VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

KIBERNETSKA VARNOST V PODJETJIH

Kandidat: Minej Pak

Vrsta študija: študent izrednega študija

Študijski program: Programsko Inženirstvo

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: dr. Robert Sedovšek

Lektorica: Ksenija Pečnik, prof. slov. jez.

Maribor, 2024

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Minej Pak sem avtor diplomskega dela z naslovom Kibernetska varnost v podjetjih, ki sem ga napisal pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli kot moje lastne – kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, junij 2024 Podpis študenta:

ZAHVALA

Iskreno se zahvaljujem mentorju mag. Dušanu Brglezu za vse nasvete in pomoč ter usmerjanje pri pisanju diplomskega dela. Zahvaljujem se tudi mentorju v podjetju Turtl, dr. Robertu Sedovšku. Prav tako gredo zahvale ostalim zaposlenim v podjetju Turtl, ki so mi iz prve roke podajali informacije, ki sem jih nujno potreboval med pisanjem diplomskega dela.

Posebej pa bi se rad zahvalil svoji partnerki, ki me je neprestano vzpodbujala in mi pomagala. Zahvala gre tudi ostalim družinskim članom, ki so mi stali ob strani in me motivirali, tudi ko mi je bilo najtežje.

Še enkrat hvala vsakemu posebej.

POVZETEK

V današnjem času je kibernetska varnost postala ena izmed nepogrešljivih stvari v podjetjih in nasploh na internetu. Dandanes skoraj ne obstaja več podjetje, ki se ne zanaša na vsaj neko vrsto tehnologije za opravljanje svojih dejavnosti. To je razlog, da je varovanje občutljivih podatkov in digitalnih sredstev postalo ključnega pomena.

Kibernetske grožnje se nenehno razvijajo ter postajajo vedno bolj napredne, posledično pa se podjetja težje obranijo pred takšnimi napadi. Posledice teh napadov so lahko katastrofalne in po navadi vključujejo finančne izgube in izgubo ugleda podjetja. Velika težava kibernetske varnosti v podjetjih je tudi širjenje dela na daljavo, kar je povečalo število napadov in posledično je za podjetja ključnega pomena, da zavarujejo celotno digitalno infrastrukturo in svoje delavce izobražujejo o praksah varnega dela na internetu. Vzpon računalništva v oblaku je omogočil večje udobje in prilagodljivost/prožnost, vendar pa je povzročil tudi več dela na področju varnosti podatkov in aplikacij v oblaku, saj je ta ključnega pomena za uspešno delovanje podjetja. Podjetja morajo zagotoviti pravilno konfiguriranje oblaka za varen dostop in uporabiti napredne rešitve za varnost v oblaku z namenom zaščite svojih digitalnih sredstev. Ob neprestanem razvoju kibernetskih napadov kriminalci uporabljajo vedno bolj sofisticirane tehnike, kot so ribarjenje (angl. Phishing), izsiljevalska programska oprema (angl. Ransomware), zlonamerna programska oprema (angl. Malware) ter druge vrste kibernetskih napadov. Podjetja morajo upoštevati tudi predpise, kot je Splošna uredba o varstvu podatkov (GDPR), saj njeno upoštevanje pripelje do večje varnosti podjetje pred kibernetskimi napadi. Istočasno pa ti predpisi pomenijo večjo odgovornost podjetja, saj morajo uskladiti svoje prakse kibernetske varnosti in varnost podatkov jemati izjemno resno, da se izognejo potencialnim pravnim ali finančnim posledicam zaradi neupoštevanja predpisov varovanja podatkov.

Velika večina podjetij iz teh razlogov izbere večplastni pristop h kibernetske varnosti, ki zajema sisteme za odkrivanje in preprečevanje vdorov, požarne zidove, šifriranje in konstantno usposabljanje svojih zaposlenih. Podjetja se poleg tega zanašajo tudi na sisteme za upravljanje varnostnih informacij ter dogodkov (SIEM) in napredne analitike, da lahko prepoznajo kibernetske grožnje v realnem času.

Ključne besede: kibernetika, kibernetski napad, varnost podatkov, podjetje, veliki podatki

ABSTRACT

Cybersecurity in Companies

In today's world, cybersecurity has become one of the indispensable elements in companies and on the internet in general. Nowadays, almost no company exists that doesn't rely on some form of technology to conduct its activities, and this is why protecting sensitive data and digital assets has become of paramount importance.

Cyber threats are constantly evolving and becoming increasingly sophisticated, making it more challenging for companies to defend against such attacks. The consequences of these attacks can be catastrophic, often involving financial losses and damage to the company's reputation. A significant challenge in corporate cybersecurity is the proliferation of remote work, which has increased the number of attacks. Therefore, it is crucial for companies to secure their entire digital infrastructure and educate their employees about safe internet practices. The rise of cloud computing has provided greater convenience and flexibility, but it also brings more responsibility regarding data and application security in the cloud. Proper cloud configuration for secure access and the use of advanced cloud security solutions are essential for protecting digital assets. In the constantly evolving landscape of cyberattacks, criminals employ increasingly sophisticated techniques such as phishing, ransomware, malware, and other types of cyberattacks. Companies must also comply with regulations like GDPR, as adherence to these regulations enhances their cybersecurity against cyberattacks. At the same time, these regulations impose greater responsibility on companies to align their cybersecurity practices and data security with a high level of seriousness to avoid potential legal or financial consequences resulting from non-compliance with data protection regulations.

For these reasons, the majority of companies adopt a multi-layered approach to cybersecurity, including intrusion detection and prevention systems, firewalls, encryption, and continuous employee training. Companies also rely on security information and event management (SIEM) systems and advanced analytics to identify cyber threats in real-time.

Keywords: Cybersecurity, Cyberattack, Data Security, Risk, Company, Big Data

KAZALO VSEBINE

1 UVOD 6

1.1 Opis področja in opredelitev problema 6
1.2 Namen, cilji in osnovne trditve 7
1.3 Predpostavke in omejitve 8
1.4 Uporabljene raziskovalne metode 8

2 KAJ JE KIBERNETSKA VARNOST 9

2.1 Definicija kibernetske varnosti 9
2.2 Definicija kibernetskega napada 10
2.3 Najpogostejše vrste kibernetskih napadov 10
2.3.1 Trojanski konj 10
2.3.2 Zlonamerna programska oprema 11
2.3.3 Ribarjenje (Phishing) 12
2.3.4 Izsiljevalsko programiranje (Ransomware) 13
2.3.5 Napadi z zavrnitvijo storitve (Denial of Service) 13
2.3.6 Napadi z vrivanjem SQL-stavkov (SQL Injection) 14
2.3.7 Napadi na gesla 15
2.4 Pomen varovanja podatkov in zasebnosti 15
2.4.1 Uporaba navideznega zasebnega omrežja 16
2.4.2 Uvedba večfaktorske avtentikacije 16
2.4.3 Redni varnostni pregledi in preizkušanje ranljivosti 16
2.4.4 Izdelava in izvajanje načrta za odziv na kibernetske incidente 17
2.5 Pravni okvir kibernetske varnosti 17
2.5.1 ISO 17
2.5.2 ISO 27001 18
2.5.3 ISO 31000:2018 19
2.5.4 Direktiva za varnost omrežij in informacij (NIS) 21
2.5.5 Direktiva za varnost omrežij in informacij (NIS 2) 22
2.5.6 Slovenija 23
2.5.7 Evropska unija 24

3 KIBERNETSKA VARNOST V PODJETJIH 26

3.1 Pomen kibernetske varnosti v podjetjih 26
3.2 Vloga zaposlenih, ki je lahko tarča kibernetskega napada 27
3.3 Sodelovanje s strokovnjaki za kibernetsko varnost 28

3.4 Učinkovitost varnostnih ukrepov v podjetjih 30
3.5 Prilagajanje podjetij novim tehnologijam v kontekstu kibernetske varnosti 31
4 PRIMERI KIBERNETSKIH NAPADOV NA PODJETJA 32
4.1 Opis kibernetskih napadov na podjetja 32
4.2 Ugotovitve o napadih na podjetja 32
4.3 Analiza učinkovitosti varnostnih ukrepov v primeru napadov na podjetja 33
5 VPLIV ANALITIKE VELIKIH PODATKOV NA KIBERNETSKO VARNOST .36
5.1 Definicija velikih podatkov 36
5.2 Prednosti analitike velikih podatkov 37
5.3 Prednosti in omejitve uporabe analitike velikih podatkov v kibernetski varnosti 38
5.3.1 Prednosti uporabe analitike velikih podatkov 38
5.3.2 Omejitve uporabe analitike velikih podatkov 38
5.4 Pomen analitike velikih podatkov za proaktivni pristop h kibernetski varnosti 40
6 PRIMER DOBRE PRAKSE 41
6.1 Opis primera dobre prakse v kibernetski varnosti 41
6.2 Analiza uspešnosti in učinkovitosti varnostnih ukrepov 43
6.2.1 Izobraževanje zaposlenih 43
6.2.2 Tehnični varnostni ukrepi 43
6.2.3 Varnost omrežja – varni Wi-Fi in požarni zidovi 44
6.2.4 Upravljanje dostopov – načelo najmanjših privilegijev 44
6.2.5 Priprava na incidente 44
6.2.6 Redni varnostni pregledi 45
6.2.7 Spodbujanje varnostne kulture 46
6.3 Priporočila za izboljšanje kibernetske varnosti v drugih podjetjih 46
7 SKLEP 48
8 VIRI IN LITERATURA 51

KAZALO SLIK

Slika 1: Kibernetska varnost 9
Slika 2: Zlonamerna programska oprema 11
Slika 3: Ribarjenje oziroma phishing 12
Slika 4: Napad vrivanja SQL-stavkov 14
Slika 5: Napadi na gesla 15
Slika 6: Kako deluje virtualno zasebno omrežje 16

SLIKA 7: MEDNARODNA ORGANIZACIJA ZA STANDARDIZACIJO 18
SLIKA 8: NAČELA – ISO 31000-2018 20
SLIKA 9: IZSTOPAJOČE ŠTEVILKE NAPADOV 26
SLIKA 10: ŠTIRINAJST ČLOVEŠKIH TVEGANJ 28
SLIKA 11: IZOBRAŽEVANJE NA PODROČJU KIBERNETSKE VARNOSTI 29
SLIKA 12: INCIDENTI SKOZI LETA 33
SLIKA 13: ČAS, KI JE POTREBEN, DA NAPADALEC UGOTOVI GESLO 34
SLIKA 14: METODE ZA PREPREČEVANJE KIBERNETSKIH NAPADOV 35
SLIKA 15: VELIKI PODATKI 36

SEZNAM KRATIC

EU – Evropska unija

ISO – Mednarodna organizacija za standardizacijo

IEC – Mednarodna komisija za elektrotehniko

VPN – virtualno zasebno omrežje

URSIV – Urad vlade Republike Slovenije za informacijsko varnost

ZInfV – Zakon o informacijski varnosti

RS – Državni zbor Republike Slovenije

GDPR – General Data Protection Regulation

SUVI – Sistem upravljanja z varnostjo informacij

NIS – Direktiva za varnost omrežij in informacij

1 UVOD

Za svoje diplomsko delo sem si želel izbrati tematiko, ki je vedno bolj aktualna, poučna, uporabna in zanimiva. Z mentorjem mag. Dušanom Brglezom sva se zato odločila za temo kibernetske varnosti v podjetjih, ki bo razsvetlila kompleksnost kibernetske varnosti. Ker sem zaposlen na področju informacijskih tehnologij, se mi zdi pomembno, da podrobno spoznam tudi kibernetsko varnost in njen pomen. V današnjem času, ki ga zaznamujeta nenehna rast in kompleksnost informacijskih tehnologij, je varovanje podatkov in omrežja postalo še bolj pomembno za normalno delovanje podjetij ter splošno uporabo interneta. Kibernetska varnost kot pomemben steber tega področja predstavlja sistematičen pristop k zaščiti informacijskih sistemov, omrežij in podatkov pred uničenjem, krajo ali nepooblaščenim dostopom. Z rastjo informacijskih tehnologij pa se nenehno razvijajo tudi kibernetske grožnje, ki postajajo vse bolj nevarne, saj se napadalci izredno hitro prilagajajo novim tehnologijam in odkrivajo ranljivosti v informacijskih sistemih, prek katerih lahko podjetjem povzročijo veliko škode. Posledično se podjetja soočajo z izzivi, kako učinkovito zaščiti svoje podatke in istočasno zagotoviti neprekinjeno delovanje svojih poslovnih procesov ter obdržati ugled podjetja. Dandanes se že praktično vse prestavlja na digitalno stran. Med drugim imamo že elektronske napotnice, e-davke, e-upravo ipd., zato je zelo pomembno, da se vse organizacije ustrezno pripravijo in zaščitijo pred grožnjami v svetu digitalizacije. Kot logično zanimivost naj omenim, da se po uradni statistiki število napadov veča in nikoli ne pada. Tako lahko tudi brez tehtnih napovedi pričakujemo še nadaljnjo rast incidentov. Vseeno pa naj bi se stanje v Evropi le nekoliko izboljševalo, saj je sprejela določene zakone in direktive, ki veljajo zlasti za kritično infrastrukturo države, s katerimi pa želijo na nek način prisiliti lastnike podjetij in organizacij, da poskušajo narediti nekaj na področju informacijske varnosti. Informacijska varnost je panoga, ki zahteva nekakšen strošek, vendar si danes poslovanja nekega podjetja brez dobro delujočega varnostnega sistema ne moremo predstavljati.

1.1 Opis področja in opredelitev problema

Za raziskovanje te tematike sem se odločil predvsem zato, ker sem zaposlen v podjetju, ki nudi spletne storitve, in se na tak način vsakodnevno ukvarjam s kibernetsko varnostjo znotraj našega podjetja, po drugi strani pa me ta tema tudi zelo zanima, saj je kibernetsko znanje v današnjem svetu nepogrešljivo in se želim iz tega diplomskega dela naučiti nekaj novega. Menim, da je kibernetska varnost vedno večji problem v današnjem digitalnem svetu, kjer je že skoraj vsaka

naprava na nek način povezana z internetom in je lahko tako lahka tarča kibernetskih napadov. Kibernetska varnost znotraj podjetji in organizacij je v zadnjem letu postala vroča tematika, saj se vsakodnevno dogajajo raznorazni kibernetski napadi na velika ter manjša podjetja, kar pa ne vpliva le na uporabnike storitev podjetja, temveč tudi na ugled podjetja in njegove zaposlene. Namen diplomskega dela je predvsem predstaviti ključne vidike kibernetske varnosti in analizirati njeno pomembnost ter vlogo v sodobnem poslovnem okolju. Kot zanimivost pa lahko omenim, da se je v zadnjem letu zgodilo preko 800.000 različnih kibernetskih napadov, kar pa samo še okrepi dejstvo, da mora vsako podjetje dodatno izobraževati svoje zaposlene o praksah informacijske varnosti ter pomenu tega za uspešno in varno opravljanje storitev podjetja. Problem pa vidim predvsem v pomanjkanju znanja na področju kibernetske varnosti večine zaposlenih v podjetjih in zanemarjanju njenih osnovnih konceptov.

