UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

ANALIZA INFORMACIJSKE VARNOSTI V IZBRANEM PODJETJU

Ljubljana, julij 2022 JAN SETNIČAR

IZJAVA O AVTORSTVU

Podpisani Jan Setničar, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza informacijske varnosti v izbranem podjetju, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Mirom Gradišarjem

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(-ke): _____

KAZALO

KAZALO SLIK

KAZALO TABEL

SEZNAM KRATIC

angl. – angleško
DIH – Digitalno inovacijsko stičišče Slovenije
GDPR – (angl. General Data Protection Regulation); Splošna uredba EU o varstvu podatkov
IoT – (angl. Internet od Things); Internet stvari
ISMS – (angl. Information Security Management System); Sistem upravljanja informacijske varnosti
ISO − (angl. International Organization for Standardisation**);** Mednarodna organizacija za standardizacijo

UVOD

V sodobnem svetu, in še posebej v zadnjem desetletju, postaja kibernetska varnost vse bolj pomembna in obsežna tematika za vse osebe, fizične in pravne. Podjetja pospešeno ter v čim večjem obsegu pretvarjajo svoje poslovanje v elektronsko obliko, kar pa je izredna podlaga in priložnost za kibernetske vdore, ki podjetju lahko huje škodijo finančno, materialno, v obliki škodovanja imenu ali pa kar vse skupaj.

Ta naloga je pomembna tako za podjetja kot za posamezne bralce, saj se dotakne danes zelo pomembne tematike kibernetske varnosti, ki kljub svoji obsežnosti in konstantnemu večanju urgentnosti obravnave še vedno ostaja premalo naslovljena. Poleg obravnave omenjene tematike bodo celotne ugotovitve predstavljene tudi na finančni ravni, in sicer v stroškovni primerjavi glede na statistične podatke; torej, razlika v stroških v primeru pregleda ter sanacij šibkosti kibernetske varnosti in v primeru potencialnega napada. Podjetjem na primeru tako pokaže potencialne nevarnosti in resnost le teh, posameznim bralcem pa potencialno lahko razširi obzorja na tem področju.

V tej nalogi sem torej opredelil vrste kibernetskih napadov ter tveganj za podjetja, identificiral tveganja za izbrano podjetje in jih predstavil iz ekonomskega vidika v obliki potencialne škode v primerjavi s stroški sanacije.

Osrednja vprašanja so:

- »Kakšna so tveganja za podjetja in specifično za izbrano podjetje na področju kibernetske varnosti?«
- »Kakšni so osnovni varnostni ukrepi in priporočila glede na opredeljena tveganja?«
- »Kakšna je potencialna škoda v primerjavi s stroški implementacije boljše kibernetske varnosti informacijskega sistema?«

Metode za pridobitev, analizo in uporabo informacij so teoretične, in sicer deskriptivna oziroma opisna metoda ter kavzalna oziroma neeksperimentalna metoda. Z drugimi besedami sem za izvedbo naloge uporabil strategijo branja in povzemanja objavljene literature v obliki člankov, publikacij ipd., ter izvedbo pogovora z izbrano osebo, s katerim sem pridobil potrebne specifične podatke izbranega podjetja.

V začetnem poglavju sem postavil osnovno podlago glede trenutnega stanja, ki služi kot temelj nadaljnjih poglavij. Zatem opredeljujem vrste kibernetskih napadov in skladnost pregledov ter nevarnosti, ki so relevantne za izbrano ter ostala splošna podjetja. Sledi kratko poglavje o osnovnih relevantnih informacijah podjetja, ki doda še dodatni temelj za naslednji dve poglavji, v katerih sem opredelil način analize podjetja in nato analizo tudi izvedel. Zatem sem smiselno opredelil potencialne stroške ob napadu in jih primerjal s splošnimi stroški izvedbe storitev na področju kibernetske varnosti. V zadnjem vsebinskem

poglavju so opisani še vavčerji za kibernetsko varnost ter za dvig digitalnih kompetenc, ki so podjetjem lahko zelo v pomoč ob financiranju izvedbe storitev na področju kibernetske varnosti.

1 PREGLED STANJA

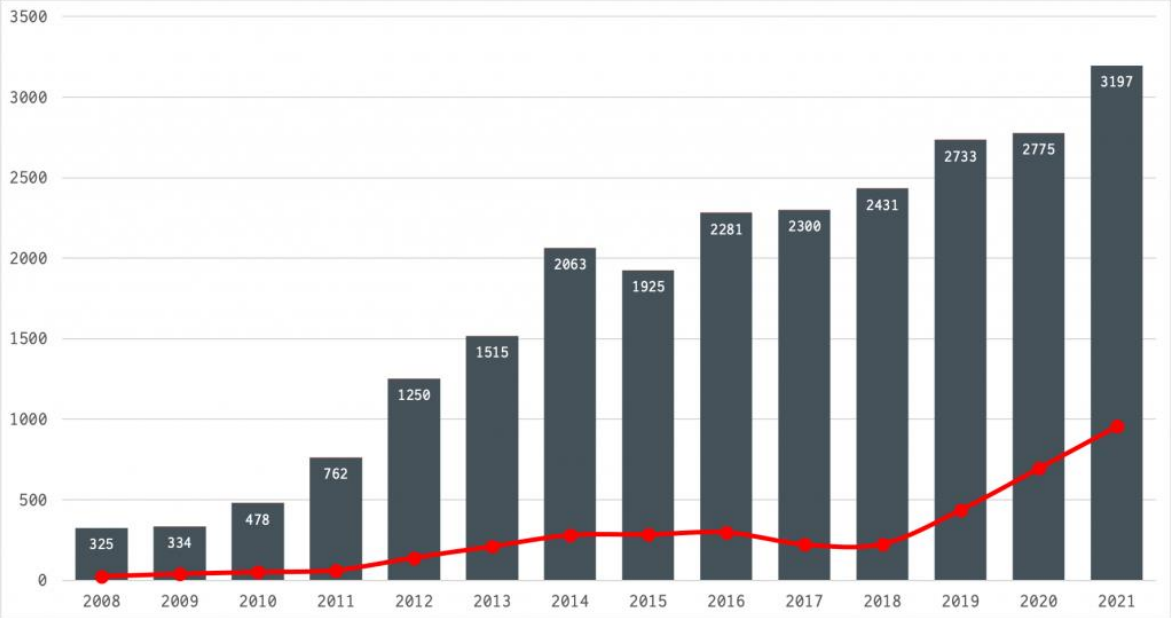
Ob eksponentni rasti elektronskega poslovanja eksponentno rastejo tudi primeri kibernetskih napadov. Napadalci namreč prežijo na podjetja, ki so resnost kibernetskih groženj podcenjevala in svojega sistema niso primerno ali vsaj minimalno zaščitila. Fizični vdori so namreč zelo podobni kibernetskim, kadar za primerjavo vzamemo »vhodna vrata«, v smislu da primerna oblika in protivlomna lastnost vhodnih vrat in obstoj ostalih osnovnih varnostnih ukrepov v večini primerov že lahko odvrne vlomilca, saj bi poskus vdora bil ali preveč tvegan ali pa preveč dolgotrajen in zahteven glede na »vhodna vrata« soseda, ki so lahko daleč manj varovana. Zaradi tega je pametno postaviti vsaj osnovne varnostne mehanizme, saj že tako lahko odvrnemo napadalca od nadaljnjega poskušanja vdora v sistem (Railmonitor, brez datuma).

Načinov za hitro preverjanje potencialnih tarč je na spletu veliko, večji primer je spletna stran shodan.io, ki je uporabljena tako iz strani izvajalcev kibernetskih varnostnih pregledov kot zlonamernih napadalcev. Tako kot Google je Shodan prav tako iskalnik, vendar posebej zasnovan za internet stvari (angl. Internet of Things – IoT) . Pri iskanju s tem iskalnikom se lahko prikaže katera koli naprava, povezana na internet. Primeri teh so strežniki, tiskalniki, domače pametne naprave, varnostne kamere, varnostni sistemi, spletne kamere, blagajne, semaforji itd. Osnovni primer potenciala za zlonamerno uporabo je preprosto iskanje s ključno besedo »default password«, ki nam vrne ogromno število najdenih serverjev, printerjev in raznih sistemov s privzetim uporabniškim imenom in geslom, nekateri od teh pa poleg navedenega tudi nimajo zahtevanih poverilnic za vpis, kar pomeni, da se lahko prijavimo iz katere koli naprave in brskalnika (Cyber Talents, brez datuma).

