Kibernetička sigurnost - aktualnosti u zaštiti podataka i regulativni okvir

Čule, Zrinka

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department of Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:973178

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČKE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

KIBERNETIČKA SIGURNOST - AKTUALNOST U ZAŠTITI PODATAKA I REGULATIVNI OBLIK

ZRINKA ČULE

Split, rujan 2024.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČKE ZNANOSTI

FORENZIKA I NACIONALNE SIGURNOSTI

DIPLOMSKI RAD

KIBERNETIČKA SIGURNOST - AKTUALNOST U ZAŠTITI PODATAKA I REGULATIVNI OBLIK

prof. dr. sc. MARIJA BOBAN

ZRINKA ČULE

0023092492

Split, rujan 2024.

Rad je izrađen u Splitu,

pod nadzorom dr.sc. Marije Boban,

u vremenskom razdoblju od 17. studenog 2023. do 30. kolovoza 2024.

Datum predaje diplomskog rada: 20. rujna 2024.

Datum prihvaćanja rada: 23. rujna 2024.

Datum usmenog polaganja: 27. rujna 2024.

Povjerenstvo: 1. prof. dr. sc. Marija Boban

_____

2. prof. dr. sc. Jozo Čizmić

_____

3. doc. dr. sc. Tonći Prodan

_____

Sadržaj

1. UVOD

Velik dio našeg života odvija se online. Svjedoci smo da je pomak prema digitalnom svijetu postao još očitiji od Pandemije COVID-a 19. Kako bismo ostali u kontaktu s voljenima, kupovali nove proizvode i radili od kuće oslanjali smo se na Internet. Međutim, uz nove prilike, prelazak na digitalni svijet donio je i nove prijetnje u obliku kibernetičkih napada. Kibernetički napadi se koriste za krađu podataka, špijuniranje korisnika, onesposobljavanje ili manipulaciju računalima i još mnogo toga. Oni ne ciljaju samo osobna računala, već i cijele mreže, a mogu ih izvoditi pojedinačni hakeri, grupe hakera ili čak države. Ukoliko prijelaz na digitalni svijet treba biti uspješan, građani i kompanije moraju koristiti nove tehnologije bez ugrožavanja njihove kibernetičke sigurnosti. Strategija EU, koja se primjenjuje i u Republici Hrvatskoj kroz Zakon o kibernetičkoj sigurnosti NN 14/24, za kibernetičku sigurnost ima za cilj ojačati našu kolektivnu kibernetičku sigurnost i naš odgovor na kibernetičke napade. Ona će izgraditi stabilan i siguran globalni Internet gdje su vladavina prava, ljudska prava i demokratske vrijednosti zaštićeni. (1)

Ubrzani razvoj napredak modernih informacijsko-komunikacijskih tehnologija i novi pristupi obradi osobnih podataka temeljni su preduvjeti za razvoj digitalne ere, no istovremeno stvaraju česte izazove i prijetnje privatnosti i zaštiti osobnih podataka. Kada govorimo o obradi podataka, osobito obradi osobnih podataka te novim IT alatima i digitalnom tržištu, dolazi do potrebe za povećanjem zaštite privatnosti novih digitalnih proizvoda i usluga. Rješenje je navedeno u EU Uredbi 2016/679 (GDPR), kroz okvir zaštite osobnih podataka, uvedene su značajne promjene u načine upravljanja osobnim podacima, a te promjene izravno se primjenjuju na sve organizacije koje obrađuju osobne podatke građana Europske unije. GDPR je uveo značajne promjene u pravilima koja definiraju osobne podatke, donoseći nove pojmove te zahtjeve za usklađivanje, planiranje, implementaciju, održavanje usklađenosti i procjenu učinka. (2)

Na tom je planu potrebno konstantno stvarati sve moguće pravne i informatičke preduvjete za postizanje učinkovite borbe protiv kibernetičkih napada i to svim osobama koje su zadužene za zaštitu od istih. Stoga je potrebno razvijati i jačati postojeću informacijsku infrastrukturu, u kojoj će forenzika, kao sve brže rastuća disciplina, imati ključnu ulogu.

Kibernetička sigurnost je ključna za zaštitu osobnih podataka, poslovnih informacija i nacionalne sigurnosti. Kako se kibernetički kriminalitet razvija, tako se i metode kibernetičke sigurnosti kontinuirano unapređuju kako bi se odgovorilo na nove prijetnje.

Kompleksnost društvenih promjena u suvremenim društvima prvenstveno se ogleda u učestaloj upotrebi pojmova poput informacija, informacijske sigurnosti, osobnih podataka, prava na privatnost, informacijskog društva i digitalne ekonomije.

2. CILJ RADA

S obzirom na vremena u kojima živimo te da je pristup Internetu lako dostupan svim dobnim skupinama te svim poslovnim korisnicima, a sigurnost na istom ovisi isključivo o educiranosti te pristup ljudi, bilo s privatnog ili poslovnog aspekta, razvila se potreba za istraživanjem ove tematike. Također, cilj je objasniti pojmove kao što su: Kibernetička sigurnost, kibernetički prostor, ukazati na prevenciju, detekciju, brz odgovor, oporavak te kao što sam ranije spomenula na obrazovanje i svijest kako do napada ne bih došlo i kako bih se iste minimiziralo. Također, u radu će se objasniti EU Uredba 2016/649 (GDPR), ukazati na njenu važnost i primjenu unutar članica Europske Unije te usporediti istu s zemljama koje je ne provode. Osim same Uredbe kroz rad će se prikazati regulatorni okvir kibernetičke sigurnosti temeljen na implementaciji NIS Direktiva s naglaskom na NIS 2 Direktivu.

Brojni članci, analize i istraživanja obrađuju ovu tematiku. U ovom radu, istraživanje se temelji na pojmovima: informacija, osobnih podataka, privatnosti i informacijske sigurnosti. Definiranjem privatnosti, odnosno rečeno zadiranja u osobnosti (individualnosti) te prava osobe (individue) postavljaju se temelji za postizanje postavljanja adekvatnog okvira prava na pristup informacijama, kao i temelji za zaštitu osobnih podataka kao temelja suvremenog informacijskog društva. S ubrzanim razvojem suvremenih informacijskih i komunikacijskih tehnologija, kao i novih načina obrade osobnih podataka, postalo je neophodno usvojiti novi zakonodavni okvir koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka te zakonodavni okvir vezan uz kibernetičku sigurnost.

2.1. Kibernetički prostor

Kibernetički prostor, odnosno Cyberspace je pojam novijeg vremena i označava sve ono što se odvija u virtualnom prostoru s pomoću globalno umreženih računala. Američki pisac William Gibson je u svojoj knjizi Neuromancer izdanoj 1948. prvi je put u upotrebu stavio pojam Cyberspace. Kibernetički prostor možemo poistovjetiti sa stvarnim prostorom jer ljudi u njemu mogu komunicirati te se družiti putem različitih društvenih mreža kao što su Facebook, Twitter, , Instagram, LinkedIn (3). Podatak koji pokazuje da je broj ljudi koji koriste kibernetički prostor, odnosno Internet, porastao s 360 milijuna na gotovo dvije milijarde korisnika u razdoblju od 2000. do 2010. godine, ilustrira rapidan rast globalne internetske populacije govori kako kibernetički

prostor postaje sve važnije sredstvo u suvremenom svijetu. Osim komunikacije, kibernetički se prostor može koristi i za druge aktivnosti kao što je znanost, uz pomoć kibernetičkog prostora znanstvenici se mogu okupiti na jednostavniji način te u stvarnom vremenu izmjenjivati svoje ideje. Također, za možemo navesti i međunarodno poslovanje u kojem se vrlo jednostavan može trgovati uslugama i robom.

Kibernetički prostor, uz sve prednosti koje daje u suvremenom svijetu, predstavlja i značajan sigurnosni izazov. U kibernetičkom prostoru sigurnosne prijetnje dijelimo na četiri razine:

- kibernetski kriminal,
- kibernetska špijunaža,
- kibernetski terorizam,
- kibernetičko ratovanje.

Te ugroze su maliciozne prirode, s ciljem nanošenja štete sustavima., kao što su kritična infrastruktura, financija, promet, komunikacije i ostalim osjetljivim sustavima. Gledajući metode napada, iste se mogu izvesti dvjema varijantama: napad na operativne tehnologije ili nadzorne sustave i napad na podatke.

Cilj napada na nadzorne sustave je za sobom ostavljaju dalekosežne posljedice. Ovakva vrsta napada se najčešće koristi za ugrožavanje kritične infrastrukture pojedine države, a izvode se probijanjem sustava nadzora odnosno operativnih tehnologija ili putem Interneta. Nadalje, ukoliko govorimo o napadima na podatke tada govorimo o sabotaži, krađi podataka ili šteti uzrokovanoj za određene podatke što ostavlja ozbiljne posljedice uzrokovane napadom. (4)

Kibernetički prostor je integriran i utječe na sve aspekte svakodnevnog života većine ljudi kao i digitalno prenesenih aktivnosti te je sastavni dio modernog društva. Sastavljen od Informacijskih i komunikacijskih tehnologija, postao je dio kritične infrastrukture koja podupire vođenje poslovanja, ostvarivanje ljudskih prava i sloboda, upravljanje nacijama i pod-društvima te socioekonomski rast. Kibernetički prostor je omogućio pristup poslovanju i informacijama, olakšao je vladine aktivnosti kao i zapošljavanje i stvaranje prihoda tvrtkama i vladama, e-učenje. Zbog prethodno navedenog, Informacijske i komunikacijske tehnologije te Internet omogućili su mnoge pozitivne aspekte suvremenog načina života i postali su nezamjenjivi dio ljudske svakodnevnice. Međutim, prihvaćanje navedenih tehnologija od strane korisnika također je

omogućilo manje poželjnim aktivnostima, prijetnjama i rizicima poput kriminala, izloženosti informacijama, špijunažama, ratovanju i terorizmu priliku da iskoriste tu istu infrastrukturu. (5) Zbog navedenih činjenica pojavila se potreba za kontrolom i zaštitom kibernetičkog prostora, što je dovelo do sve veće rasprave o važnosti kibernetičke sigurnosti.

2.2. Kibernetička sigurnost

Kibernetička sigurnost postaje ključan element unutar nacionalne sigurnosti. Naime, svjedoci smo sve većeg porasta kibernetičkih prijetnji, dok napadi postaju sve napredniji i složeniji, s utjecajem ne samo na naš svakodnevni život, već i na poslovanje. Vrste napada u kibernetičkom prostoru su različite, ali možemo navesti neke od njih kao što su zloporabe financijskih i osobnih podataka, maliciozni programi, zloporabe na društvenim mrežama te računalne prijevare (6).

Slika 1. Kibernetička sigurnost [7]

Pojam "kibernetička sigurnost" primjenjuje se u raznim kontekstima, a možemo ga podijeliti na nekoliko uobičajenih kategorija:

- *Sigurnost mreže* odnosi se na praksu osiguravanja računalne mreže od uljeza, bilo da se radi o zlonamjernom softveru ili o ciljanom napadaču.
- *Sigurnost aplikacija* se fokusira na održavanje softvera i uređaja bez prijetnji. Kompromitirana aplikacija može omogućiti neovlašteni pristup podacima koji su, pri njenom dizajniranju, trebali biti zaštićeni. Uspješna sigurnost počinje već u fazi kreiranja aplikacije, mnogo prije nego što se program ili uređaj implementira.
- *Sigurnost informacija* štiti privatnost podataka te integritet istih, u prijenosu i pohrani.
- *Operativna sigurnost* obuhvaća procese i odluke vezane uz rukovanje i zaštitu osjetljivih informacija te upravljanje rizicima kako bi se spriječio neovlašteni pristup ili kompromitacija podatkovnih resursa. Dozvole koje korisnici imaju prilikom pristupa mreži, kao i postupci koji određuju kako i gdje se podaci mogu pohraniti ili dijeliti, spadaju u kategoriju operativne sigurnosti.
- *Oporavak od* katastrofe i kontinuitet poslovanja definiraju kako organizacija reagira na kibernetički sigurnosni incident ili bilo koji drugi događaj koji uzrokuje gubitak operacija ili podataka, osiguravajući brzu obnovu i minimalizaciju prekida poslovanja. Politike oporavka od katastrofe određuju kako organizacija obnavlja svoje operacije i informacije, s ciljem povratka na istu razinu radne sposobnosti kao prije incidenta. Kontinuitet poslovanja je plan na koji se organizacija oslanja kako bi nastavila s operacijama u slučaju nedostupnosti određenih resursa.
- *Obrazovanje krajnjih korisnika* usmjereno je na najnepredvidljiviji aspekt kibernetičke sigurnosti: ljudski faktor. Svaka osoba može nenamjerno unijeti virus u inače siguran sustav ne slijedeći dobre sigurnosne prakse. Poučavanje korisnika da brišu sumnjive privitke e-pošte, ne priključuju neidentificirane USB pogone i razne druge važne lekcije ključno je za sigurnost svake organizacije (7).

Kako bi se smanjila vjerojatnost kibernetičkog napada, važno je implementirati i slijediti niz najboljih praksi, uključujući sljedeće:

- Redovito ažuriranje softvera: Osigurati da su svi softveri, uključujući operativne sustave i aplikacije, redovito ažurirani kako bi se otklonile poznate ranjivosti.

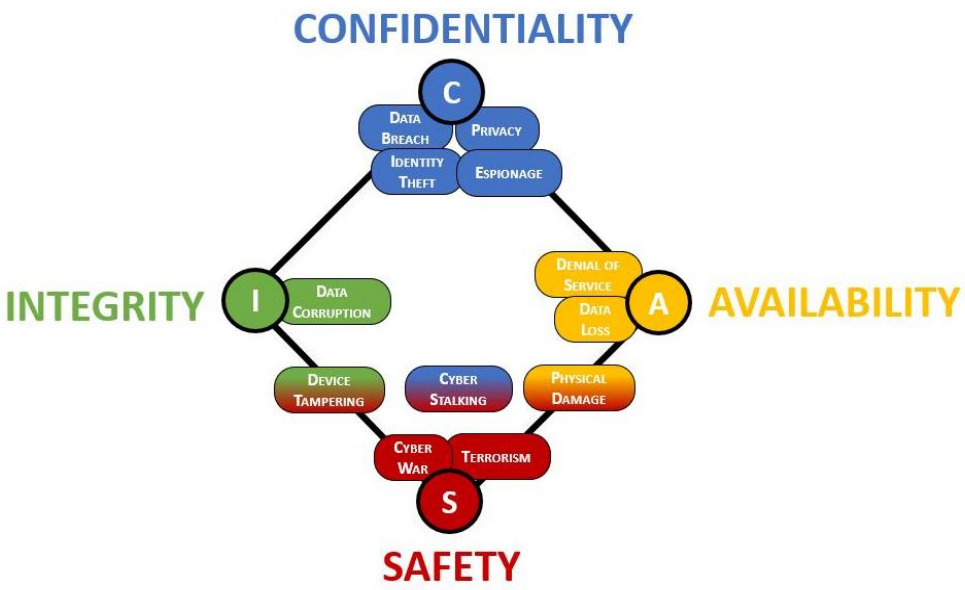
- Korištenje snažne lozinke: Zaposlenici bi trebali birati lozinke koje koriste kombinaciju slova, brojeva i simbola, što ih čini teškim za provaljivanje putem napada brutalnom silom ili pogađanjem. Također, zaposlenici bi trebali redovito mijenjati svoje lozinke.
- Korištenje višefaktorske autentifikacije (MFA): MFA zahtijeva najmanje dva elementa identifikacije za pristup, čime se smanjuje mogućnost da zlonamjerni akter dobije pristup uređaju ili sustavu.
- Educirajnje zaposlenika o sigurnosnoj svijesti: Ovo pomaže zaposlenicima da pravilno razumiju kako naizgled bezopasne radnje mogu ostaviti sustav ranjivim na napade. Edukacija bi trebala uključivati i prepoznavanje sumnjivih e-poruka kako bi se izbjegli napadi putem phishinga.
- Implementacija sustav za upravljanje identitetima i pristupom (IAM): IAM definira uloge i pristupne privilegije za svakog korisnika unutar organizacije, kao i uvjete pod kojima mogu pristupiti određenim podacima.
- Korištenje vatrozida: Vatrozidi ograničavaju nepotreban izlazni promet, što pomaže spriječiti pristup potencijalno zlonamjernim sadržajima.
- Implementiranje postupaka za oporavak od katastrofe: U slučaju uspješnog kibernetičkog napada, plan oporavka od katastrofe pomaže organizaciji u održavanju operacija i vraćanju ključnih podataka. (7)

2.2.1. Koncepti povjerljivosti, integriteta i dostupnosti

Saltzer i Schroeder su 1975. godine, u svojem radu "The Protection of Information in Computer Systems", navode i definiraji osnovne principe informacijske sigurnosti: povjerljivost, integritet i dostupnost. (8)

Navedeni osnovni principi su prikazani na Slici 2., imaju različite zahtjeve, a definiraju se kao:

- Povjerljivost: ovim svojstvom je neovlaštenim osobama, procesima ili entitetima onemogućen pristup informacijama
- Integritet: ovim svojstvom je osigurano vjerovanje informacijama te ih uređuju samo ovlaštene osobe,
- Dostupnost: ovim svojstvom je zagarantirana dostupnost informacija ukoliko budu zatražene od ovlaštenog korisnika.



Slika 2. Prikaz osnovnih principa informacijske sigurnosti (9)

Prema ta tri temeljna principa razvili su se različiti modeli informacijske sigurnosti, koji služe kao okvir za implementaciju mjera zaštite podataka i sustava, osiguravajući povjerljivost, integritet i dostupnost informacija., poput: CIA, International Organization for Standardization Model (ISO) Model, Parkerian Hexad te mnogi drugi. U Tablici 1. se prikazani neki sigurnosni modeli te njihova svojstva.

Tablica 1. Primjeri sigurnosnih modela te njihova svojstva (9)

Svojstva modela	CIA	7ISO svojstvo	Parkerian Hexad
Povjerljivost	✓	✓	✓
Integritet	✓	✓	✓
Dostupnost	✓	✓	✓
Autentičnost		✓	✓
Prihvatljivost			
Autentifikacija			
Posjed			✓
Korisnost			
Pouzdanost		✓	
Odgovornost		✓	
Neopozivost		✓	

2.3. Kibernetički napadi

Kibernetički napadi se mogu dogoditi bilo kada, a kao mete imaju državne i lokane vlasti, kritične infrastrukture, pojedince i poduzeća. Zbog naprednih informatičkih alata postaju sve više sofisticirani, a samim tim utječu na svakodnevni život i poslovanje. Posljedice kibernetičkih napada uključuju izgubljenu produktivnost, ukradeni novac, gubitak kontinuiteta poslovanja, brisanje i vraćanje podataka, uništavanje podataka, krađu intelektualnog vlasništva, krađu financijskih i osobnih podataka kao i narušavanje ugleda. Napadi mogu biti različite vrste te je teško znati tko, kako i zašto može biti žrtva napada. Također, teško je predvidjeti koliko će se napadi raširiti i o kojoj će se vrsti radi. Stoga je potrebno biti upoznat s vrstama napada te na koji način se zaštiti od istog. U nastavku ćemo objasniti neke od kibernetičkih napada (10):

1. Phishing - jedan od najraširenijih kibernetičkih napada. Ovakva napad je vrsta računalne prijevare čiji je cilj krađa identiteta. Način na koji se ovakva vrsta napada je slijedeći,

računalni kriminalci šalju lažne elektroničke poruke koje često uključuju lažne poruke ili web stranice koje izgledaju kao da su poslane od izvornih institucija, čime napadači na prevaru dobivaju pristup povjerljivim korisničkim podacima. (10) Primjer Phishing napada je prikazan na Slici 3. gdje se isti može uočiti u gramatičkoj pogrešci. Kako bismo spriječili ovu vrstu napada, potrebno je pažljivo provjeravati e-mail poruke i izbjegavati otvaranje pošte od nepoznatih izvora. Također je važno provjeriti legitimnost poveznica i priloga prije nego što ih otvorimo.


Pošiljatelj: Olt Director <Olt.Director@tgie.ro>
Poslano: 20. veljače 2020. 10:44
Primatelj: no-reply@microsoft.net
Predmet: Vaš račun za e-poštu treba odmah potvrditi

MICROSOFT VAŽNA OBAVIJEST

Vaš račun za e-poštu treba odmah **potvrditi** ili će vaš račun za e-poštu biti obustavljen ako nije potvrđen sada.

https://ismcadmissions.wixsite.com/mysite

Hvala na razumijevanju

Microsoftov tim za provjeru

Slika 3. Primjer Phishing napada (11)

Man-in-the-Middle (MITM) - napadi su oblik prisluškivanja u kojem napadač, smješten na kanalu između resursa i tražitelja resursa, zaobilazi komunikacijske protokole i iskorištava ranjivosti mreže. Time napadač ostvaruje mogućnost nadgledanja sadržaja, mijenjanja komunikacije te pohranjivanja datoteka bez znanja sudionika. (10). Kako bismo spriječili ovakvu vrstu napada podaci se mogu kriptirati na mrežnim uređajima.

2. Napadi zlonamjernih softvera (eng. malware) - najčešća vrsta kibernetičkih napada. Programi koji su najčešće tajno ubačeni u sustav s ciljem ometanja ili nanosa štete, ugrožavaju povjerljivost, integritet ili dostupnost podataka, aplikacija, operacijskog sustava ili drugih dijelova računalnog ili informacijskog sustava. Zlonamjerni softver

prodire u sustave kroz mrežne ranjivosti. Kada korisnik klikne na zaraženu poveznicu ili preuzme privitak iz e-maila, zlonamjerni softver može ući u sustav. Ove napade moguće je spriječiti upotrebom antivirusnih programa kao što su Avast, Norton ili McAfee, te vatrozida koji filtriraju mrežni promet i blokiraju sumnjive aktivnosti. (10)

Zlonamjerni softveri uključuju:

- Računalne crve (eng. worms)
- Špijunski softver (eng. spyware)
- Ucjenjivački softver (eng. ransomware)
- Zlonamjerni oglašivački softver (eng. adware),
- Trojanske viruse, koji se prikazuju kao legitimni softveri kako bi prevarili korisnike.

3. SQL napadi (eng. SQL injection) – su napadi kod kojih se se zlonamjerni kod ubacuje u SQL server s ciljem izvršavanja određenih naredbi, napadač tada može pregledavati, uređivati i brisati podatke u bazama podataka (12). Ovakvi napadi mogu se spriječiti provjerom valjanosti podataka i instaliranjem softvera za otkrivanje neovlaštenog pristupa mreži .
4. Unutarnji napadi ne uključuju treću stranu, već su izvedeni od strane korisnika informacijskog sustava ili zaposlenika organizacije. Ovi napadi su češći u manjim organizacijama zbog manje segmentacije uloga nego u većim organizacijama. U većini slučajevima, napadač koristi značajnu količinu alata, resursa te vještina kako bi izveo sofisticirani računalni napad s ciljem potencijalnog uklanjanja svih dokaza napada. (13) Kako bi se spriječili ovakvi napadi organizacije bi trebale imati zdravu organizacijsku kulturu te visoku razinu svijesti o sigurnosti.
5. Eksploatacija nultog dana (eng. Zero-Day Exploit) odnosi se na ranjivost u uređaju ili sustavu koja je otkrivena, ali još nije zakrpana. (14) Iako vijest o ranjivosti može stići do napadača, zaposlenici su također najčešće obaviješteni. Ovisno o stupnju ranjivosti, može proći neko vrijeme dok se problem ne riješi, a napadači tijekom tog perioda ciljaju otkrivenu ranjivost. Eksploatacije nultog dana mogu se spriječiti učinkovitim upravljanjem i automatizacijom procesa razvijanja zakrpa kako bi se izbjegla kašnjenja u njihovoj implementaciji.
6.

7. Napad na pouzdano i često posjećeno web mjesto (eng. Watering Hole Attack) usmjeren je na otkrivanje web stranica koje žrtva redovito posjećuje kako bi se omogućio udaljeni pristup računalu žrtve ili kompromitirali osobni podaci. Krajnji cilj ovakvog napada je dobiti pristup mreži na radnom mjestu ili zaraziti računalo ciljanog korisnika.(15) Prevencija takvih napada uključuje redovito održavanje sustava, korištenje VPN-a za prikrivanje mrežnih aktivnosti te upotrebu sustava za sprječavanje upada (IPS).

2.4. Informacijska sigurnost i sigurnost podataka

Informacija predstavlja osnovno obilježje informacijske znanosti, informacijskog doba, samog društva te tehnologije. Ukoliko želimo reći općenito, koncept pojma informacije je usko povezan s pojmovima poput upravljanja, oblika, ograničenja, podataka, komunikacije, znanja, uzorka, instrukcije, opažanja, značenja, predstavljanja te mentalnog podražaja (16). Informacijska sigurnost se postiže organizacijskom podrškom za poslove provjere, planiranja, dorade mjera i standarda i provedbe, kao i primjenom propisanih mjera i standarda informacijske sigurnosti. To je stanje cjelovitosti, povjerljivosti te raspoloživosti podatka. Opća pravila zaštite podataka su mjere informacijske sigurnosti koje su realizirane na tehničkoj, organizacijskoj ili fizičkoj razini. Informacijska sigurnost, odnosno njena područja, predstavljaju podjelu informacijske sigurnosti na pet područja:

- Fizička sigurnost,
- Sigurnosna provjera,
- Sigurnost informacijskog sustava
- Sigurnost podataka,
- Sigurnost poslovne suradnje.

Cilj ovakve podjele je učinkovita i sustavna realizacija donošenja, standarda informacijske sigurnosti, nadzora i primjena mjere. Također, u okviru informacijske sigurnosti bitno se dotaknuti mjera i standarda informacijske sigurnosti koje se utvrđuju za neklasificirane i klasificirane podatke. Mjere i standardi informacijske sigurnosti se utvrđuju shodno ugrozama neklasificiranih i klasificiranih podataka na nekoj određenoj lokaciji te sukladno broju, vrsti te stupnju tajnosti (17).

Člankom 2. Zakona o tajnosti podataka tajnim podatkom se smatra svaki dokument u umnoženom, slikovnom, pisanom, nacrtanom, magnetnom, tiskanom, snimljenom, elektroničkom

ili optičkom načinu, govorimo li o podacima, mjerama, predmetima, saznanjima, postupcima, informaciji ili usmenom priopćenju. Nadalje, trebamo razlikovati pojmove neklasificiranih, klasificiranih te deklasificirani podataka. Klasificirani podaci su oni koje je nadležno tijelo, prema propisanom postupku, označilo kao tajne te im je određen stupanj tajnosti. Također, to uključuje podatke koje je Republika Hrvatska primila kao tajne od međunarodne zajednice, drugih država ili institucija s kojima surađuje. Neklasificirani podaci su oni koji se koriste u službene svrhe, ali nemaju određeni stupanj tajnosti. To uključuje i podatke koje je Republika Hrvatska primila bez tajne oznake od međunarodne zajednice, drugih država ili institucija s kojima surađuje. Deklasifikacija podataka nastaje utvrđivanjem prestanka postojanja razloga zbog kojeg je neki određeni podatak utvrđen određenim stupnjem tajnosti pa se potom takav podatak koristi samo u službene svrhe. Nadležno tijelo, u čijem okviru djelovanja je podatak nastao bilo da je riječ o klasificiranom ili neklasificiranom podatku je vlasnik podataka koji su nastali, a pristup klasificiranim podacima omogućava certifikat koji predstavlja uvjerenje o sigurnosnoj provjeri. (18). Člankom 4. spomenutog Zakona određeni su stupnjevi tajnosti:

- Vrlo tajni,
- Tajni,
- Povjerljivi,
- Ograničeni.

Za navedenu klasifikaciju podatka se trajno provodi sigurnosna prosudba ugroze. „Vrlo tajno“ stupnjem tajnovitosti klasificiraju se podaci čijim bi se otkrivanjem nanijela nepopravljiva šteta vitalnim interesima Republike Hrvatske, kao i nacionalnoj sigurnosti naročito govoreći o vrijednostima poput: cjelovitosti i sigurnosti Republike Hrvatske, temeljima Ustavom utvrđenog ustrojstva Republike Hrvatske, neovisnosti, sigurnosti građana, osnovama gospodarskog i financijskog sustava Republike Hrvatske, sigurno . obavještajnom sustavu, tehnologija od važnosti za nacionalnu sigurnost Republike Hrvatske te znanstvenim otkrićima. „Tajno“ stupanjem tajnosti se klasificiraju podaci čijim bi se neovlašteno otkrivanjem teško naštetilo prethodno navedenim vrijednostima. „Povjerljivo“ stupnjem tajnosti se klasificiraju podaci čijim bi neovlaštenim otkrivanjem naštetilo navedenim vrijednostima. „Ograničeno“ stupnjem tajnosti se klasificiraju podaci čijim bi se neovlaštenim otkrivanjem kao posljedica dogodila šteta djelovanja i izvršenje zadaća državnih tijela pri obavljanju poslova (19).

2.5. Procedure

Kada govorimo o mjerama Europske Unije (u daljnjem tekstu EU) za zaštitu od kibernetičkih napada ,možemo reći, EU je aktivna u raznim područjima s ciljem promicanja kibernetičke otpornosti, kao i borbe protiv kibernetičkog kriminaliteta jačanjem kibernetičke obrane. Od 2016. godine ministarstvo pravosuđa EU-a raspravlja kako unaprijediti kazneno pravosuđa u kibernetičkom prostoru. Prva zakonodavna mjera na razini EU-a, Direktiva o sigurnosti mrežnih i informacijskih sustava (NIS) uvedena je 2016. Potom, šest godina nakon 2022. godine EU je revidirala direktivu o sigurnosti mrežnih i informacijskih sustava (NIS 2) kojom je novim pravilima dala odgovor sve jače kibernetičke prijetnje kojima su izložene sve članice EU uzimajući u obzir globalnu krizu koja je uslijedila nakon pandemije bolesti COVID-19 te nagli rast digitalne transformacije (20). Također, kao i sve zemlje članice, tako i Republika Hrvatska daje sve odgovore na kibernetičke prijetnje Zakonom o Kibernetičkoj sigurnosti, sustavom SK@UT, riječ je o najvećem projektu zaštite nacionalnog kibernetičkog prostora. (21) Nastavno na globalni rast digitalne transformacije i trend informacijskog društva uslijed kojeg se oplemenjuje razvoj tehnologija, unaprjeđuje kvaliteta komunikacija postavlja se ključno pitanje, na koji način je potrebno uspostaviti model zaštite podataka, pogotovo govoreći o zaštitih osobnih podataka koji se razmjenjuju unutar kibernetičkog prostora. Osobni podaci su najvrjedniji dio osobnosti, a odgovor EU tome je Regulativa zaštite podataka koja je stupila na snagu 27. travnja 2016.g. Opća EU uredba o zaštiti podataka 2016/679, u široj javnosti poznata pod nazivom GDPR – General Data Protection Regulation, izravno se primjenjuje na sve organizacije čija je odgovornost kontrola načina upravljana osobnim podacima EU građana, te unosi velike promjene u načinu upravljanja osobnim podacima. Hrvatska je, kao članica Europske unije, imala obvezu uskladiti svoje zakonodavstvo s Općom uredbom EU o zaštiti podataka (GDPR) do 2018. godine. Dio usvojenog zakonodavnog paketa, uz Opću uredbu, uključuje i Direktivu o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhu istrage, sprečavanja, otkrivanja ili progona kaznenih djela, te izvršavanja kaznenih sankcija, kao i slobodnom protoku takvih podataka. Ovom Direktivom se ujednačila zaštita osobnih podataka koje obrađuju pravosudna i policijska tijela unutar država članica.(22) U Republici Hrvatskoj, za nadzor neovisnog tijela zaduženog za zaštitu osobnih podataka i nadzor nad njihovom obradom odgovorna je Agencija za

zaštitu osobnih podataka (AZOP). Agencija za zaštitu osobnih podataka odgovorna je za osiguranje provedbe svih prava i obveza u području zaštite osobnih podataka.(23)

3. IZVORI PODATAKA I METODE

U hrvatskom jeziku pojam zaštite i umreženih sustava te sigurnost informacijskih sustava primarno označava primjenu zaštite svih komponenata informacijskih sustava, poput podataka, računala, osobe, programa i komunikacije. Kada govorimo o pojmu zaštite podataka većina ljudi pod tom prizmom smatra očuvanje tajnosti, zbog toga je ključno najprije istaknuti definiciju zaštite, koja uključuje očuvanje integriteta, dostupnosti i povjerljivosti podataka. Naglasak se obično stavlja na cjelovitost podataka i njihovu pravodobnu dostupnost, dok se povjerljivost uglavnom odnosi na manji dio podataka koji su klasificirani kao osobna, službena, poslovna, vojna ili državna tajna. Glavni cilj zaštite i sigurnosti podataka u umreženim sustavima je eliminacija prijetnji kojima je sustav izložen.

Kada govorimo o zaštiti informacijskog sustava te podataka istu dijelimo na:

- Unutarnju zaštitu: Fokusira se na zaštitu unutar same organizacije, uključujući kontrolu pristupa, enkripciju podataka i sigurnosne politike.
- Vanjsku zaštitu umreženih sustava: Usmjerena na obranu od vanjskih prijetnji, kao što su vatrozidi, zaštita od DDoS napada i sigurnosne mrežne mjere. (24)

Jedna od metoda razlikovanja vanjske i unutarnje zaštite je kontrola uz pomoć računala te u tim slučajevima istu klasificiramo kao unutarnju zaštitu.

3.1. Podjela zaštite i sigurnosti podataka

Podjela zaštite i sigurnosti podataka u umreženim sustavima može se razvrstati u sljedeće kategorije:

- Tehnička sigurnost: Zaštita softvera, mreža i podataka od kibernetičkih napada pomoću enkripcije, antivirusnih programa.
- Fizička sigurnost: Zaštita hardverske infrastrukture od fizičkih prijetnji poput krađe ili oštećenja.
- Pravna i regulatorna sigurnost: Usmjerenost na usklađivanje s pravnim regulativama i standardima zaštite podataka, poput GDPR-a.
- Organizacijska sigurnost: Uvođenje sigurnosnih politika, procedura i pravila za zaštitu sustava i podataka. (25)

Hardversko-softverska zaštita i sigurnost, kao i fizička i organizacijska zaštita i sigurnost sa stajališta sigurnosti umreženih sustava su minimum zaštite pojedine organizacije ili osoba gledajući iz perspektive organizacije i zaštite primjerene tehnološkom napretku.
Zakonodavna zaštita i sigurnost obrađena je Općom EU uredbom o zaštiti podataka spomenutom u prethodnom poglavlju. Na posljednju navedenu kategoriju komunikacijske zaštite (kriptozaštita) i informacijske sigurnosti treba obratiti posebnu pažnju jer polazi od zaštite osobnih prava i zaštite privatnosti te o sigurnosti osoba.
Suvremeni način poslovanja i razmjena informacija putem globalnih mreža doveli su do sve veće povezanosti, kako među ljudima, tako i među informacijskim sustavima. Sve veća povezanost i uključivanje informacijskih sustava na Internet, u globalne informacijske mreže, kao i na mnoge druge mreže koje su nastale logičnim razvojem poput WLAN-a, doveli su do potrebe promatranja zaštite tih sustava kao cjeline, umjesto izoliranog rješavanja segment po segment, što je bio slučaj u prošlosti. Otvorenost informacijskih sustava, uz sve veći broj korisnika, dodatno je oslabila sigurnost. Zbog toga je potrebno pristupiti ovom problemu s šireg aspekta, uzimajući u obzir informacijske mreže koje objedinjuju više segmenata. „Dakle, pitanje sigurnosti i zaštite interneta postaje jedno od osnovnih pitanja, kako za same informacijske sustave i njihove korisnike, tako i za cijelu međunarodnu zajednicu“ (24).

3.2. Krizno upravljanje i analiza rizika kibernetičke sigurnosti

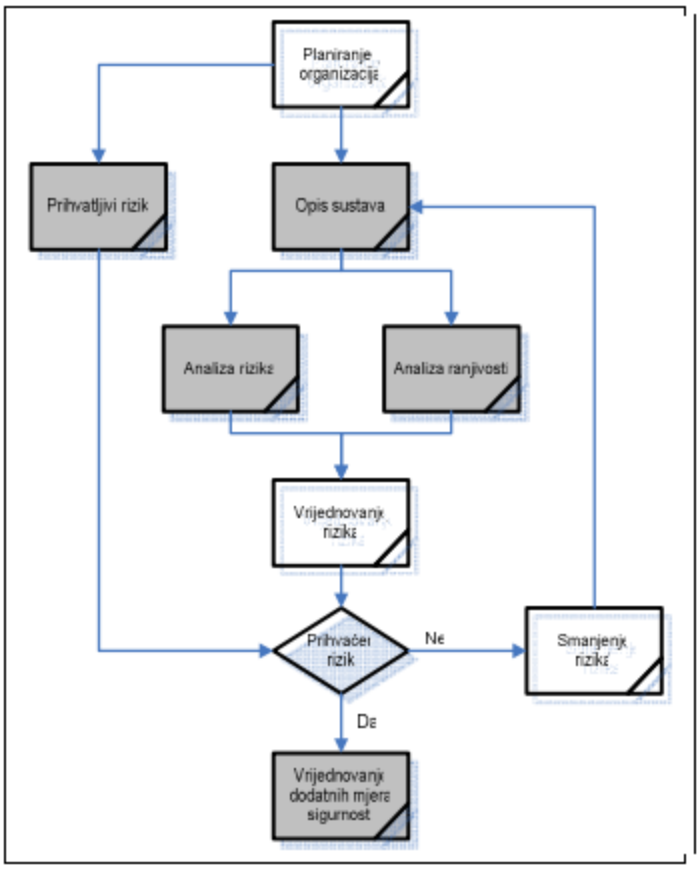
World Wide Web komunikacija na razne načine olakšava prijenos „znanja“ , kao i podataka, kako na globalnoj razini, tako i na nacionalnoj. Posljedice navedenog su novi: komunikacijski obrasci, konfiguracije znanja, sustavi edukacije, tipovi pismenosti te nove digitalne zajednice korisnika. Sustavna i planska digitalizacija znanja je pretpostavka nacionalnog i lokalnog djelovanja u globalnom informacijskom prostoru. Zaključak istoga je kako je javno znanje u cyber prostoru podložnije upravljanju i oblikovanju u puno većoj mjeri nego što je javno znanje na konvencionalnim medijima i konvencionalnoj formi. „Međutim, za rješavanje globalnih pitanja, zajedničkih za cijelu mrežu nadležan je World Wide Web Consortium ili W3C“ (24). Kako je s vremenom došlo do što većeg broja korisnika Interneta došlo je do rasta i promjena količine dostupnih informacija. Također, zbog navedene činjenice dolazi i do potrebe za što većom informacijskom pismenosti kao i težnje za povećanjem svijesti o potrebi zaštite, kao i sigurnosti, pri razmjeni informacija putem Interneta. Najčešći ciljevi napadača su upravo podaci, korisničke

lozinke te informacije o samoj memoriji kompjutera, odnosno o datotekama, web stranicama koje korisnik pretražuje, računalnim programima kojima se koristi, a sve s ciljem ograničavanja računalnog sustava (26).

