Izdajatelj: Republika Slovenija Ref. št. dokumenta: 842-2/2018/11
Številka certifikata: af 92 46 a9 00 Čas podpisa: 08:05, 24.10.2018
Potek veljavnosti: 20.09.2023 Podpisnik: Rudi Medved

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 83 00
F: 01 478 83 31
E: gp.mju@gov.si
www.mju.gov.si

Številka: 842-2/2018/11
Datum: 26. 9. 2018

OCENA KIBERNETSKIH TVEGANJ

Verzija 1.0

	ORGAN	ODGOVORNA OSEBA
PRIPRAVILO IN SPREJELO	Ministrstvo za javno upravo	Rudi Medved Minister

Pripravil, uredil in oblikoval:

Marjan Kavčič, Ministrstvo za javno upravo, Direktorat za informacijsko družbo
© 2018 Ministrstvo za javno upravo

Kazalo

1. Uvod

Delovanje in celo sam obstoj sodobne družbe je neločljivo povezan z neprekinjenim in zanesljivim delovanjem informacijskih sistemov in omrežij. Vedno hitrejši razvoj informacijsko-komunikacijskih tehnologij po eni strani prinaša koristi za moderno družbo, po drugi strani pa vpliva na pojav vedno novih in tehnološko vse bolj dovršenih kibernetskih groženj. Vse izrazitejši je trend uporabe informacijsko-komunikacijskih tehnologij za kriminalne dejavnosti, terorizem in politično, gospodarsko ter vojaško prevlado. Uresničitev katere izmed kibernetskih groženj v večjem obsegu lahko ogrozi normalno delovanje gospodarstva in družbe kot celote, v najhujšem primeru tudi življenja ljudi. Nedvomno so prav kibernetska tveganja ena izmed najpomembnejših varnostnih tveganj v sodobnemu svetu, katerih obvladovanje je izjemnega pomena za zagotavljanje nacionalne varnosti države.

Ocena kibernetskih tveganj je izdelana na podlagi Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite (Uradni list RS, št. 62/14, 13/17), ki je v slovensko zakonodajo prenesla vsebino točke a 6. člena Sklepa št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L št. 347, z dne 20. 12. 2013, str. 924).

Ocena kibernetskih tveganj spada med ocene tveganja za posamezne nesreče za celotno območje države oziroma za posamezna območja države, kot je določeno v 2. členu Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite. Nosilec izdelave ocene je ministrstvo, pristojno za informacijsko družbo in elektronske komunikacije (trenutno Ministrstvo za javno upravo - MJU).

Ocena kibernetskih tveganj je bila narejena z namenom, da se celovito ugotovijo in opišejo pojavne oblike kibernetskih tveganj in njihove značilnosti. Namen ocene je tudi, da se z analizami tveganja ugotovi, kakšne posledice in v kakšnem obsegu lahko pričakujemo ob uresničitvi izbranih oziroma pripravljenih scenarijev tveganja.

2. Opis metod in tehnik, uporabljenih pri izdelavi Ocene kibernetskih tveganj

Vsebinsko in metodološko Ocena kibernetskih tveganj sledi določbam Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite.

Pri izdelavi ocene je bilo uporabljenih več raziskovalnih metod, in sicer deskriptivna metoda s proučevanjem področja kibernetskih groženj, njihovih akterjev in vektorjev napada, zgodovinska metoda s proučevanjem realiziranih kibernetskih groženj v preteklosti v Sloveniji in po svetu ter metoda analize in sinteze z aplikacijo razpoložljivih podatkov na primerih različnih scenarijev tveganja.

Pri izdelavi Ocene kibernetskih tveganj so bili uporabljeni številni strokovni in poljudni viri.

3. Klasifikacija kibernetskih groženj

Evropska agencija za kibernetsko varnost ENISA za razvrstitev kibernetskih groženj uporablja naslednjo klasifikacijo:

1. škodljiva koda (Malware),
2. spletni napadi (Web Based Attacks),
3. napadi na spletne aplikacije (Web Application Attacks),
4. zvabljanje (Phishing),
5. nezaželena elektronska pošta (Spam),
6. onemogočanje storitve (Denial of Service),
7. izsiljevalsko programje (Ransomware),
8. botneti,
9. grožnje od znotraj (Insider Threat),
10. fizična manipulacija/poškodba/kraja/izguba (Physical manipulation/damage/ theft/loss),
11. kršitve podatkov (Data Breaches),
12. kraja identitete (Identity Theft),
13. odtekanje informacij (Information leakage),
14. kompleti za izkoriščanje (Exploit Kits),
15. kibernetsko vohunjenje (Cyber-Espionage).

3.1. Škodljiva koda (Malware)

V letu 2017 so bili primeri škodljive kode najpogostejša oblika kibernetskih groženj, ki se stalno razvija tako glede izpopolnjenosti kot raznolikosti. Tako je bilo po podatkih nekaterih ponudnikov protivirusne programske opreme odkrito več kot 4 milijonov vzorcev na dan[1] ali več kot 700 milijonov vzorcev v prvem četrtletju leta 2017, medtem[2] ko je na črnem trgu na voljo na stotine za takojšnjo uporabo pripravljenih orodij, ki onemogočajo analizo škodljive kode. Čeprav se je na eni strani zmanjšalo število edinstvenih vzorcev škodljive kode za mobilne naprave, pa se je po drugi strani povečala njihova izpopolnjenost. V porastu so okužbe, ki ne zahtevajo odziva uporabnika (npr. klika na povezavo ali okuženo datoteko) ter okužbe, ki niso skrite v datotekah, kar še otežuje njihovo odkrivanje. Za napade se vedno pogosteje uporabljajo orodja, ki so že nameščena na računalnikih (npr. ukazne lupine) ali pa se skriptni ukazi poganjajo neposredno v delovnem spominu računalnika.

Hiter razmah okužb z izsiljevalskim virusoma WannaCry je spodbudil napadalce, da ponovno ovrednotijo uporabo računalniških črvov za hitro razširjanje okužb. Za zakrivanje sledi pri operacijah kibernetskih sabotaž in kibernetskega vohunjenja se je pričela uporabljati nadgrajena generacija brisalcev, iz istega razloga se je povečala uporaba skriptnih ukazov.

[1] https://www.avira.com/en/threats-landscape, dostop julij 2018

[2] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf, dostop julij 2018

Napadalci za razširjanje škodljive kode uporabljajo kategorijo potencialno neželenih programov (npr. različni dodatki, specialni brskalniki, lažno oglaševanje). Pri naprednih napadih se izkoriščajo tudi pomanjkljivosti strojne in programske opreme, ko se lahko s posodobitvami nevede namešča tudi škodljiva koda.

WannaCry *(WannaCrypt) je izsiljevalski virus, ki je maja leta 2017 povzročil enega največjih kibernetskih napadov na svetovnem spletu. Izkoristil je varnostne ranljivosti in pomanjkljivosti neposodobljenih Microsoftovih operacijskih sistemov Windows XP, Vista, 7, 8 in 10 ter napadel računalnike, na katerih so nameščeni omenjeni sistemi. Uporabnikom je zašifriral shranjene datoteke, za njihovo povračilo pa je zahteval plačilo odkupnine. Na tak način je prizadel več kot 300.000 računalnikov. Poleg posameznikov so bila med žrtvami tudi številna podjetja in organizacije.*[3]

Za doseganje čim boljšega uspeha napadalci izvajajo hibridne napade z uporabo dveh ali več različnih načinov napada. Pri tem je prvi način namenjen pritegnitvi pozornosti in preusmeritvi vseh varnostnih mehanizmov nanj, medtem, ko drugi oziroma več drugih načinov dejansko služi za izpolnitev napadalčevega namena.

Čeprav različice operacijskega sistema Windows tudi zaradi svoje razširjenosti še vedno prednjačijo po številu okužb, pa se je pričel povečevati tudi delež okužb v operacijskih sistemih MacOS in Linux.

V svetovnem merilu je z 90 do 95 % uspešnih napadov zvabljanje (phishing) prevladujoči vektor napada za razširjanje škodljive kode.

Zvabljanje *(ang. phishing) je v računalništvu nezakoniti način zavajanja uporabnikov, namenjen pridobivanju tujih občutljivih osebnih podatkov (številk kreditnih kartic, gesel, podatkov o računih itd.). Zvabljanje običajno poteka tako, da napadalec pod pretvezo uradne ustanove prepriča žrtev, da mu nujno posreduje te podatke. Prevare zvabljanja uporabniki običajno prejmejo z neželeno elektronsko pošto ali kot pojavna okna.*[4]

3.2. Spletni napadi (Web Based Attacks)

Spletni napadi zajemajo zlorabo spletnih brskalnikov skupaj z njihovimi dodatki in razširitvami, napade na spletišča skupaj s sistemi za upravljanje vsebin (Content Management Systems) ter zlorabe IT komponent spletnih storitev in spletnih aplikacij. Spletni napadi so bili ena najpomembnejših kibernetskih groženj v letu 2017[5], tako pa bo glede na pomembnost spletnih tehnologij in spletnih komponent v digitalnem svetu verjetno tudi v prihodnjih letih. Spletni napadi so v kombinaciji z napadi s škodljivo kodo zelo priljubljeni za širjenje okužb in nadzor

[3] https://sl.wikipedia.org/wiki/WannaCry, dostop avgusta 2018

[4] https://sl.wikipedia.org/wiki/Lažno_predstavljanje, dostop avgusta 2018

[5] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf, dostop julij 2018

žrtev. Pri tem razširjanje večine škodljive kode za področje bančništva[6] temelji na spletnih napadih. Odkriti so bili hrošči v priljubljenih aplikacijah za takojšnje sporočanje, ki napadalcu lahko omogočijo vdor v šifrirano sporočilo. Za širjenje škodljive kode se uporabljajo tudi java skripte, ker ne potrebujejo odziva s strani uporabnika. Pri tem za uporabnike veliko grožnjo predstavljajo ranljivosti v tako rekoč vseh spletnih brskalnikih. Vedno več je napadov tipa napajališče, ko se škodljiva koda z okuženih spletišč prenese na računalnike v mimohodu, ne da bi uporabniki za to vedeli. Take napade je težko raziskati, ker so ciljno usmerjeni. Tako so npr. napadeni samo uporabniki s specifično verzijo določenega brskalnika ali operacijskega sistema, uporabljajo IP naslov ciljane organizacije oziroma so z določenega geografskega področja. Število škodljivih spletnih naslovov, uporabljenih za globalno širjenje škodljive kode, ostaja visoko. Glede na poročila je bilo v drugem četrtletju leta 2017 takih naslovov več kot 33 milijonov[7] na strežnikih v ZDA (32 %), na Nizozemskem (20 %), v Franciji (11 %), na Finskem (10 %) in v Nemčiji (8 %).

Število spletnih napadov se je v letu 2017 močno povečalo in se je po številu odkritih primerov zelo približalo napadom s škodljivo kodo. V letu 2017 je 48 % zaznanih groženj prišlo do brskalnikov prek obiskov in prenosov z okuženih spletišč. 58 % distribucije škodljive kode v proizvodnih okoljih poteka prek spletnih prenosov[8]. Več kot polovica kibernetskih napadov sloni na spletnih tehnologijah.

Kot vektorji napada se pri spletnih napadih uporabljajo ranljivosti v spletnih brskalnikih, prenosi v mimohodu, škodljivi spletni naslovi in napajališča.

Napajališče *je strategija računalniškega napada, v kateri je žrtev določena skupina (organizacija, industrija ali regija). V tem napadu napadalec ugane ali opazuje, katere spletne strani skupina pogosto uporablja, potem pa okuži eno ali več od njih z zlonamerno programsko kodo. Samo ime izhaja iz narave, ko plenilci napadajo svoj plen blizu napajališč.*[9]

3.3. Napadi na spletne aplikacije (Web Application Attacks)

Napadi na spletne aplikacije so usmerjeni proti spletnim aplikacijam, spletnim storitvam in mobilnim aplikacijam ter poskušajo zlorabiti njihove vmesnike. Čeprav se nekoliko prekrivajo s spletnimi napadi, se ti napadi izvajajo v okviru okolja spletne aplikacije in aplikacijskih vmesnikov. Ta vrsta napadov je zelo priljubljena in verjetno bo tako tudi vnaprej, ker je večina spletnih aplikacij in spletnih storitev običajno izpostavljenih in javno dostopnih. Spletne aplikacije, ki so jih vzpostavile vladne in finančne organizacije, so priljubljen cilj napadov, čeprav je zaznati manjši upad v primerjavi s številom napadov na spletne aplikacije v letu 2016[10]. Napadi so usmerjeni v dobro znane sisteme in take, ki temeljijo na odprtokodnih

6 https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, dostop julij 2018

7 https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, dostop julij 2018

8 https://www.nttcomsecurity.com/us/gtic-2017-q2-threat-intelligence-report/, dostop julij 2018

9 https://en.wikipedia.org/wiki/Watering_hole_attack, dostop avgusta 2018

10 https://www.ptsecurity.com/upload/corporate/ww-en/analytics/WebApp-Attacks-2017-eng.pdf, dostop julij 2018

rešitvah, kot so npr. razširitve za sisteme za upravljanje vsebin (CMS) Wordpress, Magento itd. Načini izkoriščanja takih sistemov so vse bolj učinkoviti in, ko je določena ranljivost posameznega sistema javno znana, so hitro razvita in uporabljena orodja za njihovo izkoriščanje. Napadi z vrivanjem (npr. SQL vrivanje) zasedajo prvo mesto, v velikem porastu so napadi z izkoriščanjem XSS-ranljivosti, ranljivosti sistemov CMS pa so še vedno pomemben vir napadov. Zadnji so za napadalce še posebej vabljivi, saj njihova množična uporaba omogoča napade na zelo veliko spletišč. Veliko sistemov CMS je ranljivih zaradi uporabe ranljivih ali zastarelih razširitev.

XSS-ranljivost *je vrsta ranljivosti, ki se običajno nahaja v spletnih aplikacijah in omogoča napadalcem, da na spletne strani vrinejo skripte, ki se izvedejo pri uporabnikih. Napadalci lahko uporabijo skripte, da bi obšli kontrole dostopa, kot je npr. politika istega izvora. Učinki XSS-ranljivosti se razlikujejo v razponu od malih nevšečnosti do občutnih varnostnih tveganj, odvisno od občutljivosti podatkov, ki jih obravnava ranljivo spletno mesto, in narave varnostnih ukrepov, ki jih izvaja lastnik spletnega mesta.*[11]

Priljubljena cilja napadalcev so spletišča vladnih organizacij in IKT podjetij. Poročilo[12] o spletnih napadih iz leta 2017 poroča o povprečno 1,8 milijardah napadov dnevno, pri čemer je bilo odkritih 6298 edinstvenih primerov, 69 % podjetij pa je zabeležilo hude napade.

3.4. Zvabljanje (Phishing)

Zvabljanje je zelo prodoren napad, ker pri napadu na končne uporabnike prvenstveno uporablja socialni inženiring. Zvabljanje je pomemben vektor okužbe pri vseh vrstah kibernetskih groženj. Ker postaja vse bolj izpopolnjeno in usmerjeno, ga je vedno težje odkriti, za njegovo preprečevanje pa je potreben večplastni varnostni pristop, ki za podporo tradicionalnim varnostnim ukrepom uporablja tudi strojno učenje. Napadi z zvabljanjem so se okrepili tako po številu kot izpopolnjenosti. Zvabljanje se v veliko primerih uporablja kot prvi korak pri kibernetskih napadih in je najbolj uspešen vektor okužbe pri kršitvah varnosti podatkov in varnostnih incidentih tako v ciljanih kot naključnih primerih napada. Zvabljanje, ki je povezano z večino kibernetskih groženj, kot so botneti, škodljiva koda, spletni napadi, kompleti za izkoriščanje, kibernetsko vohunjenje itd., je na voljo tudi v obliki storitve, ki jo lahko najamejo spletni kriminalci.

Socialni inženiring *(ang. social engineering) je med prevaranti najpogosteje uporabljena tehnika v primerih zlorabe osebnih podatkov. Gre za tehniko, s katero napadalec od žrtve pridobi zaupne podatke in informacije s pomočjo zlorabe zaupanja. To je manipulacija, ki je v večini primerov psihološko pogojena, saj napadalec uporablja različne psihološke tehnike kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva in podobno, ter z uporabo socialnih*

[11] https://en.wikipedia.org/wiki/Cross-site_scripting, dostop avgusta 2018

[12] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf, dostop julij 2018

veščin in zlorabo zaupanja pridobi od žrtve zaupne informacije. Temeljni cilj te tehnike je pridobitev podatka, ki se ne pojavlja samo v digitalni obliki, temveč tudi kot pisano besedilo, slika, ustni podatek ali informacija. Pridobljene podatke lahko napadalec uporabi za pridobivanje premoženjske koristi, redkeje pa se lahko zgodi, da jih uporabi tudi v druge namene kot so izsiljevanje, grožnje, šikaniranje itd.[13]

Napadi z zvabljanjem so bili prvotno del obsežnih neciljanih kampanj neželene elektronske pošte. Njihov cilj je bil, da bi dovolj veliko število računalnikov okužili in na ta način od uporabnikov pridobili zaupne podatke. V novejšem času je cilj še vedno isti, vendar so postali napadi z zvabljanjem bolj ciljno usmerjeni in izpopolnjeni[14]. Izraz „Spear-phishing“ označuje napad na določenega posameznika ali skupino ljudi. Primer so napadi na vodstveni kader v organizacijah z namenom kraje denarja in kibernetskega vohunjenja. Neželena elektronska pošta in zvabljanje sta povezani kibernetski grožnji, medtem, ko se botneti[15] običajno uporabljajo za njuno dostavo. Po navedbah podjetja Kaspersky lab[16] je prišlo do povečanja ciljnih napadov, pri katerih je bila elektronska pošta predstavljena kot poslovna korespondenca. Napadalci pri svojih napadih uporabijo podatke resničnih organizacij in na ta način pridobijo zaupne podatke nasprotne strani (npr. pri medsebojnem komuniciranju organizacij in podjetij). Takšni ciljni napadi so običajno namenjeni pridobivanju finančnih koristi, bodisi z dostavo izsiljevalskega programja, ki zahteva odkupnino za dešifriranje podatkov, dostavo vohunskega programja za krajo finančnih informacij itd. Uspeh napadov z zvabljanjem pogosto temelji na občutku nujnosti, ki ga napadalci vzbudijo pri svojih žrtvah. Tako npr. zahtevajo odziv v kratkem časovnem obdobju, kar pri uporabnikih sproži hiter in nepremišljen odziv, zaradi katerega napadalci pridejo do želenih zaupnih informacij.

3.5. Nezaželena elektronska pošta (Spam)

Neželena elektronska pošta, ki je ena od najbolj razširjenih in trajnih kibernetskih groženj že vse od začetkov interneta, je bila ter še vedno je glavno sredstvo za dostavo zlonamerne programske opreme s pomočjo njenih prilog ter povezav do okuženih spletišč. Neželena elektronska pošta v svetovnem merilu predstavlja večino elektronske pošte. Večina elektronskih sporočil skuša oglaševati proizvode s področja zdravja in različne načine za spoznavanje ljudi, razpošiljajo pa jih predvsem omrežja botnetov.

Čeprav je količina neželene elektronske pošte od leta 2016 nekoliko upadla, pa se je izboljšala zmožnost preslepitve filtrov za njeno zatiranje. Po poročilih Spamhaus[17] do 80 % neželene elektronske pošte ustvari skupina okrog sto znanih stalnih kriminalnih združb.

13 https://sl.wikipedia.org/wiki/Socialni_inženiring, dostop avgusta 2018

14 https://www.eff.org/deeplinks/2017/09/phish-future, dostop julij 2018

15 https://thehackernews.com/2017/10/peter-levashov-kelihos.html, dostop julij 2018

16 https://securelist.com/spam-and-phishing-in-q2-2017/81537/, dostop julij 2018

17 https://www.spamhaus.org/statistics/spammers/, dostop julij 2018

Napadalci so za doseganje svojih ciljev v sporočilih pričeli uporabljati imena resničnih podjetij in ljudi. Nov razvoj neželene elektronske pošte se je pričel s prehodom z elektronskih sporočil na družbena omrežja. Na ta način so se napadalci izognili filtrom neželene elektronske pošte na poštnih strežnikih in še povečali svoj doseg.

V četrtem četrtletju leta 2017 je bil povprečen dnevni obseg neželene elektronske pošte približno 454 milijard, kar predstavlja približno 85 % obsega vse elektronske pošte dnevno[18]. Statistični podatki o neželeni elektronski pošti kažejo, da 88 % vse neželene pošte pošiljajo botneti, 91 % sporočil vsebuje kakšno obliko povezave, 66 % neželene elektronske pošte pa je povezanih s farmacevtskimi izdelki[19].

3.6. Onemogočanje storitve (Denial of Service)

Napadi z onemogočanjem storitve (DoS) in še zlasti distribuirani napadi z onemogočanjem storitve (DDoS) so še naprej pomembna grožnja za skoraj vsa podjetja in organizacije, ki so prisotna na spletu. IoT botnet Mirai je bil v zadnjem četrtletju leta 2017 odgovoren za največje DDoS napade v zgodovini s pasovno širino več kot 1Tbps. S tem so bila potrjena opozorila strokovnjakov o vplivu nepravilno zavarovanih naprav interneta stvari (IoT) na delovanje interneta.

Napovedi za v prihodnje[20] predvidevajo povečanje napadov s stalnim onemogočenjem storitve (Permanent Denial of Service - PDoS) za podatkovne centre in naprave interneta stvari, povečan pomen in izpopolnjenost napadov telefonskega onemogočanja storitve (Telephony Denial of Service - TDoS) ter povečanje segmentiranih (in celo osebnih) napadov onemogočanja storitve v kombinaciji s kibernetskim izsiljevanjem (Ransom-DoS), pri čemer so možni cilj zdravstveni sistemi. Izbruha izsiljevalskih virusov WannaCry in Petya sta primera povezave izsiljevalskih virusov in napadov z onemogočanjem storitve.

Število napadov DDoS narašča. Glede na raziskave[21] se je s takim napadom leta 2017 srečala več kot tretjina (33 %) organizacij. Leta 2016 je bilo takih organizacij le 17 %, kar kaže na zelo hiter razvoj na področju kibernetskih groženj, to pa pomeni, da so vsa podjetja, ne glede na velikost, ogrožena zaradi tovrstnih napadov. Napadalci so pričeli uporabljati impulzne napade z onemogočanjem, ki v nasprotju s trajnim onemogočanjem enega cilja delujejo s kratkimi impulzi za onemogočanje več ciljev hkrati. Pojavila se je možnost najema storitev napada z onemogočanjem (DDoS as a Service), cene takih storitev pa se znižujejo. Napadi DDoS se včasih uporabljajo za zakrivanje drugih vrst napadov, npr. okužb s škodljivo kodo (50 %), odtekanja ali kraje podatkov (49 %), vdorov v omrežje (42 %) ali finančne kraje (26 %).

[18] https://www.talosintelligence.com/reputation_center/email_rep#global-volume,. dostop julij 2018

[19] https://antispamengine.com/spam-statistics/, dostop julij 2018

[20] https://security.radware.com/ddos-experts-insider/ddos-practices-guidelines/cyber-security-predictions-2017/, dostop julij 2018

[21] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizacije, dostop julij 2018

3.7. Izsiljevalsko programje (Ransomware)

V zadnjih letih je izsiljevalsko programje vidna grožnja. Njihova dobičkonosnost je visoka in še naprej raste. Za razliko od tradicionalnega zlonamernega programja, kot so bančni trojanci, vohunska programska oprema in snemalniki vnosov na tipkovnici, ki zahteva več korakov preden napadalci dosežejo svoje cilje, se da z izsiljevalskim programjem hitro priti do premoženjske koristi. Z najemanjem izsiljevalskih storitev (Ransomware as a Service – RaaS) se jih lahko poslužujejo tudi manj vešči napadalci. Napadalci so se usmerili na ciljane napade na podjetja, medtem, ko imajo masovni napadi na navadne uporabnike manjši pomen. V svetovnem merilu so predvsem izpostavljene finančne organizacije. Višine odkupnin se višajo. Ocena skupnega zneska plačanih odkupnin v letu 2017 presega pet milijard dolarjev. Ta trend je zaskrbljujoč, saj napadalci izvajajo napade na nove in potencialno bolj dobičkonosne cilje. Izbruha izsiljevalskih virusov WannaCry in Notpetya sta pokazala skrb zbujajoč uničevalni potencial takih groženj.

Trend pri izsiljevalskem programju gre v smeri vedno večje zahtevnosti. Ogrožene so naprave in operacijski sistemi vseh vrst. Povečuje se število izsiljevalskih virusov za mobilne naprave, prav tako so ogrožene medicinske naprave, pri katerih se je kot vektor napada udomačil izraz Medical Device Hijack – MADJACK.

V letu 2017[22] je v 60 % primerih škodljiva koda vsebovala izsiljevalske viruse. 15 % ali več podjetij v glavnih desetih industrijskih sektorjih je bilo napadenih z izsiljevalskim programjem. Višina povprečne odkupnine se je povišala na 1077 dolarjev. Pri tem kljub plačilu odkupnine 20 % podjetij nikoli ni prišlo do svojih podatkov. Kar 72 % okuženih podjetij ni imelo dostopa do svojih podatkov dva ali več dni.

3.8. Botneti

Zaradi izredne rasti števila naprav interneta stvari (IoT), je to področje z vidika varnosti postalo resna grožnja. Velik delež naprav je ranljivih, kar je pokazal obsežen DDoS napad, izveden z botnetom Mirai. IoT botneti so postali del izsiljevalskih računalniških črvov. Kriminalci napadajo navidezne strežnike (Virtual Machines) v računalniških oblakih, tako pridobijo nadzor nad njimi ter jih uporabijo za nadaljnje botnet napade. Botneti se uporabljajo pri lažnem oglaševanju, ko napadalci uporabijo omrežja botnetov za kreiranje lažnih računov priljubljenih spletnih strani z namenom napada na uporabnike, ki želijo plačati za oglaševanje.

Kriminalci uporabljajo javno objavljeno kodo znanih botnetov (npr. Mirai) za kreiranje novih botnetov, ki jih potem uspešno uporabijo za pridobitev nadzora nad raznovrstnimi napravami IoT ali drugimi pametnimi napravami.

Največji botneti do sedaj so bili Bredolab, Mariposa, Conficker in Marina Botnet[23].

[22] https://blog.barkly.com/ransomware-statistics-2017, dostop julij 2018

[23] https://themerkle.com/top-4-largest-botnets-to-date/, dostop julij 2018

3.9. Grožnje od znotraj (Insider Threat)

Grožnje od znotraj so opredeljene kot grožnje, ko oseba znotraj organizacije vede ali nevede uporabi svoj dostop (npr. do zaupnih informacij) z namenom, da bi škodila organizaciji.

Grožnje od znotraj že dalj časa predstavljajo veliko tveganje za vlade in organizacije po vsem svetu Kot take so pomembne, saj jih večina organizacij težko razlikuje od nenevarnih dejavnosti. Tudi napredni zunanji nasprotniki želijo zlorabiti osebe z dostopom do notranjih informacij, da bi ogrozili organizacijo. Grožnje od znotraj so lahko namerne ali nenamerne, slednje so tudi najpogostejša oblika notranjih zlorab (npr. v primeru zvabljanja). Glede na to, da organizacije namenjajo večjo pozornost stabilnosti, varnosti in odpornosti svojih sistemov na zunanje vplive, so napadalci osebe z dostopom do notranjih informacij prepoznali kot morebiten dober vektor napada. Obravnavanje groženj od znotraj zato zahteva kombinacijo različnih tehnik in ukrepov za odkrivanje groženj in blažitev njihovih posledic, ki posegajo na tehnično, sociološko in sociološko-tehnično področje.

Grožnje od znotraj naraščajo. Pri tem so izgube, nastale zaradi njih, povečini neznanka. Ker organizacije groženj od znotraj ne morejo finančno ovrednotiti tudi niso njihova prioriteta, kljub temu, da vzbujajo skrb. Največja grožnja organizacijam so osebe z velikimi pooblastili[24], npr. vodilni delavci z dostopom do občutljivih informacij (60 %), sledijo jim pogodbeni izvajalci in svetovalci (57 %) ter redno zaposleni (51 %). V 60 % primerih zaposleni zadržijo podatke v upanju, da se bodo z njimi okoristili v prihodnosti, včasih pa jih posredujejo novemu delodajalcu ali pa jih uporabijo pri zagonu konkurenčnega podjetja (15 %)[25]. Še posebej je na udaru zdravstveni sektor, za katerega se ocenjuje, da je v več kot 59 % primerih zlorab zapisov o pacientih šlo za dejavnost zaposlenih znotraj organizacij[26].

Odkrivanje groženj od znotraj je za odkrivanjem naprednih in neznanih groženj ter za pomanjkanjem varnostnih inženirjev tretji največji izziv za organizacije.

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

Čeprav je ni vedno mogoče šteti med kibernetske grožnje, ima fizična manipulacija/poškodba/ kraja/ izguba še vedno resne posledice za vse vrste digitalnih sredstev. Fizična izguba in kraja, ki so jo v zadnjem času nadomestili hekerski napadi in škodljiva koda, sta bila včasih najpomembnejša vzroka za kršitev podatkov in kot taki ostajata pomembni tudi sedaj[27]. Glede na povečano število naprav IoT in mobilnih naprav ter povečanje obsega storitev v oblaku, bo

[24] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, dostop julij 2018

[25] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, dostop julij 2018

[26] https://post-healthcare.com/31-health-data-breaches-disclosed-in-january-as-hhs-fines-for-late-reporting-d72c533034fa, dostop julij 2018

[27] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, dostop julij 2018

fizično varovanje vedno pomembnejše ter hkrati eden od izzivov na področju kibernetske varnosti.

Fizični napadi prav tako predstavljajo veliko tveganje za kritično infrastrukturo[28]. Fizična nevarnost je trajna in ji bo treba posvetiti več pozornosti tako s strani uporabnikov kot podjetij, še zlasti, ker lahko ukrepi za njeno preprečevanje presežejo učinkovitost vseh drugih varnostnih ukrepov.

3.11. Kršitve podatkov (Data Breaches)

Kršitve podatkov so posledica uspešnih incidentov, ki so privedli do izgube podatkov. Sama zase ni kibernetska grožnja, ampak je skupni izraz za uspešno izvedene kibernetske grožnje. Zato je izogibanje kršitvam podatkov povezano z izvajanjem obrambe, ki zajema celotno področje kibernetskih groženj.

V letu 2017 je pripravljenost na primer kršitev podatkov postala ključni cilj za večino podjetij. Obramba pred kršitvami podatkov mora upoštevati tako že znane kot tudi nove grožnje in pripraviti ustrezne načrte za odzivanje[29].

Do veliko kršitev podatkov prihaja zaradi šibkih, ukradenih in zlorabljenih gesel. Pojavlja se prehod od vohunjenja do kibernetskih napadov, sponzoriranih s strani posameznih držav. Ocenjuje se, da bo večina organizacij, na katere bodo usmerjeni novi, zahtevnejši napadi, iz zdravstvenega sektorja. Spletni kriminalci bodo še naprej prodajali uporabniške poverilnice na temnem spletu. Zaradi ponovne uporabe gesel bodo podjetja izpostavljena tveganju, da postanejo cilj vdorov v njihove sisteme.

V letu 2017 se je število potrjenih uspešnih napadov povečalo za 25 %[30], pri tem pa je bilo več kot 35 % ciljev v sektorju zdravstva in zdravstvene oskrbe[31].

3.12. Kraja identitete (Identity Theft)

Kraja identitete je kibernetska grožnja, katere cilj je pridobiti zaupne informacije, ki se uporabljajo za identifikacijo osebe ali celo računalniškega sistema. Take zaupne informacije so lahko prepoznavna imena, naslovi, kontaktni podatki, poverilnice, finančni podatki, zdravstveni podatki, dnevniki itd. Te informacije se lahko zlorabijo z namenom izdajanja za osebo, ki ji dejansko pripada identiteta. Kraja identitete je poseben primer kršitve podatkov. Je

[28] https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf, dostop julij 2018

[29] https://www.cio.com/article/3155724/security/5-data-breach-predictions-for-2017.html, dostop julij 2018

[30] https://www.riskbasedsecurity.com/2017/07/over-2200-data-breaches-disclosed-so-far-in-2017-exposing-over, dostop julij 2018

[31] https://revisionlegal.com/data-breach/2017-security-breaches/, dostop julij 2018

rezultat uspešnih napadov, povezanih z drugimi kibernetskimi grožnjami, ki so usmerjeni v pridobitev podatkov o identiteti. Kriminalci pridobijo take podatke na različne načine, npr. s hekerskimi napadi, z nakupom na temnem spletu, na družbenih omrežjih, s socialnim inženiringom itd. Vedno več odkritih kraj identitete kaže na resnost grožnje. Poročila[32] kažejo, da se število poskusov zlorabe identitete vsako leto povečujejo in je v letu 2017 doseglo visoko raven. Zaradi pogostih obsežnih kršitev podatkov v kombinaciji z nizkimi cenami informacij o identiteti na črnem trgu je kraja identitete enostavna in cenovno dostopna tudi za tehnološko slabše opremljene kriminalce. Tako npr. podatki o kreditnih karticah stanejo od 10 do 20 dolarjev, drugi podrobni osebni podatki pa so na voljo že za 10 dolarjev[33]. Pri tem veliko ljudi podcenjuje splošno tveganje povezano s krajo identitete in posledično osebno izpostavljenostjo[34].

3.13. Odtekanje informacij (Information leakage)

Ena glavnih groženj na področju kibernetske varnosti v letu 2017 so bila odtekanja informacij različnih vrst, od osebnih podatkov, ki jih zbirajo internetni velikani in spletne storitve, do poslovnih podatkov iz podjetij[35]. Kriminalci napadajo tisto, kar je najdragocenejše za organizacije. Zato bi morale organizacije opredeliti zanje najpomembnejše sisteme in podatke ter jih temu ustrezno zaščititi in nadzorovati. Pri tem so pri odtekanju informacij še vedno najpomembnejši dejavnik zaposleni v organizacijah. Do odtekanja informacij lahko tako pride tudi nenamerno npr. z napačno naslovljeno elektronsko pošto, pošiljanjem zaupnih informacij po nezavarovanih kanalih ali z izgubljenimi napravami. Veliko tveganje lahko predstavljajo tudi administratorji informacijskih sistemov s popolnim dostopom do infrastrukture organizacij, kjer lahko že njihova manjša napaka nehote povzroči katastrofo. Do odtekanja informacij v velikem obsegu prav tako lahko pride zaradi napak v programski kodi mobilnih aplikacij, ki se množično uporabljajo.

Incidenti, povezani z odtekanjem informacij, so vedno pogostejši, večji po obsegu in vedno bolj izpopolnjeni[36].

3.14. Kompleti za izkoriščanje (Exploit Kits)

Kompleti za izkoriščanje vključujejo zbirko že pripravljenih kompletov, ki so običajno nameščeni na okuženih spletiščih ali pa se uporabljajo v kampanjah razširjanja škodljive kode.

[32] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels, dostop julij 2018

[33] https://www.secureworks.com/resources/rp-2017-state-of-cybercrime,. dostop julij 2018

[34] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-theves/? PC = prt_expri_0 & cc = prt_0817_itpraziskava, dostop julij 2018

[35] https://www.bloomberg.com/news/articles/2016-12-21/data-leaks-from-social-networks-threat-in-2017-kasperky, dostop julij 2018

[36] http://thelibrary.solutions/library/newsletters/2017-cyber-attack-trends%20Mid-Year%20Report%20 (EN).pdf, dostop julij 2018

Z uporabo kompletov za izkoriščanje je mogoče prepoznati ranljivosti v spletnih brskalnikih ali spletnih aplikacijah in jih samodejno izkoristiti. Njihova tarča so pogosto dodatki za brskalnike, kot sta Java in Adobe Flash. Čeprav se število kompletov za izkoriščanje zmanjšuje, pa še vedno predstavljajo grožnjo za nezaščitena in nenadgrajena informacijska okolja. V letu 2017 so bili uporabljeni za okužbo svojih ciljev v nekaterih najpomembnejših kampanjah razširjanja škodljive kode. Ker so kompleti za izkoriščanje zanesljivo orodje za dostavo škodljive kode, so pomemben vektor okužbe v primerih napadov z izsiljevalskim programjem. Na temnem spletu so nekateri na voljo za dnevni, tedenski ali mesečni najem[37]. Kompleti za izkoriščanje se v zadnjem času vse bolj uporabljajo v povezavi s socialnim inženiringom, njihova primarna metoda okužbe pa je skrita namestitev na računalnik v mimohodu, ko uporabnik brska po spletu.

3.15. Kibernetsko vohunjenje (Cyber-Espionage)

Globalna podjetja in organizacije so kibernetsko vohunjenje prepoznala kot eno najresnejših groženj v letu 2017, kar je verjetno tudi posledica večjega medijskega pokritja tega področja. Strokovnjaki s področja kibernetske varnosti v prihodnosti pričakujejo porast kibernetskega vohunjenja zaradi geopolitičnih razlogov, ekonomskih sankcij in tudi zaradi strateških ciljev posameznih držav. Akterji na področju kibernetskega vohunjenja, med katerimi je tako organiziran kriminal kot tudi države, razvijajo nove tehnike in orodja za krajo intelektualne lastnine in skrivnosti. Kibernetsko vohunjenje spada med napredne trajne grožnje.

Napredna trajna grožnja *(ang. Advanced Persistent Threat - APT) je izraz, ki se uporablja za niz prikritih in kompleksnih hekerskih procesov, katerih namen je napad na točno določeno informacijsko infrastrukturo. Napadi so usmerjeni tako proti zasebnim organizacijam kot tudi proti vladnim organizacijam, zaradi poslovnih in političnih razlogov. Napadalci želijo čim dlje ostati prikriti v omrežju žrtve. Beseda »napredna« označuje izpopolnjeno tehniko uporabe zlonamerne programske kode, ki izkorišča ranljivosti sistemov. Beseda »trajna« označuje da zunanji nadzorni sistem nenehno spremlja in pridobiva podatke od žrtve napada. Beseda »grožnja« pa predstavlja vključenost človeka v vodenje napada.*

Izraz napredna trajna grožnja se običajno nanaša na skupino, kot je vlada, ki ima zmogljivost in cilj določen subjekt napadati učinkovito in trajno. Izraz se običajno uporablja za sklicevanje na kibernetske grožnje, zlasti kibernetsko vohunjenje s pomočjo različnih obveščevalnih tehnik za dostop do občutljivih podatkov, vendar enako velja tudi za druge grožnje, kot je tradicionalno vohunjenje ali napadi.[38]

Kibernetsko vohunjenje, ki lahko zasleduje namen podtalnega delovanja npr. v obdobju pred in med volitvami, je v zadnjem času postalo zelo pomembno in predstavljajo novo obliko

[37] http://securityaffairs.co/wordpress/62021/malware/disdain-exploit-kit.html,. dostop julij 2018

[38] https://sl.wikipedia.org/wiki/Napredna_trajna_grožnja, dostop avgusta 2018

odmevnih ciljanih napadov. Zasebne organizacije, ki izvajajo občutljive dejavnosti ali podpirajo vladne sisteme, so enako verjetne tarče napada kot javne institucije.

Ena od najpogosteje uporabljanih taktik v tej kategoriji je »zanikanje in prevara« z uporabo lažne identitete za prikrivanje sledi. Pri tem države uporabljajo sredstva za anonimiziranje napadov, zato je določitev dejanskega izvora napada zelo težko. Značilnost državno sponzoriranih hekerjev je njihova predanost in po potrebi velika količina porabljenega časa za dosego določenega cilja.

3.16. Hibridne grožnje

Hibridne grožnje same po sebi ne spadajo med kibernetske grožnje, a so slednje zelo pogosto njihov del skupaj z ostalimi grožnjami. Hibridne grožnje predstavljajo medsebojno povezano, kompleksno in nepredvidljivo visoko integrirano uporabo prikrite ali odkrite kombinacije tradicionalnih in neregularnih vojaških kot tudi nevojaških sredstev (npr. ekonomskih, političnih, propagandnih, kriminalnih...). Enotna definicija hibridnih groženj sicer ne obstaja, vendar pa izraz hibridno v prvi vrsti pomeni predvsem kompleksno kombinacijo groženj.

3.17. Globalni trendi kibernetskih groženj

V letu 2017 so imeli v svetovnem merilu naraščajoč trend spletni napadi, napadi na spletne aplikacije, zvabljanje, nezaželena elektronska pošta, onemogočanje storitve, izsiljevalsko programje, botneti, kršitve podatkov, kraje identitete, odtekanje informacij in kibernetsko vohunjenje.

Škodljiva koda, grožnje od znotraj in fizična manipulacija/poškodba/kraja/izguba so imeli v letu 2017 stabilen trend, medtem, ko je bil trend kompletov za izkoriščanje padajoč.

Preglednica 1: Prikaz globalnih trendov pri posameznih kibernetskih grožnjah v letu 2017
Vir: ENISA, 2018

Kibernetska grožnja	Globalni trend v letu 2017
Škodljiva koda	➡
Spletni napadi	⬆
Napadi na spletne aplikacije	⬆
Zvabljanje	⬆
Nezaželena elektronska pošta	⬆
Onemogočanje storitve	⬆
Izsiljevalsko programje	⬆
Botneti	⬆
Grožnje od znotraj	➡
Fizična manipulacija/ poškodba/kraja/izguba	➡
Kršitve podatkov	⬆
Kraja identitete	⬆
Odtekanje informacij	⬆
Kompleti za izkoriščanje	⬇
Kibernetsko vohunjenje	⬆

4. Akterji kibernetskih groženj

Razvoj na področju akterjev kibernetskih groženj je napredoval podobno kot je napredoval razvoj samih kibernetskih groženj. Opazno je povečanje kompleksnosti, izpopolnjenosti in napredka v razvoju zmogljivosti pri večini skupin akterjev. Zaradi uporabe lažnih identitet in prikritega delovanja je vedno težje prepoznati posamezne akterje kibernetskih groženj. Uporabniki prav tako vedno težje ločijo med dobrimi in slabimi akterji, kar vodi k zmanjševanju zaupanja ne samo do komercialnih ponudnikov storitev, ampak celo do institucionalnih akterjev v kibernetskem prostoru.

4.1. Kibernetski kriminalci

V letu 2017 so bili kibernetski kriminalci še vedno najdejavnejša skupina akterjev kibernetskih groženj, saj so bili odgovorni za najmanj dve tretjini evidentiranih incidentov[39]. Usmerili so se

[39] http://www.hackmageddon.com/, dostop julij 2018

v monetizacijo svojih aktivnosti, saj so se osredotočili na ozko usmerjene napade z izsiljevalskim programjem na žrtve z visokim potencialom za plačilo odkupnin. Namesto obsežnih napadov na velike skupine uporabnikov s škodljivimi orodji nizke zahtevnosti, so se usmerili na potencialno visoko donosne cilje, katerim so prilagodili svoje napade. Posledično to pomeni, da so se žrtve njihovih napadov skoncentrirale v poslovnem sektorju.

Kljub naraščajočemu trendu izsiljevalskega programja v letu 2017, so kibernetski kriminalci uporabljali tudi bolj „tradicionalne“ oblike goljufij. Pomemben vir dohodka kibernetskih kriminalcev je povezan s storitvami, ki se prodajajo pod nazivom »Crime as a Service« in ki temeljijo na kršitvah podatkov.Trajno povečanje števila kršitev podatkov je jasen pokazatelj velikega interesa kriminalcev za okoriščanje z ukradenimi podatki. S tem v zvezi se je domnevno povečala tudi intenzivnost sodelovanja med kibernetskimi kriminalci in kibernetskimi vohuni[40].

4.2. Osebe znotraj

Grožnje od znotraj in z njimi povezan akter osebe znotraj so prepoznani kot pomemben dejavnik na področju kibernetskih groženj. Tako kot kibernetski kriminalci tudi osebe znotraj zasledujejo predvsem finančno pridobitne cilje s tem, da neposredno in/ali posredno prodajajo svoje storitve na črnem trgu. Akterjem kibernetskih groženj osebe znotraj, tako namernim kot nenamernim, pripada levji delež incidentov v finančnem (58 %) in zdravstvenem (71 %) sektorju[41]. V primeru oseb znotraj, ki so nenamerni akterji, običajno gre za zlorabo njihovih dostopov ali okužbe njihovih računalnikov, ki so dejansko pod nadzorom drugih akterjev groženj. Vzrok, da lahko pride do tega, so lahko dolga neprekinjena obdobja, ko so uporabniki prijavljeni v svoje račune, pošiljanje podatkov iz službenih na zasebne račune, shranjevanje podatkov na nosilce izven organizacije in dostopnost (npr. zaradi nepazljivosti) njihovih gesel.

4.3. Države

Z deležem več kot 20 % priglašenih incidentov so bile države tretja največja skupina akterjev kibernetskih groženj v letu 2017. Glede na napredne zmogljivosti te skupine, je njihove napade pogosto težko identificirati in se jim zoperstaviti. Zelo verjetno je, da je dejansko število njihovih napadov veliko večje. Dejstvo, da vedno več držav razvija kibernetske zmogljivosti prispeva k večji dejavnosti celotne skupine. Glavna cilja državno sponzoriranih kibernetskih aktivnosti so proizvodne zmogljivosti in javne uprave drugih držav, kar odraža njihov velik interes za industrijsko vohunjenje in državne skrivnosti. Take države veliko vlagajo v razvoj svojih napadalnih kibernetskih orožij, istočasno pa uporabljajo inovativne pristope tako za napade kot tudi obrambo pred njimi. Zaradi uporabe naprednih tehnik napada, uporabe t.i. zero-day

[40] https://www.theregister.co.uk/2017/10/05/fog_of_cyberwar/, dostop julij 2018

[41] https://www.ibm.com/security/data-breach/threat-intelligence, dostop julij 2018

ranljivosti in močne tehnične in finančne podpore, so države najbolj strah vzbujajoč akter kibernetskih groženj.

Zero-day ranljivost *je ranljivost programske ali strojne opreme, ki še ni bila javno odkrita oziroma objavljena in zato zanjo tudi ne obstaja popravek ali rešitev. Žrtev se je ne zaveda, zato je vse do razkritja na voljo napadalcu.*

4.4. Hektivisti

Hektivisti spadajo med pet najpomembnejših akterjev kibernetskih groženj. Spodbujeni z nekaterimi političnimi dogodki, so odgovorni za razobličenja spletnih strani ter kampanje kraj in kršitev podatkov prvenstveno usmerjenih proti vladam ter organizacijam in podjetjem v javnem sektorju. V to skupino spadajo posamezniki z različnim nivojem sposobnosti za izvajanje kibernetskih napadov. Skupina je predvsem aktivna na področju razobličenja spletnih strani, širjenja propagande in medijsko odmevnih DDoS napadih. Predvideva se, da ti akterji kibernetskih groženj za svoje napade uporabljajo razpoložljive storitve kibernetskega kriminala (Cyber Crime as a Service – CCaaS). Za svoje napade imajo običajno politične motive, ki lahko pritegnejo tudi druge akterje kibernetskih groženj, predvsem države, ki hektiviste pogosto uporabijo kot krinko za svoje kibernetske napade.

4.5. Kibernetski bojevniki

Kibernetski bojevniki ostajajo na prizorišču akterjev kibernetskih groženj kot nacionalno ali versko motivirane skupine. Glede na razvoj dogodkov v Siriji in begunsko krizo, je možno, da radikalizirani posamezniki povzročijo napetosti v etničnih skupnostih. To pa lahko posledično pripelje tudi do zlonamernih aktivnosti v kibernetskem prostoru. Aktivnosti te skupine akterjev kibernetskih groženj zajemajo vse od razobličenj spletnih strani in napadov DDoS do bolj naprednih kibernetskih napadov, podobnih aktivnostim držav. Značilna skupina kibernetskih borcev z vladno podporo je Iranska kibernetska vojska, ki ima zelo dolgo dejavnost v kibernetskem prostoru[42].

4.6. Kibernetski teroristi

Kibernetski teroristi se podobno kot hektivisti poslužujejo aktivnosti, povezanih z razobličenjem spletnih strani in napadi DDoS, ki pa so lahko usmerjene proti kritični infrastrukturi. Predvideva se, da se zanimajo za razvoj zmogljivosti na področju kriptovalut, predvsem z namenom skrivanja svojih virov pred mednarodnim finančnim nadzorom in za pranje denarja. Prav tako se lahko zanimajo za nakup storitev kibernetskega kriminala, orožja in drog na črnem trgu.

[42] https://thebuckleyclub.com/the-rising-iranian-cyber-threat-15028b76e0f9, dostop julij 2018

Grožnja kibernetskega terorizma lahko izvira tudi od drugih skupin akterjev kibernetskih groženj, npr. tistih, povezanih s političnim ekstremizmom.

4.7. Script kiddies

Skupina akterjev kibernetskih groženj, poimenovana »Script kiddies«, obsega akterje z nizko stopnjo zmogljivosti za izvajanje kibernetskih groženj in z nizko motiviranostjo za napade. Tukaj gre predvsem za populacijo najstnikov. Njihove aktivnosti imajo običajno majhen vpliv, vendar lahko v določenih okoliščinah in v povezavi z drugimi skupinami akterjev kibernetskih groženj prerastejo v resne kibernetske napade.

4.8. Akterji kibernetskih groženj in glavne grožnje

V preglednici 2 so prikazane kibernetske grožnje in njihovi akterji. Pri tem so za različne grožnje nekatere skupine akterjev primarne (označeno z rdečo), druge pa sekundarne (označeno z zeleno). Skupine akterjev, ki so primarne za večje število kibernetskih groženj imajo višje razvite zmogljivosti za njihovo izvedbo in obratno.

Preglednica 2: Prikaz kibernetskih groženj in njihovih akterjev. Vir: ENISA, 2018

	Akterji kibernetskih groženj						
Kibernetska grožnja	Kibernetski kriminalci	Osebe znotraj	Države	Hektivisti	Kibernetski bojevniki	Kibernetski teroristi	Script kiddies
Škodljiva koda							
Spletni napadi							
Napadi na spletne aplikacije							
Onemogočanje storitve							
Botneti							
Zvabljanje							
Neželena elektronska pošta							
Izsiljevalsko programje							
Grožnje od znotraj							
Fizična manipulacija/ poškodba/kraja/izguba							
Kompleti za izkoriščanje							
Kršitve podatkov							
Kraja identitete							
Odtekanje informacij							
Kibernetsko vohunjenje							

Legenda	Primarna skupina za grožnje	Sekundarna skupina za grožnje

5. Vektorji napada

Razširjanje različnih kibernetskih groženj se izvaja z uporabo enega ali več vektorjev napada. Vektor napada je sredstvo, s katerim lahko akter kibernetske grožnje zlorabi slabost ali ranljivost na napadenih sredstvih (vključno z ljudmi), da doseže določen cilj.

Poznavanje vektorjev napada je pomembno za razumevanje delovanja različnih kibernetskih groženj, tehnik, taktik in postopkov ter za učinkovito obrambo pred njimi.

5.1. Taksonomija vektorjev napada

Spodaj je prikazana razvrstitev vektorjev napada:

1. Napad na človeški element,
   - Socialni inženiring,
   - Zvabljanje / usmerjeno zvabljanje / zloraba poslovne e-pošte / zvabljanje visoko pozicioniranih uslužbencev / neželena e-sporočila preko elektronske pošte, družbenih medijev, spletnih storitev,
     - Zlonamerne priponke e-sporočil,
     - Naslovi zlonamernih spletnih strani, e-pošte in družbenih medijev,
     - Vektorji napada skozi programe Microsoft Office (makro ukazi itd.),
   - Prevare,
     - Prevare na področju tehnične ali uporabniške podpore,
     - Telefonske prevare,
     - SMS prevare,
   - Zbiranje informacij na internetu in v družbenih medijih,
2. Vektorji napada, ki temeljijo na spletu in brskalnikih,
   - Prenosi v mimohodu,
   - Rudarjenje v mimohodu (cryptojacking),
   - Zlonamerne skripte/spletni naslovi,
   - Kompleti za izkoriščanje,
   - Oglaševanje škodljive kode,
   - Napadi na spletne aplikacije (SQL vrivanje),
   - Napadi, ki temeljijo na brskalnikih,
     - Zlonamerni dodatki za brskalnike (posodobitve),
   - Zlorabljene/lažne spletne strani,
3. Sredstva, izpostavljena na internetu,
   - Nezaščitena sredstva, izpostavljena na internetu,
   - Privzete/šibke poverilnice za storitve,
   - Ponovna uporaba gesel,
4. Izkoriščanje ranljivosti/napačnih nastavitev in napak kriptografskih, omrežnih, varnostnih protokolov,
5. Napadi v dobavni verigi,
6. Razširjanje po omrežju,
7. Aktivni omrežni napadi,
   - DNS napadi (DNS ugrabitev / zastrupitev),
8. Pasivni omrežni napadi,
   - Vohljanje v brezžičnem omrežju (WiFi-Sniffing),
9. Odtekanje podatkov,
10. Napadi z zavajanjem (smokescreen attacks),

11. Trgovine za mobilne aplikacije,
12. Zlonamerne USB naprave,
13. Snemanje kartic.

6. Kibernetska varnost v Sloveniji

Področju kibernetske in širše tudi informacijske varnosti se v Sloveniji dolgo časa ni in se mu še vedno ne posveča ustrezne pozornosti. Kljub temu pa je država v zadnjih letih vendarle storila nekatere korake, ki kažejo na razvoj v pravi smeri.

6.1. Pravna in organizacijska ureditev

Prvi korak k sistemski ureditvi področja je bil storjen leta 2016, ko je Vlada RS sprejela Strategijo kibernetske varnosti, ki predstavlja okvir za pripravo in izvedbo ukrepov na področju zagotavljanja kibernetske varnosti. Temu je aprila 2017 sledila dopolnitev Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov (UVTP), s katero so bile določene strokovne naloge in organizacija UVTP na področju kibernetske varnosti. UVTP je s tem postal pristojni organ na strateški ravni nacionalnega sistema informacijske varnosti.

Na operativni ravni sistema so bile že dotlej zmogljivosti za odzivanje na incidente v kibernetskem prostoru porazdeljene med SI-CERT kot nacionalnim odzivnim centrom za omrežne incidente (nacionalni CSIRT), Sektorjem za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno upravo (MJU) kot bodočim CSIRT organov državne uprave, Ministrstvom za obrambo kot odgovornim za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Slovensko obveščevalno-varnostno agencijo (SOVA), ki deluje na področju protiobveščevalnega delovanja ter Policijo, v okviru katere delujeta Urad za informatiko in telekomunikacije in Center za računalniško preiskovanje v Upravi kriminalistične policije z zmogljivostmi za zatiranje kibernetskega kriminala.

Pred Slovenijo sta bila izziva sistemske ureditve področja informacijske varnosti ter prenos Direktive 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (Direktiva NIS) v nacionalni pravni red. Ker sta bila izziva povezana, je država k njunemu reševanju pristopila s pripravo Zakona o informacijski varnosti (ZInfV), ki bi v nacionalni pravni red prenesel omenjeno direktivo, istočasno pa bi bil tudi podlaga za vzpostavitev celovitega nacionalnega sistema informacijske varnosti, ki se bo sposoben odzivati na naraščajoči trend kibernetskih incidentov. Ker je bil v času priprave predloga zakona v Državnem zboru RS sprejet Zakon o kritični infrastrukturi, je bila potrebna tudi uskladitev s tem zakonom. Posledica je bila, da sta se naboru osnovnih sedmih sektorjev (energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga), v katerih po Direktivi NIS delujejo izvajalci bistvenih storitev, pridružila dva dodatna sektorja, in sicer preskrba s hrano in varstvo okolja. Izvajalci bistvenih storitev v teh sektorjih bodo določeni na

podlagi meril in metodologije iz podzakonskih aktov, ki je v času nastajanja te ocene še v pripravi, poleg teh pa bo vlada kot izvajalce bistvenih storitev določila tudi tiste upravljavce kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo področje kritične infrastrukture, ter nosilce obrambnega načrtovanja, ki so določeni v skladu s predpisi, ki urejajo področje obrambe in katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov.

***Direktiva NIS**, ki je bila sprejeta 6. 7. 2016, želi zagotoviti krepitev obrambnih kibernetskih zmogljivosti na nacionalni ravni držav članic, krepitev kibernetske varnosti EU z mednarodnim sodelovanjem in uvedbo obveznega upravljanja s tveganji ter poročanja o incidentih za izvajalce bistvenih storitev in ponudnike digitalnih storitev. Države članice morajo določiti enega ali več pristojnih nacionalnih organov za varnost omrežij in informacijskih sistemov, ki spremljajo uporabo direktive na nacionalni ravni. Poleg tega morajo določiti enotno kontaktno točko za komunikacijo in sodelovanje z relevantnimi organi v drugih državah članicah ter enega ali več nacionalnih odzivnih centrov CSIRT (angl. Computer security incident response team), ki so odgovorni za nadzor in spremljanje incidentov na nacionalni ravni, zagotavljanje zgodnjega odkrivanja, vzpostavitev učinkovitega sistema obveščanja ter razširjanje informacij o tveganjih in incidentih med ključnimi skupinami, odziv na incidente, oceno možnosti incidentov ter stopnje ozaveščenosti o kibernetski izpostavljenosti in sodelovanje v mreži nacionalnih odzivnih centrov CSIRT. Vsaka država članica mora določiti svoje izvajalce bistvenih storitev. Osnovna merila za določitev so, da je subjekt izvajalec storitev, ki so ključnega pomena za vzdrževanje in nemoteno delovanje gospodarskih in družbenih dejavnosti, da je nemoteno delovanje storitev izvajalca odvisno od delovanja omrežja in informacijskih sistemov ter da bi varnostni incident prekinil ali resno okrnil delovanje storitev, ki jih izvajalec zagotavlja. Pri določanju stopnje resnosti incidenta se upošteva, kakšno je število prizadetih uporabnikov, trajanje incidenta in geografska razširjenost oziroma doseg incidenta. Poleg izvajalcev bistvenih storitev Direktiva NIS določa tudi ponudnike digitalnih storitev, in sicer so to spletne tržnice, storitve računalništva v oblaku ter spletni iskalniki.*

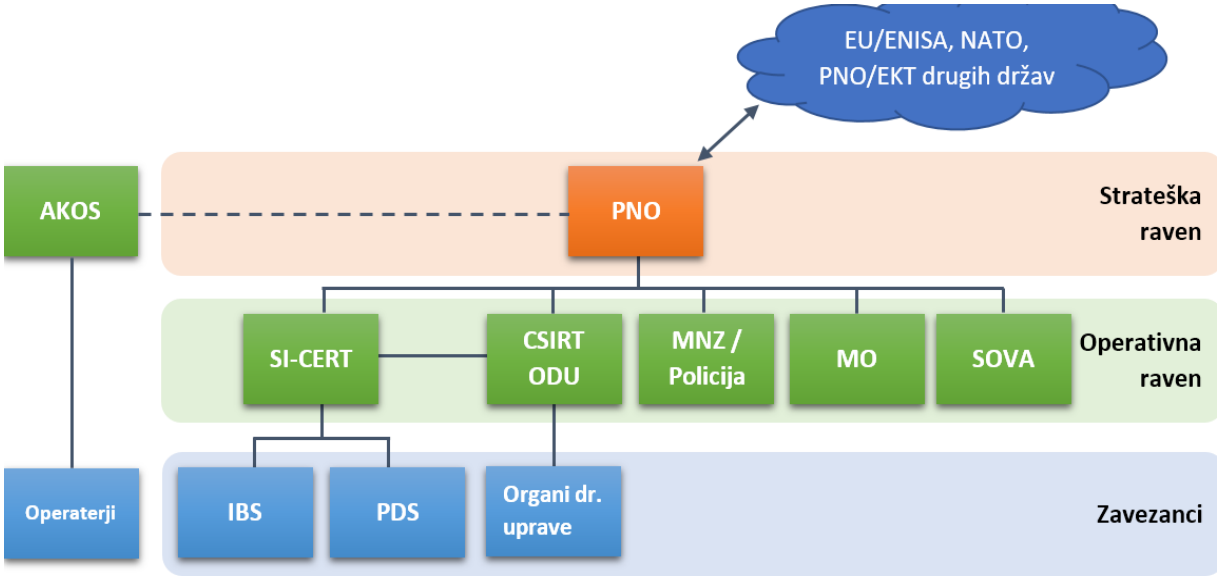
Prav tako so bili med potencialne zavezance po ZInfV poleg izvajalcev bistvenih storitev iz zgoraj omenjenih sektorjev in ponudnikov digitalnih storitev, vključeni še organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v ZInfV poimenovani organi državne uprave).

Pri tem za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (operaterji), veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz VII. poglavja (Varnost omrežij in storitev ter delovanje v izjemnih stanjih) Zakona o elektronskih komunikacijah (ZEKom-1), kjer gre za prenos 13.a in 13.b člena Direktive 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva). Operaterji morajo namreč sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, zlasti zaradi

preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, ki je primerna predvidenemu tveganju. Določene so tudi obveznosti obveščanja in poročanja o kršitvah varnosti ali celovitosti AKOS[43], ki potem po potrebi poroča UVTP. Iz tega razloga Direktiva NIS v tretjem odstavku 1. člena operaterje izključuje iz svojega dometa, temu pa sledi tudi ZInfV. Določbe ZInfV se prav tako ne uporabljajo za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 (t. i. Uredba eIDAS), ki jih Direktiva NIS v tretjem odstavku 1. člena prav tako izključuje.

Z ZInfV se vzpostavlja pristojni nacionalni organ za informacijsko varnost na strateški ravni sistema, katerega naloge bo do vzpostavitve Uprave za informacijsko varnost opravljal UVTP. Le-ta bo tudi enotna kontaktna točka države na področju informacijske varnosti. Zakon podrobneje ureja tudi delovanje organov na operativni ravni sistema, in sicer nacionalnega CSIRT (SI-CERT) in CSIRT organov državne uprave. Prvi bo tako kot do sedaj skrbel za informacijsko varnost na nacionalni ravni, drugi pa za informacijsko varnost v omrežjih in informacijskih sistemih državnih organov, razen pri organih, ki že posedujejo lastne zmogljivosti vsaj na ravni varnostno-operativnih centrov (npr. Ministrstvo za obrambo, Ministrstvo za notranje zadeve, SOVA). Poleg tega zakon opredeljuje tudi medsebojne odnose in način sodelovanja med pristojnim nacionalnim organom, obema CSIRT in ostalimi deležniki v sistemu informacijske varnosti.

Slika 1: Shema nacionalnega sistema zagotavljanja informacijske varnosti



Legenda:	MNZ/Policija – Ministrstvo za notranje zadeve/Policija
PNO – Pristojni nacionalni organ za informacijsko varnost	MO – Ministrstvo za obrambo
EKT – Enotna kontaktna točka	SOVA – Slovenska obveščevalno-varnostna agencija
SI-CERT – Nacionalni CSIRT	IBS – Izvajalci bistvenih storitev
CSIRT ODU – CSIRT organov državne uprave	PDS – Ponudniki digitalnih storitev

[43] Agencija za komunikacijska omrežja in storitve Republike Slovenije

6.2. Stanje na področju kibernetskih groženj

Stanje na področju kibernetskih groženj že od leta 1995 spremlja SI-CERT (Slovenian Computer Emergency Response Team), ki je nacionalni odzivni center za kibernetsko varnost. SI-CERT opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah v elektronskih omrežjih. Slovenija se k sreči še ni srečala z obsežnejšimi kibernetskimi napadi, razen napada skupine Anonimni (Anonymous) leta 2012, ki ni imel večjih posledic, in napada z izsiljevalskim virusom WannaCry leta 2017, ki pa je povzročil kar nekaj finančne škode.

Naslednja preglednica prikazuje pregled obravnavanih kibernetskih incidentov (groženj) v obdobju od 2008 do 2017.

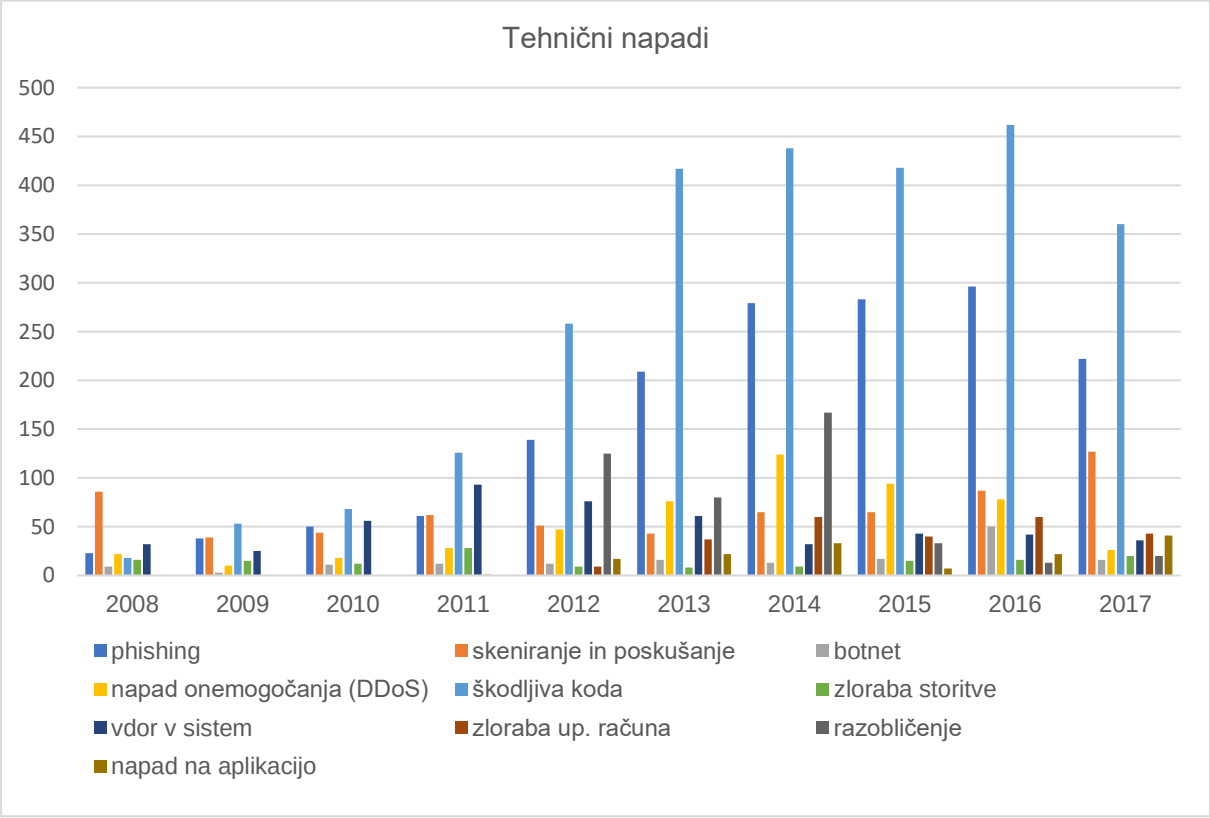
Preglednica 3: Pregled obravnavanih incidentov na SI-CERT v obdobju od 2008 do 2017

Vrsta incidenta	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Zvabljanje	23	38	50	61	139	209	279	283	296	222
Skeniranje in poskušanje	86	39	44	62	51	43	65	65	87	127
Botnet	9	3	11	12	12	16	13	17	50	16
Napad onemogočanja storitve (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 uporab. 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 skupaj	206	183	259	411	743	969	1220	1015	1126	911
Kraja identitete			10	52	67	56	77	70	103	106
Nigerijska prevara							38	26	73	119
Spletno nakupovanje							68	88	183	258
Druge goljufije	5	24	26	89	161	210	309	322	354	492
Neželena e-pošta	21	22	36	25	74	50	63	112	140	80
Dialler					1		3		1	3
Goljufije in prevare skupaj	26	46	72	166	303	316	558	618	854	1058
Skupaj	232	229	331	577	1046	1285	1778	1633	1980	1969

***Nigerijska prevara**, znana tudi kot prevara 419 oziroma prevara z vnaprejšnjim plačilom stroškov, je ena izmed mnogih tipov spletnih prevar oziroma goljufij, pri kateri želi goljuf navezati stik z žrtvijo preko e-sporočil, faksa ali telefona. Ko mu to uspe, si prizadeva pridobiti žrtvino zaupanje in jo prosi za denar. Prevara se najpogosteje začne tako, da goljuf razpošlje množično sporočilo preko elektronske pošte, v katerem se običajno predstavi kot premožen poslovnež oziroma predstavnik vlade, pove, od kod prihaja (običajno iz Nigerije) in opiše svojo težavo. Goljuf želi osebne podatke žrtve ter bančni račun, ker želi prenesti veliko vsoto denarja iz svoje države v tujino, za pomoč pa ponudi visoko nagrado. Če se prejemnik odzove, mu odgovori, da je potrebno pred tem poravnati stroške odprtja računa in nekatere druge stroške, pri čemer so ti stroški zanemarljivi v primerjavi z obljubljeno nagrado. Zahteva nakazilo preko plačilnega sistema Western Union, ki je neizsledljivo. Po izvedenem nakazilu goljuf prekine komunikacijo z žrtvijo.*[44]

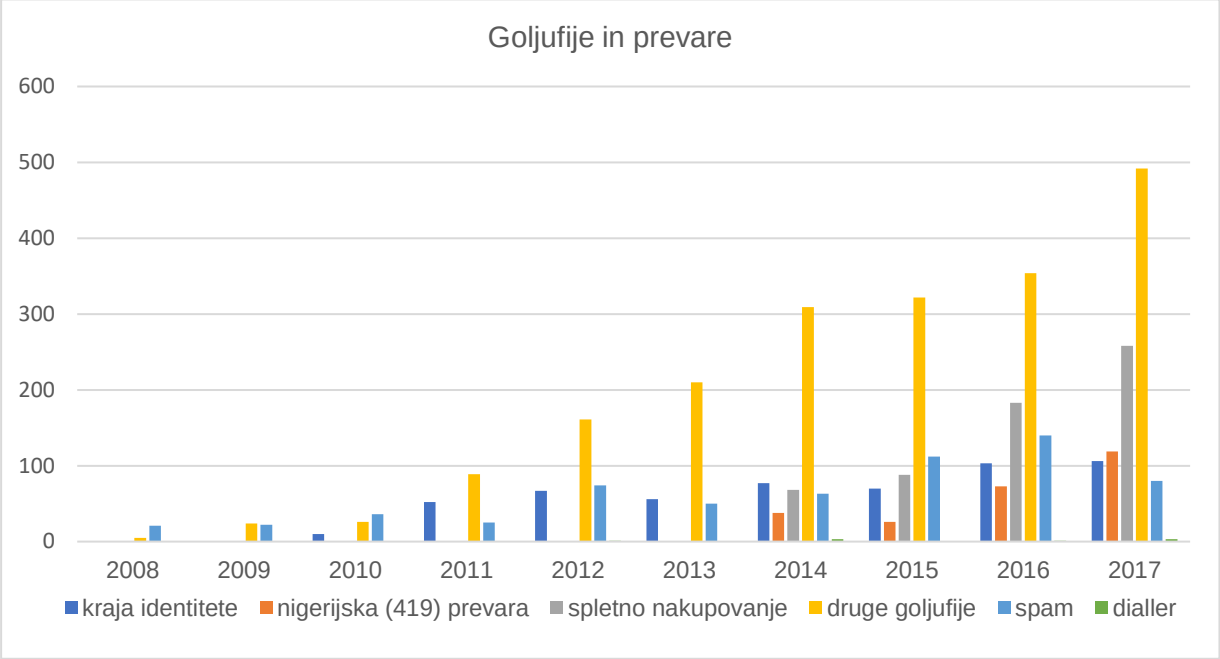
Slike v nadaljevanju prikazujejo gibanje incidentov iz skupin tehnični napadi ter goljufije in prevare v obdobju od 2008 do 2017 ter gibanje mesečnih prijav izsiljevalskih virusov v obdobju od aprila 2012 do januarja 2018.

Slika 2: Prikaz incidentov iz skupine tehničnih napadov v obdobju od 2008 do 2017.
Vir: SI-CERT, 2018



[44] Wikipedia, https://sl.wikipedia.org/wiki/Nigerijska_prevara, dostop julij 2018

Slika 3: Prikaz incidentov iz skupine goljufije in prevare v obdobju od 2008 do 2017. Vir: SI-CERT, 2018



7. Scenariji kibernetskih tveganj

Scenariji tveganja za nesrečo oziroma v našem primeru uresničitev določene grožnje spadajo pri vsaki oceni tveganja med ključne vsebine. So namreč podlaga za pripravo najpomembnejšega dela vsake ocene tveganja, to je analiz tveganja, s katerimi se skušajo oceniti oziroma ugotoviti stvarne posledice nekega dogodka. Za pripravo te ocene so bili namerno izbrani scenariji tveganja, ki predstavljajo tri primere, kjer kibernetske grožnje realizirajo različni akterji. V vseh treh primerih gre za onemogočenje poslovanja oziroma izvajanja storitev. V prvem scenariju gre za napad na spletišča državne uprave (v resničnem primeru ga je izvedla hektivistična skupina), v drugem za napad z izsiljevalskim programjem (v resničnem primeru so ga izvedli kibernetski kriminalci) in v tretjem za napad na kritično infrastrukturo v energetskem sektorju (v resničnem primeru ga je izvedla suverena država). Stopnja tveganja, negativni vplivi in resnost posledic v uporabljenih scenarijih so različne. Pri tem se omejujemo na osnovne scenarije brez dodatne kompleksnosti, ki jo prinese vzajemno delovanje več različnih kibernetskih groženj ali njihovih akterjev ter samo na neposredne vplive in posledice realiziranih groženj. V nasprotnem primeru bi bili negativni vplivi in posledice neprimerno večji. Vsi trije scenariji temeljijo na dejanskih incidentih, od katerih se je prvi zgodil v Sloveniji, drugi je imel svetovne razsežnosti, vključno s Slovenijo, tretji pa v Ukrajini. Ocene vplivov vseh treh scenarijev se nanašajo na Republiko Slovenijo.

7.1. Scenarij tveganja 1: Napad na spletišča državne uprave

Slovenija je konec januarja 2012 v Tokiu skupaj z 21 drugimi članicami EU podpisala sporazum ACTA (Anti-Counterfitting Trade Agreement). Podpisu je sledila javna napoved napadov hektivistične skupine Anonimni in ultimat Vladi RS, naj zamrzne ali umakne podpis s sporazuma. Od 4. do 17. februarja se je zvrstilo več distribuiranih napadov onemogočanja storitve (DDoS), poskusi vdora v sisteme javne uprave ter nekaj razobličenj spletnih mest. Za krajši čas so bili z DDoS napadi onemogočeni strežniki Nove Ljubljanske banke, spletna mesta nekaterih slovenskih političnih strank in portala predlagaj.vladi.si. Trajne škode v teh napadih ni bilo, DDoS napadi na državno infrastrukturo pa niso imeli nobenega učinka. Objavljena je bila datoteka imen državnih uradnikov, nekaterih internih IP naslovov v HKOM[45] omrežju in seznam preklicanih certifikatov iz leta 2006. Slednje se je v nekaterih medijih napačno prikazalo kot vdor v sistem za dodeljevanje certifikatov (digitalnih potrdil), šlo pa je le za nekaj let staro datoteko na pozabljenem strežniku, ki pa nikakor ni omogočala dostopa do sistemov javne uprave. Skupina Anonimni je identificirala nekaj pomanjkljivosti spletnih aplikacij na javno dostopnih strežnikih državnih ustanov, ki so omogočali izrabe XSS (cross-site scripting). Prek njih je skupina lahko na primer na vladnem spletnem iskalniku med rezultati prikazala svoje grafične znake in sporočila. Tovrstni napad sicer ne pomeni vdora v sistem, a takšno »grafitiranje« je vzbudilo zanimanje medijev.

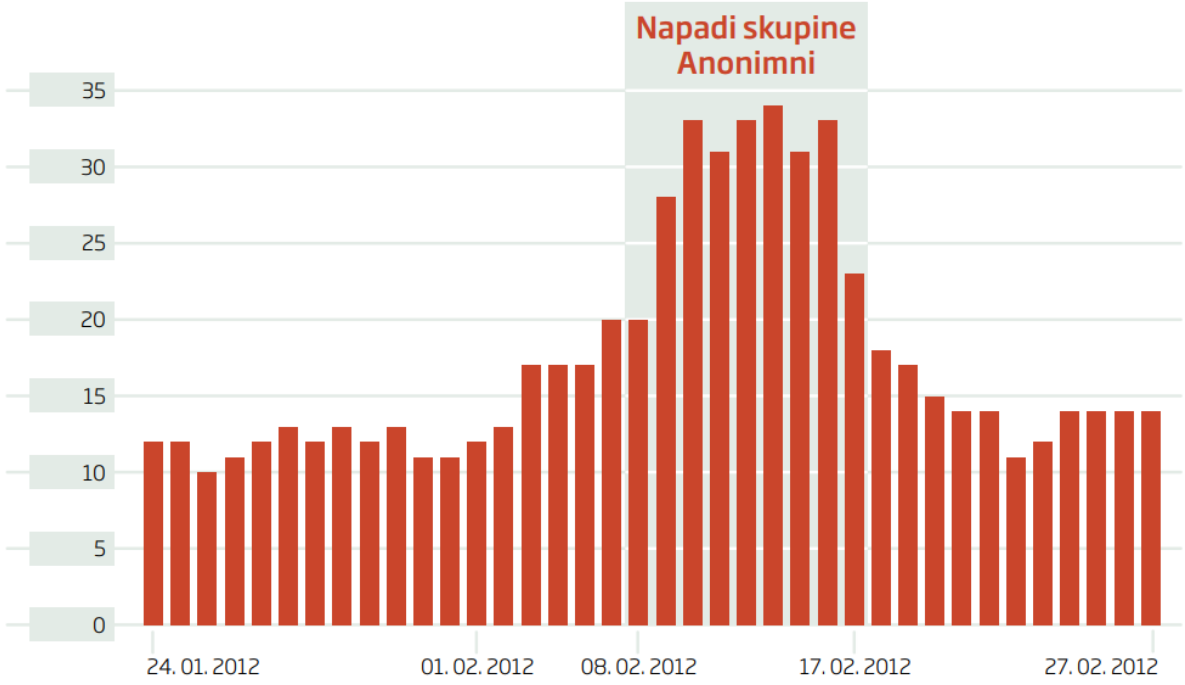
ACTA *(Anti-Counterfeiting Trade Agreement) oziroma trgovinski sporazum za boj proti ponarejanju je dogovor za oblikovanje novih standardov zaščite globalne intelektualne lastnine, ki je razprave iz bolj demokratičnih večstranskih forumov, kot sta Svetovna trgovinska organizacija WTO in Svetovna organizacija za intelektualno lastnino WIPO, spremenil v skrivna regionalna pogajanja. ACTA je želela omogočiti večjo avtoriteto organom pregona, ki naj bi zasegli vso blago, ki je povezano s kriminalno aktivnostjo, kršitvami zakona, izogibanjem digitalnim varnostnim tehnologijam in piratstvom na digitalnih omrežjih. ACTA je nastajala od leta 2007 do 2010 s pogovori med ZDA, EU, Švico, Kanado, Avstralijo, Novo Zelandijo, Mehiko, Singapurjem, Marokom, Japonsko in Južno Korejo.*[46]

Ker napadi na državne ustanove niso uspeli, je skupina iskala druge cilje. Napad z razobličenjem spletnega mesta Zveze potrošnikov Slovenije 12. februarja je pomenil velik preobrat v kampanji skupine Anonimni, saj je napad negativno vplival na podobo skupine v javnosti, intenzivnost napadov pa se je v naslednjih dneh bistveno zmanjšala. Čeprav napadi resnejših posledic za sisteme državnih ustanov niso imeli, pa so pritegnili izredno veliko zanimanje medijev. Hektivistična skupina je dosegla, da je bilo moč vsak dan brati o sporazumu ACTA in povezanih napadih. V javnosti je prišlo do diskusije na temo omrežnega aktivizma in pravice do spletnih protestov.

[45] Skupno komunikacijsko omrežje organov in organizacij državne uprave

[46] Wikipedia, https://sl.wikipedia.org/wiki/ACTA, dostop avgusta 2018

Slika 4: Prikaz napadov skupine Anonimni v Sloveniji januarja in februarja 2012. Vir: SI-CERT, 2018



Anonimni *so mednarodna hektivistična skupina brez jasne organizacijske strukture, ki je postala znana zaradi DDoS napadov na vladne, verske in druge spletne strani. Že od začetka svojega delovanja leta 2003 so odgovorni za mnoge potegavščine, napade, proteste in javna obrekovanja. Pripadniki skupine so iz celega sveta, njihova ideja in način delovanja pa ostajata enaka – doseči nek cilj, običajno politično motiviran brez razkrivanja svoje identitete. V povezavi z delovanjem skupine se velikokrat pojavljajo stavčne zveze »We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.«.*[47]

[47] Wikipedia, https://sl.wikipedia.org/wiki/Anonymous, dostop avgusta 2018

7.2. Scenarij tveganja 2: Napad z izsiljevalskim programjem

WannaCry (WannaCrypt) je bil izsiljevalski kripto virus, ki je maja leta 2017 povzročil enega največjih kibernetskih napadov na svetovnem spletu. Izkoristil je varnostne ranljivosti in pomanjkljivosti neposodobljenih operacijskih sistemov ter napadel računalnike z nameščenimi operacijskimi sistemi Microsoft Windows XP, Vista, 7, 8 in 10. Uporabnikom je zašifriral shranjene datoteke, za njihovo povračilo pa je zahteval plačilo odkupnine. Na tak način je prizadel okoli 300.000 računalnikov, med njimi tudi mnogo pomembnih za infrastrukturo kot so električne postaje, transportna vozlišča, nacionalni in mednarodni bančni sistemi, globalna proizvodna omrežja in logistični centri. Virus je deloval tako, da je ob okužbi računalnika naredil kopije vseh datotek na trdem disku in izbrisal originalne datoteke. Kopije je zakodiral, tako da je bil dostop možen samo s ključem za dešifriranje. Uporabniki zato do datotek niso imeli dostopa. V najhujšem primeru jim je bil celo onemogočen dostop do računalnika. Uporabniki so lahko do svojih podatkov prišli le, če so imeli varnostno kopijo. V nasprotnem primeru so za dostop do podatkov morali plačati odkupnino v vrednosti 300 dolarjev v kripto valuti Bitcoin, virus pa je po treh dneh zahtevani znesek podvojil. Če zneska žrtve niso poravnale v enem tednu, je virus izbrisal podatke. Plačilo odškodnine sicer ni bilo zagotovilo, da bodo žrtvam povrnjeni izgubljeni podatki.

Slika 5: Obvestilo izsiljevalskega virusa WannaCry o odkupnini

Virus WannaCry je uporabljal kibernetska orodja, ki so izkoriščala ranljivost operacijskih sistemov Microsoft Windows. Orodja je razvila ameriška varnostna agencija NSA za namene državne varnosti, njej pa jih je ukradla skupina Shadow Brokers. Le-ta je orodja dalj časa

skušala prodati na črnem trgu, na koncu pa jih je javno objavila. Po nekaterih podatkih naj bi potem orodja uporabila in virus razvila znana hekerska skupina Lazarus, ki jo povezujejo s Severno Korejo, a uradno storilci oziroma razvijalci niso znani.

WannaCry se je razširil v več kot 150 držav po celem svetu. Največ škode je povzročil v Rusiji, Ukrajini, ZDA, Indiji, na Kitajskem, Tajvanu in v Braziliji. Čeprav je bilo na Bitcoin račune nakazano samo okoli 150.000 dolarjev odkupnine, pa se ocenjuje, da je celotna škoda kibernetskega napada znašala okoli pol milijarde dolarjev[48]. Napad je prizadel posameznike, še posebej nevaren pa je bil za večje organizacije, npr. letališča, banke, univerze, bolnišnice in druge vladne ter nevladne službe. Med žrtvami so bile na primer organizacije v britanskem zdravstvenem sistemu UK's National Health Service, nemške železnice Deutsche Bahn, špansko telekomunikacijsko podjetje Telefónica, ruski mobilni operater Megafon, logistično podjetje FedEx, proizvodni podjetji Hitachi in Renault, pri nas pa preko njega tudi Revoz. Škoda, ki jo je povzročil virus je imela zelo velike posledice, še posebej v zdravstvenem sektorju. Zaradi virusa je prišlo do daljših izpadov proizvodnje in storitev v napadenih podjetjih in organizacijah.

7.3. Scenarij tveganja 3: Napad na kritično infrastrukturo v energetskem sektorju

Konec decembra leta 2015 je bil izveden koordiniran kibernetski napad na tri podjetja za distribucijo električne energije v Ukrajini. To je povzročilo večurne izpade oskrbe z električno energijo za okoli 225 tisoč uporabnikov na različnih koncih države. Napadeni so bili informacijski sistemi in sistemi SCADA omenjenih podjetij. Napadalec je na daljavo izklopil omrežje 110 in 35 kV razdelilnih postaj. Za ponovno vzpostavitev oskrbe so podjetja morala preiti na ročno upravljanje sistema.

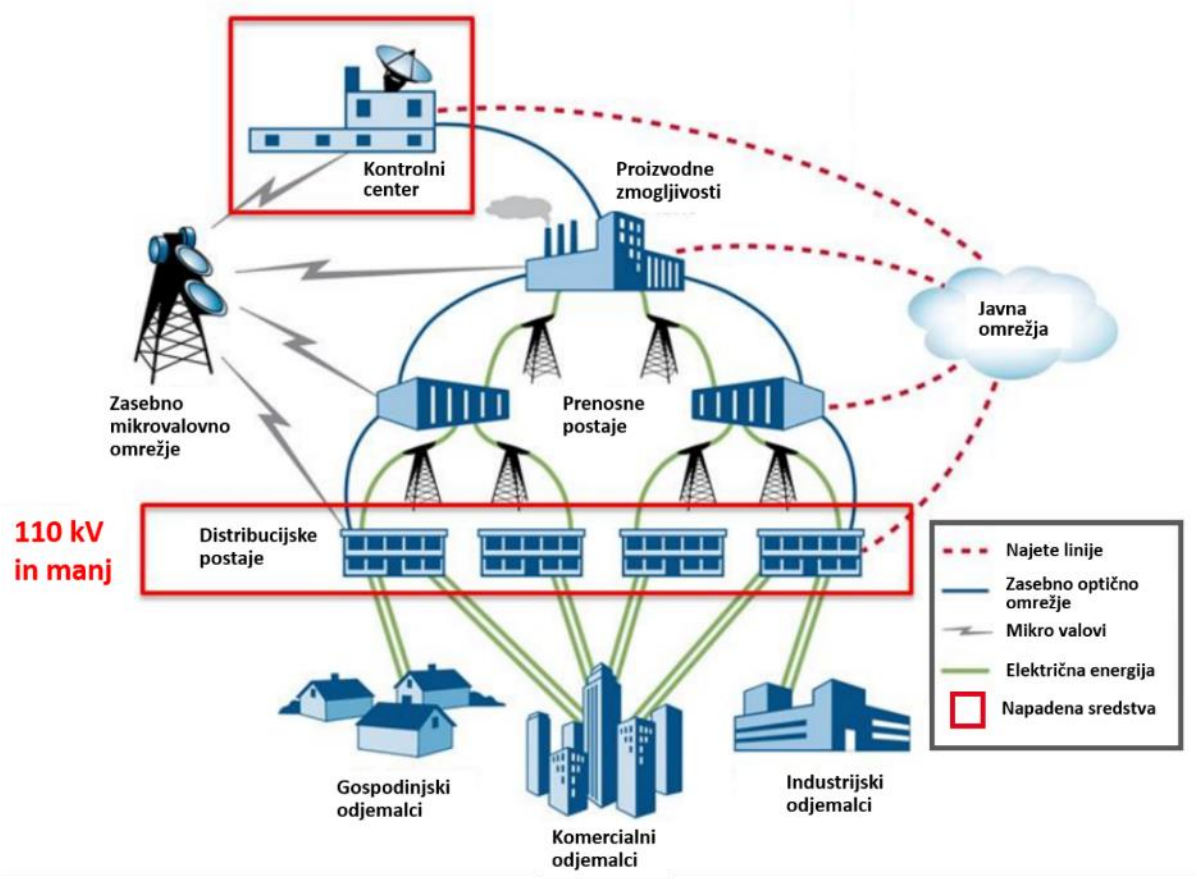
*Sistem za nadzor in pridobivanje podatkov (Supervisory control and data acquisition - **SCADA**) je arhitektura nadzornega sistema, ki uporablja računalnike, omrežne podatkovne komunikacije in grafične uporabniške vmesnike za nadzor nad procesi na visoki ravni. Sistem uporablja tudi druge zunanje naprave, kot so programabilni logični krmilniki (PLC) in diskretni PID krmilniki za povezavo z napravami ali stroji ter objekti nadzora. Vmesniki omogočajo spremljanje in izvajanje ukazov za procese, nadzorno logiko in izračune krmilnikov pa izvajajo omrežni moduli, ki so povezani s senzorji in aktuatorji na terenu.*

Koncept SCADA je bil razvit kot univerzalno sredstvo za oddaljeni dostop do različnih lokalnih kontrolnih modulov, ki omogočajo dostop prek standardnih protokolov za avtomatizacijo. V praksi so veliki SCADA sistemi po funkciji postali zelo podobni porazdeljenim nadzornim sistemom, vendar z uporabo različnih sredstev za povezovanje z objekti nadzora. Nadzorujejo obsežne procese, ki lahko vključujejo več lokacij in delujejo tako na majhnih kot velikih razdaljah.

[48] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf, str. 15, dostop avgust 2018

Kasnejša preiskava ukrajinskih in tujih preiskovalcev, med katerimi so bili tudi strokovnjaki za kibernetsko varnost iz ameriške vlade, je pokazala, da je napadalcu že šest mesecev pred izklopom distribucijskega omrežja uspelo vdreti v nadzorne sisteme podjetij. Za to je uporabil več različnih pristopov, od usmerjenih napadov zvabljanja (spear phishing) do okuženih dokumentov zbirke Microsoft Office. Napadalec je tako skrivaj pridobil dostop do informacijskih sistemov podjetij in potem ves čas prikrito zbiral informacije, ki so kasneje služile za izvedbo napada. Izkazalo se je, da je imel vse potrebno znanje in izkušnje tako z omrežno infrastrukturo in napravami IKT, kot tudi z nadzornimi sistemi SCADA. Poleg tega je bil sposoben pripraviti in namestiti prilagojeno strojno programsko opremo (firmware) na naprave v distribucijskih postajah. Napadalec je poleg tega v enem primeru uporabil telefonski sistem, ki je s tisoči telefonskih klicev dobesedno poplavil klicni center enega od napadenih podjetij, kar je njegovim strankam onemogočilo prijavo prekinitev oskrbe z električno energijo.

Slika 6: Prikaz napada na omrežje ukrajinskih podjetij za distribucijo električne energije. Vir: SANS, 2016



Največja sposobnost napadalca ni bila v izbiri uporabljenih orodij in tehnik ali strokovnem znanju, temveč v njegovi sposobnosti za dolgoročno pridobivanje informacij, potrebnih za spoznavanje okolja napada in za izvedbo visoko sinhroniziranih večstopenjskih napadov na

različnih lokacijah. Vse to je kazalo na verjetnost, da je bil napadalec državno sponzoriran. Kasnejša analiza[49] je pokazala, da so za napad odgovorne ruske obveščevalne službe.

7.4. Verjetnost in zanesljivost scenarijev tveganja

V Sloveniji do sedaj razen že omenjenega napada na spletišča državne uprave in napada z izsiljevalskim virusom WannaCry k sreči ni bilo obsežnejših in načrtovanih kibernetskih napadov s težjimi posledicami[50], kar pa ne pomeni, da bo tako tudi v prihodnje. Področje kibernetskih groženj se nenehno spreminja in razvija, odvisno od razvoja na različnih področjih, predvsem na področju tehnologije, pa tudi na geopolitičnem področju. Tako lahko v prihodnje pričakujemo porast kibernetskih groženj, ki bodo realizirane skozi naprave interneta stvari. Prav tako bo vedno večja digitalizacija na vseh področjih po eni strani prinesla mnogo pozitivnih učinkov za gospodarstvo in družbo, po drugi strani pa ju bo še bolj izpostavila obstoječim in tudi novim kibernetskim grožnjam. Zaradi geopolitičnih sprememb, oblikovanja novih in slabitve starih zavezništev ter prerazporejanja ekonomske in politične moči v svetu, je mogoče pričakovati vedno več kibernetskih napadov, ki bodo sponzorirani s strani držav. Pri tem bo lahko šlo za tehnološko vohunjenje, vplivanje na politične sisteme znotraj posameznih držav ali pa za uveljavljanje vojaške in politične premoči.

Slovenija je resda majhna in tako v političnem kot tudi gospodarskem smislu neizstopajoča, tako da doslej kot država v večini primerov ni bila cilj različnih akterjev kibernetskih groženj. Kljub temu so opisani scenariji, temelječi na dejanskih kibernetskih incidentih, popolnoma verjetni. Pri tem je pri vseh scenarijih kot prizadeto območje upoštevano celotno ozemlje države.

Scenarij tveganja 1: Napad na spletišča državne uprave je dokaj verjeten in bi bil lahko spodbujen z opredelitvijo države do političnih, ekonomskih in ekoloških vprašanj (npr. priznanje novih držav, sodelovanje pri ekonomskih, političnih ali vojaških sankcijah proti kateri od držav, sodelovanje v vojaških konfliktih, opredelitev do trgovinskih in ekoloških sporazumov itd.). Najverjetnejša akterja kibernetske grožnje v tem primeru so hektivisti in države.

Scenarij tveganja 2: Napad z izsiljevalskim programjem je zelo verjeten, saj na ta način kriminalne združbe lahko monetizirajo svoje aktivnosti, drugi akterji kibernetskih groženj (npr. države) pa posredno in prikrito z onemogočanjem delovanja podjetij in organizacij dosežejo svoje cilje. Dober primer je bil uspeh virusa WannaCry v letu 2017. Glavni cilj kriminalcev so sicer organizacije v javnem in zasebnem sektorju, a so žrtve lahko tudi posamezniki. Nekoliko specifično za Slovenijo je, da k uspešnem širjenju izsiljevalskih virusov pripomore tudi še vedno nezanemarljiva uporaba nelegalne programske opreme in vsebin, ki so lahko že v

[49] Analysis of the Cyber Attack on the Ukrainian Power Grid, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, dostop avgust 2018

[50] Izjema je družba Revoz, kjer je imel napad z izsiljevalskim virusom WannaCry leta 2017 konkretne finančne posledice.

osnovi okužene. Najverjetnejši akter kibernetske grožnje v tem primeru so kibernetski kriminalci, lahko tudi v povezavi z državami.

Scenarij tveganja 3: Napad na kritično infrastrukturo je zaradi nevpletenosti države v politične ali vojaške konflikte sicer najmanj verjeten, a bi bile posledice njegove izvedbe najhujše, sploh če upoštevamo, da bi onemogočanje preskrbe z električno energijo v sektorju energetike vplivalo na takorekoč vse ostale sektorje kritične infrastruktre. Tukaj bi bil kibernetski napad, verjetno kot del hibridne grožnje, lahko spodbujen npr. zaradi sodelovanja države v vojaškem konfliktu. Najverjetnejši akter kibernetske grožnje v tem primeru so države.

Zgoraj opisano velja za Slovenijo, obravnavano samostojno. Verjetnost opisanih scenarijev pa bi se lahko povečala, ko bo država v drugi polovici leta 2021 predsedovala Svetu Evropske unije in bi napad nanjo lahko simbolično pomenil tudi napad na Evropsko unijo.

Uporabljeni scenariji tveganja so razmeroma zanesljivi, saj izhajajo iz preteklih resničnih kibernetskih incidentov.

7.5. Reprezentativni scenarij tveganja

Razvoj področja kibernetskih groženj je lahko resnično nepredvidljiv. Obstaja veliko različnih tipov groženj, različnih vektorjev napada in različnih akterjev, ki grožnje realizirajo. Kombinacij vsega naštetega je ogromno in nemogoče bi bilo vse predvideti, kaj šele opisati. Zaradi vsega naštetega in trenutnih trendov na področju kibernetskih groženj ter upoštevajoč ekonomsko-politični položaj Slovenije, je bil kot reprezentativni scenarij tveganja izbran scenarij tveganja 2: Napad z izsiljevalskim programjem.

8. Analize tveganja

V nadaljevanju so podane analize tveganja za tri izbrane scenarije tveganja.

8.1. Analiza tveganja - Scenarij tveganja 1: Napad na spletišča državne uprave

Napadi na spletišča državne uprave leta 2012 niso povzročili trajne škode. Predvsem je šlo za razobličenja[51] naslovnih spletnih strani posameznih organov, kar pa je bilo vidno že na prvi pogled.

V današnjem času bi podoben napad lahko poleg spreminjanja dokaj statičnih informacij na spletnih straneh obsegal tudi napad z onemogočanjem storitve (DDoS) na državne spletne portale, ki so namenjeni tako pravnim kot fizičnim osebam. Prav zaradi tega in ker še ni možno naročanje na vse storitve, tukaj ne bomo upoštevali portala za eNaročanje na zdravstvene

[51] Zamenjava prikazanih informacij na spletni strani s sporočili napadalca.

storitve. Primera portalov, katerih nedelovanje bi povzročilo težave tako državnim organom kot njunim uporabnikom, sta portala eDavki in eVEM[52]. Preko prvega davčni zavezanci (poslovni subjekti in fizične osebe) oddajajo razne vloge (obrazce, napovedi, ugovore in obračune). Po podatkih AJPES je bilo v Sloveniji na dan 30. 6. 2018 skupno 214.474 poslovnih subjektov (gospodarskih družb, pravnih oseb javnega prava, samostojnih podjetnikov posameznikov, društev, nepridobitnih organizacij, zadrug in drugih fizičnih oseb, ki opravljajo registrirane dejavnosti oziroma s predpisom določene dejavnosti)[53]. Več kot 190.000 omenjenih poslovnih subjektov preko portala eDavki FU posreduje različne vloge z različno frekvenco, od mesečnih do letnih. Pri tem je tak način poslovanja s FU edini možen. Obratno FU portal eDavki uporablja za elektronsko vročanje različnih dokumentov. Tako je bilo v letu 2017 elektronsko vročenih 684.000 dokumentov.

Portal eVEM je namenjen podjetnikom, ki lahko na njem najhitreje ustanovijo ali zaprejo podjetje ter izvedejo druge aktivnosti povezane s podjetjem (sprememba in dopolnitev informacij o podjetju, sprememba statusne oblike itd.). V letu 2017 je bilo preko portala posredovanih 922.017 vlog[54]. Vse vloge, ki jih je mogoče posredovati preko portala eVEM je za razliko od portala eDavki še vedno mogoče oddati tudi fizično na točkah VEM.

V oceni se bomo omejili samo na poslovne subjekte. Pogosto se dogaja, da uporabniki svoje obveznosti poročanja opravijo zadnji dan predpisanih rokov. V takih primerih občasno pride do nedostopnosti portala eDavki zaradi preobremenjenosti (dejansko gre za podobno nedostopnost, kot bi ga sprožil obsežen napad DDoS). Če zaradi tega ali pa kakšnega drugega tehničnega razloga portal ni dostopen, FU podaljša rok za oddajo vlog. Neoddaja vlog v predpisanih rokih je sicer sankcionirana z denarno kaznijo. V primeru nedostopnosti portala eVEM uporabnik vlogo še vedno lahko odda po klasični poti preko točke VEM.

Lahko predvidevamo, da bi tudi v primeru kibernetskega napada, katerega posledica bi bila nedostopnost portala eDavki, FU omogočila vsem uporabnikom oddajo njihovih vlog, ko bi bilo delovanje portala spet vzpostavljeno. Na drugi strani pa bi nezmožnost e-vročanja dokumentov preko portala FU povzročilo dodatne stroške, ker bi bila potrebna klasična vročitev.

Predpostavimo, da bi bilo treba zaradi nedostopnosti portala eDavki opraviti petino (20 %) klasičnih vročitev dokumentov (136.800 vročitev), kar bi po podatkih FU zneslo okoli 60.000 EUR za navadno vročanje enostranskih dokumentov (osebna vročitev in več stranski dokumenti bi bili dražji). Prav tako predpostavimo, da bi zaradi nedostopnosti portala eVEM uporabniki petino vlog (184.400) oddali po klasični poti na točki VEM. Glede na to, da mora uporabnik zaradi preverjanja istovetnosti osebno do točke VEM, bi lahko predpostavili, da dostava in obdelava posamezne vloge zahteva tri ure, kar je okoli 30 EUR (vrednost treh

[52] Elektronska oblika točke VEM (Vse na Enem Mestu)

[53] https://www.ajpes.si/Registri/Poslovni_register/Porocila, dostop avgust 2018

[54] https://data.si/blog/2018/03/09/izjemen-uspeh-vem-tocke-data/, dostop avgust 2018

povprečnih bruto ur dela)[55]. Ocenjeni dodatni stroški bi tako znašali 5.532.000 EUR, skupaj s stroški FU zaradi klasičnih vročitev davčnih dokumentov zaradi nedostopnosti portala eDavki pa blizu 5.600.000 EUR.

Napad na spletišča državnih organov bi povzročil nevšečnosti tako posameznikom kot tudi podjetjem in organizacijam, saj bi morali zaradi nedostopnosti e-storitev določena opravila opraviti po klasični poti, kar bi povzročilo dodatne stroške in izgubo časa. Nastale razmere pa ne bi vplivale na zdravje ljudi oziroma ne bi ogrožale življenj.

Napad bi poleg onemogočanja delovanja najbolj izpostavljenih spletnih portalov državne uprave, lahko povzročil tudi razobličenja spletnih mest. Če bi bile na tak način na spletišča posredovane dezinformacije, ki bi vsaj na prvi pogled delovale verodostojno, bi to lahko imelo vpliv na kakšnega od procesov v družbi (npr. sprememba javnega mnenja in s tem povezani pritiski bi lahko vplivali na kakšno politično ali gospodarsko odločitev oziroma usmeritev). To zadnje bi lahko imelo precej večje (tudi negativne) posledice, kot zgoraj opisana neposredna škoda zaradi izpada delovanja posameznih spletišč.

Opisani scenarij je po obsegu posledic še sprejemljiv. V njemu opisan kibernetski napad bi vsekakor opozoril na napadalca oziroma njegove zahteve, pa naj gre za hektivistično skupino ali državo. Obseg posledic pa bi bil lahko tudi neprimerno večji, če bi napad obsegal spletišča vseh državnih in paradržavnih organov in organizacij. V državi, kjer je precejšen del gospodarstva posredno ali neposredno v rokah države bi to lahko pomenilo, da bi bilo število potencialnih žrtev precej večje.

8.2. Analiza tveganja - Scenarij tveganja 2: Napad z izsiljevalskim programjem

Trend napadov z izsiljevalskim programjem v svetu je naraščajoč. To je po svoje logično, saj napadalci, pa naj gre za kibernetske kriminalce ali pa kak drug akter kibernetskih groženj, na ta način najlažje monetizirajo svoje aktivnosti. Napad z izsiljevalskim virusom WannaCry leta 2017 je bil doslej v svetovnem merilu največji napad take vrste. Z vidika finančne škode, ki jo je povzročil, je bil celoten znesek plačanih odškodnin zanemarljiv v primerjavi s škodo, ki je nastala zaradi izpada proizvodnje ali storitev.

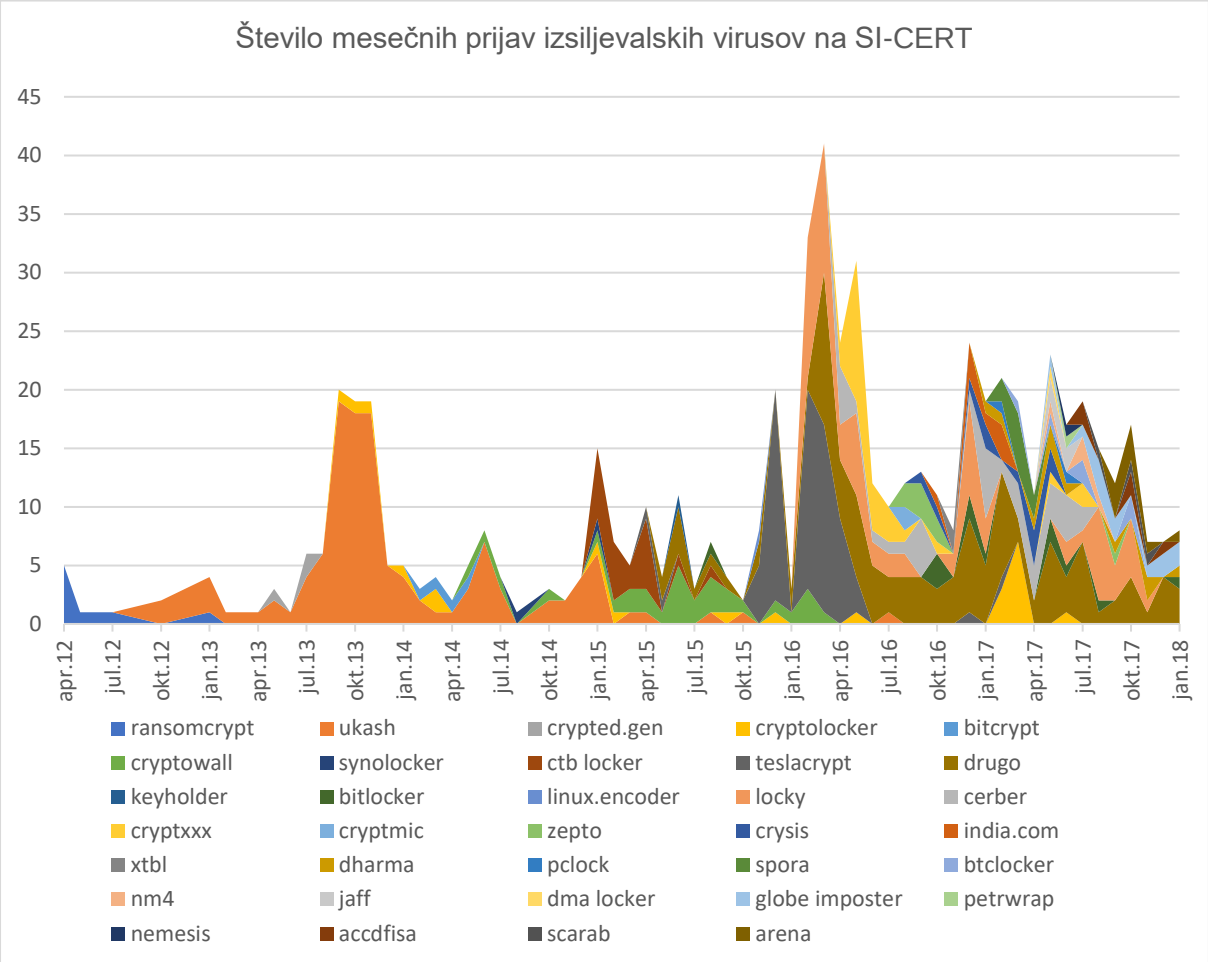
WannaCry pa še zdaleč ni edini virus take vrste. Na SI-CERT je bilo v zadnjih šestih letih prijavljenih več kot 33 različnih izsiljevalskih virusov, ki pa v javnosti niso bili tako prepoznavni. Sodovni virusi večinoma delujejo po naslednjem principu:

1. Po zagonu virus ustvari unikatni par ključev RSA-4096 in unikatni identifikator okuženega računalnika,
2. identifikator in zasebni del RSA ključa pošlje v napadalčev nadzorni strežnik,
3. zasebni del RSA ključa izbriše iz računalnika,
4. naredi seznam vseh dostopnih datotek na dosegljivih diskovnih pogonih,

[55] https://www.stat.si/StatWeb/Field/Index/74, dostop avgust 2018

5. za vsako datoteko ustvari lasten AES ključ, z njim zašifrira datoteko, nato pa sam AES ključ zašifrira z javnim ključem RSA in ga v šifrirani obliki doda v žrtvino datoteko,
6. v vse mape odloži izsiljevalsko sporočilo, ki vsebuje povezavo na spletno stran, skrito prek TOR omrežja; povezava vsebuje identifikator, s katerim napadalci najdejo zasebni del RSA ključa, ki je potreben za dešifriranje podatkov.

Slika 7: Prikaz mesečnih prijav incidentov z izsiljevalskimi virusi v obdobju od aprila 2012 do januarja 2018. Vir: SI-CERT, 2018



Kampanje izsiljevalskih virusov se ponujajo na črnem trgu kot storitev, okužbe pa se širijo prvenstveno s priponkami v elektronski pošti. Te so lahko različnih oblik: kot navidezne PDF datoteke, kot dokumenti zbirke Microsoft Office z makri ali kot ZIP arhivske datoteke s kodo javascript. Manj pogost način je okužba v mimohodu (angl. drive-by download) s katerim od kompletov za izkoriščanje.

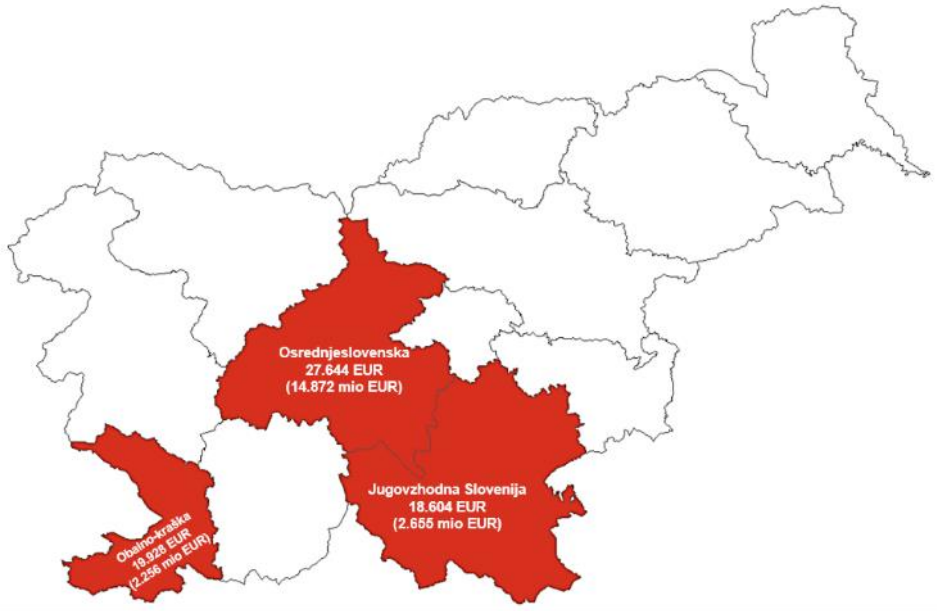
SI-CERT je v preteklih dveh letih prejel tudi več prijav uporabnikov, ki so postali žrtev izsiljevalskega virusa ob prebiranju novic. Napadalci so namreč na novičarsko spletno stran z oglasom podtaknili škodljivo kodo. Ta preveri, ali je v sistemu neposodobljena programska

oprema, ki omogoča nepooblaščen dostop in namestitev dodatnih zlonamernih komponent. Podtaknjena koda lahko iz sistema pridobi tudi zaupne informacije, gesla in certifikate.

Z vidika ogroženosti z napadi z izsiljevalskim programjem, so najbolj izpostavljena mikro, mala in srednja podjetja (MSP), ki so že dosegla določeno stopnjo digitalizacije svojih proizvodnih in poslovnih procesov ter nimajo lastnih strokovnjakov s področja IT. Na drugi strani so lahko ogroženi tudi veliki sistemi v zasebnem in javnem sektorju (npr. zdravstvo), kjer predstavlja nadgradnja strojne in programske opreme velik strošek. Virus WannaCry je izkoriščal ranljivost neposodobljenih operacijskih sistemov, med njimi tudi starejših, za katere je proizvajalec že pred časom ukinil podporo. V tem primeru se je izkazalo, da je še vedno zaradi različnih razlogov v uporabi programska oprema, ki ni več podprta s strani proizvajalca in je zato bolj ranljiva. Lahko gre za industrijske ali pa poslovne računalnike s posebnimi aplikacijami, ki delujejo samo na določenih operacijskih sistemih. Njihova nadgradnja bi zahtevala tudi nadgradnje teh aplikacij ali celotnih procesov, kar pa je lahko finančno in organizacijsko zahtevno. Prav tako je finančno in organizacijsko zahtevna nadgradnja velikega števila računalnikov v velikih sistemih, saj nova programska oprema običajno zahteva tudi novo strojno opremo. V primeru WannaCry se je po drugi strani mnogokrat izkazalo, da bi bili programski popravki lahko nameščeni, pa zaradi različnih razlogov niso bili. Lahko je šlo za malomarnost ali pa preprosto pomanjkanje strokovnega znanja (kot že rečeno, mala podjetja nimajo svojih strokovnjakov IT). Morda je rešitev v takem primeru najem storitev IKT in podpis ustrezne pogodbe SLA[56] z zunanjim izvajalcem.

Lahko predpostavimo, da je stopnja digitalizacije višja v okoljih, ki dosegajo višjo dodano vrednost, zato smo v tem scenariju uporabili tri slovenske statistične regije z najvišjim BDP na prebivalca, in sicer osrednjeslovensko in obalno-kraško regijo ter regijo jugovzhodna Slovenija. Vse tri regije skupno ustvarijo 49 % BDP države. V okoljih z višjo stopnjo digitalizacije bi napad z izsiljevalskim programjem lahko imel največje posledice. Predpostavimo, da bi zaradi napada prišlo do izpada proizvodnje in storitev za pet delovnih dni in da bi skupna povzročena škoda, ki bi jo utrpela prizadeta podjetja in organizacije znašala 15 % ustvarjenega BDP v teh regijah v dnevih izpada.

[56] Service Level Agreement (nivo zagotavljanja storitev)



Preglednica 4: Tri slovenske statistične regije z največjim BDP na prebivalca, Slovenija 2016. Vir: SURS, 2018

Statistična regija	Mio. EUR	EUR / prebivalca	Število prebivalcev	Število ranljivih[57]	Število podjetij
1. Osrednjeslovenska	14.872	27.644	537.023	177.687	65.412
2. Obalno-kraška	2256	19.928	113.070	37.458	13.855
3. Jugovzhodna Slovenija	2655	18.604	142.566	47.038	10.378
SKUPAJ	19.783		792.659	262.183	89.645
Delež	48,9%		38,4%	38,2%	45,7%

Leta 2016 je bilo v Sloveniji 252 delovnih dni. To število je treba ustrezno prilagoditi (povečati), ker določeni deli gospodarstva oziroma družbe (npr. del zdravstva in socialnega varstva ter obrambe) obratujejo celo leto. Upoštevaje to dejstvo je prilagojeno število delovnih dni 256,6[58]. Ustvarjeni BDP na dan v treh upoštevanih regijah bi tako znašal 77,10 mio. EUR.

Če bi bil napad z izsiljevalskim programjem ciljan, bi povzročil največjo škodo v podjetjih in v sektorjih kritične infrastrukture ter pri izvajalcih storitev, pomembnih za delovanje države, hkrati pa bi napadalcu potencialno prinesel največjo korist z možnostjo odkupnin (v primeru akterja kibernetski kriminalci) ter z izpadom proizvodnje in storitev (v primeru akterja države). V našem primeru bi ob upoštevanju zgoraj navedenih predpostavk ocenjena skupna neposredna škoda zaradi izpada proizvodnje in storitev znašala 57.820.000. EUR[59]. To bi veljalo, če ne pride do trajne izgube podatkov in je obnovitev poslovanja normalna. Če pa bi v določenih subjektih

[57] Skupno število prebivalcev iz skupin, starih 14 let ali manj in 65 let ali več.

[58] Sektorji družbe z večino zaposlenih (96 %) so leta 2016 obratovali 252 dni v letu, sektorji s 4 % zaposlenih pa 366. Upoštevaje to razmerje je število delovnih dni 256,6, 5 dni pa tako predstavlja slaba 2 %.

[59] Izračun: (14.872 + 2.256 + 2.655) mio. EUR / 256,6 dni x 5 dni x 0,15 = 57,82 mio. EUR

prišlo do delne ali popolne izgube podatkov, bi to lahko v najslabšem primeru privedlo tudi do propada takega subjekta.

Opisani scenarij je po obsegu posledic še sprejemljiv. Scenarij na eni strani vsebuje nekatere predpostavke, ki so pri oceni vplivov in posledic na spodnji meji, kot je npr. dokaj kratko obdobje izpada zaradi delovanja grožnje in povrnitve v normalno stanje (5 dni), omejeno število prizadetih (skupna škoda 15 % BDP, ki bi bil ustvarjen v času izpada) ter zaradi lažje predstavitve omejitev na samo tri statistične regije. Na drugi strani pa so ozaveščenost in varnostni ukrepi, tudi zaradi izkušnje z virusom WannaCry, na višji stopnji kot v preteklosti. V prihodnosti se bo izpostavljenost zaradi vedno višje stopnje digitalizacije in večje uporabe izsiljevalskega programja povečevala, a bodo temu sledili tudi višja stopnja ozaveščenosti ljudi in izboljšani varnostni ukrepi.

8.2.1 Vplivi na ljudi

V obravnavanih statističnih regijah je po podatkih SURS leta 2016 živelo 792.659 ljudi, kar je dobrih 38 % vseh ljudi v Sloveniji. V skupini ranljivih, ki jo tvorita skupini starih 14 let ali manj in 65 let ali več, je bilo 262.183 ljudi, kar je na ravni države prav tako predstavljalo nekaj več kot 38 % delež. Odvisno od tarč napada z izsiljevalskim programjem, bi bile prizadete različne skupine ljudi. V primeru virusa WannaCry so bili po svetu prizadeti tako posamezniki kot velika podjetja in organizacije. Povzročil je izpade proizvodnje in storitev v sektorjih industrije, telekomunikacij, zdravstva, prometa in javne uprave.

Če bi prišlo do okužbe z virusom v organizacijah v slovenskem zdravstvenem sistemu (bolnišnice, zdravstveni domovi), kot se je to zgodilo v primeru WannaCry v Veliki Britaniji (prizadetih je bilo 80 od 236 bolnišnic in 595 od 7454 splošnih ambulant)[60], bi lahko prišlo do odpovedi oziroma preložitve operacij, do težav pri izdaji zdravil ter pri obravnavi bolnikov v zdravstvenih domovih in bolnišnicah, če ne bi bili dostopni njihovi elektronski zdravstveni kartoni. To bi v nekaterih primerih na dolgi rok lahko imelo tudi posledice za njihovo zdravje. Če bi zaradi okužbe prišlo do motenj v delovanju sistemov za preskrbo s pitno vodo in čiščenje odpadnih voda, bi to lahko privedlo do onesnaženja pitne vode in posledično do obolevanja ljudi. V najhujših primerih bi lahko prišlo do smrtnih žrtev med ranljivimi skupinami prebivalstva. Zaradi napada bi lahko prišlo do motenj pri oskrbi z živili in njihovi prodaji, do zamud in odpovedi v javnem prometu ter do motenj pri poslovanju z organi državne uprave.

8.2.2 Gospodarski in okoljski vplivi in vplivi na kulturno dediščino

V obravnavanih statističnih regijah je po podatkih SURS leta 2016 delovalo 89.645 podjetij, kar je slabih 46 % vseh podjetij v Sloveniji. Izkušnja z izsiljevalskim virusom WannaCry je pri njih verjetno pripomogla k večji ozaveščenosti glede samozaščitnih ukrepov, vendar tudi

[60] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

napadalci uporabljajo vedno nove vektorje napada, ki so pogosto korak pred zaščitnimi ukrepi. Po podatkih Urada RS za varovanje tajnih podatkov, je nekaj dnevni izpad proizvodnje zaradi virusa WannaCry podjetju Revoz povzročil za 3 milijone EUR škode. V Revozu je prišlo do okužbe po internem omrežju podjetja Renault, ki je bilo med najbolj prizadetimi v svetovnem merilu. Kot je bilo že omenjeno so podobnim primerom lahko bolj izpostavljena, mala in srednja podjetja ter organizacije brez lastnih IT služb, pa tudi večja, kjer nadgradnje velikega števila strojne in programske opreme predstavlja velik strošek. Z vse večjo stopnjo digitalizacije proizvodnih in poslovnih procesov so podjetja in organizacije življensko odvisne od svojih informacijskih sistemov in podatkov v njih.

Napad z izsiljevalskim programjem lahko v industrijskih ter storitvenih panogah za krajši ali daljši čas onemogoči proizvodnjo in storitve. Ker so slovenska podjetja v določenih panogah velik proizvajalec in dobavitelj sestavnih delov za druga, predvsem tuja podjetja, bi izpad proizvodnje lahko negativno vplival na njihov položaj predvsem na zelo konkurenčnih trgih. Daljši čas onemogočen dostop do podatkov ali celo njihova trajna izguba lahko privede do izgube poslov, ki bi jih bilo kratkoročno težko nadomestiti, v najslabšem primeru pa lahko pride do propada podjetja ali organizacije.

V prometu lahko pride do zmede pri voznih redih ter do zamud in odpovedi v cestnem, železniškem, letalskem in ladijskem prometu. To bi lahko negativno vplivalo na logistična podjetja. Zloraba ali kraja zaupnih podatkov podjetja ali organizacije (npr. osebni podatki strank in partnerjev, intelektualna lastnina) lahko povzroči vdore v sisteme drugih podjetij in organizacij, zlorabo elektronske identitete posameznikov ter izgubo konkurenčnih prednosti. Z vsem naštetim je lahko povezana velikanska in včasih nepopravljiva škoda.

8.2.3 Politični in družbeni vplivi

Če bi prišlo do napada z izsiljevalskim programjem bi lahko prišlo do težav pri delovanju organov državne uprave in posledično tudi do motenj pri izvajanju storitev za državljane. Zaradi motenj v maloprodaji bi lahko prišlo do težav predvsem zaradi onemogočenega nakupa živil. Lahko bi nastopile težave v plačilnem prometu, pri dvigih gotovine na bankomatih in na splošno pri dostopu do interneta, ker bi operaterji zaradi preprečitve širjenja okužb izvajali omejitve v internetnem prometu. Če bi težave trajale dalj časa, bi to v nekaterih primerih lahko povzročilo nezadovoljstvo prebivalstva in v najslabšem primeru privedlo do nemirov.

8.3. Analiza tveganja - Scenarij tveganja 3: Napad na kritično infrastrukturo v energetskem sektorju

Uspešen napad na kritično infrastrukturo v energetskem sektorju na strani napadalca zahteva dolgotrajne priprave in koordinirano sodelovanje različnih profilov strokovnjakov. Gre za končni rezultat napredne trajne grožnje (APT), ki uporablja niz prikritih in kompleksnih hekerskih procesov, katerih namen je napad na točno določeno informacijsko infrastrukturo. Pri tem želi napadalec čim dlje ostati prikrit v omrežju žrtve. Zaradi kompleksnosti operacije, časovne

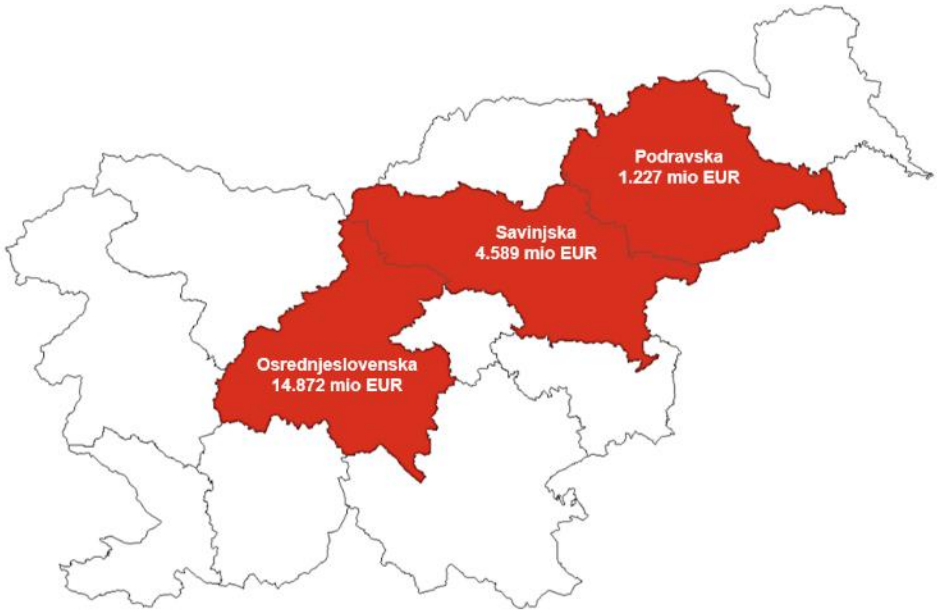
dimenzije, potrebnih naprednih znanj in udeležbe večjega števila ljudi, je tak napad praviloma podprt s strani tuje države, ki želi doseči svoje politične ali vojaške cilje. Kibernetski napad je pogosto del hibridne grožnje in lahko služi tudi kot sredstvo za odvračanje pozornosti od aktivnosti, ki jih napadalec za realizacijo svojih ciljev izvaja vzporedno.

Napad se prične z infiltracijo v informacijske sisteme žrtve, samostojno ali pa s pomočjo kakšne osebe znotraj sistema. Od tu naprej se prične prikrito zbiranje informacij, ki se uporabijo za pripravo dejanskega napada. V obdobju prikritega delovanja se v omrežjih žrtve namestijo orodja, ki napadalcu omogočijo oddaljeni prevzem nadzora nad informacijskimi sistemi žrtve. Ko je vse skupaj pripravljeno, napadalec samo še počaka na primeren trenutek, ko bo imel napad največji učinek. Tak trenutek je lahko odvisen od poteka vzporednih aktivnosti (npr. pri hibridnih grožnjah), lahko pa napadalec napad tudi odloži in ga sproži kdaj kasneje, ko z njim doseže največji učinek. Če bi bil napad izveden v času, ko bi žrtev doletela huda naravna ali druga nesreča, bi imel neprimerno večji negativni učinek.

Raziskovalna organizacija Cambridge Centre for Risk Studies je po kibernetskem napadu na podjetja za distribucijo električne energije v Ukrajini leta 2015 pripravil študijo električnega mrka v Veliki Britaniji, ki bi ga povzročil katastrofalni kibernetski napad[61] tuje države s pomočjo oseb znotraj sistema. Po tem scenariju naj bi osebe znotraj sistema po razdelilnih postajah neopazno namestile naprave, s katerimi je mogoče na daljavo prekinjati delovanje postaj in s tem oskrbo z električno energijo. Scenarij, ki predvideva serijo izpadov omrežja v JV delu države, kjer je skoncentrirano največje število ljudi in podjetij (ekonomsko najmočnejši del Velike Britanije), ima glede na obseg in trajanje napadov ter kasnejše obnovitve sistema tri različice. Dejanski skupni izpadi omrežja trajajo od 1,5 do 6 tednov (sami napadi sicer trajajo od 3 do 12 tednov), odpravljanje posledic skupaj s potrebnim načrtovanjem pa od 2 do 10 tednov.

V našem primeru predpostavljamo, da bi napadalec izvedel koordiniran napad na elektro distribucijski sistem v treh slovenskih statističnih regijah z največjim deležem v BDP države , in sicer v osrednjeslovenski, podravski in savinjski regiji, ki skupno ustvarijo 61 % slovenskega BDP. Distribucijo električne energije na tem področju izvajajo trije različni operaterji (pri tem zanemarimo zaprte distribucijske sisteme), kar je podobno, kot v primeru napada v Ukrajini. Predpostavimo, da bi koordiniran kibernetski napad povzročil skupno samo pet delovnih dni izpada preskrbe z električno energijo, ko bi bila popolnoma onemogočena proizvodnja in izvajanje storitev.

[61] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf



Preglednica 5: Tri slovenske statistične regije z največjim deležem v BDP države, Slovenija 2016. Vir: SURS, 2018

Statistična regija	Mio EUR	% v BDP države	Število prebivalcev	Število ranljivih	Število podjetij
1. Osrednjeslovenska	14.872	36,8	537.023	177.687	65.412
2. Podravska	5.170	12,8	322.553	105.428	26.125
3. Savinjska	4.589	11,4	254.318	83.663	21.490
SKUPAJ	24.631	61	1.113.894	366.778	113.027
Delež	60,9%		54,0 %	53,4%	57,6 %

Tako kot v primeru scenarija 2: Napad z izsiljevalskim programjem, je tudi tukaj prilagojeno število delovnih dni 256,6[62]. Ustvarjeni BDP na dan v treh upoštevanih statističnih regijah bi tako znašal 95.990.000 EUR.

V obravnavanih statističnih regijah je po podatkih SURS leta 2016 živelo 1.113.894 ljudi, kar je 54 % vseh ljudi v Sloveniji. V skupini ranljivih je bilo 366.778 ljudi, kar je na ravni države predstavljalo več kot 53 % delež. Vsi prebivalci bi čutili vpliv izpada preskrbe z električno energijo. Napad bi imel največji vpliv na ljudi v obdobjih z najvišjimi oziroma najnižjimi temperaturami v letu. V prvem primeru zaradi izpada hlajenja in pokvarljivosti hrane, v drugem pa predvsem zaradi problemov z ogrevanjem, tudi zaradi nesreč z uporabo neprilagojenih kurišč (smrti in poškodbe), pa tudi zaradi pokvarljivosti hrane. V obeh primerih je mogoče pričakovati več nesreč v cestnem prometu zaradi neosvetljenosti vozišč in s tem več smrtnih žrtev in poškodovanih. Prav tako bi bile v obeh primerih bolj ogrožene ranljive skupine prebivalstva, ki težje prenašajo temperaturne ekstreme (vročino in mraz). Zaradi izpada

[62] Sektorji družbe z večino zaposlenih (96 %) so leta 2016 obratovali 252 dni v letu, sektorji s 4 % zaposlenih pa 366. Upoštevaje to razmerje je število delovnih dni 256,6, 5 dni pa tako predstavlja slaba 2 %.

zdravstvenih storitev (npr. odpovedi operacij) bi lahko na kratki ali dolgi rok pri nekaterih bolnikih prišlo do poslabšanja zdravstvenega stanja ali smrti.

V obravnavanih statističnih regijah je po podatkih SURS leta 2016 delovalo 113.027 podjetij, kar je slabih 58 % vseh podjetij v Sloveniji. Podjetja, pa tudi druge organizacije, bi utrpele neposredno škodo zaradi izpada njihove proizvodnje in storitev. Ker so slovenska podjetja v določenih panogah velik proizvajalec in dobavitelj sestavnih delov za druga, predvsem tuja podjetja, bi izpad proizvodnje lahko negativno vplival na njihov položaj predvsem na zelo konkurenčnih trgih. V najslabšem primeru bi lahko prišlo do izgube poslov, ki bi jih bilo kratkoročno težko nadomestiti. V prometu bi prišlo do težav predvsem v železniškem transportu, kar bi negativno vplivalo na tovorni promet, posredno lahko tudi na Luko Koper. Nedelovanje komunikacijskih povezav in interneta bi pri poslovanju, v plačilnem prometu in pri drugih dejavnostih , ki so odvisne od interneta, občutili vsi, tako podjetja kot fizične osebe.

Zaradi izpadov oskrbe z električno energijo in s tem povezanih problemov pri čiščenju odpadnih voda bi lahko prišlo do onesnaženj okolja (predvsem rek, podtalnice in pitne vode), kar bi posledično negativno vplivalo na zdravje ljudi in živali.

Prav tako bi zaradi izpadov oskrbe z električno energijo lahko prišlo do težav pri oskrbi z osnovnimi prehrambenimi proizvodi in zdravili. To bi poleg zmanjšanja možnosti komunikacij in dostopa do informacij v nekaterih primerih lahko privedlo do nezadovoljstva prebivalstva in v najslabšem primeru do nemirov.

Ker bi izpad oskrbe z električno energijo vplival takorekoč na vse segmente družbe, lahko predpostavimo, da bi bilo v primeru scenarija 3 zaradi napada izgubljenega 80 % običajno ustvarjenega BDP. Ocenjena skupna neposredna škoda zaradi pet dnevnega izpada proizvodnje in storitev v treh obravnavanih regijah bi tako znašala 383.960.000 EUR[63].

Opisani scenarij je po obsegu posledic še sprejemljiv. Scenarij sicer vsebuje nekatere predpostavke, ki so pri oceni vplivov in posledic na spodnji meji, kot je npr. dokaj kratko obdobje izpada zaradi delovanja grožnje in povrnitve v normalno stanje (5 dni) ter zaradi lažje predstavitve omejitev na samo tri statistične regije Tudi v tem primeru se bo izpostavljenost v prihodnosti zaradi vedno višje stopnje digitalizacije z uporabo pametnih omrežij povečala. Kljub temu je glede na trenutni politični in ekonomski položaj (neizpostavljenost) države verjetnost realizacije grožnje iz scenarija dokaj nizka.

8.4. Verjetnost analiz tveganja

Ocenjuje se, da predstavljajo opisani in podobni vplivi tveganja iz Scenarija tveganja 1 splošno nevarnost, vplivi iz Scenarija tveganja 2 posebno in takojšnjo (trajno) nevarnost, vplivi iz Scenarija tveganja 3 pa mogočo nevarnost. Te vrednosti so v nadaljevanju ocene primerjane

[63] Izračun: (14.872 + 5.170 + 4.589) mio. EUR / 256,6 dni x 5 dni x 0,8 = 383,96 mio EUR

z merili za ovrednotenje verjetnosti za realizacijo grožnje in v matrikah tveganja za realizacijo grožnje.

8.5. Zanesljivost analiz tveganja

Ker se celovit nacionalni sistem zagotavljanja kibernetske in informacijske varnosti šele vzpostavlja, na žalost še ne obstajajo potrebni podatki za celovitejše analize. Ko bodo konec leta 2018 določeni zavezanci po ZInfV, ki bodo morali priglašati kibernetske incidente s pomembnim vplivom na neprekinjeno izvajanje njihovih storitev, bo postopno na voljo tudi več podatkov tako o kibernetskih grožnjah kot tudi o potencialnih akterjih teh groženj. Na osnovi teh podatkov bo lažje pripraviti ustrezne in zanesljivejše analize. Obstoječe analize so narejene na podlagi trenutnih (z)možnosti, v prihodnje pa na tem področju verjetno lahko oziroma celo moramo doseči napredek. Ne glede na to lahko trdimo, da so analize tveganja srednje do razmeroma zanesljive.

8.6. Reprezentativna analiza tveganja

Ker je bil kot reprezentativni scenarij tveganja izbran Scenarij tveganja 2: Napad z izsiljevalskim programjem, je za reprezentativno analizo tveganja določena analiza tveganja na podlagi tega scenarija.

9. Ovrednotenje vplivov tveganja

Da bi lahko ugotovili resnost oziroma težo tveganja za realizacijo grožnje, je bilo treba določiti merila za ovrednotenje vplivov in verjetnosti tveganja za nesreče, s katerimi je mogoče primerjati posledice oziroma vplive realiziranih groženj in njihovo verjetnost oziroma pogostost.

9.1 Merila za ovrednotenje vplivov tveganja in verjetnosti za realizacijo grožnje

Vplivi tveganja za realizacijo grožnje so razdeljeni na vplive na ljudi, gospodarske in okoljske vplive, vplive na kulturno dediščino ter politične in družbene vplive. Merila za ovrednotenje tveganja in verjetnosti za realizacijo grožnje so bila spomladi leta 2015 usklajena in sprejeta znotraj delovanja URSZR[64] kot Državnega koordinacijskega organa za ocene tveganj za nesreče, skupaj z vsemi ministrstvi, ki pripravljajo ocene tveganja za posamezne nesreče (v našem primeru za realizacijo grožnje) oziroma sodelujejo pri tem. Leta 2017 so bila merila malenkostno spremenjena. Merila za ovrednotenje vplivov tveganja in verjetnosti za nesreče so enotna za vsa tveganja in oblikovana v pet stopenj, pri čemer je po stopnjah vpliv oziroma verjetnost:

[64] Uprava Republike Slovenije za zaščito in reševanje

1. zelo majhna,
2. majhna,
3. srednja,
4. velika,
5. zelo velika.

9.2 Primerjava rezultatov analiz tveganja za realizacijo grožnje z merili za ovrednotenje vplivov in verjetnosti za nesreče

Primerjava rezultatov analiz tveganja za realizacijo grožnje z ustreznimi merili za ovrednotenje vplivov tveganja in verjetnosti za nesrečo pomeni enega najpomembnejših delov vsake ocene tveganja za posamezno grožnjo. Z merili lahko vrednotimo težo vsake realizirane grožnje oziroma vplivov in verjetnosti tveganja ter posameznih scenarijev oziroma analiz tveganja. Ker so merila za ovrednotenje vplivov tveganja in verjetnosti za nesrečo enotna za vsa tveganja, je omogočena tudi primerjava vplivov oziroma posledic in verjetnosti med posameznimi nesrečami (realiziranimi grožnjami).

Grafično pa se vpliv tveganja in verjetnost za realizacijo grožnje oziroma posamezne analize scenarijev tveganja lahko prikažejo v matrikah tveganja za realizacijo grožnje, ki sledijo temu poglavju.

V preglednicah v poglavjih 9.2 in 9.3 (Matrike tveganja za realizacijo grožnje) so analize scenarijev tveganja lahko poimenovane tudi kot:

- analiza tveganja – Scenarij tveganja 1: Napad na spletišča državne uprave: **S1** ali **Scenarij 1 ali Scenarij tveganja 1**;
- analiza tveganja – Scenarij tveganja 2: Napad z izsiljevalskim programjem: **S2** ali **Scenarij 2 ali Scenarij tveganja 2**;
- analiza tveganja – Scenarij tveganja 3: Napad na kritično infrastrukturo v energetskem sektorju: **S3** ali **Scenarij 3 ali Scenarij tveganja 3.**

9.2.1 Primerjava rezultatov analiz tveganja z merili za ovrednotenje vplivov tveganja na ljudi

Vplivi tveganja na ljudi so v odvisnosti od vrste tveganja lahko predvsem število smrtnih žrtev, število ranjenih ali bolnih, število trajno evakuiranih, število ljudi, ki živijo in delajo na območjih, prizadetih zaradi realizacije grožnje, in drugo (na primer vplivi na ranljive skupine prebivalstva, kot so otroci, starejši, socialno ogroženi). Merila za ovrednotenje vplivov tveganja na ljudi so izražena v številu mrtvih, ranjenih ali bolnih in trajno evakuiranih ljudi.

Preglednica 6: Merila za ovrednotenje vplivov tveganja na ljudi ter uvrstitev scenarijev tveganja v stopnje vpliva

Merila za ovrednotenje vplivov tveganja na ljudi	1	2	3	4	5
Število mrtvih	do 5	5 - 10	10 - 50	50 - 200	nad 200
Število mrtvih (10 let)*	do 5	5 - 10	10 - 50	50 - 100	nad 100
Število ranjenih ali bolnih**	do 10	10 - 50	50 - 200	200 - 1.000	nad 1.000
Število ranjenih ali bolnih (10 let)*	do 10	10 - 50	50 - 200	200 - 500	nad 500
Število evakuiranih (trajni ukrep)	do 20	20 - 50	50 - 200	200 - 500	nad 500
Scenarij tveganja		S2		S3	

** Za nesreče z morebitnimi dolgotrajnimi učinki (npr. do 10 let), kot so npr. nesreče z nevarnimi snovmi, jedrske ali radiološke nesreče, se dolgoročne vrednosti za mrtve in ranjene ali bolne ljudi (10 let) po potrebi določijo posebej oziroma dodatno, kot je navedeno zgoraj.*

*** Med ranjene ali bolne ljudi spadajo tudi obsevani, kontaminirani ali zastrupljeni ljudje, ki se v analizah tveganj lahko ob posameznih tveganjih obravnavajo posebej.*

Pri številu mrtvih in ranjenih se upoštevajo tudi morebitni mrtvi in poškodovani pripadniki sil za zaščito, reševanje in pomoč na intervencijah zaščite, reševanja in pomoči, ter število policistov, vojakov SV in intervencijskih ekip različnih služb (službe nujne medicinske pomoči, ekipe elektropodjetij, komunalnih podjetij itd.), ki so umrli ali bili poškodovani pri izvajanju nujnih ukrepov iz svojih pristojnosti in pri začetnih sanacijskih aktivnostih, vendar najdlje eno leto po nesreči. Za uvrstitev v matrike tveganja za realizacijo grožnje se upošteva vrednost, ki doseže najvišjo stopnjo vpliva glede na usklajena merila za ovrednotenje vplivov tveganja na ljudi.

V poglavju 8 smo v okviru analize tveganj za realizacijo groženj pri posameznih scenarijih ocenili tudi vplive na ljudi. Pri Scenariju tveganja 1 ne bi bilo posledic za ljudi. Pri scenariju tveganja 2 bi posledice nastale zlasti zaradi možnega izpada storitev v slovenskem zdravstvenem sistemu. Ocenjuje se, da bi realizacija grožnje v tem primeru lahko na daljši rok povzročila do 50 bolnih ljudi, kar uvršča Scenarij 2 glede števila bolnih ljudi v drugo stopnjo (kar je reprezentativna vrednost) vpliva tveganja na ljudi. Reprezentativni podatek pri tem scenariju je število bolnih ljudi. Pri Scenariju tveganja 3 se ocenjuje, da bi realizacija grožnje povzročila do 20 smrtnih žrtev ter do 250 ranjenih oziroma bolnih, kar uvršča Scenarij 3 glede števila mrtvih v tretjo stopnjo, glede števila ranjenih oziroma bolnih ljudi pa v četrto stopnjo (kar je reprezentativna vrednost) vpliva tveganja na ljudi. Reprezentativni podatek pri tem scenariju je število ranjenih oziroma bolnih ljudi.

9.2.2 Primerjava rezultatov analiz tveganja z merili za ovrednotenje gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino

Med gospodarske in okoljske vplive tveganja ter vplive tveganja na kulturno dediščino v odvisnosti od tveganja lahko spadajo vplivi, kot so število, posledice in višina škode na objektih in v njih, stroški delovanja ministrstev ter organov, ki dejavnosti iz svojih pristojnosti izvajajo v zaostrenih razmerah, obseg in višina škode na kmetijskih in gozdnih površinah, na objektih/območjih kulturne dediščine, stroški omejitve uporabe hrane ter dolgoročni stroški v

verigi preskrbe s hrano, obseg in višina škode na vodnih telesih, število poškodovanih ali uničenih prometnih sredstev in škoda, ki pri tem nastane, število, škoda in stroški zaradi mrtvih ali poškodovanih oziroma obolelih domačih ali prostoživečih živali ter živali, ki jih je treba usmrtiti ali zdraviti, stroški za zdravljenje oziroma zdravstveno oskrbo ljudi, škoda zaradi prekinitve gospodarske dejavnosti, socialni in drugi podobni stroški, stroški intervencij ter morebitne mednarodne pomoči, stroški celovite dolgoročne obnove (sanacije) objektov in opreme, stroški celovite dolgoročne obnove (sanacije) kmetijskih in gozdnih površin ter objektov/območjih kulturne dediščine, stroški celovite dolgoročne obnove (sanacije) vodnih teles, okoljske obnove in druge okoljske škode ter dodatno (kar se ne upošteva pri izračunu škode in stroškov) še obseg prizadetega območja (v kvadratnih kilometrih in odstotkih površine države), višina zavarovalniških izplačil zaradi nesreče, zmanjšanje BDP, zmanjšanje tujega turističnega obiska ter povečanje brezposelnosti zaradi nesreče.

Preglednica 7: Merila za ovrednotenje gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino ter uvrstitev scenarijev tveganja v stopnje vpliva

1	2	3	4	5
Do 100 milijonov EUR	Od 100 milijonov EUR - 0,6 % BDP 100 - 243 milijonov EUR	0,6 % - 1,2 % BDP 243 - 485 milijonov EUR	1,2 % - 2,4 % BDP 485 - 970 milijonov EUR	nad 2,4 % BDP nad 970 milijonov EUR
S1, S2		S3		
** Upoštevan je BDP za leto 2016.*				

Merila za ovrednotenje gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino se izražajo z višino stroškov in škode, ki jo povzroči določeno tveganje. Meja vpliva tveganja med drugim in tretjim razredom od petih je postavljena na 0,6 odstotka bruto družbenega proizvoda (BDP). Iz tega so izpeljane mejne vrednosti za preostale razrede. Ta izhodiščna vrednost se v precejšnji meri navezuje na vrednost 0,6 odstotka bruto nacionalnega dohodka (BND). Če škoda zaradi neke nesreče namreč preseže vrednost 0,6 odstotka BND, lahko država Evropsko unijo zaprosi za nepovratna finančna sredstva. V RS sta vrednosti BND in BDP zelo podobni (BND je malenkost nižji), zato pri merilih za ovrednotenje vplivov tveganja za nesrečo uporabljamo kar BDP. Višina BDP leta 2016[65] je bila okoli 40.42 milijarde evrov, vrednost 0,6 odstotka BDP pa je zaokroženo približno 243 milijonov evrov.

Iz analiz podatkov scenarijev tveganja, je razvidno, da škoda ob realizaciji groženj iz prvih dveh scenarijev tveganja najverjetneje ne bi presegla višine 100 milijonov evrov, kar oba scenarija oziroma analizi tveganja uvršča v prvo stopnjo gospodarskih in okoljskih vplivov ter vplivov tveganja na kulturno dediščino. Iz analize Scenarija tveganja 3 pa je razvidno, da bi višina okoljskih in gospodarskih vplivov tveganja in vplivov tveganja na kulturno dediščino

[65] Uporabljena je vrednost BDP za leto 2016, ker so bili pri drugih izračunih na voljo samo podatki do vključno leta 2016.

dosegla okoli 384 milijonov evrov (0,95 % BDP iz leta 2016), kar scenarij in analizo tveganja 3 uvršča v tretjo stopnjo od petih možnih.

9.2.3 Primerjava rezultatov analiz tveganja z merili za ovrednotenje političnih in družbenih vplivov tveganja

Politični in družbeni vplivi tveganja lahko v odvisnosti od tveganja vsebujejo kategorije, kot so vpliv tveganja na delovanje državnih organov, vpliv nedelovanja pomembnih infrastrukturnih sistemov na vsakodnevno življenje, psihosocialni vplivi, notranjepolitična stabilnost ter vpliv na javni red in mir, finančna stabilnost in zunanjepolitična oziroma mednarodna stabilnost (položaj) države. Merila za ovrednotenje političnih in družbenih vplivov tveganja so polkvalitativna. Za razliko od prejšnjih dveh skupin vplivov, ki jih je bilo mogoče kvantitativno oceniti, gre pri tej skupini vplivov bolj za ocenjevanje velkostnega reda obravnavanih vplivov. Končna vrednost oziroma stopnja političnih in družbenih vplivov tveganja se ugotovi tako, da se seštevek vrednosti posameznih vplivov deli s številom uporabljanih meril, ki obravnavajo politične in družbene vplive tveganja, tako v okviru posameznih vplivov kot skupin vplivov. Vplivi, ki niso bili ocenjeni, se pri tem ne upoštevajo. Prav tako se ne upoštevajo vplivi tveganja, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso mogli bili ocenjeni.

9.2.3.1 Merila za ovrednotenje vpliva tveganja na delovanje državnih organov in primerjava z rezultati analiz tveganja

Merila za ovrednotenje vpliva tveganja na delovanje državnih organov in primerjava z rezultati analiz tveganja so v preglednicah 8 in 9. Vsi trije scenariji tveganja bi posegali v možnosti izvajanja nalog iz pristojnosti državnih organov. Pri tem bi bilo v primeru Scenarija tveganja 1, ko bi šlo za napad na spletišča državne uprave, delovanje državnih organov zelo okrnjeno do 7 dni in za toliko časa vplivalo tudi na 5000 do 50.000 ljudi (prva in druga stopnja vpliva). V primeru Scenarija tveganja 2, ko bi šlo za napad z izsiljevalskim programjem, lahko predvidevamo, da so centralizacija državne informatike in izkušnje z virusom WannaCry pripomogli k višji stopnji odpornosti. Kljub temu bi bilo delovanje državnih organov še vedno lahko omejeno do 7 dni in za toliko časa vplivalo tudi na 500 do 5000 ljudi (prva in druga stopnja vpliva). V primeru Scenarija tveganja 3, ko bi šlo za izpad oskrbe z električno energijo, med drugim tudi v regiji, kjer deluje večina državnih organov, bi bilo njihovo delovanje onemogočeno do 7 dni in za toliko časa vplivalo tudi na več kot 50.000 ljudi (druga in tretja stopnja vpliva).

Preglednica 8: Možnost izvajanja nalog iz pristojnosti državnih organov (vlada, ministrstva, organi v sestavi, upravne enote) na prizadetem območju in uvrstitev scenarijev tveganja v stopnje vpliva

Trajanje	Omejena	Zelo okrnjena	Onemogočena
Do 2 dni	1	1	2
Do 7 dni	1 (S2)	1 (S1)	2 (S3)
Do 15 dni	2	2	3
Do 30 dni	2	3	4
Več kot 30 dni	3	4	5
Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če vplivi nesreče ne posegajo v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).			

Preglednica 9: Število ljudi, za katere je s strani državnih organov fizično ali funkcionalno ovirano ali moteno izvajanje storitev in uvrstitev scenarijev tveganja v stopnje vpliva

Število ljudi/ trajanje	Do 500	Od 500 do 5000	Od 5000 do 50.000	Več kot 50.000
Do 2 dni	1	1	1	2
Do 7 dni	1	2 (S2)	2 (S1)	3 (S3)
Do 15 dni	2	3	3	4
Do 30 dni	3	4	4	5
Več kot 30 dni	4	5	5	5
Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).				

Končna stopnja ali vrednost vpliva tveganja na delovanje državnih organov se določi tako, da se vsota posameznih vrednosti iz preglednic 8 in 9 deli s številom upoštevanih vplivov.

Če seštejemo stopnje vplivov iz te skupine in ju delimo s številom upoštevanih vplivov (2), dobimo skupne vrednosti vplivov tveganja na delovanje državnih organov:

- Scenarij tveganja 1: 1,5,
- Scenarij tveganja 2: 1,5,
- Scenarij tveganja 3: 2,5.

9.2.3.2 Merila za ovrednotenje vpliva tveganja na delovanje pomembnih infrastrukturnih sistemov in primerjava z rezultati analiz tveganja

Merila za ovrednotenje vpliva tveganja na delovanje pomembnih infrastrukturnih sistemov in primerjava z rezultati analiz tveganja so v preglednicah 10 in 11.

Preglednica 10: Pomanjkanje ali otežen dostop do pitne vode, hrane in energentov (elektrika, ogrevanje, gorivo) ter uvrstitev scenarijev tveganja v stopnje vpliva

Število ljudi/ trajanje	Do 500	Od 500 do 5000	Od 5000 do 50.000	Več kot 50.000
Do 2 dni	1	1	1	2
Do 7 dni	1	2	2	3 (S2, S3)
Do 15 dni	2	3	3	4
Do 30 dni	3	4	4	5
Več kot 30 dni	4	5	5	5

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva vpliv, zaradi katerega je prizadetih največ ljudi. Če je najmanj v dveh primerih prizadeto enako število ljudi, se upošteva tisti, ki traja dlje.

Če vplivi grožnje ne morejo posegati v ocenjevano vsebino, se vpliv grožnje na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

V preglednici 10 je upoštevano stanje oskrbe z električno energijo in pa dostop do pitne vode in hrane. Vpliv grožnje iz Scenarija tveganja 1 se v tem primeru ne ocenjuje. Realizacija grožnje iz Scenarija tveganja 2 bi potencialno imela vpliv na dostop do hrane, če bi zaradi izsiljevalskega programja prišlo do motenj v maloprodaji prehrambenih izdelkov. Realizacija grožnje iz Scenarija tveganja 3 pa bi vplivala na oskrbo z električno energijo in dostop do pitne vode. Oba ocenjevana scenarija tveganja sta umeščena v tretjo stopnjo vpliva.

Preglednica 11: Zelo okrnjeni ali onemogočeni uporaba interneta in telekomunikacijskih sistemov, prihod na delovna mesta in v vzgojno-izobraževalne ustanove, uporaba javnih storitev (dostop do medijev, zdravstvene storitve, bančne storitve itd.), uporaba javnega prometa, oskrba oziroma nakup življenjskih potrebščin in uvrstitev scenarijev tveganja v stopnje vpliva

Število ljudi/ Trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Več kot 50.000
Do 2 dni	1	1	1	2
Do 7 dni	1	2	2	3 (S2, S3)
Do 15 dni	2	3	3	4
Do 30 dni	3	4	4	5
Več kot 30 dni	4	5	5	5

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva tisti, zaradi katerega je prizadetih največ ljudi. Če je najmanj v dveh primerih prizadeto enako število ljudi, se upošteva tisti, ki traja dlje.

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče nanjo ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Tudi v tem primeru se ne ocenjuje vpliv grožnje iz Scenarija tveganja 1. V ostalih dveh primerih pa sta scenarija tveganja zaradi vpliva na zmožnost uporabe interneta in telekomunikacijskih sistemov umeščena v tretjo stopnjo vpliva.

Končna stopnja oziroma vrednost vpliva tveganja na delovanje pomembnih infrastrukturnih sistemov se določi tako, da se vsota posameznih vrednosti iz preglednic 10 in 11 deli s številom upoštevanih vplivov. Vrednost te skupine vplivov je bodisi celo bodisi decimalno število.

Če seštejemo stopnje vplivov iz te skupine in ju delimo s številom upoštevanih vplivov (2), dobimo skupne vrednosti vplivov tveganja na delovanje pomembnih infrastrukturnih sistemov:

- Scenarij tveganja 1: NO,
- Scenarij tveganja 2: 3,
- Scenarij tveganja 3: 3.

9.2.3.3 Merila za ovrednotenje psihosocialnih vplivov tveganja in primerjava z rezultati analiz tveganja

Merila za ovrednotenje psihosocialnih vplivov tveganja in primerjava z rezultati analiz tveganja so opredeljeni v preglednicah 12, 13 in 14.

Preglednica 12: Število ljudi, pri katerih nesreča povzroči nenavadno ali neželeno obnašanje (behavioural reactions), kot npr. izogibanje obiskovanju šol, vrtcev, zavestno odsotnost z dela, zavestno izogibanje javnemu prevozu, težnje po preselitvi, neracionalne finančne operacije (množični dvigi gotovine itn.), kopičenje in prisvajanje zalog življenjskih potrebščin ipd. ter uvrstitev scenarijev tveganja v stopnje vpliva

Število ljudi trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Nad 50.000
Do 2 dni	1	1	1	2
Do 7 dni	1 (S1)	2 (S2, S3)	2	3
Do 15 dni	2	3	3	4
Do 30 dni	3	4	4	5
Več kot 30 dni	4	5	5	5

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva tista, pri kateri je prizadetih največ ljudi in nato tista, ki traja najdlje. Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Realizacija groženj iz kateregakoli scenarija tveganja bi povzročila pritisk na tiste zaposlene, ki so odgovorni za ponovno vzpostavitev normalnega delovanja oziroma poslovanja. Daljši izpadi storitev ali preskrbe lahko povzročijo paniko pri določenem delu prebivalstva. Scenarij tveganja 1 se glede socialnih vplivov ne ocenjuje, glede psiholoških vplivov pa je umeščen v prvo stopnjo vpliva. Scenarija tveganja 2 je glede socialnih vplivov umeščen v prvo stopnjo vpliva, glede psiholoških vplivov pa v drugo stopnjo vpliva. Scenarija tveganja 3 je glede socialnih vplivov umeščen v drugo stopnjo vpliva, glede psiholoških vplivov pa v tretjo stopnjo vpliva.

Preglednica 13: Socialni vplivi in uvrstitev scenarijev tveganja v stopnje vpliva

Vrste socialnih vplivov	Stopnja vpliva	Uvrstitev scenarijev tveganja
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	Se ne ocenjuje (NO)	S1
Majhen/nepomemben vpliv	1	S2
Revnejši sloji prebivalstva se znajdejo v hudi socialni stiski, poveča se število prošenj za izredno denarno socialno pomoč.	2	S3
Posledice nesreče občuti tudi srednji sloj prebivalstva, to se kaže v povečanem številu vlog za izredno denarno socialno pomoč.	3	
Posledice nesreče občuti večina prebivalstva, kar se kaže v velikem povečanju števila vlog za socialno pomoč.	4	
Posledice občutijo vsi prebivalci, kar se kaže predvsem z novimi vlogami za socialno pomoč ter ponovnimi vlogami za dodelitev pomoči.	5	
Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).		

Preglednica 14: Psihološki vplivi in uvrstitev scenarijev tveganja v stopnje vpliva

Vrste psiholoških vplivov	Stopnja vpliva	Uvrstitev scenarijev tveganja
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)	
Majhen/nepomemben vpliv.	1	S1
Pojavljajo se posamezni primeri strahu med prebivalci zaradi nepoznavanja vzrokov in značilnosti nesreče ter njenih posledic.	2	S2
Povečan je pojav strahu med prebivalci, predvsem pred novo nesrečo in njenimi posledicami.	3	S3
Med prebivalci vlada strah za obstanek, zaupanje v pristojne organe, povezane z odzivom ter odpravljanjem posledic nesreče, upade, povečuje se želja po preselitvi.	4	
Zaradi negativnih dogodkov ali posledic nesreče je večina ljudi izgubila zaupanje v to, da bi se življenje na prizadetem območju lahko vrnilo v normalne okvire, pojavlja se množično preseljevanje.	5	
Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).		

Končna stopnja oziroma vrednost psihosocialnih vplivov tveganja se določi tako, da se vsota vrednosti v preglednicah 12, 13 in 14 deli številom upoštevanih vplivov. Vrednost te skupine vplivov je bodisi celo bodisi decimalno število.

Če seštejemo stopnje vplivov iz te skupine in jih delimo s številom upoštevanih vplivov (2 ali 3), dobimo skupne vrednosti psihosocialnih vplivov tveganja:

- Scenarij tveganja 1: 1,
- Scenarij tveganja 2: 1,67,
- Scenarij tveganja 3: 2,33.

9.2.3.4 Merila za ovrednotenje vplivov tveganja na notranjepolitično stabilnost in primerjava z rezultati analiz tveganja

Merila za ovrednotenje vplivov tveganja na notranjepolitično stabilnost in primerjava z rezultati analiz tveganja so v preglednici 15.

Preglednica 15: Vpliv tveganja na notranjepolitično stabilnost in javni red in mir ter uvrstitev scenarijev tveganja v stopnje vpliva

Vrste vplivov	Stopnja vpliva	Uvrstitev scenarijev tveganja
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	Se ne ocenjuje (NO)	
Majhen/nepomemben vpliv.	1	
Pojavljajo se posamezni primeri javnega izražanja nestrinjanja z ukrepanjem pristojnih institucij ali posamezne motnje delovanja političnih institucij (vlada, parlament itn.) ter posamezni pojavi sovražnih kampanj.	2	S1
Znani so posamezni primeri kršitev javnega reda in miru (JRM) ter kaznivih dejanj (KD) zaradi nesreče in izražanje občutka strahu za svojo varnost in premoženje; posamezniki ali skupine skušajo omajati notranjepolitične razmere, zmanjšano je zaupanje prebivalstva v delovanje političnih inštitucij.	3	S2
Povečano je število kršitev javnega reda in miru ter organiziranih kaznivih dejanj, povečan je tudi strah med prebivalstvom; politične stranke in druge interesne skupine skušajo spodkopati notranjepolitično stabilnost ter pridobiti politične koristi z »vsiljevanjem« svojih programov za izboljšanje razmer, zmanjšano je zaupanje v delovanje državnih inštitucij.	4	S3
Kršitve javnega reda in miru, vključno z nasilnimi demonstracijami, so množične, veliko več je kaznivih dejanj, notranja varnost države je ogrožena. Notranjepolitična stabilnost države je spodkopana, temeljne ustavno zagotovljene pravice in vrednote so ogrožene in razvrednotene.	5	
Če se oceni, da vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnje vpliva ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np). Vrednost te skupine vplivov je lahko le celo število.		

Pričakovati je, da bi v primeru realizacije katerekoli grožnje iz scenarijev tveganja, to marsikdo lahko izrabil za (morda tudi upravičeno) kritiko oblasti. Če bi bile razmere v državi že pred tem zaostrene (npr. zaradi ekonomskih ali političnih vzrokov), bi realizacija grožnje lahko sprožila nemire, še posebej, če bi bile njene posledice težje in dolgotrajnejše. V primeru kibernatskih

napadov, sponzoriranih s strani tujih držav, spada povzročanje politične in ekonomske nestabilnosti med glavne cilje takega napada. Scenariji tveganja so glede na povzročene posledice razvrščeni v različne stopnje vpliva, od druge do četrte.

9.2.3.5 Merila za ovrednotenje vplivov tveganja na finančno stabilnost in primerjava z rezultati analiz tveganja

Merila za ovrednotenje vplivov tveganja na finančno stabilnost in primerjava z rezultati analiz tveganja so prikazani v preglednicah 16, 17 in 18.

Preglednica 16: Vpliv na plačilno sposobnost pravnih in fizičnih oseb zaradi nedelovanja plačilnega prometa in uvrstitev scenarijev tveganja v stopnje vpliva

Vrednost izpada / Trajanje izpada	Izpad poravnave plačil v vrednosti, manjši kot 10 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti, med 10 % in 20 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti med 20 % in 50 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti med 50 % in 80 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti, večji kot 80 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj
Ni vpliva, ker vplivi nesreče ne morejo posegati v ocenjevano vsebino	Se ne ocenjuje (NO)	Se ne ocenjuje (NO)	Se ne ocenjuje (NO)	Se ne ocenjuje (NO)	Se ne ocenjuje (NO)
Motnje v plačilnem prometu, ki trajajo do 2 uri	1	1	2	3	3
Motnje v plačilnem prometu, ki trajajo do 4 ure	1	2	2	3	4
Motnje v plačilnem prometu, ki trajajo do 8 ur	2	3	3	4	4
Motnje v plačilnem prometu, ki trajajo ves poslovni dan, ali motnje, ki do konca poslovnega dne niso odpravljene*	3	4	4	5	5
Motnje v plačilnem prometu, ki trajajo več kot en poslovni dan	4	5	5 (S2)	5 (S3)	5

** Motnje ob koncu poslovnega dne, tudi če je obdobje motenj kratko, lahko povzročijo enodnevni zamik poravnave plačil.*

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Pričakovati je, da Scenarij tveganja 1 ne bi vplival na aktivnosti, povezane z ocenjevalno vsebino in se ga zato ne ocenjuje, medtem ko bi lahko imela Scenarija tveganja 2 in 3 velik vpliv nanjo, zato sta obakrat uvrščena v peto stopnjo vpliva.

Preglednica 17: Vpliv na plačilno sposobnost pravnih in fizičnih oseb zaradi pomanjkanja gotovine ter uvrstitev scenarijev in analiz tveganja v stopnje vpliva

Število prizadetih oseb/trajanje	Do 5000	Do 50.000	Več kot 50.000
Do 2 dni	1	2 (S2)	3
Od 2 do 7 dni	2	3	4 (S3)
Več kot 7 dni	3	4	5

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Legenda:

1 – Ni nobenega vpliva oziroma je majhen.
2 – Gotovina je pravnim in fizičnim osebam težje dostopna v njihovem kraju.
3 – Gotovina je pravnim in fizičnim osebam dostopna v sosednjih krajih.
4 – Gotovina je pravnim in fizičnim osebam dostopna v večjih mestih oziroma posameznih krajih.
5 – Gotovina ni dostopna.

Scenarij tveganja 1 na ocenjevano vsebino ne bi imel bistvenega vpliva, zato se ga v tem primeru ne ocenjuje. Scenarij tveganja 2 je uvrščen v drugo stopnjo vpliva, ker bi napad z izsiljevalskim programjem lahko prizadel tudi bančni sektor, Scenarij tveganja 3 pa je uvrščen v četrto stopnjo vpliva predvsem zaradi dolgotrajnejših in obsežnejših prekinitev oskrbe z električno energijo, kar vpliva na delovanje bančnih ustanov, še bolj pa na delovanje denarnih bankomatov.

Preglednica 18: Spremembe rasti BDP zaradi posledic nesreče v letu nesreče ali naslednjem letu in uvrstitev scenarijev tveganja v stopnje vpliva

Sprememba rasti BDP	Stopnja vpliva	Uvrstitev scenarijev tveganja
Ni vpliva, ker vplivi nesreče ne posegajo v vsebino/brez posledic	Se ne ocenjuje (NO)	
Od 0 do -0,5 odstotne točke	1	S1, S2
Do -1 odstotne točke	2	S3
Do -1,5 odstotne točke	3	
Do -2 odstotni točki	4	
Več kot -2 odstotni točki	5	

Če se oceni, da nesreča ne bo imela negativnega vpliva na gibanje BDP oziroma če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnje vpliva ne ocenjuje (NO). Ne upoštevajo se vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Ugotavljamo, da Scenarija tveganja 1 in 2 ne bi bistveno vplivala na rast oziroma padec BDP. Scenarij tveganja 3 pa bi lahko nekoliko bolj vplival na negativno rast BDP, saj bi po oceni povzročil tudi 0,95 % izpad BDP.

Končna stopnja oziroma vrednost vpliva tveganja na finančno stabilnost se določi tako, da se vsota posameznih vrednosti v preglednicah 16, 17 in 18 deli s številom upoštevanih vplivov. Vrednost te skupine vplivov je bodisi celo bodisi decimalno število.

Če seštejemo stopnje vplivov iz te skupine in jih delimo s številom upoštevanih vplivov (3), dobimo skupne vrednosti vplivov tveganja na finančno stabilnost države:

- Scenarij tveganja 1: 1,
- Scenarij tveganja 2: 2,67,
- Scenarij tveganja 3: 3,33.

9.2.3.6 Merila za ovrednotenje vplivov tveganja na zunanjepolitično oziroma mednarodno stabilnost in primerjavo z rezultati analiz tveganja

Merila za ovrednotenje vplivov tveganja na zunanjepolitično oziroma mednarodno stabilnost in primerjavo z rezultati analiz tveganja prikazuje preglednica 19.

Preglednica 19: Zunanjepolitični (mednarodni) vpliv tveganja in uvrstitev scenarijev tveganja v stopnje vpliva

Vrsta zunanjepolitičnega oziroma mednarodnega vpliva	Stopnja vpliva	Uvrstitev scenarijev tveganja
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	Se ne ocenjuje (NO)	
Majhen/nepomemben vpliv.	1	
Ni nobenega večjega neposrednega vpliva na mednarodni položaj države, ki bi bil zaznan. Posamezne tuje države spremljajo dogajanje v RS.	2	
Posamezne (sosednje) države in nekatere regionalne ter mednarodne organizacije se po diplomatski poti odzivajo na dogodek z izražanjem podpore ali zaskrbljenosti zaradi razmer.	3	S1, S2
Del mednarodne skupnosti (države, mednarodne organizacije) se odziva na dogodek z izražanjem močne podpore ali zaskrbljenosti zaradi razmer. ali/in RS je deležna mednarodne pomoči, predvsem v opremi in človeških virih. Kljub mednarodni pomoči je še vedno stabilna država. ali/in Tuja diplomatsko-konzularna predstavništva v RS svojim državljanom odsvetujejo potovanja na nekatera območja v RS.	4	S3
Večji del mednarodne skupnosti se intenzivno odziva na dogodke v državi, saj dogodki močno vplivajo na varnost drugih držav. ali/in RS je deležna večje mednarodne pomoči (oprema, denar, človeški viri). Za normalno delovanje celotnega sistema RS nujno potrebuje pomoč. ali/in Tuja diplomatsko-konzularna predstavništva svojim državljanom odsvetujejo potovanja v RS in zaradi razmer zmanjšujejo ali povečujejo število osebja v predstavništvih. ali/in Mednarodni dogodki, katerih glavna tema je položaj oziroma razmere v RS.	5	
Če se oceni, da vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnje vpliva ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np). *Vrednost te skupine vplivov je lahko le celo število.*		

Scenariji tveganja bi imeli različne stopnje vpliva na zunanjepolitično oziroma mednarodno stabilnost države. Scenarija tveganja S1 in S2 sta uvrščena v tretjo stopnjo vpliva, medtem, ko je scenarij tveganja S3 uvrščen v četrto stopnjo vpliva. Ker gre v tem primeru za sovražno dejanje tuje države, bi bil v primeru dalj časa trajajočih posledic na večini ozemlja države uvrščen v najvišjo, peto stopnjo vpliva. Takrat bi bila država verjetno tudi primorana v večjem obsegu zaprositi za mednarodno pomoč.

9.2.3.7 Končna vrednost oziroma stopnja političnih in družbenih vplivov tveganja

Končna vrednost oziroma stopnja političnih in družbenih vplivov tveganja se določi tako, da se seštejejo končne vrednosti oziroma stopnje vseh skupin političnih in družbenih vplivov tveganja in se delijo s številom skupin vplivov. Če neka skupina političnih in družbenih vplivov tveganja ni bila ocenjena, ker vplivi nesreče ne posegajo v ocenjevalno vsebino (NO), se ta skupina pri končnem izračunu ne upošteva. Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np). V tej oceni so bile ocenjene vse skupine vplivov.

Preglednica 20: Pregled vrednosti oziroma stopenj posameznih skupin vplivov v okviru političnih in družbenih vplivov tveganja

Scenarij	Vrednost prve skupine vplivov	Vrednost druge skupine vplivov	Vrednost tretje skupine vplivov	Vrednost četrte skupine vplivov	Vrednost pete skupine vplivov	Vrednost šeste skupine vplivov	Vsota vrednosti vplivov	Povprečje vrednosti vplivov
Scenarij 1	1,5	NO	1	2	1	3	8,50	1,70
Scenarij 2	1,5	3	1,67	3	2,67	3	14,84	2,47
Scenarij 3	2,5	3	2,33	4	3,33	4	19,16	3,19

Končna izračunana vrednost političnih in družbenih vplivov tveganja je lahko tudi decimalno število. V tem primeru je treba izračunati končno stopnjo političnih in družbenih vplivov tveganja, ki mora biti celo število in za katero je bila uporabljena spodnja preglednica.

Preglednica 21: Pretvorba vrednosti političnih in družbenih vplivov v stopnjo političnih in družbenih vplivov tveganja

Povprečje vrednosti političnih in družbenih vplivov tveganja	Stopnja političnih in družbenih vplivov tveganja
do 1,49	1
1,50 - 2,49	2
2,50 - 3,49	3
3,50 - 4,49	4
4,50 - 5,00	5

Tako lahko izračunamo stopnje političnih in družbenih vplivov tveganja za vse štiri scenarije in analize tveganja.

Preglednica 22: Pretvorba vrednosti političnih in družbenih vplivov scenarijev tveganja v stopnjo političnih in družbenih vplivov tveganja

	Scenarij 1	Scenarij 2	Scenarij 3
Povprečje vrednosti političnih in družbenih vplivov tveganja	1,70	2,47	3,25
Stopnja političnih in družbenih vplivov tveganja	2	2	3

9.2.4 Primerjava rezultatov analiz tveganja z merili za ovrednotenje verjetnosti za realizacijo grožnje

Verjetnost tveganja za realizacijo grožnje je lahko opredeljena bodisi numerično oziroma odstotkovno bodisi opisno, kar je razvidno iz naslednje preglednice.

Preglednica 23: Merila za ovrednotenje verjetnosti za nesreče (realizacijo groženj) in uvrstitev scenarijev tveganja v stopnje verjetnosti

1	2	3	4	5
Enkrat na več kot 250 let (letna verjetnost do 0,4 %). Ni skoraj nobene nevarnosti (grožnje).	Enkrat na 100 do 250 let (letna verjetnost od 0,4 % do 1 %). Mogoča, vendar malo verjetna nevarnost (grožnja).	Enkrat na 25 do 100 let (letna verjetnost od 1 % do 4 %). Mogoča nevarnost (grožnja).	Enkrat na 5 do 25 let (letna verjetnost od 4 % do 20 %). Splošna nevarnost (grožnja).	Enkrat ali večkrat na 5 let (letna verjetnost nad 20 %). Posebna in takojšnja (trajna) nevarnost (grožnja).
		S3	S1	S2
Opisna razlaga se uporablja predvsem za nesreče, ki nimajo nekega naravnega cikla pojavljanja oziroma za namerna dejanja, ki jih je glede na posebnosti pojavljanja nemogoče napovedati (na primer terorizem). Za druge nesreče se upoštevajo v zgornjem delu preglednice navedena časovna obdobja				

Ocenjuje se, da predstavljajo opisani in podobni vplivi tveganja iz Scenarija tveganja 1 splošno nevarnost, vplivi iz Scenarija tveganja 2 posebno in takojšnjo (trajno) nevarnost, vplivi iz Scenarija tveganja 3 pa mogočo nevarnost. Te vrednosti uvrščajo Scenarij tveganja 1 v četrto stopnjo, Scenarij tveganja 2 v peto stopnjo, Scenarij tveganja 3 pa v tretjo stopnjo verjetnosti tveganja za realizacijo grožnje.

9.3 Matrike kibernetskih tveganj

Z matrikami kibernetskih tveganj lahko grafično prikažemo velikost vplivov, ugotovljenih v poglavju 9.2, in verjetnosti tveganja za realizacijo grožnje oziroma posameznih scenarijev tveganja, če obravnavamo le eno tveganje. Matrike kibernetskih tveganj so eden glavnih ciljev pri izdelavi ocen tveganja za posamezne nesreče oziroma v našem primeru grožnje.

Matrike kibernetskih tveganj imajo pet polj na ordinatni osi za prikaz velikosti vplivov tveganja in pet polj na abscisni osi za prikaz stopnje verjetnosti tveganja. Polja so obarvana od zelene do rdeče, pri čemer se stopnje vplivov in verjetnosti stopnjujejo od zelene prek rumene in

oranžne do rdeče barve. Obarvanost polj se hitreje spreminja na ordinatni osi kot na abscisni, kar pomeni, da je v matrikah tveganja za realizacijo grožnje večji poudarek na vplivih tveganja kot na verjetnosti tveganja za realizacijo grožnje. Matrika ima skupaj 25 polj, v katera odvisno od vsebine matrike lahko uvrstimo posamezna tveganja (ali posamezne vplive tveganja) glede na odnos med velikostjo v analizah tveganja ugotovljenih vplivov in merili za ovrednotenje tveganja za realizacijo grožnje. Enako velja tudi za verjetnost tveganja. Kombinacija verjetnosti in vplivov je v matriki kibernetskih tveganj predstavljena v štirih stopnjah, in sicer:

- majhno tveganje z zeleno obarvanimi polji,
- srednje tveganje z rumeno obarvanimi polji,
- veliko tveganje z oranžno obarvanimi polji,
- zelo veliko tveganje z rdeče obarvanimi polji.

Poznamo dve vrsti matrik kibernetskih tveganj:

- matrike tveganja z razdruženim vplivom tveganja (matrika vplivov tveganja na ljudi, matrika gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino, matrika političnih in družbenih vplivov tveganja), vsaka za svoje vrste vplivov in z enovito verjetnostjo;
- matrike tveganja z združenim prikazom vplivov tveganja (matrika tveganja s povprečji vseh treh vplivov tveganja in enovito verjetnostjo).

V obe vrsti matrik tveganja so uvrščene vse analize tveganja na podlagi vseh treh scenarijev tveganja, posebej pa se označi reprezentativna analiza tveganja (na podlagi reprezentativnega scenarija), ki tveganje predstavlja v primerjavah z drugimi tveganji oziroma v nacionalnih matrikah tveganja za nesreče. V oceni tveganja za posamezne grožnje so torej narejene štiri matrike. Reprezentativni scenarij in analiza tveganja sta v matrikah kibernetskih tveganj vpisana s poševno pisavo.

Stopnja skupnega oziroma povprečnega vpliva se izračuna tako, da se seštevek stopnje (1) vplivov tveganja na ljudi, (2) gospodarskih in okoljskih vplivov in vplivov tveganja na kulturno dediščino ter političnih in družbenih vplivov tveganja (3) deli s tri. Če kakšen od vplivov ni bil ocenjen ali ga ni, se tega ne upošteva. Končna izračunana vrednost vplivov je lahko tudi decimalno število. V tem primeru je treba ugotoviti končno stopnjo skupnih (povprečnih) vplivov, ki mora biti celo število.

Preglednica 24: Pretvorba skupne (povprečne) stopnje vplivov tveganja za uvrščanje v polja matrik tveganja z združenim prikazom vplivov

Izračunana vrednost vseh treh vrst vplivov	Stopnja vpliva tveganja v matrikah tveganja z združenim prikazom vplivov tveganja
Do 1,49	1
1,50 - 2,49	2
2,50 - 3,49	3
3,50 - 4,49	4
4,50 - 5,00	5

Ob upoštevanju preglednice tako dobimo končno razvrstitev z vsemi potrebnimi podatki za izračun stopenj vplivov tveganja v matriki tveganja z združenim prikazom vplivov tveganja. V preglednici sta temneje obarvana stolpca, ki sta uporabljena za matriko kibernetskih tveganj z združenim prikazom vplivov tveganja.

Preglednica 25: Izračun povprečnih vplivov tveganja za matrike tveganja z razdruženim in z združenim prikazom vplivov

Scenariji tveganja	Stopnja vplivov na ljudi	Stopnja gospodarskih in okoljskih vplivov in vplivov na kulturno dediščino	Stopnja političnih in družbenih vplivov	Izračunana vrednost skupnih (povprečnih) vplivov	Stopnja skupnih (povprečnih) vplivov tveganja	Verjetnost	Zanesljivost rezultatov analize tveganja
Scenarij tveganja 1	/	1	2	1,50	**2**	**4**	Razmeroma zanesljiva
Scenarij tveganja 2	2	1	2	1,67	**2**	**5**	Srednje zanesljiva
Scenarij tveganja 3	4	3	3	3,33	**3**	**3**	Razmeroma zanesljiva
Reprezenta-tivni scenarij in analiza tveganja (S2)	2	1	2	1,67	**2**	**5**	Srednje zanesljiva

Če je stopnja povprečnih vplivov posameznih analiz ali tveganj več kot dve stopnji nižja kot stopnja vplivov na ljudi, se povprečna stopnja poveča za toliko, da je razlika med stopnjo vplivov na ljudi in povprečno stopnjo dve stopnji. Tako se zagotovi, da ima največjo težo med ugotovljenimi stopnjami vplivov stopnja vplivov tveganja na ljudi. Predvidoma so takšni popravki bolj izjema kot pravilo. V tej oceni tveganja takšnih popravkov ni bilo treba narediti.

V matrikah tveganja za realizacijo posamezne grožnje je zapis scenarija oziroma analize posameznega tveganja glede na zanesljivosti analize vplivov tveganja označen s tremi različnimi barvami, kot sledi iz preglednice.

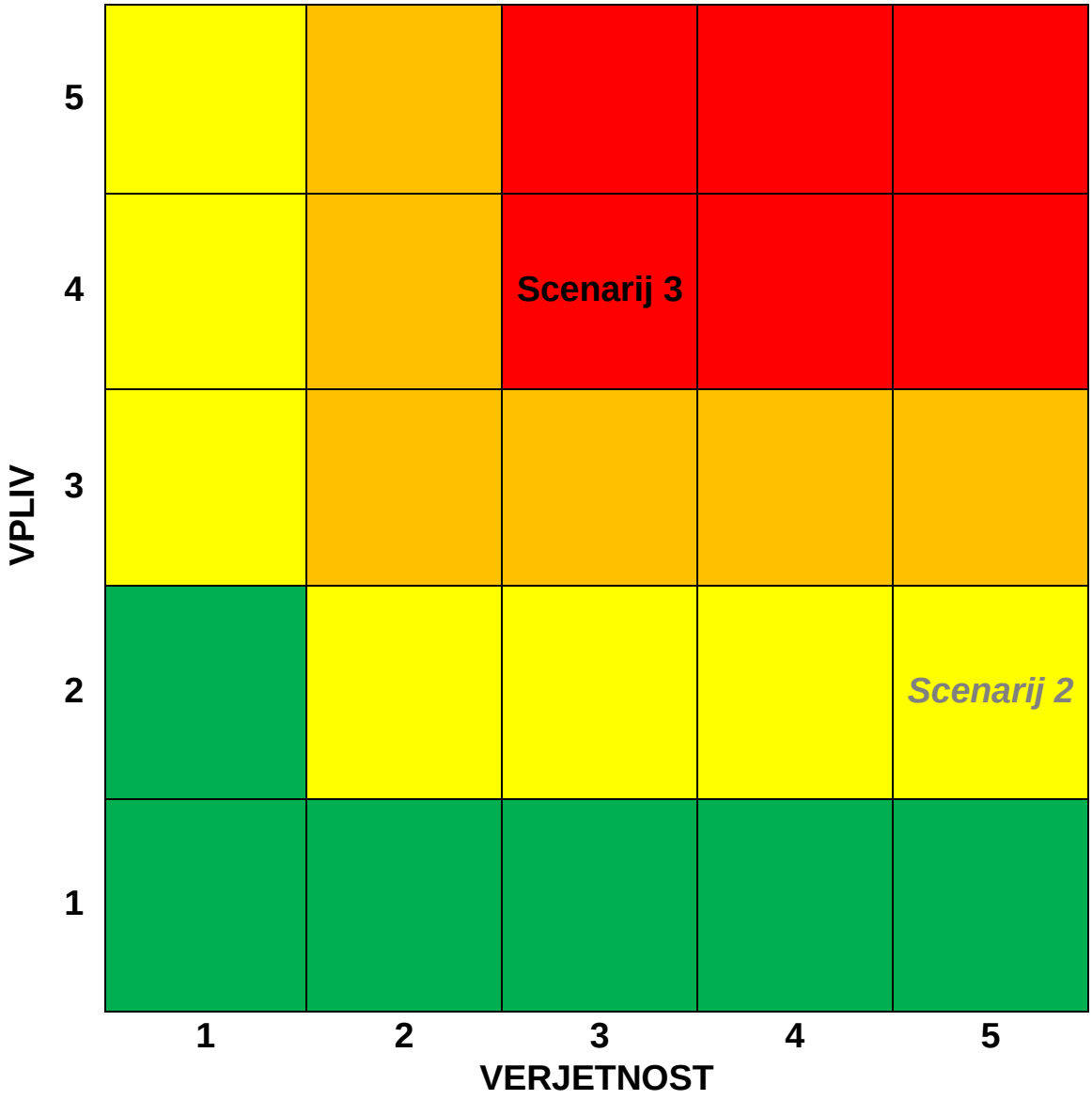
Preglednica 26: Zanesljivost analiz tveganja

Zanesljivost analize tveganja	Barva zapisa ali znaka v matriki tveganja
Razmeroma zanesljiva	Črna ■
Srednje zanesljiva	Temno siva ▩
Razmeroma nezanesljiva	Svetlo siva □

Rezultati analiz tveganja v tej oceni so v enem primeru srednje in v dveh primerih razmeroma zanesljivi.

Iz matrike kibernetskih tveganj z združenim prikazom vplivov, ki predstavlja povprečne vplive analiz tveganja, je razvidno, da je reprezentativni Scenarij tveganja 2 uvrščen v rumeno polje, oziroma drugo stopnjo tveganja od štirih, in torej predstavlja srednjo stopnjo tveganja. Scenarij tveganja 1 prav tako predstavlja srednjo stopnjo tveganja, medtem, ko Scenarij tveganja 3 predstavlja veliko stopnjo tveganja.

Slika 8: Matrika kibernetskih tveganj - Vplivi na ljudi

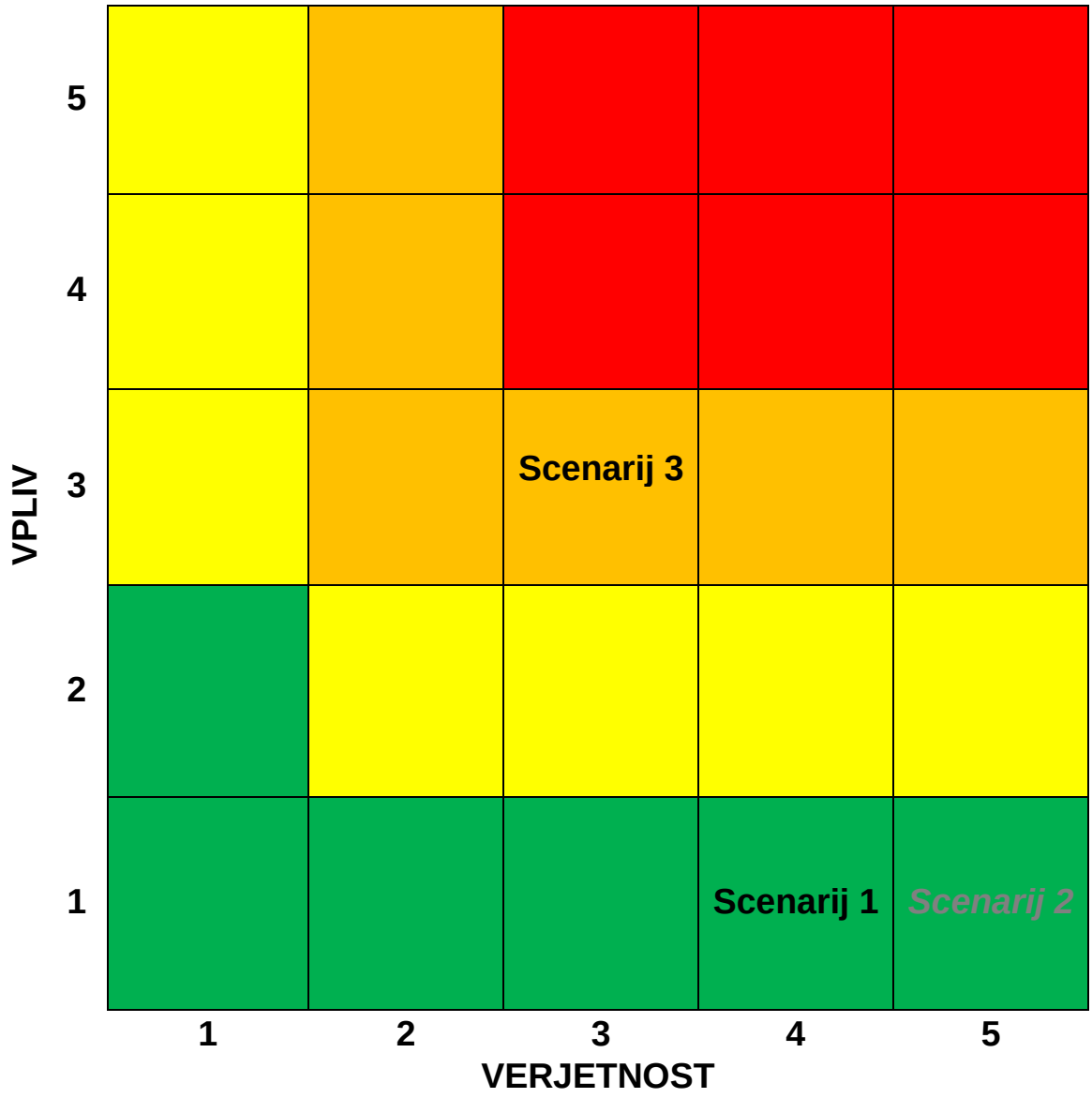


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 9: Matrika kibernetskih tveganj - Gospodarski in okoljski vplivi in vplivi na kulturno dediščino

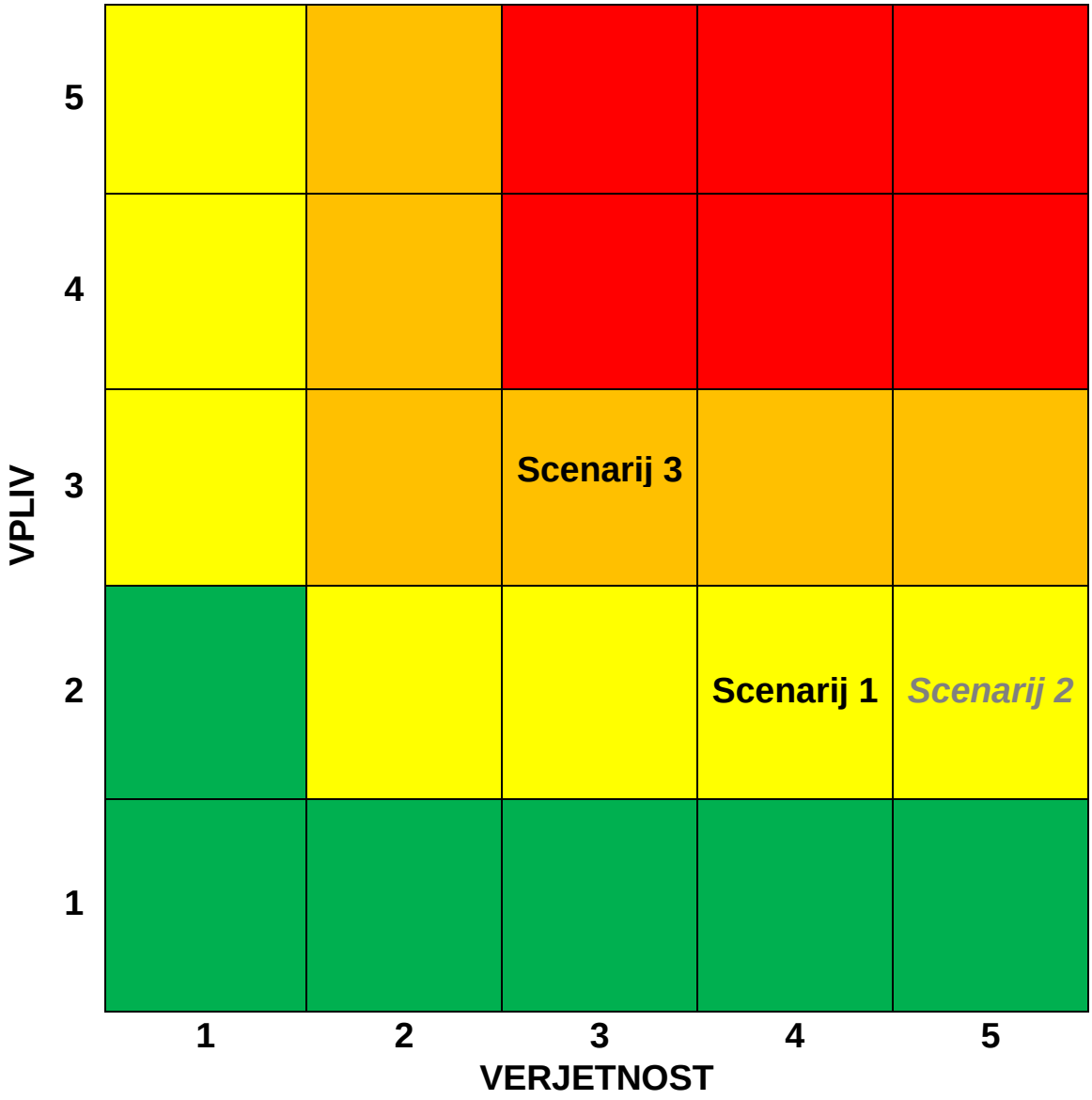


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 10: Matrika kibernetskih tveganj - Politični in družbeni vplivi

