OFICIÁLNÍ ZPRÁVA

ODEMČENÉ DVEŘE

PRŮZKUM UKAZUJE, ŽE TISKÁRNY ČASTO BÝVAJÍ NEZABEZPEČENÉ PROTI KYBERNETICKÝM ÚTOKŮM

Zatímco se týmy IT soustředí na jiná koncová zařízení, zabezpečení firemních tiskáren zaostává

Tiskárny jsou přitom snadným cílem: Většina tiskáren připojených k síti nemá žádná omezení a není ani bezpečně uzamčena.

Hrozba je však skutečná, a nelze ji ignorovat. Firemní tiskárny se vyvinuly v silná, síťová zařízení, která jsou však stejně zranitelná jako kterákoliv jiná koncová zařízení v síti. Vzhledem k tomu, že jsou tyto vstupní body často nezabezpečené, stávají se velmi reálnými cíli kybernetických útoků; zároveň také mohou poskytnout přístup k finančním a osobním údajům vaší společnosti, což pro vás může mít závažné obchodní důsledky.

Přesto nedávný průzkum společnosti Spiceworks, kterého se zúčastnilo více než 300 podnikových činitelů odpovědných za IT, ukázal, že jen 16 % respondentů se domnívá, že tiskárnám hrozí vysoké riziko ohrožení/narušení zabezpečení, což je výrazně méně než u stolních počítačů/notebooků a mobilních zařízení.[1] Tato představa odráží způsob, jakým oddělení IT přistupují k zabezpečení sítě. Přestože téměř tři z pěti organizací využívají bezpečnostní postupy pro tiskárny, toto procento je mnohem nižší než u ostatních koncových zařízení – tiskárny tak zůstávají nezabezpečené, přestože existují jednoduchá řešení, která dokáží tato vstupní zařízení spolehlivě ochránit.

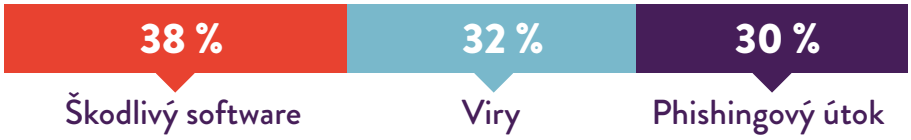
Tato oficiální zpráva prezentuje údaje o zabezpečení tiskáren založené na průzkumu společnosti Spiceworks, dopad narušení zabezpečení, jakož i některé moderní vestavěné funkce zabezpečení tiskáren navržené k jejich ochraně před kybernetickými útoky.

JEN 16 % RESPONDENTŮ SE DOMNÍVÁ, ŽE TISKÁRNÁM HROZÍ VYSOKÉ RIZIKO OHROŽENÍ/NARUŠENÍ ZABEZPEČENÍ.[1]

