UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

ZAGOTAVLANJE KIBERNETSKE VARNOSTI V IZBRANEM PODJETJU

Ljubljana, avgust 2021 TILEN KRIŽANIČ

IZJAVA O AVTORSTVU

Podpisani Tilen Križanič, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Zagotavljanje kibernetske varnosti v izbranem podjetju, pripravljenega v sodelovanju s svetovalcem doc. dr. Luko Tomatom

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 preko 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

SEZNAM KRATIC

angl. – angleško
DDoS – (angl. Distributed denial-of-service); napad za zavrnitev storitev
GDPR – (angl. The General Data Protection Regulation); Splošno uredbo Evropske unije o varstvu podatkov
ID – (angl. Identity document); osebni dokument
IP naslov – (angl. Internet Protocol address); določa sistemski položaj računalnika v omrežju
ISMS – (angl. Information Security Management System); sistem za upravljanja informacijske varnosti
ISO – (angl. International Organization for Standardization); Mednarodna organizacija za standardizacijo
RBAC – (angl. Role-Based Access Control); Nadzor dostopa na podlagi vlog
SHA-1 – (angl. Secure Hash Algorithm 1); algoritem varnostne razpršitve
SQL – (angl. Structured Query Language); strukturirani povpraševalni jezik za delo s podatkovnimi bazami

SUVI – sistem za upravljanje varovanja informacij
USB – (angl. Universal Serial Bus); Univerzalno serijsko vodilo
Wi-Fi – (angl. Wireless networking technology); brezžična tehnologija, ki omogoča, da se lahko naprava poveže v računalniško omrežje
ZDA – Združene države Amerike
ZVOP – Zakon o varstvu osebnih podatkov

UVOD

Varnost na spletu predstavlja čedalje večji problem tako za podjetja kot tudi za posameznike. Upravljanje je vedno zahtevnejše, a tudi učinkovitejše, napadi pa so vse pogostejši. Gre za sodoben kriminal, ki se ukvarja z uničevanjem in zlorabo podatkov, ki so tajne narave in pomembni za podjetja in posameznike. Diplomska naloga se osredotoča na informacijsko varnost, ki jo lahko z drugimi besedami imenujemo kibernetska varnost.

To področje je pomembno zaradi vse pogostejših napadov in zlorabe podatkov, ki povzročijo ogromno škode in razkrijejo tajne podatke, s katerimi lahko napadalci zaslužijo.

Za podjetja in posameznike je smiselno, da so kibernetsko varni, saj bodo na ta način zaščiteni pred digitalnimi napadi. Napadi ogrožajo sisteme, omrežja, naprave in programe, ki tvorijo skupino, ta pa predstavlja velik oblak podatkov in informaciji.

Namen naloge je opredeliti kibernetsko varnost ter predstaviti sistem za upravljanje varovanja informacij. Poleg tega v nalogi predstavljam ISO standarde ter njihov pomen za podjetja, s pomočjo intervjuja z ustreznim zaposlenim v izbranem podjetju pa predstavim, kako v podjetju zagotavljajo kibernetsko varnost.

Metodologija naloge temelji na analizi znanstvene in strokovne literature ter internetnih virov, na podlagi katerih v teoretičnem delu opredelim in predstavim kibernetsko varnost ter njen pomen za podjetja, nato pa v empiričnem delu s pomočjo intervjuja predstavim, v kolikšni meri kibernetsko varnost zagotavljajo v izbranem podjetju.

Delo je razdeljeno na pet tematskih poglavij. V prvem poglavju predstavim, kaj je kibernetska varnost, kakšne kibernetske grožnje poznamo ter kakšna so tveganja za podjetje. Drugo poglavje opisuje upravljanje informacij ter se deli na podpoglavja: Varnost podatkov za podjetja in zaposlene, Požarni zid in Sistemi za upravljanje varovanja informacij. Tretje poglavje opredeljuje standarde ISO 27000, četrto poglavje opisuje zagotavljanje kibernetske varnosti v izbranem podjetju, peto poglavje pa vključuje intervju, izveden v izbranem podjetju. V šestem poglavju povzemam ključne ugotovitve intervjuja.

1 KIBERNETSKA VARNOST

Kibernetska varnost je praksa zaščite sistemov, omrežij in programov pred digitalnimi napadi. Slednji so navadno namenjeni spreminjanju ali uničevanju občutljivih informacij, za primer lahko izpostavimo izsiljevanje uporabnikov za denar ali prekinitev običajnih poslovnih procesov. Vzpostavitev kibernetske varnosti je v današnjih časih z ozirom na dejstvo, da je na svetu več naprav kot ljudi, posebej učinkovit ukrep proti takšnim napadalcem, je pa tudi izziv, saj postajajo napadalci vse bolj inovativni in iznajdljivi (Cisco Systems, 2021).

Kibernetsko varovanje se uporablja v različnih kontekstih poslovnega in mobilnega računalništva, ki ga lahko razdelimo v naslednje kategorije (AO Kaspersky Lab, 2021):

- Omrežna varnost je zaščita računalniškega omrežja pred napadalci ali priložnostno programsko opremo.
- Varnost aplikacij je usmerjena v zaščito programske opreme in naprav pred grožnjami. Ogrožena aplikacija lahko napadalcu zagotovi dostop do podatkov, zato je uspešno zaščito potrebno načrtovati pred uvedbo novega programa ali naprave.
- Med prenosom in shranjevanjem podatkov pomaga zaščita informacijskih sistemov, saj varuje integriteto in zasebne podatke.
- Za vključevanje procesov in odločitve za obdelavo in zaščito podatkovnih sredstev je ključna operativna varnost. Dovoljenja, ki jih uporabniki imajo za dostopanje do omrežij, in navodila, ki določajo, kako in kje se podatki shranijo, spadajo med operativno varnost.
- Obnovitev ob nesrečah in neprekinjeno poslovanje določata, kako se organizacija odzove na incident kibernetske varnosti ali katerikoli drugi dogodek, ki povzroči izgubo poslovanja ali podatkov. Politike obnove po katastrofi narekujejo, kako organizacija obnovi svoje delovanje in informacije, da se vrne v enako operativno zmogljivost, kot jo je imela pred dogodkom. Neprekinjenost poslovanja pomeni, da organizacija še naprej deluje brez določenih virov, dokler se ne vrne na normalo.
- Izobraževanje končnih uporabnikov je nepredvidljiv dejavnik kibernetske varnosti. Vsakdo lahko nenamerno vnese virus v sicer varen sistem, v kolikor ne upošteva dobrih varnostnih praks. V kolikor si želijo organizacije zagotoviti varnost, morajo izobraziti uporabnike na področju ustrezne rabe računalniške opreme, orodij …(izogibanje rabe neznanih USB pogonov, brisanje sumljivih e-sporočil …).

1.1 Vrste kibernetskih groženj

Kibernetske grožnje se nenehno povečujejo. V prvih desetih mesecih leta 2019 je bilo zabeleženih 5183 kršitev s 7,9 milijarde evidentiranih zapisov. V primerjavi s sredino leta 2018 se je skupno število kršitev povečalo za 33 %, skupno število razkritih evidenc pa se je podvojilo, saj se je povečalo kar za 112 %. Ko se poglobimo v podatke, ugotovimo, da med incidenti po pogostosti najbolj izstopajo vdori (RiskBesed security, 2019).

Največ groženj in kršitev doživljajo trgovci na drobno, zdravstvene službe in javni subjekti, ki so tarča kriminalcev. Nekateri od teh so še bolj izpostavljeni, saj v svojih bazah beležijo tajne in zaupne podatke, kot so na primer finančni in zdravstveni podatki, ogrožena pa so tudi vsa podjetja, ki uporabljajo omrežja in beležijo podatke o strankah. Posledično prihaja do vohunjena podjetji in napadov na stranke, zaradi česar se je v ZDA Nacionalni inštitut za standarde in tehnologijo odločil za neprekinjeno sprotno spremljanje vseh elektronskih virov (AO Kaspersky Lab, 2021).

Grožnje, ki jih preprečuje kibernetska varnost, lahko razdelimo na tri nivoje (AO Kaspersky Lab, 2021):

- Kibernetski kriminal: ta vključuje skupine ali posameznike, ki ciljajo na sisteme, povezane s finančno koristijo, ali pa povzročajo motnje sistemov.
- Kibernetski napadi: ti so politično naravnani in vključujejo in vključujejo zbiranje političnih informacij.
- Kibernetski terorizem: cilja na elektronske sisteme in s tem povzroči paniko in strah.

Zlonamerna programska oprema je izraz za viruse, črve, trojanske konje in druge škodljive programe, ki jih hekerji uporabljajo za dostop in uničevanje občutljivih informacij. Izraz zlonamerna programska oprema se nanaša na katerokoli programsko opremo, namenjeno povzročanju škode na računalniku, strežniku ali računalniškem omrežju. Razliko med zlonamerno programsko opremo in virusom lahko pojasnimo z dejstvom, da je virus res vrsta zlonamerne programske opreme, vendar ni vsak zlonameren program obenem tudi virus (IDG Communications, Inc, 2019).

