Interviu — June 28, 2016 at 4:32 am

Conștientizarea importanței protecției datelor

*by **clubitc***

Asigurarea securității cibernetice trebuie să constituie o prioritate pentru instituții și entități private pentru aplicarea atât a politicilor cât și a soluțiilor optime de securitate. Despre monitorizarea și protejarea datelor confidențiale în cloud, pe sisteme mobile și în organizație, am discutat cu CEO-ul Cososys, Roman Foeckl.

Club IT&C: Peisajul actual al securităţii informatice trebuie să includă protecţia avansată, tehnologii actuale ce permit și stoparea atacurilor necunoscute. Cum răspunde Cososys acestor cerințe?

Roman Foeckl: Tehnologiile noastre de Prevenirea Pierderilor de Date (Data Loss Prevention) compatibile cu Windows Mac OS X și Linux, se adresează unor categorii de amenințări din ce în ce mai pregnante în organizații – eroarea umană și scurgerile intenționate de date de către angajați. Unele din cele mai mari breșe de securitate au fost cauzate de angajați ai companiilor din neatenție, prin intermediul dispozitivelor de stocare pierdute sau încărcarea de fișiere confidențiale pe platforme neautorizate. De asemenea, cazuri cu angajații care, din motive de răzbunare sau alte motive, fură datele companiei și le publică online sau le încredințează competiției, sunt tot

mai frecvente.

Soluțiile DLP vin în completarea politicilor de securitate, întrucât acestea monitorizează și blochează transferurile de informații confidențiale către dispozitive portabile de stocare sau către aplicații online și bazate pe cloud. Conținutul transferat este analizat în detaliu, pentru a detecta informații de identificare personală, cuvinte cheie, numere de carduri de credit, ș.a. și blocat dacă transferul contravine politicilor în vigoare.

Club IT&C: Cloud-ul creează noi provocări în domeniul protecției datelor, informațiile confidențiale trecând adesea dincolo de sistemele de securitate ale rețelelor din mediul de business. Cum ajută platforma de securitate CoSoSys Endpoint Protector la monitorizarea și prevenirea pierderii datelor?

Roman Foeckl: Endpoint Protector permite crearea de politici pentru monitorizarea și blocarea transferurilor de date prin intermediul aplicațiilor în cloud. Există mai multe filtre ce se pot stabili pentru a marca fișierele ca și confidențiale și o listă de aplicații ce servesc ca destinație și care se actualizează în mod continuu. Filtrele constau în tipul de fișier, conținut predefinit, precum numere de carduri de credit, adrese de e-mail, numere de cărți de identitate, și altele, conținutul personalizat pe bază de cuvinte cheie si expresii regulate. Politicile pot fi stabilite în modul de raportare sau raportare și blocare. În momentul în care un utilizator încearcă să transfere documente marcate ca și confidențiale, prin web-browser, aplicații precum Dropbox, Google Drive, mesagerie instantanee, webmail, și alte aplicații online, Endpoint Protector raportează acțiunea administratorului și o blochează dacă este în modul raportare și blocare. Utilizatorul primește de asemenea o notificare precum că nu este autorizat să transfere acel fișier, iar acest mesaj poate fi și personalizat.

Inclusiv încercările de a copia și lipi paragrafe ce conțin date confidențiale pot fi blocate sau încercările de a face print screen. În plus, softul oferă rapoarte detaliate cu privire la ce utilizator, de pe ce computer, în ce moment, prin intermediul cărei aplicații și ce informații a transferat sau a încercat să transfere. Astfel administratorii pot detecta acțiuni suspicioase și neconforme cu politicile de securitate ale companiei și pot lua măsuri în consecință.

Club IT&C: Dispozitivele de stocare portabile pot provoca probleme grave în ceea ce privește controlul utilizării datelor în interiorul și în afara companiei. Oferă Endpoint Protector soluții pentru împiedicarea utilizatorilor să ia date neautorizate din afara companiei/să aducă fișiere cu potențial dăunător pe dispozitive de stocare?

Roman Foeckl: Prin modulul de Control al Dispozitivelor de stocare portabile (USB, HDD, etc.), dispozitivelor media (CD, DVD, etc.) și altor dispozitive (smartphone, camere digitale, carduri de memorie interne, etc.) Endpoint Protector blochează și previne conexiunea de dispozitive neautorizate, politicile rămânand active și cand computerele sunt în afara rețelei companiei. Astfel și angajații care lucrează de acasă sau în delegații și încearcă să conecteze dispozitive nepermise, vor fi blocați. În cazuri excepționale, angajații pot cere deblocarea temporară a dispozitivelor. Configurarea politicilor este flexibilă, permițând setarea drepturilor în funcție de dispozitiv, pe bază de număr de serie, și alte elemente unice de identificare, în funcție de user, computer sau grup, având diferite nivele de autorizare. Se poate permite utilizarea dispozitivelor, cu rapoarte detaliate despre

folosirea acestora, inclusiv numele fișierelor ce se transferă și o copie a acestora. De asemenea, se pot da drepturi de read-only, se pot bloca dispozitivele sau se pot autoriza doar dispozitivele USB criptate. Pentru această politică, oferim și o soluție de criptare USB, numită EasyLock, care se poate instala de la distanță pe toate dispozitivele USB conectate la computerele unde Endpoint Protector este de asemenea instalat.