Najveći izazov za okruženje govoreći o privatnom ili javnom sektoru, koji su suočeni sa rizicima svog poslovanja, predstavlja metodologija upravljanja sigurnošću informacijskih sustava uz pomoć koje se pronalazi strategija za rješavanje istih uz pomoć načela za umanjivanja sigurnosnih rizika. Upravljanje rizicima je kao i svaki drugi upravljački proces te ga je potrebno pomno planirati. Ukoliko se želi prevenirati rizike, treba se obratiti pozornost kada se planiraju procesi na sljedeće aktivnosti:

- ispitivati vjerojatnosti i kvantifikaciju rizika,
- utvrđivanje odnosa troškova i koristi od primjene protumjera,
- identifikacija rizika,
- utvrđivanje prioriteta rizika,
- definirati mjere otklanjanja šteta koje mogu nastati,
- izbor najdjelotvornijih protumjera,
- modifikaciju plana i postupaka, kao i nadzor te reviziju (27).

Definiranjem rizika postoji direktan odnos između ranjivosti sustava i vjerojatnosti događanja štetnog događaja. Metodologija analize rizika predstavlja koliko je sustav ranjiv, odnosno kolika je vjerojatnost događanja neželjenih događaja i prijetnji, prikazana na Slici 7. (28).



Slika 7. Prikaz dijagrama tijeka procesa analize rizika (28)

Također, ukoliko se želi stvoriti učinkovita sigurnosna politika, potrebno je razmotriti mogućnosti njezine implementacije, što uključuje educiranje zaposlenika o njihovim odgovornostima te osiguranje da svaki djelatnik odgovara za pridržavanje te politike. Osim poznavanja određenog stupnja odgovornosti zaposlenici su obvezni provoditi određene procedure sigurnosne politike koje je definirala kompanija. (29)

3.3. Elektronički dokazi i računalna forenzička analiza

Elektronički dokazi, iako nemaju direktan učinak na slučaj počinjenje kaznenog djela, računalo je ključan čimbenik pri počinjenju kaznenog djela tijekom istraživanja počinjenja računalnog kriminaliteta. Kada govorimo o takvom postupku, radilo se o počinjenu djela putem mreže ili stvarnom fizičkom svijetu tada istražitelj može pretraživanje učiniti putem mreže kako bih došao do elektroničkih dokaza. Navedeni postupak se naziva računalna forenzička analize (30). Također, svakodnevne aktivnosti korisnika putem računalnih mreža, poput plaćanja računa, korištenja

elektroničke pošte, kao i raznih drugih načina komunikacije, omogućavaju razvoj različitih oblika napada na informacijske sustave. Čovjek sadašnjice je postao dio virtualnog svijeta koji mu postaje prirodni ambijent te on u njemu svakodnevno djeluje i živi u kojem ostvaruje svoje povijesno nastale potrebe (31).

Novim tehnološkim inovacijama dolazi do novih zloupotreba unutar računalnog sustava te je stoga zaštita od računalnog kriminaliteta jedna od najvažnijih funkcija. Mogućnost računalne prevare se susreće na svim razinama bilo da je riječ o regionalnim, lokalnim, nacionalnim ili pak svjetskim. Načinima na kojima dolazi do počinjenja zlodjela uvelike pridonose digitalni oblici dostupnih informacija i podataka kojima se pristupa na daljinu, upravljanje i manipuliranje te korištenje istih. Važno je naglasiti kako je kriminalne aktivnosti, čiji se razvoj događa rapidno a koje su potpomognute novim tehnologijama, istražiteljima vrlo teško pratiti te im je gotovo nemoguće držati korake s istima. Ključnu ulogu pri povećanja kriminalnih radnji imaju:

- brzi razvoj te širenje telekomunikacijskih uređaja,
- povećana zlouporaba komunikacijskih sredstava,
- munjevit razvoj, kao i sve složenija primjena tehnika kriminalističke analitike, operativnih metoda te računalnih mreža, omogućuje neovlašteni pristup,
- mediji koji u sve većim razmjerima neopravdano veličaju hakerske napade i vještine,
- korištenje računala i primjena mogućnosti koje nudi osobama koje nemaju duboko stručna znanja,
- hakerski BBS-ovi (engl. Bulletin Board System) koji razvijaju programe koji omogućavanju programe čija je namjena provala u sustave kao i tajnu komunikaciju,
- kompleksnost i sporost u donošenju te primjeni pravne regulative. (32)

Kako na globalnoj razini, kao i na razini Europske unije borba za suzbijanje kibernetičkog kriminaliteta je sve snažnija te se primjenjuje u gotovo svim sferama. Uzimajući u obzir kako se radi o globalnoj razini, ukoliko se želi spriječiti suzbijanje kibernetičkog kriminaliteta za isto nisu dovoljni samo ekspertne skupine i stručnjaci za sigurnost već je potrebno ostvariti sveobuhvatnu akciju zakonodavstva, kao i cjelovitiju koordinaciju kako bi došlo do sprječavanja napada.

3.4. Regulatorni okvir kibernetičke sigurnosti temeljen na implementaciji NIS Direktiva s naglaskom na NIS 2 Direktivu

Prvi korak u razvoju okvira kibernetičke sigurnosti poduzet je 6. srpnja 2016., kada je Europski parlament uključio u politiku Direktivu o sigurnosti mrežnih i informacijskih sustava (Direktiva (EU) 2016/1148). NIS Direktiva 1 (Direktiva (EU) 2016/1148), što je akronim za Network and Information Security (Mrežna i informacijska sigurnost), sastoji se od 75 uvodnih izjava, 27 članaka i tri priloga te je bila prva zakonodavna inicijativa na europskoj razini s ciljem jačanja suradnje između država članica i uspostavljanja početne harmonizacije u području kibernetičke sigurnosti. Svim državama članicama EU-a dano je 21 mjesec za uključivanje odredbi direktive u svoje nacionalne zakone. (NIS 1 Direktiva, 2016.) NIS Direktiva predstavlja prvi pravni akt o kibernetičkoj sigurnosti, čiji je cilj osigurati visoku razinu sigurnosti mrežnih i informacijskih sustava, što je nametnulo obvezu državama članicama EU-a da prenesu NIS Direktivu u nacionalno zakonodavstvo do 9. svibnja 2018. i identificiraju operatore ključnih usluga (OES) koji imaju poslovno sjedište na njihovom teritoriju do 9. studenog 2018. (NIS 1 Direktiva, Članak 25). Prije usvajanja NIS Direktive, svaka država članica unutar EU-a imala je vrlo različite razine pripravnosti u području kibernetičke sigurnosti, što je značilo da, u cjelini, postojeći kapaciteti nisu bili dovoljni za osiguranje visoke razine sigurnosti mrežnih i informacijskih sustava u Europskoj uniji. (33) S obzirom na činjenicu kako je nakon primjene spomenute direktive kibernetička otpornost u pojedinim zemljama članicama bila zavidnoj razini, dok je u drugima značajno zaostajala došlo je do potrebe za korigiranjem NIS direktive novom, NIS2 direktivom. Ovom Direktivom se uspostavlja unutarnji okvir kako bih se upravljalo kibernetičkim sigurnosnim rizicima, kontrolu rizika i upravljanje, kao i razmjena informacija o rizicima i izvještavanje. IICB je novo tijelo - Međuinstitucionalni odbor za kibernetičku sigurnost koji za zadatak ima praćenje provedbe Direktive. Uz navedeno IICB je dužan pružati podršku subjektima Unije u provedbi Direktive, strateško usmjeravanje CERT-EU-a i nadzor nad provedbom (34).

(NIS 1 Direktiva, 2016.) NIS Direktiva 1 identificira dvije kategorije područja kojima su upućene specifične odredbe:

- Operatori ključnih usluga (ESP) obuhvaćaju javna ili privatna područja koja imaju ključnu ulogu u društvu i ekonomiji, pružajući vitalne usluge (obično prepoznate kao kritična infrastruktura). Države članice izravno identificiraju ESP-ove u kritičnim sektorima (energija, transport, bankarstvo, financijska tržišta, zdravstvo, opskrba i

distribucija pitke vode te digitalna infrastruktura) Na osnovu važnosti usluge i rizika povezanih s incidentom koji je na nju utjecao,

- Pružatelji digitalnih usluga (DSP): Tvrtke koje pružaju usluge poput e-trgovine, računalstva u oblaku ili internetskih tražilica, osim ako se ne radi o malim i srednjim poduzećima (MSP).

NIS Direktiva 1 ostavlja državama članicama slobodu da prošire sektore/kategorije entiteta na koje bi se kibernetičke obveze trebale primjenjivati. Cilj NIS Direktive je stvoriti općenito višu razinu kibernetičke sigurnosti u EU. Operatori ključnih usluga uključuju sve organizacije čije bi poslovanje bilo uvelike pogođeno u slučaju sigurnosnog proboja ako se bave kritičnim društvenim ili gospodarskim aktivnostima. I DSP-ovi i OES-ovi sada su obvezni prijavljivati veće sigurnosne incidente timovima kao odgovor na računalne sigurnosne incidente (CSIRT). NIS Direktiva ima tri glavna cilja:

- poboljšanje nacionalnih kapaciteta za kibernetičku sigurnost implementacijom nacionalne strategije,
- jačanje suradnje na razini EU-a,
- promicanje kulture upravljanja rizicima i prijavljivanja incidenata za OES i DSP.

NIS Direktiva obuhvaća operatore ključnih usluga (OES) u sljedećim sektorima koji se smatraju ključnim uslugama:

- energija: električna energija, nafta i plin,
- promet: zračni, željeznički, vodni i cestovni promet,
- bankarstvo: kreditne institucije,
- infrastrukture financijskog tržišta: trgovačka mjesta, središnje druge ugovorne strane,
- zdravstvo: zdravstvene institucije,
- voda: opskrba i distribucija pitke vode,
- digitalna infrastruktura: internetske točke razmjene, pružatelji usluga sustava naziva domena (DNS), registri domena na najvišoj razini (TLD) (35).

U prosincu 2022. godine, NIS 2 Direktiva, Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za osiguranje visoke zajedničke razine kibernetičke sigurnosti u Uniji, kojom se mijenja Uredba (EU) br. 910/2014 i Direktiva (EU) 2018/1972, te

kojom se ukida Direktiva (EU) 2016/1148 (NIS 2 Direktiva), objavljena je. Ova direktiva odgovara na potrebu za ažuriranjem i jačanjem regulatornog okvira koji je pružala NIS Direktiva 1. Velike razlike u provedbi obveza prema NIS Direktivi 1 dovele su do neujednačenih razina sigurnosti i ranjivosti među državama članicama, s mogućim utjecajima na EU u cjelini. Cilj NIS Direktive 2 – koja ukida NIS Direktivu 1 – je eliminirati razlike između pravnih sustava, pojačati obveze u području kibernetičke sigurnosti, proširiti broj sektora i aktera uključenih u taj proces te pojačati suradnju među državama članicama s ciljem se postigla veća ujednačenost u primjeni (36).

Prvo je važno navesti tekuće rokove vezane uz uspostavu NIS 2 Direktive u državama članicama:

- Do 17. listopada 2024. godine, države članice moraju usvojiti i objaviti mjere potrebne za usklađivanje s NIS 2 Direktivom,
- Do 17. srpnja 2024. godine i svakih 18 mjeseci nakon toga, EU-CyCLONe mora podnijeti izvještaj o evaluaciji Europskom parlamentu i Vijeću,
- Do 17. listopada 2024. godine, Komisija će usvojiti provedbene akte koji će definirati tehničke i metodološke zahtjeve za mjere koje se odnose na pružatelje DNS usluga, registrima naziva domena na najvišoj razini (TLD), pružateljima usluga računalstva u oblaku, pružateljima usluga podatkovnih centara, pružateljima upravljanih usluga, pružateljima upravljanih sigurnosnih usluga, online tržnicama, online tražilicama i platformama društvenih mreža, te pružateljima usluga povjerenja,
- Dana 17. siječnja 2025. godine, Grupa za suradnju će, uz pomoć Komisije i ENISA-e te, prema potrebi, mreže CSIRT-ova, Uspostaviti metodologiju i organizacijske aspekte vršnjačke revizije s ciljem razmjene iskustava, jačanja međusobnog povjerenja i postizanja visoke zajedničke razine kibernetičke sigurnosti, kao i jačanja kapaciteta i politika kibernetičke sigurnosti država članica potrebnih za provedbu ove Direktive. Sudjelovanje u reviziji je dobrovoljno. Stručne provjere provode eksperti za kibernetičku sigurnost koje imenuju najmanje dvije države članice, osim države članice koja se pregledava,
- Države članice će do 17. travnja 2025. uspostaviti popis ključnih i važnih entiteta, uključujući entitete koji pružaju usluge registracije naziva domena. Taj će popis biti redovito pregledavan, a najmanje svake dvije godine ažuriran, prema potrebi.
- Do 17. travnja 2025. godine nadležna tijela će, svakih dvije godine nakon toga, obavijestiti Komisiju i Grupu za suradnju o broju ključnih i važnih subjekata u svakom sektoru,

- Do 17. listopada 2027. godine će Komisija, kao i svakih 36 mjeseci nakon toga, pregledavati funkcioniranje ove Direktive i podnijeti izvještaj Europskom parlamentu i Vijeću. (37)