V Sloveniji je bilo število obravnavanih kibernetskih napadov iz strani SI-CERT-a (nacionalni odzivni center za kibernetsko varnost) kot pričakovano dokaj večje od prejšnjih let (Slika 1), dodatno rast pa je prispevalo tudi obdobje dela od doma, za katerega je bila odgovorna porast okužb in s tem razglašena pandemija virusa covid-19. Delo od doma je namreč v večini primerov predstavljalo novo širitev obsega elektronskega poslovanja, kar pa je prestavljalo nove možnosti za vdore, saj se veliko podjetij ni zavedalo dodatnih tveganj, ki jih novi in dodatni način poslovanja predstavlja in tako niso primerno oziroma pravočasno naslovila in implementirala dodatnih varnostnih ukrepov.

Posledično je največjo rast med načini kibernetskih vdorov pridobila strategija kibernetskega napada z uporabo socialnega inženiringa (SI-CERT, 2021).

Slika 1: »Število obravnavanih incidentov na SI-CERT po letih (z deležem phishing incidentov in projekcijo za 2021)«



Vir: SI-CERT (2021).

2 VRSTE NAPADOV IN PREGLEDOV TER OPREDELITEV SPLOŠNIH ŠIBKOSTI

Vrste napadov sem opredelil skladno z načini preverjanja varnosti sistemov oziroma izvedbe storitev za preprečitev napada, saj so pregledi zelo podobni dejanskim napadom z razliko, da so pregledi zasnovani na predhodni pogodbi o nerazkritju informacij (angl. Non-Disclosure Agreement) in dodatno ne ovirajo poslovanja. Vrste napadov in pregledov so torej napad s pomočjo uporabe socialnega inženiringa, zunanji napad in notranji napad. Na koncu sledi še poglavje, ki se dotakne tematike kraje podatkov, kar sicer samo po sebi ni strategija za napad, je pa zelo pogost cilj napadalcev in je zato kot šibkost predstavljen v svojem sklopu.

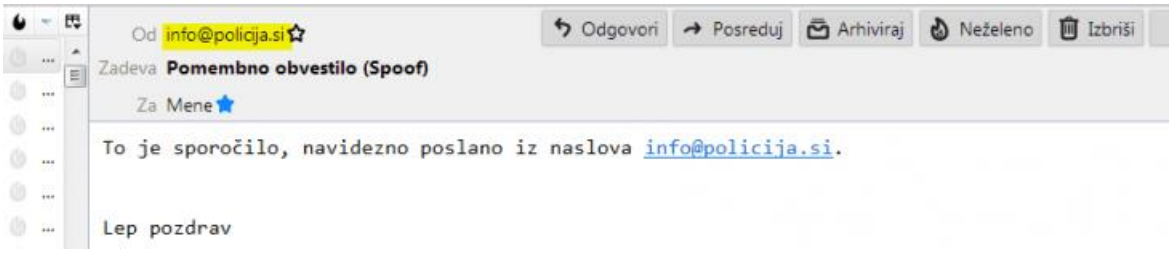
2.1 Napad s pomočjo socialnega inženiringa

Kibernetski napadi s pomočjo socialnega inženiringa (kratko socialni inženiring) so najbolj široka, znana in pogosta oblika vdiranja v podjetja. Delujejo na principu izkoriščanja človeškega elementa v verigi varnosti. Znan rek namreč narekuje, da je najbolj variabilen in tvegan člen v varnosti vedno človek, zato pa so napadi s pomočjo socialnega inženiringa največkrat tudi najbolj preprosti in uspešni. Ljudje imajo namreč razne potencialne subjektivne šibkosti, ki jih objektivni program ne vsebuje in jih je tako možno veliko lažje zlorabiti kot programe, ki se držijo napisane kode.

Načini zlorabe oseb so raznovrstni, po navadi pa ciljajo na emocionalne ali razumne šibkosti. Primer emocionalne zlorabe je primer prežanja na osamljene zaposlene, s katerimi pod lažno identiteto in krinko zainteresirane osebe storilec začne navezovati stike, kasneje pa s pomočjo pridobljenega zaupanja prične pridobivati kočljive informacije, ki jih žrtev sicer ne bi smela razkriti. Opisani način je v resnici sicer redkeje uporabljen, saj zahteva več dela v primerjavi z ostalimi tehnikami. Pod razumne šibkosti spada na primer strategija nujnosti hitrega odziva, ki nepoučeni ali nepazljivi osebi poda občutek nujne hitre reakcije in s tem zmanjša čas za primeren razmislek (podobna strategija je sicer vidna tudi pri raznih oglasih) (Webroot, brez datuma).

Na podlagi napisanega je zelo preprosta oblika socialnega inženiringa strategija »phising« oziroma ribarjenje, pri kateri se ustvari avtentičen videz nekega sporočila in njegovega pošiljatelja; lahko je od strank podjetja, zaposlenih, bližnjih … Tako se prejemnika prelisiči ali v razkritje kočljivih informacij ali pa v obisk lažne strani in prenos datoteke s prikritim virusom. Razlog za tako široko uporabo phisinga je predvsem nezahtevnost in statistična uspešnost, saj poleg nekaj osnovnih znanj phising ni zahteven za izvedbo, uspešnost pa temelji na šibkem členu v verigi varnosti – posamezniku. V primeru napada na podjetje storilec preprosto ustvari lažno avtentično sporočilo na podlagi informacij o podjetju in zaposlenih in čaka na odgovore oziroma prenose datoteke, okužene z virusom. Od tu tudi izvira ime – ribarjenje (angl. fishing). Tu je edini bolj zahtevni del prelisičenje filtra za nezaželeno pošto in zbiranje informacij o podjetju in zaposlenih, na podlagi katerih napadalec kasneje priredi sporočilo. Najbolj pogosti, in zato tudi najmanj nevarni, so redni phising e-maili, ki nimajo nobene resne zveze s podjetjem in so bili razposlani masovno. Večji problem za zaznavo pa so istovrstni e-maili, ki so bili prilagojeni glede na interne informacije o podjetju in poslani le specifičnim tarčam. V tem primeru se pošiljatelj zamaskira kot nekdo iz podjetja, oziroma nekdo, ki je s podjetjem povezan in posledično pozove zaposlene, naj naredijo nekaj, kar v primeru, da bi pošiljatelj bil resničen, niti ne bi bilo tako zelo nenavadno. Dober primer je poziv iz strani »tajnice« k ogledu novih vizitk (v okuženi datoteki na strani umetnega ponudnika) ali pa sporočilo »lastnika« tajnici, naj pošlje določeno vsoto na TRR račun ponarejenega ponudnika. Na spodnji sliki (Slika 2) je dobro vidna učinkovitost zamaskiranja pravega pošiljatelja v poljubni ciljni e-mail naslov. Na ta način pridobljeni podatki oziroma prenesen virus služijo kot neke vrste vdor (angl. breach) v sistem, na podlagi katerega se kasneje naredi škoda. V opisanih primerih, torej kadar je tarča bolj specifična in je zato napad njej bolj prilagojen, se tej strategiji lahko reče tudi spear phising oziroma ribarjenje s sulico (Phising, brez datuma).

Slika 2: Primer ponarejenega e-maila



Vir: Domenca (2019).

Spear phising zaradi svojega osredotočenja na specifično tarčo vsebuje tudi nekaj ostalih strategij, ki se sicer izvajajo tudi posamezno in jih je zato smiselno opredeliti. Med njimi je vabljenje (angl. baiting), kjer napadalci s pomočjo lažnih obljub o na primer zastonj programski opremi poskušajo prelisičiti tarčo v prenos datotek ali pa izdajanje informacij. Sledita strategija pretvarjanja, torej uporaba lažne, osebi relevantne identitete in strategija vodnjaka (angl. watering hole), kjer napadalci ponaredijo relevantno stran, na kateri oseba po navadi vpiše določene ključne informacije ali pa prenaša datoteke. Osnovni primer uporabe vodnjaka so lažne vpisne strani raznih socialnih omrežij ali e-mail ponudnikov. Dodatna težava pri tej vrsti zlorabe je posameznikova uporaba enakega gesla na več spletnih straneh, kar v zelo veliki večini pomeni le eno ali dve gesli za celoten spekter storitev, ki jih oseba uporablja, kar pomeni, da napadalec s pridobitvijo enega gesla potencialno lahko povzroči škodo na več računih (Bolland, brez datuma).

