Emaze Networks

informed security

Background

Le reti e gli ambienti IT aziendali sono caratterizzati da un rapido aumento dei rischi dovuto principalmente alla loro intrinseca complessità, all'inevitabile apertura richiesta dai servizi verso la clientela (e i fornitori) nonché ad attacchi sempre più sofisticati. Con l'aumentare della consapevolezza degli organismi regolatori, i requisiti di conformità a normative e standard diventano sempre più stringenti. Tutto ciò rende necessario un nuovo approccio proattivo e pervasivo alla Sicurezza delle Informazioni.

I tradizionali meccanismi di protezione (firewall, antivirus, intrusion detection, controllo degli accessi, ecc.) richiedono di essere integrati implementando un efficace processo di Risk e Vulnerability Management.

Informed Security Management

L'Informed Security Management (ISM) è il framework completo di sicurezza inteso come l'insieme dei processi e delle infrastrutture, da integrare su scala aziendale per rendere la rete e gli ambienti IT più sicuri, migliorando allo stesso tempo le capacità di verifica continua e di misurazione dell'aderenza alle politiche di sicurezza adottate.

L'implementazione del framework ISM prevede tre fasi principali:

1. La ***definizione del perimetro***, che include l'analisi del rischio, la definizione del livello di rischio accettabile, le linee guida per la configurazione dei dispositivi, per l'accesso alle risorse e per l'Identity management degli utenti

2. L'***implementazione del processo di Vulnerability Management*** basato sugli ormai classici 4 step ciclici: (I) Identificazione delle vulnerabilità; (II) Definizione delle contromisure; (III) Implementazione delle contromisure; (IV) Verifica della neutralizzazione delle vulnerabilità

3. La ***gestione degli incidenti*** effettuata da personale specializzato grazie alla quale affrontare prontamente qualunque evento non previsto o non prevedibile che può avere un impatto sulla sicurezza dei sistemi e delle informazioni

La visione strategica del problema "vulnerabilità" va oltre la semplice difesa degli asset digitali effettuata tramite l'eliminazione delle singole criticità (obiettivo spesso difficilmente raggiungibile nelle realtà aziendali) ma presuppone un coordinamento tra gli strumenti di protezione di reti, host e applicazioni ed il livello organizzativo.
La tecnologia impiegata è essenziale nel processo di ISM e deve essere integrata in maniera efficace ed efficiente con i sistemi ed i processi aziendali esistenti.

eMaze
informed security

www.emaze.net
info@emaze.net

Emaze Networks S.p.A.
reg. Imp. Trieste
c.f. - p.iva 00998050322
r.e.a. 116618
cap. Soc. € 100.000 i.v.

Sede legale
Area Science Park
ss 14 Km 163,5
loc. Basovizza
I - 34012 Trieste (TS)
tel +39 040 3757580
fax +39 040 3757581

Direzione Generale
Via D. Balestrieri, 6
I - 20154 Milano (MI)
tel +39 02 89078400
fax +39 02 89078420

Allo stesso tempo il processo deve consentire la piena misurabilità di quello che si sta osservando in fase di indagine e di quello che succede in fase di esercizio e consentire un continuo confronto con benchmark e policy di riferimento (standard internazionali e aziendali).

In questo modo è possibile ottenere risultati valutabili tramite Key Security Indicator (KSI) opportunamente definiti, con conseguente misurabilità del ritorno degli investimenti in termini di sicurezza (RoSI), traguardando una riduzione dei costi di gestione (OPEX).

In ottica ISM le quattro componenti tecnologiche fondamentali per gestire i problemi di sicurezza in azienda sono:

1. **Verifiche di Sicurezza**
2. **Security configuration management e Policy compliance**
3. **(IT Security) Risk Management**
4. **Security Information Event Management (SIEM) e Control Room**

1. Verifiche di Sicurezza

Vulnerability Assessment (VA), Penetration Testing (PT) e Code Auditing (CA), detti collettivamente Verifiche di Sicurezza, sono le attività per la ricerca e l'identificazione dei problemi alla base del processo di Vulnerability Management.
Lo scopo delle **Verifiche di Sicurezza** è di cercare sistematicamente tutti i punti di attacco dell'infrastruttura, per evidenziare le situazioni di vulnerabilità riconoscibili in maniera tempestiva e aggiornata. Il risultato di tali attività è una documentazione esaustiva di analisi, differenziata in funzione dei diversi ruoli aziendali dei destinatari dei report, delle criticità riscontrate in tutto l'ambiente informatico (rete, server, client, applicazioni, procedure, processi, ecc).
Le informazioni riportate permettono di pianificare gli interventi ed eliminare le cause di possibili intrusioni, ridurre le potenzialità dei vettori di attacco e soprattutto limitare l'impatto degli incidenti di sicurezza. Un completo assessment di sicurezza a livello Enterprise deve misurare in termini oggettivi tutte queste evidenze.

