BELA KNJIGA

ODKLENJENA VRATA

RAZISKAVA KAŽE, DA SO TISKALNIKI IZPOSTAVLJENI SPLETNIM NAPADOM

Skupine za informacijsko tehnologijo se usmerjajo na druge končne točke, pri tem pa pozabljajo na varnost tiskalnikov podjetja

Tiskalniki so lahke tarče: preveč tiskalnikov, povezanih v omrežje, nima nobenih omejitev in niso varno zaklenjeni.

Toda grožnja je resnična in je ne bi smeli zanemariti. Sodobni tiskalniki poslovnega razreda so zmogljive omrežne naprave s prav takšnimi ranljivostmi, kot so značilne za druge končne točke v omrežju. Te značilno nezaščitene končne točke predstavljajo zelo resnično možnost za spletne napade; preko njih je mogoče vdreti tudi v finančne in osebne podatke podjetja, kar ima zelo velike poslovne posledice.

Toda kljub temu nedavna anketa, ki so jo opravili pri 300 upraviteljih informacijske tehnologije v podjetjih kaže, da samo 16 % anketirancev meni, da so tiskalniki izpostavljeni visokemu tveganju za varnostno grožnjo/kršitev, kar je bistveno manj kot za namizne/prenosne in mobilne naprave.[1] To mnenje je hiba v pristopu osebja za informacijsko tehnologijo k varnosti omrežja. Tri od petih organizacij uporabljajo varnostne prakse za tiskalnike, toda ta odstotek je veliko nižji kot pri drugih končnih točkah, zato so tiskalniki izpostavljeni, čeprav so na voljo preproste rešitve za zašito te posebne končne točke.

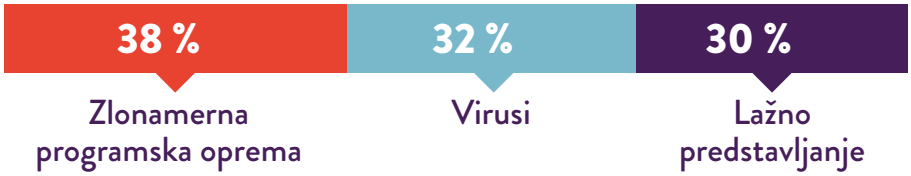
Ta bela knjiga predstavlja podatke o varnosti tiskalnikov na podlagi ankete, ki jo je opravilo podjetje Spiceworks, vplivu varnostnih kršitev in nekaterih sodobnih vgrajenih varnostnih funkcijah tiskalnikov, ki so oblikovane za zaščito pred spletnimi napadi.

SAMO 16 % ANKETIRANCEV MENI, DA SO TISKALNIKI IZPOSTAVLJENI VISOKEMU TVEGANJU ZA VARNOSTNO GROŽNJO/KRŠITEV.[1]