Prema Članku 20 (Upravljanje), upravna tijela ključnih i važnih područja moraju odobriti mjere za upravljanje rizicima u kibernetičkoj sigurnosti koje ti entiteti poduzimaju, pratiti njihovu provedbu te "mogu biti odgovorna za kršenja". Također, u skladu s Člankom 20, države članice su dužne osigurati da "članovi upravnih tijela ključnih i važnih entiteta moraju pohađati obuku" te poticati ključne i važne entitete da redovito pružaju sličnu obuku svojim zaposlenicima, kako bi stekli dovoljno znanja i vještina za omogućavanje identifikacije i procjene rizika te upravljanje praksama kibernetičke sigurnosti i njihovim utjecajem na usluge koje entitet pruža (NIS 2 Direktiva, Članak 20). Prilikom procjene proporcionalnosti ovih mjera, potrebno je uzeti u obzir stupanj izloženosti entiteta rizicima, veličinu entiteta, vjerojatnost pojave incidenata te njihovu ozbiljnost, uključujući društveni i ekonomski utjecaj. Mjere NIS 2 Direktive temelje se na mjerama za upravljanje rizicima u kibernetičkoj sigurnosti koje imaju za cilj zaštititi mrežne i informacijske sustave te fizičko okruženje navedenih sustava od incidenata, a uključivat će "najmanje" sljedeće:

- politike za analizu rizika i sigurnost informacijskih sustava,
- postupak u slučaju incidenata,
- kontinuirano poslovanje, poput upravljanja sigurnosnim kopijama i oporavka od katastrofa, te krizno upravljanje,
- sigurnost u lancima opskrbe, uključujući aspekte sigurnosti u odnosima između pojedinca i njegovih izravnih dobavljača ili pružatelja usluga,
- sigurnost pri nabavi, razvoju i održavanju mrežnih i informacijskih sustava, s naglaskom na upravljanje ranjivostima i njihovo otkrivanje,
- politike i postupci za evaluaciju učinkovitosti mjera upravljanja rizicima u kibernetičkoj sigurnosti,
- politike i postupke vezane uz korištenje kriptografije i, gdje je primjenjivo, enkripcije,
- korištenje višestruke autentifikacije ili rješenja za kontinuiranu autentifikaciju, osigurane glasovne, video i tekstualne komunikacije te osigurani sustavi za hitnu komunikaciju unutar entiteta, gdje je primjenjivo (37).

Kako bih se poboljšanju koordinacije i odgovora na kibernetičke krize na razini cijele Europske unije Europska unija je uspostavila Europsku mrežu za povezivanje organizacija za kibernetičke krize (EU-CyCLONe). EU-CyCLONe sastoji se od predstavnika tijela za upravljanje kibernetičkim krizama država članica, kao i, u slučajevima kada potencijalni ili tekući veliki kibernetički incident ima ili bi mogao imati značajan utjecaj na usluge i aktivnosti koje potpadaju pod ovu Direktivu, Komisije. U drugim slučajevima, Komisija će sudjelovati u aktivnostima EU-CyCLONe-a kao promatrač. NIS 2 Direktiva, Članak 15, stavak 3kaže kako EU-CyCLONe ima sljedeće zadatke: povećati razinu pripremljenosti za upravljanje velikim kibernetičkim incidentima i krizama; razviti zajedničku situacijsku svijest o velikim kibernetičkim incidentima i krizama; procijeniti posljedice i utjecaj relevantnih velikih kibernetičkih incidenata i kriza te predložiti moguće mjere za ublažavanje; koordinirati upravljanje velikim kibernetičkim incidentima i krizama te podržati donošenje odluka na političkoj razini u vezi s takvim incidentima i krizama; raspravljati, s obzirom na zahtjev zainteresirane države članice, o nacionalnim planovima kao i pripremiti odgovor na velike kibernetičke incidente i krize iz Članka 9(4) (37). Provedba NIS2 Direktive od strane relevantnih entiteta također će uključivati razmatranje okvira već uspostavljenog Općom uredbom o zaštiti podataka (GDPR) (33).

3.5. Zaštita osobnih podataka i nova opća uredba o zaštiti podataka (GDPR)

Nezaustavljivi razvoj informacijskog društva poboljšava kvalitetu komunikacije i potiče tehnološki napredak, ali nosi sa sobom i važan zadatak - uspostavu sustava zaštite podataka, posebno osobnih podataka, koji su ključni dio ljudske osobnosti i individualnosti. U skladu s globalnim trendovima, jedan od glavnih ciljeva reforme regulative o zaštiti podataka, koja je stupila na snagu 27. travnja 2016., jest osigurati učinkovitu zaštitu privatnosti. (38). Četiri godine pregovora te više od sedam godina prošlo je od početka inicijative do konačnog usvajanja okvira. Opća uredba EU o zaštiti podataka 2016/679 (GDPR) donosi značajne promjene u načine upravljanja osobnim podacima i izravno se primjenjuje na sve organizacije koje obrađuju osobne podatke građana Europske unije. (39) Sastavni dio usvojenog zakonodavnog paketa, pored navedene Opće uredbe, je i Direktiva o zaštiti pojedinaca kada se obrađuju osobni podaci od strane tijela koja su za navedeno nadležna a u svrhu istrage, otkrivanja, sprečavanja ili izvršavanja kaznenih sankcija, kao i slobodnom kretanju podataka2016/680. Navedenom Direktivom

ujednačit će se zaštita osobnih podataka pri obradi istih od strane pravosudne policije i policijskih tijela u država koje su članice Europske unije. Ukoliko je potrebno, navedena Direktiva omogućava obradu osobnih podataka ispitanika, te uključuje njihovo iznošenje u treće zemlje kao i osiguravanje visokih standarda zaštite pojedinaca proporcionalno potrebama pri provedbi odgovarajućih pravosudnih i policijskih postupaka. Ova Direktiva jasno utvrđuje nadzor neovisnog tijela za zaštitu osobnih podataka nad njihovom obradom. Važno je napomenuti da GDPR zamjenjuje Direktivu 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnim protokom takvih podataka. GDPR stupa na snagu danom donošenja i izravno se primjenjuje u svim državama članicama EU-a. (40) Za provedbu osiguranja usklađenosti organizacije nužni su eksperti koji razumiju primjenu GDPR-a te koji imaju vještine: implementacije, planiranja te održavanja usklađenosti organizacije s obzirom na Uredbu.

Članak 37. EU Opća uredba o zaštiti podataka propisuje da, stupanjem GDPR-a na snagu, kompanije imaju obvezu imenovati kvalificiranog službenika za zaštitu podataka (engl. Data Protection Officer - DPO), koji će izravno odgovarati Upravi. Nadalje, prema čl. 38 GDPR-a službenik za izvršavanje odgovara izravno upravi te ima zadatak djelovati neovisno pri izvršenju obveza. Također, prema. čl. 37. st. 3. GDPR-a kaže da se za izvršitelja obrade ili voditelj obrade, ukoliko se radi o tijelu javne vlasti ili javnom tijelu, kada govorimo o više takvih tijela ili vlasti, tada se također može imenovati jedan službenik za zaštitu podataka, s tim da se treba uzeti u obzir njihova veličina, kao i njihova organizacijska struktura. Ukoliko osoba želi postati službenik za zaštitu podataka mora imati kvalifikacije koje se temelje na stručnim kvalifikacijama, a posebno stručna znanja o praksama i pravu iz područja zaštite podataka i sposobnost vršenja zadataka koje nalaže članak 39 GDPR-a.

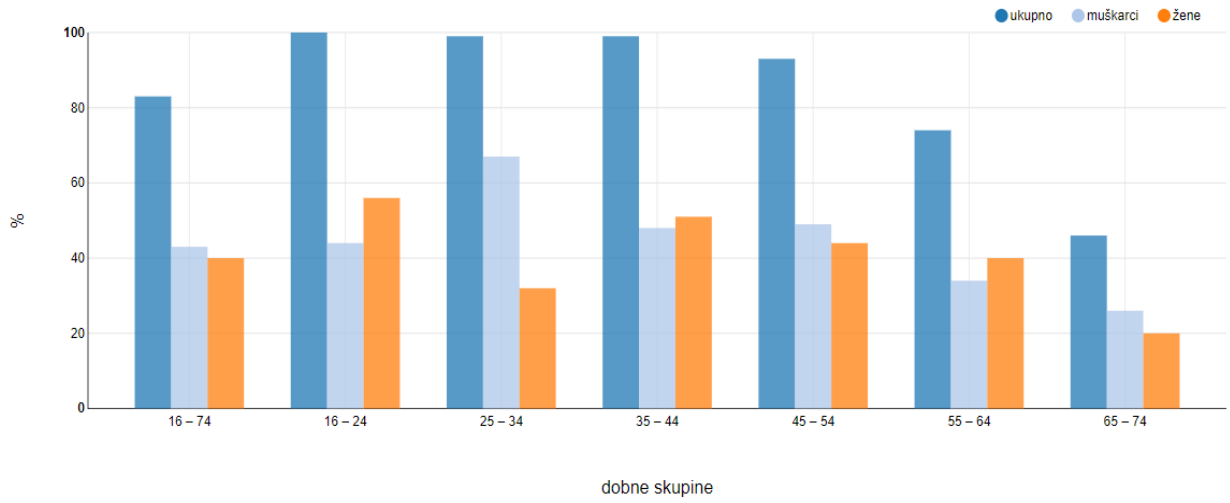
Službenik za zaštitu podataka, uz razumijevanje osnovnih procesa i klasifikacije obavlja najmanje navedene zadaće:

- informirati te savjetovati izvršitelja obrade ili voditelja obrade, kao i zaposlenike koji obrađuju podatke, o njihovim obvezama prema ovoj Uredbi i zakonima države članice koje se odnose na zaštitu podataka.,
- pratiti poštovanja navedene Uredbe, odnosno države članice o politikama i zaštiti podataka izvršitelja obrade ili voditelja obrade sukladno pravilima o zaštiti osobnih podataka, što uključuje raspodjelu podizanje svijesti, educiranje osoblja i odgovornosti svih koji su zaduženi sudjelovati u postupcima obrade podataka i povezanim revizijama

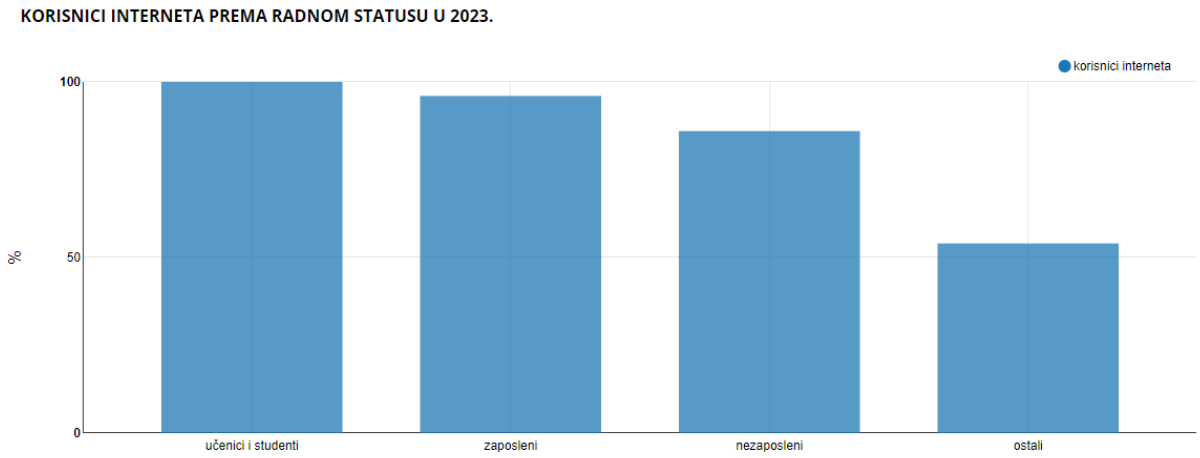
- ukoliko je zatraženo pružiti savjet, kao i pratiti njezino izvršavanje u skladu s člankom 35.,
- surađivati s nadzornim tijelima,
- djelovati kao poveznica za nadzorno tijelo te pri obavljanju svojih zadaća službenik za zaštitu podataka ima zadatak voditi računa o riziku koji je povezan s postupcima obrade te sagledati prema čl. 39. st. 2 opseg, prirodu, svrhu obrade i kontekst (40).

