Naj tiskalniki ne bodo najšibkejši člen varnostne enačbe

Povezovanje tiskalniških naprav v omrežje in na različne strežnike v podjetjih je občutno pospešilo in poenostavilo delo zaposlenih. A brez ustreznih varnostnih mehanizmov in zaščite pomeni tudi resno varnostno pomanjkljivost, ki jo napadalci vse pogosteje izkoristijo za krajo podatkov.

Naprave za tiskanje v podjetjih so od starih in izoliranih naprav, ki so ždele v kotu in čakale na ukaz za tiskanje, precej napredovale. Današnje večopravilne naprave so povezane v omrežja, poganja jih napreden operacijski sistem, opremljene so z zmogljivim procesorjem in diskom za shranjevanje dokumentov (oziroma drugih podatkov). Prek omrežja so povezane tudi v svetovni splet, saj je »v modi«, da podpirajo tiskanje prek storitev in aplikacij iz oblaka, tiskanje z mobilnih naprav … Torej premorejo vse, kar kibernetski kriminalci potrebujejo za vdor v IT-okolje podjetja.

Medtem ko se IT-osebje v boju z grožnjami zlonamerne programske opreme in vdori hekerjev osredotoča predvsem na izzive, povezane z zaščito osrednje IKT-infrastrukture, kot so strežniki, delovne postaje in baze podatkov, tiskalniki v številnih organizacijah ostajajo slabše zaščiteni. To so ugotovili tudi hekerji, ki vse pogosteje ciljajo prav na tiskalnike, saj so posebej starejše naprave skoraj brez obrambe.

Je skrb za informacijsko varnost tehten argument za nadgradnjo ali zamenjavo tiskalnika ali večopravilne naprave? Vsekakor.

Skrb za varno tiskanje

Potreba po robustni zaščiti podatkov in dokumentov še nikoli ni bila večja, temu trendu pa sledijo tudi proizvajalci tiskalniške opreme – eni hitreje, drugi počasneje. Med vodilnimi na področju zagotavljanja informacijske varnosti so naprave proizvajalca Kyocera Document Solutions, ki slovijo po nadstandardni zaščiti podatkov v procesu obdelave dokumentov, kar so potrdili tudi strokovnjaki laboratorija BLI Keypoint Intelligence. Letos poleti so Kyoceri podelili prestižni certifikat Keypoint Intelligence Security Validation Testing, ki potrjuje, da je družina tiskalniških naprav TASKalfa pripravljena na izzive varovanja podatkov na najvišji ravni.

Kako torej naprave Kyocera TASKalfa skrbijo za varnost dokumentov, ki se (vsaj začasno) hranijo na napravah? Podobno kot računalniki so opremljene s kopico naprednih varnostnih mehanizmov, ki skrbijo, da so zaščitene že od zagona. Izboljšana je varnost komunikacije po omrežju (TLS), uvedena uporaba certifikatov za prijave, šifriranje podatkov je kompleksnejše in naprave lahko sporočajo dogodke in stanje v varnostne nadzorne sisteme (SIEM). Varnostne posodobitve večnamenskih naprav pa se lahko izvajajo samodejno ali pa jih prejemajo prek centralnega nadzornega sistema – v primeru kritičnih posodobitev se te samodejno namestijo najpozneje v 72 urah po objavi.


KYOCERA

Naprave proizvajalca Kyocera Document Solutions slovijo po nadstandardni zaščiti podatkov v procesu obdelave dokumentov.

»Za varno tiskanje je potrebna tudi ustrezna varnostna higiena uporabnikov tiskalnikov. Strokovnjaki oddelkom IT, ki najpogosteje skrbijo za tiskalniška okolja, ali pa zunanjim izvajalcem priporočajo, naj se temeljito pogovorijo z uporabniki, katere funkcije potrebujejo in katerih ne. Z varnostnega vidika je namreč precej bolje, če je digitalnih poti do tiskalnika čim manj, torej naj skrbniki izklopijo vse protokole in vmesnike, ki niso v uporabi, ter zaklenejo neuporabljana komunikacijska vrata,« svetuje Ciril Kraševec, direktor podjetja Xenon forte.

Varna integracija v IT-okolje

Ob nakupu novega tiskalnika ali večopravilne naprave, ki bo povezana v omrežje podjetja, naj oddelek IT preveri, ali zagotavlja močno šifriranje podatkov, in ga tudi vklopi. Če naprava podpira integracijo z aktivnim imenikom ter upravljanje uporabnikov in njihovega dostopa do posameznih funkcij večopravilnih naprav, je treba nastaviti tudi to. V sodobnih tiskalniških napravah Kyocera so vgrajeni tudi trdi diski ali pogoni SSD, na katerih so podatki zaščiteni, stopnjo zaščite lahko izbere skrbnik. Za brisanje podatkov (zaradi dostopa serviserja ali ob odklopu naprave) pa skrbi sistem z različnimi stopnjami brisanja.

Za še višjo varnost dokumentov in podatkov strokovnjaki podjetjem priporočajo, naj uvedejo dostop do naprav z uporabo identifikacijskih kartic ali aplikacij ter šifrirajo vsebine na diskih oziroma pogonih SSD v napravi. Poslovnim okoljem priporočajo tudi rabo rešitev za nadzor tiskanja in skeniranja, kot so MyQ, Kyocera Net Manager, PaperCut in podobne.

»Kakovostna varnostna zaščita poleg zaščite občutljivih podatkov in zaupnih dokumentov omogoča tudi boljšo kakovost dela zaposlenih. Varne tiskalniške naprave lahko brez težav odpremo navzven, saj za varno tiskanje skrbijo šifriranje, samodejno nadgrajevanje sistemske programske opreme, certifikati in drugi varnostni mehanizmi, ter tako zaposlenim omogočimo varno delo z oddaljenih lokacij, od doma ali na poti,« dodaja Kraševec.