V primeru večjega zanimanja za podjetje lahko napadalci denimo pridejo tudi fizično v podjetje in poskusijo svojo srečo z uporabo strategije »tailgating«, pri kateri počakajo, da nekdo izstopi iz podjetja. Takrat napadalec pridrži vrata in vstopi v podjetje. V podjetju ima več možnosti. Najbolj pogosti sta iskanje odklenjenih računalnikov in nastavljanje vab v obliki »izgubljenih« USB ključkov.

Lahko se zgodi, da napadalec pod pretvezo nekoga iz podjetja ali naročenega izvajalca poskuša najti delovno mesto z računalnikom, ki ga zadolžena oseba ni zaklenila. V tem primeru se nadaljnja škoda lahko obravnava kot notranji napad, ki je podrobneje razložen v poglavju 2.3 (CyberTalk, 2021).

V primeru nastavljanja vab v obliki »izgubljenih« USB ključkov (angl. USB key drop) napadalec na ključnih mestih odvrže predhodno okuženi USB ključek. Na videz je ključek podoben predmetom podjetja ali pa ključku, ki bi ga lahko uporabljal kdo od zaposlenih. Namen vab je, da zaposleni USB ključek ob zapaženju vzamejo in vstavijo v svoj računalnik, z namenom identifikacije lastnika ali pa uporabe za svoje namene. Na USB ključku so lahko razni kodirni ali vohunski virusi, ena izmed bolj slavnih pa je aplikacija, ki ali beleži vse pritiske tipk in tako tudi vse uporabniške račune in gesla ali pa se v računalnik registrira kot pomožna tipkovnica in nato skozi pritiske določenih tipk izvede razne zlonamerne dejavnosti na okuženem računalniku. V primeru uporabe omenjenih

aplikacij napadalci USB ključke pogosto prikrito vstavljajo v zapuščene delovne postaje že sami (Talamantes, brez datuma).

2.2 Zunanji napad (Black box način preverjanja varnosti s penetracijskim testom)

Zunanji napad je definiran po obliki kot napad, pri katerem napadalec ne lasti internih podatkov podjetja, temveč uporablja le meta podatke, pridobljene na spletu. Napadalec je v tem primeru za sistem tujec in si prvotno ne lasti nobenih pravic pri upravljanju s sistemom. Kot ranljive in šibke točke se v tem primeru smatra zunanjo plast varovanj in vrat, ali z drugimi besedami »obzidje« sistema, ter razne naprave z brezžično povezavo. Primer izvedbe zunanjega napada je uporaba omenjenega iskalnika Shodan za pridobitev prvih informacij o napravah in sistemih podjetja. S pomočjo pridobljenih informacij o podjetju napadalec prične napad na način iskanja in izrabljanja pomanjkljivosti v sistemu. Napad se lahko zgodi preko spleta (na daljavo) ali pa iz neposredne bližine podjetja. V tem primeru napadalec poskuša priti v sistem preko lokalnih naprav, kot so na primer modemi za brezžično povezavo, uporabni pa so lahko tudi brezžični kopirni stroji. Zunanji napad je v večini primerov tudi predhodni in tako uvodni korak za posledični notranji napad (Imperva, brez datuma).

2.3 Notranji napad (White box način preverjanja varnosti)

V primeru notranjega napada se je napadalec že vključil v sistem kot uporabnik in ne tujec, kar pomeni, da že ima oziroma bo pridobil dostop do določenega števila internih informacij. Kot uporabnik ima že določene pravice, zato se tej vrsti napada tudi reče notranji napad. Tu zunanje varnostne sheme nimajo več večjega pomena, saj je napadalec iz strani sistema že identificiran kot uporabnik, kar pomeni, da je zunanji sistem varnosti že bil ali pretentan ali zaobiden. Tu se kot šibke točke smatra sistem pravic med uporabniki sistema, torej koliko škode lahko uporabnik naredi sistemu iz svoje delovne postaje in koliko omejitev in števil avtorizacijskih zahtev bo omejevalo delo škodoželjnega uporabnika, preden le ta povzroči večjo škodo. Tu so avtorizacijske omejitve lahko izvedene iz strani sistema in zaposlenih. Kot notranji napad se ne smatra le napade, izvedene na daljavo oziroma preko spleta, ampak tudi, kadar napadalec fizično pridobi dostop do notranjega sistema preko ene izmed naprav v podjetju. Kot že omenjeno v poglavju 2.1, se ena izmed strategij fizičnega vdora v podjetje imenuje tailgating (Imperva, brez datuma).

2.4 GDPR

Splošna uredba Evropske unije o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR) je uredba, ki je pogosto uporabljena pri splošnem vprašanju kibernetske varnosti. V uporabo je stopila 25. maja 2018, zavzema pa vsa pravila

in zahteve glede varstva osebnih podatkov. Stari predpisi so bili že dokaj zastarani in niso imeli zadostnega obsega za pravilno varovanje osebnih podatkov. S tem so ovirali digitalno rast, kar je povzročilo nezaupanje v varnost in zasebnost na spletu (IPRS, brez datuma).

Dodaten velik problem je bil in še danes je »puščanje« (angl. leaking) osebnih informacij iz strani korporacij in nato uporaba skupka teh in drugih informacij, imenovanih vele podatki (angl. Big data), v namene lastne dodatne koristi. Velepodatki so po definiciji izredno velike zbirke podatkov, ki jih je mogoče računalniško analizirati, da bi razkrili vzorce, trende in povezave, zlasti v zvezi z vedenjem in interakcijami med ljudmi. Oseba s tem na spletu izgubi zasebnost, saj lahko skozi algoritme in analize podjetje izve o osebi mnogo več, kot je vidno iz prve roke. Primeri tega so uporaba informacij in rezultatov analiz vele podatkov v namene vrednotenja zavarovanja, vrednotenja prošenj za zaposlitev, pretehtanja glede izdaje posojila ipd. S tem se zmanjšuje uporaba spletnih storitev, saj uporabniki zaradi skrbi pred omenjenimi analizami začenjajo izvajati tako imenovano samocenzuro (Social Cooling, brez datuma).

Ob vsem omenjenem pa je seveda primarna težava kršenje zasebnosti in razkrivanje zasebnih informacij, ki jih je posameznik določeni organizaciji zaupal v pričakovanju odgovornosti te organizacije do primerne obravnave prejetih podatkov

Podjetja so ob navedenem zatorej strogo odgovorna za pravilno skladiščenje in varovanje osebnih podatkov. V našem primeru so to podatki zaposlenih. Kazni so hude, regulacija pa prav tako ne pušča veliko prostora, zato organizacije, še posebej tiste, ki imajo bolj občutljive osebne podatke ali osebne podatke v večjih količinah (bolnišnice, odvetniške pisarne, hoteli ipd.), še posebej strogo skrbijo za redno skladnost z uredbo in tako tudi za varnost podatkov, saj so zaradi podatkov, ki jih hranijo, še toliko bolj pogoste tarče istovrstnih napadov (Smart Com d. o. o., 2019).

Podjetja imajo tako zaradi stroge uredbe in tudi na sploh odgovornosti do skladiščenja in varovanja osebnih informacij dodatno šibko točko, ki jo napadalci redno poskušajo izkoristiti. Napad v tem primeru zavzema vdor v kočljive podatkovne baze podjetja in nato izsiljevanje v smislu zahtevanega plačila v zameno, da osebni podatki niso javno objavljeni. V tem primeru podjetje nima veliko izbire, saj če so podatki zares bili ukradeni in bodo objavljeni, jim hude finančne posledice ne uidejo, pojavi pa se tudi nezaupanje strank. Varnost in pravilno skladiščenje podatkov, še posebej osebnih, je torej ena izmed prioritet podjetij na področju informacijske varnosti (Smart Com d. o. o., 2019).

3 OPIS IZBRANEGA PODJETJA

V tem sklopu so predstavljene osnovne ter relevantne informacije izbranega podjetja, torej informacije, ki so potrebne za analizo tveganj podjetja na področju informacijske varnosti.