4. REZULTATI

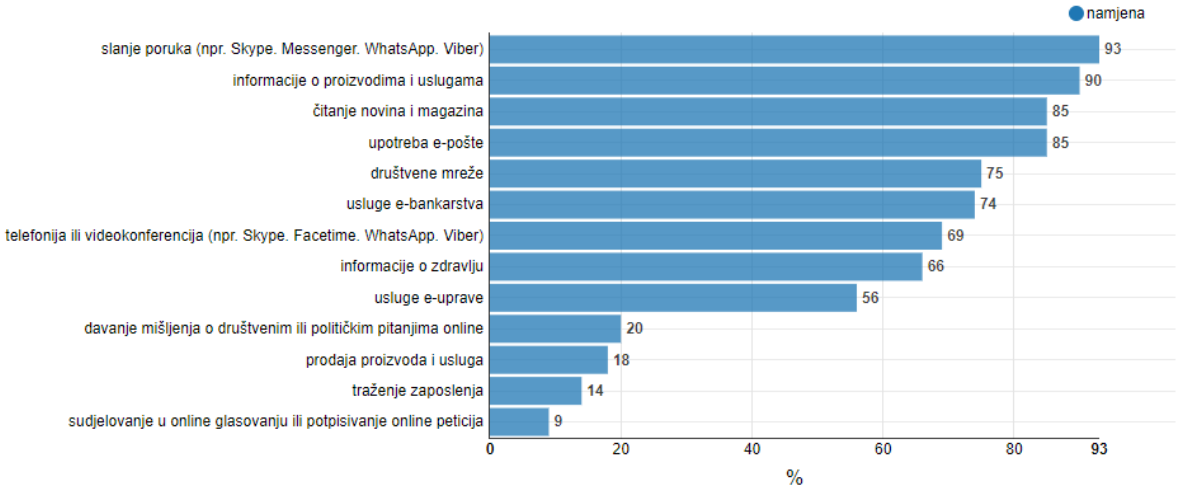
U svom trenutnom opsegu skoro cijeli svijet komunicira unutar kibernetičkog prostora, bilo da se gleda iz perspektive uporabe interneta po dobnim skupinama i prema spolu, korisnicima interneta prema radnom statusu, namjeni upotrebe interneta kod pojedinaca ili pak internetskoj kupnji kod pojedinaca. Svakim danom, sve više korisnika različitih dobnih skupa razmjenjuje informacije putem Interneta što možemo vidjeti na grafu prikazanom na Slici 4. koji prikazuje upotrebu interneta u 2023. godini prema dobnim skupinama i prema spolu. Osim navedenog grafa zanimljivo je promatrati i korisnike interneta prema radnom statusu u 2023., a isto je prikazano na Slici 5. Najveći porast uporabe Interneta je u dobnoj skupini od 65 do 74 godine, očekivano najmlađa populacija prednjači u upotrebi interneta, dok je sami broj korisnika proporcionalan njihovoj dobi. Promatrajući strukturu prema radnom mjestu, iz grafa na Slici 5. možemo primijetiti kako učenici i studeni najčešće upotrebljavaju internet. Također, zanimljivo je promotriti namjenu upotrebe interneta kod pojedinaca u 2023. godini, a koja je prikazana na Slici 6. Korisnici Internet najčešće koriste za slanje poruka (93%), prikupljaju informacije o proizvodima i uslugama (91%), čitajući dnevne novosti i časopise (90%), koriste e-poštu (80%), sudjeluju na društvenim mrežama (75%). Ukoliko pojedinac nije dovoljno educiran o napadima koji se mogu dogoditi prilikom razmjene informacija, kao i o pretraživanju istih, davanjem osjetljiv podataka poput osobnih podataka tada posljedica može biti ugrožavanje osobne esencije. Svaki segment ovakve komunikacije osim navedene ugroženosti esencije može dovesti i do povrede dostupnosti, cjelovitosti kao i tajnosti podataka (41).



Slika 4. Prikaz upotrebe interneta u 2023. godini po dobnim skupinama i prema spolu (41)



Slika 5. Prikaz upotrebe interneta u 2023. godini prema radnom statusu (41)



Slika 6. Prikaz namjene upotrebe interneta kod pojedinaca u 2023. (41)

Uslijed povećane uporabe interneta dolazi i do sve većih pokušaja, manje ili više uspješnih, što prikazuju Tablica 2. i Tablica 3. U Tablici 2. možemo vidjeti prikaz računalnih i kibernetičkih kriminaliteta prema kaznenim dijelima u 2023. godini, dok u Tablici 3. možemo vidjeti usporedbu prikaza kaznenih djela kibernetičkog kriminaliteta kao i usporedbu istih u 2022. godini i 2023. godini.

Tablica 2. Prikaz kaznenih djela kibernetičkog kriminaliteta (42)

Kaznena djela	Prijavljena kaznena djela			Razriješena kaznena djela		Naknadno razriješena kaznena djela	
	Ukupno	Zatečen	Nepoznat	Ukupno	u %	Ukupno	u %
Neovlašten pristup	48		46	17	35,4	15	32,6
Ometanje rada računalnog sustava	5		5	1	20,0	1	20,0
Oštećenje računalnih podataka	39		39	5	12,8	5	12,8
Neovlašteno presretanje računalnih podataka	1		1	1	100,0	1	100,0
Računalno krivotvorenje	20		17	18	90,0	15	88,2
Računalna prijevara	1.571		1.543	604	38,4	576	37,3
Zlouporaba naprava	4		3	3	75,0	2	66,7
Iskorištavanje djece za pornografiju	342	3	275	330	96,5	263	95,6
Povreda žiga	2		2	2	100,0	2	100,0
UKUPNO	**2.032**	**3**	**1.931**	**981**	**48,3**	**880**	45,6

Tablica 3. Prikaz usporedbe kaznenih djela kibernetičkih kriminaliteta (42)

Kaznena djela	Prijavljena kaznena djela			Razriješena kaznena djela			Naknadno razriješena kaznena djela		
	Broja djela		Trend u %			Trend u %			Trend u %
	2022.	**2023.**		2022.	**2023.**		2022.	**2023.**	
Neovlašten pristup	31	**48**	+54,8	13	**17**	+30,8	8	**15**	+87,5
Ometanje rada računalnog sustava	5	**5**	0,0	2	**1**	-50,0	1	**1**	0,0
Oštećenje računalnih podataka	25	**39**	+56,0	7	**5**	-28,6	5	**5**	0,0
Neovlašteno presretanje računalnih podataka	8	**1**	-87,5	3	**1**	-66,7	2	**1**	-50,0
Računalno krivotvorenje	39	**20**	-48,7	38	**18**	-52,6	38	**15**	-60,5
Računalna prijevara	1.425	**1.571**	+10,2	771	**604**	-21,7	749	**576**	-23,1
Zlouporaba naprava	7	**4**	-42,9	7	**3**	-57,1	7	**2**	-71,4
Iskorištavanje djece za pornografiju	311	**342**	+10,0	308	**330**	+7,1	252	**263**	+4,4
Povreda žiga	13	**2**	-84,6	13	**2**	-84,6	5	**2**	-60,1
UKUPNO	**1.864**	**2.032**	**+9,0**	**1.162**	**981**	**-15,6**	**1.067**	**880**	**-17,5**

Analizirajući Tablicu 2. možemo uvidjeti kako se povećava svijest ljudi o prijavljenim kaznenim djelima te da najviše kaznenih djela kibernetičkog kriminaliteta kod računalnih prevara te iskorištavanje djece za pornografiju putem interneta što ukazuje na dvije činjenice, prva je kako treba povećavati svijest građana te ih što više educirati o potencijalnim napadima kojima mogu biti izloženi uzevši u obzir činjenicu iz prethodnih grafova kako je porast upotrebe korištenja interneta u svim dobnim skupinama. Druga činjenica koja zabrinjava je kako je velik broj iskorištavanje djece za pornografiju putem interneta što ukazuje na činjenicu da iako je velik broj učenika na internetu, prikazano na Slici 5. i dalje je velika needuciranost istih. Zanimljivo je također, analizirajući Tablicu 3. koja prikazuje usporedbu prikaza kaznenih djela kibernetičkih kriminaliteta u 2022. i 2023. godini kako su kaznena djela u porastu što potvrđuje prethodnu tezu o nedovoljnoj educiranosti te potrebi za što većom primjenom kako NIS2 direktive tako i Opće Uredbe. U Tablici 4. je prikazana razlika između Direktive 95/46/EZ i GDPR-a.

Tablica 4. Prikaz razlike Direktiva 95/46/EZ i GDPR-a

Direktiva 95/46/EZ	GDPR
• Identitet kontrolora • Svrhe obrade • Obaveza odgovoriti na subjekta podataka • Pravo pristupa, ispravaka i prigovora • Primatelji • Prijenos podataka	• Identitet kontrolora i DPO-a • Svrha • Razdoblje čuvanja podataka • Pravo pristupa, ispravaka, ograničenja i prigovora • Pravo na podnošenje žalbe • Primatelji • Prijenosi • Pravo povlačenja suglasnosti u bilo kojem trenutku • Legitiman interes kontrolora ili treće osobe (ako je relevantno) • Informacije o profiliranju • Sve ostale informacije koje jamče zakonitost prerade

Opća uredba o zaštiti podataka, uredba čiji je cilj zaštita pojedinaca vezano uz obradu osobnih podataka kao i slobodnome kretanju takvih podataka, predstavlja bitan i veliki napredak u području zaštite osobnih podataka. Donošenjem ovakve odluke osigurava se jednoobrazno i ujednačeno djelovanje nadzornih tijela za zaštitu osobnih podataka, a rezultat tome su jednaka i jednostavnija zaštita prava svakog pojedinca zemalja članica Europske unije. Uredbom se pojednostavljuju postojeće definicije, a uvode se i nove, određuju se genetski i biometrijski podaci. Najveća novost ove Uredbe je obveza procjene učinka koja kaže, sukladno čl. 35.st.1. GDPR-a, ukoliko postoji vjerojatnost da neka vrsta obrade, a pogotovo one putem novih tehnologija uzevši u obzir opseg, prirodu, svrhu i kontekst obrade, može prouzročiti visok rizik za slobodu i prava pojedinaca. U

takvim slučajevima dužnost voditelja obrade je, prije same obrade osobnih podataka, provoditi procjenu učinka postupaka koji su predviđeni postupkom obrade za zaštitu osobnih podataka (39). Također, kako bismo spriječili kaznena djela kibernetičkog kriminaliteta, strategije poput Nacionalne strategije kibernetičke sigurnosti imaju primarni cilj uspostaviti učinkovitu i racionalnu koordinaciju različitih institucija za uspješno suočavanje s prijetnjama u kibernetičkom prostoru. Naime, treba uzeti u obzir da se stvaranjem strategije svi problemi vezani uz računalne sustave i komunikaciju u kibernetičkom prostoru ne mogu riješiti odjednom (43). To je samo početna ideja za poboljšanje trenutnog stanja kada govorimo o komunikaciji i kibernetičkoj sigurnosti uopće. Osim toga, cilj takve strategije je zaštititi sve korisnike modernih elektroničkih usluga, kako u javnom, tako i u privatnom sektoru. Na taj način bi se povećala svijest o važnosti kibernetičke sigurnosti, kao i o mehanizmima za razmjenu podataka i pristup informacijama. Razvoj usklađenih obrazovnih programa u školama i sveučilištima bio bi potaknut povezivanjem akademskog, javnog i gospodarskog sektora. Kako bih kibernetički prostor bio jasno definiran, siguran i funkcionalan, ključno je imati angažirane i odgovorne sudionike. Svaki sudionik treba preuzeti odgovornost za provođenje mjera unutar svoje nadležnosti, surađivati s ostalima i prilagođavati se prema potrebi. Integracija različitih sektora društva i koordinacija institucija omogućuje učinkovit proces kibernetičke sigurnosti u specifičnim situacijama. (33).

NIS 2 Direktiva uvodi posebne odredbe o zaštiti osobnih podataka (posebno u vezi s međunarodnom suradnjom ili provedbom baza podataka za registraciju naziva domena). Obveza prijave svakog kršenja osobnih podataka koje proizlazi iz incidenta navedena je u članku 23 nove direktive. (NIS 2 Direktiva, Članak 23) Od velike je važnosti da entiteti moraju obavijestiti nacionalni CSIRT ili drugo nacionalno tijelo o svakom značajnom incidentu koji ima veliki utjecaj na pružanje njihovih usluga. Značajan incident, po definiciji, je incident koji je prouzročio ili bi mogao prouzročiti ozbiljan operativni poremećaj u pružanju usluga ili financijski gubitak za dotični entitet, ili je takav incident utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe, uzrokujući znatnu materijalnu, fizičku ili moralnu štetu. U području kibernetičke sigurnosti, prilikom rješavanja incidenata, može doći i do kršenja osobnih podataka kao posljedice tih incidenata. Prilikom rješavanja incidenata koji dovode do kršenja osobnih podataka, nadležna tijela moraju usko surađivati s nadzornim tijelima u skladu s Uredbom (EU) 2016/679, ne dovodeći u pitanje nadležnost i zadaće nadzornih tijela. Dakle, u kontekstu nadzora ili provedbe obveza prema Direktivi, kada nadležna tijela postanu svjesna kršenja koje je počinio ključni ili važni

entitet u vezi s obvezama iz članaka 21. i 23., a to kršenje može dovesti do kršenja osobnih podataka, nadležno tijelo mora bez odgode obavijestiti nadzorna tijela. U skladu s Člankom 32 GDPR-a, voditelji obrade i izvršitelji obrade podataka provode potrebne organizacijske, kao i tehničke mjere kako bi osigurali razinu sigurnosti primjerenu riziku. Članak 21. Direktive utvrđuje srodnu obvezu kibernetičke sigurnosti za ključne i važne entitete, koji moraju poduzeti tehničke, operativne i organizacijske mjere za upravljanje rizicima koji ugrožavaju sigurnost mreža i informacijskih sustava koje ti entiteti koriste u obavljanju svojih aktivnosti ili pružanju usluga. Ove provedene mjere kibernetičke sigurnosti tako doprinose usklađenosti s obvezama zaštite osobnih podataka utvrđenim u Članku 32. GDPR-a. Uvodi 77 i 78 NIS 2 Direktive podržavaju ovaj pristup, jer su ključni i važni entiteti odgovorni za osiguravanje sigurnosti mreža te informacijskih sustava. Također, od strane tih entiteta sigurnosni podaci se prenose, pohranjuju, te obrađuju (33). Prilikom obrade osobnih podataka i provođenja ove vrste analize rizika i sigurnosne politike, entiteti bi trebali razmotriti provođenje procjene učinka na zaštitu podataka (PIA). Ova analiza učinka uključivat će tehnički dio koji se odnosi na rizike za sigurnost podataka. Taj dio omogućit će voditelju obrade/entitetu da utvrdi tehničke i organizacijske mjere potrebne za zaštitu podataka. Te mjere su inherentne kibernetičkoj sigurnosti. Kako bi pokazao usklađenost s NIS 2 Direktivom i GDPR-om, na kraju će biti ključno za entitet da dokumentira svoje analize i mjere koje je poduzeo (44).