1.2 Namen, cilji in osnovne trditve

Namen diplomskega dela je podrobneje proučiti pomen kibernetske varnosti v podjetjih zaradi naraščajoče grožnje kibernetskih napadov, prav tako pa se želim naučiti nekaj več o vrstah groženj, ki pretijo organizacijam in podjetjem. Proučim tudi vpliv zaposlenih v podjetju na kibernetsko varnost podjetja, istočasno pa raziščem, ali podjetja lahko na podlagi preverjanja in posodabljanja svojih varnostnih ukrepov in z ozaveščanjem zaposlenih o tveganju kibernetskih napadov izboljšajo svojo varnost in tako zanesljivo nudijo svoje storitve. Cilj se je torej predvsem dodatno podučiti o kibernetski varnosti, saj menim, da lahko najdem veliko novih in zanimivih informacij, ki mi bodo pomagale priti do dodatnega in uporabnega znanja, ki ga lahko uporabim tako v zasebnem življenju kot tudi med opravljanjem dela v podjetju.

Hipoteze:

1. **Izobraževanje zaposlenih o kibernetski varnosti in ozaveščanje o tveganjih kibernetskih napadov lahko zmanjšata tveganje za napade v podjetju.**
2. **Uporaba večplastne varnostne strategije, ki vključuje več različnih varnostnih ukrepov, zmanjšuje tveganje za uspešen kibernetski napad.**
3. **Podjetja, ki redno preverjajo in posodabljajo svoje varnostne ukrepe, so bolje pripravljena na kibernetske napade in imajo manjšo verjetnost za uspešen napad.**
4. **Uporaba analitike velikih podatkov (angl. Big Data) omogoča boljše odkrivanje in razumevanje vzorcev ter naprednih kibernetskih groženj, kar prispeva k proaktivnemu pristopu h kibernetski varnosti.**

1.3 Predpostavke in omejitve

Za izdelavo diplomskega dela sem želel opraviti intervju z zaposlenimi znotraj svojega podjetja ter opisati del varnostne strategije, ki jo uporabljamo. Vodstvo podjetja je zavrnilo mojo prošnjo, saj so ti podatki poslovna skrivnost in bi lahko povečali tveganje kibernetskega napada. Zaradi tega sem s pomočjo lastne raziskave in znanja poizkušal pridobiti čim več podatkov za uspešno pisanje diplomskega dela.

1.4 Uporabljene raziskovalne metode

Za izdelavo diplomskega dela sem uporabil predvsem lastno znanje, ki sem ga dopolnil s pomočjo raznih uporabnih internetnih strani in člankov, uporabil sem tudi zapiske, ki sem jih pridobil v času študija, nekaj informacij pa sem dobil tudi od podjetja Dhimahi, v katerem sem opravljal praktično izobraževanje. Glavni raziskovalni pristop je analiza podatkov o vplivu izobraževanja zaposlenih na kibernetsko varnost v podjetju in vplivu posodabljanja ter testiranja varnostnih ukrepov.

2 KAJ JE KIBERNETSKA VARNOST

2.1 Definicija kibernetske varnosti

Kibernetska varnost je zaščita sistemov, povezanih z internetom, kot so strojna oprema, programska oprema in podatki pred kibernetskimi grožnjami. Znana je tudi kot varnost informacijske tehnologije ali varnost elektronskih informacij. Kibernetska varnost zajema vrsto ukrepov, tehnologij in procesov, ki so namenjeni zagotavljanju zaupnosti, celovitosti in razpoložljivosti digitalnih informacij in virov. Cilj kibernetske varnosti je preprečevanje, zaznavanje ter odzivanje na raznorazne kibernetske grožnje, ki med drugim vključujejo zlonamerno programsko opremo, izsiljevalsko programsko opremo, krajo poslovne identitete in podobno. Področje kibernetske varnosti se neprestano razvija z namenom obravnavanja groženj v digitalnem okolju, v zadnjih letih pa opažamo velik porast števila kibernetskih napadov tako na podjetja kot na fizične osebe. S kibernetsko varnostjo odkrivamo ranljivosti informacijskih sistemov, preprečujemo vdore v sisteme in kibernetske grožnje, s tem pa se tudi dvigne splošna raven računalniške varnosti (Gillis, 2024).



Slika 1: Kibernetska varnost

Vir: (https://racunalniske-novice.com/sodobni-casi-in-kibernetska-varnost-2/)

2.2 Definicija kibernetskega napada

Kibernetski napad je nepooblaščen dostop oziroma vdor v informacijski sistem druge osebe ali organizacije z namenom uničenja, kraje, razkritja, onemogočanja ali pridobitve zaupnih podatkov. Kibernetski napad lahko izvede posameznik, skupina, družba ali celo organizacija. Oseba ali organizacija, ki izvaja napad, cilja predvsem na računalniške informacijske sisteme, računalniška omrežja in osebne računalniške naprave. Kibernetski napad lahko popolnoma spremeni ali uniči določen cilj z vdorom v želeni sistem. Napadi lahko segajo vse od namestitve vohunske programske opreme na računalnik do uničenja ciljnega podjetja. Kibernetski napadi postajajo vedno bolj izpopolnjeni in nevarnejši. Ker pa se tehnologija zelo hitro razvija, je vključena tudi v avtomobilsko industrijo, kar pa postaja tudi grožnja avtomobilom. Zaposleni morajo biti izredno previdni, kadar zasledijo nenavadne povezave ali na primer nenaden upad hitrosti interneta, kajti to je lahko opozorilni znak, ki bi moral zaposlene opozoriti, da to lahko kaže na možnost kibernetskega napada. Cilji kibernetskih napadov se z leti spreminjajo. Kot primer lahko izpostavim, da je bil namen napadov v preteklosti predvsem neko dokazovanje, kaj nekdo zna in česa je sposoben, za povrh vsega pa so se še javno izpostavili in na tak način tudi bahali. V današnjem času pa je namen napadov predvsem zaslužiti denar ali pa na primer tako imenovano sponzorirano hekanje s strani določenih držav, ki lahko tako pridobijo geopolitično korist. Ravno zato pa ne govorimo le o denarju kot takem, ampak napadalci lahko na kakršenkoli način izsiljujejo žrtev napada. Med najbolj znane hekerske organizacije spadajo Anonymous, Lazarus group, Fancy Bear, Crabanak in The Dark Overlord (b2.eu, 2022).

2.3 Najpogostejše vrste kibernetskih napadov

Glavni cilj kibernetskih napadov je poškodovati, odtujiti zaupne podatke ali na drug način oškodovati sisteme v poslovnem ali osebnem računalniškem omrežju. Za dosego tega poznamo več različnih vrst kibernetskih napadov. V nadaljevanju opišem najpogostejše kibernetske napade, njihov namen in njihov način delovanja ter kakšne posledice lahko imajo za podjetje, ki je bilo tarča kibernetskega napada.

2.3.1 Trojanski konj

Virus, poznan kot trojanski konj, svojo pot v sistem najde prek programa, ki se izdaja kot legitimen program, in v tem primeru hudo ogrozi kibernetsko varnost sistema. Da sploh pride

do tega, da se naš sistem okuži s trojanskim konjem, je v večini primerov potreben socialni inženiring, s katerim heker v legitimno programsko opremo skrije svojo zlonamerno kodo in s tem poskusi pridobiti dostop do sistema. V večini primerov se to zgodi, ko uporabnik prenese priponko, poslano v elektronskem sporočilu, in jo namesti na svoj sistem, nato zlonamerna programska koda izvede nalogo, za katero jo je napadalec zasnoval, in na tak način pridobi dostop do sistema, kar mu omogoči vohunjenje in krajo zaupnih podatkov. Če bi uporabnik v tem primeru imel na svojem sistemu kakovostno protivirusno opremo, bi ta najverjetneje zaznala zlonamerno programsko kodo in uporabnikov sistem obvarovala pred napadom (b2.eu, 2022), (varnost-it.si).

2.3.2 Zlonamerna programska oprema



Slika 2: Zlonamerna programska oprema

Vir: https://www.a7la-home.com/sl/what-is-malware/

Zlonamerna programska oprema je vsak zlonamerni program ali programska koda, ki je škodljiva za sisteme. Poznana je tudi pod izrazi, kot so sovražna, vsiljiva ali grda, njen edini namen je kraja, šifriranje, izbris, sprememba, odtujitev ali vohunjenje podatkov. Zlonamerna programska oprema lahko v sistem prodre na veliko različnih načinov, dva najpogostejša načina sta prek interneta ali elektronske pošte, brez katerih si dandanes ne predstavljamo življenja. Sistem si lahko okužimo z brskanjem po okuženih spletnih straneh, prenašanjem okuženih datotek, namestitvijo programa ali aplikacije od nezaupnih ponudnikov, odpiranjem priponke

v elektronski pošti in podobno. Brez kakovostnega protivirusnega sistema smo izredno izpostavljeni nevarnosti zlonamerne programske opreme (varnost-it.si), (b2.eu, 2022).

2.3.3 Ribarjenje (Phishing)

Ribarjenje (angl. Phishing) je ena od najpogostejših oblik kibernetskega napada, ki ga uvrščamo med socialni inženiring, pogosto pa se uporablja za krajo uporabniških podatkov, kot so na primer gesla, številke kreditnih kartic, naslov ter ostale zaupne informacije. Socialni inženiring sam po sebi temelji na grajenju odnosov z osebo (tarčo) in jo zavede s tem, da odpre priponko ali povezavo v prejetem elektronskem sporočilu, direktnem sporočilu ali kakšni drugi vrsti komunikacije prek spleta. Namestitev programa ali klik na povezavo lahko privede do namestitve zlonamerne programske opreme in napadalcu tako omogoča dostop do sistema uporabnika in vodi do vohunjenja, razkritja ter kraje zaupnih podatkov. Takšne vrste napadov lahko imajo uničujoče posledice. Za posameznike lahko to pomeni krajo sredstev, krajo identitete in nepooblaščene nakupe. Ribarjenje se pogosto uporablja tudi za vdore v organizacije prek zaposlenih tako, da je okužen njihov sistem ter sistem drugih zaposlenih znotraj enake organizacije. V tem primeru govorimo o napredni trajni grožnji ali APT. Organizacija, ki je žrtev tovrstnih napadov, običajno utrpi hude finančne izgube, zmanjša se ji tržni delež in na dolgi rok vodi do izgube ugleda ter zaupanja potrošnikov (b2.eu, 2022), (varnost-it.si).



Slika 3: Ribarjenje oziroma phishing

Vir: https://www.loginradius.com/blog/identity/phishing-for-identity/

2.3.4 Izsiljevalsko programiranje (Ransomware)

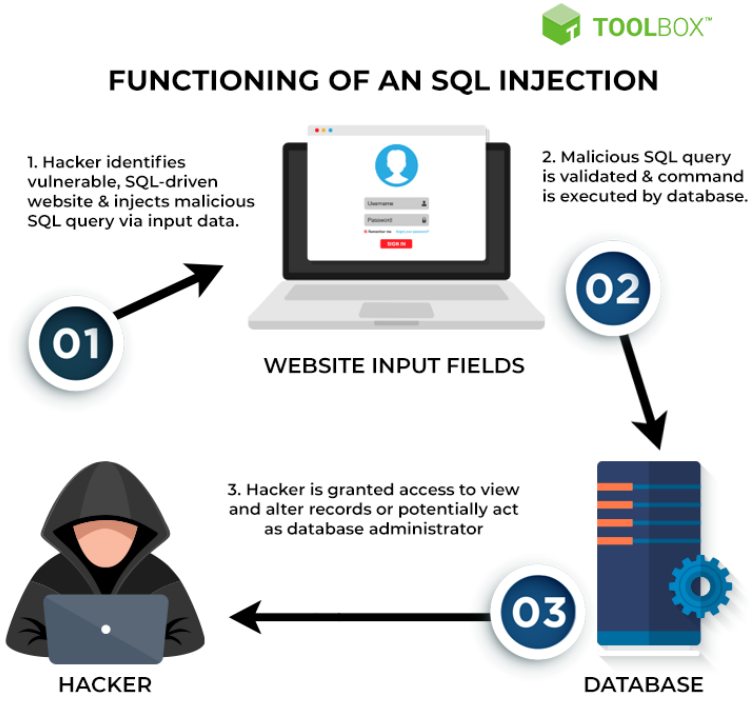
V zadnjih letih se je zelo dobro razvilo tako imenovano izsiljevalsko programiranje (angl. Ransomware), ki pa je le še ena od oblik zlonamerne programske opreme, ki s pomočjo šifriranja zahteva odkupnino od žrtve. Oseba, ki je bila žrtev napada, odpre prejeti dokument in ji na tak način z zlonamerno kodo zašifrirajo računalnik, nato pa od osebe zahtevajo odkupnino v zameno za ukradene podatke. Kriminalci so to tehniko v zadnjih treh do štirih letih razvili do potankosti. Njihov celoten sistem deluje dobro, zato so lahko čisto navadni uporabniki, v primeru da nimajo arhivske kopije teh podatkov, resno ogroženi, saj lahko podatke pridobijo nazaj le v primeru, če plačajo odkupnino v zahtevanem znesku. V takšnih primerih so ključne funkcije sistema šifrirane, saj na takšen način ne morejo dostopati do žrtvinih datotek, aplikacij ali podatkovnih zbirk, na katerih se nahajajo zaupni podatki. Če so tarča napada strežniki podatkovnih zbirk in datotek, se zlonamerna programska oprema razširi po celotnem omrežju in tako zelo hitro ohromi celotno organizacijo, ki je bila napadena. Kot sem že omenil, Ransomware v zadnjih letih velja za vse večjo grožnjo, ki kibernetskim kriminalcem prinaša ogromne zneske denarja. Tukaj gre za milijone ali pa celo milijarde evrov, istočasno pa podjetjem in vladnim ter drugim organizacijam povzroča veliko škode ter tako negativno vpliva na njihov ugled in zaupanje njihovih uporabnikov. Podjetja v večini primerov ravno zaradi takšnih groženj gledajo bolj dolgoročno in poskrbijo za varnostne kopije podatkov, hrkati pa tudi za varnostne mehanizme (b2.eu, 2022), (varnost-it.si).

2.3.5 Napadi z zavrnitvijo storitve (Denial of Service)

Napad z zavrnitvijo storitve (angl. Denial of Service attack) je vrsta napada, ki povzroči okvaro informacijskega sistema ali pa ga tako obremeni z informacijami, da ta ne more več učinkovito delovati. V večini primerov se napad izvede tako, da se sistem (večinoma strežniki) obremeni oziroma zasuje s prometom v takšnem obsegu, da ne zmorejo obdelati vseh zahtevkov in zaradi tega postanejo počasni, kar lahko vodi tudi do popolne neodzivnosti. To vrsto napada lahko napadalci izvedejo s pomočjo okuženih internetnih povezav, nad katerimi prevzamejo nadzor, temu pravimo »zombiji« (b2.eu, 2022), (varnost-it.si).

2.3.6 Napadi z vrivanjem SQL-stavkov (SQL Injection)

Napad z vrivanjem SQL-stavkov je napad na spletne aplikacije, iz katerega napadalci pridobijo vsebine podatkovnih baz. Napadalec v vnosno polje (obrazec na spletni aplikaciji) vnese zlonamerno kodo za manipulacijo baze podatkov v tako imenovanem Backendu (zaledju) spletne aplikacije z namenom, da bi pridobil dostop do zaupnih informacij, ki so shranjene v podatkovni bazi spletne aplikacije. V veliki večini primerov gre za podatke uporabnikov (b2.eu, 2022), (varnost-it.si).