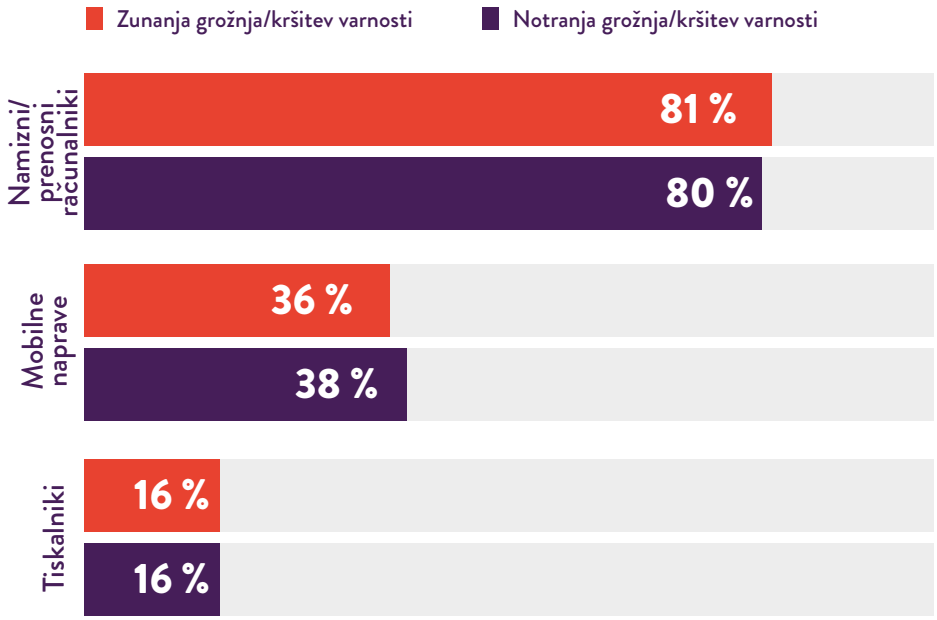
VHODI ZA NAPADE

V raziskavi, ki jo je opravilo podjetje Spiceworks, je 74 % anketirancev povedalo, da je njihova organizacija v preteklem letu izkusila neke vrste zunanje grožnje ali kršitve, povezane z varnostjo informacijske tehnologije. 70 % med njimi je izkusilo notranjo grožnjo ali kršitev, povezano z informacijsko tehnologijo, najpogosteje zaradi uporabniške napake, uporabe osebnih naprav za službene namene ali uporabe domačega ali javnega omrežja za službene namene.[1]

NAJPOGOSTEJŠE ZUNANJE GROŽNJE/KRŠITVE VARNOSTI INFORMACIJSKE TEHNOLOGIJE



Vir največjih groženj so v glavnem namizni in prenosni računalniki, druge pa prihajajo tudi prek mobilnih naprav in tiskalnikov.[1] (16 %, ki prihajajo prek tiskalnikov, je bistveno več kot 4 %, ki jih je razkrila podobna študija podjetja Speceworks iz leta 2014.) Možno je tudi, da je število napadov prek tiskalnikov podcenjeno, ker se za tiskalnike ne izvaja tako strog nadzor kot za računalnike in mobilne naprave.



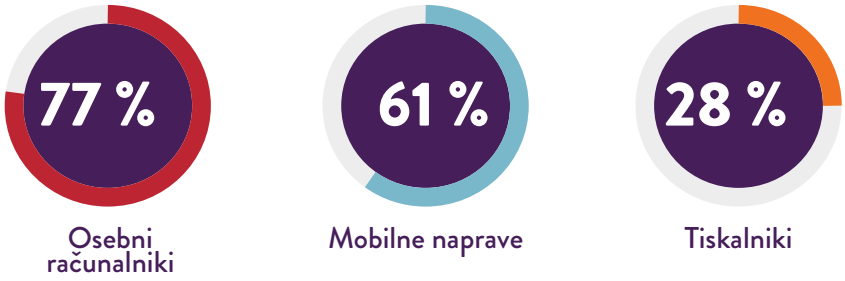
TISKALNIKI SO PREZRTI

V vsakem primeru anketa podjetja Spiceworks jasno kaže, da je varnost tiskalnikov pogosto na drugem mestu.

Organizacije se dobro zavedejo pomena varnosti omrežja, končnih točk in podatkov. Več kot tri četrtine anketirancev uporablja varnost omrežja, nadzor/upravljanje dostopa, zaščito podatkov ali varnost končnih točk ali kombinacijo vseh.[1]

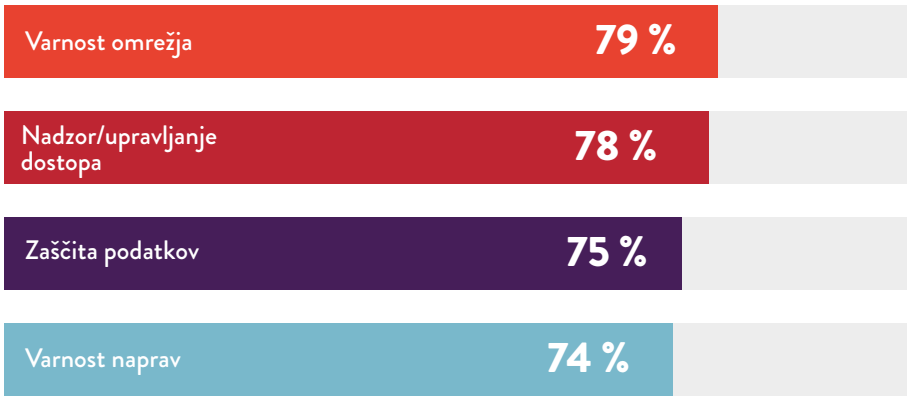
Toda te rešitve so veliko redkeje uporabljene na tiskalnikih. 83 % anketirancev uporablja varnost omrežja za namizne/prenosne računalnike in 55 % za mobilne naprave, toda samo 41 % med njimi jo uporablja za tiskalnike.[1]

Neskladje je še večje za varnost končnih točk:



Poleg tega niti ena tretjina (28 %) anketirancev za tiskalnike ne uporablja varnostnih potrdil za razliko od računalnikov, za katere jih uporablja 79 % med njimi, in mobilne naprave, za katere jih uporablja 54 % med njimi.[1]

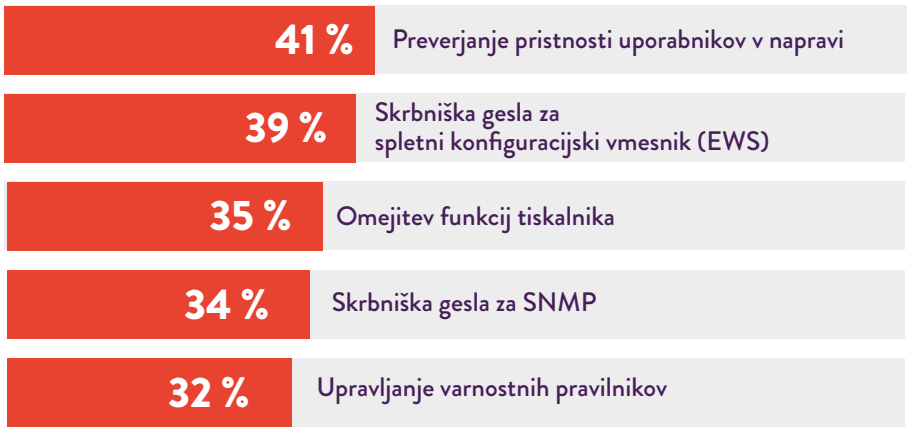
GLAVNE VARNOSTNE PRAKSE ZA KONČNE TOČKE



Med varnostnimi ukrepi, uporabljenimi za splošne končne naprave, so bili za tiskalnike najpogosteje uporabljeni varnost dokumentov, varnost omrežja in nadzor dostopa, toda manj kot polovica anketirancev je odgovorila, da jih v organizaciji uporabljajo za tiskalnike.[1]

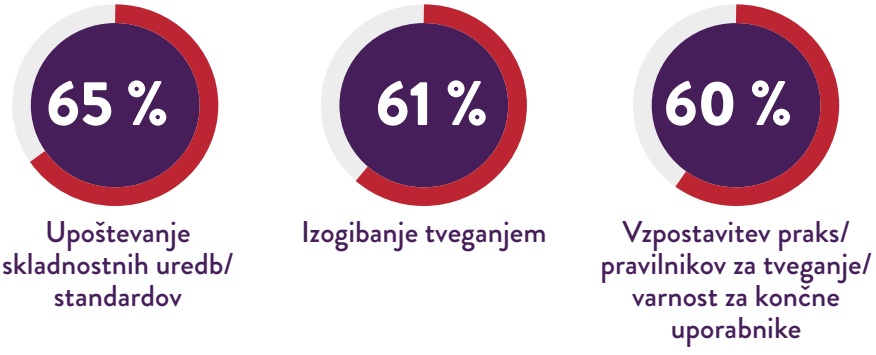
V nekaterih podjetjih imajo razvite varnostne prakse, specifične za tiskalnike, toda te prakse so povsem različne. Malo več kot 40 % organizacij uporablja za spletni konfiguracijski vmesnik preverjanje pristnosti uporabnikov, manj kot 40 % pa skrbniška gesla.[1] Za močnejšo zaščito bi morale te organizacije uporabljati kombinacijo vseh teh pristopov in še več.

GLAVNE VARNOSTNE PRAKSE, SPECIFIČNE ZA TISKALNIKE



Na področju praks skladnosti in pregledov za končne točke je varnost tiskalnikov skoraj za vsemi drugimi končnimi točkami. Skoraj 90 % organizacij uporablja pravilnik za varnost informacij, toda ti pravilniki običajno ne vključujejo tiskalnikov. 57 % anketirancev je na primer odgovorilo, da uporablja zaščito proti zlonamerni programski opremi na računalnikih, samo 17 % med njimi pa jo uporablja na tiskalnikih.[1]

SKORAJ 9 OD 10 STROKOVNJAKOV ZA INFORMACIJSKO TEHNOLOGIJO NAVAJA, DA V ORGANIZACIJI UPORABLJAJO VARNOSTNI PRAVILNIK ZA INFORMACIJE ZA NASLEDNJE NAMENE:



Jasno je, da organizacije varnosti tiskalnikov ne jemljejo dovolj resno, čeprav bi jo morale.

