]HackingTeam[| Sipra

SIPRA

Protezione dei dati su file server e laptop

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	01/03/2005	Prima stesura

INFORMAZIONI		
Data di Emissione	01/03/2005	
Versione	1.0	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo		
Numero Pagine	7	
Numero Allegati	-	
Descrizione Allegati	1	
	2	
Redatto da	Federico Guerrini	
Approvato da	Gianluca Vadruccio	

INDICE

1 Obiettivo

Sipra ha richiesto di formulare una proposta tecnica relativamente ad una soluzione per la cifratura di dati residenti su file server all'interno della rete aziendale e/o su laptop in dotazione all'utenza mobile. Tale soluzione deve rispondere ai seguenti requisiti funzionali:

- cifratura di singoli file su disco locale o file server remoto;
- cifratura di cartelle su disco locale o file server remoto;
- condivisione di dati cifrati residenti su file server fra diversi utenti;
- cifratura completa dell'hard disk dei laptop.

Allo scopo di permettere una valutazione del livello di rispondenza della soluzione proposta alle proprie esigenze, Sipra richiede di includere nella proposta una attività pilota per l'implementazione di un prototipo per un numero limitato di utenti.

2 Descrizione della soluzione

Hacking Team, a seguito di una analisi delle tecnologie per la protezione dei dati attualmente disponibili sul mercato, ha identificato una soluzione rispondente ai requisiti sopraelencati. Tale soluzione si basa sulla suite di prodotti ***SafeBoot***.

Il presente documento descrive sia i componenti software necessari, sia l'approccio proposto per la loro corretta integrazione nel sistema informativo di Sipra.

2.1 Tecnologia scelta

SafeBoot (http://www.safeboot.com) è sviluppato da Control Break International, una multinazionale leader nel settore delle tecnologie crittografiche per la protezione dei dati sensibili, presente in Europa e negli Stati Uniti.

Control Break International ha ricevuto i seguenti riconoscimenti:

- ***Aprile 2004***: SafeBoot riceve il "SC Magazine Reader Award" come miglior software di cifratura dei dati per utenti mobili;
- ***Febbraio 2005***: SafeBoot riceve la certificazione "FIPS 140-2" dal National Institute for Standards and Technology (NIST), USA.

E' attualmente in corso il processo di certificazione di SafeBoot per la conformità ai Common Criteria.

2.1.1 Standard crittografici supportati

SafeBoot utilizza i seguenti algoritmi crittografici:

- ***AES 256 bit***;
- ***RC5 1024 bit***.

2.2 Architettura della soluzione

L'architettura proposta da Hacking Team prevede due livelli.

- ***Livello distribuito***: è costituito dai componenti software installati sulle macchine dove risiedono dati cifrati (sia file server connessi in modo permanente alla rete aziendale interna, sia laptop che accedono ad essa dall'esterno). Per la cifratura di file e cartelle su dischi locali e/o file server sarà utilizzato il componente ***SafeBoot Content Encryption***. Per la protezione completa dei laptop si utilizzerà ***SafeBoot Device Encryption***.
- ***Livello centrale***: è costituito da un tool di management (***SafeBoot Admin***) per il deployment, la configurazione e la gestione di tutti i componenti della soluzione (Content Encryption, Device Encryption) distribuiti nel sistema informativo.

Le principali funzionalità dei componenti della suite sono descritte nei seguenti paragrafi.

2.2.1 SafeBoot Device Encryption

SafeBoot Device Encryption permette la cifratura completa dell'hard disk di un laptop. L'accesso al disco è consentito solo previa autenticazione dell'utente, che avviene prima che il processo di bootstrap abbia inizio. Tale autenticazione può essere basata sull'uso di una password oppure su hardware crittografico (Smart Card, USB key, ecc).

2.2.2 SafeBoot Content Encryption

Content Encryption permette di cifrare file e/o cartelle locali su qualsiasi tipo di supporto, garantendo la persistenza della cifratura: i dati cifrati rimangono tali indipendentmente dal dispositivo su cui vengono spostati o copiati. La presenza di Content Encryption non altera la normale operatività degli utenti, che devono solo inserire, quando accedono a materiale cifrato, le opportune credenziali.

2.2.3 SafeBoot Admin

Admin è lo strumento di gestione che permette di centralizzare le operazioni di configurazione e gestione degli altri prodotti della suite. In particolare, Admin consente di:

- utilizzare, per la gestione degli utenti, directory aziendali preesistenti
- distribuire chiavi di cifratura agli utenti

- definire, distribuire e garantire il rispetto di politiche di accesso al materiale cifrato
- definire, distribuire e garantire il rispetto di politiche di accesso alle funzionalità di cifratura della suite
- offrire agli utenti servizi web-based di help desk per eseguire operazioni di recovery in seguito allo smarrimento di credenziali.

2.3 Gestione delle credenziali

La gestione delle credenziali in possesso degli utenti finali rappresenta nella maggior parte dei casi l'aspetto più critico del progetto di una soluzione di sicurezza. La presente proposta include anche l'identificazione della strategia più opportuna di gestione delle credenziali, in rapporto al livello di sicurezza, ai requisiti ed ai vincoli che il Committente riterrà opportuno indicare.
La scelta tecnologica descritta nei precedenti paragrafi permette di considerare due differenti possibilità.

- ***Utilizzo di username/password***: gli utenti accedono alle funzionalità di cifratura ed al materiale cifrato digitando una coppia username/password che devono ricordare. Questo approccio richiede il minore effort in fase di deployment, ma presenta limiti significativi sia per quanto riguarda il livello di sicurezza, sia per quanto riguarda le problematiche di gestione (necessità di servizi di help desk per supportare gli utenti in caso di smarrimento/compromissione della password).
- ***Utilizzo di token crittografici***. Questo approccio permette, a fronte di un maggiore effort di integrazione, una gestione delle credenziali di accesso al materiale cifrato più sicura ed efficiente. SafeBoot si integra con token prodotti da diversi vendor (Rainbow, ActivCard, ecc.).

3 La metodologia

In risposta alle esigenze di Sipra, la metodologia proposta per l'integrazione del prodotto prevede due fasi.

- ***Svolgimento di un progetto pilota*** finalizzato all'implementazione di un prototipo che implementi tutte le funzionalità di cifratura e gestione centralizzata descritte nel paragrafo precedente. Da tale attività pilota rimangono escluse tutte le problematiche relative a:
  - vincoli imposti da caratteristiche peculiari del sistema informativo di Sipra;
  - deployment della soluzione in ambiente di produzione.

- ***Implementazione della soluzione in ambiente di produzione***. Per garantire la corretta integrazione delle funzionalità offerte dalla suite SafeBoot nel sistema informativo di Sipra, Hacking Team propone l'approccio seguente:
  - ***Analisi dei requisiti***. In questa fase vengono formalizzati i requisiti del Cliente, sia in termini funzionali, sia in termini tecnici. Vengono inoltre individuati i vincoli di natura tecnica e/o procedurale che devono essere rispettati nelle successive fasi di implementazione.
  - ***Definizione delle policy di sicurezza***. Questa fase consiste nella formalizzazione delle policy di sicurezza che il Committente vuole applicare all'interno della propria organizzazione. A tale formalizzazione si giunge in seguito all'analisi dei requisiti funzionali del progetto.
  - ***Piano di intervento***. In seguito all'identificazione delle policy di sicurezza è possibile delineare nel dettaglio le caratteristiche tecniche della soluzione pianificare le fasi di installazione, configurazione e deployment della soluzione nell'ambiente di produzione.
  - ***Installazione in ambiente di test***. In questa fase viene creato un ambiente di test nel quale si procede all'installazione dei componenti software che costituiscono la soluzione proposta.
  - ***Configurazione in ambiente di test***: In questa fase si procede alla configurazione dei prodotti installati ed, eventualmente, dei sistemi (di test) con i quali si devono interfacciare (ad esempio, servizi LDAP), secondo quanto definito nel piano di intervento.
  - ***Testing***. In questa fase la soluzione viene sottoposta ad una serie di test volta a determinarne la conformità ai requisiti individuate.
  - ***Deployment in produzione***. Al termine della fase di test, si attua la strategia di deployment secondo quanto definito nel piano di intervento.

4 Tempistiche

Si fornisce una indicazione dell'*ordine di grandezza* dell'effort per le attività proposte:

- progetto pilota svolto presso il Committente: 4 gg/uu;
- progetto completo (ambiente di produzione): 15 gg/uu.