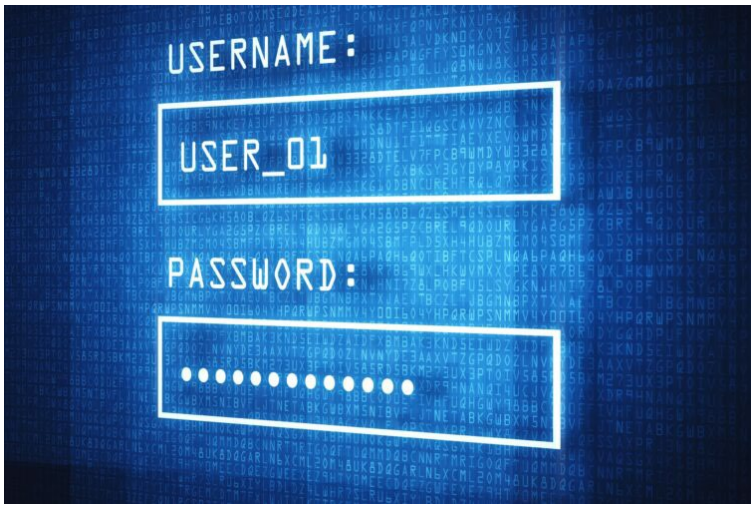


Slika 4: Napad vrivanja SQL-stavkov

Vir: https://www.spiceworks.com/it-security/application-security/articles/what-is-sql-injection/

2.3.7 Napadi na gesla

Kadar govorimo o napadih na gesla, poznamo več različnih vrst napadov, kot so napadi z grobo silo (angl. Brute force attack), napadi z mavričnimi tabelami, napadi z beležniki tipkanja itd. Največja problematika teh napadov je kompleksnost našega gesla. Kadar gre za primer napada z grobo silo, lahko ta razbije geslo samo v par sekundah, minutah ali urah, če imamo nastavljeno močnejše geslo z vsaj 12 znaki, velikimi in majhnimi črkami ter simboli, pa se količina časa, potrebnega za ugotovitev gesla, v takšnih napadih lahko zavleče v mesece, leta ali celo desetletja, kar pomeni, da je izvedba takšnega napada v tem primeru praktično nemogoča. Težava gesel je tudi v tem, da večina uporabnikov svojih gesel ne spreminja ali pa uporablja enako geslo za vse elektronske naslove, socialna omrežja, bančni račun itd. (b2.eu, 2022), (varnost-it.si).



Slika 5: Napadi na gesla

Vir: https://n1info.si/magazin/digitalno/dodatno-zascitite-gesla-pred-hekerskim-vdorom-posolite-jih/

2.4 Pomen varovanja podatkov in zasebnosti

Zaščita podatkov je izrednega pomena, sploh kadar govorimo o podjetjih. Vsako podjetje, ki želi delovati učinkovito, mora zagotoviti varnost svojih informacij v skladu z načrtom o varstvu podatkov. Z večanjem količine podatkov, ki jih shranjuje podjetje, pa narašča tudi pomen varstva podatkov. Kibernetski napadi lahko pri večjih količinah podatkov povzročijo nepopravljivo škodo in lahko vodijo celo do propada podjetja, zato morajo podjetja proaktivno zaščiti svoje podatke in redno posodabljati zaščitne ukrepe z vseh zornih kotov.

2.4.1 Uporaba navideznega zasebnega omrežja

Navidezno zasebno omrežje (angl. Virtual Private Network, v nadaljevanju VPN) je zasebno omrežje, katerega namen je uporabniku omogočiti varno in zasebno brskanje po spletu. VPN se največ uporabljajo v poslovnem svetu, vendar so se v zadnjih letih močno razširili tudi na širšo javnost. Tudi sam uporabljam VPN. Glavne prednosti VPN so šifriranje podatkov za večjo zasebnost na spletu, izogibanje lokacijskim omejitvam in uporaba javnega Wi-Fi omrežja, ki je brez uporabe VPN dandanes izredno tvegana.



Slika 6: Kako deluje virtualno zasebno omrežje

Vir: (https://community.fs.com/article/what-is-vpn-router-why-you-need-it.html)

2.4.2 Uvedba večfaktorske avtentikacije

Dvofaktorska avtentikacija nam omogoča, da poleg uporabniškega imena in gesla uporabimo še dodaten faktor avtentikacije. To so lahko gesla, enkratna koda, poslana prek SMS-sporočila, ali uporaba aplikacije za generiranje avtentikacijske kode, ki jo uporabnik priloži ob prijavi v aplikacijo.

2.4.3 Redni varnostni pregledi in preizkušanje ranljivosti

Redno preverjanje varnostnih rešitev in skeniranje omrežij ter aplikacij za odkrivanje morebitnih ranljivosti sta lahko izrednega pomena. Podjetja lahko za to najamejo strokovnjake,

ki preizkusijo njihov sistem ter najdejo potencialne ranljivosti, ki jih podjetje lahko potem tudi ustrezno odpravi. S tem si podjetje izboljša svojo varnost in bistveno zmanjša možnosti, da bi postalo tarča kibernetskega napada.

2.4.4 Izdelava in izvajanje načrta za odziv na kibernetske incidente

Podjetja si morajo pripraviti načrt, v katerem so jasno opisani postopki za obravnavo kibernetskih napadov, kako obvladati krizno situacijo ter kako obnoviti sisteme podjetja po napadu. S tem morajo biti seznanjeni vsi zaposleni, da ob potencialnem kibernetskem napadu vedo, kako postopati ter kako čim bolj omiliti posledice kibernetskega napada.

2.5 Pravni okvir kibernetske varnosti

Pravni okvir za kibernetsko varnost je ključnega pomena za zagotavljanje varnosti informacijskih sistemov in zaščito podatkov pred kibernetskimi grožnjami. Poleg zakonodaje je sodelovanje med državo in podjetji ključno za učinkovito obravnavo kibernetskih groženj. Slovenija sodeluje z drugimi članicami Evropske unije (v nadaljevanju EU) ter mednarodnimi organizacijami, kot je Interpol, za izmenjavo informacij o kibernetskih incidentih ter dobrih praksah zaščite pred njimi. Pravni okvir na ravni Slovenije in Evrope je v celoti oblikovan z namenom, da spodbuja varno upravljanje informacijskih sistemov in zaščito podatkov pred kibernetskimi grožnjami ter zagotavlja učinkovit odziv na morebitne incidente.

V nadaljevanju podrobneje predstavim pravni okvir kibernetske varnosti na ravni Slovenije ter Evropske unije in opišem standarda ISO 27001 in ISO 31000:2018 ter direktivi NIS in NIS 2.

2.5.1 ISO

Mednarodna organizacija za standardizacijo (v nadaljevanju ISO) je bila ustanovljena leta 1947, vanjo je vključenih preko 140 držav. Je neodvisen nevladni organ, ki združuje strokovnjake z namenom izmenjevanja informacij in razvijanja standardov. V času pisanja diplomskega dela je bilo v ISO 165 partnerskih držav, njen sedež pa je v Švici (Ženeva).

Dandanes so ti standardi mednarodno priznani in temeljijo na poenoteni terminologiji ter skrbijo za to, da je poslovanje na področju kakovosti, varnosti in zdravja pri delu ter ravnanja

z okoljem skladno. S pridobitvijo teh standardov je poslovanje podjetij lažje in bolj kakovostno (vsi.si), (sl.economy-pedia.com, 2024).



Slika 7: Mednarodna organizacija za standardizacijo

Vir: https://www.fdiworlddental.org/international-organization-standardization

2.5.2 ISO 27001

Standard ISO 27001 je vodilni mednarodni standard za izvajanje celovitega sistema za upravljanje informacijske varnosti. Z njim se predvsem prepoznava, ocenjuje in obvladuje tveganja, ki bi lahko nastala pri postopkih ravnanja z informacijami. Za podjetja je uporaben predvsem zato, ker je uvedba sistema upravljanja z varnostjo informacij (v nadaljevanju SUVI) v skladu s standardom predvsem strateška odločitev. Njegova uvedba v podjetju izboljša varnost, zmanjšuje obstoječa tveganja, zaposleni so bolj ozaveščeni, na koncu pa vse to privede tudi do večjega zadovoljstva strank. Še en pozitivni vidik pa je, da lahko s tem tudi večje organizacije, kot so na primer banke in zavarovalnice, pridobijo višjo raven zaupanja v podjetje, ki ima ta standard. Ta standard je namenjen prav vsem organizacijam in velja po vsem svetu, ne glede na to, kakšne vrste so, ne glede na velikost ali naravo dela, prav tako pa je namenjen tako javnemu kot tudi zasebnemu sektorju. Podjetjem vseh velikosti zagotavlja načrtovanje, spremljanje in izvajanje informacijske varnosti. Ta standard se še posebej priporoča organizacijam, ki pri svojem delu upravljajo z zelo zahtevnimi, inovativnimi in ključnimi procesi za obratovanje gospodarstva, ki mora ostati nemoteno, ali pa morajo obdelati izredno veliko količino občutljivih podatkov. Te organizacije so lahko na primer zdravstvene ustanove; državne in finančne institucije; medijske hiše; različna informacijska podjetja; podjetja s področja informacijsko-komunikacijskih tehnologij; podjetja, ki se ukvarjajo z oskrbo z

energijo, vodo in podobno. Bolj kot so podatki občutljivi in pomembnejšo vlogo kot ima informatika v delovnem procesu, bolj pomembno je, da te zaščitimo z omenjenim standardom. Z uporabo tega standarda se ohranja zaupnost, celovitost in razpoložljivost informacij (siq.si), (dqsglobal.com).

Podjetje mora za uspešno uvedbo standarda ISO/IEC 27001 skozi proces certificiranja, ki je sestavljen iz naslednjih korakov:

- opredelitev obsega certifikacije standarda,
- ocena in diagnoza trenutnega stanja podjetja glede na zahteve standarda,
- certifikacija v dveh fazah:
    - 1. faza – presoja stanja sistema vodenja z namenom, da se preveri, ali je organizacija pripravljena za certificiranje,
    - 2. faza – presoja implementacije zahtev, vključno z učinkovitostjo sistema vodenja znotraj podjetja.
- Po zadovoljivih rezultatih iz 2. faze certifikacije se izda certifikat, ki je veljaven 3 leta.

Po uspešni izdaji certifikata ta velja 3 leta, med veljavnostjo pa pride tudi do kontrolnih presoj z namenom preverjanja, ali sistem vodenja še vedno izpolnjuje vse zahteve standarda, istočasno pa spremlja tudi njegov napredek. Po pretečenih 3 letih po prvi izdaji certifikata pa je obvezno treba opraviti recertifikacijo, da se ponovno presodi skladnost in učinkovitost sistema v celoti (bureauveritas.si).

2.5.3 ISO 31000:2018

Mednarodni standard ISO 31000:2018 je standard, ki ga je izdala organizacija ISO. Standard opisuje smernice, načela in okvir z namenom obvladovanja tveganj v podjetjih ne glede na njihovo velikost, tip ali dejavnost, ki jo opravljajo. Cilj tega standarda je, da podjetjem pomaga razviti ustrezne strategije z namenom prepoznavanja, ocenjevanja in obvladovanja tveganj (tudi kibernetikih), s čimer lahko izboljšajo svoje ukrepe in posledično povečajo uspešnost poslovanja. Ta standard je sestavljen iz treh ključnih elementov:

1. **Načela obvladovanja tveganj:** standard jih vključuje v vse vidike organizacije; prilagodljivost pristopov obvladovanja tveganj, ki so specifični za potrebe organizacije; vključitev kulture tveganja in neprestano izboljševanje procesov obvladovanja tveganj.



Slika 8: Načela – ISO 31000-2018

Vir: https://cdn.standards.iteh.ai/samples/65694/5c27d980f52a42b394056c1f90ae5346/SIST-ISO-31000-2018.pdf

2. **Okvir obvladovanja tveganj:** standard poudarja pomen ustrezne vzpostavitve okvira z namenom vzdrževanja in podpore za obvladovanje tveganj. To vsebuje dodelitev odgovornosti, določitev politike obvladovanja tveganj in zagotavljanje virov za obvladovanje tveganj.
3. **Proces obvladovanja tveganj:** standard opisuje proces obvladovanja tveganj, ki pa vključuje identifikacijo tveganj, analizo tveganj, vrednotenje tveganj, obravnavo tveganj, spremljanje in pregled tveganj.

Kar se specifično tiče kibernetske varnosti v kontekstu obvladovanja tveganj po tem standardu, je kibernetska varnost zagotovo pomemben del širšega sistema obvladovanja kibernetskih tveganj. S pomočjo tega podjetja lahko:

- **identificirajo kibernetska tveganja:** podjetja lahko zaznajo potencialne kibernetske grožnje, kot so vdori v omrežje, zlonamerna programska oprema, phishing napadi ipd.;
- **analizirajo in ocenijo morebitna tveganja:** poskrbijo, da vsi zaposleni v podjetju razumejo verjetnost, pomen in vpliv kibernetskih tveganj na poslovanje in vtis podjetja;

- **obravnavajo kibernetska tveganja:** to lahko dosežejo tako, da razvijejo strategije, namenjene za zmanjšanje, izogibanje in prenašanje kibernetskih tveganj. To pa vključuje uvedbo dodatnih varnostnih ukrepov, kot so požarni zidovi, šifriranje podatkov, kreiranje kopij podatkov, izobraževanje zaposlenih ipd.;
- **spremljajo in pregledujejo varnostne ukrepe:** spremljanje in analiza učinkovitosti posameznih varnostnih ukrepov z namenom krepitve strategije za obvladovanje kibernetskih tveganj ter prilagajanje ustreznih varnostnih ukrepov.

Z uporabo standarda ISO 31000:2018 si lahko podjetje zmanjša verjetnost, da bi prišlo do kibernetskih incidentov. Če bi do incidenta kljub temu prišlo, pa podjetje lahko ustrezno ublaži posledice in izboljša svojo odpornost na vse kibernetske grožnje (cdn.standards.iteh.ai, 2018).

2.5.4 Direktiva za varnost omrežij in informacij (NIS)

Direktiva za varnost omrežij in informacij (angl. Network and Information Security, v nadaljevanju NIS) je na ravni celotne EU poenotila uredbe o kibernetski varnosti. Veljati je začela avgusta 2016. Vse države članice EU so takrat imele na voljo 21 mesecev za uspešno implementacijo direktive in še pet dodatnih mesecev za identifikacijo administratorjev kritične infrastrukture. Njen glavni namen je izboljšanje kibernetske varnosti v celotni EU. Direktiva določa pravila za varnost omrežij in informacijskih sistemov, ki so ključni za delovanje gospodarstva in družbe, ter krepi odpornost na kibernetske grožnje.

Ključni elementi direktive NIS so vključevali:

1. **Nacionalne strategije za kibernetsko varnost:** vse države članice so dolžne razviti nacionalne strategije za kibernetsko varnost, ki pa morajo vključevati ukrepe za zaščito kritičnih infrastrukturnih sistemov.
2. **Nacionalni organi za kibernetsko varnost:** vse države članice morajo prav tako ustanoviti nacionalni organ za kibernetsko varnost (v Sloveniji je to Urad vlade Republike Slovenije za informacijsko varnost, v nadaljevanju URSIV), ki je odgovoren za spremljanje izvajanja direktive in sodelovanje na ravni EU.
3. **Operaterji bistvenih storitev in ponudniki digitalnih storitev:** ta direktiva prav tako določa obveznosti za operaterje ključnih storitev (zdravstvo, energetika, bančništvo in

promet). Ti subjekti so dolžni sprejeti ustrezne tehnične in organizacijske ukrepe z namenom obvladovanja varnostnih tveganj in poročati o resnih incidentih.

