Sfaturi pentru securizarea dispozitivelor dvs. conectate în rețea în scopul respectării cerințelor de conformitate.

Regulamentul General de Protecția Datelor cu Caracter Personal impune companiilor să implementeze măsuri tehnice și organizaționale pentru a asigura protecția datelor cu caracter personal și să notifice persoanele vizate și autoritățile în cazul unui incident de securitate referitor la datele personale ale acestora.

Această cerință reprezintă o provocare pentru companii din punctul de vedere al alocării timpului și resurselor necesare.

Din cauza faptului că reglementările se modifică constant, poate fi dificil pentru companii să găsească timpul și resursele necesare pentru a ține pasul cu noile cerințe. Pe de altă parte, dacă nu oferă decât un simplu firewall ca protecție împotriva atacurilor, companiile pot fi atacate din exterior și, ca urmare, pot fi amendate cu sume de ordinul milioanelor. Fără îndoială, orice companie se va confrunta cu o breșă de securitate la un moment dat, așa că este esențial ca aceasta să fie identificată la timp și corectată cât mai repede cu putință cu ajutorul produselor, proceselor și instrumentelor adecvate.

Această listă cu măsuri constituie o resursă cu ajutorul căreia companiile care urmăresc să-și îmbunătățească securitatea IT și să-și protejeze reputația mărcii pot evita consecințele costisitoare ale unei breșe de securitate și se pot conforma noilor reglementări stricte din domeniu. Începeți cu măsurile de bază și progresați apoi către niveluri superioare de securitate. În acest fel, vă puteți asigura că securitatea dispozitivelor din rețea va fi aliniată cu noile reglementări stricte.

O listă practică pentru securizarea dispozitivelor conectate la rețeaua dumneavoastră.

Nivel de securitate de bază

- Achiziționați doar dispozitive cu protecție anti-malware integrată și hard discuri criptate
- Actualizați firmware-ul, mai ales la versiunile ce conțin patchuri de securitate critice - la fel ca atunci când vă actualizați aplicațiile de pe telefonul mobil
- Configurați interfețele dispozitivelor și blocați protocoalele de tipul FTP și telnet care nu sunt necesare pentru rularea aplicațiilor pe care le utilizați
- Examinați dispozitivele noi și închideți porturile sau protocoalele pe care nu le utilizați, deoarece acestea pot oferi acces intrușilor
- Folosiți parole administrative unice pentru fiecare dispozitiv
- Blocați accesul la panourile frontale de comenzi pentru a dezactiva accesul la funcțiile de administrare
- Criptați schimburile de date dintre dispozitive
- Stabiliți proceduri de ștergere a datelor vechi de pe hard discuri - mai ales la imprimantele pe care le schimbați

Odată ce ați efectuat aceste proceduri, treceți la următorul nivel de securitate.

Nivel de securitate mediu

- Integrați jurnalele sistemelor de imprimare în instrumentul dvs. SIEM pentru a putea monitoriza mai precis rețeaua în scopul identificării amenințărilor. În contextul noilor reglementări de conformitate, vizibilitatea reprezintă cheia îndeplinirii cerințelor de raportare
- Implementați metode de autentificare a utilizatorilor pentru conectarea la imprimantă în scopul monitorizării persoanelor care copiază, scanează sau trimit faxuri de pe dispozitiv. Aceste date sunt utile în cazul investigațiilor vizând identificarea breșelor de securitate.
- Implementați soluții de pull printing pentru a evita ca informațiile confidențiale să rămână în memoria imprimantei. De asemenea, aceste soluții ajută la menținerea standardelor de protecție a mediului prin reducerea deșeurilor de hârtie rezultate în urma imprimării

Odată ce aceste ați efectuat aceste proceduri, treceți la nivelul de securitate final.

Avansat

- Configurați un sistem de urmărire și raportare a sarcinilor trimise către imprimantă
- Luați în considerare stabilirea și impunerea unor reguli cu privire la persoanele care au acces și pot utiliza imprimantele (și care anume imprimante) pe baza unei autorizări, în funcție de postul deținut
- Implementați certificate digitale unice pentru fiecare imprimantă, precum și pentru celelalte dispozitive conectate la internet din rețeaua dumneavoastră
- Implementați o soluție mobilă de administrare a imprimării care să controleze criptarea datelor, accesul dispozitivelor în rețea, autentificarea și monitorizarea utilizatorilor

4AA7-1093ROE