VPLIV PANDEMIJE COVID-19 NA KIBERNETSKO VARNOST: ANALIZA STANJA S PRIPOROČILI ZA MALA PODJETJA

ALENKA BREZAVŠČEK
Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija
E-pošta: alenka.brezavscek@um.si

Povzetek V prispevku smo se osredotočili na problematiko pandemije COVID-19 z vidika njenega vpliva na kibernetsko varnost. V prvem delu smo podali celovit pregled obstoječe literature. Analizirali smo ključne vzroke za porast kibernetskega kriminala v obdobju pandemije ter izpostavili kibernetske napade, ki so se najbolj razmahnili. Povzeli smo, katere gospodarske dejavnosti so najbolj prizadete kakor tudi geografsko razpršenost s COVID-19 povezanih kibernetskih napadov. V drugem delu smo razvili smernice za obvladovanje kibernetskih tveganj, ki so ključni doprinos prispevka. Smernice smo zasnovali na ogrodju NIST CSF, pri čemer smo jih prilagodili segmentu MSP in tudi dopolnili z aktivnostmi, ki so za učinkovito obvladovanje kibernetskih tveganj v času pandemije ključnega pomena. Smernice so uporabne za vse organizacije, predvsem pa so dobrodošle za mikro in mala podjetja, kjer se običajno soočajo z zelo omejenimi resursi, predvsem z vidika ustreznih znaj in kompetentnega kadra s področja kibernetske varnosti.

Ključne besede:
kibernetska varnost,
pandemija COVID-19,
vpliv,
mala podjetja,
smernice

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-509-2.6
ISBN 978-961-286-509-2

Impact of COVID-19 Pandemic on Cybersecurity: An Overview with Recommendations for Small Sized Business

Alenka Brezavšček
University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
E-mail: alenka.brezavscek@um.si

Abstract This paper addresses the topic of COVID-19 pandemic in terms of its impact on cybersecurity. In the first part, a comprehensive literature review is provided. Specific circumstances that influenced the rise of cybercrime during the pandemic are highlighted. Besides, the main types of cyberattacks associated with COVID-19 are discussed and the intensity of COVID-19 related cybercrime according to the business sector and geographic distribution is presented. The main contribution of the paper is our guidelines for cybersecurity risk management, which are listed in the second part of the paper. The guidelines are based on the NIST CSF framework, but have been adapted to the SME environment, and expanded to include activities for securing the organization against pandemic-related cyberthreats. The guidelines are useful for all organizations, but especially for micro and small sized enterprises, which usually face very limited resources, especially in terms of relevant skills in the field of cybersecurity.

Keywords: cybersecurity, COVID-19 pandemic, impact, small sized business, guidelines

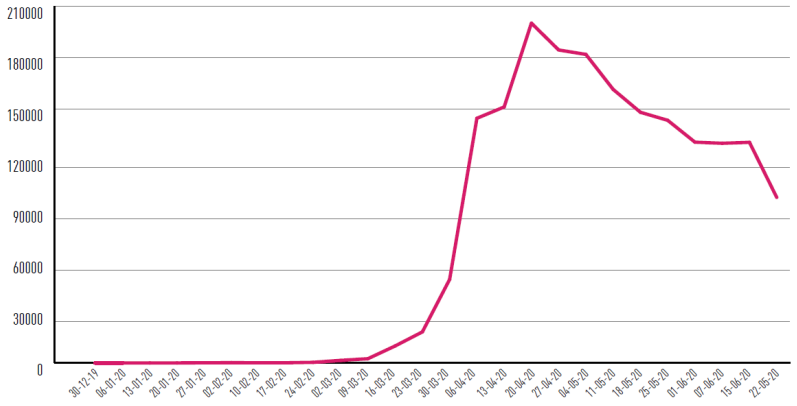
https://doi.org/10.18690/978-961-286-509-2.6 DOI
978-961-286-509-2 ISBN
University of Maribor Press

1 Uvod

COVID-19 je globalna pandemija, ki je kritično vplivala na cel svet, ohromila ekonomijo in resno prizadela poslovanje organizacij v različnih industrijskih panogah in geografskih področjih. V zelo kratkem času je pandemija močno spremenila ustaljene načine dela, preoblikovala vzorce potrošnje ter na splošno spremenila načine povezovanja in sodelovanja.

Številne varnostne organizacije (npr., Insikt Group, 2020; Malwarebytes, 2020; Thales, 2020), ki bdijo nad dogajanjem v kibernetskem prostoru, vse od januarja 2020 poročajo o drastičnem porastu kriminalnih, lažnih kampanj, povezanih s pandemijo COVID-19. Videti je, da intenziteta kiber kriminalnih aktivnosti, povezanih s pojmom COVID-19, po svetu sovpada s širjenjem samega koronavirusa SARS-CoV-2, tako z vidika intenzivnosti kot z vidika geografske razpršenosti. Tako kot same okužbe bolezni COVID-19 so bili tudi prvi COVID-19 kibernetski napadi zabeleženi v Aziji, nato pa so se razširili na področje srednje, vzhodne in zahodne Evrope (Thales, 2020).

Graf na sliki 1 ponazarja gibanje števila s COVID-19 povezanih kibernetskih incidentov, ki so jih na tedenski ravni zaznale omrežne varnostne naprave podjetja Check Point. Razvidno je, da skokovit porast aktivnosti sovpada s pričetkom prvega vala epidemije sredi marca 2020.

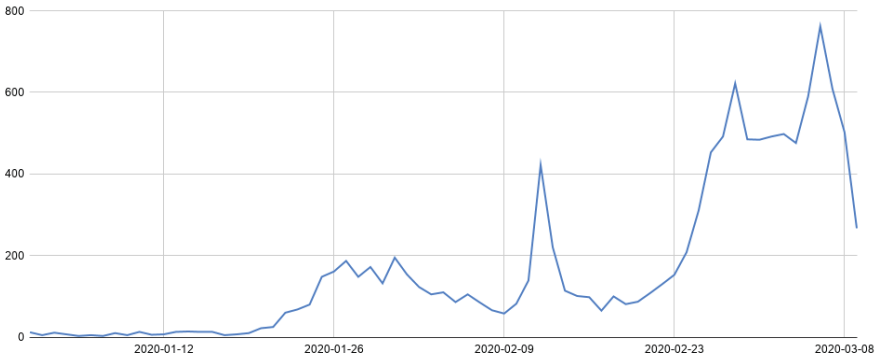


Slika 1: Tedensko gibanje števila kibernetskih napadov v prvi polovici leta 2020
Vir: Check Point (2020).

Sočasno s pojavom pandemije je bil zaznan tudi porast števila različnih prevar in tudi škodljive programske opreme (npr. Gallagher in Brandt, 2020; SI-CERT, 2020). Kot navajajo Kumaran in Lugani (2020), so v aprilu 2020 pri Google poročali, da se dnevno soočajo s preko 240 milijoni sporočil, vezanih na tematiko COVID-19, ki sodijo v kategorijo neželena e-pošta (angl. spam). Poleg teh je bilo na dnevni bazi kar 18 milijonov sporočil takih, ki vsebujejo zlonamerno programsko kodo ali se uvrščajo v kategorijo zvabljanje oz. ribarjenje (angl. phishing). Kot navaja Shi (2020), je intenzivnost ciljno usmerjenih tovrstnih napadov (ang. spear-phishing attack) v marcu 2020 narasla za preko 600 % v primerjavi z meseci poprej. Z namenom povečanja možnosti za uspešnost napada se taka sporočila pogosto sklicujejo na aktualno COVID-19 tematiko, za katero v danih razmerah vlada v splošni javnosti izjemno veliko zanimanje. Ponujajo se potencialno zelo donosne, s COVID-19 povezane naložbe na borznih trgih. Pogosto gre tudi za lažno predstavljanje sicer zaupanja vredne vladne ali zdravstvene institucije (npr. Europol, 2020; Lallie idr., 2020).

Da so kiber kriminalci pripoznali pandemijo COVID-19 kot učinkovit vektor napada, dokazuje tudi dejstvo, da se je od izbruha pandemije dalje izjemno povečalo število na novo registriranih domen, povezanih s koronavirusom (slika 2). Kot navajajo pri podjetju Trend Micro[1], so v tretji četrtini leta 2020 zabeležili preko milijon zadetkov na škodljive URL naslove. Več kot polovica teh domen naj bi služila kot infrastruktura za izvajanje obsežnih zlonamernih kampanj, ki se pogosto uporabljajo za razpečevanje izsiljevalskega programja (angl. ransomware) ali drugega zlonamernega programja za krajo bančnih ali drugih finančnih podatkov (npr. Insikt Group, 2020). Sprva so tovrstne napade izvajali kiber kriminalci sami, a vse pogosteje se pojavljajo kiber kriminalne skupine, ki so financirane s strani državnih institucij (angl. state-sponsored hacking groups), ki pod krinko COVID-19 izvajajo različne vrste vohunjenja (npr. Thales, 2020a).

[1] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains



Slika 2: Gibanje dnevnega števila na novo registriranih domen, povezanih s COVID-19
Vir: Insikt Group (2020).

Zaradi razsežnosti kibernetskih groženj in resnosti njihovih posledic uvrščajo strokovni krogi pandemijo COVID-19 med največje grožnje kibernetski varnosti v zgodovini človeštva (Europol, 2020). Zato ne preseneča, da je na obvladovanje kibernetske varnosti tekom pandemije COVID-19 v svetovnem merilu osredotočena domala vsa, s problematiko povezana, strokovna in znanstvena javnost.

Kibernetski kriminal v povezavi s pandemijo COVID-19 je tako v zadnjem letu osrednja tema poročil in študij številnih varnostnih organizacij in globalnih analitskih družb (npr., Check Point, 2020; Check Point, 2020a; Deloitte, 2020; ECSO, 2020; ETH, 2020; Europol, 2020; FAL, 2020; Insikt Group, 2020; Interpol, 2020; KPMG, 2020; Malwarebytes, 2020; Mimecast, 2020; PwC, 2020; PwC, 2020a).

V luči nove realnosti je Evropska organizacija za kibernetsko varnost (European Cyber Scurity Organization – ECSO) izdala tudi priporočila za obvladovanje kibernetske varnosti tekom COVID-19 krize (ECSO, 2020a). Poleg tega je zaznati tudi pobude za ustrezne prilagoditve varnostnih politik na nivoju EU (npr. Carrapico in Farrand, 2020).

Problematika obvladovanja kibernetske varnosti je deležna velike pozornosti tudi v znanstvenih krogih, kar dokazuje število objav v mednarodnih bibliografskih bazah, ki iz dneva v dan intenzivno narašča.

Na zapaženi problem se sicer po malem opozarja tudi v Sloveniji, a menimo, da glede na njegovo razsežnost nikakor ne dovolj intenzivno. Zasledili smo sicer nekaj objav v dnevnem časopisju in na spletnih straneh nekaterih vladnih in strokovnih organizacij (npr. SI-CERT), ki so seveda za splošno javnost dobrodošle, pa vendar smo mnenja, da je problematika tako pereča, da si »zasluži« bolj poglobljene analize. S pričujočim prispevkom želimo to vrzel vsaj deloma omiliti.

2 Metodologija

V prvem delu prispevka na celovit način analiziramo posledice pandemije COVID-19 z vidika kibernetske varnosti. Pripravili smo sistematičen pregled znanstvene literature na tem področju. Izpostavili smo ključne vzroke, ki botrujejo izjemnemu porastu kibernetskega kriminala v tem obdobju. Proučili smo, katere vrste kibernetskih napadov so se najbolj razmahnile. Analizirali smo, katere gospodarske dejavnosti so najbolj prizadete in geografsko razpršenost s COVID-19 povezanih kibernetskih napadov.

Drugi del prispevka smo posvetili razvoju smernic za obvladovanje kibernetskih tveganj v obdobju pandemije v malih podjetjih.

Tako v svetu kot pri nas predstavljajo mikro, mala in srednja podjetja – MSP (angl. small and medium sized enterprises - SME) hrbtenico celotnega gospodarstva. V evropskem merilu[2] obsegajo MSP kar 99 % vsega gospodarstva, zaposlujejo preko 100 milijonov ljudi in prispevajo več kot polovico bruto domačega proizvoda – BDP. V Slovenji[3] so razmere popolnoma primerljive. Med MSP spada kar 99,8 % vseh slovenskih podjetij, zaposlujejo skoraj 70 % ljudi in ustvarijo 65 % BDP. Zaščita teh organizacij pred kibernetskimi napadi se mora tako uvrščati med prioritetne naloge tako globalnih kot tudi lokalnih strategij kibernetske varnosti.

Dejstvo, ki ga v kontekstu obravnavane problematike ne gre prezreti, pa je, da so zaradi specifičnih razmer in lastnosti MSP pogosto med lažje osvojljivimi cilji kibernetskih kriminalcev. Po poročanju mednarodne gospodarske zbornice International Chamber of Commerce - ICC[4] so bila v 2019 MSP targetirana v preko

[2] https://ec.europa.eu/growth/smes_en
[3] https://www.gov.si/teme/mala-in-srednje-velika-podjetja/
[4] https://iccwbo.org/

40 % kibernetskih napadov, s povprečno škodo preko 188.000 $ na napad (raziskava podjetja Verizon[5]). V poročilu podjetja Datto[6] ugotavljajo, da je v 2019 eno od petih MSP postalo žrtev napada z izsiljevalskim programjem. Kot navaja skupina Anti Phishing Working Group – APWG[7], je število napadov z zvabljanjem oz. ribarjenjem v MSP v 2019 doseglo vrhunec zadnjih treh let. Razlog za tako stanje gre v prvi vrsti pripisati pomanjkanju resursov, predvsem z vidika ustreznega strokovnega kadra in posledično kompetentnega znanja. Še posebej to velja za mikro in mala podjetja (med vsemi slovenskimi MSP je takih kar 98,92 %[8]), kjer je funkcija skrbnika za informacijsko/kibernetsko varnost pogosto zaupana zunanjemu izvajalcu.