4. **Sodelovanje in izmenjava informacij:** direktiva prav tako spodbuja sodelovanje in izmenjavo informacij znotraj držav članic EU z namenom izboljšanja odziva na kibernetske grožnje in incidente.

Direktiva NIS predstavlja pomemben korak k izboljšanju kibernetske varnosti v EU in krepitvi odpornosti proti kibernetskim grožnjam. Vredno pa je omeniti tudi to, da so bile vse države članice EU dolžne prenesti določbe direktive v svojo nacionalno zakonodajo do maja 2018 (cyberwiser, 2016).

2.5.5 Direktiva za varnost omrežij in informacij (NIS 2)

Direktiva NIS 2 je posodobitev in razširitev prvotne direktive NIS in je bila sprejeta z namenom, da bi se kibernetska varnost po vsej EU še dodatno izboljšala in okrepila. Ta direktiva je bila primarno predlagana zaradi vse večjih in naraščajočih kibernetskih groženj ter dodatne potrebe EU po izboljšanju varnosti omrežij in informacijskih sistemov.

Spremembe in novosti direktive NIS 2 so prinesle več pozitivnih sprememb, ki so ključnega pomena za zagotavljanje večje varnosti. Najprej bi rad omenil strožje varnostne zahteve, ki jih je direktiva uvedla za vse ponudnike ključnih storitev (zdravstvo, energetika, bančništvo in promet) in za vse ponudnike raznih digitalnih storitev. V sklopu teh sprememb morajo izvajati učinkovite ukrepe za upravljanje kibernetskih tveganj. Ti ukrepi vključujejo redne ocene tveganj, vzpostavitev učinkovitih postopkov za obvladovanje incidentov in izvajanje politik informacijskih varnosti. NIS 2 v primerjavi z NIS 1 pokriva še širši spekter sektorjev in entitet ter sedaj vključuje še javno upravo, ponudnike oblačnih storitev, podatkovne centre in kritične sektorje, kot so farmacija, proizvodnja hrane, kemična industrija, komunalne storitve ipd. V sklopu nove direktive se je izboljšalo tudi poročanje o kibernetskih incidentih s pomočjo uvedbe strožjih zahtev, predvsem kar se tiče časovnih okvirov za obveščanje pristojnih organov in delitve informacij s strankami, ki so bile prizadete zaradi nastalega kibernetskega napada. Poudarek se je dal tudi na izboljšanje kibernetske varnosti v celotnih dobavnih verigah, kar pa vključuje ocenjevanje in obvladovanje varnostnih tveganj, povezanih z dobavitelji in partnerji. Poleg vsega tega je direktiva NIS 2 uvedla strožje ukrepe za nadzor izvajanja kazni, kar pa vključuje višje kazni za neupoštevanje predpisov, ki so navedeni v direktivi. Tako kot prejšnja

direktiva, tudi posodobljena, še dodatno spodbuja tesnejše sodelovanje med državami članicami EU pri obvladovanju kibernetskih groženj in izmenjavi informacij. To vključuje vzpostavitev evropske mreže (EU-CyCLONE) za kibernetske varnostne incidente in krizne odzive.

Če povzamemo, direktiva NIS 2 kot celota predstavlja še en pomemben korak za EU, kar se tiče izboljšanja kibernetske varnosti. Zagotavlja še bolj robustne in dosledne ukrepe za zaščito ključnih omrežij in informacijskih sistemov v dandanes že skoraj čisto digitalizirani družbi, kjer nam pretijo raznorazne kibernetske grožnje (Unija, 2022), (siq.si, 2024).

2.5.6 Slovenija

2.5.6.1 Zakon o informacijski varnosti

V Sloveniji je ključnega pomena Zakon o informacijski varnosti (v nadaljevanju ZInfV), ki ga je 17. 4. 2018 sprejel Državni zbor Republike Slovenije (v nadaljevanju RS), za katerega je odgovorno Ministrstvo za javno upravo. Ta zakon ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežja in informacijskih sistemov RS, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah, ter zagotavlja bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v RS. ZInfV morajo spoštovati institucije, organizacije, ustanove in podjetja, ki so bistvenega pomena za nemoteno delovanje RS v vseh varnostnih razmerah, saj se le tako lahko ohranijo najpomembnejše gospodarske in družbene dejavnosti. »*Zakon te zavezance deli v tri kategorije:*

- *izvajalci bistvenih storitev,*
- *ponudniki digitalnih storitev,*
- *organi državne uprave.*«

(nil.com), (pisrs.si, 2018).

2.5.6.2 Nacionalni organ za informacijsko varnost

Urad Vlade RS za informacijsko varnost je pristojni nacionalni organ za to, ki deluje kot samostojna vladna služba. Na strateški ravni nacionalnega sistema urad deluje kot osrednji koordinacijski organ za zagotavljanje kibernetske varnosti, hkrati pa je tudi enotna kontaktna točka države pri mednarodnem sodelovanju na tem področju (gov.si, 2023).

2.5.6.3 Nacionalni odzivni center za kibernetsko varnost (SI-CERT)

V okviru akademske in raziskovalne mreže Slovenije naloge nacionalnega odzivnega centra za kibernetsko varnost opravlja Nacionalni odzivni center za kibernetsko varnost (v nadaljevanju SI-CERT).

»*SI-CERT izvaja program o ozaveščanju o kibernetski varnosti (Varni na internetu), ki je namenjen najširši slovenski javnosti, poseben sklop vsebin pa tudi malim podjetjem, obrtnikom in samostojnim podjetnikom. Cilji programa so:*

- *dvig stopnje zavedanja slovenskih spletnih uporabnikov o različnih nevarnostih, ki so jim izpostavljeni na internetu,*
- *informiranje o varni uporabi spletnega bančništva in varnem spletnem nakupovanju,*
- *informiranje o različnih oblikah spletnih goljufij in predstavitev načinov, kako se zavarovati,*
- *informiranje o varstvu osebne identitete*« (gov.si, 2023).

2.5.7 Evropska unija

EU ima številne zakone in direktive, ki obravnavajo področje kibernetske varnosti. Med njimi je Splošna uredba o varstvu podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR), ki določa zahteve za varstvo osebnih podatkov državljanov EU.

2.5.7.1 Splošna uredba o varstvu podatkov

Uredba GDPR določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o njihovem prenosu. GDPR prav tako varuje temeljne pravice in svoboščine posameznikov ter njihovo pravico do varstva osebnih podatkov. GDPR posebej navaja, da pretok osebnih podatkov v EU ne sme biti omejen ali prepovedan iz razlogov, povezanih z varstvom posameznikov pri obdelavi osebnih podatkov (gdpr-info.eu).

2.5.7.2 Direktiva o varnosti omrežij in informacij (NIS Directive)

Direktiva o varnosti omrežij in informacij je vseevropska zakonodaja o kibernetski varnosti, ki zagotavlja pravne ukrepe za povečanje splošne ravni kibernetske varnosti v EU. Pravila EU o kibernetski varnosti, ki so bila uvedena leta 2016, so bila posodobljena z direktivo o varnosti omrežij in informacij 2, ki je začela veljati leta 2023. Posodobila je obstoječi pravni okvir, da

bi sledil povečani digitalizaciji in spreminjajočim se razmeram, ki ogrožajo kibernetsko varnost.

Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v EU (Direktiva o varnosti omrežij in informacij 2) določa pravne ukrepe za povečanje splošne ravni kibernetske varnosti v EU z zagotavljanjem (digital-strategy.ec.europa.eu, 2023):

- pripravljenosti držav članic z zahtevo, da so ustrezno opremljene. Na primer s skupino za odzivanje na incidente na področju računalniške varnosti (CSIRT) in pristojnim nacionalnim organom za omrežja in informacijske sisteme (NIS);
- sodelovanja med vsemi državami članicami z ustanovitvijo skupine za sodelovanje, ki bo podpirala in olajšala strateško sodelovanje in izmenjavo informacij med državami članicami;
- kulture varnosti v vseh sektorjih, ki so bistveni za gospodarstvo in družbo ter so močno odvisni od IKT, kot so energetika, promet, voda, bančništvo, infrastrukture finančnih trgov, zdravstvo in digitalna infrastruktura.

3 KIBERNETSKA VARNOST V PODJETJIH

3.1 Pomen kibernetske varnosti v podjetjih

Podjetja se redno srečujejo z izzivi, kako učinkovito zaščititi podjetje pred kibernetskimi napadi, saj je varnost ključnega pomena za uspešno poslovanje. Z varovanjem, ki je uspešno, se ne varujejo le informacije in podatki, temveč se varuje tudi ugled podjetja, s tem pa se tudi ohranja zaupanje in zadovoljstvo strank, kar pa prinaša tudi uspešnost in rast podjetja.



Slika 9: Izstopajoče številke napadov

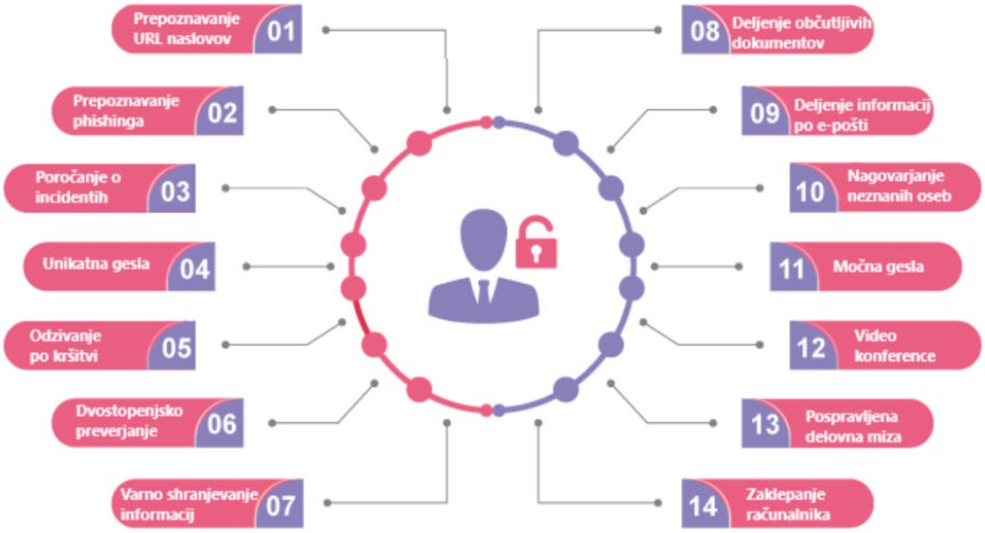
Vir: https://www.cert.si/wp-content/uploads/2024/05/2024-04-B-Arnes-letno-porocilo-izstopajoce-stevilke-2048x1024.jpg

Na spletu lahko zasledimo več primerov napadov na slovenska podjetja, ki so tudi podelila svoje izkušnje in na podlagi tega pojasnila, kako lahko poskrbimo za kibernetsko varnost. Ker se število kibernetskih napadov v zadnjem desetletju povečuje, se ne sprašujemo več, ali bodo podjetja napadena, temveč kdaj bodo napadena. Vsako peto podjetje je že bilo tarča napada in kar vsakih 39 sekund se zgodi kibernetski napad. Zavedati se moramo, da hekerji lahko podjetju obrnejo svet na glavo. Zelo velik izziv je zmanjševanje tveganj za kibernetske napade. Še posebej to velja dandanes, ko veliko zaposlenih opravlja svoje delo na daljavo, hkrati pa imajo zato odgovorni manjši nadzor nad delom zaposlenih in varnostjo naprav. Zaradi tega je izredno velikega pomena, da se zaposleni stalno izobražujejo na področju kibernetske varnosti. Zelo velik pomen imajo tudi redne in temeljite ocene tveganja, preverjanje kibernetske ranljivosti in spremljanje dogodkov po svetu. Kibernetski napadi lahko podjetja oškodujejo tudi za milijarde evrov in lahko povzročijo nepopravljivo škodo. Prav tako pa so lahko tarča tudi osebni podatki uporabnikov oziroma strank oškodovanega podjetja. Podjetje pa ne le, da ima finančno izgubo,

takšni napadi lahko podjetja stanejo tudi strank in predvsem ugleda. Da bi bilo podjetje uspešno pri upravljanju kibernetske varnosti, mora poskrbeti vodstvo. Poskrbljeno mora biti predvsem za varnost spletnih aplikacij, omrežja, podatke, procese, gesla in podobno. Pomembni so predvsem trije elementi – zaščita, zaznavanje in odziv v primeru incidenta. Največja prednost napadalcev pred podjetji je v tem, da imajo ti praktično neomejeno časa. Če se odločijo za napad, lahko to počnejo nekaj dni, en mesec, lahko pa tudi več let, če jim je tarča napada zanimiva. Podjetje lahko zato ne glede na stopnjo zaščite pričakuje, da bo napadalcem enkrat uspelo vdreti v informacijski sistem. Zato je zelo pomembno, da je podjetje sposobno poskus napada zaznati čimprej in se na koncu tudi pravilno odzvati in poskusiti kar se da omejiti morebitno škodo. Velika razlika je med tem, ali nam napadalci uničijo celoten informacijski sistem ali pa bo napad zelo izoliran in bo podjetje lahko normalno poslovalo še naprej. Do incidenta lahko pride kadarkoli, najbolj pomembno pa je predvsem to, da podjetje zna škodo omejiti, izolirati in ustrezno komunicirati.

3.2 Vloga zaposlenih, ki je lahko tarča kibernetskega napada

Kot sem že omenil, sta na prvem mestu predvsem izobraževanje in usposabljanje zaposlenih, saj njihova ravnanja najbolj vplivajo na varnost sistemov. Zaposleni morajo biti nujno opremljeni z znanjem na področju spopadanja z nevarnostmi, s katerimi se lahko med opravljanjem dela tudi soočijo. Nemalokrat pa se zgodi, da zaposleni zaupajo in verjamejo klicu ali sporočilu nekoga in mu tako na primer omogočijo dostop do orodij za oddaljen dostop. Kar 85–95 % kibernetskih vdorov se zgodi predvsem zaradi človeške napake. Praktično že skoraj vsak zaposleni pri svojem delu uporablja internet in tehnologijo, pri tam pa se velika večina ne zaveda tveganj, ki jih prinesejo tehnologije. Večina napadov temelji predvsem na družbenem inženiringu, ki pa ga lahko z znanjem učinkovito prepoznamo. Zaposleni velikokrat vedo, kaj morajo storiti v kritičnih trenutkih, pa vendar vseeno včasih ne ravnajo tako. Zavedajo se pravilnega ravnanja, vendar to še ne pomeni, da se bo to na koncu dejansko pravilno izvedlo. Na primer velika večina oziroma praktično vsi zaposleni vedo, da morajo uporabljati močna gesla, vendar je povprečna moč gesla v podjetjih še vedno prešibka. Zaradi tega moramo tudi poznati razliko med zavedanjem in vedenjem in se tako osredotočiti na izpolnjevanje obojega.



Slika 10: Štirinajst človeških tveganj

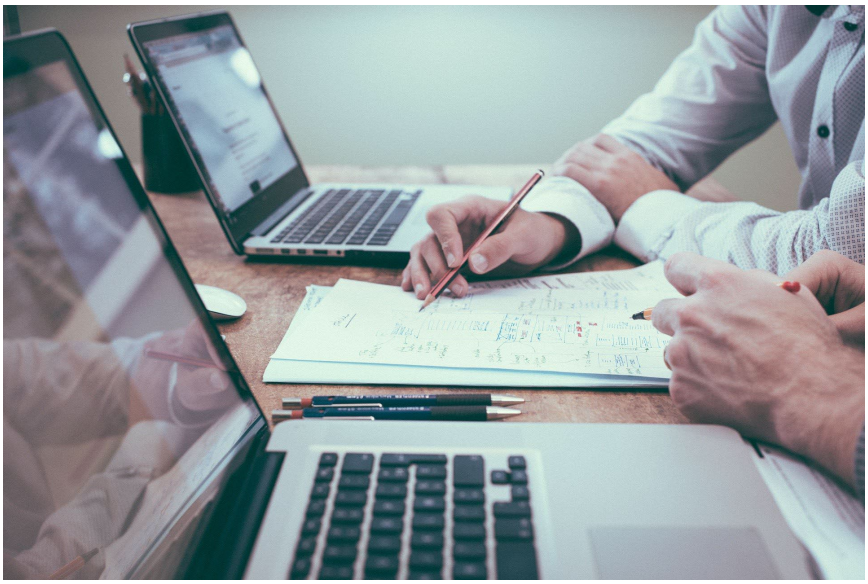
Vir: https://www.bureauveritas.si/magazine/zakaj-je-razvoj-kulture-kibernetske-varnosti-pomemben-za-vsako-organizacijo

Tako lahko namerno ali pa popolnoma nenamerno zaposleni v podjetju s svojim nepazljivim ravnanjem pogosto ogrozijo varnost svojega podjetja. Ko pride do napada, morajo zaposleni znati ukrepati na pravilen način glede na vrsto incidenta. Če se je na primer napad zgodil na nekem pomembnejšem strežniku, je pomembno, da se tega zelo omeji ali pa se ga celo popolnoma ugasne in na tak način preprečimo morebitno nadaljnjo škodo. Do največjega problema pa pride predvsem takrat, ko podjetje ne zazna, da je bilo kibernetsko napadeno. Zaradi tega je zelo pomembno, da ima podjetje pokrite vse vrste zaščite, še boljše pa je, da se to dopolnjuje s simuliranimi napadi (svetkapitala.delo.si, 2019), (bureauveritas.si, 2024).

3.3 Sodelovanje s strokovnjaki za kibernetsko varnost

Ker z razvojem tehnologije napredujejo načini, kako lahko to izkoristijo napadalci, je zelo pomembno, da podjetja sodelujejo tudi s strokovnjaki za kibernetsko varnost. Izzivi kibernetske varnosti so vedno bolj kompleksni, saj v znanju rastejo tudi napadalci, kar pa da podjetjem velik izziv. Ravno zato pa je nujno sodelovanje podjetja z zato usposobljenimi podjetji, ki ugotavljajo stanje odpornosti podjetja in kibernetskih tveganj glede na vrsto poslovnih interesov, hkrati pa pomagajo pripraviti kar se da optimalni program ukrepov. Pri tem pa je zelo pomembno, da se tega držijo vsi v podjetju, saj se lahko le tako zagotovi uspešnost ukrepov. Pomembno pa je

tudi, da sodelujejo strokovnjaki za kibernetsko varnost iz različnih držav, saj si lahko tako med seboj izmenjujejo pomembne informacije, ki so temelj za zagotavljanje informacijske varnosti in varovanja informacij. V primeru kompleksnejših sistemov ter s tem tudi varnostnih izzivov je smiselno sodelovati s strokovnjaki za kibernetsko varnost ali podjetji, ki so specializirana za kibernetsko varnost. Ta podjetja namreč nudijo specializirane storitve in rešitve in s podjetjem izdelajo varnostni načrt ter izvajajo tako imenovane penetracijske teste nad sistemom podjetja za odkrivanje pomanjkljivosti ter potencialnih lukenj v sistemu. Zavedati pa se moramo, da noben ukrep ni stoodstotno zagotovilo pred kibernetskimi napadi, vendar pa izvajanje kombinacije navedenih ukrepov lahko znatno zmanjša tveganje za kibernetski napad in omogoči hitrejši in natančnejši odziv v primeru incidentov.



Slika 11: Izobraževanje na področju kibernetske varnosti

Vir: https://www.carbonsec.com/sl/podjetje/zaposlitev/

Pomembno pa je tudi sodelovanje z etičnimi hekerji, ki se postavijo v vlogo napadalcev in na takšen način lahko simulirajo napad na podjetje. Za to pa imajo dovoljenje in tako na zakonit način vdrejo v varnostne sisteme podjetja. Tako poskušajo najti šibke točke in potem glede na ugotovitve napišejo tudi priporočila, kako zaščititi varnostne sisteme, nato pa jih še enkrat preverijo, ali so v redu ali pa so še prisotne kakšne pomanjkljivosti, ki jih je treba odpraviti (PR, 2024).

3.4 Učinkovitost varnostnih ukrepov v podjetjih

Da bi lahko odgovorno pristopili k zagotavljanju varnosti podjetja, je najprej pomemben ustrezen in dobro napisan načrt. Prav tako je treba analizirati informacijsko okolje, za srednje velika in večja podjetja pa je zelo dobro narediti tudi penetracijski test, pri katerem se ugotovijo morebitne pomanjkljivosti in kritične točke. Na podlagi vseh teh ugotovitev pa se lahko pripravi predlog za izboljšave. Izredno pomembno pri tem je tudi, da se preveri raven znanja zaposlenih, ki ga je treba redno preverjati in nadgrajevati, saj so zaposleni v večini primerov prva tarča spletnih prevar in napadalcem tako nevede omogočijo dostop v podjetje. Zaradi tega so res pomembna izobraževanja, v katera morajo biti vključeni vsi v podjetju, prav tako pa je treba redno preverjati varnostno zaščito podjetja. Učinkovitost ukrepov je lahko zelo dobra, če se podjetje odloči uporabiti kakovostno in najnovejšo zaščito, hkrati pa morajo svoje znanje izpopolniti tudi vsi zaposleni, saj je, kot že rečeno, najpogostejši razlog za vdor v sistem napaka oziroma nepozornost zaposlenih. Možnost napada bo vedno prisotna, saj nobena zaščita ni 100 %, z dobrim sistemom in znanjem pa se lahko možnost napada oziroma obseg napada kar precej zmanjša. Da bi lahko uspešno pristopili h kibernetski varnosti, morajo zaposleni upoštevati več načinov oziroma plasti zaščite. Ti so razporejeni po računalnikih, omrežjih, programih ali podatkih, ki jih podjetje namerava varovati. Zelo pomembno je, da se dopolnjujejo ljudje, procesi in obstoječa tehnologija, saj se podjetje lahko le tako učinkovito obrani pred morebitnimi kibernetskimi napadi. Bistvenega pomena je tehnologija, ki mora biti kakovostna in napredna, saj lahko le na tak način zagotovimo najvišjo stopnjo zaščite pred napadi organizacij ali posameznikov. Zaščitene morajo biti tri najbolj glavne entitete, to so računalniki, pametne naprave in usmerjevalniki; omrežja in oblak. Zelo pogosta tehnologija, ki se uporablja za njihovo zaščito, vključuje požarne zidove, filtriranje DNS, zaščito pred zlonamerno programsko opremo, protivirusno programsko opremo in varnostno zaščito za e-pošto. Trenutno na svetu obstaja veliko najrazličnejših vrst zaščit in orodij, ki imajo vsako različne funkcije in metode, vsemu temu orodju pa je skupno to, da prispevajo k varnosti podatkov, informacij in podjetja nasploh (Finance, 2024).

3.5 Prilagajanje podjetij novim tehnologijam v kontekstu kibernetske varnosti

Podjetja se morajo, če se želijo kar se da dobro zaščititi pred morebitnimi napadi, prilagajati najnovejšim in najnaprednejšim tehnologijam, ki so v tistem času na voljo, saj so lahko v nasprotnem primeru že potencialna tarča za napad. Napadalci lahko zelo hitro poiščejo slabo ali pa neustrezno zaščitena podjetja, k temu pa prispeva tudi slabša in zastarela varnostna zaščita, ki podjetju včasih ne nudi prevelike pozornosti, kar pa je lahko zelo slaba poteza v primeru, da se takšno podjetje znajde na listi napadalcev. Podjetja bi morala vedno, ne glede na vse, stremeti k najnovejšim in kakovostnim tehnologijam kljub večjim stroškom, saj je lahko podjetje v nasprotnem primeru veliko huje oškodovano, poleg tega pa so oškodovani tudi vsi zaposleni in uporabniki. V primeru napada je podjetje lahko oškodovano za zelo visoke zneske, poleg tega pa so lahko ukradeni še vsi podatki, kar pa lahko vodi tudi do propada podjetja zaradi obsežnejšega napada. Poleg prilagajanja glede novih tehnologij se morajo redno izvajati tudi izobraževanja zaposlenih na področju kibernetske varnosti, ki pa naj vključujejo predavanja, na koncu pa morajo zaposleni rešiti tudi preizkus. Pomembno je, da se podjetje prilagaja novim tehnologijam, ki jih v tistem trenutku ponuja trg, saj vsi vemo, da napadalci razvijajo in uporabljajo najnovejše in najučinkovitejše metode in so tako nekako vedno korak pred nami, zato pa je izredno pomembno upoštevanje strokovnjakov za kibernetsko varnost, da se lahko podjetje najučinkoviteje zaščiti pred morebitnim napadom.

4 PRIMERI KIBERNETSKIH NAPADOV NA PODJETJA

4.1 Opis kibernetskih napadov na podjetja

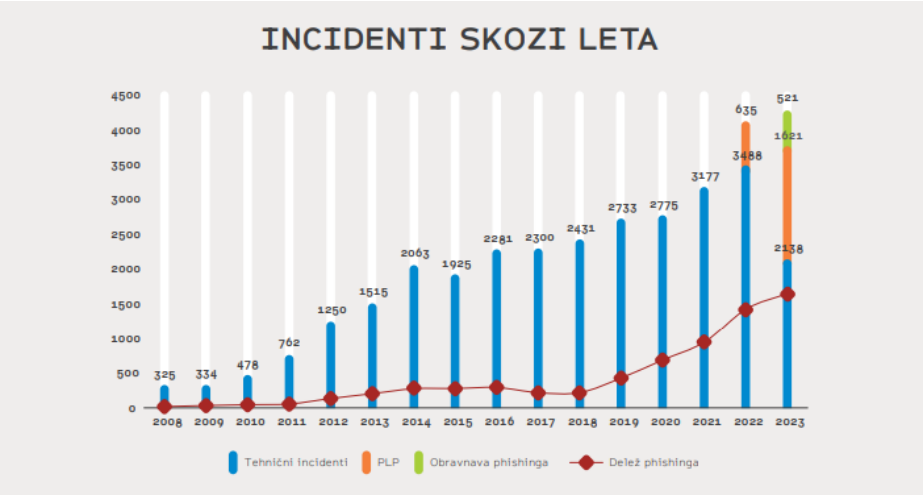
Primer napada na podjetje s pomočjo glasbene datoteke

Napad na podjetje je sprožila z virusom okužena, na pogled nič nenavadna glasbena datoteka, ki jo je zaposleni odprl, s tem pa se je zaradi človeške napake prebila v sistem podjetja in se sprožila ob zagonu glasbe. Podjetje je tako dan po tistem ostalo brez celotne računalniške infrastrukture, v času napada pa niso več pomagali niti trije požarni zidovi, prav tako ni več koristila certificirana programska zaščita. Sistem je bil zaradi ene same odprte datoteke v celoti blokiran in ni bilo več možnosti ukrepanja. Sistem se je popolnoma sesul v zgolj šestih minutah. Pri tem napadu je šlo za izsiljevalski virus, ki se mu je uspelo dokopati do zelo pomembnih podatkov v računalniškem sistemu napadenega podjetja. Kot pričakovano, so napadalci nato po koncu napada zahtevali visoko plačilo v zameno za vračilo zaseženih podatkov. Zahteva oziroma sporočilo je bilo poleg vsega zelo nestrokovno napisano v tako imenovani googlovski slovenščini oziroma je bilo zelo slabo prevedeno prek spletnega prevajalnika Google. Podjetje zahtevanega zneska ni plačalo, s pomočjo strokovnjakov pa jim je uspelo pridobiti vse podatke v sedmih dneh (vsebovredu.triglav.si, 2018).

4.2 Ugotovitve o napadih na podjetja

Ugotovil sem, da je problem predvsem v tem, da je veliko podjetij neustrezno zaščitenih, verjetno gre v tem primeru za to, da podjetje lahko na tak način prihrani nekaj denarja, saj so neustrezne in slabše zaščite tudi cenovno ugodnejše oziroma dostopnejše. Verjetno pa ne pomislijo na to, do kakšne škode bi lahko prišlo v primeru, da bi bilo takšno podjetje deležno kibernetskega napada. Na spletu lahko zasledimo več informacij glede napadov na podjetja, med drugim tudi na slovenska. Na eni od slovenskih spletnih strani sem zasledil, da so opravili raziskavo, v kateri so izvedeli, da naj bi le slabih 27 % vprašanih podjetij uporabljajo napredno protivirusno zaščito, medtem ko jih kar 48 % uporablja osnovni protivirusni program, ostalih 15 % podjetij pa nima nikakršne varnostne zaščite. To torej pomeni, da kar 63 % vprašanih podjetij nima ustrezne zaščite in so na podlagi tega lažja tarča kibernetskih napadov. Večje organizacije velikokrat menijo, da so dobro kibernetsko zavarovane, a se jim nato s penetracijskimi testi dokaže ravno nasprotno. Še vedno pa je glavni vzrok za napade na podjetja

predvsem človeški dejavnik. Težava je predvsem v tem, da zaposleni do nekaterih storitev dostopajo prek javnega interneta, te pa nimajo dvofaktorske avtentikacije.