Izbrano podjetje je bilo ustanovljeno že več kot 30 let nazaj in se specializira v proizvodnji strojev za obdelavo lesa. Brez upoštevanja kooperantov ima podjetje že prek 70 zaposlenih, število pa še vedno strmo raste. Prisotni so v več kot 40 državah, v tujini pa imajo že več kot 10 zastopnikov.

Njihova glavna registrirana dejavnost je kovinostrugarstvo; kmetijski in gozdarski stroji. Je torej proizvodno podjetje, kar pomeni, da je večina delovne sile zaposlena v proizvodnji in njej neposredno povezanih kadrih. Z leti podjetje še vedno strmo raste, kar zahteva širjenje tudi kadrov v upravi in tako povečanje števila uporabnikov računalniških naprav.

V podjetju je približno 30 % zaposlenih redno v stiku z računalnikom in s tem tudi potencialna tarča morebitnih kibernetskih napadov.

4 ISO 27001

V tej zaključni strokovni obravnavam izbrano podjetje na podlagi deleža osnovnih zahtev po ISO 20071 standardu. ISO 27001 je vodilni mednarodni sistem za upravljanje z informacijsko varnostjo, vpeljan iz strani Mednarodne organizacije za standardizacijo (angl. International Organization for Standardisation, v nadaljevanju ISO) v sodelovanju z Mednarodno komisijo za elektrotehniko (angl. International Electrotechnical Commision - IEC) (Advisera, brez datuma).

Podjetje poleg danes nujnih usmeritev za zaščito informacijskega sistema lahko ob izvedbi storitev in primerni dokumentaciji pridobi tudi ISO 27001 certifikat, s katerim izkaže partnerjem in ostalim podjetjem konkurenčni nivo svoje informacijske varnosti, ki je zadovoljiv na mednarodni ravni (ISO Standard SI, brez datuma).

Omenjeni standard je sestavljen je iz kombinacij politik in procesov za uporabo v podjetjih vseh velikosti in panog, deluje pa na sistematičen in nizko stroškoven način s pomočjo uporabe Sistema upravljanja informacijske varnosti (angl. information Security Management System, v nadaljevanju ISMS). Z drugimi besedami; ISO 27001 je mednarodno priznan standard, ki narekuje in opisuje primerno izvedbo strategije ISMS (Advisera, brez datuma).

ISMS je torej skupek zahtev oziroma korakov, ki jih podjetje izvede ob vzpostavljanju in vzdrževanju sistema za zaščito informacij (Advisera, brez datuma):

1. Identificiranje deležnikov in njihovih pričakovanj do podjetja v smislu informacijske varnosti.
2. Identificiranje tveganj.
3. Definiranje zaščitnih ukrepov za zmanjševanje tveganj z namenom izpolnitve opredeljenih pričakovanj.
4. Oblikovanje jasnih ciljev glede tega, kaj je potrebno doseči z ISMS.

5. Implementacija vseh zaščitnih ukrepov.
6. Konstantno spremljanje, ali izvedeni ukrepi delujejo v skladu s pričakovanji.
7. Nenehne izboljšave z namenom boljšega delovanja ISMS.

5 ISMS ANALIZA PODJETJA

V tem poglavju je delno izvedena omenjena ISMS analiza. Za namene odkritja osnovnih tveganj podjetja sem od korakov, naštetih v ISMS strategiji (poglavje 6), uporabil le teoretični del postopka, torej prve 4 korake.

5.1 Identificiranje deležnikov in njihovih pričakovanj do podjetja v smislu informacijske varnosti

Deležniki podjetja v smislu informacijske varnosti so vse pravne in fizične osebe, ki so tako ali drugače povezane s podjetjem in imajo določen interes za varovanje podatkov znotraj podjetja (Slavec Gomezel, 2021a, str. 35−37).

Deležnike sem zaradi uporabnosti in preglednosti razdelil v 2 skupini, in sicer v notranje in zunanje deležnike, torej v deležnike, ki so povezani s poslovanjem podjetja interno oziroma od znotraj ter deležnike, ki so povezani s poslovanjem podjetja in nanj vplivajo eksterno oziroma od zunaj. K vsaki skupini deležnikov sem dodal tudi obliko njihovih interesov do kibernetske informacijske varnosti v izbranem podjetju (Slavec Gomezel, 2021b, str. 14):

- Notranji deležniki:
  - lastniki (splošno),
  - zaposleni (osebni podatki, varnost transakcij).

- Zunanji deležniki:
  - stranke (podatki o poslovanju s podjetjem, kočljive notranje informacije ter varnost transakcij),
  - partnerji (podatki o poslovanju s podjetjem, kočljive notranje informacije ter varnost transakcij),
  - zastopniki (podatki o poslovanju s podjetjem, kočljive notranje informacije ter varnost transakcij),
  - vladne in nevladne organizacije (splošna varnost podjetij, varnost transakcij).

5.2 Identificiranje tveganj

Glavna tveganja, vezana na kibernetsko informacijsko varnost glede na identificirane deležnike, so torej naslednja:

- kraja osebnih podatkov (kršitev uredbe GDPR);
- ogrožena varnost transakcij med deležniki in podjetjem;
- ogrožena varnost notranjih informacij podjetja in deležnikov;
- ogrožena varnost zasebnega komuniciranja med podjetjem in deležniki.

Oblike napadov glede na podana tveganja se v podjetju kažejo kot izsiljevalski virusi (angl. ransomware), kodirni virusi, vdor v e-mail strežnik ter vdor v baze podatkov, še posebej baze osebnih podatkov (kršitev GDPR). V času pisanja naloge podjetje že začenja urejanje shranjevanja podatkov skladno z uredbo GDPR, zato bom ukrepe na tem področju le definiral na koncu naslednjega podpoglavja.

5.3 Definiranje zaščitnih ukrepov za zmanjševanje tveganj z namenom izpolnitve opredeljenih pričakovanj

V tem podpoglavju so definirani vsi relevantni zaščitni ukrepi, ki naj jih podjetje izpolni z namenom minimizacije tveganja kibernetskega vdora. V vsakem poglavju sem storitve ločil glede na izvedljivost, torej kaj naj podjetje naroči za izvedbo zunanjim izvajalcem in kaj lahko stori že samo. Z namenom boljše preglednosti in nadaljnje uporabnosti sem skladno z 2. poglavjem storitve primerno razvrstil po področjih varnosti sistema in podjetja nasploh.

5.3.1 Socialni inženiring

Glavni ukrep za zaščito pred napadi s pomočjo socialnega inženiringa so primerna izobraževanja v obliki delavnic, predavanj ipd., ki zaposlenim prikažejo čim več različnih uporabljenih načinov izkoriščanja oseb za pridobitev ključnih informacij.

Vsebina izobraževanj največkrat obsega večino možnih načinov uporabe socialnega inženiringa, med njimi pa so predvsem (Webroot, brez datuma):

- uporaba raznih e-mailov, ki pozivajo tarčo k urgentnim transakcijam oziroma prenosom datotek (phising);
- pošiljanje fiktivnih računov finančni službi;
- uporaba vabe s pomočjo (namerno) odvrženega okuženega USB ključka na kočljivih mestih v podjetju oziroma v njegovi bližini oziroma v bližini domov zaposlenih;
- tailgating, oziroma fizičen vdor v podjetje pod pretvezo zaposlene osebe oziroma izvajalca s pomočjo pridržanja vrat;
- emocionalno izkoriščanje.

Glavni cilj izobraževanj je zaposlenim prikazati enostavnost izvedbe raznih načinov istovrstnih napadov in kako hitro lahko oseba le tem podvrže.

