Gucci Logistica S.p.A.

Progetto per la protezione applicativa

Analisi tecnica della struttura di sicurezza applicativa web di Gucci

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*

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
0.1	3 giugno 2008	Emissione
//	//	//
//	//	//
0.1	3 giugno 2008	Emissione

INFORMAZIONI		
Data di Emissione	3 Giugno 2008	
Versione	0.1	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	8	
Numero Allegati	0	
Descrizione Allegati	1	1
	2	2
Redatto da	Salvatore Rumore	
Approvato da	Roberto Banfi	

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

INDICE

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

1 Obiettivo

Lo scopo del presente documento consiste nel descrivere una soluzione per la protezione degli applicativi web presenti all'interno dell'infrastruttura di Gucci.

2 Ambiente di riferimento

Le reti e il relativo volume di traffico generato dagli host si può riassumere in circa una decina di applicazioni web, tutte con PHP eseguite su Apache Web server. Il Throughput totale di tutte le applicazioni web varia tra gli 1 e i 2 Mbps (in genere il throughput che non supera i 100/150 KB/s con picchi di traffico che può raggiungere i 250 KB/s).
Le connessioni al secondo sono circa una ventina e in determinate fasce orarie si hanno picchi di 1800.

3 Analisi dei requisiti

Obiettivi del progetto:

- Protezione applicativa degli applicativi web attestati sulla rete DMZ.
- Monitoraggio in tempo reale delle richieste http/https dirette ai web server.
- Rilevamento e blocco di eventuali attacchi incapsulati nelle richieste http/https.
- Gestione centralizzata degli eventi e delle politiche di accesso e/o blocco.

4 Descrizione della soluzione

La soluzione proposta è basata sulla tecnologia SecureSphere di Imperva. Questa soluzione consiste in apparati hardware (gateway) gestibili centralmente da un apparato di management (MX Server). Gli apparati di protezione possono essere collocati in una infrastruttura esistente in diversi modi:

- Modalità INLINE: il gateway viene inserito tra due segmenti di rete in modalità trasparante (layer 2) con schede di rete configurabili in fail-open. Quest'ultima caratteristica permette di evitare disservizi in caso di fault dell'apparato rinunciando, però, alla protezione delle applicazioni.
- Modalità REVERSE PROXY: il gateway viene configurato per agire come un reverse proxy. In questo modalità il gateway termina le connessioni provenienti dagli utenti

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

dell'applicazione e ne crea una verso i web server. La configurazione ha lo svantaggio di introdurre un ritardo dovuto alla terminazione e alla creazione delle connessioni.

4.1 Caratteristiche

Di seguito vengono elencate alcune delle caratteristiche principali messe a disposizione dalla tecnologia.

4.1.1 Protezione Centralizzata

- Protezione da attacchi specifici per diverse Applicazioni
- Protezione da Worms e Platform Exploits
- Protezione da Attacchi di Rete

4.1.2 Policy di Sicurezza Automatizzate

- Profili Dinamici modellano struttura e risorse dell'applicazione
- Adattamento ai cambiamenti dell'applicazione
- Protezione avanzata dagli attacchi

4.1.3 Implementazione con impatto minimo

- Nessun cambiamento all'infrastruttura di rete
- Nessun cambiamento all'applicazione
- Nessun impatto sulle performance

