napada. Poduzeće Molson Coors je napravilo je značajan napredak u informacijskim sustavima zbog kibernetičkog napada i unaprijedilo svoju kibernetičku sigurnost.

3.7 Financije

U 2017. napadači su iz američke multinacionalne agencije za izvještavanje o potrošačkim kreditima, Equifax, izvukli stotine milijuna podataka o klijentima. Agencija je prvotno napadnuta putem web portala za pritužbe potrošača, a napadači su koristili opće poznatu ranjivost koja je trebala biti zakrpana, ali nije zbog kvarova u internim procesima Equifaxa. Napadači su se mogli pomaknuti s web portala na druge poslužitelje jer sustavi nisu bili adekvatno segmentirani jedan od drugoga, a mogli su pronaći korisnička imena i lozinke pohranjene u običnom tekstu koji im je omogućio pristup daljnjim sustavima (Fruhlinger, 2020). Od svibnja do srpnja 2017. napadači su uspjeli dobiti pristup višestrukim bazama podataka Equifaxa koje sadrže informacije o stotinama milijuna ljudi. Poput mnogih kibernetičkih lopova, Equifaxovi napadači šifrirali su podatke koje su premještali kako bi ih administratori teže uočili; kao i mnoga velika poduzeća, Equifax je imao alate koji su dešifrirali, analizirali i zatim ponovno šifrirali interni mrežni promet, posebno kako bi nanjušili događaje krađe podataka kao što je ovaj. Ali kako bi ponovno šifrirali taj promet, ovi alati trebaju certifikat javnog ključa koji se kupuje od trećih strana i mora se obnavljati svake godine (Fruhlinger, 2020). Equifax nije uspio obnoviti jedan od svojih certifikata prije gotovo 10 mjeseci što je značilo da se šifrirani promet ne provjerava. Equifax nije objavio kršenje do više od mjesec dana nakon što su otkrili da se dogodilo; prodaja dionica od strane najviših rukovoditelja otprilike u to vrijeme dovela je do optužbi za trgovanje povlaštenim informacijama.

Equifax posluje s osobnim podacima, tako da su informacije koje su napadači kompromitirali i odnijeli bile prilično detaljne i pokrivale su ogroman broj ljudi. Potencijalno je pogodio 143 milijuna ljudi čija su imena, adrese, datumi rođenja, brojevi socijalnog osiguranja i brojevi vozačkih dozvola bili izloženi. Mali podskup zapisa (oko 200 000) također je uključivao brojeve kreditnih kartica. Čim objavljen napad, stručnjaci su počeli nadzirati dark web stranice, čekajući goleme količine podataka koji bi mogli biti povezani s njima, ali podaci nisu objavljeni. Zbog toga se smatra da je napad bio sponzoriran od kineske države čija je svrha bila špijunaža, a ne krađa. U veljači 2020. Ministarstvo pravosuđa Sjedinjenih Država službeno je optužilo četiri pripadnika kineske vojske za napad.

Povredu Equifaxa istraživalo je nekoliko saveznih tijela, uključujući FBI, FTC i CFPB. Komisija za vrijednosne papire i burzu (SEC) i Ured američkog državnog odvjetnika u Atlanti proveli su dodatnu istragu trgovanja povlaštenim informacijama u vezi s prodajom dionica Equifaxa u vrijednosti od 2 milijuna dolara od strane rukovoditelja nakon otkrića kršenja (Fruhlinger, 2020). Povredu je također istražio Stalni istražni pododbor za domovinsku sigurnost (PSI), pododbor odgovoran za istraživanje vladinih operacija, usklađenosti s propisima i zakonima te slučajeva kriminala i prijevare koji prijete nacionalnoj dobrobiti (HSGAC).

Equifax se suočio s tužbama lokalnih i državnih vlasti. U 2019. bivša direktorica informiranja Jun Ying proglašena je krivom za trgovanje povlaštenim informacijama i osuđena na četiri mjeseca zatvora. Bivši menadžer Equifaxa Sudhakar Reddy Bonthu također je proglašen krivim za trgovanje povlaštenim informacijama i osuđen na 8 mjeseci kućnog zatvora.

U srpnju 2019., u nagodbi s FTC-om, Uredom za financijsku zaštitu potrošača, 48 država, Distriktom Columbia i Portorikom, Equifax je pristao platiti do 700 milijuna dolara kazni i odštete za 147 milijuna pogođenih pojedinaca. 300 milijuna dolara od nagodbe podijeljeno je pojedincima čiji su osobni podaci bili izloženi tijekom kršenja. Equifax je također trebao platiti do 125 milijuna dolara naknade potrošačima za dodatne gubitke (Fruhlinger, 2020).

Kako bi se riješili nedostaci u kibernetičkoj sigurnosti Equifaxa, FTC je također zahtijevao od Equifaxa da uspostavi sveobuhvatan program informacijske sigurnosti koji bi uključivao godišnje procjene unutarnjih i vanjskih sigurnosnih rizika i osiguravao da pružatelji usluga s pristupom osobnim podacima koje pohranjuje Equifax također implementiraju odgovarajuće sigurnosne programe.

3.8 Proizvodnja, skladištenje i prijevoz opasnih tvari

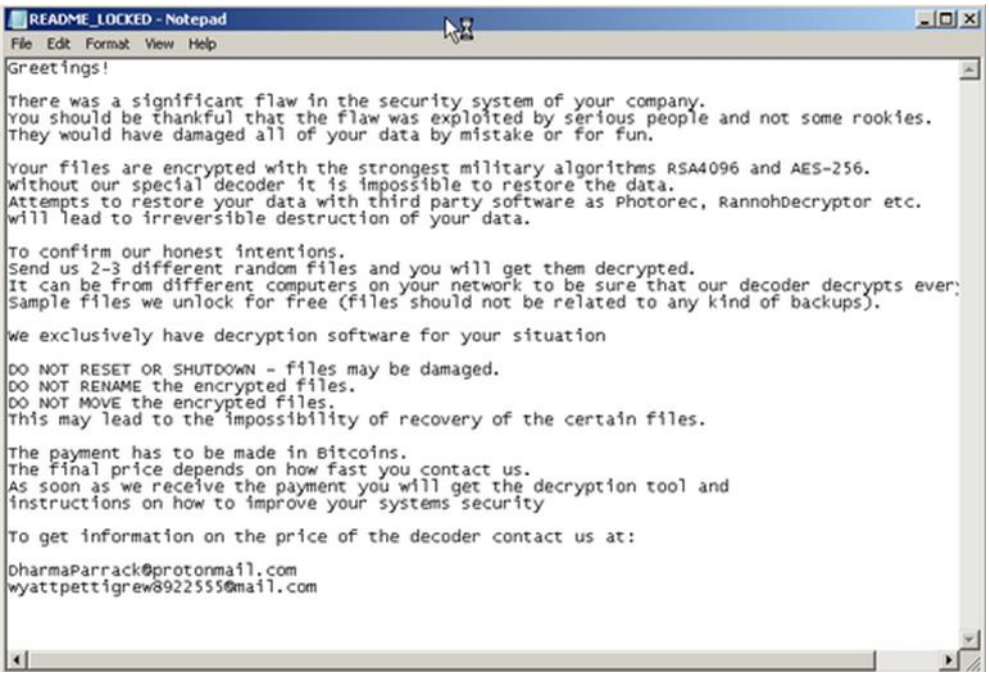
Norsk Hydro je jedan od najvećih proizvođača aluminija u svijetu i poduzeće za proizvodnju obnovljive energije. U 2019. godini poduzeće je napadnuto LockerGoga ransomware-om. LockerGoga je zlonamjerni ransomware program koji je napravljen za šifriranje podataka pohranjenih na računalima i za ucjenjivanje korisnika traženjem otkupnine u zamjenu za alate za dešifriranje (Beaumont, 2019).

Pretpostavlja se da je za širenje virusa iskorišten Aktivni Direktorij. Napadači su dobili pristup oko 2-3 tjedna prije napada. Te su oko ponoći u utorak, 19. ožujka, otkriveni sigurnosni napadi. Nakon što su dobili pristup mreži, iskoristili su prava administratora domene da izvrše napad te su stavili izvršnu datoteku negdje gdje svaki sustav u organizaciji može doseći, Aktivni Direktorij. Također, LockerGoga mijenja svaku zaporku lokalnih administratorskih računa i nakon toga nije moguća prijava za oporavak sustava jer podaci o administratorima nisu točni te dolazi do odjave. Na prijenosnim i stolnim računalima moguće je ponovna prijava pomoću korisničkih računa domene u predmemoriji, no sve što korisnik može učiniti je pročitati poruku o otkupnini. Budući da je postavljen kao administrator napadač ima punu kontrolu nad svim datotekama. To je omogućilo korištenje grupnih pravila kao što je planirano stvaranje zadatka ili stvaranje usluge za automatsko pokretanje izvršne datoteke LockerGoga. Svako prijenosno računalo, stolno računalo i poslužitelj spojen na Aktivni Direktorij odmah pokreće zlonamjerni softver. Do jutra je Nord Hydro odlučio isključiti svoju mrežu. Kako bi se spriječilo širenje virusa na ostale dijelove infrastrukture, poduzeće je prekinulo kontakt s računalnim sustavima i stoga je morao tvornički komunicirati telefonom i održavati rad ručno. Obavijestili su burze da prelaze na ručnu proizvodnju, što znači da će upravljati tvornicama bez moderne informatike. Svaki upravitelj lokalne tvornice imao je zadatak održavati narudžbe kupaca.

Svaki pogođeni sustav imao je četiri ključna elementa:

- Svi su pokretali Microsoft Windows.
- Datoteke, uključujući neke sistemske datoteke, bile su šifrirane.
- Mrežno sučelje na svakom sustavu bilo je onemogućeno.
- Lokalni korisnički računi na svakom sustavu promijenili su lozinku (Beaumont, 2019).

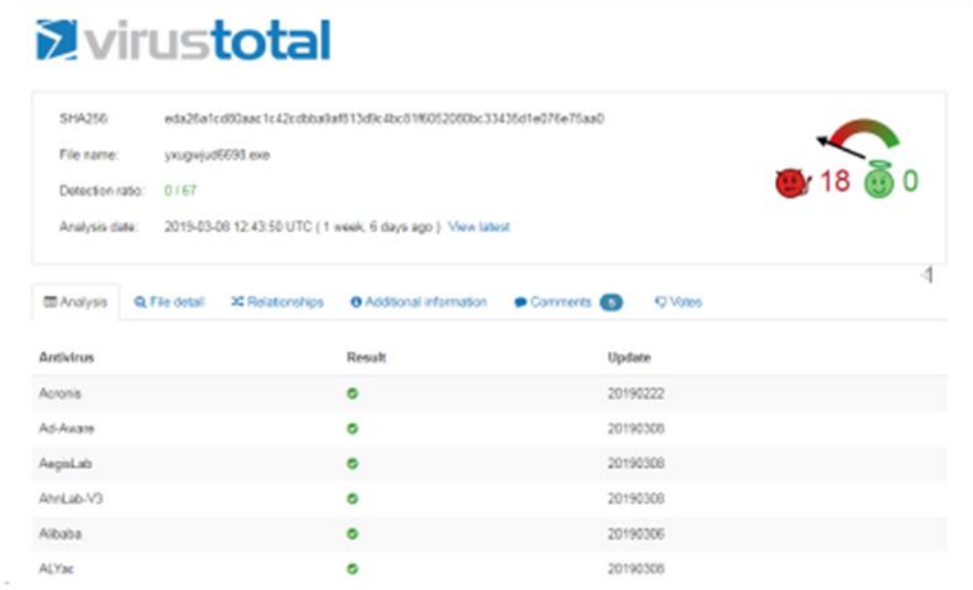
Slika 12 LockerGoga poruka za otkupninu



Izvor: DoublePulsar (2019)

Datoteka README navodi da su iskoristili značajan propust u sigurnosti sustava i kriptirali sve podatke koristeći RSA-4096 i AES-256 kriptografske algoritme. Svakoj šifriranoj datoteci LockerGoga dodaje ".locked!?" ili ".locked". Datoteka "1.pdf" na primjer postaje "1.pdf.locked!?" ili "1.pdf.locked". Kao dokaz da im se može vjerovati i da imaju alat sposoban za dešifriranje, žele da žrtve pošalju dvije ili tri datoteke za besplatno dešifriranje (Beaumont, 2019).

Slika 13 Nadzorna ploča Virus Total



Izvor: DoublePulsar (2019)

LockerGoga nema kod za samoširenje, što znači da se ne može sam replicirati po mreži za razliku od drugih destruktivnih kodova kao što su WannaCry i NotPetya. To zapravo može biti namjerno budući da ne koristi C2 (eng. Command and Control) poslužitelje i DNS promet, to znači da je manja vjerojatnost da će ga prepoznati i alati za otkrivanje mreže i klasifikaciju krajnjih točaka (Trend Micro, 2019). Nadzorna ploča Virus Total pokazuje da je je stopa otkrivanja bila 0 od 67 antivirusnih točaka. To znači da je Nord Hydro imao nultu detekciju što je izuzetno loš znak jer anti-malware rješenje nije otkrilo prijetnju.

Prema početnoj financijskoj procjeni ransomware je prouzročio gubitak od 30 do 40 milijuna dolara. Norsk Hydro nije platio novac napadačima. Tvrtka je vraćala sustave pomoću sigurnosnih kopija. Na oporavku i rješavanju problema radio je tim iz Microsoft-a i neimenovanih tvrtki te su surađivali s nacionalnim tijelima za kibernetički kriminal i policijom.

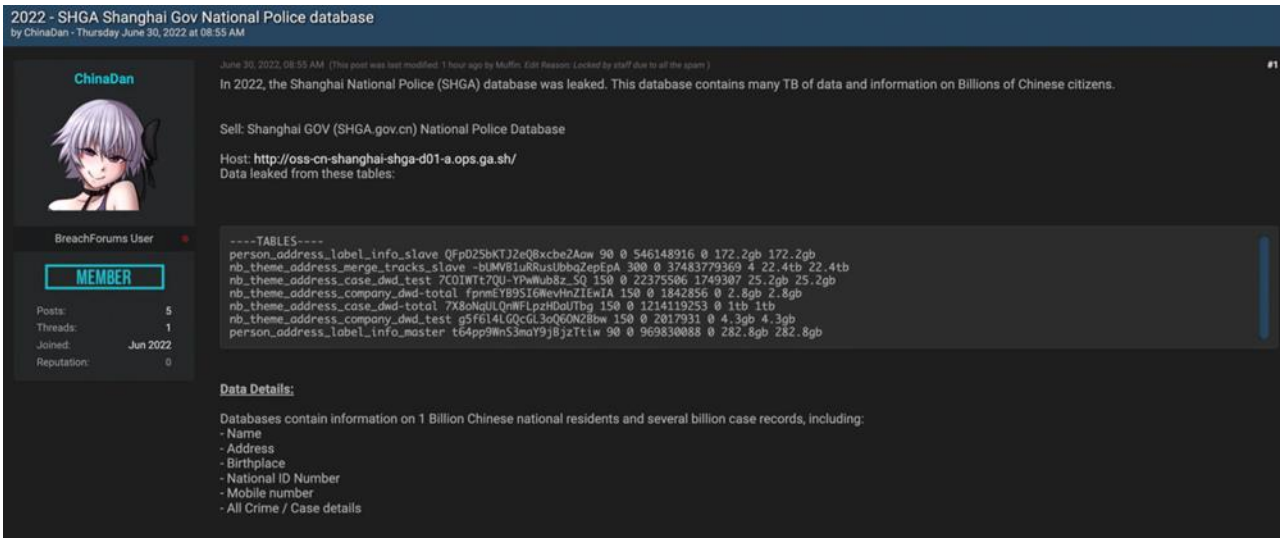
Nord Hydro je imao vrlo dobar plan za predstavljanje incidenta, Imali su privremenu web stranicu, objavili su široj javnosti, svim zaposlenicima i nisu skrivali nikakve detalje te su čak imali dnevne internetske prijenose s Upravom., a čak su odgovarali na pitanja gledatelja. Za razliku od nekih drugih incidenata, njihova je cijena dionica zapravo porasla zbog transparentnosti.

Osim kod napada na Nord Hydro, LockerGoga pojavio se u još nekoliko napada. Jedna od prvih poznatih žrtava LockerGoga bila je francuska inženjerska konzultantska tvrtka Altran Technologies, a napadnuta su i kemijska poduzeća Hexion i Momentive. Nakon napada, poduzeća Hexion i Momentive su objavila kako rade na ponovnom uspostavljanju mreža i normalnog rada nakon što su pretrpjeli mrežne sigurnosne incidente koji su spriječili pristup određenim IT sustavima i podacima. Incident je prisilio poduzeće da naruči stotine novih računala i da nekim zaposlenicima otvori nove račune e-pošte jer su njihovi stari postali nedostupni. Hexion i Momentive su u vlasništvu iste grupe investitora pa je moguće da su njihovi sustavi povezani i da je tako virus prešao iz jedne organizacije u drugu. Stručnjak za sigurnost Kevin Beaumont (2019), koji je pratio napade LockerGoga, rekao je da je na temelju broja jedinstvenih uzoraka zlonamjernog softvera pogođeno najmanje osam organizacija.

3.9 Javne službe

30. lipnja 2022. godine na hakerskom forumu, BreachForum, je osoba pod imenom ChinaDan postavila ponudu za prodaju skupa podataka od 23,88 terabajta koji navodno sadrži milijardu osobnih podataka stanovnika Kine za cijenu od 10 bitcoina što je otprilike $200.000. ChinaDan je naveo kako su podaci nabavljeni sa servera Šangajske nacionalne policije te da sadrže imena, adrese, mjesto rođenja i datume rođenja, nacionalne osobne brojeve, brojeve mobitela i još mnogo toga. Na forumu je također objavljen dio tih podataka (750.000) te su novinari Rachel Cheung iz VICE World Newsa i Karen Hao iz Wall Street Journala nazvali pojedince čiji su podaci objavljeni te su utvrdili da su podaci točni (Lam, 2022). Kako se vijest proširila društvenim mrežama, neki kineski korisnici interneta počeli su testirati objavljeni uzorak. Međutim, njihove rasprave i nalazi brzo su cenzurirani na društvenim mrežama.

Slika 14 Prikaz ponude na BreachForumu



Izvor: Grid News (2022)

Osim osobnih podataka datoteke uključuju korisničke narudžbe za kupnju, narudžbe za dostavu, plaćanja, narudžbe hrane, karte i evidenciju putovanja, evidenciju useljenika, informacije o mjestima za zabavu, upute za kontrolu prometa i pojedinosti o pojedincima klasificiranim kao sedam ciljanih skupina što se obično odnosi na potencijalne teroriste, aktivisti, kriminalci, dileri droge, bjegunci, mentalno poremećeni pojedinci i molitelji. Također, uključuju informacije o kibernetičkim istragama, zalagaonicama, pritvorskim centrima i objektima, centrima za liječenje ovisnosti, evidenciji vlasnika nekretnina, evidenciji o registraciji stanovnika, evidenciji o registraciji kućanstava, redovitom stanovništvu, stvarnom stanovništvu, medicinskim kartonima, evidenciji o korištenju goriva i još mnogo toga. Prikupljanje podataka od strane policijskih organa obavlja se pomoću softvera "Police Cloud" koji prikuplja i analizira sve podatke o stanovnicima i može upozoriti policijske službenike na promjene u ponašanju (Pike, Powers, Paladino, 2022). Softver je osmišljen kako bi korisnicima omogućio ciljanje određenih skupina ljudi koji se smatraju sumnjivima. Također, u skupu podataka nalazi se i datoteka u kojoj se nalaze pozivi građana policiji, kao i prijave koje su uslijedile, identifikacijske informacije o pozivateljima i osumnjičenicima, evidencija kaznenih djela poput krađe, obiteljskog nasilja i silovanja.

