De ce fiecare firmă are nevoie de o strategie de servicii de imprimare inteligentă

Toate firmele au nevoie de câte o strategie pentru serviciile de imprimare, pentru securitate şi productivitate. Consultanţii Jason O'Keefe şi Michael Howard, specializaţi în servicii HP de securitate a imprimării, explică de ce.

Aflați mai multe

"Majoritatea companiilor nu consideră că au nevoie de securitate pentru infrastructurile lor de imprimare, în consecință, imprimarea se regăsește spre finalul listei de priorități în securizare"

Jason O'Keefe, Consultant în servicii HP de securitate

Imprimantele conectate la reţea sunt mult mai vulnerabile decât ar crede majoritatea organizaţiilor. În faţa ameninţărilor de securitate care se înmulţesc şi devin absolut dezastruoase, firmele de toate dimensiunile au nevoie de strategii pentru serviciile de imprimare, pentru a-şi proteja organizaţiile şi a minimiza riscurile. La baza dezvoltării unei strategii puternice pentru multe firme stă colaborarea cu un furnizor de servicii de imprimare gestionată, care poate să identifice şi să fortifice punctele cu vulnerabile din punct de vedere al securităţii, precum şi să rezolve problemele (gândiţi-vă: întreţinerea echipamentelor), aşadar imprimarea nu stă niciodată în calea productivităţii.

Cum se tratează problema insecurităţii imprimantelor

Potrivit unui studiu realizat în rândul a peste 2.000 de specialişti în securitatea IT la nivel global – condus de Institutul Ponemon – 60% dintre respondenţi au confirmat că a survenit o breşă în securitatea datelor, care a implicat o imprimantă conectată la reţea şi majoritatea respondenţilor prevăd o breşă în securitatea datelor în următoarele 12 luni, cauzată de imprimantele nesigure, conectate la reţea.

Dar numai 34% dintre respondenţi au spus că organizaţia lor are un proces de restricţionare a accesului la imprimantele cu risc ridicat, inclusiv la documentele imprimate. Lipsa evidentă a măsurilor de securitate poate lăsa în special, firmele mici şi mijlocii, expuse la atacuri, care sunt costisitoare în cel mai bun caz şi dăunătoare în cel mai rău caz.

Jason O'Keefe, consultant în servicii HP de securitate a imprimării, a spus că majoritatea organizaţiilor nu apreciază corect cât de vulnerabile sunt prin intermediul infrastructurilor de imprimare „Majoritatea companiilor nu se gândesc că au nevoie de securitate pentru infrastructurile lor de imprimare, astfel încât imprimarea se află pe o treaptă inferioară în lista lor de priorităţi pentru securitate", a declarat el. „Noi prezentăm cadrul nostru de lucru, care are până la 200 de elemente de control pe care le evaluăm din punct de vedere al vulnerabilităţii la nivelul infrastructurii de imprimare. Dintr-o dată, în ochi se citeşte interesul şi tonul se schimbă complet. Scepticismul iniţial devine neîncredere şi şoc, deschizând apoi calea pentru o discuţie foarte sinceră şi vie."

O bună strategie a serviciilor de imprimare trebuie să înceapă cu o evaluare a vulnerabilităţilor. După cum spune Michael Howard, consultantul şef de securitate HP, majoritatea vulnerabilităţilor de securitate legate pe imprimare se reduc la patru factori: tehnologie învechită; implementarea necorespunzătoare a controalelor de securitate; medii eterogene de furnizori; şi medii de imprimare negestionate.

Ştiaţi că o organizaţie medie are aproximativ şase utilizatori per imprimantă? În timp ce computerele şi laptopurile se pot bloca între utilizări, imprimantele nu urmează aceleaşi protocoale – lăsând câte o vulnerabilitate pentru fiecare dintre cei şase utilizatori. „Multe echipe de securitate nu ar fi în stare să vă spună câte dispozitive de imprimare există în mediile lor. Ar putea fi 5.000 de dispozitive – toate deschise", a spus Howard. „Când ne gândim cât de generalizată este imprimarea în majoritatea organizaţiilor, lipsa unei securităţi proactive este şocantă şi înspăimântătoare."