Kljub dejstvu, da več mednarodnih raziskav kaže, da so se med pandemijo COVID-19 kiber kriminalci zaradi večjih finančnih koristi bolj usmerili v velike korporacije, vlade in kritično infrastrukturo, mora biti učinkovito obvladovanje kibernetskih tveganj v okolju MSP ena izmed prioritetnih nalog samih podjetnikov kakor tudi države in vse strokovne javnosti. Pri podjetju Symantec[9] namreč ugotavljajo, da zaradi ranljivosti MSP kot najšibkejšega člena v oskrbovalni verigi kiber kriminalci le-te pogosto uporabijo kot odskočno desko za napad na večje korporacije. Menimo, da bomo z oblikovanjem smernic za obvladovanje kibernetskih tveganj v malih podjetjih znatno pripomogli k ublažitvi tega perečega problema.

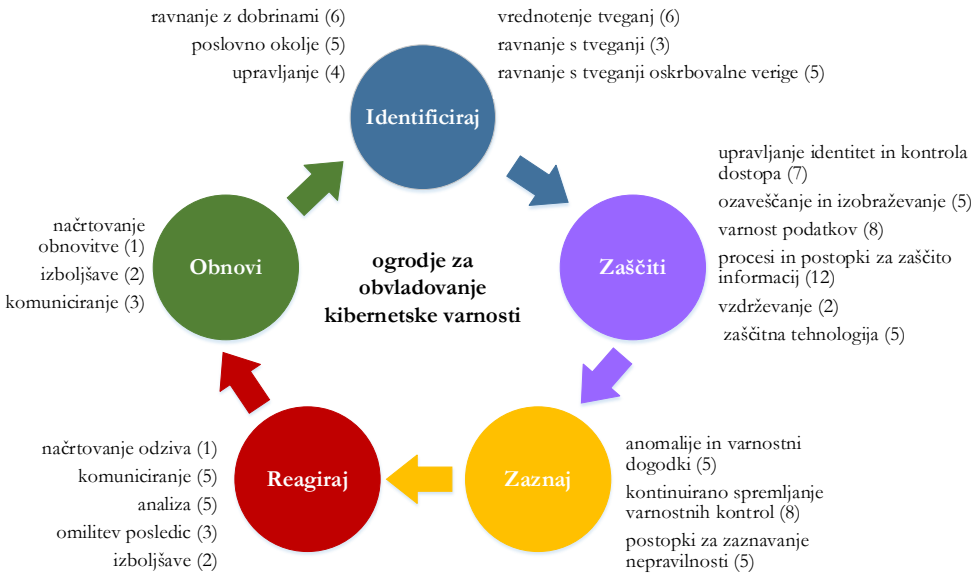
Smernice za mala podjetjih bomo zasnovali na zadnji verziji NIST-ovega ogrodja za kibernetsko varnost kritične infrastrukture NIST CSF[10] (NIST, 2018). Namen ogrodja NIST CSF je nuditi pomoč pri opredelitvi kibernetskih tveganj in strateškem načrtovanju aktivnosti za obvladovanje teh tveganj. Poleg tega lahko ogrodje služi tudi kot orodje pri digitalizaciji poslovnih funkcij v smislu proaktivnega obvladovanja kibernetskih tveganj. Ogrodje je usmerjeno v doseganje 5 temeljnih funkcij kibernetske varnosti: *identificiraj* (angl. identify), *zaščiti* (angl. protect), *zaznaj* (angl. detect), *reagiraj* (angl. respond) in *obnovi* (angl. recover). Posamezne funkcije so razdeljene na več kategorij, le-te pa na več podkategorij, ki predstavljajo aktivnosti,

[5] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[6] https://www.datto.com/resources/dattos-global-state-of-the-channel-ransomware-report
[7] https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf
[8] Po podatkih SURS (https://pxweb.stat.si/SiStatData/pxweb/sl/Data/-/1418801S.px) je bila v letu 2019 struktura MSP glede na število zaposlenih sledeča: 0-1: 74,34 %, 2-9: 20,61 %, 10-49: 3,97 %, 50-249: 1,08 %.
[9] https://docs.broadcom.com/doc/istr-24-2019-en
[10] Prva verzija NIST CSF je bila predložena v letu 2014, https://www.nist.gov/cyberframework/framework.

ki jih je priporočljivo implementirati za doseganje določenega cilja kibernetske varnosti. Kot pomoč pri implementaciji so pri posamezni aktivnosti dodane tudi reference na ustrezna poglavja v drugih uveljavljenih metodologijah s področja informacijske/kibernetske varnosti (npr. ISO/IEC 27001, COBIT ipd.).

Struktura ogrodja, na kateri temelji NIST CSF, je ponazorjena na sliki Slika 3. Poleg petih temeljnih funkcij so na sliki navedene tudi kategorije, obravnavane znotraj posamezne funkcije, številke v oklepajih pa predstavljajo število aktivnosti za izboljšanje stanja znotraj posamezne kategorije. Razvidno je torej, da za celovito obvladovanje kibernetske varnosti predvideva ogrodje skupno 108 aktivnosti (in posledično ciljev). Posamezne aktivnosti niso obligatorne, organizacija si jih izbere skladno s svojo naravo in potrebami. Poleg tega je ogrodje možno implementirati na celotno organizacijo ali pa le na posamezen segment organizacije (npr. proces), ki je iz vidika kibernetske varnosti kritičen.

Čeprav je bilo ogrodje NIST CSF v svoji osnovi razvito za kritično infrastrukturo, se je zaradi njegove celovitosti in fleksibilnosti uporaba razširila tudi na druge organizacije. Danes velja za eno najbolj uveljavljenih metodologij na tem področju. Kot navajajo pri NIST-u, je ogrodje uporabno za vse organizacije, ne glede na njihovo velikost, dejavnost ali stopnjo kibernetske sofisticiranosti (NIST, 2018). Z izdajo smernic Toth in Paulsen (2016) pa so pri NIST-u spodbudili implementacijo ogrodja tudi v segment MSP.



Slika 3: Ogrodje za obvladovanje kibernetske varnosti
Vir: povzeto po NIST (2018).

3 Pregled literature

Problematika kibernetske/informacijske[11] varnosti v povezavi s pandemijo COVID-19 je vse pogosteje zastopana tudi v strokovni in znanstveni literaturi. Sistematičen pregled le-te za obdobje december 2019–junij 2020 podajata Chigada in Madzinga (2021), pri čemer se avtorja osredotočata predvsem na najbolj pogoste kibernetske napade tekom pandemije COVID-19. Izsledki te analize so seveda koristni, a se avtorja v glavnem osredotočata na strokovno in ne toliko na znanstveno literaturo, ki jo želimo sistematično analizirati v nadaljevanju.

[11] Izraza kibernetska in informacijska varnost se v literaturi pogosto zamenjujeta in velikokrat neupravičeno uporabljata kot sinonima. Čeprav imata področji veliko skupnih stičnih točk, je potrebno med njima jasno razlikovati.
Kot izhaja iz definicij v NIST-ovem pojmovniku (https://csrc.nist.gov/glossary), se koncept informacijske varnosti nanaša na zaščito informacijskih dobrin (ne glede na njihovo pojavno obliko) pred nepooblaščenim dostopom, uporabo, razkritjem, spremembo ali uničenjem z namenom zagotoviti zaupnost, celovitost in razpoložljivost.
Po drugi strani pa je kibernetska varnost definirana kot zmožnost zaščite ali obvarovanja uporabe kibernetskega prostora pred kibernetskimi napadi.
Skupno informacijski in kibernetski varnosti je torej varovanje digitalnih informacijskih dobrin, ki so lahko dostopne in posledično ranljive preko kibernetskega prostora.

Posamezni avtorji, ki se ukvarjajo z obravnavano problematiko, ponujajo globalna razmišljanja o posledicah pandemije COVID-19 in o dolgoročnem vplivu le-te na kibernetsko varnost (npr. Mihailović in Rašović, 2020; Eian idr., 2020; Baz idr., 2021). Celovit vpogled vpliva pandemije COVID-19 na organizacije v digitalni dobi in na današnjo digitalno družbo nasploh najdemo tudi v prispevku Dwivedi idr. 2020.

Določene študije se ukvarjajo s proučevanjem vpliva pandemije na kibernetsko varnost v ožjem smislu, vezano na ožje geografsko področje oz. na posamezno državo (npr. Ekvador - Toapanta Toapanta idr., 2020; Nigerija - Omodunbi idr., 2020; Ukrajina - Karpenko, Kuczabski in Havryliak, 2021; države EU - Meghisan-Toma in Nicula, 2020). Nekateri avtorji pa se osredotočajo na posamezne gospodarske dejavnosti ali specifične segmente družbe, kot npr. kritična infrastruktura (Georgiadou, Mouzakitis, in Askounis, 2020), zdravstvo (Muthuppalaniappan in Stevenson, 2021) ali javne organizacije (Toapanta Toapanta idr., 2020). Zanimivi so izsledki raziskave Kashif idr. (2020), ki poleg prizadetosti poslovnih subjektov opozarjajo tudi na znaten porast kiber kriminalnih napadov in oškodovanja končnih uporabnikov internetnih storitev.

Avtorji raziskave Lallie idr. (2020) analizirajo kibernetske napade tekom pandemije COVID-19 v luči časovnega poteka globalnih dogodkov, povezanih s samo biološko pandemijo. Na primeru analize dogajanja v Veliki Britaniji pokažejo sovpadanje vladnih objav in ključnih dogodkov v državi, ki so jih kiber kriminalci spretno izkoristili za načrtovanje svojih kampanj. Podobne zaključke navaja tudi Naidoo (2020), ki poudarja fleksibilnost kiber kriminalcev in njihovo sposobnost prilagajati se situacijskim spremembam tekom pandemije, kar seveda povečuje učinkovitost njihovih zlonamernih aktivnosti.

Posamezni avtorji (Hakak idr., 2020; Khan, Brohi in Zaman, 2020; Malhotra in Dave, 2020; Savitha, 2020) analizirajo različne tehnike napadov, ki se v času pandemije najpogosteje uporabljajo. Med temi študijam najbolj celovite izsledke podaja raziskava Hakak idr. (2020), ki podaja strukturiran pregled najpogostejših vrst zlonamernih aktivnosti, povezanih s COVID-19. Z namenom učinkovitejšega obvladovanja tovrstnih incidentov v prihodnosti avtorji predložijo tudi taksonomijo COVID-19 kibernetskega napada in nanizajo predloge zaščitnih ukrepov.

Pri analizi posameznih tehnik COVID-19 kibernetskih napadov je posebna pozornost posvečena socialnemu inženiringu (angl. social engineering) (Alzahrani, 2020; Hijji in Alam, 2021; Venkatesha, Reddy, in Chandavarkar, 2021), ki se v obdobju izrednih razmer pandemije pokaže kot posebej »učinkovita« metoda napadalcev (več v poglavju 4.3).

Inovativni pristop pri napovedovanju in preprečevanju kibernetskih napadov tekom izrednih razmer pandemije COVID-19 predstavlja tudi model, zasnovan na tehnologiji IoT, ki ga v svojem prispevku predstavljajo Tawalbeh idr. (2020).

Weil in Murugesan (2020) opozarjata na ključna IT tveganja, ki so pogojena z nastopom pandemije COVID-19 in so ogrozila različna področja delovanja, kot npr. šolstvo, zdravstvo, industrijo ipd., ter razmišljata o učinkovitih odzivih nanje.

Mandal in Khan (2020) izpostavljata povečano ogroženost informacijskih storitev v oblaku, ki so s pojavom pandemije COVID-19 morale nenadoma, brez ustrezne predpriprave in prilagoditve platforme prevzeti izvajanje različnih (tudi ključnih) poslovnih funkcij tako v gospodarskih kot tudi v negospodarskih dejavnostih. Avtorja podajata tudi nabor preventivnih ukrepov za zniževanje varnostih tveganj in zaščito teh storitev.

Nova realnost je potegnila za sabo tudi nujo uvedbe dela na daljavo, ki zopet s seboj prinaša dodatna varnostna tveganja in potrebo po spremembi varnostnih politik organizacij (Okereafor in Manny, 2020). Izsledki raziskave Georgiadou, Mouzakitis, in Askounis (2021), izvedene v Evropi, nudijo različna varnostna priporočila, ki naslavljajo tako tehnične ranljivosti, povezane z delom na daljavo, kot tudi potrebo po nadgradnji varnostne kulture med zaposlenimi. Učinke dela na daljavo tekom pandemije COVID-19 v smislu samoocene učinkovitosti zaposlenih in njihovega zaupanja v varnost informacijskih tehnologij za delo na daljavo proučuje tudi študija Buchanan Turner, Turner in Shen (2020), ki je bila izvedena v ZDA. Rezultati so pokazali, da zaposleni zaupajo informacijskim rešitvam, vendar jih kljub temu ocenjujejo za manj zanesljive in primerne, kot je neposredni osebni stik.

Za naše nadaljnje delo so še posebej zanimivi prispevki, ki obravnavajo vpliv pandemije COVID-19 na MSP. Večina tovrstnih študij obravnava učinke na delovanje MSP z ekonomskega vidika v širšem ali ožjem smislu. Avtorji Gourinchas idr. (2020) na primer predstavljajo rezultate obsežne raziskave, v kateri analizirajo vpliv COVID-19 krize na poslovanje MSP iz 17 držav, pri čemer so podatke za analizo črpali iz obsežene baze Orbis, ki jo vzdržuje analitska družba Bureau van Dijk (BvD). Rezultati so med drugim pokazali kar 8,8-% porast propadlih MSP v letu 2020 v primerjavi z letom poprej. S proučevanjem vpliva pandemije na ekonomsko učinkovitost MSP se ukvarjajo tudi študije, kot so: Bartik idr. (2020), Fairlie (2020), Kyung in Whitney (2020), Nazarov, Kovtun in Reichert (2020), NIST (2020), Gregurec, Tomičić Furjan in Tomičić-Pupek (2021) ali Santiago-Omar in Caballero-Morales (2021). Nadalje Beglaryan in Shakhmuradyan (2020) podajata rezultate raziskave, izvedene v Armeniji, kjer analizirata vpliv pandemije COVID-19 na zaposlene v MSP. V literaturi lahko zasledimo tudi nekatere inovativne ideje, kot je na primer ideja avtorjev Bonazzi idr. (2020), ki promovirajo razvoj programske rešitve, ki bi po zgledu aplikacij za spremljanje širjenja virusa SARS-CoV-2 med ljudmi omogočala MSP-jem pridobiti informacijo o morebitni ogroženosti njihovih potencialnih poslovnih partnerjev z vidika likvidnostnih tveganj.

