

M Magazine II.08



ATTUALITÀ

"Data Leakage Protection: l'evoluzione dell'Anti-X" di Dario Forte

DLP: l'evoluzione dell' "Anti-X"

La Data Leakage Protection sembra essere una tendenza del mercato attuale della sicurezza informatica. In questo articolo cercheremo di analizzare se si tratta di un semplice strumento, ideato dai Vendors di Antivirus, per aumentare le vendite oppure una vera necessità.

Con il termine "Anti-X" si intende l'insieme delle soluzioni destinate alla prevenzione e alla detection/cleaning di qualsiasi agente negativo presente su una determinata macchina. Una parte di queste soluzioni specifiche operano anche prevenendo l'entrata di questi agenti, comunemente indicati con il termine malware.

Sono molti i produttori che, direttamente o a mezzo di acquisizioni mirate, hanno deciso di entrare in questo mercato, ottenendo due differenti risultati:

- a) l' Anti-X è ormai diventato una commodity;
- b) il cliente è più interessato ad abbattere i costi piuttosto che ad ottenere un rendimento tecnico finalizzato all'efficacia.

Per questo, i vendor hanno deciso, ormai da un paio d'anni, di concentrarsi sulla prevenzione di atti aziendali non conformi alle politiche di sicurezza interne. Stiamo parlando evidentemente di violazioni "from inside", che di solito generano fughe e perdite di informazioni riservate.

Da qui, il termine "Data Leakage", che necessita di una protezione avanzata, possibilmente gestibile in maniera centralizzata.

Le soluzioni DLP, infatti, sono destinate a prevenire la fuoriuscita di informazioni riservate, sia attraverso i canali trasmissivi convenzionali (outbound), sia attraverso dispositivi negati per policy, quali le chiavi USB, gli ipod e via dicendo e, last but not least, fuoriuscite causate da malicious code. Chi conosce le problematiche sopra citate, soprattutto negli ambienti molto popolati, si rende conto della difficoltà di coprire tutto lo spettro dei dati strutturati e non. Si tratta di concetti, infatti, che ricordano vagamente quelli del DRM espressi ormai cinque anni fa, la cui gestione difficile è stata poi la causa del fallimento. Tuttavia il trend è quello di un miglioramento.



SECURITY

Nel presente articolo valuteremo come un progetto DLP può essere vincente e proveremo a porci alcuni interrogativi sui risvolti strategici di una scelta tecnologica, sia dal punto di vista del fornitore che da quello del cliente.

Dunque, i primi Vendor ad essere entrati nel mercato sono stati i produttori di Antimalware, approfittando, dal punto di vista tecnico, dell'agente antivirale (che hanno provveduto ad espandere in termini di funzionalità) mentre, dal punto di vista commerciale, sono stati in grado di spalmare i costi aggiuntivi di sviluppo annegandoli all'interno di una base installata già esistente.

Invece, per il cliente, avere una relazione consolidata con un vendor potrebbe favorire l'ingresso di una soluzione DLP come mera feature aggiuntiva. Ciò dovrebbe dare la possibilità di abbassare i tempi di approvvigionamento e, contestualmente, migliorare i tempi operativi e di prevenzione degli attacchi. Questo tipo di ragionamento è maggiormente applicabile in quelle aziende dove la sicurezza informatica è di ratio tattica.

Il fatto di affidarsi allo stesso fornitore degli "Antivirus", non è proprio delle aziende che guardano alla sicurezza da una prospettiva strategica. Queste ultime, infatti, pur vedendo facilitata la trattativa commerciale con un fornitore già esistente, hanno l'esigenza comunque di ottenere un risultato ottimale, che prescindano dal business e si concentri anche sulla qualità e sui risultati.



Dario Forte, CFE, CISM, si occupa di sicurezza dal 1992 ed è Founder and CEO di DFLabs. Docente di Gestione degli Incidenti informatici all'Università di Milano, ha lavorato con NASA, Esercito Americano e Governo Italiano. Ha pubblicato nove libri e circa trecento articoli in Italia, Usa, Sudamerica e Asia. www.dflabs.com

Guardando allo scenario sopra descritto, da un punto di vista puramente strategico, possiamo individuare la presenza di fornitori già affermati presso i clienti tattici (la maggior parte delle aziende italiane) una barriera implicita di ingresso per i vendor che si stanno specializzando su soluzioni DLP innovative che però vengono viste con una certa riluttanza specialmente per questioni di branding. Questo fenomeno, da un lato, limita il business dei fornitori più piccoli e, dall'altro, facilita le operazioni di acquisizione da parte dei "pesci grossi".

