UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

KIBERNETSKA VARNOST IZBRANEGA PODJETJA

Ljubljana, junij 2022 BORUT PILETIČ

IZJAVA O AVTORSTVU

Podpisani Borut Piletič, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Kibernetska varnost izbranega podjetja, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Miro Gradišar

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
ALO – (angl. Annual Loss Expectancy); pričakovana letna izguba
ARO – (angl. Annual Rate of Occurence – ARO); letna stopnja pojavljanja
GDPR – (angl. General Data Protection Regulation); Splošna uredba varstva osebnih podatkov
HTTPS – (angl. Hypertext Transfer Protocol Secure); varni HTTP-protokol
IT – (angl. Information Technology); informacijske tehnologije
KPI – (angl. Key Performance Indicator); ključni kazalnik uspešnosti
LAN – (angl. Local Area Network); lokalno omrežje
NIST – (angl. National Institute of Standards and Technology); Nacionalni inštitut za standarde in tehnologijo

RDP – (angl. Remote Desktop Protocol); protokol oddaljenega namizja
SLE – (angl. Single Loss Exposure); stopnja vpliva
VPN – (angl. Virtual Private Network); navidezno zasebno omrežje

UVOD

Živimo v času hitrega tehnološkega napredka, ki je skoraj brez izjeme možen zaradi povečanja računske moči procesorja, kot ga opisuje tudi Moorov zakon (Rotman, 2020). Zaradi vsesplošne informatizacije poslovnih procesov in široke uporabe informacijskih tehnologij so podjetja dnevno postavljena pred izziv, kako zavarovati svoje najpomembnejše sredstvo – informacije. O tem, da se je za podjetja povečal izziv varnosti, govori dejstvo, da informacijska varnost ni več le integrirana v domeno informacijsko-tehnoloških (v nadaljevanju IT) služb, ampak so zato nastali ločeni profili kompetenc, specializiranih za informacijsko varnost (primer: direktor informacijske varnosti, angl. Chief Information Security Officer – CISO), kakor tudi ločeni oddelki, namenjeni informacijski varnosti (Yildirim, 2017, str. 18).

Jedro upravljanja informacijske varnosti je trajni proces ocenjevanja tveganja, ki zajema naslednje: ugotavljanje varnostnih tveganj in groženj, merjenje in ocenjevanje vzpostavljenih varnostnih kontrol ter izvrševanje načrtov za reševanje odkritih ranljivosti in pomanjkljivosti (Mujeeb, 2019).

Na podlagi svojih delovnih izkušenj predpostavljam, da informacijska varnost organizacijam predstavlja vedno večji izziv tudi zaradi trenutno aktualne globalne zdravstvene krize, zaradi katere so se podjetja morala na pandemijo prilagoditi z delom od doma. Glavni medij komunikacije je postal internet. Interna omrežja so se preselila na navidezna zasebna omrežja (angl. Virtual Private Network, v nadaljevanju VPN), sestanke in sejne sobe nadomeščajo konferenčni klici, delovna komunikacija poteka prek oblačnih platform za skupinsko komuniciranje (primer: Microsoft Teams) ter projektno vodenje s pomočjo oblačnih aplikacij (primer: Jira). Glede na opravljeno globalno študijo Grant Thornton je bilo že vsako šesto podjetje v preteklosti tarča določene oblike kibernetskega napada (Weishäup, Yasasin & Schryen, 2018, str. 2). Poročilo IBM Security za leto 2019, ki je posledica študije inštituta Ponemon, ocenjuje, da je povprečni strošek uhajanja zaupnih informacij zaradi kibernetskih napadov ocenjen na okoli 3,92 milijona dolarjev. Vrtoglavi znesek je odraz povprečja nekaterih večjih napadov. Eden od takšnih primerov je British Airways, ki je leta 2018 doživel kibernetski napad spletne strani in mobilne aplikacije. V njem so odtujili osebne podatke, vključno s podatki kreditnih kartic, za približno 400.000 strank. Za nastali incident jim je informacijski pooblaščenec na podlagi kršitve Splošne uredbe o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR) naložil kazen v višini 183 milijonov funtov (Gromenko, 2018, str. 12).

Namen magistrskega dela je v izbranem podjetju ugotoviti stanje kibernetske varnosti z uporabo naslednjih dveh analiz:

– analize ozaveščenosti zaposlenih o kibernetski varnosti in
– analize omrežja VPN.

Cilj je na podlagi analiz izdelati seznam predlogov izboljšav za posamezna področja, kjer so bile odkrite varnostne pomanjkljivosti oz. ranljivosti.

V prvem poglavju s proučevanjem literature predstavim področje kibernetske varnosti. Sledi predstavitev procesov upravljanja kibernetske varnosti in upravljanja tveganj, ki predstavlja jedro upravljanja kibernetske varnosti. Kot rešitev za izzive upravljanja kibernetske varnosti poglavje zaključim s pregledom delovnih ogrodij in podrobneje predstavim delovno ogrodje Nacionalnega inštituta za standarde in tehnologijo (angl. National Institute of Standards and Technology, v nadaljevanju NIST).

V empiričnem delu naloge s pomočjo anketnega vprašalnika najprej analiziram stanje ozaveščenosti zaposlenih v izbranem podjetju o kibernetski varnosti. Analiza je razdeljena na naslednja tri področja: varna uporaba računalnika, varnost na spletu in upravljanje uporabniških podatkov. Na podlagi pridobljenih rezultatov analize nato pripravim seznam predlogov izboljšav oz. rešitev za posamezno področje. V drugem delu analize na podlagi intervjuja IT-službe podjetja analiziram stanje kibernetske varnosti VPN-omrežja.

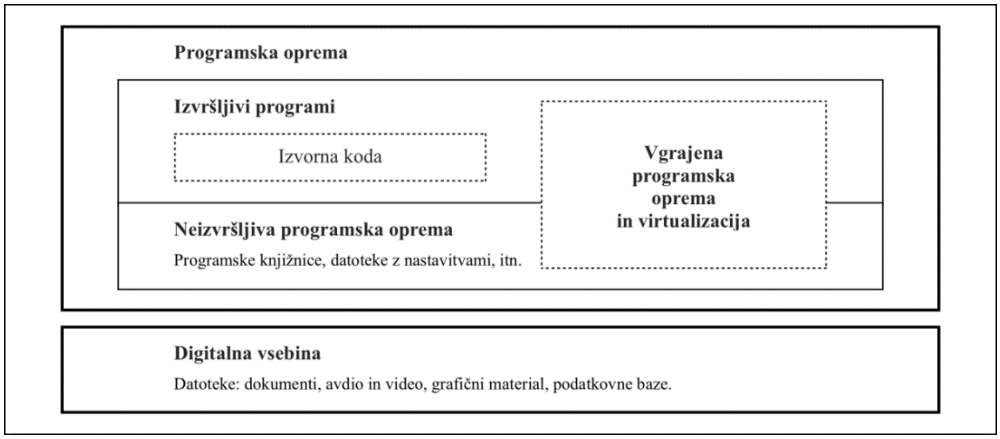
1 KIBERNETSKA VARNOST PODJETJA

Široka digitalizacija poslovanja, ki smo ji danes priča, je za podjetja neposredno odprla nov tehnološki izziv oziroma področje, imenovano kibernetska varnost. Skoraj vsak teden lahko beremo naslove novic, v katerih so žrtve kibernetskih napadov multinacionalne korporacije, kot so Sony, Apple, JP Morgan Chase, Target in druge. Čeprav po navadi beremo imena znanih zahodnih podjetij, se vdori prav tako dogajajo tudi v podjetjih na Kitajskem, Bližnjem vzhodu, Rusiji in drugod po svetu. Opravka imamo z globalnim problemom. Na tej točki se Donaldson, Siegel, Williams in Aslam (2015, str. xxxi) sprašujejo, če so v boju proti kibernetskim napadom neuspešna tako velika podjetja, kakšne imajo potem realne možnosti zaščite pred kibernetskimi napadi srednje velika in majhna podjetja. Dejstvo je, da je lahko škoda, ki jo podjetje utrpi po kibernetskem napadu, lahko nepopravljiva (Donaldson, Siegel, Williams & Aslam, 2015, str. 31). O resnosti izzivov priča tudi zadnji odmevni hekerski napad v Združenih državah Amerike (v nadaljevanju ZDA), ki je v času nastajanja tega magistrskega dela prizadel naftovodni sistem v zvezni državi Teksas. Podjetje Colonial Pipeline, ki upravlja naftovod za oskrbo Vzhodne obale, je doživelo napad z izsiljevalskim virusom (angl. Ransomware). Vdor je bil izveden z javno razkritim VPN-geslom. Podjetje je bilo za ustavitev širjenja prisiljeno ustaviti sistem in s tem prekiniti oskrbo nafte. Skupna nastala škoda še ni ocenjena, znano pa je, da je podjetje hekerjem za obnovitev šifriranih podatkov plačalo odkupnino v višini okoli 4,4 milijona dolarjev. Oskrbo so nato morali izvesti s cisternami in tankerji (Kerner, 2022).

1.1 Definicija kibernetske varnosti

Kibernetska varnost je ožja podskupina področja informacijske varnosti, ki se ukvarja izključno z zaščito digitalnega ekosistema in njegovih sredstev. Informacijska sredstva predstavljajo vse dragocene informacije, s katerimi podjetje razpolaga. Najdemo jih lahko v različnih oblikah, kot so: dokumenti v datotekah, podatkovne baze, gesla, šifrirni ključi itd. (ISO/IEC, 2017). Slika 1 prikazuje glavne tipe digitalnih sredstev.

Slika 1: Digitalna sredstva



Prirejeno po ISO/IEC (2017).

1.2 Upravljanje kibernetske varnosti

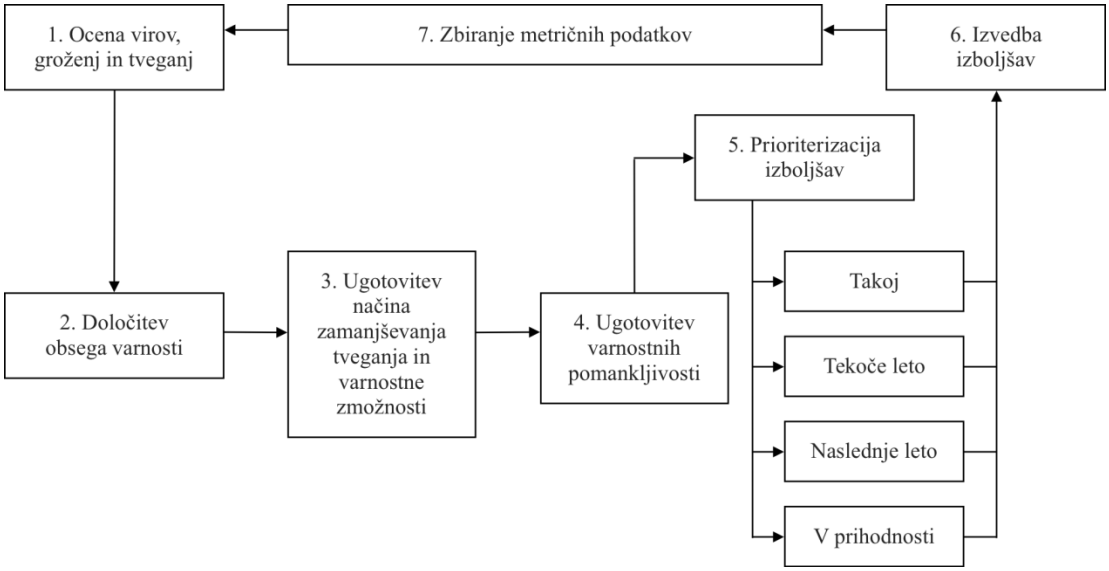
Moschovitis (2018, str. 15) navaja, da so glavni cilji kibernetske varnosti naslednji: zagotoviti in ohranjati zaupnost, zagotoviti integriteto, zagotoviti razpoložljivost digitalnih informacij ter zagotoviti varnost ljudi v delovnem okolju:

- **Zaupnost**: zaupnost si lahko predstavljamo kot nekaj zasebnega, pri tem pa moramo upoštevati, da se lahko zaupnost predmeta kadarkoli spremeni (primer: prekinitev pogodbe med podjetji).
- **Integriteta**: gre za zagotavljanje točnosti podatkov skozi njihov življenjski cikel, da lahko zaupamo podatkom. Na voljo so različna orodja in prakse, ki pomagajo ohranjati in zaščititi podatke.
- **Razpoložljivost**: skrb, da so nam podatki vedno na voljo. To rešujemo z redundantnimi sistemi, ki zagotavljajo razpoložljivost in varnostne kopije.
- **Varnost**: skrb za varnost ljudi, ki upravljajo in uporabljajo naprave, kjer bi kibernetski napad lahko povzročil poškodbe ali celo smrt (primer: zdravstvene naprave).

1.3 Proces upravljanja kibernetske varnosti

Proces upravljanja kibernetske varnosti poveže skupaj naslednje štiri glavne naloge: upravljanje tveganj, izvajanje nadzora, izboljševanje procesov in merjenje uspešnosti. Te naloge izvajamo ciklično in pri vsaki iteraciji skušamo vpeljati izboljšave, kjer je to potrebno (Donaldson, Siegel, Williams & Aslam, 2015, str. 243). Cikel je sestavljen iz operacij, ki jih prikazuje diagram (glej sliko 2).

Slika 2: Cikel upravljanja kibernetske varnosti



Vir: Donaldson, Siegel, Williams & Aslam (2015).

1. Ocena virov, groženj in tveganj: v tem koraku skušamo ugotoviti, katera sredstva podjetja morajo biti zavarovana in katere so potencialne grožnje.
2. Določiti obseg varnosti: v prvem koraku definiramo sredstva, ki jih želimo zaščititi, tukaj pa določimo, kje in v kakšni meri bomo ta sredstva obvarovali. Pri tem moramo paziti na ravnotežje pri omejevanju in dovoljevanju določenih operacij, saj s tem ne želimo zmanjšati obstoječe učinkovitosti izvajanja procesov. Pretirane varnostne politike in pravila imajo lahko drastičen vpliv na učinkovitost poslovanja.
3. Ugotoviti načine zmanjševanja tveganja in varnostne zmožnosti: pri ugotavljanju tveganja skušamo z demonstracijo kibernetskega napada oceniti zmožnost odkrivanja napadov in zaščite pred napadi.
4. Določiti obseg varnosti: cilj tega koraka je iskati primeren obseg varnosti, ki je za podjetje ustrezen, stroškovno učinkovit ter čim manj obremenjuje poslovni proces.
5. Ugotovitve varnostnih pomanjkljivosti: rezultat tega koraka je seznam področij, kjer smo odkrili varnostne pomanjkljivosti ter je treba izboljšati varnost. Področja z večjim številom pomanjkljivosti imajo višjo prioriteto.
6. Prioterizacija izboljšav: določitev prioritete izboljšav je odvisna od znanja in usposobljenosti, soodvisnosti izboljšav in stroškov. Ko smo določili prioritete, jih

logično umestimo v skupine glede na zaporedje posameznih operacij in realen časovni okvir:
   - Takoj: s sanacijo je mogoče začeti takoj. Na voljo so vsi razpoložljivi viri in sredstva.
   - Tekoče leto: izboljšave je mogoče izvesti v tekočem letu. Vsi potrebni predpogoji pa so bili naslovljeni.
   - Naslednje leto: v to skupino umestimo izboljšave, ki jih načrtujemo izvesti v naslednjem letu (po tem, ko smo naslovili vse nujne).
   - V prihodnosti: v tej skupini imamo izboljšave z nižjo prioriteto. Po navadi zahtevajo dodatna finančna sredstva, kader in znanje. Gre za izboljšave, ki jim je težje določiti realen časovni okvir.
7. Izvedba izboljšav: po določenih prioritetah v prejšnjem koraku začnemo z izvajanjem. Pomembno je, da pri tem vodstvo, ki je odgovorno za kibernetsko varnost, naloge tudi usmerja in nadzoruje.
8. Zbiranje metričnih podatkov: zbiramo vse koristne in merljive informacije, ki bi lahko bile v pomoč vodstvu (primer: št. varnostnih incidentov, št. zaznanih potencialnih groženj, št. opravljenih skeniranj itd.). Ti podatki so nam v pomoč pri analizi in spremljanju trenda kibernetske varnosti v podjetju.

1.4 Upravljanje tveganj kibernetske varnosti

V prejšnjem poglavju sem predstavil posamezne procese znotraj celotnega cikla upravljanja kibernetske varnosti. V tem poglavju pa bolj podrobno predstavim jedro upravljanja kibernetske varnosti – upravljanje tveganj. Chapple in Seidl (2017, str. 66) pravita, da so pri upravljanju tveganj najbolj pomembni naslednji trije pojmi: ranljivosti, grožnje in tveganje. Pod ranljivosti štejemo vse mogoče šibke točke (naprave, aplikacije, sistemi, procesi), ki bi jih lahko napadalec izkoristil. Grožnja predstavlja zunanjo silo, ki bi lahko izkoristila eno ali več izmed omenjenih ranljivosti. Tveganje predstavlja kombinacijo ranljivosti in grožnje (Van Impe, 2017, str. 67).

1.4.1 Proces upravljanja tveganj

Refsdal, Solhaug in Stølen (2015, str. 12) definirajo proces upravljanja tveganja kot obseg usklajenih dejavnosti, ki usmerjajo in nadzorujejo tveganje v organizaciji. Proces upravljanja tveganj je na najvišji ravni razdeljen na: komuniciranje, ocenjevanje tveganj ter monitoring in revidiranje. Avtorji so mnenja, da za ustrezno, učinkovito in optimalno upravljanje tveganj kibernetske varnosti znotraj organizacije potrebujemo delovno ogrodje za kibernetsko varnost (angl. Cybersecurity framework). Le na ta način lahko zagotovimo, da je upravljanje tveganj kibernetske varnosti integrirano skozi vse poslovne procese. Delovno ogrodje definira osnovna načela za upravljanje tveganj na najvišji ravni organizacije. Primer takšnih osnovnih načel so smernice za upravljanje tveganj »ISO

31000 Risk management – Guidelines«. Te pa za upravljanje tveganj od organizacije zahtevajo naslednje (Hutchins, 2019):

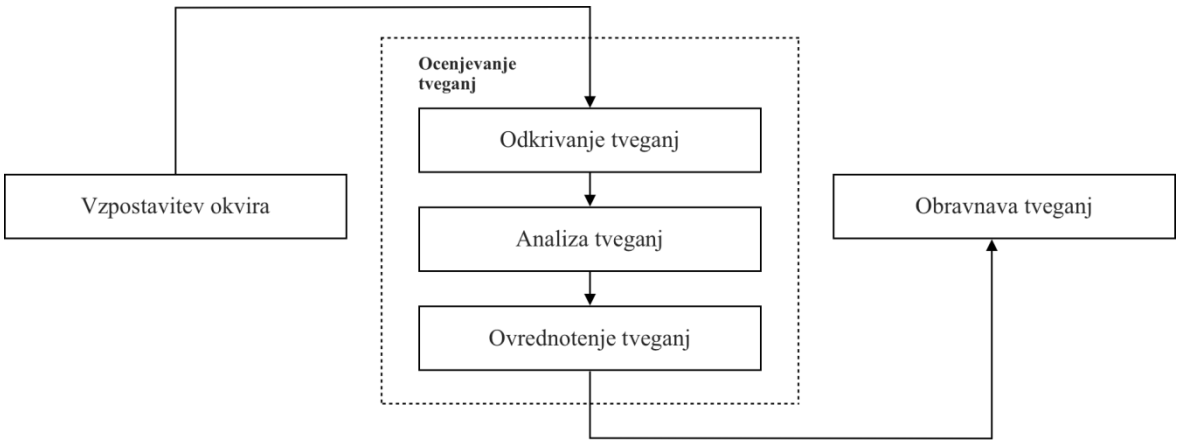
– da je integrirano v vse poslovne procese,
– da je del odločitvenih procesov,
– da eksplicitno obravnavamo negotovost,
– da je sistematično, strukturirano in pravočasno,
– da je prilagojeno organizaciji,
– da upošteva tudi človeški dejavnik,
– da je transparentno in dovolj obsežno,
– da stremi k nenehnim izboljšavam,
– da je dinamično (prilagodljivo) in se spreminja skupaj z organizacijo,
– da ga izvajamo na čimboljših informacijah in podatkih.