Pri ocenjevanju učinkovitosti MSP ob soočanju s pandemijo COVID-19 je lahko uporabno konceptualno ogrodje, imenovano »5-P«, ki sta ga oblikovala Ravindran in Boh (2020). Ogrodje je zasnovano na podlagi s stališča poslovanja različnih modelov MSP iz različnih koncev sveta (Kitajska, Indija, Bahrajn, ZDA). Tako ogrodje je lahko vodstvu MSP v pomoč pri sistematičnem ocenjevanju zrelosti njihove organizacije ob soočanju s pandemijo, pri čemer so upoštevani različni vidiki (procesi, ljudje, produkti, lokacije, resursi), ki na samo zrelost lahko vplivajo.

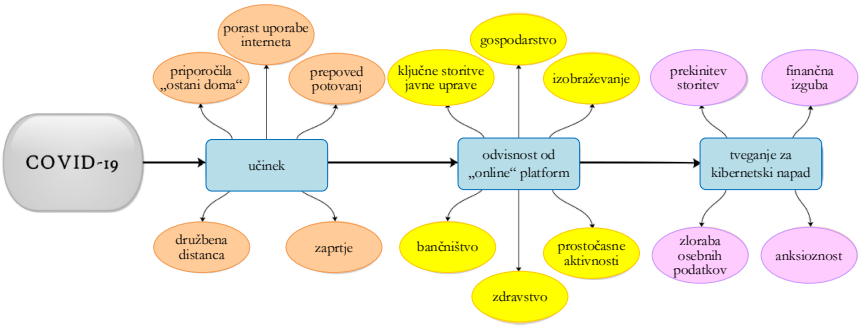
Kljub opozorilom strokovnih krogov glede ranljivosti MSP na COVID-19 kibernetske napade (ICC, n. d.; Karr, Loh in Wirjo, 2020; CISCO, n. d.) pa je na področju znanstvenih prispevkov, ki bi obravnavali vpliv pandemije COVID-19 na delovanje MSP z vidika kibernetske/informacijske varnosti zaslediti precejšnjo raziskovalno vrzel. V tem segmentu smo našli le tri prispevke, in sicer: Papadopoulos, Baltas in Balta (2020) ter Tam, Rao in Hall (2020, 2021).

Papadopoulos, Baltas in Balta (2020) razpravljajo in razmišljajo o vlogi digitalnih tehnologij pri zagotavljanju neprekinjenega poslovanja MSP v kriznih pandemičnih razmerah. Nadalje avstralski avtorji Tam, Rao in Hall (2020) izpostavljajo ukrepe, s katerimi bi lahko vlada posamezne države na strateškem nivoju pripomogla k boljši odpornosti MSP na kibernetska varnostna tveganja tako tekom pandemije kot tudi po zaključku le-te. V drugem prispevku Tam, Rao in Hall (2021) pa isti avtorji predstavljajo idejno zasnovo napredne, strokovno in tehnično podprte spletne platforme za izvajane samoocene izpostavljenosti kibernetskim tveganjem. Po navedbah avtorjev je platforma prirejena specifikam MSP, ki pogosto ne razpolagajo z zadostnimi kibernetsko obrambnimi resursi niti z ustreznim tehničnim znanjem. Lastnikom MSP bi tako ob podpori v platformo vključenih kompetentnih partnerskih organizacij omogočila hitro in učinkovito oceno obstoječega stanja na področju kibernetske varnosti, kar je osnova za načrtovanje ustreznih varovalnih ukrepov, še posebej v nestabilnem obdobju pandemije.

4 Ozadje pandemije COVID-19 z vidika kibernetske varnosti

4.1 Globalne posledice pandemije COVID-19

Nenadni pojav pandemije je globoko posegel v ustaljene načine življenja tako na širši, družbeni ravni kot tudi na osebnih ravneh. Države širom sveta so bile v trenutku primorane sprejeti rigorozne ukrepe prepovedi potovanj, socialnega distanciranja in uveljavljanja načela »ostani doma«. Iz dneva v dan pa nam je bolj jasno, da globalna pandemija COVID-19 ne predstavlja le enega bolj kritičnih zdravstvenih izzivov človeštva, temveč tudi izjemen izziv na področju obvladovanja kibernetskega kriminala. Povezavo med pandemijo COVID-19 in povečanim tveganjem za kibernetske napade strnjeno prikazuje slika 4, v nadaljevanju pa smo izpostavili tiste dejavnike, ki so k porastu kibernetskega kriminala v tem obdobju ključno pripomogli.



Slika 4: Povezava med pandemijo COVID-19 in povečanim tveganjem za kibernetske napade
Vir: prirejeno po Hakak idr. (2020).

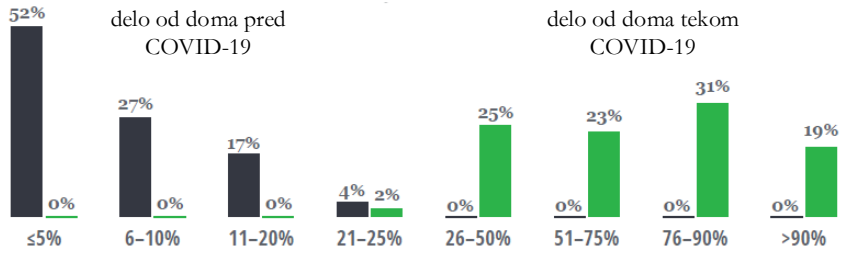
4.2 Vzroki za porast kibernetskega kriminala tekom pandemije COVID-19

Ko razmišljamo, zakaj je kibernetski kriminal v času pandemije COVID-19 v takem porastu, težko pridemo do enoznačnega odgovora in »glavnega krivca«, saj so razmere zelo kompleksne in večplastne. Pa vendar so določene spremembe načina življenja in dela, ki jih je moralo človeštvo zaradi pojava pandemije praktično čez noč usvojiti, botrovale izjemnemu porastu zlonamernih aktivnosti v kibernetskem prostoru. V nadaljevanju izpostavljamo tiste, ki so po mnenju strokovnih krogov za nastalo situacijo ključne.

4.2.1 Varnostne pasti dela od doma

Da bi omejili širjenje virusa, so vlade posameznih držav širom sveta uvedle različne ukrepe za zmanjšanje fizičnih kontaktov med ljudmi. Kjer je bilo le možno, so delodajalci omogočili svojim zaposlenim delo od doma. Rezultati raziskave Deloitte (2020), izvedene v maju 2020, v kateri so sodelovali skrbniki za informacijsko varnost (angl. Chief Information Security Officer – CISO) ključnih regionalnih podjetij iz 51 zveznih držav v ZDA, so pokazali, da se je pred pandemijo v večini organizacij (52 %) dela od doma posluževalo le 5 % njihovih zaposlenih, v nobenem primeru pa ni od doma delalo več ko 25 % zaposlenih. Z grafa na sliki 5 je razvidno, da so se razmere s pojavom pandemije drastično spremenile. Delež organizacij, v katerih se je dela od doma posluževala več kot polovica zaposlenih, je narasel kar na 73 %, pri čemer je v 19 % organizacij od doma delalo celo več kot 90 % zaposlenih.

Menimo, da je situacija v Sloveniji in tudi v ostalih evropskih državah s tega vidika dokaj primerljiva.



Slika 5: Delež zaposlenih, ki delajo od doma: črna barva pred, zelena barva po nastopu pandemije COVID-19
Vir: prirejeno po Deloitte (2020).

Čeprav je bil prehod na delo z vidika zagotavljanja kontinuiranega poslovanja nujen, pa je dejstvo, da je ta nenadni preobrat odprl številna varnostna tveganja.

V želji, da bi delo od doma kar najhitreje steklo, so v mnogih organizacijah namestili številne dodatne vmesnike, ki so omogočili oddaljeni dostop (angl. remote access) zaposlenih do omrežja organizacije. Take »ad-hoc« rešitve so seveda uporabnikom olajšale delo, a so tudi otežile administriranje samega omrežja (tudi iz vidika varnosti). Poleg tega pa se je na ta način napadalcem lahko ponudila dodatna možnost za vzpostavitev nepooblaščenega dostopa do internega omrežja organizacije.

Znatno varnostno tveganje predstavlja tudi nenaden in skokovit porast števila zasebnih IT naprav, ki so se začele uporabljati v poslovne namene. Za razliko od IKT infrastrukture v poslovnih okoljih, ki je običajno deležna sistematične in kontinuirane zaščite, skladno z uveljavljenimi varnostnimi standardi, so zasebna domača omrežja in posledično domače IT naprave pogosto mnogo slabše zavarovane. V domačih okoljih se profesionalna varnostna orodja (protivirusna zaščita, požarne pregrade, sistemi za nadzor omrežij ipd.) uporabljajo bistveno redkeje (pogosto zaradi neustreznega strokovnega znanja in tudi zavoljo stroškov licenc). Uporabniki se povečini poslužujejo prosto dostopne programske opreme, ki pa, če ni ustrezno vzdrževana, lahko vsebuje resne varnostne vrzeli.

Nemalokrat zasledimo tudi uporabo programske opreme, ki je v zaključni fazi svojega življenjskega cikla in kot taka ni več deležna varnostnih posodobitev s strani proizvajalca. Kot tipičen primer bi lahko navedli operacijski sistem Windows 7. Čeprav je Microsoft ta sistem nehal podpirati že v začetku leta 2020, ga še vedno uporabljajo milijoni uporabnikov širom po svetu (Warren, 2021).

4.2.2 Rekorden porast uporabe internetnih storitev in storitev v oblaku

Dejstvo, da so se številne dejavnosti v trenutku prestavile v domače okolje (delo od doma, šolanje na daljavo, socialni stiki, nakupovanje izključno prek spleta ipd.), je za seboj potegnilo nenaden in rekorden porast uporabe številnih komunikacijskih kanalov. Različna orodja za skupinsko delo, videokonferenčni sistemi, IKT tehnologije za delo na daljavo, socialna omrežja, elektronska pošta, pretočne vsebine in druge storitve v oblaku se uporabljajo intenzivneje kot kadarkoli doslej. Kot navaja študija ETH (2020), pri McAfee-ju poročajo, da se je sredi marca 2020 v primerjavi z začetkom leta 2020 uporaba orodij za skupinsko delo v oblaku več kot podvojila. Največji porast beležijo naslednja orodja: Slack: +200 %, Microsoft Teams: +300 %, Zoom: +350 % in Cisco Webex: celo +600 %.

Slika6: Orodja za skupinsko delo v oblaku, ki so s pojavom pandemije COVID-19 zabeležila največji porast uporabe
Vir: Prirejeno po ETH (2020).

Nenadna sprememba načina življenja in dela se odraža tudi na intenziteti uporabe in posledično obremenjenosti posameznih internetnih storitev. Sredi marca 2020 je podjetje DE-CIX[12], ki v svetovnem merilu predstavlja enega izmed večjih globalnih ponudnikov internetnih storitev, zabeležilo rekordno količino podatkovnega

[12] https://www.de-cix.net/

prometa 9,1 TBit na sekundo, kar ustreza količini približno 1.800 prenesenih HD filmov v eni sekundi (Wiggen, 2020).

Intenzivnejša raba internetnih storitev in storitev v oblaku ter izjemen porast števila uporabnikov (pogosto tudi novih in neizkušenih) v kibernetskem prostoru zagotovo ustvarja nove priložnosti za zlonamerne in kriminalne dejavnosti.

4.2.3 Izkoriščanje izrednih razmer in splošne prestrašenosti ljudi

Pandemija COVID-19 je prinesla tudi negotove socialne in ekonomske razmere, kar pri ljudeh vzbuja strah in zaskrbljenost. Izredne razmere pa so kot voda na mlin za uspeh kiber kriminalcev, ki globalno prisoten strah ljudi pred samim virusom izkoriščajo kot sredstvo za izvedbo kibernetskih napadov in/ali generiranje novih tipov napadov. Tako stanje dobro okarakterizira izraz »fearware«[13], ki se je v zadnjem obdobju uveljavil v tuji literaturi in strokovni javnosti.

Nadalje izredne razmere in splošna negotovost krepijo potrebo ljudi (uporabnikov interneta) po ustreznih informacijah, povezanih z osebnim zdravjem, zaščitnimi ukrepi, metodah zdravljenja in/ali cepljenja ter informacijah s strani vladnih institucij. Izkušnje pa dokazujejo, da postanejo uporabniki interneta v svoji veliki želji in potrebi po pridobitvi ustreznih informacij bolj zaupljivi in kot taki bistveno lažji plen za metode socialnega inženiringa (več v poglavju 4.3).

4.3 Najbolj pogosti tipi COVID-19 kibernetskih napadov in motivi zanje

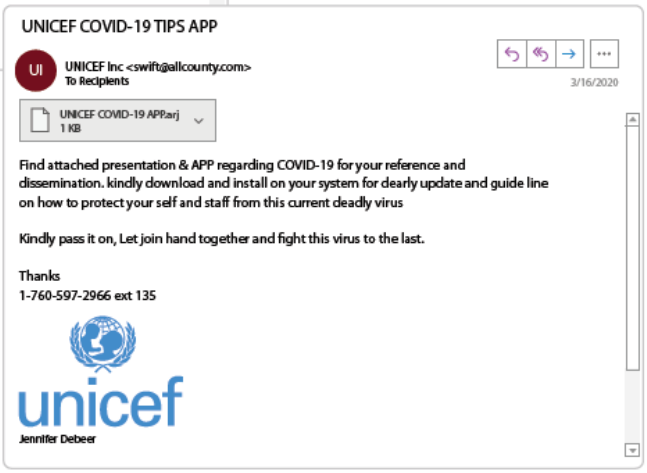
V tem poglavju izpostavljamo tiste vrste kibernetskih napadov, ki so od pričetka pandemije COVID-19 do danes najbolj razmahnili. V večini primerov gre znane in tudi v preteklosti aktualne vektorje napada, ki pa so jih v obdobju pandemije napadalci spretno prilagodili trenutnim razmeram.

[13] Vir: https://www.certsign.ro/en/fearware-cyberattacks-in-the-context-of-covid-19-what-are-they-and-how-do-we-avoid-them/

Socialni inženiring (tudi družbeni inženiring, angl. social engineering) je manipulacija človeške naravne, tj. nagnjenosti k naivnosti in zaupanju. Na področju informatike razumemo socialni inženiring kot uporabo psiholoških trikov na legitimnih uporabnikih informacijskega sistema z namenom pridobitve nepooblaščenega dostopa do resursov informacijskega sistema, ne da bi napadalec moral za potrebe dostopa v sistem dejansko vdreti.

Zaradi vse bolj dovršenih tehnoloških rešitev, ki kibernetskim kriminalcem otežujejo izvedbo tehničnih napadov, je uporaba metod in tehnik socialnega inženiringa s strani napadalcev v velikem porastu. Rezultati nekaterih raziskav tako dokazujejo, da kibernetski napadi s pomočjo socialnega inženiringa beležijo v preko 80 % primerov zelo veliko verjetnost uspeha (Salahdine in Kaabouch, 2019).

Razmere, ki smo jim zaradi pandemije COVID-19 priča (poglavje 4.2), so za uspeh socialnega inženiringa praktično idealne, kar kiber kriminalci s pridom izkoriščajo. Da bi pri uporabnikih dosegli (lažno) kredibilnost in jih pripravili do tega, da odprejo zlonamerno prilogo ali sledijo lažni povezavi, se kiber kriminalci pogosto skrijejo pod »blagovno znamko« kake zaupanja vredne institucije (npr. WHO - World Health Organization, Unicef; slika Slika 7).



Slika 7: Primer COVID-19 socialnega inženiringa – lažno sporočilo v imenu organizacije Unicef

Vir: Malwarebytes (2020).

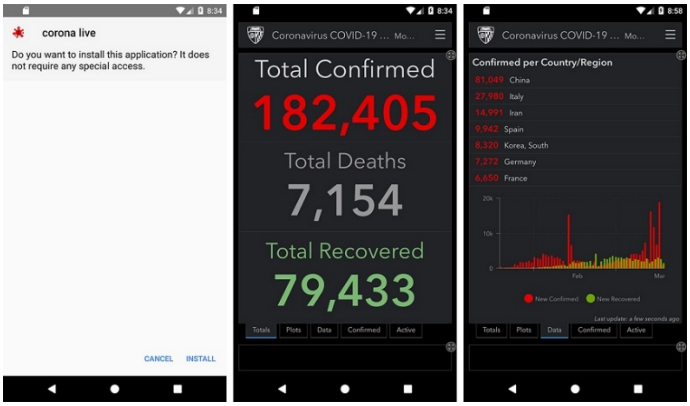
Kljub svoji majhnosti in jeziku, ki ga govori le peščica zemljanov, tudi v Sloveniji nismo povsem imuni na tovrstne napade. Slika 8 prikazuje lažno sporočilo z zadevo "Distribucija zaščitne opreme Covid-19 (Ministrstvo za zdravje Slovenija) Junij 2020", ki je bilo v juniju 2020 razposlano na večje število slovenskih e-poštnih naslovov. V lažnem imenu Nacionalnega inštituta za javno zdravje – NIJZ in Ministrstva za zdravje RS avtor sporočila nagovarja uporabnika, da odpre datoteko v prilogi ("Prijavnica za distribucijo zaščitne opreme covid-19.pot" oz. "Preventivni ukrepi Covid-19.ppt"). Priponka je zlonamerna, saj vsebuje makro, ki iz več spletnih mest na lokalni računalnik prenese škodljivo kodo in jo izvede.

Slika 8: Primer COVID-19 socialnega inženiringa v Sloveniji – lažno sporočilo v imenu NIJZ
Vir: SI-CERT, https://www.cert.si/si-cert-2020-05-lazno-sporocilo-nijz/.

Vohunsko programje (angl. spyware) je zlonamerno programje, ki omogoča nepooblaščeno in pritajeno spremljanje stanja informacijskega sistema in tudi aktivnosti njegovih pooblaščenih uporabnikov (Islovar, www.islovar.org). Primer COVID-19 vohunskega programja predstavlja npr. Android aplikacija »Corona Live 1.1«. Gre za zlorabo legitimne aplikacije »Corona Live« za spremljane širjenja koronavirusa, v katero je vgrajena komercialna različica vohunskega programja SpyMax, ki napadalcu omogoči nadzor nad okuženo napravo v realnem času. Tako aplikacija »Corona Live 1.1« takoj po namestitvi zahteva dostop do pomnilniških medijev naprave, nadzor nad lokacijo naprave in tudi dovoljenje za fotografiranje in snemanje.

Za razpečevanje vohunskega programja se v praksi pogosto uporabljajo prej opisane tehnike socialnega inženiringa. Tak primer predstavlja tudi sporočilo s slike 7, kjer je datoteka »UNICEF COVID-19 APP.arj«, ki je v prilogi sporočila, vohunski program, ki se aktivira, če (ko) uporabnik priponko odpre.

Ohromitev storitve (angl. denial of service – DoS) je napad s pošiljanjem velikega števila zahtev za izvajanje omrežne storitve, kar lahko povzroči nedostopnost storitve za legitimne uporabnike (Islovar, www.islovar.org). Naprednejša različica tega napada je t. i. porazdeljena ohromitev storitve (angl. Distributed Denial of Sevice – DDoS), kjer nepooblaščene zahteve za izvajanje storitve prihajajo hkrati iz več, v omrežje povezanih, računalnikov (angl. botnet). Taki napadi lahko povzročijo motnje v delovanju posameznih (tudi ključnih) storitev ali celo njihovo prekinitev delovanja in tudi začasno ali trajno izgubo kritičnih informacij.



Slika 9: Zaslonska slika vohunskega programa »Corona Live 1.1«
Vir: https://www.bankinfosecurity.com/covid-19-themed-malware-goes-mobile-a-13981

Kot navajajo Kupreev, Badovskaya in Gutnikov (2020), ki povzemajo rezultate analize podjetja Kaspersky, je bil v prvem kvartalu preteklega leta zabeležen izjemen porast DDoS napadov. Napadi so usmerjeni predvsem v zdravstvene ustanove (ameriško ministrstvo za zdravstvo in človeške storitve: US Health and Human Services)[14], večja skupina bolnišnic v Parizu (Assistance Publique-Hôpitaux de

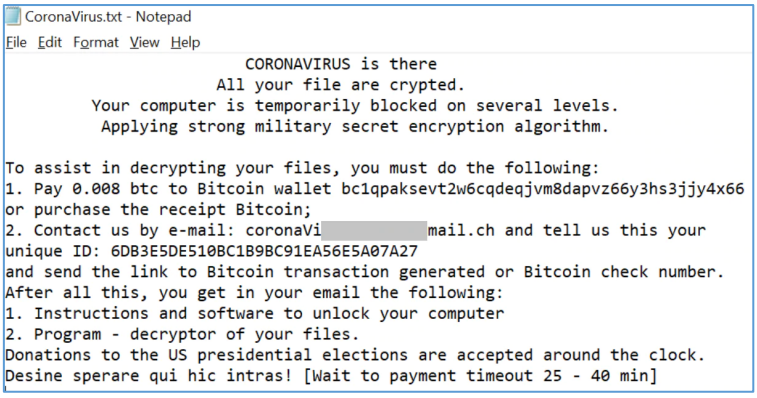
[14] https://www.theregister.com/2020/03/16/hhs_reports_cyberattack/

Paris)[15], organizacije za dostavo hrane (nemški Lieferando[16], nizozemski Thuisbezorgd[17]), platforme za podporo šolanju na daljavo (nemški Mebis[18], slovenski ARNES[19]) ipd. Kot glavni razlog za občuten porast DDoS napadov v obdobju pandemije se v literaturi navaja ravno skokovit porast uporabe interneta in storitev v oblaku, o katerem je bilo govora v poglavjih 4.2.1 in 4.2.2 (Hope, 2021).
Izsiljevalsko programje (angl. ransomware) je škodljivo programje, ki onemogoči uporabo sistema ali storitve (običajno tako, da šifrira celoten pomnilniški medij) in za nadaljnjo uporabo (tj. dešifriranje podatkov) zahteva plačilo odkupnine (običajno v kriptovaluti) (Islovar, www.islovar.org).

Tako kot v primeru vohunskega programja se za širjenje izsiljevalskega programja napadalci pogosto poslužujejo različnih metod socialnega inženiringa. Seveda je glavni motiv napadalca zaslužek. Garancije za vračilo izgubljenih podatkov kljub plačilu odkupnine pa ni nobene.

Kot izhaja iz raziskave Hakak, idr. (2020), se je v obdobju pandemije pojavilo kar nekaj novih primerkov izsiljevalskega programja, tako za računalniške operacijske sisteme (Ransomware-GVZ, Netwalker) kot tudi za mobilne različice (CovidLock, ki deluje na Android operacijskem sistemu). Slika 10 prikazuje sporočilo, ki se uporabniku prikaže po zagonu izsiljevalskega programa Ransomware-GVZ. Razvidno je, da za povrnitev zašifriranih podatkov napadalec zahteva plačilo v višini 0,008 Bitcoin, kar je približno 400 €. V napadih na poslovne subjekte pa so ti zneski pogosto mnogo višji. Pri podjetju Coveware[20] na primer poročajo, da je v prvi četrtini leta 2020 povprečna odkupnina, ki jo je napadalec z izsiljevalskim programjem iztržil od žrtve, znašala 111.605 $, kar je 33 % več kot v zadnji četrtini leta poprej.

[15] https://www.tellerreport.com/tech/2020-03-23---hospital-systems-paris-inaccessible-for-hours-on-end-due-to-ddos-attack-.ByG627LILL.html
[16] https://www.darkreading.com/attacks-breaches/ddos-attack-targets-german-food-delivery-service/d/d-id/1337359
[17] https://nltimes.nl/2020/03/19/ddos-attack-hinders-popular-food-delivery-service
[18] https://www.security-insider.de/bayerische-lernplattform-mebis-durch-ddos-angriff-lahmgelegt-a-914085/
[19] https://www.rtvslo.si/slovenija/arnesove-ucilnice-zjutraj-za-nekaj-casa-ohromil-ddos-napad-drugega-so-odbili/539801
[20] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report



Slika 10: Zaslonska slika sporočila, ki se uporabniku prikaže po zagonu izsiljevalskega programa Ransomware-GVZ

Vir: Sriram, Karnik in Grindstaff (2020).

Spletna prevara (angl. digital fraud) je dejanje v spletnem okolju, s katerim napadalec uporabnika namerno zavede (običajno z določenim namenom), pogosto tudi finančno oškoduje (Islovar, www.islovar.org). Spletni goljufi na primer pozorno spremljajo modne trende, sledijo povpraševanju ljudi v spletnih trgovinah ter temu ažurno in spretno »prilagajajo« svoje lažne spletne trgovine. Tudi pri teh napadih odigra ključno vlogo socialni inženiring.

Vsake neobičajne razmere, kot so naravne katastrofe ali izredni dogodki, so priložnost za prevarante in goljufe, zato tudi pandemija COVID-19 s tega vidika ni izjema. V tem obdobju je povpraševanje uporabnikov intenzivno usmerjeno v zaščitno opremo, ki se v lažnih spletnih trgovinah pogosto prodaja po astronomskih cenah. O tovrstnih prevarah se poroča tudi v Sloveniji. Na spletnih straneh Varni na internetu (slika 11) navajajo primer slovenskega podjetja, ki je od domnevno španskega dobavitelja naročilo in z nakazilom na bančni račun vnaprej vplačalo večjo količino zaščitnih rokavic. Sledilo je potrdilo logističnega podjetja, da je pošiljka na poti, potem se pa žal ni zgodilo nič in podjetje je bilo oškodovano.

O COVID-19 spletnih prevarah so v juniju 2020 poročali tudi na NIJZ. Pojavila so se različna lažna spletna sporočila, ki so zlorabljala znak NIJZ, da bi ustvarila lažen vtis, da gre za uradno sporočilo NIJZ in Ministrstva za zdravje Republike Slovenije. Primer takega sporočila, ki obljublja posredovanje pri zagotavljanju zaščitne opreme, prikazuje slika Slika 12.

Slika 11: Lažna spletna stran goljufivega ponudnika zaščitne opreme
Vir: https://www.varninainternetu.si/lazne-spletne-trgovine-z-medicinsko-opremo/

Slika 12: Spletna prevara z lažnim NIJZ sporočilom, ki obljublja posredovanje pri zagotavljanju zaščitne opreme za zaščito pred okužbo
Vir: https://www.nijz.si/sl/opozorilo-spletna-prevara-glede-zagotavljanja-zascitne-opreme

Zvabljanje (tudi ribarjenje; angl. phishing) je oblika spletnega socialnega inženiringa, ki temelji na navidezno verodostojnem, a dejansko lažnem e-poštnem sporočilu, ki od uporabnika neposredno zahteva vnos občutljivih zasebnih informacij (npr. dostopno geslo) ali pa ga za vnos teh informacij usmeri na lažno spletno mesto.

Izčrpni poročili o razmahu napadov zvabljanja tekom pandemije COVID-19 so pripravili pri podjetju F5 Labs (Warburton idr., 2020) in v skupini APWG (APWG, 2021), kjer poročajo o 15-% porastu tovrstnih napadov v začetku 2020 v primerjavi s preteklim letom, pri čemer se je število tovrstnih napadov do konca leta celo podvojilo. Glavni motivi napadalcev so pridobivanje finančne koristi (npr. prošnja za donacije za lažne dobrodelne organizacije), pridobivanje uporabniških poverilnic za dostop do različnih občutljivih storitev (npr. PayPal) in distribucija zlonamernega programja. Primer »phishing« sporočila, vezanega na COVID-19, prikazuje slika Slika 13.


----- Forwarded message -----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

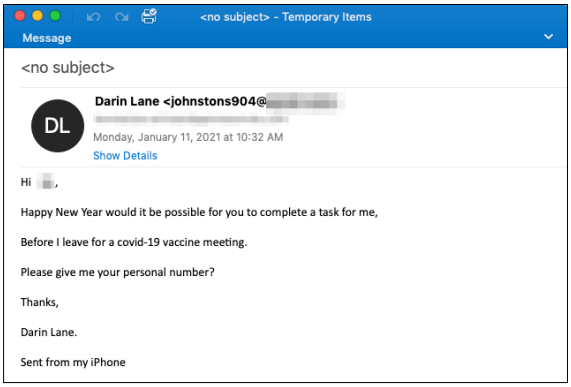
From Government Gateway

This is an automatic email - please don't reply.

Slika 13: Primer phishing« sporočila, vezanega na COVID-19
Vir: https://www.badn.org.uk/News/COVID-19/Stay-Alert-Have-you-seen-some-of-the-latest-Coronavirus-COVID-19-scams.aspx

Kot posebno različico napadov zvabljanja tekom pandemije COVID-19 velja omeniti t. i. usmerjeno zvabljanje (angl. spear phishing), kjer gre za ciljno targetiran napad na točno določenega posameznika ali skupino posameznikov (običajno nivo vodstva organizacije ali skrbnik informacijskega sistema). Tak primer predstavlja napad, imenovan »Business e-mail compromise – BEC« (Warburton idr., 2020;

APWG, 2021). Primer BEC sporočila, ki od prejemnika želi pridobiti telefonsko številko, je prikazan na sliki Slika 14.



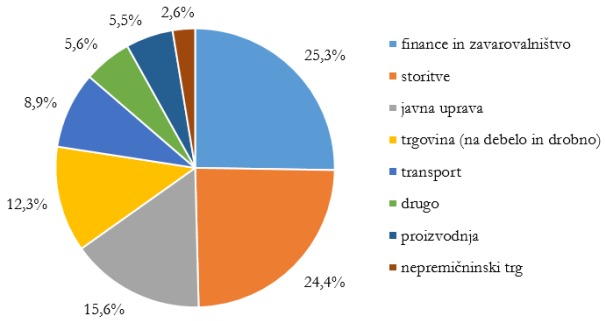
Slika 14: Primer usmerjenega zvabljanja »Business e-mail compromise – BEC«, ki od prejemnika želi pridobiti telefonsko številko
Vir: https://www.proofpoint.com/us/blog/threat-insight/attackers-use-covid-19-vaccine-lures-spread-malware-phishing-and-bec

Poleg opisanih vrst napadov je v poročilu podjetja Trend Micro (2020) in ostali relevantni literaturi izpostavljenih še nekaj pogosto zabeleženih izvedb kibernetskih napadov, ki na različne načine izkoriščajo pandemijo COVID-19 za doseganje svojih ciljev. Med njimi velja izpostaviti napade na protokol za oddaljeno namizje (angl. remote desktop protocol (RDP) attack), neželeno e-pošto (angl. spam), različne vrste zlonamernega programja (angl. malware), lažne in zlonamerne domene (angl. malicious domains), lažna in zlonamerna spletna mesta (angl. malicious websites), zlonamerno sporočanje preko socialnih omrežij (angl. malicious social media messaging) ter širjenje neresnic z namenom zavajanja uporabnikov (angl. Covid-related fake news).

4.4 Kibernetski napadi glede na gospodarske dejavnosti in geografsko razpršenost

Posledice izjemnega porasta kibernetskega kriminala v obdobju pandemije COVID-19 občutijo prav vse gospodarske dejavnosti, še posebej pa tiste z večjimi donosi. Zaradi ranljivosti v času izrednih razmer je posebej ogrožen zdravstveni sektor in z njim povezana industrija. V tem segmentu so bile po rezultatih študije podjetja IBM

zabeležene finančne izgube zaradi kibernetskih napadov v višini preko 7 mio $, kar je daleč največ med vsemi gospodarskimi in industrijskimi panogami[21]. Graf na sliki 15 pa prikazuje udeleženost ostalih gospodarskih dejavnosti pri COVID-19 kibernetskih incidentih v prvih treh kvartalih leta 2020.

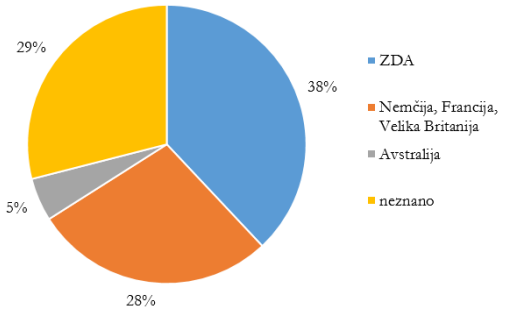


Slika 15: Struktura COVID-19 kibernetskih incidentov glede na targetirano gospodarsko dejavnost – brez upoštevanja zdravstvenega sektorja in z njim povezane industrije
Vir: prirejeno po Aldasoro idr. (2021).

Tako kot je sama bolezen SARS-CoV2 ogrozila vse države sveta, prav nobena med njimi ni ostala imuna niti na COVID-19 kibernetske grožnje. Zanimiva je ugotovitev, da so bile ravno države, ki so bile najbolj prizadete s stališča same bolezni, najpogosteje vključene tudi v COVID-19 kibernetske napade.

Kot poroča spletni medij SecurityWorldmarket.com[22], je »Atlas VPN Team« (https://atlasvpn.com/) v letu 2020 zabeležil 16,4 milijona kibernetskih napadov, povezanih s COVID-19. Največ od teh groženj izvira iz ZDA (38 % oziroma 6,3 milijonov napadov), ki velja tudi za najbolj prizadeto državo zaradi bolezni nasploh. V skupnem, 28 % ali 4,6 milijonov primerov, prihaja iz treh največjih evropskih držav (Nemčija, Francija in Velika Britanija), ki se tudi uvrščajo na lestvico 10 držav z največjim številom okužb. Približno 5 % (cca 770 tisoč) COVID-19 kibernetskih napadov prihaja iz Avstralije, medtem ko ostaja izvor preostalega deleža napadov (29 %) neznan. Strukturo COVID-19 kibernetskih incidentov glede na geografski izvor prikazuje graf na Sliki 16.

[21] https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/#industry
[22] https://www.securityworldmarket.com/int/News/Business-News/over-16-million-covid-related-cyber-attacks-recorded-in-2020



Slika 16: Struktura COVID-19 kibernetskih incidentov glede na geografski izvor
Vir: prirejeno po SecurityWorldmarket.com[23].

5 Smernice za obvladovanje kibernetskih tveganj v malih podjetjih

Pri oblikovanju smernic za obvladovanje kibernetskih tveganj v okolju MSP smo sledili strukturi ogrodja NIST CSF (NIST, 2018). Prednosti implementacije tega ogrodja za obvladovanje kibernetsko varnostnih tveganj v MSP poudarjajo mnogi avtorji (Sage, 2018; Benz in Chatterjee, 2020). Zaradi specifičnih lastnosti MSP pa naletimo pri implementacij ogrodja NIST CSF v okolje MSP tudi na določene omejitve, ki jih velja upoštevati. Pridružujemo se mnenju avtorjev Benz in Chatterjee (2020), ki kot ključno omejitev izpostavljata dejstvo, da je NIST CSF kljub vsemu dokaj kompleksno ogrodje, katerega implementacija je lahko razmeroma zahtevna naloga, kar je lahko v okolju MSP z omejenimi ali celo podhranjenimi resursi precejšnja ovira.
Pri oblikovanju smernic za obvladovanje kibernetskih tveganj v času izrednih razmer pandemije COVID-19 je potrebno torej upoštevati, da bodo le-te služile svojemu namenu le, če bodo za okolja MSP razumljive, obvladljive in jih bo možno v prakso implementirati hitro, kljub morebitnim omejitvam z vidika finančnih, tehnoloških in človeških resursov. Slednje je bilo tudi vodilo pri razvoju naših smernic za mala podjetja, ki jih podajamo v tabeli 1.

Smernice smo oblikovali tako, da smo iz ogrodja NIST CSF izluščili tiste aktivnosti, ki so po našem mnenju za obvladovanje kibernetskih tveganj v malih podjetjih

[23] https://www.securityworldmarket.com/int/News/Business-News/over-16-million-covid-related-cyber-attacks-recorded-in-2020

ključnega pomena, ter jih ustrezno prilagodili potrebam in lastnostim malih podjetij. Na osnovi analize, opravljene v poglavju 4, smo te aktivnosti nadgradili tudi z aktivnostmi za obvladovanje kibernetskih groženj, ki so se v izrednih razmerah pandemije COVID-19 pokazale kot najbolj pereče. V skupnem tako naše smernice obsegajo 36 aktivnosti, pri čemer jih je 11 usmerjenih v vzpostavitev funkcije *identificiraj*, 17 v *zaščiti*, 2 v *zaznaj*, 4 v *reagiraj* in 2 v *obnovi*. Kjer smo ocenili, da je koristno, smo pri posamezni aktivnosti podali tudi dodatna pojasnila, ki bodo vodstvu MSP v pomoč pri implementaciji ali pri samooceni trenutnega stanja na področju obvladovanja kibernetskih tveganj. Na ta način smo oblikovali celovito in pregledno ogrodje, ki ga bodo mala podjetja lahko implementirala nemudoma, učinkovito in z lastnimi resursi.

Poleg tega lahko smernice služijo vodstvu podjetja tudi kot osnova za izvedbo hitre samoocene stanja na področju kibernetske varnosti. Ob predpostavki, da so vse aktivnosti znotraj smernic z vidika kibernetske varnosti enako pomembne, predlagamo, da podjetja k samooceni trenutnega stanja pristopijo tako, da svoje doseganje posamezne aktivnosti ovrednotijo na naslednji način:

- dosegamo v celoti: 100 točk
- dosegamo v veliki meri: 70 točk
- delno dosegamo: 40 točk
- ne dosegamo: 0 točk

Seštevek doseženih točk po kategorijah bo tako omogočal določitev ocene skladnosti po posameznih funkcijah kibernetske varnosti. Ob upoštevanju, da je ob predlaganem načinu ocenjevanja največje možno število točk 360, pa bo skupni seštevek doseženih točk osnova za določitev splošne skladnosti z ogrodjem, kar je zagotovo dobrodošla informacija za vsakega podjetnika.

6 Zaključek

V prispevku smo se osredotočili na pandemijo COVID-19 z vidika njenega vpliva na kibernetsko varnost. Glede na razsežnosti in posledice tega vpliva se pridružujemo mnenju svetovnih strokovnjakov, da predstavlja pandemija COVID-19 največjo grožnjo kibernetski varnosti v zgodovini človeštva doslej. Tako lahko trdimo, da se trenutno ne soočamo le z biološko, pač pa tudi s kibernetsko pandemijo. Slednja pa ima po našem mnenju za svoj razmah še večji potencial kot prva. Namreč, če je za prenos virusa SARS-CoV2 potreben osebni stik, se COVID-19 kibernetski napadi ne ozirajo na državne meje niti na geografsko oddaljenost. Kibernetski kriminalci, ki s pridom izkoriščajo negotove pandemične razmere, svoje aktivnosti skrbno organizirajo in načrtujejo ob ustrezni finančni podpori, zato je njihov »uspeh« zelo pogosto zagotovljen.

Izkušnje kažejo, da je poleg samih tehnoloških rešitev v boju proti kibernetskim grožnjam ključnega pomena ustrezno znanje in ozaveščenost druge strani, torej uporabnikov informacijskih storitev. Ker smo ugotovili, da se v slovenskem prostoru na problematiko s COVID-19 povezanega kibernetskega kriminala tako v znanstvenih kot v strokovnih krogih premalo opozarja, smo s pričujočim prispevkom želeli to vrzel omiliti in tako prispevati k boljši ozaveščenosti zainteresirane slovenske javnosti.

Ključni doprinos našega dela predstavljajo smernice za obvladovanje kibernetskih tveganj, ki smo jih prilagodili razmeram pandemije. Z implementacijo smernic v svoja okolja bodo podjetja lažje in učinkoviteje botrovala intenzivnim in agresivnim akcijam kiber kriminalcev in s tem ključno doprinesla k bolj stabilnemu poslovanju svoje organizacije. Smernice so uporabne za vse organizacije v segmentu MSP, predvsem pa bodo po našem mnenju dobrodošle za mikro in mala podjetja, kjer se običajno soočajo z zelo omejenimi resursi, predvsem z vidika ustreznih znaj in kompetenc na področju kibernetske varnosti.