De ce fiecare firmă are nevoie de o strategie de servicii de imprimare inteligentă

De ce sunt importante strategiile pentru serviciile de imprimare

O strategie de imprimare inteligentă blochează imprimantele (ca în cazul computerelor), limitează privilegiile administrative, implementează recomandări pentru nume de utilizatori şi parole şi furnizează activităţi de monitorizare. Aceste măsuri sunt esenţiale pentru a crea vizibilitate, trasabilitate şi responsabilitate.

„Vizibilitatea este esenţială", a spus O'Keefe. „De asemenea, doresc să evidenţiez faptul că un factor cheie pentru securitatea efectivă a imprimării este colaborarea. Pentru a obţine informaţiile bogate necesare unei securităţi puternice, companiile trebuie să elimine barierele dintre administratorii de imprimare, specialiştii în securitate şi personalul de audit intern. Aceste grupuri trebuie să fie dispuse să colaboreze pentru a asigura o componentă cheie a reţelei, care a fost omisă ani de zile."

În plus, organizaţiile îşi pot remedia vulnerabilităţile legate de imprimare prin:

- Actualizarea constantă a firmware-ului
- Reducerea administrării la nivelul infrastructurii de imprimare
- Actualizarea bazelor de date de imprimare de la ediţiile predefinite la ediţiile pentru întreprinderi
- Implementarea proceselor şi a documentaţiei pentru a menţine securitatea consistentă şi măsurabilă
- Instruirea administratorilor de imprimare referitor la problemele de securitate.

„Securitatea imprimării, ca şi securitatea companiei, este un proces continuu", a spus Howard. „Drept urmare, este esenţial să se urmărească îmbunătăţirea continuă, prin evaluări mai aprofundate şi consultanţă de specialitate."

Evaluările aprofundate şi constante sunt legate de importanţa dată actului de administrare. Pentru imprimare, administrarea trebuie să includă managementul conturilor de utilizatori (cine accesează infrastructura de imprimare), conformitatea cu politicile de întreprindere, managementul riscurilor, documentaţia de securitate şi arhivarea evenimentelor.

Gestionat sau negestionat – aceasta este întrebarea

O strategie solidă necesită o gamă largă de componente. Pentru majoritatea firmelor, în special la firmele mici şi mijlocii, construirea şi executarea acestui tip de strategie la faţa locului este improbabilă. Mai degrabă, acestea îşi dedică timpul şi energia pentru a gestiona efectiv afacerea. O soluţie de calitate este colaborarea cu furnizorii de servicii de imprimare gestionată, care pot să manevreze toate detaliile importante şi să asigure nivelul de securitate pe care firmele îl pot gestiona în mod cursiv.

Primul pas în crearea unei strategii de imprimare inteligente este să se pună întrebări. Pentru început, ce imprimante sunt potrivite pentru organizaţia noastră? Trebuie să utilizăm imprimante cu cerneală sau cu laser? De ce caracteristici de imprimare avem nevoie? Răspunsurile la aceste întrebări trebuie să asigure un echilibru între fiabilitate, cost şi performanţă.

Apoi, firmele trebuie să se gândească la securitate, întreţinere şi asistenţă. Vom gestiona imprimantele cu resurse proprii sau vom colabora cu un furnizor? În contextul acestei întrebări, există şi altele, precum: Este echipa noastră IT echipată pentru a gestiona problemele imprimantelor? Va costa mai mult gestionarea serviciilor de imprimare la sediu pe termen lung? Pentru firmele mai mici, răspunsul este deseori afirmativ.

Firmele care aleg un serviciu de imprimare gestionată trebuie să se gândească la condiţiile încheierii unui contract, precum şi la ce furnizor vor alege. Acest lucru presupune adresarea unor întrebări precum: Care sunt serviciile de care avem nevoie? Ce prevede acordul la nivel de serviciu? Care va fi costul? Cât de repede ne aşteptăm să crească reţeaua noastră de imprimante? Pe măsură ce ne dezvoltăm, cum trebuie modificată strategia de imprimare?

Pericolele legate de imprimantele nesigure, conectate la reţea sunt clare, iar firmele de toate dimensiunile trebuie să includă serviciile de imprimare în planul lor general de securitate şi productivitate. Din fericire, există furnizori de soluţii care se ocupă de activităţile aparent complexe.

> "Securitatea imprimării, ca şi securitatea companiei, este un proces continuu,"
>
> Michael Howard, Consultantul şef de securitate HP

Aflați mai multe
hp.com

4AA7-1720ROE, Noiembrie 2017