CARTE ALBĂ

UȘI DESCUIATE

CERCETĂRILE ARATĂ CĂ IMPRIMANTELE RĂMÂN VULNERABILE LA ATACURILE CIBERNETICE

În timp ce echipele IT se concentrează asupra altor puncte terminale, securitatea imprimantelor de întreprindere rămâne în urmă

Imprimantele sunt ținte ușoare: prea multe imprimante conectate la rețea nu impun restricții și nu sunt asigurate corespunzător.

Dar amenințarea este reală și nu trebuie ignorată. Imprimantele din clasa Enterprise au evoluat, devenind dispozitive puternice, conectate la rețea, care au aceleași vulnerabilități ca orice alt punct terminal din rețeaua dumneavoastră. Aceste puncte de intrare, de obicei neprotejate, oferă o posibilitate foarte reală de a cădea pradă atacurilor cibernetice; de asemenea, acestea pot oferi accesul la datele financiare și private ale companiei dumneavoastră, ducând la consecințe foarte grave asupra afacerii.

Cu toate acestea, un studiu recent realizat de Spiceworks, la care au participat peste 300 de factori de decizie din departamente IT din întreprinderi, arată că doar 16% dintre respondenți consideră că imprimantele prezintă riscuri mari de amenințări/breșe în securitate, restul apreciind că sunt mult mai puțin vulnerabile decât desktopurile/laptopurile și dispozitivele mobile.1 Această percepție a afectat negativ modul în care personalul IT abordează securitatea rețelelor. Cu toate că aproape trei din cinci organizații implementează practici de securitate pentru imprimante, acest procentaj este cu mult sub cel corespunzător altor puncte terminale, imprimantele rămânând vulnerabile, deși există soluții simple, destinate protejării acestui punct de intrare particular.

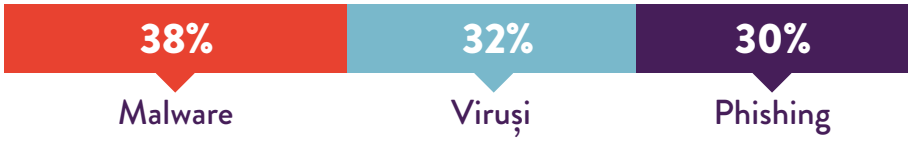
Această Carte albă prezintă date despre securitatea imprimantelor, pe baza studiului realizat de Spiceworks, impactul breșelor în securitate și unele dintre caracteristicile de securitate moderne, integrate în imprimante și concepute pentru a asigura protecția împotriva atacurilor cibernetice.

NUMAI 16% DINTRE RESPONDENȚI CONSIDERĂ CĂ IMPRIMANTELE PREZINTĂ RISCURI MARI DE AMENINȚĂRI/BREȘE ÎN SECURITATE.[1]

