Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Proposta di aumento del livello di Sicurezza di AtaHotels

Sistema Anti-Intrusione

Obiettivo

La tecnologia di analisi delle intrusioni é nata con lo scopo di rilevare attività estranee al consueto utilizzo della rete e dei sistemi di una società. Analizzando il traffico che passa sulla rete e le attività che si eseguono sui sistemi è in grado di scovare sia eventuali attacchi che scostamenti dalle politiche definite ed impostate dall'organizzazione. Si tratta quindi di un sistema che difende gli assets informatici e di conseguenza il business che su di essi si sviluppa: la difesa che esercita lo strumento è considerata una "seconda linea" in quanto protegge dagli attacchi esterni che riescono a sorpassare la barriera firewall e dagli attacchi interni provenienti da personale interno alla sede principale ed eventualmente anche dalle sedi remote.

Progettato in maniera opportuna, lo strumento di analisi e rilevamento delle intrusioni può essere utilizzato anche per contrastare frodi informatiche (decreto legislativo n. 547 del 1993), tutelare la società da eventuali illeciti amministrativi (decreto legislativo n. 231 del 2001) e proteggere la rete ed il business da virus e worm che non sono ancora stati segnalati e cancellati dai sistemi antivirus.

Soluzione

Utilizzando strumenti standard per il rilevamento delle intrusioni, si propone quindi di progettare un sistema che vigili sul traffico di rete e di sistema, proteggendo l'organizzazione da tutto ciò che non è identificabile dai sistemi attualmente presenti e dalle operazioni lesive che eventualmente potrebbero nascere. Si tratta quindi di un progetto che mira a proteggere la società dagli attacchi, da eventuali denunce, da possibili nuovi virus e da comportamenti (seppur leciti) non voluti dalle proprie politiche.

Con una opportuna configurazione (attivabile o meno a seconda delle esigenze e delle volontà) del sistema si potrà anche reagire agli eventi in real-time in maniera da essere proattivi ed evitare (ove possibile) di subire il danno con opportune azioni di contrasto e blocco.

Autenticazione forte e gestione delle password

Obiettivo

Le soluzioni di autenticazione forte e gestione delle credenziali hanno lo scopo di ridurre il rischio di accessi ai sistemi e alle applicazioni aziendali da parte di soggetti non autorizzati.

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Autenticazione forte e gestione delle credenziali agiscono in modo complementare. La prima permette di realizzare meccanismi identificazione degli utenti più sofisticati, basati sull'uso di credenziali complesse e quindi robusti a fronte di tentativi di intrusione. La seconda permette agli utenti autorizzati di conservare ed utilizzare credenziali complesse senza esporsi al rischio di furto o intercettazione delle stesse. In particolare, rendono più semplice la gestione di password lunghe (di difficile memorizzazione) e la modifica frequente delle stesse.
In quest'ottica le soluzioni di autenticazione forte e gestione delle credenziali rappresentano una risposta tecnologica agli adempimenti imposti dalla normativa relativa alla privacy e dichiarata nella stesura del relativo documento programmatico (DPS).

Soluzione

Hacking Team progetta ed implementa soluzioni di autenticazione forte e gestione delle credenziali che automatizzano i processi di emissione/revoca/rinnovo delle credenziali. In base alle specifiche esigenze, tali soluzioni possono comprendere diversi insiemi di funzionalità: gestione centralizzata di credenziali, servizi di single-sign-on, servizi di self service per gli utenti finali, ecc. I vantaggi che ne derivano riguardano sia le problematiche di amministrazione, che risultano snellite e semplificate, sia le problematiche degli utenti finali, che accedono ad infrastrutture complesse ed eterogenee in modo trasparente ed uniforme ma soprattutto utilizzando una sola password.

Valutazione delle applicazioni web

Obiettivo

I principali attacchi degli ultimi periodi riguardano essenzialmente le applicazioni rese disponibili via web. Questo è dovuto a due fattori importanti: la parte rete e sistemistica è sempre più protetta dalle organizzazioni, trattandosi di sicurezza tradizionale; un errore o una vulnerabilità applicativa consente di arrivare direttamente ai dati senza subire altri controlli. Nel caso si parli di dati sensibili, si capisce immediatamente la pericolosità di questa possibilità.
Le principali tipologie di attacco applicativo sono le seguenti:

- Attacchi al protocollo di comunicazione: debolezze di comunicazione dell'applicativo
- Cross-site scripting: possibilità di impersonare un'altra utenza
- Parameter Tampering/Hidden field manipulation: tentativo di blocco dell'applicazione
- Stealth Commanding: esecuzione di comandi illeciti da remoto sul sistema target
- Forceful browsing: navigazione dei dati non permessa
- Cookie Poisoning: possibilità di impersonare un'altra utenza o di danneggiare un'altra comunicazione
- SQL Injection: tentativo di manipolazione dei dati del database

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

- Buffer overrun: tentativo di crash dell'applicazione

Soluzione

La metodologia di assessment utilizzata e proposta da Hacking Team permette di proteggere ad altissimo livello le applicazioni di una società e si fonda su un approccio iterativo, che prevede l'esecuzione ripetuta di quattro attività:

- analisi (architetturale ed implementativa): questa fase consiste nella raccolta di informazioni relative all'applicazione oggetto del vulnerability assessment, sulla cui base definire la strategia di analisi e di attacco.
- identificazione delle vulnerabilità: questa fase consiste nella ricerca di errori logico/architetturali ed implementativi che possono essere sfruttati per compromettere la sicurezza dell'applicazione.
- definizione degli scenari di attacco: sulla base dei risultati della fase di individuazione delle vulnerabilità, vengono definite le strategie di attacco che possono essere utilizzate per una specifica applicazione.
- esecuzione degli attacchi: poiché il vulnerability assessment viene svolto senza conoscere i dettagli implementativi dell'applicazione (cioè senza la disponibilità del codice sorgente) l'effetto di un attacco può essere determinato soltanto mediante la sua effettuazione.

La necessità di operare in modo iterativo nasce dal fatto che l'esecuzione di ogni attacco può accrescere il livello di conoscenza dell'applicazione e/o il livello di privilegio di chi lo esegue, rendendo necessaria una nuova fase di analisi, sulla cui base identificare nuovi scenari di attacco.

L'assessment si conclude quando, sulla base di tutte le informazioni raccolte e dei privilegi ottenuti non si possono identificare ulteriori scenari di attacco. L'output dell'assessment è costituito da un documento, che descrive:

- come la metodologia è stata applicata al caso particolare in esame
- i risultati degli attacchi effettuati
- le contromisure da adottare per eliminare le vulnerabilità individuate
- presentazione a slides dei risultati
- executive summary (breve descrizione dei risultati con terminologia non tecnica)

Analisi della sicurezza esterna

Obiettivo

Le vulnerabilità dei sistemi e delle applicazioni sono ormai scoperte quotidianamente ed altrettanto quotidianamente vengono sfruttate per sferrare attacchi mirati sensibilmente dannosi. In maniera analoga, se non addirittura più diffusa, si parla di virus e worm che infestano tutti i sistemi, principalmente di navigazione e di

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

posta elettronica degli utenti; senza contare il fatto che i moderni spyware riempiono le postazioni dopo solo qualche minuto di navigazione.

Quello che rende più pericoloso il fenomeno è l'aumento vertiginoso di programmi free già preconfezionati e scaricabili senza problemi da parte di chiunque: questo rende possibile un attacco anche ad una persona con pochissimi skills in materia di sicurezza informatica. Ciò allarga notevolmente lo spettro delle possibili persone in grado di portare a compimento un attacco e quindi non si parla solo di una ristretta cerchia di hackers.

Le attività di attacco ad un sistema informatico potrebbe portare alla distruzione di dati sensibili, al rallentamento o addirittura al blocco di un servizio ed in entrambi i casi (come pure in tanti altri) con forti ripercussioni sull'attività di business dell'organizzazione.

Una buona protezione da attacchi esterni è inoltre richiesta dalla legge sulla privacy per tutte quelle società che trattano dati sensibili: si parla tanto dei famosi "requisiti minimi", specificati nell'articolo 34 e precisamente nel paragrafo e) con le parole "protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici".

Soluzione

Tenere sotto controllo l'infrastruttura perimetrale dal punto di vista della sicurezza è indispensabile per una società che si voglia tutelare dalle numerose insidie che potrebbero minacciarla dall'esterno. Si propone quindi un'azione di monitoring dei sistemi e delle applicazioni raggiungibili da Internet o comunque da una sede esterna con l'obiettivo di rilevare tutte le eventuali minacce di sicurezza presenti. L'azione sarebbe condotta a livello di rete, a livello architetturale, a livello di sistema, a livello applicativo e a livello procedurale, in maniera tale da fornire all'azienda un quadro completo del suo stato di salute della frontiera informatica.

Lo studio genererà un documento in cui saranno dettagliate le seguenti parti:

- descrizione dello stato di sicurezza e della architettura/topologia esistenti
- analisi dettagliata delle vulnerabilità presenti
- valutazione delle priorità e del grado di minaccia effettivamente corrispondente ad ogni debolezza
- strategia di sistemazione dei problemi riscontrati
- piano della sicurezza per la copertura a step di tutte le vulnerabilità
- eventuale piano di miglioramento delle procedure di sicurezza
- presentazione a slides dei risultati
- executive summary (breve descrizione dei risultati con terminologia non tecnica)