Bílá kniha technických informací

Dodržujte požadavky předpisů pro zabezpečení sítí a dat

Doporučení pro uplatňování kontrol zabezpečení všech tiskových zařízení

Obsah

Kliknutím zde ověříte nejnovější verzi tohoto dokumentu

Porušování předpisů může poškodit vaše podnikání

Kromě nákladných pokut a soudních řízení může v důsledku narušení zabezpečení dojít ke ztrátám v příjmech a poškození pověsti. Až budete připravovat svůj plán zabezpečení, pamatujte, že vaše síť je zabezpečená pouze tak, jako její nejslabší článek. Zobrazovací a tisková zařízení mají mnoho zranitelných míst, která se shodují se slabými místy osobních počítačů. Je proto nezbytné nasadit zařízení a řešení, která vám pomohou dodržovat předpisy a chránit vaše obchodní informace před bezpečnostními hrozbami.

Jaká jsou rizika?

Nedodržení zákonů a předpisů znamená pro globální organizace vysoké náklady v podobě pokut, ušlého zisku, poškození dobré pověsti a hromadných žalob.

Nechráněné nebo nedostatečně chráněné koncové body vytvářejí další příležitosti pro počítačovou kriminalitu. Organizace dotazované v průzkumu společnosti Ponemon zaznamenaly v roce 2016 v průměru dva útoky týdně, což představuje meziroční nárůst o 23 %. Průměrně tak v boji proti kybernetické kriminalitě přišly o 9,5 milionu USD.[1] A jen v uplynulém roce došlo celosvětově k úniku 4 miliard datových záznamů, což je o 400 % více než v předchozích dvou letech.[2]

Ačkoli mnoho IT oddělení důsledně uplatňuje bezpečnostní opatření na počítače a síť, bývají tisková zobrazovací zařízení často přehlížena. Tiskárny však mohou sloužit jako vstupní bod do vaší sítě a jejich zabezpečení je proto stejně důležité. 26 % všech závažných případů porušení ochrany dat oznámených manažery IT souviselo s jejich tiskárnami.[3]

Ve snaze rostoucí hrozbu omezit zavádějí vládní organizace po celém světě nové přísné bezpečnostní předpisy, které vyžadují, aby podniky údaje svých zákazníků lépe chránily. Jedním takovým klíčovým opatřením, které vstoupí v platnost v roce 2018, je Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR) Evropské unie. GDPR zvyšuje požadavky kladené na ochranu dat v podnicích. Proto doporučujeme ujistit se, že jsou zabezpečená všechna zařízení ve vaší síti, od počítačů přes tiskárny až po mobilní zařízení. Nové nařízení se netýká jen zemí EU, musí je dodržovat i globální společnosti, které shromažďují a používají údaje o rezidentech EU. Organizace budou muset sledovat a posuzovat každé zařízení, aby mohly odhalit a ohlásit narušení bezpečnosti do 72 hodin od zjištění. Pokud při auditu vyjde najevo, že narušení bezpečnosti nebylo sledováno nebo ohlášeno, hrozí podnikům pokuty ve výši až 20 milionů EUR nebo 4 % ročního obratu.

Zdokonalte dodržování předpisů pomocí běžných kontrol zabezpečení

Držet krok s předpisy a nařízeními v odvětví a hlídat jejich dodržování je náročný úkol. Naštěstí Centrum pro internetovou bezpečnost (CIS) vytvořilo sadu běžných kontrol zabezpečení, aby zjednodušilo doporučení pro kybernetickou bezpečnost. Kritické kontroly zabezpečení CIS zahrnují 20 konkrétních opatření, která mohou pomoci blokovat kybernetické útoky. (Podrobnosti naleznete na https://www.cisecurity.org/critical-controls.cfm.) Kontroly jsou v souladu s nařízeními v mnoha dalších odvětvích, např. PCI-DSS, ISO 27001, doporučení US CERT, HIPAA, FFIEC a NIST. Cílem těchto kontrol není tyto jiné systémy nahradit, nicméně podniky je hojně využívají souběžně s jinými systémy.