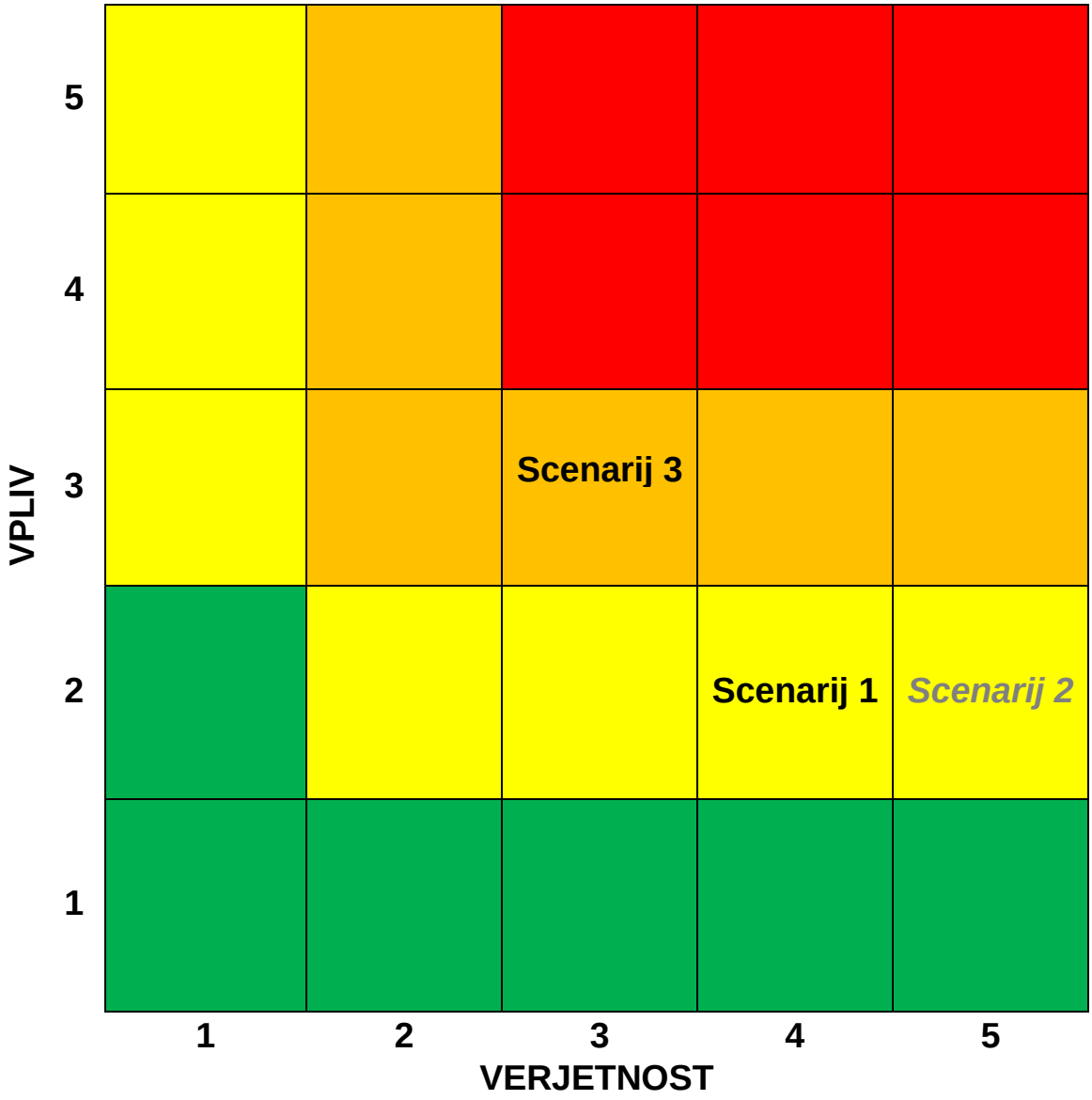


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 11: Matrika kibernetskih tveganj z združenim prikazom vplivov



Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

9.4 Notranja kategorizacija tveganja

Uporabljeni scenariji tveganja za realizacijo posamezne kibernetske grožnje so pripravljeni za uporabo na nacionalni ravni, saj je narava kibernetskih groženj taka, da le-te ne poznajo ne mednarodnih in tudi ne notranjih meja. V primeru scenarijev tveganja 2 in 3 so bile uporabljene po tri slovenske regije samo zaradi lažje ponazoritve. Možno je namreč sklepati, da so regije z višjim BDP na prebivalca dosegle višjo stopnjo digitalizacije in bi jih kibernetski napad (v našem primeru z izsiljevalskim programjem) tudi bolj prizadel. Prav tako je možno sklepati, da bi v primeru državno sponzoriranega napada na kritično infrastrukturo napadalec za dosego čimvečje škode verjetno izbral področja oziroma regije, katere ustvarijo največji delež v BDP države. Oba opisana parametra pa se v času spreminjata in sta v obeh primerih uporabljena samo zaradi lažje ponazoritve. Dejansko je verjetnost kibernetskega napada v okviru države verjetno precej izenačena, zato je treba krepiti kibernetsko odpornost na ravni celotne države. Iz tega razloga kibernetska tveganja niso bila razdelana na nižji (regionalni oziroma občinski) ravni.

10. Povzetek ocene kibernetskih tveganj

Ocena kibernetskih tveganj, ki jo je pripravilo Ministrstvo za javno upravo, je izdelana na podlagi Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite (Uradni list RS, št. 62/14, 13/17), ki je v slovensko zakonodajo prenesla vsebino točke a 6. člena Sklepa št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L št. 347, z dne 20. 12. 2013, str. 924).

Ocena je bila narejena z namenom, da se celovito ugotovijo in opišejo pojavne oblike kibernetskih tveganj in njihove značilnosti. Namen ocene je tudi, da se z analizami tveganja ugotovi, kakšne posledice in v kakšnem obsegu lahko pričakujemo ob uresničitvi izbranih oziroma pripravljenih scenarijev tveganja.

Delovanje in celo sam obstoj sodobne družbe je neločljivo povezan z neprekinjenim in zanesljivim delovanjem informacijskih sistemov in omrežij. Le-ta ogrožajo različne kibernetske grožnje, ki jih izvajajo različni akterji. V oceni je uporabljena klasifikacija kibernetskih groženj, ki jo uporablja evropska agencija za kibernetsko varnost ENISA. Po tej klasifikaciji obstaja 15 različnih kibernetskih groženj:

1. škodljiva koda (Malware),
2. spletni napadi (Web Based Attacks),
3. napadi na spletne aplikacije (Web Application Attacks),
4. zvabljanje (Phishing),
5. nezaželena elektronska pošta (Spam),
6. onemogočanje storitve (Denial of Service),
7. izsiljevalsko programje (Ransomware),
8. botneti,

9. grožnje od znotraj (Insider Threat),
10. fizična manipulacija/poškodba/kraja/izguba (Physical manipulation/damage/ theft/loss),
11. kršitve podatkov (Data Breaches),
12. kraja identitete (Identity Theft),
13. odtekanje informacij (Information leakage),
14. kompleti za izkoriščanje (Exploit Kits) in
15. kibernetsko vohunjenje (Cyber-Espionage).

V letu 2017 so bili primeri škodljive kode najpogostejša oblika kibernetskih groženj, ki se stalno razvija tako glede izpopolnjenosti kot raznolikosti. Z vidika globalnih trendov na področju kibernetskih groženj, so imeli v letu 2017 v svetovnem merilu naraščajoč trend spletni napadi, napadi na spletne aplikacije, zvabljanje, nezaželena elektronska pošta, onemogočanje storitve, izsiljevalsko programje, botneti, kršitve podatkov, kraje identitete, odtekanje informacij in kibernetsko vohunjenje. Škodljiva koda, grožnje od znotraj in fizična manipulacija/ poškodba/kraja/izguba so imeli v letu 2017 stabilen trend, medtem, ko je bil trend kompletov za izkoriščanje padajoč.

Razvoj na področju akterjev kibernetskih groženj je napredoval podobno kot je napredoval razvoj samih kibernetskih groženj. Opazno je povečanje kompleksnosti, izpopolnjenosti in napredka v razvoju zmogljivosti pri večini skupin akterjev. Zaradi uporabe lažnih identitet in prikritega delovanja je vedno težje prepoznati posamezne akterje kibernetskih groženj. Uporabniki prav tako vedno težje ločijo med dobrimi in slabimi akterji, kar vodi k zmanjševanju zaupanja ne samo do komercialnih ponudnikov storitev, ampak celo do institucionalnih deležnikov v kibernetskem prostoru.

Akterji (izvajalci) kibernetskih groženj so:

1. kibernetski kriminalci,
2. osebe znotraj,
3. države,
4. hektivisti,
5. kibernetski bojevniki,
6. kibernetski teroristi in
7. script kiddies.

Z vidika povzročene škode in resnosti posledic so najnevarnejši kibernetski kriminalci in države. V preglednici 27 so prikazane kibernetske grožnje in njihovi akterji. Pri tem so za različne grožnje nekatere skupine akterjev primarne (označeno z rdečo), druge pa sekundarne (označeno z zeleno). Skupine akterjev, ki so primarne za večje število kibernetskih groženj imajo višje razvite zmogljivosti za njihovo izvedbo in obratno.

Preglednica 27: Prikaz kibernetskih groženj in njihovih akterjev. Vir: ENISA, 2018

	Akterji kibernetskih groženj						
Kibernetska grožnja	Kibernetski kriminalci	Osebe znotraj	Države	Hektivisti	Kibernetski bojevniki	Kibernetski teroristi	Script kiddies
Škodljiva koda							
Spletni napadi							
Napadi na spletne aplikacije							
Onemogočanje storitve							
Botneti							
Zvabljanje							
Neželena elektronska pošta							
Izsiljevalsko programje							
Grožnje od znotraj							
Fizična manipulacija/ poškodba/kraja/izguba							
Kompleti za izkoriščanje							
Kršitve podatkov							
Kraja identitete							
Odtekanje informacij							
Kibernetsko vohunjenje							

Legenda	Primarna skupina za grožnje	Sekundarna skupina za grožnje

Akterji kibernetskih groženj za njihovo razširjanje uporabljajo enega ali več vektorjev napada. Vektor napada je sredstvo, s katerim lahko akter kibernetske grožnje zlorabi slabost ali ranljivost na napadenih sredstvih (vključno z ljudmi), da doseže določen cilj. Tako kot pri kibernetskih grožnjah, tudi tukaj obstaja taksonomija vektorjev napada, in sicer:

1. Napad na človeški element,
   - Socialni inženiring,
   - Zvabljanje / usmerjeno zvabljanje / zloraba poslovne e-pošte / zvabljanje visoko pozicioniranih uslužbencev / neželena e-sporočila preko elektronske pošte,

družbenih medijev, spletnih storitev,
    - Zlonamerne priponke e-sporočil,
    - Naslovi zlonamernih spletnih strani, e-pošte in družbenih medijev,
    - Vektorji napada skozi programe Microsoft Office (makro ukazi itd.),
  - Prevare,
    - Prevare na področju tehnične ali uporabniške podpore,
    - Telefonske prevare,
    - SMS prevare,
  - Zbiranje informacij na internetu in v družbenih medijih,
2. Vektorji napada, ki temeljijo na spletu in brskalnikih,
  - Prenosi v mimohodu,
  - Rudarjenje v mimohodu (cryptojacking),
  - Zlonamerne skripte/spletni naslovi,
  - Kompleti za izkoriščanje,
  - Oglaševanje škodljive kode,
  - Napadi na spletne aplikacije (SQL vrivanje),
  - Napadi, ki temeljijo na brskalnikih,
    - Zlonamerni dodatki za brskalnike (posodobitve),
  - Zlorabljene/lažne spletne strani,
3. Sredstva, izpostavljena na internetu,
  - Nezaščitena sredstva, izpostavljena na internetu,
  - Privzete/šibke poverilnice za storitve,
  - Ponovna uporaba gesel,
4. Izkoriščanje ranljivosti/napačnih nastavitev in napak kriptografskih, omrežnih, varnostnih protokolov,
5. Napadi v dobavni verigi,
6. Razširjanje po omrežju,
7. Aktivni omrežni napadi,
  - DNS napadi (DNS ugrabitev / zastrupitev),
8. Pasivni omrežni napadi,
  - Vohljanje v brezžičnem omrežju (WiFi-Sniffing),
9. Odtekanje podatkov,
10. Napadi z zavajanjem (smokescreen attacks),
11. Trgovine za mobilne aplikacije,
12. Zlonamerne USB naprave,
13. Snemanje kartic.

Za pripravo ocene kibernetskih tveganj so bili izbrani scenariji tveganja, ki predstavljajo tri primere, kjer kibernetske grožnje realizirajo različni akterji. V vseh treh primerih gre za onemogočenje poslovanja oziroma izvajanja storitev. V prvem scenariju gre za napad na spletišča državne uprave (v resničnem primeru ga je izvedla hektivistična skupina), v drugem za napad z izsiljevalskim programjem (v resničnem primeru so ga izvedli kibernetski kriminalci) in v tretjem za napad na kritično infrastrukturo v energetskem sektorju (v resničnem primeru ga je izvedla suverena država). Stopnja tveganja, negativni vplivi in resnost posledic v uporabljenih scenarijih so različne. Pri tem smo se omejili na osnovne scenarije brez dodatne kompleksnosti, ki jo prinese vzajemno delovanje več različnih kibernetskih groženj ali njihovih akterjev ter samo na neposredne vplive in posledice realiziranih groženj. V nasprotnem primeru bi bili negativni vplivi in posledice neprimerno večji. Vsi trije scenariji temeljijo na dejanskih incidentih, od katerih se je prvi zgodil v Sloveniji, drugi je imel svetovne razsežnosti, vključno s Slovenijo, tretji pa v Ukrajini. Ocene vplivov vseh treh scenarijev se nanašajo na Republiko Slovenijo, pri izračunih ocenjenih škod pa so bili uporabljeni podatki za leto 2016.

Scenarij tveganja 1: Napad na spletišča državne uprave je dokaj verjeten in bi bil lahko spodbujen z opredelitvijo države do političnih, ekonomskih in ekoloških vprašanj (npr. priznanje novih držav, sodelovanje pri ekonomskih, političnih ali vojaških sankcijah proti kateri od držav, sodelovanje v vojaških konfliktih, opredelitev do trgovinskih in ekoloških sporazumov itd.). Najverjetnejša akterja kibernetske grožnje v tem primeru so hektivisti in države.

Scenarij tveganja 2: Napad z izsiljevalskim programjem je zelo verjeten, saj na ta način kriminalne združbe lahko monetizirajo svoje aktivnosti, drugi akterji kibernetskih groženj (npr. države) pa posredno in prikrito z onemogočanjem delovanja podjetij in organizacij dosežejo svoje cilje. Dober primer je bil uspeh virusa WannaCry v letu 2017. Glavni cilj kriminalcev so sicer organizacije v javnem in zasebnem sektorju, a so žrtve lahko tudi posamezniki. Najverjetnejši akter kibernetske grožnje v tem primeru so kibernetski kriminalci, lahko tudi v povezavi z državami.

Scenarij tveganja 3: Napad na kritično infrastrukturo je zaradi nevpletenosti države v politične ali vojaške konflikte sicer najmanj verjeten, a bi bile posledice njegove izvedbe najhujše, sploh če upoštevamo, da bi onemogočanje preskrbe z električno energijo v sektorju energetike vplivalo na takorekoč vse ostale sektorje kritične infrastruktre. Tukaj bi bil kibernetski napad, verjetno kot del hibridne grožnje, lahko spodbujen npr. zaradi sodelovanja države v vojaškem konfliktu. Najverjetnejši akter kibernetske grožnje v tem primeru so države.

Opisano velja za Slovenijo, obravnavano samostojno. Verjetnost opisanih scenarijev pa bi se lahko povečala, ko bo država v drugi polovici leta 2021 predsedovala Svetu Evropske unije in bi napad nanjo lahko simbolično pomenil tudi napad na Evropsko unijo.

Uporabljeni scenariji tveganja so razmeroma zanesljivi, saj izhajajo iz preteklih resničnih kibernet-skih incidentov, kot reprezentativni scenarij tveganja pa je bil izbran scenarij tveganja 2: Napad z izsiljevalskim programjem, ki mu je bilo v oceni namenjeno tudi največ pozornosti.

V scenariju tveganja 1 so na primeru nedostopnosti državnih portalov eDavki in eVEM prikazane posledice kibernetskega napada z onemogočanjem storitve. V takem primeru bi najverjetneje šlo za napad DDoS. Ocenjena skupna škoda pri uporabnikih portalov in državnih organih zaradi izpada storitev znaša blizu 5.600.000 EUR. Scenarij tveganja 1 je po obsegu posledic še sprejemljiv. V njemu opisan kibernetski napad bi vsekakor opozoril na napadalca oziroma njegove zahteve, neglede ali bi šlo za hektivistično skupino ali državo. Obseg posledic pa bi bil lahko tudi neprimerno večji, če bi napad obsegal spletišča vseh državnih in paradržavnih organov in organizacij.

V scenariju tveganja 2 so na primeru treh slovenskih statističnih regij z najvišjim BDP na prebivalca (osrednjeslovenska in obalno-kraška regija ter regija jugovzhodna Slovenija), ki skupno ustvarijo 49 % BDP države, prikazane posledice napada z izsiljevalskim programjem po vzoru na izsiljevalski virus WannaCry leta 2017. Omenjene regije so bile izbrane zaradi predpostavke, da je stopnja digitalizacije višja v okoljih, ki dosegajo višjo dodano vrednost. V takih okoljih bi napad z izsiljevalskim programjem lahko imel največje posledice. V oceni je uporabljena predpostavka, da bi zaradi napada prišlo do izpada proizvodnje in storitev za pet delovnih dni in da bi skupna povzročena škoda, ki bi jo utrpela prizadeta podjetja in organizacije znašala 15 % ustvarjenega BDP v teh regijah v dnevih izpada. V našem primeru bi ocenjena skupna neposredna škoda zaradi izpada proizvodnje in storitev znašala 57.820.000. EUR. Ocenjuje se, da bi izpad na daljši rok lahko povzročil do 50 bolnih ljudi. To bi veljalo, če ne bi prišlo do trajne izgube podatkov in bi bila obnovitev poslovanja normalna. Če pa bi v določenih subjektih prišlo do delne ali popolne izgube podatkov, bi to lahko v najslabšem primeru privedlo tudi do propada takega subjekta. Opisani scenarij je po obsegu posledic še sprejemljiv. Scenarij na eni strani vsebuje nekatere predpostavke, ki so pri oceni vplivov in posledic na spodnji meji, kot je npr. dokaj kratko obdobje izpada zaradi delovanja grožnje in povrnitve v normalno stanje (5 dni), omejeno število prizadetih (skupna škoda 15 % BDP, ki bi bil ustvarjen v času izpada) ter zaradi lažje predstavitve omejitev na samo tri statistične regije. Na drugi strani pa je na mestu tudi predpostavka, da so ozaveščenost in varnostni ukrepi, tudi zaradi izkušnje z virusom WannaCry, na višji stopnji kot v preteklosti. Pričakovati pa je, da se bo v prihodnosti izpostavljenost zaradi vedno višje stopnje digitalizacije in večje uporabe izsiljevalskega programja povečevala.

V scenariju tveganja 3 so na primeru treh slovenskih statističnih regij z največjim deležem v BDP države (osrednjeslovenska, podravska in savinjska regija), ki skupno ustvarijo 61 % slovenskega BDP, prikazane posledice koordiniranega napada na elektro distribucijski sistem po vzoru na resničen napad na podoben sistem v Ukrajini leta 2015. V scenariju je uporabljena predpostavka, da bi napad povzročil skupno pet delovnih dni izpada preskrbe z električno energijo, ko bi bila popolnoma onemogočena proizvodnja in izvajanje storitev. Ocenjena skupna neposredna škoda zaradi izpada proizvodnje in storitev bi znašala 383.960.000 EUR. Ocenjuje se, da bi izpad lahko povzročil do 20 smrtnih žrtev ter do 250 ranjenih oziroma bolnih. Opisani scenarij je po obsegu posledic še sprejemljiv. Scenarij sicer vsebuje nekatere predpostavke, ki so pri oceni vplivov in posledic na spodnji meji, kot je npr. dokaj kratko obdobje izpada zaradi delovanja grožnje in povrnitve v normalno stanje (5 dni) ter zaradi lažje

predstavitve omejitev na samo tri statistične regije Tudi v tem primeru se bo izpostavljenost v prihodnosti zaradi vedno višje stopnje digitalizacije z uporabo pametnih omrežij povečala. Kljub temu je glede na trenutni ekonomsko politični položaj in neizpostavljenost države verjetnost realizacije grožnje iz scenarija tveganja 3 dokaj nizka.

Ocenjuje se, da predstavljajo opisani in podobni vplivi tveganja iz Scenarija tveganja 1 splošno nevarnost, vplivi iz Scenarija tveganja 2 posebno in takojšnjo (trajno) nevarnost, vplivi iz Scenarija tveganja 3 pa mogočo nevarnost. Te vrednosti uvrščajo Scenarij tveganja 1 v četrto stopnjo, Scenarij tveganja 2 v peto stopnjo, Scenarij tveganja 3 pa v tretjo stopnjo verjetnosti tveganja za realizacijo grožnje.

Ker se celovit nacionalni sistem zagotavljanja kibernetske in informacijske varnosti šele vzpostavlja, na žalost še ne obstajajo potrebni podatki za celovitejše analize. Ko bodo konec leta 2018 določeni zavezanci po ZInfV, ki bodo morali priglašati kibernetske incidente s pomembnim vplivom na neprekinjeno izvajanje njihovih storitev, bo postopno na voljo tudi več podatkov tako o kibernetskih grožnjah kot tudi o potencialnih akterjih teh groženj. Na osnovi teh podatkov bo lažje pripraviti ustrezne in zanesljivejše analize. Analize v tej oceni pa so narejene na podlagi trenutnih (z)možnosti. Ne glede na to lahko trdimo, da so analize tveganja srednje do razmeroma zanesljive.

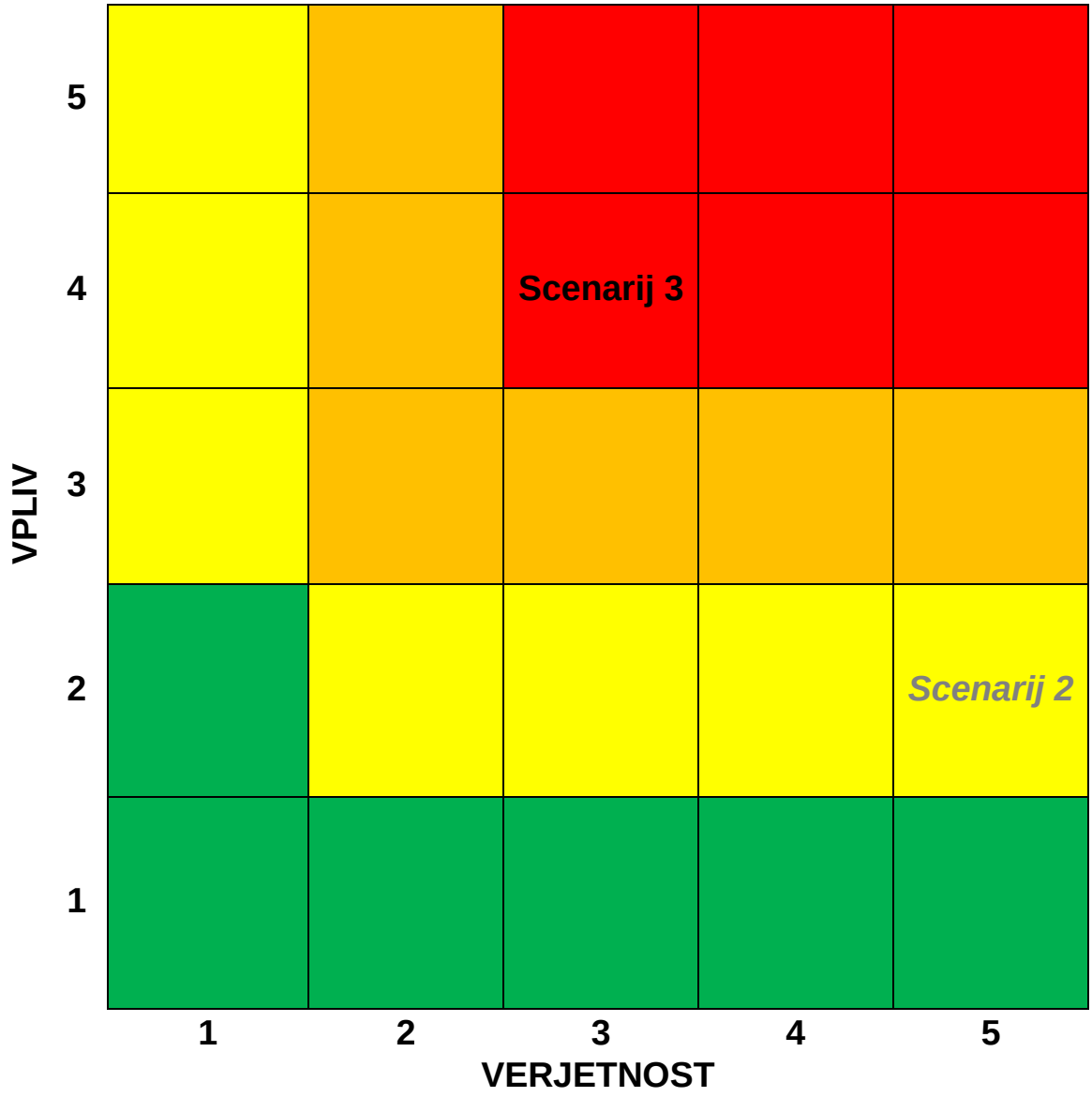
V nadaljevanju so v matrikah kibernetskih tveganj ovrednoteni vplivi tveganj iz posameznih scenarijev tveganj. Pri tem so vplivi prikazani tako v matrikah tveganja z razdruženim vplivom tveganja (matrika vplivov tveganja na ljudi, matrika gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino, matrika političnih in družbenih vplivov tveganja), vsaka za svoje vrste vplivov in z enovito verjetnostjo, kot tudi v matriki tveganja z združenim prikazom vplivov tveganja (matrika tveganja s povprečji vseh treh vplivov tveganja in enovito verjetnostjo).

Izračun povprečnih vplivov tveganja za matrike kibernetskega tveganja z razdruženim in z združenim prikazom vplivov je prikazan v preglednici 28.

Preglednica 28: Izračun povprečnih vplivov tveganja za matrike tveganja z razdruženim in z združenim prikazom vplivov

Scenariji tveganja	Stopnja vplivov na ljudi	Stopnja gospodarskih in okoljskih vplivov in vplivov na kulturno dediščino	Stopnja političnih in družbenih vplivov	Izračunana vrednost skupnih (povprečnih) vplivov	Stopnja skupnih (povprečnih) vplivov tveganja	Verjetnost	Zanesljivost rezultatov analize tveganja
Scenarij tveganja 1	/	1	2	1,50	**2**	**4**	Razmeroma zanesljiva
Scenarij tveganja 2	2	1	2	1,67	**2**	**5**	Srednje zanesljiva
Scenarij tveganja 3	4	3	3	3,33	**3**	**3**	Razmeroma zanesljiva
Reprezenta-tivni scenarij in analiza tveganja (S2)	2	1	2	1,67	**2**	**5**	Srednje zanesljiva

Slika 12: Matrika kibernetskih tveganj - Vplivi na ljudi

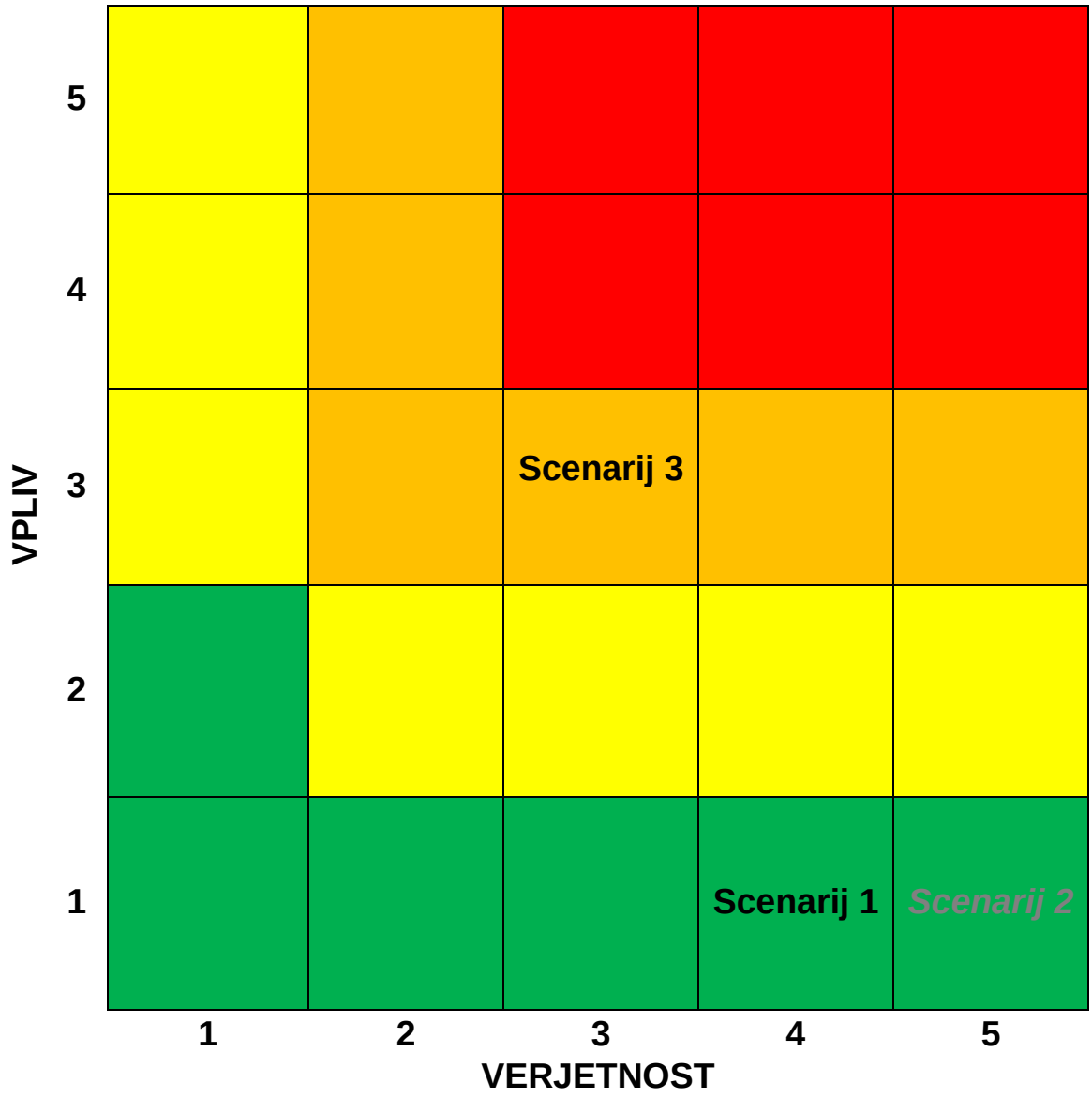


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 13: Matrika kibernetskih tveganj - Gospodarski in okoljski vplivi in vplivi na kulturno dediščino