1.4.2 Ocenjevanje tveganj

Pri kibernetski varnosti upravljamo z visoko negotovostjo. Za zmanjšanje te negotovosti in varnostnih tveganj je treba verjetnosti in posledice varnostnih incidentov na nek način odkriti in ovrednotiti. Ta proces imenujemo ocenjevanje tveganj. Ocenjevanje tveganj kibernetske varnosti je del širšega področja upravljanja tveganj znotraj organizacije. Gre za proces, s katerim želimo na dokumentiran način identificirati kibernetska tveganja, s čimer lažje določimo prioritete ter potrebne vire za njihovo zmanjševanje in ublažitev (Kohnke, Shoemaker & Sigler, 2016, str. 70).

Diagram na sliki 3 prikazuje korake pri procesu ocenjevanja tveganj kibernetske varnosti. V naslednjih poglavjih bolj podrobno predstavim posamezne korake.

Slika 3: Proces ocenjevanja tveganj



Prirejeno po Cherdantseva (2016, str. 19).

1.4.3 Vzpostavitev okvira

Za vzpostavitev okvira je treba določiti cilje in predmete ocenjevanja tveganja (primer: intranet omrežje). Glavni cilj ocenjevanja tveganj je vedno zmanjševanje tveganj, vendar so cilji lahko tudi sekundarni (primer: skladnost s standardi za kibernetsko varnost). Določiti je treba obseg analize, kaj vse bomo pri ocenjevanju obravnavali. Kot zadnji korak določimo potrebne kriterijske lestvice za ocenjevanje tveganj, kot so: verjetnost (angl. Likelihood), stopnja vpliva (angl. Impact) in stopnja resnosti (angl. Severity) (Refsdal, Solhaug & Stølen, 2015, str. 15–17).

Glede na potrebe in razpoložljive podatke izdelamo stopnje verjetja. Za predstavitev stopnje verjetja in vpliva sem izbral preprosto petstopenjsko lestvico (glej tabeli 1 in 2). Kadar imamo na voljo dovolj podatkov, je smiselno uporabiti racionalne ocene ali interval, s čimer lahko ocene zajemamo z večjo natančnostjo.

Pri določevanju lestvice moramo upoštevati naslednje vodilne dejavnike groženj (Stoneburner, Goguen & Feringa, 2008, str. 21):

– motivacija in zmožnosti,
– lastnosti ranljivosti,
– obstoj in učinkovitost trenutne kontrole in zaščite.

Tabela 1: Primer lestvice verjetja

Verjetnost	**Opis**
Zelo velika (5)	Varnostni incident je pričakovan.
Velika (4)	Do varnostnega incidenta bo enkrat prišlo.
Srednja (3)	Glede verjetja, da bo do varnostnega incidenta prišlo, smo indiferentni.
Majhna (2)	V normalnih okoliščinah varnostni incident ni pričakovan.
Zelo majhna (1)	Do varnostnega incidenta lahko pride le v izrednih primerih.

Vir: Maritime Cybersecurity (2015).

Tabela 2: Primer lestvice stopnje vpliva

Stopnja vpliva	**Opis**
Zelo velika (5)	Pričakujemo, da bo varnostni incident imel večje št. hudih posledic za poslovanje in organizacijo.
Velika (4)	Varnostni incident bi lahko imel večje št. hudih posledic za poslovanje in organizacijo.
Srednja (3)	Varnostni incident bi lahko imel resne posledice za poslovanje in organizacijo.
Majhna (2)	Varnostni incident bi lahko imel posledice za poslovanje in organizacijo.
Zelo majhna (1)	Vpliv na poslovanje in organizacijo je zanemarljiv.

Vir: Maritime Cybersecurity (2015).

1.4.4 Odkrivanje tveganj

V tem koraku skušamo s pomočjo različnih tehnik odkriti tveganja za različne scenarije, ki so relevantni za naša sredstva. Zanimajo nas grožnje in ranljivosti ter njihov izvor. Pri tem upoštevamo tudi tveganja, ki niso zlonamerna (primer: programski hrošč), kjer je lahko škoda povzročena neposredno. Nepogrešljiv in koristen pa je tudi seznam potencialnih varnostnih incidentov, ki jih lahko povzroči posamezna grožnja ali ranljivost (Refsdal, Solhaug & Stølen, 2015, str. 61–63).

1.4.5 Analiza tveganj

Analiza tveganj zajema določitev verjetja in stopnjo vpliva varnostnih incidentov kibernetske varnosti, ki so podlaga za naslednji korak – določiti raven tveganja. Raven tveganja predstavlja zmnožek stopnje vpliva (včasih imenovan tudi posledica) in verjetja. V tem koraku določimo stopnjo vpliva, ki ga ima varnostni incident na sistem in organizacijo, ter verjetnost, da bo do varnostnega incidenta prišlo. Natančnost ocene je odvisna od količine in kakovosti podatkov ter izkušenj, s katerimi razpolagamo (Refsdal, Solhaug & Stølen, 2015, str. 81–82). Stopnje vpliva in ocene verjetja so predpogoj za izvedbo vrednotenja tveganj, ki ga opisujem v naslednjem poglavju.

Za oceno verjetja in stopnjo vpliva imamo na voljo kvantitativno in kvalitativno metodo ocenjevanja. Pri kvantitativni metodi je ocena po navadi sestavljena iz več statistično merljivih ključnih kazalnikov (angl. Key Performance Indicators – KPI), kot so: povprečno št. incidentov, čas, potreben za odziv in saniranje, raven zaščite, št. oseb z dostopom do sistema itd. Ocenjevanje lahko izvedemo z različnimi pristopi: Monte Carlo, večkriterijska odločitvena analiza (angl. Multi-criteria Decision Analysis – MCDA), odločitvena drevesa in drugi. Slabost kvantitativne metode je predvsem njena zahtevnost – potrebujemo veliko podatkov in terja veliko časa za izvedbo (Ramona, 2011, str. 1108). Kvalitativna metoda velja za hitrejšo in cenovno ugodnejšo. Služi kot dober temelj pri načrtovanju bolj natančne in podrobne kvantitativne metode. Slabost te metode je, da temelji na subjektivnih ocenah, zaradi česar ni najbolj natančna (Meyer, 2015, str. 3). Zaradi omejene razpoložljivosti podatkov sem v raziskovalnem delu naloge izbral kombinacijo kvalitativne in kvantitativne metode.

Kot zadnji korak analize tveganj je treba določiti stopnje resnosti posameznega incidenta. Navadno uporabimo preprosto ordinalno lestvico (primer: majhna, srednja, visoka) ter definiramo pričakovane posledice za vsak varnostni incident kibernetske varnosti (Refsdal, Solhaug & Stølen, 2015, str. 87).

1.4.6 Vrednotenje tveganj

Dobljene ocene iz prejšnjega koraka analize tveganj (verjetnost in stopnja vpliva) v tem koraku uporabimo za vrednotenje tveganj. Ocenjena raven tveganja nam je v pomoč pri prioretizaciji tveganj in načrtovanju odzivov na tveganja. Ker je ocenjeno raven tveganja in verjetja zahtevno komunicirati, za vrednotenje uporabimo matriko tveganja (imenovano tudi matrika verjetja). Primer matrike tveganja prikazuje tabela 3. Izdelana je na podlagi izbranih kriterijev za stopnjo vpliva in verjetja na začetni stopnji ocenjevanja tveganj (poglavje 1.4.3). Prednosti takšnega ocenjevanja sta enostavnost izvedbe in komunikacija z deležniki (Elmontsri, 2013, str. 51).

Tabela 3: Primer matrike tveganj

VERJETJE	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
STOPNJA VPLIVA						

Prirejeno po Refsdal, Solhaug & Stølen (2015, str. 60).

Glede na ocenjene kriterije verjetja in stopnje vpliva iz poglavja 1.4.3 izdelamo matriko tveganja, iz katere lahko razberemo raven tveganja za posamezno tveganje. Z visokim tveganjem upravljamo, kadar se naše ocene gibljejo na intervalu [12,25]. Srednje tveganje predstavljajo ocene na intervalu [5,10], vse ocene, nižje od 5, pa predstavljajo nizko tveganje.

1.4.7 Obravnava tveganj

Zadnji korak upravljanja tveganj je obravnava tveganj. Pripraviti je treba dokument, ki vsebuje navodila, kako bomo obravnavali ocenjena tveganja. Izbrati je treba način in implementacijo obravnave tveganj, vrstni red izvajanja kontrol in določiti časovni okvir ter potrebna sredstva. Obravnava tveganj je iterativni proces, pri katerem (Jereb, 2014, str. 43):

– izbiramo med možnostmi obravnave,
– načrtujemo implementacijo,
– ponovno odločamo, ali je ocenjeno tveganje sprejemljivo (v primeru, da ni, je potrebna ponovna obravnava).

ISO 31000:2000 definira naslednje možnosti obravnave tveganj (Jereb, 2014, str. 28):

– izogibanje tveganju (prekinemo z aktivnostjo, ki povzroča tveganje),

– povečamo tveganje, s čimer izzovemo priložnost,
– odpravimo vir tveganja,
– spremenimo verjetnost dogodka,
– spremenimo stopnjo vpliva dogodka,
– delitev tveganja (prek pogodbe in/ali nakupa zavarovanja),
– ohranjanje tveganja s premišljenimi odločitvami.

Cilj procesa je razvoj strategij, ki zmanjšajo verjetnost in/ali vpliv. Podjetja se morajo osredotočati na zaščito in protiukrepe proti tveganju, ki ima ocenjeno visoko verjetnost in vpliv, saj ima ta največje posledice oz. predstavlja največji strošek za podjetje. Obravnavanje tveganj, ki imajo majhen vpliv in majhno verjetnost, po navadi ni smotrno in predstavlja le izgubo (Sumner, 2009).

1.5 Delovna ogrodja za kibernetsko varnost

Delovna ogrodja so podjetju v pomoč pri usmeritvah najboljših praks, varnostnih politik, procedur, standardov in procesov. Usmeritve izvajamo z namenom povečanja kibernetske varnosti. Glavni namen vpeljave delovnega orodja je vzpostavitev kontrol in najboljših praks za zmanjševanje tveganja kibernetskega napada in njegovega vpliva na podjetje. Donaldson, Siegel, Williams in Asla (2015, str. 274) menijo, da različna delovna ogrodja lahko organizirajo kibernetsko varnost na različne načine, vendar so vsem po navadi skupna naslednja glavna področja:

– razdelitev podjetja in njegove zaščite na različna kontrolna področja,
– upravljanje tveganj,
– nadzor varnosti,
– mehanizmi za revizijo in ocenjevanje varnostnih kontrol, ki jih delovno ogrodje definira.

Delovna ogrodja integriramo v poslovne procese podjetja. Zasnovana so na način, ki čim manj spremeni obstoječe poslovne procese.

Nekatera so bolj usmerjena v podjetja iz določene industrije, medtem ko so druga bolj splošna. V praksi večje organizacije izdelajo tudi svoja delovna ogrodja, ki so izpeljanke obstoječih, vendar prilagojena lastnim potrebam. Podjetju ni treba vpeljati celotnega delovnega ogrodja, ampak samo sklope, ki so relevantni za podjetje. Ker so tehnološko neodvisna, je njihova velika prednost prilagodljivost. Z njimi definiramo varnostne cilje, ne pa tudi načine, kako naj podjetje te cilje doseže (Donaldson, Siegel, Williams & Asla, 2015, str. 29). V naslednjem poglavju predstavim primer, kako nas delovno ogrodje s pomočjo kategorij in podkategorij ter oznak usmeri v bolj podrobne informacije za doseganje posameznih ciljev kibernetske varnosti.

Na trgu je v uporabi vrsta različnih delovnih ogrodij za kibernetsko varnost. Najbolj pogosto zasledimo naslednjih pet delovnih ogrodij (Cisternelli, 2021):

- NIST CSF, krajše NIST, je delovno ogrodje za kibernetsko varnost, ki ga je izdelal ameriški Nacionalni inštitut za standarde in tehnologijo. Delovno ogrodje temelji na upravljanju tveganja kibernetske varnosti z integracijo industrijskih standardov in najboljših praks. Gre za relativno novo delovno ogrodje, prva različica 1.0 je bila predstavljena leta 2014. Po navedbah družbe Gartner research naj bi bilo že leta 2015 delovno ogrodje uporabljeno v 30 % organizacij znotraj ZDA (NIST, 2020). V naslednjem poglavju omenjeno delovno ogrodje tudi bolj podrobno predstavim.
- COBIT 5: je delovno ogrodje za razvoj, vpeljavo, spremljanje ter izboljšanje vodenja in upravljanja IT znotraj organizacije. Razvilo ga je strokovno združenje ISACA (angl. Information Systems Audit and Control Asociaiton, v nadaljevanju ISACA). Poleg upravljanja in vodenja IT pokriva širše področje informacijske varnosti in upravljanja tveganj. Znotraj delovnega ogrodja NIST je zelo pogosto naveden kot referenca na podrobnejšo implementacijo. NIST in COBIT 5 sta združljiva, kar pomeni, da se lahko odločimo za vpeljavo NIST z uporabo ogrodja COBIT 5 (Kohnke, Shoemaker & Sigler, 2016, str. 79).
- ISO 27001 in ISO 27002: bolj kot za delovno ogrodje gre za serijo standardov, povezanih z informacijsko varnostjo, ki jih je ustvarila Mednarodna organizacija za standardizacijo ISO (angl. International Organization for Standardization). Vsebuje tudi mednarodno priznan certifikat, s katerim podjetja dokazujejo skladnost upravljanja informacijske in kibernetske varnosti svojim partnerjem (Irwin, 2021).
- SOC2: ustvaril ga je Ameriški inštitut potrjenih računovodskih strokovnjakov (angl. American Institute of CPAs – AICPA), ki temelji na petih principih zaupanja – varnost, dostopnost, integriteta procesov, zaupnost ter zasebnost. Gre za revizijsko poročilo o skladnosti organizacije z zahtevami SOC2. V obliki internega poročila organizacija dobi boljši vpogled v načine upravljanja s podatki. Za vsako področje posebej je tudi izdan certifikat o skladnosti. SOC2 ne definira napotkov ali usmeritev pri vpeljavi varnostnih praks (primer: ISO 27001), temveč zahteva le, da je določeno področje ustrezno implementirano (IT Governance Ltd, 2022).
- HIPAA Security Rule, ki ga je razvilo ameriško ministrstvo za zdravje in socialne zadeve (angl. U.S. Department of Health and Human Services – HHS), je industrijsko specifično delovno ogrodje, usmerjeno v zaščito informacij v zdravstvu. Vsebuje usmeritve za vpeljavo tako imenovanega HIPAA Security Rule, ki se osredotoča na zaščito zaupnosti, integriteto in dostopnost elektronskih informacij v zdravstvu. Vse entitete, ki sodelujejo pri izmenjavi teh informacij, morajo biti skladne s Security Rule (NIST, 2021).

1.6 Delovno ogrodje NIST

Za predstavitev delovnega ogrodja za kibernetsko varnost sem izbral ogrodje NIST. Razlogi so predvsem dostopnost virov, njegova razširjenost in dejstvo, da gre za najnovejše in najmodernejše delovno ogrodje na tem področju. Delovno ogrodje NIST je razdeljeno na naslednje osnovne komponente: jedro, ravni in profil. Jedro delovnega ogrodja je sestavljeno iz funkcij in kategorij, opisanih v tabeli 4. Kategorije predstavljajo širše cilje kibernetske varnosti organizacije. Identifikator predstavlja enolično oznako kategorije. Zapis prvega dela identifikatorja (do pike) predstavlja skrajšan zapis imena funkcije (Primer: »ID« – angl. Identify), drugi del zapisa pa ime kategorije v angleškem jeziku (Primer: »AM« – angl. Asset Management) (NIST, 2018 a).

Tabela 4: NIST – funkcije in kategorije

Funkcija	**Opis funkcije**	**Identi-fikator**	**Kategorije**
Opredelitev (ID)	Organizacijsko razumevanje obvladovanja tveganja in kibernetske varnosti sistemov, ljudi, sredstev, podatkov in zmogljivosti.	ID.AM	Upravljanje virov in sredstev
		ID.BE	Poslovno okolje
		ID.GV	Upravljanje kibernetske varnosti
		ID.RA	Ocena tveganj
		ID.RM	Strategija upravljanja tveganj
Zaščita (PR)	Izvajanje ustreznih zaščitnih ukrepov za zagotavljanje delovanja kritičnih storitev.	PR.AC	Upravljanje identitete in nadzor dostopa
		PR.DS	Varnost podatkov
		PR.MA	Vzdrževanje
		PR.PT	Tehnologija za zaščito
		PR.AT	Ozaveščanje in izobraževanje
Odkrivanje (DE)	Izvajanje aktivnosti za prepoznavanje dogodkov, povezanih s kibernetsko varnostjo.	DE.AE	Anomalije in dogodki
		DE.CM	Spremljanje in opazovanje (monitoring)
		DE.DP	Procesi za odkrivanje
Odziv (RS)	Izvajanje aktivnosti za ustrezno ukrepanje ob zaznavi varnostnih incidentov.	RS.RP	Načrtovanje odziva
		RS.CO	Komuniciranje
		RS.AN	Analiza
		RS.MI	Ublažitev incidentov
		RS.IM	Izboljšave
Obnova (RC)	Izvajanje aktivnosti za obnovo storitev in zmožnosti, ki so bile prizadete med varnostnim incidentom v stanju pred nastopom incidenta.	RC.RP	Načrtovanje obnovitve stanja
		RC.IM	Izboljšave
		RC.CO	Komuniciranje

Vir: NIST (2018).

Kategorije naprej delimo na podkategorije, ki predstavljajo podrobnejšo usmeritev ter pričakovani končen rezultat. Zaradi obsežnega seznama (skupaj jih je 108) navedem le dva primera kategorije in podkategorij s pripadajočimi oznakami. Oznaka predstavlja referenco na podrobnejši tehnični opis implementacije, ki ga kategorija opisuje. Zajema sorodne vsebine in bolj konkretne usmeritve iz drugih standardov, kot sta COBIT 5 in ISO/IEC. Če za primer vzamemo oznako »COBIT 5 BAI09.01«, nas ta usmeri na delovno ogrodje COBIT 5 in identifikacijsko oznako kategorije »BAI09.01«. Oznaka kategorije predstavlja kategorijo Odkrivanje in beleženje obstoječih sredstev (angl. Identify and record current assets), kjer bomo našli podrobnejše usmeritve za izvedbo (NIST, 2018 c).

V tabeli 5 predstavim dva primera podkategorij in oznak NIST, ki vodijo na podrobnejši opis implementacije.

Tabela 5: NIST – primer podkategorije

Funkcija	**Kategorija**	**Podkategorija**	**Oznake**
Opredelitev (ID)	ID.AM – upravljanje virov in sredstev	ID.AM-1 – seznam oz. popis vseh fizičnih naprav in sistemov znotraj podjetja	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.2 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev 4 CM-8
		ID.AM-2 – seznam oz. popis vse programske opreme znotraj podjetja	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.2, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev 4 CM-8

Vir: NIST (2019).