Kritické kontroly zabezpečení CIS upřednostňují nižší počet opatření s vysokou účinností. Zaměřují se na nejběžnější vzorce útoků uváděné ve významných zprávách o útocích. Na jejich sestavení se podílela široká skupina odborníků z odvětví – včetně několika špičkových organizací zabývajících se forenzní vědou a reakcemi na incidenty. Kontroly jsou navíc průběžně aktualizovány na základě vyvíjejících se hrozeb a útoků.

Kritické kontroly zabezpečení CIS vám pomůžou sestavit váš plán bezpečnostních opatření a dodržovat požadavky právních nařízení. Bílá kniha uvádí navrhovaná opatření pro všech 20 kontrol s cílem pomoci vám zabezpečit vaše tisková zařízení, data a dokumenty v rámci vašeho širšího plánu zabezpečení. Kontroly 4, 6, 8, 12, 13 a 15 konkrétně řeší ochranu údajů a monitorování spojené s novými požadavky GDPR.

Kritické kontroly zabezpečení (CSC) a navrhovaná opatření

CSC 1: Soupis oprávněných a neoprávněných zařízení

Kontrola – spravujte aktivně (sepište, sledujte a opravte) všechna hardwarová zařízení v síti tak, aby do sítě měla přístup pouze oprávněná zařízení a zároveň se odhalila neoprávněná a nespravovaná zařízení a zabránilo se jim v přístupu.

Doporučení – ujistěte se, že jsou zahrnuta všechna tisková zařízení v síti a že jsou aktivně spravována, co se týče dodržování předpisů a vašich zásad zabezpečení. Efektivní nástroj pro správu zabezpečení tisku dokáže objevit a zviditelnit všechna síťová zařízení a zařízení připojená k PC.

CSC 2: Soupis oprávněného a neoprávněného softwaru

Kontrola – spravujte aktivně (sepište, sledujte a opravte) veškerý software v síti tak, aby bylo možné instalovat a spouštět pouze oprávněný software a zároveň se odhalil neoprávněný a nespravovaný software a zabránilo se jeho instalaci nebo spuštění.

Doporučení – ujistěte se, že veškerý firmware a řešení nahrané do tiskových a zobrazovacích zařízení jsou aktuální, podepsané a ověřené jako pravé. Vybírejte si tisková zařízení s integrovanou ochranou BIOSu a firmwarem, povolující nahrání pouze originálního kódu. Proaktivní aktualizace firmwaru lze provádět pro všechny tiskárny najednou pomocí řešení pro správu všech tiskáren. Software (uložený na serveru nebo u klienta) by měl být podepsaný a ověřený jako pravý.

CSC 3: Bezpečné konfigurace hardwaru a softwaru v mobilních zařízeních, laptopech, pracovních stanicích a serverech

Kontrola – stanovte, zaveďte a aktivně spravujte (sledujte, zaznamenávejte a opravujte) bezpečnostní konfiguraci laptopů, serverů a pracovních stanic pomocí přísné správy konfigurace a procesu řízení změn, abyste zabránili útočníkům ve zneužití zranitelných služeb a nastavení.

Doporučení – tiskárny by měly být stejně jako ostatní koncové body sítě bezpečně konfigurovány. Měli byste připravit a nasadit zásady zabezpečení platné pro všechna tisková zařízení a jakékoli odchylky od těchto zásad aktivně napravovat. Kontrolní seznamy zabezpečení (např. NIST) nebo poradenské služby v oblasti zabezpečení vám mohou pomoci navrhnout a nasadit komplexní zásady zabezpečení tisku. Efektivní nástroj pro správu zabezpečení tisku dokáže zásady automaticky vytvořit, nasadit a vyhodnocovat a opravovat nastavení zařízení napříč všemi tiskárnami. Multifunkční tiskárny podnikové třídy mají více než 250 bezpečnostních nastavení, zautomatizování tohoto procesu proto může výrazně ušetřit čas.

CSC 4: Průběžná kontrola zranitelnosti a její odstranění

Kontrola – průběžně získávejte a vyhodnocujte nové informace a na jejich základě přijímejte opatření s cílem identifikovat a odstranit zranitelná místa a minimalizovat tak příležitost pro útočníky.

Doporučení – řešení pro správu bezpečnostních informací a událostí (SIEM), např. ArcSight, Splunk nebo SIEMonster, dokážou monitorovat aktivity ve vaší síti v reálném čase a upozorňovat správce na výskyty incidentů. Monitorování tiskových zařízení je stejně důležité jako monitorování PC – ujistěte se, že vaše tiskárny odesílají do vašeho nástroje SIEM zprávy syslog o událostech.

Vybírejte si tisková zařízení s funkcemi, které umí odhalit útoky v reálném čase a zařízení automaticky obnovit, čímž maximalizují dobu jeho provozu a minimalizují IT zásahy.

K omezení zranitelnosti použijte nástroj pro správu zabezpečení všech tiskáren, který identifikuje nové tiskárny a automaticky pro ně, jakmile se zařízení připojí do sítě, uplatní vaše podnikové zásady pro nastavení zabezpečení. Naplánujte si pravidelná hodnocení/nápravy, aby všechny vaše tiskárny byly v souladu s těmito zásadami.

CSC 5: Řízené používání oprávnění správce

Kontrola – sledujte, řiďte, omezte a opravujte používání, přidělování a konfiguraci správcovských oprávnění v počítačích, sítích a aplikacích.

Doporučení – vybírejte si tisková zařízení a řešení s možností ověření uživatelů a funkcí řízeného přístupu podle pracovního zařazení, aby nastavení a konfiguraci zařízení mohli provádět pouze oprávnění pracovníci IT. Použijte software pro správu zabezpečení všech tiskáren, kterým zadáte správcovská hesla na všech tiskárnách.

CSC 6: Údržba, monitoring a analýzy kontrolních protokolů

Kontrola – shromažďujte, spravujte a analyzujte kontrolní protokoly událostí, které mohou pomoci odhalit a poznat útok a zařízení obnovit.

Doporučení – tisková zařízení by měla umět generovat syslog zprávy o incidentech, aby váš bezpečnostní tým mohl pravidelně nahlížet do kontrolních protokolů a na jejich základě zjišťovat a odstraňovat případné problémy. Vybírejte si zařízení, která dokážou posílat tyto zprávy do řešení pro správu zabezpečení všech tiskáren a nástrojů SIEM, protože umožňují monitoring v reálném čase a jsou schopná generovat zprávy pro audity nebo jiné požadavky právních předpisů.

CSC 7: Ochrana e-mailů a webových prohlížečů

Kontrola – minimalizujte prostor pro útok a příležitosti pro útočníky k falšování lidského chování během interakce s webovými prohlížeči a e-mailovými systémy.

Doporučení – multifunkční tiskárny bývají běžně připojené k internetu, takže mohou například odeslat naskenovaný obsah e-mailem. Zajistěte, aby byl naskenovaný text posílaný e-mailem šifrovaný a citlivá data tak byla chráněna. Nasaďte zařízení a řešení, která mohou ověřovat uživatele a řídit přístup ke zdrojům v rámci zařízení (např. webové servery nebo možnost e-mailu) podle pracovního zařazení uživatele. Vytvořte seznam „důvěryhodných stránek“ pro vaše multifunkční tiskárny a tento seznam důsledně spravujte tak, aby ze zařízení povoloval přístup pouze na důvěryhodné stránky. Integrujte různé metody ověřování (např. ověřování pomocí kódů PIN/PIC, LDAP nebo Kerberos) společně se službou Active Directory v zájmu efektivní správy a vyššího zabezpečení. Tisková zařízení, která jsou připojená k síti, by měla mít integrovanou antimalwarovou a antivirovou ochranu a v zájmu nejvyšší ochrany by se měl zároveň pravidelně aktualizovat jejich firmware.

