



Redakční otázky k tématu "DATA LOSS/LEAK PREVENTION" na ICT SECURITY

Jak účinně řešit DLP na firemní úrovni

Autor odpovědí:

Robert Šefr, IT Security Consultant, COMGUARD a.s.

1) Jak nejjistěji detekovat únik dat?

Samozřejmostí je pokrytí hlavních komunikačních kanálů jako je email, web a ftp. Monitorován je pouze odchozí provoz, aby nedocházelo k plýtvání prostředků. Šifrování, které má sloužit k ochraně dat, se paradoxně stává při monitorování dat problémem. Analýzu šifrovaných dat (např. https) lze provádět na specializovaných proxy, které mají přístup k vlastnímu obsahu komunikace a mohou jej konzultovat se specializovaným DLP zařízením. Podobné principy platí i pro další protokoly. Pokud nejsme schopni komunikaci dešifrovat (např. email zašifrovaný pomocí PGP), zbývá nám pouze možnost ji úplně blokovat.

Síťové řešení však nepokrývá zdaleka všechny vektory úniku dat. Druhým přístupem je distribuce DLP řešení přímo na koncové stanice. Tak můžeme monitorovat používání přenosných datových úložišť, monitorovat citlivé informace před pokusem o jejich zašifrování, pozměněním nebo dokonce monitorovat data na stanicích i mimo podnikovou síť (např. zaměstnanci na služební cestě). Agent na koncové stanici poskytne díky tagování úplnou kontrolu nad definovanými citlivými daty, ať je pokus o jejich další neoprávněné šíření jakýkoliv. Toto řešení je ale zcela závislé na důsledné distribuci a monitorování DLP softwaru. Pokud není software na stanici nainstalován (nebo z nějakého důvodu nefunkční) nemáme nad data a jejich pohybem žádnou kontrolu.

Obě řešení mají svoje slabá místa, ale navzájem se velmi vhodně doplňují. Nejjistější detekce dat je tedy zajištěna kombinací DLP síťového i na stanicích.

2) Jakým způsobem nejlépe třídít a katalogizovat data, abychom je mohli adekvátním způsobem chránit?

Definice některých citlivých dat jsou natolik globální, že se o ně nemusíme příliš starat a obdržíme je s každým kvalitním DLP systémem. Příkladem mohou být čísla kreditních karet. Většina společností nebude chtít, aby od nich taková data odcházela. Několik regulárních výrazů se postará o identifikaci takových údajů a stejné regulární výrazy může použít jakákoliv společnost na světě. Obtížnějším problémem ale bude identifikace citlivých dat se strukturou charakteristickou pro konkrétní společnost.

Ať již se jedná o smlouvy, zdrojové kódy, osobní informace nebo jiné důvěrné dokumenty, těžko pro ně budeme vytvářet regulární výrazy. Pro tyto dokumenty musíme použít sofistikovanější metody, které budou schopné porovnávat obsah nejen jako celek, ale i po částech. Výsledkem porovnání částečně upraveného dokumentu s původním bude procentuelní shoda, na základě které se můžeme rozhodnout, jakou akci uplatnit. Celý systém si můžeme představit jako internetový vyhledávač, který indexuje webové stránky.

Na rozdíl od internetového vyhledávače ale nechceme indexovat každý dokument, ale pouze vybrané skupiny. Nasměrováním indexovacího stroje na



některá síťová úložiště zařídíme, že budeme indexovat pouze vybrané typy dokumentů. Každé (takto indexované) úložiště by mělo sdružovat dokumenty s podobnou úrovní důvěrnosti. DLP systém využívající agenty naopak umožňuje nastavit politiky i dle aplikací, tj organizace může jednoduše určit typy aplikací (například ERP, CRM apod.) a oprávněné toky dat přes oprávněné uživatele, nebo skupiny uživatelů (i s využitím například Active Directory). Díky již zmíněnému tagování jsou tato data identifikována i přes různé snahy o zašifrování, modifikaci apod.

3) Nakolik je ochrana před úniky dat otázkou technickou a nakolik administrativní/organizační?