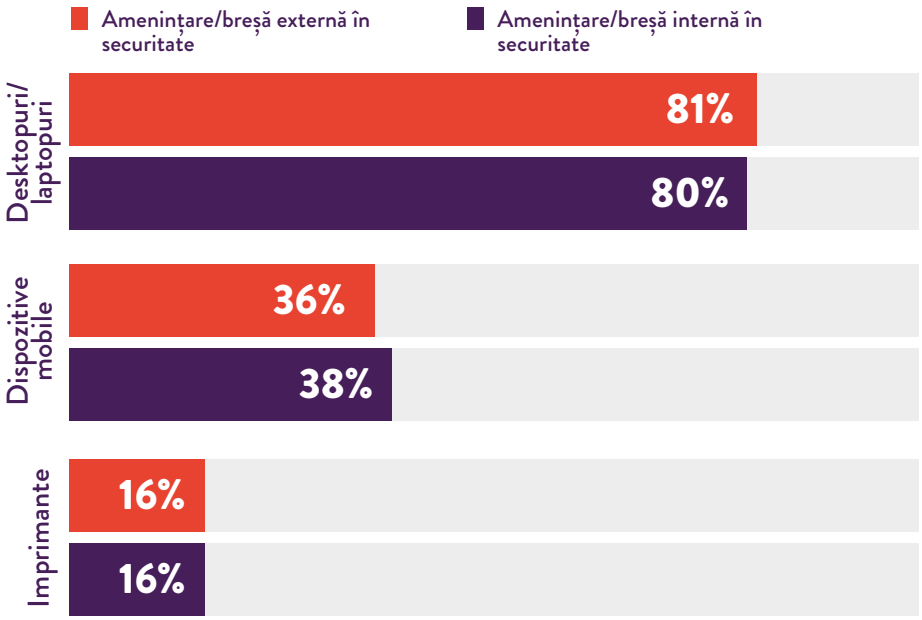
PORȚI DESCHISE ATACURILOR

În studiul realizat de Spiceworks, 74% dintre respondenți (net) au declarat că organizația din care fac parte s-a confruntat în ultimul an cu cel puțin un tip de amenințare sau breșă externă în securitatea IT. Iar 70% (net) s-au confruntat cu o amenințare sau breșă internă în securitatea IT, cauzată de obicei de erori ale utilizatorilor, de utilizarea dispozitivelor personale pentru lucrările de serviciu sau de utilizarea de către angajați a unei rețele de domiciliu sau publice pentru lucrările de serviciu.[1]

PRINCIPALELE AMENINȚĂRI/BREȘE EXTERNE ÎN SECURITATE ÎNTÂLNITE ÎN IT



Principalele amenințări s-au strecurat prin intermediul desktopurilor și laptopurilor, iar altele prin intermediul dispozitivelor mobile și imprimantelor.[1] Procentajul celor care s-au concretizat prin intermediul imprimantelor, de 16%, este considerabil mai ridicat decât cel de 4%, constatat în urma unui studiu similar, realizat de Spiceworks în 2014. De asemenea, este posibil ca numărul de atacuri realizate prin intermediul imprimantelor să fie subestimat, deoarece imprimantele nu sunt monitorizate atât de amănunțit precum PC-urile și dispozitivele mobile.



NE IGNORĂM IMPRIMANTELE

Indiferent de caz, studiul realizat de Spiceworks arată clar că securitatea imprimantelor este adesea luată în considerare prea târziu.

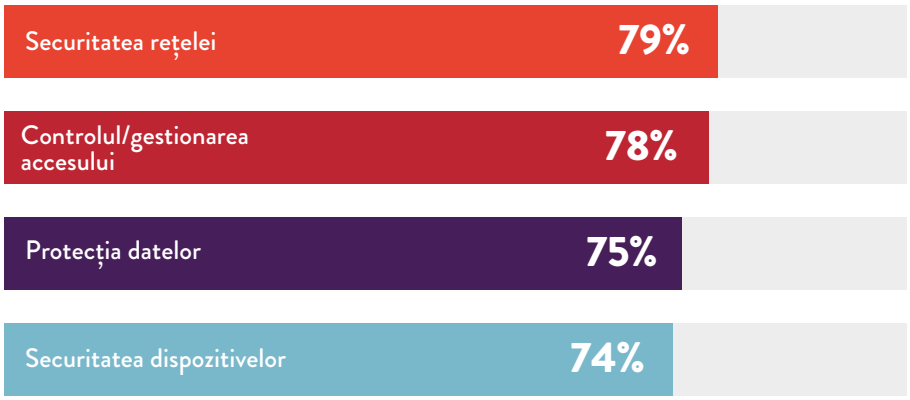
Organizațiile sunt foarte de conștiente de importanța securității datelor, rețelelor și punctelor terminale. De fapt, mai mult de trei pătrimi dintre respondenți utilizează separat soluții de securitate pentru rețele, controlul/gestionarea accesului, soluții de protecție pentru date sau soluții de securitate pentru punctele terminale, ori o combinație a acestora.[1]

Dar aceste soluții sunt implementate mult mai rar în cazul imprimantelor. În timp ce 83% dintre respondenți utilizează soluții de securitate de rețea pentru desktopuri/laptopuri și 55% pentru dispozitive mobile, doar 41% le utilizează pentru imprimante.[1]

Diferența este și mai mare în cazul securității punctelor terminale:

În plus, nici măcar o treime (28%) dintre respondenți nu implementează certificate de securitate pentru imprimante, față de 79% pentru PC-uri și 54% pentru dispozitive mobile.[1]