Vrste zlonamerne programske opreme, ki okužijo ciljne računalnike, so naslednje:

- Črv: samostojni del zlonamerne programske opreme, ki se sam širi z računalniškimi programi ali dokumenti ter omrežji od računalnika do računalnika. Črvi so nevarni zaradi načina širjenja, saj se lahko širijo po omrežju brez kakršnekoli pomoči ali ukrepov. Svoje delo opravljajo tako, da izkoriščajo ranljivost v operacijskem sistemu računalnika. Poznamo več kategorij širjenja črvov: e-poštni črvi, črvi za takojšne poročanje, črvi za skupno rabo datotek in internetni črvi (Avast Software, 2020).
- Trojanski konj: vrsta zlonamerne programske opreme ali kode, ki je videti v skladu s splošno veljavnimi pravicami, vendar lahko prevzame nadzor nad računalnikom. Zasnovan je tako, da poškoduje, krade, moti ali povzroči kakšno drugo dejanje na podatkih v računalniku ali omrežju. Za delovanje trojanskega konja je potreben zagon trojanskega programa, ki se po pomoti zažene. Ko se program zažene, se zlonamerna programska oprema razširi na druge datoteke in tako poškoduje računalnik (NortonLifeLock, 2020).
- Izsiljevalska programska oprema: zlonamerna programska oprema, ki zaklene uporabnikove datoteke in podatke z grožnjo izbrisa vseh podatkov oziroma ponudi rešitev težav ob izplačilu odkupnine (AO Kaspersky Lab, 2021).
- Oglaševalni program: oglaševalska programska oprema, ki se lahko uporablja za širjenje zlonamerne programske opreme (AO Kaspersky Lab, 2021).
- Botneti: omrežja računalnikov, ki so okužena z zlonamerno programsko opremo in jih kriminalci uporabljajo za izvajanje spletnih nalog brez dovoljenja uporabnika (AO Kaspersky Lab, 2021).
- Injekcija SQL (poizvedba strukturiranega jezika) je vrsta kibernetskega napada, ki se uporablja za prevzem nadzora in krajo podatkov iz baze podatkov. Kriminalci izkoriščajo ranljivosti v podatkovno vodenih aplikacijah tako, da zlonamerno kodo vstavijo v zbirko podatkov z zlonamernim stavkom SQL. To jim omogoča dostop do občutljivih informacij, ki jih vsebuje baza podatkov (AO Kaspersky Lab, 2021).
- Lažno predstavljanje: o njem govorimo, ko kriminalci ciljajo na žrtve z e-pošto, za katero

se zdi, da prihaja s strani zakonitega podjetja, ki zahteva občutljive podatke. Napadi z lažnim predstavljanjem se pogosto uporabljajo za prevaro ljudi pri predaji podatkov o kreditnih karticah in drugih osebnih podatkov (AO Kaspersky Lab, 2021).
- Napad »človek v sredini« je vrsta kibernetske grožnje, pri kateri kriminalec prestreže komunikacijo med dvema posameznikoma, da bi ukradel podatke. V nezaščitenem omrežju Wi-Fi, na primer, lahko napadalec prestreže podatke, ki jih posredujejo napadene naprave preko omrežje (AO Kaspersky Lab, 2021).
- Do napada zaradi zavrnitve storitve prihaja, ko kriminalci računalniškemu sistemu preprečijo izpolnjevanje zakonitih zahtev na takšen način, da omrežja in strežnike preobremenijo s prometom. Zaradi tega je sistem neuporaben in organizaciji preprečuje izvajanje vitalnih funkcij (AO Kaspersky Lab, 2021).

1.2 Zanimivi dogodki kibernetskih napadov

Poglavje opisuje zanimive kibernetske napade, ki so se zgodili velikim znanim podjetjem po svetu. Opisuje napade, ki so jih napadalci povzročili, ter škodo, ki je nastala. Poleg tega pojasnjuje še, kaj so podjetja dolgovala uporabnikom, ki so bili oškodovani.

Adobe. V oktobru leta 2013 je Adobe poročal, da so hekerji ukradli skoraj 3 milijone šifriranih evidenc kreditnih kartic strank in podatke o prijavi za nedoločeno število uporabniških računov. Adobe je kasneje to oceno še zvišal, saj so številke zrasle na kar 38 milijonov ID-jev aktivnih uporabnikov. Raziskave so pokazale, da so bila razkrita imena strank, osebne izkaznice, gesla in podatki bančnih kartic (Finkle, 2013).

LinkedIn. Kot eno izmed glavnih omrežji za poslovneže je tudi LinkedIn postal privlačna tarča napadalcev, katerih cilj je izvajanje napadov socialnega inženiringa. Družba je leta 2012 objavila informacijo, da so napadalci ukradli 6,5 milijona gesel in jih objavili na ruskem hekerskem forumu. Nekaj let kasneje ja bil razkrit celoten obseg napada: heker, ki je prodajal podatke MySpaceu, je obenem ponujal podatke približno 165 milijonov uporabnikov LinkedIna. Takrat je šlo za vrednost 5 bitcoinov, kar je pomenilo približno 2000 dolarjev. LinkedIn je takrat priznal kršitev in ponastavil vsa gesla prizadetih računov (IDG Communications, Inc, 2021).

Yahoo. Družba Yahoo je poročala, da je bila leta 2016 žrtev enega izmed največjih napadov v zgodovini, povezanega s kršitvijo podatkov. Napadalci so ogrozili prava imena, e-poštne naslove in telefonske številke 500 milijonov uporabnikov. Po mnenju Yahooja je večina ogroženih gesel razpršena. Za to kršitev je moral Yahoo odšteti približno 350 milijonov dolarjev (MIT Technology Review, 2016).

My Fitness Pal. Fitnes aplikacija MyFitnessPal je bila v lasti UnderArmorja. Med množičnimi odlagališči informacij je bilo ogroženih 16 spletnih strani, na katerih je bilo približno 617 milijonov računov strank, ki so bili ponujeni v prodajo na Dream Marketu. Leta 2018 so bila ukradena uporabniška imena, e-naslovi, naslovi IP, SHA-1 in gesla z

razprtošifriranim okrožjem. Ta gesla so potem bila prodana leto pozneje tako kot Dubsmash in drugi. MyFitnessPal je priznal kršitev in od uporabnikov zahteval, naj si spremenijo gesla. Podatka, koliko računov je bilo prizadetih in kako so napadalci dobili dostop, pa niso razkrili (IDG Communications, Inccso, 2021).

1.3 Kibernetska tveganja za podjetje

Kibernetski napadi so vse pogostejši, zato podjetja vedno bolj skrbi za svojo informacijsko varnost. Ogroženost pred napadi je velika skrb evropskih in drugih držav. Z enim samim klikom lahko napadalci odstranijo celotna spletna mesta ali ukradejo občutljive podatke, zato je pomembno, da so podjetja proaktivna pri razumevanju tveganja kibernetske varnosti in se tudi primerno zaščitijo (AO Kaspersky Lab, 2021).

Največja kibernetska tveganja za podjetja so:

- Socialni inženiring je manipulacijska tehnika, ki temelji predvsem na izkoriščanju človekovih napak, kadar gre za pridobivanje zasebnih informacij, dostopa ali dragocenosti. Napadi se po navadi zgodijo na spletu, osebno ali preko drugih interakcij. Napadalci izkoristijo razmišljanje in delovanje ljudi, tako da z njimi manipulirajo in iz njih izvlečejo kakšno koristno informacijo. Napadalci navadno s takimi ljudmi manipulirajo in iz njih izvlečejo kakšno koristno informacijo. Poleg neznanja uporabnikov se mnogi tudi ne zavedajo groženj, kot so prenosi s pogonom. Napadalčev cilj je poškodovanje in motenje podatkov, zaradi katerih nastanejo škoda ali številne nevšečnosti. Poleg sabotaže podatkov pa pride tudi do kraje in pridobivanja dragocenosti, kot so informacije, dostopi in denar (AO Kaspersky Lab, 2021).
- Management popravkov: gre za nadgradnjo programske opreme, ki je kot del kode prilagojena odpravljanju napak ali dodajanju novih funkcij v aplikaciji. Upravljanje popravkov je postopek upravljanja omrežja računalnikov z rednim izvajanjem popravkov za posodobitev računalnikov. Ta način pomaga pri zmanjšanju okvar, povezanih s sistemom, zaradi česar pride do izboljšanja produktivnosti in prihranka pri stroških, povezanih s slabim upravljanjem popravkov. Napadalci navadno radi iščejo zastarelo programsko opremo, ki ni dokončno posodobljena, in jo napadejo. Podjetja zaradi strahu pred ogroženostjo prav zaradi tega stremijo k takojšnji posodobitvi (ManageEnginePatch Management Plus, brez datuma).
- Izsiljevalska programska oprema je razvijajoča se oblika zlonamerne programske opreme, namenjane šifriranju datotek v napravi, zaradi česar so vse datoteke in sistemi, ki se nanje opirajo, neuporabni. Napadalci zahtevajo kasneje odkupnino v zameno za dešifriranje. V kolikor žrtev odkupnine ne poravna, napadalci grozijo s prodajo ali širjenjem podatkov oziroma informacij, pomembnih za podjetja. Takšni napadi so že marsikatero podjetje pripeljali do prenehanja poslovanja (Stop Ransomware, brez datuma).
- Internet stvari sestavlja omrežje fizičnih predmetov, vgrajenih s programsko opremo,

senzorji in druga tehnologija, potrebna za izmenjavo in povezovanje podatkov s tretjo napravo preko internetnega sistema. Napadalci to izkoriščajo tako, da šibko varnost naprav izkoristi v botnet, ki se potem uporablja za napad v druge naprave. Preko interneta napadalec vstopi v napravo in izsledi geslo. To geslo napiše v svoj botnet, ta pa mu potem pomaga pri napadih na druge naprave (Reuters graphics, brez datuma).