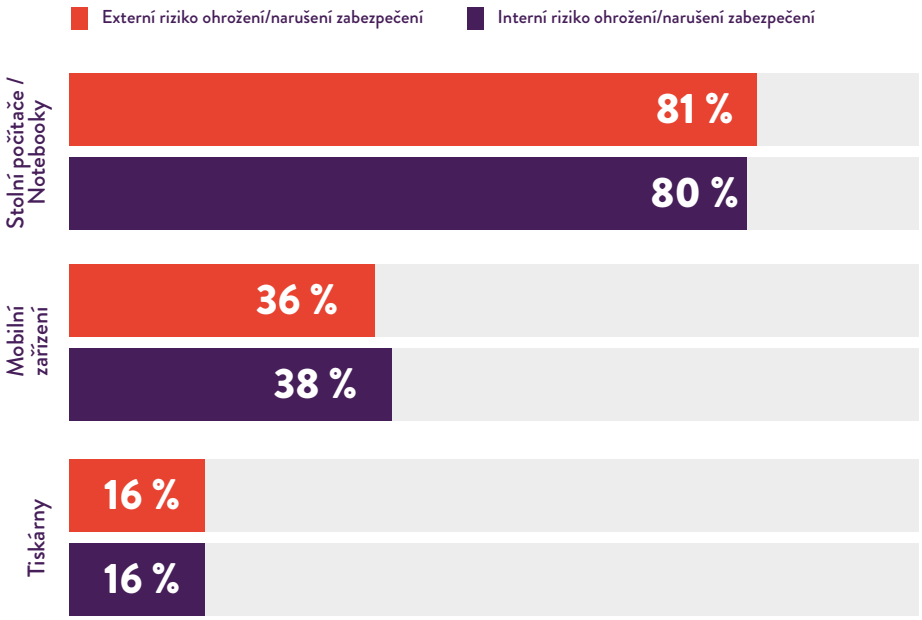
VSTUPNÍ BRÁNY PRO ÚTOKY

V průzkumu společnosti Spiceworks 74 % respondentů uvedlo, že jejich organizace v minulém roce zažila alespoň jeden druh externího ohrožení nebo narušení bezpečnosti IT. A 70 % zažilo interní ohrožení nebo narušení bezpečnosti IT, které bylo nejčastěji způsobeno chybou uživatele, používáním osobních zařízení pro pracovní účely, nebo používáním domácí nebo veřejné sítě pro pracovní účely.[1]

HLAVNÍ EXTERNÍ OHROŽENÍ NEBO NARUŠENÍ BEZPEČNOSTI IT



Hlavní hrozby se přitom primárně vplížily přes stolní počítače a notebooky, zatímco ostatní přišly přes mobilní zařízení a tiskárny.[1] 16 % hrozeb přicházejících přes tiskárny je přitom pozoruhodně vyšší údaj než 4 % zjištěná při podobné studii společnosti Spiceworks provedené v roce 2014. Je také možné, že počet útoků přicházejících přes tiskárny je podceňován, protože tiskárny nejsou tak pečlivě sledovány jako počítače a mobilní zařízení.



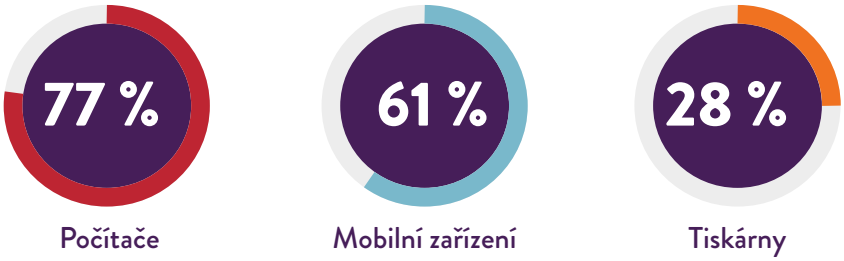
ZAPOMÍNÁME NA NAŠE TISKÁRNY

Ať tak či onak, průzkum společnosti Spiceworks jasně ukazuje, že zabezpečení tiskáren bývá často druhořadé.

Organizace si plně uvědomují důležitost zabezpečení sítě, koncových zařízení i dat. Ve skutečnosti více než tři čtvrtiny respondentů používají zabezpečení sítě, řízení/správu přístupu, ochranu dat, zabezpečení koncových zařízení nebo jejich kombinaci.[1]

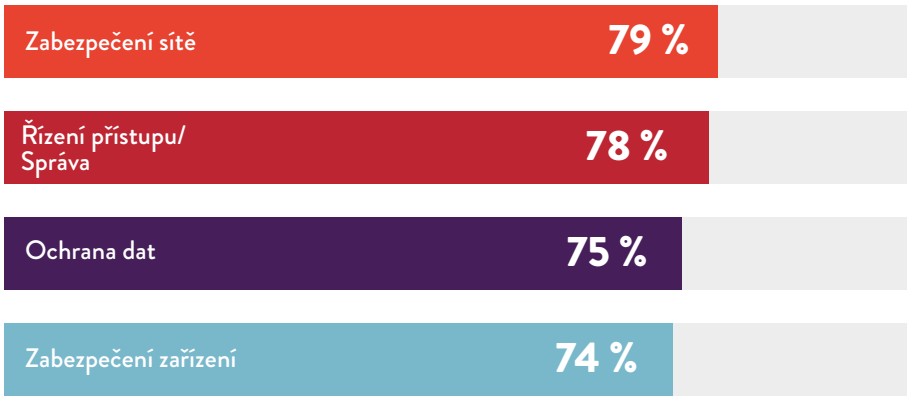
Tato řešení jsou však méně často implementována u tiskáren. Zatímco 83 % respondentů využívá zabezpečení sítě u počítačů/notebooků a 55 % u mobilních zařízení, jen 41 % jej používá u tiskáren.[1]

A tento rozdíl je pak ještě větší u zabezpečení koncových zařízení:



Navíc pouze necelá třetina (28 %) respondentů chrání své tiskárny pomocí bezpečnostních certifikátů, zatímco u osobních počítačů to je 79 % a u mobilních zařízení 54 %.[1]

