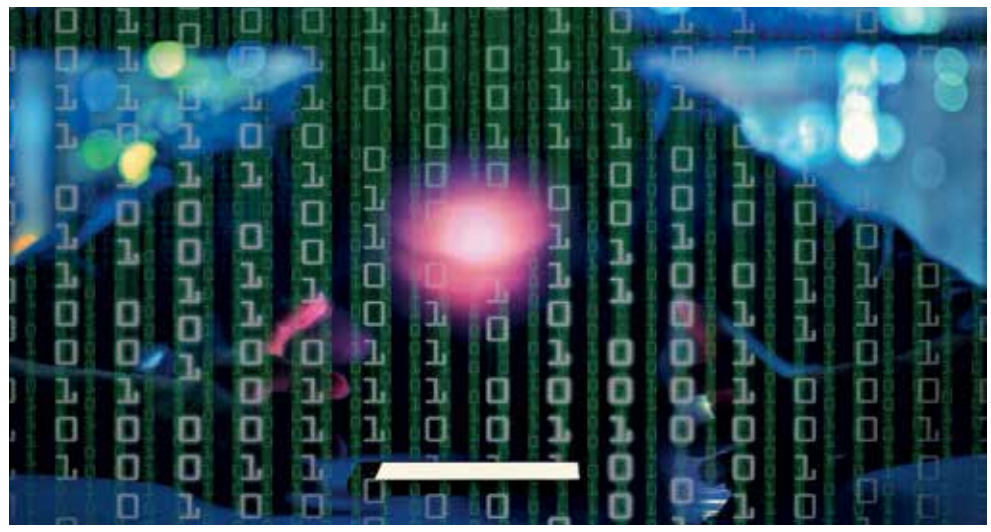
www.finance.si
Četrtek, 17. septembra 2020, št. 180

Zaprite hekerjem poti do svojih IKT-sistemov



GETTY IMAGES/ISTOCKPHOTO

V Sloveniji je lani največja škoda zaradi kibernetskega napada znašala 2,4 milijona evrov, povprečna izplačana odkupnina za povrnitev zašifriranih dokumentov pa je 866 evrov.

Globalna statistika je neizprosna in skrb zbujajoča. Lani je bilo vsak dan v povprečju 750 tisoč kibernetskih napadov, kar je 44 odstotkov več kot leto prej. Med letošnjo pandemijo COVID-19 pa je število napadov s pomočjo ribarjenja v primerjavi z istim lanskim obdobjem poskočilo za 350 odstotkov. Več kot petina napadenih podjetij je škodo ocenila na več kot 50 milijonov evrov.

Ta statistika se na prvi pogled za Slovenijo ne zdi tako pomembna, ker naj bi bili majhna država in zato nezanimiva za spletne kriminalce. Takšno razmišljanje je zelo tvegano, če vemo, da slovenska podjetja izvozijo slabo polovico vseh izdelkov in storitev. To pomeni, da so redno v digitalnih stikih s poslovnimi partnerji v tujini. Naš največji zunanjetrgovinski partner je Nemčija, ki je na lestvici kibernetsko najbolj napadanih držav na visokem tretjem mestu. Zato je zelo velika verjetnost, da se bo v primeru napada na neko nemško podjetje ta napad nenamerno razširil tudi v Slovenijo.

Slovenska podjetja niso imuna za težave

A tudi statistika napadov za Slovenijo ni bleščeča. Kot poročajo na nacionalnem odzivnem centru SI-CERT, je lani največja zabeležena škoda znašala 2,4 milijona evrov, sicer pa je bilo prijavljenih 5.854 varnostnih incidentov, kar je 12 odstotkov več kot leto prej.

Če pogledamo še nekoliko starejše podatke, lahko razberemo, da je imelo leta 2018 težave z varnostnimi incidenti, ki so povezani z IKT, kar 14 odstotkov slovenskih podjetij. Približno desetina podjetij z več kot desetimi zaposlenimi je imela težave z dosegljivostjo storitev IKT, kar je bila posledica okvare strojne ali programske opreme, zavrnitve storitve (DDoS) ali napadov z izsiljevalskimi virusi. Pri teh je treba omeniti, da povprečna izplačana odkupnina za povrnitev zašifriranih dokumentov v Sloveniji znaša 866 evrov.

