]HackingTeam[

AXA Assicurazioni

Studio e deployment di una soluzione di firewalling di livello applicativo

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	2/9/2004	Emissione
//	//	//
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	2/9/2004	
Versione	1.0	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	10	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Federico Guerrini, Marco Valleri	
Approvato da	Valeriano Bedeschi	

INDICE

1 Obiettivo

Scopo delle attività descritte in questo documento è la progettazione e la messa in opera di un application level firewall atto a proteggere da attacchi esterni le applicazioni web del Committente.
Un web application firewall analizza le richieste dei client prima che queste raggiungano il web server e blocca quelle considerate "maligne", basandosi su una serie di policy preimpostate. Questo permette di bloccare tutta una serie di attacchi basati su errori di implementazione delle applicazioni web, che potrebbero portare alla perdita/furto/modifica di dati sensibili relativi alle applicazioni o, addirittura, alla compromissione totale delle macchine ospitanti tali applicazioni. Un web application firewall rappresenta quindi una risposta semplice e immediata alle vulnerabilità applicative di tipo classico (Cross-site-scripting, SQL Injection, etc.), che non richiede lunghe e costose modifiche al codice delle applicazioni[1].
Come riscontrato nel vulnerability assessment condotto da Hacking Team, le applicazioni web del committente presentano gravi vulnerabilità che richiedono l'adozione di contromisure di veloce implementazione. In risposta a questa esigenza, si propone una soluzione, basata su *InterDo* di *KavaDo*, avente le seguenti caratteristiche:

- Integrazione trasparente alle applicazioni e agli apparati preesistenti;
- Rispondenza ai requisiti di performance e di affidabilità specificati dal cliente;
- Amministrazione remota tramite protocollo sicuro.

Allo scopo di non aumentare l'effort di gestione della rete, si è scelto un prodotto che può essere integrato con un application level scanner automatico, che interagisce con esso e ne modifica dinamicamente la configurazione, a fronte di nuove vulnerabilità introdotte da modifiche delle applicazioni.

2 Ambiente di riferimento

Il firewall di livello applicativo dovrà essere integrato nel sistema informativo del committente in modo tale da prevenire attacchi sia sugli host di front end, sia su quelli di back end.
L'architettura e le caratteristiche dell'ambiente target sono solo parzialmente note ad Hacking Team. Poiché l'integrazione di un application firewall nella rete del committente deve

[1] E' consigliabile effettuare comunque, anche in un secondo tempo, un audit del codice sorgente al fine di portare il grado di sicurezza generale ai massimi livelli.

necessariamente tenere conto delle caratteristiche e dei vincoli posti dalla stessa, si renderà necessaria una fase di analisi per definire la strategia di intervento più appropriata.

3 Analisi dei requisiti

Sulla base dei risultati del vulnerabilty assessment svolto sui sistemi e sulle applicazioni in oggetto, la soluzione proposta dovrà rispondere ai requisiti descritti nei successivi sottoparagrafi.

3.1 Requisiti funzionali

- L'application firewall deve permettere di identificare e bloccare le richieste HTTP che configurano attacchi di livello applicativo attualmente noti. In particolare, deve essere in grado di rilevare e bloccare richieste HTTP che sfruttano le vulnerabilità identificate nelle applicazioni web del committente durante il vulnerability assessment.
- L'application firewall deve disporre di tool automatici a supporto delle attività di configurazione, allo scopo di ridurre l'effort necessario per la manutenzione del prodotto ed il suo aggiornamento a fronte di modifiche delle applicazioni web e/o della pubblicazione di nuove vulnerabilità.
- L'application firewall deve disporre di tool di amministrazione che ne consentano l'amministrazione (in sicurezza) da postazioni remote.
- L'application firewall non deve costituire un *single point of failure* per il sistema. Dovrà pertanto supportare configurazioni in alta affidabilità e/o una modalità di funzionamento di fail over che preveda l'esclusione del firewall stesso.

3.2 Requisiti di performance

- L'application firewall non deve causare cali di performance dell'intero sistema tali da essere percepiti dall'utente finale.

4 Descrizione della soluzione

4.1 Livello di rete

Dal punto di vista sistemistico e di rete, InterDo funziona come un reverse proxy. In base alle caratteristiche dell'ambiente target, è possibile utilizzare diverse configurazioni. Le principali opzioni sono le seguenti.

