VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

Vpliv digitalne preobrazbe na okolje in varnostno politiko v podjetjih

Kandidatka: Tina Pajsar

Vrsta študija: študentka izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Anton Kravanja

Lektorica: dr. Alenka Čuš, univ. dipl. slov.

Maribor, 2022

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Tina Pajsar, sem avtorica diplomskega dela z naslovom Vpliv digitalne preobrazbe na okolje in varnostno politiko v podjetju, ki sem ga napisala pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbela, 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.

Vrhnika, december 2022 Podpis študenta:

ZAHVALA

Zahvaljujem se mentorju, mag. Dušanu Brglezu, ter mentorju v podjetju, Antonu Kravanji, za vse smernice in vložen čas v mentorstvo pri pisanju diplomskega dela.

Prav tako se zahvaljujem družini za potrpežljivost in podporo v času študija ter sošolcem za vzpodbudo in nepozabni dve leti študija.

POVZETEK

V zadnjih nekaj letih so bila podjetja primorana k vsaj določeni meri digitalizacije zaradi epidemije COVID-19. S tem so si podjetja, poleg dodatnih stroškov in nepripravljenosti za delo od doma, nehote pridobila razkritje varnostnih lukenj, saj prej verjetno niso omogočala dela od doma, tako da zaposleni niso bili opremljeni s prenosnimi računalniki in niso imeli urejenih pravilnikov dela od doma ali prilagojenega delovnega okolja doma. Kar naenkrat pa so podjetja morala svojim zaposlenim omogočiti oddaljen dostop, kar lahko nepridipravom odpre dodatna vrata, ki niso dovolj dobro zavarovana. Obenem pa je sistem varen toliko, kot je izobražen o nevarnostih in varovanju podatkov najšibkejši zaposleni.

Varnostna politika informacijske tehnologije je dokument, ki določa pravila, pričakovanja in splošni pristop, ki ga organizacija uporablja za ohranjanje zaupnosti, celovitosti in razpoložljivosti svojih podatkov. Varnostni pravilniki obstajajo na številnih različnih ravneh, od konstrukcij na visoki ravni, ki opisujejo splošne varnostne cilje in načela podjetja, do dokumentov, ki obravnavajo posebna vprašanja, kot je oddaljen dostop ali uporaba WI-FI. Varnostni pravilnik se pogosto uporablja v povezavi z drugimi vrstami dokumentacije, kot so standardni operativni postopki. Ti dokumenti skupaj pomagajo podjetju pri doseganju varnostnih ciljev.

V sklopu diplomskega dela bomo ugotovili kaj vse sestavlja varnostno politiko, da je učinkovita. Prav tako kako varnostno politiko sploh napisati in kako pogosto jo je potrebno obnavljati. Obstajajo tudi standardi, kot je ISO 27001, ki vsebuje smernice kako mora podjetje pristopati k varovanju podatkov podjetja. Prav tako bomo upoštevali standard TISAX, ki je mehanizem za ocenjevanje in izmenjavo informacijske varnosti v avtomobilski industriji. Najbolj pomemben člen pa so seveda zaposleni, torej prav tako bomo pregledali kako zaposlenim predstaviti varnostno politiko ter kako jo uresničiti, saj varnostna politika ni le dokument, na katerem se nabira prah, ampak je živ dokument, ki mora biti redno posodobljen. Ne smemo pa niti pozabiti kako digitalizacija, delo od doma ter epidemija vplivajo na okolje. Zaradi dela od doma se je povečala digitalizacija podjetij in še bolj ozaveščenost, da ni potrebno vsakega dokumenta natisniti, kar pa je za večino podjetij eden izmed redkih načinov, kako podjetje vpliva na okolje s svojo digitalizacijo.

Ključne besede: varnostna politika informacijske tehnologije, digitalizacija, okolje, kibernetska varnost, nepovratna sredstva

ABSTRACT

The impact of digital transformation on the environment and security policy in companies

In the last couple of years, companies have been forced to at least some degree of digitization due to the COVID-19 epidemic. With this, in addition to additional costs and unwillingness to work from home, companies unintentionally exposed security holes, because previously they may not have been allowed working from home, so employees were not equipped with laptops, and they did not have regulations for working from home nor adapted work environment at home. All of a sudden, companies had to provide their employees with remote access, which can open additional doors for miscreants that are not sufficiently secured. Also, the system is only as safe as the weakest employee is educated about dangers and data protection.

An information technology security policy is a document that sets out the rules, expectations, and overall approach an organization uses to maintain the confidentiality, integrity, and availability of its data. Security policies address many different levels, from high-level constructs that describe the general security goals and principles of an enterprise to documents that address specific issues such as remote access or WI-FI use. A security policy is often used in conjunction with other types of documentation, such as standard operating procedures. Together, these documents help the company achieve its security goals.

As part of the thesis, we will examine what constitutes an effective security policy. Also, how to write a security policy, and how often it needs to be renewed. There are standards such as ISO 27001 as well, which has guidelines on how a company should approach the protection of the company data. We will also take into account the TISAX standard, which is a mechanism for evaluating and exchanging information security in the automotive industry. The most important element is of course the employees, so we will also check on how to present the security policy to employees and how to implement it, because the security policy is not just a document that collects dust, but it is a living document that must be regularly updated. We must not forget how digitalization, working from home and the epidemic affects the environment. As a result of working from home, the digitization of companies has increased and there is even more awareness that it is not necessary to print every document, which for most companies is one of the few ways in which a company affects the environment through its digitalization.

Keywords: Security policy of information technology, Digitalization, Environment, Cyber security, Grants

KAZALO VSEBINE

KAZALO SLIK

KAZALO GRAFIKONOV

1 UVOD

1.1 Opis področja in opredelitev problema

Informacije imajo eno najpomembnejših vlog v poslovanju podjetja. Zaradi pomembnosti informacij, je informacijska varnost ključni dejavnik v razvoju izdelkov in storitev podjetja. Z ustrezno identifikacijo in sistematizacijo infomacij ter z izvajanjem sistematične ocene tveganja, v kateri se prepoznajo grožnje in ranljivosti, lahko organizacija izbere in uvede ustrezne kotrole za upravljanje teh tveganj, s čimer lahko organizacija dokaže strankam, da učinkovito ohranja zaupnost, celovitost in razpoložljivost informacij.

Predvidevam, da veliko podjetij ne ve kaj je varnostna politika in le te nimajo opredeljene. Saj podjetja, ki mogoče nimajo IT oddelka v »hiši«, niso seznanjene s standardi in certifikati, ker to za njihovo poslovanje ni nujno potrebno (npr. podjetje, ki se ukvarja s prodajo kanalizacijskega materiala, mogoče nima varnostne politike, medtem ko podjetje, ki izdaja digitalna potrdila le to ima urejeno). Zastavljene trditve bom dokazala ali ovrgla na podlagi spletne ankete, katero bom poslala vsem dobitnikom vavčerja za kibernetsko varnost pri Slovenskem podjetniškem skladu ter dobitnikom razpisa Spodbude za digitalno transformacijo MSP.

1.2 Namen, cilji in osnovne trditve

Namen diplomskega dela je ugotoviti ali podjetja imajo varnostno politiko, ter v kolikor je nimajo ali imajo namen opredeliti varnostno politiko podjetja v prihodnosti. Prav tako pa izvedeti, ali se zavedajo kako njihova digitalizacija vpliva na okolje, saj se je v zadnjih nekaj letih ogromno podjetij prijavilo na razpis, ki ga je objavil Slovenski podjetniški sklad za spodbude digitalne transformacije MSP.

Osnovne trditve:

- Podjetja imajo varnostno politiko.
- Podjetja so varnostno politiko oblikovale s pomočjo zunanjega podjetja.
- Podjetja redno posodabljajo varnostno politiko.
- Podjetja izdelajo varnostno politiko zaradi zahtev strank.
- Podjetja imajo opredeljene odzive na kibernetski napad v varnostni politiki.
- Podjetja se prijavljajo na nepovratna sredstva za digitalizacijo.
- Podjetja so že opravila varnostni pregled sistema.

- Podjetja so spremenila procese zaradi vpeljave varnostne politike.
- Podjetja spreminjajo procese v podjetju na podlagi digitalizacije.
- Podjetja se zavedajo kako vpliva digitalizacija na okolje.
- Podjetja sprejemajo različne ukrepe za zmanjšanje negativnega vpliva na okolje.

1.3 Predpostavke in omejitve

Omejitev, katero pričakujem pri diplomskem delu je, da podjetja na sicer kratko in jedrnato anketo ne bodo odgovorila.

1.4 Uporabljene raziskovalne metode

Preko spletne ankete bom dobitnikom vavčerja za kibernetsko varnost ter razpisa za spodbude digitalizacije poslala vprašalnik, na podlagi pridobljenih rezultatov bom ovrgla ali potrdila hipoteze.

H1: Podjetja imajo varnostno politiko.
H2: Podjetja se prijavljajo na nepovratna sredstva za digitalizacijo.
H3: Podjetja spreminjajo procese v podjetju na podlagi digitalizacije.
H4: Podjetja se zavedajo kako vpliva digitalizacija na okolje.

2 VARNOSTNA POLITIKA V PODJETJIH

2.1 Kaj je varnostna politika

Veliko časnikov, med njimi tudi The Economist, so izjavili, da so podatki najdragocenejši vir na svetu. Zaradi tega je nastal še večji pritisk na podjetja, da zavarujejo podatke, ki jih hranijo. Nedavni vdori, v katerega so bili vključeni Solarwinds, Twitter in Garmin kažejo, da se grožnje informacijske varnosti še naprej razvijajo in da organizacije nimajo druge izbire, kot da si prizadevajo za vzpostavitev in vzdrževanje potrebnih kontrol kibernetske varnosti, ne glede na to, ali je njihov IT na mestu uporabe, v oblaku ali gre za zunanje izvajanje (Mathenge, 2021).

Varnostna politika informacijske tehnologije (IT) opredeljuje pravila in postopke za vse posameznike, ki dostopajo in uporabljajo IT sredstva in vire organizacije. Učinkovita varnostna politika IT je model kulture organizacije, v kateri pravila in postopki izhajajo iz pristopa zaposlenih do njihovih informacij in dela. Tako je učinkovita varnostna politika IT edinstven dokument za vsako organizacijo, ki se oblikuje iz perspektive ljudi o toleranci tveganja, o tem, kako vidijo in cenijo svoje informacije, in posledično razpoložljivosti teh informacij, ki jo vzdržujejo. Iz tega razloga se bo mnogim podjetjem zdela okvirna varnostna politika IT neprimerna zaradi pomanjkanja upoštevanja kako ljudje v organizaciji dejansko uporabljajo in delijo inforamcije med seboj. Cilji varnostne politike IT so ohranjanje zaupnosti, celovitosti in razpoložljivosti sistemov in informacij, ki jih uporabljajo člani organizacije. Ta tri načela sestavljajo triado CIA:

- Confidentiality (Zaupnost),
- Integrity (Integriteta),
- Availability (Razpoložljivost), (Paloalto, 2022).

Slika 1 Triada CIA

Vir: https://blackkite.com/wp-content/uploads/2022/04/cia-triad-300x252.png

Zaupnost podatkov se osredotoča na zaščito občutljivih informacij, kot so nejavni osebni podatki ali podatki imetnika kartice pred nepooblaščenim dostopom. Zlonamerni akterji pogosto ciljajo na zaupne podatke, ker se ti lahko uporabijo za krajo identitete in goljufije. Zaupni podatki lahko vključujejo tudi občutljive informacije podjetja, kot so poslovne skrivnosti. Potrebno je upoštevati sledeče:

- kako nadzorovati dostop do informacij,
- kako preprečiti vohljanje,
- kako preprečiti kršitev podatkov,
- kako preprečiti uhajanje podatkov (SecurityScorecard, 2021).

Integriteta pokriva področje celovitosti podatkov. Celovitost podatkov se osredotoča na zagotavljanje točnosti podatkov in preprečevanje sprememb informacij, vnesenih v bazo podatkov ali drug vir. Organizacije morajo vzdrževati kakovost podatkov s preprečevanjem zlonamernih ali nenamernih sprememb podatkov, ki lahko škodujejo lastnikom podatkov. Upoštevati je potrebno sledeče smernice:

- kako zmanjšati tveganje človeške napake,
- kako zlonamernim akterjem preprečiti dostop do informacij in njihovo spreminjanje,
- kako vzpostaviti procese nadzora sprememb,
- kako preprečiti nenamerne napake pri prenosu,
- kako zagotoviti, da napačne konfiguracije ali varnostne napake ne vplivajo na informacije,

- kako utrditi strojno opremo, da preprečimo kompromis,
- kako revidirati procese in postopke za zagotovitev sledjivosti (SecurityScorecard, 2021).

Razpoložljivost podatkov se osredotoča na točnost, popolnost in doslednost informacij, da se uporabnikom zagotovi dostop do informacij, ko jih potrebujejo. Organizacije morajo vzpostaviti postopke in procese za shranjevanje podatkov, obnovitev po katastrofi in neprekinjeno poslovanje. Pri vključitvi razpoložljivosti podatkov je potrebno paziti na:

- kako preprečiti, da bi naravne nesreče, človeške napake ali erozija skladišč vplivale na fizično celovitost,
- kako preprečiti človeške napake ali zlonamerne napade, ki vplivajo na logično celovitost,
- kako ohraniti edinstvene vrednosti podatkovnih delov za zaščito celovitosti entitete,
- kako vzpostaviti procese, ki ohranjajo podatke shranjene in enotno uporabljene za zaščito referenčne celovitosti,
- kako izmeriti obliko, vrsto in količino podatkov, da zaščitimo celovitost domene,
- kako ustvariti pravila, ki obravnavajo potrebe uporabnikov, da ohranijo uporabniško določeno celovitost (SecurityScorecard, 2021).

Ko sem že omenila, je cilj politike informacijske varnosti vzpostaviti zaščito in omejiti distribucijo podatkov samo na tiste s pooblaščenim dostopom. Podjetja vzpostavijo varnostno politiko za:

- vzpostavitev splošnega pristopa k informacijski varnosti,
- dokumentiranje varnostnih ukrepov in politike nadzora dostopa uporabnikov,
- zaznavanje in zmanjševanje vpliva ogroženih informacijskih sredstev, kot so zlorabe podatkov, omrežij, mobilnih naprav, računalnikov in aplikacij,
- zaščito ugleda organizacije,
- upoštevanje zakonskih in regulativnih zahtev, kot so NIST, GDPR, HIPPA in FERPA,
- zaščito podatkov svojih strank, kot so številke kreditnih kartic,
- zagotovitev učinkovitih mehanizmov za odzivanje na pritožbe in poizvedbe v zvezi z resničnimi ali domnevnimi tveganji kibernetske varnosti, kot so lažno predstavljanje, zlonamerna programska oprema in izsiljevalska programska oprema,
- omejitev dostopa do ključnih sredstev informacijske tehnologije (Tunggal Tyas, 2022).

2.2 Kaj vse zajema varnostna politika

Politika varnosti IT je živ dokument, ki se nenehno posodablja, da se prilagodi razvijajočim se zahtevam poslovanja in IT. Institucije, kot je mednarodna organizacija za standardizacijo (ISO), je objavila standarde in najboljše prakse za oblikovanje varnostne politike. Vendar pa je politika informacijske varnosti lahko široka kolikor podjetje želi. Zajema lahko varnost informacijske tehnologije in/ali fizično varnost, pa tudi uporabo družbenih medijev, upravljanje življenjskega cikla in varnostno usposabljanje (Tunggal Tyas, 2022).

Vsi uporabniki v vseh omrežjih in infrastrukturi IT v celotni organizaciji se morajo tega pravilnika držati. V nasprotnem primeru so lahko podatki organizacije ranljivi za napad. Na splošno pravilnik velja za vse digitalne podatke organizacije in zajema področja, kot so podatki, infrastruktura, omrežje, programi, sistemi, uporabniki. Za najboljše rezultate mora biti politika informacijske varnosti organizacije praktična in izvršljiva. Hkrati pa mora biti tudi dovolj prilagodljiva, da se prilagodi potrebam različnih oddelkov in ravni v organizaciji. Dobra varnostna politika dosega sledeče cilje:

- opredelitev splošnega organizacijskega pristopa k organizacijski varnosti,
- določanje politik nadzora dostopa uporabnikov in varnostnih ukrepov,
- odkrivanje ogroženih sredstev, kot so podatki, omrežja, računalniki, naprave in aplikacije,
- zmanjšanje negativnih vplivov vseh ogroženih sredstev,
- varovanje ugleda organizacije glede informacijske varnosti,
- skladnost z veljavnimi pravnimi zahtevami, standardi in regulacijami (GDPR),
- zaščita občutljvih podatkov strank, kot so zdravstveni podatki, osebni podatki, številke kreditnih kartic,
- vzpostavitev okvirov za odgovarjanje na vprašanja in pritožbe o grožnjah kibernetske varnosti,
- omejevanje dostopa do informacij uporabnikom, ki jih upravičeno potrebujejo (BoxBlogs, 2021).

Varnostna politika je nepogrešljiva za vsako podjetje, ki mora odgovorno ravnati z občutljivimi podatki strank in pridobiti zaupanje strank. Obstaja nekaj razlogov, zaradi katerih je danes tako pomembna pri poslovanju. Prvič, varnostna politika pomaga zaščititi pred zlonamernimi grožnjami. Varnostni incidenti, kot so uhajanje podatkov in kršitve podatkov, hitro spodkopajo

zaupanje potrošnikov. Dobra varnostna politika pomaga preprečiti incidente in ohranja visoko zaupanje strank. Prav tako zmanjša tveganje znatnih finančnih izgub (BoxBlogs, 2021).

Pravilno načrtovanje varnostne politike je ključnega pomena tudi za zaščito zelo občutljivih podatkov. Vse informacije v poslovnem svetu niso enake. Izjemno občutljivi podatki, ki bi lahko povzročili ogromne izgube, če bi ušli, skupaj z intelektualno lastnino in podatki, ki omogočajo osebno identifikacijo, zahtevajo višjo raven zaščite kot druge vrste podatkov. Varnostna politika daje podjetjem definiran način za določanje prednosti in zaščito teh vrst podatkov.

2.3 Kako vpliva na delovanje organizacije

Ustvarjanje učinkovite politike varnosti informacij, ki izpolnjuje vse zahteve skladnosti, je ključni korak pri preprečevanju varnostnih incidentov, kot so uhajanje podatkov in kršitve podatkov. Varnostna politika je pomembna tako za nove kot tudi uveljavljene organizacije. Vse večja digitalizacija pomeni, da vsak zaposleni ustvarja podatke in da mora biti del teh podatkov zaščiten pred nepooblaščenim dostopom. Odvisno od dejavnosti podjetja, je to morda zaščiteno celo z zakoni in predpisi (Tunggal Tyas, 2022).

Namen varnostnih politik ni krasiti prazne prostore knjižnih polic. Varnostni pravilniki lahko sčasoma zastarajo, če se ne vzdržujejo aktivno. Varnostno politiko je treba vsaj enkrat letno pregledati in po potrebi posodobiti. Dobra praksa je, da zaposleni potrdijo prejem in se strinjajo, da jih bodo upoštevali tudi vsako leto (Dunham, 2020).

Informacijska varnostna politika tvori hrbtenico strategije in prizadevanj organizacije za kibernetsko varnost. Dobro razvite in dokumentirane politike pomagajo podjetju zaščititi interese v primeru kršitve ali kibernetskega incidenta. Varnosta politika tako obravnava potencialne grožnje podjetja in implementacijo strategij za zaščito podjetja pred notranjimi in zunanjimi grožnjami. Pomaga tudi prepoznati tveganja in oblikovati nagnjenost k tveganju. Prav tako opisuje posledice, s katerimi se soočajo zaposleni, če ne upoštevajo varnostnih pravil podjetja in jih tako ohranjajo odgovorne za svoja dejanja (IdenHaus, 2021).

Kot že večkrat omenjeno, je eden od glavnih namenov varnostne politike zagotoviti zaščito, zaščito organizacije in zaposlenih. Varnostne politike ščitijo kritične informacije ter intelektualno lastnino organizacije z jasnim opisom odgovornosti zaposlenih glede tega, katere informacije je potrebno zaščititi in zakaj. Varnostna politika mora biti podpora poslanstvu

podjetja. Strokovnjaki morajo biti občutljivi na potrebe podjetja, zato je potrebno pri pisanju varnostnih politik paziti na poslanstvo podjetja (Dunham, 2020).

Pomembno je, da vsi od glavnega direktorja do najnovejših zaposlenih spoštujejo pravilnike, vključno z varnostno politiko. Saj če najvišje vodstvo ne spoštuje varnostnih politik in posledice neskladnosti s politiko niso uveljavljene, potem se bo to prej ali slej pojavilo tudi pri ostalih zaposlenih. Navada je, da zaposleni ob pristopu na delovno mesto preberejo varnostno politiko in potrdijo, da so z njo seznanjeni, ponavadi s podpisom izjave (Dunham, 2020).

Kršitve kibernetske varnosti so lahko drage in škodljive za katerokoli podjetje, tako v smislu financ kot tudi ugleda. Nedavne raziskavge so pokazale, da je 43 % organizacij v zadnjih dveh letih doživelo kršitev podatkov, ki je vključevala občutljive podatke o strankah ali podjetju. Na podlagi teh podatkov, dve od petih podjetij vsako leto prizadane resna kršitev, pri kateri je ogrožena znatna količina občutljivih podatkov. Opaziti gre, da skoraj ne mine teden brez vsaj enega poročila o kršitvi podatkov v novicah. Trgovini lahko ukradejo podatke o kreditni kartici. Zdravstvena zavarovalnica je morda izgubila evidenco svojih zavarovancev. Vlada izgubi evidenco dovoljenj – medtem ko je tisto, kar bi morala biti zasebna elektronska pošta, zdaj objavljeno na aktivističnih spletnih mestih. Zdi se, da nobena zasebna ali javna organizacija ni v celoti zaščitena pred kibernetskimi napadi. Narava kibernetskih napadov je veliko bolj napredna. Sprva je bila najpogostejša tarča elektronska pošta, na primer sporočila »bank«, ki zahtevajo podrobnosti o računu ali osebne podatke. Ko pa je računalništvo napredovalo, so se tudi kibernetski napadi premaknili k operacijam večjega obsega, ki niso več omejene na posameznika, temveč na podjetja, finančne trge in vladni sektor. Glede na študije, ki jih je izvedel IBM je povprečni strošek vdora podatkov 3,62 milijona dolarjev, kar je za številna podjetja neznosen strošek (Senhasegura, 2021).

2.4 Standardi SIST ISO/IEC 27001:2013

ISO (Mednarodna organizacija za standardizacijo) in IEC (Mednarodna komisija za elektrotehniko) tvorita specializiran sistem za svetovno standardizacijo. Nacionalni organi, ki so člani ISO ali IEC, sodelujejo pri razvoju mednarodnih standardov prek tehničnih odborov, ki jih ustanovi zadevna organizacija za obravnavanje dooločenih področij tehnične dejavnosti. Tehnična odbora ISO in IEC sodelujeta na področjih skupnega interesa. Pri delu sodelujejo tudi druge mednarodne organizacije, vladne in nevladne, v povezavi z ISO in IEC (ISO, 2013).

ISO/IEC 27001:2013 je mednarodni standard, ki je bil pripravjen, da zagotovi zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja varnosti informacij. Uvedba sistema upravljanja informacijske varnosti je strateška odločitev organizacije. Na vzpostavitev in izvajanje sistema upravljanja informacijske varnosti organizacije vplivajo potrebe in cilji organizacije, varnostne zahteve, uporabljeni organizacijski procesi ter velikost in struktura orgnaizacije (ISO, 2013).

V skladu s standardom ISO 27001:2013 je cilj politik informacijske varnosti zagotoviti vodenje in podporo za varnost informacij v skladu s poslovnimi zahtevami ter ustreznimi zakoni in predpisi (Mathenge, 2021).

Standard SIST ISO/IEC 27001 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve 2013 ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27001 (Slovenski inštitut za standardizacijo, 2013).

Pridobitev standarda SIST ISO/IEC 27001:2013 je strateška odločitev za organizacijo. Na to odločitev vplivajo potrebe, cilji organizacije, varnostne zahteve, uporabljeni organizacijski procesi ter velikost in struktura organizacije. Varnostna politika, kot prej omenjeno vsebuje zaupnost, celovitost in razpoložljivost informacij, kar pa je tudi namen standarda, saj sistem upravljanja informacijske varnosti ohranja te lastnosti. Standard določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti v okviru organizacije. Določene so tudi zahteve za ocenjevanje in obravnavanje tveganj informacijske varnosti, prilagojene potrebam organizacij (Slovenski inštitut za standardizacijo, 2013).

V anketi je ena oseba omenila, da imajo TISAX certifikat, katerega bomo na kratko tudi upoštevali, saj doda informacijski varnosti neko novo razsežnost, seveda za točno določeno skupino podjetij. TISAX (Trusted Information Security Assessment Exchange) je standard, ki so ga razvili evropski proizvajalci vozil, dobavitelji in organizacije kot mehanizem za ocenjevanje in izmenjavo informacijske varnosti v avtomobilski industriji. Prinaša standardizacijo, zagotovilo in medsebojno priznavanje presoj informacijske varnosti, skladnih s standardi ISO 27001. V letu 2017 je TISAX postal usklajen z zahtevami VDA ISA (VDA je nemško združenje avtomobilske industrije, ISA pa je okrajšava za »Information Security Assessment«), zato nekateri ta standard poznajo tudi kot VDA TISAX. Podjetju omogoča, da izpolni industrijske zahteve in končnim uporabnikom dokaže, da varstvo podatkov jemlje resno.

Poleg standardizacije TISAX prinaša zagotovilo in vzajemno priznavanje presoj informacijske varnosti v skladu s standardi ISO 27001. V avtomobilski industriji obstaja veliko povpraševanje po dobaviteljih, skladnih s standardom TISAX, kot zagotovilo, da bodo občutljivi podatki ustrezno zaščiteni. Zato pridobitev tega certifikata daje podjetjem konkurenčno prednost. Zanimivo je tudi, da je ta standard zelo podoben standardu ISO 27001 in varnostnim kontrolam priloge A. Kot standard, ki ga priznavajo glavni akterji v avtomobilski industriji, TISAX proizvajalcem zagotavlja skupno podlago za oceno tveganj za varnost informacij o svojih izdelkih in izvajanje ustreznih kontrol za njihovo obravnavo. Poleg tega omogoča tudi varno izmenjavo informacij o ocenah različnih proizvajalcev ter njihovo primerjavo, kar povečuje razumevanje tveganj in zrelost varnostnega pristopa v panogi kot celoti. Kot rečeno, je TISAX zelo podoben kontrolam ISO 27001 dodatku A, vendar dodajajo posebne varnostne kontrole za povezavo s tretjimi osebami, zaščito prototipa in varstvo podatkov. Za vsako zahtevo TISAX uporablja stopnje zrelosti, da pokaže učinkovitost, poleg tega pa TISAX za vsako zahtevo opredeli ciljno zrelost. V ISO 27001 koncept stopenj zrelosti ne obstaja, ker morajo le implementirati varnostne kontrole, ki so potrebne za oceno tveganja (Leal, 2019).

2.5 Postopek izdelave varnostne politike

Podjetje brez pravil bi bilo v kaosu. Nihče ne želi obravnavati skrbi, za katero ni prepričan, kako ravnati v skladu s postopkom podjetja. Zato je nujno, da se varnostne smernice napišejo že na samem začetku. Veliko vzorcev se najde na spletnih straneh, obstajajo pa tudi podjetja, ki lahko pomagajo podjetjem pri izdelavi varnostne politike. Eno izmed teh podjetij je tudi B2 IT d.o.o., ki omogoča vzpostavitev in vpeljavo sistema informacijske varnosti.

Tisti, ki želijo ustvariti varnostno politiko, je dobro, da pregledajo ISO 27001. Čeprav standard ne navaja posebnih vprašanj, ki jih mora zajeti varnostna politika, zagotavlja okvir okoli katerega lahko podjetje gradi. Z upoštevanjem standarda bo varnostna politika zagotovo obsegala cilje informacijske varnosti, zagotavljanje informacijske varnosti, informacije o izpolnjevanju pogodbenih, pravnih in regulativnih zahtev ter zavezo za nenehno izboljševanje (Irwin, 2020).

Glede na zadnja leta, se je uporaba oddaljenega dostopa povečala. Že zaradi vpliva koronavirusa so podjetja morala prilagoditi varnostno politiko, saj mogoče določena podjetja do takrat niso imela urejenih oddaljenih dostopov oziroma ne za celotno podjetje. Ta del varnostne politike obravnava ranljivosti, ki se pojavljajo, ko zaposleni niso zaščiteni z omrežno varnostjo organizacije. V tem delu se določi stališče organizacije glede dostopa do omrežja na

daljavo. Lahko na primer piše, da je oddaljeni dostop prepovedan, da ga je mogoče izvajati le prek VPN ali da morajo biti dostopni na daljavo samo nekateri deli omrežja (Irwin, 2020).

Naslednja pomembna točka so gesla. Praktično vsaka organizacija daje svojim zaposlenim uporabniške račune, ki jim omogočajo dostop do občutljivih informacij. Toda če zaposleni ne zavarujejo teh računov z močnimi gesli, jim bodo kriminalni hekerji lahko vdrli v nekaj sekundah. Organizacije morajo to tveganje zmanjšati z oblikovanjem strogih pravil o tem, kaj je sprejemljivo geslo (Irwin, 2020).

Vodje pogosto skrbi, da osebje med uradnimi urami opravlja dejavnosti, ki niso povezane z delom. Vendar bi jih moralo bolj skrbeti, kaj delajo zaposleni, kot kdaj to počnejo. Organizacije so na splošno sprejele, da bodo zaposleni občasno preverjali svojo osebno e-pošto ali Facebook. Vendar bi morali potegniti črto pri dejavnostih, ki bi lahko vplivale na varnost organizacije, kot je obiskovanje zahrbtnih spletnih mest, nameščanje potencialno nevarnih aplikacij ali deljenje delovnih informacij z ljudmi, ki ne delajo v organizaciji. Velik del tveganja lahko podjetja preprečijo tako, da blokirajo določena spletna mesta. Vendar to ni sistem lažne prevare, zato je priporočljivo, da se zaposlenim prepoveduje obiskovanje kateregakoli mesta, ki se nam zdi nevarno. Seveda v kolikor v nastavljena pravila pade spletno mesto, ki je varno, se le to lahko pošlje na IT podporo, kjer zahtevek preverijo in v kolikor je spletno mesto varno, se dostop do tega omogoči (Irwin, 2020).

Pisanja varnostne politike se lahko lotimo na več načinov. En način je, da se napiše en zelo obsežen dokument, drugi način pa, da naredimo več politik glede na različne kategorije varnostne politike. S tem ko se varnostna politika razbije na več manjših delov, lahko lažje obvestimo točno določene osebe glede varnostne politike – namreč kakšen del varnostne politike se ne bo dotikal vseh zaposlenih a le peščico zaposlenih. Tako prav tako dosežemo, da bodo zaposleni bolj verjetno prebrali in se seznanili z varnostno politiko, če je le ta sestavljena v več kratkih delih. Seveda pa ima vsaka izbira dobre in slabe lastnosti. Dobre lastnosti le enega dokumenta so, da jih je lažje posodabljati in vzdrževati, slabe pa, kot navedeno, da je težje politiko skomunicirati s samo določeno publiko. Na spletnem svetu pa krožijo tudi raznorazne predloge za pisanje varnostne politike, katero si je moč prenesti in prilagoditi glede na potrebe in velikost posamezne organizacije ali podjetja (Barker, 2022).

Dobro je začeti nekako tako. Najprej se je potrebno dogovoriti na kakšen način se bo politiko nadzorovalo in kako se jo bo spreminjalo. ISO 27001 zahteva kontrolo, spremembe, datume sprememb itd. Tako da si lahko za smernice vzame podjetje tudi kontrole, ki jih zahteva ISO.

Seveda se iz tega izlušči kar je primerno za podjetje. Nato napišemo, kaj je namen samega dokumenta, na primer namen določenega dela varnostne politike je zaščita pred izgubo podatkov. Prav tako je potrebno razmisliti o obsegu varnostne politike in koga vse se bo varnostna politika dotikala. Minimalno mora obsegati vse zaposlene v podjetju ter tretje osebe, ki delajo za podjetje (zunanje podjetje, ki skrbi za sistem, zunanje podjetje, ki zagotavlja ERP, BI storitve ipd.). Seveda pa je pri vsakem pravilniku, ki živi v podjetju pomembno, da se tudi najvišje vodstvo strinja z vsebino politike, jo razume ter najbolj pomembno jo podpira in tudi samo uporablja ter je dober zgled ostalim zaposlenim. Zato je dobro, da se napiše izjava, da se najvišje vodstvo oz. kader zavezuje k organizaciji informacijske varnosti. Sedaj pa je potrebno razmisliti katere politike spadajo v varnostno politiko glede na velikost in potrebe. Potrebno je ustvariti definicijo vsake vloge za informacijsko varnost ter kakšne so njihove odgovornosti. Glede na spisano je sedaj treba načrtovati ukrepe in monitoring, ki se bo uporabljal ali pa se že za preverjanje učinkovitosti varnostne politike. Vedno pa je potrebno pregledati še zakonske zahteve. Sedaj že dobro poznana zakonska zahteva GDPR je vsekakor veliko vplivala na varnostno politiko ter organizacijo podjetja, katere osebe lahko dostopajo do podatkov in katere dostopa ne smejo imeti. S tem smo pridobili tudi potrebe za izjave o soglasju o obdelavi osebnih podatkov itn. V kolikor je dejavnost podjetja taka, ki zbira in na kakršen koli način obdeluje osebne podatke, je to vsekakor potrebno vključiti v varnostno politiko podjetja. Potrebno pa se je zavedati, da papir prenese vse. Zato je dobro, da se navede kako in na kakšen način bo dosežena skladnost novo obstoječega pravilnika (Barker, 2022).

3 VPLIV DIGITALNE PREOBRAZBE NA OKOLJE

Kljub navidezno ločenemu obstoju od fizičnega sveta je digitalna dejavnost ustvarila svoj malo verjeten ogljični odtis. Glede na študijo projekta Shift iz leta 2019 je skupni digitalni ogljični odtis na svetu dejansko predstavljal skoraj 3,7 odstotka vseh toplogrednih emisij, kar je primerljivo z ravnmi emisij letalske industrije. Poleg tega se je poraba energije digitalne tehnologije med letoma 2013 in 2020 povečala za skoraj 70 odstotkov (Geneva Environment Network, 2021).

Čeprav je digitalna tehnologija pogosto spregledana kot primarni proizvajalec ogljika, je njen vpliv na globalno trajnost zelo razširjen – tako kot njene izvorne točke. Digitalna dejavnost je postala večplastna entiteta, ki vključuje vse od pretakanja videa in spletnih iger, do trgovanja s kriptovalutami in digitalnega bančništva. Ti mediji, čeprav so sami po sebi pogosto koristni in napredni, imajo okoljsko ceno. Prispevajo k naraščajočemu dotoku podatkov, spodbujajo cikel obdelave podatkov in posledično ustvarjanje emisij (Geneva Environment Network, 2021).

Biti in bajti so našim očem nevidni, motorji ki vodijo to skrito mrežo, pa so zgrajeni iz izvlečnih materialov. Tudi ta postopek ekstrakcije kot proizvodni proces za pretvorbo mineralov v celico telefonov, računalnikov in strežnikov ima svoj okoljski odtis v celotnem življenjskem ciklu. Življenjska doba strojne opreme pa je relativno kratka. Pogosto le nekaj let. Izzivov pravilnega zbiranja in v najboljšem primeru recikliranja je še vedno ogromno. T. i. »e-odpadki« so najhitreje rastoči tok gospodinjskih odpadkov na svetu. Okvirno 20 odstotkov e-odpadkov se reciklira, preostalih 80 odstotkov pa konča na odlagališčih. E-odpadki, ki so odloženi na odlagališčih, onesnažujejo zemljo in podtalnico (UN Environment programme, 2021).

Microsoft je že preizkusil podvodni podatkovni center z 864 strežniki in 27,6 petabajtov diska (približno enako 27,6 milijona gigabajtov), tesno zapakiranih v jekleni valj, ki je napolnjen s suhim dušikom in potopljen v Severno morje. Analiza samega poskusa še poteka, vendar zaenkrat kaže na uspeh in možen nov trend v prihodnosti. Prve ugotovitve so pokazale, da je imel podvodni podatkovni center le osmino manjšo stopnjo napak kot na kopnem, in da so podvodni podatkovni centri izvedljivi ter logistično, okoljsko in ekonomsko praktični. Podatkovni centri, postavljeni na morsko dno, stran od jedkega kisika, vlage in udarcev lahko dejansko bolje uspevajo kot v istem okolju v katerem živimo ljudje (Christian, 2020).

Strokovnjaki ocenjujejo, da skoraj dva odstotka vsega svetovnega ogljičnega odtisa prihaja iz podatkovnih centrov. Tako da so podatkovni centri lahko za planet tudi dobri. Skoraj 20

odstotkov energije, ki jo porabijo kopenski podatkovni centri, ohranja vse hladno s pomočjo klimatskih naprav in sladkovodnih virov. Kar pa je naredil Microsoft, je prelomno, saj je naravna morska voda delovala kot hladilno sredstvo namesto umetno črpanega zraka. Zdi se, da so podvodni podatkovni centri bolj zanesljivi in energetsko učinkovitejši a se obala polna potopljenih podatkovnih centrov morda ne zdi najboljša ideja za morsko življenje. Vendar pa morski ekologi ne vidijo negativnega vpliva, saj kadar se neka stvar postavi v morje, pride do procesa obraščanja. Obloga bakterij se pojavi v nekaj dneh, ki lahko v bodoče deluje tudi kot umetni greben okoli katerega se nato zbirajo ribe (Christian, 2020).

Slika 2 Microsoftov podatkovni center vzet iz Severnega morja

Vir: https://www.wired.co.uk/article/data-centres-underwater-climate-crisis

Microsoft podvodnih podatkovnih centrov ne vidi kot zamenjavo kopenskih, vendar kot dodatno ponudbo za storitve strankam (Christian, 2020).

3.1 Spreminjanje varnostne politike

V današnjem zelo povezanem svetu se nove kibernetske grožnje in tveganja pojavljajo vsako uro. Ne glede na to za kakšen napad gre, povezovanje sistemov in delovnih postaj organizacije z internetom vedno odpre možnost kibernetskega napada. Tako kot se kibernetske grožnje

nenehno razvijajo, bi se morale spreminjati tudi varnostne politike, ki so temelj kibernetske varnosti (Mallory, 2020).

Zastarele varnostne politike lahko ogrozijo našo organizacijo, onemogočijo skladnost z novimi zakoni in predpisi, ustvarijo neskladja med najboljšimi praksami in dejanskimi operacijami ter pustijo naše IT sisteme in tehnologijo ranljive. V nekaterih primerih redne preglede predpisujejo industrijski in vladni standardi skladnosti, na primer na področju javne varnosti, bančništva, izobraževanja in zdravstvenega varstva (Mallory, 2020).

Če ne prej, bo morala organizacija pregledati in posodobiti varnostno politiko v skladu z nenehno spreminjajočimi se zakoni ter predpisi. Vsakič ko bo prišlo do regulativne spremembe, bo morala organizacija opraviti pregled pravilnika, ugotoviti kaj je potrebno spremeniti ali dodati, koliko časa lahko traja uvedba teh sprememb in morebitne druge posledice za poslovanje (Mallory, 2020).

3.2 Vpeljava sprememb zaposlenim

Potrebno je zagotoviti veliko usporabljanja pred uvedbo novih varnostnih politik za zaposlene, lahko vse naenkrat ali pa po oddelkih, v kolikor veljajo določene specifike. S tem se zagotovi, da bodo zaposleni imeli priložnost razumeti kakšne so politike, zakaj se izvajajo ter kakšne so posledice varnosti za organizacijo. To bo zaposlenim dalo dovolj časa, preden bodo pravilniki stopili v veljavo, da se bodo seznanili z njimi ter postavili morebitna vprašanja ali obravnavali pomisleke. Ko pride čas za izdajo posodobljene ali nove varnostne politike, je potrebno zagotoviti, da so vsi zaposleni prebrali in podpisali novo varnostno politiko (OSI, 2021).

Varnostna politika niso le smernice, ampak morajo biti obvezna sestavina zaposlovanja v podjetju. Pravilniki v podjetju morajo jasno navajati kazni za vsako kršitev ali kršitve varnostnih pravil. Če kdo te pravilnike krši, je potrebno zagotoviti, da obstaja ustrezen postopek pri kadrovski službi, da zaposlenega ustrezno opomni ali ponovno usposobi (OSI, 2021).

Prav tako je potrebno vzeti na znanje, da v današnji dobi digitalizacije obstaja nešteto podatkovnih točk, do katerih imajo zaposleni dostop, da jih uredijo ali prenesejo, ali celo delijo z drugimi. Podjetje mora varovati podatke o podjetju in strankah znotraj in zunaj pisarniških prostorov, hkrati pa imajo zaposleni temeljno človekovo pravico do zasebnosti in spoštovanja zasebnega življenja, zato je pri izvajanju varnostnih politik pomembno upoštevati in najti primerno ravnotežje (GVZH Advocates, 2020).

Še posebej pa je potrebno pripraviti proces vpeljave varnostne politike in možnih novih omejitev pri uporabi službenih računalnikov, v kolikor so do sedaj zaposleni imeli dostop do vsega. Povsem jasno je, da v službenem času ni primerno uporabljati službeno opremo za privatne namene, pa vseeno večina zaposlenih oseb to počne. Od spletnega nakupovanja, rezervacije dopusta, pregled novic, igranje spletnih iger ipd. Že na podlagi Zakona o delovnih razmerjih mora delodajalec varovati in spoštovati delavčevo osebnost ter upoštevati in ščititi njegovo zasebnost. Večina podjetij to rešuje tako, da omejijo dostop do raznih spletnih strani, spletnih omrežij itd. (Brajnik, 2019).

Smernice, katere lahko pomagajo pri vpeljavi varnostne politike in njihovih sprememb zaposlenim so:

- Bodimo zgled (z zgledom svoji ekipi dokazujemo, da ravnamo v skladu s praksami kibernetske varnosti svojega podjetja, kar jim ne daje razloga, da tega ne bi storili. Če od zaposlenih zahtevamo, da naredijo nekaj, česar nam ni prijetno ali preprosto, se bodo spraševali zakaj bi potem to morali oni).
- Postavimo mejnike (če svoji ekipi posredujemo načrt upravljanja IT, bomo preprečili, da bi bili bombandirani s preveč spremembami in opravili naenkrat. Poleg sporočanja časovnice izvajanja novih ukrepov jim sporočimo kaj točno velja pri posameznem ukrepu in zakaj je tako pomemben. Ugotovili bomo, da ko bo naša ekipa razumela, kaj se dogaja in zakaj, bo bolj nagnjena k podpori procesa, namesto da bi ovirala uvedbo).
- Pojasnimo zakaj so varnostne politike IT pomembne (vsak ukrep, ki ga nameravamo izvesti, pojasnimo zakaj je tako pomemben. Zaposlenim dajmo jasen razlog, zakaj potrebujemo njihovo podporo. Vredno je vložiti čas in trud v razlago ukrepov na začetku, da preprečimo zamude in neskladnosti).
- Naj bo stvar kadrovske službe (povežimo se s svojim kadrovskim oddelkom, strokovnjaki za človeške vire so vešči učinkovite komunikacije, izboljšanja kulture podjetja in razumevanja zaposlenih na globji ravni, zaradi česar so bolje opremljeni za obvladovanje vseh nasprotnih argumentov, ki se lahko pojavijo).
- Zagotovimo si aktivno pomoč (vsi se ne spoznajo na sisteme IT, kar se zdi nekomu v oddelku IT preprosto in samoumevno, je lahko totalna novost za enega od zaposlenih, zato z aktivno pomočjo zaposlenim natančno pokažimo, kako se lotiti izvajanja novih pravilnikov).

- Upoštevajmo vrzel v znanju (prepričajmo se, da je IT dokumentacija napisana in ilustrirana v lahko razumljivem slogu za nestrokovne bralce z ustreznimi predlogami varnostnih politik; tako bodo vsi lahko razumeli in sledili zahtevi ne da bi pri tem ovirali IT žargon).
- Pojasnimo posledice (brez varnega omrežja IT obstaja velika nevarnost, da postanemo tarča hekerjev in jim omogočimo odprt dostop do občutljivih informacij. Bodimo odkriti s svojimi zaposlenimi glede tega, kaj je ogroženo, če se ti varnostni pravilniki ne izvajajo in gredo stvari narobe).
- Nagrajuje skladnost (ugotovimo katero vrsto nagrade bi naši zaposleni najbolj cenili in jo uporabimo kot spodbudo za najhitrejšo osebo, da izvede določen varnostni ukrep, nekateri bodo morda cenili dodatno uro kosila itd.).
- Vaja dela mojstra (izkoristimo različne metode usposabljanja, ki so na voljo, da poučimo svoje zaposlene o novih varnostnih ukrepih, dober primer je Varnost v pisarni).
- Zahtevajmo povratne informacije o politikah (ni boljšega načina za izboljšanje uvajanja, kot da prisluhnemo izkušnjam zaposlenih in ukrepamo v skladu s tem).
- Uveljavimo lažjo pot (poenostavimo postopek, kolikor je le mogoče. Manj kot je zapleten postopek, bolj poenostavljena bo naša uvedba).
- Bodimo sočutni (bodimo razumevajoči in sočutni v svojem pristopu, za osebje zunaj IT oddelka te zadeve niso samoumevne, pogovarjajmo se z njimi, preglejmo problematična področja in ponudimo čim več pomoči).
- Načrt (začrtajmo vsak korak postopka uvedbe že od začetka, ko uvajamo nove varnostne politike. To dela čudeže, saj zagotavlja, da se tega lotimo brez nepotrebnih zamud in ovir).
- Pridobimo marketing (pri uvajanju novih varnostnih protokolov bi lahko bilo zelo koristno imeti marketinško ekipo našega podjetja, ki bi nam pomagala »prodati« idejo našim zaposelnim) (EASYDMARC, 2021).

3.3 Spodbude digitalne preobrazbe in nepovratna sredstva

Slovenski podjetniški sklad je imel v zadnjih letih kar nekaj razpisov ter vavčerjev vezano na digitalizacijo podjetij. Podjetja so lahko prejela do sto tisoč evrov nepovratnih sredstev za digitalno nadgradnjo poslovnih procesov, sofinanciranje je 60-odstotno. Vsaka preobrazba in korak v smeri digitalizacije se začne, ko vodstvo sprejme odločitev, da bo podjetje naredilo nekaj v smeri digitalizacije. Vodstvo mora stati za odločitvijo digitalizacije in v to vključiti tudi

zaposlene ter jim razložiti, da bo to dobro vplivalo na vse. Saj so ravno zaposleni tisti, ki bodo imeli na koncu največ opravka z digitalizacijo, ker se bodo lahko poslovni procesi spremenili, mogoče bo potrebno uvesti nov program, ki bo zahteval sodelovanje zaposlenih iz vseh oddelkov (Ogorevc, 2021).

Pri vseh razpisih za nepovratna sredstva je potrebno pred prijavo izdelati načrt, kaj se bo spremenilo, kaj podjetje potrebuje, kaj je ključnega pomena in kako bodo to uresničili. S katerimi izvajalci bodo nastopili ter ali izvajalci lahko uresničijo zastavljene cilje podjetja. Pod upravičene stroške lahko padejo različne stvari, odvisno od razpisa ali vavčerja. Nekateri razpisi dovoljujejo nakup opredmetenih osnovnih sredstev (strojna oprema), nakup neopredmetenih osnovnih sredstev (nova programska oprema), stroške storitev zunanjih izvajalcev ter določen odstotek stroškov plač zaposlenih, ki so ključni akterji pri izvedbi razpisa (Ogorevc, 2021).

Poleg dobrega načrta digitalizacije pa je potrebno doseči določeno število točk za prag uspešnosti in odobritve nepovratnih sredstev. Na vse to vpliva, kakšen bo vpliv na okolje zaradi transformacije, zvišanje dodane vrednosti na zaposlenega, ocena projekta digitalne transformacije ter ocena skladnosti akcijskega načrta z zastavljenimi cilji. So pa tudi točke na katere podjetje ne more vplivati, kot so status vlagatelja (starost podjetja, regija sedeža podjetja ipd.) (Ogorevc, 2021).

3.3.1 Vavčer za kibernetsko varnost

Slovenski podjetniški sklad je nekajkrat objavil vavčer za kibernetsko varnost, za mikro, mala ter srednja podjetja. Vavčer je moč izkoristiti za sofinanciranje v višini deset tisoč evrov za sistemski varnostni pregled in/ali penetracijski test. Pri penetracijskem testu etični hekerji poskušajo vstopiti v poslovni informacijski sistem. S tem poskušajo dokazati, da je ranljivosti, ki so bile odkrite pri sistemskem varnostnem pregledu, dejansko možno izkoristiti. Sistemski varnostni pregled pa poišče varnostne pomankljivosti v računalniških sistemih in omrežju. Kakovostni varnostni pregled vključuje v analizo nekaj več kot 50 tisoč različnih ranljivosti (Žnidaršič, 2021).

Varnostni pregled je cenejša metoda ugotovitve aktualnega stanja ranljivosti podjetja. Priporočljivo je, da se pregled izvede vsaj enkrat letno. Za penetracijski test pa velja, vsaj za večino podjetij, da se opravi ob vsaki resni nadgradnji lastne programske opreme ali pri razvoju nove lastne aplikacije. Priporočljivo je prav tako, da se pred pregledom ne spreminja nič na

sistemu. Ravno namen pregleda je ugotoviti realno stanje sistema in ne t. i. olepšanega sistema za namene pregleda. Najbolj pogoste pomanjkljivosti sistema so zastarele programske opreme brez potrebnih posodobitev, varnostno nepodprto opremo, odpra vrata, neustrezne politike gesel ter raba privzetih in premalo varnih gesel (Žnidaršič, 2021).

V splošnem je dobro spremljati razne razpise za nepovratna sredstva, saj nam lahko podjetjem prihranijo nekaj denarja za izvedbo varnostnih pregledov in penetracijskega testa. Na podlagi poročila lahko podjetje odpravi pomanjkljivosti in lahko dopolni varnostno politiko, glede na ugotovljena tveganja med pregledom ali testom in se tako bolje pripravi na postopek reševanja grožnje v kolikor se le ta uresniči.

3.3.2 Vavčer za digitalno strategijo

Podjetja se zavedajo, da pri digitalni transformaciji potrebujejo pomoč. Pri tem je v zadnjih letih veliko pripomogel Slovenski podjetniški sklad, ki je izdal razne vavčerje ter razpise za pomoč pri digitalizaciji. Za pomoč pri razpisih in vavčerjih pa so podjetja lahko našla strokovnjake preko kataloga digitalnih strokovnjakov na spletni strani DIH Slovenija – Digitalno inovacijsko stičišče Slovenije. V njem podjetja najdejo za vsak vavčer posebej potrebne strokovnjake ter okvirno vrednost njihovih storitev (AskIT, 2022).

Digitalna strategija vsebuje odgovor, kako bo podjetje uspešno vpeljalo digitalizacijo glede na obstoječe stanje, ki mogoče ne obstaja ali pa je ekstremno slabo razvito. Za potrebe vavčerja za digitalno strategijo mora biti le ta pripravljena v skladu s smernicami DIH Slovenija, saj bodo oni preverjali samo ustrezne strategije. Strategija mora nujno vsebovati sledeče tri sklope: ocena stanja na področju digitalizacije podjetja, priprava načrta razvoja digitalnih zmožnosti podjetja, priprava strategije za podjetje za digitalno strategijo s ključnimi področji (izkušnja kupca, podatkovna strategija, procesi in digitalne rešitve za podporo poslovanja, kibernetska varnost, industrija 4.0, strategija razvoja digitalne kulture, strategija razvoja digitalnih kadrov in digitalnih delovnih mest, digitalni poslovni modeli, produkti in storitve ipd.) (AskIT, 2022).

Podjetja zmotno mešajo IT strategijo z digitalno strategijo. Digitalna strategija je nadgradnja IT strategije in je integriran del poslovne strategije. Digitalna strategija vleče osnovo iz poslovanja podjetja, njegovih kupcev in na podlagi tega dodaja zmožnosti digitalnih tehnologij in rešitev. Zato je pomembno, da si strokovni svetovalec iz DIH kataloga, vzame zadosti časa,

da dobro razume poslovni del celotne zgodbe, ki vključuje tako digitalno ekonomijo ter digitalne kupce, kot tudi notranji proces in kulturo organizacije (AskIT, 2022).

3.3.3 Vavčer za dvig digitalnih kompetenc

Namen vavčerja je spodbuditi zagotovitev ustreznih znanj zaposlenih in vodstvenega kadra za ključna področja digitalizacije, s čimer bi se povečala njihova konkurenčnost, dodana vrednost ter prihodki od prodaje. Upravičenci so mikro, mala in srednje velika podjetja s sedežem v Republiki Sloveniji, ki se kot pravna ali fizična oseba ukvarjajo z gospodarsko dejavnostjo in so organizirana kot gospodarske družbe, samostojni podjetniki posamezniki ali zadruge. Minimalna višina subvencije za omenjeni vavčer je 1.000,00 EUR, maksimalna višina subvenije pa 9.999,00 EUR. Kot upravičen strošek se smatrajo usposabljanja, torej stroški zunanjega izvajalca, ki pa mora biti definiran v DIH katalogu (RCR, 2022).

3.3.4 Vavčer za digitalni marketing

Namen vavčerja za digitalni marketing je uvajanje digitalnega marketinga pri podjetju in si s tem povečati konkurenčnost, dodano vrednost ali prihodke od prodaje. Za izdelavo spletne strani je podjetje lahko dobilo sofinancirane stroške do 60 %, in sicer največ 1.500 EUR, za izdelavo spletne trgovine je podjetje lahko dobilo sofinancirane stroške zopet do 60 %, ampak največ 2.500 EUR, za mobilno aplikacijo je bilo sofinanciranje tudi 60 % v višini 1.000 EUR in nazadnje za rezervacijsko platformo je podjetje ponovno lahko dobilo sofinancirano do 60 %, in sicer v višini 2.500 EUR (DIH Slovenija, 2022).

3.3.5 Razpis za digitalno transformacijo

Upravičenci na razpisu za digitalno transformacijo so bila mikro, mala in srednje velika podjetja z najmanj petimi zaposlenimi na dan objave javnega razpisa in pravne ali fizične osebe, ki se ukvarjajo z gospodarsko dejavnostjo. Višina financiranja 60 % je variirala glede na prijavljen znesek, in sicer v rangu od 30.000 EUR pa vse do 100.000 EUR, ob predpostavki, da DDV ni upravičen strošek. Kot upravičen strošek se je štel nakup opredmetenih in neopredmetenih osnovnih sredstev pod pogojem, da so nove, stroški zunanjih izvajalcev, na primer kibernetski

varnostni pregled, razna izobraževanja ipd. ter stroški plač in povračil stroškov v zvezi z delom za največ dva zaposlena (DataLAB, 2021).

4 KONČNE UGOTOVITVE HIPOTEZ

Anketo, ki je priložena v prilogi sem poslala naokoli podjetjem, ki so dobila vavčer za kibernetsko varnost ali prejela sredstva iz naslova razpisa za digitalno transformacijo podjetja.

Na anketo je odgovorilo skupaj 40 podjetij. Od tega je bilo devet mikro podjetij, 21 majnih in deset srednjih. Velikost podjetja je opredeljena v zakonu o gospodarskih družbah ZGD-1.

Graf 1 Velikost anketiranih podjetij

Vir: lasten

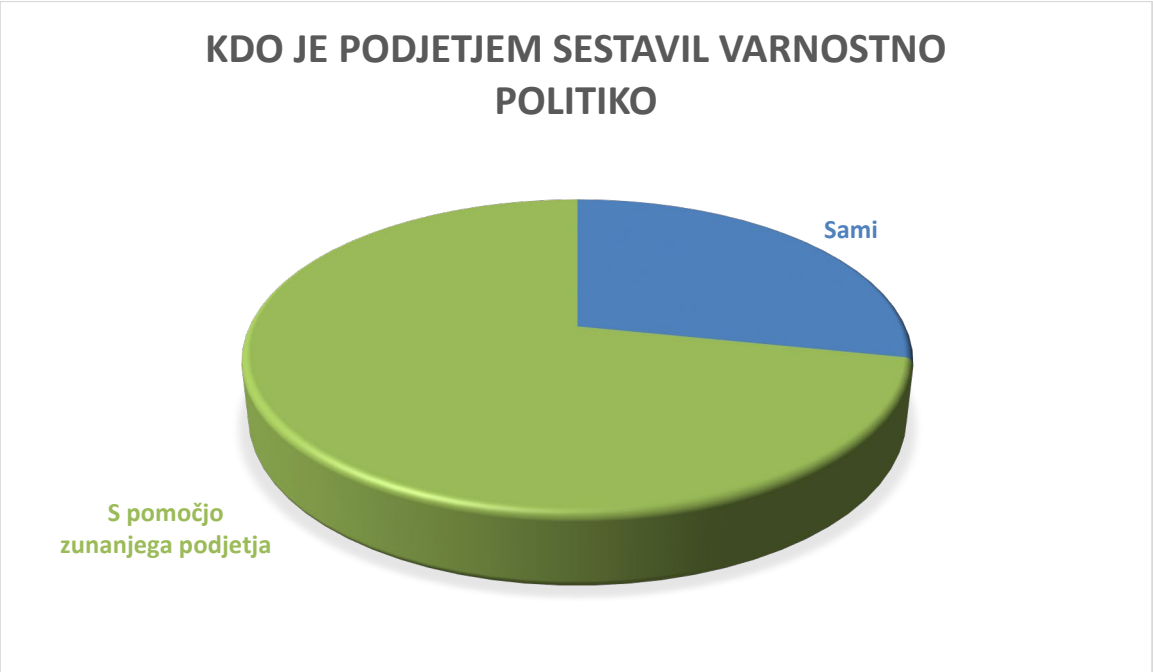
Poleg velikosti podjetja, ima določen vpliv še v kateri kohezijski regiji ima podjetje sedež; namreč večji del subvencij se ponavadi prispeva Vzhodni regiji kot Zahodni, z namenom, da se poveča razvoj tudi na tem delu Slovenije. Vendar je med anketiranimi podjetji večina podjetij iz Zahodne regije, kar je presenetljivo, saj imajo ponavadi prednost podjetja iz Vzhodne regije.

Graf 2 Kohezijska regija anketiranih podjetij

Vir: Lasten

4.1 Podjetja imajo varnostno politiko

Sledilo je vprašanje, ali si podjetja varnostno politiko sestavijo sami ali s pomočjo zunanjega podjetja. Namreč v Sloveniji je kar nekaj podjetij, ki sestavijo varnostno politiko glede na zahteve, eno izmed teh podjetij je B2 d.o.o. Od 40 anketiranih podjetij je 11 podjetij oblikovalo varnostno politiko samo, 28 podjetij pa je za izdelavo izbralo zunanje podjetje. Eno podjetje na to vprašanje ni odgovorilo, kar pomeni, da podjetje varnostne politike nima izdelane.



Graf 3 Kdo je podjetjem sestavil varnostno politiko?

Vir: Lasten

Potrebno se je zavedati, da je varnostna politika živ dokument, ki ga je potrebno nenehno spreminjati in dopolnjevati. 17 podjetij varnostno politiko posodobi na letni ravni, dve podjetji na polletni ravni, medtem ko jo 11 podjetij posodobi le ob pomembnih dogodkih, na žalost pa osem podjetij svoje varnostne politike še ni posodobilo. V kolikor so jo ravno izdelali in vpeljali, slednje ne predstavlja težav in upamo, da bodo v prihodnje posodobitve izvajali redno.

Graf 4 Pogostost posodabljanja varnostne politike

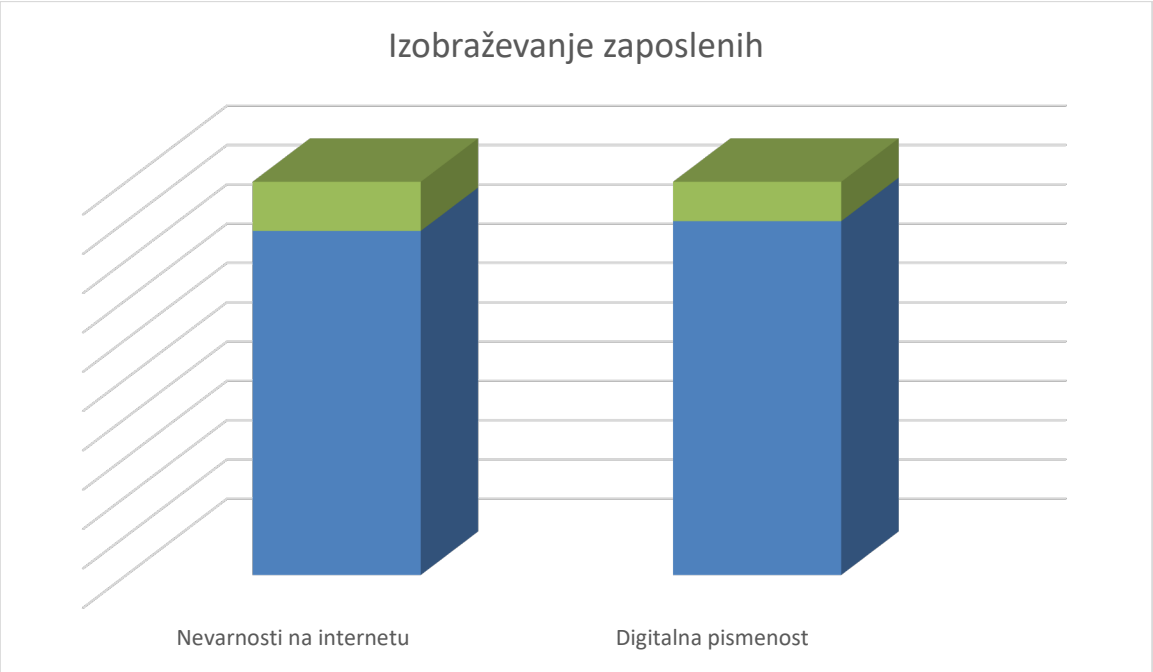
Vir: Lasten

Zaradi vedno večjih groženj na področju informacijske varnosti, razlogi za vpeljavo varnostne politike variirajo. Šest podjetij je izdelalo varnostno politiko zaradi zahtev strank, 12 podjetij zaradi zakonskih zahtev, medtem ko je 21 podjetij izbralo drugo.

Graf 5 Razlog za izdelavo varnostne politike

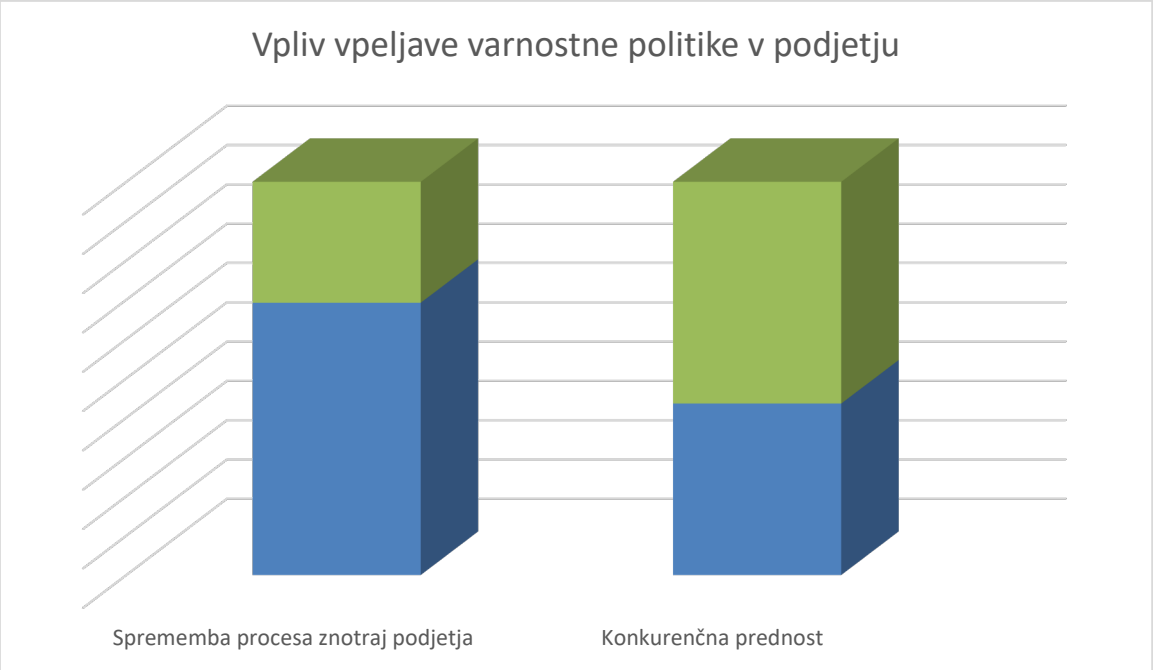
Vir: Lasten

Seveda pa varnostna politika v podjetju ne zadostuje v kolikor zaposleni niso izobraženi. Podjetja izobražujejo svoje zaposlene, in sicer na področju nevarnosti na internetu ter na področju digitalne pismenosti. 35 podjetij izobražuje svoje zaposlene na področju nevarnosti na internetu in eno podjetje več svoje zaposlene na področju digitalne pismenosti izobražuje. Kar je glede na trenutne razmere in pogostost vdorov dober pokazatelj, je, da se podjetja zavedajo, da so tako varna kot njihov najmanj izobražen zaposleni.



Graf 6 Izobraževanje zaposlenih

Vir: Lasten

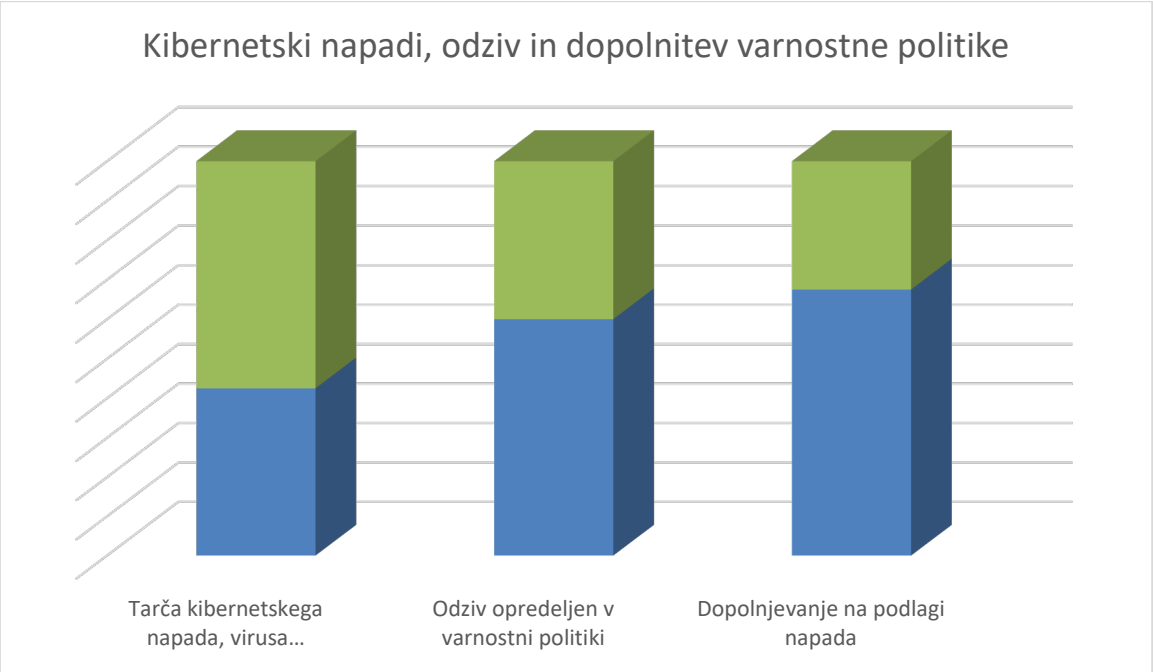


Graf 7 Vpliv varnostne politike v podjetju

Vir: Lasten

Na podlagi ankete 27 podjetij trdi, da so se nekateri procesi v podjetju spremenili zaradi uvedbe varnostne politike, kar je logično, saj je potrebno odpraviti pomanjkljivosti in narediti načrt za odziv na možen vdor. Ter le 17 podjetij meni, da so zaradi varnostne politike pridobile konkurenčno prednost na trgu.

Le 17 podjetij je bilo tarča kibernetskega napada ali virusa, 23 pa se jih očitno še dobro drži in ima dobro urejeno zaščito ter izobražen kader. 24 podjetij od 40 ima opredeljen odziv na kibernetski napad v svoji varnostni politiki, ter 27 podjetij posodablja svojo varnostno politiko na podlagi preteklih kibernetskih napadov oziroma ima namen dopolniti varnostno politiko na podlagi kibernetskega napada ali virusa.



Graf 8 Kibernetski napadi, odziv in dopolnitev varnostne politike podjetij

Vir: Lasten

Večina podjetij ISO certifikata 27001 nima, kar 34 od 40 anketiranih. Tri podjetja certifikat že imajo, tri podjetja pa so v postopku pridobivanja certifikata. Anketiranci so se odločili za ISO certifikat zaradi zahtev strank ali zakonskih zahtev, da imajo določeno stopnjo varnosti podatkov. Pet podjetij od šestih pa meni, da so si s certifikatom pridobili konkurenčno prednost.

4.2 Podjetja se prijavljajo na nepovratna sredstva za digitalizacijo

Podjetja se v večini prijavljajo na razpise za nepovratna sredstva, 34 od 40 anketiranih se je prijavilo na razpise ali vavčerje za nepovratna sredstva, dve podjetji se nista prijavili. medtem ko se štiri podjetja že nekaj časa s prijavo spogledujejo.

Graf 9 Prijava na razpise za nepovratna sredstva

Vir: Lasten

Največ podjetij se za prijavo na razpise za nepovratna sredstva prijavi zaradi sredstev, saj večina razpisov ponuja približo 60-odstotno subvencioniranje vložka, kar je ogromno še posebej za mikro, mala ter srednja podjetja. Podjetja se za razpise odločajo tudi zaradi naslednjih razlogov:

- konkurenčna prednost,
- napredovanje na področju digitalizacije procesov,
- digitalizacija podjetja,
- povečanje informacijske varnosti,
- hitrejša vpeljava sprememb, novosti kot brez razpisa.

Eno podjetje je izpostavilo, da nimajo standarda ISO 27001, vendar pa imajo standard TISAX. ISO standard 27001, kot že prej omenjeno, določa splošne zahteve za vsa podjetja na področju upravljanja informacijske varnosti, prav tako TISAX z dopolnitvijo zahtev, ki so posebej namenjene dobaviteljem v avtomobilski industriji.

Naslednje vprašanje se navezuje na to, ali so podjetja pred pridobljenim razpisom opravila varnostni pregled sistema; namreč eden izmed pogojev za pridobitev več točk je bilo, da ima podjetje opravljen varnostni pregled sistema in da v sklopu sistema določene ugotovljene pomanjkljivosti odpravi. 31 od vseh anketiranih podjetij je pritrdilo, da so pred pridobljenim razpisom opravili varnostni pregled sistema ter osem podjetij, da pregleda ni opravilo.

Graf 10 Opravljen varnostni pregled sistema pred pridobitvijo razpisa

Vir: Lasten

Podjetja, ki so odgovorila z NE, so kot razlog navedla visoko ceno pregleda sistema, ali pa, da kibernetskega napada še niso doživela.

Podjetja pa so v sklopu razpisa ali vavčerja za krepitev digitalnih kompetenc morala določen del svojega kadra ustrezno izobraziti. Nekaj izobraževanj s katerimi so podkrepili kompetence zaposlenih so sledeče:

- Etični heker,
- Office 365,
- Varni v pisarni,
- Kibernetska varnost,
- Napredna obdelava podatkov in podatkovna analitika,
- Kakovostna komunikacija znotraj organizacije,

- Varno poslovanje na internetu,
- Digitalni marketing,
- Simulirani phishing napadi,
- Izobraževanja za uvedbo ERP, DMS, WMS programov, B2B portalov ipd.

So pa podjetja razdvojena pri odgovoru, ali je pridobitev razpisa dvignila konkurenčno prednost, čeprav je bil to eden izmed pogojev, da podjetja lahko razpis prejmejo. 20 podjetij je odgovorilo z NE in 20 podjetij je odgovorilo z DA.

4.3 Podjetja spreminjajo procese v podjetju na podlagi digitalizacije

Podjetja spreminjajo procese znotraj podjetja na podlagi digitalizacije, 22 podjetij je spremenilo procese, šest podjetij vztraja pri ustaljenih procesih ter 12 podjetij je v postopku vpeljave sprememb procesov na podlagi digitalizacije podjetja. Procese, ki so jih podjetja spreminjala zaradi digitalizacije so:

- postopen prehod na brezpapirno poslovanje,
- vpeljevanje novih programskih rešitev (ERP, WMS, DMS itd.),
- ustvarili podporni portal za stranke,
- sledenje proizvodnje in hitrejše ugotavljanje odstopanj,
- digitalizacija delovnih nalogov in njihovo potrjevanje,
- uvajanje mobilnih pisarn,
- avtomatizacija kreiranja certifikatov o ustreznosti dobavljenega materiala.

4.4 Podjetja se zavedajo kako vpliva digitalizacija na okolje

Večji del podjetij se strinja, da digitalizacija vpliva na okolje pozitivno, in sicer 38 anketiranih podjetij od 40 – le dve podjetji sta mnenja, da digitalizacija na okolje ne vpliva dobro.

Graf 11 Vpliv digitalizacije na okolje

Vir: Lasten

Podjetja sem pozvala, naj napišejo na kakšen način pripomorejo k zmanjševanju vpliva na okolje, odgovori so sledeči:

- Obnavljanje starih računalnikov
- Storitve v oblakih
- Nakup rabljene in obnovljene opreme
- Manj porabljenega materiala (papir)
- Zmanjšanje porabe goriva – delo od doma
- Povratna in trajna embalaža za njihove produkte
- Skrbno ravnanje z opremo, za maksimalno dolgo uporabnost le te
- Nakup kolesa za bližje obiske uradov
- Sončne elektrarne – obnovljiv vir električne energije idr.

Odgovor, ki pa je posebej pritegnil mojo pozornost pa je »obstoječo opremo redno vzdržujemo in obnavljamo ter jo na tak način lahko uporabljamo zelo dolgo. Storitve v oblaku sicer uporabljamo, vendar po naši izkušnji te ne zmanjšujejo vpliva na okolje – \"oblak\" je še vedno

lociran na neki napravi, ki pa je zaradi zahtevnosti delovanja in oddaljenosti od naših delovnih mest bolj potratna tako z vidika materialov, potrebnih za izdelavo in povezavo, kot tudi z energetskega vidika«. V kolikor se delno strinjam s trditvijo, saj je res, da je oblak vseeno lociran na neki napravi oziroma serverju, ne vidim razlog,a da je ta način bolj potraten. Namreč dostim podjetjem se bolj splača najeti oblak in hraniti podatke tam, kot pa nakupiti opremo za npr. 100.000 EUR in le to vzdrževati. Namreč serverji v lasti podjetja prinesejo prednost iz vidika, da vemo kdo ima dostop do podatkov, pri storitvah v oblaku pa le slepo zaupamo rečenemu s strani ponudnika, vendar se je vseeno potrebno zavedati, da se ponudniki storitev v oblaku zavedajo kaj ponujajo ter kakšno raven storitve zagotavljajo, in redno posodabljajo opremo, imajo redne preglede sistema itd. Saj če nek nivo zaupnosti in vsega kar prodajajo ne bi vzdrževali, bi stranke odšle drugam. In še, s tem ko ima podjetje storitve v oblaku, se zmanjša strošek in potreba po zelo izobraženem IT oddelku, saj za celotno infrastrukturo skrbi ponudnik storitev.

Sama oskrba infrastrukture ni preprosta, in je potreben dober sistemski delavec, da bo lahko to tudi vzdrževal in urejal. Za manjša podjetja se tako bolj splača imeti zunanje podjetje v kolikor ima server v »hiši«, da oni s svojim izobraženim kadrom redno posodabljajo in spremljajo potrebne spremembe za infrastrukturo. Seveda za večje podjetje ali multinacionalke je lahko zgodba drugačna. Vseeno pa so se v zadnjih letih storitve v oblaku izkazale za dobre, prav tako večino podjetij strmi tudi k temu, da ne omogočajo več drugih storitev kot le v oblaku. V kolikor je anketiranec mislil na slednje tudi kot zgolj internetno povezavo, je malo nesmiselno, saj podjetja, ki delujejo v razvitem svetu imajo vsa dostop do interneta. Prav tako se internet ne plačuje po porabi ampak po hitrosti, za katero smo se vsi razvadili in želimo že v osnovi čim boljšo za čimbolj nemoteno delovanje.

Omenil je tudi energetski vidik, namreč če podjetje nima serverja v hiši, ima najverjetneje manjše stroške z električno energijo, saj server ni priključen na elektriko, prav tako ni potrebna klimatska naprava, ki bi server ohranjala na njemu primerni temperaturi, in tudi ni potrebe po UPS napravi, ki stanejo tudi po nekaj tisočakov. Vseeno se torej vsaj manjšim ter srednjim podjetjem bolj splača uporabljati storitve v oblaku kot pa imeti svoj lasten server, saj bodo težko zagotavljala interno tako izobražen kader, da bo slednje lahko funkcioniralo. Prav tako je sama dostopnost do storitev enostavna, ponavadi je potreben le dostop do interneta (Office 365), medtem ko če imamo lastne serverje, je ponavadi potrebna prijava v mrežo preko RDP ali VPN.