2. Security configuration management e policy compliance

La gestione della configurazione delle apparecchiature di sicurezza e la consulenza nella fase di definizione e implementazione delle relative policy forniscono all'IT il supporto necessario nell'adeguamento ai requisiti di sicurezza.
Tali requisiti sono identificati dall'organizzazione sia con riferimento agli standard e *best practice* del settore sia sulla base dei risultati delle verifiche di sicurezza effettuate.

Si definisce così una configurazione di sicurezza ottimale in grado di rispondere sia alle proprie esigenze di business sia ai requisiti e vincoli normativi.
La corrispondenza dei sistemi con questa configurazione ottimale è monitorata attraverso un processo di verifica costante; si possono in questo modo identificare gli interventi correttivi necessari e recepire prontamente le eventuali modifiche intercorse a livello di policy o di requisiti di sicurezza.

3. (IT Security) Risk Management

L'obiettivo primario dell'**IT Security Risk Management** è quantificare il rischio IT e definire la priorità delle attività di remediation. Un approccio bilanciato al Risk Management combina la criticità degli asset in termini di business con le policy di sicurezza e con i risultati delle Verifiche di Sicurezza: in questo modo i dati tecnici sono riconsiderati alla luce dei processi aziendali e valutati in ottica di business. Un ulteriore obiettivo è quello di predisporre un piano per la remediation dei problemi ed insieme di verifica dei progressi compiuti nell'eliminazione.
Implementare l'IT Security Risk Management implica sviluppare un asset inventory aziendale in termini di gestione delle relative vulnerabilità, con cui classificare gli stessi asset in funzione di priorità, impatto sul business ed attuale livello di esposizione alle minacce, garantendola capacità di elaborare report periodici sul livello di rischio.

4. Security Information and Event Management (SIEM) e Control Room

La fase di monitoraggio del processo di ISM deve essere supportata da periodiche Verifiche di Sicurezza, dalla gestione dei processi di configurazione e dall'adozione ed integrazione di sistemi di aggregazione dei log e degli eventi (detti SIEM) correlati a strumenti di monitoring e analisi degli eventi sotto forma di Control Room di alto livello.
L'effettiva integrazione di SIEM e Control Room, insieme ai KSI raccolti, permette la gestione in tempo reale di comportamenti anomali e la possibilità di analizzare i dati di sicurezza, anche storici, provenienti dall'insieme eterogeneo dei sistemi IT e dalla rete. Questa tecnologia è utilizzata per trasformare le informazioni dei singoli eventi in dati che possono essere usati a supporto di eventuali indagini a valle di incidenti o reati. E' inoltre uno strumento con cui monitorare in maniera centralizzata l'intero insieme dei processi di sicurezza per migliorare la comprensione di quanto accade sulla propria infrastruttura.

Il bisogno di mantenere un supporto costante alle necessità di monitoraggio, misurazione, compliance e conformità è diventato un importante fattore di mercato che spinge all'implementazione di soluzioni di Control Room.

Emaze Networks

informed security

(Perché) eMaze

La gran parte dei player attivi nel mercato del Risk e Vulnerability Management è rappresentata da Società strettamente impegnate sulla consulenza e da System Integrator, che impiegano tipicamente suite di prodotti o singole componenti di terze parti (*off-the-shelf*), che indirizzano solo in parte l'intero processo di ISM.

eMaze è nel panorama italiano il solo fornitore chiavi in mano dell'intero framework di ISM aziendale.

eMaze combina la propria tecnologia altamente innovativa (ISM Product Suite) con le migliori competenze e know-how nel campo dell'Information e Logical Security.

eMaze ha acquisito la necessaria esperienza per permettere alle grandi imprese e alla Pubblica Amministrazione di integrare l'intero framework di ISM in ambiti complessi, sia in termini di sistemi sia di processi, con la dovuta flessibilità ed efficacia.

eMaze si distingue per la capacità di sviluppare, integrare e portare sul mercato una soluzione completa ed Enterprise-class di Informed Security Management, offrendo alle organizzazioni la possibilità di avere un unico partner per questo tipo di esigenze.
La leadership tecnologica e le particolari capacità di **eMaze** sono state adottate dalle più importanti aziende nei settori Finance, Telco, Utility e Pubblica Amministrazione.

eMaze garantisce la sicurezza dei dati e sistemi aziendali tramite la progettazione, l'implementazione e l'utilizzo di una framework multilivello in grado di correlare le informazioni aziendali con i digital asset, le relative vulnerabilità e i rischi IT, garantendo ai propri Clienti il raggiungimento degli obiettivi di protezione del proprio business con l'ottimale rapporto costo-beneficio, realizzando così il paradigma della cosiddetta Informed Security.

eMaze offre soluzioni di sicurezza proattiva per aiutare le grandi aziende a gestire i rischi di sicurezza e ad adempiere ai requisiti di compliance e conformità.

L'offerta include avanzate soluzioni chiavi in mano nei seguenti campi:

- **Le soluzioni di Informed Security (ISM) con forte focalizzazione alla progettazione e alla realizzazione di Control Room della sicurezza**
- **I Prodotti della suite eMaze ISM**
- **Una serie completa di servizi professionali e di consulenza**
- **La verifica della conformità**
- **L'implementazione degli standard di Information Security**