www.finance.si
Torek, 27. junija 2023, št. 118

KIBERNETSKA VARNOST

Pri delu od doma ali z dopusta je nujna še večja skrb za varnost

Delo od doma se je med pandemijo covida-19 zelo razširilo po vsem svetu in je po njenem koncu v številnih panogah ostalo prevladujoča oblika dela. Čeprav takšno delo omogoča različne ugodnosti in koristi, tako posamezniko kot tudi podjetjem, s stališča kibernetske varnosti prinaša vrsto tveganj. Ta so še toliko večja, na primer, na poti ali na dopustu, kar bo še zlasti aktualno v prihajajočih poletnih dopustniških dneh.

Medtem ko na delovnih mestih v podjetjih in ustanovah za varnost skrbijo IT-ekipe, pri delu na daljavo za to večinoma skrbijo uporabniki sami. Pri delu od doma je delovno okolje uporabnika nekoliko bolje nadzirano ter manj izpostavljeno neposrednim napadom vsaj iz bližine, medtem ko so nevarnosti na internetu bolj ali manj podobne. Pri delu od koderkoli (na primer iz hotelske sobe na dopustu) pa zaposleni pogosto uporabljajo omrežja, kjer je edina zaščita preprosto geslo.

Pomanjkanje virov za pomoč

V podjetju Alliance Virtual Offices so še marca 2022 ocenili, da je prehod na delo na daljavo prinesel 238-odstotno rast števila kibernetskih napadov. Analitsko podjetje Gartner je na koncu leta 2022 ocenilo, da sta delo na daljavo in uporaba oblaka postala glavna skrb v povezavi s kibernetsko varnostjo. Lumu Technologies pa je konec leta 2022 poročal, da sta izboljšanje varnosti za tiste, ki delajo na daljavo, in upravljanje s tem povezanih ranljivosti postala »najbolj nujna projekta« za 78 odstotkov anketiranih direktorjev informacijske varnosti (CISO). Po oceni varnostnega podjetja UpGuard več kot 70 odstotkov zaposlenih dela na daljavo vsaj enkrat na teden, kljub temu pa je še vedno premalo virov, ki bi tem zaposlenim pomagali obvladati tveganja kibernetske varnosti, ki jih prinaša takšno delo.

Ključ do zaščite je protivirusni program

Kibernetski kriminal po oceni podjetja Kaspersky organizacijam po vsem svetu povzroča velikanske škode. Glede na stalno rast števila hekerskih vdorov v domača in podjetniška omrežja, katerih cilj je dostop do občutljivih datotek in podatkov, bodo škode le še večje. Uspešni vdori izpostavljajo organizacije in zaposlene napadom izsiljevalskih virusov, napadom za zavrnitev storitve (DDoS), vdorom zlonamerne programske opreme in vohunskih virusov ter drugim vrstam groženj.

Ključno sredstvo za kibernetsko zaščito je celovit in napreden protivirusni progam, ki ne poskrbi le za tako rekoč popolno odbijanje varnostnih groženj, ampak se tudi samodejno posodablja in s tem usposablja za odzivanje tudi v primeru novih groženj.

Naprava naj se čim prej zaklene

Celovit in kakovosten protivirusni program učinkovito deluje tudi proti napadom nultega dne, kjer virusi izkoriščajo varnostne pomanjkljivosti, preden se te zakrpajo. Dober program prav tako omogoča odkrivanje in preprečevanje delovanja zlonamernih in vohunskih virusov, trojancev in črvov, programske opreme za ribarjenje, predvsem tiste v obliki e-pošte, in drugih zlonamernih dejanj.

Strokovnjaki svetujejo, da imajo zaposleni, ki delajo od doma, na mobilnih napravah nameščen sistem za samodejno zaklenitev po desetih sekundah neuporabe, na računalnikih pa po petih minutah neuporabe. Organizacije bi morale še poskrbeti, da imajo njihovi zaposleni vključeno možnost iskanja naprave v primeru izgube ali kraje. Prav tako je zaželeno, da je za takšen primer vključena tudi možnost brisanja vsebine naprave.