CSC 8: Obrana před malwarem

Kontrola – blokujte instalaci, šíření a aktivaci škodlivého viru na různých bodech v podniku a zároveň optimalizujte využití automatizace ke spuštění bleskové aktualizace obrany, shromažďování dat a nápravného opatření.

Doporučení – vybírejte si tisková zařízení, která nahrají pouze ověřený a podepsaný kód a která mají integrované antimalwarové funkce, jež aktivně monitorují paměť zařízení a v případě útoku zařízení restartují. Efektivní nástroj pro správu zabezpečení tisku dokáže automaticky vyhodnotit a opravit nastavení zařízení napříč všemi tiskárnami. Měli byste se rovněž přesvědčit, že všechna tisková softwarová řešení jsou podepsaná a ověřená jako pravá.

CSC 9: Omezení a řízení síťových portů, protokolů a služeb

Kontrola – spravujte (sledujte, řiďte a opravujte) průběžné provozní využívání portů, protokolů a služeb u síťových zařízení, abyste minimalizovali zranitelná místa dostupná útočníkům.

Doporučení – nejsou-li již zakázané ve výchozím nastavení, zakažte nepoužívané porty a nezabezpečené protokoly (např. FTP nebo Telnet), jichž by útočníci mohli využít k přístupu do zařízení. Ušetřete čas IT a snižte riziko nasazením nástroje pro správu zabezpečení tisku, pomocí kterého zachováte nastavení všech zařízení v souladu s předpisy. Používejte správcovská hesla, ověřování a řízený přístup podle pracovního zařazení pro omezení přístupu k funkcím a nastavení zařízení.

CSC 10: Možnost obnovy dat

Kontrola – zálohujte náležitě důležité informace pomocí osvědčené metody pro jejich včasnou obnovu.

Doporučení – tato kontrola se v současné době netýká tiskáren.

CSC 11: Bezpečnostní konfigurace síťových zařízení, např. firewallů, routerů a přepínačů

Kontrola – stanovte, zaveďte a aktivně spravujte (sledujte, zaznamenávejte a opravujte) bezpečnostní konfiguraci zařízení síťové infrastruktury pomocí přísné správy konfigurace a procesu řízení změn, abyste zabránili útočníkům ve zneužití zranitelných služeb a nastavení.

Doporučení – tiskárny jsou umístěné v síti, proto by měly být bezpečně konfigurovány stejně jako ostatní koncové body sítě. Efektivní nástroj pro správu zabezpečení tisku dokáže automaticky nasadit, vyhodnotit a opravit nastavení zařízení napříč všemi tiskárnami a hlídat tak zabezpečení sítě – a zároveň šetřit čas IT.

CSC 12: Obrana hranic

Kontrola – odhalujte, omezujte a opravujte tok informací přenášených sítěmi s různými úrovněmi důvěryhodnosti se zaměřením na data narušující zabezpečení.

Doporučení – používejte šifrování na ochranu přenášených dat (tiskové nebo skenovací úlohy přenášené z nebo do tiskárny) i dat uložených na pevném disku zařízení. Vybírejte si tisková zařízení a řešení s možností ověření uživatelů a funkcí řízeného přístupu podle pracovního zařazení, aby např. posílání skenovaných úloh e-mailem nebo odesílání souborů na místa v cloudu mohli provádět pouze oprávnění uživatelé. Konfigurujte v zařízení důvěryhodné webové strany ze seznamu „důvěryhodných stránek“, abyste zamezili přístup na škodlivé webové stránky. Řešení pro bezpečný mobilní tisk usnadňují uživatelům tisk z jejich mobilních zařízení a zároveň chrání sít.

CSC 13: Ochrana dat

Kontrola – zabraňte úniku dat, zmírněte důsledky uniklých dat a zajistěte důvěrnost a integritu citlivých informací.