2 UPRAVLJANJE VAROVANJA INFORMACIJ

2.1 Varnost podatkov za podjetja

Varstvo podatkov je ukrep, ki preprečuje nepooblaščen dostop do podatkovnih baz, računalnikov in spletnih mest. V podjetju pomeni varnost pomemben člen, ki ga, v izogib kakršnekoli kršitve slednje, ne gre spregledati. Da bi bili varnejši pred kibernetskimi napadi, mora biti oprema ustrezno zaščitena. Zaščitimo jo lahko na več načinov (Traveles, brez datuma a):

- Varovanje delovnega prostora in opreme: Gotovo je za varovanje delovnega prostora in opreme potreben odgovoren odnos. Občutljivi podatki morajo biti ločeni od drugih in shranjeni na varnih mestih. Pozorni moramo biti tudi na okolico. Vsak umik od računalnika zahteva od uporabnika njegovo zaklepanje, ponovno ga pa zaženemo šele z ustreznim geslom. Pri slednjem mora biti uporabnik posebno pozoren, saj lahko pomeni shranjevanje gesel v lastne naprave veliko grožnjo in ob neustrezni varnosti vabo za napadalce.
- Raba e-sporočil: Uporaba e-sporočil zahteva od uporabnikov precejšno previdnost. Marsikatera e-sporočila so ponarejena, z njimi pa lahko napadalci dostopajo do žrtev in uporabljajo podatke kreditne kartice in njihovo osebno identiteto in identitete ali pridobivajo nadzor nad računalnikom in omrežjem. Pri tem prihaja do kraj gesel in dostopa do informaciji o podjetju. Sumljiva e-poštna sporočila je potrebno prijaviti svojim informatikom ali pa jih preprosto izbrisati.
- Metoda izbire gesla: Z metodo uporabe daljših gesel in z rednim spreminjanjem le-teh se napadalcem otežuje dostop do informacij. Geslo mora biti zaupno, z drugimi osebami ga ne delimo. Varno geslo ne vključuje osebnega lastnega imena ali ID-ja, na drugi strani pa mora vsebovati najmanj sedem znakov, med katerimi so številke, simboli, male in velike črke.

2.2 Varnost podatkov za zaposlene

Prepoznavanje kibernetskih groženj je za podjetja zelo pomembno, saj to pripomore k računalniški varnosti podjetja. Poznavanje kibernetske varnosti in informacijske tehnologije je izjemno pomembno, ker se s tem uči razumeti ranljivost in grožnje za poslovanje. Seveda je pomembno tudi zavedanje o odgovornosti zaposlenih pri uporabi računalnika v

poslovnem omrežju. Zaposlene je potrebno ustrezno usposobiti na področju kibernetske varnosti, saj se je na ta način mogoče izogniti, prepoznati ali sporočiti grožnjo ustreznemu oddelku v podjetju. Veliko grožnjo predstavlja človeška napaka, ta pa je glavni razlog za kibernetsko usposabljanje (Sloan, 2021).

Na računalnik podjetja zaposleni nepooblaščene programske opreme ne smejo nameščati. Prenos nepooblaščene programske opreme lahko namreč povzroči izpostavljenost podjetja napadu z zlonamerno programsko opremo, ki lahko poškoduje njegove podatke (Traveles, brez datuma b).

Tudi uporaba interneta zahteva od zaposlenih odgovorno ravnanje, pozorni morajo biti na morebitne prevare. Sumljive povezave lahko na primer sprostijo zlonamerno programsko opremo, ukradejo podatke podjetja in okužijo računalnik. V izogib temu podjetja navadno določijo pravila in omejitve glede uporabe interneta zaposlenih na delovnem mestu (Zoe, 2020)

2.3 Požarni zid

Požarni zdi je programska oprema, ki preprečuje nepooblaščen dostop do omrežja in spremlja dohodni in odhodni promet z uporabo nabora pravil za prepoznavanje in blokiranje groženj.

Uporaba požarnih zidov pride v poštev v osebnih in poslovnih nastavitvah. Požarni zidovi so sestavni del omrežne varnosti. Pomembni so, saj vplivajo na sodobne varnostne tehnike in so še vedno v uporabi. Začeli so jih uporabljati v prvih dveh letih po vzpostavitvi interneta, ko so omrežja potrebovala nove varnostne metode, ki so preprečevale večje zaplete. Od takrat so postali temelj omrežne varnosti (Lutkevich, 2021).

Požarni zidovi vzpostavljajo mejo med zunanjim omrežjem in omrežjem, ki ga varujejo. Preko omrežne povezave vstopijo v mrežo in tako preverijo vse podatke, ki vstopajo in izstopajo iz varovanega omrežja. Med pregledovanjem uporabljajo vnaprej konfigurirana pravila za razlikovanje med paketi, ki se razširijo in niso nevarni, in paketi, ki so zlonamerni. Beseda paket se nanaša na podatke, ki so oblikovani za prenos po internetu. V vsakem paketu so podatki, ki vsebujejo podatke podatkov – na primer od kod podatki izvirajo. Požarni zid na podlagi teh paketov zazna informacije o paketu, torej, ali je ta paket pravi oziroma če spoštuje nabor pravil. V kolikor ne izpolnjuje vseh pogojev, bo zavrnjen in mu bo vstop v varovano omrežje onemogočen (Lutkevich, 2021).

Paketni podatek vključuje tri značilnosti:

- njihov cilj,
- njihov vir,
- njihovo vsebino.

Te značilnosti se prikazujejo različno na različnih ravneh omrežja. Ko paket (paketi se nanašajo na podatke, ki so oblikovani za internetni prenos) potuje po omrežju, se večkrat preoblikuje, da lahko pove protokolu, kam naj ga pošlje. Na različnih omrežnih ravneh obstajajo različne komponente:

- za filtriranje paketov, pri čemer ne poznajo konteksta paketa,
- za preverjanje stanja omrežnega prometa in ugotavljanje, ali je določen paket povezan z drugim,
- posredniški strežnik,
- požarni zid za preprečevanje vdorov in za nadzor aplikacij.

Podjetja se morajo ob nakupu požarnih zidov zavedati svojih potreb in razumeti mrežno arhitekturo. Na trgu je veliko prodajalcev, specializiranih za različne za različne potrebe uporabnikov. Med najbolj prepoznanimi so: Palo Alto, Sonic Wall, Cisco, Sophos, Barracuda in Fortinet.

2.4 Sistem za upravljanje varovanja informacij

Sistem za upravljanje varovanja informacij (SUVI) pomeni sistem upravljanja informacijske varnosti. Gre za dokumentiran sistem, sestavljen iz sklopov varnostnih kontrol, ki ščiti zaupnost, razpoložljivost in celovitost sredstev pred grožnjami in ranljivostmi. Z zasnovo, upravljanjem, izvajanjem in vzdrževanjem SUVI lahko podjetje zaščiti svoje osebne, zaupne in občutljive podatke pred uhajanjem, uničenjem, poškodovanjem in pred drugimi škodljivimi dejavniki. Cilj SUVI je proaktivno omejiti vpliv kršitve varnosti podatkov (IT Governance, 2018).

Načini pristopa k izvajanju SUVI so najpogosteje metode, ki jih je potrebno upoštevati pri načrtu preverjanja zakona. Med te lahko štejemo ISO/IEC 27001. Gre za mednarodni varnostni standard, ki podrobno opisuje zahteve SUVI, medtem ko sta ISO 27001 in ISO 27002 standarda, ki služita kot vodiča za začetek izvajanja SUVI. Sistem SUVI, ki je potrjen in nerazviden pooblaščen organ za potrjevanje, je zagotovilo strankam, da je podjetje sprejelo potrebne ukrepe za zaščito svojih informacij pred vrsto tveganj. Za vsako izvajanje je pomembna moč SUVI, ki je temelj trdnosti ocene tveganja informacijske varnosti (IT Governance, 2018).

Cilji varovanja informacijske varnosti vključujejo tri glavne vidike (Myra Security, brez datuma):

- **Zaupnost.** Zaupne informacije lahko raziskujejo in gledajo samo pooblaščene osebe, ki imajo do njih dostop. Dostopi do teh informaciji morajo biti ustrezno zavarovani. Kršenje zaupnosti pomeni že samo napadalčevo prisluškovanje komunikaciji.
- **Celovitost.** Za ohranjanje natančnosti in popolnosti je potrebno, da informacije ostanejo zaščitene in neodkrite pred manipulacijami. S tem ohranjajo natančnost in popolnost.

Integriteta je kršena takrat, ko lahko napadalec spremeni podatke, brez da bi kdo opazil.
- **Razpoložljivost.** Viri, informacije ali storitve morajo biti na razpolago zakonitim uporabnikom. Ta razpoložljivost je lahko motena na primer z napadom za zavrnitev storitev DDoS (angl. Denial-of-service attack), ki namerno preobremeni sistem. Pod druge vidike lahko štejemo še odgovornost, verodostojnost, zavestnost in zanesljivost. Te stopnje informacijske varnosti je mogoče določiti na podlagi izpolnjevanja omenjenih ciljev zaščite.

