CO ZNAMENÁ DLP

DLP je zkratka dvou termínů. Jedním z nich je Data Loss Prevention a druhým je Data Leak Prevention či Data Leakage Protect. Ať si vybereme kterýkoli z popisů, všechny zahrnují stejnou vlastnost - tou je možnost uchránit společnost před únikem dat. Jeden příklad výzkumu - tři čtvrtiny uživatelů odnáší každý týden mimo firmu až 10 dokumentů na přenosných zařízeních. Ve většině případů jsou data zcizena, případně zneužita vlastními zaměstnanci. Ti mají k datům v rámci plnění svých povinností naprosto legitimní přístup. Dokonce i společnosti, které řídí přístup k datům na principu need to know, citlivá data šifrují, auditují a vyhodnocují veškeré činnosti uživatele v systému, jsou tomuto riziku vystaveny.

Hlavní přínos DLP

DLP je technologie, která si najde své místo jak v malých firmách, tak obrovských korporacích, které si uvědomují cenu svých dat v elektronické podobě. Ztráta dat souvisí nejen s obnovou dobrého jména společnosti, obnovením důvěry zákazníků, poklesem akcií, finančními dopady, ale také s náklady na bezpečnostní řešení incidentů a kroků vedoucích k omezení jejího dalšího výskytu. DLP nabízí proaktivní ochranu, a to nejen pro úmyslné pokusy o odcizení dat, ale také proti lidským omylům, které tvoří drtivou většinu úniku citlivých informací.

Systém pod kontrolou

Technologie DLP umí pracovat často ve více místech v prostředí sítě. Pracuje jako agent nasazený na koncových klientských stanicích, na serverech. Může být nasazen na kontrolu databází, souborových serverů a může být nasazen na kontrolu síťového provozu (Network DLP). Nasazení DLP umožní mj. splnit některé požadavky GDPR (nařízení EU), jako je:

- zajištění důvěrnosti, integrity, dostupnosti a odolnosti osobních údajů (OÚ)
- zohlednění rizik zpracování OÚ, mezi něž patří např. ztráta, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ
- prokazatelnost, tj. schopnost správce doložit, že zpracování OÚ je prováděno v souladu s GDPR
- vedení záznamů o činnostech zpracování OÚ a další

NASAZENÍ DLP

- Nasazení DLP je závislé na komunikaci se zákazníkem. Ten dodává informace , co považuje za bezpečností incident a jaká data jsou pro něj důležitá.
- Po nasazení DLP softwaru probíhá doba sledování provozu a doladění politik tak, aby nedocházelo k vysokému počtu false-positive incidentů.
- V řadě implementací je DLP řešení nasazeno v monitorovacím módu, kde lze dohledávat úniky a neoprávněné manipulace s daty.
- Přechod do režimu, kde dochází k blokacím akcí, se realizuje postupně v čase po odladění pravidel.

DLP a USB flash

S příchodem USB flash disků - jejich dostatečnou přenosnou kapacitou, rychlostí zápisů, lehkostí zapojení a plnou podporou v operačních systémech - se staly USB flash paměti určitou hrozbou. Jednou hrozbou je návrat virů šířících se přes tato média, ale to je kapitola k jinému produktu. Druhou je právě možnost pohodlně odnášet data ze společnosti ven. S DLP je možné velmi účinně omezit tuto hrozbu, a to bez omezení samotných uživatelů. Politika DLP je schopná některé USB povolit jiné zakázat, z jiných povolit například jen čtení apod.

DLP na hardware

Pomocí technologie DLP lze omezovat přístupy na hardware. Je možné specifikovat povolený HW, a to například dle typu, konkrétního výrobce, modelu či konkrétního sériového čísla. Lze blokovat USB disky, iPod, telefon, a jiné mass storage, CD-R, RW a DVD-R, RW, diskety, bluetooth a IrDA, zobrazovací zařízení, COM a LPT porty aj.

Práce s DLP

V DLP specifikujeme, co je pro nás důležité, co jsou data, která potřebujeme uchránit. Například banka bude kontrolovat, zdali dokumenty, které opouštějí úložiště, neobsahují například čísla kreditních karet. Pojišťovna bude monitorovat popis úrazů, autoservis SPZ apod.

DLP kontroluje, dle pravidel, soubory, se kterými se operuje nejčastěji na klientech a soubory v pohybu na síti (upload souborů, FTP, mail komunikace) a na základě pravidel zajistí akci.

Akcí, kterou DLP nabízí, je například omezení manipulace s daty. Uživatel je sice autorem dokumentu, může jen modifikovat či mazat na své pracovní stanici. Ale například nahrání na flash disk už bude řízeno centrálními pravidly.

Mezi akce, které lze pomocí DLP aplikovat, patří: blokování činnosti, soubor nebude odeslán či nahrán nebo monitoring činnosti. Akce je zaznamenána se specifikací - kdo, kdy, odkud a kam. Případně lze monitorovat pro důkazní řízení, co konkrétně porušilo pravidla (obsah dokumentu, e-mailu, výřez obrazovky). Vždy je možné monitoring provádět v tichosti nebo s upozorněním uživatele, že právě provedená akce byla zaznamenána.

Lze blokovat tisk na libovolnou tiskárnu, takže například účetní oddělení může soubory, které obsahují finanční informace, tisknout jen na konkrétní tiskárně, aby nedošlo k případnému omylu.