Od boljšega nadzora do kibernetske higiene

Strokovnjaki za kibernetsko varnost priporočajo še več ukrepov, ki bi jih morali skrbniki IT zagotoviti, namestiti ali svetovati zaposlenim v podjetjih:

- namestitev ustrezne rešitve za nadzor dostopa,
- uporaba močnih kod PIN oziroma gesel,
- namestitev programa za upravljanje gesel,
- uporaba dvostopenjske avtentikacije, ki omogoča dostop šele po pravilni uporabi gesla in še enega elementa avtentikacije,
- uporaba navideznega zasebnega omrežja (VPN), ki omogoča deljenje podatkov z zasebnim omrežjem prek javnega omrežja,
- izogibanje programom iz nezanesljivih ali neznanih virov,
- prepoved odpiranja neznanih priponk iz e-pošte, za katere se ne ve, kaj je v njih ter od kod in zakaj so bile poslane,
- izobraževanje o kibernetski varnosti,
- skrb za kibernetsko higieno.

Anton Horvatič, Sfera IT:
Število kibernetskih napadov na računalniške povezave pri delu od doma se je v času pandemije povečalo za 768 odstotkov.

Žiga Humar, Our Space Appliances:
Raziskave kažejo, da je bilo delo od doma povod za 20 odstotkov uspešnih napadov.

Rok Peršak, Telekom Slovenije:
Ključno je, da imajo podjetja vzpostavljene jasne protokole, ki omogočajo varno in učinkovito delo.

Zaposleni, ki delajo od doma, naj imajo na mobilnih napravah nameščen sistem za samodejno zaklenitev po desetih sekundah neuporabe, na računalnikih pa po petih minutah neuporabe.

Ključno izvajanje predpisanih ukrepov

»Domača omrežja praviloma nimajo enake ravni varnosti kot omrežja podjetij, saj jih šibka gesla, zastarela vdelana programska oprema in napačno konfigurirani usmerjevalniki naredijo ranljive za kibernetske napade, kar pomeni tudi resno tveganje za vdor v omrežje podjetja,« ocenjuje Anton Horvatič, direktor prodaje varnostnih rešitev v podjetju Sfera IT. Delo od doma vključuje prenos občutljivih poslovnih podatkov zunaj varnih omrežij podjetja, kar povečuje možnost uhajanja podatkov in kršitev zasebnosti. »Nepravilno ravnanje ali shranjevanje podatkov v osebnih napravah ali storitvah v oblaku lahko povzroči nepooblaščen dostop do podatkov podjetja in namestitev zlonamerne programske opreme,« poudarja. »Da bi ublažili ta tveganja, je za organizacije in zaposlene, ki delajo od doma, ključnega pomena, da dosledno izvajajo predpisane varnostne ukrepe,« razlaga.

Koncept »predvidevajmo vdor«

To vključuje uporabo varnih omrežnih povezav, uporabo močnih mehanizmov za preverjanje pristnosti, stalno vzdrževanje posodobljene programske opreme, izvajanje dobre varnostne higiene in redno izobraževanje oddaljenih zaposlenih o najboljših praksah kibernetske varnosti. Horvatič ob tem svetuje, da podjetja čim prej sledijo novemu konceptu »predvidevajmo vdor«, ki obstoječim varnostnim elementom doda še posebno raven močnega varovanja podatkov kot zadnjo obrambno črto. Ta vključuje nespremenljivo varnostno kopijo, napredno odkrivanje napadov s pomočjo umetne inteligence in orkestrirano avtomatizirano obnovo podatkov. »Za podjetja je pomembno, da svoje strategije kibernetske varnosti nenehno prilagajajo spreminjajočemu se delovnemu okolju ter vlagajo v tehnologije in prakse, ki zagotavljajo varnost in zasebnost dela od doma,« poudarja Horvatič.

