PREVENIREA PIERDERILOR DE DATE PRIN CLASIFICARE

Elena-Andreea AVRIGEANU

S.C. Crucial Systems & Services S.R.L.

REZUMAT. Prevenirea pierderilor de date prin Clasificare, reprezintă în zilele noastre un must-have pentru orice companie care dorește ca informațiile din interiorul organizației sale să fie în deplină siguranță. În timp ce noile tehnologii cresc productivitatea și eficiența muncii, se slăbește abilitatea companiilor de a asigura securizarea informațiilor sensibile dacă instrumentele adecvate nu sunt implementate pentru a ajuta angajații să decidă modul în care informațiile sunt gestionate sau folosite. Producatorul Titus – Canada oferă o soluție completă, un set de produse numit Titus Classification Suite, menite să protejeze informațiile cu care lucrează.

Cuvinte cheie: informație, tehnologie, clasificare, securitate.

ABSTRACT. Data Loss Prevention by Classification , is now a must-have for any company that wants information from within the organization to be safe. While new technologies increase productivity and work efficiency , weakens the ability of companies to help secure sensitive information if appropriate tools are in place to help employees decide how information is managed or used. Titus manufacturer - Canada offers a complete solution set of products called Titus Classification Suite , designed to protect the information with which they work.

Keywords: information technology, classification , security.

1. INTRODUCERE

Provocările legate de protejarea informaţiilor sensibile şi de prevenirea încălcări regulilor de securitate nu sunt noi. Breslele de securitate sunt, în zilele noastre, în companiile mari, estimate la 93%.

Acțiunile răuvoite sau greşelile neintenționate sunt o realitate a zilelor noastre. În plus, presiunea cu care se confruntă organizațiile pentru a preveni încălcarea normelor de securitate este în creştere deoarece fiecare persoană partajează şi efectuează schimburi de date, zi de zi, într-un volum în creştere.

Statistic, 60% din aceste persoane efectuează schimburi de date zilnic (în interior şi exterior) cu alte 10 persoane.

Esența problemei „cât şi cum partajăm informații" este rata cu care noile tehnologii sunt adoptate sau dacă ele sunt permise sau nu.

În timp ce noile tehnologii cresc productivitatea şi eficiența muncii, se slăbeşte abilitatea companiilor de a asigura securizarea informațiilor sensibile dacă instrumentele adecvate nu sunt implementate pentru a ajuta angajații să decidă modul în care informațiile sunt gestionate sau folosite.

2. STATISTICĂ

- 20% din angajați au copiat informații ale companiei în aplicații personale.
- 46% din angajați permit altora să împrumute telefonul lor.
- Deşi 85% din companii interzic partajarea informațiilor in cloud …. Totuşi 58% din angajați le folosesc.

3. IMPORTANȚA CLASIFICĂRII INFORMAȚIILOR

Ca o consecință a creşterii gradului de partajare a informațiilor şi a creşterii inovării tehnologice şi

adoptării de noi tehnologii, organizațiile continuă să se confrunte cu consecințele incidentelor generate de:

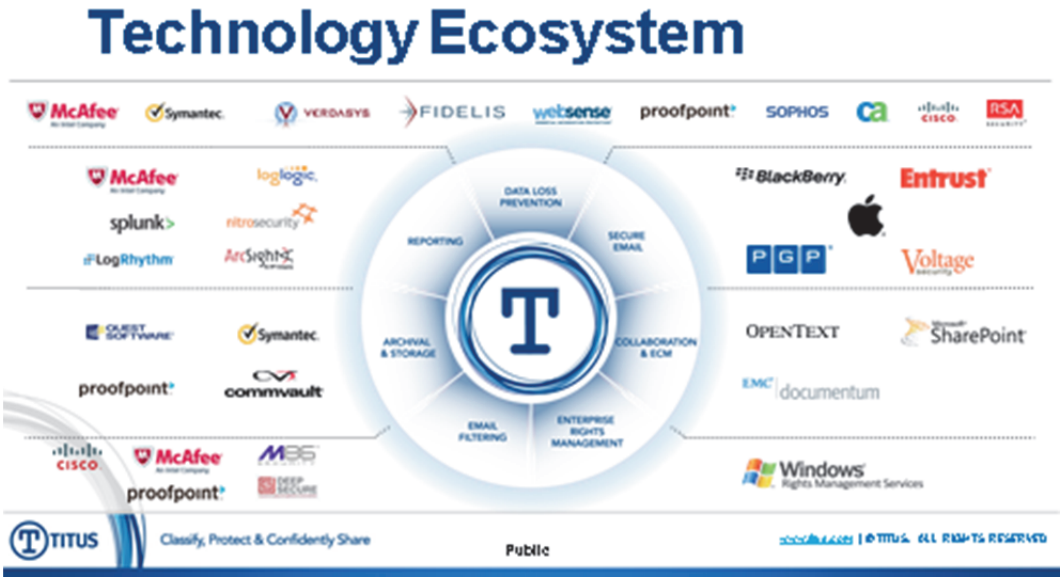
− abuzuri pe email (transmiterea documentelor în proprietatea organizației folosind un cont de email personal);

− pierderile/scurgerile de informații confidențiale (transmiterea accidental a unui email intern către exterior).

Orice organizație are multiple proiecte de securitate. Orice organizație are proiecte de securitate multiple care încearcă să abordeze provocările legate de schimbul de informații și protecția informației. Cu toate acestea, organizațiile încep să realizeze că multe dintre aceste proiecte devin propria lor „insulă" și nu funcționează coerent împreună pentru a proteja informațiile organizației.

Când o companie oferă angajaților instrumente ușor de utilizat în luarea deciziilor cu privire la sensibilitatea datelor, să capturați informații despre datele care nu pot fi reproduse prin orice mașină. Această inteligență este stocată în metadatele persistente și poate acționa ca un liant care aduce întreaga securitate programată împreună și de a crește rentabilitatea investiției proiectului de ansamblu. Câteva exemple includ:

- creșterea acurateței în funcționare a soluțiilor Data Loss Prevention;
- posibilitatea adoptării soluțiilor de criptare;
- Retenția și arhivarea diferențiată a informațiilor în funcție de gradul de sensibilitate sau de alte criterii de segmentare a informației în organizație;
- nu în ultimul rând, asigurarea complianței cu standardele și regulamentele.



Implicarea utilizatorilor conduce la mai multe rezultate cheie. În primul rând, aceasta permite schimbul securizat de date. Asta înseamna că:

− utilizatorii pot partaja cu încredere informații cu angajații, partenerii și clienții – inclusiv informații sensibile, dacă este necesar;

− informațiile sunt manipulate în mod constant și în mod corespunzător, în sprijinul cerințelor de guvernanță a datelor în organizație;

− odată ce valoarea informatiei este identificata, când informația este partajată, se știe cum trebuie protejată.

Definiția guvernării datelor: Guvernarea de date cuprinde tehnologia, oamenii, procesele și informațiile necesare pentru a crea o manipulare consistentă și adecvată a datelor unei organizații în întreaga întreprindere.

Implicând utilizatorii, crează de asemenea responsabilitatea utilizatorului:

− se încurajează și cultivă o cultură a protecției informațiilor acolo unde securitatea este responsabilitatea tuturor;

− utilizatorii încep să se gândească serios la valoarea de business a informației pe care o creează/manipulează, astfel încat o pot identifica și îi pot determina și pe ceilalți utilizatori să fie de asemenea responsabili;

− permite aplicarea forțată și obligatorie a politicilor de guvernare a datelor și prevenire a scurgerilor de date, nu numai din spatele scenei prin departamentul IT, ci chiar de la nivel utilizatorului – punctul de creare și utilizare a datelor.

Implicarea utilizatorilor creează de asemena o creștere persistentă a conștientizării noțiunii și nevoii de Securitate a datelor:

− utilizatorii sunt capabili să identifice clar valoarea de business a informației din e-mail-uri, documente, fișiere;

− destinatarii informațiilor sunt avertizați (devin conștienți) despre sensibilitatea informațiilor prin etichete vizuale și marcaje protective;

− organizația dumneavoastră este în măsură să încurajeze manipularea sigură pentru a preveni divulgarea.