V osmih odstotkih podjetij je zaradi okužbe z zlonamerno programsko opremo ali nedovoljenega dostopa do podatkov prišlo do okvare strojne ali programske opreme, zaradi česar so bili uničeni ali popačeni podatki. Pri dveh odstotkih teh podjetij je prišlo tudi do razkritja zaupnih podatkov zaradi vdora, ribarjenja ter namernih ali nenamernih dejanj zaposlenih.

Glavna šibka točka so zaposleni

Prav zaposleni so najpogostejša tarča kibernetskih napadov in zato glavna šibka točka pri zagotavljanju informacijske varnosti v podjetjih. Število obravnavanih primerov družbenega inženiringa in goljufij je namreč tudi v Sloveniji že preseglo število tehničnih napadov. Zato je pri zagotavljanju kibernetske varnosti pomembno vlaganje v izobraževanje zaposlenih o varni uporabi IKT, kar v Sloveniji počne le 53 odstotkov podjetij.

Vsekakor hekerski napadi niso le težava velikih podjetij, saj so v 43 odstotkih kibernetskih napadov tarča mali podjetniki ter mala in srednja podjetja. Ker gre za manj spektakularne zneske, se o teh napadih v javnosti ne govori, niso pa zato za napadene nič manj usodni.

Uporaba pametnih naprav, kot so mobilni telefoni, tablice, računalniki in čedalje bolj tudi druge povezane naprave, hitro narašča, zato se povečuje tudi prostor za kibernetske napade. Največ jih poteka prek družbenih omrežij, elektronske pošte ter spletnih in mobilnih aplikacij. Pri tem skrbi zbuja podatek, da lahko mine tudi več kot 200 dni, preden uporabnik ugotovi, da je nekaj narobe. V tem času je lahko škoda že zelo velika in marsikdaj tudi nepopravljiva.

Zavarujte se pri A1 Slovenija

V podjetju A1 Slovenija ponujajo širok spekter rešitev in orodij, ki lahko tako rezidenčnim kot poslovnim uporabnikom pomagajo preprečiti škodo, ki bi lahko nastala zaradi kibernetskega napada. Poslovnim uporabnikom ponujajo protivirusni program F-Secure in požarni zid naslednje generacije Stormshield, rezidenčnim uporabnikom pa rešitev A1 Protekt.

F-Secure za računalnike in delovne postaje zagotavlja celovito zaščito pred virusi, vohunskimi programi, vdori in nezaželeno pošto. F- Secure za mobilne naprave pa zagotavlja popolno zaščito pred krajo podatkov, virusi in vohunskimi programi za pametne telefone in tablice. Vgrajeno ima tudi funkcionalnost iskanja izgubljene oziroma odtujene naprave. Zaupne podatke varuje, tudi če je telefon izgubljen ali ukraden.

S požarnim zidom Stormshield pridobite dostop do vseh integriranih varnostnih funkcij za klasično infrastrukturo ali oblak. Upravljanje varnosti v podjetju prek enega samega vmesnika je nadvse enostavno, izbirate lahko med štirimi licenčnimi paketi, rešitev pa med drugim vsebuje tudi algoritem, ki dinamično prilaga varnostni pravilnik. To pomeni, da višje ko je tveganje, višja je stopnja zaščite.

Rešitev A1 Protekt, ki jo lahko vklopimo s poslanim SMS, pa varuje vaš mobilni telefon pred virusi, vohunsko programsko opremo, spletnimi prevarami in zlonamernimi spletnimi naslovi v mobilnem omrežju A1. Zaznane grožnje blokira, preden napadejo vaš pametni telefon.

Kako so v NKBM optimizirali tiskanje in za polovico razbremenili zaposlene

»Ljudje ponavadi težko sprejemamo spremembe ključnih procesov v podjetju, v tem primeru pa se je izkazalo nasprotno – zaposleni smo se sami zavzemali za čim hitrejšo vpeljavo rešitve in predlagali celo vrsto dopolnitev, ki nam pomagajo pri dnevnem delu,« je povedal Alen Šibanc, vodja oddelka upravljanja sprememb za prebivalstvo, podjetja in digitalizacijo v Novi KBM, kjer so poenotili in optimizirali floto tiskalnikov in večopravilnih naprav ter tako znižali visoke stroške upravljanja dokumentov in prihranili veliko časa pri pridobivanju dokumentacije strank.

Banke se morajo pri sklepanju poslov s strankami držati zakonskih regulativ in internih pravil, zaradi katerih morajo od njih pridobiti kopije številnih dokumentov. V NKBM, drugi največji slovenski banki, zaposleni vsak dan skenirajo, označijo in arhivirajo več tisoč dokumentov. Dokler niso optimizirali flote tiskalnikov, je ta postopek vzel veliko časa. V banki so imeli namreč nameščene tiskalniške naprave različnih proizvajalcev in z njimi sklenjene pogodbe o vzdrževanju, vsak pa je imel svoje pogoje. Stroški tiskanja so bili zato nepregledni in visoki, naprave pa pogosto v okvari, kar je zmanjševalo učinkovitost zaposlenih.

Učinkovitejši postopki zajema dokumentov

V NKBM so se odločili, da bodo upravljanje tiskalniških naprav poenotili. Skupaj s podjetjem Xenon forte so razdrobljeno floto nadomestili z optimiziranim naborom tiskalnikov in večopravilnih naprav proizvajalca Kyocera. Hkrati so najeli celostno zunanjo storitev upravljanja naprav z enotno podporo in vzdrževanjem ter zalaganjem s potrošnim materialom na daljavo. Stroški upravljanja tiska so tako postali preglednejši in tudi nižji, dosegljivost naprav pa je zdaj 99-odstotna.

V NKBM so se skupaj s podjetjem Xenon forte lotili tudi izboljšave učinkovitosti postopkov zajema in hrambe dokumentacije o strankah. Ker je bil vnos podatkov razdrobljen v več različnih sistemih, so bili postopki za pridobivanje dokumentacije strank dolgotrajni in zamudni. Zato so razvili namensko aplikacijo oziroma preprost uporabniški vmesnik, ki je prilagojen posameznim poslom, in s tem večopravilne naprave povezali z zalednimi sistemi banke. Zaposlenim so tako omogočili enoten, hiter in zanesljiv zajem dokumentacije v celotni mreži poslovalnic banke z jasno revizijsko sledjo zajema dokumentov. Možnost za napake in zastoje se je s tem precej zmanjšala, zadovoljstvo strank pa se je povečalo, saj so zdaj postopki precej hitrejši.

NKBM

Optimizacija tiskalniške flote v celotni mreži poslovalnic in uvedba centralne rešitve za upravljanje tiska MyQ sta bili uvod v plodovito in učinkovito sodelovanje med NKBM in podjetjem Xenon forte.

Celosten nadzor dostopa do dokumentov

Zaradi velike razpršenosti poslovalnic so zagotovili tudi centralni nadzor nad aplikacijo in celosten nadzor dostopa zaposlenih do dokumentov na tiskalnikih. Določili so skupine zaposlenih z jasno opredeljenimi pravicami, nadzor dostopa pa poteka prek avtentikacije s službenimi karticami. To pomeni, da se dokument natisne šele, ko zaposleni pride do tiskalniške naprave in se na njej identificira s kartico. S tem so dosegli, da dokumenti, ki so lahko tudi zaupne narave, ne ležijo pozabljeni na tiskalnikih, kjer so lahko na očeh vsem.

»Dobili smo ne le optimizirano floto naprav in naprednih storitev tiskanja, temveč tudi partnerja, ki nam je znal prisluhniti in se poglobiti v naše procese dela. Skupaj smo razvili rešitev za upravljanje dokumentov, ki prinaša precejšnje prihranke pri času pridobivanja dokumentacije strank in stroških,« je povedala Diana Matić, sistemska administratorka v NKBM.

V banki ocenjujejo, da so s premišljeno programsko nadgradnjo večopravilnih naprav zmanjšali obremenjenost bančnih delavcev, banka pa se je v tem segmentu delovnih procesov uspešno digitalizirala.