TECHNICKÁ DOKUMENTÁCIA

OTVORENÉ DVERE

PRIESKUM POTVRDZUJE, ŽE TLAČIARNE MOŽNO ĽAHKO ZNEUŽIŤ PRI KYBERNETICKÝCH ÚTOKOCH

Stredobodom pozornosti IT tímov sú iné koncové zariadenia, zatiaľ čo zabezpečenie podnikových tlačiarní zaostáva

Tlačiarne sú ľahkým terčom: veľké množstvo tlačiarní pripojených do siete možno používať bez obmedzení a nie sú zabezpečené blokovaním.

Je tu však reálna hrozba, ktorú netreba ignorovať. Podnikové tlačiarne sú dnes už výkonné sieťové zariadenia, ktoré čelia rovnakým bezpečnostným rizikám ako ktorékoľvek iné koncové zariadenie zapojené do siete. Sú to častokrát nezabezpečené vstupné body, ktoré predstavujú skutočnú potenciálnu hrozbu kybernetických útokov, a možno ich využiť na získanie prístupu k finančným a osobným údajom vo vašej spoločnosti, čo môže mať vážne dôsledky pre vaše podnikanie.

Napriek tomu ale podľa najnovšieho prieskumu spoločnosti Spiceworks, ktorého sa zúčastnilo viac ako 300 vedúcich pracovníkov IT, iba 16 % opýtaných považuje tlačiarne za vysoko rizikové z pohľadu bezpečnostných hrozieb alebo narušenia zabezpečenia. Je to výrazne menej v porovnaní s počítačmi, notebookmi a mobilnými zariadeniami.[1] Toto vnímanie má vplyv na to, ako IT pracovníci pristupujú k zabezpečeniu sietí. Postupy zabezpečenia tlačiarní bežne používajú takmer tri spoločnosti z piatich, ale tento pomer je výrazne nižší ako v prípade iných koncových zariadení a tlačiarne sa tak stávajú zraniteľným miestom aj napriek tomu, že na ochranu tohto vstupného bodu existujú jednoduché riešenia.

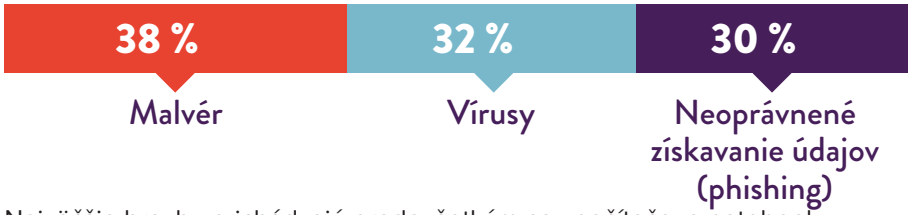
Táto technická dokumentácia poskytuje informácie o zabezpečení tlačiarní vyplývajúce z prieskumu Spiceworks, vplyve bezpečnostných prienikov a niektorých moderných zabudovaných bezpečnostných funkciách tlačiarní určených na ochranu proti kybernetickým útokom.

LEN 16 % OPÝTANÝCH POVAŽUJE TLAČIARNE ZA VYSOKO RIZIKOVÉ Z POHĽADU BEZPEČNOSTNÝCH HROZIEB ALEBO NARUŠENIA ZABEZPEČENIA.[1]

