Data Loss Prevention

Proposta per attività di analisi

Milano

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	6 ottobre 2008	Prima emissione

INFORMAZIONI		
Data di Emissione	6 ottobre 2008	
Versione	1.0	
Tipologia Documento	Allegato tecnico all'offerta	
Numero di Protocollo		
Numero Pagine	9	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Costantino Imbrauglio	
Approvato da	Roberto Banfi	

INDICE

1 Introduzione

Il presente documento è da intendersi quale allegato tecnico all'offerta per un'attività di analisi preliminare in tema di Data Loss Prevention (di seguito indicata con l'acronimo DLP).

In particolare verrà presentata la metodologia seguita da HT srl per l'implementazione di opportune contromisure in tema DLP.

2 Metodologia

HT srl è leader nella progettazione e implementazione di contromisure volte alla protezione del patrimonio informativo aziendale. In qesto senso HT srl ha sviluppato e propone una propria metodologia che affronta il suddetto problema attraverso l'introduzione di opportuni meccanismi di controllo operanti su tre distinti livelli: organizzativo, operativo e tecnologico.

La metodologia proposta prevede le seguenti fasi:

- Valutazione del rischio
  - Analisi del modello organizzativo aziendale
  - Caratterizzazione del sistema (asset analysis)
  - Analisi dei macrodati e analisi d'impatto
- Definizione dell'architettura DLP:
  - Definizione del numero e del tipo di sonde e relativo posizionamento
  - Definizione delle policy di sicurezza in tema DLP
  - Definizione delle modalità di audit
  - Configurazione delle sonde e del policy server
  - Reportistica

2.1 Valutazione del rischio

L'attività di valutazione del rischio è il primo passo nel processo di governo del medesimo e mira a determinare l'estensione delle minacce potenziali nonché il rischio associati ad una infrastruttura IT. L'output di questo processo aiuta ad identificare gli opportuni controlli per ridurre o eliminare il rischio nella fase di mitigazione del medesimo (vedi sezioni successive).

> ***Definizione*** *– Si definisce rischio (R) il prodotto scalare tra la gravità (G) delle conseguenze che un evento pericoloso determinerebbe e la probabilità (P) che tale evento pericoloso (minaccia) si realizzi.*

$$R = G * P$$

Per determinare la probabilità che si verifichi un futuro evento negativo è necessario analizzare le minacce che incombono su una infrastruttura IT nonché le vulnerabilità potenziali e i meccanismi di controllo posti in essere sull' infrastruttura medesima.

L'attività di identificazione del rischio consta delle seguenti fasi:

- Analisi del modello organizzativo aziendale
- Caratterizzazione del sistema (asset analysis)
- Analisi dei macrodati e analisi d'impatto

2.1.1 Analisi del modello organizzativo aziendale

In questa fase viene analizzato il modello organizzativo aziendale in termini d funzionigramma. Questa attività è propedeutica a quella di definizione dei macrodati, ovvero alla mappatura dele informazioni utilizzate in seno alle diverse funzioni aziendali.

2.1.2 Caratterizzazione del sistema (asset analysis)

In questa fase vengono identificati i confini del sistema informativo. L'attività di caratterizzazione del sistema stabilisce l'ambito di applicazione dell'attività di identificazione del rischio, definisce i confini delle autorizzazioni operative e fornisce informazioni essenziali per definire il rischio.

2.1.3 Analisi dei macrodati e analisi d'impatto

Operativamente lo scopo di questa fase è la ricognizione e classificazione delle informazioni gestite dal sistema informativo dell'organizzazione, siano esse prodotte e gestite attraverso sistemi informatici o attraverso altri mezzi. Le informazioni sono, in generale, un'aggregazione di dati, ai

quali, singolarmente, potrebbe non essere attribuibile nessun valore. Al termine di questa fase si dovrebbe raggiungere la conoscenza di quali classi di informazioni contengono valore per l'organizzazione e le relazioni esistenti con i dati che le compongono.

In tema di sicurezza delle informazioni e dei sistemi informativi vengono definiti tre obiettivi (per una definizione formale si veda FISMA - Federal Information Security Management Act):

- **Riservatezza –** Ovvero garantire le restrizioni e le autorizzazioni nell'accesso e nella divulgazione delle informazioni nonché i mezzi atti a proteggere la privacy degli individui e la proprietà delle informazioni.

  ("Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information" – FISMA Sec. 3542)

- **Integrità –** Ovvero impedire la modifica o la cancellazione non autorizzate delle informazioni nonché l'autenticità e la non ripudiabilità delle stesse.

  ("Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity" – FISMA Sec. 3542)

- **Disponibilità** – Ovvero garantire l'utilizzo e il tempestivo accesso alle informazioni.

  ("Availability, which means ensuring timely and reliable access to and use of information" – FISMA Sec. 3542)

L'Analisi d'Impatto (IA – Impact Analysis) è un'attività critica volta a comprendere le risorse (asset e/o macrodati) del sistema informativo, le interdipendenze e l'impatto potenziale legato a condizioni di inattività (per una definizione formale si veda NIST SP800-100, "Information Security Handbook: A Guide for Managers, Marzo 2007, Cap. 9).

Lo standard FIPS 199 definisce tre livelli di impatto potenziale (si veda FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems", Febbraio 2004, pag. 2):

- **BASSO (LOW)** – Ove la perdita di riservatezza, integrità o disponibilità può avere un effetto negativo limitato sulle attività o sulle risorse dell'organizzazione ovvero sugli individui che vi operano.

"*effetto negativo limitato"* significa ad esempio che la perdita di riservatezza, integrità o disponibilità può:

- causare un percepibile degrado nella capacità di perseguire gli obiettivi di missione ad un livello e per una durata tali da garantire comunque all'organizzazione l'esecuzione delle funzioni principali, ma a fronte di una percepibile riduzione in termini di efficienza;
- risultare in un lieve danno alle risorse dell'organizzazione;
- risultare in una lieve perdita finanziaria;
- risultare in lievi danni agli individui.

- **MEDIO (MODERATE)** – Ove la perdita di riservatezza, integrità o disponibilità può avere un serio effetto negativo sulle attività o sulle risorse dell'organizzazione ovvero sugli individui che vi operano.

  "*serio effetto negativo*" significa ad esempio che la perdita di riservatezza, integrità o disponibilità può:

  - causare un significativo degrado nella capacità di perseguire gli obiettivi di missione ad un livello e per una durata tali da garantire comunque all'organizzazione l'esecuzione delle funzioni principali, ma a fronte di una significativa riduzione in termini di efficienza;
  - risultare in un danno significativo alle risorse dell'organizzazione;
  - risultare in una significativa perdita finanziaria;
  - risultare in significativi danni ad individui, senza che però ciò si traduca in perdite di vita o gravi lesioni.

- **ALTO (HIGH)** – Ove la perdita di riservatezza, integrità o disponibilità può avere un grave o catastrofico effetto negativo sulle attività o sulle risorse dell'organizzazione ovvero sugli individui che vi operano.

  "*grave o catastrofico effetto negativo*" significa ad esempio che la perdita di riservatezza, integrità o disponibilità può:

  - causare un grave degrado ovvero la totale inibizione nella capacità di perseguire gli obiettivi di missione;

- risultare in un grave danno alle risorse dell'organizzazione;
- risultare in una grave perdita finanziaria;
- risultare in gravi danni agli individui, con perdite di vite o gravi lesioni.

2.2 Definizione dell'architettura DLP

Questa fase comprende le seguenti attività:

- Definizione del numero e del tipo di sonde e relativo posizionamento
- Definizione delle policy di sicurezza in tema DLP
- Definizione delle modalità di audit
- Configurazione delle sonde e del policy server
- Reportistica

Un'infrastruttura DLP mira a proteggere il patrimonio informativo aziendale dai rischi connessi a fenomeni di *information leakage.* A livello architetturale un'infrastruttura DLP è composta da due tipi di entità: il policy server e le sonde.

2.2.1 Definizione del numero e del tipo di sonde e relativo posizionamento

Le sonde analizzano l'accesso e l'impiego delle informazioni da parte delle utenze da tre distinte angolazioni:

- Informazioni a riposo (memorizzate all'interno dei datacenter)
- Informazioni in transito (sulle reti)
- Informazioni in uso (sulle postazioni di lavoro delle utenze)

Di qui l'esistenza di tre distinte tipologie di sonde. Obiettivo della presente fase è dunque quello di definire il numero di sonde occorrenti e il loro posizionamento in seno al sistema informativo aziendale.

2.2.2 Definizione delle policy di sicurezza in tema DLP

Come spiegato nella precedente sezione, la funzione delle sonde consiste nell'intercettazione delle attività che le utenze svolgono sulle informazioni sensibili dell'azienda. Una volta che le suddette attività vengono monitorate, è necessario verificare se esse si configurino come violazioni di specifiche policy di sicurezza aziendale.

Il policy server è la componente di un'architettura DLP in cui vengono codificate le policy di sicurezza aziendali (per quanto attiene all'accesso e al trattamento dei dati sensibili) e avviene la verifica di eventuali violazioni.

In questa fase vengono dunque definite le policy aziendali in tema di protezione dei dati sensibili. Tali policy vengono poi caricate sul policy server che procederà ad analizzare i log record provenienti dalle sonde al fine di identificare eventuali violazioni delle policy medesime.

2.2.3 Definizione delle modalità di audit

Un'infrastruttura DLP può operare in due distinte modalità (non mutuamente esclusive):

- Modalità di monitoraggio
- Modalità di prevenzione

Nel primo caso l'infrastruttura si limita ad analizzare le modalità di accesso e impiego dei dati sensibili da parte delle utenze e a segnalare eventuali violazioni delle policy di sicurezza.

Nel secondo caso l'infrastruttura provvede a intercettare e bloccare le eventuali violazioni dele policy di sicurezza.

2.2.4 Configurazione delle sonde e del policy server

In questa fase si procede alla effettiva configurazione delle sonde e del policy server.

2.2.5 Reportistica

Un corretto processo di governo del rischio è sempre definito come un ripetersi ciclico di due distinte fasi:

- Analisi del rischio
- Riduzione del rischio

La reiterazione ciclica di questo modello è possibile solo ed esclusivamente attraverso continue attività di auditing. Le attività di auditing non possono prescindere dalla disponibilità di report periodici che riassumano le eventuali violazioni delle policy di sicurezza.

In questa fase vengono dunque definiti i report periodici relativi alle violazioni delle policy di sicurezza. Viene inoltre configurato il policy server per la generazione dei suddetti report.