Omrežena škatla v pisarni je lahko varnostna luknja

Uhajanje podatkov *Osebni in drugi podatki lahko odtekajo tudi iz tiskalnikov, zato jih je pametno ustrezno zaščititi*

Naprave za tiskanje v podjetjih so od starih samostojnih naprav zelo napredovale. Današnje večopravilne naprave so vključene v omrežja, poganja jih napreden operacijski sistem. Pa vendar so v številnih organizacijah ostale varnostne črne pege, saj se strokovnjaki za IKT v borbi z grožnjami zlonamerne programske opreme in vdori hekerjev osredotočajo predvsem na izzive zaščite osrednje infrastrukture, kot so, na primer, strežniki, delovne postaje in baze podatkov.

Vinko Seliškar

Proizvajalci tiskalnikov se trudijo vanje vgraditi varnostne funkcije. Foto Arhiv Kyocera

V smislu vse večje aktivnosti na področju kibernetičnega kriminala, ki neposredno meri na šibke člene sistemov, torej na v omrežje povezane naprave, zanemarjanje tiskalniških naprav pomeni veliko tveganje. Organizacije morajo brez odlašanja sprejeti ukrepe in vključiti večopravilne naprave v svoje strategije varovanja podatkov, sploh ker spremembe zakonodaje, lep primer je evropska uredba GDPR, prinašajo finančne in pravne posledice, ki so lahko uničujoče za podjetje.

Proizvajalci tiskalnikov seveda ne sedijo križem rok. Japonski proizvajalec Kyocera je pripravil veliko praktičnih napotkov za IT-strokovnjake, kako izkoristiti vgrajene varnostne funkcije večopravilnih naprav in sprejeti dodatne, izboljšane ukrepe za zaščito podatkov. Cilj informatikov mora biti, da kar najbolj otežijo ali onemogočijo tako neavtoriziran vstop v omrežje organizacije prek večopravilnih naprav, kot je izvajanje kriminalnih aktivnosti v primeru nepooblaščenega vstopa, če se to vendarle zgodi.

Najprej analiza, potem ukrepi

Marsikdo sploh ne pomisli, da bi podatki lahko odtekali prek tiskalnikov. A vendarle so ti, predvsem če so povezani v omrežje podjetja, ena lažjih tarč. So nekakšni miniaturni računalniki, opremljeni s pomnilnikom, trdimi diski ali pogoni SSD, na katerih (vsaj za krajši čas) hranijo datoteke, ki ji tiskajo ali skenirajo (večopravilne naprave). Naprednejši med njimi premorejo tudi funkcijo shranjevanja vsebin na omrežne vire, torej imajo dostop do drugih strežnikov in naprav v omrežju podjetja. Posebno večopravilne naprave so lahko izpostavljene številnim naprednim grožnjam, kot so nepooblaščen dostop do naprav prek omrežja, spreminjanje informacij med prenosom po omrežju ali uhajanje podatkov s pomnilniških medijev naprav.

»Nezaščiten tiskalnik je tiha varnostna grožnja. Prvi korak naj bo varnostna analiza tiskalniškega okolja, krpanje očitnih lukenj ter preverjanje, kdo vse in kako uporablja omrežne tiskalnike,« pravi Ciril Kraševec, direktor podjetja Xenon Forte.

Osnovna zaščita brez izgovorov

Kyocera vsem organizacijam, ki uporabljajo večopravilne naprave, priporoča, da uvedejo in dejavno upoštevajo vsaj osnovne ukrepe zaščite naprav za tiskanje. Morebitni dodatni ukrepi pa naj bodo uvedeni poleg osnovnih in ne namesto njih. Kje torej začeti?

Tiskalniške naprave so tovarniško opremljene s privzetim geslom za dostop. Zelo priporočljivo je, da ga IT-osebje spremeni, pri čemer naj izbere novo primerno močno geslo, ki bo skladno z varnostno politiko podjetja. Slednji nasvet je očiten, a v praksi žal ne samoumeven: za dostop do tiskalnika ne uporabljajte enakega gesla ali uporabniškega imena, ki ga uporabljate za prijavo v računalnik. Avtentikacija z geslom ali pametno kartico mora uporabnikom priti v kri, pa ne le pri tiskanju, ampak tudi pri drugih opravilih – nekatere naprave podpirajo nastavitev, s katero mora uporabnik pri odpiranju, tiskanju ali spreminjanju datotek PDF (ali drugih datotek, ki bi lahko vsebovale škodljive kode) vnesti pravilno geslo.