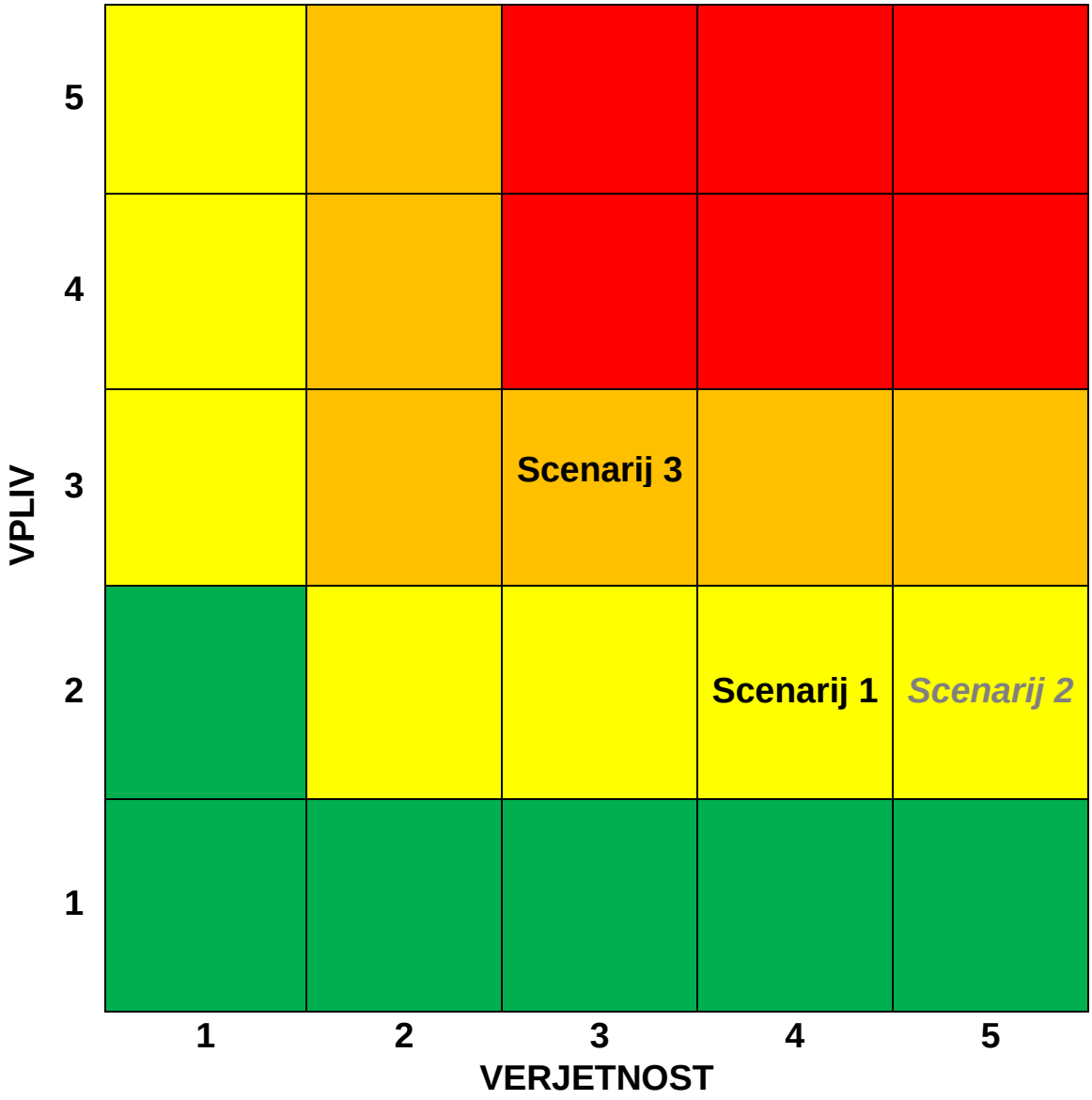


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 14: Matrika kibernetskih tveganj - Politični in družbeni vplivi

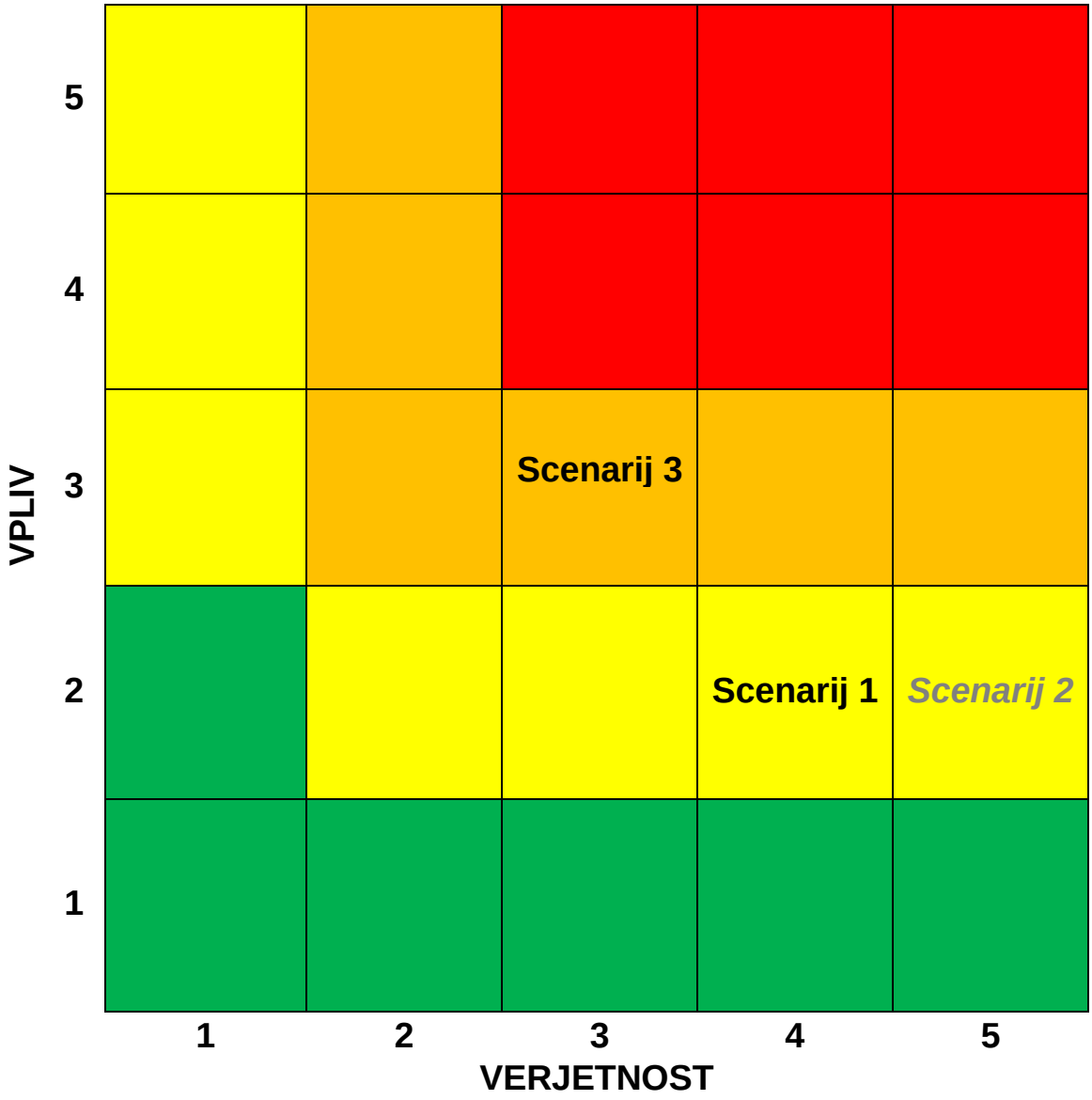


Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

Slika 15: Matrika kibernetskih tveganj z združenim prikazom vplivov



Stopnje vplivov in verjetnosti	
5	Zelo velika
4	Velika
3	Srednja
2	Majhna
1	Zelo majhna

Stopnje tveganja	
	Zelo velika
	Velika
	Srednja
	Majhna

Zanesljivost rezultatov analiz tveganja	Barva zapisa v matriki tveganja
Razmeroma zanesljiva	Črna
Srednje zanesljiva	Temno siva
Razmeroma nezanesljiva	Svetlo siva

11. Zaključek

Namen ocene je bil poleg ocenitve realnih tveganj za realizacijo različnih kibernetskih groženj tudi dvig ozaveščenosti o izredni pomembnosti zagotavljanja kibernetske in širše informacijske varnosti ter o potencialnih kibernetskih grožnjah, ki to varnost ogrožajo. Če bo izpolnila ta cilj, bo velik del njenega namena dosežen.

V oceni uporabljeni scenariji kibernetskih tveganj so morda izbrani nekoliko arbitrarno, vendar predstavljajo realno stanje v času nastajanja. Zaradi vedno več poskusov vplivanja na demokratične procese v posameznih državah tudi preko kibernetskega prostora ter zaradi geopolitičnih sprememb v svetu, bo Slovenija v prihodnje lahko zaradi različnih razlogov postala zanimiva tudi za poskuse vplivanja na njene demokratične procese ter za napade na njeno kritično infrastrukturo, kot je nakazano v uporabljenem Scenariju tveganja 3. Zato bi bilo smiselno in potrebno, da bi se naslednja ocena kibernetskih tveganj posvetila tema dvema grožnjama, ki bi lahko imeli dolgoročne negativne posledice za državo.

Priprava podobnih pregledov in ocen bi morala postati stalna praksa pristojnega nacionalnega organa za informacijsko varnost, seveda, ko bodo za to izpolnjeni nekateri pogoji, v prvi vrsti povezani s kadrovskimi viri. Ko bo nacionalni sistem informacijske varnosti v celoti deloval, bo imel organ na strateški ravni na voljo vse informacije iz operativne ravni sistema, pa tudi od podobnih organov po EU in še od kod. Zagotavljanje kibernetske in širše tudi informacijske varnosti, je izrednega pomena za nacionalno varnost. Skladno s tem mora država področju informacijske varnosti nameniti neprimerno več pozornosti kot doslej in resnično tudi tukaj stopiti v korak z najboljšimi. Morda bo pravšnji prvi korak kar čimprejšnji pričetek izvajanja vseh ukrepov in določb iz Strategije kibernetske varnosti ter Zakona o informacijski varnosti.

12. Razlaga pojmov, kratic in krajšav

ACTA	Anti-Counterfitting Trade Agreement (Trgovinski sporazum za boj proti ponarejanju)
AJPES	Agencija Republike Slovenije za javnopravne evidence in storitve
AKOS	Agencija za komunikacijska omrežja in storitve Republike Slovenije
APT	Advanced Persistent Threat (Napredna trajna grožnja)
BDP	Bruto družbeni proizvod
BND	Bruto nacionalni dohodek
CCaaS	Cyber Crime as a Service (Storitev kibernetskega kriminala)
CERT	Computer Emergency Response Team
CMS	Content Management System (Sistem za upravljanje vsebin)
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service (Distribuiran napad onemogočanja storitve)
DNS	Domain Name Server (Strežnik domenskih imen)
DoS	Denial of Service (Napad onemogočanja storitve)
ENISA	Evropska agencija za kibernetsko varnost
eVEM	Elektronska oblika točke VEM (Vse na Enem Mestu)
FU	Finančna uprava
HKOM	Skupno komunikacijsko omrežje organov in organizacij državne uprave
IKT	Informacijsko komunikacijska tehnologija
MADJACK	Medical Device Hijack (Napad na medicinske naprave)
MJU	Ministrstvo za javno upravo
PDoS	Permanent Denial of Service (Stalno onemogočenje storitve)
RSA	Algoritem za šifriranje z javnim ključem
SCADA	Supervisory control and data acquisition (Sistem za nadzor in pridobivanje podatkov)
SI-CERT	Nacionalni odzivni center za omrežne incidente
SLA	Service Level Agreement
SOVA	Slovenska varnostno obveščevalna agencija
SQL	Structured Query Language (Strukturirani povpraševalni jezik)
SURS	Statistični urad Republike Slovenije
URSZR	Uprava Republike Slovenije za zaščito in reševanje
UVTP	Urad Vlade RS za varovanje tajnih podatkov
WannaCry	Izsiljevalski virus
WiFi	Brezžično računalniško omrežje

WTO	Svetovna trgovinska organizacija
ZEKom-1	Zakona o elektronskih komunikacijah
Zero-day	Ranljivost programske ali strojne opreme, ki še ni bila odkrita oziroma javno objavljena
ZinfV	Zakon o informacijski varnosti

13. Viri

[1] Ban, V. WannaCry - vse, kar morate vedeti [online]. Ljubljana: Smart Com d.o.o., 2017, [ogled avgust 2018]. Dostopno na: http://www.smart-com.si/wp-content/uploads/2017/05/WannaCry_vse_kar_morate_vedeti_e-knjiga.pdf

[2] CERT.hr. Analiza WannaCry ransomwarea: NCERT-PUBDOC-2018-1-354 [online]. Zagreb: CERT.hr, 2017, [ogled avgust 2018]. Dostopno na: https://www.cert.hr/wp-content/uploads/2018/02/WannaCry.pdf

[3] Cyber Risk Outlook 2018 [online]. Newark: Risk Management Solutions, Inc., 2018, [ogled avgust 2018]. Dostopno na: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf

[4] ENISA. ENISA Threat Landscape Report 2017 [online]. Heraklion: ENISA, 2018, [ogled julij 2018]. Dostopno na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[5] Kelly, S. et al. Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy [online]. Cambridge: Centre for Risk Studies, University of Cambridge, 2016, [ogled avgust 2018]. Dostopno na: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf

[6] Podrobnejša vsebina ocen tveganja za posamezne nesreče s prilogami, različica 3 [online]. Ljubljana: Ministrstvo za obrambo Republike Slovenije – Uprava za zaščito in reševanje, 2017, [ogled avgust 2018]. Dostopno na: http://www.sos112.si/slo/page.php?src=os17.htm

[7] SANS. Analysis of the Cyber Attack on the Ukrainian Power Grid [online]. Washington: SANS, 2016, [ogled avgust 2018]. Dostopno na: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[8] SI-CERT. Poročilo o omrežni varnosti za leti 2016 in 2017 [online]. Ljubljana: Arnes, 2018, [ogled avgust 2018]. Dostopno na: https://www.cert.si/wp-content/uploads/2018/04/SI-CERT_LP_2016_2017.pdf

[9] SI-CERT. Poročilo o omrežni varnosti za leto 2012 [online]. Ljubljana: Arnes, 2013, [ogled avgust 2018]. Dostopno na: https://www.cert.si/wp-content/uploads/2017/08/SI-CERT_porocilo_2012.pdf

[10] Smart, W. Lessons learned review of the WannaCry Ransomware Cyber Attack [online]. London: Skipton House, 2018, [ogled avgust 2018]. Dostopno na: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

[11] SURS. Statistični portal STAGE [online]. Ljubljana: SURS, 2018, [ogled avgust 2018]. Dostopno na: http://gis.stat.si/

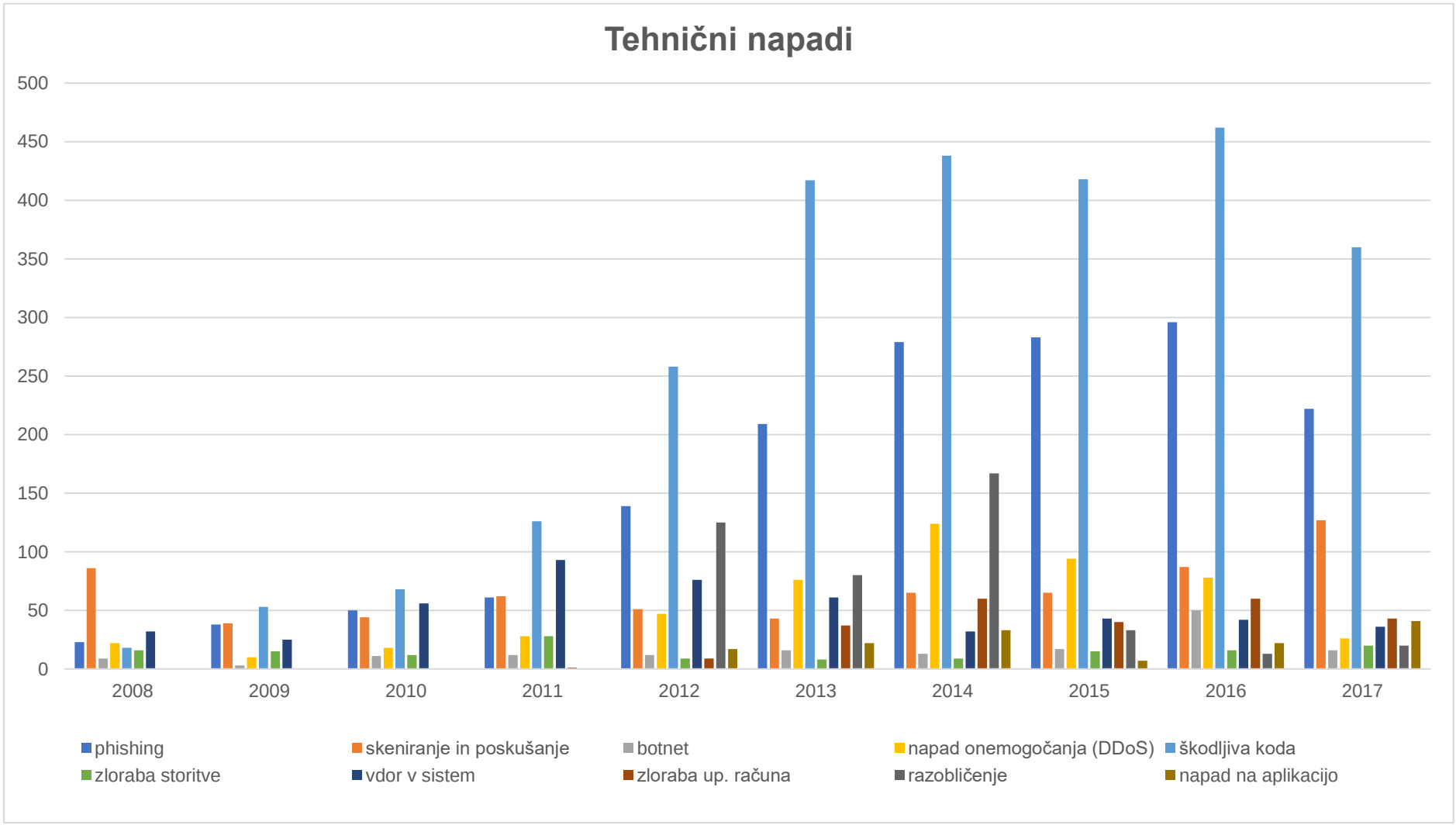
[12] Šipec, S. Ocena tveganja za žled [online]. Ljubljana: Ministrstvo za obrambo Republike Slovenije – Uprava za zaščito in reševanje, 2016, [ogled avgust 2018]. Dostopno na: http://www.sos112.si/slo/tdocs/ocena_tveganja_zled_v2.pdf

[13] Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite [online]. Uradni list RS, št. 62/14 in 13/17) [ogled avgust 2018]. Dostopno na: http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED6795

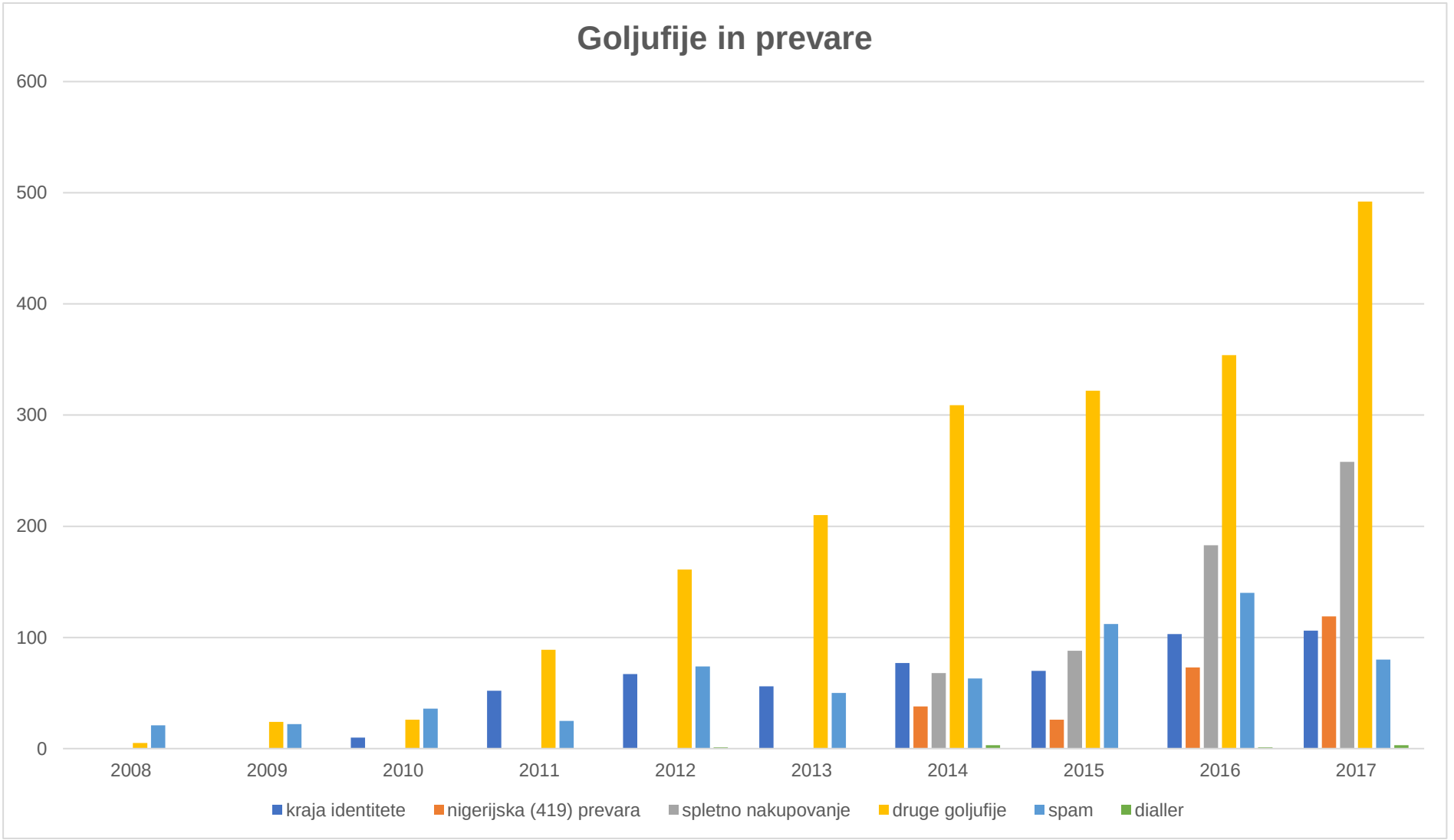
14. Priloge

- Prikaz incidentov iz skupine tehnični napadi v obdobju od 2008 do 2017,
- Prikaz incidentov iz skupine goljufije in prevare v obdobju od 2008 do 2017,
- Prikaz mesečnih prijav incidentov z izsiljevalskimi virusi v obdobju od aprila 2012 do januarja 2018,
- Bruto domači proizvod po izbranih statističnih in kohezijskih regijah v letu 2016,
- Tri slovenske statistične regije z največjim BDP na prebivalca v letu 2016, uporabljene v scenariju 2,
- Tri slovenske statistične regije z največjim deležem v BDP države v letu 2016, uporabljene v scenariju 3.

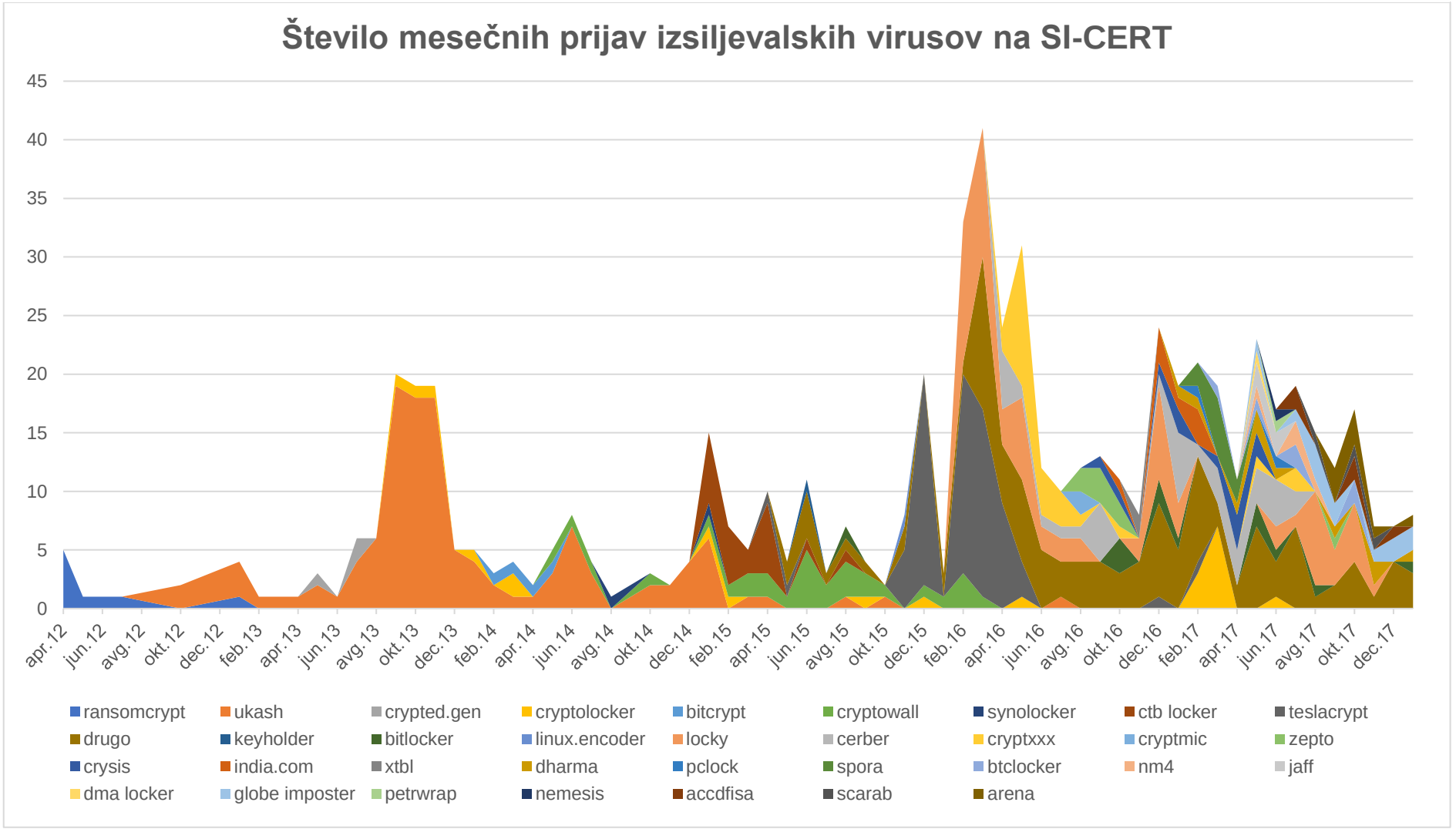
Slika 16: Prikaz incidentov iz skupine tehnični napadi v obdobju od 2008 do 2017. Vir: SI-CERT, 2018



Slika 17: Prikaz incidentov iz skupine goljufije in prevare v obdobju od 2008 do 2017. Vir: SI-CERT, 2018



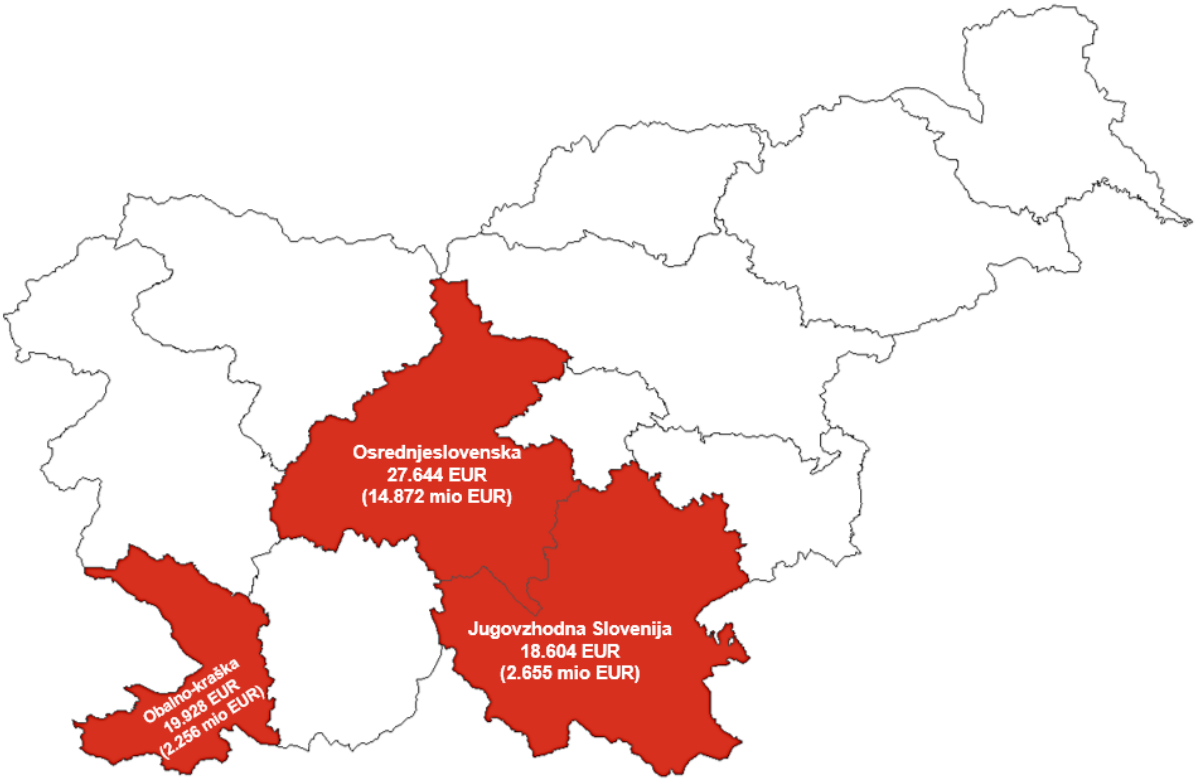
Slika 18: Prikaz mesečnih prijav incidentov z izsiljevalskimi virusi v obdobju od aprila 2012 do januarja 2018. Vir: SI-CERT, 2018



Preglednica 29: Bruto domači proizvod po statističnih in kohezijskih regijah v letu 2016. Vir: SURS, 2018

Statistična / kohezijska regija	Mio. EUR	EUR / prebivalca	Število prebivalcev	Delež v SLO	Število ranljivih	Delež v SLO	Število podjetij	Delež v SLO
Vzhodna Slovenija	**17.653**	**16.169**						
Pomurska	1533	13.232						
Podravska	5170	16.078	322.553	15,6%	105.428	15,4%	26.125	13,3%
Koroška	1121	15.781						
Savinjska	4589	18.006	254.318	12,3%	83.663	12,2%	21.490	11,0%
Zasavska	600	10.443						
Posavska	1227	16.202						
Jugovzhodna Slovenija	2.655	18.604	142.566	6,9%	47.038	6,9%	10.378	5,3%
Primorsko-notranjska	758	14.412						
Zahodna Slovenija	**22.765**	**23.401**						
Osrednjeslovenska	14.872	27.644	537.023	26,0%	177.687	25,9%	65.412	33,4%
Gorenjska	3518	17.269						
Goriška	2119	17.968						
Obalno-kraška	2256	19.928	113.070	5,5%	37.458	5,5%	13.855	7,1%

Slika 19: Tri slovenske statistične regije z največjim BDP na prebivalca v letu 2016, uporabljene v scenariju 2. Vir: SURS, 2018



Slika 20: Tri slovenske statistične regije z največjim deležem v BDP države v letu 2016, uporabljene v scenariju 3. Vir: SURS, 2018