V podjetju je za zagotavljanje informacijske varnosti treba razpolagati z vsemi potrebnimi sredstvi. Za to je odgovorno vodstvo podjetja, ki tudi poda sredstva za izvedbo in posledično nosi odgovornost za informacijsko varnost in ustrezen SUVI. Odgovornost podjetja je, da sproži varnostni postopek v organizacijski strukturi in opredeli varnostne cilje ter zagotovi splošne pogoje, ki določajo smernice za upravljanje informacijske varnosti. Za to zasnovo in za izvajanje teh smernic lahko podjetje prenese odgovornost na vodje in zaposlene. Vodstvo imenuje vodjo za informacijsko varnost, ki deluje kot kontaktna točka za vsa vprašanja v zvezi z informacijsko varnostjo. Ta oseba mora biti vključena v proces ISMS in tesno povezana z vodjo informacijske tehnologije. Z njim soodloča o novi izbiri komponent in IT-aplikaciji (Myra Security, brez datuma).

3 STANDARD ISO 27000

Standard ISO 27000 pojasnjuje zahteve za sistemsko upravljanje varnosti informacij (SUVI) v podjetjih. Podjetjem omogoča dokazovanje in izpolnjevanje regulativih zahtev, povezanih z informacijsko varnostjo, obenem pa lahko tako dokazujejo svoje zavzemanje za zaščito občutljivih in zaupnih podatkov. Standardi ISO 27000 zato zagotavljajo okvir, ki ga podjetje lahko uporablja pri zaščiti informacij. Običajno se to izvede z revizijsko prakso, testi in z uporabo različnih tehnologij. Podjetja imajo v večini primerov vrsto različnih varnostnih kontrol, ki jih uporabljajo za uravnavanje pretoka informaciji v in iz podjetja. Varnostni nadzor se zaradi udobja pogosto izvaja kot točkovna rešitev za določanje področja poslovanja, vendar ga ni mogoče nadzorovati z osrednjega območja. ISMS skuša te varnostne kontrole poenostaviti, da bi olajšal upravljanje varnosti podatkov. Pristop je sistematičen, saj gre za upravljanje z občutljivimi podatki podjetja. Da bi jih zaščitili, je za vsako podjetje priporočljiva uporaba ISMS sistema ne glede na njegovo velikost (Miller, 2019).

ISO 27001 standard zahteva od osebja upoštevanje vseh ranljivih točk v sistemu podjetja ter da opazijo grožnje, ki lahko škodujejo podjetju, in ostale stvari, ki na splošno vplivajo na upravljanje podatkov. Prav tako zahteva načrtovanje kontrol za varnost informaciji. Te se lahko štejejo med nevarne in tvegane. Od vodstvenega osebja se pričakuje, da spremlja postopek upravljanja, ki zagotavlja, da vsi nadzori informacijske varnosti ustrezajo potrebam organizacije po informacijski varnosti (Miller, 2019).

Standardi ISO 27000 so zasnovani za pomoč podjetjem pri obvladovanju tveganj kibernetskih napadov in notranjih groženj varnosti podatkov. Z rastjo podjetja se širi tudi tehnologija, ki jo podjetje uporablja, s tem pa prihaja do možnosti več ranljivosti, ki niso očitne in jih napadalci lahko izkoristijo. Podjetje uporablja ISO standarde za pomoč pri uvajanju učinkovitih in cenovno dostopnih rešitev, te pa pomagajo pri zaščiti poslovnih in osebnih podatkov ter intelektualnih lastnostih. Poznamo več vrst ISO 27000 standardov, med temi pa je standard ISO 27001 najbolj priljubljen, saj je edini, ki podjetju zagotovi revidirano potrdilo (Miller, 2019).

Po oceni (IT Governance, 2020) sodijo med najbolj prodajane ISO 27000 standarde:

- ISO/IEC 27001: 2013 in ISO / IEC 27002: 2013 Informacijska tehnologija – Varnostne tehnike;
- ISO/IEC 27017: 2015 (ISO 27017) Informacijska tehnologija – Varnostne tehnike – Kodeks ravnanja za nadzor informacijske varnosti na podlagi ISO/IEC 27002 za storitve v oblaku;
- ISO/IEC 27031: 2011 (ISO 27031) Informacijska tehnologija – Varnostne tehnike – Smernice za pripravljenost informacijske in komunikacijske tehnologije za neprekinjeno poslovanje;
- ISO/IEC 27000: 2018 (ISO 27000) Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in besedišče.

V družino ISO 27000 sodijo standardi (IT Governance, 2020):

- ISO/IEC 27000: 2018 (ISO 27000) – Pregled in besedišče,
- ISO/IEC 27001: 2013 (ISO27001) – Najnovejša različica standarda ISO 27001,
- ISO/IEC 27001: 2013/Cor 1: 2014 (ISO27001) – Tehnični popravek 1,
- ISO/IEC 27001: 2013/Cor 1: 2015 (ISO27001 – Tehnični popravek 2. Najnovejša različica standarda ISO 27001,
- ISO/IEC 27003: 2017 (ISO 27003) – Navodila,
- ISO/IEC 27004: 2016 (ISO 27004) – Upravljanje informacijske varnosti – Spremljanje, merjenje, analiza in vrednotenje,
- ISO/IEC 27005: 2018 (ISO 27005) – Obvladovanje tveganja informacijske varnosti,
- ISO/IEC 27006: 2015 (ISO 27006) – Zahteve za organe, ki zagotavljajo revizijo in certificiranje sistemov upravljanja informacijske varnosti,
- ISO/IEC 27007: 2017 (ISO 27007) – Smernice za revizijo sistemov upravljanja informacijske varnosti,
- ISO/IEC TR 27008: 2011 (ISO 27008) – Smernice za revizorje pri nadzoru informacijske varnosti,
- ISO/IEC 27009: 2016 (ISO 27009) – Sektorska uporaba ISO/IEC 27001 – Zahteve,
- ISO/IEC 27010: 2015 (ISO 27010) – Upravljanje informacijske varnosti za medsektorske in medorganizacijske komunikacije,
- ISO/IEC 27011: 2016 (ISO 27011) – Kodeks ravnanja pri nadzoru informacijske

varnosti na podlagi ISO/IEC 27002 za telekomunikacijske organizacije,
- ISO/IEC 27013: 2015 (ISO 27013) – Smernice za celostno izvajanje ISO/IEC 27001 in ISO/IEC 20000-1,
- ISO/IEC 27014: 2013 (ISO 27014) – Upravljanje informacijske varnosti,
- ISO/IEC TR 27016: 2014 (ISO 27016) – Upravljanje informacijske varnosti – Organizacijska ekonomija,
- ISO/IEC 27017: 2015 (ISO 27017) – Kodeks ravnanja za nadzor informacijske varnosti na podlagi ISO/IEC 27002 za storitve v oblaku,
- ISO/IEC 27018: 2014 (ISO27018) – Kodeks ravnanja za zaščito osebnih podatkov (PII) v javnih oblakih, ki delujejo kot PII procesorji,
- ISO/IEC 27023: 2015 (ISO 27023) – Preslikava revidiranih izdaj ISO/IEC 27001 in ISO/IEC 27002,
- ISO/IEC 27031: 2011 (ISO 27031) – Smernice za pripravljenost informacijske in komunikacijske tehnologije za neprekinjeno poslovanje,
- ISO/IEC 27032: 2012 (ISO 27032) – Smernice za kibernetsko varnost,
- ISO/IEC 27033-1: 201 (ISO 27033-1) – Omrežna varnost – 1. del: Pregled in koncepti,
- ISO/IEC 27033-2: 2012 (ISO 27033-2) – Omrežna varnost – 2. del: Smernice za načrtovanje in izvajanje omrežne varnosti,
- ISO/IEC 27033-3: 2010 (ISO27033-3) – Omrežna varnost – 3. del: Referenčni mrežni scenariji – Nevarnosti, tehnike oblikovanja in vprašanja nadzora,
- ISO/IEC 27033-4: 2014 (ISO 27033-4) – Omrežna varnost – 4. del: Zaščita komunikacije med omrežji z uporabo varnostnih prehodov,
- ISO/IEC 27033-5: 2013 (ISO 27033-5) – Varnost omrežja – 5. del: Zaščita komunikacij v omrežjih z uporabo navideznih zasebnih omrežij (VPN),
- ISO/IEC 27033-6: 2016 (ISO 27033-5) – Omrežna varnost – 6. del: Zavarovanje brezžičnega dostopa do omrežja IP,
- ISO/IEC 27034-1: 2011 (ISO 27034-1) – Varnost aplikacij – 1. del: Pregled in koncepti,
- ISO/IEC 27034-1: 2011/Cor 1: 2014 (ISO 27034-1) – Varnost aplikacij – 1. del: Pregled in koncepti – Tehnični popravek 1,
- ISO/IEC 27034-2: 2015 (ISO 27034-2) – Varnost aplikacij – 2. del: Organizacijski normativni okvir,
- ISO/IEC 27034-3: 2018 (ISO 27034-3) – 3. del: Postopek upravljanja varnosti aplikacij,
- ISO/IEC 27034-5: 2017 (ISO 27034-5) – Varnost aplikacije – 5. del: Protokoli in nadzor varnosti podatkovne strukture,
- ISO/IEC TS 27034-5-1: 2018 (ISO 27034-5-1) – Zaščita aplikacij – 5. –1. Del: Protokoli in nadzor varnosti podatkovne strukture, sheme XML,
- ISO/IEC 27034-6: 2016 (ISO 27034-6) – Varnost aplikacij – 6. del: Študije primerov,
- ISO/IEC 27034-7: 2018 (ISO 27034-7) – 7. del: Okvir za napovedovanje zagotovil,
- ISO/IEC 27035-1 2016 (ISO 27035-1) – Obvladovanje incidentov na področju informacijske varnosti - 1. del: Načela upravljanja incidentov,
- ISO/IEC 27035: 2016-2 (ISO 27035-2) - Obvladovanje incidentov na področju informacijske varnosti - 2. del: Smernice za načrtovanje in pripravo na odziv na incident,

