White Paper

Firmele şi securitatea datelor – România vs. Germania

Februarie 2010

COSOSYS

Cuprins

Introducere

Pierderea sau furtul datelor confidențiale reprezintă unul dintre cele mai mari riscuri de securitate cu care se confruntă firmele. De la expunerea accidentală a unor planuri de dezvoltare, liste de clienți, rezultate ale unor cercetări, la furtul planificat prin breşe în securitatea rețelelor, toate pot avea efecte devastatoare asupra companiilor. Cu atât mai mult în condițiile economice actuale, în care angajații fie sunt concediați, fie se tem de o eventuală disponibilizare şi vor să îşi asigure o oarecare siguranță financiară, alegând astfel să îşi însuşească şi să vândă informații confidențiale, sau să le păstreze pentru a avea un atu în negocieri viitoare cu potențiali angajatori din rândurile competiției.

Costuri şi pierderi generate de breşele de securitate

Pierderile generate de o astfel de breşă de securitate sunt semnificative. Într-o primă fază, e vorba de venituri ce nu vor mai fi realizate. Pierderea unei baze de date cu clienți poate însemna că aceştia vor fi contactați şi atraşi de competitori. Furtul unui prototip poate însemna producerea lui în masă de către o altă firmă. Un alt val de pierderi este determinat de clienți – o astfel de breşă făcută publică (iar în cele mai multe cazuri firmele sunt obligate să furnizeze aceste informații) înseamnă capital de imagine redus, pierderea încrederii clienților şi plecarea acestora către competitori din proprie inițiativă. În plus, există posibilitatea unor amenzi, în funcție de legile şi regulamentele din zone şi țări diferite, sau a unor procese ce pot avea drept consecință plata unor despăgubiri uriaşe.

Cele de mai sus sunt pierderile mai uşor de observat de către firme, ele subestimând astfel costurile ce țin de refacerea după o astfel de breşă de securitate. Este vorba de resurse financiare şi timp al angajaților investit în recâştigarea încrederii clienților, găsirea de noi clienți, redobândirea poziției pe piață şi a capitalului de imagine.

Desi toate aceste plăți uriaşe pe care companiile sunt forțate să le facă pot fi prevenite relativ uşor prin implementarea unor soluții de securitate a porturilor şi de prevenire a pierderii de date, de cele mai multe ori firmele fie amână achiziționarea şi instalarea unui astfel de soft, din motive ce țin fie de bugete insuficiente, fie de prea puțin personal calificat, fie de subestimarea flagrantă a costurilor generate de astfel de incidente.

Breşele de securitate – studii şi date relevante

Studiile realizate în perioade similare de către CoSoSys în România, intervievând 88 de firme, şi institutul Emnid pentru KPMG în Germania (http://www.dw-world.de/dw/article/0,,5124070,00.html), arată o situație asemănătoare: *un număr mare de breşe de securitate, o subevaluare a riscurilor şi lipsa unor bugete pentru asigurarea securității datelor.*

De multe ori, cei aflați la conducerea firmelor sunt convinşi că breşele de securitate li se pot întâmpla doar altora, considerând că datele ce le-au fost încredințate nu sunt suficient de importante, sau că afacerea lor este prea mică pentru a prezenta interes. Cu toate acestea, majoritatea – 90% dintre managerii IT din România - este conştientă că păstrează date confidențiale, angajații având acces la aceste date şi putând oricând să şi le însuşească.

Mai mult, 75% dintre managerii IT chestionați au declarat că personalul poate folosi fără restricții şi nemonitorizat dispozitive de stocare portabile, în condițiile în care un hard portabil, un stick USB sau chiar un telefon mobil de ultimă generație ar fi suficient pentru a stoca toate fişierele importante dintr-o firmă. 45% dintre ei sunt, de asemenea, conştienți că o eventuală breşă ar însemna costuri mari pentru companiile pentru care lucrează, informațiile cele mai valoroase şi cele expuse celor mai multe riscuri fiind informațiile financiare, bazele de date cu clienți, planurile de cercetare şi dezvoltare, listele de prețuri, contractele cu furnizorii sau rețetele de produse.

Într-adevăr, accesul nu presupune neapărat şi furtul sau pierderea, dar 25% dintre firmele intervievate în România au declarat că au fost victimele pierderii de date în urma plecării unor angajați. Deşi proporția este de doar o pătrime, este important de menționat că restul de 75% nu ştiu dacă au existat pierderi sau furturi de date, fişierele confidențiale şi accesul la ele nefiind monitorizate.

Şi în Germania amenințarea din interior este una importantă. 37% dintre firmele intervievate de Emnid au fost victimele unor infracțiuni economice în ultimii trei ani, principalele riscuri fiind frauda prin Internet şi furtul datelor confidențiale. În cazul a 62% dintre firmele mici şi mijlocii afectate, furtul a fost facilitat de o persoană din interior. În cazul firmelor mari, procentul este mai mic, şi anume 40%.