1.6.1 Vpeljava delovnega ogrodja v organizacijo

Delovno ogrodje NIST definira štiri ravni integracije kibernetske varnosti (angl. Tiers). Ravni predstavljajo obsežnost integracije in so nam v pomoč pri ocenjevanju in načrtovanju kibernetske varnosti. Višja kot je raven, bolj široko ima organizacija integrirano delovno ogrodje. Prva raven predstavlja bolj neformalen »ad hoc« pristop, medtem ko četrta raven vpeljuje bolj dovršen in agilen pristop k načinu obvladovanja tveganj kibernetske varnosti. Ravni so nam v pomoč pri izdelavi profila trenutnega stanja in profila podjetja, ki si ga zastavimo kot cilj. Po opravljeni analizi dobimo podroben pregled nad integriranostjo organizacije, ki nam lahko služi kot načrt za nadaljnje izboljšave (ISACA, 2014, str. 32). V tabelah 6 in 7 lahko vidimo opis posamezne ravni integracije, pri čemer stolpci opisujejo naslednje (ISACA, 2014, str. 32):

– upravljanje tveganj: opis formalnosti upravljanja tveganj kibernetske varnosti za posamezno raven;
– integriranost: ozaveščenost o upravljanju tveganja na organizacijski ravni podjetja;
– zunanji udeleženci: raven deljenja informacij z zunanjimi partnerji z namenom izboljšanja kibernetske varnosti.

Tabela 6: Podrobnosti integracije

Upravljanje tveganj	Integriranost	Zunanji udeleženci
PRVA RAVEN INTEGRACIJE		
- Neformalno, - prioritetne aktivnosti kibernetske varnosti niso usklajene z organizacijskimi cilji in potrebami poslovanja.	- Omejeno zavedanje tveganj kibernetske varnosti na organizacijski ravni, - upravljanje tveganj je integrirano le za posamezne primere, - opcijsko interno deljenje informacij o kibernetski varnosti.	- Ni deljenja informacij z zunanjimi udeleženci, - podjetje ni ozaveščeno o tveganju kibernetske varnosti znotraj dobavne verige.
DRUGA RAVEN INTEGRACIJE		
- Odobreno s strani menedžmenta, vendar ni vzpostavljeno na ravni organizacije, - prioritetne aktivnosti kibernetske varnosti so usklajene z organizacijskimi cilji in potrebami poslovanja.	- Obstaja zavedanje tveganj kibernetske varnosti na organizacijski ravni, - upravljanje s tveganji na organizacijski ravni ni vzpostavljeno, - obstaja ocena glede varnostnega tveganja za sredstva podjetja, vendar se ocenjevanje ne izvaja ponavljajoče.	- Podjetje sodeluje z zunanjimi udeleženci, kakor tudi pridobiva informacije od zunaj, - podjetje je ozaveščeno o tveganju kibernetske varnosti znotraj dobavne verige, vendar za to nima formalno dogovorjenih postopkov.

se nadaljuje

Tabela 6: Podrobnosti integracije (nad.)

Upravljanje tveganj	Integriranost	Zunanji udeleženci
TRETJA RAVEN INTEGRACIJE		
- Formalno dogovorjeno izvajanje varnostnih politik.	- Upravljanje tveganja je izvedeno na organizacijski ravni, - procesi so definirani, implementirani in revidirani, - določitev politik z upoštevanjem varnostnega tveganja, - komuniciranje o varnostnem tveganju kibernetske varnosti znotraj vodstva je pogosto.	- Podjetje sodeluje z zunanjimi udeleženci, kakor tudi pridobiva informacije od zunaj, - podjetje pridobljene informacije deli z zunanjimi udeleženci, - podjetje je ozaveščeno o tveganju kibernetske varnosti znotraj dobavne verige in izvaja formalne ukrepe.
ČETRTA RAVEN INTEGRACIJE		
- Stalne izboljšave z vpeljavo naprednih tehnologij in najboljših praks, - aktivna prilagodljivost glede na pretekle in trenutne aktivnosti kibernetske varnosti (učenje iz izkušenj in napovedni kazalniki), - odzivanje na varnostne grožnje na časovno in stroškovno učinkovit način.	- Upravljanje tveganja je izvedeno na organizacijski ravni, - vzpostavljeni so procesi za naslavljanje potencialnih varnostnih groženj, - sprejemajo se politike z upoštevanjem varnostnega tveganja.	- Podjetje prejema, ustvarja in revidira informacije za analizo tveganj, - podjetje je ozaveščeno o tveganju kibernetske varnosti znotraj dobavne verige, zato nenehno spremlja informacije v realnem času za lažje odzivanje, - proaktivno formalno komuniciranje znotraj dobavne verige, s čimer se ustvari in ohranja močnejše zaupanje.

Vir: ISACA (2014, str. 33–34).

1.6.2 Profil delovnega ogrodja

Izdelava profila nam omogoča vpogled v to, kako dobro se podjetje ujema z jedrom delovnega ogrodja. Izdelamo dva profila: trenutni in ciljni profil. Izdelan trenutni profil uporabimo za opredelitev trenutnega stanja kibernetske varnosti, ki ga primerjamo s ciljnim profilom. Pri izdelavi profila naredimo pregled kategorij in podkategorij glede na potrebe podjetja na podlagi pripravljenih ocen tveganja. Profil trenutnega stanja nam služi kot podpora pri določevanju prioritet in lažjem merjenju napredka proti ciljnem profilu, kakor tudi za lažjo samooceno ter komuniciranje kibernetske varnosti znotraj in zunaj podjetja (ISACA, 2014, str. 35).

Pri izdelavi profila ima podjetje povsem proste roke, saj delovno ogrodje ne vsebuje predlogov oblikovanja. Cilj je oblikovati profil, kjer bomo opredelili zahteve, glavne cilje

in metodologije dela na način, da so skladne s podkategorijami jedra delovnega ogrodja (ISACA, 2014, str. 36).

Tabela 7: Primer profila

Podkategorija	Prioriteta	Razlika	Proračun	Aktivnosti (leto 1)	Aktivnosti (leto 2)
ID.AM-2	Srednja	Majhna	€	x	
PR.MA-2	Visoka	Majhna	€		x
PR.PT-1	Srednja	Velika	€	x	
DE.AE-3	Nizka	Srednja	€	x	

Vir: NIST (2018).

Tabela 7 prikazuje preprost primer profila delovnega ogrodja. Posamezni stolpci tabele predstavljajo naslednje:

- **podkategorija**: podkategorija jedra delovnega ogrodja, ki jo ocenjujemo,
- **prioriteta**: nujnost sanacije,
- **razlika**: razlika med trenutnim stanjem in želenim ciljnim stanjem,
- **proračun**: finančna sredstva, ki jih imamo na voljo pri izvedbi,
- **aktivnosti**: predviden časovni okvir za izvedbo aktivnosti.

2 ANALIZA KIBERNETSKE VARNOSTI V IZBRANEM PODJETJU

Zaposleni imajo ključno vlogo pri zagotavljanju kibernetske varnosti podjetja. Študija Univerze Oxford ugotavlja, da mala in srednje velika podjetja bolj kot orodja za oceno tveganja potrebujejo ozaveščenost zaposlenih o kibernetskih grožnjah. Ozaveščenost je ključna za razvoj trajnostnih protiukrepov znotraj podjetja, saj predstavlja dodaten in cenovno ugoden način zmanjševanja tveganja na sprejemljivo raven (Bada, Sasse & Nurse, 2015, str. 120). Namen analiz kibernetske varnosti izbranega podjetja je raziskati ozaveščenost zaposlenih o kibernetski varnosti ter odkriti potencialne grožnje in ranljivosti v navideznem zasebnem omrežju VPN, ki ga izbrano podjetje uporablja za delo. Analiza je razdeljena na dva dela: na analizo ozaveščenosti zaposlenih o kibernetski varnosti in analizo VPN-omrežja. V prvem delu s pomočjo anketnega vprašalnika analiziram ozaveščenost zaposlenih o kibernetski varnosti in njeno prakticiranje. Vsako področje vsebuje tematska vprašanja, ki predstavljajo določen izziv kibernetske varnosti. Poglavje zaključim s predstavitvijo rezultatov, predlogi izboljšav in ugotovitvami. V drugem delu analize uporabim intervju z vodstvom IT-službe podjetja za pridobitev informacij o arhitekturi omrežja, programski opremi in trenutnem stanju kibernetske varnosti. V nadaljevanju analize na podlagi pridobljenih informacij definiram potencialne grožnje in ranljivosti VPN-omrežja ter izdelam analizo tveganj.

2.1 Predstavitev podjetja

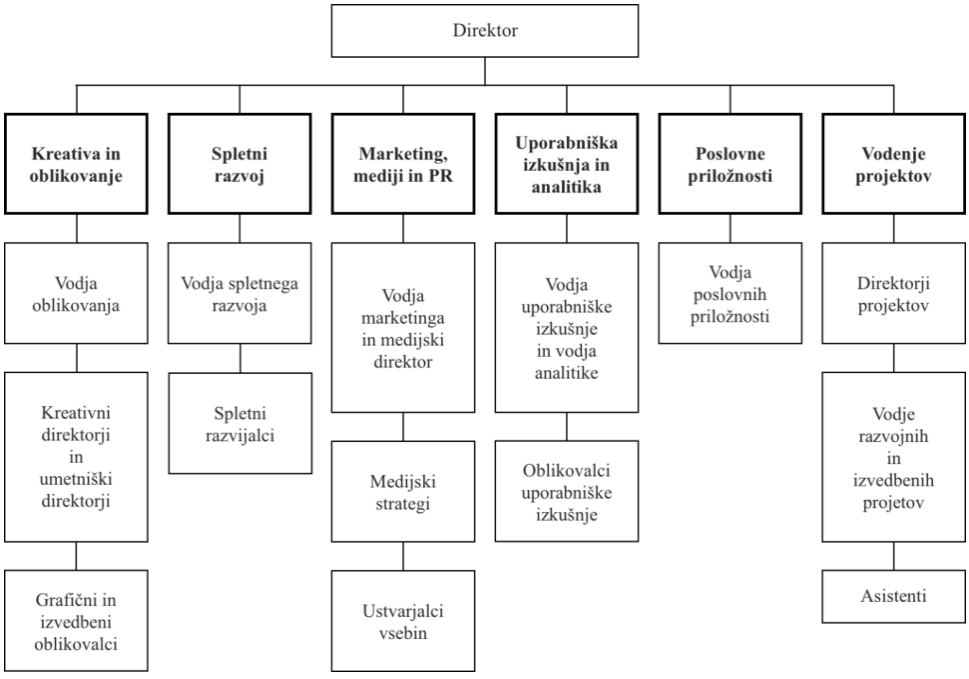
Kljub anonimnosti predstavljenih podatkov je prepričati podjetje za sodelovanje v analizi kibernetske varnosti vse prej kot enostavna naloga. Podjetje mora biti pripravljeno deliti in razkriti občutljive informacije ter zaupati raziskovalcu, da s pridobljenimi podatki ne bo prišlo do zlorab. V ta namen sem z izbranim podjetjem podpisal sporazum o zaupnosti in nerazkritju informacij. Celotna analiza kibernetske varnosti torej temelji na podatkih, pridobljenih od IT-službe in zaposlenih, s čimer sem se izognil potrebi po dostopu do njihovega omrežja in uporabniških računov. To bi za podjetje predstavljalo veliko večje tveganje.

V analizi je bilo pripravljeno sodelovati srednje veliko podjetje, katerega glavna dejavnost je digitalno oglaševanje. Podjetje je razdeljeno na naslednje delovne skupine:

– kreativa in oblikovanje,
– spletni razvoj,
– marketing, mediji in PR,
– uporabniška izkušnja in analitika,
– poslovne priložnosti in
– vodenje projektov.

Slika 4 predstavlja organizacijsko struktura podjetja. Podjetje spada v matrično organizacijsko strukturo. Sprejemanje pomembnih odločitev za delovne skupine poteka horizontalno, zaradi česar te skupine kljub hierarhiji niso avtonomne.

Slika 4: Organizacijska struktura podjetja



Vir: lastno delo.

2.2 Analiza ozaveščenosti o kibernetski varnosti

Za raziskavo ozaveščenosti zaposlenih o kibernetski varnosti v izbranem podjetju sem uporabil anketni vprašalnik. Vprašanja sem povzemal po vprašalniku Trenton (2021, str. 2–7) ter jih razdelil na tri glavna področja: varna uporaba računalnika, varnost na spletu in upravljanje gesel. Vsako posamezno vprašanje predstavlja potencialno ranljivost, ki jo analiziram znotraj področja. Z vprašalnikom sem želel prek ocene splošne ozaveščenosti zaposlenih o prakticiranju kibernetske varnosti na delovnem mestu ugotoviti, ali obstaja tveganje za ranljivost. Rezultati so mi bili v pomoč pri lažji oceni tveganj v drugem delu analize omrežja VPN.

Vzorec anketirancev zajema 24 zaposlenih v podjetju, ki pri svojem delu aktivno uporabljajo VPN-omrežje. Zaposleni, ki so sodelovali, izvirajo iz delovnih skupin, predstavljenih v poglavju 2.1, kjer sem podrobneje predstavil organizacijsko strukturo podjetja.

Metodologija ocenjevanja. Za merjenje ozaveščenosti sem izbral preprost model. Najvišja ocena posameznega odgovora je 1. Delež, ki ga posamezen odgovor predstavlja, je odvisen od potencialnega tveganja kibernetske varnosti. Ocena ozaveščenosti je izražena kot povprečni relativni delež vsote doseženih vseh ocen pri vprašanju. Tabela 8 predstavlja primer interpretacije ocen posameznih odgovorov za vprašanje »Imate na vašem računalniku nastavljen protivirusni program?«.

Tabela 8: Metodologija ocenjevanja

Odgovor	Ocena	Interpretacija
Da	1	Zaposleni se zaveda, da je protivirusni program vklopljen, kakor tudi posodobitve programa, zato je ocena najvišja.
Da, vendar imam izklopljene posodobitve	0,3	Zaposleni se zaveda, da je protivirusni program vklopljen, vendar ima posodobitve izklopljene, iz česar sklepam, da ozaveščenost o tveganju izklopljenih posodobitev ne obstaja, zato je ocena nižja.
Ne	0,1	Zaposleni se zaveda, da ima protivirusni program izklopljen (zato ocena ni 0). Iz tega sklepam, da ozaveščenost o tveganju izklopljenega protivirusnega programa ne obstaja.
Ne vem	0	Zaposleni ni prepričan, ali ima protivirusni program oz. ali je ta vklopljen. Ozaveščenost ne obstaja, varnostno tveganje pa je največje.

Vir: lastno delo.

Kriterij ocenjevanja vprašanj. Za ocenjevanje odgovorov sem izdelal ordinalno petstopenjsko lestvico (glej tabelo 9), ki predstavlja oceno ozaveščenosti na podlagi povprečne vrednosti doseženih točk pri posameznem vprašanju. Delež vrednosti, ki ga posamezno vprašanje predstavlja so v nadaljevanju navedene v grafih.

Tabela 9: Ocene ozaveščenosti – lestvica

Ocena	Rezultat vprašanja (%)
Nezadovoljivo	0–50
Sprejemljivo	50–70
Dobro	70–80
Zelo dobro	80–95
Odlično	95–100

Vir: lastno delo.

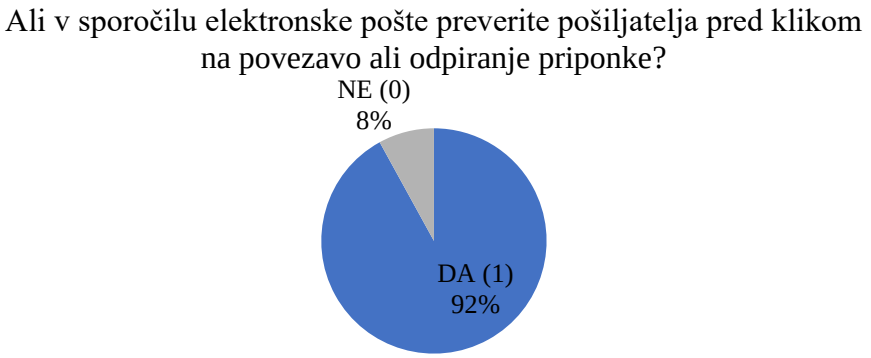
2.2.1 Varna uporaba računalnika

Namen poglavja raziskave varne uporabe računalnika je pridobiti vpogled v izvajanje osnovnih varnostnih praks uporabnika VPN-omrežja podjetja. Poglavje vsebuje skupno sedem vprašanj, ki zajemajo osnovne preventivne ukrepe kibernetske varnosti pri uporabi računalnika.

Preverjanje elektronskega naslova pošiljatelja. Pri prvem vprašanju me je zanimala ozaveščenost o škodljivih priponkah in spletnih prevarah oz. ribarjenju. Dvaindvajset zaposlenih je pritrdilo, da so pri uporabi elektronske pošte pozorni na pošiljatelja pred klikom na povezavo ali odpiranjem priponke. Iz tega sklepam, da je ozaveščenost glede obstoja tveganja spletnih prevar oz. ribarjenja in nevarnosti odpiranja priponk nepoznanih pošiljateljev zelo dobra.

Ocena ozaveščenosti: zelo dobro (92 %).

Slika 5: Preverjanje pošiljatelja elektronske pošte



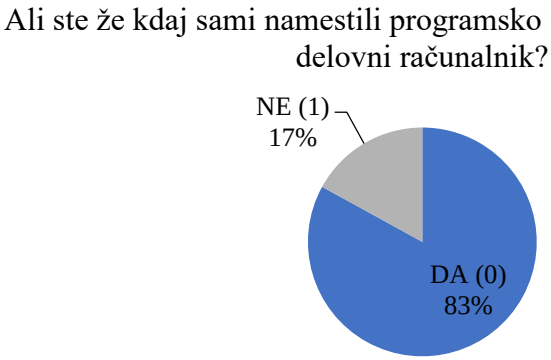
Vir: lastno delo.

Nameščanje programske opreme na službeni računalnik. Pri drugem vprašanju me je zanimalo, ali zaposleni kljub uporabniškim omejitvam domenskega uporabnika nameščajo programsko opremo s spleta na delovni računalnik. To predstavlja problem, saj moramo v primeru kibernetske varnosti vsak vir obravnavati kot potencialno grožnjo, medtem ko

vsak zaposleni ni enako vešč ocenjevanja sumljivih virov in preventivnega upravljanja. Skupno 20 zaposlenih je na vprašanje odgovorilo pritrdilno. Glede na pridobljene informacije od vodja IT-službe, da nameščanje programov za njih opravljajo sistemski administratorji, sedaj ni povsem jasno, kako so v tem primeru zaposleni to omejitev zaobšli. Obstaja tudi verjetnost, da so to storili v preteklosti v primeru, da omenjenega varnostnega ukrepa še niso izvajali. Ker tega podatka nimam na voljo, je treba sklepati, da je varnostno tveganje kljub ukrepom prisotno, omenjen varnostni ukrep pa bi bilo treba bolj podrobno raziskati.

Ocena ozaveščenosti: nezadovoljivo (17 %).

Slika 6: Nameščanje programske opreme na službeni računalnik



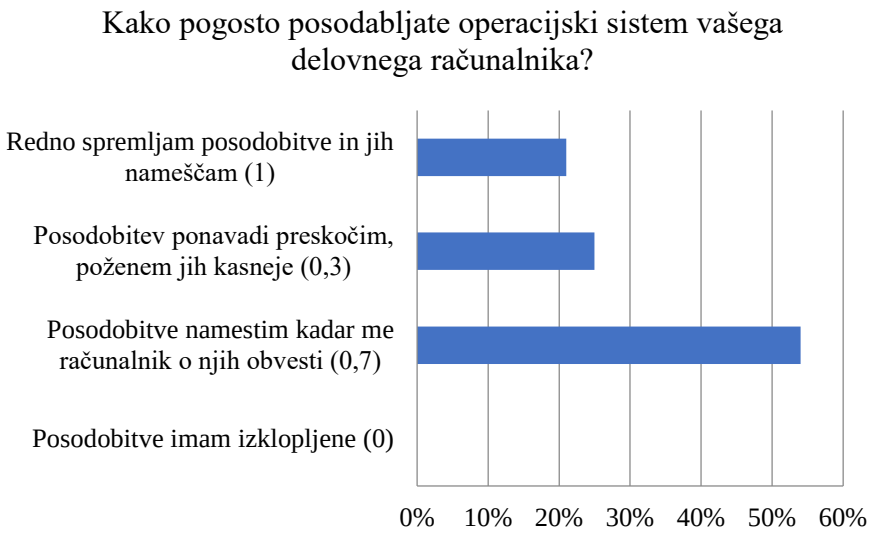
Vir: lastno delo.

