Ste tiskalnike pogledali **skozi prizmo varnosti?**

Kibernetski kriminalci so pretkani, razpoke v informacijski varnosti iščejo povsod, še najraje ciljajo na šibke člene sistemov. To so pogosto v omrežje povezane naprave, ki jih nihče ne sumi, npr. tiskalniki. Zanemarjanje tiskalniških naprav predstavlja precejšnje varnostno tveganje.

Hekerski napadi, industrijsko vohunjenje, nezadovoljni zaposleni … razlogov za »odtekanje« podatkov iz podjetja je lahko več. Podjetja pa le redko pomislijo, da je glavni krivec lahko tudi tiskalnik.

Tiskalniške naprave so danes računalniki v malem – opremljene so s pomnilnikom, trdimi diski ali pogoni SSD, na katerih (vsaj za krajši čas) hranijo datoteke, ki ji tiskajo ali skenirajo (večopravilne naprave). Naprednejše med njimi premorejo tudi funkcijo shranjevanja vsebin na omrežne vire, torej imajo dostop do drugih strežnikov in naprav v omrežju podjetja. Posebej večopravilne naprave so lahko izpostavljene številnim naprednim grožnjam, kot so na primer nepooblaščen dostop do naprav prek omrežja, spreminjanje informacij med prenosom po omrežju ali uhajanje podatkov s pomnilniških medijev naprav.

Žal so v mnogih poslovnih okoljih tiskalniki povsem spregledani, 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. To velja čim prej spremeniti.

»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 za podjetje uničujoče,« svari Ciril Kraševec, direktor podjetja Xenon forte, in dodaja: »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.«

Po toči zvoniti je prepozno

Japonski proizvajalec tiskalnikov Kyocera vsem organizacijam, ki uporabljajo večopravilne naprave, priporoča, da uvedejo in dejavno upoštevajo vsaj osnovne ukrepe zaščite tiskalniških naprav. Kje začeti? Pri upravljanju dostopa. Tiskalniške naprave so tovarniško opremljene s privzetim geslom za dostop. Nadvse priporočljivo je, da ga IT-osebje spremeni, saj napadalci najprej preizkusijo, ali so v uporabi tovarniške nastavitve. Skrbnik tiskalnika naj zato izbere novo ter ustrezno močno geslo, ki bo skladno z varnostno politiko podjetja. Pomnite tudi: za dostop do tiskalnika ni pametno uporabljati 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, temveč tudi 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 geslo.

Enkripcija podatkov in izklop funkcij, ki niso v uporabi

Varnostni strokovnjaki podjetjem svetujejo, naj skrbniki naprav preventivno izklopijo vse protokole in komunikacijska vrata (npr. priključke USB, bralnike kartic ipd.), ki ne bodo v uporabi. Novejše tiskalniške naprave poznajo tudi t. i. filtriranje IP-naslovov, ki dostop dovoli le »pooblaščenim« napravam. Za višjo raven zaščite tiskalniškega okolja velja uvesti dodatne varnostne ukrepe, npr. takšne, ki so skladni s standardom ISO 15408. Sodobne tiskalniške naprave omogočajo zaščito podatkov s šifriranjem, torej bi bili podatki, če bi jih napadalec uspel 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.

Tiskalniško okolje pod nadzorom

Za večja tiskalniška okolja je priporočljiva uporaba rešitev za nadzor tiskanja. Obstaja veliko različnih vrst nadzornih sistemov za tiskanje, ti delujejo na način, da uporabnik pošlje tiskalniško nalogo/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. ◀