



Miért van szüksége minden vállalkozásnak megfelelő nyomtatási szolgáltatásokkal kapcsolatos stratégiára

Minden vállalkozásnak szüksége van egy biztonsággal és produktivitással foglalkozó nyomtatási szolgáltatásokkal kapcsolatos stratégiára. A HP nyomtatási biztonsággal foglalkozó szakértői, Jason O'Keefe és Michael Howard elmagyarázzák, hogy miért.



Tudjon meg többet



„A legtöbb cég nem gondolja, hogy biztonságra van szükség a nyomtatási infrastruktúrával kapcsolatban, ezért a nyomtatás a biztonsági prioritási lista alján szerepel”

Jason O'Keefe,
HP nyomtatásbiztonsági tanácsadó

A hálózathoz kapcsolt nyomtatók sokkal kevésbé biztonságosak, mint amennyire a legtöbb vállalkozás gondolja. Mivel egyre több a biztonsági fenyegetés – és ezek egyre katasztrófálisabbak – a vállalkozásoknak méretüktől függetlenül nyomtatási szolgáltatásokra van szükségük, hogy megvédjék magukat, és lecsökkentsék a kockázatokat. A vállalkozások számára létrehozott kimagasló nyomtatási stratégia középpontjában a legtöbb esetben kulcsfontosságú, hogy felügyelt nyomtatási szolgáltatást biztosító partnerrel dolgozzanak együtt, amely képes azonosítani és elhárítani a biztonsági hiányosságokat, valamint közben tudja tartani a problémákat (gondoljon a felszerelések karbantartására), így a nyomtatás soha nem kerül a produktivitás útjába.

A nyomtatási biztonság hiánya

Egy több mint 2000 globális IT szakembert felölelő kutatás szerint – amelyet a Ponemon Institute végzett el – a válaszadók 60%-a ismeri el, hogy egy hálózathoz kapcsolt nyomtató miatt történő adatvesztésre vagy adatlopásra már sor kerülhetett, valamint a legtöbb válaszadó úgy jósolja, hogy a következő 12 hónapban adatvesztésre vagy adatlopásra kerül sor a nem megfelelő biztonsággal rendelkező hálózathoz kapcsolt nyomtatók miatt.

Azonban a válaszadók csupán 34%-a közölte azt, hogy a vállalatuk rendelkezik olyan folyamattal, amely képes korlátozni a hozzáférést a nagy kockázatot jelentő nyomtatókhoz, beleértve a kinyomtatott dokumentumokat. Ezek a kártevő biztonsági rések leginkább a kis- és közepes méretű vállalkozásokat teszik ki olyan támadásoknak, amelyek a legjobb esetben csak drágák, a legrosszabb esetben azonban végzetesek is lehetnek.

Jason O'Keefe, a HP nyomtatási biztonsággal foglalkozó szakértője szerint a legtöbb vállalkozás alábecsüli, hogy mennyire sebezhető a nyomtatási infrastruktúráján keresztül. „A legtöbb cég nem gondolja, hogy biztonságra van szükség a nyomtatási infrastruktúrával kapcsolatban, ezért a nyomtatás a biztonsági prioritási lista alján szerepel,” – mondta. „Egy olyan keretrendszert mutatunk be, amely közel 200 irányítási ponttal rendelkezik, így értékelhetjük a gyenge pontokat a teljes nyomtatási infrastruktúrán belül. Hirtelen a szemek tágra nyílnak, és a hangnem teljesen megváltozik. A kezdeti szkeptikus hozzáállás hitetlenséggé és sokká alakul, amely megfelelő légkört teremt egy őszinte és élénk beszélgetéshez.”

Egy jó nyomtatási szolgáltatásokkal kapcsolatos stratégia a gyenge pontok értékelésével kezdődik. Michael Howard, a HP fő biztonsági tanácsadója szerint a legtöbb nyomtatási biztonsággal kapcsolatos gyenge pont négy tényezőt alapszik: előregedő technológia; a biztonsági ellenőrzések megfelelő bevezetésének hiánya; heterogén beszállító-környezetek; és nem felügyelt nyomtatási környezetek.

Tudta, hogy egy átlagos vállalat kb. hat felhasználóval rendelkezik nyomtatóként? Míg a számítógépek és laptopok sok esetben lezárásra kerülnek a használatok között, a nyomtatók nem rendelkeznek ezekkel a protokollokkal – így a gyenge pontok hatással vannak mind a hat felhasználóra. „Számos biztonsági csapat nem tudott beszámolni arról, hogy hány nyomtatókészülékkel rendelkezik a környezetükben. Lehet akár 5000 készülék is – mind védtelen,” – mondta Howard. „Amikor arra gondolunk, hogy mennyire mindent átható a nyomtatás a legtöbb vállalat esetében, a védelmi biztonság hiánya megrázó és félelmetes.”

Miért van szüksége minden vállalkozásnak megfelelő nyomtatási szolgáltatásokkal kapcsolatos stratégiára

A nyomtatási szolgáltatásokkal kapcsolatos stratégiák fontossága

Egy okos nyomtatási stratégia lezárja a nyomtatásokat (akár a számítógépek esetében), korlátozza a rendszergazdai jogköröket, felhasználónévvel és jelszóval kapcsolatos irányelveket vezet be, és monitorozást tesz lehetővé. Ez kulcsfontosságú az átláthatóság, követhetőség és elszámoltathatóság létrehozásában.

