UNIVERZA V MARIBORU
EKONOMSKO-POSLOVNA FAKULTETA

Delo diplomskega projekta

KIBERNETSKA VARNOST V EU

September, 2019 Lucija Kos

UNIVERZA V MARIBORU
EKONOMSKO-POSLOVNA FAKULTETA

Delo diplomskega projekta

KIBERNETSKA VARNOST V EU

Cyber Security in EU

Kandidat: Lucija Kos

Študijski program: Ekonomske in poslovne vede

Študijska usmeritev: Elektronsko poslovanje

Mentorica: dr. Simona Sternad Zabukovšek

Jezikovno pregledala: Ksenija Pečnik, prof. slov. jezika

Študijsko leto: 2018/19

Maribor, september 2019

ZAHVALA

Za vodenje in strokovno pomoč pri izdelavi dela diplomskega projekta se iskreno zahvaljujem mentorici dr. Simoni Sternad Zabukovšek.

Zahvalila bi se tudi staršem in sestri Katji, ki so me spodbujali in podpirali v času študija.

POVZETEK

Živimo v času, v katerem se tehnologija razvija z neverjetno hitrostjo, skupaj z njo pa se razvijajo tudi vedno bolj sofisticirane tehnike napadov, ki lahko, če so izvedene, ogrozijo varnost kritične infrastrukture, organizacij in posameznikov. Uporabniki hitro sprejmemo tehnologijo, ki nam olajša in izboljša vsakdanje delo in življenje, ter si ne predstavljamo, kako bi bilo življenje brez nje, zato je pomembno, da se vsi uporabniki ne glede na starost zavedamo pasti ob uporabi tehnologije. V prvem delu diplomskega projekta pojasnimo temeljne pojme, pomen kibernetske varnosti ter definiramo in predstavimo kibernetske grožnje po klasifikaciji Evropske agencija za kibernetsko varnost ENISA. Nadaljujemo z opisom usmeritev Evropske unije (EU) na področju zagotavljanja kibernetske varnosti, kjer predstavimo glavne akterje, odgovorne za kibernetsko varnost v EU, ter direktive, akte in uredbe, ki jih je EU sprejela, da bi čim bolje zagotavljala in nadzorovala področje kibernetske varnosti. Prav tako predstavimo Strategijo kibernetske varnosti Republike Slovenije.

Ključne besede: kibernetska varnost, Evropska unija, kibernetski napadi, kibernetske grožnje

ABSTRACT

We live in a time when technology is evolving at an incredible pace, and, consequently resulting in development of more and more sophisticated attack techniques that can potentially cause major/serious disruption in the security of critical infrastructure, organizations and individuals. technology that not only makes our life and work easier but also improves it is quickly and enthusiastically accepted by its users. In fact, we can no longer imagine life without it, therefore, it is of crucial importance for all users, regardless of gender, and socio-economic background, to be aware of the pitfalls of using modern technology. In the first part of the diploma project we explain the basic concepts, such as the importance of cyber security, as well as define and present cyber threats according to the classification of the European Cyber Security Agency ENISA. We continue with a description of the European Union's cyber security policies, outlining the major cybersecurity actors in the EU, and explaining the directives, acts and regulations adopted by the EU to ensure the control of cyber security as much as possible. Last but not least, we also present the Cyber Security Strategy that was adopted by Republic of Slovenia.

Key Words: cyber-security, European union, cyber-attacks, cyber-threats

KAZALO

KAZALO SLIK

KAZALO TABEL

SEZNAM OKRAJŠAV

BBC	British Broadcasting Corporation
CSIRT	Skupina za reševanje varnostnih incidentov
EC3	Evropski center za boj proti kibernetski kriminaliteti
EDA	Evropska obrambna agencija
EEAS	Evropska služba za zunanje delovanje
ENISA	Agencija Evropske unije za varnost omrežij in informacij
EU	Evropska unija
GD CONNECT	Generalni direktorat za informacijsko družbo in medije
GD DIGIT	Generalni direktorat za informatiko
GD HOME	Generalni direktorat za migracije in notranje zadeve
GDPR	Splošna uredba EU o varstvu podatkov
HTTP	metoda za prenos informacij na spletu
IP	številka, ki natančno določa računalnik v internetnem omrežju
NATO	Organizacija severnoatlantske pogodbe
OPKO	Okvir EU za politiko kibernetske obrambe
PP	Point-to-Point Protocol
SIGOV-CERT	Odzivni center za incidente v informacijskih sistemih organov državne uprave
SMTP	protokol za prenos elektronske pošte
SOVA	Slovenska obveščevalno-varnostna agencija
SVOP	Skupna varnostna in obrambna politika
TCP	protokol transportnega sloja, ki se uporablja za zanesljiv pretok podatkov med gostitelji in omrežji
UDP	nepovezovalni protokol za prenašanje paketov
ZDA	Združene države Amerike

1 UVOD

Tehnologija nam kot uporabnikom odpira popolnoma nov svet priložnosti. Vsak nov izdelek ali storitev, ki nam prinaša izboljšanje ali olajšanje naše vsakodnevne rutine, postane v neki točki ključni del našega vsakdana. Tako se z vsakim pomembnejšim tehnološkim razvojem poveča tudi naša odvisnost od tehnologije, vzporedno z njo pa se poveča pomembnost kibernetske varnosti. Kot uporabniki na spletu se moramo zavedati, da bolj kot smo povezani in več osebnih informacij kot izdamo, večja je verjetnost, da bomo na neki točki tudi sami postali žrtev kibernetskega kriminala ali napada.

Idejo za temo dela diplomskega projekta smo dobili na dogodku, ki ga je organizirala katedra za elektronsko poslovanje. Katedra je na dogodku gostila etičnega hekerja Milana Gaborja, ki je predaval o svojem delu in o tem, kako lahko je enkrat, ko poznaš nekaj osebnih informacij o posamezniku, tega zvabiti, da bo odprl zlonamerno elektronsko pošto, s pomočjo katere da napadalcu praktično dostop do svojega računalnika in vseh ostalih informacij. Šele v tistem trenutku smo se zamislili, koliko in kakšne nevarnosti nam dejansko pretijo ob uporabi spleta vsak dan in kako nepazljivo smo in še uporabljamo svetovni splet tudi sami.

1.1 Opis področja in opredelitev problema

Osnovni cilj dela diplomskega projekta je pojasniti, prikazati in proučiti kibernetsko varnost. V nalogi poskušamo pojasniti, zakaj je pomembno, da v današnjem času vsi razumemo in se zavedamo pomena kibernetske varnosti. Z boljšim razumevanjem tega pojma bomo lahko sami veliko bolje poskrbeli, da bomo ob uporabi svetovnega spleta in pametnih naprav bolj pazljivi na razne pasti, ki pretijo na nas. Za njihovo boljše razumevanje opišemo in pojasnimo več različnih tehnik napadov, ki jih opredeli Agencija ENISA. Predstavimo najpomembnejše strategije in akte, ki jih je EU sprejela, da bi čim bolje zagotavljala kibernetsko varnost. Dodatno predstavimo tudi strategijo kibernetske varnosti Republike Slovenije.

1.2 Namen, cilji in hipoteze raziskave

Kot je razvidno iz naslova, je namen predstaviti področje kibernetske varnosti in ukrepe, ki jih vpeljuje EU za nadzorovanje tega področja.

Cilji, ki jim sledimo v delu diplomskega projekta, so:

- opis področja kibernetske varnosti,
- predstavitev kibernetskih groženj,
- predstavitev delovanja EU na področju kibernetske varnosti,
- analiza in prikaz informiranosti državljanov EU glede kibernetskih tveganj,
- predstavitev strategije kibernetske varnosti.

V delu diplomskega projekta poskusimo odgovoriti na dve izbrani hipotezi:

- H1: Kibernetski kriminal je v porastu.
- H2: Uporabniki interneta in pametnih naprav so vedno bolj ozaveščeni o pasteh kibernetskega kriminala.

1.3 Predpostavke in omejitve

Glavna predpostavka je, da v slovenski literaturi ni na voljo dovolj aktualnih knjižnih virov na temo kibernetske varnosti. Kot je opisano v nalogi, se z razvojem tehnologije razvijajo tudi nove kibernetske grožnje, prav zato so lahko opisane grožnje v delu diplomskega projekta že zastarele.

Glavna omejitev je širina obravnavanega področja, v delu diplomskega projekta obravnavamo le en majhen del problema in ne celotnega področja kibernetske varnosti. Druga omejitev je verodostojnost sekundarnih virov, saj je v današnji poplavi virov težko ločiti med verodostojnimi in neverodostojnimi viri. Zakonodaja EU ureja različna področja kibernetske varnosti v različnih sektorjih, zato je vsem zakonom, aktom in direktivam na tem področju težko slediti.

1.4 Predvidene metode raziskovanja

Uporabimo deskriptivno metodo raziskovanja, pri kateri si pomagamo z domačo in tujo literaturo. Uporabimo tudi komparativno metodo, s katero analiziramo in povzamemo do sedaj opravljene raziskave, in metodo kompilacije, s katero povzamemo spoznanja in citate drugih avtorjev. Pomagamo si tudi s sekundarnimi viri, ki jih pridobimo na domačih in tujih spletnih straneh. Razne statistične podatke pridobimo iz predhodnih raziskav, ki so dosegljive na svetovnem spletu.

2 TEMELJNI POJMI

Kibernetski prostor (angl. *cyberspace*)

Beseda kibernetski prostor se prvič pojavi leta 1982 v znanstveno-fantastični knjigi Burning Chrome, katere avtor je kanadski pisatelj William Gibson. Tako je od prve omembe besede kiberprostor minilo že več kot 35 let. S časom se je razvilo mnogo definicij, pri čemer opazimo, da različni avtorji in organizacije različno poudarjajo razsežnosti kibernetskega prostora (Mikelj, 2016).

Za opredelitev kiberprostora smo izbrali definicijo, ki je zapisana v Nacionalni strategiji za zaščito kibernetskega prostora Združenih držav Amerike (National Strategy to Secure Cyberspace), katere opredelitev daje prednost tehnološkim komponentam. Kibernetski prostor je opisan kot živčni sistem – nadzorni sistem države. Definirajo, da je kiberprostor sestavljen iz več sto tisoč medsebojno povezanih računalnikov, strežnikov, usmerjevalnikov, stikal in optičnih kablov, ki omogočajo delovanje kritične infrastrukture. V definiciji izpostavijo, da je zdravo delovanje kibernetskega prostora bistvenega pomena za gospodarstvo in nacionalno varnost (Homeland Security, 2019).

Digitalno potrdilo javnega ključa (angl. *public key certificate*)

Digitalno potrdilo javnega ključa je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo, institucijo ali strežnikom.

Kritična infrastruktura (v povezavi s kibernetsko varnostjo)

K sklopu kritične infrastrukture spadajo sektorji na področju zagotavljanja energetske podpore, prometnih povezav, preskrbe s hrano oziroma pitno vodo, varstva okolja, financ ter informacijske in komunikacijske podpore (Maček, Mulec, & Močilar, 2016).

Heker

V Slovarju slovenskega knjižnega jezika najdemo naslednjo obrazložitev termina heker: héker hékerja in hêker hêkerja; tudi hacker *samostalnik moškega spola* [héker] in [hêker], kdor navadno nepooblaščeno vdira v računalniške sisteme, zlasti z namenom dokazovanja računalniške spretnosti, finančnega okoriščanja, ali navdušen, spreten računalniški uporabnik, programer.

Etični heker

Je stalna besedna zveza, ki je v Slovarju slovenskega knjižnega jezika opisana kot: heker, ki preverja varnost računalniških sistemov in njihovo zaščito pred nepooblaščenimi vdori, navadno za organizacijo, podjetje.

Slovenski etični heker Milan Gabor je za nacionalni program ozaveščanja o informacijski varnosti Varni na spletu povedal: »*Definicij je več in včasih je izjemno težko povedati na kratko. Če poskušam nekako povzeti, delamo etični hekerji enake stvari kot neetični hekerji, vendar na legalen način in na koncu etični hekerji dobimo še plačilo. Poleg tega*

etični hekerji izvajamo varnostne preglede, penetracijske teste ali varnostne analize z vednostjo naročnika in v kontroliranem okolju« (Varni na internetu, 2018).

SQL-jezik

SQL (angl. *Structured Query Language*) je standardiziran jezik za upravljanje zbirk podatkov. SQL-jezik se uporablja za ustvarjanje, urejanje in iskanje določenih podatkov. Ti podatki so po navadi organizirani v tabelah, vsaka tabela vsebuje svoje podatke. S pomočjo SQL-jezika lahko podatke poiščemo, uredimo in pridobimo (Smart Ninja, 2017). Na primer relacijske zbirke podatkov, kot je Microsoft Office Access, uporabljajo jezik SQL za delo s podatki.

Podatkovne baze (angl. *Database*)

Podatkovne baze so sestavljene iz podatkov, ki so razvrščeni v tabele in vrstice, podobno kot v Microsoft Excelu. Podatki v teh tabelah so medsebojno povezani v odnose. Struktura tabel je vnaprej določena, kar zagotavlja, da so podatki v pravilni obliki in na pravem mestu (NEFOS, 2019).

Socialni inženiring (angl. *social engineering*)

Socialni inženiring je ena izmed najpogosteje uporabljenih tehnik za pridobivanje osebnih podatkov druge osebe s pomočjo manipulacije oziroma z zlorabo zaupanja.

Tako kot za večino izrazov obstaja tudi za socialni inženiring več definicij. Skupno vsem definicijam pa je, da opisujejo socialni inženiring kot uporabo socialnih ali psiholoških trikov, katerih namen je pridobiti osebne podatke druge osebe. Ob tem pa velja, da napadalec ne potrebuje poglobljenega tehničnega in računalniškega znanja (Informacijski pooblaščenec, 2009).

»Socialni inženir torej z zlorabo zaupanja, z uporabo socialnih veščin oziroma psiholoških tehnik, kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva ipd., pridobi od žrtve osebne podatke (najpogosteje ime, priimek, št. transakcijskega računa, razna gesla, EMŠO, št. potnega lista …) in jih uporabi za pridobivanje večinoma premoženjske koristi. Redkeje od zasledovanja premoženjskih koristi, pa vendar ne zanemarljivo, se zgodi, da napadalec žrtev s pridobljenimi osebnimi podatki izsiljuje, grozi, jo šikanira ali kako drugače spravlja v slabši položaj« (Informacijski pooblaščenec, 2009).

Socialni inženiring razlikujemo po tehničnih in netehničnih pristopih. Netehnični pristop zajema osebni pristop, anketiranje, brskanje po smeteh, kontaktiranje prek telefona. Tehnični pristop na drugi strani zajema ribarjenje, napade s posrednikom in uporabo elektronske pošte.