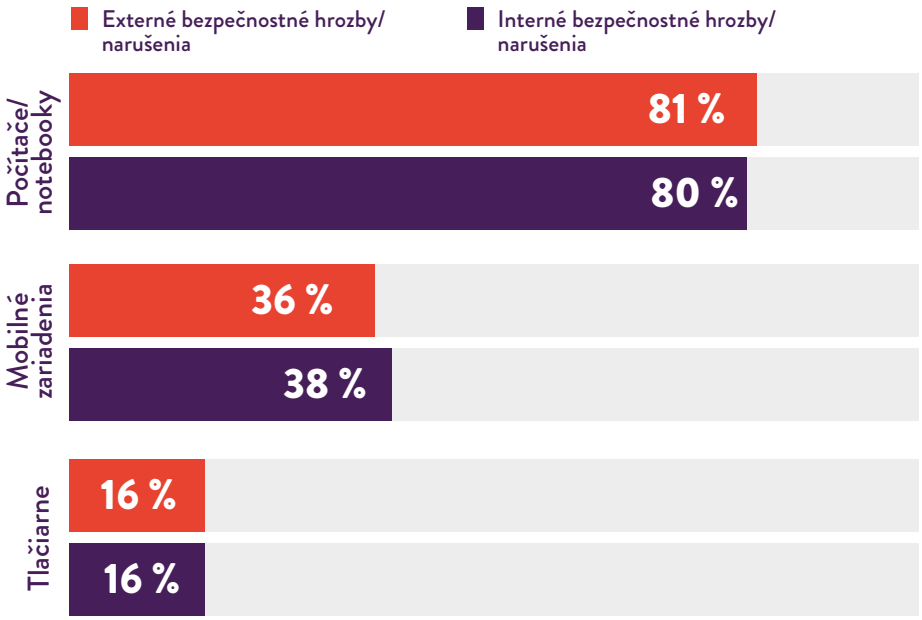
OTVORENÉ DVERE PRE ÚTOKY

74 % (čistý počet) opýtaných v prieskume Spiceworks uviedlo, že v ich IT spoločnosti došlo v priebehu uplynulého roku k nejakému druhu externej bezpečnostnej hrozby alebo narušenia zabezpečenia. Ďalších 70 % (čistý počet) zaznamenalo internú bezpečnostnú hrozbu alebo narušenie zabezpečenia IT, pričom najčastejším dôvodom bola chyba používateľa, používanie osobných zariadení na pracovné účely alebo situácia, keď zamestnanci pri práci používajú domácu alebo verejnú sieť.[1]

NAJVÄČŠIE ZAZNAMENANÉ EXTERNÉ BEZPEČNOSTNÉ HROZBY ALEBO NARUŠENIA ZABEZPEČENIA IT



Najväčšie hrozby prichádzajú predovšetkým cez počítače a notebooky a ďalšie si hľadajú cestu cez mobilné zariadenia a tlačiarne.[1] (Podiel 16 % hrozieb pochádzajúcich z tlačiarní je výrazne vyšší ako 4 % zaznamenané v podobnej štúdii spoločnosti Spiceworks z roku 2014.) Je tiež možné, že počet útokov prichádzajúcich cez tlačiarne je podhodnotený, pretože tlačiarne sa nesledujú tak prísne ako počítače a mobilné zariadenia.



ZANEDBÁVAME SVOJE TLAČIARNE

Z prieskumu spoločnosti Spiceworks jasne vyplýva, že bez ohľadu na konkrétny prípad sa na zabezpečenie tlačiarní často myslí až dodatočne.

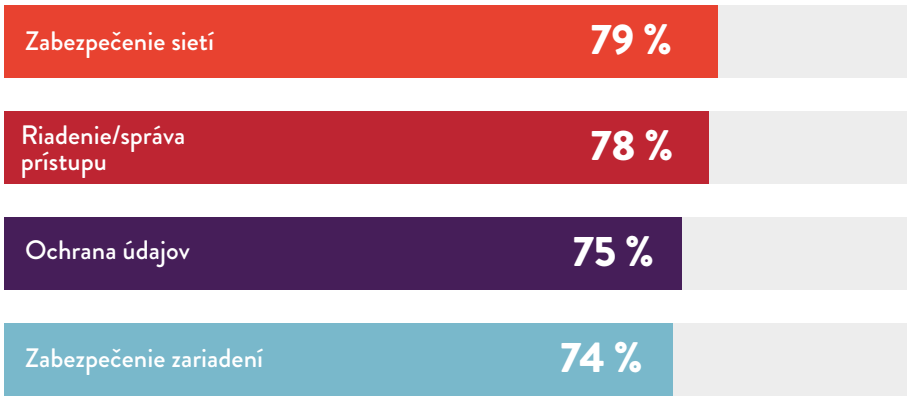
Spoločnosti si veľmi dobre uvedomujú, aké dôležité je zabezpečenie siete, koncových zariadení a údajov. Pravdou je, že viac ako tri štvrtiny opýtaných používa zabezpečenie sietí, riadenie/správu prístupu, ochranu údajov alebo zabezpečenie koncových zariadení, prípadne kombináciu týchto riešení.[1]

Čo sa ale týka tlačiarní, tieto postupy sa často zavádzajú v oveľa menšej miere. Hoci 83 % opýtaných používa zabezpečenie sietí v počítačoch a notebookoch a 55 % v mobilných zariadeniach, len 41 % používa takéto zabezpečenie v tlačiarňach.[1]

Ešte priepastnejší nepomer sa prejavuje v oblasti zabezpečenia koncových zariadení:

Certifikáty zabezpečenia tlačiarní má navyše zavedené ani nie tretina opýtaných (28 %), pričom pre porovnanie v prípade počítačov je to 79 % a v prípade mobilných zariadení 54 %.[1]