Z technického hlediska jde hlavně o výběr mezi DLP na koncové stanice nebo síťovým (optimálně kombinace obojího). Výběr nástroje zcela zásadním způsobem ovlivní možnosti při stanovování politik a úspěšnost při nasazení do společnosti. Výsledek výběru špatného nástroje může být nedokonalá politika (protože DLP nástroj nemá dostatek možností) a nespokojenost uživatelů (omezování v práci, nestabilita, negativní vliv na výkon, atd.). Výsledek nasazení takového systému bude spíše kontraproduktivní.

Samotný DLP systém je ale „pouze“ nástroj, který sám o sobě před únikem dat neochrání. Výběr nástroje samozřejmě ovlivní, jaké možnosti budeme v ochraně dat vůbec mít, ale zásadním (a nejobtížnějším) krokem je stanovení politiky. Management společnosti musí identifikovat, jaká data mají být chráněna a jakým způsobem. Tato práce vyžaduje spolupráci více oddělení ve společnosti a může být velmi obtížná. Společnosti si často ani neuvědomují, jaká data mají chránit nebo proč.

Úspěch v ochraně dat je tedy výsledkem výběru kvalitního nástroje a stanovení kvalitní politiky. Podcenění jedné ze složek povede k celkovému neúspěchu.

4) Co je podle vás největší překážkou rozšíření kvalitních DLP technologií?

Často to bývá podceňování vážnosti úniku dat. To je ovšem častý problém bezpečnosti informačních a komunikačních technologií obecně. Navíc ještě donedávna byly DLP technologie považovány za sezónní záležitost. DLP technologie jsou ale již za svým vrcholem na „hype křivce“ a potvrzují svou praktickou použitelnost a přínos.

Další překážkou může být málo hmatatelný přínos této technologie. Správně nasazený DLP systém se postará o omezení bezpečnostních incidentů. Důkazem důležitosti a použitelnosti DLP pro management může být souhrnný report o zablokovaných (nebo zaznamenaných) incidentech, které by bez DLP prošly bez povšimnutí.

Častým omylem také bývá, že hlavním smyslem DLP je zabránit cíleným útokům. Velká většina úniků dat je způsobena neúmyslně (email odeslaný na špatnou adresu, ztráta flash disku, tisk dokumentů pro práci doma, atd.). DLP se správně nastavenou politikou zvládne takovéto úniky zastavit (případně monitorovat). V případě sofistikovaného útoku, kdy se některý ze zaměstnanců snaží data odcizit, nemusí DLP systém přímo uspět, ale soustavné snahy o



vynesení důvěrných dokumentů vygenerují velké množství záznamů v logu. Takto nápadné množství incidentů je zřetelně určí pokus o vynesení dat.

5) Která technologie v oblasti DLP by rozhodně neměla uniknout naší pozornosti?

Aktuálně se stalo nejúplnější řešení společnosti McAfee. Nabídka této společnosti zahrnuje jak řešení na stanice (Host DLP), tak síťové DLP (Network DLP) sestávající ze tří sond „Discover“, „Monitor“ a „Prevent“, které obohatily portfolio McAfee díky akvizici společnosti Reconnex (Leader Magic Quadrantu podle společnosti Gartner) v roce 2008. McAfee takto umí nabídnout dvě plnohodnotná řešení, která lze navíc společně integrovat do ePolicy Orchestrator.

McAfee NetworkDLP Reconnex umí navíc pracovat jako ICAP a SMTP server. Lze přes něj tedy filtrovat webový a emailový provoz z proxy serverů. Kromě toho nabízí velmi pokročilou indexaci dat z rozličných síťových úložišť.

Host DLP řešení umí sledovat USB zařízení, tisk, snímání obrazovky, schránky, síťovou komunikaci, atd. Správa politik pro Host DLP je plně integrováno do centrální správy McAfee ePolicy Orchestrator, což zaručuje úplnou kontrolu nad všemi stroji ve společnosti a tedy nejvyšší efektivitu ochrany proti úniku dat.