- ***Installazione su macchine Windows, Solaris, Linux o appliance***: InterDo viene distribuito sia come pacchetto software (per i suddetti sistemi operativi), sia come appliance. Performance, hardenizzazione e semplicità di manutenzione/aggiornamento sono gli aspetti da considerare nella scelta.
  - *Installazione su macchina dedicata o su web server*: qualora si decida di utilizzare InterDo In versione software, è possibile utilizzare hardware dedicato oppure eseguire l'installazione sullo stesso host del server http da proteggere. In questo secondo caso, l'occupazione di risorse sul web server in condizioni di normale utilizzo non deve superare, prima dell''installazione di InterDo, il 65% per la memoria RAM ed il 50% per la CPU.

    Per l'installazione su hardware dedicato, Hacking Team consiglia le seguenti caratteristiche: processore PIV 2.4 GHz o sup., RAM 2GB, hard disk IDE 80 GB.

    Performance, costo dell'hardware e numero di host da gestire sono gli aspetti da considerare nella scelta.
- ***Configurazioni in alta affidabilità***: poiché il firewall applicativo deve filtrare tutto il traffico HTTP da e verso i web server, viene a rappresentare un *single point of failure*. InterDo supporta configurazioni in alta affidabilità integrandosi con switch di layer 7. Sono possibili anche configurazioni di tipo attivo-attivo che garantiscono, oltre all'alta affidabilità, anche la scalabilità del throghput. Costo, criticità dei servizi web da proteggere e complessità di eventuali procedure di esclusione del firewall sono gli aspetti da considerare nella scelta.
- ***Configurazioni con una o più interfacce di rete***: InterDo supporta configurazioni con una sola o più interfacce di rete, che permettono di ottenere diversi livelli di isolamento delle risorse protette dal resto della rete. La collocazione delle risorse da proteggere all'interno della rete, l'architettura e la topologia della stessa sono i parametri che determinano la scelta più appropriata.

4.2 Architettura logica

InterDo dispone di una interfaccia grafica che presenta, secondo un approccio object based, una astrazione di alto livello del funzionamento del firewall. I diversi aspetti della configurazione sono separati in tre categorie di oggetti.

- ***Oggetti per la configurazione del firewall a livello di rete***: permettono di impostare i parametri delle interfacce di rete del firewall.
- ***Oggetti per la definizione delle politiche di accesso agli strumenti di configurazione***: è possibile assegnare agli utenti che hanno accesso alla console di amministrazione diversi livelli di visibilità e di accesso ai parametri di configurazione.
- ***Oggetti per la definizione del traffico HHTP da sottoporre ai controlli di sicurezza***: permettono di definire quali pacchetti HTTP il firewall deve analizzare. Il traffico HTTP da sottoporre a verifica può essere specificato a diversi livelli di granularità:
  - *URL*: specifico URL o parametro associato alla richiesta per specifico URL;
  - *Application path*: insieme di URL identificati mediante path parziale o regular expression;
  - *Virtual host*: nome di virtual host attestato su un web server protetto dal firewall;
  - *Tunnel*: socket (indirizzo IP e porta TCP) su un host protetto dal firewall;
  - *Web application*: insieme di tunnel relativi a risorse logicamente appartenenti alla stessa applicazione Web.
- ***Oggetti per la definizione dei controlli di sicurezza***: permettono di definire il comportamento dei diversi moduli (*security pipe*) che effettuano controlli per identificare specifiche vulnerabilità di livello applicativo. *InterDo* permette di far fronte a tutti gli attacchi applicativi che ricadono nelle seguenti categorie:
  - *SQL Injection*: concatenazione di comandi SQL nelle richieste del client.
  - *Parameter Tampering*: manipolazione dei parametri dell'applicazione.
  - *Cookie Poisoning*: modifica delle informazioni contenute nei cookie.
  - *3rd Party Misconfiguration*: sfruttamento di errori di configurazione su prodotti di terze parti come web server o database.
  - *Vulnerability Patterns*: sfruttamento di vulnerabilità generiche conosciute in prodotti comuni.
  - *SOAP & WebServices Message Exploitation*: modifiche degli attributi dei messaggi dei WebServices.

- *Application Language Mismatch*: invio di caratteri non consentiti dal linguaggio utilizzato dall'applicazione.
- *HTTP Methods Exploitation*: utilizzo indiscriminato di metodi HTTP non utilizzati dall'applicazione.
- *Files Upload*: upload di file eseguibili o script e successiva esecuzione.
- *Protocol Piggyback*: modifica della struttura del protocollo applicativo.
- *Buffer Overflow Attack*: invio di richieste di lunghezza eccessiva o malformate per indurre in fallimento il codice dell'application server.
- *Data Encoding*: invio di richieste codificate secondo standard particolari (Unicode, UTF-8, UTF-16).

4.3 Funzionalità avanzate

InterDo dispone di una serie di funzionalità avanzate che ne semplificano la configurazione e l'aggiornamento.

- ***Autopolicy***: e' una tecnologia che permette di utilizzare i report prodotti dal web application scanner *ScanDo* (prodotto dalla stessa *Kavado*), per creare automaticamente policy per InterDo basate sulle caratteristiche e vulnerabilità riscontrate nelle applicazioni sottoposte a scansione. Questa funzionalità, già inclusa nella presente offerta, permette di mantenere il livello di sicurezza raggiunto anche in seguito a modifiche nel codice e nella struttura delle applicazioni.
- ***Learn mode***: è una modalità di funzionamento delle security pipe che permette, utilizzando un browser per navigare all'interno delle applicazione da proteggere, il rilevamento automatico di potenziali vulnerabilità e la conseguente configurazione della pipe corrispondente. Questa funzionalità semplifica notevolmente le fasi di configurazione iniziale, permettendo di ottenere in tempi rapidi un insieme di security policy sulla base delle quali procedere con una azione di fine tuning manuale.
- ***Allarmistica e reportistica****: InterDo* offre inoltre un sistema di notifica in tempo reale dei tentativi di intrusione configurabile e un sistema di reportistica automatica per tenere traccia nel tempo degli attacchi ed evidenziare le applicazioni maggiormente a rischio.

5 Descrizione degli impatti

5.1 Impatti a livello rete

L'installazione di InterDo comporta, come anticipato nei precedenti paragrafi, l'introduzione di un proxy fra la rete esterna (da cui provengono le richieste di accesso alle applicazioni) ed i server web che devono essere protetti. In generale, questo può comportare interventi di configurazione sugli apparati di rete (router, firewall) presenti fra il perimetro ed i web server e/o la modifica degli indirizzi IP dei web server.

Nel caso specifico della presente offerta, l'elenco degli interventi necessari verrà definito in seguito all'analisi dell'architettura di rete dell'ambiente target, alla collocazione dei componenti di front end (web server) e di back end (database server) nella stessa e alla configurazione scelta (si veda il paragrafo 4).

5.2 Impatti procedurali

L'installazione di InterDo comporta anche la necessità, ai fini di un corretto ed efficace utilizzo del prodotto, l'identificazione di figure professionali e di procedure per:

- amministrazione ordinaria del firewall;
- analisi dei report;
- reazione agli allarmi;
- aggiornamento a fronte di aggiunta/rimozione/modifica di applicazioni;
- recovery in caso di crash del firewall (in assenza di configurazioni in alta affidabilità, queste procedure possono comprendere il restore della configurazione di rete in assenza di firewall).

6 La metodologia

La metodologia utilizzata da Hacking Team per l'integrazione di soluzioni di firewalling di livello applicativo prevede le seguenti fasi.

- Analisi della configurazione di rete dell'ambiente target: l'obiettivo di questa fase è l'identificazione di:
  - risorse che devono essere protette;
  - loro collocazione sulla rete;
  - utilizzo del protocollo SSL;

- organizzazione della rete (rete pubblica, reti interne, DMZ, collocazione dei firewall, ecc.).

- Identificazione della modalità di installazione più appropriata (si veda il paragrafo 4).
- Identificazione degli interventi di configurazione sugli apparati preesistenti
  - per ridirigere il traffico HTTP attraverso il firewall;
  - per consentire l'amministrazione remota del firewall;
- Configurazione del firewall, in base a:
  - Best practices in application security
  - Caratteristiche HW/SW delle piattaforme da proteggere
  - Risultati del vulnerabilità assessment svolto precedentemente
- Analisi della funzionalità e delle prestazioni in ambiente di test
- Definizione delle procedure di gestione del firewall (si veda il paragrafo 5.2)
- Deployment in ambiente di produzione e verifiche di funzionalità.

7 Planning

Attività	***Giorni/uomo***
Analisi configurazione di rete dell'ambiente target	4
Studio della modalità di installazione	2
Definizione delle procedure di gestione del firewall	2
Interventi di configurazione sugli apparati preesistenti	2
Definizione delle policy di sicurezza	3
Installazione in ambiente di test e verifica funzionale e di performance	4
Deployment in ambiente di produzione e verifiche di funzionalità.	3
Totale giorni/uomo	***20***