- ISO/IEC 27036-1: 2014 (ISO 27036-1) – Informacijska varnost za odnose z dobavitelji - 1. del: Pregled in koncepti,
- ISO/IEC 27036-2: 2014 (ISO 27036-2) – Informacijska varnost za odnose z dobavitelji - 2. del: Zahteve,
- ISO/IEC 27036-3: 2013 (ISO 27036-3) – Informacijska varnost za odnose z dobavitelji - 3. del: Smernice za varnost dobavne verige informacijske in komunikacijske tehnologije,
- ISO/IEC 27036-4: 2016 (ISO 27036-4) - Informacijska varnost za odnose z dobavitelji - 4. del: Smernice za varnost storitev v oblaku,
- ISO/IEC 27037: 2012 (ISO 27037) – Smernice za identifikacijo, zbiranje, pridobivanje in hranjenje digitalnih dokazov,
- ISO/IEC 27038: 2014 (ISO 27038) – Specifikacija za digitalno redakcijo.
- ISO/IEC 27039: 2015 (ISO 27039) – Izbira, uvajanje in delovanje sistemov za odkrivanje in preprečevanje vdorov (IDPS).
- ISO/IEC 27040: 2015 (ISO 27040) – Varnost shranjevanja,
- ISO/IEC 27041: 2015 (ISO 27041) – Smernice za zagotavljanje primernosti in ustreznosti metod preiskovanja incidentov,
- ISO/IEC 27042: 2015 (ISO 27042) – Smernice za analizo in razlago digitalnih dokazov,
- ISO/IEC 27043: 2015 (ISO 27043) – Načela in postopki preiskovanja incidentov,
- ISO / IEC 27050-1: 2016 (ISO 27050) – Elektronsko odkrivanje – 1. del: Pregled in koncepti,
- ISO 27050-2: 2018 (ISO 27050-2) – Elektronsko odkrivanje – 2. del: Smernice za upravljanje in upravljanje elektronik.

4 ZAGOTAVLJANJE KIBERNETSKE VARNOSTI V IZBRANEM PODJETJU

Izbrano slovensko podjetje posluje na domačem in tujem trgu ter ponuja napredne rešitve in storitve s področja podatkovnih centrov, računalništva v oblaku, omrežij in informacijske varnosti za industrijska in poslovna okolja, javne institucije, državno upravo in ponudnike telekomunikacijskih storitev. Ukvarja se s svetovalnimi storitvami, vzdrževanjem in upravljanjem, sistemsko integracijo, razvojem učnih vsebin in izobraževalnimi storitvami. Glavni usmeritvi, tj. razvoju omrežij, sta sledila sistemska integracija in pionirski nastop na področju računalništva v oblaku. Danes se podjetje osredotoča predvsem na storitve in rešitve, povezane z novo generacijo programsko upravljanih omrežij, in z njihovo avtomatizacijo, s kibernetsko varnostjo, mobilnostjo, produktivnim sodelovanjem uporabnikov ter z naprednimi podatkovnimi centri (NIL, brez datuma).

Širok spekter izbranih partnerjev, več kot 80 strokovnjakov ter izkušnje s projektih v Sloveniji in tujini jim omogočajo, da ponujajo rešitve za tehnološke ter poslovne izzive strankam. Zaupajo jim vodilna svetovna podjetja na področju informacijskih tehnologij – Cisco Systems, Microsoft, IBM, EMC, VMware, Palo Alto Networks, Pure Storage,

MobileIron, RSA, F5, VCE, Sandvine, Veeam in drugi. Sedež podjetja je v Sloveniji, z rešitvami in storitvami pa so prisotni po vsem svetu. Lokalna predstavništva imajo tudi v Južnoafriški republiki, Maroku, ZDA, Savdski Arabiji in Srbiji. Izbrano podjetje se z IT-varnostjo ukvarja na področju varnostnega operativnega centra (SOC), varnosti v oblaku, zaščite pred škodljivo programsko opremo, ocene tveganja in pregledov z varno mobilnostjo. Naloga SOC je, da (24 ur na dan vse dni v tednu) spremlja in analizira dogajanja v IT-okolju. Tako lahko prepozna potencialne poskuse napadov ali varnostnih incidentov. V IT-okolju 100-odstotna varnost ne obstaja, zato je pomemben odzivni čas, s katerim se odzovejo na napad. Zato 24-urno spremljanje, ki ga zagotavlja SOC, podjetjem omogoča, da so v prednost pri obrambi pred incidenti in vdori ne glede vir, čas ali vrsto napada. Z analizami teh dejavnosti v omrežjih, strežnikih in bazah podatkov so ekipe SOC ključnega pomena za varnost podjetja (NIL, brez datuma).

Naloge SOC so:

- da se osredotoča na razvoj varnostne strategije,
- da oblikuje varnostno arhitekturo,
- da izvajanje zaščitne ukrepe,
- da skrbi za stalno delovanje komponent informacijske varnosti v podjetju,
- napredni SOC vključujejo napredne forenzične analize,
- kriptoanalize in obrano inženirstvo zlonamerne programske opreme za incidente.

SOC ekipo sestavljajo analitiki, ki so izredno usposobljeni in skupaj z inženirji in nadzorniki zagotavljajo, da vse deluje nemoteno. Tisti, ki so usposobljeni za uporabo različnih varnostnih orodji, še posebej poznajo tudi posebne procese, ki jih je treba upoštevati v primeru kršitve infrastrukture (Splunk, brez datuma).

Ekipa SOC temelji na hierarhičnem pristopu, kjer so analitiki in inženirji razvrščeni na podlagi svojih znanj in izkušenj. Ekipa je lahko strukturirana na sledeči način (Splunk, brez datuma):

1. stopnja: odzivniki. Varnostni strokovnjaki, ki spremljajo in bdijo nad opozorili ter določajo nujnost opozorila oziroma kdaj ga premakniti na 2. stopnjo. Poleg tega sta njihovi nalogi še upravljanje varnostnih orodji in vodenje rednih poročil.
2. stopnja: strokovnjaki, ki imajo več strokovnega znanja, pridejo na hitrejši način do izvora težave in lahko tako ocenijo, kateri del infrastrukture je napaden. Na ta način upoštevajo postopke za odpravo težav in popravilo morebitne škode, ki nastane ob napadu.
3. stopnja: to stopnjo sestavlja osebje, ki ima veliko znanja glede varnostne analitike in išče ranljivosti znotraj omrežja. Pomagajo si z naprednimi orodji, ki odkrivajo grožnje, in diagnosticirajo varnostne slabosti organizacije. V to skupino lahko sodijo tudi strokovnjaki, kot so revizorji skladnosti, forenzični preiskovalci in analitiki kibernetske varnosti.

4. stopnja: v to stopnjo sodijo vodje, ki so zelo usposobljeni in imajo največ izkušenj. Ti nadzirajo ekipo SOC in odgovarjajo za usposabljanje in ocenjevanje splošne uspešnosti. Poleg tega so odgovorni še za zagotavljanje skladnosti z organizacijskimi, industrijskimi in vladnimi predpisi. Svoji ekipi pomagajo tudi v kriznih situacijah in povezujejo ekipo SOC z ostalo organizacijo.

Poleg ekipe SOC ima podjetje tudi ekipo omrežnega operativnega centra (NOC). Naloga NOC je zagotavljanje, da sta zmogljivost in hitrost omrežja na enaki ravni in da je čas izpada omejena. Ekipa NOC išče kakršnekoli težave, ki bi upočasnile hitrost omrežja ali povzročile izpad. Tako imata SOC in NOC nekaj podobnost, saj sproti zagotavljata, da ne pride do težav, ki bi prizadele stranke ali zaposlene. Iščeta načine za izboljševanje, da težave ne bi več nastale ali se pojavile (Splunk, brez datuma).

Varnost v oblaku je sestavljena iz sklopa postopkov, politik, kontrol in tehnologij, ki skupaj ščitijo sisteme podatkov infrastrukture v oblaku. Varnostni ukrepi so konfigurirani za zaščito podatkov v oblaku in so določeni za preverjanje prisotnosti za posamezne uporabnike in naprave. Oblak omogoča nastavitev filtriranja prometa, ki se potem konfigurira in omogoči lažje upravljanje varnosti v oblaku. Gre za izvajanje varnosti procesa v oblaku, ki je odgovornost podjetja in ponudnika rešitev. Računalništvo v oblaku podjetjem omogoča, da delujejo v velikem obsegu, znižujejo stroške in uporabljajo sisteme, ki jim zagotavljajo konkurenčno prednost pred drugimi podjetji. Podjetje se na ta način lažje obvaruje pred krajo podatkov, korupcijo in izbrisom podatkov (NIL, brez datuma).

5 IZVEDBA INTERVJUJA

Z namenom dopolnitve ugotovitev iz prvega dela naloge je bil v empiričnem delu naloge izveden intervju. Intervju sem opravil ustno z vodjo SOC oddelka v izbranem podjetju. Za raziskavo sem se odločil, ker bi rad ugotovil, ali se zagotovljena kibernetska varnost v izbranem podjetju sklada z literaturo iz prvega dela naloge. Želel sem podrobneje izvedeti, na kakšen način se v izbranem podjetju ukvarjajo s kibernetsko varnostjo, kako se spopadajo z grožnjami in kako zahtevni so napadalci, ki ogrožajo informacijske sisteme. V nadaljevanju so predstavljena vprašanja in odgovori, pridobljeni s pomočjo intervjuja.

