Foto: Depositphotos

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

Kibernetska varnost

Pozornost podnevi in ponoči – za varnost in konkurenčnost

Digitalna preobrazba prinaša nove rešitve s še večjo odvisnostjo od digitalnih tehnologij in zagotavljanja kibernetske varnosti. Med vodilnimi vse bolj prevladuje prepričanje, da je uveljavljanje ukrepov kibernetske varnosti del obvladovanja tveganj, ki podjetjem zagotavljanja konkurenčno prednost.

Mihael Nagelj, predsednik Sekcije za kibernetsko varnost, Združenje za informatiko in telekomunikacije (ZIT), GZS

Živimo v obdobju stalnih in hitrih sprememb, ki stalno pospešujejo digitalno preobrazbo vseh področij delovanja družbe. Stanje zaradi COVID-19 je spremenilo način delovanja podjetij in marsikje še pospešilo digitalno preobrazbo. A žal je prineslo tudi nove oblike ogrožanja.

Zapostavljeni varnostni ukrepi v podjetjih so dobro opremljenim in motiviranim napadalcem odprli dodatne možnosti za lažje vdore v pogojih dela od doma. V tej situaciji so se podjetja in varnostni strokovnjaki v Sloveniji dobro odzvali, brez večjih posledic vdorov.

Za večjo gospodarsko rast

Poleg skrbi za delovanje v obstoječih pogojih številna podjetja že načrtujejo delovanje v fazi prehoda po obdobju COVID-19 za obdobje gospodarske rasti, kot jo po strmem padcu dejavnosti v letu 2020 napovedujejo poslovni analitiki. Digitalna preobrazba prinaša nove rešitve in še večjo odvisnost od digitalnih tehnologij, te pa bodo zahtevale tudi ustrezno raven varnosti.

Vse bolj med vodilnimi v podjetjih prevladuje prepričanje, da je uveljavljanje ukrepov kibernetske varnosti del obvladovanja tveganj v podjetjih, ki jim prinaša konkurenčno prednost, saj z zmanjšanjem tveganj lahko zanesljiveje oskrbujejo svoje

Ukrepi kibernetske varnosti niso enkraten dogodek, so stalna skrb vodilnih, zaposlenih in strokovnjakov kibernetske varnosti.

Dogodek 24/7/365 je bil priložnost, da so podjetja v sektorju kibernetske varnosti in predstavniki države spregovorili o odprtih vprašanjih kibernetske varnosti v podjetjih in tudi s praktičnimi primeri dobre prakse predstavili možnosti za izboljšanje stanja. To je nujno, če bodo podjetja želela uspešno izvajati svojo digitalno preobrazbo.

odjemalce, zmanjšujejo nepotrebne stroške in zagotavljajo svoj ugled na trgu.

Z zmanjšanjem tveganj lahko zanesljiveje oskrbujemo svoje odjemalce, zmanjšujemo nepotrebne stroške in zagotavljamo ugled na trgu.

Analizi kibernetskih tveganj o uresničevanju poslovnih ciljev podjetja morajo slediti ukrepi, ki se nanašajo na zmanjševanje ranljivosti v omrežjih, na ozaveščanje o grožnjah, izobraževanje pri uporabi storitev informacijskih in komunikacijskih tehnologij ter uveljavljanje ukrepov varnosti v dnevni praksi. Za optimalno uresničevanje ukrepov kibernetske varnosti je nujno uravnotežiti poslovna tveganja in ukrepe kibernetske varnosti, kar pa je mogoče uresničiti le ob tesnem sodelovanju vodstva podjetja in specialistov kibernetske varnosti. Nujna je tudi povezanost podjetja z ostalimi dejavniki kibernetske varnosti v družbi. Šele z aktivnim delovanjem vodstev podjetij, organov države, posameznikov in strokovnjakov bomo lahko dosegali ustrezno raven odpornosti podjetij in družbe v celoti.

Nacionalna strategija kibernetske varnosti je načrt ukrepov, namenjen izboljšanju varnosti in odpornosti nacionalnih infrastruktur in storitev.

Širša družbena odgovornost

Večkrat slišimo o nujnosti širše družbene odgovornosti za kibernetsko varnost. Prepletenost telekomunikacijskih in informacijskih tehnologij in njihova skokovita rast zahtevata angažiranost vseh, tako uporabnikov storitev, ponudnikov storitev in specialistov. V zadnjih letih Republika Slovenija zmanjšuje zaostajanje, ki pa ga v kratkem času ni mogoče odpraviti, saj je področje zelo kompleksno. Potrebni bodo nadaljnji koraki za zmanjšanje zaostankov. Eden od teh je sprejetje nacionalne strategije kibernetske varnosti, ki bo skupaj z akcijskim načrtom podlaga za hitrejši razvoj področja.

Nacionalna strategija kibernetske varnosti je načrt ukrepov, namenjen izboljšanju varnosti in odpornosti nacionalnih infrastruktur in storitev. To je pristop, ki na visoki ravni določa vrsto nacionalnih ciljev in prednostnih nalog, ki jih je treba uresničiti v določenem časovnem obdobju za odpravljanje tveganj v kibernetskem prostoru, ki bi lahko ogrozila ekonomske in socialne koristi. S Strategijo kibernetske varnosti iz leta 2016 je Slovenija okrepila sistem zagotavljanja kibernetske varnosti, vzpostavila nove rešitve in istočasno odprla pot nadaljnjim izboljšavam. S stanjem v podjetjih ne moremo biti zadovoljni, saj o tem pričajo pokazatelji v raziskavi SURS Kibernetska varnost v podjetjih z vsaj 10 zaposlenimi (vir: https://www.stat.si/StatWeb/News/Index/8421). O nujnosti sprememb je letos tekla razprava na številnih srečanjih strokovnjakov kibernetske varnosti, vse pogosteje pa se v razpravo vključujejo tudi vodilni iz podjetij, ki jih k zagotavljanju varnosti zavezuje tudi zakonodaja. Prevladujoča mala in srednja podjetja (MSP) so v specifični situaciji zaradi še večjega pomanjkanja virov, se pa varnostni dogodki teh podjetij ne izognejo.

Ne pozabimo na izobraževanje pri uporabi storitev informacijskih in komunikacijskih tehnologij!

Prihajajoče spremembe Strategije kibernetske varnosti in akcijskega načrta za njeno uresničevanje predstavljajo priložnost za podjetja, da v krovnem dokumentu kibernetske varnosti države in še posebej v akcijskem načrtu predlagajo umestitev ustreznih rešitev za izzive prihodnosti, ki se nanašajo na vključevanje novih tehnologij, raziskav in razvoja, razvoj novih produktov, javno zasebnega partnerstva, vključevanja v mednarodne trge, specifičnosti MSP ali zagotavljanja potrebnih specialističnih kadrov. Razvoj in zadrževanje specialističnega kadra postajata vse bolj kritična in zahtevata drugačne rešitve na strateški ravni. Specifičen je položaj MSP v sektorju kibernetske varnosti, ki je zasnovan predvsem na vrhunskem znanju posameznikov. V okviru projekta CYBER pod okriljem programa Interreg Europe se deležniki na GZS posebej ukvarjajo z vprašanji sprememb ekosistema za delovanje MSP, ki delujejo v sektorju kibernetske varnosti. Skupaj s partnerji v evropskih regijah na podlagi izmenjave dobrih praks in izkušenj projektna skupina pripravlja predloge, ki bodo izboljšali ekosistem delovanja MSP v sektorju kibernetske varnosti, zagotovili njihov razvoj in tudi tako prispevali k razvoju odpornosti družbe.

Foto: Depositphotos

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

Vse bolj rafinirane metode napadalcev

Iz letnega poročila SI-CERT je razvidno, da je v letu 2019 prišlo do velikega porasta »phishing« prijav (t. i. internetno ribarjenje oziroma lažno predstavljanje podjetja), saj uporabniška gesla odpirajo vrata nadaljnjim zlorabam. Še naprej se kaže trend ciljanja na podjetja, kjer je povzročena finančna škoda še višja kot pretekla leta. Ta trend se v tem letu še krepi. Rast »phishinga« je znašala v letošnjem septembru celo 65 % glede na enako obdobje lani.

Metode napadalcev so vedno bolj rafinirane in se prilagajajo specifični situaciji uporabnikov. Če uporabnik ni previden, lahko hitro napadalcu omogoči vnos škodljive kode. Ta pristop je za napadalce najbolj učinkovit in jim omogoča nadaljnje aktivnosti v internem omrežju. Znani so primeri, kako z lahkoto posamezniki pridejo do sredstev ogrožanja varnosti, da ne omenjam organiziranega kriminala, ki razpolaga z znatnimi viri in stalno prednostjo pred obrambo.

Najbolj prepoznavne posledice so šifriranje virov podatkov podjetja (angl. ransomware) ob uničevanju varnostnih kopij in dodatno izsiljevanje z objavo podatkov v javnih medijih. Izrednega pomena je, da podjetja posredujejo informacije o takšnih dogodkih nacionalnemu odzivnemu centru za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team), saj s tem omogočijo ukrepe za preprečevanja nadaljnje širitve napadov in vzpostavitev ustreznih preventivnih ukrepov.

Podjetjem so na voljo številne storitve, s katerimi si lahko pri obvladovanju kibernetskih tveganj pomagajo pri implementaciji varnostnih standardov, kot je denimo standard ISO/IEC 27001, pri izvajanju preventivnih ukrepov ali v primerih varnostnega incidenta. Vendar pa je treba poudariti, da se podjetje lahko in tudi mora organizirati na način, da se koncepti kibernetske varnosti uveljavljajo v vseh delih organizacije. Tako obvladovanje kibernetskih tveganj postane dnevna praksa, ki omogoča učinkovito odkrivanje in ukrepanje ob poizkusih vdorov. gg

65 % je letos septembra znašala rast pojava »phishinga« v primerjavi z enakim obdobjem lani.

Če uporabnik ni previden, lahko napadalcu omogoči vnos škodljive kode.