Slika 12: Incidenti skozi leta

Vir: https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf

4.3 Analiza učinkovitosti varnostnih ukrepov v primeru napadov na podjetja

Med pisanjem diplomskega dela sem poskušal glede na pridobljeno znanje analizirati učinkovitost varnostnih ukrepov, ki bi lahko preprečili ali pa vsaj nekoliko omejili kibernetske napade. Ker se kibernetska tveganja znatno povečujejo, je smiselno, da se jih zavedamo v čim večji meri. Predvsem pa ga moramo znati tudi definirati, saj ga lahko tako kasneje zmanjšamo ali v najboljšem primeru tudi preprečimo, kar pa je cilj vsakega podjetja in organizacije. Prvi korak je predvsem ta, da se vsi zaposleni v podjetju tega zavedajo in tako lažje upravljajo z ukrepi za izboljšanje učinkovite varnosti. Najpomembnejše se mi zdi, da se najprej oceni in identificira tveganje. To torej pomeni, da se analizira, kakšna je stopnja možnosti, da se bo zgodil kibernetski napad. Nato pa je pomembno, da se usposobi in redno izobražuje ljudi na področju kibernetske varnosti, saj se večina napadov zgodi ravno zaradi človeške nepazljivosti in nepozornosti oziroma napake. Zelo pomembno pa je tudi, da podjetje sodeluje s strokovnjaki za kibernetsko varnost, saj so ravno oni tisti, ki so posebej usposobljeni in izobraženi na področju kibernetike. Na drugi strani pa je izrednega pomena tudi, da ima podjetje zagotovljene varnostne kopije, saj napadalci na tak način ne morejo izsiliti denarja za vrnjene podatke, ki so ključnega pomena za podjetje. Seveda so v takšnem primeru podatki ukradeni, vendar napadalci ne morejo izsiliti velike vsote denarja v zameno za podatke, ki so jih podjetju odtujili. To se mi zdi ena izmed učinkovitih metod, saj se lahko podjetje na takšen način izogne morebitnim

nepotrebnim stroškom. Druga zelo pomembna in učinkovita metoda je, da se programska oprema avtomatsko posodablja, saj zastarela programska oprema vedno slabše ščiti podjetje, tehnologija pa se nenadzorovano izboljšuje in napreduje. Posodobitve programske opreme so posodobitve, ki nadgradijo že obstoječe programe, operacijske sisteme in aplikacije. To je torej eden izmed boljših načinov učinkovite zaščite. Tako izboljšujemo varnostne sisteme, hkrati pa dosežemo tudi zmanjšano možnost za kibernetski napad. Ena izmed zelo pomembnih metod je tudi protivirusna zaščita. To so programi, ki samodejno skenirajo programe in aplikacije, ki jih želimo namestiti, ali pa na primer datoteke in tako zaznajo, ali te vsebujejo kakšen virus. Že čisto osnovni programi lahko odpravijo veliko napadov. Tudi blokiranje neželene pošte je učinkovita metoda, saj imajo na primer nam poznani Gmail, Yahoo in podobni vgrajene algoritme, ki s pomočjo filtrov sami izločijo prejeto pošto, ki naj bi bila nezaželena (spam). Ta sporočila se sicer ne izbrišejo, pač pa jih program pošilja v za to namenjeno mapo. Zelo pomembno je tudi, da je internetno omrežje ustrezno in dobro zavarovano. Da bi podjetje izboljšalo varnost, mora internetne povezave zavarovati s požarnim zidom in šifriranjem podatkov. Prav tako se morajo uporabljati močna gesla, ki jih je treba redno spreminjati. Na sliki 13 je nazorno prikazano, kako pomembna je dobra izbira gesel. Lepo je razvidno, da več kot imamo znakov v geslu (črk, številk ipd.), dlje napadalci potrebujejo, da ga razvozljajo.

Število znakov	Samo številke	Male črke	Velike in male črke	Številke, velike in male črke	Številke, velike, male črke in simboli
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

© Hive Systems

Slika 13: Čas, ki je potreben, da napadalec ugotovi geslo

Vir: https://repozitorij.uni-lj.si/Dokument.php?id=160031&lang=slv

Učinkovitost varnostnih ukrepov je torej odvisna predvsem od tega, koliko je podjetje pripravljeno vložiti v varnost. Tukaj lahko v to vključimo voljo, čas in denar. Če se na primer

podjetju ne ljubi vložiti preveč truda v izobraževanje zaposlenih, ti ne bodo znali pravilno ukrepati, če pride do kakšnega incidenta. Enako pa velja tudi za denar. Dražji kot je sistem, boljšo in učinkovitejšo zaščito bo nudil. Preveč manjših podjetij meni, da ne bodo zanimiva za napadalce zaradi premajhnega dobička in premajhne konkurence, vendar se s tem ne strinjam in tudi ni tako. Najbolje je, da se podjetja čim bolj zaščitijo in ne preizkušajo svoje sreče, saj so lahko v primeru napada v veliko večji izgubi in v veliko slabšem položaju. Vredno se je potruditi za dobro zaščito sistema, saj je treba pomisliti tako na podjetje in njegovo uspešnost ter ugled in na varnost zaposlenih ter uporabnikov. Na spodnji sliki lahko vidimo, kako učinkoviti so različni ukrepi, ki bi lahko preprečili kibernetsko tveganje.

UKREP	CENA	ČASOVNO POTRATNA	UČINKOVITOST PRI ZAŠČITI PRED NAPADOM
posodobitev programske opreme	SREDNJE VISOKA	NE	VISOKA
varnostne kopije	SREDNJE VISOKA	ob avtomatskem shranjevanju NE	SLABA (učinkovita le za okrevanje)
antivirusna prog. oprema	VISOKA	NE	ZELO VISOKA
blokiranje neželene pošte	NIZKA	NE	VISOKA
močna gesla	NIZKA	NE	VISOKA
večstopenjsko preverjanje prisotnosti	SREDNJE VISOKA	DA	VISOKA
nadzor dostopa	NIZKA	NE	VISOKA
izobraževanje	VISOKA	DA	ZELO VISOKA

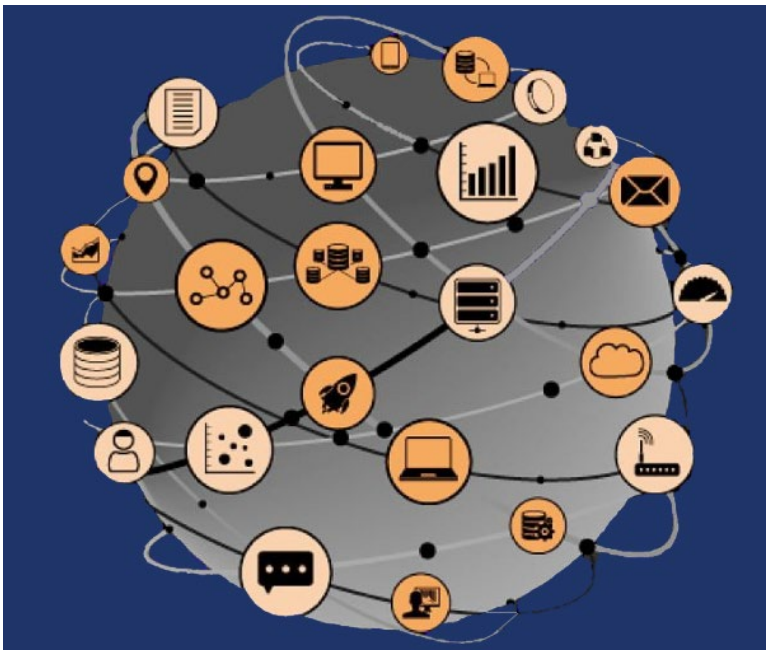
Slika 14: Metode za preprečevanje kibernetskih napadov

Vir : https://repozitorij.uni-lj.si/Dokument.php?id=160031&lang=slv

5 VPLIV ANALITIKE VELIKIH PODATKOV NA KIBERNETSKO VARNOST

5.1 Definicija velikih podatkov

Podatki v današnjem času predstavljajo ključno prednost za gospodarstvo in našo družbo. Veliki podatki, poznani tudi kot masovni ali množični podatki, se nanašajo predvsem na velike količine podatkov, ki hitro proizvedejo ogromno število različnih virov. Podatki so lahko ustvarjeni s pomočjo ljudi ali jih ustvarijo stroji, kot so na primer razni senzorji, ki so namenjeni za zbiranje informacij o podnebju, satelitski posnetki, videoposnetki in slike v digitalni obliki, transakcijski zapiski, navigacijski signali in podobno. Poleg tega pa so tukaj zajeti še številni sektorji, vse od zdravstvenega varstva pa do prometa in energije, ker se na dnevni ravni obrne ogromna količina podatkov. Z leti podatki eksplozivno rastejo ravno zaradi močnega porasta in napredka v tehnologiji. Vse, kar se je pretvorilo v digitalno obliko, že predstavlja neke podatke.



Slika 15: Veliki podatki

(http://sasa.musiclab.si/eri1/INFORMATIKA/Podatki_in_informacije/masovniPodatki/masovniPodatki.html)

Veliki podatki (angl. Big Data) so lahko prikazani v treh oblikah. Prva oblika so strukturirani podatki, drugi so nestrukturirani in tretji so polstrukturirani podatki.

Med pisanjem diplomskega dela se mi je porajalo vprašanje, kako veliki sploh so veliki podatki. Najbolj enostavno povedano, kot že sama beseda veliki pove, gre za ogromno velikost. V praksi

in dejanskem pomenu pa ni tako preprosto. Velikost podatkov, da se štejejo za velike podatke, je predvsem odvisna od naloge in konteksta, v kateri se bodo podatki uporabljali. Za primer lahko povem, da če poizkusimo poslati neko datoteko, ki ima nekaj 100 ali 200 megabajtov, prek e-pošte, in nam te ne bo uspelo poslati, se to že lahko na primer šteje za veliki podatek. Če pa bi kopirali enako veliko datoteko v neko drugo napravo na istem lokalnem omrežju, pa to ne bi vzelo veliko časa, zato v takšnem primeru tega podatka ne bi obravnavali kot velikega. Velike podatke pa lahko analiziramo glede na obseg, hitrost in raznolikost. Obseg se, če logično pomislimo, nanaša na velikost podatkov. Z drugo besedo lahko rečemo tudi volumen podatkov. Velikost nabora podatkov se z leti izboljšuje oziroma povečuje, saj tehnologija iz leta v leto napreduje. Zato imamo danes na voljo že zelo prostorne trde diske in USB-ključke. Dandanes je vse več podatkov, saj napreduje tudi tehnologija, s tem pa tudi uporaba kamer, senzorjev in podobnih naprav za zbiranje podatkov. Hitrost se nanaša na hitrost premikanja podatkov oziroma na to, koliko podatkov se bo ustvarilo v nekem določenem času. Nabor podatkov vsebuje različne vrste podatkov, zato temu pravimo raznolikost podatkov. Ti so lahko sestavljeni iz različnih oblik, kot so na primer video, zvok, besedilo. Da pa bi lahko lažje analizirali velike podatke, so nam na voljo različna orodja in razne platforme, ki podatke analizirajo in iz njih izluščijo pomembne vzorce. »*Orodja za analizo velikih podatkov vključujejo sisteme, kot so ZOHO Analytics, Cloudera in Microsoft BI«* (digital-strategy.ec.europa.eu), (Nelson, 2022).

5.2 Prednosti analitike velikih podatkov

Na začetku 21. stoletja so masovni podatki začeli postajati vse bolj popularni. Spletne organizacije, kot so na primer Google, LinkedIn, Facebook in podobne, so najprej začele uvajati te vrste podatkov. Na tak način naj bi se drastično znižali stroški in čas storitev, prav tako pa se novi proizvodi in storitve lažje in hitreje vpeljejo v proces podjetja. Veliki podatki so tako nekako podobni navadnim podatkom, vendar za razliko od njih zahtevajo drugačen pristop in cilje reševanja problematike. Uporabljajo se torej drugačne tehnike, orodja in zgradba. Tudi organizacijam je lahko obdelava velikih podatkov v veliko pomoč, saj lahko na preprost način dostopajo do družbenih omrežij in spletnih mest, kot sta na primer LinkedIn in Facebook, in tako izboljšajo svoje poslovne strategije (digital-strategy.ec.europa.eu), (sl.itpedia.nl).

5.3 Prednosti in omejitve uporabe analitike velikih podatkov v kibernetski varnosti

Uporaba analitike velikih podatkov v kibernetski varnosti nam lahko prinese več prednosti, vendar pa se poraja tudi vprašanje, kakšne omejitve nam lahko prinese. V nadaljevanju opišemo nekaj ključnih prednosti in omejitev uporabe analitike teh podatkov.

5.3.1 Prednosti uporabe analitike velikih podatkov

Poznamo več prednosti velikih podatkov. Ena izmed najpomembnejših prednosti je zaznavanje nenavadnih vzorcev in groženj v realnem času, saj nam analitika velikih podatkov omogoča, da lahko v zelo kratkem časovnem obdobju analiziramo veliko količino podatkov, kar pa na koncu vodi v hitrejše zaznavanje nenavadnih vzorcev in s tem potencialnih varnostnih groženj. Prav tako lahko z uporabo stojnega učenja in uporabe bolj naprednih algoritmov za prepoznavanje vzorcev sistemi bolje in hitreje prepoznajo vzorce, ki so značilni in kažejo na kibernetski napad, glede na to pa posledično izboljšajo preventivne varnostne ukrepe, da se podjetje zaščiti pred napadi. Ko analiziramo takšne ogromne količine podatkov, nam to omogoča pregled nad dogodki, ki so vodili do kibernetskega napada, saj imamo s pomočjo velike količine podatkov širši vpogled v nastale incidente, kar pa nam spet pomaga preprečiti morebitne potencialne grožnje. Varnostni strokovnjaki se lahko zaradi avtomatizacije analiz bolj osredotočijo na kompleksnejše in pomembnejše naloge, ki pa jih ni mogoče avtomatizirati. Prednost je tudi v tem, da se lahko na tak način kombinira več različnih virov podatkov hkrati, kar pa lahko vodi v izboljšanje učinkovitosti varnostih ukrepov. Še ena velika prednost velikih podatkov je napovedovanje groženj, saj lahko s pomočjo analize podatkov, ki so bili zbrani zaradi v preteklosti že nastalih incidentov, napove potencialne prihodnje grožnje in s tem poskrbi za boljši pristop k izboljšanju varnostnih ukrepov in posledično tudi splošne kibernetske varnosti (Onur Savas, 2017).

5.3.2 Omejitve uporabe analitike velikih podatkov

Analitika velikih podatkov prinaša tudi nekaj omejitev; to je predvsem kompleksnost sistemov in s tem posledično visoki stroški, saj kot bi lahko pričakovali, sta implementacija in vzdrževanje teh sistemov zelo draga in zahtevata ogromno tehničnega znanja, kar bi lahko bil

velik zalogaj in ovira predvsem za manjša ali srednje velika podjetja. Tudi kakovost podatkov lahko podjetjem povzroča težave, saj je uspešnost analitike, predvsem analitike velikih podatkov, odvisna od kakovosti vhodnih podatkov. Slabša kakovost podatkov pa lahko vodi do ustvarjanja napačnih zaključkov in s tem implementacije neučinkovitih varnostnih ukrepov. Včasih je torej tudi preveliko število podatkov lahko slabo, saj so ti lahko manj kakovostni ali celo napačni. Ker pa analitika velikih podatkov zahteva uporabo večje količine podatkov, sta zelo pomembna zasebnost in varovanje zaupnih podatkov. Ker pa se obrača veliko podatkov, lahko to predstavlja tveganje z vidika zasebnosti uporabnikov, zato so tukaj potrebni strogi ukrepi, kar se tiče obdelovanja in shranjevanja teh podatkov. Tako kot v analitiki vseh vrst podatkov se tudi pri analitiki velikih podatkov lahko zgodi, da pride do lažno pozitivnih ali celo negativnih rezultatov zaradi napak, ki so nastale zaradi nenatančnih podatkov, kar pa lahko zopet privede do sklepanja in posledično do napačnih varnostnih odločitev. Še ena izmed omejitev je pomanjkanje strokovnjakov in izobraženega kadra s tega področja in področja kibernetske varnosti, kar morda predstavlja celo največjo težavo današnjega časa v informacijskem sektorju. Ravno zaradi pomanjkanja takšnih strokovnjakov lahko podjetjem predstavljajo precejšno finančno breme. Še eno veliko oviro pa predstavlja integracija novih analitičnih orodij v že obstoječe varnostne sisteme in procese, saj to zahteva veliko časa ter predvsem tehnično podkovanost in dobro razumevanje obstoječega in novega sistema.

Če povzamem ugotovitve glede prednosti in omejitev uporabe analitike velikih podatkov v kibernetski varnosti, lahko ugotovim, da predstavlja močno orodje za izboljšanje varnostnih ukrepov in posledično zniža možnost nastanka kibernetskih incidentov, prav tako pa omogoča predvidevanje prihodnjih groženj z uporabo zgodovinskih podatkov in vzorcev z namenom izboljšanja varnostnih ukrepov. Po drugi strani pa analitika velikih podatkov za učinkovito uporabo zahteva premišljeno načrtovanje, ustrezne vhodne podatke ter natančno izvedbo. Največje omejitve pa so visoki stroški, kompleksnost implementacije, vzdrževanje, težave s pridobivanjem kakovostnih vhodnih podatkov, pomanjkanje strokovnjakov na trgu in integracija z obstoječimi sistemi (Onur Savas, 2017).

5.4 Pomen analitike velikih podatkov za proaktivni pristop h kibernetski varnosti

Kot sem že omenil, analitika velikih podatkov igra veliko vlogo pri proaktivnem pristopu h kibernetski varnosti, saj podjetjem omogoča, da se ne le odzivajo na napade, ampak jih tudi uspešno predvidijo in ustrezno preprečijo. Z integracijo naprednejših analitičnih sistemov v svojo varnostno strategijo lahko dosežejo večjo učinkovitost in odpornost v boju proti nenehno spreminjajočim se kibernetskim grožnjam. Velika prednost analitike velikih podatkov je prepoznavanje vzorcev in odstopanj, ki bi lahko kazala na potencialni kibernetski napad. To omogoča podjetjem, da predhodno pripravijo ustrezne varnostne ukrepe, še preden pride do dejanskega napada, kar pa bistveno zmanjšuje tveganja in potencialno škodo ali vpliv na ugled podjetja in prispeva k proaktivnemu pristopu varnosti. Avtomatizacija varnostnih procesov lahko prav tako prispeva k proaktivnemu pristopu, saj analitični sistemi samodejno zaznajo in se odzovejo na varnostne incidente, zmanjšajo čas odziva in izboljšujejo učinkovitost varnostnih ukrepov. Analitika velikih podatkov lahko podjetju omogoča tudi pridobitev celovitega vpogleda v svoje varnostno okolje in vzpostavljene varnostne ukrepe. S pomočjo povezovanja in analiziranja podatkov iz raznoraznih virov lahko prepoznajo kompleksne napade, ki bi jih sicer lahko spregledali.

6 PRIMER DOBRE PRAKSE

6.1 Opis primera dobre prakse v kibernetski varnosti

Za prikaz primera dobre prakse v kibernetski varnosti sem se odločil, da se postavim v vlogo direktorja manjšega podjetja z nekaj zaposlenimi. Podjetje se ukvarja s prodajo računalniških komponent. Ima tako fizično kot tudi spletno trgovino, v kateri uporabnikom omogoča registracijo, prijavo in nakup računalniških komponent. Kot direktor manjšega podjetja, ki ima zaposlenih nekaj ljudi, je ključno vzpostaviti močan sistem kibernetske varnosti, saj trend kaže, da so prav takšna podjetja najbolj izpostavljena raznoraznim kibernetskim grožnjam, prav tako pa tudi najmanj vložijo v svojo varnost. Ker so v veliki večini za kibernetske incidente krivi zaposleni (več kot 80 %), menim da bi se moralo veliko več poudarka dati na izobraževanje in usposabljanje zaposlenih. V svojem podjetju bi organiziral redne delavnice, kjer bi zaposleni spoznali osnovne koncepte kibernetske varnosti, kot so na primer prepoznavanje phishing elektronskih sporočil, pomembnosti uporabe močnih gesel in pomen dvofaktorske avtentikacije. Poleg tega bi uvedel obvezno testiranje zaposlenih o poznavanju dobrih praks v kibernetski varnosti, ki bi potekalo na vsake tri mesece in bi se izvajalo prek platforme, ki je namenjena testiranju poznavanja kibernetskih groženj. Prednost te platforme je predvsem v tem, da si lahko vsako podjetje personalizira svoj preizkus o poznavanju groženj, ki nam pretijo na spletu. V sklopu izobraževanja zaposlenih bi uvedel tudi simulacijske phishing napade, katerih namen je preverjanje pripravljenosti zaposlenih in njihovega odziva na takšen napad. Napad bi potekal tako, da bi pripravil na prvi pogled popolnoma legitimno elektronsko sporočilo, ki bi vsebovalo z virusom okuženo priponko v obliki PDF-datoteke. Sporočilo bi bilo odposlano vsem zaposlenim hkrati. V poslanem sporočilu bi se izdajal kot nekdo izmed zaposlenih, ti pa bi morali opaziti, da sporočilo ne prihaja iz legitimnega elektronskega naslova, ki ga uporabljajo zaposleni v podjetju (primer legitimnega naslova: rok.novak@podjetje.com, primer napačnega naslova: rok.n0vak@podjetje.com). Znotraj svojega podjetja bi med svoje vrste zaposlil vsaj enega strokovnjaka za informacijsko varnost, ki bi bil zadolžen za pomoč pri organiziranju izobraževanj zaposlenih, simuliranju phishing napadov, pripravi uporabnega gradiva za zaposlene, kar se tiče kibernetske varnosti. Prav tako je zelo pomembno tudi ozaveščanje zaposlenih o varovanju občutljivih podatkov in spoštovanju zasebnosti strank. V prvem koraku je treba jasno določiti, kateri podatki se štejejo za občutljive, kot so osebni podatki strank (npr. ime, naslov, telefonska številka, elektronski naslov), finančni podatki

(kreditne kartice, bančni računi) in poslovno občutljivi podatki (poslovni načrti ipd.). Kar se tiče zaposlenih, bi tukaj za njih lahko organizirali uvodna izobraževanja za nove zaposlene, kjer se jih pouči o osnovah varovanja podatkov, pomenu spoštovanja zasebnosti in obstoječih politikah, ki so določene znotraj podjetja. Znotraj našega podjetja bi zaposlenim dodelili ustrezen dostop do podatkov v sistemu glede na njihovo potrebo, torej glede na vlogo posameznega zaposlenega z namenom omejevanja dostopa do podatkov in tako posledično zmanjšanja tveganja, da bi podatki prišli v roke napadalcev. Tako kot izobraževanje zaposlenih so pomembni tudi tehnični varnostni ukrepi, ki pa zajemajo uporabo varnih sistemov in programov ter varnost omrežja. Za svoje podjetje bi priskrbeli namestitev protivirusne programske opreme na vseh računalnikih in ostalih napravah, ki to potrebujejo. Protivirusna programska oprema mora biti redno posodobljena, saj se s tem izboljšuje njihova sposobnost v premagovanju in prepoznavanju kibernetskih groženj ali zlonamerne programske opreme. Poleg posodabljanja protivirusne programske opreme pa mora biti poskrbljeno tudi za redno posodabljanje operacijskih sistemov in druge programske opreme za zaščito pred najnovejšimi varnostnimi ranljivostmi. Za dostop do sistemov podjetja in računov bi implementirali obvezno dvofaktorsko avtentikacijo, kar pa bi še dodatno zaščitilo varnost podjetja. Prav tako ne smemo pozabiti na varnost omrežja. Znotraj našega podjetja bi ločili omrežje za stranke od poslovnega omrežja, prav tako bi namestili in konfigurirali požarne zidove za zaščito pred nepooblaščenimi vstopi. Vse Wi-Fi povezave bi bile šifrirane s WPA3-standardom, vsi zaposleni pa bi med opravljanjem dela bili dolžni uporabljati VPN. Kot direktor podjetja bi najel strokovnjake za kibernetsko varnost, da bi občasno izvajali penetracijske teste in preverjali varnost naših sistemov, saj dobro vemo, da noben sistem ni popoln in vedno obstajajo možnosti za izboljšave varnostnih ukrepov. Znotraj podjetja bi tako redno pregledovali in ocenjevali sprejete varnostne ukrepe in prilagodili strategijo glede na vse nove grožnje in ranljivosti. V primeru, da bi prišlo do incidenta, bi v podjetju imeli razvit in implementiran načrt odziva na incidente, ki vključuje postopke za hitro ukrepanje in obveščanje vseh potrebnih oseb za uspešno ublažitev ali celo preprečitev incidenta. Vsi zaposleni v podjetju bi bili dolžni poznavati vsebine tega načrta, saj lahko v primeru incidenta šteje prav vsaka sekunda. Poleg vseh ostalih ukrepov pa ne smemo pozabiti na izdelavo varnostnih kopij ključnih podatkov, ki morajo biti shranjeni ločeno in na varni nerazkriti lokaciji. Kot primer, če bi naše podjetje bilo deležno Ransomware napada in bi zaradi njega prišlo do šifriranja podatkov podjetja, bi varnostna kopija za nas bila izrednega pomena.

V svojem podjetju bi vzpodbujal odprto komunikacijo o poročanju sumljivih aktivnosti in potencialnih varnostnih incidentov brez strahu pred posledicami. Želel bi, da bi bila kibernetska varnost prioriteta za vse zaposlene v podjetju ne glede na njihovo vlogo v podjetju.

6.2 Analiza uspešnosti in učinkovitosti varnostnih ukrepov

V nadaljevanju predstavim analizo uspešnosti in učinkovitosti varnostnih ukrepov, v opis vsakega ukrepa pa vključim njegov namen in rezultat njegove pravilne uporabe.

6.2.1 Izobraževanje zaposlenih

Analizo izobraževanja zaposlenih lahko razdelimo na dva dela, prvi del so uvodna in redna usposabljanja ter simulacije napadov.

Uvodna in redna usposabljanja:

Namen: Zaposleni, ki so deležni rednega usposabljanja, znajo bolje prepoznati potencialne grožnje, kar pa lahko zmanjšuje tveganje za uspešne phishing ali druge social engineering napade.

Rezultat: Tako se lahko zmanjša število uspešnih napadov, saj so zaposleni zaradi usposabljanj in izobraževanj bolj ozaveščeni o grožnjah in pravilnem postopanju v primeru napada, poleg tega pa je tudi število prijavljenih sumljivih aktivnosti večje.

Simulacije phishing napadov

Namen: Simulacije napadov pomagajo zaposlenim pri prepoznavanju in pravilnem odzivu na grožnje, kar pa tudi zelo zmanjša verjetnost uspešnega kibernetskega napada.

Rezultat: Stopnja uspešnosti simuliranih napadov postopoma upada skozi čas, saj zaposleni na začetku nasedejo simuliranemu napadu, kasneje pa že vedo, da to ni pravi napad, in ga prijavijo kot sumljivo elektronsko sporočilo.

6.2.2 Tehnični varnostni ukrepi

Tehnične varnostne ukrepe lahko prav tako razdelimo na dva dela, protivirusno programsko opremo in dvofaktorsko avtentikacijo.

Protivirusna programska oprema

Namen: Redno posodobljena protivirusna programska oprema lahko učinkovito zazna in odstrani zlonamerno programsko opremo, kar zmanjša tveganje za okužbo sistema.

Rezultat: S pomočjo te opreme je število zlonamernih, zaznanih in odstranjenih virusov večje, hkrati pa se zato zmanjša število okužb z zlonamerno programsko opremo.

Dvofaktorska avtentikacija

Namen: Močno zmanjšanje verjetnosti nepooblaščenega dostopa tudi v primeru, ko so uporabljena bolj kompromitirana gesla.

Rezultat: S tem se število uspešnih prijav z dvofaktorsko avtentikacijo zviša, tako pa se posledično zmanjša število nepooblaščenih dostopov in hkrati poveča varnost dostopa do občutljivih podatkov.

6.2.3 Varnost omrežja – varni Wi-Fi in požarni zidovi

Namen: Uporaba šifriranih Wi-Fi povezav in požarnih zidov uspešno preprečuje nepooblaščene dostope do omrežja in zmanjšuje tveganje za vdor v sistem podjetja.

Rezultat: Z uporabo tega se število zaznanih poizkusov nepooblaščenega dostopa poviša, ravno zaradi tega pa se posledično zmanjšuje število uspešnih vdorov v zaščiteno omrežje.

6.2.4 Upravljanje dostopov – načelo najmanjših privilegijev

Namen: Omejevanje dostopa zaposlenih do podatkov, ki jih ne potrebujejo za svoje delo, zmanjšuje tveganje groženj znotraj podjetja in površino napada.

Rezultat: Če se omeji dostop, se število incidentov, ki so povezani z nepooblaščenim dostopom, zniža, poveča pa se nadzor nad dostopi do podatkov.

6.2.5 Priprava na incidente

Pripravo na incidente lahko razdelimo na dva dela, prvi je načrt odziva na incidente, v drugi del pa spadajo varnostne kopije.

Načrt odziva na incidente:

Namen: Pripravljen načrt za odziv na incidente omogoča hitro in učinkovito ukrepanje ob kibernetskem napadu, kar zmanjšuje škodo in čas okrevanja.

Rezultat: Dobro sestavljen načrt poskrbi, da se čas odziva na incidente bistveno zniža, posledično pa je tudi učinkovitost ukrepov za zmanjševanje škode zvišano, to pa privede tudi do povečanega števila uspešno rešenih incidentov.

Varnostne kopije:

Namen: Redno izdelovanje varnostnih kopij zmanjšuje izgubo podatkov ob incidentu in omogoča hitro obnovitev sistemov.

Rezultat: Če podjetje redno opravlja varnostno kopiranje, se pogostost in uspešnost obnovitev podatkov iz varnostnih kopij znatno poviša, zmanjša pa se možnost izgube podatkov, kar lahko reši podjetje večjih nepopravljivih težav.

6.2.6 Redni varnostni pregledi

Varnostne preglede lahko razdelimo na penetracijske teste in varnostne ocene s strani strokovnjakov za kibernetsko varnost.

Penetracijski testi:

Namen: Če se redno izvajajo penetracijski testi, to lahko pomaga pri lažjem odkrivanju ranljivosti podjetja in njegovih sistemov, hkrati pa zagotavlja, da so vsi varnostni ukrepi tudi učinkoviti.

Rezultat: Število odkritih ranljivosti se poviša, zviša pa se tudi uspešnost izboljšav in popravkov. Skozi čas pa se lahko zmanjša tudi število potencialnih ranljivosti, ki bi lahko grozile podjetju.

Redne varnostne ocene:

Namen: Redne ocene varnostnih ukrepov zagotavljajo stalno prilagajanje in izboljšanje varnostnih strategij.

Rezultat: Z rednimi ocenami varnostnih ukrepov se njihovi rezultati zelo izboljšajo, če pa redno izboljšujemo varnostne ukrepe, se lahko na splošno zmanjša tveganje za kibernetske incidente.

6.2.7 Spodbujanje varnostne kulture

Varnostno kulturo v podjetju lahko prav tako razdelimo na dva dela, prvi je zavedanje in odgovornost zaposlenih, drugi pa nagrade in priznanja za zaposlene.

Zavedanje in odgovornost:

Namen: Spodbujanje kulture varnosti med zaposlenimi povečuje splošno varnostno ozaveščenost in odgovorno ravnanje z občutljivimi podatki.

Rezultat: Če se zaposleni zavedajo dejanj in so odgovorni, se lahko tako število prijav sumljivih dejavnosti zviša, prav tako pa se izboljša aktivno sodelovanje zaposlenih v varnostnih programih, kar pa lahko znatno zmanjša število varnostnih incidentov.

Nagrade in priznanja:

Namen: Nagrajevanje zaposlenih za varnostno odgovorno vedenje spodbuja proaktivno varnostno ravnanje in krepi zavest o pomenu kibernetske varnosti.