1. Kako v podjetju zagotavljate IT varnost?

Ko govorimo o varnosti informacijskih sistemov, vedno sprejemamo kompromise. Nikoli namreč ne moremo zagotoviti 100-% zaščite pred kibernetskimi grožnjami, lahko pa z njimi povezana tveganja zmanjšamo na (še) sprejemljivo raven. Kadar (in pravilno je, da) razmišljamo o kibernetski varnosti na nivoju vodstva organizacije, je bistveno razumevanje, kaj nam takšna varnost nudi. Očitno ne gre za tipično investicijo, katere vložena sredstva nadejano rezultirajo v njeno plemenitenje. V procesu uresničevanja strategije kibernetske obrambe prvenstveno vlagamo v zaščito svojih ključnih dobrin. Te so praviloma specifične

za posamezne organizacije ali branže. In vendar je obojim danes skupno eno; dobrine so svojim lastnikom in uporabnikom vse pogosteje dostopne tudi v digitalni obliki.

V našem podjetju se dobro zavedamo šibkega člena, ki je pogosta vstopna točka kibernetskih napadov, to so zaposleni v podjetju. Napadalci se poslužujejo različnih metod socialnega inženiringa, med njimi pa je najbolj pogosta tehnika zavajanja z ribarjenjem oz. »phishing« napad. Zavedajoč se tveganja, na redni ravni izvajamo izobraževanja zaposlenih, kjer jih ozaveščamo o potencialnih grožnjah in najbolj pogostih tehnikah zavajanja. Zaposlene hkrati usmerjamo, kako takšne grožnje pravočasno prepoznati, in še pomembneje, kako se v primerih varnostnih incidentov odzvati.

Stremimo tudi k zasnovi varnostno utrjenega informacijskega sistema po principu »zero-trust«. Koncept je z vidika varovanja digitalnih virov bistvenega pomena, še posebej v današnjem času, ko zaposleni delajo tudi od doma in dostop do internega omrežja ni več omejen le na lokacijo in »digitalne varovalke« podjetja. Zato je ključnega pomena, da uporabniku ali uporabnikovi napravi prvenstveno ne zaupamo, temveč ju pri vsakem dostopu do posamičnega vira ponovno overimo.

V poslu, ki ga moje podjetje opravlja, imamo pri več strankah omogočen neposreden vpogled v njihovo omrežno infrastrukturo in sisteme. Tveganji, ki ju je pri tem potrebno naslavljati, sta možnosti nepooblaščenega dostopa in odtekanja (ali kraje) občutljivih podatkov. Obe tveganji naslavljamo z implementacijo »Role-Based Access Control« (RBAC) politike in nadzorom dostopa do varnostno klasificiranih dokumentov.

Varnost informacijskih okolij se ne zaključi pri varnostnih napravah, programih in procesih, temveč mora biti tudi pravno podprta. V podjetju aktivno sodelujemo s pravno službo, ki skrbi, da so procesi in akcije IT-varnosti skladne z zakonodajo RS (kot npr. ZVOP, GDPR).

2. Ali je kibernetska varnost prisotna na vseh področjih poslovanja? Kje ni prisotna?

V zadnjih letih se je poslovanje podjetji v veliki meri digitaliziralo. Digitalizacija podjetjem nudi hitrejše in cenejše poslovanje, ob enem pa prinaša tudi dodatna tveganja. Kibernetska varnost mora biti prisotna na vseh področjih poslovanja, ki so digitalizirana, in tudi na področju dostopov do nedigitaliziranih delov poslovanja (arhivov).

Naše podjetje se ukvarja izključno z IT-storitvami, zato je naše celotno poslovanje digitalizirano. Naši specialisti na področju kibernetske varnosti ščitijo celotno infrastrukturo podjetja, proaktivno iščejo potencialne grožnje in se nanje odzivajo.

3. S kakšnimi grožnjami ste se že srečevali? Kako pogoste so te grožnje?

V podjetju smo zaznali že kar nekaj usmerjenih poskusov socialnega inženiringa, ki pa so bili tudi pravočasno prepoznani in ustrezno ustavljeni. Večino poskusov prepoznajo že varnostni sistemi in varnostne politike, ki jih imamo implementirane, nekaj pa jih prijavijo

tudi končni uporabniki. Potreba po poglobljeni analizi potencialnih napadov socialnega inženiringa se pojavi v povprečju 10-krat letno.

Opažamo pa v Sloveniji porast »ransomware« napadov. Ti napadi so v večini uspešni zaradi varnostno neustrezne postavitve ali konfiguracije naprav in pomanjkanja implementiranih varnostnih rešitev ter procesov. Ta vrsta napadov je v slovenskih podjetjih zelo pogosta, v povprečju v našem varnostno operativnem centru obravnavamo 1–2 takšna incidenta mesečno.

4. V svetu je opaziti porast kibernetskih napadov. Vas kakšen izmed njih izrecno skrbi?

Kibernetskih napadov se ne bojimo, saj smo nanje zelo dobro pripravljeni. To še ne pomeni, da kibernetske kriminalce podcenjujemo ali da se resnosti groženj ne zavedamo. Imamo vzorno zaščiteno informacijsko okolje, ki ga dodatno varuje varnostno operativni center (SOC) in neprekinjeno išče oz. zaznava potencialna varnostna odstopanja. Napadi, za katere ustrezna zaščita ne obstaja, se imenujejo »zero day« napadi. Ti napadi izkoriščajo (še) nepoznane ranljivosti, pred njimi pa se ni mogoče enostavno zaščititi. Edini možni zaščiti proti tej vrsti napadov sta aktivno spremljanje dogajanja v IT-okolju ter iskanje nevsakdanjih orodij in tokov podatkov.

V kolikor napadalcem uspe prodreti v okolje organizacije, je ključnega pomena, da imamo pripravljen načrt odzivanja na varnostne incidente (angl. incident response plan). Ta narekuje akcije, potrebne za zajezitev napada in zmanjšanje poslovne škode, ter tudi navodila, kako postopati po napadu in okolje vrniti v prvotno stanje.

5. Katero je po vašem mnenju največje tveganje pri kibernetskem napadu na podjetje?

Največje tveganje v primeru kibernetskega napada je vsekakor poslovna škoda. Ta lahko nastane zaradi odtujitve ali kraje podatkov, prekinitve poslovanja, plačila napadalcem in ponovne postavitve IT-okolja.

6. Menite, da zaposleni v podjetju dovolj dobro poznajo nevarnosti, ki jih prinaša kibernetski kriminal? Se znajo zaščititi npr. pred socialnim inženiringom?

V našem podjetju imamo več nivojev zaščite pred napadi na osnovi socialnega inženiringa. Prvi nivoji zaščite so tehnični. To so raznorazni varnostni filtri, ki preverjajo vhodno pošto in datoteke, nato pa imamo implementirane sisteme in politike, ki podrobno preverjajo prejete datoteke in spletne povezave (linke).

Drugi nivo zaščite pred napadi s socialnim inženiringom z drugimi besedami imenujemo tudi človeški požarni zid (angl. human firewall). V podjetju zaposlene redno izobražujemo o novostih na področju socialnega inženiringa in njihovo znanje tudi občasno v praksi

preverimo. Zaposleni, v kolikor opazijo potencialno nevarno pošto ali dokument, lahko na zelo enostaven način obvestijo varnostno operativni center, ki nevarnost preuči in analizira.

7. Kako skrbite za varnost podatkov v podjetju?

V podjetju imamo implementiran Role-Based Access Control (RBAC) varnostne politike, s katerimi dostop do podatkov omejimo le na osebe in digitalne vire, ki te podatke potrebujejo za svoje delo. Dostopi do podatkov se beležijo tako, da lahko v primeru kraje podatkov odkrijemo krivca. Vse tehnične rešitve za zaščito podatkov so tudi pravno podprte.

8. Kako v podjetju skrbite za varnost podatkov zaposlenih?

Skrb za osebne podatke v podjetju jemljemo zelo resno. Temu primerno smo ukrojili tudi svoj organizacijskih poslovnik in notranje procese, ki so skladni z uveljavljenimi varnostnimi standardi, uredbami in zakonodajo (ISO27001, ZVOP, GDPR).

Osebnih podatkov, ki jih za poslovanje ali zaposlovanje ne potrebujemo, ne zbiramo. Dostop do zbranih osebnih podatkov je omejen s še bolj strogimi role-based access control (RBAC) politikami. Prav tako se tudi dostop do teh podatkov enoumno beleži.

9. Je za podjetje pomembno, da ima kakovostno tako strojno kot programsko opremo, ki ščiti pred kibernetskimi napadi? Kaj za podjetje pomeni imeti kakovostnejši (dražji) požarni zid?

Kakovost izdelkov je seveda povsod izjemno pomembna. Pri programski in strojni opremi IT-sistemov pa je pomembna tudi kredibilnost proizvajalca, saj nam lahko ta ali njegovi partnerji v opremo skrijejo škodljivo kodo oz. zanjo niti ne vedo (zadnji primeri »supply chain« napadov).

Tudi če imamo kakovostno opremo kredibilnih proizvajalcev, pa previdnost pri nameščanju posodobitev ni odveč. V lanskem letu smo bili priča napadu, v katerem so napadalci dostop do sistemov dobili preko SolarWinds programske opreme. Takšen napad se imenuje »supply chain« napad. Proti takšni vrsti napadov se lahko ščitimo s preverjanjem posodobitev programske opreme v testnih okoljih.