Razvijanje varnostne kulture

»Poleg tehničnih ukrepov, ki znižajo tveganja, je treba razvijati tudi varnostno kulturo in ozaveščenost o pasteh dela od doma. Tukaj naredimo največ z usposabljanji uporabnikov,« meni Žiga Humar, vodja ekipe za informacijskovarnostne rešitve v podjetju Ourspace Appliances. Hkrati poudarja, da ni priporočljivo uporabljati javnih odprtih brezžičnih omrežij, če pa že, »je treba nujno uporabiti VPN-povezavo, s katero preprečujemo prestrezanje komunikacije, v kateri se lahko razkrijejo tudi naše poverilnice«. Pri tem ne zadošča zgolj vpis uporabniškega imena in gesla, ampak je nujna uporaba dodatnega elementa, kot je varnostni PIN ali avtentikacijska aplikacija. »Geslo za oddaljeno povezovanje mora biti ustrezne dolžine in kompleksnosti – priporočam dolžino 12 znakov, male in velike črke ter številke –, ne uporabljamo pa ga na drugih spletnih straneh.«

Povezovanje le iz službenih naprav

»Organizacije ne smejo dopuščati povezovanja v organizacijsko omrežje, če naprava nima nameščenih vseh posodobitev, vklopljene požarne pregrade in ustrezne zaščite končnih točk,« razlaga Humar. Še bolje pa je, da je povezovanje omogočeno le iz naprav, ki so v lasti in pod nadzorom organizacije. Pri delu z oddaljene lokacije je tveganje tudi kraja naprave. »Ne samo, da moramo takšno napravo nadomestiti z novo – še večjo težavo lahko pomenijo zaupne informacije, če niso ustrezno šifrirane,« pravi.

»V primeru kraje ali izgube lahko podatki pridejo v roke napačni osebi, zato poskrbimo, da bodo diski in USB-ključki šifrirani,« svetuje Humar. V podjetju mnogokrat zasledijo, da mobilne naprave v lasti podjetja uporabljajo tudi otroci zaposlenih. »Ta praksa ni priporočljiva, saj otroci praviloma ne poznajo tveganj pri uporabi neznane programske opreme in obiskovanju dvomljivih spletnih strani.«

Delo na daljavo povečuje tveganje

»Zaposleni pri delu na daljavo namreč pogosto uporabljajo tudi neslužbeno opremo, kot so domači računalniki ali periferne naprave, ki ne izpolnjujejo varnostnih standardov podjetij,« poudarja Rok Peršak, vodja Operativnega centra kibernetske varnosti v Telekomu Slovenije. »V omrežje se povezujejo z nezaščiteno mrežno opremo, kot so domači usmerjevalniki, kar je tvegano, ker lahko pride do izpostavljanja napadom,« pojasnjuje. »Nemalokrat se dogaja tudi, da zaposleni svojih računalnikov ne zaklepajo dovolj skrbno, s čimer omogočajo nepooblaščen dostop do službenih omrežij,« pravi. Podjetja zato lahko kot prvi korak poskrbijo za pripravo in uveljavitev pravilnikov o varni rabi službene opreme pri delu od doma. »Zaposleni naj uporabljajo izključno službene računalnike, ki jih upravlja podjetje in ki imajo vpeljane ustrezne varnostne politike, napisane po smernicah varnostnih standardov in priporočil,« pravi Peršak.

Izvajanje XDR-zaščite

Podjetja morajo zagotoviti ustrezne VPN-povezave do službenega omrežja, s čimer omogočijo varne povezave. Vse povezave naj gredo skozi požarno pregrado, kjer veljajo varnostne politike podjetja. Ob vsem tem pa je priporočljivo izvajati tudi XDR-zaščito. Ti sistemi zbirajo in samodejno analizirajo podatke iz različnih virov in na različnih točkah v omrežju, kar vključuje oblačne in omrežne naprave, končne točke, kot so računalniki in mobilne naprave, ter aplikacije. Z uporabo umetne inteligence in strojnega učenja sistemi XDR identificirajo grožnje, ki jih tradicionalni varnostni sistemi morda ne bi prepoznali. Zaradi te celovite in avtomatizirane narave lahko sistemi XDR hitro prepoznajo in se odzovejo na grožnje, kar omogoča boljšo zaščito podatkov in omrežij. »Prav tako je pomembno nenehno izobraževanje in usposabljanje zaposlenih s področja kibernetske varnosti,« dodaja Peršak.

Podpornik rubrike Kibernetska varnost je Telekom Slovenije, d. d.