Foto: Despsitphotos

Poskrbite za ustrezno zaščito

Ustrezni in pravočasni ukrepi lahko preprečijo nastanek velike poslovne škode. K iskanju rešitev je treba pristopiti celovito.

Barbara Perko

Informacijska oziroma kibernetska varnost je čedalje bolj pomembna, zato morajo podjetja temu nameniti pozornost in poskrbeti za ustrezne ukrepe, nadzore in postopke, da zagotovijo tako varnost sistemov, ki jih uporabljajo, kot podatkov, s katerimi razpolagajo.

Statistični urad RS je v začetku oktobra objavil ugotovitve raziskave o kibernetski varnosti v slovenskih podjetjih z vsaj 10 zaposlenimi. Raziskava je pokazala, da več kot polovica podjetij uporablja močna gesla in kontrolo dostopa do omrežja podjetja. 77 odstotkov podjetij iz varnostnih razlogov posodablja programsko opremo ali operacijski sistem, več kot 60 odstotkov hrani kopije podatkov na drugi lokaciji ali v oblaku. Približno četrtina podjetij periodično izvaja penetracijske teste, testira varnostne sisteme, pregleduje varnostne ukrepe in testira sisteme za izvajanje varnostnih kopij. 16 odstotkov podjetij ne izvaja nobenega od varnostnih ukrepov ali postopkov, med njimi je največ malih podjetij. Več kot polovica podjetij redno obvešča zaposlene o njihovih obveznostih v zvezi z varno uporabo IKT.

V letu 2018 je po podatkih statističnega urada 14 odstotkov podjetij najmanj enkrat naletelo na težave, ki so bile posledica varnostnih incidentov, povezanih z uporabo IKT.

»Če je bilo področje kibernetske varnosti v preteklosti precej zanemarjeno, pa v zadnjih treh letih tudi na osnovi zahtev EU in Nata opažamo napredek. Najbrž so k temu pripomogli tudi odmevni kibernetski incidenti v preteklosti, ki so imeli posledice tudi v Sloveniji, npr. izsiljevalski virus WannaCry pred leti ali pa incident v Ljubljanskih lekarnah pred kratkim,« je prepričan dr. Uroš Svete, v. d. direktorja Uprave za informacijsko varnost (UIV). »Tako na nacionalni ravni kot na ravni vsakega posameznega podjetja ali organizacije se moramo zavedati, da je nemoteno poslovanje podjetij ali pa delovanje celotne družbe zelo odvisno od zanesljivega delovanja IKT sistemov in omrežij. Prej, ko bomo sprejeli dejstvo, da je za obvladovanje kibernetskih tveganj tako kot za obvladovanje drugih tveganj treba izvajati določene

»Prej, ko bomo sprejeli dejstvo, da je za obvladovanje kibernetskih tveganj treba izvajati določene varnostne ukrepe in za to zagotoviti kadrovske, materialno tehnične in finančne vire, prej bomo povečali našo odpornost na kibernetska tveganja,« pravi dr. Uroš Svete, v. d. direktorja UIV.

varnostne ukrepe in za to tudi zagotoviti kadrovske, materialno tehnične in finančne vire, prej bomo povečali našo odpornost na kibernetska tveganja in manjše bodo škodljive posledice v primeru uresničitve takih tveganj.«

Potrebni so celoviti ukrepi

Podjetja se lahko sama poskušajo izogniti nekaterim najpogostejšim napakam. Mihael Nagelj, koordinator področja Kibernetska varnost v Horizontalni mreži IKT, meni, da so napake odvisne od stanja zavedanja o kibernetskih tveganjih v podjetju in velikosti podjetja. Pri tem so mala in srednja podjetja v specifični situaciji. »Najpogostejša napaka je, da ne storijo nič ali pa premalo,« pravi. Veliko lahko storijo že z zelo osnovnimi ukrepi (varovanje gesel, poznavanje trikov socialnega inženiringa) ter usposabljanjem in ozaveščanjem. Potrebni so celoviti organizacijski, tehnološki in kadrovski ukrepi. »Sistematična ocena tveganj, poznavanje svoje infrastrukture in njihove ranljivosti lahko pripelje do pravih in učinkovitih ukrepov. Redno posodabljanje opreme z varnostnimi popravki je vedno nujen ukrep,« poudarja Nagelj.

Izkušnje kažejo, da je večina omrežnih incidentov posledica pomanjkljive osnovne varnostne kulture in ustreznega znanja o varnostnih tveganjih.