Doporučení – používejte šifrování na ochranu přenášených dat (tiskové nebo skenovací úlohy přenášené z nebo do tiskárny) i dat uložených na pevném disku zařízení. Nasaďte řešení tisku na vyžádání, kterým zabráníte, že citlivé dokumenty zůstanou volně ve výstupních zásobnících. Ujistěte se, že data uložená na pevných discích zařízení jsou bezpečně smazána, než budete pronajatá zařízení vracet nebo je na konci jejich životnosti recyklovat.

CSC 14: Řízený přístup na základě principu „potřebuji vědět“

Kontrola – sledujte, kontrolujte, omezujte, opravujte a zabezpečte přístup k důležitému majetku (např. informacím, zdrojům a systémům) podle formálního rozhodnutí, jaké osoby, počítače a aplikace potřebují a mají právo přistupovat k tomuto důležitému majetku na základě schválené klasifikace.

Doporučení – vybírejte si tisková zařízení a řešení s možností ověření uživatelů a funkcí řízeného přístupu podle pracovního zařazení uživatelů. Integrujte různé metody ověřování (např. ověřování pomocí kódů PIN/PIC, LDAP nebo Kerberos) společně se službou Active Directory v zájmu efektivní správy a vyššího zabezpečení. Řešení pull print zajistí, že se citlivé dokumenty nedostanou do špatných rukou.

CSC 15: Kontrola bezdrátového přístupu

Kontrola – sledujte, řiďte, omezujte a opravujte zabezpečení bezdrátových místních sítí (LANS), přístupových bodů a systémů bezdrátového klienta.

Doporučení – efektivní nástroj pro správu zabezpečení tisku automaticky nasadí, vyhodnotí a opraví nastavení zařízení – včetně bezdrátového nastavení – napříč všemi tiskárnami. Pomocí řešení pro řízený přístup omezíte přístup k funkcím zařízení, např. skenování do e-mailu, podle pracovního zařazení uživatele. Řešení pro bezpečný mobilní tisk usnadňují uživatelům tisk z jejich mobilních zařízení a zároveň chrání sít. Například zařízení, která podporují bezdrátový tisk technologií peer-to-peer, umožňují uživatelům mobilních zařízení tisknout přímo přes samostatný signál bezdrátového připojení tiskárny – bez potřeby firemní sítě nebo bezdrátové služby.

CSC 16: Monitorování a řízení účtů

Kontrola – spravujte aktivně životní cyklus účtů systémů a aplikací – jejich zakládání, využívání, nečinnost, rušení – abyste minimalizovali příležitosti k jejich zneužití ze strany útočníků.

Doporučení – vybírejte si tisková zařízení a řešení s možností ověření uživatelů a funkcí řízeného přístupu podle pracovního zařazení uživatele. Integrujte ověřování se službou Active Directory v zájmu centralizované správy a vyššího zabezpečení. Kontrolujte pravidelně uživatelské účty a ty zbytečné zakažte, a používání účtů monitorujte pomocí řešení pro sledování. Šifrujte uživatelská jména účtů a přihlašovací údaje pro ověřování, a to jak přenášené, tak i uložené v paměti zařízení. Bezpečnostní poradci vám pomůžou navrhnout komplexní plán zabezpečení tisku s cílem minimalizovat rizika – a v některých případech vám mohou pomoci i se správou zabezpečení, včetně monitorování a řízení účtů.

CSC 17: Posouzení bezpečnostních dovedností a zaplnění mezer vhodným školením

Kontrola – určete specifické znalosti, dovednosti a schopnosti potřebné na podporu obrany podniku; připravte a realizujte integrovaný plán posouzení, určení a odstranění mezer na základě zásad, organizačního plánování, školení a osvětových programů pro všechny pracovní pozice v organizaci.

Doporučení – poradci zabezpečení tisku vám pomůžou na základě svých odborných znalostí posoudit vaše bezpečnostní rizika, připravit komplexní zásady a plán zabezpečení a zavést doporučené procesy a technologie. Některé služby zabezpečení za vás mohou dokonce zajišťovat správu zabezpečení tisku a dodržování předpisů.

CSC 18: Zabezpečení aplikačního softwaru

Kontrola – spravujte bezpečný životní cyklus veškerého interně vyvinutého i zakoupeného softwaru, abyste omezili, odhalili a opravili slabá místa v zabezpečení.

Doporučení – držte se osvědčených postupů pro bezpečný vývoj u všech vyvíjených tiskových řešení. Vybírejte si softwarová řešení, která jsou podepsaná a ověřená jako pravá.

CSC 19: Reakce na incidenty a jejich správa

Kontrola – chraňte informace organizace a její pověst navržením a zavedením infrastruktury pro reakce na incidenty (např. plány, vymezení rolí, školení, komunikace a dohled nad správou).

Doporučení – přesvědčte se, že je vaše tiskové prostředí zahrnuto ve vašem plánu reakcí na incidenty.

CSC 20: Testy penetrace a cvičení týmu simulujícího napadení

Kontrola – otestujte celkovou pevnost obrany organizace (technologie, procesy a lidé) simulací cílů a akcí ze strany útočníků.

Doporučení – do testů penetrace zahrňte i své tiskové prostředí. Pravidelně posuzujte své tiskové prostředí a jeho zranitelná místa a aktualizujte svůj plán zabezpečení s důrazem na tato slabá místa.

Udělejte další krok

Zavedením doporučení v této bílé knize upevníte zabezpečení tisku a pomůžete zajistit dodržování právních nařízení. Potřebujete pomoc? Poradenské služby zabezpečení a správy tisku vám pomůžou připravit plán a nasadit procesy a technologie, které zdokonalí zabezpečení vašich tiskových zařízení, dat a dokumentů.

Příloha A: Funkce, řešení a služby zabezpečení tisku HP

Funkce zabezpečení integrované do zařízení HP spolu se špičkovými softwarovými řešeními a službami vám mohou pomoci zajistit dodržování regulačních a zákonných požadavků a chránit vaše obchodní informace před bezpečnostními hrozbami.

Funkce zabezpečení integrované do tiskáren a multifunkčních zařízení HP Enterprise chrání zařízení před malwarem, automaticky detekují útok a zařízení následně obnoví. Pouze funkce zabezpečení tisku HP nabízejí detekci v reálném čase, automatické monitorování a ověřování integrovaného softwaru, díky čemuž dokážou zastavit hrozby hned v samém počátku.[4] (Přínosy splňují CSC 2, 4, 6 a 8.) hp.com/go/PrintersThatProtect

Řešení HP Access Control nabízí kromě sledování a počítání úloh různé možnosti ověřování a řízeného přístupu podle pracovního zařazení s cílem omezit potenciální narušení zabezpečení. (Přínosy splňují CSC 5, 7, 10, 12, 13, 14, 15 a 16.) hp.com/go/hpac

Řešení šifrování a **HP JetAdvantage pro pracovní postupy** chrání data uložená v zařízení HP Enterprise i data přenášená do nebo z tiskových zařízení nebo cloudu. (Přínosy splňují CSC 12 a 13.) hp.com/go/upd, hp.com/go/documentmanagement

Řešení HP pull printing chrání důvěrné dokumenty ukládáním tiskových úloh na chráněném serveru, cloudu nebo ve vašem PC. Uživatelé jsou ověřováni na jimi zvolených tiskárnách, na kterých mohou aktivovat své tiskové úlohy. (Přínosy splňují CSC 10, 13 a 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

Nástroj HP JetAdvantage Connect poskytuje uživatelům mobilních telefonů snadný přístup k tisku z chytrých telefonů a tabletů a zároveň zajišťuje požadovanou kontrolu zabezpečení a správy. (Přínosy splňují CSC 12 a 15.) hp.com/go/JetAdvantageConnect

Údaje o událostech tiskárny HP lze odesílat do nástrojů SIEM, např. ArcSight, Splunk nebo SIEMonster. Váš bezpečnostní tým může snadno nahlížet na koncové body tiskáren v rámci širšího ekosystému IT a provádět nápravná opatření. (Přínosy splňují CSC 4 a 6.)