Rezultat: Z nagrajevanjem se poveča motivacija zaposlenih za sodelovanje v varnostnih pobudah, tako pa se posledično zmanjšuje število incidentov zaradi človeških napak.

6.3 Priporočila za izboljšanje kibernetske varnosti v drugih podjetjih

Vsako podjetje se mora zavedati nevarnosti, ki mu lahko pretijo na spletu. Če si želijo izboljšati varnost v svojem podjetju, je zelo pomembno, da upoštevajo določena priporočila, izogniti pa se morajo tudi prepogostim napakam. Kot sem že večkrat omenil, je najbolj pomembno, da se izobražuje in ozavešča zaposlene, saj so ravno ti v večini primerov krivi za nastali incident. Vsem podjetjem bi torej priporočil, da uvedejo obvezna redna izobraževanja vseh zaposlenih, v to pa morajo biti vključeni tudi simulacijski napadi, ki zaposlene pripravijo na morebitne incidente, ki bi lahko nastopili med opravljanjem dela. Prav tako morajo zaposleni točno vedeti, kako je treba komunicirati, zato je treba zagotoviti, da so vsi s tem seznanjeni. Izredno pomembno je tudi, da ima podjetje nameščeno ustrezno in dobro protivirusno zaščito, ki naj bo redno posodobljena na vseh napravah. Izpostavil bi tudi dvofaktorsko avtentikacijo, ki naj bo uporabljena pri vseh pomembnih računih in sistemih, da se lahko zmanjša tveganje za nepooblaščen dostop do občutljivih in pomembnih informacij. Priporočil bi tudi šifriranje podatkov za shranjevanje in prenos podatkov, ki so občutljivi. Eno izmed pomembnejših priporočil je tudi ustrezno zavarovano in šifrirano Wi-Fi omrežje, ki pa mora biti ločeno za

poslovno uporabo in za stranke. Za večjo varnost je treba namestiti tudi požarne zidove in sisteme za zaznavanje in preprečevanje vdorov, saj lahko tako še dodatno zaščitimo omrežje. Zelo pomembno se mi zdi tudi, da podjetje omeji dostop zaposlenih do podatkov in sistemov glede na to, kakšne naloge in delovne potrebe imajo v podjetju. V to pa bi vključil tudi redno pregledovanje dostopnih pravic zaposlenih v podjetju. Neizogibni se mi zdijo tudi načrti odzivov na incidente, ki naj vključujejo točne postopke za čim hitrejše ukrepanje in obveščanje v primeru kibernetskega napada. Kot sem tudi že omenil, so prav tako izredno pomembne varnostne kopije ključnih podatkov, saj si lahko podjetje tako zagotovi, da se ti ne morejo izgubiti ali biti ukradeni s strani napadalcev, ki želijo oškodovati podjetje in od njega zahtevati denar v zameno za ukradene podatke. Če podjetje izvaja redne penetracijske teste, lahko tako odkrijejo in posledično tudi odpravijo pomanjkljivosti, kar pa zmanjša varnostno ranljivost podjetja. Pametno bi bilo tudi, da podjetje redno ocenjuje varnostne ukrepe in se prilagaja glede na novo nastale grožnje in ranljivosti. Zaposlene je treba spodbujati, da med seboj komunicirajo in sprotno poročajo o njim sumljivim in potencialnim nevarnostnim ter da naj nimajo strahu pred posledicami. Podjetjem bi priporočil tudi, da uvedejo sisteme nagrajevanja za zaposlene, ki bi izkazali skrb za varnost podjetja, podatkov in spoštovanja zasebnosti.

7 SKLEP

Med raziskovanjem in pisanje, diplomskega dela sem ugotovil predvsem, da kljub naraščajoči grožnji kibernetskih napadov večina podjetji še vedno ne vlaga dovolj v ustrezno izobraževanje zaposlenih in ne izboljšanje svojih varnostnih ukrepov. V veliki večini so najlažja tarča kibernetskih napadov manjša ter srednje velika podjetja, saj prav ta najmanj vlagajo v svoje varnostne ukrepe in premalo ali sploh ne izobražujejo svojih zaposlenih, prav tako pa nimajo vzpostavljenih nobenih varnostnih politik in postopkov. Zanimivi dejstvi sta, da je vsako peto podjetje že bilo tarča kibernetskega napada in da se vsakih 39 sekund na svetu zgodi kibernetski napad na podjetje. Torej ni več vprašanje, ali bo naše podjetje tarča napada, ampak kdaj se bo zgodil ta napad. Ugotovil sem, da so za nastanek kibernetskega napada kar v 80 % primerov odgovorni zaposleni v podjetju, najpogostejša vrsta kibernetskega napada pa je ribarjenje (Phishing) prek elektronskih sporočil. Vredno je tudi omeniti, da je vedno bolj popularno delo od doma, vendar pa zaposleni za dostop do službenih sistemov ne uporabljajo VPN in uporabljajo enaka gesla za dostop do zasebnih in službenih računov, kar lahko predstavlja veliko varnostno tveganje. Podjetja zelo redko izvajajo ocene tveganja in preverjanje njihove ranljivosti s pomočjo penetracijskih preizkusov, saj mislijo, da bo to predstavljalo prevelik finančen zalogaj, in na to ne dajejo dovolj poudarka, čeprav so to dokazano najboljši načini odkrivanja pomanjkljivosti v sistemih podjetij. Če pogledamo projekcije števila kibernetskih napadov za leto 2024 in jih primerjamo s preteklimi leti, ugotovimo, da se frekvenca napadov iz leta v leto dviguje in ne kaže znakov upadanja. Na splošno je stanje kibernetske varnosti v podjetjih zaradi tega vedno bolj zaskrbljujoče. Kot sem že omenil, se frekvenca napadov viša, podjetja pa temu ne dajejo nobene pozornosti in v veliki večini ravnajo šele takrat, ko je že prepozno. Na podlagi vseh analiz in študij sem ugotovil, da je ključ do izboljšanja varnosti v podjetjih celovit pristop, ki vključuje izobraževanje in ozaveščanje zaposlenih, nadgradnjo varnostnih tehnologij, vzpostavitev varnostnih politik ter upoštevanje standardov (ISO 28001 in ISO 31000). Prav tako pa ne smemo pozabiti na kulturo varnosti znotraj podjetja, kjer vsak zaposleni razume svojo vlogo pri ohranjanju varnosti informacijskih sistemov. Po mojem mnenju je za podjetja danes pomembno, da se varnost postavi na vrh njihovega seznama prioritet, saj lahko zelo hitro pride do neprijetne situacije zaradi kibernetskega napada, kar pa lahko vpliva tudi na njihovo poslovanje in ugled. Samo z doslednim in celovitim pristopom k varnosti lahko podjetja učinkoviteje zaščitijo svoje podatke in zagotovijo nemoteno poslovanje pred vse bolj naprednimi kibernetskimi grožnjami.

H1: Izobraževanje zaposlenih o kibernetski varnosti in ozaveščanje o tveganjih kibernetskih napadov lahko zmanjšata tveganje za napade v podjetju.

Glede na ugotovljeno prvo hipotezo potrdim. V vseh opravljenih študijah in analizah, ki sem jih našel v knjigah, člankih in drugi virih, je vedno znova izpostavljena pomembnost izobraževanja ter ozaveščanja zaposlenih o tveganjih kibernetskih napadov. Dodatna potrditev je, da lahko redno ozaveščanje in izobraževanje znižata možnosti nastanka kibernetskega napada za kar 60 %, kar lahko ima izredno močan vpliv na uspešno in nemoteno poslovanje podjetja.

H2: Uporaba večplastne varnostne strategije, ki vključuje več različnih varnostnih ukrepov, zmanjšuje tveganje za uspešen kibernetski napad.

Drugo hipotezo lahko z gotovostjo potrdim. Večplastna varnostna strategija z uporabo več različnih varnostnih ukrepov uvaja več različnih slojev obrambe, kar pomeni, da v primeru, če en varnostni ukrep odpove, drugi še vedno lahko zaščitijo sistem, kar potencialno bistveno zmanjšuje možnosti, da napadalci uspešno prodrejo skozi vse zaščite. Uporaba večplastne varnostne strategije pa prav tako zmanjša tveganje za človeške napake. Primer: zaposleni spregleda phishing elektronsko pošto, protivirusni sistem ali filtri za e-pošto lahko zaznajo in blokirajo okuženo prilogo v elektronski pošti. Večplastna strategija, specifična segmentacija omrežja in nadzor dostopa pa lahko poskrbita tudi za omejitev škode tako, da napadalcem preprečijo razširitev svojega napada po celotnem sistemu.

H3: Podjetja, ki redno preverjajo in posodabljajo svoje varnostne ukrepe, so bolje pripravljena na kibernetske napade in imajo manjšo verjetnost za uspešen napad.

Prav tako lahko potrdim tudi tretjo hipotezo, saj študije kažejo, da podjetja, ki aktivno upravljajo svoje varnostne ukrepe, beležijo manj varnostnih incidentov in so bolj odporna na kibernetske napade. Ta ugotovitev temelji na tem, da podjetja sproti zaznavajo in odpravljajo ranljivosti, kar jim omogoča, da pravočasno zaznajo in odpravijo morebitne varnostne luknje in druge ranljivosti, ki bi jih napadalci lahko drugače izkoristili. Prav tako so ta podjetja skladna z najnovejšimi varnostnimi standardi in praksami, saj se varnostne grožnje nenehno spreminjajo, redno posodabljanje varnostnih ukrepov pa pomeni, da podjetja sledijo varnostnim standardom, praksam in priporočilom, kar povečuje njihovo odpornost proti novim vrstam napadov. Prav tako ta podjetja redno posodabljajo svojo programsko opremo, oprema, ki ni posodobljena, pa v veliki večini vsebuje znane ranljivosti, ki jih napadalci lahko izkoristijo. Redno preverjanje in posodabljanje varnostnih ukrepov pa vključuje tudi izobraževanje in

usposabljanje zaposlenih glede novih groženj in varnostnih praks, kar pa, kot smo potrdili že pri prejšnji hipotezi, vodi k znižanju možnosti za nastanek incidenta.

H4: Uporaba analitike velikih podatkov (Big Data) omogoča boljše odkrivanje in razumevanje vzorcev ter naprednih kibernetskih groženj, kar prispeva k proaktivnemu pristopu h kibernetski varnosti.

Četrto in zadnjo hipotezo lahko prav tako potrdim. Uporaba analitike velikih podatkov omogoča obdelavo ogromne količine podatkov, kar podjetjem pomaga pri prepoznavanju vzorcev in nenavadnih dogodkov, ki bi lahko nakazovali potencialne kibernetske grožnje. S pomočjo uporabe naprednih algoritmov in tehnik strojnega učenja lahko avtomatsko prepoznajo grožnje, ti algoritmi pa se učijo iz zgodovinskih podatkov in lahko odkrijejo napade, ki jih tradicionalni varnostni ukrepi morda ne bi. Z uspešno analizo lahko dobimo tudi vpogled v aktualno varnostno stanje in kakovost vzpostavljenih varnostnih ukrepov, istočasno pa lahko tudi optimiziramo in izboljšamo obstoječe varnostne ukrepe, kar pa, kot smo že potrdili pri drugi hipotezi, vodi k boljši pripravljenosti in odpornosti na napade.

8 VIRI IN LITERATURA

b2.eu. (2. februar 2022). Pridobljeno iz https://www.b2.eu/sl/novice/najpogostejse-oblike-kibernetskih-napadov-2022-02-02

bureauveritas.si. (brez datuma). Pridobljeno iz https://www.bureauveritas.si/certificiranje/iso-27001

bureauveritas.si. (12. januar 2024). Pridobljeno iz https://www.bureauveritas.si/magazine/zakaj-je-razvoj-kulture-kibernetske-varnosti-pomemben-za-vsako-organizacijo

cdn.standards.iteh.ai. (maj 2018). Pridobljeno iz https://cdn.standards.iteh.ai/samples/65694/5c27d980f52a42b394056c1f90ae5346/SIST-ISO-31000-2018.pdf

cyberwiser. (julij 2016). *cyberwiser.eu.* Pridobljeno iz https://www.cyberwiser.eu/sites/default/files/Wiser_BookletB5_July2016_inner_web_SL.pdf

digital-strategy.ec.europa.eu. (brez datuma). Pridobljeno iz https://digital-strategy.ec.europa.eu/sl/policies/big-data

digital-strategy.ec.europa.eu. (14. 9 2023). Pridobljeno iz https://digital-strategy.ec.europa.eu/sl/policies/nis2-directive

dqsglobal.com. (brez datuma). Pridobljeno iz https://www.dqsglobal.com/sl-si/potrdite/certificiranje-iso-27001

Finance. (2024). *finance.si.* Pridobljeno iz https://www.finance.si/file/kibernetska-varnost-2024?cfd_id=494125

gdpr-info.eu. (brez datuma). Pridobljeno iz https://gdpr-info.eu/

Gillis, A. S. (februar 2024). *techtarget.com*. Pridobljeno iz https://www.techtarget.com/searchsecurity/definition/cybersecurity

gov.si. (22. maj 2023). Pridobljeno iz https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/o-uradu/

Nelson, D. (9. december 2022). *unite.ai*. Pridobljeno iz https://www.unite.ai/sl/kaj-so-veliki-podatki/

nil.com. (brez datuma). Pridobljeno iz https://nil.com/sl/znanje/zakon-o-informacijski-varnosti-zinfv-je-zakon/

Onur Savas, J. D. (2017). *Big Data Analytics in Cybersecurity.* Auerbach Publications.

pisrs.si. (26. april 2018). Pridobljeno iz https://pisrs.si/pregledPredpisa?id=ZAKO7707

PR, F. (Petek. Marec 2024). *finance.si*. Pridobljeno iz https://www.finance.si/slovenija/kaj-se-zgodi-ko-zdruzijo-moci-strokovnjaki-za-kibernetsko-varnost-iz-razlicnih-drzav/a/9021394

siq.si. (brez datuma). Pridobljeno iz https://www.siq.si/nase-dejavnosti/certificiranje-organizacij/predstavitev/informacijska-varnost/iso-iec-27001/

siq.si. (11. junij 2024). Pridobljeno iz https://www.siq.si/izobrazevanje/program/izobrazevanje/kaj-prinasa-direktiva-za-kibernetsko-varnost-nis-2-in-kako-se-pripraviti-nanjo/KAJPRIerkw/

sl.economy-pedia.com. (2024). Pridobljeno iz https://sl.economy-pedia.com/11032647-iso-international-organization-for-standardization

sl.itpedia.nl. (brez datuma). Pridobljeno iz https://sl.itpedia.nl/2017/08/29/big-data-soorten-kenmerken-en-voordelen/

svetkapitala.delo.si. (27. november 2019). Pridobljeno iz https://svetkapitala.delo.si/delove-podjetniske-zvezde/kako-pravocasno-poskrbeti-za-kibernetsko-varnost-v-podjetju/

Unija, E. (27. december 2022). *eur-lex.europa.eu.* Pridobljeno iz https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022L2555

varnost-it.si. (brez datuma). Pridobljeno iz https://varnost-it.si/kibernetska-varnost/

vsebovredu.triglav.si. (December 2018). Pridobljeno iz https://vsebovredu.triglav.si/posel/kibernetska-varnost-podjetja

vsi.si. (brez datuma). Pridobljeno iz https://www.vsi.si/bureauveritas/iso-standardi