Așa că, DE CE ETICHETARE? Și cum marcajele vizuale conlucrează pentru realizarea guvernarii datelor?

− companiile trebuie să identifice sensibilitatea datelor din fișierele electronice;

− companiile trebuie să angajeze utilizatorul ca actor în politica de protecție a datelor din companie deoarece utilizatorul știe mai bine natura informației pe care o manipulează.

Clasificarea PERSISTENTĂ și marcajele vizuale pot fi, de asemena, aplicate și fișierelor electronice. Acestea indică utilizatorilor și ecosistemului de guvernare a datelor din companie cum să gestioneze fișierele, cum ar fi restricționarea partajării, aplicarea criptării sau autorizarea ștergerilor.

Dispozitivele mobile conțin un mix de informații inofensive și sensibile. În implementările BYOD (Bring your own device), această problemă este agravată de faptul că datele de business sunt mixate cu cele personale.

Vă puteți identifica datele sensibile ?

Care sunt datele pe care utilizatorii și sistemul de Securitate al companiei ar trebui să se concentreze?

Fără a ști care date sunt sensibile și care nu, nu se poate aplica o politică de protecție: toată informația trebuie tratată la fel – ceea ce duce fie la un mare grad de aplicare a protecției (îngreunarea proceselor și blocarea mașinilor, scăderea productivității și frustrarea utilizatorilor), fie la aplicarea unui nivel insuficient de protecție.

Când datele sunt clar identificate/clasificate, compania beneficiază de:

− creșterea conformității cu standardele în privința marcajelor de protecție, retenția documentelor, accesul la documente și distribuirea de documente;

− o cultură sporită de conștientizare a securității și protecției datelor (în interiorul și exteriorul organizației);

− punerea în aplicare a prevenirii pierderilor de date la un nivel superior (la nivel uman și nivel de tehnologie).

4. SOLUȚIA: TITUS CLASSIFICATION SUITE

Producatorul Titus – Canada oferă un set de produse numit Titus Classification Suite. Această suită de instrumente oferă utilizatorului posibilitatea de a identifica și proteja informațiile cu care lucrează, fie că informația este în Outlook Email, documente Office, fișiere de alte tipuri în mediul Windows Desktop.

Produsele de clasificare Titus includ de asemenea clasificare pentru dispozitive mobile (Titus Classification for Mobil) care este un instrument ușor de folosit pentru a preveni pierderile de date (email și documente) de pe mobil și pentru a preveni accesul utilizatorilor la informații la care nu ar trebui să aibă acces.

Și dacă organizația folosește Microsoft SharePoint, soluțiile Titus pot crește productivitatea administrării și securitatea datelor în SharePoint.

Cu peste 2 milioane de utilizatori în toată lumea, TITUS se mândrește a fi lider de piața în domeniul clasificării informațiilor.

5. CONCLUZII

Clasificarea datelor este o tehnologie simplă care răspunde unei probleme complexe (și anume, îi face pe utilizatori actori în strategia de protecție a datelor, îi face parte din soluție). Strict din perspectiva tehnologiei, clasificarea datelor este ușor de implementat (100.000 de utilizatori în mai puțin de o săptămână).

În final, Titus a implementat soluțiile sale în toată lumea, pe e-mail multe verticale: comercial, militar, organizații guvernamentale, instituții financiare, telecomunicații.

BIBLIOGRAFIE

http://www.titus.com/data-classification-products.php, accesat la 16.11.2015.

Despre autor

Elena-Andreea Avrigeanu
Diretor general S.C. Crucial Systems & Services S.R.L.

Absolventă a Facultății de Matematică și Informatică din cadrul Universității „Ovidius“ – Constanța în anul 1997, este directoare generală din anul 1998, de când a fost înființată firma S.C. Crucial Systems & Services S.R.L. Compania activează de la mai bine de 17 ani ca deschizător de drumuri în domeniul noilor tehnologii informatice.