HP JetAdvantage Security Manager je nástroj pro dodržování předpisů o zabezpečení tisku, který jako jediný v odvětví uplatňuje firemní zásady.[5] Pomůže vám zavést zásady zabezpečení pro všechny tiskárny, automaticky opraví nastavení zařízení a instaluje a obnovuje jedinečné certifikáty, a zároveň generuje zprávy potvrzující dodržování předpisů. Funkce zabezpečení Instant-On automaticky konfiguruje nová zařízení, která byla přidána do sítě nebo restartována. (Přínosy splňují CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 a 15.) hp.com/go/securitymanager

Služba **HP Secure Managed Print Services** nabízí nejsilnější a nejkomplexnější zabezpečení tisku v odvětví.[6] Zabezpečení tisku může být složité. Nechte společnost HP, aby vaše zabezpečení tisku, počínaje posílením zařízení a konče pokročilými bezpečnostními řešeními se zaměřením na lidi, procesy a dodržovaní požadavků, spravovala za vás. (Přínosy splňují CSC 2, 3, 12, 16, 17, 18 a 19.) hp.com/go/SecureMPS

Služby HP Print Security Professional Services zprostředkovávají bezpečnostní odborníky, kteří posoudí vaše tiskové prostředí, proaktivně zavedou zásady zabezpečení a zajistí, aby váš plán zabezpečení byl vždy aktuální. Zajišťovat pro vás můžeme i dodržování předpisů pro zabezpečení tisku. (Přínosy splňují CSC 2, 3, 12, 16, 17 a 19.) hp.com/go/SecureMPS

Poznámky

[1] Studie společnosti Ponemon „2016 Cost of Cyber Crime Study & the Risk of Business Innovation“ z roku 2016, podpořená společností HPE.

[2] Zpráva „The 2016 Year End Data Breach QuickView“ společnosti RiskBased Security, leden 2017.

[3] 26,2 % respondentů zaznamenalo závažné porušení zabezpečení IT, jež si vyžádalo nápravné opatření s tím, že více než 26,1 % těchto incidentů souviselo s tiskem. IDC, „Průzkum zabezpečení IT a tisku, 2015“ IDC #US40612015, září 2015.

[4] Týká se zařízení HP podnikové třídy představených na začátku roku 2015 a vychází z hodnocení integrovaných bezpečnostních funkcí představených v roce 2016 u konkurenčních tiskáren ve stejné třídě, zveřejněného společností HP. Pouze společnost HP nabízí kombinaci bezpečnostních funkcí pro kontrolu integrity až na úroveň BIOSu spolu se samoregeneračními funkcemi. Aktivace bezpečnostních funkcí může vyžadovat aktualizaci servisního balíčku FutureSmart. Seznam tiskáren naleznete na: hp.com/go/PrintersThatProtect. Další informace zjistíte na hp.com/go/printersecurityclaims.

[5] Řešení HP JetAdvantage Security Manager je nutné zakoupit samostatně. Více se dozvíte na hp.com/go/securitymanager. Prohlášení o konkurenceschopnosti na základě průzkumu konkurenčních nabídek, provedeného interně společností HP (Srovnání zabezpečení zařízení, leden 2015) a zprávy o řešení HP JetAdvantage Security Manager 2.1, zveřejněné laboratoří Buyers Laboratory LLC, únor 2015.

[6] Včetně funkcí zabezpečení zařízení, dat a dokumentů od předních poskytovatelů řízených tiskových služeb. Na základě porovnání veřejně dostupných informací o službách zabezpečení, softwaru pro zabezpečení a správu a funkcích zabezpečení integrovaných v zařízeních u konkurenčních tiskáren stejné třídy, provedeného společností HP v letech 2015–2016. Další informace zjistíte na hp.com/go/MPSsecurityclaims nebo hp.com/go/mps.

Přihlaste se k odběru aktualizací
hp.com/go/getupdated

Sdílet dokument s kolegy

4AA6-8821CSE, červen 2017, rev. 1