»Veliko tiskalnikov še vedno uporablja privzeta gesla ali sploh nobenih gesel ali pa jih deset med njimi uporablja isto geslo«, je junija za Computerworld povedal Michael Howard, glavni svetovalec podjetja HP za varnost. »Tiskalnik brez zaščite z geslom je zlata jama za hekerja. Ena od kršitev, ki smo ji pogosto priča, je napad s posrednikom (man-in-the-middle), pri katerem se napadalec polasti tiskalnika in preusmeri [dohodne dokumente] na prenosni računalnik, preden so natisnjeni. Tako si lahko ogleda vse, kar natisne direktor.«[2]

MOŽEN VPLIV VDOROV V TISKALNIKE

Glavni analitik za e-grožnje v podjetju Bitdefender, Bogdan Botezatu, pravi, da tiskalniki predstavljajo veliko potencialno varnostno luknjo. »V naših laboratorijih za preučevanje pomanjkljivosti prejmemo veliko telemetričnih podatkov. Usmerjevalnik ni več najslabša v internet povezana naprava. Zdaj je to tiskalnik.«[3]

Ta pomanjkljivost ima lahko zelo velik vpliv na podjetje. Že z enim samim nezavarovanim tiskalnikom lahko izpostavite celotno omrežje povezanih naprav napadu in hekerjem omogočite, da vohunijo v omrežnih napravah, s čimer ogrozite varnost celotnega omrežja.

Vsi smo že videli posledice varnostnih kršitev. V anketi podjetja Spiceworks so anketiranci odgovorili, da je to pet največjih vplivov kršitev:[1]

1. Več klicev službi za pomoč uporabnikov in več porabljenega časa za podporo

2. Zmanjšana storilnost/učinkovitost

3. Daljši čas nedelovanja sistema

4. Več porabljenega časa za klice za pomoč

5. Zvišana raven uveljavitve pravilnikov za končne uporabnike

Toda kršitev varnosti tiskalnika je lahko veliko resnejša, še posebej, če uporabljate večnamenski tiskalnik, ki lahko shranjuje podatke tiskalnika v elektronski obliki. Hekerji lahko prek tiskalniških opravil, shranjenih v pomnilniku tiskalnika, pridobijo dostop do občutljivih osebnih ali poslovnih informacij.

Še bolj zaskrbljujoče pa je dejstvo, da lahko hekerji prek nezavarovanega omrežja dostopajo do širšega omrežja podjetja in ukradejo locally irrelevant, replace with »davčne številke«, finančne informacije, interne dopise¸ in dokumente. Te ukradene informacije ne vplivajo samo na posamezne uslužbence, pač pa jih lahko uporabi tudi konkurenca ali resno škodujejo ugledu podjetja.

PREPROSTA REŠITEV: VGRAJENE VARNOSTNE FUNKCIJE

Jasno je, da se morajo podjetja posvetiti tudi varnosti tiskalnikov. Nekateri od sodobnih tiskalnikov za podjetja vključujejo za uporabo preproste vgrajene varnostne funkcije, ki se spopadajo z grožnjami za tiskalnike. Te so:

- samodejno odkrivanje napadov, zaščita in popravilo;
- spremljanje uporabe za preprečevanje nepooblaščene uporabe;
- preproste možnosti prijave, na primer gesla ali pametne kartice;
- bralnik približevalnih kartic, ki uporabnikom omogoča hitro preverjanje pristnosti in varno tiskanje na tiskalniku z obstoječo identifikacijsko oznako;
- varno šifrirano tiskanje za občutljive dokumente.

Ko boste razmišljali o nakupu naslednjega tiskalnika, pa naj bo namizni ali večnamenski, raziščite njegove vgrajene varnostne funkcije in jih aktivirajte. Z uporabo preprostih, za tiskalnik specifičnih funkcij, kot so te, boste odpravili ranljivost prek tiskalnikov; konec koncev internet stvari ponuja še veliko drugih dostopnih točk, ki nas lahko skrbijo in ni **treba, da so tiskalniki ena med njimi.**

IŠČETE VARNEJŠE TISKALNIKE?

VEČ INFORMACIJ ›

Viri:

[1] Anketa podjetje Spiceworks, v kateri je sodelovalo 309 upraviteljev informacijske tehnologije v Severni Ameriki, državah EMEA in APAC, ki je bila na zahtevo HP-jeva izvedena novembra 2016.

[2] Članek »Printer Security: Is your company's data really safe?« Computerworld, 1. junij 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] Članek »Printers Now the Least-secure Things on the Internet«, The Register, 8. september 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/