Soluții pentru prevenirea acestor incidente există, iar cei responsabili cu securitatea sunt interesați de achiziționarea lor. Problema principală este că, deşi riscurile sunt evidente la nivelul departamentelor de IT, managerii din vârful piramidei sunt mai greu de convins. Specialiştii în IT, dincolo de dificultatea de a prezenta eficient riscurile de securitate şi soluțiile, au o problemă în a explica modul în care o astfel de investiție poate fi recuperată.

De cele mai multe ori, astfel de breşe trec neobservate. Firmele fie nu monitorizează activitatea angajaților şi modul în care utilizează datele confidențiale, aşa cum se întamplă în România, fie chiar şi atunci când le descoperă, aleg să nu le declare – în Germania se estimează că 80% dintre infracțiunile economice sunt nedetectate sau neraportate, costurile incidentelor cunoscute fiind estimate la 3,43 miliarde de Euro.

Deşi sumele sunt suficient de mari încât să sperie într-o primă fază şi să ajute conştientizarea riscurilor, procentele mici declarate îi fac pe numerosi manageri să creadă că pot ramâne în procentul majoritar neafectat de aceste infracțiuni. Cum însă în Germania, ținând cont de cele 80 de procente neraportate şi de investițiile în general mai mari în soluții de securitate, putem să presupunem că majoritatea firmelor au fost victimele unor crime economice, putem, de asemenea, să extindem această estimare şi asupra firmelor din România.

Care este soluția?

Cea mai eficientă măsură pentru prevenirea unor astfel de incidente şi a costurilor imense asociate este implementarea unei soluții pentru prevenirea pierderilor de date şi a controlului dispozitivelor portabile. Soluția dezvoltată de CoSoSys, Endpoint Protector 2009, este concepută pentru a minimiza amenințările interne, a reduce riscul scurgerilor de date şi a controla dispozitivele conectate la calculator. Soluția le permite departamentelor IT să controleze în mod proactiv utilizarea internă a dispozitivelor, în timp ce înregistrează toate datele transferate prin rețea şi criptează datele în tranzit pe dispozitivele portabile.

Endpoint Protector ajută, de asemenea, companiile să economisească timp şi să îşi mărească productivitatea, simplificând activitățile departamentelor IT şi ale utilizatorilor atehnici. Soluția are o interfață de administrare web intuitivă, disponibilă în cinci limbi (engleză, germană, română, franceză şi maghiară). Activitățile uzuale sunt automatizate şi de wizard-ul pentru managementul eficient al dispozitivelor din rețea şi de capturile de sistem, care permit revenirea rapidă la configurațiile anterioare.

Pentru a susține eficiența şi mobilitatea angajaților atehnici, Endpoint Protector 2009 oferă o gamă extinsă de dispozitive portabile controlate, de la iPod-uri, aparate foto şi sick-uri USB, până la imprimante şi ExpressCard-uri SDD, precum şi suport pentru numeroase sisteme de operare Windows, Linux şi Mac OS.

Endpoint Protector 2009 oferă în plus modalități de protejare a informațiilor în modul de lucru offline, acestea având scopul de a proteja datele confidențiale atunci când nu există o conexiune permanentă la Internet, permițându-le în acelaşi timp oamenilor de afaceri ce călătoresc să ramână activi şi productivi. Astfel, ei sunt protejați de riscurile folosirii dispozitivelor de stocare portabile ce pot cauza importante breşe de securitate.

Cum demonstrați eficiența investiției?

Pentru a sprijini profesioniştii IT în efortul lor de a securiza datele firmelor, explicând în acelaşi timp utilitatea financiară a unei noi achiziții, CoSoSys a conceput un utilitar dedicat vizualizării modului în care investiția va fi recuperată, disponibil aici (http://www.endpointprotector.com/en/index.php/resources/ROI_Calculator/).

Despre CoSoSys

Compania CoSoSys este specializată în dezvoltarea de software pentru securizarea rețelelor şi pentru îmbunătățirea dispozitivelor de stocare portabile. Portofoliul aplicațiilor include funcții de la protejarea prin parolă şi sincronizarea datelor, până la împiedicarea accesului neautorizat la dispozitivele periferice ataşate calculatoarelor. Distribuirea produselor CoSoSys se face la nivel global prin fabricanții de hardware de talie mondială, dar şi direct către utilizatorii finali prin magazinul electronic disponibil pe http://www.CoSoSys.com şi http://www.EndpointProtector.com. Compania CoSoSys se bucură de o creştere continuă a numărului de utilizatori la nivel mondial. Aceasta are sediul în Cluj-Napoca, România, şi are reprezentanți de vânzări în Statele Unite şi Germania.

Copyright