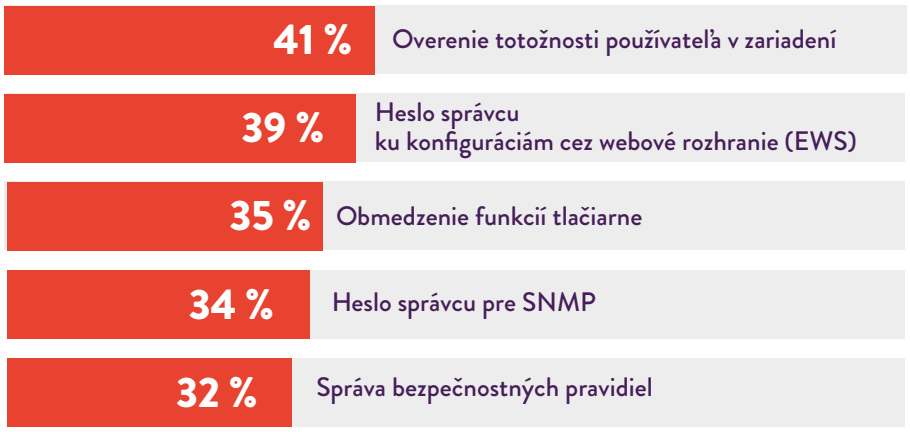
NAJČASTEJŠIE POSTUPY ZABEZPEČENIA KONCOVÝCH ZARIADENÍ



Čo sa týka ochrany všeobecných koncových zariadení, medzi najpoužívanejšie bezpečnostné opatrenia pre tlačiarne patria zabezpečenie dokumentov, zabezpečenie sietí a riadenie prístupu. Používanie niektorého z týchto riešení v rámci spoločnosti však uviedla menej ako polovica opýtaných.[1]

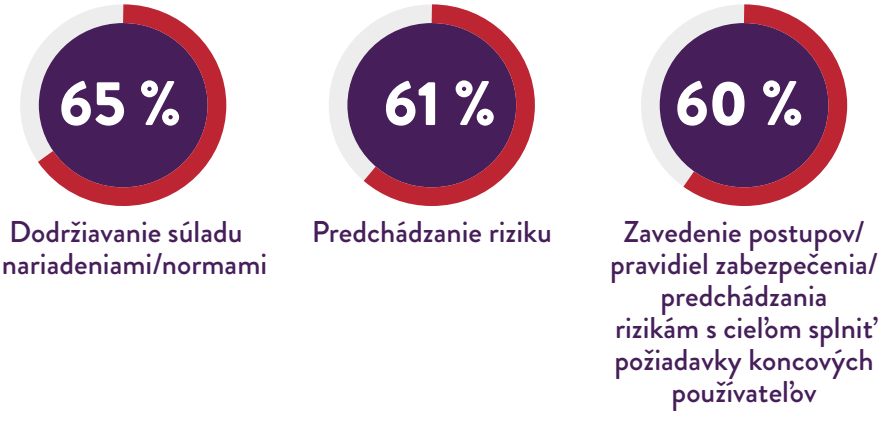
Niektoré spoločnosti majú postupy zabezpečenia určené osobitne pre tlačiarne, ale aj tak sú tieto postupy značne nesúrodé. Len niečo vyše 40 % spoločností zaviedlo overenie používateľa a menej ako 40 % používa heslá správcov pri konfigurácii cez webové rozhranie.[1] Všetky spoločnosti by mali používať spojenie všetkých týchto prístupov – a omnoho viac – ak sa má dosiahnuť silná ochrana.

NAJČASTEJŠIE POSTUPY ZABEZPEČENIA TLAČIARNÍ



Pokiaľ ide o dodržiavanie súladu a postupy auditov koncových zariadení, tlačiarne zaostávajú v kontrolách zabezpečenia za všetkými ostatnými koncovými zariadeniami. Takmer 90 % spoločností zaviedlo pravidlá zabezpečenia informácií, ktoré sa ale zvyčajne netýkajú tlačiarní. Ochranu pred malvérom napríklad vo svojich počítačoch používa 57 % opýtaných, ale iba 17 % opýtaných takúto ochranu zaviedlo v tlačiarňach.[1]

TAKMER 9 Z 10 IT ODBORNÍKOV UVÁDZA, ŽE ICH SPOLOČNOSŤ ZAVIEDLA PRAVIDLÁ ZABEZPEČENIA INFORMÁCIÍ Z TÝCHTO DÔVODOV:



Niet pochýb, že spoločnosti neberú zabezpečenie tlačiarní dostatočne vážne, pritom by jednoznačne mali.