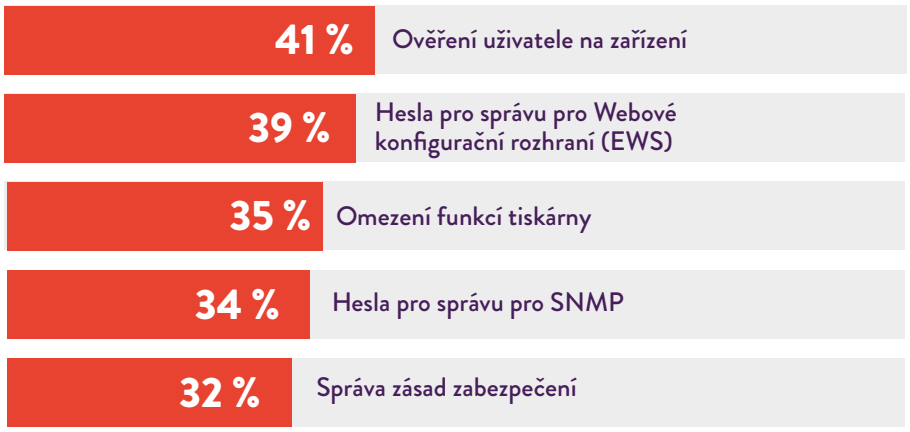
HLAVNÍ BEZPEČNOSTNÍ POSTUPY PRO KONCOVÁ ZAŘÍZENÍ



Z ochranných bezpečnostních opatření používaných u běžných koncových zařízení byla u tiskáren nejčastěji použita zabezpečení dokumentů, zabezpečení sítě a řízení přístupu, ale méně než polovina respondentů uvedla, že jejich organizace některé z nich u svých tiskáren používá.[1]

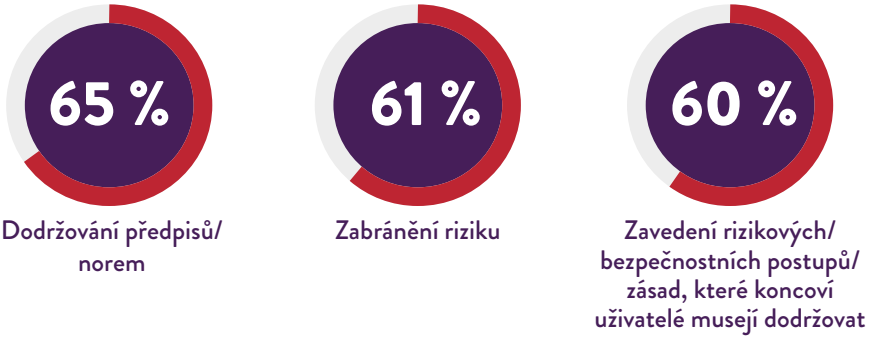
Některé společnosti používají bezpečnostní postupy pro konkrétní tiskárny, ale i v tomto případě jsou velmi nesourodé. Jen něco málo přes 40 % organizací ověřuje uživatele a méně než 40 % používá hesla správce pro webové konfigurační rozhraní.[1] Pro zajištění silné ochrany by každá organizace měla používat kombinaci všech těchto prvků, a ještě mnohem více.

HLAVNÍ BEZPEČNOSTNÍ POSTUPY PRO KONKRÉTNÍ TISKÁRNY:



Co se týče postupů pro dodržování předpisů a audity koncových zařízení, bezpečnostní opatření u tiskáren zůstávají pozadu téměř za všemi ostatními zařízeními. Téměř 90 % organizací má zásady zabezpečení informací, které však většinou nedosahují až k tiskárnám. Například zatímco 57 % respondentů uvedlo, že na svých počítačích používá ochranu proti škodlivému softwaru, pouze 17 % z nich ji používá také u svých tiskáren.[1]

TÉMĚŘ 9 Z 10 PROFESIONÁLŮ V OBORU IT UVÁDÍ, ŽE JEJICH ORGANIZACE ZAVEDLA ZÁSADY ZABEZPEČENÍ INFORMACÍ, A TO Z NÁSLEDUJÍCÍCH DŮVODŮ:



Je zřejmé, že organizace neberou zabezpečení tiskáren dostatečně vážně – ale to by rozhodně měly.