Večina naprav podpira različne profile uporabnikov – najpogosteje dva ali tri: skrbnik naprave, skrbnik v podjetju ter uporabnik. Stopnje zaščite navadno lahko spreminja samo skrbnik naprave. Uporabnikom, ki se ne morejo prijaviti v napravo, lahko skrbnik dovoli uporabljati funkcije naprave v omejenem obsegu. Pri metodah avtentikacije je treba izbrati med naprednejšimi možnostmi, hkrati pa izklopiti protokole in komunikacijska vrata, ki ne bodo v uporabi. Novejše tiskalniške naprave poznajo tudi tako imenovani filter IP-naslovov, ki dostop dovoli le pooblaščenim napravam.

- Kibernetski kriminal meri na šibke člene, v omrežje povezane naprave.
- Prvi korak pri zaščiti tiskalnika je varnostna analiza tiskarniškega okolja.
- Avtentikacija z geslom ali pametno kartico mora uporabnikom priti v kri.
- Sodobne tiskalniške naprave omogočajo zaščito podatkov s šifriranjem.

Napadalci lahko pridejo fizično do tiskalnika

Čeprav je za napadalce omrežni dostop do tiskalnika idealna možnost, saj tako lahko ostanejo neopaženi, pa ne gre pozabiti tudi na filmske scenarije, ko se napadalec sprehodi do tiskalnika in ga pod pretvezo uporabnika ali vzdrževalca zlorabi. Včasih so napadalci lahko celo nezadovoljni zaposleni.

Varnostni strokovnjaki podjetjem svetujejo, da naj v primeru večopravilnih naprav onemogočijo vse funkcije, ki niso aktivno v uporabi – na primer funkcije USB-vrat in dodatnih vmesnikov, kot so zunanji pomnilniški mediji, bralniki kartic, tipkovnice in podobno. Zelo priporočljivo je omejiti tudi možnosti glede rabe e-poštne funkcionalnosti. Skrbnik lahko uporabnikom omeji dovoljenje za pošiljanje na izbrane e-poštne naslove. Naslovi, na katere je pošiljanje dovoljeno, se vnaprej registrirajo, kakor tudi naslovi, na katere pošiljanje ni dovoljeno.

Implementacija šifriranja in nadzornih orodij

Za višjo raven zaščite tiskalniškega okolja je treba uvesti dodatne varnostne ukrepe, na primer takšne, ki so skladni s standardom ISO 15408. Sodobne tiskalniške naprave omogočajo zaščito podatkov s šifriranjem, torej bi bili podatki, če bi jih napadalcu uspelo odtujiti, zanj brez posedovanja ustreznega ključa še vedno neuporabni. Naprave lahko šifrirajo dokumente, uporabniške nastavitve in podatke o napravi, za kodiranje pa velja uporabiti algoritem AES s 128- ali 256-bitno enkripcijo.

Za večja tiskalniška okolja je priporočljiva uporaba rešitev za nadzor tiskanja. Obstaja veliko različnih vrst nadzornih sistemov za tiskanje, delujejo pa na način, da uporabnik pošlje opravilo v skupno navidezno čakalno vrsto, ki je shranjena na osrednjem tiskalniškem strežniku. Naročilo je shranjeno na strežniku, dokler se uporabnik ne prijavi na napravo in izbere opravila, ki ga želi izvesti. Nato je opravilo tiskanja poslano na napravo, ki izpiše izbrane dokumente, na strežniku pa se zapišejo revizijski podatki za namene poročanja.

Čist se j

Top 50

Če zaokrožin hodkov 50 n panogi infor cijske tehnol ji, tudi po pr datkov za le da so skupaj enako vsoto dobre 1,7 mil prihodkov. G mesta zaseda in peti sta za je prehitel C

Božena Križ

Podjetja iz p kazujemo v ustvarila 1,72 tnih prihodk manj kot let 2015. Zaposlo (po izračunu ur) ali skoraj prej. Novinci Selectium Ad cehash, Micr See, Beenius, gorn, Sfera I polovici lestv

Daleč naj Slovenije. Ta hodke v prim žal za dobra milijona evr število zapos Drugi, A1 je s je približno ustvaril 216,2 tnih prihodk zaposlenimi

Čisti dobič 2016 več kot s skupaj neka čistega dobič izgube je pet la na 45,8 mi in 678.000 izgubo je pos tabele, skora vsote je prid Telemach (3 Oracle, Na zv munikacije i je z izgubo p ba (TSmedia evrov minus podjetja.

Zdrs čist primerjava n venski Telek sloval z dobr čistega dobič na 1,7 milijon no, zaradi o za morebitn stroške pres zaradi zmanj di sprememl telekomunik lani čisti do skoraj polovi milijona evr predlanskih 4 sko leto celo tisočaki minu