

DLP – Data Leak Prevention

A DLP napjaink slágertémája, azonban már abban sincs konszenzus az egyes piaci szereplők között, hogy mint jelent ez a három betű. A számtalan névfeloldási lehetőség közül a Websense azt választotta, amely a leginkább fókuszál az információra és a megelőzésre. A Gartner, az IDC és a Forrester által egyaránt vezetőnek minősített technológia ugyanis nem állományokra koncentrál, hanem az információra, legyen az bármilyen formában tárolva vagy továbbítva.

A PreciseID technológia

A Websense DLP-megoldásának egyik alapköve a PreciseID technológia, mely egyedülálló pontossággal ismeri fel az információt. Legyen szó egy adatbázisról, melynek egyes rekordjait meghatározott számú mezőből ismerjük fel, vagy egy szöveges dokumentumról, melyből csak egyetlen bekezdést próbálnak elküldeni, a PreciseID nagy pontossággal ismeri fel a véletlenül vagy szándékosan kiszivárogtatott információt. Több konkurens megoldástól eltérően nem az állományokat jelöli meg, hanem az információt indexeli, így akár újragépelés vagy nyomtatás esetén is biztos felismerést nyújt.

Szabályrendszer

A Websense Data Security Suite-nál az információ van a középpontban. Az információ paramétereire alapján határozhatók meg a szabályok, így előírhatjuk, hogy mire és milyen információra vonatkozzon egy szabály, mely címzettnek és milyen csatornán közlekedő adatot szeretnénk vizsgálni. A szabályrendszer alapján eldönthető, hogy egy információ kijuthat, csak naplózva legyen, karanténozzuk vagy teljesen blokkoljuk. Ezen rugalmas szabályrendszer biztosítja, hogy a DLP rendszer alkalmazkodjon az üzleti folyamatokhoz, és ne az utóbbit kelljen átalakítani a megoldást kedvéért.

Who	What	Where	How
Human Resources	Source Code	Benefits Provider	File Transfer
Customer Service	Business Plans	Internet Auction	Web
Marketing	Employee Information	Business Partner	Instant Messaging
Finance	M&A Plans	Blog	Peer-to-Peer
Accounting	Patient Information	Customer	Email
Sales	Financial Statements	Spyware Site	Network Printing
Legal	Customer Records	North Korea	
Technical Support	Technical Documentation	Competitor	
Engineering	Competitive Information	Analyst	



A Websense DSS architektúra

A Websense Data Security Suite több modulból épül fel, melyek egymástól külön, de együttműködve üzemelnek. Lehetőség van arra is, hogy lépésről lépésre alakítsuk ki a DLP infrastruktúrát, így nem szükséges hatalmas beruházásra vállalni elkötelezettséget, bizonytalan célokat kitűzve egy sok hónapos vagy éves projectben. Kezdetben akár csak monitorozással, majd később lépésről lépésre blokkolva a bevezetés lépcsői előre tervezhetők. Az alacsonyabb kockázat, a kisebb kezdeti beruházás biztosítja, hogy a DLP ne csak beszédtema legyen, hanem sikeres projecteket lehessen megvalósítani.

A Websense DSS az alábbi pontokon épül be a rendszerbe:

adatbázis-szerverek

Bármely ODBC-kapcsolattal rendelkező adatbázis-szerverben található információ indexelhető, illetve a Websense DSS által lefedett bármely ponton felismerhető az innen szivárgó információ

file és SharePoint szerverek

A file- és SharePoint szervereken tipikusan a könyvtárstruktúra alapján határozzuk meg a biztonsági klasszifikáció szintjeit, az itt tárolt információt indexelve biztosítható a későbbi felismerés.

nyomtatószerverek

A nyomtatószervereken OCR-technológiával ismerjük fel a nyomtatandó információt, a unicode rendszer segítségével nyelv- és karaktertípustól függetlenül.

web- és e-mail átjárók

A Websense Data Security Suite integrálódik a Websense webtartalom-szűrő és e-mail tartalomszűrő termékeivel, ezen csatornákat is egyedülálló hatékonysággal kontroll alatt tartva.

tetszőleges hálózati szegmens

A Websense Data Protect modul bármely hálózati szegmensbe telepíthető egy önálló szerverre, mely snifferként az adatfolyamot megfigyelve vagy bridge-ként abba láthatatlanul beépülve a hálózat tetszőleges pontján képes védelmet nyújtani.

végpont (PC-k, notebookok)

Bizonyos tevékenységeket (vágólap, titkosított protokollok (pl Skype), CD-DVD írás, pendrive-ok és egyéb csatlakoztatott perifériák ellenőrzése) kizárólag a végponton lehetséges felderíteni vagy meggátolni, mely a Data Endpoint modul segítségével történik.

Az Ön viszonteladója: