

Často opomíjeným faktem bývá ochrana dobrého jména společnosti. Kromě toho, že mohou uniknout citlivá data, mohou ze sítě společnosti odcházet i data, která pak na společnost často vrhnou špatné světlo.

Může se jednat například o zprávy elektronické pošty zaměstnanců, kteří neudrželi své nervy na uzdě, nebo materiály, které konkurence zneužije k poškození společnosti v očích zákazníků či partnerů. Jen těžko lze vyčíslit dopad podobných externalit bezpečnostních incidentů, ale jejich vliv na výsledky společnosti je zřejmý.

Pomocí nástrojů DLP (Data Loss Prevention, Data Loss Protection apod.) lze vynutit politiky nakládání s daty, a přitom není nutné měnit původní procesy a návyky uživatelů. To je také jeden z předpokladů pro úspěšné nasazení technologie ve společnosti. Čím větší interakci uživatele technologie požaduje, tím spíše bude odmítnuta, a výsledkem bude pouze ignorace nebo rozladěnost uživatelů.

Oproti tomu kvalitní DLP nástroj s odladěnou politikou nebude mít na běžnou práci žádný vliv a jeho efektivita ani v nejmenším nebude záviset na úrovni znalosti a proškolení uživatele. Vše je centrálně spravováno, konfigurováno a sledováno.

Kde může DLP pracovat?

Velmi podstatné je umístění DLP funkcionality v rámci sítě. To ovlivní možnosti a omezení na podobném principu jako u ostatních bezpečnostních nástrojů – zde lze použít analogii s nasazením antivirových řešení na stanici a s webovými proxy.

není software nainstalován, nejsme schopni nic kontrolovat). Ideálně tak vychází kombinace obou řešení, která se navzájem doplňují.

Jak DLP funguje?

Hlavním předpokladem pro spolehlivost DLP nástroje je to, že se opravdu dostane k relevantním datům. Je zcela jasné, že veškerá data nebudou uložena v čistě textovém formátu, aby je mohl program bez problémů zpracovat. Proto je jedna z nezbytných funkcí DLP znalost formátů různých souborů a datových struktur. Z těch běžně používaných například dokumenty MS Office nebo různé archivy.

Právě inteligence nástroje ovlivní, jak přesně je organizace schopna definovat politiku a jaká opatření naopak nebude moci definovat. Výraznou pomocí mohou být například připravené slovníky (třeba xenofobní či jinak nevhodná slova, která je nutné blokovat v e-mailové komunikaci) nebo výrazy týkající se různých regulačních nařízení (například jde o čísla kreditních karet, rodná čísla, čísla občanských průkazů atd.), které je možné použít při vytváření vlastních specifických politik.

Kromě nastavení a vynucování politik by mělo DLP nabídnout i detailní reporty a správu jednotlivých případů. Jeden případ může vygenerovat vícero pokusů o porušení politik, ty je pak vhodné sdružovat pod jednou hlavičkou a držet si záznamy o řešení prohřešku, pokud je třeba jej řešit.

Je možné také zaměstnance například informovat o tom, proč nesmí podobný e-mail

daty je prakticky nemožné, proto je zapotřebí hlídat samotný tisk, resp. data, která jsou na tiskárnu zaslána. Kromě lokálních a síťových tiskáren by DLP nemělo zapomínat ani na virtuální.

Častým bezpečnostním opatřením bývá zákaz přenosných médií, hlavně oblíbených USB klíčenek. Pokud je jejich nebezpečí uživatelům pouze vysvětleno, může si být podnik téměř jist, že se taková snaha mine účinkem. Plošný zákaz těchto zařízení zase může znepříjemňovat práci a zdržovat.

Rozumným kompromisem se jeví vytvoření seznamu povolených zařízení (respektive povolit identifikátor výrobce nebo modelu) a blokovat pouze ta ostatní. Přenášená data na tato zařízení mohou být navíc šifrována, pokud zařízení samo o sobě šifrovat neumí.

Kontrola provozu na perimetru sítě

Pro kontrolu zařízení potřebuje organizace jednoznačně DLP nástroje instalované přímo na stanicích, jinak tento dohled není schopna realizovat. Síťové řešení jí ale poskytne jiné výhody, a to hlavně na perimetru sítě, ve spolupráci s již zavedenými proxy.

Pokud je podnik schopen zajistit, že veškerý webový a e-mailový provoz musí být přenášen přes proxy, pak není problém právě v tomto místě provoz kontrolovat, resp. nechat proxy konzultovat s DLP systémem odchozí provoz. Pokud navíc organizace může prozkoumávat i SSL provoz, pak lze jednoduše kontrolovat veškeré HTTP požadavky, a to i z koncových bodů, na kterých DLP není z nějakého důvodu nainstalováno. To stejné pak platí pro e-mailový provoz.

Jak poznat kvalitní DLP nástroj?

Systémy DLP se postupně prosazují a zájem o podobná řešení roste. Tento trend ale přilákal velké množství výrobců, kteří své narychlo představené produkty nazývají DLP. Chlubí se obrovským množstvím vlastností, ale je třeba produkt prozkoumat do hloubky a přesvědčit se, co v podání kterého výrobce znamená například kontrola e-mailové komunikace, přenosných zařízení, centrální správa atd.

Většinou se totiž v jejich případě naneštěstí jedná pouze o velmi povrchní funkce, které neumožňují opravdovou práci s daty. Z kontroly e-mailové komunikace se vyklube pouze kontrola odesílatele a adresáta, z kontroly přenosných zařízení pouze možnost je globálně povolit nebo zakázat.

Autor pracuje jako IT Security Consultant ve společnosti Comguard.

Řešení od McAfee

Pokud bych měl vybrat opravdu komplexní řešení, zaměřil bych se v současné době na společnost McAfee, která získala velký náskok před konkurencí díky akvizici společnosti Reconnex v roce 2008. Ta byla zaměřena čistě na síťové DLP řešení.

McAfee již delší dobu nabízí DLP řešení na koncové body (Host Data Loss Prevention), které je kompletně integrováno do centrální správy ePolicy Orchestrator. Řešení, které vychází z původního nástroje společnosti Reconnex, nazvalo McAfee jako Network Data Loss Prevention a je již také integrováno do centrální správy, navíc komunikuje i s Host DLP.

Propojením velmi kvalitního síťového i host řešení (společnost Gartner obě řešení zvláště umístila do Leader kvadrantu) přes centrální správu posunulo McAfee technologii DLP o krok dále. Doufáme, že konkurence McAfee neztratí dech a vývoj DLP technologií bude dále postupovat.

Robert Šefr, Comguard

Pokud se podnik rozhodne použít zařízení na perimetru sítě, získá výhodu kontroly nad kompletním příchozím i odchozím provozem, ale není schopen pokrýt ostatní vektory (přenosná paměťová zařízení nebo notebook zaměstnance na služební cestě).

Tyto problémy eliminuje kontrola přímo na koncových bodech, ale ta nemusí být všude možná (nepodporované systémy) nebo nemusí být důsledně vynucována (pokud

odesílat, nebo zjistit, jak se dostal k nějakému typu dokumentu. Záznamy také organizaci mohou pomoci najít „false positives“, podle kterých lze politiku dále ladit, zpřesňovat a eliminovat další falešné poplachy.

Kontrola zařízení

Kontrolou zařízení nejsou myšlena pouze přenosná paměťová média, ale důležitou roli hrají i tiskárny – mít dohled nad vytištěnými