Casarea mediilor de stocare

Mai devreme sau mai târziu toate mediile de stocare sunt retrase. Având în vedere că marea majoritate a unităţilor aruncate conţin date sensibile, proprietarul unității ar trebui fie să elimine datele de pe mediul de stocare fie să distrugă complet unitatea. Multe organizaţii nu reuşesc nici să înţeleagă care sunt riscurile de a lăsa datele pe mediile de stocare la momentul casării acestora. Uneori organizațiile cred in mod eronat că datele critice pentru afacerea proprie au fost eliminate în condiţii de siguranţă atunci când, de fapt, acestea pot fi încă recuperate. Aceast articol oferă un set de orientări şi indică cele mai bune practici pentru a asista organizaţiile în eliminarea în mod corespunzător a datelor de pe mediile de stocare înainte de casarea sau de reutilizarea lor.

1. Cele mai multe medii de stocare conţin date sensibile

Analiștii din industrie estimează că 80 la sută dintre stațiile lucru ale unei organizații conţin date sensibile. Procentul de servere de întreprindere cu date sensibile este mai mare. La momentul casării aproape nu există mediu de stocare, cum ar fi un hard-disk, care să nu includă informații personale sensibile, cum ar fi nume de persoane, adresele fizice şi de e-mail ale acestora, eventual şi telefonul mobil. Alte informații care se pot găsi pe discul unei stații de lucru se referă la coduri numerice personale, numere de cărţi de credit, numere de conturi bancare, liste de clienţi şi informaţii de contact, date şi informaţii sensibile referitoare la resurse umane.

Pe cele mai multe medii de stocare se găsesc și cantităţi variabile de proprietate intelectuală, cum ar fi secrete de serviciu, note şi email-uri confidenţiale, informații tehnice, de vânzări, date financiare. De asemenea pot exista coduri şi parole de acces, parole şi chei de decriptare prin care se poate realiza acces la sisteme de aplicații, baze de date sau volume care conțin date sensibile pentru afacere.

2. Cele mai bune practici privind casarea discurilor

Următoarele recomandări reprezintă un ecxemplu de punere în aplicare a procedurilor de eliminare sau de retragere a unităților de disc.

Stare disc	Discuri criptate	Discuri necriptate
Operațional	Pentru unitățile de disc pe care toate datele sensibile au fost criptate utilizând practicile standard şi acceptate de criptare, cum ar fi AES, Triple-DES, Blowfish, etc, şi pe care a fost implementată o metodă de ştergere sigură a cheii de decriptare, curățarea se realizează cel mai bine criptografic. Această metodă de ștergere permite eliminarea sau redistribuirea unității.	Unităţile fără criptare trebuie suprascrise cu un program software care îndeplineşte specificația de cerințe DoD 5220.22. Acest lucru necesită ca datele să fie suprascrise de cel puţin trei ori înainte de eliminare sau de reutilizare. Distrugerea unității fie prin distrugerea fizică fie prin demagnetizare este, de asemenea, o opţiune în cazul în care unitatea nu este reutilizată.

Stare disc	Discuri criptate	Discuri necriptate
Non- operațional	Dacă o unitate criptată este definitiv non-operaţională, înseamnând că nu mai poate fi recuperată cheia de decriptare în scopul retragerii de date se poate considera că unitatea a fost deja ștearsă. Cu toate acestea, în cazul în care există chiar şi cel mai mic risc ca unitatea să poată fi făcută operaţională, cheia trebuie să fie distrusă indiferent unde este stocată.	Unităţile necriptate care sunt defecte, și pentru care nu poate finaliza un proces de suprascriere conform cu standardele DoD 5220.22 sau NIST 800-88 ar trebui să fie demagnetizate sau distruse fizic.

3. Concluzii

Este necesară dezvoltarea şi diseminarea unui set clar de politici care guvernează casarea unităților de disc.

- educarea utilizatorilor despre politicile de confidenţialitate ale organizaţiei, inclusiv politicile şi tehnicile corespunzătoare pentru casarea unităţilor de disc
- generarea şi menţinerea unei documentaţii corespunzătoare cu privire la procedurile de casare a mediilor de stocare.
- pe măsură ce organizațiile înlocuiesc echipamentele de calcul calculatoarele existente, personalul cu atribuții de securitatea informației trebuie să încurajeze implementarea de discuri criptate pentru a reduce costurile și a simplifica procedurile tehnice de casare.

4. Referințe

[1] *),** SR ISO/CEI 27001, Tehnologia informației, Tehnici de securitate, Sisteme de management a securității informației, Cerințe, 2006

[2] *),** SR ISO/CEI 27002, Tehnologia informației, Tehnici de securitate, Cod de bună practică pentru managementul securității informației, Cerințe, 2006

[3] Seagate Technology LLC, Drive Disposal Best Practices, 2007