Kina je donijela novi Zakon o zaštiti podataka u studenom 2021. godine kojim se ograničava korištenje osobnih podataka u javnom i privatnom sektoru, ali se državi daje mogućnost manipulacije i monopola nad informacijama. Također, posljednjih nekoliko godina država je

prikupljala opsežne podatke o stanovnicima u sigurnosne svrhe te ih spremala u nacionalnu policijsku bazu podataka šangajske vlade, a ovaj napad pokazao je kako država raspolaže informacijama kojima može nadzirati stanovništvo.

Kina koristi jedan od najsofisticiranijih policijskih sustava te da bi se osigurala sigurnost takvih podataka potrebno je imati jaku kibernetičku obrane. Naime, ova krađa podataka nije zahtijevala napredno hakiranje jer je portal za pristup i upravljanje podacima bio otvoren, bez lozinke, što ga je činilo ranjivim.

Ovako velike količine podataka mogu biti vrlo opasne te ukoliko se ne koriste odgovarajuće mjere sigurnosti mogu ugroziti živote i poslovanja ljudi. Kineske vlasti nisu imale resurse niti sigurno okruženje kako bi spriječile curenje podataka. Mnogi smatraju kako bi odgovor na ovaj incident trebalo biti sustavno smanjivanje državnih ovlasti prikupljanja i zadržavanja osobnih podataka.

Curenje podataka moglo je doći s poslužitelja u oblaku Aliyuna, tvrtke za računalstvo u oblaku, podružnice Alibaba Grupe (Lam, 2022). Kineske vlasti nisu niti potvrdile niti opovrgle curenje podataka, umjesto toga, odlučile su cenzurirati raspravu o tome na kineskim vijestima i društvenim medijima. Ukoliko je skup podataka od 23,88 TB stvaran, to bi bilo najveće curenje podataka u povijesti.

3.10 Nacionalni spomenici i vrijednosti

Prvi kibernetički napad koji je pogodio cijelu državu dogodio se 2007. godine u Estoniji. Naime, u Talinu su donijeli odluku da premjeste sovjetski spomenik iz Drugog svjetskog rata iz središta glavnog grada na što je Rusija zaprijetila stanovnicima. Nakon što je spomenik premješten, Estonija je ostala bez pristupa Internetu. Rusija je izvršila raspodijeljeni napad uskraćivanjem usluge (eng. Distributed Denial of Service - DDoS) kojim se koordinirano, upotrebom više računala, ponekada i botneta, napadaju određeni resursi sustava s ciljem onemogućavanja njihova rada (Spremić, 2017). Botnetovi su slali ogromne količine neželjene pošte, a automatizirani online zahtjevi preplavili su poslužitelje. Rezultat za građane bio je da bankomati i usluge internetskog bankarstva nisu radili; državni službenici nisu mogli međusobno komunicirati e-poštom; a novine i televizijske kuće iznenada su otkrile da ne mogu prenositi vijesti. Napadi su došli s ruskih IP adresa, online upute bile su na ruskom jeziku, a pozivi Moskvi za pomoć su bili ignorirani, no nije bilo konkretnih dokaza da je te napade doista izvela ruska vlada.

Osim kibernetičkog napada, istovremeno se dogodio i fizički napad. Naime, odluka o premještanju je izazvala bijes u medijima na ruskom jeziku. Policija se morala suočiti s prosvjednicima koji su bili većinom govornici ruskog jezika. Zbog premještaja spomenika u Talinu su se odvile dvije noći nereda i pljačka. Ozlijeđeno je 156 osoba, jedna osoba je poginula, a 1.000 osoba je privedeno (McGuinness, 2017).

Kao rezultat napada iz 2007., Estonija ima sektor kibernetičke sigurnosti svjetske klase te je uspostavljena je dobrovoljna Jedinica za kibernetičku obranu. Kooperativni centar izvrsnosti za kibernetičku obranu s akreditacijom NATO-a (iako nije financiran niti pod zapovjedništvom NATO-a) pokrenut je u Estoniji godinu dana nakon napada, okupljajući kibernetičke stručnjake iz vojske, vlade i industrije.

Estonija je označila prekretnicu u korištenju kibernetičkih napada, od strane države, za postizanje vanjskopolitičkih ciljeva.

4. ISTRAŽIVANJE RAZINE INFORMIRANOSTI O KIBERNETIČKIM NAPADIMA

4.1 Cilj istraživanja

Cilj provedenog istraživanja je dobiti informacije o tome koliko su ispitanici informirani o važnosti kibernetičke sigurnosti i kibernetičkim napadima koji su se dogodili te utvrditi razinu informiranosti studenata smjera Menadžerska informatika na Ekonomskom fakultetu Zagreb kao buduće radne snage u IT sektoru. Istraživanje je potaknuto istraživanjima iz poglavlja 2.3.2 Kibernetički napadi u brojkama.

4.2 Hipoteze istraživanja

Bitno je iznijeti hipoteze istraživanja s obzirom da one utječu na cilj samog istraživanja:

1) Ekonomski fakultet u Zagrebu pruža dovoljno informacija o kibernetičkoj sigurnosti.

2) Studenti smjera Menadžerska informatika Ekonomskog fakulteta u Zagrebu prisustvovali bi edukaciji o kibernetičkoj sigurnosti.

3) Studenti smjera Menadžerska informatika Ekonomskog fakulteta u Zagrebu, nakon diplomiranja, spremni su za rad u IT području.

4.3 Metodologija istraživanja

U svrhu izrade diplomskog rada istraživanje je provedeno putem anketnih upitnika, koje su ispitanici mogli ispuniti online, putem Google obrasca. Link je ispitanicima proslijeđen putem e-maila te su se podaci prikupljali od 13.08. do 19.08. 2022. godine. Pitanja su oblikovana prema izvještajima o kibernetičkoj sigurnosti koji su navedeni u poglavlju 2.3.2 Kibernetički napadi u brojkama. U odabrani uzorak ispitanika odabrani su studenti smjera Menadžerska informatika na Ekonomskom fakultetu Zagreb. U anketi je sudjelovalo 60 ispitanika.

4.4 Moguća ograničenja prilikom istraživanja

Prilikom izbora anketnog upitnika kao istraživačke metode potrebno je voditi računa o mogućim ograničenjima. Tijekom provođenja istraživanja neki od problema su bili:

- pronalazak kompetentnih ispitanika
- istinitost rezultata.

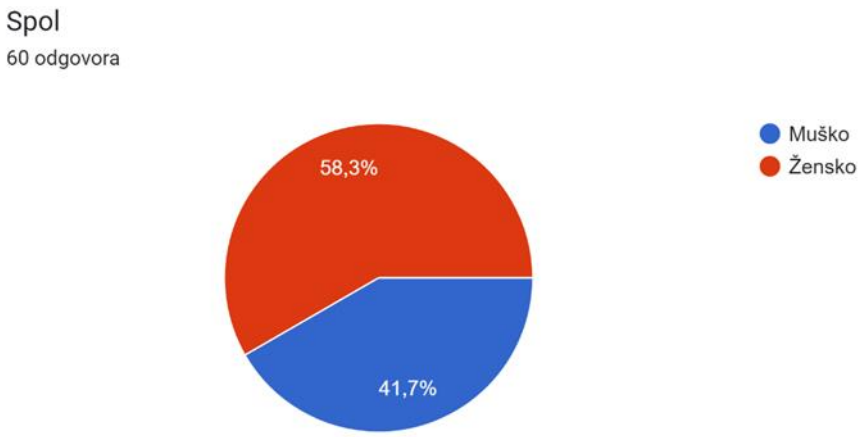
Bez obzira na spomenuta ograničenja, istraživanje je uspješno provedeno.

4.5 Rezultati istraživanja

U nastavku su prikazani rezultati provedenog istraživanja pomoću grafikona popraćeni tekstualnim objašnjenjima i kratkim zaključcima. Za potrebe istraživanja sastavljeno je 28 pitanja kojima se pokrivaju istraživačka pitanja, ciljevi istraživanja i postavljene hipoteze kako bi se došlo do što relevantnijih rezultata.

- Pitanje 1: Spol

Slika 15 Spol ispitanika



Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 58,3% bilo je ženskog spola, a ostatak od 41,7% muškog spola.

- Pitanje 2: Koja ste godina na smjeru Menadžerska informatika?

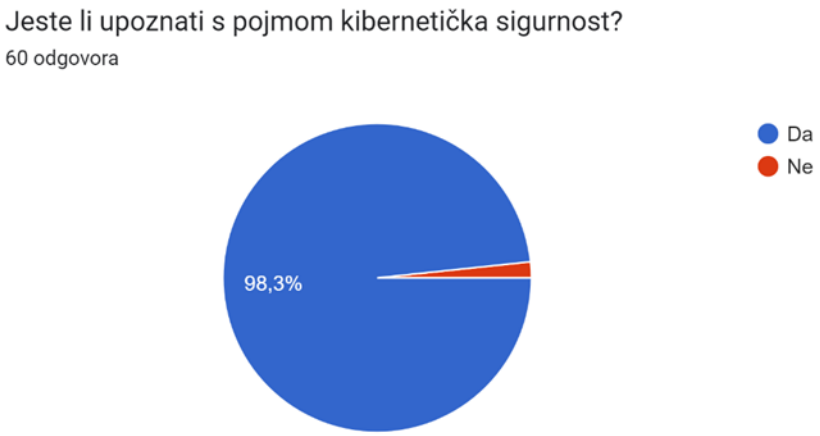
Slika 16 Godina na smjeru u koju je student upisan

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 50% bilo je peta godina, 43,3% četvrta godina i 6,7% ih je bilo na apsolventskoj godini.

- Pitanje 3: Jeste li upoznati s pojmom kibernetička sigurnost?

Slika 17 Pojam kibernetička sigurnost



Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 98,3% upoznato je s pojmom kibernetička sigurnost, dok njih 1,7% nije.

- Pitanje 4: Shvaćate li važnost kibernetičke sigurnosti za poslovanje organizacija?

Slika 18 Važnost za poslovanje

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 95% shvaća važnost kibernetičke sigurnosti za poslovanje organizacija, dok njih 5% nije sigurno.

- Pitanje 5: Smatrate li da je kibernetička sigurnost jednako važna kao i fizička sigurnost?

Slika 19 Fizička sigurnost vs. kibernetička sigurnost

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 88,3% smatra da je kibernetička sigurnost jednako važna kao i fizička sigurnost, 8,3% ispitanika nije sigurno, dok njih 3,4% ne smatra da imaju jednaku važnost.

- Pitanje 6: Jeste li upoznati s pojmovima kibernetički rizik i prijetnja?

Slika 20 Pojmovi kibernetički rizik i prijetnja

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 96,7% upoznato je s pojmovima kibernetički rizik i prijetnja, dok njih 3,3% nije.

- Pitanje 7: Jeste li upoznati s pojmom kibernetički napad?

Slika 21 Pojam kibernetički napad

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 96,7% upoznato je s pojmom kibernetički napad, dok njih 3,3% nije.

- Pitanje 8: Smatrate li da ste dovoljno informirani o kibernetičkim napadima?

Slika 22 Informiranost o kibernetičkim napadima

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 75% smatra da je dovoljno informirano o kibernetičkim napadima, dok 25% smatra da je nedovoljno informirano.

- Pitanje 9: Smatrate li da se broj kibernetičkih napada povećava?

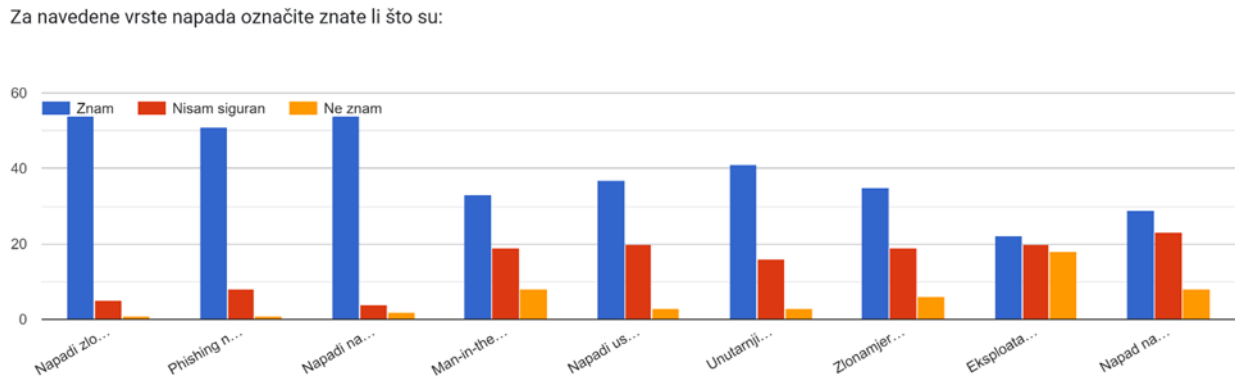
Slika 23 Povećanje broja kibernetičkih napada

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 95% ispitanika smatra da se broj kibernetičkih napada povećava, 3,3% ispitanika se izjasnilo kako ne znaju, dok 1,7% ispitanika smatra da se broj napada ne povećava.

- Pitanje 10: Za navedene vrste napada označite znate li što su:

Slika 24 Vrste napada

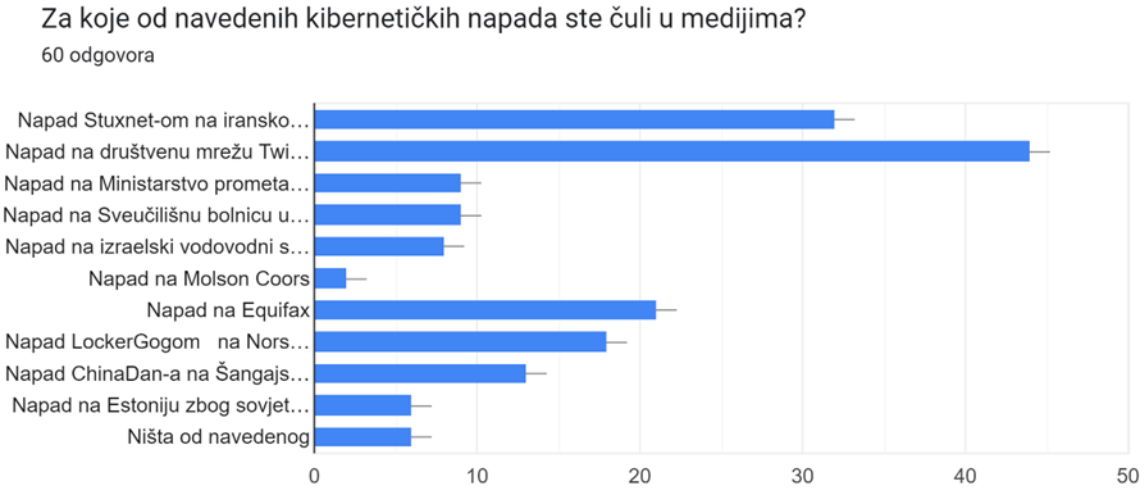


Izvor: samostalna izrada autorice rada

Ispitanici su generalno upoznati s navedenim vrstama napada. Za napade zlonamjernih softvera, phishing napade i napade na lozinke, većina ispitanika odgovorila je kako znaju što su. Ispitanici su najmanje upoznati s napadima na pouzdano i posjećeno web mjesto i eksploatacijom nultog dana.

- Pitanje 11: Za koje od navedenih kibernetičkih napada ste čuli u medijima?

Slika 25 Kibernetički napadi u svijetu

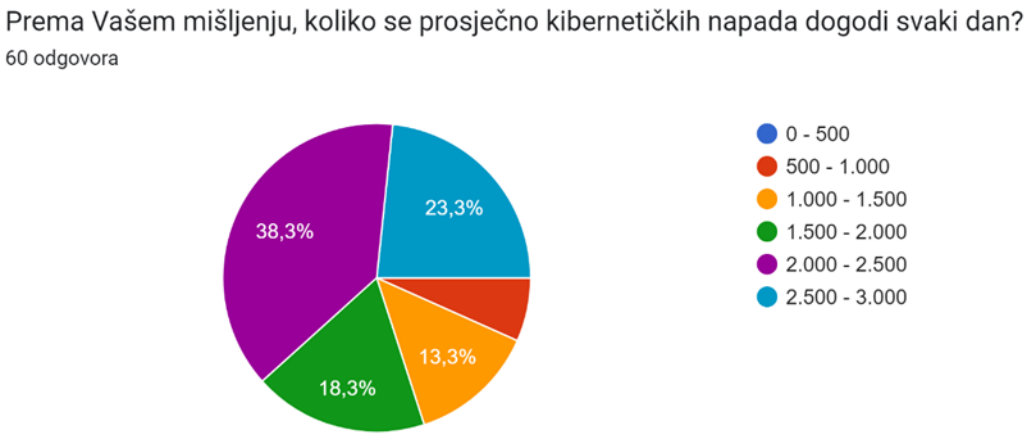


Izvor: samostalna izrada autorice rada

Za napad na društvenu mrežu Twitter čulo je čak 44 od 60 ispitanika, nakon toga slijedi napad Stuxnet-om na iransko nuklearno postrojenje (32 ispitanika), napad na Equifax (21 ispitanik) te napad LockerGogom na Norsk Hydro (18 ispitanika). Najmanje ispitanika čulo je za napad na Molson Coors i to samo 2 od 60 ispitanika.

- Pitanje 12: Prema Vašem mišljenju, koliko se prosječno kibernetičkih napada dogodi svaki dan?

Slika 26 Prosječan broj kibernetičkih napada dnevno

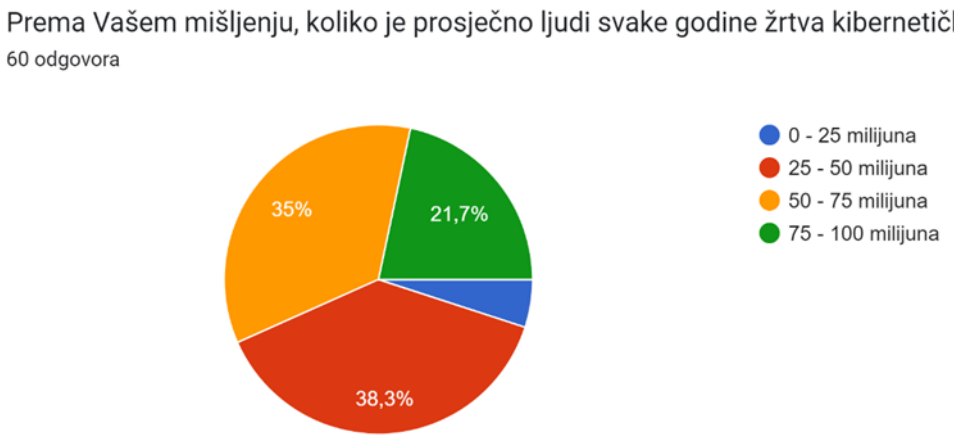


Izvor: samostalna izrada autorice rada

Najviše ispitanika, njih 38,3% smatralo je da se prosječno dogodi 2.000 – 5.000 napada svaki dan, što je i točan podatak. Prema istraživanju koje je proveo Norton (2021) prosječno se dnevno dogodi 2.200 napada što znači da se napad dogodi otprilike svakih 39 sekunda. 23,3% ispitanika smatralo je da se dogodi 2.500 – 3.000 napada, 18,3% ispitanika da se dogodi 1.500 – 2.000 napada i 13,3% ispitanika da se dogodi 1.000 – 1.500 napada. Ostatak ispitanika smatralo je da se dogodi 500 - 1.000 napada, a niti jedan ispitanik nije odgovorio da smatra da se dogodi 0 – 500 napada.

- Pitanje 13: Prema Vašem mišljenju, koliko je prosječno ljudi svake godine žrtva kibernetičkih napada?

Slika 27 Prosječan broj žrtava kibernetičkih napada

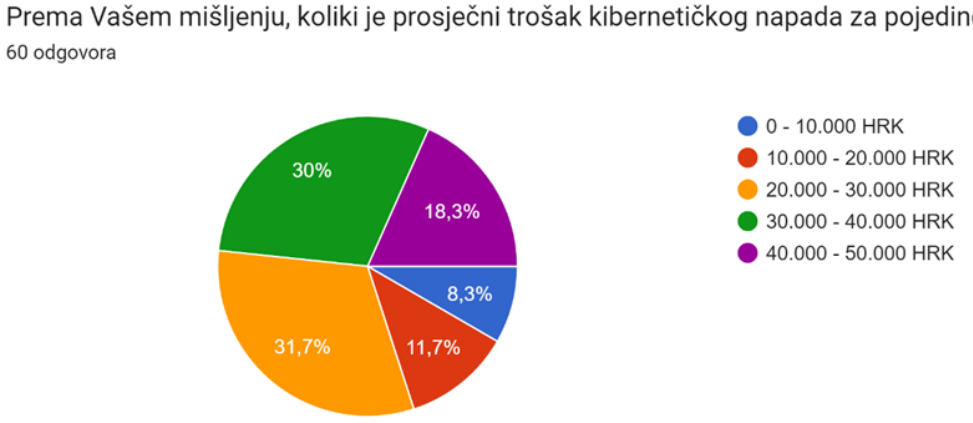


Izvor: samostalna izrada autorice rada

Najviše ispitanika, njih 38,3% smatralo je da je prosječno godišnje 25 – 50 milijuna žrtava kibernetičkih napada, no ta brojka doseže čak 71.1 milijun prema istraživanju Purplesec-a (2022) te je 35% ispitanika točno odgovorilo. 21,7% ispitanika smatralo je da je prosječno godišnje 75 – 100 milijuna žrtava kibernetičkih napada.

- Pitanje 14: Prema Vašem mišljenju, koliki je prosječni trošak kibernetičkog napada za pojedinca?

Slika 28 Prosječni trošak kibernetičkog napada za pojedinca

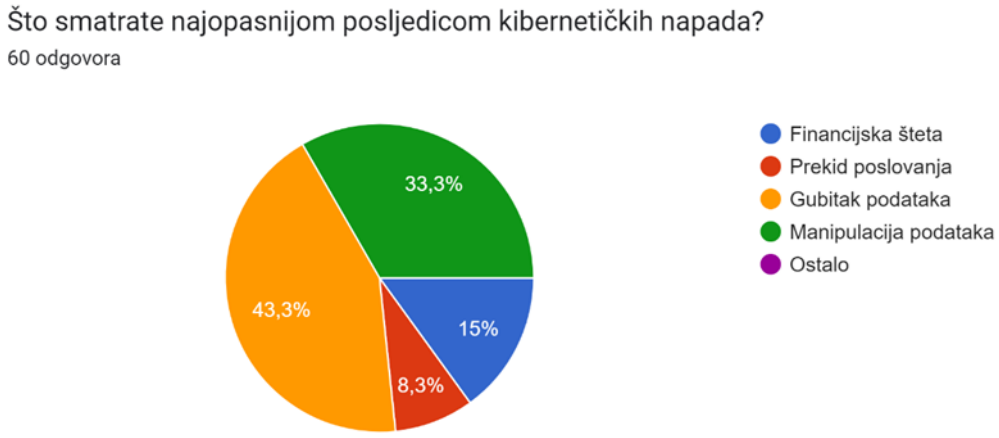


Izvor: samostalna izrada autorice rada

Najviše ispitanika, njih 31,7% smatralo je da je prosječni trošak kibernetičkog napada za pojedinca 20.000 – 30.000 HRK, no prema istraživanju Purplesec-a (2022) prosječan trošak iznosi 33.502 HRK te je 30% ispitanika točno odgovorilo. 18,3% ispitanika odgovorilo je kako smatra da prosječan trošak iznosi 40.000 – 50.000 HRK, a 11,7% je odgovorilo da trošak iznosi 10.000 – 20.000 HRK. Najmanje ispitanika smatralo je da trošak iznosi do 10.000 HRK.

- Pitanje 15: Što smatrate najopasnijom posljedicom kibernetičkih napada?

Slika 29 Posljedice kibernetičkog napada

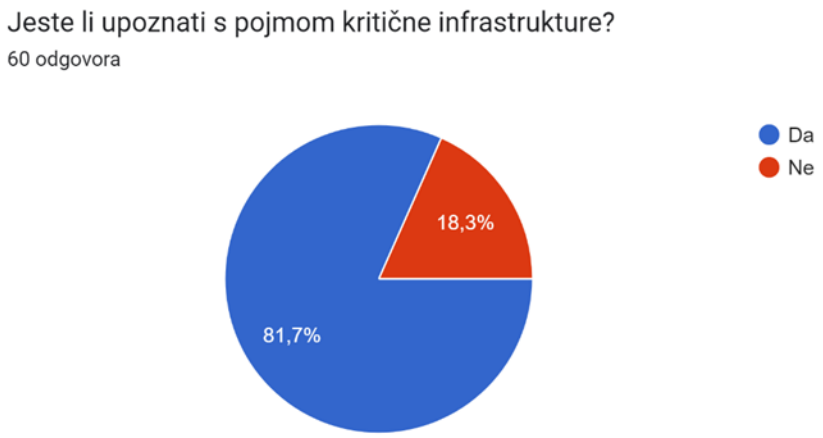


Izvor: samostalna izrada autorice rada

Prema odgovorima ispitanika najopasnije posljedice kibernetičkih napada su gubitak podataka (43,3% ispitanika) i manipulacija podacima (33,3% ispitanika). Nakon toga slijede financijska šteta s 15% i prekid poslovanja s 8,3%.

- Pitanje 16: Jeste li upoznati s pojmom kritične infrastrukture?

Slika 30 Pojam kritične infrastrukture

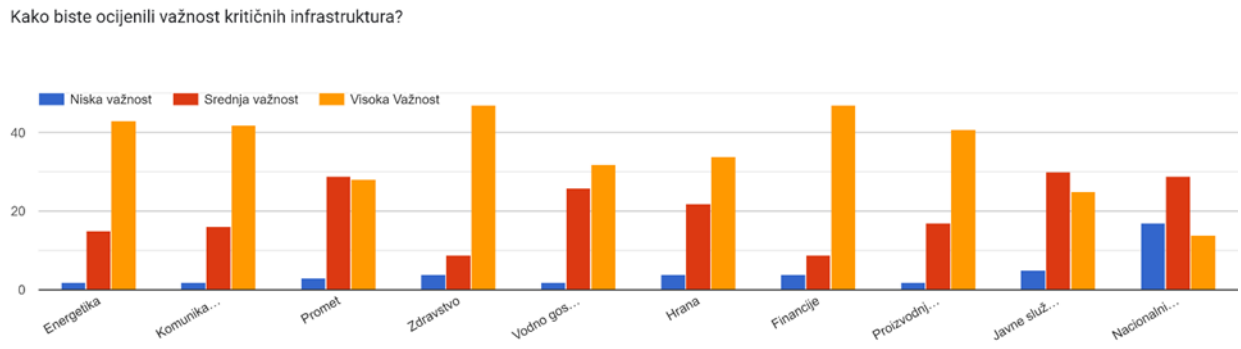


Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 81,7% upoznato je s pojmom kritične infrastrukture, dok 18,3% nije.

- Pitanje 17: Kako biste ocijenili važnost kritičnih infrastruktura?

Slika 31 Važnost kritičnih infrastruktura



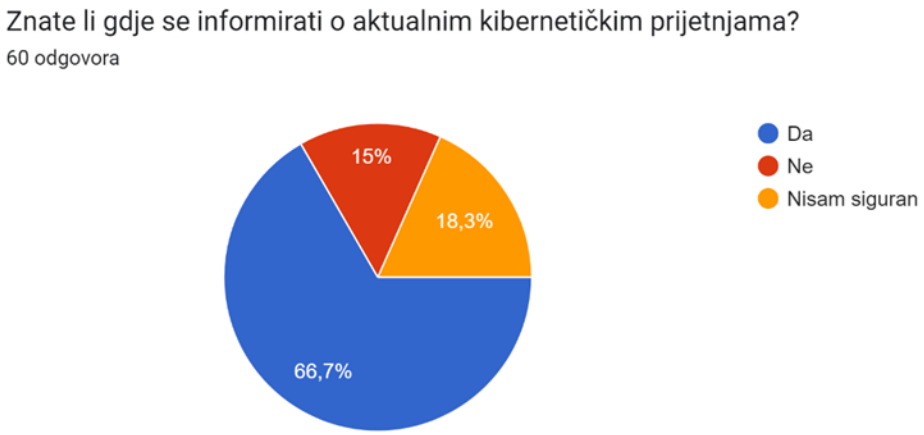
Izvor: samostalna izrada autorice rada

Prema odgovorima ispitanika možemo zaključiti kako najveću važnost imaju redom: zdravstvo, financije, energetika, komunikacijska i informacijska tehnologija, proizvodnja, skladištenje i prijevoz opasnih tvari, hrana i vodno gospodarstvo. Također, ispitanici smatraju kako srednju važnost imaju promet, javne službe i nacionalni spomenici i vrijednost. Za ni jednu kritičnu

infrastrukturu ne prevladava odgovor niske važnosti, no najviše ispitanika ocijenilo je nacionalne spomenike i vrijednosti kao infrastrukturu niske važnosti.

- Pitanje 18: Znate li gdje se informirati o aktualnim kibernetičkim prijetnjama?

Slika 32 Izvori informiranja



Izvor: samostalna izrada autorice rada

Većina ispitanika (66,7%) smatra kako zna gdje se mogu informirati o aktualnim kibernetičkim prijetnjama. 18,3% ispitanika nije sigurno gdje mogu pronaći informacije, a 15% ispitanika je odgovorilo kako ne zna gdje se mogu informirati.

- Pitanje 19: Pratite li izvještaje o kibernetičkoj sigurnosti?

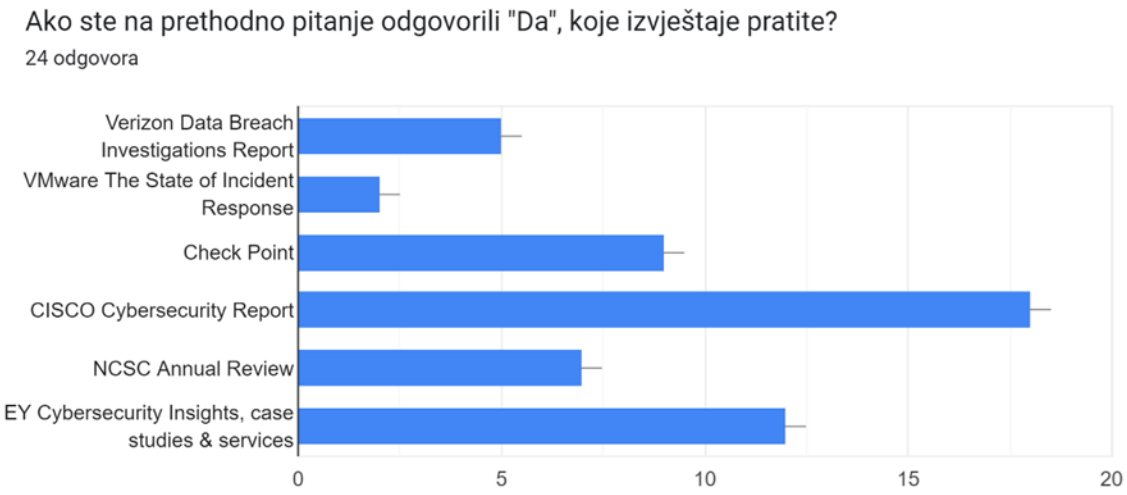
Slika 33 Praćenje izvještaja

Izvor: samostalna izrada autorice rada

Od ukupno 60 ispitanika, njih 63,3% prati izvještaje o kibernetičkoj sigurnosti, dok njih 36,7% ne prati.

- Pitanje 20: Ako ste na prethodno pitanje odgovorili "Da", koje izvještaje pratite?

Slika 34 Vrste izvještaja



Izvor: samostalna izrada autorice rada

Najpoznatiji izvještaj prema odgovorima ispitanika je CISCO Cybersecurity Report koji prati 18 ispitanika, a nakon njega slijedi EY Cybersecurity Insights, case studies & services koji prati 12 ispitanika. Najmanje ispitanika prati Verizon Data Breach Investigations Report (5 ispitanika).

- Pitanje 21: Smatrate li da biste mogli prepoznati da ste napadnuti nekom vrstom kibernetičkog napada?

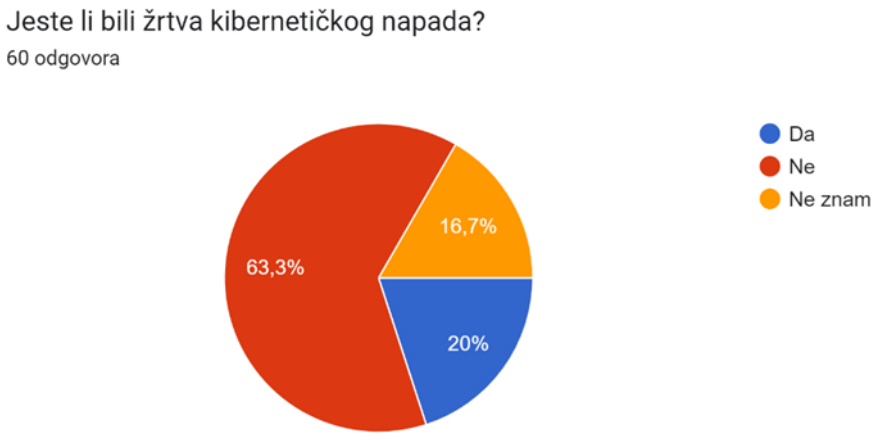
Slika 35 Sposobnost prepoznavanja napada

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 73,3% smatra da bi mogli prepoznati da su napadnuti nekom vrstom kibernetičkog napada. 25% nije sigurno bi li mogli prepoznati, a samo 1,7% smatra kako ne bi prepoznali da su žrtva napada.

- Pitanje 22: Jeste li bili žrtva kibernetičkog napada?

Slika 36 Žrtve kibernetičkog napada

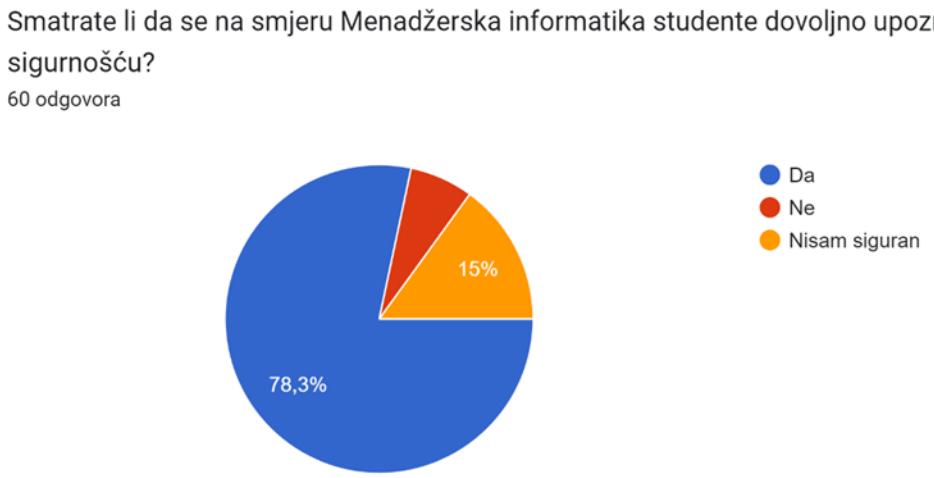


Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 63,3% nije bilo napadnuto, 16,7% nije sigurno, a 20% ispitanika bilo je žrtva kibernetičkog napada.

- Pitanje 23: Smatrate li da se na smjeru Menadžerska informatika studente dovoljno upoznaje s kibernetičkom sigurnošću?

Slika 37 Upoznatost studenata smjera s kibernetičkom sigurnošću

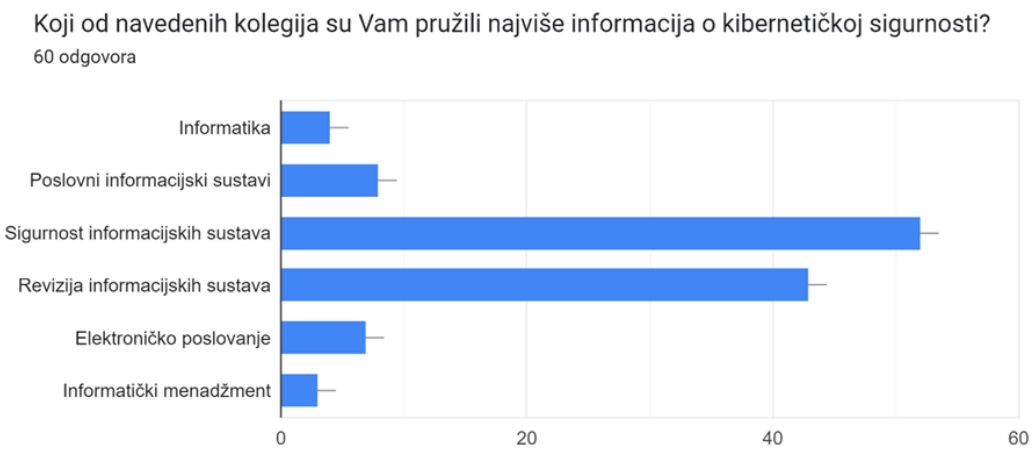


Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 78,3% smatra da se na smjeru Menadžerska informatika studente dovoljno upoznaje s kibernetičkom sigurnošću, dok 15% ispitanika nije sigurno, a 6,7% ispitanika smatra da studenti nisu dovoljno upoznati s kibernetičkom sigurnošću.

- Pitanje 24: Koji od navedenih kolegija su Vam pružili najviše informacija o kibernetičkoj sigurnosti?

Slika 38 Informacije o kolegijima

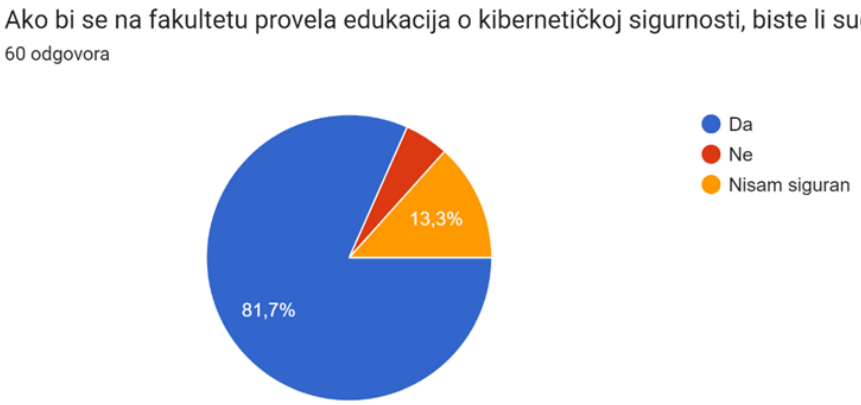


Izvor: samostalna izrada autorice rada

Od ukupno 60 ispitanika smjera Menadžerska informatika, njih 86,7% odgovorilo je kako im je na kolegiju Sigurnost informacijskih sustava pruženo najviše informacija o kibernetičkoj sigurnosti, a nakon toga slijedi kolegij Revizija informacijskih sustava sa 71,7% ispitanika.

- Pitanje 25: Ako bi se na fakultetu provela edukacija o kibernetičkoj sigurnosti, biste li sudjelovali?

Slika 39 Zainteresiranost ispitanika za edukaciju



Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 81,7% sudjelovalo bi na edukaciji o kibernetičkoj sigurnosti, 13,3% nije sigurno, a 5% ne bi sudjelovalo.

- Pitanje 26: Koliko često u svakodnevnom životu primjenjujete znanje stečeno na kolegijima?

Slika 40 Svakodnevna primjena znanja

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 61,7% vrlo često ili često primjenjuje znanje stečeno na kolegijima u svakodnevnom životu. 33,3% ispitanika odgovorilo je kako ponekad primjenjuje znanje, a 5% je odgovorilo da ne primjenjuje znanje stečeno na kolegijima.

- Pitanje 27: Smatrate li da na tržištu nedostaje stručnjaka za kibernetičku sigurnost?

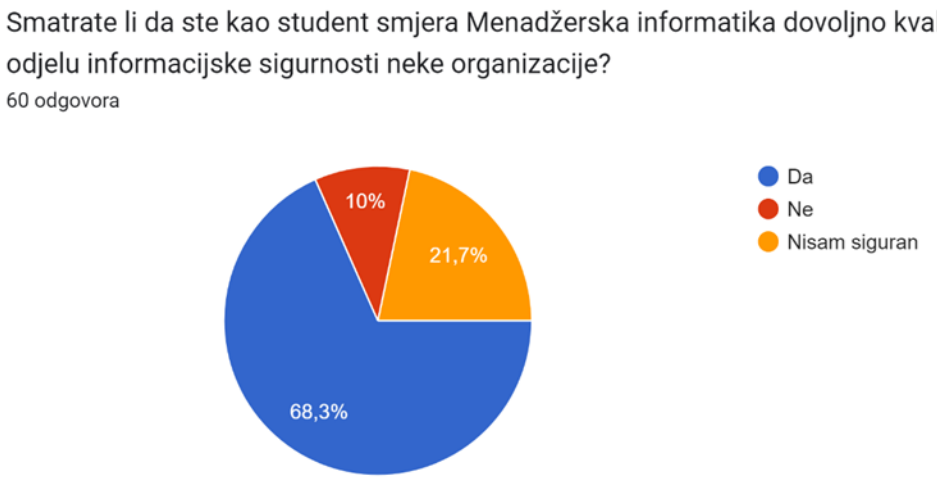
Slika 41 Stručnjaci za kibernetičku sigurnost

Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 81,7% smatra kako na tržištu nedostaje stručnjaka za kibernetičku sigurnost, 16,7% nije sigurno, a 1,7% smatra da ih na tržištu ima dovoljno.

- Pitanje 28: Smatrate li da ste kao student smjera Menadžerska informatika dovoljno kvalificirani za rad u odjelu informacijske sigurnosti neke organizacije?

Slika 42 Kvalificiranost za rad



Izvor: samostalna izrada autorice rada

Od ukupno 60 anonimnih ispitanika smjera Menadžerska informatika, njih 68,3% smatra da je dovoljno kvalificirano za rad u odjelu informacijske sigurnosti. 21,7% ispitanika nije sigurno, a 10% ispitanika smatra kako nije dovoljno kvalificirano.

Rezultati istraživanja pokazali su da su hipoteze postavljene na početku istinite, odnosno da Ekonomski fakultet u Zagrebu pruža dovoljno informacija o kibernetičkoj sigurnosti, da bi studenti smjera Menadžerska informatika Ekonomskog fakulteta u Zagrebu prisustvovali edukaciji o kibernetičkoj sigurnosti i da su studenti smjera Menadžerska informatika Ekonomskog fakulteta u Zagrebu, nakon diplomiranja, spremni za rad u IT području. Dodatno, istraživanje je pokazalo da značajan postotak ispitanika shvaća važnost kibernetičke sigurnosti i da je upoznato s osnovnim pojmovima koji se vežu uz nju što pokazuje da se na kolegijima na Ekonomskom fakultetu pruža dovoljno teorijskog znanja. Istraživanjem je utvrđeno kako su studenti smjera Menadžerska informatika zainteresirani za dodatne edukacije o kibernetičkoj sigurnosti kako bi stekli dodatna znanja i dobili informacije o mogućnostima zaposlenja u području informacijske sigurnosti.

5. ZAKLJUČAK

Kibernetička sigurnost pojam je koji ima mnogo definicija, ali sve ukazuju na njezinu sveprisutnost i važnost. Postoji niz znanstvenih radova koji se bave temom zaštite od kibernetičkih napada čija je putanja strmovito uzlazna te proučavaju utjecaj na pojedince, organizacije, ekonomije, politike i druge dimenzije društva. Iako se napredak tehnologije smatra pozitivnim za društvo, on sa sobom donosi i negativne učinke. Paralelno s razvojem i napredovanjem tehnologije, nastaju i nove slabosti koje napadači iskorištavaju. Pandemija korona virusa imala je negativan utjecaj na kibernetičku sigurnost jer se intenzivnije koristila tehnologija i stvorile su se nove mogućnosti za prijetnje. Postoje razne vrste kibernetičkih prijetnji koje kao cilj imaju povredu podataka (gubitak ili manipulacija), financijsku štetu, narušavanje ugleda i još mnoge druge. Kako bi korištenje tehnologije bilo što sigurnije, potrebno je poznavati prijetnje i rizike koji se pojavljuju. Nažalost, najveća slabost su ljudi koji nisu dovoljno educirani te su ljudske greške najčešći faktor uspješnih napada. Kako bi se smanjio broj kibernetičkih napada potrebno je educirati društvo o važnosti kibernetičke sigurnosti i na koji način odgovoriti na prijetnje s kojima se susreće. Manjak stručnjaka za područje kibernetičke sigurnosti dovodi do situacija u kojima se na napade ne odgovara adekvatno i u skladu s dobrim praksama koje su propisale institucije. Za organizacije je ključno da im je poslovanje agilno i prilagodljivo svim kibernetičkim rizicima koji nastaju. Brzina i način odgovora na kibernetičke napade od ključne su važnosti. Kibernetički napadi na kritične infrastrukture imaju utjecaj na države i mogu izazvati međusobne sukobe stoga je bitno posvetiti posebnu pažnju pronalasku rješenja za rizike kojima su infrastrukture izložene. Napadi na kritične infrastrukture moraju se detaljno analizirati te istraživanja moraju biti transparenta i dostupna javnosti kako bi se učilo na greškama. U interesu cijelog društva je da svi budu obaviješteni o prijetnjama koje se pojavljuju jer je prevencija najbolji način borbe protiv kibernetičkih napada. Zaštita kritičnih infrastruktura važan je sigurnosni zadatak za cijelo društvo.

POPIS LITERATURE

1. (ISC)^2 (2021.), Cybersecurity Workforce Study [e-publikacija], preuzeto 30.06.2022. s https://www.isc2.org/Research/Workforce-Study#
2. Akrap, G. (2019.), Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura, Strategos: Scientific journal of the Croatian Defence Academy , 3(2)
3. Alcaraz, C., Zeadally, S. (2015.), Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection, 8, 53-66
4. Amoroso, E. (2006.), Cyber Security, New Jersey: Silicon Press
5. Arbanas, K., Spremić, M., Žajdela Hrustek, N. (2021.), Holistic framework for evaluating and improving information security culture, Aslib Journal of Information Management, 73(5), 699-719
6. Beaumont, K. (2019.), How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business, preuzeto 23.05.2022. s https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
7. Britannica (b.d.), Stuxnet, preuzeto 02.05.2022. s https://www.britannica.com/technology/Stuxnet
8. Chai, W., Posey, B. (2022.), Remote desktop protocol (RDP), preuzeto 18.7.2022. s https://www.techtarget.com/searchenterprisedesktop/definition/Remote-Desktop-Protocol-RDP
9. Check Point (2022.), Check Point Research: Cyber Attacks Increased 50% Year over Year [e-publikacija], preuzeto 30.06.2022. s https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/)
10. Chickowski, E. (2022.), Cryptojacking explained: How to prevent, detect, and recover from it, preuzeto 08.08.2022. s https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
11. Chuang, T. (2020.), How SamSam ransomware took down CDOT and how the state fought back — twice, preuzeto 14.05.2022. s https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/

12. Department of Financial Services (2020.), Twitter Investigation Report, preuzeto 01.07.2022. s https://www.dfs.ny.gov/Twitter_Report
13. DHS (2014.), A Glossary of Common Cybersecurity Words and Phrases, preuzeto 01.07.2022. s http://niccs.us-cert.gov/glossary#letter_c
14. Eddy, M., Perlroth, N. (2020.), Cyber Attack Suspected in German Woman's Death, preuzeto 03.06.2022. s https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
15. Encyclopedia.com (b.d.), Critical infrastructure, preuzeto 30.06.2022. s https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/critical-infrastructure
16. European Union Agency for Cybersecurity (2021.), ENISA Threat Landscape 2021 [e-publikacija], preuzeto 30.06.2022. s https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
17. Fruhlinger, J. (2017.), What is Stuxnet, who created it and how does it work?, preuzeto 12.06.2022. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
18. Fruhlinger, J. (2020.), Equifax data breach FAQ: What happened, who was affected, what was the impact?, preuzeto 01.07.2022. s https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
19. Galinec, D., Možnik, D., Guberina, B. (2017.), Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, ppreuzeto 15.01.2022. s https://doi.org/10.1080/00051144.2017.1407022
20. Gross, J. A. (2021.), After alleged Iranian cyberattack, Israel's Water Authority beefs up defenses preuzeto 01.07.2022. s https://www.timesofisrael.com/after-alleged-iranian-cyberattack-israels-water-authority-beefs-up-defenses/
21. Hajdarevic, K., Allen, P., Spremić, M. (2016.), Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments, 24th Telecommunications Forum (TELFOR), 1-4
22. Hope, A. (2021.), A Suspected Ransomware Cyber Attack Shuts Down World's Fifth Largest Beermaker Molson Coors, preuzeto 25.06.2022. s

https://www.cpomagazine.com/cyber-security/a-suspected-ransomware-cyber-attack-shuts-down-worlds-fifth-largest-beermaker-molson-coors/

23. Huremović, L. (2021.), Kako IT timovi mogu zaštiti medije od SQL napada, preuzeto 25.07.2022. s https://www.balkansmedia.org/bs/korisni-savjeti-i-alati/kako-it-timovi-mogu-zastiti-medije-od-sql-napada
24. ITU (2009.), Overview of Cybersecurity. Recommendation ITU-T X.1205. preuzeto 16.05.2022. s http://www.itu.int/rec/T-REC-X.1205-200804-I/en
25. Jackson, A. (2019.), The Norsk Hydro LockerGoga ransomware cyber attack, preuzeto 04.05.2022. s https://swimlane.com/blog/norsk-hydro-ransomware-attack
26. Kemmerer, R. A. (2003.), Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715., preuzeto 16.05.2022. s http://dx.doi.org/10.1109/ICSE.2003.1201257
27. Kovacs, E. (2019.), Major U.S. Chemical Firms Hit by Cyberattack, preuzeto 24.06.2022. s https://www.securityweek.com/major-us-chemical-firms-hit-cyberattack
28. Kovač, D. (2021.), Ulaganje u kibernetičku sigurnost, Zbornik radova Veleučilišta u Šibeniku, vol. 15(1-2), pp. 61-73, preuzeto 01.07.2022. s https://hrcak.srce.hr/file/378328
29. Lam, O. (2022.), China: Possible police database breach exposes at least 1 billion citizens' personal data, preuzeto 05.07.2022. s https://globalvoices.org/2022/07/06/china-possible-police-database-breach-exposes-at-least-1-billion-citizens-personal-data/
30. Limba, T., Pleta, T., Agafonov, K., Damkus, M. (2017.), Cyber security management model for critical infrastructure, preuzeto 01.07.2022. s https://www.researchgate.net/publication/317715298_Cyber_security_management_model_for_critical_infrastructure
31. McGuinness, D. (2017.), How a cyber attack transformed Estonia, preuzeto 24.06.2022. s https://www.bbc.com/news/39655415
32. Morgan, S. (2020.), Cybercrime To Cost The World $10.5 Trillion Annually By 2025, preuzeto 24.06.2022. s https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
33. MS-ISAC (2019.), Security Primer – LockerGoga, preuzeto 15.06.2022. s https://www.cisecurity.org/insights/white-papers/security-primer-lockergoga

34. Muscat, I., (2019.), Cyber Threats, Vulnerabilities, And Risks, Acunetix, preuzeto 10.01.2022. s https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/
35. Noguchi, M., Ueda, H. (2017.), An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures, [e-publikacija], preuzeto 14.06.2022. s https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html
36. Ottis, R. (2007.), Analysis of the Attacker Profiles in the 2007 Cyber Attacks Against Estonia, Unpublished MSc dissertation, Tallinn Technical University, Tallinn
37. PC Chip (2018.), Koliko su uistinu ”veliki” gigabajti, terabajti i petabajti?, preuzeto 30.06.2022. s https://pcchip.hr/ostalo/tech/koliko-su-uistinu-veliki-gigabajti-terabajti-i-petabajti/
38. Pike, L., Powers, B., Paladino, J. (2022.), A massive leak of Chinese government data on hundreds of millions tests a new privacy law, preuzeto 14.07.2022. s https://www.grid.news/story/global/2022/07/07/a-massive-leak-of-chinese-government-data-on-hundreds-of-millions-tests-a-new-privacy-law/
39. Purplesec (2022.), Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022, preuzeto 17.08.2022. s https://purplesec.us/resources/cyber-security-statistics/
40. Ralston, W. (2020.), The untold story of a cyberattack, a hospital and a dying woman, preuzeto 05.06.2022. s https://www.wired.co.uk/article/ransomware-hospital-death-germany
41. Shruti, M. (2022.), 10 Types of Cyber Attacks You Should Be Aware in 2022, preuzeto 30.06.2022. s https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
42. Sigurnosno–obavještajna agencija (b.d.), Kibernetička sigurnost, preuzeto 30.06.2022. s https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/
43. Spremić, M. (2017.), Digitalna transformacija poslovanja, Sveučilište u Zagrebu, Ekonomski fakultet
44. Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Ekonomski fakultet
45. Spremić, M., Šimunic, A. (2018.), Cyber security challenges in digital economy, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, pp. 341-347, IAENG, Hong Kong

46. Staff, T. (2020.), Cyber attacks again hit Israel's water system, shutting agricultural pumps, preuzeto 01.07.2022. s https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/
47. Stouffer, C. (2021.), 115 cybersecurity statistics and trends you need to know in 2021, preuzeto 17.08.2022. s https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html
48. Swiss Cyber Institute (2020.), Cyber Security Threats in Energy Sector: Everything You Need to Know, preuzeto 24.06.2022. s https://swisscyberinstitute.com/blog/all-you-need-to-know-about-cyber-security-threats-in-energy-sector/
49. Tamkin, E. (2020.), 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?, preuzeto 15.06.2022. s https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/
50. Techopedia (b.d.), Internal attack, preuzeto 16.08.2022. s https://www.techopedia.com/definition/26218/internal-attack
51. Thompson, N., Barrett, B. (2020.), How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One, preuzeto 01.07.2022. s https://www.wired.com/story/inside-twitter-hack-election-plan/
52. Todd, D. (2021.), Molson Coors Still Recovering, Counting Cost of Data Breach, preuzeto 30.06.2022. s https://www.secureworld.io/industry-news/molson-coors-recovering-data-breach
53. Trend Micro (2019.), What You Need to Know About the LockerGoga Ransomware, preuzeto 15.06.2022. s https://www.trendmicro.com/vinfo/hk-en/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware
54. Trend Micro (b.d.), Zero-Day Vulnerability , https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability
55. Verizon (2022.), Data Breach Investigations Report [e-publikacija], preuzeto 30.06.2022. s https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
56. VMware (2021.), The state of incident response 2021: It's time for a confidence boost [e-publikacija], preuzeto 30.06.2022 s

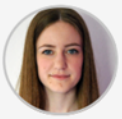
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-state-of-incident-response-2021.pdf

57. Warrick, J., Nakashima, E. (2020.), Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran, preuzeto 01.07.2022. s https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html
58. Weinberg, A. (2021.), Analysis of top 11 cyber attacks on critical infrastructure, preuzeto 01.07.2022. s https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
59. Wetsman, N. (2020.), Woman dies during a ransomware attack on a German hospital, preuzeto 15.05.2022. s https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity
60. Wright, R. (2020.), Colorado CISO details SamSam ransomware attack, recovery, preuzeto 23.05.2022. s https://www.techtarget.com/searchsecurity/news/252479128/Colorado-CISO-details-SamSam-ransomware-attack-recovery
61. Wright, G., Bacon, M. (2021.), Watering hole attack, preuzeto 20.07.2022. s https://www.techtarget.com/searchsecurity/definition/watering-hole-attack
62. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine br. 64/18 (2018.)
63. Zakon o kritičnim infrastrukturama, Narodne novine 56/13 (2013.)

POPIS TABLICA

POPIS SLIKA

ŽIVOTOPIS



Tonka Sviben

Datum rođenja: 03/10/1997 | **Državljanstvo:** hrvatsko | **Spol:** Žensko |
(+385) 953795110 | tonka.sviben7@gmail.com |
https://www.linkedin.com/in/tonka-sviben-550210152 |
Sajmišna ulica 66A, 49 250, Zlatar, Hrvatska

RADNO ISKUSTVO

01/07/2021 – TRENUTAČNO – Zagreb, Hrvatska
INTERN U IT REVIZIJI – ERNST & YOUNG SAVJETOVANJE D.O.O.

01/03/2021 – 31/05/2021 – Zagreb, Hrvatska
INTERN U REVIZIJI – ERNST & YOUNG D.O.O.

01/07/2019 – 28/02/2021 – Zagreb, Hrvatska
ASISTENTICA U RAČUNOVODSTVU – OLYMPUS CZECH GROUP, S.R.O. , ČLAN KONCERNA, PODRUŽNICA ZAGREB

01/06/2019 – 30/06/2019 – Zagreb, Hrvatska
ASISTENTICA U PRODAJI – STUDIO MODERNA D.O.O.

OBRAZOVANJE I OSPOSOBLJAVANJE

2017 – TRENUTAČNO – Zagreb, Hrvatska
STUDIJ – Ekonomski fakultet

Poslovna ekonomija - Menadžerska informatika

2016 – 2017 – Zagreb, Hrvatska
STUDIJ – Prirodoslovno-matematički fakultet

Matematika; smjer nastavnički

2012 – 2016 – Zabok, Hrvatska
SREDNJA ŠKOLA – Gimnazija Antuna Gustava Matoša

Jezična gimnazija

2004 – 2012 – Zlatar, Hrvatska
OSNOVNA ŠKOLA – Osnovna škola Ante Kovačića

JEZIČNE VJEŠTINE

Materinski jezik/jezici: **HRVATSKI**

Drugi jezici:

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna produkcija	Govorna interakcija	
ENGLESKI	C2	C2	C2	C2	C2
NJEMAČKI	A2	A2	A2	A2	A2
TALIJANSKI	A1	A1	A1	A1	A1
ŠPANJOLSKI	A1	A1	A1	A1	A1

Razine: A1 / A2: temeljni korisnik; B1 / B2: samostalni korisnik; C1 i C2: iskusni korisnik

DIGITALNE VJEŠTINE

Moje digitalne vještine

Internet | MS Office (Word, Excel, PowerPoint) | Skype, Zoom, Google Meet | Društvene mreže | MS Dynamics NAV | Rad na računalu

VOZAČKA DOZVOLA

Vozačka dozvola: B