www.finance.si
Četrtek, 22. novembra 2018, št. 223

Naj tiskalnik ne bo najšibkejši člen informacijske varnosti

Puščanje natisnjenih dokumentov na tiskalnikih in nezaščiteni omrežni tiskalniki so vse pogosteje razlog za odtekanje podatkov v poslovnih okoljih.

Naprave, ki v poslovnih okoljih dobesedno bruhajo papirnate dokumente, so občutno napredovale od samostojnih tiskalnikov, ki smo jih poznali nekoč. Sodobni tiskalniki in večopravilne naprave so inteligentni omrežni pripomočki, ki so, enako kot osebni računalniki, opremljeni z zaslonom, tipkovnico in trdim diskom, na katerem se lahko hranijo občutljivi podatki in datoteke.

Priljubljeni cilj kiberkriminalcev

Omrežne naprave, med katere sodijo tudi tiskalniki, so trenutno med najbolj napadanimi cilji kibernetskih kriminalcev. Zato so pogosto šibki člen v obrambi pred zlonamernimi napadi in pri varovanju zaupnih podatkov podjetij. To je posledica tega, da podjetja pogosto spregledajo varnost tiskalniških naprav. Nezaščitene naprave se lahko okužijo z zlonamerno programsko opremo, ki se nato razširi po celotnem omrežju in ogroža varnost občutljivih podatkov ter informacij.

»Strokovnjaki za informacijsko tehnologijo in varnost morajo upoštevati tiskalniške naprave pri oblikovanju strateškega pristopa k varovanju IT-okolij, omrežij in podatkov. Začeti velja z najpreprostejšimi koraki in po potrebi uvesti bolj izpopolnjene ukrepe ter zagotoviti zaščito pred zlonamernimi napadi in izgubo občutljivih podatkov, ki bi za vstopno točko izbrali tiskalnik ali večopravilno napravo v podjetju,« razlaga Ciril Kraševec, direktor podjetja Xenon forte.

Preverite, kje pušča

Proizvajalec tiskalnikov in dokumentnih rešitev Kyocera je razvil orodje SecureAudit, ki podjetjem omogoča enostavno preverjanje večopravilnih naprav glede varnostnih pomanjkljivosti, vključno z napačnimi konfiguracijami in privzetimi nastavitvami. Orodje, razvito skladno z zahtevami GDPR, podjetjem pomaga zadostiti varnostnim zahtevam nove evropske in lokalne zakonodaje s področja informacijske varnosti.

SecureAudit je le del širšega programskega nabora družbe Kyocera. Ta vsebuje tudi rešitev Net Manager, s katero podjetja vzpostavijo popoln nadzor nad podatki v dokumentih, poslanih na večopravilne naprave. Net Manager spremlja vse vrste osebnih podatkov in dokumente izpiše le uporabnikom z ustrezno identifikacijo, hkrati pa s tiskalnikov zanesljivo izbriše starejše dokumente in podatke ter tako preprečuje, da bi prišli v napačne roke.

Rešitev skrbi za zaščito pred krajo dokumentov

Kakovostna rešitev za nadzor tiskanja obvlada marsikatero nalogo, na primer samodejno izbriše zadržane tiskalniške naloge na napravi, če se te niso izvedle. Prav tako skrbi za zaščito pred krajo dokumentov, s tem ko preprečuje morebitno skeniranje dokumentov na ključek USB ali pa njihovo pošiljanje na nepooblaščen e-poštni naslov.

Zahtevnejša poslovna okolja lahko uvedejo tudi funkcijo samodejnega označevanja zaupnih dokumentov z vodnim žigom. Tiskalniška varnostna rešitev nadzira tudi tiskanje iz različnih aplikacij glede na določena pravila – tako lahko uporabniku omogoči dvostransko barvno tiskanje dokumentov iz urejevalnika besedil, medtem ko mu vsebine, poslane na tiskalnik s spletnega brskalnika, privzeto natisne črno-belo.

Nezaščitene naprave se lahko okužijo z zlonamerno programsko opremo, ki se nato razširi po celotnem omrežju in ogroža varnost občutljivih podatkov ter informacij.