È accaduto alla maggior parte dei Vendor affermati e, d'altro canto, non ci si poteva aspettare altrimenti.

Overview tecnologica

Dal punto di vista tecnologico esistono due tipologie principali di DLP: Client/host Based e Network Based. Le prime prevedono, di fatto, delle installazioni a livello agent (così come descritto nei paragrafi precedenti) mentre le seconde asseverano ad un paradigma noto come Activity Audit Lifecycle, che prevede il monitoraggio di porzioni del traffico con conseguente segnalazione di violazione policy. La soluzione ottimale sarebbe quella di coordinare un bilanciamento tra i due modelli, che potrebbe creare dei potenziali spunti di riflessione sul modello di technology governance. A questo punto, verrebbe spontaneo porsi delle domande:

1. quale modello adottare? Un modello ibrido (lo abbiamo appena detto) può essere la soluzione ottimale. D'altro canto i costi di progetto potrebbero aumentare a causa della necessità di effettuare alcuni studi di fattibilità di tipo legale e di risk management. Il modello Host/agent based, infatti, dovrebbe fornire la possibilità di gestire un livello minimo di prevenzione, senza per questo dover estendere il tavolo decisionale ad un numero troppo elevato di persone, che, ovviamente, allungerebbe i termini di delivery. D'altro canto, la scelta di un modello network based dovrebbe fornire uno strumento in più svincolato dagli agenti e, di conseguenza, garantire una maggiore trasparenza e potenza nell'ispezione del traffico potenzialmente malicious.
2. A chi affidarsi? Di solito è consigliabile effettuare uno studio di fattibilità indipendente ed individuare ogni possibile impatto

sulla security Governance. Lo studio sarà multilivello e relativo a più parti dell'architettura. Solo dopo il suo esito sarà possibile operare una scelta a livello di fornitore, stabilendo una serie di obblighi contrattuali, necessari anche per il risultato.

Varie ed eventuali

Ci sono poi dei fattori di cui bisogna tener assolutamente conto. In un progetto di DLP, infatti, il numero di persone interessate per analisi e delivery può risultare alto, e in generale una failure se non viene rigorosamente controllato. Di solito, l'obiettivo si raggiunge con un forte e visibile commitment della Direzione Generale, unito ad cooperazione e continua comunicazione tra i vari settori della sicurezza. Ciò detto, i vantaggi sono molti anche in termini di raccordo tra funzioni aziendali, non solo IT. Questi ultimi aspetti sembrano lontani dal field che stiamo discutendo in questo articolo, ma l'esperienza diretta sul campo suggerisce di guardare alla loro globalità per evitare inutili esposizioni legali al primo incidente di sicurezza.

Conclusioni

Per fortuna sono in aumento i manager lungimiranti che capiscono l'importanza di proteggere le Informazioni visto che queste scorrono fra reti business e sistemi dove sono esposte ad accessi non autorizzati, abuso o negligenza; i management sono consapevoli che da incidenti gravi successi alle informazioni classificate può risultare l'inadempienza di leggi e norme. A parere di molti, oltre ad avere le incombenze normative, le aziende, che hanno ormai tutti gli strumenti tecnologici disponibili per prevenire gli abusi, dovrebbero ricevere multe, anche se non hanno subito un incidente. Le norme giuridiche sono in fase di miglioramento e continueranno a migliorare, fenomeno che prende il nome di information security nelle aziende. Sono troppe le organizzazioni che non implementeranno security se non saranno forzate dalla legge; molte, soprattutto nel tessuto medio, non considerano necessari i costi per information security. E' una triste verità che gran parte delle organizzazioni non vogliano investire nella security senza essere forzati a farlo. Il DLP, forse, potrà contribuire al doppio scopo della prevenzione delle fughe di dati e, contestualmente, al raggiungimento di un buon livello di compliance.