5. RASPRAVA

Kibernetička sigurnost postaje sve važnija u globalnom kontekstu digitalizacije i povezanosti. Rasprava o kibernetičkoj sigurnosti obuhvaća nekoliko ključnih tema poput: prijetnji i napada rast sofisticiranih napada, poput ransomware-a, phishinga i napada sponzoriranih od strane država (APT - Advanced Persistent Threats). Napadi ciljaju kritičnu infrastrukturu, državne institucije, privatne kompanije, ali i pojedince. Tehnološka rješenja kao to su: implementacija naprednih tehnologija, uključujući AI, strojno učenje, pomažu u otkrivanju i odgovoru na prijetnje. Sigurnosni sustavi moraju biti fleksibilni i sposobni prilagoditi se novim prijetnjama. Primjena Regulativa i zakona te važnost usklađivanja sa zakonodavstvom, poput GDPR-a, te usvajanje novih regulativa koje mogu pomoći u zaštiti podataka i osiguravanju privatnosti mogu biti odgovor prijetnjama. Osim Zakona, Uredbi i Direktiva edukacija korisnika o sigurnosnim prijetnjama ključna je za smanjenje rizika. Ljudi su često najslabija karika u sigurnosnom lancu, pa je podizanje svijesti o kibernetičkim prijetnjama presudno. Rezultati koji su analizirani u prethodnom poglavlju ukazuju kako se sve više ljudi koristi kibernetičkim prostorom, ali i kako je sve više napada kibernetičkih napada i kibernetičkih kaznenih djela. Samim tim dolazi do učestalih kibernetičkih napada poput onih:

- U 2015. godine zabilježen je kibernetički napad na Ministarstvo vanjskih i europskih poslova Republike Hrvatske. Napadači su uspjeli prodrijeti u informacijske sustave ministarstva i potencijalno su imali pristup povjerljivim informacijama.
- U 2016. godine grupa Anonymous Hrvatska izvršila je napade na nekoliko vladinih web stranica, uključujući web stranicu Vlade RH, u sklopu svojih aktivnosti protiv korupcije i drugih društvenih problema. Ovi napadi su uključivali promjenu sadržaja na web stranicama i privremeno njihovo obaranje.
- U 2017. godine došlo je do napada na računalne sustave nekoliko ministarstava, uključujući Ministarstvo unutarnjih poslova i Ministarstvo obrane. U tim napadima kompromitirane su određene datoteke, ali su poduzete mjere za sprječavanje većih šteta.
- U 2019. godine nekoliko hrvatskih banaka bilo je meta sofisticiranih kibernetičkih napada usmjerenih na krađu podataka s kreditnih kartica i druge financijske prijevare. Ovi napadi pokazali su ranjivost financijskog sektora na napredne metode napada.

- Ransomware napad 2020. godine zabilježen je ransomware napad na bolničke ustanove, uključujući bolnice u Zagrebu. Napadači su šifrirali podatke i tražili otkupninu za dešifriranje. Ovi napadi uzrokovali su poremećaje u pružanju zdravstvenih usluga, ali je odgovor na napad bio brz i spriječena je veća šteta.
- Tijekom pandemije Covid-19, povećan je broj kibernetičkih napada u Hrvatskoj, usmjerenih na zdravstvene ustanove i institucije koje su se bavile upravljanjem krizom. Ovi napadi uključivali su pokušaje krađe podataka i ometanja operacija.
- U 2023. godini, Republika Hrvatska bila je izložena značajnim kibernetičkim napadima, s posebnim porastom napada sponzoriranih od strane države (APT - Advanced Persistent Threats). Do svinja 2023. godine zabilježeno je najmanje 15 takvih napada, što predstavlja značajan porast u usporedbi s prethodnim godinama. Ovi napadi su uglavnom ciljali državne institucije i kritičnu infrastrukturu, uključujući ministarstva i sektore energetike i transporta. Posebno su istaknuti napadi povezani s Rusijom, kao dio šireg geopolitičkog konteksta.
- U 2024. godini, KBC Zagreb (Klinički bolnički centar Zagreb), najveća bolnicu u Hrvatskoj je bila napadnuta od strane ransomware grupe LockBit na. Ovaj napad je privremeno oborio IT sustave bolnice, a napadači su tvrdili da su došli do osjetljivih podataka, uključujući medicinske evidencije i ugovore. Ovaj incident je ukazao na ranjivost ključne infrastrukture, posebno u zdravstvenom sektoru, na sofisticirane kibernetičke prijetnje.
- Također, u 2024. Zračna luka Sveti Jeronim u Splitu je bila napadnuta od strane ransomware od strane Akira, koja se pokazala kao jedna od opasnijih varijanti zlonamjernog softvera u upotrebi.

Republika Hrvatska, kao i mnoge druge zemlje, kontinuirano je izložena kibernetičkim prijetnjama koje postaju sve sofisticiranije. Kao odgovor, Hrvatska poboljšava svoje obrambene kapacitete, uključujući jačanje kibernetičke sigurnosti u ključnim institucijama i infrastrukturi. Osim na području Republike Hrvatske na kojoj je analiza rađena, porast korištenja kibernetičkog prostora je u porastu u cijelom svijetu. Shodno tome dolazi i do što više kibernetičkih napada, osim ratova s oružjem sve je više kibernetičkih napada u porastu te je porast i kibernetičkih kaznenih djela.

Neka od kibernetičkih kaznenih djela u svijetu do kojih je došlo uslijed loše zaštite koja je navedena ranije kroz rad su:

- 1. srpnja 2024. godine, Patelco Credit Union je objavio da su iskusili ransomware napad koji je doveo do gašenja nekoliko njihovih bankarskih sustava za klijente. Napad se dogodio 29. lipnja 2024. godine, a kao odgovor na njega Patelco je poduzeo proaktivne mjere kako bi ograničio utjecaj incidenta na svoje sustave.
- 1. srpnja 2024. godine, japanski gigant za anime i igre, Kadokawa, priznao je curenje podataka nakon ransomware napada od strane grupe BlackSuit. Ovaj napad rezultirao je krađom informacija o poslovnim partnerima, uključujući ugovore i druge dokumente, kao i internim podacima kompanije, poput osobnih podataka svih zaposlenika njezine podružnice Dwango, koja upravlja popularnom japanskom video-platformom Niconico. BlackSuit grupa tvrdi da ima pristup 1,5 TB podataka i prijeti objavljivanjem preostalog sadržaja ako ne bude plaćena otkupnina.
- 12. srpnja 2024. godine, hakeri su ukrali metapodatke o "gotovo svim" pozivima i SMS porukama korisnika AT&T-a tijekom šestomjesečnog razdoblja u 2022. godini. Napad se dogodio u travnju, kada su hakeri provalili u platformu za pohranu podataka ovog telekomunikacijskog giganta. Grupa ShinyHunters preuzela je odgovornost za ovaj napad.
- 15. srpnja 2024. godine, Rite Aid Pharmacy objavio je da je u lipnju došlo do kršenja podataka u kojem je ukradeno osobnih podataka 2,2 milijuna korisnika. Hakerska grupa RansomHub tvrdila je da je preuzela više od 10 GB podataka, uključujući imena, adrese, brojeve vozačkih dozvola, datume rođenja i brojeve Rite Aid nagradnih kartica.
- 26. srpnja 2024. godine, australska IT uslužna tvrtka **Insula Group**, sa sjedištem u Victoriji, potvrdila je da je bila žrtva napada ransomwarea BianLian. Hakerska grupa tvrdi da je ukrala 400 gigabajta podataka, uključujući projektne i konstrukcijske podatke, podatke o klijentima, korisničke mape, podatke s datotečnih servera i izvorne kodove tvrtke. Grupa je na svojoj darknet stranici objavila da će uskoro prenijeti ukradene podatke, pozivajući zainteresirane strane da ih kontaktiraju. ()

Stoga je važno također naglasiti i Međunarodnu suradnju kibernetičke sigurnosti koja se potrebna na međunarodnom nivou. Zajednički napori između država, organizacija i privatnog sektora ključni su za učinkovitu obranu od kibernetičkih prijetnji. Navedene teme ukazuju na

kompleksnost kibernetičke sigurnosti i potrebu za kontinuiranim prilagođavanjem kako bi se zaštitili podaci i infrastruktura od rastućih prijetnji (45).

6. ZAKLJKUČCI

Kibernetika, kao znanstvena disciplina, utječe na razvoj brojnih znanstvenih područja, omogućujući nove pristupe analizi i razvoju ideja. Fokusira se na opća pitanja upravljanja sustavima, ne na detalje njihovog funkcioniranja. Budući da se sustavi razlikuju, različiti su i načini njihovog upravljanja, što je dovelo do razvoja različitih izvedenica kibernetike. Te izvedenice istražuju specifične metode upravljanja za pojedine vrste sustava, pružajući alate za rješavanje složenih problema u različitim kontekstima. Kibernetički prostor, iako virtualan, postaje stvarna arena u kojoj dolazi do manipulacije podacima, što olakšava provedbu kaznenih djela. Kibernetičke prijetnje, koje se šire s razvojem tehnologije, obuhvaćaju kibernetički kriminal, špijunažu, terorizam, rat i hibridni rat. Svaka od ovih prijetnji predstavlja ozbiljan izazov za sigurnost i zahtijeva sveobuhvatan pristup u zaštiti informacija i sustava. Kibernetički napadi postaju jedna od najvećih prijetnji suvremenom društvu, naglašavajući potrebu za stalnim razvojem sigurnosnih mjera i međunarodnom suradnjom. Kibernetički kriminal obuhvaća kaznena djela kao što su prijevare u internetskom bankarstvu, gdje je upotreba računala ključna za izvršenje napada. Kibernetička špijunaža uključuje otkrivanje tajnih ili povjerljivih informacija korištenjem špijunskog softvera. Kibernetički terorizam odnosi se na planirane napade na računalne sustave od strane nacionalnih grupa, dok je kibernetički rat usmjeren na uništavanje infrastrukture drugih država. Hibridni rat kombinira kibernetičke napade s tradicionalnim metodama kako bi se postigli ekonomski, politički i drugi ciljevi. Borba protiv kibernetičkih prijetnji temelji se na međunarodnoj suradnji specijaliziranih organizacija. Kao odgovor na stalne sigurnosne prijetnje, Konvencija o kibernetičkom kriminalu koju je usvojilo Vijeće Europe pruža čvrstu osnovu za učinkovitu borbu protiv kibernetičkog kriminala i drugih kibernetičkih prijetnji. Uz to, NIS Direktiva Europske unije uspostavila je temelj za poboljšanje sigurnosti mreža i informacijskih sustava unutar EU-a, doprinoseći jačanju kibernetičke sigurnosti na razini cijelog kontinenta. Kroz svoje obveze i direktive, Europska unija značajno je doprinijela podizanju svijesti o kibernetičkoj sigurnosti te osiguravanju odgovarajućih mjera zaštite. NIS2 Direktiva, kao najnoviji zakonodavni okvir, uvodi nove obveze za organizacije i jača upravljanje rizicima i incidentima. Ova direktiva ima za cilj unaprijediti sigurnost mreža i informacijskih sustava u EU, čime će se značajno oblikovati budućnost kibernetičke sigurnosti na europskoj razini. Primjena GDPR direktive značajno je utjecala na način na koji organizacije diljem Europe upravljaju osobnim podacima. Ova regulativa postavila je visoke standarde za zaštitu podataka, osiguravajući transparentnost i odgovornost u

obradi podataka. Organizacije su morale prilagoditi svoje postupke kako bi se uskladile s ovim pravilima, što je uključivalo poboljšanje sigurnosnih mjera, obuku zaposlenika i uspostavu jasnih politika privatnosti. Iako je implementacija GDPR-a predstavljala izazov, rezultirala je povećanjem povjerenja korisnika i smanjenjem rizika od kibernetičkih prijetnji.

7. LITERATURA

(1) Cybersecurity, dostupno na: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (1.7.2024.)

(2) J. ČIZMIĆ, M. BOBAN, Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu...Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410, 2018.

(3)Hrvatska enciklopedija, mrežno izdanje. Kibernetički prostor. http://www.enciklopedija.hr/Natuknica.aspx?ID=68098. 2021.

(4) Vuković, Hrvoje .Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future, 2012.

(5) Rein, R. i Van Niekerk, J., From Information Security to Cyber Security Cultures. Research gate, 2014. https://www.researchgate.net/publication/281107085_From_Information_Security_to_Cyber_Security_Cultures_Organizations_to_Societies

(6) Središnji državni ured razvoj digitalnog društva. Kibernetička sigurnost. https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436., 2022.

(7) Sharon Shea, Alexander S. Gillis, TechTarget. What is Cybersecurity?, dostupno na: https://www.techtarget.com/searchsecurity/definition/cybersecurity (2.7.2024.)

