



KYBERBEZPEČNOSŤ

AKO PREDÍŠŤ ÚNIKU CITLIVÝCH ÚDAJOV

Viete, ako vaši zamestnanci nakladajú s digitálnymi informáciami?

Vyzerá to ako neškodné situácie, ktoré nastávajú každý deň:

Zamestnanec nestíha, rozhodne sa, že úlohu dokončí večer doma, a tak si dokumenty odošle na súkromnú e-mailovú adresu. Doma si ich stiahne na súkromnom počítači a pokračuje v práci v nádeji, že všetko stihne dodať načas. Iný zamestnanec si pred ukončením pracovného pomeru vo firme uloží „svoje dokumenty“ na USB kľúč: „Veď to je moja práca, ešte sa mi to môže zísť.“ Ďalším príkladom môže byť zamestnanec, ktorý nájde rýchle riešenie na odoslanie veľkého súboru obsahujúceho firemné dáta a zvolí verejné úložisko.

Možno si poviete, že toto sa vo vašom podniku nedeje, nemôže stať, alebo vás po prečítaní týchto príkladov zalial pot.

V skutočnosti ide o reálne situácie, ktoré sa môžu stať – a často sa aj dejú v každej organizácii, len si to neuvedomujeme. Všetky tieto prípady však majú spoločný dôsledok: digitálne údaje opúšťajú bezpečné prostredie firmy – smerujú na súkromné e-maily, neznáme USB kľúče či verejné úložiská a sú ďalej spracovávané na nespravovaných zariadeniach, na ktoré sa neaplikujú bezpečnostné politiky a pravidlá definované firmou.

Dokážete vôbec ustriechnuť, ako vaši zamestnanci pracujú s firemnými údajmi alebo údajmi vašich zákazníkov a aké digitálne stopy zanechávajú?

DLP – nenápadný hrdina vašich firemných dát

V dnešnom digitálnom svete, kde sa dáta stali cennejšími než zlato, je ochrana dát (Data Lost Prevention – DLP) nevyhnutnosť. Systémy DLP sú ako šikovní strážcovia, ktorí neustále monitorujú, čo sa s dátami deje – kam sa posielajú, kto k nim prístupuje, ako sa s nimi narába. A keď zistia, že sa niečo deje inak, než by malo, zasiahnu, pomôžu zistiť, čo sa stalo, kto bol zapojený a ako minimalizovať škody.

O čo pri DLP vlastne ide?

Dôležitý prvý krok je identifikácia, aké dáta sú kritické a vyžadujú ochranu. Sú to osobné údaje, finančné informácie, obchodné tajomstvá a iné citlivé informácie. Systémy DLP sú konfigurované pomocou pravidiel a politik, ktoré definujú, aké dáta sú chránené a aké akcie sú povolené alebo zakázané. Monitorujú pohyby dát v sieti a na koncových zariadeniach, aby identifikovali potenciálne úniky a prípadne im zabránili.

Po identifikácii takéhoto úniku dát systém DLP prijme preventívne opatrenia, ako napríklad blokovanie prenosu – či už s upozornením používateľa, alebo bez neho. V prípade úniku dát systém DLP pomáha pri reakcii na incident, v jeho vyšetrení vrátane identifikácie zdroja úniku a obmedzenia jeho dosahu. Zaznamenáva a uchováva aktivity súvisiace s ochranou dát, čo umožňuje sledovanie a analýzu potenciálnych únikov.

Nasad'te DLP rozumne – a s ľudským prístupom

Implementácia DLP nie je len o technológii. V prvom rade je dôležité dôkladne naplánovať a analyzovať vaše potreby. Identifikovať, ktoré dáta sú pre vás najcennejšie a najzraniteľnejšie. Potom treba zvoliť riešenie, ktoré sa hodí k veľkosti a charakteru vašej firmy. Dôležité je DLP dôkladne nakonfigurovať a otestovať, pretože aj najlepší systém je zbytočný, ak ho nikto nevie používať alebo ak je nesprávne nakonfigurovaný.

Používatelia musia vedieť, čo DLP robí, prečo je dôležitý a čo od nich očakávajú. Preto školenie a otvorená komunikácia sú neoddeliteľnou súčasťou zavedenia systému. A napokon DLP nie je technológia typu „nastav a zabudni“. Potrebuje pravidelné sledovanie, údržbu a aktualizácie.

Ochrana dát nie je luxus – je to základ

DLP je nástroj, ktorý vám pomôže mať pod kontrolou to najcennejšie, čo vo firme máte – informácie. Ak ho zavediete s rozumom a správnym nastavením, bude pre vás fungovať ako neviditeľný štít, ktorý chráni nielen vaše dáta, ale aj vašu dôveru, povesť a budúcnosť.

» Ing. LUBOMÍR ŠIDLÍK,

koordinátor programátorov, špecialista interného rozvoja,
interný koordinátor pre ISM
HOUR, spol. s r. o.