Tabela 1: Smernice za obvladovanje kibernetskih tveganj v okolju MSP

Identificiraj Aktivnosti v tej kategoriji so organizaciji v pomoč pri razumevanju potrebe po varovanju svojih resursov in obvladovanju kibernetskih tveganj.	
Aktivnost/cilj	**Dodatna pojasnila**
Definirana je »politika informacijske/kibernetske varnosti«.	– V varnostni politiki naj bo opredeljeno, kateri podatki/informacije in drugi resursi IS so za organizacijo pomembe, zakaj jih je potrebno zaščititi ter kdo je odgovoren za implementacijo določil varnostne politike. – Vsi zaposleni naj podpišejo izjavo o seznanjenosti z varnostno politiko in ostalimi dokumenti, ki iz nje izhajajo (postopki, procedure, pravilniki ipd.). – Varnostna politika naj bo formalno zapisana. Z njo morajo biti seznanjeni vsi deležniki (zaposleni, zunanji sodelavci). – Varnostna politika naj se revidira in posodablja na letni ravni.
Vloge in odgovornosti na področju informacijske/kibernetske varnosti so za vse deležnike jasno opredeljene.	– Pri opredeljevanju vlog in odgovornosti na področju informacijske/kibernetske varnosti je treba upoštevati vse zaposlene in zunanje sodelavce. – Vloge naj bodo ustrezno koordinirane in usklajene med vsemi deležniki, vsi morajo biti z njimi seznanjeni. – Določi naj se skrbnik za informacijsko/kibernetsko varnost. V primeru večje organizacije se lahko določi tudi ustrezni tim, ki ga poleg skrbnika za informacijsko/kibernetsko varnost sestavljajo še predstavniki ključnih procesov organizacije. – Pri večjih organizacijah se priporoča, da je funkcija skrbništva nad informacijsko/kibernetsko varnostjo ločena od IT oddelka in neposredno podrejena vodstvu organizacije.
Identificirani so ključni procesi organizacije.	– Ker je običajno zelo težko obvladovati celotno organizacijo, se je treba osredotočiti na tiste poslovne procese, ki so za poslovanje organizacije strateškega pomena. – Za vsak tak proces je treba oceniti stopnjo njegove podprtosti (odvisnosti) od IKT infrastrukture. – Z vidika kibernetske varnosti so ključni tisti procesi, ki so za poslovanje organizacije strateškega pomena, pri čemer je stopnja njihove odvisnosti od IKT infrastrukture visoka.
Identificirani so ključni resursi informacijskega sistema. Za posamezni ključni resurs je določena njegova vrednost glede na njegovo pomembnost pri izvajanju ključnih procesov.	– Ključni resursi so vsi resursi IS organizacije, ki so za izvajanje ključnih procesov strateškega pomena. – Upoštevati je treba strojno opremo, programsko opremo, zbirke podatkov in podatkovne tokove, druge informacije v digitalni obliki, IS zunanjih partnerjev ipd. – Pomembnejša kot je vloga posameznega resursa pri izvajanju ključnih procesov, višja naj bo njegova ocena. – Pri ocenjevanju vrednosti resursa naj se uporabi 3–5-stopenjska kvalitativna lestvica (npr. 1 (nizka vrednost, resurs za izvajanje ključnih procesov ni pomemben oz. je pogrešljiv) – 5 (zelo visoka vrednost, resurs je za izvajanje ključnih procesov izjemnega pomena). Pri ocenjevanju je lahko v pomoč kakšna od uveljavljenih metodologij za ocenjevanje varnostnih tveganj (npr., ISO/IEC 27005).
Opredeljeno je, kdo in na kakšen način ima dostop do ključnih resursov.	– Preveriti je treba, kdo lahko dostopa do ključnih resursov in kakšne poverilnice se pri tem uporabijo (npr. administratorske pravice, geslo, ključ ipd.). – Treba je preveriti možnost tako fizičnega kot logičnega dostopa.

Identificiraj Aktivnosti v tej kategoriji so organizaciji v pomoč pri razumevanju potrebe po varovanju svojih resursov in obvladovanju kibernetskih tveganj.	
Aktivnost/cilj	**Dodatna pojasnila**
	– Predlagamo, da se pripravi sistematičen seznam dostopov po uporabniških računih, upoštevaje zaposlene in zunanje sodelavce.
Identificirane in dokumentirane so kibernetske grožnje, ki pretijo ključnim resursom.	– Kibernetska grožnja je vsaka okoliščina ali dogodek, ki (če se zgodi) lahko preko IKT tehnologije neposredno ali posredno negativno vpliva na samo organizacijo in njene resurse. – Neposredni vpliv se običajno pokaže kot motnja pri izvajanju poslovnih procesov oz. samem poslovanju, posredni vpliv pa lahko okrni zunanjo podobo, ugled pri poslovnih partnerjih, izzove morebitne sodne spore ipd.. – Kibernetska grožnja se lahko realizira na različne načine, kot npr.: nepooblaščen dostop, nepooblaščena sprememba, uničenje ali razkritje informacij in/ali ohromitev storitve. – Za posamezen ključni resurs naj se pripravi seznam relevantnih groženj, ki mu pretijo.
Za ključne resurse so identificirane in dokumentirane ranljivosti z vidika kibernetske varnosti.	– Ranljivost z vidika kibernetske varnosti je vsaka pomanjkljivost resursa organizacije, ki jo kibernetska grožnja lahko izkoristi. – Ranljivosti se lahko nanašajo na tehnološke pomanjkljivosti (npr. hrošči v programski opremi), organizacijske pomanjkljivosti (npr. slabosti v konfiguraciji sistemov, nedorečeni in/ali neusklajeni postopki) ali na neustrezen nadzor nad obstoječimi varnostnimi kontrolami in mehanizmi.
Izvaja se sistematično ocenjevanje kibernetskih tveganj za ključne procese.	– Tveganje določimo za vsako kombinacijo ključni resurs – kibernetska grožnja, ki je za ta resurs relevantna. – Pri je treba upoštevati vrednost ključnega resursa, verjetnost realizacije posamezne grožnje in stopnjo izpostavljenosti tega resursa za to grožnjo. – Pri oceni stopnje izpostavljenosti je treba upoštevati identificirane ranljivosti in tudi že implementirane varnostne kontrole. – Pri ocenjevanju tveganj naj se uporabi kvalitativna lestvica (npr. 1 (zanemarljivo tveganje) – 8 (zelo visoko tveganje)). – Pri ocenjevanju je lahko v pomoč kakšna od uveljavljenih metodologij za ocenjevanje varnostnih tveganj (npr., ISO/IEC 27005).
Definirane so meje kritičnosti kibernetskih tveganj, skladno s katerimi so vzpostavljeni postopki za upravljanje s tveganji.	– Meje kritičnosti kibernetskih tveganj določimo po svoji presoji (npr. 1–2: nizko tveganje, tveganje sprejmemo; 3–4: zmerno tveganje, dolgoročno nadziramo in po potrebi ukrepamo; 5–6 srednje tveganje, zahteva srednjeročno obravnavo (npr. v roku 6 mesecev); 7–8: visoko tveganje, zahteva takojšnjo obravnavo. – Pri obravnavi tveganj imamo več možnosti: tveganje skušamo znižati na sprejemljivo raven (npr. z uvedbo dodatnih varnostnih kontrol), tveganju se skušamo izogniti (npr. zamenjava tehnologije) ali tveganje skušamo prenesti na tretjo osebo (npr. zavarovalnica). – Če so kritična tveganja povezana z zunanjimi partnerji, jih je treba nasloviti tudi v pogodbah o sodelovanju.
Definiran in vzpostavljen je »načrt odziva na kibernetski incident«.	– O kibernetskem incidentu govorimo, kadar je bila ranljivost nekega resursa IS izrabljena s strani ene ali več kibernetskih groženj. – Potencialni kibernetski incidenti naj se rangirajo glede na resnost posledic z vidika poslovanja organizacije. Za vsako kategorijo incidenta naj se pripravi scenarij odziva, v katerem se opredelijo aktivnosti, ki jih je treba opraviti. – Z načrtom morajo biti seznanjeni vsi deležniki (zaposleni, zunanji sodelavci). Načrt mora biti usklajen tudi z dobavitelji in morebitnimi zunanjimi ponudniki storitev.

Identificiraj Aktivnosti v tej kategoriji so organizaciji v pomoč pri razumevanju potrebe po varovanju svojih resursov in obvladovanju kibernetskih tveganj.	
Aktivnost/cilj	**Dodatna pojasnila**
	– Preveriti je treba tudi prilagojenost načrta razmeram pandemije. Namreč, v času pandemije je fizična prisotnost v organizaciji lahko omejena, zato je treba preveriti, ali bo možno koordinacijo ustrezno opraviti tudi na daljavo. V nasprotnem primeru je treba načrtovati in uskladiti fizično prisotnost v organizaciji. – V stabilnih razmerah (v času normalnega poslovanja, brez prisotnosti kibernetskih incidentov) je potrebno načrt periodično (vsaj na letni ravni) preskušati glede njegove učinkovitosti in ga po potrebi nadgraditi.
Definiran in vzpostavljen je »načrt okrevanja po kibernetskem incidentu«.	– »Načrt okrevanja po kibernetskem incidentu« je eden od temeljev zagotavljanja neprekinjenega izvajanja ključnih procesov organizacije in s tem neprekinjenega poslovanja. – V načrtu morajo biti jasno opredeljene vloge in odgovornosti posameznih deležnikov (zaposlenih, zunanjih partnerjev). Le-ti morajo biti z vsebino seznanjeni in jo razumeti. Načrt naj bo usklajen tudi z dobavitelji in morebitnimi zunanjimi ponudniki storitev. – V stabilnih razmerah (v času normalnega poslovanja, brez prisotnosti kibernetskih incidentov) je treba načrt periodično (vsaj na letni ravni) preskušati glede njegove učinkovitosti in ga po potrebi nadgraditi.

Zaščiti Aktivnosti v tej kategoriji zagotavljajo zmožnost omejevanja in/ali obvladovanja potencialnih kibernetskih incidentov.	
Aktivnost/cilj	**Dodatna pojasnila**
Za vse ključne resurse so vzpostavljeni mehanizmi kontrole logičnega dostopa.	– Vzpostavitev kontrole logičnega dostopa obsega naslednje aktivnosti: proces identifikacije (npr. dodelitev uporabniškega računa), avtentikacija (način in postopek preverjanja istovetnosti uporabnikov, npr. uporaba gesla), avtorizacija (upravljanje dostopnih pravic) ter vzpostavitev in vodenje dnevniških datotek. – Vsak uporabnik (tako zaposleni kot zunanji) naj ima dodeljen sebi lasten uporabniški račun. – Za običajno delo naj uporabniki na svojih računalnikih ne uporabljajo uporabniških računov z administratorskimi pravicami, kar preprečuje možnost (namerno ali nenamerno) nameščanja neavtorizirane programske opreme. – Po potrebi naj se vzpostavi uporabniški račun »gost« z minimalnimi dostopnimi pravicami (npr. zgolj dostop do interneta). – Od uporabnikov naj se zahteva ustrezna kompleksnost njihovih gesel (dolžina, vsebnost posebnih znakov) in tudi periodično spreminjanje le-teh. Premisli naj se o potrebi po uvedbi večfaktorske avtentikacije – Zagotovljeno naj bo, da se ob prenehanju sodelovanja z organizacijo (prenehanje zaposlitve ali pogodbenega sodelovanja) ukinejo vse dostopne pravice uporabnika, ki odhaja.
Pri upravljanju dostopnih pravic se dosledno upoštevata načeli »minimalnih dostopnih pravic« in »ločitev dolžnosti«.	– Zagotovljeno naj bo, da ima vsak uporabnik minimalen možen nivo in obseg dostopnih pravic, ki mu še zagotavlja nemoteno opravljanje njegovih delovnih nalog. – Ključne aktivnosti in naloge naj bodo porazdeljene na več oseb (npr. predložitev in potrditev pomembne (npr. finančne) transakcije naj ne bo v domeni ene osebe). Razvojno in tesno okolje naj bo ločeno od produkcijskega.
Uporabniki z višjimi dostopnimi pravicami (npr. skrbnik sistema) se zavedajo svoje odgovornosti.	– Skrbnik sistema naj ima poseben uporabniški račun za izvajanje administratorskih funkcij in drugi račun za izvajanje ostalih funkcij. – Skrbnik sistema naj nima možnosti spreminjanja vsebine dnevniških datotek.
Omrežje organizacije je ustrezno segmentirano in razdeljeno na varnostna območja različnih stopenj.	– O smiselnosti ukrepa se odloči glede na kompleksnost omrežja organizacije. Bolj kot je omrežje kompleksno, večja je smotrnost implementacije.
Brezžične dostopne točke so zaščitene.	– Zagotovljeno je, da so prednastavljene nastavitve brezžičnega usmerjevalnika zamenjane (SSID, uporabniško ime in geslo za administriranje). Nivo zaščite naj bo vsaj WPA-2 z AES. Pod nobenim pogojem naj se ne uporablja WEP. – Morebitni brezžični dostop za stranke in goste naj bo ločen od poslovnega omrežja.
Nameščena je zaščitna tehnologija, ki je ustrezno konfigurirana in redno posodabljana.	– Na vse naprave, ki se uporabljajo v omrežju organizacije (računalnike in mobilne naprave, tako na lokaciji organizacije kot v domačem okolju zaposlenih), naj se namesti programska oprema za zaznavanje prisotnosti škodljivega programja (npr. antivirusni program, program za odkrivanje vohunskega programja ipd.).

Zaščiti Aktivnosti v tej kategoriji zagotavljajo zmožnost omejevanja in/ali obvladovanja potencialnih kibernetskih incidentov.	
Aktivnost/cilj	**Dodatna pojasnila**
	– Na vse meje med posameznimi segmenti omrežja naj se namestijo požarne pregrade. Posebno pozornost je treba posvetiti meji med internim omrežjem organizacije in zunanjim omrežjem (internet). Skladno z možnostmi naj se aktivirajo tudi požarne pregrade na posameznih napravah v internem omrežju. – Namesti naj se tudi druga zaščitna tehnologija: sistem za zaznavanje/preprečevanje vdorov (IDS/IPS), filtriranje e-pošte, filtriranje dostopa do spletnih strani, id. – Pred implementacijo IDS/IPS sistemov je treba jasno opredeliti meje med normalnim in nenormalnim delovanjem IS. – Priporoča se tudi uporaba t. i. skenerjev ranljivosti (angl. vulnerability scanning). – Pri vsej uporabljeni tehnologiji je ob namestitvi treba zagotoviti zamenjavo prednastavljenega administratorskega računa.
Vzpostavljeni so mehanizmi za upravljanje in zaščito oddaljenega dostopa.	– V obdobju pandemije in intenzivne uporabe dela od doma napadalci pogosto izrabljajo ranljivost storitve za oddaljen dostop (angl. Remote Desktop Service - RDS), ki omogoča napadalcu zagon poljubne programske kode na ciljnem sistemu. Ranljive so različice Windows 7 in Windows Server 2008, Microsoft pa je izdal popravke tudi za starejše, nepodprte operacijske sisteme (več na https://www.cert.si/si-cert-2019-03/). Svetujemo takojšnjo namestitev popravkov. V nasprotnem primeru je nujno storitev RDS začasno onemogočiti ali vsaj zelo strogo omejiti na omrežnem nivoju. – Če je le možno, naj se za potrebe kakršnega koli oddaljenega dostopanja do internega omrežja organizacije vzpostavi VPN povezava.
Orodja za skupinsko delo so ustrezno zaščitena. Opredeljen je način hrambe poslovnih podatkov.	– Orodja za skupinsko delo (videokonference, klepetalnice ali druge oblike sporočanja) lahko delujejo na IKT opremi organizacije, ali pa organizacija uporablja storitve v oblaku. V obeh primerih je potrebno treba in z varnostno politiko uskladiti hrambo poslovnih podatkov (npr. vsebino klepetov, video posnetkov ipd.). – V primeru, da se ti podatki hranijo pri ponudniku storitve v oblaku, naj si organizacija pridrži pravico do njihove uporabe. Dogovoriti je treba tudi ukrepe v primeru zlorabe ponudnikove platforme.
Vsi deležniki so deležni rednega in sistematičnega izobraževanja in ozaveščanja na področju informacijske/ kibernetske varnosti.	– Za vse deležnike (zaposlene, zunanje sodelavce) naj se izvaja obvezno izobraževanje in ozaveščanje, ki naslavlja vprašanja, kot npr.: o zavedanje vloge in odgovornosti posameznika pri zagotavljanju informacijske/kibernetske varnosti v organizaciji, o seznanjanje z dovoljenimi in nedovoljenimi aktivnostmi (npr. dostop do zasebnega poštnega računa na službenih IKT napravah se ne dovoli), o ravnanje v primeru kibernetskega incidenta, – Pri načrtovanju izobraževalnih vsebin naj bo poseben poudarek tudi na grožnjah in tipih napadov, ki so se v obdobju pandemije izkazale za najbolj aktualne in pogoste (npr. socialni inženiring, izsiljevalsko programje, napadi z zvabljanjem ipd. (poglavje 4.3)). – Vsebina in zahtevnost izobraževanja in ozaveščanja naj se prilagodi znanju in potrebam posameznih skupin uporabnikov (npr. navadni uporabniki, IT osebje …). – Aktivnosti izobraževanja in ozaveščanja je treba takoj po zaposlitvi izvesti tudi za vsakega na novo zaposlenega. – Aktivnosti izobraževanja in ozaveščanja naj se izvajajo sistematično in kontinuirano (npr. hitro ozaveščanje na mesečni ravni, izobraževanje na letni ravni).

Zaščiti Aktivnosti v tej kategoriji zagotavljajo zmožnost omejevanja in/ali obvladovanja potencialnih kibernetskih incidentov.	
Aktivnost/cilj	**Dodatna pojasnila**
Občutljivi podatki so šifrirani.	– Občutljivi podatki, če organizacija z njimi razpolaga, naj bodo šifrirani tako med hranjenjem kot tudi med prenosom. – Poskrbeti je treba za varno hranjenje šifrirnih ključev in gesel za dostop do šifrirnih ključev.
Popravki programske opreme se redno in sistematično izvajajo.	• To velja tako za operacijski sistem kot za vso ostalo programsko opremo. – Uporablja naj se le taka programska oprema, za katero proizvajalec zagotavlja podporo, nadgrajevanje in vzdrževanje. – Koristno je določiti dan (npr. dan v tednu ali mesecu), ko se popravki samodejno preverijo in namestijo. – Interval samodejnega posodabljanja programske opreme naj se prilagodi potrebam (npr. anivirusni program se mora posodabljati na dnevni ravni, kakšna druga programska oprema pa lahko tudi redkeje).
Definirani so postopki za varno uničenje odsluženih podatkovnih nosilcev.	– Pred odstranitvijo IKT opreme iz uporabe je treba zagotoviti, da so vsi podatkovni nosilci varno uničeni. – Priporoča se uporaba specializiranih orodij, ki uporabljajo algoritme za varno brisanje z večkratnim prepisovanjem (angl. wipe) in tudi fizično uničenje.
Vzpostavljeni so postopki nadzora nad upravljanjem in spremembami konfiguracij.	– Pri upravljanju konfiguracij se upošteva načelo »minimalne zadostne funkcionalnosti«. – Postopki morajo biti dokumentirani, zagotovljena mora biti sledljivost izvedenih sprememb.
Zasebne naprave, ki se uporabljajo v internem omrežju organizacije, so ustrezno preverjene, zaščitene in ažurno posodobljene.	– Ustrezno pozornost je treba posvetiti vsem zunanjim IKT napravam, ki se povezujejo v interno omrežje organizacije (npr. za izvajanje dela od doma) in niso neposredno pod okriljem varnostne politike (npr. zasebne naprave, kot so telefoni, tablice, osebni računalniki, domača brezžična omrežja ipd.). Dogovoriti je treba tudi pravila uporabe teh naprav za družinske člane zaposlenega. – Za potrebe dostopa do internega omrežja organizacije so uporabniki dolžni te naprave uporabljati skladno z varnostno politiko organizacije (npr. obvezna uporaba varnega gesla).
Vzpostavljeni so postopki rednega in sistematičnega izvajanja varnostnih kopij. Varnostne kopije se ustrezno vzdržujejo in sistematično preskušajo glede berljivosti.	– Izdelati je treba režim izdelave varnostnih kopij tako, da le-teh ne bo mogoče ostraniti (npr. izbrisati) z internega omrežja. – Pri izvajanju varnostnih kopij naj se upošteva pravilo 3-2-1: za pomembne podatke se izdela 3 kopije, uporabi 2 različna medija, 1 kopija naj bo fizično ločena od ostalih. – V režim izvajanja varnostnih kopij je treba zajeti vse podatke, tudi tiste, ki se morda nahajajo na zasebnih napravah uporabnikov (ki npr. delajo od doma). – Varnostne kopije občutljivih podatkov naj se šifrirajo. – Po potrebi naj za storitev izvajanja varnostnih kopij organizacija angažira zunanjega ponudnika.
Vzpostavljene so dnevniške datoteke.	– Skladno z možnostmi uporabljene zaščitne tehnologije naj se vzpostaviti beleženje dogodkov v dnevniške datoteke. Ti zapisi so uporabni v primeru analize nastalega kibernetskega incidenta (npr. vzroki, načini, učinki ipd.) in so lahko v pomoč pri odzivu na incident. – Izvajajo naj se varnostne kopije dnevniških datotek, ki naj se hranijo vsaj eno leto.

Zaščiti Aktivnosti v tej kategoriji zagotavljajo zmožnost omejevanja in/ali obvladovanja potencialnih kibernetskih incidentov.	
Aktivnost/cilj	**Dodatna pojasnila**
Vzpostavljena so načela fizične varnosti.	– Čeprav se informacijska/kibernetska varnost v veliki meri osredotoča na zaščito logičnih dostopov do resursov IS organizacije (tj. preko komunikacijskih poti), se je treba zavedati, da je predpogoj za doseganje ustreznega nivoja logične varnosti vzpostavljen ustrezen nivo fizične varnosti. – V kategorijo fizične varnosti spadajo: nadzor fizičnih dostopov do resursov organizacije, zagotavljanje stabilne in neprekinjene oskrbe z električno energijo, zaščita zoper druge fizične grožnje (npr. ogenj, voda ipd.). – V pomoč pri implementaciji je lahko kakšna izmed uveljavljenih dobrih praks (npr. standard ISO/IEC 27002).

Zaznaj Aktivnosti v tej kategoriji omogočajo ažurno zaznavanje morebitne prisotnosti kibernetskih incidentov.	
Aktivnost/cilj	**Dodatna pojasnila**
S pomočjo nameščene tehnologije se dogajanje v internem omrežju organizacije kontinuirano nadzira.	– Izvaja naj se kontinuiran nadzor omrežnega prometa z namenom odkrivanja potencialno škodljivih oblik prometa. – Izvaja naj se preverjane prisotnosti škodljivega programja. Koristno je antivirusni program nastaviti tako, da se pregled vseh pomnilniških medijev samodejno izvaja periodično (npr. na dnevni ravni, lahko tudi v nočnem času). – Periodično naj se izvaja skeniranje ranljivosti.
Nadzorni procesi se kontinuirano nadgrajujejo in v skladu z izkušnjami izboljšujejo.	– Kontinuirano izboljševanje je eden od ključnih principov obvladovanja kibernetske varnosti.

Reagiraj Aktivnosti v tej kategoriji so pomembe za učinkovito omejevanje kibernetskega incidenta in obvladovanje njegovih posledic.	
Aktivnost/cilj	**Dodatna pojasnila**
V primeru zaznanega kibernetskega incidenta se aktivira »načrt odziva na kibernetski incident«.	– Izvede naj se scenarij načrta, skladno s stopnjo kritičnosti zaznanega kibernetskega incidenta.
Morebitne na novo odkrite ranljivosti se dokumentirajo in ustrezno obravnavajo.	– Na novo odkrite ranljivosti naj se obravnavajo skladno z vzpostavljeni postopki za upravljanje s kibernetskimi tveganji.
Prouči naj se možnost in/ali smotrnost zavarovanja za kibernetsko varnost.	– Tudi nekatere zavarovalnice v Sloveniji že ponujajo to možnost (npr. Zavarovalnica Triglav https://vsebovredu.triglav.si/tehnologija/kibernetska-zascita).
Po zaključenih postopkih odziva se na podlagi izkušenj »načrt odziva na kibernetski incident« ustrezno korigira in nadgradi.	– Kontinuirano izboljševanje je eden od ključnih principov obvladovanja kibernetske varnosti.

Obnovi Aktivnosti v tej kategoriji pomagajo organizaciji pri vzpostavitvi normalnega delovanja informacijskega sistema po opravljenem kibernetskem incidentu.	
Aktivnost/cilj	**Dodatna pojasnila**
Po zaključenih postopkih odziva (lahko tudi vmes) se aktivira in izvede »načrt okrevanja po kibernetskem incidentu«.	– Za uspešno in učinkovito vzpostavitev normalnega delovanja je ključnega pomena ustrezno predpripravljen »načrt okrevanja po kibernetskem incidentu« (funkcija »identificiraj«). – Za uspešnost obnovitvenih postopkov imajo lahko ključno vlogo varnostne kopije (funkcija »identificiraj«). – »Načrt okrevanja po kibernetskem incidentu« bo v »izrednih« razmerah učinkovito deloval, če bo v »normalnih« razmerah večkrat preskušen.
Po zaključenih postopkih okrevanja se na podlagi izkušenj »načrt okrevanja po kibernetskem incidentu« ustrezno korigira in nadgradi	– Kontinuirano izboljševanje je eden od ključnih principov obvladovanja kibernetske varnosti.

Literatura

Aldasoro, I., Frost, J., Gambacorta, L. in Whyte, D. (2021). Covid-19 and cyber risk in the financial sector, BIS Bulletin, 37, 14 January 2021. dosegljivo na: https://www.bis.org/publ/bisbull37.htm

Alzahrani, A. (2020). Coronavirus Social Engineering Attacks: Issues and Recommendations, *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(5), str. 154-161, doi: http://dx.doi.org/10.14569/IJACSA.2020.0110523

APWG (2021). Phishing Activity Trends Report, 4th Quarter 2020, Anti Phishing Working Group – APWG, 9 February 2021. dosegljivo na https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

Bartik, A. W., Bertrand, M., Cullen, Z., Glaeser, E. L., Luca, M. in Stanton, C. (2020). The Impact of COVID-19 on Small Business Outcomes and Expectations, *Proceedings of the National Academy of Sciences*, Jul 2020, 117 (30) 17656-17666; doi: 10.1073/pnas.2006991117

Baz, M., Alhakami, H., Agrawal, A., Baz, A. in Khan, R. A. (2021). Impact of covid-19 pandemic: a cybersecurity perspective, *Intelligent Automation & Soft Computing*, 27(3), str. 641–652, 2021.

Beglaryan, M. in Shakhmuradyan, G. (2020). The impact of COVID-19 on small and medium-sized enterprises in Armenia: Evidence from a labor force survey, *Small Business International Review*, 4(2), str. 298-298, doi: https://doi.org/10.26784/sbir.v4i2.298

Benz, M. in Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs, *Business Horizons*, 63(4), str. 531-540, https://doi.org/10.1016/j.bushor.2020.03.010.

Bonazzi, R., Cimmino, F. M., Beuchat, J. in Vérolet, F. (2020). Tracing Effects of Covid-19 Over Small and Medium Enterprises, *Proceedings of the ENTRENOVA - ENTerprise REsearch InNOVAtion Conference*, Virtual Conference, 10. – 12. september 2020, IRENET - Society for Advancing Innovation and Research in Economy, Zagreb, str. 309-321, dosegljivo na https://ideas.repec.org/h/zbw/entr20/224698.html

Buchanan Turner, C., Turner, C. in Shen, Y. (2020). Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior, *Proceedings of The 3rd International Conference on Research in Social Sciences*, 27. – 29. november, 2020, Dublin, Republic of Ireland, dosegljivo na https://www.dpublication.com/abstract-of-3rd-rssconf/2012-12/

Carrapico, H. in Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy, *Journal of European Integration*, 42(8), str.1111-1126, doi: 10.1080/07036337.2020.1853122

Chigada, J. in Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, 23(1), 11 str. doi:https://doi.org/10.4102/sajim.v23i1.1277

CISCO (n.d.). *Beyond Survival: A Small Business Resiliency Guide.* CISCO, dosegljivo na https://www.cisco.com/c/en/us/solutions/small-business/small-business-recovery.html

Check Point (2020). *Cyber Attack Ttrends: 2020 Mid-Year Report*, Check Point Software Technologies Ltd., dosegljivo na https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/

Check Point (2020a). *Cyber Security in the Age of Coronavirus*, Check Point Software Technologies Ltd., dosegljivo na https://pages.checkpoint.com/cyber-security-in-the-age-of-coronavirus.html

Deloitte (2020). 2020 *Deloitte–NASCIO Cybersecurity Study States at Risk: The Cybersecurity Imperative in Uncertain Times*, A Joint Biennial Report (6th Ed. From Deloitte and the National Association of State Chief Information Officers (NASCIO), dosegljivo na https://www2.deloitte.com/us/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K. in Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55, 102211. 0.1016/j.ijinfomgt.2020.102211.

ECSO (2020). *ECSO Barometer 2020: »Cybersecurity in Light of COVID-19 Crisis«, Report on the results of surveys with ECSO members and the cybersecurity community*, European Cyber Security Organisation (ECSO), dosegljivo na https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf

ECSO (2020a). *ECSO Recommendations on Cybersecurity in Light of the COVID-19 Crisis*, European Cyber Security Organisation (ECSO), dosegljivo na https://ecs-org.eu/documents/publications/5f6ca2989c78f.pdf

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H. in Zahra, F. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. Preprints 2020, doi: 10.20944/preprints202009.0630.v1

ETH (2020). *The Evolving Cyber Threat Landscape during the Coronavirus Crisis*, Center for Security Studies (CSS), ETH Zürich, dosegljivo na https://css.ethz.ch/en/services/digital-library/publications/publication.html/6a9f69c0-46d0-46d4-b789-398a04d2f0c4

Europol (2020). *Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis*, Europol, dosegljivo na https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Fairlie, R. (2020). The impact of COVID-19 on small business owners: Evidence from the first three months after widespread social-distancing restrictions. *J Econ Manage Strat*., 29, str. 727–740. https://doi.org/10.1111/jems.12400

FAL (2020). *Cybersecurity in the time of COVID-19 and the transition to cyberimmunity*, Facilitation of Transport and Trade in Latin America and the Caribbean, FAL Bulletin, št. 6, ISSN: 1564-4227, dosegljivo na https://repositorio.cepal.org/bitstream/handle/11362/46511/1/S2000678_en.pdf

Gallagher, S. in Brandt, A. (2020). Facing down the myriad threats tied to covid-19, dosegljivo na https://news.sophos.com/enus/2020/04/14/covidmalware

Georgiadou, A., Mouzakitis, S. in Askounis, D. (2020). Towards Assessing Critical Infrastructures' Cyber-Security Culture During COVID-19 Crisis: A Tailor-made Survey. Wyld D. C. et al. (Eds): CSEA, DMDBS, NSEC, NETWORKS, Fuzzy, NATL, SIGEM – 2020, str. 71-80, 2020. CS & IT - CSCP 2020, doi: 10.5121/csit.2020.101806

Georgiadou, A., Mouzakitis, S. in Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*. https://doi.org/10.1057/s41284-021-00286-2

Gourinchas P.O., Kalemli-Özcan, S., Penciakova, V. in Sander, N. (2020). Covid-19 and SME Failures. National Bureau of Economic Research No. w27877, doi: 10.3386/w27877

Gregurec, I., Tomičić Furjan, M. in Tomičić-Pupek, K. (2021). The Impact of COVID-19 on Sustainable Business Models in SMEs. *Sustainability*, 2021 (13), 1098. https://doi.org/10.3390/su13031098

Hakak, S., Khan, W. Z., Imran, M., Choo, K. R. in Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies, *IEEE Access*, 8, str. 124134-124144, doi: 10.1109/ACCESS.2020.3006172

Hijji, M. in Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions, *IEEE Access*, 9, str. 7152-7169, doi: 10.1109/ACCESS.2020.3048839

Hope, A. (2021). DDoS Attacks Increased Rapidly During the COVID-19 Pandemic as Hackers Exploited New Tools and Techniques, *CPO Magazine*, 29 January 2021. dosegljivo na https://www.cpomagazine.com/cyber-security/ddos-attacks-increased-rapidly-during-the-covid-19-pandemic-as-hackers-exploited-new-tools-and-techniques/

ICC (n.d.). COVID-19: *Cyber security threats to MSMEs, An ICC guide to help MSMEs minimise cyber security risks during the COVID-19 crisis*, International Chamber of Commerce, dosegljivo na https://iccwbo.org/publication/covid-19-cyber-security-threats-to-msmes/

Insikt Group (2020). *Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide*, Recorded Future, FR-2020-0312. dosegljivo na https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

Interpol (2020). *Cybercrime: COVID-19 Impact*, INTERPOL General Secretariat, dosegljivo na https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Karr, J., Loh, K. in Wirjo, A. (2020). Supporting MSMEs' Digitalization Amid COVID-19, APEC Policy Support Unit, *POLICY BRIEF*, 35, July 2020, Asia-Pacific Economic Cooperation, dosegljivo na https://www.apec.org/Publications/2020/07/Supporting-MSMEs-Digitalization-Amid-COVID-19

Karpenko, O., Kuczabski, A. in Havryliak, V. (2021). Mechanisms for providing cybersecurity during the COVID-19 pandemic: Perspectives for Ukraine. *Security and Defence Quarterly*, 33(1). https://doi.org/10.35467/sdq/133158

Kashif, M., idr. (2020). A Surge in Cyber-Crime During COVID-19. *Indonesian Journal of Social and Environmental Issues*, 1(2), str. 48-52, dosegljivo na https://www.neliti.com/publications/319380/a-surge-in-cyber-crime-during-covid-19

Khan, N. A., Brohi, S. N. in Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. *TechRxiv*. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1

KPMG (2020). *Surviving and thriving through a pandemic. COVID-19 Risk assessment survey*, KMPG, dosegljivo na https://assets.kpmg/content/dam/kpmg/in/pdf/2020/06/kpmg-covid-survery-2020.pdf.

Kumaran, N. in Lugani, S. (2020). Protecting businesses against cyber threats during covid-19 and beyond, dosegljivo na https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Kupreev, O., Badovskaya, E. in Gutnikov, A. (2020). *DDoS attacks in Q1 2020, SECURELIST*, Kaspersky, 6 May 2020, dosegljivo na https://securelist.com/ddos-attacks-in-q1-2020/96837/

Kyung, A. in Whitney, S. (2020). A Study on The Financial and Entrepreneurial Risks of Small Business Owners Amidst COVID-19, *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Vancouver, BC, Canada, 2020, str. 1-4, doi: 10.1109/IEMTRONICS51293.2020.9216384

Lallie, H.S., Shepherd, L. A., Nurse, J. R. C., Erola, A. Epiphaniou, G., Maple, C. in Bellekens, X. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, *arXiv*:2006.11929, dosegljivo na https://arxiv.org/abs/2006.11929

Malhotra, H. in Dave, D. (2020). A Comparative Study of Cyber Attacks during Covid-19, *High Technology Letters*, 26(9), str. 1394-1404. doi: 10.37896/HTL26.09/1834, dosegljivo na http://www.gjstx-e.cn/Vol-26-Issue-9/

Malwarebytes (2020). *Enduring from home COVID-19's impact on business security*, Malwarebytes, dosegljivo na https://resources.enterprisetalk.com/ebook/Malwarebytes-Enterprise-EN-7-landing.html

Mandal, S. in Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic, *Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2020, str. 837-842, doi: 10.1109/ICOSEC49089.2020.9215374

Meghisan-Toma, G. M. in Nicula, V. C. (2020). ICT Security Measures for the Companies within European Union Member States – Perspectives in COVID-19 Context, *Proceedings of the International Conference on Business Excellence*, Sciendo, 14(1), str. 362-370. https://doi.org/10.2478/picbe-2020-0035

Mihailović, A. in Rašović, N. (2020). Cybersecurity in the New Reality: Systematic Review in the Context of COVID-19, *International Journal of Innovative Science and Research Technology*, 5(12), str. 1088-1091.

Mimecast (2020). *100 Days of Coronavirus (COVID-19)*, Mimecast, dosegljivo na https://www.mimecast.com/resources/white-papers/threat-intelligence-report-100-days-of-coronavirus/

Muthuppalaniappan, M. in Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International journal for quality in health care : journal of the International Society for Quality in Health Care*, 33(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime, *European Journal of Information Systems*, 29(3), str. 306-321, doi: https://doi.org/10.1080/0960085X.2020.1771222

Nazarov, D. M., Kovtun, D. B. in Reichert, T. N. (2020). SAP Analytics Cloud: intellectual analysis of small and medium-sized business activities in Russia in the context of COVID-19, *2020 IEEE 14th*

International Conference on Application of Information and Communication Technologies (AICT), Tashkent, Uzbekistan, 2020, str. 1-6, doi: 10.1109/AICT50176.2020.9368635.

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1., April 16, 2018, National Institute of Standards and Technology, dosegljivo na https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST (2020). *Respondent Summary Report Business Survey: COVID-19 Impacts and Recovery in the Context of Complex Events*, NIST SP - 1264, December 2020, National Institute of Standards and Technology, dosegljivo na https://www.nist.gov/publications/respondent-summary-report-business-survey-covid-19-impacts-and-recovery-context-complex

Okereafor, K. in Manny, P. (2020). Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic. *International Journal in IT & Engineering (IJITE)*, 8(6), str. 13-23. doi: 10.6084/m9.figshare.12421049.

Omodunbi, B. A., idr. (2020). Cyber Security Threats in the Era of COVID-19 Pandemic: A Case Study of Nigeria System. *International Journal of Advanced Research in Engineering and Technology*, 11(9), str. 387-396. dosegljivo na: https://ssrn.com/abstract=3713682

Papadopoulos, T., Baltas, K. N. in Balta, M. E. (2020). The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice, International Journal of Information Management, 55(2020). https://doi.org/10.1016/j.ijinfomgt.2020.102192.

Toth, P. in Paulsen, C. (2016). Small Business Information Security: The Fundamentals, NISTIR 7621, Revision 1, National Institute of Standards and Technology, dosegljivo na https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

PwC (2020). *Managingthe impact of COVID-19 on cybersecurity*, Pricewaterhouse Coopers, dosegljivo na https://www.pwccn.com/en/issues/cybersecurity-and-privacy/covid-19-impact-mar2020.html

PwC (2020a). *Succeeding in Uncertainty: Responding to COVID-19, Cybersecurity*, Pricewaterhouse Coopers, dosegljivo na https://www.pwc.com/jg/en/issues/covid-19/covid-19-succeeding-in-uncertainty.pdf

Ravindran, T. in Boh, W. F. (2020). Lessons From COVID-19: Toward a Pandemic Readiness Audit Checklist for Small and Medium-Sized Enterprises, IEEE Engineering Management Review, 48(3), str. 55-62. doi: 10.1109/EMR.2020.3015488.

Sage, O. (2018). Every Small Business Should Use the NIST Cybersecurity Framework, White Paper, april 2020, CyberRx, dosegljivo na https://cyber-rx.com/wp-content/uploads/2020/04/CyberRx-white-paper_SMBs-should-use-NIST-CSF_2018.pdf

Salahdine, F. in Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*. 11(4):89. https://doi.org/10.3390/fi11040089

Santiago-Omar in Caballero-Morales, (2021). Innovation as recovery strategy for SMEs in emerging economies during the COVID-19 pandemic, Research in International Business and Finance, 57, 101396. https://doi.org/10.1016/j.ribaf.2021.101396

Savitha, J. (2020). A Study on the Cybersecurity Campaigns for the Coronavirus Pandemic. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 6(6), str. 263-267. doi: 10.32628/CSEIT206648.

Sriram, P., Karnik, A. in Grindstaff, L. (2020). *COVID-19 – Malware Makes Hay During a Pandemic*, McAfee, 06 May 2020. dosegljivo na https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/#_Toc37776299

Shi, F. (2020). Threat spotlight: Coronavirus-related phishing, dosegljivo na https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

SI-CERT (2020). Izkoriščanje COVID-19 v kibernetskih napadih, SI-CERT 2020-01, dosegljivo na https://www.cert.si/si-cert-2020-01/

Tam, T., Rao, A. in Hall, J. (2020). The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath, *Digital Government: Research and Practice*, 2(2), str. 23:1-23:8. doi: https://doi.org/10.1145/3436807

Tam, T., Rao, A. in Hall, J. (2021). Rapid Cybersecurity Assessment System for Small Business' COVID Move to Online, Workshop on Secure IT Technologies against COVID-19 (CoronaDef) 2021, 21 February 2021, Virtual, https://dx.doi.org/10.14722/coronadef.2021.23004

Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M. in Saldamli, G. (2020). Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model, *Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*, Valencia, Spain, 2020, str. 113-118, doi: 10.1109/MCNA50957.2020.9264301.

Thales (2020). *Covid-19 Threats on remote working*, Thales, dosegljivo na https://www.thalesgroup.com/sites/default/files/database/document/2020-04/2020-04-03_COVID-19_THREAT_ON_REMOTE_WORKING_%28ENG%29%20%283%29.pdf

Thales (2020a). *COVID-19 Cyber Threat Assessment, Cyber Threat Intelligence Assessment*, Thales, dosegljivo na https://www.thalesgroup.com/sites/default/files/database/document/2020-04/2020-03-24_COVID-19_CYBER_THREAT_ASSESSMENT_%28ENG%29_0.pdf

Toapanta Toapanta, S. M., Alfredo Espinoza Carpio, J. in Mafla Gallegos, L. E. (2020). An Approach to Cybersecurity, Cyberbullying in Social Networks and Information Security in Public Organizations during a Pandemic: Study case COVID-19 Ecuador, Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI), Bogotá, Colombia, 2020, str. 1-6, doi: 10.1109/CONIITI51147.2020.9240375.

Trend Micro (2020). *Developing Story: COVID-19 Used in Malicious Campaigns*, Trend Micro, November 11, 2020. dosegljivo na https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Venkatesha, S., Reddy, K. R. in Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. *SN Computer Science*, 2, 78. https://doi.org/10.1007/s42979-020-00443-1

Warburton, D. idr. (2020). *2020 Phishing and Fraud Report, Phishing During A Pandemic*, F5 Labs. dosegljivo na https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/ F5Labs-2020-Phishing-and-Fraud-Report.pdf

Warren, T. (2021). Windows 7 is still running on at least 100 million PCs, It could be even more than 100 million, The Verge, Jan 6, 2021. dosegljivo na https://www.theverge.com/2021/1/6/22217052/microsoft-windows-7-109-million-pcs-usage-stats-analytics

Weil, T. in Murugesan, S. (2020). IT Risk and Resilience - Cybersecurity Response to COVID-19, *IT Professional*, 22(3), str. 4-10, doi: 10.1109/MITP.2020.2988330.

Wiggen, J. (2020). The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities. Konrad Adenauer Stiftung. doi:10.2307/resrep25300.