Temni splet (angl. *Dark Web*)

Svetovni splet je sestavljen iz površinskega spleta, ki predstavlja približno 10 % celotnega spleta. V večini je nefiltriran in neurejen. Spletne strani so indeksirane s strani standardnih spletnih iskalnikov, kot so Google, Yahoo!, Najdi.si, Bing in drugi.

Sledi globoki splet (angl. *Deep Web*), do katerega je potreben poseben dostop, predstavlja 90 % celotnega spleta in se nanaša na spletno vsebino, ki ni indeksirana s strani standardnih spletnih iskalnikov. Globoki splet v glavnem vsebuje neškodljive stvari, kot so zdravstveni podatki, vladni viri, akademski podatki, podatki e-poštnih sistemov, pravni dokumenti in plačilni sistemi. Globoki splet je dobro organiziran in urejen.

Del globokega spleta predstavlja temni splet. Gre za javni prostor, ampak sta za dostop do njega potrebna poseben dostop in program. Najpogostejši program, ki se uporablja za dostop do temne strani interneta, se imenuje Tor. Temni internet je sestavljen predvsem iz strani, na katerih se prodajajo orožje, droge, ponarejen denar in druge ilegalne storitve ali izdelki (Žlogar, 2019).

Interoperabilnost

Novak (2010, str. 87) opredeli termin »interoperabilnost« kot zmožnost informacijskih sistemov, da medsebojno izmenjujejo podatke, informacije in znanja.

3 KIBERNETSKA VARNOST

3.1 Opredelitev kibernetske varnosti

Kibernetski prostor se spreminja z veliko hitrostjo, zadnjih nekaj let pa je tudi pod velikim nadzorom medijev zaradi različnih perečih vprašanj, ki se pojavljajo. V ospredju se pojavljajo vprašanja glede varnosti posameznikov, organizacij in držav. Večina dobro informiranih organizacij meni, da kibernetska varnost postaja ključno poslovno vprašanje. Pomembnosti kibernetične varnosti se zavedajo tudi države, ki so že v večini izdale nacionalne strategije in usmeritve na področju kibernetske varnosti (Lord, 2019).

Standardne oziroma splošno sprejete definicije kibernetske varnosti ni. Na splošno lahko kibernetsko varnost opišemo kot skupek zaščitnih ukrepov, ki so sprejeti za zaščito informacijskih sistemov in uporabnikov pred nepooblaščenimi dostopi in napadi.

Završnik (2015, str. 16) *pojasni, da se »kibernetska varnost nanaša na varnost omrežij in informacij pred tveganji in incidenti, ki niso nujno povezani s kriminaliteto. 'Tveganja' so v tem smislu okoliščine ali dogodki, ki imajo lahko negativen učinek na varnost. 'Incidenti' pa so okoliščine ali dogodki, ki imajo dejansko negativen učinek na varnost«.* Avtor pojasni, da *»tako široka definicija izhaja iz strukture interneta. Internet je mrežni tehnološki sistem, sestavljen iz več plasti: na vrhu interneta je plast aplikacij (na primer e-pošta), tej plasti sledijo prenosna plast (na primer HTTP, SMTP, nato TCP in UDP), internetni protokol (IP), nato povezovalna plast, ki omogoča komunikacijo med usmerjevalniki različnih proizvajalcev (na primer PPP), in na koncu plast fizične infrastrukture (na primer optični kabli)«.*

Kibernetska varnost se torej osredotoča na zaščito računalniških sistemov in njihovih komponent – vključno s strojno opremo, programsko opremo in podatki ter digitalno infrastrukturo pred napadi in nepooblaščenimi dostopi.

Kot izraz, ki se uporablja v političnih krogih EU, kibernetska varnost ni omejena samo na omrežje in varnost informacij, ampak zajema vse nezakonite dejavnosti, ki vključujejo uporabo digitalne tehnologije v kibernetskem prostoru. To lahko vključuje tudi kibernetske zločine, kot so izvajanje napadov z računalniškimi virusi, goljufija pri brezgotovinskem plačevanju, manipulativne kampanje za vpliv na spletne razprave in poseganje v potek volitev (European Court of Auditors, 2019).

Europol v oceni groženj organiziranega kriminala na internetu (Internet Organised Crime Threat Assessment) iz leta 2017 prepozna pet področij in podkategorije, ki predstavljajo tveganje za kibernetsko varnost. Področja in podkategorije so predstavljene v tabeli 1 (SAINT Consortium, 2019).

Tabela 1: Tveganja, ki jih je prepoznal Europol

Področja kibernetske varnosti	Podkategorije kibernetske varnosti
Kibernetski zločini	• Zlonamerna programska oprema; • napadi na kritično infrastrukturo; • kršitev varnosti podatkov in omrežni napadi.
Spolno izkoriščanje otrok s pomočjo spleta	• Spolna prisila in izsiljevanje mladoletne osebe; • vsebine, povezane z otroškim spolnim izkoriščanjem; • komercialno spolno izkoriščanje otrok; • obnašanje kršitelja.
Goljufije s plačili	• Goljufija, pri kateri ni treba vpisovati podatkov s kartice; • goljufija pri plačilu s kartico.
Ilegalni spletne tržnice	• Prodaja blaga na temni strani spleta.
Terorizem	• Kibernetski terorizem.

Vir: (SAINT Consortium, 2019).

Tako kot Europol tudi Interpol preiskuje kibernetska tveganja na podobnih področjih. Interpol glavno prednost nameni visokotehnološkim zločinom, ki ogrožajo strojno in programsko računalniško opremo, na področjih financ, zlorabe otrok, goljufij in terorizma.

Tveganja glede kibernetske varnosti je opredelila tudi Evropska agencija za varnost omrežij in informacij (angl. *European Union Agency for Network and Information Security*, v nadaljevanju ENISA). Agencija v poročilu iz leta 2017, Threat Landscape Report, predstavi 15 kibernetskih groženj. Zanimivo je, da seznam vključuje tveganja, kot so kraja identitete, paket zlonamernih programov in vohunjenje, ki jim Europol in Interpol še nista določila jasne prednosti.

Tveganja s seznama agencije ENISA so (SAINT Consortium, 2019)[1]:

- zlonamerna programska oprema (angl. *Malware*),
- spletni napadi (angl. *Web-based attacks*),
- napadi na spletne aplikacije (angl. *Web application attacks*),
- ribarjenje (angl. *Phishing*),
- neželena pošta (angl. *Spam*),
- porazdeljena ohromitev storitve (angl. *Distributed Denial of Service*),
- izsiljevalni programi (angl. *Ransomware*),

[1] Opis kibernetskih groženj sledi v nadaljevanju.

- omrežje okuženih računalnikov (angl. *Botnet*),
- notranja grožnja (angl. *Insider threat*),
- fizična manipulacija, škoda,
- kršitev varnosti podatkov (angl. *Data breaches*),
- uhajanje informacij (angl. *Data leakage*),
- paket zlonamernih programov (angl. *Exploit kit*),
- kibernetsko vohunjenje (angl. *Cyber espionage*),
- kraja identitete (angl. *Identity theft*).

Stroški kršitev podatkov naraščajo. Organizacije morajo slediti novonastalim zakonodajam na področju varovanja osebnih podatkov, saj bodo v nasprotnem primeru primorane plačati znatne globe. Na območju EU je 25. 5. 2018 stopila v veljavo Splošna uredba EU o varstvu podatkov s kratico GDPR.

»*Po GDPR morajo podjetja za zakonito pridobivanje podatkov od vsakega uporabnika pridobiti njegovo izrecno soglasje, še preden pričnejo z zbiranjem podatkov. Uporabniku naj bi bilo omogočeno tudi, da soglasje za obdelavo in shranjevanje svojih podatkov zlahka umakne. Podjetja morajo uporabnikom svojih storitev zagotoviti tudi pregledne in razumljive informacije v zvezi s tem, kako lahko pridobijo informacije o namenu zbiranja in obdelave njihovih podatkov, o trajanju hrambe podatkov in o vrstah podatkov, ki jih podjetje zbira in obdeluje. GDPR dovoljuje, da je organizacija za hujše kršitve kaznovana s kaznijo v maksimalni višini 4 % njihovega letnega prihodka*« (Žagar, 2019).

Tako je bila na primer Googlu zaradi kršitev določb GDPR izrečena do sedaj najvišja globa. Googlu je bila izrečena globa v višini 50 milijonov evrov, ker svojim uporabnikom niso zagotovili dovolj nadzora nad pregledom dejanske uporabe njihovih osebnih podatkov in ker niso priskrbeli dovolj razumljivih in preglednih informacij o svoji politiki obdelave podatkov. Google se je na to odločitev pritožil in komentiral, da so v podjetju povsem predani doseganju najvišjih standardov nadzora in transparentnosti, ki se od njih pričakuje (Žagar, 2019).

3.2 Kibernetski napadi

Kibernetski napadi postajajo vse bolj pogosti in izpopolnjeni. Globalna dostopnost do informacij in podatkov tako še dodatno ogroža posameznike in organizacije, ki so v še večji nevarnosti, da jih napadejo. Dovolj je že, da samo eden izmed zaposlenih odpre lažno elektronsko sporočilo, ki lahko dostopa, šifrira, uničuje datoteke in okuži celoten sistem, ki ga podjetje uporablja za poslovanje.

Kibernetski napadi so donosni. Kibernetski napadalci običajno iščejo koristi. Veliko so pripravljeni vložiti v različne tehnike, orodja in tehnologijo, da bi dosegli svoje namene. Finančni dobiček je pogosta motivacija, vendar jih lahko vodijo tudi politične, etične, intelektualne ali socialne spodbude. Najvišja izplačana odškodnina za izsiljevalski virus v Sloveniji je leta 2016 znašala 10.000 evrov, leta 2017 pa 14.800 evrov (SI-CERT, 2018a).

Novo poročilo podjetja Radware kaže, da povprečni stroški kibernetskega napada sedaj presegajo milijon dolarjev. Poročilo o globalni aplikaciji in varnosti omrežja 2018–2019 ugotavlja, da so organizacije, ki izračunajo (v primerjavi z oceno) stroške napada, povišale

to oceno na 1,67 milijona dolarjev. Po poročanju anketirancev so kibernetski napadi v največji meri vplivali na operativno produktivnost (54 %), skoraj polovica anketirancev (45 %) je poročala, da je bil cilj napada ovirati delo, sledijo negativne izkušnje s strankami (43 %). Tretjina (35 %) anketirancev pa je dejala, da je bil cilj napada kraja podatkov. Anna Convery-Pelletier, direktorica marketinga za Radware, je dejala: »*Medtem ko morajo biti napadalci uspešni le enkrat, morajo biti organizacije pri preprečitvi napadov zmeraj 100 % uspešne. Kibernetski napadi imajo lahko zaradi motenj ali kršitev uničujoče posledice za podjetja*«. Raziskava dalje pojasnjuje, da medtem ko stroški za ublažitev napadov še naprej naraščajo, narašča tudi število organizacij, ki jih napadejo. Iz podatkov raziskave je razvidno, da je večina organizacij v letu dni doživela nekakšen napad, le 7 % jih trdi, da napada na njihovo organizacijo ni bilo (Radware, 2019).

Druge ugotovitve poročila vključujejo (Radware, 2019):

- da je 43 % vprašanih po uspešnem napadu poročalo o negativnih izkušnjah s strankami in izgubi ugleda,
- uhajanje podatkov in izguba informacij ostajata največji problem več kot tretjine (35 %) podjetij, čemur sledijo izpadi storitev,
- napadi aplikacijske plasti povzročijo veliko škode. Dve tretjini anketirancev je doživelo napade na aplikacijski ravni, 34 % pa jih predvideva, da bo v prihodnjem letu glavna skrb ranljivost,
- 86 % anketiranih podjetij je navedlo, da že raziskujejo, kako bi lahko strojno učenje in umetna inteligenca pomagala pri zagotavljanju varnosti.

Družba PricewaterhouseCoopers (PwC), ena izmed največjih revizijskih in svetovalnih hiš na svetu, je objavila globalno gospodarsko raziskavo o kriminalu 2018 na področju Združenega kraljestva (Global Economic Crime Survey 2018: UK findings). Ugotovitve družbe PwC potrjujejo, da so goljufije kot kibernetski kriminal v porastu, po izkušnjah anketirancev jim sledijo onemogočanje storitve, podkupnine in goljufije pri naročilih. Rast napadov se je zvišala, čeprav so podjetja v Združenem kraljestvu zaznala upad goljufij s 55 % v letu 2016 na 50 % v letu 2018. Raziskava je pokazala, da je bila goljufija najpogostejši kibernetski napad, ki predstavlja 49 % žrtev v Združenem kraljestvu in 31 % po vsem svetu. Goljufije so finančno močno prizadele podjetja. Več kot polovica najhujših goljufij v Združenem kraljestvu je ustvarilo 70.000 GBP izgube, medtem ko je približno 24 % žrtev zaradi goljufije izgubilo več kot 700.000 GBP. Takšne izgube so lahko usodne za podjetja po vsem svetu. Izkupički goljufij pa pogosto končajo v rokah organiziranega kriminala (PwC, 2019).

3.3 Incidenti v Sloveniji

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za kibernetsko varnost v Sloveniji. Iz slike 1 je razvidno, da so v letu 2017 obravnavali 911 incidentov, povezanih s tehničnimi napadi, 1.058 incidentov, povezanih s spletnimi goljufijami in prevarami, in 312 incidentov, povezanih z vprašanji in zahtevki.

Tehnične incidente največkrat povzroči škodljiva koda, ki se širi prek raznih priponk v elektronski pošti ali pri prenosu datotek z interneta.

Izjemno opazen naraščajoč trend lahko opazimo pri spletnih goljufijah. Napadalec za izvajanje goljufije ne potrebuje poglobljenega znanja uporabe programske opreme. Napadalec se osredotoči na obnašanje žrtve, s katero najpogosteje stopi v stik prek elektronske pošte ali družabnih omrežij.

Slika 1: Statistika obravnavanih incidentov.

Vrsta incidenta	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
phishing	23	38	50	61	139	209	279	283	296	222
skeniranje in tipanje naprav	86	39	44	62	51	43	65	65	87	127
botnet	9	3	11	12	12	16	13	17	50	16
napad z onemogočanjem (DDoS)	22	10	18	28	47	76	124	94	78	26
škodljiva koda	18	53	68	126	258	417	438	418	462	360
zloraba storitve	16	15	12	28	9	8	9	15	16	20
vdor v sistem	32	25	56	93	76	61	32	43	42	36
zloraba uporabniškega računa				1	9	37	60	40	60	43
razobličenje					125	80	167	33	13	20
napad na aplikacijo					17	22	33	7	22	41
Tehnični napadi	183	145	209	350	604	760	941	732	830	911
kraja identitete			10	52	67	56	77	70	103	106
nigerijska (419) prevara							38	26	73	119
spletno nakupovanje							68	88	183	258
druge goljufije	5	24	26	89	161	210	309	322	354	492
neželena pošta (spam)	21	22	36	25	74	50	63	112	140	80
dialler in neznani klici na mobilne telefone					1		3		1	3
Goljufije in prevare	26	46	72	166	303	316	558	618	854	1058
zahtevek sodišča	11	6	11	11	9	6	4	2	2	
avtorske pravice	2	4	2	5	9	1	4	4	8	5
interno	3	4	16	38	25	25	31	23	33	19
novinarska vprašanja					18	16	21	12	14	10
splošna vprašanja	70	74	92	120	128	145	179	184	201	278
Vprašanja in zahtevki	86	88	121	174	189	193	239	225	258	312

Vir: (SI-CERT, 2018a).