Cena in kakovost nista vedno povezana. Imeti kakovostnejši požarni zid, pomeni, da lahko z njim boljše nadzorujemo promet in da nam omogoča zaznavo ter avtomatiziran odziv na zaznane grožnje.

10. Kateri proizvajalec ima po vašem mnenju najboljše požarne zidove in zakaj?

Sami smo pri izbiri kvalitetnih rešitev z ustrezno kasnejšo podporo (posodobitvami, proizvajalčevim nivojem nudenja podpore) zelo izbirčni in strokovno kritični. Interno v podjetju najmanj 2-krat letno izvedemo poglobljeno tehnično evalvacijo konkurenčnih varnostnih rešitev različnih proizvajalcev. Izbiramo tiste rešitve, ki nudijo najvišjo stopnjo

kibernetske obrambe pred najsodobnejšimi tehnikami napadalcev. Zavedati pa se moramo, da je namestitev varnostne rešitve (npr. požarnega zidu) v okolju organizacije šele prvi korak zagotavljanja učinkovite kibernetske obrambe. Takšne sisteme je potrebno varnostno utrjevati, jih negovati, neprekinjeno spremljati in se v primerih incidentov tudi odzivati.

Če bi že moral izbirati svojega najljubšega proizvajalca požarnih pregrad, bi izbral takšnega, ki mi tudi v neugodni situaciji (npr. zero day napad ali izpad komponente) kar najhitreje pomaga iz zagate (zajezi napad ali nudi podporo pri odpravi napake). Osebno sem mnenja, da bolj kot barva šasije požarnega zidu (beri: proizvajalec) odtehta oseba, ki za požarno pregrado skrbi in z njo upravlja (skrbi za selektivnost in utrjevanje varnostne politike, posodobitve, nadgradnje …).

11. Kako pomemben je po vašem mnenju SUVI za podjetje? Ali v podjetju uporabljate/sledite SUVI? Imate strategijo kibernetske varnosti? Ali v podjetju sledite kakšnemu mednarodnemu standardu, npr. ISO27001? V kolikšni meri? Zakaj je pomembno, da se v podjetju upošteva varnostne standarde?

SUVI je za podjetja zelo pomemben, saj so v njem obravnavane grožnje, ki pretijo podjetju, in opisuje procese naslavljanja teh groženj. V podjetju imamo implementiran SUVI. Tveganja večkrat letno naslavljamo in preverjamo, kako so bila že identificirana tveganja naslovljena. Obenem smo tudi dobro pripravljeni na kibernetski napad, saj aktivno in pasivno iščemo grožnje, ob enem pa imamo tudi razvite procese za odziv na napad.

V podjetju posedujemo in tudi redno obnavljamo ISO 27001 certifikat. S certifikatom interno in tudi navzven izkazujemo, da imamo ustrezno implementirane varnostne rešitve, politike in procese.

Certifikati so zelo pomembni, saj lahko le na tak način, preko neodvisnih presojevalcev, podjetja izkažejo pripravljenost na kibernetski napad.

12. Imate v podjetju vzpostavljen SOC? Kakšen je njegov namen?

V podjetju imamo vzpostavljen interni varnostno operativni center, katerega nameni so aktivno in pasivno iskanje, zaznava in odziv na groženje. V varnostno operativnem centru (NIL SOC) si nalagamo odgovornost rednega izboljševanja kibernetske odpornosti uporabnikov naših storitev. Zakoreninjene zmogljivosti tradicionalnih informacijskih sistemov, ki pogosto temeljijo izključno na preventivi in krpanju šibko oskrbovanih ran, bogatimo s (pre)potrebno ekspertizo zaznavanja in odzivanja na pomenljive varnostne dogodke. V ta namen smo sistemizirali visoko usposobljene varnostne analitike, ki bdijo nad – priznajmo si – varnostno neidealnimi informacijskimi okolji in odvračajo pozornost kibernetskih kriminalcev.

13. Kako skrbite za kibernetsko varnost v svojih oblačnih sistemih?

Pri oblačnih rešitvah je zelo pomembna pravna podlaga za varovanje podatkov, saj se ti v večini primerov nahajajo zunaj matične države. V podjetju za varovanje rešitev, ki se nahajajo v oblaku, primarno uporabljamo produkte ponudnika oblačnih rešitev, ki se za res ne razlikujejo od produktov, ki varujejo naprave v podatkovnem centru. Oblak je le podatkovni center, ki se ne nahaja v kleti podjetja, temveč nekje drugje. Pri varovanju oblačnih rešitev sta ključnega pomena avtentikacija uporabnikov in »zero-trust« varnostna arhitektura. Pomembno je tudi, da se dostopi do oblačnih rešitev beležijo, saj nam to omogoča zaznavo groženj.

14. Kako v letu 2022 izboljšati informacijsko varnost v podjetju?

Pomembno je, da ima podjetje vzpostavljeno strategijo vlaganja v kibernetsko varnost za npr. naslednja 3 leta in da tej strategiji sledi. Ker se grožnje spreminjajo na dnevni, tedenski in mesečni ravni, kibernetska varnost ni enkraten projekt, enako tudi ne produkt. Gre za kontinuiran proces, za katerim v prvi vrsti stoji že samo vodstvo podjetja. Pomembno je, da podjetja iz leta v leto ta proces dopolnjujejo in naslavljajo grožnje, ki jih zadevajo. Na ta način bo iz leta v leto implementiranih več varnostnih rešitev in procesov, ki bodo sčasoma zadoščali tudi mednarodnim standardom (npr. ISO 21001).

6 KLJUČNE UGOTOVITVE

Ključne ugotovitve so opredeljene na podlagi teoretičnega dela naloge in intervjuja vodje SOC oddelka v izbranem podjetju.

Zagotavljanje varnosti informacijskih sistemov temelji na sprejemanju kompromisov. Podjetje nikoli ne more zagotoviti 100-odstotne zaščite pred kibernetskimi grožnjami, temveč lahko prepozna in zmanjša tveganja na še spremenljivo raven. Ko razmišljajo podjetja o kibernetski varnosti, razmišljajo o tem, kaj jim takšna varnost nudi in kako bodo zaščitili svoje dobrine. Največje tveganje za podjetje v primeru kibernetskega napada predstavlja škoda. Ta lahko nastane zaradi odtujitve ali kraje podatkov, prekinitve poslovanja, plačila napadalcem in ponovne postavitve IT-okolja.

V izbranem podjetju se dobro zavedajo, da so njihova šibka točka zaposleni, saj se napadalci poslužujejo različnih metod socialnega inženiringa. Med najpogostejšimi tehnikami zavajanja je »phishing« napad. Na ta način zavajajo uporabnike in od njih pridobivajo občutljive osebne podatke (številke kreditnih kartic, podatke o računu, gesla), zato v podjetju izvajajo izobraževanja zaposlenih, kjer jih ozaveščajo o potencialnih grožnjah in najpogostejših tehnikah zavajanja.

Podjetje še posebej v današnjih časih stremi k zasnovani varnosti utrjenega informacijskega sistema po principu »zero-trust«. Ta način je uporabljen, ko uporabniki delajo od doma in dostop do internetnega omrežja ni več omejen na lokacijo podjetja, zato je ključnega pomena, da uporabnikom naprav prvenstveno ne zaupajo in jih pri vsakem dostopu do

nekega vira ponovno overijo. Podjetje sodeluje tudi s pravno službo, ki skrbi, da so procesi in akcije IT-varnosti skladne z zakonodajo Republike Slovenije.

Digitalizacija podjetij nudi podjetjem hitrejše in cenejše poslovanje, obenem pa prinaša tudi dodatna tveganja. Kibernetska varnost mora biti prisotna na vseh področjih poslovanja, ki so digitalizirana, in tudi na področju dostopov do nedigitaliziranih delov poslovanja (arhivov). Izbrano podjetje se ukvarja z IT-storitvami, zato je njihovo poslovanje digitalizirano. Njihovi specialisti pa na področju kibernetske varnosti ščitijo celotno infrastrukturo podjetja in proaktivno iščejo potencialne grožnje ter se nanje odzivajo.

Podjetje se je največkrat srečalo s poskusi socialnega inženiringa, ki so jih pravočasno prepoznali in ustrezno ustavili. V Sloveniji opažamo vse več napadov, povezanih z odkupninami programske opreme, ki zaradi neustrezne postavitve ali konfiguracije naprav in pomankanja implementacije varnostnih rešitev in procesov povzročajo škodo. V izbranem podjetju obravnavajo 1–2 taka incidenta mesečno.

Podjetje za varnost podatkov skrbi tako, da ima implementirane nadzore dostopa na podlagi vlog tako imenovan »Role-Based Access Control« (RBAC) varnostne politike, s katerimi dostop do podatkov omejimo le na osebe in digitalne vire, ki te podatke potrebujejo za svoje delo. Dostopi do podatkov se beležijo tako, da lahko v primeru kraje podatkov odkrijejo krivca. Vse tehnične rešitve za zaščito podatkov so tudi pravno podprte. Za osebne podatke zaposlenih podjetje zelo skrbi. Podjetje je ukrojilo svoj organizacijski poslovnik in svoj notranji proces, ki je skladen z varnostnimi standardi, uredbami in zakonodajo (ISO 27001).