„Ešte stále majú mnohé tlačiarne heslo nastavené výrobcom, nemajú vôbec žiadne heslo alebo jedno heslo používajú desiati používatelia," uviedol v júni pre Computerworld Michael Howard, vedúci poradca spoločnosti HP pre oblasť zabezpečenia. „Tlačiareň bez ochrany heslom je pre hekera zlatá baňa. Jeden z útokov, s ktorým sa často stretávame, je zachytenie dát počas ich prenosu, keď heker získa kontrolu nad tlačiarňou a presmeruje (prichádzajúce dokumenty) na notebook skôr ako sa vytlačia. Vidí všetko, čo dáva generálny riaditeľ tlačiť."[2]

MOŽNÝ VPLYV PRIENIKOV DO TLAČIARNÍ

Podľa slov hlavného analytika spoločnosti Bitdefender v oblasti elektronických hrozieb Bogdan Botezatu, tlačiarne môžu predstavovať značné diery v bezpečnosti. „V našich laboratóriách na posudzovanie zraniteľnosti robíme veľa telemetrických meraní. Najhorším zariadením na internete už nie je smerovač. Teraz je to tlačiareň."[3]

Táto zraniteľnosť sa môže výrazne podpísať na podnikaní. Stačí jedna nezabezpečená tlačiareň a celú sieť pripojených zariadení môže ohroziť útok, ktorý hekerom umožní sledovať vaše sieťové zariadenia a narušiť zabezpečenie celej siete.

Všetci poznáme dôsledky hekerských prienikov. V prieskume spoločnosti Spiceworks respondenti označili týchto päť najvýznamnejších dôsledkov narušenia zabezpečenia:[1]

1. Nárast počtu volaní na oddelenie technickej podpory a predĺženie času poskytovania podpory

2. Znížená produktivita/účinnosť

3. Vyššia miera výpadkov systému

4. Predĺženie času volaní na technickú podporu

5. Viac prípadov presadzovania pravidiel určených pre koncových používateľov

Narušenie zabezpečenia tlačiarne môže byť ale oveľa vážnejšie, najmä ak používate multifunkčnú tlačiareň s funkciou elektronického ukladania údajov tlačiarne. Tlačové úlohy uložené vo vyrovnávacej pamäti tlačiarne hekerom umožňujú získať prístup k citlivým osobným alebo obchodným informáciám.

Ešte znepokojujúcejšie je, že hekeri môžu pomocou nezabezpečenej

tlačiarne získať prístup do širšej siete spoločnosti a zmocniť sa napríklad rodných čísiel, finančných informácií alebo interných poznámok a dokumentov. Tieto odcudzené informácie nielenže môžu ovplyvniť jednotlivých zamestnancov, ale môžu poslúžiť aj konkurencii alebo výrazne poškodiť meno spoločnosti.

JEDNODUCHÉ RIEŠENIE: ZABUDOVANÉ BEZPEČNOSTNÉ FUNKCIE

Je nepochybné, že spoločnosti sa musia zaoberať otázkou zabezpečenia aj v tlačiarňach. V súčasnosti sú niektoré moderné podnikové tlačiarne zabezpečené zabudovanými funkciami s jednoduchou obsluhou na boj proti hrozbám zameraným na tlačiarne. Medzi tieto funkcie patria:

- Automatické odhaľovanie útokov, ochrana proti nim a ich riešenie
- Sledovanie používania na predchádzanie neoprávnenému použitiu
- Jednoduché možnosti prihlásenia, napríklad pomocou PIN kódu alebo čipových kariet
- Čítačka bezkontaktných kariet, ktorá používateľom umožňuje bezpečné použitie tlačiarne s rýchlym overením pomocou identifikačnej karty
- Bezpečná šifrovaná tlač citlivých dokumentov

Keď budete najbližšie uvažovať o tlačiarni, či už o stolnej alebo multifunkčnej, informujte sa o jej zabudovaných funkciách zabezpečenia a dbajte na to, aby boli zapnuté. Keď máte k dispozícii takéto jednoduché funkcie určené osobitne pre tlačiarne, nie je dôvod, aby ste sa prostredníctvom svojich tlačiarní naďalej vystavovali riziku. Napokon, keď pomyslíme na Internet vecí, existuje kvantum iných prístupových bodov, pre ktoré si treba robiť starosti – **tlačiareň nemusí byť jedným z nich.**

HĽADÁTE TLAČIARNE S VYŠŠÍM ZABEZPEČENÍM?
ĎALŠIE INFORMÁCIE ›

Zdroje:

[1] Prieskum spoločnosti Spiceworks, ktorý sa uskutočnil v novembri 2016 v mene spoločnosti HP medzi 309 vedúcimi pracovníkmi IT v Severnej Amerike, regiónoch EMEA a APAC.

[2] „Printer Security: Is your company's data really safe?", Computerworld, 1. júna 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. septembra 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/