3.4 Klasifikacija kibernetskih groženj

V tem poglavju predstavimo glavne značilnosti kibernetskih groženj, ki jih za razvrstitev uporablja ENISA.

Zlonamerna programska oprema (angl. *Malware*)

Zlonamerni programi služijo predvsem omrežnim napadom, kraji identitete in podatkov (Varni na internetu, 2019).

Računalniški virusi so računalniški programi, ki so se sposobni samostojno razširiti prek drugih dokumentov ali računalniških programov. Napisani so z namenom uničevanja podatkov, oteževanja dela ali zbiranja podatkov s programsko opremo, ki je nameščena na računalniku. Virus je lahko pripet kot priloga elektronski pošti, datoteki ali kakemu drugemu programu. Napravo običajno okužimo z odprtjem okužene datoteke. Ko je naprava enkrat okužena, se virus samodejno prenese na ostale datoteke in programe, ki jih uporabljamo (EGRADIVO.ECNM, 2019).

Črv je podoben računalniškemu virusu, toda za svoje širjenje ne potrebuje drugih datotek. Je samostojen program, ki se poskusi samodejno razširiti na vse naprave oziroma računalnike (Pomagalnik, 2017).

Trojanski konj je škodljiva koda, ki lahko povzroči veliko škode na računalniku. Škodljiva koda vdre v računalnik, skrita za na videz neškodljivimi operacijami, kot so igre ali celo programi za odkrivanje virusov. Namen zlonamerne kode je dostopati do pomembnih podatkov ali jih uničiti. Tak virus je sposoben izbrisati trdi disk ali ukrasti zaupne informacije (Safe.si, 2019).

Zlonamerni programi se lahko med drugim širijo prek USB-ključev, družbenih omrežij, elektronske pošte in programov za hipno sporočanje (Varni na internetu, 2019).

Omrežje okuženih računalnikov (angl. *Botnet*)

Bot, okrajšava besede robot, predstavlja podtaknjen program, ki se iz našega računalnika poveže na nadzorni strežnik napadalca. Napadalec lahko nadzira od nekaj sto, tisoč ali še veliko več botov po vsem svetu. Skupino tujih nadzorovanih računalnikov imenujemo botnet, računalnike, ki so del botneta, pa včasih imenujemo tudi zombiji. Najpogosteje se uporabljajo za napade s poplavo podatkov ali za razpošiljanje neželene pošte (Varni na internetu, 2019).

Napadi na spletne aplikacije (angl. *Web Application Attacks*)

Število aplikacij je v porastu, prav tako pa tudi napadi nanje. Najpogostejše napade na spletne aplikacije predstavljajo vrivanje programske kode na spletno stran (angl. *cross-site scripting*, XSS) in napadi na zbirke podatkov ob pomoči vrivanja SQL-stavkov (angl. *SQL injection*) in napadi na piškotke (angl. *cookies*). Namen napada je lahko pridobivanje in zloraba podatkov, nameščanje zlonamerne kode ter zloraba ranljivosti aplikacije (Hölbl, 2019).

Spletni napadi (angl. *Web Based Attacks*)

Pri spletnih napadih gre največkrat za vzpostavitev lažnih spletnih strani, ki se uporabijo za nameščanje in širjenje zlonamerne programske opreme. Gre lahko za različne spletne strani, ki zahtevajo prijavo z uporabniškim imenom in geslom, tako napadalec pridobi zaupne podatke uporabnika. Tako kot pri napadih na spletne aplikacije predstavljajo tudi tukaj najpogostejše metode vrivanje programske kode na spletno stran, vrivanje SQL-stavkov, neželena oglaševalska oprema in preusmeritev rezultatov iskalnika (Hölbl, 2019).

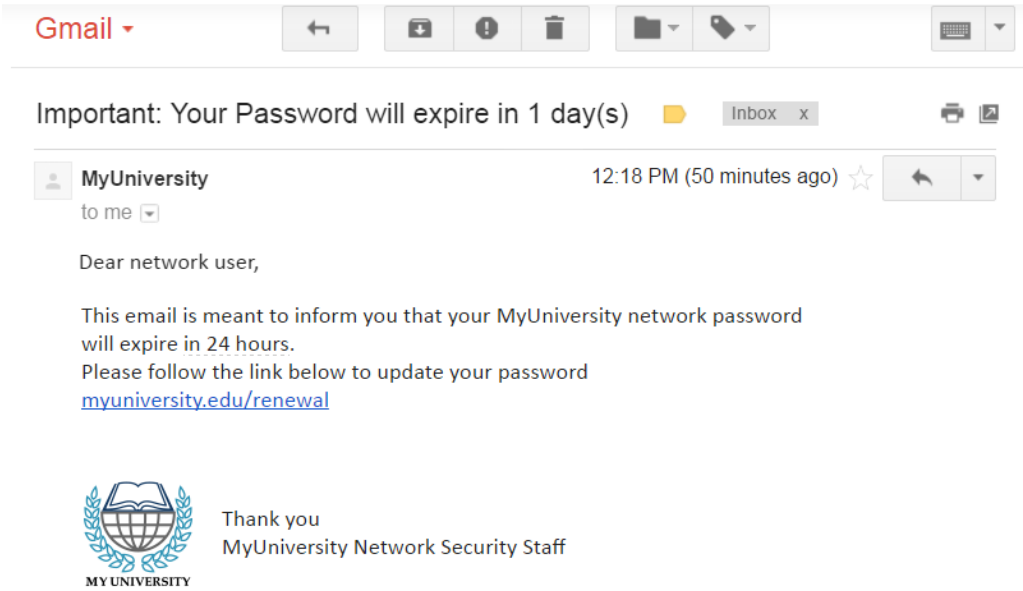
Ribarjenje (angl. *Phishing*)

Ribarjenje predstavlja nezakonito pridobivanje zasebnih in občutljivih podatkov, kot so številke kreditnih kartic, osebna identifikacija ter uporabniška imena in gesla. Do tega pride, ko napadalec, ki se maskira kot zaupanja vreden subjekt, žrtev pripravi v odpiranje e-poštnih sporočil ali neposrednih sporočil. Prejemnik je, ko odpre sporočilo, zvabljen, da odpre zlonamerno povezavo, ki ga največkrat privede na lažno stran banke ali kake druge spletne storitve, kjer se običajno pod pretvezo zahteva, da prejemnik preveri svoje

podatke ali pa se mu ponuja kakšna dodatna ugodnost ob prijavi. Če prejemnik na tej lažni spletni strani vpiše uporabniško ime in geslo za dostop in doda še kakšne druge osebne podatke kot svojo telefonsko številko, elektronsko pošto, naslov, številko kreditne kartice, se vsi vpisani podatki naprej posredujejo storilcu. Ribarjenje je mogoče uporabiti za napade na posameznike, različna podjetja in državne ustanove (Imperva, 2019).

Zelo pogosto se na področju ribarjenja pojavljajo zlorabe z elektronsko pošto. Na sliki 2 je prikazano elektronsko sporočilo, ki s pomočjo ribarjenja poskuša pridobiti uporabniško ime in geslo. Gre za klasično obliko socialnega inženiringa, saj se storilec izdaja za uslužbenca univerze. Storilec pošlje elektronsko sporočilo, ki je videti na primer kot pravo sporočilo univerze. Pošiljatelj v sporočilu prosi, naj vsi uporabniki posodobijo svoja uporabniška imena in gesla v roku 24 ur, saj bodo v nasprotnem primeru potekla. V sporočilu je dodana spletna povezava, na kateri si uporabnik lahko podaljša svojo uporabniško ime in geslo. Če uporabnik odpre to spletno stran in ne opazi, da bi bilo karkoli narobe, in vpiše svoje podatke, bodo ti podatki avtomatsko poslani napadalcu.

Slika 2: Primer elektronskega sporočila, ki s pomočjo ribarjenja poskuša pridobiti naše uporabniško ime in geslo



Vir: (Imperva, 2019)

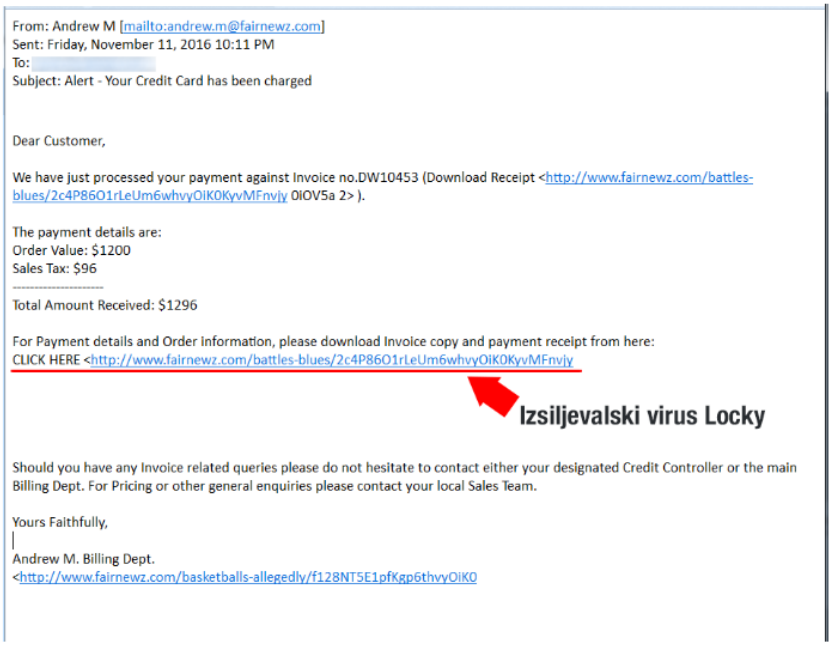
Prevaram se lahko izognemo tako, da nikoli ne odgovarjamo na elektronska sporočila, ki od nas zahtevajo osebne ali finančne podatke. Odsvetuje se odpiranje takšnih spletnih strani, saj nam legitimna podjetja ne bodo pošiljala takšnih zahtev po spletu ali elektronski pošti. Dobro je, da redno preverjamo izpise bančnih računov in kreditnih kartic, da morebitno prevaro hitro zaznamo in ustavimo. Svetuje se tudi, da imamo na računalnikih nameščene najnovejše popravke operacijskega sistema in da uporabljamo posodobljene protivirusne programe (SI-CERT, 2013).

Izsiljevalni programi (angl. *Ransomware*)

Izsiljevalni program je vrsta zlonamerne programske opreme, ki uporabnikom preprečuje dostop do njihovega osebnega in službenega računalnika ali drugih naprav. Čeprav so ti programi prišli v ospredju medijske pozornosti šele v zadnjih nekaj letih, so bile njihove najzgodnejše različice razvite že v poznih 80. letih prejšnjega stoletja. Obstaja več možnih načinov okužbe računalnika. Najpogostejša metoda danes je zlonamerna elektronska pošta. Postopek zavajanja je enak tistemu, ki smo ga opisali pri ribarjenju. Razlika je v tem, da gre pri ribarjenju za zlorabo osebnih podatkov, pri izsiljevalnih programih pa se uporabniku, ko odpre spletno povezavo v elektronskem sporočilu, nevede prenese izsiljevalni program. Druga priljubljena metoda okužbe, ki je svoj vrhunec dosegla leta 2016, je spletno oglaševanje. Na to metodo lahko naletimo med brskanjem po spletu, tudi če smo na varnih spletnih straneh, se nam lahko v pasicah pojavljajo zlonamerni oglasi in če oglas odpremo, nas lahko vodi na zlonamerno spletno mesto, kjer si lahko prenesemo izsiljevalni program (Malwarebytes, 2019). Izsiljevalski virusi delujejo tako, da na računalniku zašifrirajo vse, dokumente, fotografije, posnetke, besedilne in službene datoteke. Žrtev pa je primorana v zameno za dokumente izsiljevalcem plačati odkupnino, običajno v digitalni valuti bitcoin.

Slika 3 prikazuje primer zamaskiranega virusa v sporočilu o neplačanem računu. Zraven sporočila je priložena priponka, ki naj bi vsebovala račun, v resnici pa vsebuje virus.

Slika 3: Primer elektronskega sporočila, v katerem je zamaskiran izsiljevalni virus



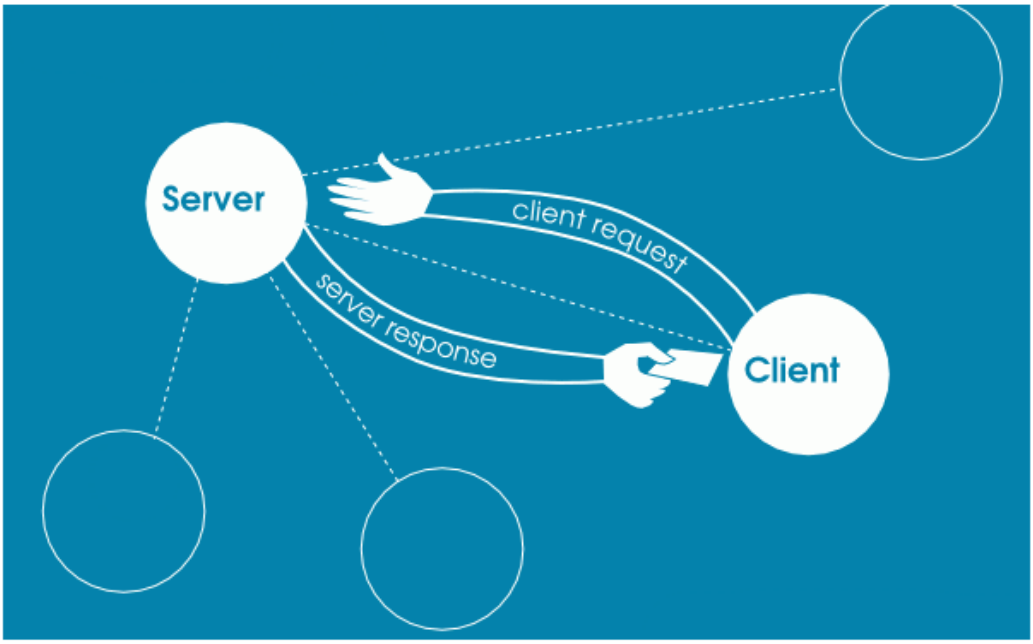
Vir: (Varni na internetu, 2016).

Porazdeljena ohromitev storitve (angl. *Distributed Denial of Service* – DDoS)

Da bi razumeli, kako delujejo napadi ohromitve storitve, moramo najprej razumeti, kako sploh deluje splet. Na sliki 4 je prikazan tipičen model odjemalec (angl. *client*) – strežnik (angl. *server*). Kliente predstavljamo mi oziroma naši spletni brskalniki na napravi. Prek

klienta dostopamo do spletne vsebine. Strežnik je opisan kot zmogljivejši računalnik, na katerem je naložena spletna vsebina, naloga strežnika je, da vsebino poda svojim klientom. Da lahko klient in strežnik komunicirata, morata biti povezana v omrežje. Komunikacija se začne pri klientu, ko obišče določeno spletno stran. Ob obisku spletne strani se strežniku avtomatično pošlje zahteva za dostop do spletne vsebine. Strežnik to zahtevo preveri, če zahteva ni zlonamerna, nam kot odziv vrne spletno stran, ki se nam naloži v brskalniku (Besal, 2015).

Slika 4: Primer modela odjemalec-strežnik



Vir: (Besal, 2015).

Celoten proces ne vzame veliko časa, odvisen je od hitrosti povezave ter programske in strojne opreme strežnika. Kako dolgo traja, da se nam stran prikaže, je lahko odvisno tudi od tega, koliko zahtev strežnik pridobi naenkrat. Če bosta tako na primer dva klienta hkrati poslala zahtevo na strežnik, razlika v času ne bo opazna, če pa je hkrati poslanih več tisoč zahtev in strežnik ni preveč zmogljiv, se lahko zgodi, da bo trajalo več sekund ali minuto, preden se bo stran naložila. Strežnik se lahko zaradi preobremenitve zruši in neha delovati (Besal, 2015). Pprav to je bistvo napada ohromitve storitev. Napadalci strežnik zasujejo z zahtevami v takšnem obsegu, da strežnik enostavno ne zmore obdelati vseh zahtevkov in odgovoriti nanje. Strežnik zaradi tega postane izjemno počasen in na koncu povsem neodziven. To pa pomeni, da normalni uporabniki ne morajo dostopati do storitev (Huš, 2017).

Napad na Dyn

Eden izmed največjih napadov ohromitve storitev se je zgodil 21. oktobra 2016 v Ameriki, kjer so hekerji napadli ponudnika internetnih storitev Dyn. Napad je povzročil, da je bilo v Evropi in ZDA nedostopnih veliko izredno priljubljenih strani, med katerimi so Amazon, BBC, Netflix, The New York Times, Twitter, Visa in številne druge. Izkazalo se je, da je šlo za obsežen napad ohromitve storitev, ki ga je izvajal bitnet Mirai. Mirai je zlonamerna

koda, ki okuži pametne naprave, povezane v internet. Ko so naprave okužene, iščejo preostale pametne naprave in se poskusijo vanje prijaviti s pomočjo različnih tovarniških uporabniških imen in gesel (Huš, 2017).

Analize so pokazale, da je bil napad delo manjše skupine, ki ga je izvedla s pomočjo kode Mirai, ki je prosto dostopna na internetu. Odgovornost za napad sta prevzeli hekerski skupini Anonymous in New World Heckers (Huš, 2017).

Neželena elektronska pošta (angl. *Spam*)

Neželena pošta so v večini tista elektronska sporočila, ki so poslana na več naslovov, običajno z oglaševalsko vsebino, na naslovnike, ki te vsebine niso želeli prejeti. Večina elektronskih sporočil nas nagovarja k nakupu izdelkov. Vmes se lahko velikokrat pojavijo tudi sporočila, ki vsebujejo zlonamerno kodo ali vsebino, če tako sporočilo odpremo, lahko postanemo žrtev prevare. Trend naraščanja pošiljanja neželene pošte je opažen tudi na družbenih omrežjih, kjer lahko napadalci na enostaven način dosežejo veliko število uporabnikov (Porenta, 2019).

Notranja grožnja (angl. *Insider Threat*)

Notranje grožnje so pomembna nevarnost v kibernetskem prostoru, ki so posledica namernih in nenamernih dejavnosti posameznikov, ki imajo omogočen dostop do notranjih informacij. Grožnjo lahko predstavljajo posamezniki, ki so zaposleni v organizaciji, nekdanji zaposleni, pogodbeni sodelavci in vsi ostali, ki so imeli in še imajo dostop do ključnih informacij o delovanju organizacije in želijo zaradi različnih interesov organizaciji škodovati (Košak, 2019).

Fizična manipulacija/poškodba/kraja/izguba (angl*. Physical manipulation/damage/ theft/loss*)

Fizična manipulacija/poškodba/kraja/izguba lahko ima resne posledice za vse vrste digitalnih sredstev. Fizično izgubo in krajo v zadnjem času nadomeščajo hekerski napadi in škodljiva koda, ki sta bila včasih pomembna vzroka za kršitev podatkov in ostajata pomembna tudi sedaj (Verizon 2018 , povzeto po Ministrstvo za javno upravo, 2018, str. 13). Prav tako fizični napadi predstavljajo veliko tveganje za kritično infrastrukturo.

Kršitev varnosti podatkov (angl. *Data Breaches*)

Kršitev varnostnih podatkov pomeni kršitev, ki vodi do nepooblaščenega razkritja oziroma dostopa do osebnih podatkov, spremembe, izgube ali uničenja podatkov (Informacijski pooblaščenec, 2019).

Pogosto pride do kršitve podatkov zaradi šibkih, ukradenih ali zlorabljenih gesel. Strokovnjaki so mnenja, da bodo organizacije vedno bolj izpostavljene novim in zahtevnejšim napadom, predvsem organizacije v zdravstvenem sektorju. Napadalci naprej prodajajo uporabniška imena in gesla na temnem spletu. Zaradi ponovne uporabe gesel bodo organizacije izpostavljene vdorom v svoje sisteme (Ministrstvo za javno upravo, 2019).

Uhajanje informacij (angl. *Data leakage*)

Uhajanje informacij predstavlja veliko grožnjo na področju kibernetske varnosti. Napadalci najpogosteje iščejo tiste informacije, ki so najdragocenejše za organizacijo. Prav zato je izjemno pomembno, da organizacije opredelijo najpomembnejše sisteme in podatke ter jih ustrezno zaščitijo in nadzorujejo. Najpomembnejši dejavnik pri uhajanju informacij so zaposleni v organizaciji. Do uhajanja informacij lahko pride namerno in tudi nenamerno, na primer z napačno naslovljeno elektronsko pošto ali z izgubljenimi napravami. Uhajanje informacij v velikem obsegu se prav tako lahko zgodi zaradi napake v programski kodi, ki jo organizacija uporablja (Ministrstvo za javno upravo, 2019).

Paket zlonamernih programov (angl. *Exploit Kits*)

Kompleti za izkoriščanje vsebujejo zbirko že vnaprej pripravljenih kompletov zlonamernih programov, ki so najpogosteje nameščeni na zlonamernih spletnih straneh ali pa se koristijo v kampanjah širjenja zlonamernih kod. Z uporabo takšnih kompletov je mogoče prepoznati ranljivosti v spletnih brskalnikih ali v spletnih aplikacijah in jih samodejno izkoristiti. Tarča kompletov za izkoriščanje so pogosto dodatki za brskalnike, kot sta na primer Adobe Flash in Java. Kompleti se zadnje čase tudi vse bolj uporabljajo za izkoriščanje v povezavi s socialnim inženiringom, najpogostejša metoda okužbe je skrita namestitev na računalnik v mimohodu, ko uporabnik brska po internetu (Ministrstvo za javno upravo, 2019).

Kibernetsko vohunjenje (angl. *Cyber-Espionage*)

Kibernetsko vohunjenje globalna podjetja in organizacije prepoznavajo kot eno od najresnejših groženj. Strokovnjaki na področju kibernetske varnosti pričakujejo v prihodnosti porast kibernetskega vohunjenja zaradi geopolitičnih razlogov, strateških ciljev posameznih držav in ekonomskih sankcij. Akterji na področju kibernetskega vohunjenja, med katere spadajo organizirani kriminal, kot tudi države, vztrajno razvijajo nova orodja in tehnike, ki bi jim pomagale pri kraji intelektualne lastnine in skrivnosti. Kibernetsko vohunjenje spada med napredne trajne grožnje (Ministrstvo za javno upravo, 2019).

Napredna trajna grožnja (angl. *Advanced Persistent Threat*) je vrsta hekerskega napada, pri katerem nepooblaščena oseba pridobi dostop do informacijskega omrežja in tam ostane neopažena dalj časa. Cilj napadalcev ni povzročiti škodo v omrežju, ampak ukrasti čim več zaupnih podatkov. Največkrat gre za organizirane skupine napadalcev s poslovnimi in političnimi motivi, ki ciljajo na organizacije, katerih informacije imajo visoko vrednost. Ko si napadalci zagotovijo vstop v omrežje, stremijo k okužbi enega ali več računalnikov z zlonamerno kodo, ki ima točno določeno nalogo, potem želijo ostati neopaženi, da si zagotovijo nemoten in dolgoročen dostop (Suhadolc, 2016).

Kraja identitete (angl. *Identity Theft*)

Kraja identitete predstavlja kibernetsko grožnjo, katere primarni cilj je pridobiti zaupne informacije, ki se lahko uporabijo za identifikacijo osebe ali računalniškega sistema. Med zaupne informacije spadajo prepoznavna imena, kontaktni podatki, naslovi, zdravstveni podatki, finančni podatki in podobno. Napadalci lahko zaupne informacije pridobijo na

različne načine, na primer na družabnih omrežjih, s hekerskimi napadi, z nakupom na temnem spletu, s pomočjo socialnega inženiringa in drugih tehnik (Ministrstvo za javno upravo, 2019).

Hiter razvoj tehnologije s sabo prinaša vedno nove pasti in grožnje, ki pretijo na nas, zato je prav, da te znamo hitro prepoznati in se pred njimi zavarovati. Nekatere od zgoraj opisanih groženj so lahko že zastarele, saj nepridipravi zmeraj iščejo nove tehnike in načine, s katerimi bi se lahko okoristili na tuj račun.

4 USMERITVE EU NA PODROČJU ZAGOTAVLJANJA KIBERNETSKE VARNOSTI

Vedno večja odvisnost od novih tehnologij, rast kibernetskih napadov in politične napetosti v svetu so prispevale k temu, da so države zadnjih nekaj let pospešeno delovale na področju kibernetske varnosti. EU se že nekaj časa zaveda, da so zapleti v zvezi s kibernetsko varnostjo vedno pogostejši in obsežnejši ter da ne poznajo meja. Takšni zapleti lahko bistveno poslabšajo varnost prebivalcev in storijo veliko škodo za gospodarstvo. Prav zaradi tega si EU prizadeva povečati zmožnosti za preprečevanje, sodelovanje in večjo preglednost na področju kibernetskih zapletov.

4.1 Organizacije, odgovorne za kibernetsko varnost

Glavni akter EU, odgovoren za kibernetsko varnost, je Evropska komisija, ki želi povečati zmogljivosti kibernetske varnosti in okrepiti sodelovanje EU kot igralca kibernetske varnosti in to vključiti v druge politike EU. Drugi akterji so glavni generalni direktorati. Generalni direktorat za informacijsko družbo in medije (GD CONNECT), ki je odgovoren za komunikacijska omrežja, vsebine in tehnologije, je služba Komisije, pristojna za politiko EU na področju enotnega trga, internetne varnosti ter digitalne znanosti. Generalni direktorat za migracije in notranje zadeve (GD HOME) je odgovoren za politiko EU na področju državljanstva, migracij in notranjih zadev. Generalni direktorat za informatiko (GD DIGIT) pa je odgovoren za digitalno infrastrukturo in druge digitalne storitve Komisije.

Evropsko komisijo podpirajo številne agencije, zlasti ENISA, ki podpira razvoj politik EU, krepitev zmogljivosti in ozaveščanje o kibernetski varnosti. Druga agencija je Evropski center za kibernetsko kriminaliteto (EC3), ki deluje v okviru Evropskega policijskega urada, Europol, ustanovljen je bil za boj proti kibernetskemu kriminalu. Naslednja agencija je CERT-EU (Computer Emergency Response Team), ki je stalna skupina za odzivanje na računalniške grožnje, ki podpira vse institucije, organe in agencije EU.

Evropska služba za zunanje delovanje (EEAS) ima nalogo, da skrbi za zunanjo in varnostno politiko ter diplomatske odnose. Vodi kibernetsko diplomacijo in strateško komuniciranje ter gosti obveščevalne centre. Evropska obrambna agencija (EDA) dela na razvoju zmogljivosti obrambe pred kibernetskimi napadi.

Primarno so države članice same odgovorne za lastno kibernetsko varnost. Na ravni EU pa prek Sveta delujejo številni organi za usklajevanje in izmenjavo informacij. Evropski parlament na tem področju deluje kot zakonodajalec.

Partnerji pri razvoju politik EU so tudi organizacije zasebnega sektorja (European Court of Auditors, 2019). Kibernetični ekosistem EU je kompleksen in večplasten ter v številnih državah članicah posega na raznorazna področja notranje politike, vse od pravosodja in notranjih zadev, enotnega digitalnega trga do raziskovalnih politik. V zunanji politiki je vprašanje kibernetske varnosti najbolj prisotno v diplomaciji, prav tako pa postaja vse bolj pomemben del nastajajoče obrambne politike EU.

4.2 Strategije na področju kibernetske varnosti

Temelj politike EU je strategija za kibernetsko varnost z naslovom »Odprt, varen in zavarovan kibernetski prostor« iz leta 2013, vključno s predlogom direktive Komisije o varnosti omrežij in informacij. V strategiji je predstavljena vizija EU ter kako najučinkoviteje preprečiti kibernetske motnje in napade. V strategiji so zapisani posebni ukrepi, ki se nanašajo na kibernetsko odpornost informacijskih sistemov, zmanjšanje kibernetskega kriminala ter na mednarodno politiko EU za kibernetsko varnost in kibernetsko obrambo EU (European Commission, 2013).

V strategiji iz leta 2013 je vizija EU za kibernetsko varnost osredotočena na pet prednostnih nalog (European Commission, 2013):

- »*krepitev kibernetske odpornosti;*
- *zmanjšanje kibernetskega kriminala;*
- *razvoj politike in zmožnosti za kibernetsko obrambo, povezanih s skupno varnostno in obrambno politiko;*
- *vlaganje v razvoj industrijskih in tehnoloških virov za kibernetsko varnost;*
- *določitev usklajene mednarodne politike EU za kibernetski prostor in spodbujanje temeljnih vrednot EU*«.

»*Direktiva je ključni del splošne strategije, na podlagi katere bi morale vse države članice, ponudniki interneta in upravljalci kritične infrastrukture, kot so platforme za elektronsko trgovanje, družabna omrežja ter upravljalci na področju energije, prevoza, bančništva in zdravstvenih storitev, zagotoviti varno in zaupanja vredno digitalno okolje po vsej EU*« (Maček, Mulec, & Močilar, 2016, str. 79).