(8) Whitman, M.; Mattord, H.: "Management of information security", Cengage Learning, 2013.

(9) Confidentiality, Integrity, Availability & Safety (CIAS) Model, dostupno na: https://complianceforge.com/free-guides/confidentiality-integrity-availability-security-cias (3.7.2024.)

(10) Spremić, Mario Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet Sveučilišta u Zagrebu, 2017

(11) Kako prepoznati e-mail prijevaru (phishing)?, dostupno na: https://csi.hr/2021/04/29/kako-prepoznati-e-mail-prijevaru-phishing-2/ (3.7.2024.)

(12) Huremović, L. (2021.), Kako IT timovi mogu zaštiti medije od SQL napada, dostupno na; https://www.balkansmedia.org/bs/korisni-savjeti-i-alati/kako-it-timovimogu-zastiti-medije-od-sql-napada (3.7.2024.)

(13)Techopedia (b.d.), Internal attack, dostupno na: https://www.techopedia.com/definition/26218/internal-attack (10.7.2024.)

(14) . Trend Micro (b.d.), Zero-Day Vulnerability , What is a zero-day vulnerability? Dostupno na:https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability (10.7.2024.)
(15) Wright, G., Bacon, M. (2021.), Watering hole attack, dostupno na: https://www.techtarget.com/searchsecurity/definition/watering-hole-attack (10.7.2024.)
(16) Zaštita podataka i pravo na privatnost u informacijskom društvu, Gospić, M. Boban, 2019.
(17) Zakon o informacijskoj sigurnosti NN 79/07, 14/24
(18) Branko Peran, Mirko Goreta, Kristina Vukošić, Pojam i vrste tajni, Stručni rad / Professional paper UDK 342(497.5)
(19) Zakon o tajnosti podataka NN 79/07, 86/12
(20) Cybersecurity: how the EU tackles cyber threats dostupno na; https://www.consilium.europa.eu/en/policies/cybersecurity/, (11.7.2024.)
(21) O sustavu SK@UT, dostupno na: https://www.skaut.hr/ (11.7.2024.)
(22) Boban, M., Zaštita osobnih podataka i nova EU uredba o zaštiti podataka, Bilten HDMI, 2018;
(23) Pravni okvir, dostupno na: https://azop.hr/djelokrug/ (11.7.2024.)
(24) M. Boban, Krizno upravljanje i upravljanje sigurnošću informacijskih sustava kao temeljni oblici prevencije računalnog kriminaliteta, Zbornik radova IV. međunarodne znanstveno-stručne konferencije „Istraživački dani visoke policijske škole u Zagrebu“, 2014
(25) Šimundić, S. „Funkcijska informatika u društvenim sustavima“, Sveučilište u Splitu Pravni fakultet, Split, 2000
(26) AOL/NCSA Online Safety Study, Dec. 2005 ,dostupno na: http://www.staysafeonline.info/pdfsafety_study_2005.pdf (15.7.2024.)
(27) Panian, Ž. „Izazovi elektroničkog poslovanja“, Narodne novine, Zagreb, 2002
(28) Boban, M. „Building eGovernment model on the principles of new economy trends and international standards considering protection of citizen privacy and personal data“, E-Society Journal Research and Applications, Volume 1, Number 2, Zrenjanin, December, 2010.
(29) Berinato, S. „Reinvention in progress, CSO, Sv. 5,Br. 5, ISSN 1540-904X, CXO Media Inc., str. 36 -38, 2006.
(30) CARNET, LS&S, Osnove računalne forenzičke analize, CCERTPUBDOC-2006-11-174, 2006
(31) CASTELLS, M., The information age: economy, society and culture, Vol. I: The rise of the network society . Cambridge: Blackwell Publishers, 2000.

(32) United Nations International cooperation in combating transnational crime, dostupno na: http://www.uncjin.org/6e.pdf (18.7.2024.)
(33) CYBERSECURITY IN THE DIGITAL AGE: REGULATORY FRAMEWORK BASED ON THE IMPLEMENTATION OF THE NIS2 DIRECTIVE, Marija Boban, 2024.
(34) Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), dostupno na: https://digital-strategy.ec.europa.eu/en/node/10361/printable/pdf (25.7.2024.)
(35) Meneghetti, M., CyberItalia: The NIS 1 Directive and the new NIS 2 Directive in a nutshell. 3 November 2023, dostupno na:https://www.dlapiper.com/en/insights/publications/law-in-tech/cyberitalia-the-nis-1-directive-and-the-new-nis-2-directive-in-a-nutshell (29.7.2024.)
(36) NIS 2 Directive, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333 27.12.2022, p. 80
(37) BOBAN, M., ePrivacy and new European Data Protection Regime, International Scientific Conference ESD 2016
(38) Službeno priopćenje Europskog parlamenta na temu usklađivanja zakonodavnog paketa, dostupno na: http://www.europarl.europa.eu/news/hr/news-room/20160407IPR21776/Reforma-za%C5%A1tite-podataka-EP-odobrio-nova-pravila (7.8.2024.)
(39) J. ČIZMIĆ, M. BOBAN, Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410, 2018
(40) EU Opća uredba o zaštiti podataka, dostupno na: https://www.privacy-regulation.eu/hr/ (17.8.2024.)
(41) Preuzeto iz Primjena informacijskih i komunikacijskih tehnologija (IKT) u kućanstvima i kod pojedinaca U 2023., dostupno na https://podaci.dzs.hr/2023/hr/58217 (19.8.2024.)
(42) Ministarstvo unutarnjih poslova glavno tajništvo sektor za pravne poslove i strateško planiranje služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled, Temeljnih sigurnosnih pokazatelja i rezultata rada u 2023. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2024/3/Statisticki_pregled_2023_.pdf (19.8.2024.)
(43) UVNS, Ured Vijeća za nacionalnu sigurnosti, 2015., dostupno na: https://www.uvns.hr/

UserDocsImages/dokumenti/Nacionalna%20strategija%20kiberneticke%20sigurnosti%20(2015.).pdf?vel=491670 (19.8.2024.)
(44) Derolulez, J., EU LAW: NIS I, NIS II, what's new? And how to implement NIS II Directive and GDPR? published 21 March 2024, dostupno na: https://www.linkedin.com/pulse/eu-law-nis-i-ii-whats-new-how-implement-directive-gdpr-deroulez-xc0ee (20.8.2024.)
(45) July 2024: Biggest Cyber Attacks, Data Breaches and Ransomware Attacks, dostupno: https://www.cm-alliance.com/cybersecurity-blog/july-2024-biggest-cyber-attacks-data-breaches-and-ransomware-attacks (21.8.2024.)

8. SAŽETCI

Kibernetička sigurnost - aktualnost u zaštiti podataka i regulativni oblik

Cilj: je prikazati značajke suvremenog kibernetičkog svijeta, sigurnosne izazove kibernetičkih prijetnji, kako se obraniti od istih, prikazati na koji način može doći do napada. Također, objasniti pojmove poput kibernetičkog prostora, način na koji se možemo zaštiti unutar istoga. Uz to analizirati vrste napada, prikazati na koji način se krizno upravlja u situacijama pri kibernetičkim napadima kao i analizirati rizike kibernetičke sigurnosti. Kroz rad se obradila EU Uredba 2016/649 (GDPR), ukazalo se na njenu važnost i primjene unutar članica Europske Unije te usporedila ista s zemljama koje je ne provode. Osim same Uredbe kroz rad se prikazao regulatorni okvir kibernetičke sigurnosti temeljen na implementaciji NIS2 Direktive.

Metode: koje su se koristile kroz rad su prikaz podjele cjelokupne zaštite i sigurnosti podataka kao i kategorije koje se koriste kako bi se sigurnost mogla ostvariti i primijeniti u umreženim sustava u kibernetičkom prostoru. Kako bi se ostvarilo definirana je analiza rizika te postoji li direktan odnos između ranjivosti sustava i vjerojatnosti događanja štetnog događaja.
Uz to analizirano je područje računalnog kriminaliteta elektronički dokaza kao jedan od najvažnijih čimbenika. Kroz metode je analiziran regulatorni okvir kibernetičke sigurnosti temeljen na implementaciji NIS 2 Direktive, kao i „Opća EU uredba o zaštiti podataka 2016/679 (engl. General Data Protection Regulation - dalje GDPR).

Rezultati: koji su doneseni u radu su prikaz svijesti te educiranosti o potencijalnim kibernetičkim napadima i kibernetičkom kriminalitetu kao i o povredi njihovih osobnih podataka koristeći se svakodnevno kibernetičkim prostorom. Zanimljiv je rezultat koji se analizirao kroz prikaz grafova o korisnicima interneta po dobnim skupinama i prema spolu, prema radnom statusu i namjene upotrebe interneta kod pojedinaca kroz rad je zaključen porast korisnika interneta po dobi, ističući porast upotrebe starije populacije, također najviše je korisnika u studentskoj i učeničkoj populaciji. Također, prikazana je kaznenih djela kibernetičkih kriminaliteta te razlike Direktiva 95/46/EZ i GDPR-a.

Zaključci: Kibernetički prostor, iako virtualan, postaje stvarna arena u kojoj dolazi do manipulacije podacima, što olakšava provedbu kaznenih djela.. Kroz svoje obveze i direktive, Europska unija značajno je doprinijela podizanju svijesti o kibernetičkoj sigurnosti te osiguravanju odgovarajućih mjera zaštite. NIS2 Direktiva, kao najnoviji zakonodavni okvir, uvodi nove obveze za organizacije i jača upravljanje rizicima i incidentima. Primjena GDPR direktive značajno je utjecala na način na koji organizacije diljem Europe upravljaju osobnim podacima. Iako je implementacija GDPR-a predstavljala izazov, rezultirala je povećanjem povjerenja korisnika i smanjenjem rizika od kibernetičkih prijetnji.

Ključne riječi: kibernetička sigurnost, kibernetički prostor, NIS2 direktiva, GDPR, osobni podaci

9. SUMMARY

Cybersecurity - Current Issues in Data Protection and Regulatory Framework

Objective: The paper aims to highlight the features of the modern cyber world, security challenges posed by cyber threats, methods of defense, and how attacks occur. It also explains concepts like cyberspace and methods of protection within it. Additionally, it analyzes types of attacks, crisis management during cyber incidents, and cybersecurity risks. The study discusses EU Regulation 2016/679 (GDPR), its importance, implementation across EU member states, and compares it with non-compliant countries. It also examines the cybersecurity regulatory framework based on the NIS2 Directive.

Methods: The methods used include the analysis of data protection and security divisions, categories applied for security in networked systems, risk analysis, and the relationship between system vulnerabilities and the likelihood of harmful events. The study also delves into cybercrime and electronic evidence, as crucial factors, while analyzing the regulatory framework based on the NIS2 Directive and GDPR.

Results: The results include raising awareness and education about potential cyberattacks and cybercrime, as well as the violation of personal data in cyberspace. The study presents findings through graphs on internet users by age, gender, employment status, and internet usage purposes, concluding an increase in internet use among the elderly, with the highest use among students. Additionally, it discusses cybercrimes and compares Directive 95/46/EC with GDPR.

Conclusions: Cyberspace, although virtual, has become a real arena for data manipulation, facilitating criminal activities. Through its obligations and directives, the European Union has significantly raised awareness of cybersecurity and ensured appropriate protection measures. The NIS2 Directive, as the latest regulatory framework, introduces new obligations for organizations and strengthens risk and incident management. The implementation of the GDPR has significantly influenced how organizations across Europe manage personal data, leading to increased user trust and reduced cybersecurity risks.

Keywords: cybersecurity, cyberspace, NIS2 directive, GDPR, personal data.

10. ŽIVOTOPIS

OSOBNI PODACI:
Ime i prezime: Zrinka Čule
Elektronička pošta: cule.zrinka@gmail.com
Državljanstvo: hrvatsko
Datum i mjesto rođenja: 12. prosinca 1992., Split

ZAPOSLJENJE:
2019. Odašiljači i veze d.o.o.

IZOBRAZBA
2018. Sveučilište u Splitu, Sveučilišni odjel za stručne studije
2013. Fakultet elektrotehnike, strojarstva i brodogradnje u Splitu

SOCIJALNE VJEŠTINE I KOMPETENCIJE
Marljivost, upornost, komunikacijske vještine, timski duh i sposobnost prilagodbe novim situacijama stečeni su kroz godine rada i učenja, kao dio obrazovanja i izvannastavnih aktivnosti

RAČUNALNE VJEŠTINE I KOMPETENCIJE
Napredno korištenje Microsoft Office alata (Word, Excel, PowerPoint), pretraživanje Interneta, osnove programiranja u C++

OSTALE VJEŠTINE I KOMPETENCIJE
2008. godine sudjelovala sam u studentskom kampu u Lindlaru, Njemačka
2010. godine sudjelovala sam u studentskom kampu u Pszczyni, Poljska
2022. položen stručni ispit za Obavljanje poslova privatne tehničke zaštite
2022. položen AXIS certificirani trening - Network video fundamentals

MATERINSKI JEZIK
Hrvatski jezik

OSTALI JEZICI
Engleski jezik
Talijanski jezik

11. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, Zrinka Čule, izjavljujem da je moj diplomski rad pod naslovom
KIBERNETIČKA SIGURNOST - AKTUALNOST U ZAŠTITI PODATAKA I REGULATIVNI OBLIK,
rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.
Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.
Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 20.09.2024.

Potpis studenta/studentice: