DIGITALNO INOVACIJSKO STIČIŠČE SLOVENIJE
REPUBLIKA SLOVENIJA MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
EVROPSKA UNIJA EVROPSKI SKLAD ZA REGIONALNI RAZVOJ NALOŽBA V VAŠO PRIHODNOST
I FEEL SLOVENIA
Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

Pomen kibernetske varnosti za mikro, mala in srednje velika podjetja

Gregor Spagnolo, SSRD d. o. o.

Povzetek – Poslovanje v digitalnem svetu prinaša številne prednosti za mikro, mala in srednje velika podjetja (v nadaljevanju MSP), vendar organizacije izpostavlja številnim kibernetskim tveganjem. Čeprav je kibernetska kriminaliteta največji izziv za številne organizacije in pogosto vodi do finančne izgube, MSP-ji še vedno ne namenjajo dovolj pozornosti in sredstev kibernetski varnosti. Namreč ko razmišljamo o kršitvah in kibernetskih napadih, se naš um ponaša s spektakularnimi incidenti, ki predstavljajo nacionalne ali mednarodne novice. Kljub temu da se tovrstne novice redke, pa so MSP-ji bolj izpostavljeni kibernetskim tveganjem in so najpogostejša tarča spletnih kaznivih dejanj.

Ključne besede – kibernetska varnost, podjetja, MSP

Abstract – The benefits of doing business in the digital world bring many opportunities for micro, small and medium-sized enterprises (below: SME), but they expose organizations to various cyber risks. Although cybercrime is the biggest challenge for many organizations and often leads to financial loss, SMEs still do not pay enough attention and resources to cybersecurity. When we think about violations and cyber-attacks, our mind boasts to spectacular incidents that represent national or international news. But even though these kind of news are rare, SMEs are even more exposed to cyber risks and are the most common target of online crime.

Keywords – cybersecurity, enterprise, SME

1. UVOD

V zadnjih letih je digitalizacija gospodarstva odprla nove priložnosti za rast poslovanja podjetij z vse hitrejšimi, pametnejšimi in bolj povezanimi sistemi ter procesi. Ne glede na cilj ali dejavnost podjetja je raven odvisnosti od IT-sistemov in omrežij vse pomembnejša. Pojavljanje novih področij in preoblikovanje tradicionalnih panog pa podjetja izpostavlja novim izzivom in tveganjem, ki so za MSP-je izredno zahtevna, saj informacijska varnost ni njihova primarna dejavnost. Prav tako dodatne izzive predstavljajo kombinacija pogostosti kibernetskih incidentov, motnje poslovanja, ki jih incidenti povzročijo, finančni vplivi in omejenost sredstev za odziv ter okrevanje v primeru uspešnega kibernetskega napada.

2. PREGLED PODROČJA

Več kot polovica vseh kibernetskih napadov je usmerjenih na MSP-je in ta številka nenehno raste. Po podatkih Inštituta Ponemon se je število ciljnih kršitev, ki zadevajo manjša podjetja, že tretje leto zapored znatno povečalo. 93 odstotkov MSP-jev, ki so doživeli kibernetski incident, je poročalo o enormnem vplivu na njihovo poslovanje. Skoraj vsa podjetja so poročala o izgubi denarja in prihrankov. 21 odstotkov jih je poročalo o škodi na ugledu, kar je povzročilo izgubo strank, pa tudi težave pri pridobivanju novih zaposlenih in poslov. 60 odstotkov MSP-jev, ki so bili žrtev kibernetskega napada, ni okrevalo in so v naslednjih šestih mesecih prenehali poslovati. Kljub temu kar 68 odstotkov MSP-jev nima sistematičnega pristopa za zagotavljanje kibernetske varnosti v podjetju. Še več, glede na to, da je za odkritje digitalne grožnje povprečno potrebnih 101 dan, se škoda hitro povečuje.

Glede na naštete vse preveč pogoste rezultate se postavlja logično vprašanje: Zakaj MSP-ji ne storijo več za zaščito kibernetske varnosti?

Prvi razlog, ki smo ga omenili že v uvodu, je, da informacijska varnost ni primarna dejavnost podjetja, v človeški naravi pa je skrb za tveganja, ki so nam blizu. Čeprav kibernetski napadi pogosto polnijo naslovnice, se novice večinoma nanašajo na velika podjetja. Posledično večina MSP-jev meni, da so premajhna, da bi jih lahko napadli in da njihov sektor ne bi bil zanimiv za kibernetske kriminalce, zaradi česar se jim kibernetska grožnja ne zdi resnična. Kar kibernetski kriminalci iščejo, kadar so na lovu za novimi žrtvami, so podjetja, v katera je preprosto vdreti, zaradi česar so MSP-ji s svojim skromnim vlaganjem v ukrepe kibernetske varnosti ali so brez njih, dejansko idealna in posledično najpogostejša tarča spletnih kaznivih dejanj. Takšna podjetja pa niso le lahka tarča napadov, temveč lahko kriminalcem nudijo veliko finančno korist – v obliki denarja za odkupnino ali ukradenih podatkov o bančnih računih, kar jim omogoča enostaven dostop do izkupička. Z napadi na MSP-je se kriminalci izognejo tudi večjim naporom in tveganjem, da bi vdrli v večje korporacije ali vladne subjekte. Posledično so MSP-ji spričo strukturnih in vedenjih značilnosti vse pogostejša ciljna skupina kibernetskih napadov.

Velike organizacije imajo mnogokrat proračun, namenjen posebej za kibernetsko varnost, saj bi morebitna kršitev lahko imela resne učinke na ugled pravne osebe ter gospodarske posledice. Na drugi strani imajo številni MSP-ji omejen proračun in jim primanjkuje sredstev za običajne varnostne prakse ter na splošno niso naklonjeni vlaganju v kibernetsko varnost, čeprav se srečujejo z večino enakih groženj.

Glede na resnost napada lahko MSP-ji utrpijo hude motnje v poslovanju, vključno s finančno škodo in škodo na ugledu. Kršitve podatkov so drage, ne samo zaradi glob, temveč tudi zaradi izgubljenega zaupanja strank, dobaviteljev in poslovnih partnerjev. Obstaja tudi tveganje, da napadalec pridobi dostop do intelektualne lastnine ali drugih občutljivih komercialnih informacij in jih uporabi v svojo korist. Možna je tudi odškodninska odgovornost MSP-ja. Takšne tožbe so pogosto, ne glede na končni izid, izjemno drage in dolgotrajne.

Čeprav nobena varnostna strategija ne more 100-odstotno preprečiti napadov, je cilj čim bolj ublažiti tveganja. Večina napadov izkorišča osnovne pomanjkljivosti v IT-sistemih in programski opremi, proti katerim se je mogoče enostavno braniti in preventivno ukrepati.

3. ZAKLJUČEK

Glede na razvoj dogodkov je jasno, da morajo MSP-ji v letu 2020 in prihodnjih letih ponovno opredeliti svoj pristop h kibernetski varnosti ter to obravnavati kot prednostno nalogo. Z doslednim pristopom k upravljanju podatkov, podprtim s potrebnimi sredstvi in usposabljanjem zaposlenih, lahko MSP-ji zagotovijo, da kibernetska varnost postane sestavni del poslovanja podjetja. MSP-ji morajo iskati rešitve, ki ustrezajo njihovi velikosti in potrebam, pri čemer ni nujno, da gre za enake rešitve, ki jih uporabljajo velike organizacije. MSP-ji imajo prednost pred večjimi podjetji, saj jim njihova agilnost omogoča fleksibilnost in hitro prilagajanje spremembam. Z dajanjem enakega pomena kibernetski varnosti kot drugim poslovnim ciljem lahko MSP-ji ohranijo svojo prednost in uspešno poslujejo v novem digitalnem svetu.

LITERATURA

[1] Anconina Dan. Why Cybersecurity Needs to Become the Top Priority for SME's. XM Cyber, 2020.

[2] Collinwood Joe. 5 Reasons why SMEs can't ignore cyber security. SME News, 2019.

[3] Cybersecurity and SMEs. SMESEC. Dostopno na: https://www.smesec.eu/cybersecurity.html

[4] Galvin Joe. 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself. Inc., 7. maj 2018. Dostopno na: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

[5] Hiscox Cyber Readiness Report 2019. Dostopno na: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

[6] Millaire Pascal, Sathe Anita, in Thielen Patrick. What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets. Chubb 2018.

[7] Ninth Annual Cost of Cybercrime Study. Accenture, 6. marec 2019. Dostopno na: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[8] Summerville Abigail. Protect against the fastest-growing crime: cyber attacks. CNBC, 2017.