4.1.4 Management Centralizzato

- Amministrazione e attività di report centralizzate

4.1.5 Reportistica

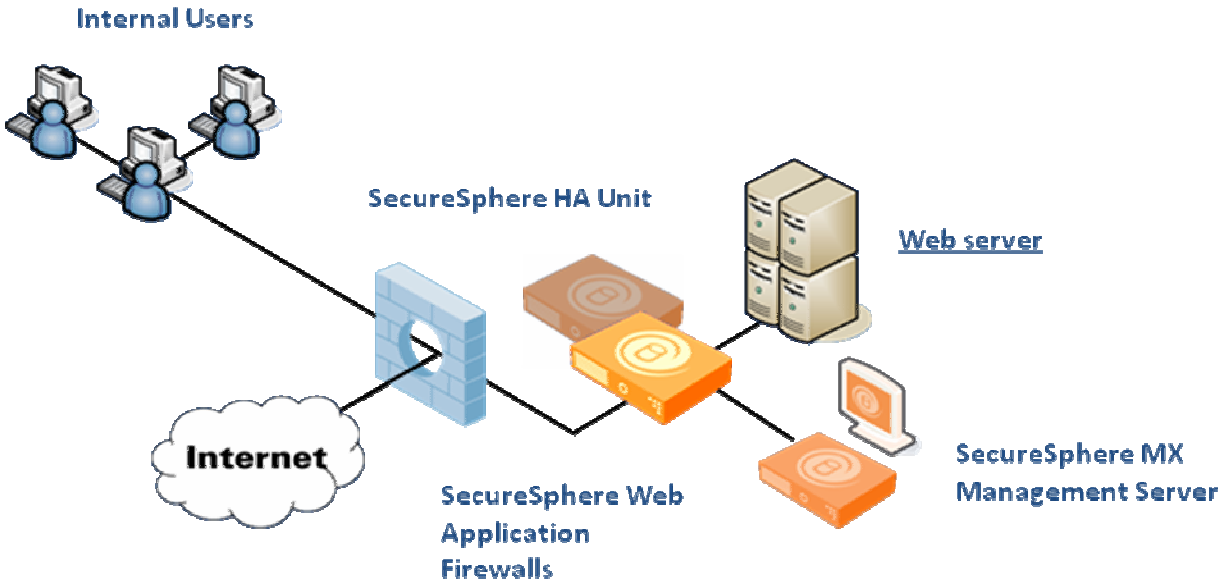
- Report predefiniti e totalmente personalizzabili
- Generazione di report immediata o email giornaliera, settimanale, mensile
- Monitoraggio in real-time delle attività
- Supporto di diverse interfacce di comunicazione (Email, Syslog, …)

5 Descrizione degli impatti

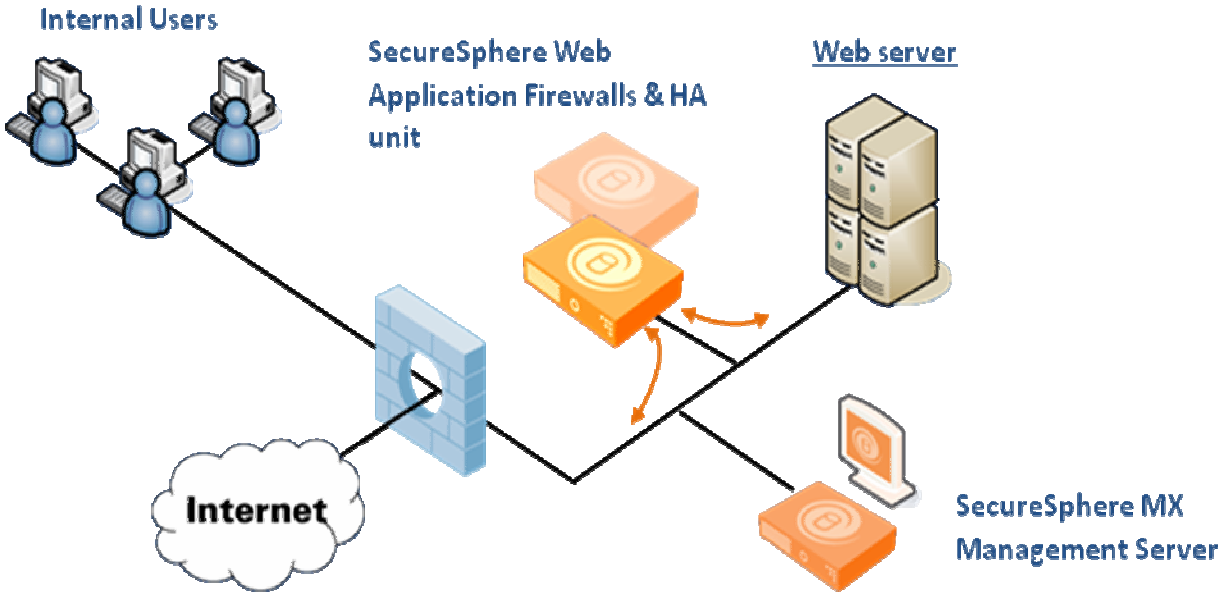
In funzione della modalità di installazione è necessario effettuare delle modifiche minime all'infrastruttura esistente e/o agli apparati di rete.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

Nel caso i gateway vengano inseriti in modalità ***inline*** è necessario posizionarli di fronte alle applicazioni web da proteggere. La figura seguente mostra come tale modalità di implementazione.



La figura successiva rappresenta la possibile configurazione di rete in modalità ***reverse proxy***:



.

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

6 La metodologia

La tecnologia di Imperva permette la completa protezione degli applicativi web da possibili attacchi veicolabili all'interno delle richieste http e https. Al fine di avere un ambiente congruente con il flusso applicativo è necessario suddividere le fasi del progetto.
La fase iniziale comprende le attività di installazione, aggiornamento e configurazione di rete degli apparati. Una volta che gli apparati sono pronti ed inseriti nell'infrastruttura di Gucci si procede con la configurazione degli applicativi da proteggere; a questo punto è necessario un periodo definito di "learning" durante il quale i gateway "imparano" i dettagli dell'applicazione (struttura, pagine, parametri, etc.).
Possiamo riassumere nei seguenti punti le attività di massima che saranno necessarie per la messa in sicurezza della infrastruttura web:

- installazione, aggiornamento e configurazione degli apparti sia gateway che management server;
- messa in esercizio in modalità inline (consigliata) e verifiche di funzionamento;
- periodo di "learning";

In questa fase le presunte richieste illecite verranno segnalate ma non bloccate (simulation). Dopo un periodo che può essere di circa una quindicina di giorni, è necessario intervenire nuovamente sulla configurazione al fine di rimuovere eventuali falsi positivi, procedendo come segue:

- ulteriore configurazione;
- analisi degli aggiornamenti;
- creazione di eventuali "custom rules" in funzione delle necessità applicative dell'utente;
- training on the job per istruire il cliente all'utilizzo cadenzato delle funzionalità del prodotto;
- creazione di report e monitoraggio in tempo reale al fine di avere sempre sotto controllo l'andamento della sicurezza applicativa, eventualmente con avvisi in tempo reale tramite mail, syslog, etc.

A seguito di una nuova fase di learning si procederà configurando i gateway in modo da bloccare le richieste ritenute illecite (protect).

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

La sicurezza offerta Imperva si basa su profili dinamici, policy e signature. Tali elementi sono già presenti all'interno del sistema e sono customizzabili. Settimanalmente Imperva rilascia aggiornamenti che possono essere scaricati automaticamente (se il sistema è in grado di accedere ad Internet) o manualmente. Tali aggiornamenti possono avere impatti sulla configurazione in quanto possono andare a modificare policy definite.
Si consiglia di eseguire insieme al personale HackingTeam controlli periodici bisettimanali o mensili per eventuali migliorie e allineamenti sulla configurazione della soluzione.

7 Planning

Di seguito viene fornita una stima delle attività previste.

	Fase	Dettaglio Attività
Prima Fase	***Progettazione***	Posizionamento nella rete
		Modalità di lavoro InLine/Reverse Proxy
	Installazione	Installazione software
		Installazione patch
		Configurazione apparati
	Configurazione	Configurazione applicazioni
	Testing	Check generale
		Test applicazioni configurate
Seconda Fase	***Configurazione***	Configurazione custom applicazioni
	Testing	Test configurazione
Terza Fase	***Configurazione***	Protezione delle applicazioni
	Testing	Test configurazione

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.