Strategia ta de Prevenirea Furtului si Pierderii de Date este un punct forte sau o slabiciune?

Chief Solutions Officers (CSOs) si Chief Information Security Officers (CISOs) stiu ca e nevoie doar de o singura bresa in securitate pentru ca cineva sa fure date sau sa provoace pagube. Rolul tot mai important al dispozitivelor mobile in mediul de afaceri, politica Bring Your Own Device (BYOD – adu-ti propriul dispozitiv) si serviciile cloud, sporesc riscurile ca informatii critice sa parareasca reteaua companiei. Mobilele si dispozitivele de stocare portabile, cat si solutiile de colaborare online, reprezinta riscuri mari de furt sau pierdere a datelor. Pentru a controla si securiza datele, adoptati cele mai bune practici pentru Prevenirea Furtului si Pierderii de Date (Data Loss Prevention – DLP).

Instruirea si educarea angajatilor in protejarea datelor este importanta, insa daca permiteti utilizarea dispozitivelor de stocare USB si a mobilelor, sau aplicatii precum Skype, Google Drive, Dropbox, nu poteti doar sa instruiti si sa va rugati sa nu se intample nimic rau. O solutie eficienta de Filtrare a Continutului (Content-Aware DLP), Controlul Dispozitivelor (de stocare USB) si Managementul Dispozitivelor Mobile (MDM) trebuie sa fie punctul de pornire.

O solutie DLP si MDM robusta, permite controlul dispozitivelor de stocare portabile, filtrarea transferului de date catre aplicatiile online, si securizeaza si administreaza mobilele. Criptarea datelor critice este absolut vitala.

Exista mai multe solutii DLP, insa complexitatea lor – sau aparenta complexitate – intarzie implementarea. O solutie usor de utilizat si care ofera criptare AES de 256-bit, va incuraja implementarea. O astfel de solutie trebuie sa se integreze cu Solutia de Controlul Dispozitivelor, transformand orice stick USB intr-un asa numit Trusted Device.

Pe langa criptare, iata cateva dintre cele mai bune practici:

· **Modul de Implementare –** Evaluati diverse moduri de implementare a solutiei DLP. Variantele populare (hardware appliance, masina virtuala, solutie cloud / SaaS sau Amazon Web Services) toate au puncte forte cat si dezavantaje;

· **Cautati o solutie multi-platforma (cross-platform) –** Alegeti o solutie care functioneaza atat pe Mac cat si Windows. Implementati o solutie flexibila, ce poate sa faca fata pe viitor schimbarii nevoilor. Alegeti solutia care se muleaza la viitoarele cerinte, fara a fi nevoie de mari costuri aditionale;

· **Setati nivelul de autorizare in functie de departament si sarcini de lucru –** Controlul si administrarea unei solutii DLP este mai usoara cand nivelul de acces este setat in functie de utilizator, calculator, dispozitiv sau global (pe intreaga companie). Asigurati-va ca doi utilizatori ai aceluiasi calculator pot avea doua niveluri complet diferite de transfer al datelor. Aceasta flexibilitate imbina securitatea cu convenienta;

· **Stabiliti si comunicati politici clare privind mobilele –** Setati o politica clara privind utilizarea dispozitivelor mobile. Pentru a proteja datele de pe mobile, acestea trebuie inrolate intr-o solutie MDM. Astfel, beneficiile se vad atat din punct de vedere al productivitatii cat si a securitatii – beneficiind de functionalitati precum parole complexe, localizare, inchidere sau stergere de la distanta, etc.). Asigurati-va ca utilizatorii

mobilelor cunosc politica organizatiei cu privire la stocarea datelor si consecintele neconformarii;

· **Testati diferite scenarii –** Testati o varietate de posibile riscuri, precum dispozitive USB portabile si continut divers. Concentrati-va pe amenintarile cauzate de tehnologiile recente insa tineti minte ca si tehnologiile mai vechi (CD-uri si DVD-uri) pot fi sursa pierderii sau furtului de date. Riscurile fisierelor locale necriptate sau stocate in cloud trebuie de asemenea luate in considerare;

· **Analizati resursele necesare functionalitatilor complexe –** Inainte de a implementa o solutie DLP, ganditi-va ce resurse sunt necesare unor funtionalitati precum File Shadowing; cantitatile de date ce trebuie monitorizate si numarul copiilor stocate pot sa utilizeze in scurt timp o parte considerabila din resurse;

· **Investigati solutiile DLP cloud –** O astfel de solutie este mult mai usor de evaluat, implementat si scalat. Este o varianta buna de a beneficia de avantajele solutiilor cloud si de protejare a datelor.

Adoptarea si mentinerea celor mai bune practice privind prevenirea furtului si pierderii de date ofera un mare randament al investitiei, daca sunt implementate corect. De tinut minte:

· Nu exista o solutie DLP universal valabila. Cele mai bune practici pot fi modificate in functie de cerintele fiecarei organizatii;

· Inainte de implementare, evaluati avantajele si dezavantajele fiecarei solutii si revizuiti eficienta programului propriu de DLP;

· O solutie DLP trebuie sa fie multi-platforma si sa ofere functionalitati de baza si pentru distributiile Linux;

· Dupa implementarea solutiilor de Controlul Dispozitivelor (de stocare USB) si Filtrarea Continutului (Content-Aware DLP), urmatorul pas in Prevenirea Furtului si Pierderii de date este implementarea MDM-ului;

· Asigurati-va ca datele si informatiile cheie sunt protejate – folositi solutii de criptare;

· Managementul solutiei DLP trebuie sa fie usor, oferind administratorului IT acces facil si rapid.

Scurgerile de date pot afecta desfasurarea activitatii cat si leza imaginea organizatiei. Reduceti expunerea la riscuri urmand o politica DLP solida, implementata corespunzator. Doriti sa investiti timp si resurse limitand expunerea la astfel de riscuri sau doriti sa va confruntati cu sume exponentiale dupa un astfel de incident? Faceti astazi pasii corespunzatori pentru a proteja angajatii si datele companiei.