Zavarujte tiskalniško okolje in dokumente

Podjetja pogosto podcenijo varnostna tveganja, ki so jim izpostavljene povezane naprave, tudi tiskalniki.

Kyocerino orodje SecureAudit omogoča enostavno preverjanje varnostnih pomanjkljivosti na večopravilnih napravah, vključno z napačnimi konfiguracijami in privzetimi nastavitvami.

V dneh, tednih in mesecih, ko se podjetja posvečajo predvsem skladnosti z novo uredbo o upravljanju osebnih podatkov (GDPR), je v poslovnih okoljih veliko pravnih in tehničnih strokovnjakov. Ti poskušajo ugotoviti, kje vse podjetja hranijo osebne podatke in kako jih uporabljajo. Za prevzem nadzora in upravljanje elektronskih podatkov v dokumentih in datotekah učinkovito poskrbita že dokumentni sistem in podatkovna baza, a podatki so pogosto raztreseni po vsem podjetju. Osredotočanje na naprave zaposlenih pogosto povzroči, da podjetja povsem spregledajo tiskalnike, čeprav ti (vsaj začasno) lahko hranijo ogromne količine osebnih podatkov – tisti, ki so omreženi, pa lahko dostopajo do najrazličnejših podatkov v podjetju. Če napadalec prevzame nadzor nad tiskalnikom, lahko sledi prava katastrofa ...

Brez identifikacije ni izpisa

Proizvajalec tiskalnikov in dokumentnih rešitev Kyocera je razvil orodje SecureAudit, ki podjetjem omogoča enostavno preverjanje varnostnih pomanjkljivosti na večopravilnih napravah, 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.

Rešitev 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.

Enkripcija kot dobra praksa

Potem ko je podjetje ugotovilo, kje vse hrani osebne podatke, strokovnjaki priporočajo uvedbo enkripcije oziroma šifriranja podatkov. Tako bodo ti, tudi če jih morebitni napadalec odtuji, še vedno zaščiteni. Napredne rešitve znajo podatke kriptirati ne le na strežnikih, računalnikih in prenosnikih, temveč tudi pametnih telefonih in tiskalnikih.

Izobraževanje zaposlenih

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

»Zaposleni morajo poznati ter razumeti pravila in dobre prakse ravnanja s podatki. 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 z GDPR bi moralo biti izobraževanje zaposlenih ena prednostnih nalog vsakega podjetja,« pravi Ciril Kraševec, direktor podjetja Xenon forte.