Protejează-ți datele cu conținut confidențial – Content Aware Protection DLP de la Endpoint Protector –

Utilizarea în ultimii ani a serviciilor cloud, de la Dropbox la aplicații de e-mail web-based, a avut ca rezultat creșterea numărului de incidente (accidentale sau intenționate) de scurgere de date. Data Loss Prevention (Prevenirea Pierderii de Date) a devenit una dintre principale provocări de securitate pentru companiile din întreaga lume. Comportamentul neglijent al angajatilor este acum considerat o amenințare de securitate mai mare decât hackerii, subliniind astfel nevoia de o monitorizare atentă și detaliată a tuturor datelor transferate în afara rețelei companiei.

Pentru a proteja datele sensibile ale companie, trebuie în primul rând să fim conștienți de conținutul lor. Dacă datele părăsesc calculatorul pe un stick USB, e-mail sau aplicatii online, trebuie asigurată conformitatea cu politicile interne. Acest lucru se poate face cu ajutorul unei soluții de Content Aware Prevention DLP.

Content Aware Protection DLP – Filtrarea Conținutului
Există mai multe soluții DLP pe piață. Pe lângă modul în care aceste soluții sunt încorporate în rețeaua companiei, diferențierea o face abordarea problemei: scanarea la nivel de endpoint (calculator) sau gateway. Avantajele aduse de o soluție endpoint este că conținutul este inspectat înaintea ca acesta să părăsească calculatorul, evitând astfel inspecția fișierelor doar după ce acestea au fost deja criptate la nivel de gateway.

Endpoint Protector – Content Aware Protection DLP de la CoSoSys
Fie că este vorba de o soluție hardware, masină virtulă sau cloud, Endpoint Protector este ușor de încorporat în orice tip de rețea. Așa cum îi spune și numele, Endpoint Protector filtrează conținutul la nivel de endpoint (calculator sau laptop), fie că este vorba de Windows sau Mac OS X, avantajele cheie fiind:

· Gama largă de aplicații– Cu o multitudine de aplicații – de la browsere web la soluții de stocare cloud sau mesagerie online – managementul fișierelor confidențiale în funcție de aplicațiile utilizate este esențială. De asemenea, este imperios necesar ca lista aplicațiilor să fie extinsă și updatată în mod constant.

· Filtre în funcție de extensie– Cu o multitudine de tipuri de fișiere (.doc, .docx, .pfd, .tiff, etc) un prim filtru se poate aplica în funcție de extensie. Ca exemplu, o companie de arhitectură va dori să impiedice schițele să părărsească rețeau companiei, în timp ce documentele .docx sau .pdf nu pot să reprezinte o scurgere esențială pentru ei.

· Filtre în funcție de cuvinte cheie– Fie că este vorba de dicționare prestabilite sau de un dicționar ce conține cuvinte cheie – specifice doar companiei – cuvintele cheie pot juca un rol esențial în depistarea conținutului cu adevărat confidențial.

· Filtre în funcție de informații de identificare personală– Numere de buletin, pașaport, adrese, numere de telefon, carduri de credit, etc sunt informații care, daca părăsesc rețeau companiei periclitează atât integritatea acesteia cât și a persoanelor în cauză.

· Filtre în funcție de Expresii Regulate– Extinzând filtrele deja menționate, regex-urile sunt modalitatea perfectă de a identifica conținut recurent. De menționat că acest tip de filtru trebuie folosit doar de către persoanele care dețin cunoștințe de formare a sintaxelor.

· Monitorizare, Control, Blocare– În funcție de activitate, departament și aplicație folosită (de

exemplu browser) nu toate fișierele trebuie blocate în toata compania. De multe ori, doar monitorizarea, și nu blocarea, este de interes pentru o organizație.

- “Liste albe” de domenii și URL-uri – Pentru a elimina și mai mult tulburarea activităților de zi cu zi a angajaților sau împiedicarea totală de la muncă a acestora, crearea de liste albe cu domenii, adrese de email sau URL-uri spre care se pot trimite documente este esențială. Aceste excepții de la politicile de filtare sunt necesare pentru a trimite de exemplu documente financiare între departamentele companiei.

- Grafice, Log-uri și Rapoarte – Cu o multitudine de date care trebuie analizate de către Administratorii IT, Endpoint Protector vine în ajutorul lor și oferă grafice pentru o înțelegere facilă. Mai mult, cu ajutorul log-urilor și rapoartelor adiționale, o imagine și mai complexă este disponibilă.

Tu cum te asiguri că conținutul documentelor care părăsesc rețeau companiei este conform politicii de securitate internă?