Z delom začela Uprava RS za informacijsko varnost

Uprava za informacijsko varnost (UIV) kot organ v sestavi deluje v okviru Ministrstva za javno upravo. UIV je pristojni nacionalni organ na področju informacijske varnosti in hkrati enotna kontaktna točka pri mednarodnem sodelovanju države na tem področju. Njena naloga je koordinacija naporov za zagotavljanje kibernetske in informacijske varnosti na nacionalni ravni. UIV želi povezati zmogljivosti na operativni ravni sistema, kjer delujejo nacionalni odzivni center za kibernetsko varnost SI-CERT na Arnes, vladni odzivni center za kibernetsko varnost na MJU, zmogljivosti za kibernetsko varnost na MNZ/Policiji, MO/SV in v obveščevalno-varnostni skupnosti ter zmogljivosti, ki jih na osnovi Zakona o elektronskih komunikacijah (ZEKOM) razvijajo operaterji elektronskih komunikacij in AKOS. Prav tako si bo UIV prizadevala v nacionalni sistem povezati tudi ostale deležnike, npr. izobraževalne ustanove, RRI organizacije, stanovska združenja in organizacije s tega področja. UIV si bo prizadevala za ozaveščanje različnih ciljnih skupin, npr. splošne javnosti, podjetij, javne uprave. Za izvedbo projektov za dvig ravni kibernetske/informacijske varnosti si bo UIV prizadevala pridobiti sredstva tako iz nacionalnih kot tudi iz evropskih virov. Poleg povezovalne in ozaveščevalne vloge pa bo zelo pomembna naloga UIV tudi izvajanje nadzora nad izvajanjem Zakona o informacijski varnosti (ZInfV), Zakona o dostopnosti spletišč in mobilnih aplikacij (ZDSMA) in prihajajoče ureditve na področju e-identitet in storitev zaupanja.

Podjetja morajo zagotoviti nadzor nad dogajanji v omrežju ter biti pripravljeni na ukrepanje v primeru varnostnih incidentov.

»Ključno je zavedanje, da smo ranljivi. Brez tega ni mogoče razvijati kulturo, ki bo pripeljala do potrebnih ukrepov v podjetju in ustreznega ravnanja uporabnikov tehnologije. Ti ukrepi so zelo odvisni od tega, kakšne so lahko posledice spregleda izvedbe preventivnih ukrepov ali pa vzdrževanja sposobnosti za obnovitev poslovanja v primeru incidenta. Za dosego teh minimalnih osnov so nujna izobraževanja zaposlenih, ne zadoščajo samo usposabljanja specialistov IT. Z razvojem digitalizacije podjetij pa bo treba poseči tudi po bolj kompleksnih in zahtevnejših ukrepih,« je prepričan Nagelj.

Kako lahko pomaga GZS? »Znotraj IKTHM področje Kibernetska varnost ponuja storitve in izdelke za celovito obvladovanje kibernetskih tveganj vsem, ki izvajajo aktivnosti digitalne transformacije. Te storitve in izdelke pomagamo vgraditi in prilagoditi rešitvam v posamezni industriji ali vertikali ter tako zagotoviti vgrajene lastnosti varnosti in zasebnosti, ki sta nujna atributa pri uspešnem trženju vseh IKT izdelkov ali storitev,« razloži sogovornik.

Skrb za varnost je prepotrebna naložba

»Edini način, kako se lahko podjetja zaščitijo pred vse pogostejšimi kibernetskimi grožnjami, je izobraževanje zaposlenih in računovodij, kako naj prepoznajo in se ustrezno odzovejo na poskuse zlorab. Predvsem pa je potrebno več zavedanja s strani vodstva, da skrb za varnost ni nepotreben strošek, ampak prepotrebna naložba,« so prepričani na SI-CERT, kjer so pripravili priročnik Kažipot varnosti za mala podjetja, ki je lahko manjšim podjetjem v pomoč.

Izkušnje kažejo, da je večina omrežnih incidentov posledica pomanjkljive osnovne varnostne kulture in ustreznega znanja o varnostnih tveganjih. »Ne smemo pozabiti, da je večina vdorov posledica napačnih odločitev ljudi in ne pomanjkljive tehnične zaščite,« pravijo.

Poslovna škoda tudi več kot 100.000 evrov

Najhujše posledice nosijo okužbe z izsiljevalskimi virusi, s katerimi napadalci v zadnjem času ciljajo na neustrezno zaščitene strežnike podjetij, predvsem na storitev oddaljenega dostopa. »Zaradi okužbe z izsiljevalskim virusom je lahko poslovanje podjetja tudi za več dni onemogočeno, zahtevana odkupnina in poslovna škoda pa lahko doseže tudi več kot 100.000 evrov,« o virusih, ki so stalnica že od leta 2012, pravijo na SI-CERT.

Finančne posledice so velike tudi, ko gre za napad vrivanja v poslovno komunikacijo, pri katerem napadalci pridobijo geslo za dostop do službenega elektronskega predala zaposlenega, nato pa v njem nastavijo filtre za posredovanje sporočil. Tako spremljajo komunikacijo in ko zaznajo, da bi moralo eno od podjetij plačati račun, posežejo v komunikacijo in pošljejo podatke o novem bančnem računu, ki

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

je pod nadzorom napadalcev. »Največje oškodovanje v tej vrsti prevare, ki smo ga zabeležili leta 2018, je bilo kar 450.000 evrov,« povedo.

Najpogostejši primer goljufije je t. i. direktorska prevara, ko napadalci na spletni strani podjetja pridobijo podatke o direktorju in računovodstvu ter v računovodstvo pošljejo ponarejeno elektronsko sporočilo z navodili za plačilo računa. Ker je sporočilo videti avtentično, lahko prejemnika zavede, opozarjajo na SI-CERT. Tako nakazan denar pristane na bančnih računih denarnih mul, ki ga takoj po prejemu pošljejo po neki drugi denarni poti naprej. Povprečno oškodovanje znaša 40.000 evrov.

Kako se lahko podjetja zaščitijo?

»Poleg tehnične zaščite, kamor spadajo filtri na poštnih strežnikih ter antivirusni programi, je zelo pomembno tudi to, da so zaposleni pazljivi pri prejemu neobičajnih elektronskih sporočil, tudi če te pridejo iz znanih naslovov. Predvsem je potrebno dodatno preveriti kakršnekoli spremembe pri plačilih mimo uveljavljenih praks, ki veljajo v podjetju,« svetujejo na SI-CERT.

V primeru hekerskega napada je nujno, da imajo podjetja izdelan načrt in strategijo ukrepanja, manjša podjetja, ki nimajo zaposlenega kadra za informacijsko varnost, se lahko po brezplačno pomoč obrnejo tudi na odzivni center SI-CERT.

Vse več dokazov vodi v tujino

Slovenska policija v zadnjih letih obravnava več kot 200 primerov kaznivih dejanj zlorabe informacijskega sistema in napada na informacijski sistem. »Storilci večinoma delujejo mednarodno, pogosto za seboj puščajo manj uporabnih sledi, dokazov, ki bi pripomogli k njihovi izsledtvi in identifikaciji. Obenem pa so tovrstne sledi v večji meri le v digitalni obliki in pogosto razpršene po več državah/celinah, kar vse vpliva na trajanje in uspešnost kriminalističnih preiskav,« pojasnjujejo na Generalni policijski upravi.

Raziskanost takih kaznivih dejanj je okoli 40 odstotkov, kar je dober rezultat, glede na to, da tako slovenska kot evropska zakonodaja večkrat omejujeta oz. podaljšujeta mednarodno pridobivanje dokazov, razlagajo. Storilci vse redkeje prihajajo iz Slovenije, saj vse več sledi in dokazov vodi v tujino. Slovenska policija kot članica Europola in Interpola aktivno sodeluje z obema organizacijama, tako kot tudi z več državami, tako s sosednjimi kot tistimi iz širše regije kot z ameriškim FBI.

Kaj ponuja trg?

Trg ponuja širok spekter opreme in storitev, ki posegajo na vsa področja kibernetske varnosti. Ponudbe različnih svetovanj so na voljo tako za celovit pristop obvladovanja kibernetskih tveganj pa do zelo specifičnih storitev. Vključujejo pomoči pri izdelavi ocene tveganj, načrtovanja potrebnih organizacijskih, tehničnih ukrepov ali pa prenosa znanja. Ponudniki opreme nudijo celoten spekter zaščitne opreme za različne potrebe, vključno s sistemi umetne inteligence. Ker specialistov kibernetske varnosti v podjetjih primanjkuje, so podjetjem na voljo tudi storitve zunanjega izvajanja (npr. storitve varnostno operativnega centra). V procesih zagotavljanja varnosti so nujni tudi notranji in zunanji varnostni pregledi. Na trgu so na voljo tudi zavarovanja kibernetskega tveganja.

Na GPU kot prvi in osnovni varnostni ukrep navedejo zaščito informacijskega sistema s funkcionalnim protivirusnim orodjem in požarnim zidom. Ustrezna informacijsko varnostna politika lahko predvidi možna varnostna tveganja in možne ukrepe za zmanjšanje škode v primeru varnostnih dogodkov. »Lahko bi rekli, da je pogosto neučinkovito posploševati priporočljive varnostne ukrepe, saj se te lahko efektivno določi zgolj individualno glede na dobro poznane okoliščine delovanja posamezne računalniške enote,« pojasnijo in zaključijo, da je bistveno ustrezno ozaveščanje vseh zaposlenih v podjetju. »Informacijski sistem je namreč varen zgolj toliko, kot je varen njegov najšibkejši člen - in v praksi se žal pogosto izkaže, da so to prav informacijsko neuki uporabniki.« gg

Informacijski sistem je varen zgolj toliko, kot je varen njegov najšibkejši člen - in v praksi se žal pogosto izkaže, da so to prav informacijsko neuki uporabniki, opozarja GPU.

Račun prejmi varno

Eden glavnih virov virusov so priponke v elektronskih sporočilih. Nemalokrat so to računi. Podjetja se lahko izognejo pošiljanju računov prek elektronske pošte z uporabo varnih elektronskih poti. »Podjetja se morajo med sabo povezati na način, da vedo, kdo je na drugi strani, kakšen certifikat ima podjetje in kakšen dokument bo poslalo. Tako na varen način povezuješ podjetja med sabo,« možnost, kako se izogniti tveganju opiše Igor Zorko, predsednik GZS – Združenja za informatiko.

	Število kaznivih dejanj									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Zloraba informacijskega sistema	11	18	26	12	8	1	6	10	34	25
Napad na informacijski sistem	98	76	236	131	226	155	162	260	171	212
Skupaj	109	94	262	143	234	156	168	270	205	237

Vir: GPU