Pogostost posodabljanja operacijskega sistema delovnega računalnika. Pri tretjem vprašanju me je zanimalo, ali zaposleni nameščajo posodobitve operacijskega sistema in kako pogosto. Namen posodabljanja operacijskega sistema je med drugim odpravljanje odkritih varnostnih ranljivosti, ki lahko predstavljajo tveganje za celotno omrežje. Dobra novica je, da imajo vsi zaposleni na svojem računalniku vklopljene posodobitve operacijskega sistema. Aktivno spremlja in namešča posodobitve skupno pet zaposlenih. Večina zaposlenih (13) je odgovorilo, da bodo posodobitev namestili, kadar jih bo računalnik o njih obvestil, šest pa jih bo posodobitve preskočilo in jih pognalo kasneje. To predstavlja potencialno varnostno grožnjo, saj v resnici ne vemo, kako dolgo uporabnik odlaša z namestitvijo posodobitev.

Kljub temu je delež teh zaposlenih majhen, sklepam, da je pogostost posodabljanja operacijskega sistema sprejemljiva. Delež vseh odgovorov prikazuje slika 7.

Ocena ozaveščenosti: sprejemljivo (66 %).

Slika 7: Posodabljanje operacijskega sistema delovnega računalnika

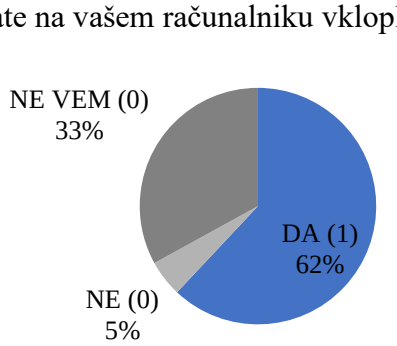


Vir: lastno delo.

Požarni zid. Poleg požarnega zidu, ki je nastavljen na omrežnih napravah (usmerjevalnik), ima operacijski sistem požarni zid, ki dodatno filtrira vhodni in izhodni mrežni promet. Takoj ko imamo računalnik povezan z internetom, je pomembno, da imamo nadzor nad odprtimi vrati in filtriranjem mrežnega prometa, ki preprečuje ranljivosti, kot je nepooblaščen oddaljeni dostop. Pri četrtem vprašanju me je zanimalo, ali obstaja zavedanje o požarnem zidu kot delu operacijskega sistema in ali je ta vklopljen. Večina zaposlenih (15) je odgovorilo, da imajo požarni zid vklopljen, osem zaposlenih pravi, da ne vedo, ali je vklopljen, eden pa je odgovoril, da ima požarni zid izklopljen. Na podlagi rezultata sklepam, da je ozaveščenost »sprejemljiva«. Slika 8 na naslednji strani prikazuje delež odgovorov na vprašanje.

Ocena ozaveščenosti: sprejemljivo (62 %).

Slika 8: Požarni zid



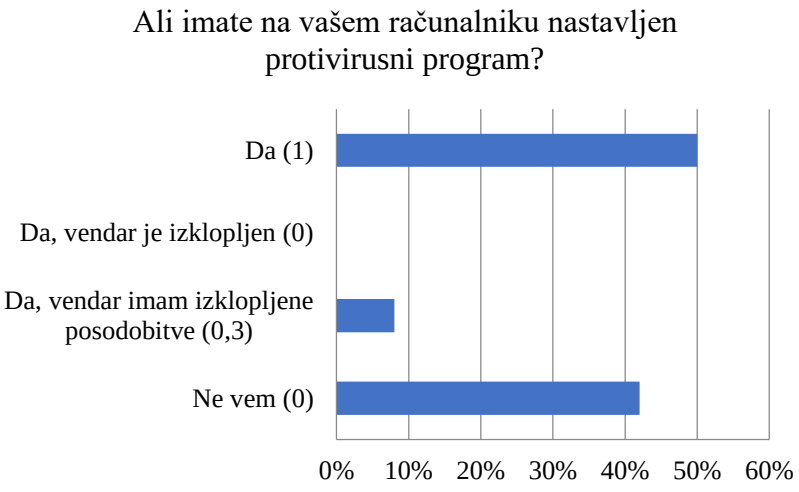
Vir: lastno delo

Protivirusni program. Podjetje za protivirusno zaščito uporablja program F-Secure, ki je nameščen na vse delovne postaje. Protivirusni programi danes odkrivajo široko paleto škodljive programske opreme. Ker z računalniki dostopamo do interneta, je pomembno, da je baza škodljive programske opreme protivirusnega programa dovolj pogosto posodobljena, saj imamo v nasprotnem primeru podobno stanje, kot da protivirusni program ni vklopljen.

Pri petem vprašanju me je zanimalo, koliko so zaposleni pozorni na to, ali je v njihovem sistemu vklopljen protivirusni program, kakor tudi na vklopljene posodobitve. Rezultati kažejo, da 12 zaposlenih protivirusnemu programu ne posveča posebne pozornosti. Deset zaposlenih pravi, da je protivirusni program vklopljen in pravilno nastavljen, dva zaposlena pa imata izklopljene posodobitve. Sklepam, da je ozaveščenost zaposlenih o protivirusnem programu in njegovih posodobitvah nezadovoljiva, zaradi izklopljenih posodobitev pa je prisotno tudi varnostno tveganje. Slika 9 na naslednji strani prikazuje delež odgovorov na vprašanje.

Ocena ozaveščenosti: nezadovoljivo (44 %).

Slika 9: Protivirusni program

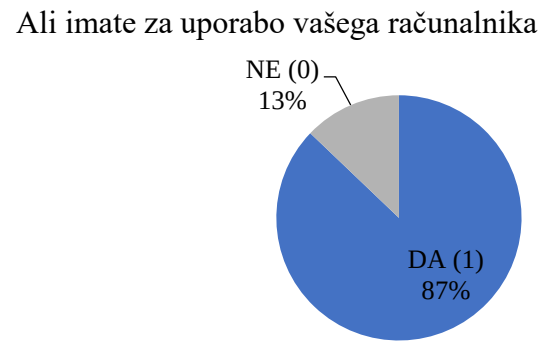


Vir: lastno delo.

Geslo za uporabo računalnika. Pisarna je okolje, kjer se poleg zaposlenih izmenjuje veliko ljudi (stranke, poslovni partnerji, servisne službe itd.), prijavno geslo pa predstavlja prvo vrsto zaščite dostopa do naših podatkov. Prijavno geslo za uporabo računalnika je torej najmanj, kar lahko naredimo, da preprečimo uporabo našega računalnika fizično prisotnim nepooblaščenim osebam. Skupno 21 zaposlenih je odgovorilo, da imajo nastavljeno geslo, iz česar sklepam, da je ozaveščenost zelo dobra.

Ocena ozaveščenosti: zelo dobro (87 %).

Slika 10: Geslo za uporabo računalnika

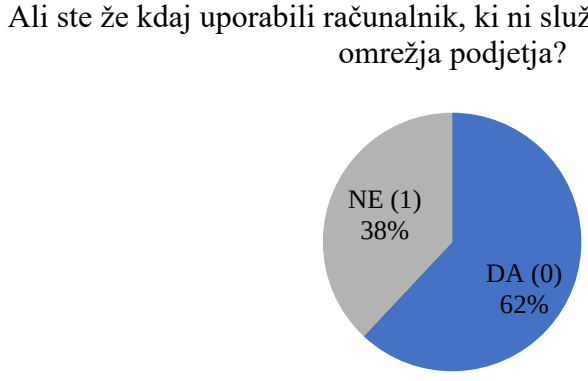


Vir: lastno delo.

Računalnik za dostop do VPN-omrežja. Pri tem vprašanju me je zanimalo, koliko zaposlenih uporablja lasten računalnik za dostop do VPN-omrežja. Problem uporabe računalnika, ki ni služben, je predvsem v varnostnih nastavitvah in programski opremi, ki jo podjetje uporablja za zaščito lastnega omrežja. Pri uporabi osebnega računalnika ne vemo, kako »varen« za uporabo omrežja podjetja je ta računalnik kot odjemalec. Skupno 15 zaposlenih pravi, da so za dostop že uporabili računalnik, ki ni služben. Slika 11 prikazuje delež odgovorov, ozaveščenost pa je glede na rezultate odgovorov tega vprašanja nezadovoljiva.

Ocena ozaveščenosti: nezadovoljivo (38 %).

Slika 11: Računalnik za dostop do VPN-omrežja



Vir: lastno delo.

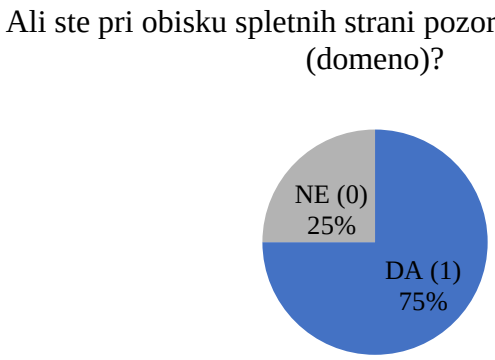
2.2.2 Varnost na spletu

Poleg prenosa škodljive programske opreme s spleta vnos podatkov na spletne strani, ki s prevaro prepričajo uporabnika, predstavlja velik problem. Spletni brskalniki se v ta namen trudijo slediti trendom varnosti in zasebnosti na spletu. Poleg izboljšav varne uporabniške izkušnje je tudi brskalnik ranljiva programska oprema, zato so posodobitve nujne. V poglavju o prakticiranju varne uporabe spleta me je zanimalo, kako pozorni so zaposleni na istovetnost spletnih mest, posodabljanje brskalnika, nezaželeno programsko opremo (angl. Unwanted software) in varni protokol HTTPS (angl. HyperText Transfer Protocol Secure), ki je postal skoraj obvezen že za vsa spletna mesta.

Spletna domena. Prvo vprašanje poglavja varnosti na spletu se nanaša na pozornost spremljanja domene. Ribarjenje izkorišča pozornost uporabnika, kjer je spletno mesto videti identično kot spletno mesto, ki ga posnema, le v domeni je lahko spremenjena črka, s čimer uporabnika preslepi, da je spletno mesto istovetno. Večina zaposlenih (18) je pritrdila, da so pozorni, šest pa jih ni pozornih na domeno spletnega mesta. Iz rezultata sklepam, da je ozaveščenost dobra.

Ocena ozaveščenosti: dobro (75 %).

Slika 12: Spletna domena

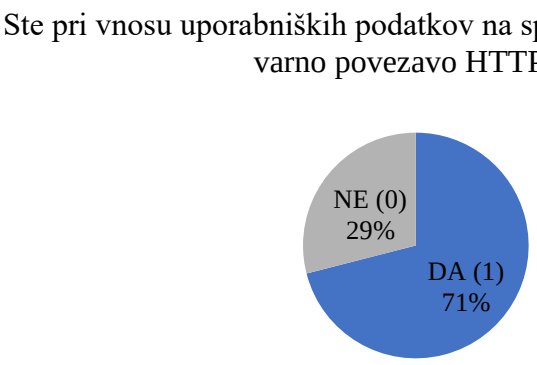


Vir: lastno delo.

HTTPS-povezava. Varna povezava HTTPS zagotavlja šifriran prenos podatkov med odjemalcem in strežnikom. Na ta način zagotovimo, da se podatki prek spleta ne prenašajo v navadni obliki (angl. Plain text). To predstavlja problem v primeru, če napadalec izvaja napad prek posrednika, saj na ta način lahko prestreza piškotke seje, uporabniške podatke ali druge občutljive podatke. Skupno 17 zaposlenih je odgovorilo, da so pozorni na HTTPS-povezavo v brskalniku, ostali pa ne. Glede na postavljen kriterij ocenjevanja je v tem primeru ozaveščenost dobra. Slika 13 na naslednji strani prikazuje delež odgovorov na vprašanje.

Ocena ozaveščenosti: dobro (70 %).

Slika 13: HTTPS-povezava

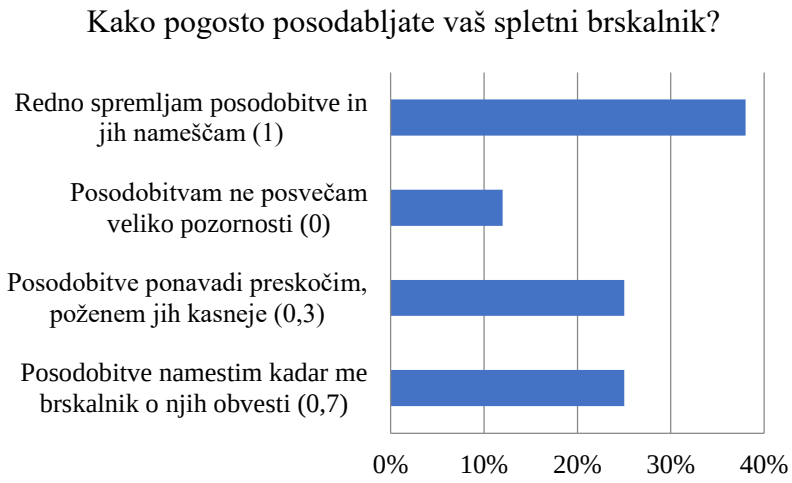


Vir: lastno delo.

Posodabljanje spletnega brskalnika. Z brskalnikom dostopamo do različnih podatkovnih virov, shranjujemo gesla, upravljamo s certifikati in zasebnostjo. Najmanj, kar lahko naredimo za varnost, je, da imamo posodobljeno različico, s čimer zmanjšamo možnost, da bi prišlo do zlorab potencialnih ranljivosti. Velik delež ranljivosti izhaja tudi iz vtičnikov (v preteklosti Adobe Flash). Ranljivosti zadevajo različne operacijske sisteme in različice. Devet zaposlenih je odgovorilo, da posodobitve redno spremljajo in nameščajo. Šest zaposlenih pravi, da posodobitve preskočijo in jih namestijo kasneje. Enako število zaposlenih posodobitve namesti, kadar jih brskalnik o tem obvesti. Trije zaposleni pa pravijo, da posodobitvam ne posvečajo posebne pozornosti.

Ocena ozaveščenosti: sprejemljivo (62 %).

Slika 14: Spletni brskalnik – posodobitve



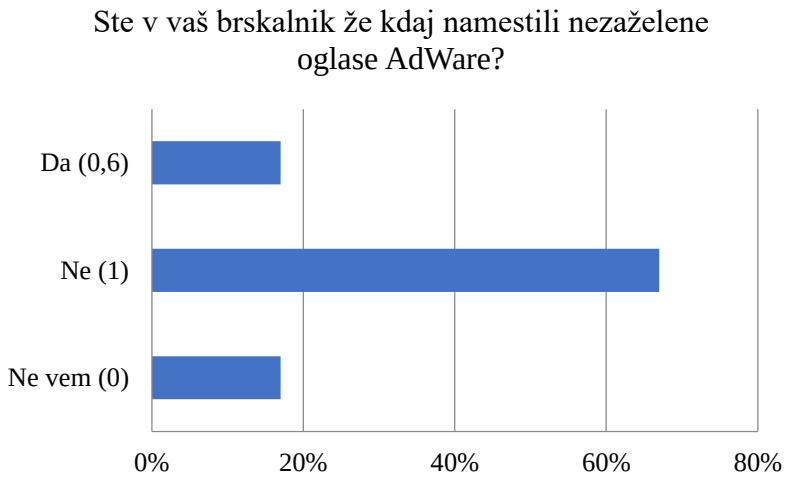
Vir: lastno delo.

Nezaželeni oglasi – AdWare. Vprašanje, ali so zaposleni že kdaj namestili nezaželene oglase, sem dodal kot primer pogoste težave nezaželene programske opreme, ki uporabnika zavede v namestitev. Po navadi s potrditvijo ali skriti znotraj namestitve kakšne druge aplikacije, prenesene iz vprašljivih virov. Gre torej za »podtaknjen« nezaželen tip programske opreme, ki nepozornim uporabnikom povzroča veliko slabe volje. Poleg uhajanja zasebnih in/ali osebnih podatkov ter prikazovanja oglasov lahko spreminja tudi nastavitve brskalnika, ki uporabnika vodijo na strani, namenjene ribarjenju.

Večina zaposlenih (16) pravi, da AdWare še niso namestili. Štirje zaposleni pa pravijo, da so AdWare že namestili, ostali štirje pa niso prepričani. Glede na postavljene kriterije vprašanja je ocena ozaveščenosti v primeru, da so AdWare že namestili, 0,6. Kljub temu da je zaposleni storil napako, predpostavljam, da je tveganje manjše kot v primeru zaposlenih, ki so odgovorili, da ne vedo. Sklepam, da je zaposleni, ki se je že srečal s to težavo, pridobil nekaj izkušenj o njenem obstoju (ozaveščenost ni 0). Iz pridobljenih rezultatov odgovorov ocenjujem, da je ozaveščenost dobra.

Ocena ozaveščenosti: dobro (76 %).

Slika 15: Nezaželeni oglasi – AdWare



Vir: lastno delo.

2.2.3 Upravljanje uporabniških podatkov

V tem poglavju me je zanimalo, kako zaposleni upravljajo z gesli. Poglavje vsebuje sedem vprašanj, ki se nanašajo na shranjevanje, deljenje in spreminjanje uporabniških podatkov.

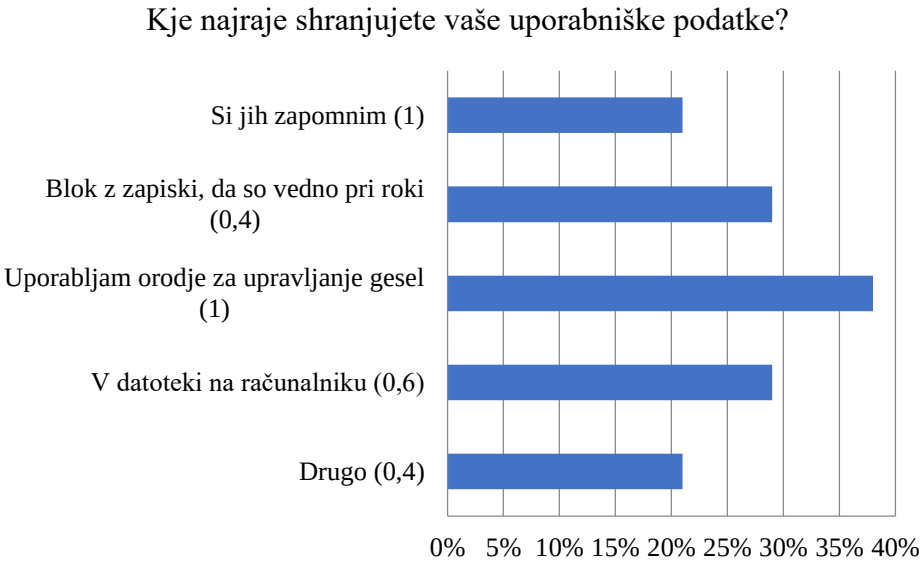
Shranjevanje uporabniških podatkov. Pri shranjevanju uporabniških podatkov me je zanimalo, kako zaposleni skrbijo za varnost gesel na delovnem mestu. Po podatkih poročila »Verizon 2021 Data Breach Investigations Report« je 80 % primerov odtekanja informacij posledica šibkega ali razkritega gesla (Widup, Pinto, Hylender, Bassett &

langlois, 2021). Politika čiste mize rešuje problem odtekanja informacij, kamor spadajo tudi uporabniški podatki. Gesla vsekakor ne sodijo na lepilne listke na zaslonu računalnika.

Večina zaposlenih (devet) uporablja orodje za upravljanje gesel. Sedem jih uporablja blok z zapiski, pet pa si jih geslo zapomni. Dva zaposlena shranjujeta podatke v datoteko na računalniku, eden zaposleni pa za shranjevanje uporablja telefon. Glede na tveganje je ocena vprašanja pri bloku z zapiski in telefonu enaka, 0,4. Blok z zapiski in telefon imata skupno težavo – prenosljivost, zaradi tega menim, da obstaja tveganje izgube ali odtujitve. Datoteka na računalniku ima oceno 0,6, saj obstaja tveganje, da je na kompromitiranem računalniku programska oprema, ki odčita vsebino datotek. Najmanjše tveganje pa predstavlja, če si jih uporabnik zapomni ali uporablja orodje za upravljanje gesel. Skupna ocena ozaveščenosti shranjevanja uporabniških podatkov je dobra.

Ocena ozaveščenosti: dobro (76 %).

Slika 16: Shranjevanje uporabniških podatkov



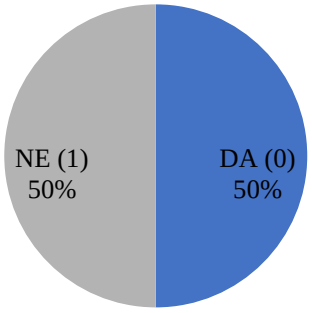
Vir: lastno delo.

Deljenje uporabniških podatkov med sodelavci. Pri tem vprašanju me je zanimalo, ali si zaposleni med sabo »izposojajo« uporabniške podatke. Razlogi za delitev uporabniškega računa so lahko različni. Iz izkušenj menim, da po navadi izhajajo iz narave dela in sodelovanja med zaposlenimi. Poleg težave, da imajo različni računi različne privilegije oz. pooblastila, obstaja tudi varnostno tveganje v primeru, ko zaposleni zapusti podjetje. Odgovori so bili povsem deljeni (12:12). Iz navedenih razlogov in rezultata odgovorov sklepam, da je ozaveščenost o tveganju glede deljenja uporabniških podatkov sprejemljiva.

Ocena ozaveščenosti: sprejemljivo (50%).

Slika 17: Deljenje uporabniških podatkov med sodelavci

Ali vaše uporabniške podatke kdaj zaupate sodelavcu?



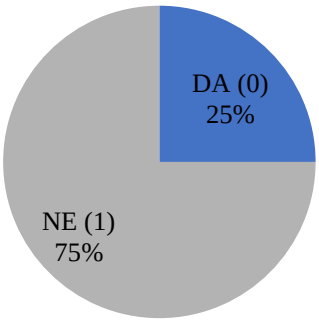
Vir: lastno delo.

Deljenje uporabniških podatkov z nezaposlenimi. Pri tem vprašanju me je zanimalo, ali je prisotno uhajanje informacij o uporabniških računih iz podjetja. Pri prejšnjem vprašanju sem bil mnenja, da pride do deljenja informacij med zaposlenimi zaradi narave dela in sodelovanja. V tem primeru je kakršenkoli razlog težje podpreti, saj obstajajo druge bolj varne rešitve (nov uporabniški račun z omejenimi pravicami) kot deljenje uporabniških podatkov zaposlenega. Skupno šest zaposlenih pravi, da so svoje uporabniške podatke že delili z osebo, ki ni zaposlena v podjetju. Na podlagi kriterija ocenjevanja je ozaveščenost dobra, vendar menim, da bi ta delež moral biti še manjši.

Ocena ozaveščenosti: dobro (75 %).

Slika 18: Deljenje uporabniških podatkov z nezaposlenimi

Ali vaše uporabniške podatke kdaj zaupate komu, ki ni vaš sodelavec?

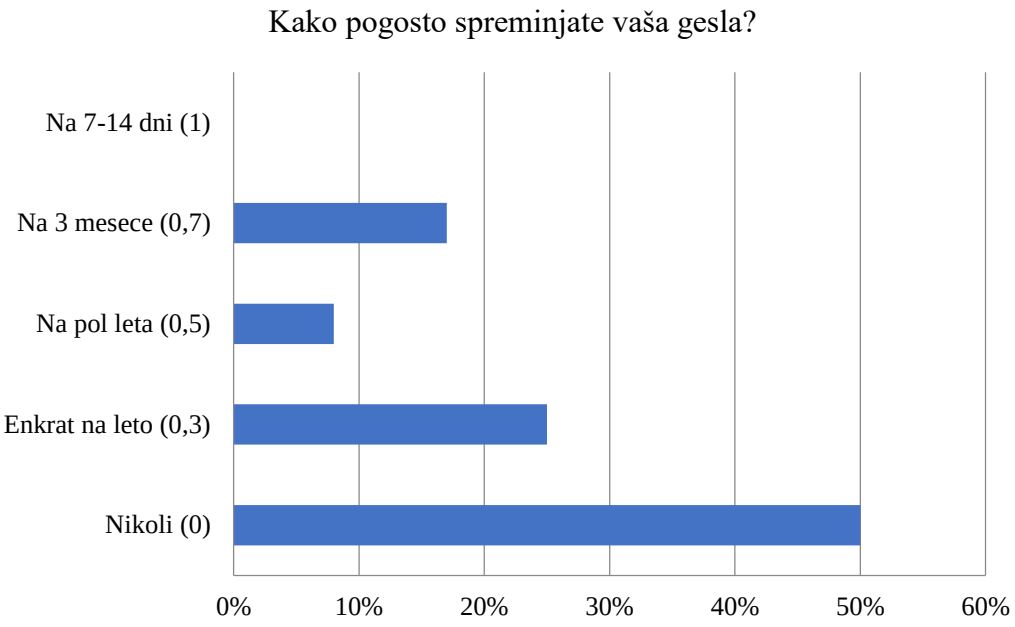


Vir: lastno delo.

Pogostost spreminjanja gesel. Ker podjetje nima zastavljene politike, ki bi narekovala pogostost spreminjanja gesel, me je pri tem vprašanju zanimalo, ali med zaposlenimi obstaja prostovoljno prakticiranje spreminjanja gesel. Polovica zaposlenih (12) pravi, da svojega gesla nikoli ne spremenijo, šest zaposlenih pa enkrat na leto. Dva zaposlena spremenita geslo na pol leta ter štirje zaposleni enkrat na tri mesece. Nihče od zaposlenih pa ne spreminja gesla na 7–14 dni. Pravilo kriterija za ocenjevanje ozaveščenosti tveganja je pri tem vprašanju zelo preprosto: manjši kot je interval (večja pogostost spreminjanja), višja je ocena. Končna ocena je na podlagi ocen intervalov nezadovoljiva.

Ocena ozaveščenosti: nezadovoljivo (23 %).

Slika 19: Pogostost spreminjanja gesla

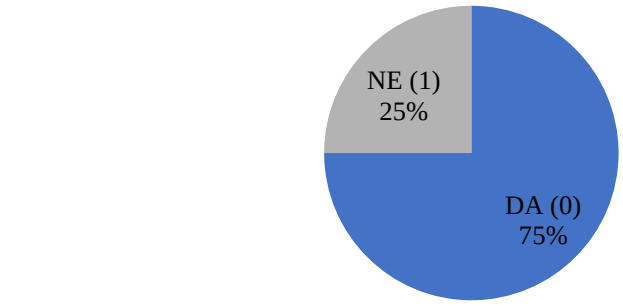


Vir: lastno delo.

Enaka gesla med uporabniškimi računi. Težava enakih gesel med različnimi uporabniškimi računi je, da so vsi uporabniški računi zaščiteni toliko kot njihovo skupno geslo. V primeru, da napadalec pridobi geslo uporabniškega računa, ga lahko poizkuša uporabiti na vseh računih, ki pripadajo uporabniku. Skupaj 18 zaposlenih je odgovorilo, da uporabljajo enaka gesla za različne uporabniške račune. Različna gesla uporablja le šest uporabnikov. Iz odgovorov sklepam, da je ozaveščenost o tveganju uporabe enakih gesel nezadovoljiva.

Ocena ozaveščenosti: nezadovoljivo (25 %).

Slika 20: Enaka gesla med različnimi uporabniškimi računi

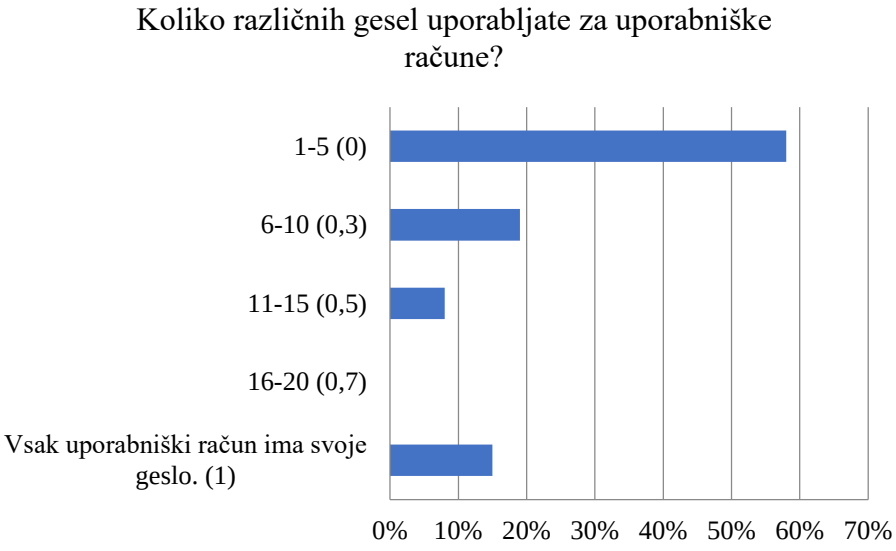


Vir: lastno delo.

Število različnih gesel. Pri tem vprašanju me je zanimalo, koliko različnih gesel uporabljajo zaposleni. Večina zaposlenih (13) uporablja 1–5 gesel, skupaj 6 zaposlenih pa jih uporablja 6–15. Štirje zaposleni pravijo, da za vsak račun uporabljajo drugo geslo. Iz rezultatov lahko sklepam, da kljub temu da zaposleni uporabljajo enaka gesla, tega ne storijo za vse račune. Iz rezultatov sklepam, da je ozaveščenost nezadovoljiva. Slika 21 prikazuje delež posameznih odgovorov.

Ocena ozaveščenosti: nezadovoljivo (24 %).

Slika 21: Število različnih gesel

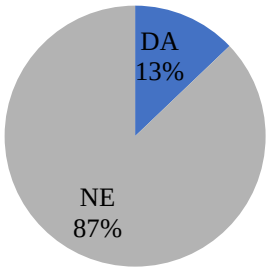


Vir: lastno delo.

Vdori v uporabniške račune. Namen tega vprašanja je bil izvedeti, kakšne so izkušnje zaposlenih oz. podjetja z vdori v uporabniške račune podjetja v preteklosti. Trije zaposleni pravijo, da je njihov uporabniški račun že bil tarča vdora. Ker gre za pretekli dogodek, o katerem nimam dovolj informacij, nisem podal ocene ozaveščenosti. Menim, da dogodek ne odraža tveganja, za katero bi lahko podal oceno. Pove nam le, da so se zaposleni v podjetju v preteklosti že soočili s težavo vdora v uporabniške račune, na kar pa ozaveščenost vsekakor vpliva.

Slika 22: Vdori v uporabniške račune

Ali je bil vaš uporabniški račun že kdaj tarča vdora?



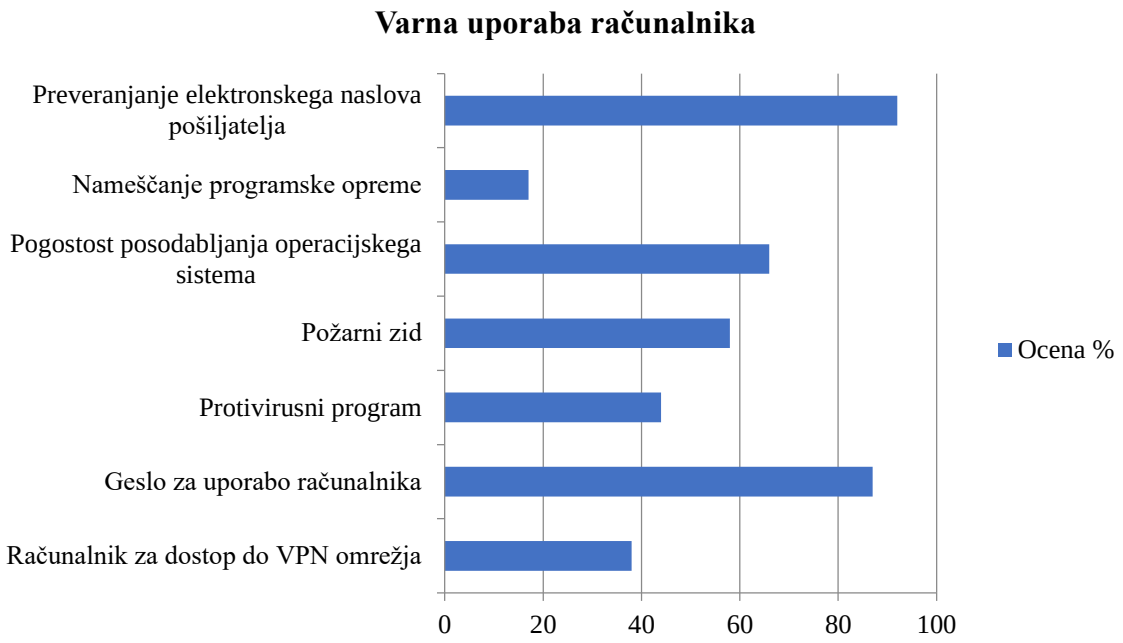
Vir: lastno delo.

2.2.4 Rezultati

V tem podpoglavju predstavljam končne ocene analize ozaveščenosti kibernetske varnosti za posamezno poglavje.

Varna uporaba računalnika. Slika 23 prikazuje pregled ocen ozaveščenosti zaposlenih o varni uporabi računalnika. Povprečna ocena ozaveščenosti za poglavje je po postavljenem kriteriju sprejemljiva (57 %). Največje tveganje kibernetske varnosti pri zaposlenih predstavljata nameščanje programske opreme s spleta in uporaba računalnika (ki ni služben) za dostop do VPN-omrežja podjetja. Najmanjše tveganje predstavljata preverjanje elektronske pošte in geslo za uporabo računalnika.

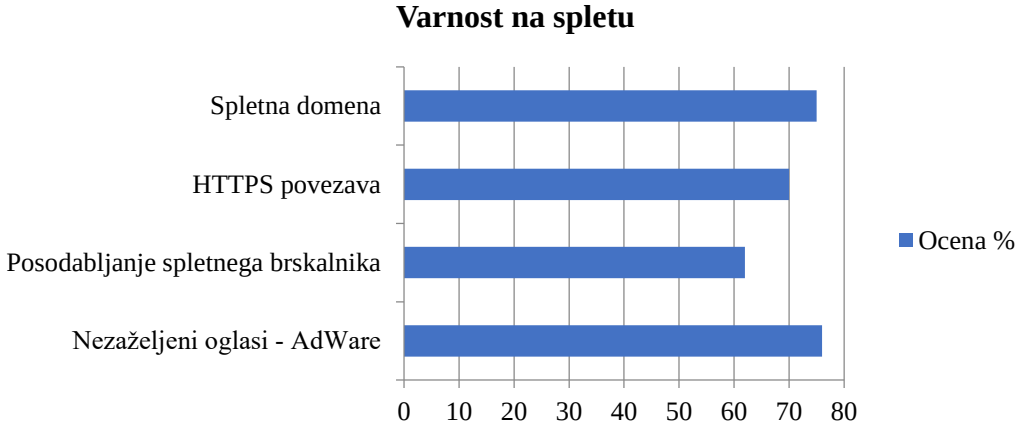
Slika 23: Varna uporaba računalnika – rezultati



Vir: lastno delo.

Varnost na spletu. Poglavje varnosti na spletu ima po postavljenem kriteriju skupno oceno dobro (71 %). Odgovori zaposlenih so nakazali, da so veliko bolje ozaveščeni glede kibernetske varnosti na spletu kot v prejšnjem poglavju – varna uporaba računalnika. Največje tveganje predstavlja posodabljanje spletnega brskalnika, najmanjše tveganje pa nezaželeni oglasi (AdWare). Slika 24 predstavlja ocene ozaveščenosti zaposlenih o posamezni temi področja varnosti na spletu.

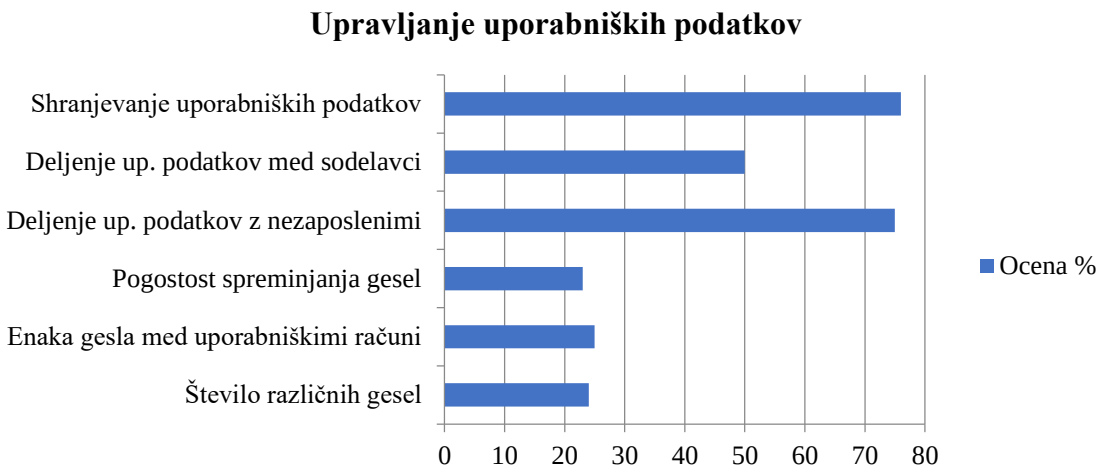
Slika 24: Varnost na spletu – rezultati



Vir: lastno delo.

Upravljanje uporabniških podatkov. V tem poglavju so zaposleni izkazali najnižjo ozaveščenost. Skupna ocena področja upravljanja uporabniških podatkov je glede na postavljeni kriterij nezadovoljiva (45 %). Največje tveganje predstavljata pogostost spreminjanja gesel in uporaba različnih gesel med uporabniškimi računi, najmanjše tveganje pa predstavljata shranjevanje uporabniških podatkov in deljenje uporabniškim podatkov z nezaposlenimi. Slika 25 prikazuje ocene ozaveščenosti za posamezen odgovor s področja upravljanja uporabniških podatkov.

Slika 25: Upravljanje uporabniških podatkov – rezultati



Vir: lastno delo.

2.2.5 Ugotovitve in predlogi izboljšav

Na podlagi rezultatov iz prejšnjega podpoglavja lahko povzamem, da je ozaveščenost zaposlenih o kibernetski varnosti »sprejemljiva«. Končna povprečna ocena je le nekoliko nad mejo postavljenega kriterija ocene »sprejemljivo« (58 %). Najbolj izstopa poglavje upravljanja uporabniških podatkov, kjer je bila ocena »nezadovoljivo« (45 %).

Namen analize ozaveščenosti zaposlenih o kibernetski varnosti je bil oceniti stanje ozaveščenosti zaposlenih in na podlagi ocen predlagati izboljšave. V nadaljevanju v ta namen izdelam seznam predlogov izboljšav za posamezne teme področij, kjer rezultati niso dosegli postavljenega kriterija ocene »dobro«. V seznam sem zajel vsa tematska vprašanja, kjer ni bil dosežen rezultat spodnje meje 70 %. Tabela 10 predstavlja seznam predlogov izboljšav za odkrite ranljivosti na področju varne uporabe računalnika.