Ne pozabite na izobraževanje zaposlenih

Čeprav tehnične rešitve lahko ustrezno zaščitijo podatke in podjetju omogočijo, da je skladno z zahtevami uredbe GDPR in drugimi zakonodajnimi ali regulatornimi zahtevami, je pomembno, da skrb za varovanje podatkov in dokumentov razumejo in izvajajo predvsem zaposleni.

Zaposleni so tisti, ki morajo poznati ter razumeti pravila in dobre prakse ravnanja s podatki in dokumenti. Predstaviti jim je treba varnostna tveganja, pravilno rabo tiskalnikov in skrb za dokumente po tem, ko jih več ne potrebujejo. Ob vseh naložbah v zagotavljanje skladnosti poslovanja z zakonodajo bi moralo biti izobraževanje zaposlenih ena od prioritet vsakega podjetja.

Koliko je na črnem trgu vredna ukradena e-identiteta

Zakaj nam lahko napadalci, ki so odnesli podatke spletnemu forumu o vrtičkanju, spraznijo bančni račun? Predvsem zato, ker ljudje uporabljamo enaka uporabniška imena in gesla na več mestih, kar je zelo narobe.

Uporabniški računi za družbeno omrežje Facebook se denimo prodajajo za slab evro, prav toliko stanejo računi z dostopom do različnih spletnih igričarskih portalov. Le malenkost dražji je dostop do uporabniškega računa pretočne videostoritve NetFlix, medtem ko se računi za glasbena nebesa Spotify prodajajo po dva evra. Nekoliko dražji so premijski e-poštni račun in podatki za dostop do osebnih računalnikov, usmerjevalnikov in drugih (povezanih) naprav v gospodinjstvu ali pisarni. »Za popolno digitalno identiteto posameznika pa je treba odšteti med 30 in 50 dolarji,« je povedal David Jacoby iz Kaspersky Laba.

Ostanemo lahko brez denarja in podatkov

Napadalci si želijo pridobiti kar največ podatkov, zato na okužene naprave nameščajo različne razširitve brskalnikov ali programčke za beleženje pritiskov tipk na tipkovnici, s katerimi precej hitro pridobijo številna uporabniška imena in gesla.

V zadnjem času je zelo priljubljena tudi tehnika spreminjanja okuženih naprav v posredniške strežnike (proxy). Po tej poti napadalec, ki je pridobil številko kreditne kartice žrtve, poskrbi, da se predstavlja kot lokalni uporabnik, in tako laže prevara varnostne mehanizme v spletnih trgovinah in spletnih bankah. Prodaja posredniških strežnikov je letos pravi hit v kibernetskem prostoru.

Napovedujejo se še večje težave

Ob tem ko napadalci nič hudega slutečim žrtvam okužijo naprave, mimogrede postavijo lastno infrastrukturo za še precej bolj nevarne kibernetske napade. Okuženi računalniki, usmerjevalniki in druge naprave se tako mimogrede spremenijo v strežnike, iz katerih bo izpeljan napad na posamezno podjetje ali omrežje.

Da bomo manj ranljivi, lahko poskrbimo tako, da se držimo napotkov, ki jih varnostni strokovnjaki poudarjajo že desetletja. »Ljudje smo del težave, saj nismo dovolj odgovorni pri uporabi svojih gesel, nimamo varnostne higiene. Ne le, da nam pogosto ni mar, še celo naivni smo in tako napadalcem močno olajšamo delo. Brez ustreznih sprememb navad pa bo kibernetskega kriminala čedalje več,« je pojasnil David Jacoby.

»Poguglajte« se!

Bi radi izvedeli, ali so med zlorabljenimi tudi vaši podatki? Kaj o nas ve internet, lahko preverimo zelo enostavno, zadostuje že vnos imena in priimka v spletni iskalnik, varnostni strokovnjaki pa priporočajo obisk namenske strani **www.haveibeenpwned.com**, kjer so zbrani doslej znani podatki o zlorabah identitet. Vanjo le vnesemo svoj e-poštni naslov in dobimo nazaj informacijo, ali je bil kdaj odtujen ponudnikom spletnih storitev. Če je bil, takoj zamenjajmo gesla za dostop – ki bi jih po varnostni higieni seveda morali zamenjati vsake tri mesece. Pri tem ne bo odveč nasvet, da uporaba enostavnih gesel ne pride več v poštev. Ameriška zvezna država Kalifornija je rabo šibkih gesel že prepovedala.