STUDIJA

OTKLJUČANA VRATA

ISTRAŽIVANJA POKAZUJU DA SU PISAČI IZLOŽENI INTERNETSKIM NAPADIMA

Dok su IT timovi usredotočeni na druge krajnje točke, sigurnost poslovnih pisača zaostaje

Pisači su lake mete: previše s mrežom povezanih pisača nema ograničenja i nije zaštićeno.

No prijetnja je stvarna i ne smije se zanemariti. Pisači poslovne klase razvili su se u napredne, umrežene uređaje s istim slabim točkama kao i druge krajnje točke u mreži. Za te je obično nezaštićene ulazne točke mogućnost internetskih napada vrlo stvarna. Uz to, one omogućuju pristup financijskim i privatnim podacima u tvrtki, što može imati vrlo stvarne posljedice za tvrtku.

Unatoč tome, nedavno provedena anketa tvrtke Spiceworks na više od 300 korporacijskih donositelja odluka povezanih s IT-jem pokazala je da svega 16 % anketiranih osoba smatra da za pisače postoji visoki rizik od sigurnosnih prijetnji i povreda sigurnosti, što je znatno manje nego za stolna/prijenosna računala i mobilne uređaje.[1] Takav se stav negativno odrazio na način na koji IT osoblje pristupa sigurnosti mreže. Premda gotovo tri od pet tvrtki i ustanova ima definirane sigurnosne postupke za pisače, taj je postotak mnogo manji nego za druge krajnje točke – i pisači su izloženi napadima premda postoje jednostavna rješenja za zaštitu te ulazne točke.

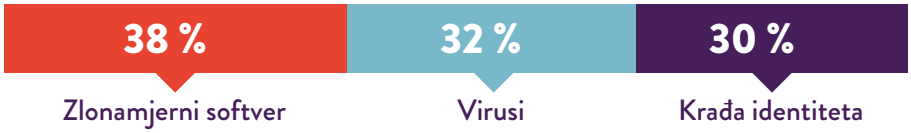
Ova studija daje uvid u podatke o sigurnosti pisača dobivene na temelju ankete tvrtke Spiceworks, posljedicama povreda sigurnosti i nekim sigurnosnim značajkama za zaštitu od internetskih napada ugrađenima u suvremene pisače.

SVEGA 16 % ANKETIRANIH OSOBA SMATRA DA ZA PISAČE POSTOJI VISOKI RIZIK OD SIGURNOSNIH PRIJETNJI I POVREDA SIGURNOSTI.[1]

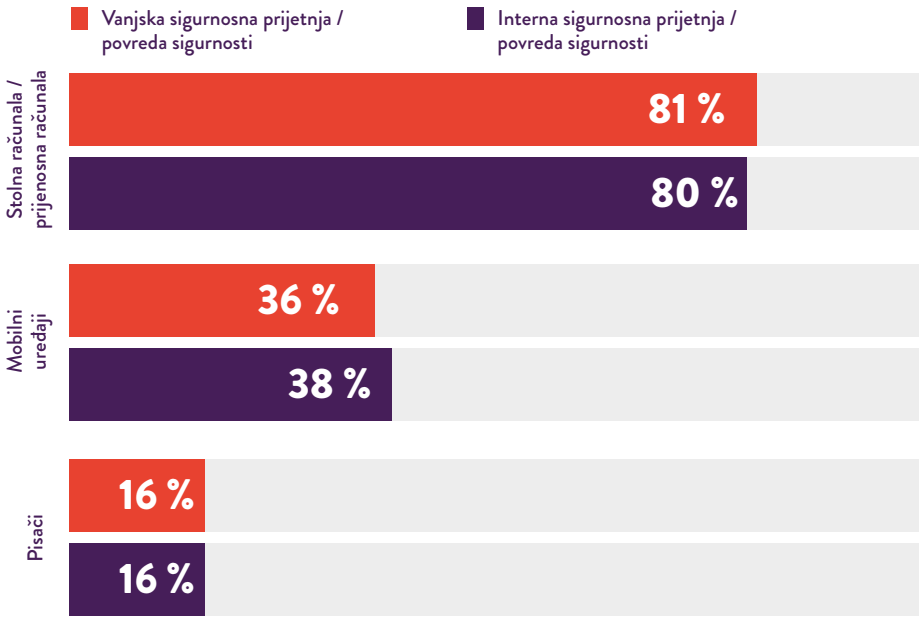
OTVORENA VRATA ZA NAPADE

U anketi tvrtke Spiceworks 74 % anketiranih osoba (neto) izjavilo je da se njihova tvrtka ili ustanova tijekom prošle godine susrela s nekom vrstom vanjske sigurnosne prijetnje ili povrede sigurnosti povezane s IT-jem. Uz to, 70 % (neto) anketiranih osoba susrelo se s internom sigurnosnom prijetnjom ili povredom sigurnosti povezanom s IT-jem, najčešće zbog korisničke pogreške, zbog korištenja osobnih uređaja u poslovne svrhe ili jer su zaposlenici koristili kućnu ili javnu mrežu u poslovne svrhe.[1]

NAJČEŠĆE VANJSKE SIGURNOSNE PRIJETNJE / POVREDE SIGURNOSTI POVEZANE S IT-JEM



Najčešće prijetnje došle su prvenstveno putem stolnih i prijenosnih računala, a ostale putem mobilnih uređaja i pisača.[1] (16 % napada putem pisača znatno je više od 4 % iz slične studije tvrtke Spiceworks iz 2014.) Moguće je i da je broj napada putem pisača podcijenjen jer se pisači ne nadziru tako pomno kao PC-ji i mobilni uređaji.



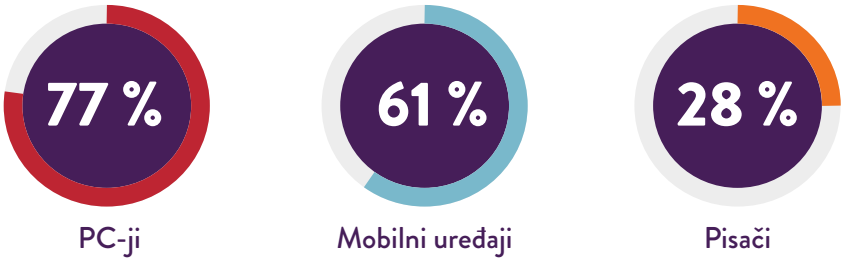
SIGURNOST PISAČA NE SHVAĆAMO DOVOLJNO OZBILJNO

U svakom slučaju, iz ankete tvrtke Spiceworks očito je da sigurnost pisača često nije prioritet.

Tvrtke i ustanove itekako su svjesne važnosti sigurnosti mreže, krajnjih točaka i podataka. Zapravo, više od tri četvrtine anketiranih osoba koristi zaštitu mreže, kontrolu pristupa / upravljanje pristupom, zaštitu podataka ili zaštitu krajnjih točaka – ili neku kombinaciju tih načina zaštite.[1]

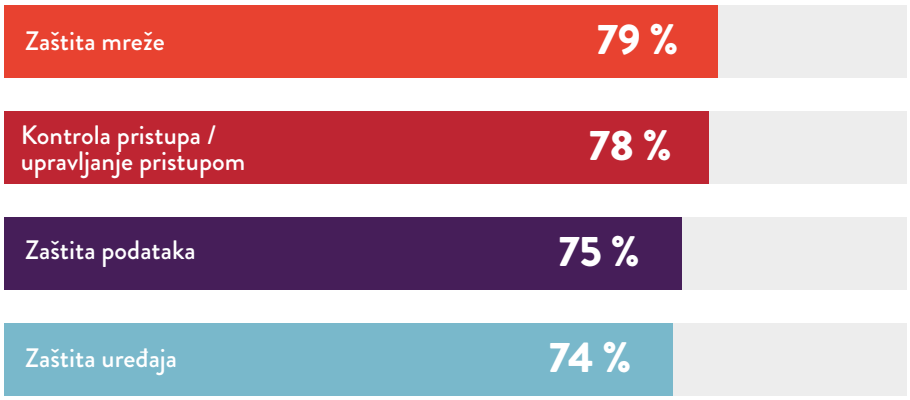
No ta se rješenja znatno rjeđe implementiraju za pisače. Premda 83 % anketiranih osoba koristi zaštitu mreže na prijenosnim/stolnim računalima i 55 % na mobilnim uređajima, na pisačima je koristi svega 41 %.[1]

Razlika je još veća za zaštitu krajnjih točaka:



Uz to, ni trećina (28 %) anketiranih osoba ne implementira sigurnosne certifikate za pisače, za razliku od 79 % za PC-je i 54 % za mobilne uređaje.[1]

NAJČEŠĆI POSTUPCI ZAŠTITE KRAJNJIH TOČAKA



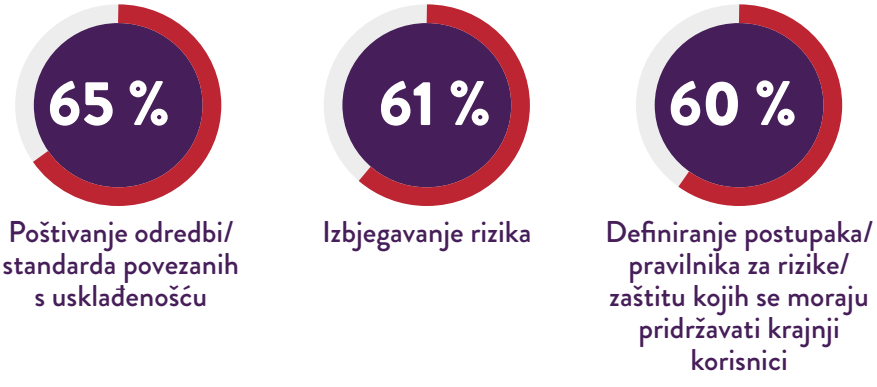
Od načina zaštite koji se koriste na uobičajenim uređajima na krajnjim točkama najčešće korištene sigurnosne mjere za pisače bile su zaštita dokumenata, zaštita mreže i kontrola pristupa, ali manje od polovice anketiranih osoba izjavilo je da se u njihovim tvrtkama ili ustanovama neki od tih načina zaštite koriste na pisačima.[1]

Neke tvrtke imaju sigurnosne postupke za pisače, ali i u njima se ti postupci međusobno znatno razlikuju. Svega nešto više od 40 % tvrtki i ustanova implementiralo je provjeru autentičnosti korisnika, a manje od 40 % koristilo je administratorske lozinke za sučelje za konfiguraciju putem weba.[1] Da bi se dobro zaštitila, svaka tvrtka i ustanova mora koristiti kombinaciju svih navedenih pristupa – i ne samo to.

NAJČEŠĆI SIGURNOSNI POSTUPCI ZA PISAČE

Kada je riječ o usklađenosti krajnjih točaka i postupcima nadzora, sigurnosne kontrole za pisače zaostaju za svim drugim krajnjim točkama. Gotovo 90 % tvrtki i ustanova ima implementiran pravilnik o zaštiti podataka, ali ti se pravilnici obično ne odnose na pisače. Na primjer, premda je 57 % anketiranih osoba izjavilo da su implementirali zaštitu od zlonamjernog softvera na PC-jima, svega 17 % implementiralo ju je za pisače.[1]

GOTOVO 9 OD 10 IT PROFESIONALACA IZJAVILO JE DA NJIHOVA TVRTKA ILI USTANOVA IMA PRAVILNIK O ZAŠTITI PODATAKA IZ SLJEDEĆIH RAZLOGA:



Tvrtke i ustanove očito ne shvaćaju zaštitu pisača dovoljno ozbiljno – a svakako bi trebale.

"Mnogi pisači još uvijek imaju zadane lozinke ili uopće nemaju lozinku ili pak deset pisača koristi istu lozinku", za Computerworld je u lipnju izjavio Michael Howard, glavni savjetnik za sigurnost u HP-u. "Pisač bez zaštite lozinkom zlatni je rudnik za hakere. Jedna je od čestih povreda sigurnosti posrednički (man-in-the-middle) napad, prilikom kojeg napadači preuzimaju pisač i preusmjeravaju [dolazne dokumente] na prijenosno računalo prije nego što se ispišu. Napadači mogu vidjeti sve što glavni direktor ispisuje."[2]

MOGUĆE POSLJEDICE NEOVLAŠTENOG PRISTUPA PISAČU

Bogdan Botezatu, viši analitičar za e-prijetnje u tvrtki Bitdefender, smatra da pisači predstavljaju poprilično potencijalnu sigurnosnu slabu točku. "Dobivamo mnogo telemetrijskih podataka u našim laboratorijima za procjenu slabih točaka. Usmjerivač nije više nagori uređaj na internetu. Sada je to pisač."[3]

Ta slaba točka može imati dalekosežne posljedice za tvrtku. Uz jedan nezaštićeni pisač cijelu mrežu povezanih uređaja ostavljate izloženu napadu i hakerima omogućujete špijuniranje umreženih uređaja te ugrožavate sigurnost cijele mreže.

Svi smo vidjeli posljedice povreda sigurnosti. U anketi tvrtke Spiceworks anketirane su osobe izjavile da su pet glavnih posljedica povrede sigurnosti:[1]

Ali povreda sigurnosti pisača može biti ozbiljnija, a posebice ako koristite višefunkcijski pisač s mogućnošću elektroničke pohrane ispisanih podataka.

Zadaci ispisa pohranjeni u predmemoriji pisača hakerima omogućuju pristup povjerljivim osobnim i poslovnim podacima.

Još više zabrinjava činjenica da hakeri putem nezaštićenog pisača mogu pristupiti široj mreži tvrtke i ukrasti podatke kao što su osobni identifikacijski brojevi, financijski podaci te interni dopisi i dokumenti. Ti ukradeni podaci mogu utjecati ne samo na pojedinačne zaposlenike, već ih mogu koristiti konkurentske tvrtke te mogu znatno narušiti ugled tvrtke.

JEDNOSTAVNO RJEŠENJE: UGRAĐENE SIGURNOSNE ZNAČAJKE

Tvrtke se očito moraju pozabaviti sa sigurnošću i za pisače. Neki su današnji suvremeni poslovni pisači opremljeni za korištenje jednostavnim ugrađenim sigurnosnim značajkama koje pisač štite od prijetnji. To uključuje sljedeće značajke:

- Automatsko otkrivanje napada, zaštita od napada i ublažavanje posljedica napada
- Praćenje korištenja radi sprječavanja neovlaštenog korištenja
- Jednostavni načini prijave, npr. putem PIN-a ili pametnih kartica
- Čitač beskontaktnih kartica koji korisnicima omogućuje brzu potvrdu identiteta i siguran ispis na pisaču pomoću identifikacijske kartice
- Siguran šifrirani ispis povjerljivih dokumenata

Prilikom odabira novog pisača, bilo stolnog ili višefunkcijskog, proučite integrirane sigurnosne značajke – i obavezno ih aktivirajte. Uz takve jednostavne, za pisač specifične značajke nema razloga da budete izloženi napadima putem pisača. Naposljetku, uz internet stvari mnogo je drugih pristupnih točaka o kojima morate brinuti –**pisači ne moraju biti među njima.**

TRAŽITE SIGURNIJE PISAČE?

SAZNAJTE VIŠE ›

Izvori:

[1] Anketa tvrtke Spiceworks provedena na 309 donositelja odluka iz područja IT-ja u Sjevernoj Americi, državama EMEA-e i državama APAC-a u ime HP-a u studenom 2016.

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

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