5 ZAKLJUČEK

V prvem poglavju smo spoznali kaj točno je varnostna politika. Izvedeli smo, da varnostna politika opredeljuje pravila in postopke za vse posameznike, ki dostopajo in uporabljajo IT sredstva in vire organizacije. Varnostna politika je nepogrešljiv del vsake organizacije, ki jo lahko podjetje sestavi samo – na internetu je namreč veliko vzorcev in pomoči, ali pa preko zunanjega podjetja, kot je na primer podjetje B2 IT d.o.o. Pomembno pa je seveda upoštevati, da varnostna politika vsebuje odgovore na vprašanja kako nadzorovati dostop do informacij, kako preprečiti vohljanje, kako preprečiti kršitev podatkov ter kako preprečiti uhajanje podatkov. Ugotovili smo, da ima varnostna politika tudi velik vpliv na delovanje organizacije, saj so lahko zaradi varnostne politike določene spletne strani nedostopne, opredeljuje do katerih informacij imajo zaposleni sploh dostop, politiko gesel in pogostost menjave le teh, ter najbolj pomembno, da se zaposleni strinjajo in varnostno politiko upoštevajo. Vse od najvišjega direktorja in do zadnjega zaposlenega. Določena podjetja pa potrebujejo za delovanje tudi ISO standard 27001, ki opredeljuje zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja varnosti informacij.

H1, da podjetja imajo varnostno politiko, je delno potrjena, saj je nimajo vsa podjetja. Od 40 anketiranih podjetij ima varnostno politiko 39 podjetij, kar je sicer velik delež, vendar je zmotno razmišljati, da imajo startup ali mikro podjetja ali pa samostojni podjetniki opredeljeno varnostno politiko. Od teh podjetij pa skoraj polovica posodobi svojo varnostno politiko na letni ravni, kar je dober pokazatelj, da se podjetja zavedajo, da je varnostna politika živ dokument. Dve podjetji varnostno politiko posodobita celo na polletni ravni, medtem ko ostali le ob pomembnih dogodkih. Podjetja so se za izdelavo varnostne politike odločile zaradi zahtev strank ali zakonskih zahtev. Vendar pa večji del podjetij vseeno izobražuje svoje zaposlene na področju digitalne pismenosti ter o nevarnostih na internetu in s tem krepijo svojo konkurenčnost ter varnost sistema.

V naslednjem poglavju smo obravnavali vpliv digitalne preobrazbe na okolje. V poslovnem okolju se za prijaznost okolju najbolj šteje brezpapirno poslovanje, da ohranimo gozdove in naravo. Kar seveda ima svoj dober vpliv, ki ga ne smemo zanemariti. Ne govori pa se, da tudi nenehna potrošnja in nakupi novih prenosnikov, novih serverjev vplivajo na ogljični odtis, ki ga pustimo na okolju. Sestava računalnika ima vseeno svoj proces proizvodnje, ki lahko pusti velik del onesnaževanja na okolje, prav tako pa je potrebno paziti tudi na pravilno razgradnjo računalnika, v kolikor ta ni več delujoč. Ker smo ujeti v vrvež, in se način življenja spreminja

tako, da norimo in v hitro potrošnjo in se to pozna tudi na okolju. Vedno več podjetij kupi prenosne računalnike, ki pa jih po približno štirih letih zavrže in kupi nove. Saj novo je vedno boljše.

Na podlagi anketiranih podjetij je **H4** »Podjetja se zavedajo kako vpliva digitalizacija na okolje« ovržena. Večina anketiranih meni, da digitalizacija vpliva na okolje pozitivno, saj zanemarijo del konstantenga nakupa novih prenosnikov in računalnikov. Nekaj podjetij pa vseeno skrbi za okolje tako, da obnavlja stare računalnike, uporablja storitve v oblakih, zmanjša porabo goriva z delom od doma, skrbno ravna z opremo in ji s tem omogočijo maksimalno uporabnost ali pa so zgradili sončne elektrarne.

V zadnjih letih so na slovenskih tleh zelo priljubljeni razpisi za nepovratna sredstva. Te zajemajo različna področja. Vedno več pa je razpisov in vavčejev s področja digitalizacije, digitalne strategije, kibernetske varnosti ipd. Od 40 anketiranih podjetij, je 34 podjetij odgovorilo, da se na razpise in vavčerje za nepovratna sredstva prijavljajo, kar pomeni, da je **H2** »Podjetja se prijavljajo na nepovratna sredstva za digitalizacijo« delno potrjena. Razlogi za prijavo pa so dokaj enotni: konkurenčna prednost, digitalizacija poslovanja in finančna pomoč, saj subvencija meri kar v višini 60 %.

V sklopu zadnjega poglavja se dotaknemo tudi tega, da podjetja spreminjajo procese v podjetju na podlagi digitalizacije. Malo več kot polovica anketiranih je odgovorilo, da je procese spremenilo, kar nas pripelje do tega, da je še zadnja **H3** »Podjetja spreminjajo procese v podjetju na podlagi digitalizacije« delno potrjena. Podjetja svoje procese spreminjajo tako, da vpeljujejo prehod na brezpapirno poslovanje, vpeljevanje novih programskih rešitev, uvajanje mobilnih pisarn, sledenje proizvodnje.

Končne ugotovitve diplomskega dela so, da večina podjetij ima sestavljeno varnostno politiko ter jo tudi redno posodablja in izobražuje svoje zaposlene, s čimer krepi varnost sistema in hkrati tudi konkurenčnost. Na področju digitalizacije in izobraževanja o vplivu digitalizacije na okolje bo v Sloveniji potrebno še postoriti veliko, saj bo potrebno zavedanje, da brezpapirno ni največ, kar podjetje lahko pripomore k ohranjanju okolja za naslednje generacije.

6 VIRI IN LITERATURA

AskIT. (4. oktober 2022). *Vavčerji za digitalizacijo 2021*. Pridobljeno iz AskIT: https://www.askit.si/sl-si/vavcerji-za-digitalizacijo-2021

Barker, S. (20. oktober 2022). *How To Write An Information Security Policy*. Pridobljeno iz HighTable: https://hightable.io/how-to-create-an-information-security-policy/

BoxBlogs. (19. april 2021). *Information security policy: Core elements.* Pridobljeno iz BoxBlogs: https://blog.box.com/information-security-policy-core-elements

Brajnik, M. (5. avgust 2019). *Nadzor zaposlenih na delovnem mestu*. Pridobljeno iz IUS INFO: https://www.iusinfo.si/medijsko-sredisce/v-srediscu/247067#

Christian, A. (20. september 2020). *Turns out dumping data centres in the ocean could be a good idea*. Pridobljeno iz Wired: https://www.wired.co.uk/article/data-centres-underwater-climate-crisis

DataLAB. (21. julij 2021). *Javni razpisi (vavčerji P4D React EU) za digitalno transformacijo MSP*. Pridobljeno iz DataLab: https://www.datalab.si/blog/digitalni-vavcerji-p4d-react/

DIH Slovenija. (4. oktober 2022). *Vavčer za digitalni marketing*. Pridobljeno iz DIH Slovenija: https://dihslovenia.si/vavcerji/vavcer-za-digitalni-marketing

Dunham, R. (5. maj 2020). *Information Security Policies: Why They Are Important To Your Organization*. Pridobljeno iz Linford & Co llp: https://linfordco.com/blog/information-security-policies/

EASYDMARC. (15. oktober 2021). *23 ways to help your employees follow IT security policies*. Pridobljeno iz EASYDMARC: https://easydmarc.com/blog/23-ways-to-help-your-employees-follow-it-security-policies/

Geneva Environment Network. (25. november 2021). *Data, Digital Technology, and the Environment*. Pridobljeno iz Geneva Environment Network: https://www.genevaenvironmentnetwork.org/resources/updates/data-digital-technology-and-the-environment/

GVZH Advocates. (1. OKTOBER 2020). *The Importance Of Having An IT Security Policy In Place*. Pridobljeno iz gvzh: https://www.mondaq.com/it-and-internet/990228/the-importance-of-having-an-it-security-policy-in-place

IdenHaus. (4. avgust 2021). *Why Every Organization Needs Information Security Policies*. Pridobljeno iz IdenHaus: https://www.idenhaus.com/why-every-organization-needs-information-security-policies/

Irwin, L. (4. junij 2020). *How to write an information security policy – with template example.* Pridobljeno iz ITgovernance: https://www.itgovernance.eu/blog/en/how-to-write-an-information-security-policy-with-template-example

ISO. (31. oktober 2013). *ISO/IEC 27001:2013*. Pridobljeno iz ISO: https://www.iso.org/standard/54534.html

Leal, R. (11. marec 2019). *TISAX – What is it, and how is it related to ISO 27001?* Pridobljeno iz Advisera: https://advisera.com/27001academy/blog/2019/03/11/how-iso-27001-and-tisax-are-related/

Mallory, P. (15. september 2020). *Time to update your cybersecurity policy?* Pridobljeno iz InfoSec: https://resources.infosecinstitute.com/topic/time-to-update-your-cybersecurity-policy/

Mathenge, J. (26. februar 2021). *IT Security Policy: Key Components & Best Practices for Every Business*. Pridobljeno iz BMC blogs: https://www.bmc.com/blogs/it-security-policy/

Ogorevc, A. (9. avgust 2021). *Kako uspešno kandidirati za sredstva v okviru razpisov za digitalizacijo.* Pridobljeno iz Finance Tovarna: https://tovarna.finance.si/8978279/Kako-uspesno-kandidirati-za-sredstva-v-okviru-razpisov-za-digitalizacijo

OSI. (21. oktober 2021). *IT Security Policies: Why Every Organization Must Have Them*. Pridobljeno iz osi: https://www.osibeyond.com/blog/it-security-policies-every-organization-must-have-them/

Paloalto. (1. julij 2022). *What is an IT Security Policy?* Pridobljeno iz paloalto: https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy

RCR. (20. oktober 2022). *Javni poziv za Vavčer za dvig digitalnih kompetenc*. Pridobljeno iz RCR: https://rcr-pro.eu/razpis/javni-poziv-za-vavcer-za-dvig-digitalnih-kompetenc/

SecurityScorecard. (6. april 2021). *What is an Information Security Policy and What Should it Include?* Pridobljeno iz SecurityScorecard: https://securityscorecard.com/blog/what-is-an-information-security-policy-and-what-should-it-include

Senhasegura. (23. avgust 2021). *Why is Information Security Important to Your Organization?* Pridobljeno iz Senhasegura: https://senhasegura.com/why-is-information-security-important-to-your-organization/

Slovenski inštitut za standardizacijo. (1. november 2013). *Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja.* Pridobljeno iz Slovenski standard: https://cdn.standards.iteh.ai/samples/54534/7c8c5a7197b040abb6869a33ac2e9d4c/SIST-ISO-IEC-27001-2013-AC-.pdf

Tunggal Tyas, A. (12. maj 2022). *What is an Information Security Policy?* Pridobljeno iz UpGuard: https://www.upguard.com/blog/information-security-policy

UN Environment programme. (30. november 2021). *The growing footprint of digitalisation.* Pridobljeno iz Foresight brief: https://wedocs.unep.org/bitstream/handle/20.500.11822/37439/FB027.pdf

Žnidaršič, B. (21. oktober 2021). *Opisujemo razliko med ukrepoma, za katera lahko porabite vavčerje za kibernetsko varnost, ki jih ponuja Slovenski podjetniški sklad.* Pridobljeno iz Finance: https://ikt.finance.si/8981194/Sistemski-varnostni-pregled-je-rentgen-penetracijski-test-pa-magnetna-resonanca