Kakovost programske opreme je podjetju pomembna. Še posebej izpostavljajo kredibilnost proizvajalca in previdnost nameščanja, saj je lahko v opremi skrita škodljiva koda, ki potem vodi v napad na programsko opremo. Zaradi povedanega je pomembno, da programsko opremo ščitimo s preverjanim posodabljanj v testnih okoljih. Vodja SOC oddelka v izbranem podjetju meni, da cena in kakovost nista vedno povezana. V podjetju se 2-krat letno poglobijo v tehnično evalvacijo konkurenčnih varnostnih rešitev različnih proizvajalcev in izberejo tiste rešitve, ki nudijo najvišjo stopnjo kibernetske obrambe pred najsodobnejšimi tehnikami napadalcev.

Podjetje ima SUVI implementiran. Tveganja večkrat letno naslavljajo in preverjajo, kako so bila že identificirana tveganja naslovljena. Zelo dobro so pripravljeni na kibernetski napad, saj aktivno in pasivno iščejo grožnje. Podjetje obnavlja ISO 27001 certifikat, s katerim navzven izkazuje, da ima ustrezno implementirane varnostne rešitve, politike in procese. Certifikati so za podjetje zelo pomembni, saj lahko na tak način preko neodvisnih presojevalcev podjetje izraža pripravljenost na kibernetski napad.

Varnostno operativni center ima podjetje vzpostavljen, saj aktivno in pasivno išče, zaznava in se odziva na grožnje. V tem oddelku podjetja si nalagajo odgovornost rednega izboljševanja kibernetske odpornosti uporabnikov svojih storitev. Visoko usposobljeni

varnostni analitiki, ki bedijo nad varnostno, neidealnim informacijskim okoljem odvračajo pozornost kibernetskih kriminalcev.

Pri oblačnih rešitvah podjetje uporablja produkte ponudnika oblačnih rešitev. Pri varovanju oblačnih rešitev sta pomembni avtentikacija uporabnikov in »zero-trust« varnostna analitika. Pomembno se jim zdi tudi, da se dostopi do oblačnih rešitev beležijo, saj jim to omogoča zaznavo groženj.

Vodja SOC oddelka je glede izboljšave informacijske varnosti v naslednjih letih mnenja, da je za podjetje pomembno sprotno vlaganje v kibernetsko varnost, saj se grožnje spreminjajo na dnevni, tedenski in mesečni ravni. Za podjetje je pomembno, da iz leta v leto ta proces dopolnjuje in da naslavlja grožnje, ki ga zadevajo. Tako bo iz leta v leto implementiralo več varnostnih rešitev in procesov, ki bodo sčasoma zadoščali tudi mednarodnim standardom.

SKLEP

V prvem delu diplomske naloge so najprej razloženi kibernetska varnost, upravljanje varovanja informaciji in standardi ISO 27000, v drugem delu pa je predstavljeno zagotavljanje kibernetske varnost v izbranem podjetju. Gre za ugotovitve, kako podjetje zagotavlja kibernetsko varnost, na katerih področjih je prisotna, s kakšnimi grožnjami se srečuje podjetje, kako zaposleni poznajo kibernetsko varnost, kako podjetje skrbi za varnost podatkov podjetja in zaposlenih, kakšno strojno opremo ima izbrano podjetje, kako pomemben je za podjetje SUVI, kakšen je namen SOC ekipe in kako izboljšati kibernetsko varnost v naslednjih letih.

Za kibernetsko varnost v podjetjih ni odgovoren samo SOC, temveč vsi zaposleni. Podjetja morajo slediti strategiji kibernetske obrambe, ki si jo zastavijo. Osebe, ki skrbijo za nadgradnje, posodobitve, selektivnost in utrjevanje varnostne politike, pomagajo podjetju, da sledi tej strategiji. Poleg teh v podjetju za kibernetsko varnost skrbijo tudi vsi ostali zaposleni, ki se nenehno izobražujejo na tem področju in na tak način pomagajo podjetju pri hitrejšem prepoznavanju kibernetskih groženj.

Do zaključkov sem prišel z intervjujem vodje SOC oddelka v izbranem podjetju. Ugotovil sem, da morajo podjetja izbirati rešitve, ki jim nudijo najvišjo stopnjo kibernetske obrambe pred najsodobnejšimi tehnikami napadalcev. Pomembno je tudi, da imajo na najvišji stopnji izobražene analitike, ki skrbijo za upravljanje in varovanje svojega podjetja ter podjetij naročnikov. Vsako podjetje ima tudi šibke člene, ki so pogosto vstopna točka kibernetskih napadov, to so zaposleni v podjetju. Zato morajo podjetja na redni ravni izvajati izobraževanja zaposlenih, kjer jih ozaveščajo o potencialnih grožnjah in najpogostejših tehnikah zavajanja. Poučevati jih morajo o tem, kako grožnjo pravočasno prepoznati in kako se odzvati v primeru varnostnega incidenta. Poleg tega naj podjetje poseduje in redno

obnavlja ISO 27001 certifikat. S tem certifikatom podjetje interno in tudi navzven izkazuje, da ima ustrezno implementirane varnostne rešitve, politike in procese.

LITERATURA IN VIRI

1. AO Kaspersky Lab. (2021). *What is Cyber Security?* Pridobljeno 6. aprila 2021 iz https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
2. Avast Software s.r.o. (2020, 22. julij). *What Is a Computer Worm?* Pridobljeno 8. aprila iz https://www.avast.com/c-computer-worm
3. Cisco Systems, Inc. (2021). *What Is Cybersecurity*. Pridobljeno 6. aprila 2021 iz https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
4. IDG Communications, Inc. (2019, 17. maj). *Malware explained: How to prevent, detect and recover from it.* Pridobljeno 8. aprila 2021 iz https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html
5. IDG Communications, Inc. (2021, 16. julij). *The 15 biggest data breaches of the 21st century*. Pridobljeno 13 aprila 2021 iz https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st century.html
6. Finkle, J. (2013, 29. oktober). *Adobe data breach more extensive than previously disclosed*. Pridobljeno 10. avgusta 2021 iz https://www.reuters.com/article/us-adobe-cyberattack-idUSBRE99S1DJ20131029
7. IT Governance Ltd. (2018, julij). *What is an information security management system (ISMS)?* Pridobljeno 25. maja 2021 iz https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2
8. IT Governance Ltd. (2020, junij). *The ISO/IEC 27000 Family of Information Security Standards*. Pridobljeno 3 junija 2021 iz https://www.itgovernance.asia/iso27000-family
9. Lutkevich, B. (2021). *Definition firewall*. Pridobljeno 25. maja 2021 iz https://searchsecurity.techtarget.com/definition/firewall
10. ManageEnginePatch Management Plus. (brez datuma). *What is patch management?* Pridobljeno 21. aprila 2021 iz https://www.manageengine.com/patch-management/what-is-patch-management.html?src=what-is-pm-FAQ
11. Miller, J. (2019, avgust). *What is the ISO 27000 series of standards?* Pridobljeno 28. maja 2021 iz https://www.bitlyft.com/resources/what-is-iso-27000
12. MIT Technology Review. (2016, december). *A History of Yahoo Hacks*. Pridobljeno 10. avgusta 2021 iz https://www.technologyreview.com/2016/12/15/106901/a-history-of-yahoo-hacks/
13. Myra Security GmbH. (brez datuma). *What Is an Information Security Management System (ISMS)?* Pridobljeno 27. maja 2021 iz https://www.myrasecurity.com/en/information-security-management-system-isms/#difference-informations-and-it-security
14. NIL d.o.o. (brez datuma). *NIL part od conscia.* Pridobljeno 27. julija 2021 iz https://www.nil.com/sl/home/

15. NortonLifeLock Inc. (2020, 24. julij). *What is a Trojan? Is it a virus or is it malware?* Pridobljeno 8. aprila 2021 iz https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
16. Reuters graphics. (brez datuma). *Hacking via the Internet of Things*. Pridobljeno 21. aprila 2021 iz http://fingfx.thomsonreuters.com/gfx/rngs/IOT-CYBER/0100307Z0J8/index.html
17. Risk Besed security. (2019, 12. november). *Number of Records Exposed Up 112% in Q3*. Pridobljeno 6. aprila 2021 iz https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/
18. Sloan, K. (2021, 7 julij). *Cybersecurity Training for Employees: What You Need to Know.* Pridobljeno 25. julija 2021 iz https://www.cybintsolutions.com/cybersecurity-training-for-employees-what-you-need-to-know/
19. Splunk Inc. (brez datuma). *What Is a Security Operations Center (SOC)?* Pridobljeno 28. julija 2021 iz https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html#overview
20. Stop Ransomware. (brez datuma). *RANSOMWARE 10*1. Pridobljeno 21. aprila 2021 iz https://www.cisa.gov/stopransomware/ransomware-101
21. Traveles. (brez datuma a). *5 Ways to Help Protect Your Company's Data*. Pridobljeno 29. aprila 2021 iz https://www.travelers.com/resources/business-topics/cyber-security/5-ways-to-help-protect-company-data
22. Traveles. (brez datuma b). *Cyber Security Training for Employees*. Pridobljeno 3. maja 2021 iz https://www.travelers.com/resources/business-topics/cyber-security/cyber-security-training-for-employees
23. Zoe, E. (2020). *What you need to know (and do) about cybersecurity training* [objava na blogu]. Pridobljeno 25. julija 2021 iz https://www.efrontlearning.com/blog/2019/03/cyber-security-training-for-employees-101.html