Tabela 10: Varna uporaba računalnika – predlogi izboljšav

Ranljivost	Predlogi izboljšav
Nameščanje programske opreme na službeni računalnik Nezadovoljivo – 17 %	- Izdelati hierarhijo vlog, kjer imajo uporabniki omejene pravice pri nameščanju programske opreme. - Dovoljeno nameščanje samo programske opreme iz Windows Store.
Pogostost posodabljanja operacijskega sistema Sprejemljivo – 66 %	Nastavitev avtomatičnega nameščanja posodobitev sistema z uporabo »Group Policy«.
Požarni zid Sprejemljivo – 62 %	- Delavnica za zaposlene o kibernetski varnosti (predstavitev požarnega zidu). - Nastavitev administratorskih pravic za upravljanje »Microsoft Defender Firewall«.
Protivirusni program Nezadovoljivo – 44 %	- Delavnica za zaposlene o kibernetski varnosti (predstavitev protivirusnega programa F-Secure). - Nastavitev »Admin approval mode« za izklop/vklop programa.
Računalnik za dostop do VPN-omrežja Nezadovoljivo – 38 %	- Vzpostavitev zaščite omrežja z NAP (Network Access Protection), kjer določimo zahteve (požarni zid, različice varnostnih posodobitev itd.) pred vzpostavitvijo povezave z VPN-omrežjem podjetja. - Delavnica za zaposlene o kibernetski varnosti (predstavitev težave javnih dostopnih točk).

Vir: lastno delo.

Tabela 11 prikazuje predloge izboljšav za področje spletne varnosti. Na tem področju so bili rezultati ozaveščenosti zaposlenih najboljši, zaradi česar je tudi seznam predlogov zelo kratek.

Tabela 11: Varnost na spletu – predlogi izboljšav

Ranljivost	Predlogi izboljšav
Posodabljanje spletnega brskalnika Sprejemljivo – 62 %	- Nastavitev avtomatičnih posodobitev brskalnika z uporabo »Group policy«. - Uporaba brskalnika v načinu virtualizacije (angl. Browser virtualization), kjer brskalnik teče v peskovniku, ločenem od operacijskega sistema.

Vir: lastno delo.

Tabela 12 prikazuje predloge izboljšav za upravljanje uporabniških računov. Temi področja »Enaka gesla med uporabniškimi računi« in »Število različnih gesel« sem združil, ker menim, da je obe težavi mogoče odpraviti z uporabo enakih rešitev.

Tabela 12: Upravljanje uporabniških računov – predlogi izboljšav

Ranljivost	Predlogi izboljšav
Deljenje uporabniških podatkov med sodelavci Sprejemljivo – 50 %	Delavnica za zaposlene o kibernetski varnosti, kjer se predstavijo tveganja, povezana z deljenjem uporabniških podatkov, in kako jih na varen način lahko delimo.
Pogostost spreminjanja gesel Nezadovoljivo – 23 %	Vzpostavitev politike gesel na ravni podjetja z gesli, ki imajo omejen rok veljavnosti.
– **Enaka gesla med uporabniškimi računi** Nezadovoljivo – 25 % – **Število različnih gesel** Nezadovoljivo – 24 %	- Vzpostavitev sistema enotne prijave (angl. Single Sign-On – SSO). - Delavnica za zaposlene o kibernetski varnosti, kjer se predstavijo tveganja, povezana z uporabo enakih gesel med uporabniškimi računi.

Vir: lastno delo.

Vsem področjem je kot predlog izboljšave skupna delavnica oz. izobraževanje zaposlenih o kibernetski varnosti. Menim, da je to prvi korak, ki ga podjetje lahko izvede za povečanje ozaveščenosti in s tem zmanjšanje varnostnega tveganja. Interno izobraževanje lahko izvede IT-služba v obliki letne delavnice. Poleg delavnice lahko zaposleni svoje znanje osvežujejo z anketnim vprašalnikom. Za lažji pretok iz teoretičnega znanja je potrebno, da zavedanje prihaja tudi s strani menedžmenta, da se lahko najboljše prakse integrirajo tudi v organizacijo dela.

Poleg seznama izboljšav, predstavljenih v tabeli 12, je za podjetje na tem področju pomembno, da vzpostavi politiko gesel, ki temelji na aktualnih usmeritvah upravljanja gesel. Primer takšnih usmeritev je »NIST 800-63B Digital Identity Guidelines – 2017«. Definira usmeritve glede dolžine in kompleksnosti gesel, čas veljavnosti gesla, zgodovino uporabljenih gesel itd. Zadnji predlogi posodobitev usmeritev so bili deležni veliko kritik med varnostnimi strokovnjaki, saj med drugimi spremembami predlaga ukinitev periodičnega spreminjanja gesel. Analiza je pokazala, da to uporabnikom povzroča veliko nevšečnosti, saj jih ta ukrep sili v sestavljanje gesel na podlagi preteklega vzorca z dodajanjem dodatne črke ali številke na koncu gesla (Bounev & Olive, 2021). Moje mnenje je, da je omenjena težava rešljiva s »pametnejšim« obrazcem za izdelavo gesla, ki prepozna takšne kombinacije oz. vzorce.

2.3 Analiza omrežja VPN

Podjetje pri svojem delu aktivno uporablja lokalno omrežje (angl. Local Area Network, v nadaljevanju LAN) v kombinaciji z navideznim zasebnim omrežjem VPN. LAN-omrežje v

osnovi uporabljajo za deljenje delovnih datotek prek datotečnih strežnikov, dostop do internih aplikacij (projektno vodenje in kadrovski sistem) ter uporabo naprav, priključenih v omrežje. Podjetje je v času epidemije večino svojega poslovanja preselilo na oddaljeno delo in tako postalo popolnoma odvisno od VPN-omrežja. VPN-odjemalec je za vse zaposlene postal nujen. Iz tega izhaja, da je VPN-omrežje postalo najbolj vitalen del infrastrukture, potreben za poslovanje podjetja, in je z vidika kibernetske varnosti tudi najbolj kritičen za obravnavo, saj gre za »vstopno točko« do digitalnih virov podjetja.

Zaposleni pri svojem delu uporabljajo VPN za oddaljen dostop z uporabo odjemalca, kar pomeni, da imajo za delo vsi zaposleni na svojem delovnem računalniku nameščen VPN-odjemalec, ki se poveže na oddaljeni VPN-strežnik podjetja. VPN-strežnik poganja Fortinet VPN, ki poleg VPN-strežnika opravlja tudi funkcijo usmerjevalnika in požarnega zidu. VPN-strežnik uporablja protokol IPsec v načinu tunela (angl. Tunnel mode). Za šifriranje komunikacije je uporabljen simetrični algoritem AES (angl. Advanced Encryption Standard). Na delovno VPN-omrežje se zaposleni povežejo z uporabo klienta FortiClient VPN, s svojim uporabniškim imenom in geslom, ki je edinstveno za vsakega zaposlenega.

Ko je VPN-povezava vzpostavljena, zaposleni dostopajo do operacijskega sistema in ostale programske opreme delovnega računalnika z uporabo oddaljenega namizja (angl. Remote Desktop Protocol, v nadaljevanju RDP). Večino dela poteka prek RDP-odjemalca Windows Desktop Client. Kot glavna razloga so navedli licenčno programsko opremo, ki je nameščena na njihove delovne postaje, in dejstvo, da se je podjetje moralo na spremembo načina dela odzvati zelo hitro. Iz teh razlogov zaposlenim zaenkrat še niso priskrbeli prenosnih računalnikov, ki bi lahko ustrezno nadomestili delovne postaje.

2.3.1 Arhitektura omrežja

Arhitekturo omrežja podjetja lahko razdelimo na tri glavna »podomrežja«, kot to prikazuje Slika 26:

- domače omrežje ali omrežje zaposlenega, ki predstavlja vstopno točko v VPN-omrežje podjetja,
- LAN predstavlja interno delovno omrežje podjetja, ki je zunaj dostopno le prek VPN-povezave,
- DMZ-cona (angl. Demilitarized zone), s katero dodatno zaščitimo LAN-omrežje, je namenjena storitvenim servisom (elektronska pošta, podatkovna baza, spletni strežnik in varnostne kopije).

Tabela 13 vsebuje bolj podroben opis storitev in programske opreme, ki jih podjetje uporablja, ter potrebnih protokolov za delovanje.

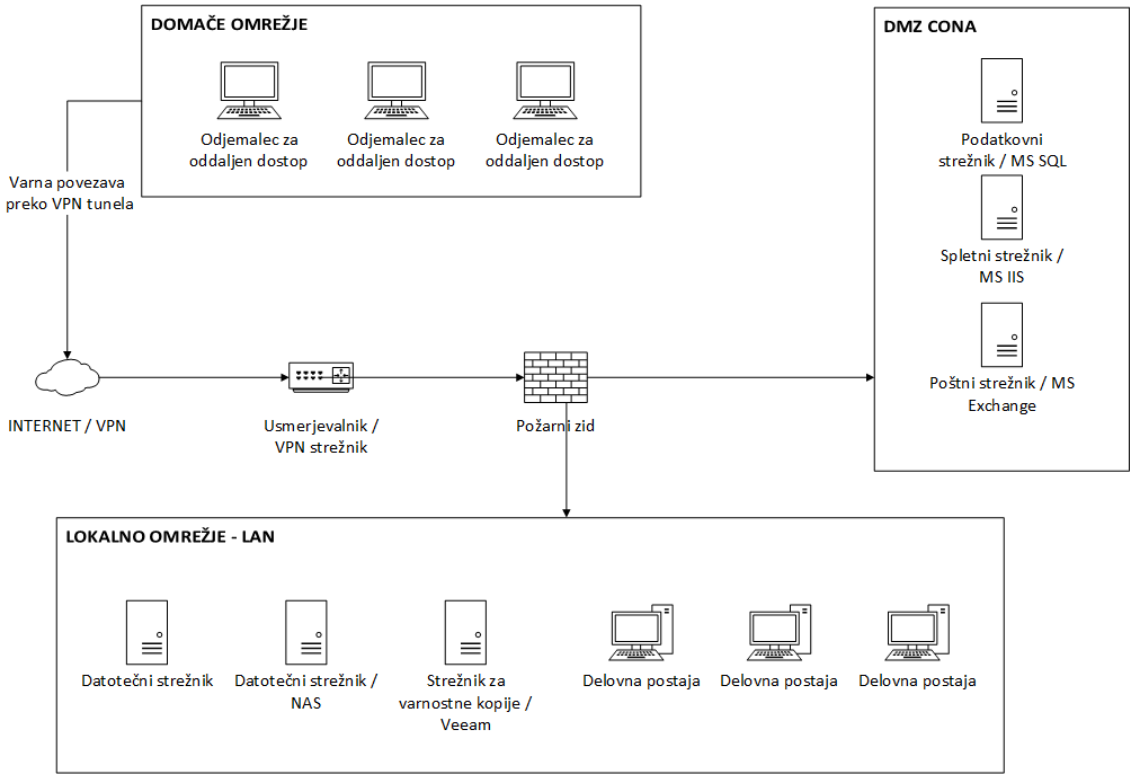
Tabela 13: Programska oprema storitev

Storitev	Programska oprema	Protokoli /vrata
Datotečni strežnik	Windows Server 2016	SMB/NFS (139, 445)
Podatkovni strežnik	MS SQL Server 2019	TCP (1433)
Spletni strežnik	Windows Server 2016 – IIS	HTTP/HTTPS (80, 443)
Poštni strežnik	MS Exchange Server 2016	SMTP (25), IMAP (143)
Varnostne kopije	Veeam Backup & Replicate	HTTPS (443)
Oblačni strežnik – NAS	Synology Disk Manager	HTTPS/SSH (odvisno od servisa)

Vir: lastno delo.

Slika 26 prikazuje arhitekturo omrežja podjetja. Del LAN predstavlja izolirna DMZ-cona, katere naloga je izpostavitev servisov brez dostopa do LAN-omrežja. Iz diagrama je razvidno, da je DMZ-cona postavljena z uporabo enega požarnega zidu. Takšen način postavitve imenujemo »single-firewall DMZ«.

Slika 26: Arhitektura omrežja



Vir: lastno delo.

Poleg že omenjenih storitev v DMZ-coni je vredno omeniti strežnik za varnostne kopije, ki z uporabo inkrementalnih varnostnih kopij v predstavljeni infrastrukturi poskrbi za takojšnjo obnovitev storitev. Varnostne kopije se izdelujejo enkrat na dan, kar pomeni, da bi podjetje v najslabšem primeru izgubilo podatke za največ en delovni dan.

2.3.2 Odkrite grožnje in ranljivosti

V tem podpoglavju na podlagi sheme omrežja iz prejšnjega poglavja definiram grožnje in ranljivosti za VPN-omrežje izbranega podjetja. Tabela 15 prikazuje grožnje, ki so človeške narave in relevantne za VPN-omrežje. Poleg človeških groženj poznamo tudi naravne (primer: požar, poplava, potres) ter okoljske grožnje (primer: napake na električnem omrežju, odpoved strojne opreme ipd.). Zaradi osredotočanja moje naloge na kibernetsko varnost, katere grožnje so po navadi človeške narave, sem naravne in okoljske grožnje pri analizi izpustil.

Grožnje. V tem koraku bom definiral potencialne grožnje za VPN-omrežje podjetja. Tabela 14 razdeli grožnje na namerne in nenamerne grožnje. O namernih grožnjah govorimo, kadar imamo opravka z osebo, ki ima za svojimi dejanji motiv (finančni, škodoželjen, želja po dokazovanju itd.). Pri nenamernih grožnjah pa imamo opravka z grožnjami posrednega vpliva. Te izhajajo iz različnih napak (človeških in tehničnih), ki predstavljajo posredno grožnjo kibernetski varnosti sistema.

Tabela 14: VPN – seznam potencialnih groženj

Grožnje	**Opis grožnje**
Namerne grožnje	
Socialni inženiring	Zlonamerna oseba skuša s prevaro pridobiti zaupne podatke (uporabniški podatki, informacije o sistemu ipd.). V številnih primerih gre za izkoriščanje zaupanja.
Kraja občutljivih podatkov	Zlonamerna oseba na nepooblaščen način pridobi občutljive podatke o sistemu (primeri: odtujitev delovnega računalnika, zapiski iz delovne mize, smeti itd.).
Prisluškovanje	Zlonamerna oseba prisluškuje komunikaciji, kjer se razkrijejo zaupni podatki. Prestrezanje komunikacije lahko poteka v elektronski komunikaciji (VoIP, instant sporočila itd.), kakor tudi fizičnem pogovoru med osebami na dovolj primerni razdalji.
Ribarjenje (angl. Phising)	Napadalec poizkuša s prevaro (primer: lažna spletna stran) od uporabnika pridobiti podatke, ki jih nato lahko zlorabi.
Zlonamerna programska oprema (angl. Malware)	V to kategorijo spada vsa programska oprema, ki lahko škoduje sistemu, kot so: virusi, vohunska programska oprema, črvi, trojanski konji itd. Povzročijo lahko izgubo podatkov, odtekanje informacij, prevzem nadzora nad sistemom itd.
Napad s posrednikom (angl. Man-in-the middle Attack)	Napadalec (posrednik) preusmeri promet odjemalca in strežnika na sebe in s tem prisluškuje mrežnem prometu. Odjemalec in strežnik tega v komunikaciji ne zaznata.

se nadaljuje

Tabela 14: VPN – seznam potencialnih groženj (nad.)

Grožnje	Opis grožnje
Namerne grožnje	
Porazdeljen napad za zavrnitev storitve (angl. Distributed Denial of Service, v nadaljevanju DDoS)	Pri tej obliki napada skuša napadalec »ohromiti« ali prekiniti delovanje storitve. V našem primeru je to VPN-strežnik. Obstaja več različnih metod DDoS-napada (primer: SSL Flooding, SSL Regeneration, TCP Blend itd.).
Prestrezanje seje (angl. Session hijacking)	Napadalec skuša pridobiti veljaven ključ seje prijavljenih uporabnikov v VPN-omrežje. Ko ta ključ pridobi, ga zlorabi za vzpostavitev povezave, saj strežnik ne loči med pravo in »ugrabljeno« sejo. Ena izmed zadnjih odkritih ranljivosti VPN-seje je CVE-2019-14899.
Napad z grobo silo (angl. Brute force attack)	Napadalec izvrši serijo zahtevkov za prijavo na VPN-strežnik z ugibanjem uporabniškega imena in gesla. Lahka tarča so po navadi strežniki in usmerjevalniki s privzetimi nastavitvami.
Nenamerne grožnje	
Razkrivanje informacij zaposlenih	Zaposleni lahko nenamerno razkrivajo več informacij, kot je potrebno, v primeru, da o kibernetski varnosti niso dobro ozaveščeni.
Nekdanji zaposleni	Kadar pride do prekinitve delovnega razmerja, je treba poskrbeti, da za zaposlenim »počistimo« vsa pooblastila, ki jih je imel v sistemu (osebni prenosnik za delo z dostopnimi podatki).
Napačne nastavitve dostopov in privilegijev uporabnikov	Pri napačnih nastavitvah, ki so plod človeške neprevidnosti, lahko pride do uporabnikov, ki imajo dostop do informacij, za katere niso pooblaščeni.
Šibka gesla	Kadar ima uporabnik možnost nastavitve gesla, obstaja veliko tveganje, da bo izbral geslo, ki je enostavno za zapomniti, vendar šibko z vidika varnosti.

Vir: Refsdal, Solhaug & Stølen (2015, str. 69–72).

Odkrite ranljivosti. Na podlagi seznama potencialnih groženj iz prejšnjega koraka opredelim ranljivosti, odkrite v izbranem podjetju, ki jih potencialna grožnja lahko izkoristi. Pri odkrivanju ranljivosti kibernetske varnosti si lahko pomagamo z bazami ranljivosti (angl. Common Vulnerabilities and Exposures, v nadaljevanju CVE). CVE-baza je katalog javno razkritih kibernetskih ranljivosti. Vsaka odkrita in objavljena ranljivost vsebuje edinstveno referenčno številko CVE, ki nam razkrije podrobnosti o odkriti ranljivosti. Referenčna številka vsebuje leto odkrite ranljivosti in identifikacijsko številko ranljivosti (primer: CVE-2019-14899) (CVE, 2021). Ena izmed baz ranljivosti CVE je National Vulnerability Database (NVD), ki je del delovnega ogrodja NIST. Dostopna je na naslovu https://nvd.nist.gov/vuln/search.

Pri odkrivanju ranljivosti sem na podlagi intervjuja z IT-službo pridobil podatke o trenutnem stanju upravljanja varnosti, nastavitev programske opreme in praks ter izdelal tabelo ranljivosti (glej Tabela 15), za katere predpostavljam, da predstavljajo tveganje kibernetske varnosti v podjetju. Skoraj vse podatke o potencialnih ranljivostih, naštete v tabeli, sem pridobil iz prejšnjega poglavja (»Analiza ozaveščenosti o kibernetski varnosti«), kjer sem kot metodo za zbiranje podatkov uporabil anketni vprašalnik. Pri ugotovitvah izstopa le ranljivost gesel na delovnih postajah. Pri primerjanju rezulatov sem ugotovil, da se odgovori zaposlenih glede gesel na delovnih postajah ne ujemajo z odgovori intervjuja IT-službe. Zaposleni so v vprašalniku analize ozaveščenosti odgovorili, da imajo nastavljeno geslo, med tem ko IT-služba pravi nasprotno.

Tabela 15: VPN – seznam odkritih ranljivosti

Ranljivost	**Opis**
Socialni inženiring	Ozaveščenost zaposlenih o deljenju zaupnih informacij.
VPN-odjemalec – prijava	VPN-odjemalec je nastavljen na privzet način prijave (uporabniško ime in geslo).
Konfiguracija DMZ-cone	DMZ-cona je vzpostavljena v najbolj osnovnem načinu single-firewal DMZ.
Ravni domenskih uporabnikov	Podjetje nima vzpostavljenega ustreznih ravni vlog za vzpostavitev uravnoteženega dodeljevanja pravic. Active directory vsebuje vlog admin in navaden uporabnik.
Posodabljanje programske opreme	Podjetje je v preteklosti že bilo tarča zastarele različice programske opreme usmerjevalnika.
Politika gesel	Podjetje nima vzpostavljene politike menjave gesel.
Shranjevanje gesel	Podatki o uporabniških računih so shranjeni v datoteki na datotečnem strežniku in dostopni vsem zaposlenim.
Gesla na delovnih postajah	Vsi zaposleni na svojih delovnih postajah nimajo nastavljenega gesla. Razlog, ki ga navajajo, je narava dela – zaposleni si včasih med sabo »posojajo« računalnik za delo.