Ukrepi, ki jih določa direktiva, so (European Commission, 2013):

- »*države članice morajo sprejeti strategijo za varnost omrežij in informacij ter določiti nacionalni organ, ki bo pristojen za varnost omrežij in informacij in bo imel ustrezne finančne in človeške vire, da bo zmožen preprečiti tveganja in zaplete na področju varnosti omrežij in informacij;*
- *vzpostavitev sistema sodelovanja med državami članicami in s Komisijo za pošiljanje zgodnjih opozoril o tveganjih in zapletih prek varne infrastrukture ter za sodelovanje in organizacijo rednih medsebojnih strokovnih pregledov;*
- *upravljavci kritičnih infrastruktur v nekaterih sektorjih (finančne storitve, prevoz, energetika, zdravstvo), ponudniki storitev informacijske tehnologije (zlasti trgovine z aplikacijami, platforme za elektronsko trgovanje, internetna plačila, računalništvo v oblaku, iskalniki, družabna omrežja) in javne uprave morajo prilagoditi svoje postopke za obvladovanje tveganja in poročati o večjih zapletih glede varnosti svojih temeljnih storitev*«.

V Resoluciji Evropskega parlamenta z dne 12. septembra 2013 (2013/2606(RSD)) navedejo tudi (Evropski parlament, 2013):

- *»ker je tehnologija temelj razvoja kibernetskega prostora in je nenehno prilagajanje tehnoloških spremembam nujno, če želimo izboljšati odpornost in varnost kibernetskega prostora EU;*

- *ker je treba sprejeti ukrepe, s katerimi bi zagotovili, da bo zakonodaja ohranila korak s tehnološkim razvojem, ter omogočili učinkovito identifikacijo in pregon kibernetskih kriminalcev in zaščito žrtev kibernetske kriminalitete;*
- *ker mora strategija EU za kibernetsko varnost vključevati ukrepe, ki se osredotočajo na ozaveščanje, izobraževanje, oblikovanje skupin za odzivanje na računalniške grožnje (CERT), vzpostavitev notranjega trga za proizvode in storitve s področja kibernetske varnosti ter spodbujanje naložb v raziskave, razvoj in inovacije«.*

V sklopu tega je takratna visoka predstavnica Unije za zunanje zadeve in varnostno politiko in podpredsednica Evropske komisije Catherine Ashton dejala (European Commission, 2013):

»*Da bi kibernetski prostor ostal odprt in svoboden, morajo na spletu veljati enaka pravila, načela in vrednote, kot jih EU podpira zunaj spleta. V kibernetskem prostoru je treba zaščititi temeljne pravice, demokracijo in pravno državo. EU sodeluje s svojimi mednarodnimi partnerji, civilno družbo in zasebnim sektorjem, da bi na splošno podkrepila te pravice.«*

Strategija kibernetske varnosti iz leta 2013 se povezuje s tremi pozneje sprejetimi strategijami (European Court of Auditors, 2019):

1. Evropska agenda za varnost, 2015. Cilji agende so izboljšati zakonodajo izvrševanja in potek sodnih procesov v boju proti kibernetskemu kriminalu, predvsem s posodabljanjem obstoječih politik in zakonodaje.
2. Strategija celotnega digitalnega trga, 2015. Strategija želi razširiti dostop do spletnih vsebin državljanom EU in predstavi vizijo posodobitve pravil o avtorskih pravicah.
3. Globalna strategija za zunanjo in varnostno politiko Evropske unije, 2016, želi okrepiti vlogo EU v svetu.

EU svoje strategije in ukrepe redno posodabljala in dopolnjuje. Zavedajo se, da se tehnologija nenehno in izjemno hitro razvija skupaj, z njo pa se z enako hitrostjo razvijajo novi možni napadi in grožnje, ki obsegajo širok spekter zlonamernih dejavnosti.

Evropski parlament je tako leta 2016 sprejel Direktivo NIS, uradno: Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Cilj te direktive je dvig ravni informacijske varnosti in vzpostavitev skupnih mehanizmov za odzivanje na kibernetske grožnje. Po direktivi bi države članice morale vzpostaviti nacionalni okvir za varnost omrežij in informacij, ki morajo vsebovati državno strategijo, vsaj en odzivni center in pristojen nacionalni organ, ki bo zadolžen za usklajevanje aktivnosti na ravni države (SI-CERT, 2018b).

Vzporedno z direktivo NIS je začela veljati tudi Splošna uredba o varstvu podatkov (GDPR), ki se uporablja od maja 2018.

20. decembra 2017 so institucije EU naredile velik korak k okrepitvi sodelovanja pri preprečevanju kibernetskih napadov. Z medinstitucionalnim dogovorom je bila

ustanovljena stalna skupina za odzivanje na računalniške grožnje CERT-EU, ki dela za vse institucije, organe in agencije EU. CERT-EU sodeluje z institucijami EU za informacijsko varnost, povezan pa je tudi z drugimi skupinami za odzivanje na računalniške grožnje v državah članicah in drugod. Smisel CERT-EU je, da z ostalimi skupinami deli informacije o grožnjah in načine za spopadanje z njimi (Generalni sekretariat, 2017).

18. oktobra 2018 so voditeljice in voditelji na zasedanju Evropskega sveta pozvali k sprejetju novejših ukrepov za okrepitev kibernetske varnosti EU. Poziv se je predvsem nanašal na ukrepe za onemogočanje kibernetskih napadov in odzivanje nanje.

Države članice EU za okrepitev svojih zmogljivosti vse bolj razvijajo sodelovanje pri kibernetski obrambi. Da bi članice dosegle ta cilj, je Svet 19. novembra 2018 sprejel posodobljen okvir politike EU za kibernetsko obrambo. Posodobitev EU omogoča upoštevanje varnostnih izzivov, ki so se, odkar je bil leta 2014 sprejet prvoten okvir, močno spremenili. V okviru so ponovno določena prednostna področja kibernetske obrambe in posodobljene vloge njenih akterjev.

V posodobljenem Okviru EU za politiko kibernetske obrambe EU določi šest prednostnih področij obravnave (Generalni sekretariat Sveta, 2018):

1. podpiranje razvoja zmogljivosti kibernetske obrambe v državah članicah;
2. izboljšanje zaščite komunikacijskih in informacijskih sistemov skupne varnostne in obrambne politike (SVOP), ki jih uporabljajo subjekti EU;
3. spodbujanje civilno-vojaškega sodelovanja;
4. raziskave in tehnologije;
5. izboljšanje možnosti za izobraževanje, usposabljanje in vaje;
6. okrepitev sodelovanja z zadevnimi mednarodnimi partnerji.

Glavni poudarek nameni razvoju zmogljivosti kibernetske obrambe in zaščiti komunikacijskih in informacijskih omrežij. Pri tem izpostavijo, da je pomembno, da se pri razvoju zmogljivosti in tehnologij kibernetske obrambe upoštevajo vsi vidiki razvoja zmogljivosti, vključno z doktrino, vodenjem, organizacijo, osebjem, usposabljanjem, industrijo, tehnologijo, infrastrukturo, logistiko in interoperabilnostjo. Kot druga prednostna področja pa izpostavijo usposabljanje in vaje, raziskave in tehnologijo, civilno-vojaško sodelovanje in mednarodno sodelovanje. V Okviru EU za politiko kibernetske obrambe (OPKO) so zapisali, da se kibernetski prostor hitro razvija in da je zato treba podpirati nov tehnološki razvoj na civilnem in vojaškem področju. Civilno-vojaško sodelovanje izpostavijo kot ključno na kibernetskem področju, saj morajo biti odzivi na kibernetske grožnje usklajeni (Generalni sekretariat Sveta, 2018).

9. aprila 2019 je Evropski svet sprejel Akt o kibernetski varnosti, ki vzpostavi sistem vseevropskih certifikacijskih shem za naprave, povezane z internetom. S tem želi doseči to, da bodo uporabniki lahko bolj zaupali v tehnologije IoT[2] in da bo podjetjem omogočeno lažje poslovanje v tujini. Certifikati se bodo uporabljali na različnih področjih, na primer za povezane igrače, pametne nosljive naprave, nadzorne sisteme in za pametna energetska omrežja. Certifikati veljajo v vseh državah EU. Nov akt podeli

[2] IoT, internet stvari, predstavlja vse naprave, ki so med seboj informacijsko povezane.

agenciji ENISA stalni mandat in jasneje določi njeno vlogo v boju zoper kibernetske nevarnosti (Svet Evropske unije, 2018).

Najaktualnejši okvir, ki ga je vzpostavil Svet 17. maja 2019, je Sklep Sveta o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo EU ali njene države članice. Na podlagi vzpostavljenega okvira lahko EU naloži ciljno usmerjene omejevalne ukrepe za odvračanje in odzivanje na kibernetske napade, ki predstavljajo zunanjo grožnjo za EU ali njene države članice, pa tudi za kibernetske napade na tretje države ali mednarodne organizacije, če EU meni, da so omejevalni ukrepi potrebni za dosego ciljev skupne zunanje in varnostne politike.

Novi režim sankcij velja za kibernetske napade, ki imajo velik učinek in (Svet Evropske unije, 2019a):

- ki so bili izvedeni iz držav zunaj EU ali
- se je uporablja infrastruktura zunaj EU ali
- so jih izvedli posamezniki, subjekti ali organi, ki delujejo zunaj EU, ali
- so bili izvedeni s podporo posameznikov, subjektov ali organov, ki delujejo zunaj EU.

Režim sankcij velja tudi za poskuse kibernetskih napadov, ki bi potencialno lahko imeli velik učinek na varnost EU in njenih držav članic.

V sklepu kibernetske napade opredelijo kot (Svet Evropske unije, 2019a):

- dostop do informacijskih sistemov;
- motnje informacijskega sistema;
- poseganje v podatke ali
- prestrezanje podatkov,

ki jih lastniki niso odobrili.

Okvir bo EU prvič omogočil, da bo naložila sankcije posameznikom ali subjektom, ki so odgovorni za kibernetske napade ali poskuse kibernetskih napadov, in tistim, ki nudijo finančno, tehnično ali materialno podporo za take napade ali so kako drugače vanje vpleteni (Svet Evropske unije, 2019b).

Omejevalni ukrepi vključujejo prepoved potovanja v EU za posameznike in zamrznitev premoženja za posameznike in subjekte (Svet Evropske unije, 2019b).

EU prav tako vlaga sredstva v podporo raziskavam in inovacijam za razvoj novih rešitev in tehnologij, ki bi pripomogle k večji kibernetski varnosti. Do leta 2020 bo EU v projekte kibernetske varnosti in v pravico do digitalne zasebnosti vložila skoraj 1 milijardo EUR. Približno polovica projektov za obdobje 2017–2020 bo izvedenih v okvirju javno-zasebnega pogodbenega partnerstva.

4.3 ENISA, Agencija EU za kibernetsko varnost

Agencija EU za varnost omrežij in informacij predstavlja središče strokovnega znanja o kibernetski varnosti. Ustanovljena je bila leta 2004. Agencija je zadolžena pomagati EU ter njenim članicam pri preprečevanju, odkrivanju in odzivanju na področju informacijske

in omrežne varnosti. Sedež agencije se nahaja na grškem otoku Kreta v mestu Heraklion, urad pa v Atenah. Trenutni direktor agencije je Udo Helmbrech.

Agencija tesno sodeluje z državami članicami in zasebnim sektorjem pri zagotavljanju nasvetov in rešitev ter izboljšanju njihovih zmogljivosti. Ta podpora med drugim vključuje:

- organizacijo vseevropskih vaj za kibernetsko varnost,
- razvoj in vrednotenje nacionalnih strategij kibernetske varnosti,
- sodelovanje in krepitev zmogljivosti CSIRT,
- študije o IoT in pametnih infrastrukturah, ki obravnavajo vprašanja varstva podatkov in tehnologij za izboljšanje zasebnosti.

ENISA prav tako podpira razvoj in izvajanje politike ter zakona EU o zadevah, povezanih z varnostjo omrežij in informacij. Od leta 2019 ima nalogo, da pripravi sistem vseevropskih certifikacijskih shem, ki bo služil kot podlaga za certificiranje izdelkov, procesov in storitev, ki podpirajo enotni digitalni trg (ENISA, 2019).

4.4 Informiranost državljanov EU na področju kibernetskega kriminala

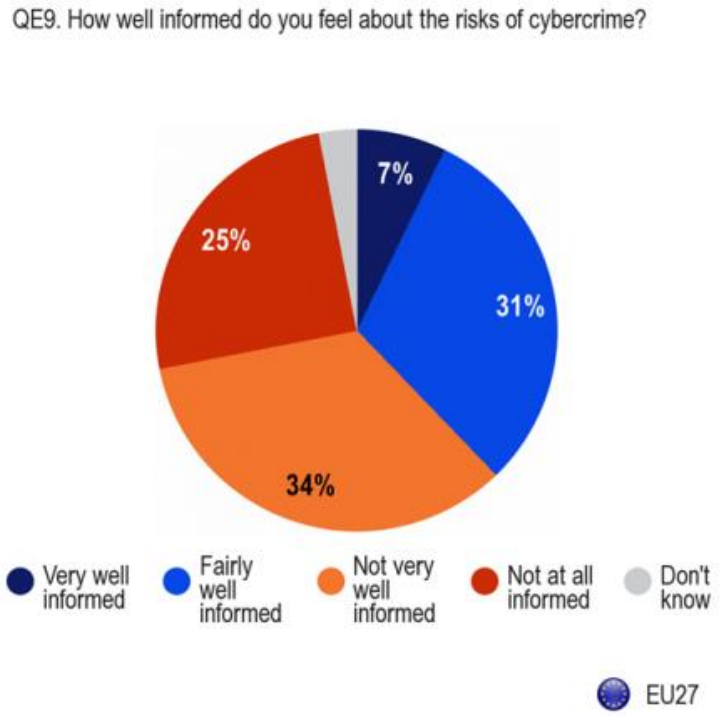
V tem delu proučimo, kako dobro informirani se državljani EU počutijo, ko govorimo o kibernetski kriminaliteti. Proučimo odnos uporabnikov interneta do kibernetske varnosti ne glede na to, ali so kdaj bili žrtev kibernetske kriminalitete ali ne.

Leta 2012 sta Evropska komisija in Generalni direktorat za notranje zadeve naročila raziskavo na temo »Cyber security« (kibernetska varnost), ki je bila izvedena s pomočjo TNS in Generalnega direktorata za notranje zadeve.

Na vprašanje, kako dobro menite, da ste informirani o kibernetski varnosti[3], je večina anketirancev odgovorila, da se ne počutijo dobro informirani. Slika 5 prikazuje (v odstotkih), kako dobro informirani se počutijo državljani EU glede tveganj kibernetskega kriminala. Samo 7 % državljanov EU se počuti zelo dobro informiranih, 31 % jih pravi, da se počutijo dokaj dobro obveščene. Večina (34 %) se jih počuti premalo informirane, 25 % pa jih meni, da sploh niso informirani.

