]HackingTeam[| ELDOR CORPORATION

Proposte per attività in tema DLP (Data Loss Prevention)

Orsenigo

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	Aprile 2008	Prima emissione
1.1	Aprile 2008	Aggiunta tabella stima effort interno

INFORMAZIONI		
Data di Emissione	Aprile 2008	
Versione	1.1	
Tipologia Documento	Allegato tecnico ad offerta	
Numero di Protocollo		
Numero Pagine	7	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Costantino Imbrauglio	
Approvato da	Gianluca Vadruccio	

INDICE

1 Introduzione 4
2 DLP (Data Loss Prevention) 5
2.1 Network DLP 5
2.2 Host based DLP 5
3 Proposta....6

1 Introduzione

Il Gruppo ELDOR ha ravvisato la necessità di introdurre un insieme di contromisure volte a ridurre il rischio informatico. Parte delle contrmisure sono di natura tecnologica e parte di natura organizzativa.

Oggetto del presente allegato tecnico è la formulazione di un insieme di proposte mirate alle contrmisure di natura tecnologica. In particolare verranno prese in considerazione contromisure in area DLP (Data Loss Prevention)

2 DLP (Data Loss Prevention)

DLP è acronimo per Data Loss Prevention. Questo termine fa riferimento a un insieme di tecnologie volte a individuare e prevenire la trasmissione, la copia e/o il trasferimento non autorizzati di informazioni riservate.

E' possibile distinguere tra due distinte tipologie di soluzioni DLP:

- Network DLP
- Host based DLP

2.1 Network DLP

Si tratta di contromisure posizionate sulla rete dell'organizzazione e mirate all'analisi del traffico di rete al fine di intercettare la trasmissione non autorizzata di informazioni riservate. L'analisi e la decodifica in tempo reale del traffico di rete è un'attività che richiede risorse di calcolo particolarmente elevate (i documenti in transito sono frammentati, codificati e mescolati ad altre informazioni in transito). Conseguentemente le soluzioni di *Network DLP* si appoggiano a tecnologie che catalogano e classificano le informazioni *a riposo* ovvero quando sono memorizzate su file system o all'interno di database. Le informazioni classificate come riservate vengono dapprima analizzate a riposo e di esse viene calcolato il cosidetto *fingerprint* (impronta). Una volta che è disponibile una base dati delle impronte associate alle informazioni riservate dell'organizzazione è possibile analizzare in tempo reale il traffico di rete e verificare se le suddette informazioni siano in transito.

2.2 Host based DLP

Queste contromisure sono installate direttamente sulle postazioni di lavoro utente e/o sui server dipartimentali. Come nel caso precedente esse sono in grado di intercettare la trasmissione non autorizzata delle informazioni riservate, ma, oltre a ciò, permettono il controllo dei servizi di posta elettronica e/o di *instant messaging*.

Un ulteriore vantaggio di queste soluzioni è rappresentato dalla possibilità di controllare l'accesso e l'impiego di dispositivi esterni di copia e storage (unità di memorizzazione di massa esterni quali dischi usb, chiavette usb, masterizzatori, ecc.)

3 Proposta

Si propone l'adozione di una soluzione DLP completa ovvero una soluzione che abbini sia tecnologie Network DLP sia tecnologie Host based DLP. Per quanto riguarda in particolare queste ultime, i sistemi coinvolti saranno:

- N. 15 Server
- N. 10 Client CAD
- N. 40 Client Notebook

L'architettura generale della soluzione DLP è presentata in figura.

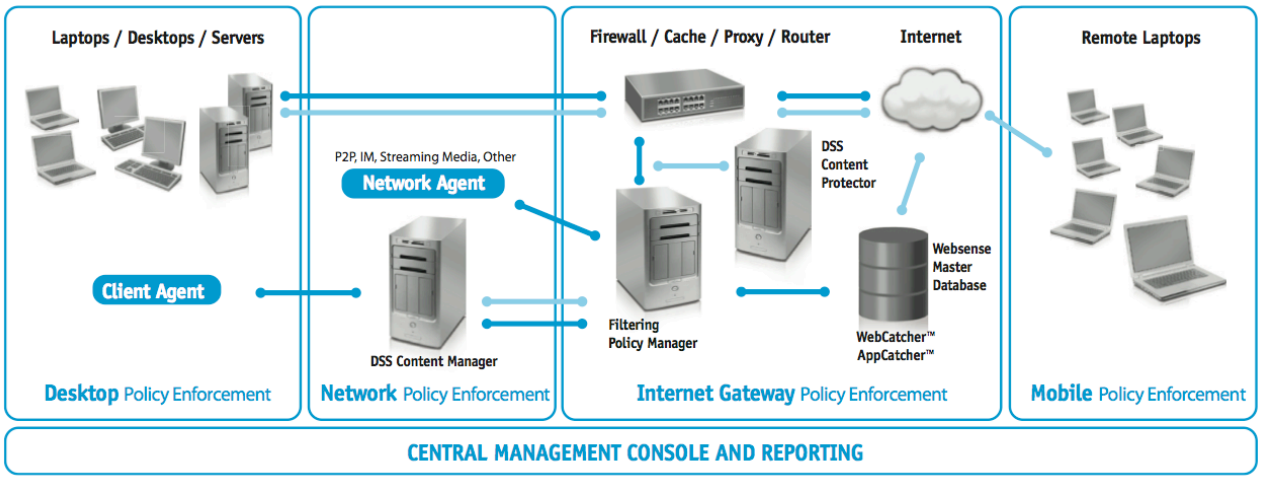

Figura 1 - Architettura generale soluzione DLP

L'attività consta delle seguenti fasi:

- Individuazione e classificazione delle informazioni
- Formalizzazione delle politiche di controllo (sia in ottica di auditing e ricostruzione degli incidenti sia in ottica di prevenzione)
- Configurazione e set-up della piattaforma DLP:
  - Configurazione e set-up della componente DSS Content Manager
  - Configurazione e set-up delle seguenti componenti:
    - Filtering Policy Manager
    - DSS Content Protector
    - Master Database

- N. 1 Agent per tipo di server
- N. 1 Agent per tipo di client cad
- N. 1 Agent per tipo client notebook

L'architettura DLP richiede la disponibilità di due distinti server (uno con funzionalità di network traffic analyzer e l'altro con funzionalità di management e policy server). I server in questione non sono oggetto della presente offerta e ne viene data per scontata la disponibilità da parte dell'organizzazione.

L'attività è quantificata in 20 gg./uomo.

La tabella seguente dettaglia analiticamente la stima dell'effort per ciascuna fase con riferimento all'impegno di affiancamento del personale interno del Gruppo ELDOR.

Tabella di stima dell'effort		
Attività	**Stima effort**	**Stima affiancamento**
Individuazione e classificazione delle informazioni	2	2
Formalizzazione delle politiche di controllo (sia in ottica di auditing e ricostruzione degli incidenti sia in ottica di prevenzione)	10	da 2 a 3
Configurazione e set-up della piattaforma DLP	8	da 4 a 5

Tabella 1 - Tabella di stima dell'effort