Podjetju se z namenom povečanja pozornosti priporoča izvedba izobraževanja na temo socialnega inženiringa in nato delavnic z namenom vzdrževanja in nadgradnje znanja z intervali vsake pol leta oziroma najmanj enkrat na leto, in sicer s strani strokovnega izvajalca. Napadi s pomočjo socialnega inženiringa so namreč najbolj pogosta in tudi najbolj uspešna vrsta napadov na podjetja, kar pomeni, da je lastnike in zaposlene potrebno še posebej pogosto ozaveščati na nevarnosti, s katerimi se lahko dnevno soočajo. Po dogovoru z lastniki oziroma zastopniki podjetja se pred izvedbo delavnic izvaja tudi predhodne, zaposlenim nenapovedane preizkušnje ozaveščenosti zaposlenih; po navadi v obliki ponarejenega e-maila in lažne datoteke, v nekaterih primerih pa tudi v ostalih oblikah, naštetih zgoraj. Tako izvajalci pridobijo podlago za način izvedbe delavnic, torej tematična področja, ki zahtevajo več poudarka, potrebno dolžino delavnice in dolžino intervala izvedbe nadaljnjih delavnic, zaposleni pa na podlagi zelo verjetnega padca na preizkušnji pridobijo dokaj realno izkušnjo glede bolj kvalitetno izpeljanih napadov in zato delavnicam posledično tudi podrobneje prisluhnejo.

Na področju socialnega inženiringa je tudi nekaj osnovnih točk, ki jih lahko podjetje že pred izvajanjem delavnic in tečajev uvede samo. Omenil sem že strategiji tailgating in nastavljanje vab v obliki »izgubljenih« USB ključkov. Ti dve nevarnosti lahko podjetje minimizira že samo s strogo politiko uporabe USB ključkov in povečanjem pozornosti zaposlenih glede dovoljenih oseb v določenih oddelkih. Stroga politika uporabe USB ključkov največkrat narekuje popolno prepoved uporabe na službenih napravah, ne glede na namen. Obstajajo namreč tudi triki lažnih študentov ali splošnih iskalcev dela, ki pridejo na razgovor za službo in želijo v tajništvu natisniti svoj življenjepis, ki ga imajo na okuženem USB ključku. Povečanje pozornosti zaposlenih glede dovoljenih oseb je lahko uvedena varnost na vhodih ali pa zahtevanje za identifikacijo vseh novih oseb, ki se nahajajo v podjetju iz strani vseh ali nekaj zaposlenih. Osnovni primer je tudi uvedba identifikacijskih kartic ali čipov, ki omogočajo vstop v posamezne oddelke.

Dodatno naj podjetje uvede tudi obvezno zaklepanje računalnikov ob zapuščanju delovnega mesta ter dodatno časovno zaklepanje po določenem času neaktivnosti.

5.3.2 Zunanja varnost sistema

Podjetju se priporoča naročilo izvedbe storitev zunanjega sistemskega pregleda s penetracijskim testom (Black box metoda).

Podjetju se priporoča tudi nekaj osnovnih korakov na tem področju, ki jih lahko predhodno izvede že samo. Osnovni korak za zaščito zunanjega sloja sistema je predvsem poslovati na način, s katerim se pušča čim manjši digitalni odtis na internetu, kar pomeni, da podjetje javno ne objavlja nobenih informacij, ki niso nujno zahtevane za potrebno poslovanje. Izpolnjevanje raznih anket iz neznanih oziroma sumljivih spletnih ali telefonskih virov in anket, ki zahtevajo preveč informacij, se ne priporoča.

Preveriti je treba tudi vse brezžične povezave v podjetju in njihovo varnost. Varnost naprav je poleg uporabe primernih gesel odvisna tudi od njihove dejanske dotrajanosti in aktivne podpore, torej rednih posodobitev. Obstaja namreč veliko skritih forumov, kjer si hekerji izmenjujejo informacije o najdenih napakah na programski opremi naprav in kako jih izkoristiti v svoj prid. Ob neprimernih in zastaranih karakteristikah se podjetju priporoča menjava vseh takih naprav.

Dodatna poglavitna šibkost so tudi vrata IP, ki so mnogokrat lahko odprta tudi takrat, ko to ni potrebno, kar pomeni, da sprejemajo širši spekter prometa, kot je za njihov namen priporočljivo.

5.3.3 Notranja varnost sistema

Podjetju se priporoča naročilo izvedbe storitev notranjega varnostnega pregleda sistema (White box metoda).

Pri zaščiti notranjega dela sistema je tematika oziroma vprašanje: »Koliko škode lahko napadalec stori, če je že v sistemu?«. Vezano na vprašanje lahko podjetje samostojno predhodno preveri in primerno prilagodi vse pravice, dostopnosti in dovoljenja za spreminjanje informacij uporabnikov informacijskega sistema glede na njihova pooblastila in položaj v podjetju. Tako na primer razvojni oddelek ne bo imel dostopa do podatkov v računovodskem oddelku ali pa ne bo imel pravic za spreminjanje podatkov. Dodatno se za bolj kočljive spremembe informacij vpelje tudi zahteve po dodatni avtorizaciji, ki ni vezana na omenjeni informacijski sistem. Poleg naštetega se po potrebi vpelje tudi zahtevnejša gesla, ki se na določeno obdobje zamenjujejo, za bolj kočljive položaje pa se jih lahko menja tudi tedensko. Notranji vdor v sistem lahko namreč pomeni tudi napad s strani nekoga iz podjetja ali nekoga, ki je v podjetje prišel s pomočjo uporabe tailgating strategije.

5.3.4 Zaščita osebnih podatkov

Izbrano podjetje je to področje že predhodno uredilo, zato je navedeno le kot splošna informacija in ne kot potreben ukrep podjetja.

Kot že omenjeno je zaščita osebnih podatkov prav tako ključnega pomena za podjetja zaradi splošnih razlogov in zaradi regulative GDPR.

Podjetje mora podatke pravilno skladiščiti in jih tudi ustrezno varovati, saj so posledice v primeru dostopa do podatkov s strani nepooblaščene osebe finančno zelo težke, sledijo pa tudi posledice nezaupanja družbe do podjetja. Veliko, če ne tako rekoč vse, podjetje za varnost podatkov stori že z izvedbo ostalih naštetih storitev, vseeno pa mora samo poskrbeti tudi za primerno skladiščenje podatkov, in sicer v smislu primerne lokacije v zavarovanem informacijskem sistemu s smiselnimi omejitvami dostopa notranjih oseb, kar je sicer tudi že področje notranje varnosti. V primeru posamezne izvedbe, torej izvedbe brez ostalih

pregledov, lahko podjetje tudi najame zunanje strokovne izvajalce, specializirane na področju urejanja skladiščenja in varnosti podatkov v skladu z GDPR uredbo.

5.3.5 Povzetek

V spodnji tabeli (Tabela 1) sem z namenom boljše preglednosti povzel storitve, opisane v zgornjih podpoglavjih, ki se priporočajo izbranemu podjetju z namenom povečanja kibernetske varnosti podjetja.

Tabela 1: Povzetek vseh priporočenih storitev za povečanje kibernetske varnosti izbranega podjetja

Zunanja izvedba	Notranja izvedba
- Preizkušnja ozaveščenosti zaposlenih glede socialnega inženiriga - Delavnice na temo socialnega inženiringa - Zunanji varnostni pregled s penetracijskim testom - Notranji varnostni pregled	- Stroga politika uporabe USB ključkov - Povečanje varnosti glede oseb v podjetju - Zaklepanje računalnikov ob zapuščanju delovnega mesta - Minimiziranje digitalnega odtisa - Preverba (in potencialno menjava) vseh povezljivih naprav - Preverba IP vrat - Prilagoditev pravic in dostopnosti uporabnikov - Varnostna politika gesel

Vir: lastno delo.

5.3.6 Dodatne opombe

Ob vsakršnih večjih oziroma kočljivih spremembah informacijskega sistema se podjetju zelo priporoča naročilo ponovnega dodatnega zunanjega in notranjega varnostnega pregleda v izogib morebitnim nezakrpanim ali novo nastalim luknjam v varnosti.

Na vsakih nekaj let se priporoča tudi kolobarjenje s ponudniki storitev na področju kibernetske varnosti, kar pomeni, da se ponudnika vsakih nekaj let zamenja za novega. Smisel te metode je v razlikovanju strategije pregledov in razmišljanja med izvajalci, kar lahko pripelje do odkritja pomanjkljivosti v varnosti sistema, ki jih prejšnje podjetje, ki sicer ni nujno slabo izvajalo pregledov, ni opazilo.

5.3.7 Koristna orodja

Poleg že omenjenih priporočil, ki se nanašajo na način poslovanja, bom v tem sklopu preletel še nekaj koristnih in priporočenih orodij, ki jih lahko podjetje, ali pa tudi posamezniki, uporabijo za povečanje svoje varnosti na internetu.

Že omenjeni spletni brskalnik Shodan ni le orodje za kibernetski kriminal, ampak tudi zelo koristno orodje za dobronamerne uporabnike. Podjetje oziroma posamezniki lahko tudi sami vpogledajo, v kakšnem stanju so njihove povezljive naprave, njihovo verzijo programske

opreme, število odprtih vrat, ipd. Kar bi sicer napadalec lahko našel na tej strani, lahko podjetje oziroma posamezniki z nekaj znanja že predčasno poiščejo sami ter popravijo, preden se zgodijo morebitne nevšečnosti (Cyber Talents, brez datuma).

Dodatno zelo koristno orodje je tudi spletna stran haveibeenpwned.com, brskalnik, ki vsebuje e-maile iz vseh spletnih podatkovnih baz, ki so utrpele vdor in s tem morebitno razkritje gesel ali ostalih zasebnih informacij, povezanih z vpisom na spletno stran, s katero je bila baza povezana. Ob vpisu relevantnega e-maila nam brskalnik pokaže, ali je bil naš e-mail vpisan v kateri od vdrtih baz in nam v tem primeru spodaj te baze tudi našteje. Pod vsako od teh baz so navedene tudi vrste podatkov, ki so bile v tem primeru ogrožene, na primer uporabniško ime, geslo, varnostno vprašanje ipd. (https://haveibeenpwned.com/).

Ker se veliko vdorov zgodi tudi zaradi istega gesla na večih računih ali pa uporabe preveč enostavnih gesel, na primer »geslo123«, »123456«, »admin« itd., se priporoča uporaba novih gesel s simboli, številkami in velikimi črkami za vsak nov račun, ker pa si je taka gesla težko izmisliti, še težje pa zapomniti, se priporoča uporabo aplikacij za upravljanje z gesli. Te aplikacije gesla ne le po potrebi naključno generirajo, ampak si jih tudi zapomnijo ter jih varnostno zakodirajo. Uporaba interneta tako ni le varnejša, ampak tudi lažja (Malwarebytes, brez datuma).

5.4 Oblikovanje jasnih ciljev glede tega, kaj je potrebno doseči z ISMS

V tem podpoglavju in s tem 4. korakom strategije ISMS so z namenom boljše podlage za sanacije in priporočila opredeljeni osnovni varnostni cilji, ki jih ISMS v izbranem primeru zadeva.

Osnovni varnostni cilji ISMS glede na izbrano podjetje so (Advisera, brez datuma):

- zaupnost podatkov,
- integriteta podatkov,
- dostopnost podatkov;

ter dodatno:

- kibernetska ozaveščenost zaposlenih,
- kibernetska varnost zaposlenih.

Interni podatki morajo torej biti strogo varovani in dostopni le pooblaščenim osebam. Dodatno imajo le pooblaščene osebe pravico do spreminjanja podatkov, ki pa jim morajo biti ob pozivu vedno na voljo. Zaposleni morajo biti trajno ozaveščeni o kibernetski varnosti, znanje pa mora biti tudi redno osveženo in nadgrajeno glede na aktualne nevarnosti. Zaposleni morajo biti deležni določene dodatne napredne zaščite pred napadi, in sicer s pomočjo dodatnih varnostnih filtrov na svojih e-mail strežnikih.

6 OPREDELITEV TVEGANJ

V tem sklopu sem ob vsem napisanem povzel potencialne škode, ki grozijo izbranemu podjetju v primeru vdora v informacijski sistem, jih s pomočjo virov ovrednotil in prikazal primerjavo med potencialnimi izgubami v primeru vdora in stroškom izvedbe storitev kibernetske varnosti. S tem želim prikazati realno sliko in potencialno nujnost za vzdrževanje varnosti informacijskega sistema in rednega izvajanja zaščitnih ukrepov, z namenom ohranitve stabilnosti podjetja ter vzdrževanja varnega in nemotenega poslovanja. Tu je naloga toliko bolj osredotočena na karakteristike izbranega podjetja, vseeno pa je v dobri večini še vedno uporabna za primerjavo z ostalimi podjetji.

Kot omenjeno, podjetju grozijo predvsem nevarnosti na področju zastoja poslovanja, vdori v e-mail strežnike in kršenje GDPR uredbe oziroma v tem primeru kraja osebnih podatkov.

6.1 Opredelitev tveganj ob različnih vrstah napadov

6.1.1 Tveganje zastoja poslovanja (izsiljevalski ali kodirni virus − ransomware)

V primeru okužbe informacijskega sistema podjetja z izsiljevalskim virusom, torej virusom, ki zakodira podatke in v zameno za dekodiranje zahteva plačilo, je poslovanje podjetja ustavljeno le v približno 30 odstotkih, saj je glavni del podjetja proizvodnja, katere stroji niso povezani na splet, 30 odstotkov zaposlenih pa redno uporablja računalnik. Podjetje sicer že izvaja redno varnostno kopiranje podatkov na lokalno trdo shranjevalno enoto, tako da bi v primeru prejetja izsiljevalskega virusa doživelo le krajši zastoj v svojem poslovanju. Obnova celotnega sistema bi po ocenah odgovornih oseb v podjetju trajala približno en delovni dan, kar bi po priloženem izračunu (1) v škodi potencialno znašalo približno 20.000,00 € izgubljenih prihodkov (letni prihodki so leta 2021 znašali zaokroženih 24 milijonov €).

$$C = \frac{24.000.000}{365} * 0{,}3 = \ 19.726{,}03 \qquad (1)$$

6.1.2 Tveganje ob potencialni odtujitvi denarja (prestreganje e-mailov)

Z namenom prikritja poslovnih skrivnosti sem večino zneskov v podjetju zakril. Transakcije zavzemajo zelo raznolike vrednosti, zato sem za izbran primer vzel neki povprečni in z namenom prikritja zelo posplošen znesek, ki je še vedno primeren za prikaz splošne slike.

Ob odtujitvi denarja zaradi prestreganja e-mailov in spreminjanja podatkov oziroma lažnih mailov z drugačnim TRR računom (kar je v primeru prestreganja e-mailov najbolj pogosta strategija) bi v povprečju stroški oziroma škoda tako znašala 25.000,00 €, v vsakem primeru pa bi lahko bila seveda tudi mnogo višja.

6.1.3 Tveganje ob kršitvi GDPR

V primeru pridobitve osebnih podatkov zaposlenih s strani nepooblaščene osebe za nastalo škodo po 83. členu Uredbe (EU) 2016/679 kazensko odgovarja podjetje, in sicer za hujše kršitve v višini 4 odstotkov letnega prihodka oziroma 20 milijonov € (izbere se višji znesek), za lažje kršitve pa v višini 2 odstotkov letnega prihodka oziroma 10 milijonov € (izbere se višji znesek) (Uredba (EU) 2016/679, 2016).

6.1.4 Ostala škoda

Treba je omeniti, da podjetju zdaleč ne grozi le finančna škoda, ki jo je v večini primerov še mogoče pokriti. Dodatna škoda je lahko tudi razkritje osebnih podatkov v pravem pomenu besede, še posebej morebitne zdravstvene in pravne informacije, negativna publikacija v medijih in škodovanje dobremu imenu podjetja. Tako lahko podjetje v nadaljevanju izgubi poslovne priložnosti iz strani strank in/ali partnerjev in v tem primeru bi bila finančna škoda na dolgi rok še mnogo večja. Iz navedenih razlogov je tu potrebno izpostaviti tudi negotovost števila dejanskih primerov napadov v Sloveniji, saj se večina podjetij, če je to le možno, poskuša izogniti uradom in širši zunanji pomoči zaradi strahu pred javnim razkritjem napada na podjetje, saj bi to pomenilo še več deležnikov, katerim mora odgovarjati in na katere lahko novica negativno vpliva.

Iz zapisa lahko sklepamo, da je v resnici kibernetskih napadov na slovenska podjetja lahko mnogo več kot jih je prikazanih na uradnih straneh, kot na primer SI-CERT.