[3] How well informed do you feel about risks of cybercrime?

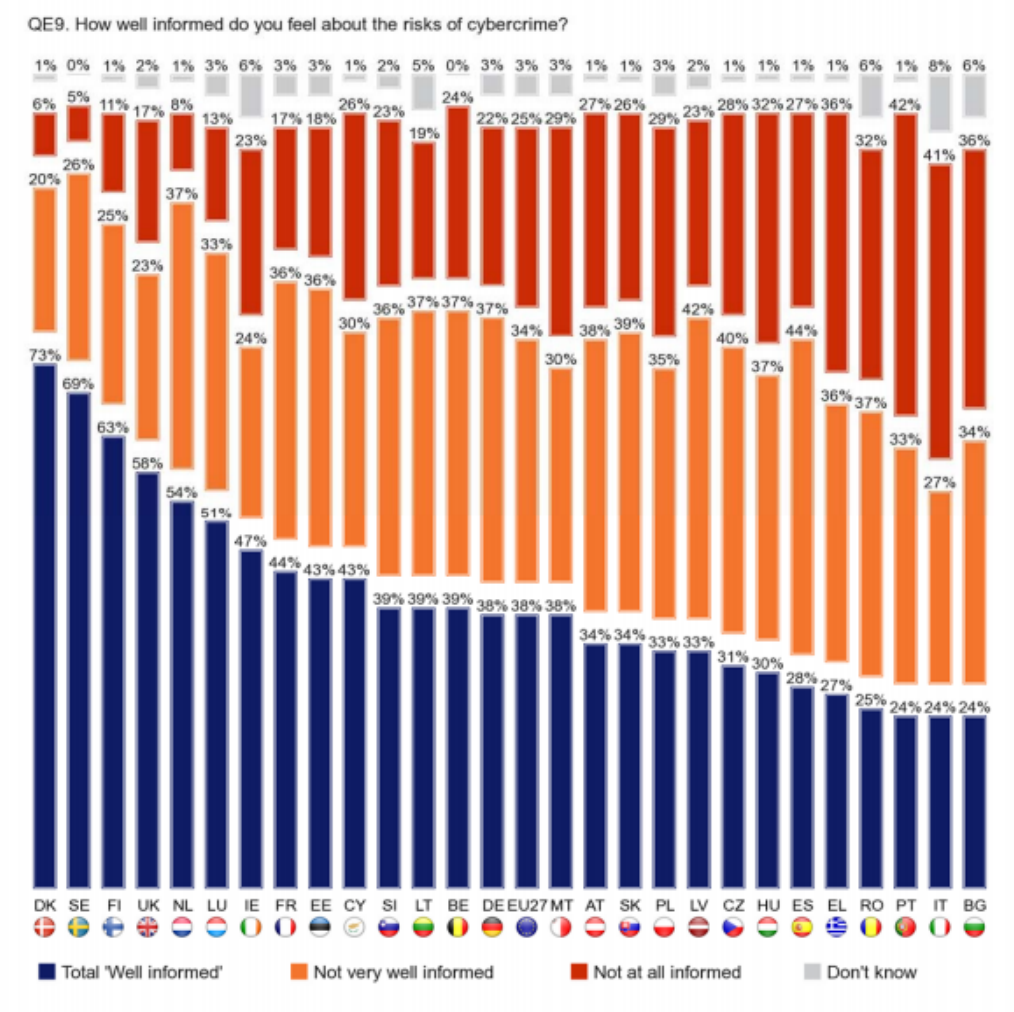
Slika 5: Tortni prikaz stopnje informiranosti v % za leto 2012



Vir: (TNS Opinion & Social, 2012).

Na sliki 6 lahko opazimo, da se pojavijo velike razlike od države do države glede na to, kako dobro se državljani počutijo informirane o kibernetskem kriminalu. Anketiranci na Danskem (73 %), Švedskem (69 %) in Finskem (63 %) se počutijo zelo ali dokaj dobro informirane, medtem ko se le četrtina anketiranih počuti zelo ali dokaj dobro informiranih v Bolgariji (24 %), Italiji (24 %), na Portugalskem (24 %) in v Romuniji (25 %). Italija in Portugalska izstopata po visokem deležu anketirancev, ki se sploh ne počutijo informirane (41 % in 42 %). V Sloveniji se kot dobro informiranih opredeli 39 % anketiranih, ne zelo dobro informiranih 36 % in kot sploh ne informiranih 23 %.

Slika 6: Stolpčni prikaz stopnje informiranosti po državah EU za leto 2012



Vir: (TNS Opinion & Social, 2012).

Raziskava je pokazala tudi, da se mlajši anketiranci po navadi počutijo bolje informirane kot starejši. Delež anketirancev, ki se počutijo zelo ali dokaj dobro informirane, se giblje med 52 % za anketirane, ki so stari med 15 in 24 let, do 25 % med starejšimi od 55 let.

Moški se pogosteje počutijo dobro informirane (43 %) v primerjavi z ženskami (33 %). Pri anketirancih, ki so ostali v izobraževanju vsaj do 20 leta (54 %), je bolj verjetno, da se počutijo bolje informirane o kibernetskem kriminalu kot tisti, ki končajo šolanje stari med 16 in 19 let (35 %) ali do 15 let (17 %).

Iz slike 7 je razvidno, da se ugotovitve razlikujejo glede na to, kako pogosto nekdo uporablja internet. Pri anketirancih, ki vsak dan dostopajo do interneta, je večja verjetnost, da se počutijo dobro informirane (55 %), kot pri anketirancih, ki dostopajo do interneta manj pogosto (30 %) ali pa do interneta sploh ne dostopajo (11 %).

Povezava obstaja tudi med dobro informiranostjo in občutkom samozavesti. Več kot polovica anketiranih, ki so samozavestni pri uporabi spletnega bančništva ali nakupovanja stvari na spletu, meni, da so dobro informirani o kibernetski kriminaliteti (59 %).

Slika 7: Prikaz stopnje informiranosti v % za leto 2012

QE9 How well informed do you feel about the risks of cybercrime?

	Total 'Well informed'	Total 'Badly informed'	DK
EU27	38%	59%	3%
Sex			
Male	43%	54%	3%
Female	33%	64%	3%
Age			
15-24	52%	47%	1%
25-39	47%	51%	2%
40-54	39%	58%	3%
55 +	25%	70%	5%
Education (End of)			
15-	17%	77%	6%
16-19	35%	62%	3%
20+	54%	44%	2%
Still studying	56%	43%	1%
Respondent occupation scale			
Self-employed	44%	53%	3%
Managers	62%	37%	1%
Other white collars	44%	54%	2%
Manual workers	36%	62%	2%
House persons	28%	68%	4%
Unemployed	39%	60%	1%
Retired	23%	71%	6%
Students	56%	43%	1%
Use of the Internet			
Everyday	55%	44%	1%
Often/ Sometimes	30%	67%	3%
Never	11%	82%	7%
Confident about its ability			
Total 'Confident'	59%	40%	1%
Total 'Not confident'	31%	67%	2%

Vir: (TNS Opinion & Social, 2012).

Raziskava je bila ponovljena leta 2015 in zajema podatke iz let 2013 in 2014. Raziskava pokaže, da se je delež državljanov EU, ki se počutijo dobro informirane o tveganjih kibernetskega kriminala, rahlo povečal.

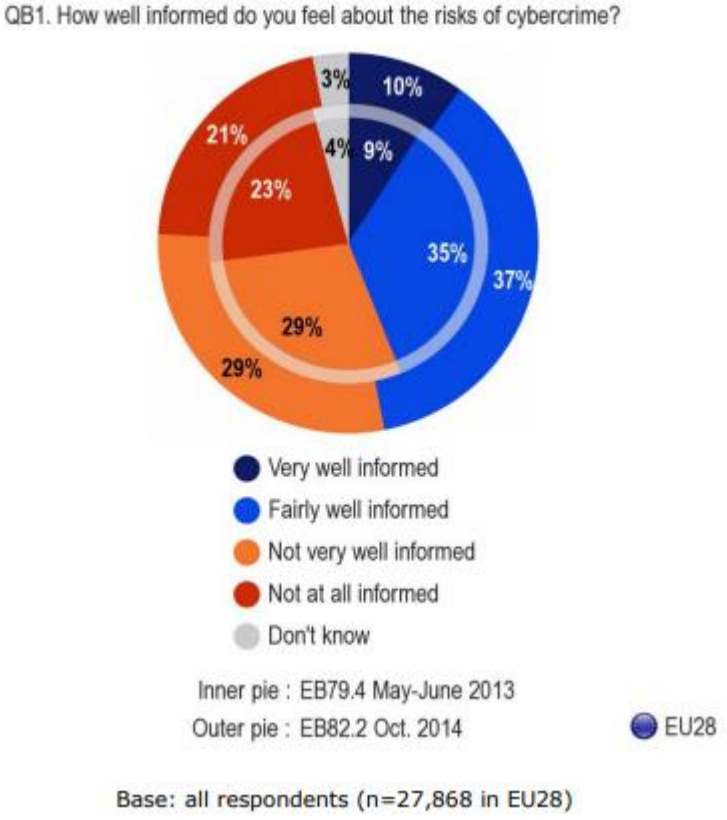
Slaba polovica državljanov EU (47 %) pravi, da se počutijo dobro obveščene o tveganjih kibernetske kriminalitete, od tega se jih 10 % počuti zelo dobro informiranih in 37 % dokaj dobro informiranih. Vendar pa 29 % vprašanih odgovarja, da se ne počutijo dobro informirane, 21 % pa, da se sploh ne počutijo informirani o tveganjih.

V notranjem delu tortnega grafikona (slika 8) so prikazani podatki za maj-junij 2013, v zunanjem delu pa za oktober 2014.

V primerjavi z raziskavo iz leta 2013 se je delež državljanov EU, ki se počutijo dobro obveščene o tveganjih kibernetskega kriminala, nekoliko povečal. V raziskavi iz leta 2014

47 % državljanov EU meni, da so zelo ali dokaj dobro informirani v primerjavi s 44 % iz leta 2013. Bistveno se zmanjša tudi delež tistih, ki pravijo, da sploh niso bili informirani, s 23 % v letu 2013 na 21 % v letu 2014.

Slika 8: Tortni prikaz stopnje informiranosti v % za leti 2013 in 2014



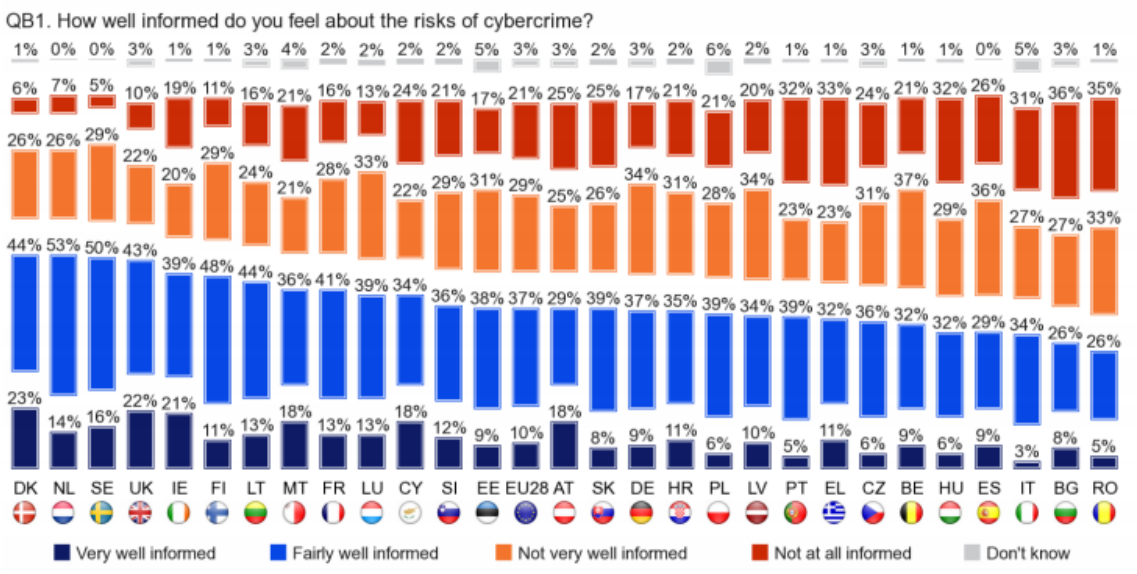
Vir: (TNS Opinion & Social, 2015).

Kako dobro so anketiranci informirani o kibernetski kriminaliteti za leti 2013 in 2014 (slika 9), se razlikuje od države do države. Anketiranci na Danskem (67 %), Nizozemskem (67 %), Švedskem (66 %) in v Združenem kraljestvu (65 %) se počutijo zelo ali dokaj dobro informirane. Najvišji delež anketirancev, ki menijo, da so zelo dobro informirani, je mogoče zaslediti na Danskem (23 %) in v Združenem kraljestvu (22 %). Anketiranci, ki se še zmeraj počutijo najmanj informirane, so v Bolgariji (34 %) in Romuniji (31 %). V Italiji in na Portugalskem se je delež državljanov, ki sploh niso bili informirani, v primerjavi z raziskavo iz leta 2012 zmanjšal za 10 %.

V Sloveniji se kot zelo ali dokaj dobro informiranih opredeli 48 % vprašanih, v primerjavi z raziskavo iz leta 2012 se je ta delež povečal za 9 %. Delež vprašanih, ki menijo, da niso dobro informirani, se je zmanjšal za 7 % in vprašanih, ki menijo, da sploh niso bili informirani, za 2 %.

Največjo rast, kjer anketiranci menijo, da so zelo ali dokaj dobro informirani, je mogoče zaslediti v Avstriji, kjer se je ta delež povečal za 13 %. Delež vprašanih, ki menijo, da so dobro informirani, se je v določenih državah zmanjšal. Na primer v Luksemburgu za 10 % in na Danskem za 7 %.

Slika 9: Stolpčni prikaz stopnje informiranosti v % za leti 2013 in 2014



Base: all respondents (n=27,868 in EU28)

Vir: (TNS Opinion & Social, 2015).

Slika 10 prikazuje, da so mlajši anketiranci po navadi bolje informirani od starejših. Delež vprašanih, ki se počutijo zelo ali dokaj dobro informirane, med 15–24 let znaša 67 %, med starejšimi od 55 let pa 31 %. Moški se pogosteje počutijo bolje informirane (53 %) kot ženske (43 %), v primerjavi z raziskavo iz leta 2012 se pri obeh spolih pojavi 10 % rast. Za anketirane, ki so ostali v izobraževanju vsaj do 20. leta (61 %), je bolj verjetno, da se počutijo bolje informirane o kibernetskem kriminalu kot tisti, ki končajo šolanje stari med 16 in 19 let (46 %) ali do 15 let (22 %).