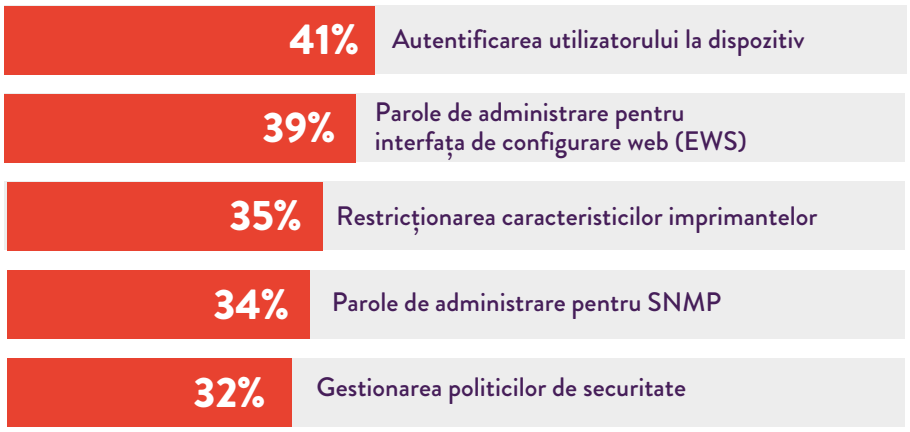
PRINCIPALELE PRACTICI DE SECURITATE PENTRU PUNCTELE TERMINALE



Printre soluțiile de protecție utilizate pentru dispozitivele generale din punctele terminale, cele mai utilizate măsuri de securitate au fost securitatea documentelor, securitatea rețelelor și controlul accesului, însă mai puțin de jumătate dintre respondenți au declarat că organizațiile lor utilizează oricare dintre aceste soluții în cazul imprimantelor.[1]

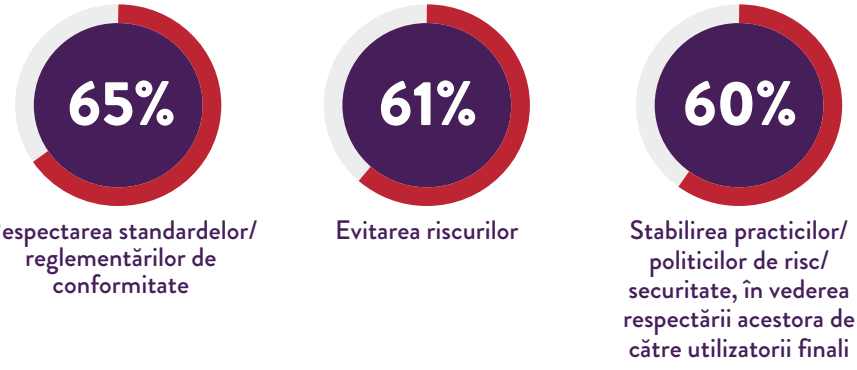
Unele companii chiar aplică practici de securitate specifice pentru imprimante, dar chiar și acolo practicile sunt foarte disparate. Puțin peste 40% dintre organizații au implementat autentificarea utilizatorilor și mai puțin de 40% au utilizat parole de administrator pentru interfața de configurare web.[1] Pentru o protecție puternică, fiecare organizație ar trebui să utilizeze o combinație a tuturor acestor abordări și nu numai.

PRINCIPALELE PRACTICI DE SECURITATE SPECIFICE PENTRU IMPRIMANTE



Când vine vorba de practicile de conformitate și de audit pentru punctele terminale, sistemele de control de securitate pentru imprimante rămân în urmă față de aproape toate celelalte puncte terminale. Aproape 90% dintre organizații au implementat o politică de securitate a informațiilor, dar în general, aceste politici nu se extind la imprimante. De exemplu, în timp ce 57% dintre respondenți au declarat că au implementat pe PC-uri măsuri de protecție împotriva malware-ului, doar 17% le-au implementat pe imprimante.[1]

APROAPE 9 DIN 10 PROFESIONIȘTI ÎN IT MENȚIONEAZĂ CĂ ORGANIZAȚIA LOR ARE STABILITĂ O POLITICĂ DE SECURITATE A INFORMAȚIILOR, DIN URMĂTOARELE MOTIVE:



În mod clar, organizațiile nu tratează cu destulă seriozitate securitatea imprimantelor, dar în mod sigur ar trebui să o facă.

„Multe imprimante încă au parole implicite sau nu au nicio parolă, ori zece imprimante utilizează aceeași parolă", a declarat Michael Howard, consilier șef de securitate la HP, pentru Computerworld, în luna iunie. „O imprimantă fără protecție prin parolă este o mină de aur pentru un hacker. Una din breșele pe care le întâlnim adesea este atacul de tip „intermediar", în care hackerul preia controlul asupra unei imprimante și deviază [documentele de intrare] către un laptop, înainte ca acestea să fie imprimate. Hackerul poate vedea tot ce imprimă directorul executiv."[2]

IMPACTUL POTENȚIAL AL INTRUZIUNILOR ÎN IMPRIMANTE

Potrivit declarațiilor lui Bogdan Botezatu, senior e-threat analyst la Bitdefender, imprimantele prezintă o potențială lacună considerabilă în securitate. „Efectuăm o mulțime de măsurări de la distanță în laboratoarele noastre de evaluare a vulnerabilităților. Ruterul nu mai este cel mai nesigur dispozitiv de pe Internet. Acum este imprimanta."[3]

Această vulnerabilitate poate avea efecte grave asupra unei firme. Chiar și cu o singură imprimantă neprotejată, întreaga rețea de dispozitive conectate poate deveni vulnerabilă la atacuri, oferindu-le hackerilor posibilitatea de a spiona dispozitivele conectate la rețea și de a compromite securitatea întregii rețele.

Am văzut cu toții efectele breșelor în securitate. În studiul realizat de Spiceworks, respondenții au declarat că principalele cinci efecte ale unei breșe sunt:[1]

1. Creșterea numărului de apeluri la biroul de asistență și a timpului de asistență

2. Productivitate/ eficiență redusă

3. Timpi crescuți de întrerupere a sistemului

4. Timpi crescuți pentru apelurile de asistență

5. Aplicare intensificată a politicilor pentru utilizatorii finali

Dar o breșă la o imprimantă poate fi și mai gravă decât atât, mai ales dacă utilizați o imprimantă multifuncțională care poate stoca în format electronic datele imprimate. Lucrările de imprimare stocate în memoria cache a imprimantei le permit hackerilor să obțină accesul la informații sensibile, personale sau de afaceri.

Un lucru și mai îngrijorător este că, prin intermediul unei imprimante neprotejate, hackerii pot accesa rețeaua mai largă a companiei și pot fura informații precum coduri numerice personale, informații financiare sau note și documente interne. Aceste informații furate pot afecta nu doar angajații individuali, dar pot fi utilizate de concurență sau pot afecta grav reputația unei companii.

SOLUȚIA SIMPLĂ: CARACTERISTICI DE SECURITATE INTEGRATE

În mod clar, companiile trebuie să rezolve problemele de securitate chiar și în cazul imprimantelor. Unele imprimante moderne de astăzi, de nivel enterprise, dispun de caracteristici de securitate integrate, simplu de utilizat, care combat amenințările la adresa imprimantelor. Printre acestea se numără:

- Caracteristici automate de detectare a atacurilor, de protecție și de reparare
- Urmărirea utilizării, pentru prevenirea utilizării neautorizate
- Opțiuni simple de conectare, precum coduri PIN sau smartcard-uri
- Un cititor de carduri de proximitate, care le permite utilizatorilor să se autentifice rapid și să imprime în siguranță la o imprimantă, utilizând ecusonul de identificare
- Imprimare criptată sigură, pentru documente sensibile

Când intenționați să achiziționați următoarea dumneavoastră imprimantă, de birou sau multifuncțională, investigați sistemele de securitate integrate și aveți grijă să le activați. Cu astfel de caracteristici simple, specifice pentru imprimante, nu există niciun motiv de a rămâne vulnerabil prin intermediul imprimantelor; în definitiv, în Internetul Tuturor Lucrurilor există multe alte puncte de acces care să vă îngrijoreze – **imprimantele nu trebuie să facă parte din acestea.**

CĂUTAȚI IMPRIMANTE MAI SIGURE?

AFLAȚI MAI MULTE ›

Surse:

1 Studiu realizat de Spiceworks în numele companiei HP, la care au participat 309 factori de decizie în IT, din America de Nord, EMEA și APAC, în noiembrie 2016.

2 „Printer Security: Is your company's data really safe?" (Securitatea imprimantelor: chiar sunt în siguranță datele companiei dumneavoastră?) Computerworld, 1 iunie 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" (Imprimantele – acum cele mai nesigure lucruri de pe Internet), The Register, 8 septembrie 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/