Dacă se optează pentru blocarea completă a accesului la dispozitive, se împiedică și infectarea cu malware.

Soluția de Control al Dispozitivelor disponibilă în Endpoint Protector 4 creează un mediu de lucru sigur cu dispozitive de stocare portabile, care facilitează accesul la date și încurajează mobilitatea și colaborarea rapidă între angajați și alți parteneri. Atât informațiile de business, know-how-ul, cât și datele angajaților sunt protejate împotriva furtului și pierderilor, asigurând continuitatea afacerii și protejând imaginea companiei.

Club IT&C: Dispozitivele mobile bazate pe iOS și Android folosite intens în mediile corporatiste pentru creșterea eficienței contribuie la o creștere a amenințărilor la adresa securității. Are platforma Cososys Endpoint Protection o componentă de Mobile Device Management și cum acționează aceasta?

Roman Foeckl: Soluția completă Endpoint Protector 4 dispune de următoarele module: Controlul Dispozitivelor, Prevenirea Pierderilor de Date (DLP) și Mobile Device Management. Motivul pentru care s-a adăugat MDM în aceeași platformă de gestiune a fost nevoia de a proteja informațiile pe toate stațiile de lucru sau toate endpoint-urile. Fie că vorbim de un laptop, desktop sau smartphone, există date confidențiale stocate care pot amenința securitatea dacă nu sunt controlate într-un fel sau altul.

Noi acoperim cele mai populare sisteme de operare, cu funcționalități complementare, DLP și Controlul Dispozitivelor pentru Windows, Mac OS X și Linux și MDM pentru iOS și Android. Funcționalitățile de MDM permit localizarea dispozitivelor, setarea parametrilor pentru parole de la distanță, pentru a obliga utilizatorii să folosească parole complexe și stabilirea restricțiilor pentru folosirea aplicațiilor. De asemenea, se pot configura de la distanță e-mail-ul, VPN-ul și WiFi-ul, se pot instala de la distanță aplicații, șterge de la distanță datele, în cazul dispozitivelor pierdute sau furate și se pot bloca acestea de la distanță.

Endpoint Protector MDM oferă și posibilitatea de a aplica politici în funcție de locație prin funcționalitatea denumita geofencing. De exemplu, dacă administratorul dorește să oprească camera foto de la smartphone-urile angajaților automat când aceștia ajung la birou, poate crea un perimetru pentru clădirea companiei în care adaugă această politică de dezactivare a camerei foto. Astfel, când angajații ies din acest perimetru, camera se activează automat, permițând folosirea în timpul liber. Această politică este mai puțin invazivă pentru utilizatori, reducând numărul reclamațiilor la adresa departamentului de IT.

Club IT&C: Criptarea datelor asigură confidențialitatea datelor în cazul dispozitivele pierdute sau furate. Care este răspunsul Endpoint Protector la această problemă?

Roman Foeckl: EasyLock, softul menționat anterior, rezolvă problema dispozitivelor USB pierdute sau furate. Practic acesta este un container protejat cu parolă pe dispozitivul de stocare și dacă dispozitivul este pierdut sau furat, nu se pot accesa datele stocate fără a cunoaște parola. Totodată, ca și măsură de protecție

suplimentară, în cazul introducerii parolei de 10 ori în mod eronat, datele vor fi șterse automat. Mai mult decât atât, prin integrarea cu Endpoint Protector 4, utilizatorii pot fi obligați să foloească doar dispozitive USB criptate. Și acest soft este cross-platform, fiind compatibil cu Windows și Mac OS X.

În ceea ce privește smartphone-urile și tabletele, prin intermediul soluției MDM, putem activa de la distanță și centralizat criptarea nativă a dispozitivelor, care în cele mai multe cazuri nu este activată de utilizatori.

Club IT&C: Cât de mult conştientizează companiile locale riscurile de securitate?

Roman Foeckl: Acum câțiva ani tehnologiile Data Loss Prevention și Mobile Device Management erau foarte puțin cunoscute în România. Cele mai multe companii conștientizau riscurile de securitate, dar își îndreptau atenția în principal către riscurile externe, precum malware, phishing, SQL injections, etc. și ignorau riscurile interne, reprezentate chiar de proprii angajați sau colaboratori. Lucrurile au început să se schimbe, tot mai multe companii locale sunt interesate și vor să implementeze soluții de securitate pentru noul val de amenințări. Cu siguranță noile reglementări (GDPR) ce se vor aplica tuturor țărilor din UE vor contribui la o conștientizare mai mare asupra importanței protecției datelor.