Slika 10: Prikaz stopnje informiranosti v % za leti 2013 in 2014

QB1 How well informed do you feel about the risks of cybercrime?

	Total 'Well informed'	Total 'Not well informed'	Don't know
EU28	47%	50%	3%
Gender			
Man	53%	45%	2%
Woman	43%	54%	3%
Age			
15-24	67%	32%	1%
25-39	60%	39%	1%
40-54	50%	48%	2%
55 +	31%	64%	5%
Education (End of)			
15-	22%	72%	6%
16-19	46%	52%	2%
20+	61%	38%	1%
Still studying	70%	29%	1%
Socio-professional category			
Self-employed	55%	44%	1%
Managers	69%	30%	1%
Other white collars	59%	40%	1%
Manual workers	48%	50%	2%
House persons	32%	64%	4%
Unemployed	45%	53%	2%
Retired	29%	65%	6%
Students	70%	29%	1%
Use of the Internet			
Every day	64%	35%	1%
Often/ Sometimes	37%	62%	1%
Never	13%	80%	7%

Vir: (TNS Opinion & Social, 2015).

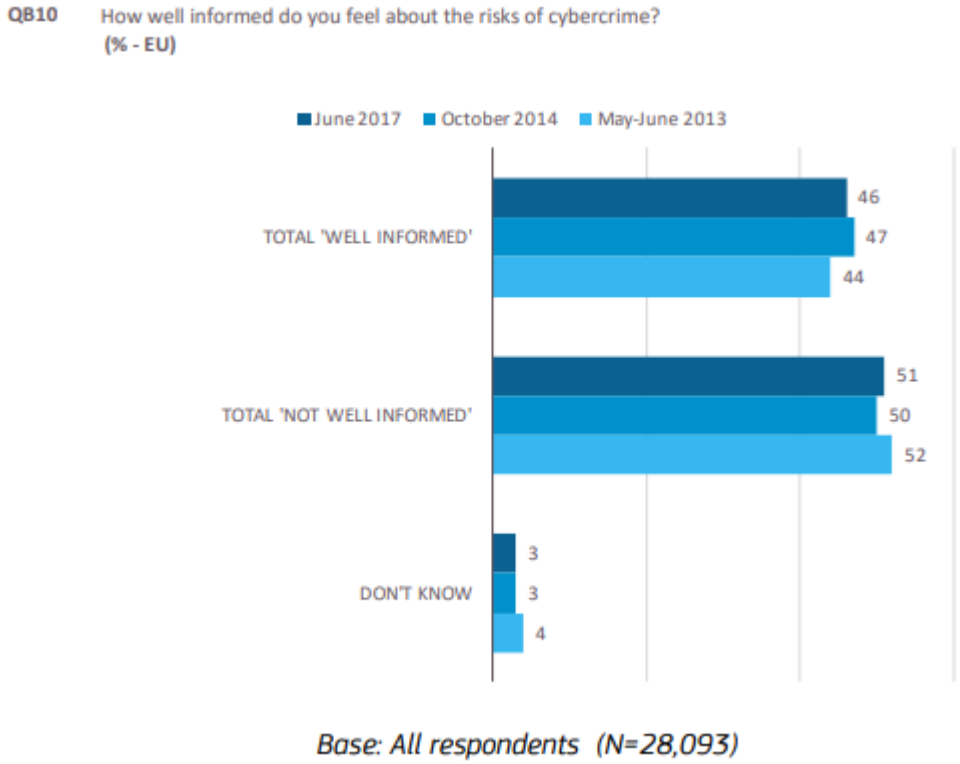
Če podatke iz leta 2012 primerjamo s tistimi iz leta 2015, vidimo, da se v raziskavi iz leta 2015 ljudje v državah članicah v povprečju počutijo bolj informirane glede kibernetskega kriminala, kot so se leta 2012. V parih letih je bilo največjo rast moč zaslediti prav v Avstriji (13 %), na Portugalskem (13 %) in Slovaškem (10 %). V Sloveniji je ta rast znašala 9 %.

Leta 2017 sta Evropska komisija in Generalni direktorat za migracije in notranje zadeve naročila raziskavo Odnos Evropejcev do internetne varnosti (Europeans' attitudes towards Internet security), ki je bila izvedena s pomočjo TNS in Generalnega direktorata za komuniciranje.

Anketiranci v tej anketi so odgovarjali na isto vprašanje kot v že omenjenih dveh anketah – kako dobro, menite, da ste informirani o kibernetski varnosti.

Skoraj polovica vprašanih meni, da so dobro informirani o kibernetskem kriminalu, vendar se odgovori močno razlikujejo po državah članicah. Slika 11 prikazuje, da 46 % anketiranih meni, da so dobro informirani, medtem ko jih 51 % meni, da niso dobro informirani.

Slika 11: Stolpčni prikaz stopnje informiranosti v % za leta 2017, 2014 in 2013



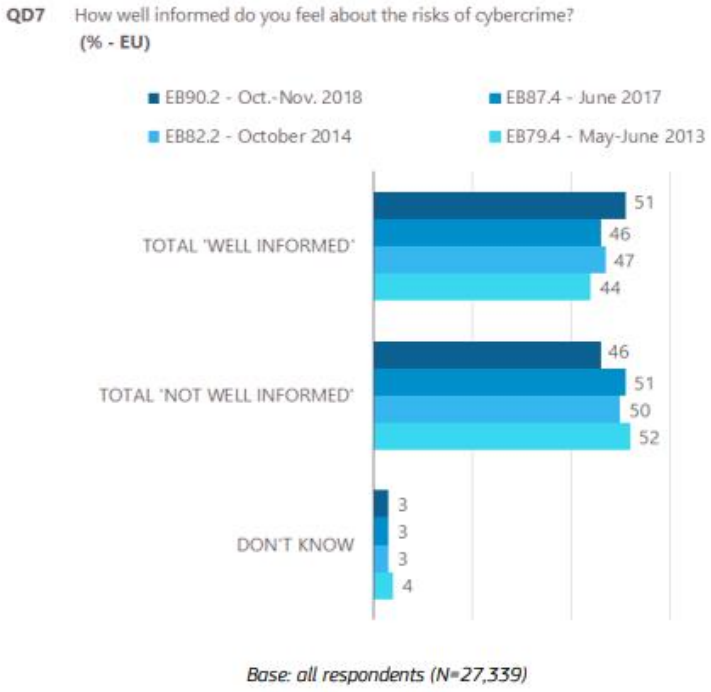
Vir: (TNS Opinion & Social, 2017).

Rezultati se v državah članicah močno razlikujejo. V 11 od 28 držav članic večina anketirancev meni, da so dobro informirani o kibernetskem kriminalu. Država, kjer večina prebivalci meni, da so dobro informirani, je Danska s 76 %. V Sloveniji se kot dobro informirane opredeli 48 % vprašanih, 29 % kot premalo informirane in 21 % kot sploh ne informirane.

Naslednja obravnavana raziskava s tega področja je iz leta 2019, Odnos Evropejcev do internetne varnosti (Europeans' attitudes towards Internet security). Tudi to raziskavo sta naročila Evropska komisija in Generalni direktorat za migracije in notranje zadeve, koordiniral pa jo je Generalni direktorat za komuniciranje in TNS.

Tako kot v prejšnjih raziskavah so tudi odgovori na to vprašanje precej enakomerno porazdeljeni. Slika 12 prikazuje, da nekaj več kot polovica državljanov EU (51 %) meni, da so dobro informirani, od tega jih 10 % meni, da so zelo dobro informirani, in 41 %, da so dokaj dobro informirani. Skoraj polovica anketirancev (46 %) je odgovorilo, da se ne počutijo dobro informirane, od tega jih 18 % meni, da sploh niso informirani, in 28 %, da so premalo informirani.

Slika 12: Stolpčni prikaz stopnje informiranosti v % za leta 2018, 2017, 2014 in 2013



Vir: (Kantar Public Brussels, 2019).

V 14 od 28 držav članic večina vprašanih meni, da so dobro informirani o kibernetski kriminaliteti. Državi, v kateri največ prebivalcev meni, da so dobro informirani, sta Danska in Švedska s 76 %. V Sloveniji se kot dobro informirane opredeli 41 % vprašanih, kar je za 8 % manj kot v raziskavi iz leta 2017, 31 % kot premalo informirane in 26 % kot sploh ne informirane. Če primerjamo podatek iz leta 2012, kjer se je 39 % anketiranih v Sloveniji opredelilo kot dobro informirane, s podatkom iz leta 2019, kjer se jih kot dobro informirane opredeli 41 %, opazimo, da gre za majhno in počasno rast v informiranosti.

Če povzamemo, se informiranost prebivalcev EU glede kibernetske varnosti iz leta v leto zelo počasi izboljšuje in raste. V raziskavi iz leta 2012 se je kot dobro informirane opredelilo 38 % državljanov EU, v zadnji raziskavi iz leta 2019 pa se kot dobro informirane opredeli 51 % državljanov EU. V nekaterih državah članicah je moč zaznati hitrejšo rast kot v drugih, v nekaterih državah pa rast tudi upade, kot je na primer v Sloveniji.

5 STRATEGIJA KIBERNETSKE VARNOSTI REPUBLIKE SLOVENIJE

Zgoraj opisanim usmeritvam na področju kibernetske varnosti EU sledi tudi Slovenija. Vlada je 25. februarja 2016 sprejela Strategijo kibernetske varnosti, ključni strateški dokument, ki ureja področje kibernetske varnosti v Sloveniji. V njej opredeljuje tveganja kibernetskega prostora, deležnike, področja udejanjanja strategije in cilje ter ukrepe za njihovo doseganje. Cilj strategije je do leta 2020 vzpostaviti celovit sistem zagotavljanja kibernetske varnosti, ki bo omogočal preprečevanje in odpravljanje posledic varnostnih incidentov. Ti ukrepi bodo prispevali k nemotenemu delovanju infrastrukture, ki je pomembna za delovanje državnih organov in gospodarstva ter za življenje vsakega posameznika (Maček, Mulec, & Močilar, 2016). Za uresničevanje strategije si je Republika Slovenija zadala osem ciljev (Agencija za energijo, in drugi, 2016).

- »okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti;
- varnost državljanov v kibernetskem prostoru;
- kibernetska varnost v gospodarstvu;
- zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore;
- zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala;
- razvoj obrambnih kibernetskih zmogljivosti;
- zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
- krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem«.

Pomembno dejstvo je, da prav internet podpira nemoteno delovanje informacijsko-komunikacijskih tehnologij na mnogih področjih, zaradi česar ga je treba ustrezno obravnavati in kot ključni podporni sistem zaščititi. Izpostavljen je tveganju, ki ga povzročajo tehnične okvare, človeške napake ter naravne in druge nesreče (Agencija za energijo, in drugi, 2016).

Za zagotavljanje kibernetske varnosti sodelujejo organizacije iz zasebnega in javnega sektorja. V strategiji kibernetske varnosti Republike Slovenije je zapisano, da imajo poleg prihodnje osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti ter vseh odzivnih centrov v državi pomembno vlogo tudi Agencija za komunikacijska omrežja in storitve, upravljalci telekomunikacijske infrastrukture in telekomunikacijski operaterji, ponudniki informacijskih storitev, nekatere raziskovalne organizacije in fakultete, zbornice s področja gospodarstva in podjetništva in razna strokovna združenja, vključno s proizvajalci programske opreme, ki nudijo podporo državnim organom. Med deležnike za zagotavljanje varnosti se v širšem pomenu štejejo tudi tuje organizacije s tega področja, v tem pogledu sta pomembna partnerja EU in NATO (Agencija za energijo, in drugi, 2016).

Vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti in jasne strukture upravljanja

Da bo Slovenija lahko nemoteno zagotavljala visoko raven kibernetske varnosti, mora učinkovito izrabljati obstoječe vire in imeti temu primerno večnivojsko organiziranost. Cilj Slovenije je, da se vzpostavi osrednja koordinacija nacionalnega sistema zagotavljanja kibernetske varnosti in da se zagotovi primerne pogoje za njeno stabilno delovanje. Slika 13 prikazuje shematski prikaz sistema zagotavljanja kibernetske varnosti. Na strateški ravni se bo koordinirala zmogljivost za zagotavljanje kibernetske varnosti na nižjih ravneh v državi in predstavljala enotno točko za mednarodno sodelovanje. Na operativni ravni bodo sodelovali:

- SI-CERT na nacionalni ravni,
- ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami,
- policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in preprečevanja kibernetskega kriminala,
- SOVA na področju protiobveščevalnega delovanja,
- SIGOV-CERT na področju javne uprave.

V sistemu bodo sodelovali tudi drugi deležniki, kot so upravljalci kritične infrastrukture v zasebnem in javnem sektorju, posebej pomembna sektorja sta energetski sektor in informacijsko-komunikacijski sektor. Na področju ozaveščanja, izobraževanja in raziskav bodo pomagale tudi nekatere fakultete in raziskovalne organizacije, ki bodo organizirale razne programe in izobraževanja na temo kibernetske varnosti. Dodatno bodo lahko razna slovenska strokovna združenja dajala pobude za izboljšave in nudila pomoč pri ozaveščanju ciljnih skupin (Agencija za energijo, in drugi, 2016).

Slika 13: Shema sistema zagotavljanja kibernetske varnosti.

VIR: (Agencija za energijo, in drugi, 2016).

SI-CERT

SI-CERT je nacionalni odzivni center za kibernetsko varnost. Naloga centra je koordinacija razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah ter drugih zlorabah. Center redno izdaja opozorila za upravitelje omrežij in javnosti o trenutnih grožnjah na elektronskih omrežjih. Deluje v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije). SI-CERT prav tako izvaja nacionalni program ozaveščanja Varni na internetu in sodeluje v projektu SAFE-SI (SI-CERT, 2019a).

Na področju Slovenije je bil 17. aprila 2018 sprejet Zakon o informacijski varnosti, ki jasno opredeli, da je SI-CERT s strani države prepoznan kot nacionalni odzivni center, in vsem zavezancem nalaga obvezno sporočanje kibernetskih incidentov na SI-CERT (SI-CERT, 2019b).

6 SKLEP

V delu diplomskega projekta smo se posvetili temi kibernetske varnosti na področju EU. Če povzamemo, lahko kibernetsko varnost opišemo kot skupek vseh zaščitnih ukrepov, ki so sprejeti za zaščito informacijskih sistemov in za našo lastno varnost pred nepooblaščenimi dostopi in napadi. Tehnologija nam v večini kot uporabnikom olajša in izboljša naša vsakodnevna opravila in življenje. Kot uporabniki tehnologije si danes več ne znamo predstavljati, kakšno bi bilo življenje brez nje. Danes praktično že vse organizacije in države digitalno shranjujejo podatke, ki jih potrebujejo za svoje delovanje. Prav tako je pomembna kritična infrastruktura, ki deluje znotraj kibernetskega prostora. Če pride do motenj ali napadov na kritično infrastrukturo, je lahko močno ogroženo delovanje držav in ljudi, ki tam živijo. Prav iz teh razlogov je ključnega pomena to, da države uredijo in razvijejo strategije odzivov na kibernetske grožnje, saj bodo v prihodnosti lahko le tako nadzorovale in se uspešno borile zoper kibernetske grožnje.