6.2 Stroški izvedbe storitev kibernetskega varnostnega pregleda, izobraževalnih tečajev in sanacij nepravilnosti

Povprečno skupno ceno pregledov za posamezna področja kibernetske varnosti podjetja sem v spodnji tabeli (Tabela 2) zaokrožil na znesek v višini 10.000,00 €, z namenom prikritja poslovnih skrivnosti na način, ki še vedno ustreza glavnemu namenu strokovne zaključne naloge. V dejanskem oblikovanju ponudbe so dejavniki za določanje cene dejavniki, kot so velikost podjetja, gospodarska panoga, delež zaposlenih, ki dela z računalniki ali ostalim napravami, povezljivimi na internet in skupek ostalih specifičnih tveganj. Stroški sanacije pomanjkljivosti in napak so odvisni od končnega poročila kibernetskega varnostnega pregleda in so tu ocenjeni le s simboličnim približkom.

Tabela 2: Posplošena povprečna cena storitev na področju kibernetske varnosti in izvedbe sanacij pomanjkljivosti

- Zunanji varnostni pregled s pen. testom (Black box)	€	4,500.00
- Notranji varnostni pregled (White box)	€	2,500.00
- Socialni inženiring	€	2,500.00
- Sanacija pomanjkljivosti	€	500.00
SKUPAJ	**€**	**10,000.00**

Vir: lastno delo.

Zunanji in notranji varnostni pregled se sicer v skupni izvedbi lahko obračunata tudi po nižji ceni, saj so določeni postopki v zunanjem pregledu enaki začetnim postopkom v notranjem. Z drugimi besedami, notranji pregled je v polnem pregledu običajna posledica zunanjega.

6.3 Primerjava tveganj ob vdoru s stroški varnostnega pregleda in sanacije pomanjkljivosti

Primerjava med tveganjem ob nepravilno oziroma pomanjkljivo zaščitenem informacijskem sistemu ter neozaveščenih zaposlenih glede nevarnosti socialnega inženiringa in stroških izvedbe pregledov, sanacije ter tečajev je za boljši pregled prikazana v spodnji tabeli (Tabela 3). Opomba: zneski so le splošni približek glede na predhodno analizo.

Tabela 3: Primerjava med potencialno, splošno približno škodo in stroški izvedbe storitev in sanacije glede kibernetske varnosti

	Škoda (povp. Znesek)	
Zakriptiranje podatkov	€	20,000.00
Prestreganje e-mailov	€	25,000.00
Kršitev GDPR	€	480,000.00

→

Minimalna škoda	€	20,000.00
Storitve in sanacija	€	10,000.00

Vir: lastno delo.

Iz tabele je vidno, da vsak potencialni tip vdora in škodovanja že samo v finančni škodi močno presega stroške izvedbe storitev glede kibernetske varnosti, ob upoštevanju vseh ostalih omenjenih posledic pa podjetju grozijo tudi nadaljnje sankcije in škode, torej škode, kot so škodovanje dobremu imenu, potencialna izguba strank, zastopnikov in morebiti tudi dobaviteljev. V najhujših primerih je pod vprašanjem tudi obstoj podjetja.

V vsakem pogledu se podjetju izplača izvesti navedene storitve, saj je škoda ob kakršnem koli načinu vdora in škodovanja že samo v obliki takojšnje škode hujša od stroškov storitev.

Dodatno se storitve zunanjega in notranjega pregleda izvedejo le enkrat in nato naprej ob vsaki večji oz. kočljivi spremembi sistema oziroma enkrat na 1 ali 2 leti, preverjanja in ozaveščanja glede socialnega inženiringa pa se nadaljnjo izvajajo v manjšem obsegu, kot je

potrebno ob prvi izvedbi, kar pomeni, da so letni stroški izvajanja storitev na področju kibernetske varnosti v naslednjih letih še mnogo nižji. Razlog za navedena dejstva je dejstvo, da so stroški izvedbe storitev znani, so mnogo nižji vsa naslednja leta, v vsakem primeru nižji od izgub ob kibernetskih napadih oziroma vdorih, ob njih pa podjetje pridobi tudi korist dobro zaščitenega sistema, izgube ob vdorih pa niso enkratne oziroma letne, temveč se bodo pojavile ob vsakem napadu, dokler na koncu podjetje ne bo prav tako izvedlo storitev kibernetske varnosti. Splošno imajo podjetja, ki so kibernetski napad že doživela in sistema niso sanirala, večjo možnost doživetja novega in hujšega napada, kot podjetja, ki napada še niso doživela ali pa so storitve kibernetske varnosti že izvedla. Razlogi za to so mnogi, glavni pa je izmenjava in uporaba informacij o šibkostih informacijskega sistema podjetja med napadalci ali pa ponovni napad s strani istih napadalcev na podlagi preteklih pridobljenih informacij o sistemu.

Omeniti je sicer treba, da informacijski sistem povprečnega podjetja nikoli ni 100-odstotno varen in zaposleni nikoli ne bodo zmožni opaziti in obraniti se vseh napadov, ki so jih lahko deležni. Namen kibernetske varnosti za povprečna podjetja je predvsem odvračanje napadalcev, da si bodo raje izbrali druga »vhodna vrata«, saj bi z »vrati« izbranega podjetja ali preveč tvegali ali pa izgubili preveč časa (več o teoriji vrat v 1. poglavju). Z drugimi besedami se povprečnim podjetjem s ponujenimi storitvami na področju kibernetske varnosti ne ponudi neprebojna varnost, kot na primer v vojaških centrih in obveščevalnih službah, ampak neki nivo varnosti, pri katerem se možnost vdora napadalcem, ki nimajo resnejše želje po specifičnem podjetju, dovolj zmanjša, da se jim poskušanje ne zdi več vredno časa in tveganja in tako poskusijo pri ostalih tarčah, kar je za povprečno podjetje stroškovno in na sploh veliko bolj smiselno.

7 VAVČERJI

Podjetje se lahko za izvedbo zunanjega in notranjega varnostnega pregleda tudi prijavi na razpis za vavčer za kibernetsko varnost. Dodatno se lahko za izvedbo delavnic na področju socialnega inženiringa podjetje prijavi na razpis za vavčer za dvig digitalnih kompetenc. Oba vavčerja sta ena izmed mnogih vavčerjev, ki jih razpisuje Slovenski podjetniški sklad, oziroma dva izmed štirih vavčerjev na področju digitalizacije poslovanja, ki jih dodatno organizira in vodi Digitalno inovacijsko stičišče Slovenije (v nadaljevanju DIH) (DIH, brez datuma).

Vavčerja za kibernetsko varnost in dvig digitalnih kompetenc sta izvedena v obliki sofinanciranja izvedbe istovrstnih storitev. Na razpis se lahko prijavijo mikro, mala in srednje velika podjetja, samostojni podjetniki in zadruge, ki imajo sedež v Republiki Sloveniji in imajo na dan oddaje vloge vsaj 1 zaposleno osebo (Slovenski podjetniški sklad, brez datuma).

Vavčerji so izvrstna priložnost, da podjetje še dodatno zmanjša stroške izvedbe storitev kibernetske varnosti in s tem še toliko izboljša razmerje med stroški in potencialnimi izgubami ob napadu. Več o posameznih zahtevah in načinu sofinanciranja v spodnjih podpoglavjih.

7.1 Vavčer za kibernetsko varnost

V vlogi za vavčer za kibernetsko varnost mora biti že naveden izbran strokovni izvajalec storitev kibernetske varnosti iz omenjenega kataloga, DIH pa mora predhodno tudi izdati pozitivno mnenje glede sofinanciranja izvedbe storitev (Slovenski podjetniški sklad, brez datuma).

Po odobritvi ima upravičenec največ 6 mesecev od podpisa pogodbe čas, da izvede vse odobrene aktivnosti, pri katerih je potrebno upoštevati minimalne zahteve oziroma smernice, ki so objavljene na spletni strani DIH. Poleg odobrenih aktivnosti je treba v istem roku oddati tudi strokovno poročilo, ki mora pridobiti pozitivno mnenje iz strani DIH, ob morebitni zavrnitvi poročila pa ima podjetje možnost enkratnega dopolnjevanja (DIH, brez datuma).

Vavčer nudi financiranje storitev sistemskega varnostnega pregleda in penetracijskih testiranj. V oblikah zunanjih in notranjih pregledov, ki sem jih navajal v tej strokovni zaključni nalogi, sta v večini primerov všteti obe obliki. Pri obeh storitvah Slovenski podjetniški sklad nudi sofinanciranje do 60 odstotkov stroškov, in sicer pri sistemskem varnostnem pregledu v višini do 5.000,00 € in penetracijskem testiranju do največ 9.999,99 € (DIH, brez datuma).