Vir: lastno delo.

2.3.3 Model ocene tveganja

Za ocenjevanje tveganja sem uporabil kvalitativno metodo vrednotenja verjetja in vpliva. Ocenjevanje sem izvedel z najpogosteje uporabljenim modelom, matriko tveganj. Faktor tveganja je ocenjen po enačbi (1):

$$R = L * I * C \quad (1)$$

kjer je:
- R ... tveganje (angl. Risk),
- L ... verjetnost (angl. Likelihood),
- I ... vpliv (angl. Impact),
- C ... strošek (angl. Cost).

Za ocenjevanje verjetja sem izdelal tristopenjsko ordinalno lestvico z naslednjimi faktorji verjetja: visoko, srednje in nizko. Tabela 16 prikazuje faktorje, uporabljene za oceno

verjetja, in njihove uteži. Uteži bodo uporabljene pri določanju intervalnih vrednosti tveganja.

Tabela 16: Lestvica faktorjev verjetja

Verjetnost	**Opis**
Zelo visoko (5)	- Obstaja zelo veliko verjetnost, da bo zaradi grožnje prišlo do izkoriščenja ranljivosti. - Za obstoječe kontrole in protiukrepe menimo, da so v primeru uresničitve grožnje neučinkoviti.
Visoko (4)	- Obstaja veliko verjetnost, da bo zaradi grožnje prišlo do izkoriščenja ranljivosti. - Za obstoječe kontrole in protiukrepe menimo, da lahko grožnje v zelo majhni meri preprečijo.
Srednje (3)	- Obstaja verjetnost, da bo zaradi grožnje prišlo do izkoriščenja ranljivosti. - Za obstoječe kontrole in protiukrepe menimo, da lahko grožnje v omejeni meri preprečijo.
Majhno (2)	- Obstaja majhno verjetnost, da bi prišlo do izkoriščenja ranljivosti. - Za obstoječe kontrole in protiukrepi menimo, da bodo v primeru uresničitve grožnje te v veliki meri preprečili.
Zelo majhno (1)	- Obstaja zanemarljivo verjetnost, da bi prišlo do izkoriščenja ranljivosti. - Za obstoječe kontrole in protiukrepe menimo, da bodo v primeru uresničitve grožnje te v zelo veliki meri preprečili.

Vir: lastno delo.

Za ocenjevanje vpliva sem izdelal tristopenjsko ordinalno lestvico z naslednjimi faktorji vpliva: visok, srednji, nizek. Tabela 17 prikazuje seznam faktorjev vpliva in njihove uteži.

Tabela 17: Lestvica faktorjev vpliva

Stopnja vpliva	**Opis**
Zelo visoka (5)	- Varnostni incident bo imel zelo resen vpliv in večje št. posledic za poslovanje v organizaciji. - Predpostavljamo, da bodo zaupnost, integriteta in dostopnost v primeru uresničitve grožnje zelo visoko ogrožene. - Zahteva takojšnje ukrepanje.
Visoka (4)	- Varnostni incident bi imel resen vpliv in posledice za poslovanje v organizaciji. - Predpostavljamo, da bodo zaupnost, integriteta in dostopnost v primeru uresničitve grožnje visoko ogrožene. - Zahteva čimprejšnje ukrepanje.
Srednja (3)	- Varnostni incident bi imel v določeni meri vpliv in posledice za poslovanje v organizaciji. - Predpostavljamo, da bodo zaupnost, integriteta in dostopnost v primeru uresničitve v določeni meri ogrožene. - Zahteva določeno mero odziva.

se nadaljuje

Tabela 17: Lestvica faktorjev vpliva (nad.)

Stopnja vpliva	**Opis**
Nizka (2)	- Varnostni incident bi imel omejen vpliv na poslovanje in organizacijo. - Predpostavljamo, da bodo zaupnost, integriteta in dostopnost v primeru uresničitve ogrožene v omejenem obsegu. Zahteva po ukrepanju ima nižjo prioriteto.
Zelo nizka (1)	- Varnostni incident bi imel zanemarljiv vpliv na poslovanje in organizacijo. - Predpostavljamo, da bodo zaupnost, integriteta in dostopnost v primeru uresničitve zanemarljivo ogrožene. - Zahteva po ukrepanju ima najnižjo prioriteto.

Vir: lastno delo.

Iz lestvice verjetja in vpliva sem nato izdelal matriko tveganja, ki jo prikazuje Tabela 18. Numerične ocene predstavljajo uteži, ki so produkt stopnje verjetja in stopnje vpliva. Z izdelanimi ocenami v naslednjem poglavju ocenim tveganje za posamezno odkrito ranljivost.

Tabela 18: Matrika tveganja

VERJETJE	**STOPNJA VPLIVA**				
	Zelo nizka (1)	**Nizka (2)**	**Srednja (3)**	**Visoka (4)**	**Zelo visoka (5)**
Zelo visoko (5)	Srednje R = (5*1) **5**	Visoko R = (5*2) **10**	Visoko R = (5*3) **15**	Zelo visoko R = (5*4) **20**	Zelo visoko R = (5*5) **25**
Visoko (4)	Nizko R = (4*1) **4**	Srednje R = (4*2) **8**	Visoko R = (4*3) **12**	Visoko R = (4*4) **16**	Zelo visoko R = (4*5) **20**
Srednje (3)	Nizko R = (3*1) **3**	Srednje R = (3*2) **6**	Srednje R = (3*3) **9**	Visoko R = (3*4) **12**	Visoko R = (3*5) **15**
Nizko (2)	Nizko R = (2*1) **2**	Nizko R = (2*2) **4**	Srednje R = (2*3) **6**	Srednje R = (2*4) **8**	Visoko R = (2*5) **10**
Zelo nizko (1)	Nizko R = (1*1) **1**	Nizko R = (1*2) **2**	Nizko R = (1*3) **3**	Nizko R = (1*4) **4**	Srednje R = (1*5) **5**

Vir: lastno delo.

2.3.4 Ugotovitve in predlogi izboljšav

Tabela 19 prikazuje ocenjeno tveganje za posamezno odkrito potencialno ranljivost in predloge izboljšav. Ocene tveganj so bile podane z uporabo matrike tveganja (tabela 18). S

pomočjo vodje službe za informatiko smo podali kvalitativne ocene stopnje verjetja in stopnje vpliva za posamezno odkrito ranljivost. Pri oceni verjetja so bile upoštevane pretekle izkušnje z varnostnimi incidenti, saj pričakujemo, da se ti utegnejo ponoviti. Eden od takšnih primerov je bila odkrita ranljivost programske opreme usmerjevalnika Fortinet, ki ga podjetje uporablja. V omenjenem usmerjevalniku je bila odkrita ranljivost prijave prek ukazne lupine SSH (angl. Secure Shell Protocol) z uporabo uporabniškega imena in gesla, ki ga je proizvajalec pozabil odstraniti na stopnji testiranja programske opreme. To napadalcu omogoča prevzem nadzora nad usmerjevalnikom. Ranljivost je bila prisotna v različicah od novembra 2012 do julija 2014 (Khandelwal, 2016). Podjetje je za omenjeno ranljivost izvedelo od partnerskega podjetja, s katerim sodeluje. Tehnične predloge izboljšav sem črpal s seznama iz analize »Common Vulnerabilities Exposed in VPN – A Survey« avtorja Bansode in Girdhar (2021, str. 6-7).

Pri analizi VPN-omrežja sem imel dve pomembni omejitvi: fizični dostop do omrežja in omejeno tehnično znanje. Podjetje bi analizo omrežja s penetracijskim testiranjem dovolilo le varnostnim strokovnjakom, kjer so jasno skomunicirani pogoji razkritja informacij. Iz tega razloga večina odkritih ranljivosti VPN-omrežja temelji na informacijah, pridobljenih v poglavju Analiza ozaveščenosti o kibernetski varnosti, predlagane ukrepe pa sem apliciral na VPN-omrežje. Iz enakih razlogov se pri oceni tveganja nisem odločil za vrednotenje stroškov, ki jih faktor tveganja lahko ovrednoti. Ukrepi, navedeni v tem poglavju, niso del analize stroškov in koristi naslednjega poglavja, saj z vpeljavo ukrepov iz prejšnjega poglavja pokrijemo skoraj celoto predlaganih ukrepov pri analizi VPN-omrežja. Zelo specifična sta le DMZ-cona in prijava z VPN-odjemalcem, ki pa po mojem mnenju končnih ocen stroškov in koristi ne spremenita bistveno.

Tabela 19: VPN-omrežje – ranljivosti in predlogi izboljšav

Ranljivost	Opis	Verjetnost	Stopnja vpliva	Tveganje	Predlogi izboljšav
Socialni inženiring	Slaba ozaveščenost zaposlenih o deljenju zaupnih informacij.	Srednje	Visoka	Srednje	Delavnica za zaposlene o kibernetski varnosti
VPN-odjemalec – prijava	VPN-odjemalec je nastavljen na privzet način prijave (uporabniško ime in geslo).	Srednje	Visoka	Srednje	Dvojno preverjanje prisotnosti (angl. Two-Factor Authentication – 2FA)
Konfiguracija DMZ-cone	DMZ-cona je vzpostavljena v najbolj osnovnem načinu »single-firewal« DMZ.	Nizko	Visoka	Nizko	Zaščita internega omrežja z vzpostavitvijo »Dual firewall« DMZ-cone
Ravni domenskih uporabnikov	Podjetje nima vzpostavljenih ustreznih ravni vlog za vzpostavitev uravnoteženega dodeljevanja pravic (obstajata samo admin in navadni uporabnik).	Srednje	Srednja	Srednje	Izdelava hierarhije uporabniških vlog z omejenimi pravicami
Posodabljanje programske opreme	Podjetje je v preteklosti že bilo tarča zastarele različice programske opreme usmerjevalnika.	Visoko	Visoka	Visoko	Med varnostne kontrolne točke dodati preverjanje posodobitev prog. opreme usmerjevalnika (angl. Firmware)
Politika gesel	Podjetje nima vzpostavljene politike menjave gesel.	Srednje	Visoko	Srednje	Vzpostavitev politike gesel na ravni podjetja z gesli, ki imajo omejen rok veljavnosti
Shranjevanje gesel	Podatki o uporabniških računih so shranjeni v datoteki na datotečnem strežniku in dostopni vsem zaposlenim.	Nizko	Srednje	Nizko	Uporaba programske opreme za upravljanje gesel (primer: Bitwarden)

Vir: lastno delo.

3 EKONOMSKA UPRAVIČENOST IZVEDBE PROTIUKREPOV

To poglavje se navezuje na poglavje 2.2, kjer je bil namen ugotoviti stanje ozaveščenosti zaposlenih o kibernetski varnosti ter pripraviti protiukrepe, ki jih podjetje lahko sprejme za zmanjšanje tveganja. Vsak sprejet varnostni protiukrep za podjetje predstavlja strošek. Ta strošek je pred pričetkom uvedbe treba upravičiti, hkrati pa ne sme presegati koristi, ki jih ima podjetje v primeru uvedbe protiukrepa. V tem poglavju skušam s pomočjo analize stroškov in koristi (angl. Cost-benefit analysis) ugotoviti, ali so predlagani protiukrepi upravičeni glede na ocenjeno tveganje za posamezno odkrito ranljivost.

Zaradi zahtevnosti ocenjevanja in manka podatkov o varnostnih incidentih pri oceni vpliva uporabim kombinacijo kvantitativne in kvalitativne metode. Analiza temelji na kvantitativni metodi, pri čemer so faktorji vpliva in verjetnost ocenjeni s kombinacijo pričakovane ocene IT-službe podjetja ter historičnih podatkov o incidentih (št. posameznih incidentov zadnjih pet let).

3.1 Model ocenjevanja

Pred pričetkom ocenjevanja stroškov je treba ovrednotiti verjetnost, vpliv in pričakovano izgubo zaradi varnostnega incidenta. Dobljene vrednosti nato uporabimo za izračun koristi. Korist je ocenjen strošek, ki se mu želimo izogniti v primeru, da za odkrito ranljivost obstaja tveganje. Za analizo tveganja uporabim metodo »pričakovane letne izgube« (angl. Annual Loss Expectancy, v nadaljevanju ALE), ki velja za najbolj pogosto uporabljeno in jo priporoča mednarodni kozorcij za certifikacijo sistemske varnosti (angl. Information System Security Certification Consortium – ISC) (Panchit, 2006, str. 34). V tem poglavju predstavim posamezne faktorje metode, ki so uporabljeni pri ocenjevanju koristi v naslednjem poglavju.

Stopnja vpliva (angl. Single Loss Exposure, v nadaljevanju SLE). Pričakovano izgubo zaradi enkratne uresničitve varnostnega incidenta imenujemo SLE. SLE zapišemo z naslednjo enačbo (2) (Douglas, 2011, str. 437):

$$SLE = AV * EF \quad (2)$$

kjer je:
- AV ... vrednost sredstev (angl. Asset value),
- EF ... pričakovana izguba v odstotkih (angl. Exposure factor).

Verjetnost (angl. Annual Rate of Occurence, v nadaljevanju ARO). Za varnostne incidente predpostavljamo, da imajo možnost uresničitve glede na ocenjeno verjetnost. Verjetnost je ocena števila varnostnih incidentov. Za ocenjevanje uporabim letno stopnjo pojavljanja. ARO definira pričakovano letno pojavnost incidenta. Primer: če je verjetnost, da se bo varnostni incident zgodil enkrat na pet let, je vrednost ARO 0,2 (20 %) (Douglas, 2011, str. 438).

Pričakovana letna izguba (ALE). Izračunamo kot produkt pričakovane izgube in ocenjenega verjetja. Predstavlja pričakovano letno finančno izgubo v primeru, da podjetje ne zmanjša tveganja oz. ne uvede protiukrepa. Pričakovano izgubo zapišemo z naslednjo enačbo (3) (Douglas, 2011, str. 437):

$$ALE = SLE * ARO \quad (3)$$

kjer je:
- SLE ... pričakovana izguba (stopnja vpliva),
- ARO... letna stopnja pojavnosti (verjetnost).

3.2 Ocena stroškov in koristi

Na podlagi ugotovitev analize ozaveščenosti zaposlenih (poglavje 2.2.5) v tem poglavju ocenim stroške in koristi predlaganih protiukrepov. V omenjenem poglavju vsaka tema področja predstavlja ranljivost. Podana ocena je obratno sorazmerna s tveganjem. Protiukrepe sem predlagal za ranljivosti, kjer je bila ocena ozaveščenosti manj kot 70 %.

Tabela 20 prikazuje ocene stroškov za tehnično izvedbo posameznega protiukrepa za obdobje petih let. Stroški zajemajo delo in vzdrževanje za obdobje petih let. Vsem protiukrepom je skupen strošek delavnica za zaposlene. Ker fluktuacija zaposlenih v izbranem podjetju ni velika, sem izbral izvedbo vsako drugo leto.

Tabela 21 prikazuje ocene koristi z uporabo metode ALE za obdobje petih let. Pri posameznem protiukrepu so kot »predpostavke« definirane ocene posameznih faktorjev analize.

Pri ocenah SLE je bila ocenjena škoda, ki jo podjetje utrpi zaradi izpada poslovanja. Upoštevan je tudi odzivni čas, ki temelji na preteklih izkušnjah, pripravljenosti in organiziranosti, varnostnih kopijah itd. Ker podjetje nima varnostnega strokovnjaka, je odzivni čas pričakovano daljši, kar dodatno povečuje stroške oz. koristi v prid protiukrepa. ARO temelji na racionalni oceni preteklih izkušenj IT-službe podjetja, kakor tudi zmanjšana stopnja verjetnosti (angl. Probability reduction rate), ki ocenjuje zmanjšano verjetnost varnostnega incidenta.

Koristi so izračunane kot zmanjšanje tveganja (angl. Reduction in risk, v nadaljevanju RIR). RIR za posamezen incident je izračunan z naslednjo enačbo (4):

$$RIR = ARO * SLE * PRR \quad (4)$$

kjer je:
- ARO ... letna stopnja pojavnosti (verjetnost),
- SLE ... pričakovana izguba (stopnja vpliva),
- PRR ... zmanjšana stopnja verjetnosti.

Pri ocenah kibernetskega napada ni bil predviden strošek v primeru, kadar imamo opravka z izsiljevalskimi virusi, ki za zaklenjene podatke zahtevajo odkupnino. V tem primeru bi

lahko uporabil povprečno »izsiljeno plačilo« za obnovitev podatkov, ki naj bi po podatkih Infosecurity Magazina (Muncaster) znašalo 541.010 ameriških dolarjev. Ta znesek je za obravnavano podjetje previsok, saj podjetje svojih digitalnih sredstev ne ceni tako visoko. Sklepam, da analiza s tem ne bi pridobila nobene dodatne vrednosti.

Na podlagi analize stroškov in koristi ocenjujem, da je izvedba predlaganih ukrepov smiselna. Prvo leto bo podjetje zaradi velikih začetnih stroškov uvedbe protiukrepov imelo predvideno izgubo v višini –13.115 €. Vsa naslednja leta pa so koristi uvedbe protiukrepov večji od stroškov. Prav tako ocenjujem, da predlagani protiukrepi ne ustvarjajo visokih letnih stroškov za vzdrževanje glede na koristi, kar poveča smiselnost uvedbe.

Investicije v informacijsko varnost je, ekonomsko gledano, težje upravičiti v primerjavi z investicijami, ki ustvarjajo dobiček (primer: oglaševanje). Informacijska varnost ne ustvarja dobička, ampak preprečuje izgube, zaradi česar je težje meriti njihovo učinkovitost (ENSIA, 2012). V prejšnjem poglavju sem na podlagi analize stroškov in koristi ugotovil, da je izvedba predlaganih ukrepov smiselna. Kljub pozitivni oceni je izvedbo protiukrepov treba upravičiti še ekonomsko tako, da upoštevamo še oportunitetne stroške. Podjetje bi lahko znesek, ki ga porabi za izvedbo protiukrepov, vložilo v alternativne naložbe, ki mu prinašajo večje finančne koristi.

Ker gre pri uvedbi varnostnih protiukrepov za dolgoročno investicijo, bi podjetje za analizo ekonomske upravičenosti izvedbe ukrepov lahko uporabilo neto sedanjo vrednost (v nadaljevanju NSV). Z uporabo NSV primerjamo stroške in koristi skozi obdobja, pri čemer njihove vrednosti diskontiramo v sedanjo vrednost. Kadar je NSV pozitiven, pomeni, da investicijo sprejmemo, ker imamo od nje koristi oz. dobiček. V primeru, da primerjamo več investicij, sprejmemo tisto, ki ima večji NSV (Panchit, 2006, str. 43). NSV zapišemo z naslednjo enačbo (5):

$$NSV = \sum_{t=0}^{T} \frac{B_t - C_t}{(1+r)^t} \qquad (5)$$

kjer je:
- B_t ... koristi obdobja,
- C_t ... stroški obdobja,
- r ... diskontna stopnja.

Ker je diskontna stopnja v zadnjih letih zelo nizka, NSV v tem primeru ni smiselno računati.

Tabela 20: Ocena stroškov

Protiukrep	1	2	3	4	5	Predpostavke
Nameščanje programske opreme na službeni računalnik						
– Izdelava hierarhije vlog – Nameščanje iz Windows Store	6.000 €	-	-	-	-	– Enkraten strošek vzpostavitve
Pogostost posodabljanja operacijskega sistema						
– Avtomatična posodobitev z uporabo »Group Policy«	5.500 €	-	-	-	-	– Enkraten strošek vzpostavitve
Požarni zid						
– Nastavitev Windows Defender pravic – Delavnica za zaposlene	4.400 €	-	-	-	-	– Enkraten strošek vzpostavitve – Delavnica vsako 2. leto
Protivirusni program						
– Nastavitev »Admin approval mode« – Delavnica za zaposlene	1.200 €	-	-	-	-	– Enkraten strošek vzpostavitve – Delavnica vsako 2. leto
Računalnik za dostop do VPN omrežja						
– Vzpostavitev zaščite omrežja NAP – Delavnica za zaposlene	3.800 €	-	-	-	-	– Enkraten strošek vzpostavitve – Delavnica vsako 2. leto

se nadaljuje

Tabela 20: Ocene stroškov (nad.)

Protiukrep	1	2	3	4	5	Predpostavke
Posodabljanje spletnega brskalnika						
- Nastavitev posodobitev z »Group policy« - Brskalnik z uporabo virtualizacije »Browser isolation« - Delavnica	7.500 €	1.200 €	1.200 €	1.200 €	1.200 €	– Enkraten strošek vzpostavitve – Letno vzdrževanje
Deljenje uporabniški podatkov med sodelavci						
Delavnica za zaposlene	Strošek delavnice*	-	-	-	-	Delavnica vsako 2. leto
Pogostost spreminjanja gesel						
Vzpostavitev politike gesel	9.000 €	-	-	-	-	Enkraten strošek vzpostavitve
Enaka gesla med uporabniškimi računi / Št. različnih gesel						
– Vzpostavitev sistema prijave SSO – Delavnica za zaposlene	15.000 €	3.000 €	3.000 €	3.000 €	3.000 €	– Enkraten strošek vzpostavitve – Delavnica vsako 2. leto
Delavnica za zaposlene						
– Priprava in izvedba delavnice o kibernetski varnosti	1.500 €	-	1.250 €	-	1.250 €	Prvo leto strošek priprave, kasneje le strošek izvedbe
Skupaj stroški	53.900 €	4.200 €	5.450 €	4.200	5.450 €	

Vir: lastno delo.

Tabela 21: Ocene koristi

Protiukrep	1	2	3	4	5	Predpostavke
Nameščanje programske opreme na službeni računalnik						
– Izdelava hierarhije vlog – Nameščanje iz Windows Store	10.925 €	10.925 €	10.925 €	10.925 €	10.925 €	RIR = –95 % ARO = 0,5 SLE = 23.000 €
Pogostost posodabljanja operacijskega sistema						
– Avtomatična posodobitev z uporabo »Group Policy«	2.040 €	2.040 €	2.040 €	2.040 €	2.040 €	RIR = –40 % ARO = 0,3 SLE = 17.000 €
Požarni zid						
– Nastavitev Windows Defender pravic – Delavnica za zaposlene	4.375 €	4.375 €	4.375 €	4.375 €	4.375 €	RIR = –70 % ARO = 0,25 SLE = 25.000 €
Protivirusni program						
– Nastavitev »Admin approval mode« – Delavnica za zaposlene	12.600 €	12.600 €	12.600 €	12.600 €	12.600 €	RIR = –90 % ARO = 0,5 SLE = 28.000 €
Računalnik za dostop do VPN-omrežja						
– Vzpostavitev zaščite omrežja NAP – Delavnica za zaposlene	900 €	900 €	900 €	900 €	900 €	RIR = –40 % ARO = 0,15 SLE = 15.000 €
Posodabljanje spletnega brskalnika						
- Nastavitev posodobitev z »Group policy« - Brskalnik z uporabo virtualizacije »Browser isolation« - Delavnica	600 €	600 €	600 €	600 €	600 €	RIR = –30 % ARO = 0,4 SLE = 5.000 €

se nadaljuje

Tabela 21: Ocene koristi (nad.)

Protiukrep	1	2	3	4	5	Predpostavke
Deljenje uporabniški podatkov med sodelavci						
Delavnica za zaposlene	1.920 €	1.920 €	1.920 €	1.920 €	1.920 €	RIR = –80 % ARO = 0,2 SLE = 12.000 €
Pogostost spreminjanja gesel						
Vzpostavitev politike gesel	3.375 €	3.375 €	3.375 €	3.375 €	3.375 €	RIR = –50 % ARO = 0,15 SLE = 45.000 €
Enaka gesla med uporabniškimi računi / Št. različnih gesel						
– Vzpostavitev sistema prijave SSO – Delavnica za zaposlene	4.050 €	4.050 €	4.050 €	4.050 €	4.050 €	RIR = –60 % ARO = 0,15 SLE = 45.000 €
Skupaj koristi	40.785 €	40.785 €	40.785 €	40.785 €	40.785 €	
Skupaj stroški/koristi	**–13.115 €**	**36.585 €**	**35.335 €**	**36.585 €**	**35.335 €**	

Vir: lastno delo.

SKLEP

Namen magistrskega dela je bil raziskati kibernetsko varnost izbranega podjetja in na podlagi ugotovitev pripraviti seznam protiukrepov oz. izboljšav.

V prvem delu naloge sem s pregledom literature opisal proces upravljanja kibernetske varnosti in tveganja v podjetjih. Kot eno izmed možnih rešitev za pomoč pri usmeritvah upravljanja kibernetske varnosti sem opisal delovno ogrodje NIST. Drugo poglavje predstavlja jedro magistrskega dela – analizo kibernetske varnosti v izbranem podjetju. Analiza je razdeljena na dva dela: na analizo ozaveščenosti zaposlenih o kibernetski varnosti in analizo VPN-omrežja podjetja. V prvem delu analize sem s pomočjo anketnega vprašalnika želel ugotoviti ozaveščenost zaposlenih za tri glavna področja: varno uporabo računalnika, varnost na spletu in upravljanje uporabniških podatkov. V analizi ozaveščenosti sem ugotovil, da so ocene posameznih področij glede na postavljene kriterije naslednje:

– varna uporabe računalnika: sprejemljivo (57 %),
– varnost na spletu: dobro (71 %),
– upravljanje uporabniških podatkov: nezadovoljivo (45 %).

Za ugotovljene potencialne ranljivosti sem izdelal seznam predlogov protiukrepov, ki jih podjetje lahko uvede za zmanjšanje tveganja kibernetske varnosti. V drugem delu analize sem ocenil tveganje za odkrite ranljivosti VPN-omrežja ter predlagane protiukrepe iz prvega dela apliciral kot protiukrepe za odkrite ranljivosti VPN-omrežja. V tretjem poglavju sem za predlagane protiukrepe s pomočjo IT-službe podjetja opravil oceno koristi in stroškov za obdobje petih let, s čimer sem želel ugotoviti, ali so ti finančno upravičeni. Kot glavno omejitev analize bi izpostavil, da ocene ne temeljijo na historičnih podatkih, ampak na subjektivni oceni in izkušnjah zaposlenih. Analiza je pokazala, da je uvedba na podlagi razmerja ocenjenih stroškov/koristi smiselna. Prvo leto bo podjetje imelo izgubo v višini –13.115 €, vsa naslednja leta pa koristi presegajo stroške.

Za ranljivosti odkrite v analizi ozaveščenosti kibernetske varnosti, bi podjetju svetoval vrstni red uvedbe predlaganih protiukrepov glede na dosežen rezultat (od najnižje do najvišje ocene) in zahtevnost izvedbe (od manj zahtevne do najbolj zahtevne). Pri analizi omrežja VPN pa bi podjetju svetoval pričetek izvedbe protiukrepov glede na višino ocenjenega tveganja. Za ranljivosti kjer je bilo odkrito visoko tveganje, se protiukrepi uvedejo takoj. Nato nadaljevati z ranljivostimi, ki imajo srednje in nizko tveganje.

Pred uvedbo predlaganih ukrepov bi podjetju svetoval pregled integriranosti delovnega ogrodja. S tem bi pridobili vpogled v trenutno stanje kibernetske varnosti, ki je nato v pomoč za določitev ciljev kibernetske varnosti. Kljub temu da sem ugotovil, da so predlagani ukrepi iz analize smiselni za uvedbo, je za izvedbo kibernetske varnosti potreben celovit pristop. V nasprotnem primeru je uvedba predlaganih varnostnih ukrepov

le vpeljava »obližev« na mesta, kjer so pomanjkljivosti najbolj očitne. Korak v pravo smer bi za podjetje bil tudi skladnost z informacijskim varnostnim standardom. Na ta način bi zagotovili celovit pristop in integriranost informacijske varnosti v vse delovne procese podjetja. Skladnost z informacijskovarnostnimi standardi po mojem mnenju dobiva vedno večji pomen in bo v prihodnosti predstavljala enega izmed temeljev za poslovanje.

LITERATURA IN VIRI

1. Bada, M., Sasse, A. & Nurse, J. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society (str. 118-131). London, UK: Researchgate.
2. Bansode, R. & Girdhar, A. (2021). Common Vulnerabilities Exposed in VPN – A Survey. Journal of Physics: Conference Series, 8.
3. Bounev, S. & Olive, C. (marec 2021). NIST Password Guidelines 2021 - Challenging Traditional Password Management. Pridobljeno aprila 2021 iz Security Boulevard: https://securityboulevard.com/2021/03/nist-password-guidelines-2021-challenging-traditional-password-management/
4. Chapple, M. & Seidl, D. (2017). Cybersecurity Analyst CSA+. Canada: Sybex.
5. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. & Stoddart, K. (2016). A Review of Cybersecurity Risk Assessment Methods for SCADA Systems. Computers & Security, 56, 1-27.
6. Cisternelli, E. (2021). 7 cybersecurity frameworks that help reduce cyber risk. Infosecurity Magazine. Pridobljeno marca 2021 iz https://www.infosecurity-magazine.com/opinions/most-influential-frameworks-1-1-1/
7. CVE. (2021). About CVE Records. Pridobljeno maja 2021 iz http://cve.mitre.org/cve/identifiers
8. Donaldson, S. E., Siegel, S. G., Williams, C. K. & Aslam, A. (2015). Enterprise Cybersecurity - How to Build a Successful Cyberdefense Program Against Advanced Threats. New York, ZDA: Apress.
9. Douglas, L. (2011). The Security Risk Assesment Handbook. Boca Raton, ZDA: CRC Press.
10. Elmontsri, M. (2013). Review of the strengths and weaknesses of risk matrices. Journal of Risk Analysis and Crisis Response, 4(1), 57.
11. ENSIA. (2012, 12. december). Introduction to return on security investment. Pridobljeno decembra 2021 iz https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.
12. Gromenko, D. (2018). Corporate Security in the EU and GDPR: Data breaches in British Airways and The Marriot International. Praga: University of Economics.
13. Hutchins, G. (2019). Accendor Reliability. ISO 31000 Princeiples Risk Managment. Pridobljeno maja 2021 iz https://accendoreliability.com/iso-31000-principles-risk-management/
14. Irwin, L. (2021). IT Governance. ISO 27001 vs. ISO 27002: What's the difference? Pridobljeni januarja 2022 iz https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002
15. ISACA. (2014). Implementing the NIST Cybersecurity Framework. Rolling Meadows, IL, ZDA: ISACA.
16. ISO/IEC. (2017). IT asset management. Pridobljeno aprila 2021 iz https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en

17. IT Governance Ltd. (2022). SOC System and Organization Controls 2 Audits. Pridobljeno marca 2021 iz https://www.itgovernance.co.uk/soc-reporting
18. Jereb, B. (2014). Upravljanje tveganj. Celje: Univerza v Mariboru - Fakulteta za logistiko.
19. Johnson, J. (2022). Statista. Average duration of downtime after a ransomware attack from 1st quarter 2020 to 3rd quarter 2021. Pridobljeno februrarja 2022 iz https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/
20. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget. Pridobljeno maja 2022 iz https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
21. Khandelwal, S. (2016, 13. januar). Fortinet Firewall Password Hack. Hacker news. Pridobljeno maja 2022 iz https://thehackernews.com/2016/01/fortinet-firewall-password-hack.html
22. Kohnke, A., Shoemaker, D. & Sigler, K. (2016). The Complete Guide to Cybersecurity Risk and Controls. Boca Raton, Florida: CRC Press.
23. Loomans, A. (2000). Qualitative scales for likelihood. Researchgate. Pridobljeno aprila 2021 iz https://www.researchgate.net/figure/Qualitative-scales-for-likelihood-a-magnitude-b-and-level-of-risk-of-adverse_tbl1_40797508
24. Maritime Cybersecurity. (2015). Cybersecurity Risk Analysis. Pridobljeno aprila 2021 iz https://erawat.es/en/vessel-cybersecurity-risk-analysis
25. Meyer, W. (2015). Quantifying Risk - Measuring the Invisible. PMI Global Congress 2015 – EMEA. London: Project Management Institute.
26. Moschovitis, C. (2018). Cybersecurity Premier. V C. Moschovitis (ur.), Cybersecurity Program Development for Business (str. 15-19). New Jersey, ZDA: Wiley.
27. Mujeeb, A. (2019). Importance of information security [objava na blogu]. Pridobljeno aprila 2021 iz https://www.infosecacademy.io/blog/importance-of-information-security/
28. Muncaster, P. (brez datuma). Ransomware Payments Hit Record Highs in 2021. Infosecurity Magazine. Pridobljeno marca 2022 iz https://www.infosecurity-magazine.com/news/ransomware-payments-hit-record/
29. NIST. (2018 a). Framework Components. Pridobljeno aprila 2021 iz NIST.gov: https://www.nist.gov/cyberframework/online-learning/components-framework
30. NIST. (2018, 16. april b). Framework for Improving Critical Cybersecurity Infrastructure. Pridobljeno aprila 2021 iz https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
31. NIST. (2018 c). Informative References. Pridobljeno aprila 2021 iz https://www.nist.gov/cyberframework/online-learning/informative-references
32. NIST. (2019). Supplemental Material for NIST Privacy Framework Workshop. Pridobljeno aprila 2021 iz https://www.nist.gov/system/files/documents/2019/07/03/pf-proposed-separated-core-06.26.2019.pdf
33. NIST. (2020). Industry impacts - Cybersecurity framework. Pridobljeno januarja 2021 iz https://www.nist.gov/industry-impacts/cybersecurity-framework
34. NIST. (2021). HIPPA Security Rule. Pridobljeno marca 2021 iz https://www.nist.gov/programs-projects/security-health-information-technology/hipaa-security-rule
35. Panchit, P. (2006). Quantified Return on Information Security Investment. Delft: Department of Technology, Delft University.

36. Pettey, C. (2020). Gartner. Gartner Top 9 Security and Risk Trends for 2020. Pridobljeno maja 2021 iz https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/
37. Ramona, S. E. (2011). Advantages and Disadvantages of Quantitative and Qualitative Approach. Chinese Business Review, 10(december), 1110.
38. Refsdal, A., Solhaug, B. & Stølen, K. (2015). Cyber-Risk Managment. New York: Springer.
39. Rotman, D. (2020). We are not prepared for the end of the Moores law. Technologyreview. Pridobljeno januarja 2021 iz https://www.technologyreview.com /2020/02/24/905789/were-not-prepared-for-the-end-of-moores-la
40. Stoneburner, G., Goguen, A. & Feringa, A. (2008). Risk Management Guide for Information Technology Systems. Pridobljeno feberuarja 2021 iz ttps://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/sp800-30.pdf
41. Sumner, M. (2009). Information Security Threats - A Comparative Analysis of Impact, Probability, and Prepardness. Information Systems Management, 26(1), 94.
42. Trenton, B. (2021). Employee Security Awarness Survey. Pridobljeno decembra 2021 iz https://devlegalsimpli.blob.core.windows.net/pdfseoforms/pdf-20180219t134432z-001/pdf/employee-security-awareness-survey.pdf
43. Van Impe, K. (2017). Security Intelligence. Simplify Risk Managment. Pridobljeno maja 2021 iz https://securityintelligence.com/simplifying-risk-management/
44. Weishäup, E., Yasasin, E. & Schryen, G. (2018). Information Security Investments - An Exploratory Multiple Case Study. Computer and Security, 77, 807-823.
45. Widup, S., Pinto, A., Hylender, D., Bassett, G. & langlois, P. (2021). Verizon Data Breach Invetigation Report - 2021. Neznan kraj, ZDA: Verizon.
46. Yildirim, E. (2017). The Importance of Risk Managment in Information Security. International Journal of Advances in Electronics and Computer Science, 4(1), 18-21.

PRILOGE

Priloga 1: Anketni vprašalnik

OZAVEŠČENOST ZAPOSLENIH O KIBERNETSKI VARNOSTI

Anketni vprašalnik

Pred vami se nahaja anonimni vprašalnik, namenjen raziskavi prakticiranja kibernetske varnosti zaposlenih. Vsa vprašanja se nanašajo na kibernetsko varnost programske opreme ter uporabniške račune in prakse, ki jih uporabljate znotraj vašega podjetja. Pri vsakem vprašanju je možen le 1 odgovor.

VARNA UPORABA RAČUNALNIKA

1. Ali v sporočilu elektronski pošte preverite pošiljatelja (elektronski naslov) pred klikom na povezavo ali odpiranjem priponke?

- Da.
- Ne.

2. Ali ste že kdaj sami namestili programsko opremo s spleta na vaš delovni računalnik?

- Da.
- Ne.

3. Kako pogosto posodabljate operacijski sistem vašega delovnega računalnika?

- Redno spremljam posodobitve in jih nameščam.
- Posodobitve namestim, kadar me računalnik o njih obvesti.
- Posodobitve po navadi preskočim, poženem jih kasneje.
- Posodobitve imam izklopljene.

4. Ali imate na vašem računalniku vklopljen požarni zid?

- Da.
- Ne.
- Ne vem.

5. Ali imate na vašem računalniku nastavljen protivirusni program?

- Da.
- Da, vendar imam izklopljene posodobitve.
- Da, vendar je izklopljen.
- Ne vem.

6. Ali imate za uporabo vašega računalnika nastavljeno geslo?

- Da.
- Ne.

7. Ali ste že kdaj uporabili računalnik, ki ni služben, za dostop do VPN-omrežja podjetja?

- Da.
- Ne .

VARNOST NA SPLETU

1. Ali ste pri obisku spletnih strani pozorni na spletni naslov (domeno)?

- Da.
- Ne.

2. Ste pri vnosu uporabniških podatkov na spletni strani pozorni na HTTPS »varno povezavo«?

- Da.
- Ne.

3. Kako pogosto posodabljate vaš spletni brskalnik?

- Redno spremljam posodobitve in jih nameščam.
- Posodobitvam ne posvečam velike pozornosti.
- Posodobitve po navadi preskočim, poženem jih kasneje.
- Posodobitve namestim samo, kadar me brskalnik o njih obvesti.

4. Ste v vaš brskalnik že kdaj namestili nezaželene oglase AdWare?

AdWare je nezaželena programska oprema (po navadi znotraj brskalnika), ki med vašim delom odpira nezaželena pojavna okna z oglasi in spremeni nastavitve brskalnika (primer: namesto iskalnika Google se vam pojavlja nepoznan iskalnik, ki ga niste nastavili).

- Da.
- Ne.
- Ne vem.

UPRAVLJANJE GESEL

1. Kje najraje shranjujete vaše uporabniške podatke?

- Si jih zapomnim.
- Blok z zapiski, da so vedno pri roki.
- Uporabljam orodje za upravljanje gesel.
- V datoteki na računalniku.
- Drugo: _____.

2. Ali ste vaše uporabniške podatke že kdaj zaupali sodelavcu?

- Da.
- Ne.

3. Ali ste vaše uporabniške podatke kdaj zaupali nekomu, ki ni vaš sodelavec?

- Da.
- Ne.

4. Kako pogosto spreminjate vaša gesla?

- Na 7–14 dni.
- Na tri mesece.
- Na pol leta.
- Enkrat na leto.
- Nikoli.

5. Ali uporabljate enaka gesla med različnimi uporabniškimi računi?

- Da.
- Ne.

6. Koliko različnih gesel uporabljate za uporabniške račune?

- 1–5.
- 6–10.
- 11–15.
- 16–20.
- Vsak uporabniški račun ima svoje geslo.

7. Ali je bil vaš uporabniški račun že kdaj tarča vdora?

- Da.
- Ne.