V delu diplomskega projekta raziščemo hipotezo, ki trdi, da je kibernetski kriminal v porastu. Raziskave, ki smo jih pregledali v začetnem delu naloge, nam to potrdijo, kibernetskih napadov je mogoče zaslediti vedno več v organizacijah, pa tudi pri posameznih uporabnikih. Tako v projektu izpostavimo 15 kibernetskih groženj, ki jih je definirala Evropska agencija za varnost omrežij in informacij ENISA. ENISA kot kibernetske grožnje navede zlonamerno programsko opremo, spletne napade, napade na spletne aplikacije, ribarjenje, neželeno pošta, porazdeljeno ohromitev storitve, izsiljevalne programe, omrežje okuženih računalnikov, notranjo grožnjo, fizično manipulacijo, kršitev varnosti podatkov, uhajanje informacij, paket zlonamernih programov, kibernetsko vohunjenje in krajo identitete. Vsako od teh groženj smo v nalogi na kratko predstavili, tako da se bomo lahko od zdaj naprej tudi mi bolj zavedali in predvsem hitreje prepoznali določen problem ali past, ki jo moramo čim prej javiti SI-CERT, kjer nam bodo svetovali in pomagali problem odstraniti ter sanirati.

V četrtem poglavju smo si podrobneje pogledali, kako področje kibernetske varnosti ureja EU, ki želi s pomočjo glavnih akterjev nadzorovati in obraniti EU pred kibernetskimi grožnjami. V ta namen EU vlaga vedno več sredstev. V sklopu tega so bile države članice zadolžene, da svoje državljane čim bolje ozavestijo in izobrazijo na področju kibernetske varnosti. V tem delu smo raziskali našo drugo hipotezo, ki trdi, da so uporabniki vedno bolj ozaveščeni glede kibernetskih tveganj. Primerjali smo dve raziskavi, eno iz leta 2012, drugo iz leta 2015, v katerih so bili zajeti podatki glede ozaveščenosti uporabnikov iz let 2012, 2013 in 2014. Iz raziskav je mogoče opaziti rahel dvig na področju ozaveščenosti uporabnikov. Povprečen dvig ozaveščenosti držav članic je leta 2014 znašal 3 %. Slovenija je glede na leto 2012 dosegla 9 % rast na področju ozaveščanja glede kibernetske varnosti.

V zadnjem delu dela diplomskega projekta na kratko predstavimo tudi Strategijo kibernetske varnosti Slovenije in pojasnimo, kako se bo Slovenija trudila vzpostaviti celovit sistem zagotavljanja kibernetske varnosti.

V delu diplomskega projekta na jedrnat način pojasnimo drugače izjemno širok pojem kibernetske varnosti. V nalogi smo zajeli osnove s tega področja, da smo lahko dobili

občutek, kako obsežno je pravzaprav to področje in delovanje EU na tem področju. Dejstvo je, da se tehnologija razvija in da se s tem razvijajo vedno nove grožnje, ki jim mora EU slediti in se prilagajati ter sprejemati takšno zakonodajo, ki bo uspešno vodila in pomagala pri reševanju sporov na področju kibernetske varnosti.

7 LITERATURA IN VIRI

Agencija za energijo, Agencija za komunikacijska omrežja in storitve, Ministrstvo za finance, Ministrstvo za gospodarski razvoj in tehnologijo, Ministrstvo za infrastrukturo, Ministrstvo za izobraževanje, znanost in šport, . . . Urad za varovanje tajnih podatkov. (2016). *KIBERNETSKA VARNOST.* Pridobljeno 15. avgust 2019 iz STRATEGIJA KIBERNETSKE VARNOSTI: http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Startegija_KV.pdf

Besal, Ž. (2015). *Kaj je DDoS napad?* Pridobljeno 12. avgust 2019 iz SmartNinja: https://www.smartninja.si/blog/kaj-je-ddos-napad-1437645281269

EGRADIVO.ECNM. (2019). *Kaj je računalniški virus?* Pridobljeno 10. avgust 2019 iz EGRADIVO.ECNM: http://egradivo.ecnm.si/osnove/kaj_je_raunalniki_virus.html

ENISA. (2019). *About ENISA.* Pridobljeno 15. avgust 2019 iz About ENISA: https://www.enisa.europa.eu/about-enisa

European Commission. (2013). *Načrt kibernetske varnosti EU za zaščito odprtega interneta ter svobode in priložnosti na spletu*. Pridobljeno 14. avgust 2019 iz Press Release Database: https://europa.eu/rapid/press-release_IP-13-94_sl.htm

European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy.* Pridobljeno 18. avgust 2019 iz Briefing Paper: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

Evropski parlament. (2013). *Strategija za kibernetsko varnost EU: odprt in varen kibernetski prostor.* Pridobljeno 14. avgust 2019 iz European Parliament: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//SL

Generalni sekretariat. (2017). *Kibernetska varnost Institucije EU okrepile sodelovanje pri preprečevanju kibernetskih napadov.* Pridobljeno 15. avgust 2019 iz Sporočila za javnost: https://www.consilium.europa.eu/sl/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/

Generalni sekretariat Sveta. (2018). *data.consilium.europa.eu.* Pridobljeno 19. avgust 2019 iz Okvir EU za politiko kibernetske obrambe (posodobitev za leto 2018): http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/sl/pdf

Generalni sekretariat Sveta. (2018). *Okvir EU za politiko kibernetske obrambe (posodobitev za leto 2018).* Pridobljeno 12. avgust 2019 iz Svet Evropske unije: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/sl/pdf

Hölbl, M. (2019). *Spletni napadi.* Pridobljeno 20. avgust 2019 iz Monitor: https://www.monitor.si/clanek/spletni-napadi/122720/

Homeland Security. (2019). *National Strategy to Secure Cyberspace*. Pridobljeno iz Homeland Security: https://www.dhs.gov/national-strategy-secure-cyberspace

Huš, M. (2017). *Največji napadi DDoS*. Pridobljeno 12. avgust 2019 iz Monitor: https://www.monitor.si/clanek/najvecji-napadi-ddos/180475/

Imperva. (2019). *Phising attacks.* Pridobljeno 10. avgust 2019 iz Imperva: https://www.imperva.com/learn/application-security/phishing-attack-scam/

Informacijski pooblaščenec. (2009). *Socialni inženiring.* Pridobljeno 8. avgust 2019 iz Informacijski pooblaščenec: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf

Informacijski pooblaščenec. (2019). *Prijava kršitev varnosti.* Pridobljeno 20. avgust 2019 iz Informacijski pooblaščenec: https://www.ip-rs.si/

Kantar Public Brussels. (2019). *Europeans' attitudes towards Internet security.* Pridobljeno 3. september 2019 iz file:///C:/Users/Lucija1/Downloads/ebs480_sum_en.pdf

Košak, M. (2019). *Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah.* Pridobljeno 20. avgust 2019 iz Univerza v Ljubljani, Fakulteta za računalništvo in informatiko: http://eprints.fri.uni-lj.si/3616/1/63020390-MATJA%C5%BD_KO%C5%A0AK-Sistem_za_podporo_odlo%C4%8Danju_pri_nadzoru_kibernetskega_tveganja_v_bankah.pdf

Lord, N. (2019). *What is Cyber Security? Definition, Best Practices & More*. Pridobljeno 8. avgust 2019 iz IT Governance: https://digitalguardian.com/blog/what-cyber-security

Maček, S., Mulec, F., & Močilar, F. (2016). *OTS 2016 Sodobne tehnologije in storitve.* (M. Heričko, & K. Kous, Ured.) Maribor: Fakulteta za elektrotehniko, računalništvo in informatiko.

Malwarebytes. (2019). *All about ransomware.* Pridobljeno 10. avgust 2019 iz Malwarebyts: https://www.malwarebytes.com/ransomware/

Mikelj, P. (2016). *Kibernetski prostor - novo področje geopolitičnega delovanja ZDA.* Pridobljeno 12. avgust 2019 iz Repozitorij Univerze v Ljubljani: http://dk.fdv.uni-lj.si/dela/mikelj-peter.PDF

Ministrstvo za javno upravo. (2019). *Ocena kibernetskih tveganj.* Pridobljeno 23. avgust 2019 iz Ministrstvo za javno upravo: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/ZKibP/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

NEFOS. (2019). *Kaj so podatkovne baze*. Pridobljeno 13. avgust 2019 iz NEFOS: https://nefos.si/podatkovne-baze/

Novak, M. (27. julij 2010). *STROKOVNA TERMINOLOGIJA – GRADNIK INTEROPERABILNOSTI KULTURNIH IN Z NJIMI POVEZANIH VSEBIN.* Pridobljeno 14. avgust 2019 iz Revija Knjižnica: https://knjiznica.zbds-zveza.si/knjiznica/article/view/6003/5650

Pomagalnik. (2017). *Virusi in škodljivi programi*. Pridobljeno 10. avgust 2019 iz Pomagalnik: https://www.pomagalnik.com/izobrazevanje/virusi-skodljivi-programi/

Porenta, J. (2019). *Spam – »mesni narezek« v vašem e-poštnem nabiralniku.* Pridobljeno 20. avgust 2019 iz Varni na internetu: https://www.varninainternetu.si/spam-mesni-narezek-v-vasem-e-postnem-nabiralniku/

PwC. (2019). *PwC's Global Economic Crime Survey 2018:UK findings.* Pridobljeno 20. avgust 2019 iz PwC: https://www.pwc.co.uk/forensic-services/assets/pwc-global-economic-crime-survey-2018-uk.pdf

Radware. (2019). *Radware Survey: Cybersecurity is no Longer a Cost Factor for $1B Organizations, Rather it's a Business Driver*. Pridobljeno 8. avgust 2019 iz Radware: https://www.radware.com/newsevents/pressreleases/c-suite-2019

Safe.si. (2019). *Trojanski konj*. Pridobljeno 10. avgust 2019 iz Safe.si: https://safe.si/pojmi/trojanski-konj

SAINT Consortium. (2019). *Cyber-Security Standards,Benchmarking & Best Practices Overview.* Pridobljeno iz SAINT: Systemic Analyzer In Network Threats: https://project-saint.eu/sites/default/files/saint_d2.7_cyber-security_standards_benchmarkingbest_practices_overview.pdf

SI-CERT. (2013). *Izsiljevalski virusi.* Pridobljeno 10. avgust 2019 iz SI-CERT: https://www.cert.si/izsiljevalski-virusi/

SI-CERT. (2018a). *Poročilo o omrežni varnosti za leti 2016 in 2017.* Pridobljeno 15. avgust 2019 iz SI-CERT: https://www.cert.si/wp-content/uploads/2018/04/SI-CERT_LP_2016_2017.pdf

SI-CERT. (2018b). *Zakon o informacijski varnosti brez glasu proti.* Pridobljeno 15. avgust 2019 iz SI-CERT: https://www.cert.si/zakon-o-informacijski-varnosti-brez-glasu-proti/

SI-CERT. (2019a). *O nas.* Pridobljeno 22. avgust 2019 iz SI-CERT: https://www.cert.si/o-nas/

SI-CERT. (2019b). *Zakon o informacijski varnosti brez glasu proti.* Pridobljeno 22. avgust 2019 iz SI-CERT: https://www.cert.si/zakon-o-informacijski-varnosti-brez-glasu-proti/

Smart Ninja. (2017). *KAJ JE SQL IN KJE GA LAHKO UPORABIMO?* Pridobljeno 13. avgust 2019 iz Smart Ninja: https://www.smartninja.si/blog/kaj-je-sql-in-kje-ga-lahko-uporabimo-1494487264334

Suhadolc, J. (2016). *Napredna trajna grožnja*. Pridobljeno 31. avgust 2019 iz LinkedIn: https://www.linkedin.com/pulse/napredna-trajna-gro%C5%BEnja-ali-apt-advanced-persistent-threat-suhadolc/?trk=hp-feed-article-title-publish&fbclid=IwAR16Dnf9hO4Wqs6FDWsXu0iOj7jAkKYhjGKWMK-kHABJQJQKixhCUyqLoy0

Svet Evropske unije. (2018). *Z dogovorom Sveta o skupni certifikacijski shemi in okrepljeni agenciji do večje kibernetske odpornosti EU.* Pridobljeno 15. avgust 2019 iz Sporočila za javnost: https://www.consilium.europa.eu/sl/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

Svet Evropske unije. (2019a). *SKLEP SVETA o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice.* Pridobljeno 14. avgust 2019 iz European Council: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/sl/pdf

Svet Evropske unije. (2019b). *Kibernetski napadi: Svet lahko zdaj naloži sankcije.* Pridobljeno 14. avgust 2019 iz Sporočila za javnost: https://www.consilium.europa.eu/sl/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

TNS Opinion & Social. (2012). *CYBER SECURITY.* Pridobljeno 12. avgust 2019 iz Special Eurobarometer 390: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf

TNS Opinion & Social. (2015). *CYBER SECURITY.* Pridobljeno 12. avgust 2019 iz Special Eurobarometer 423: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

TNS Opinion & Social. (2017). *Europeans' attitudes towards cyber security.* Pridobljeno 3. september 2019 iz https://internetsegura.cat/wp-content/uploads/2018/12/Sumari_ebs_464a_en_eurobarometre-2017.pdf

Varni na internetu. (2016). *Izsiljevalski virusi v letu 2016.* Pridobljeno 10. avgust 2019 iz Varni na internetu: https://www.varninainternetu.si/izsiljevalski-virusi-v-letu-2016/

Varni na internetu. (2018). *Kdo so etični hekerji?* Pridobljeno 13. avgust 2019 iz Varni na internetu: https://www.varninainternetu.si/kdo-so-eticni-hekerji/

Varni na internetu. (2019). *Vrste zlonamernih programov.* Pridobljeno 20. avgust 2019 iz Varni na internetu: https://www.varninainternetu.si/article/vrste-zlonamernih-programov/

Završnik, A. (2015). *Kibernetska kriminaliteta.* Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Žagar, A. (2019). *Kršitev GDPR zakonodaje: Googlu naložena 50 milijonska kazen*. Pridobljeno 8. avgust 2019 iz Mladipodjetnik: https://mladipodjetnik.si/novice-in-dogodki/novice/krsitev-gdpr-zakonodaje-googlu-nalozena-50-milijonska-kazen

Žlogar, M. (2019). *Temni splet – kaj se skriva v globinah dežele kriminala in prikritih storitev.* Pridobljeno 23. avgust 2019 iz Siol.net: https://siol.net/digisvet/novice/temni-splet-kaj-se-skriva-v-globinah-dezele-kriminala-in-prikritih-storitev-445007