„Spousta tiskáren stále používá výchozí hesla, nebo pro jistotu vůbec žádná hesla nemá, nebo se používá jedno heslo pro deset tiskáren," uvedl v červnu Michael Howard, hlavní bezpečnostní poradce společnosti HP, pro časopis Computerworld. „Tiskárna, která není chráněna heslem, je pro hackery zlatým dolem. Jedním z narušení zabezpečení, se kterým se často setkáváme, je útok s využitím prostředníka, při kterém dochází k přesměrování příchozích dokumentů dříve, než se dostanou k tiskárně. Mohou tak například vidět vše, co si tiskne generální ředitel."[2]

POTENCIÁLNÍ DOPAD ÚTOKŮ NA TISKÁRNY

Podle hlavního analytika elektronických hrozeb společnosti Bitdefender, Bogdana Botezata, představují tiskárny závažnou potenciální bezpečnostní díru. „V našich laboratořích provádíme spoustu měření pro hodnocení chyb zabezpečení. Router již není nejzranitelnějším zařízením na internetu. Tím je nyní tiskárna."[3]

Tato zranitelnost přitom může mít závažné následky pro celý podnik. Jediná nezabezpečená tiskárna může vystavit celou vaši síť propojených zařízení útoku tím, že hackerům umožní tajně sledovat vaše síťová zařízení, čímž ohrozí bezpečnost celé sítě.

1. Vyšší počet hovorů s technickým oddělením i čas potřebný na podporu

2. Nižší produktivita/ efektivita

3. Větší doba nečinnosti systému

4. Více času stráveného voláním na oddělení podpory

5. Důraznější prosazování zásad vztahujících se na koncové uživatele

Každý z nás ví, jaké dopady může mít narušení bezpečnosti. V průzkumu společnosti Spiceworks respondenti uvedli, že mezi pět hlavních dopadů narušení bezpečnosti patří:[1]

Narušení zabezpečení tiskárny však může být mnohem závažnější, zvláště pokud používáte multifunkční tiskárnu, která je schopna uchovávat tištěná

data v elektronické podobě. Tiskové úlohy uložené v mezipaměti tiskárny umožňují hackerům přístup k citlivým osobním nebo obchodním informacím.

Ještě více znepokojivé je však to, že prostřednictvím nezabezpečené tiskárny mohou hackeři získat přístup do širší firemní sítě, kde mohou krást různé údaje, jako jsou čísla sociálního zabezpečení, finanční informace, nebo interní poznámky a dokumenty. Takovéto odcizené údaje mohou ovlivnit nejen jednotlivé zaměstnance, ale mohou být také použity konkurencí, nebo mohou způsobit vážné poškození dobrého jména společnosti.

SNADNÉ ŘEŠENÍ: VESTAVĚNÉ FUNKCE ZABEZPEČENÍ

Je zřejmé, že společnosti musí řešit zabezpečení také u svých tiskáren. Některé z dnešních moderních podnikových tiskáren nabízejí snadno použitelná integrovaná zabezpečení, která vás ochrání proti případným hrozbám. Patří mezi ně následující:

- Automatické rozpoznávání útoku, ochrana a oprava
- Sledování využití s cílem zabránit neoprávněnému použití
- Jednoduché možnosti přihlášení, jako je PIN nebo identifikační karta
- Čtečka karet Proximity Card Reader, která umožňuje rychlé ověření uživatele a bezpečný tisk na tiskárně pomocí stávajících identifikačních karet.
- Bezpečný šifrovaný tisk citlivých dokumentů

Až budete zvažovat koupi nové tiskárny, ať už stolní nebo multifunkční, zjistěte si, jaká má integrovaná bezpečnostní ochranná opatření, a nezapomeňte je aktivovat. Díky takovýmto jednoduchým funkcím konkrétních tiskáren již nebudete přes vaše tiskárny dále zranitelní; koneckonců, s internetem věcí přichází spousta jiných přístupových bodů, kterých byste se měli obávat – **a vaše tiskárny nemusí být jedním z nich.**

HLEDÁTE ZABEZPEČENOU TISKÁRNU?
VÍCE INFORMACÍ ›

Zdroje:

[1] Průzkum společnosti Spiceworks, kterého se zúčastnilo 309 činitelů odpovědných za IT ze Severní Ameriky, oblasti EMEA a oblasti APAC, jménem společnosti HP, listopad 2016.

[2] „Printer Security: Is your company's data really safe?" (Zabezpečení tiskáren: Jsou vaše firemní údaje opravdu v bezpečí?) Computerworld, 1. června, 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" (Tiskárny jsou nyní nejméně bezpečnou věcí na internetu), The Register, 8. září, 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/