„Az átláthatóság létfontosságú,” – mondta O’Keefe. „Ki szeretném emelni, hogy milyen nagy hatással van az együttműködés a hatékony nyomtatási biztonságra. Annak érdekében, hogy a robusztus biztonsághoz szükséges kimagasló tudásra szert tegyenek, a vállalatoknak le kell dönteniük a nyomtatási rendszergazdák, biztonsági szakértők és belső auditszemélyzet közötti falakat. Ezeknek a csoportoknak hajlandóknak kell lenniük az együttműködésre, hogy megbiztosítsák a hálózat egy kulcsfontosságú pontját, amelyet éveken át figyelmen kívül hagytak.”

Továbbá, a vállalatoknak javítaniuk kell a nyomtatási gyenge pontokat a következők segítségével:

- A firmware folyamatos frissítése
- Adminisztráció csökkentése a nyomtatási infrastruktúrán
- Nyomtatási adatbázisok frissítése expressz verzióról vállalati verzióra
- Folyamatok és dokumentáció bevezetése a biztonság következetessége és mérhetősége érdekében
- Biztonsági tudatossági képzések biztosítása a nyomtatási rendszergazdáknak

„A nyomtatási biztonság, akár a vállalati biztonság, egy folyamat” – mondta Howard. „Ennek eredményeképp kimagasló fontosságú a folyamatos javítások eszközölése széles körűbb értékelések és szakértői tanácsok segítségével.”

A széles körű, folyamatos értékelés kapcsolódik a felügyelet fontosságához. A nyomtatás esetében a felügyelet a felhasználói fiókok kezelését (ki éri el a nyomtatási infrastruktúrát), a megfelelést a vállalati irányelveknek, a kockázatkezelést, a biztonsági dokumentációt és az események részletes rögzítését jelenti.

Felügyelni vagy nem felügyelni – ez itt a kérdés

Egy komoly stratégiához elemek széles palettája szükséges. A legtöbb vállalkozás, főleg kis- és közepes méretű vállalkozások esetén nem lehet házon belül megoldani egy ilyen típusú stratégia kidolgozását és végrehajtását. Inkább abba fektetik idejüket és energiájukat, hogy a vállalkozást fenntartsák. Minőségi megoldás az olyan felügyelt nyomtatási szolgáltatást nyújtókkal való együttműködés, akik kézben tartják az apró-cseprő részleteket és a megfelelő működéshez szükséges biztonsági szintet nyújtanak.

Egy okos nyomtatási stratégia létrehozásának első lépése a kérdések feltevése. Először is, mely nyomtatók a megfelelők a vállalatunknak? Tintapatronos vagy lézeres nyomtatókat használunk? Milyen nyomtatási funkciókra van szükségünk? Ezen kérdések megválaszolásához szükséges a megbízhatóság, ár és teljesítmény megfelelő aránya.

Ezt követően a vállalkozásnak el kell gondolkodni a biztonságon, karbantartáson és támogatáson. Házon belül kezeljük a nyomtatóinkat, vagy keressünk fel egy szolgáltatót? Ehhez a kérdéshez kapcsolódva további kérdések merülnek fel, például: Az IT-csapatunk megfelelő eszközökkel van ellátva, hogy orvosolja a nyomtatók problémáit? Többe kerül házon belül megoldani a nyomtatási szolgáltatásokat hosszú távon? Kisvállalkozások esetében a válasz gyakran igen.

A vállalkozásoknak, amelyek felügyelt nyomtatási szolgáltatásokat választanak, el kell gondolkodniuk azon, hogy mikor írjanak alá szerződést, és melyik szolgáltatóval dolgozzanak. Ehhez például a következő kérdések megválaszolására van szükség: Milyen szolgáltatásokra van szükségünk? Mi kerül a szolgáltatás szint-szerződésbe? Mennyibe fog ez kerülni? Milyen ütemben várható a nyomtatói hálózatunk növekedése? A növekedés során hogyan kell változnia a nyomtatási stratégiának?

A nem biztosított hálózathoz kapcsolt nyomtatók veszélye egyértelmű, és a vállalatoknak, mérettől függetlenül, a biztonság és hatékonyság megközelítése során figyelembe kell venniük a nyomtatási szolgáltatásokat. Szerencsére vannak olyan megoldásokat nyújtó szolgáltatók, amelyek képesek megbirkózni a piszkos munkával.

„A nyomtatási biztonság, akár a vállalati biztonság, egy folyamat”

Michael Howard,
HP vezető biztonsági tanácsadó

Tudjon meg többet
hp.com

© Copyright 2017 HP Development Company, L.P. Az itt szereplő információk külön bejelentés nélkül megváltozhatnak. A HP termékeire és szolgáltatásaira vonatkozó jóállás és szavatosságot kizárólag az adott terméket vagy szolgáltatást kísérő kifejezett jóállási nyilatkozat tartalmazza. Az itt szereplő információk semmilyen tekintetben nem minősülnek kiegészítő jóállásnak. A HP nem tehető felelőssé a jelen dokumentumban esetleg előforduló technikai vagy szerkesztési hibákért, illetve hiányosságokért.

4AA7-1720HUE, 2017. november

