Ochrana pred únikom informácií

Prečo je dôležitá ochrana pred únikom informácií?

Ochrana citlivých informácií, resp. prevencia úniku dát (DLP – Data Loss Prevention*) je súčasťou životného cyklu informácií. Dnes už nie je možné ohraničiť ich spracovávanie a používanie len na istú oblasť. Informácie sú distribuované na viacerých miestach, z ktorých mnohé nemáme pod kontrolou. Rovnako musíme zabezpečiť, aby boli informácie prístupné iba oprávneným používateľom. Títo používatelia sa takmer vždy v čase dynamicky menia.

„Klasické" metódy ochrany citlivých informácií, ako sú šifrovanie, prípadne režimové opatrenia, sú v tejto situácii nepostačujúce. Stačí si predstaviť interného zamestnanca, ktorý náhodne odošle citlivú informáciu na nesprávny e-mail alebo úmyselne skopíruje databázu klientov a poskytne ju konkurencii. Informácie môžu uniknúť aj pri spracovávaní mzdovej agendy či pri reportovaní obchodných výsledkov. V praxi dochádza k podobným nežiaducim únikom častejšie, ako si myslíme, resp. sme ochotní pripustiť. A práve ochranou pred takýmito útokmi sa zaoberá oblasť prevencie únikov informácií.

Hlavné výhody DLP:

- identifikácia, monitorovanie a ochrana citlivých informácií
- ochrana informácií pri ich spracovávaní, prenose a aj po ich uložení
- detekcia a prevencia neautorizovaného použitia a prenosu citlivých informácií
- jednoduchšia implementácia noriem a štandardov

Ciele DLP:

- zamedziť úniku citlivých informácií
- zvýšiť úroveň bezpečnosti používaných, uložených a prenášaných informácií

Ako vám vieme pomôcť pri ochrane pred únikom informácií?

Spoločnosť TEMPEST poskytuje riešenia na ochranu pred únikom citlivých informácií. Po analýze konkrétneho prostredia a procesov nasadíme vhodnú DLP technológiu. Skúsený tím odborníkov po analýze najprv pomôže zodpovedať nasledujúce otázky:

- aké typy citlivých informácií sú spracovávané?
- kde sú citlivé informácie uložené?
- akým spôsobom a kam sú citlivé informácie prenášané?
- ako je možné detekovať potenciálny únik citlivých informácií a ako naň reagovať?
- aké následky a dopady na spoločnosť by mal prípadný únik citlivých informácií?

Po zodpovedaní týchto otázok vám vieme odporučiť DLP technológiu vhodnú priamo pre vaše prostredie, pričom výber berie do úvahy lídrov v oblasti DLP. Túto technológiu integrujeme do vášho prostredia, pomôžeme vám nakonfigurovať prostredníctvom DLP riešenia pravidlá relevantné pre vašu spoločnosť a naviazať riešenie na vaše interné procesy.

* Data Loss Protection, príp. Data Leak Protection

Tempest
IT makes sense

Implementácia DLP

Spoločnosť TEMPEST na základe odbornosti a skúseností tak v analytickej, ako aj technologickej oblasti pristupuje k tejto problematike komplexne. Dodáme DLP riešenie „šité" priamo na uspokojenie potrieb vašej organizácie, naviazané na vaše procesy a nasadené v súlade so všetkými pravidlami, predpismi a politikami platnými pre vaše interné prostredie.

Implementácia DLP riešenia nekončí (a ani nezačína) nasadením samotnej technológie. Technologická spoločnosť, ktorá síce úspešne nasadí konkrétnu DLP technológiu, totiž nemusí byť schopná vykonať úvodnú klasifikáciu a inventarizáciu informácií, prípadne nakonfigurovať nasadené riešenie v súlade s bezpečnostnými politikami platnými vo vašom prostredí. A naopak, spoločnosť schopná vykonať analytickú časť riešenia nemusí byť rovnako úspešná pri nasadzovaní samotnej technológie.

Ako funguje samotná technológia?

DLP riešenia pri ochrane pred únikom citlivých informácií vo všeobecnosti rozdeľujú dáta na tri typy:

- prenášané dáta (angl. Data in Motion),
- uložené dáta (angl. Data at Rest),
- používané dáta (angl. Data in Use).

DLP riešenia majú za cieľ ochrániť uvedené tri typy dát, a tým dosiahnuť celkovú ochranu pred únikom citlivých informácií. Ku každému z troch uvedených typov pritom logicky pristupujú diferencovane. V prípade prenášaných dát pracujú DLP riešenia na úrovni monitorovania sieťovej komunikácie (a to najmä protokolov HTTP, SMTP, IMAP, Instant Messaging). V prípade uložených dát analyzujú najmä dáta nachádzajúce sa na zdieľaných úložiskách (napr. zdieľané disky, MS SharePoint, relačné databázy). V prípade používaných dát DLP riešenia analyzujú činnosti koncových používateľov na ich pracovných staniciach.

DLP riešenia identifikujú citlivé informácie podľa zadefinovaných pravidiel. V praxi môže ísť o vyšpecifikované kľúčové slová, regulárne výrazy popisujúce rodné čísla alebo čísla kreditných kariet, prípadne o celé vzorky dát (napr. obsah tabuľky zamestnancov z personálnej databázy).

Po identifikovaní citlivých informácií a stanovení kontextu DLP riešenia, v závislosti od konkrétneho typu dát, vykoná DLP systém špecifickú činnosť, ktorá zabezpečí ochranu pred nežiaducim únikom citlivých informácií. Príkladom takejto činnosti v danom kontexte môže byť zablokovanie odoslania e-mailu, ak sa v ňom nachádzajú citlivé informácie o zamestnancoch (typ dát: prenášané dáta). Ďalším príkladom môže byť automatické odoslanie e-mailu na oddelenie informačnej bezpečnosti, ak sa používateľ pokúsi skopírovať citlivé zdrojové kódy na USB kľúč (typ dát: uložené dáta). Príkladom pre uložené dáta môže byť tiež situácia, ak sú citlivé informácie uložené priamo na zdieľanom disku v adresári, ktorý je verejne prístupný. V tomto prípade môže DLP riešenie (v súlade s príslušnou bezpečnostnou politikou) tieto citlivé informácie zmazať.

Ďalšie služby

Pri úvahách o nasadení DLP riešenia sa často zvažuje vzťah DLP riešení k podobným (prípadne konkurenčným) technológiám. Ide najmä o technológie detekcie prienikov označované ako IDS (z angl. Intrusion Detection System) a IPS (z angl. Intrusion Prevention System), prípadne technológie ochrany práva označované ako DRM (z angl. Digital Right Management). Spoločnosť TEMPEST poskytuje svoje služby aj v týchto oblastiach.

Technológie IDS/IPS sa zameriavajú na analýzu premávky na nižšej sieťovej úrovni so zameraním na vysokú priepustnosť. DLP riešenia sa zameriavajú na analýzu sieťovej premávky na úrovni e-mailovej a webovej komunikácie, pričom je implementované naviazanie vyhodnocovacích pravidiel na obchodné procesy organizácie (napr. schválenie odoslania e-mailu nadriadeným). Technológie DRM sú ponúkané najmä pre najrozšírenejšie formáty dokumentov od spoločností Microsoft a Adobe. Nasadenie technológie DRM predpokladá aktívnu spoluprácu koncových používateľov pri definovaní úrovne citlivosti konkrétnych dokumentov a nastavovaní príslušných prístupových pravidiel. Naproti tomu DLP riešenie vo väčšine prípadov nevyžaduje súčinnosť koncových používateľov a interakcia môže prebehnúť až pri zistení úniku citlivých údajov.

Spoločnosť TEMPEST má v oblasti DLP skúsenosti s produktmi od spoločností Symantec, Websense a RSA (The security division of EMC).