7.2 Vavčer za dvig digitalnih kompetenc

Vavčer za dvig digitalnih kompetenc ni toliko zahteven glede dokumentacije kot njegov sorodni vavčer za kibernetsko varnost. Po končanem usposabljanju mora izvajalec le oddati poročilo, listo prisotnosti in fotografijo usposabljanja, udeleženci pa izpolnijo vprašalnik z oceno zadovoljstva (DIH, brez datuma).

Financiranje znaša maksimalno 600,00 € subvencije na posameznega udeleženca, v skupni višini celotnega sofinanciranja do 9.999,00 € (DIH, brez datuma).

SKLEP

V zaključni strokovni nalogi sem si zadal nalogo opredeliti vrste in načine napadov ter jih primerno aplicirati na izbrano podjetje, z namenom prikaza nujnosti vzdrževanja kibernetske in občasno tudi fizične varnosti informacijskega sistema podjetja. Ob vseh opredelitvah vrst napadov sem prikazal tudi nekaj osnovnih metod varovanja pred njimi,

navedel pa sem tudi nekaj dodatnih relevantnih strategij in orodij, ki jih podjetja lahko uporabijo ali izvajajo sama. Glavni namen je torej bil ozaveščanje izbranega podjetja, splošnih podjetij in posameznika o nujnosti kibernetske varnosti za nemoteno in varno poslovanje, saj glede na številke, navedene v začetnih poglavjih, lahko z gotovostjo sklepamo, da ta tema še ni dovolj dobro obravnavana.

Metodi, uporabljeni za izdelavo zaključne strokovne naloge, sta bili teoretični, in sicer deskriptivna (opisna metoda) in kavzalna (neeksperimentalna) metoda. Z njima sem preko čitanja člankov in izvedbe pogovora z izbrano osebo prišel do želenih informacij in jih primerno uporabil v namen izdelave naloge.

Rezultati obravnave potencialnih izgub ob kibernetskih napadih napram izvedbi storitev kibernetske varnosti so bili večinoma dokaj pričakovani in tako tudi zadovoljivi, namreč že ob začetku izdelave naloge, in glede na pretekle osebne izkušnje na področju kibernetske varnosti informacijskih sistemov sem sklepal, da se že za srednje velika in tudi določena mala podjetja v vsakem primeru izplača izvedba omenjenih storitev, kajti obseg poslovanja in kočljivost podatkov se pri izbrani velikosti podjetja poveča že do te mere, da je skoraj ali že vsakršen napad dražji za podjetje kot izvedba vsaj osnovnih storitev z namenom preprečevanja vdorov in zagotavljanja varnosti. Kot omenjeno v zadnjem poglavju se storitve še toliko bolj splačajo ob uspešni pridobitvi vavčerjev iz strani DIH in Slovenskega podjetniškega sklada, ki stroške navedenih storitev dodatno zmanjšajo in tako nadaljnjo povečajo koristnost izvedbe.

Menim, da sem z vsebino naloge raznoliko in temeljito odgovoril na poglavitna vprašanja: »Kakšna so tveganja za podjetja in specifično za izbrano podjetje na področju kibernetske varnosti?«, »Kakšni so osnovni varnostni ukrepi in priporočila glede na opredeljena tveganja?« in »Kakšna je potencialna škoda v primerjavi s stroški implementacije boljše kibernetske varnosti informacijskega sistema?«. Podjetja in posameznik so ob celotni nalogi potencialno pridobili vsaj malo širša obzorja glede kibernetske varnosti in bodo pridobljeno znanje morebiti tudi uporabili za povečanje pozornosti glede istovrstnih groženj. Ob upoštevanju napotkov lahko tako podjetja varneje poslujejo brez večjih skrbi glede nepričakovanih napadov in škod.

LITERATURA IN VIRI

Railmonitor. (brez datuma). *Did you remember to lock your cyber-door?*. Pridobljeno 10. junija 2022 iz https://railmonitor.dk/did-you-remember-to-lock-your-cyber-door/

Cyber Talents. (brez datuma). *Shodan | The search engine for Hackers* [objava na blogu]. Pridobljeno 10. junija 2022 iz https://cybertalents.com/blog/shodan-the-search-engine-for-hackers

SI-CERT. (2021a, 27. december). *Hitri pregled leta 2021*. Pridobljeno 10. junija 2022 iz https://www.cert.si/hitri-pregled-leta-2021/

SI-CERT. (2021b, 27. december). *Število obravnavanih incidentov na SI-CERT po letih (z deležem phishing incidentov in projekcijo za 2021)*. Pridobljeno 10. junija 2022 iz https://www.cert.si/hitri-pregled-leta-2021/

Webroot. (brez datuma). *What is social engineering?*. Pridobljeno 11. junija 2022 iz https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Phising. (brez datuma). *What is Phising?*. Pridobljeno 11. junija 2022 iz https://www.phishing.org/what-is-phishing

Domenca. (2019, 28. februar). *Posnetek ponarejenega e-maila* [objava na blogu]. Pridobljeno 11. junija 2022 iz https://www.domenca.com/blog/2019/02/28/izsiljevalska-sporocila/

Bolland, E. (brez datuma). *Social Engineering Explained: Reduce Your Employee Cyber-Security Risk* [objava na blogu]. Pridobljeno 11. junija 2022 iz https://blog.usecure.io/employee-social-engineering

CyberTalk. (2021, 12. november). *What is tailgating and why it matters.* Pridobljeno 12. junija iz https://www.cybertalk.org/2021/11/12/tailgating-social-engineering-attacks-what-is-tailgating-and-why-it-matters/

Talamantes, J. (brez datuma). *USB Drop Attacks: The Danger Of "Lost And Found" Thumb Drives* [objava na blogu]. Pridobljeno 12. junija iz https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives

Imperva. (brez datuma a). *Black Box Testing*. Pridobljeno 12. junija 2022 iz https://www.imperva.com/learn/application-security/black-box-testing/

Imperva. (brez datuma b). *White Box Testing*. Pridobljeno 12. junija 2022 iz https://www.imperva.com/learn/application-security/white-box-testing/

IPRS. (brez datuma). *Reforma evropskega zakonodajnega okvira za varstvo osebnih podatkov*. Pridobljeno 15. junija 2022 iz https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/

Social Cooling. (brez datuma). *Like oil leads to global warming... Data leads to social cooling*. Pridobljeno 17. junija 2022 iz https://www.socialcooling.com/

Smart Com d. o. o. (2019, 19. junij). *Kršitev varnosti (osebnih) podatkov.* Pridobljeno 17. junija 2022 iz https://www.smart-com.si/zloraba-ukradenih-podatkov/

ISO standard SI. (brez datuma). ISO 27001*: Sistem za upravljanje informacijske varnosti.* Pridobljeno 18. junija 2022 iz https://www.iso-standard.si/iso-27001/

Advisera. (brez datuma). *What is ISO 27001?*. Pridobljeno 18. junija 2022 iz https://advisera.com/27001academy/what-is-iso-27001/

Slavec Gomezel, A. (2021a). *Poslovno okolje podjetja – Uvod*. Ljubljana: Ekonomska fakulteta v Ljubljani.

Slavec Gomezel, A. (2021b). *Poslovno okolje podjetja – Družbena odgovornost podjetij*. Ljubljana: Ekonomska fakulteta v Ljubljani.

Uredba o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Uredba (EU) 2016/679 (24. 4. 2016). Pridobljeno 24. junija s https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679

Malwarebytes. (brez datuma). *What is a password manager?.* Pridobljeno 28. junija 2022 iz https://www.malwarebytes.com/what-is-password-manager

Digitalno inovacijsko stičišče Slovenije. (brez datuma). *Vavčer za kibernetsko varnost.* Pridobljeno 30. junija iz https://dihslovenia.si/vavcerji/vavcer-za-kibernetsko-varnost

Slovenski podjetniški sklad. (brez datuma). *Vavčer za kibernetsko varnost*. Pridobljeno 30. junija 2022 iz https://www.podjetniskisklad.si/vsebinska-podpora/vavcerski-sistemi/vavcer-za-kibernetsko-varnost/