Risk Assesment: Identificazione degli asset, analisi delle vulnerabilità e analisi delle minacce

23/04/24

Traccia

Creare un report in cui includere:

1. Identificazione valore degli asset

2. Analisi delle vulnerabilità

3. Analisi delle minacce

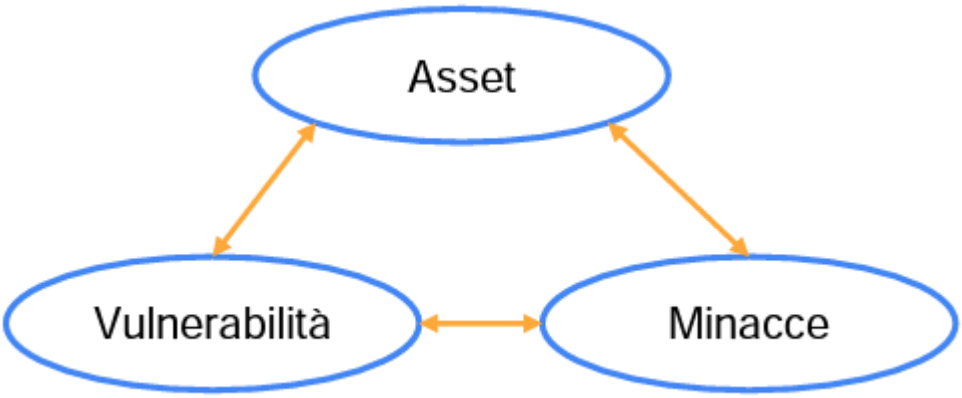
Siete iberidi estendere ed ipotizzarlo scenario, il numerosi asset da cui partire a vostra scelta. Potete utilizzare qualsiasi supporto come CVE, CVSS, tabelle NIST SP 800-30, ecc.

Scenario

Un'azienda vi ha incaricato di svolgere un'analisi delle vulnerabilità e delle minacce sui propri asset organizzativi. L'azienda opera nel settore metal meccanico, produzione di ingranaggi, ha circa 200 impiegati ed un proprio e-commerce. Sono presenti circa 200 pc (1.000 €/pc) e 30 server (3.000 €/server).

Il servizio di cui dispone è: sito-commerce (fatturato10.000 €/giorno), ERP di gestione aziendale (30.000€), server di posta elettronica (5.000€) e un sistema di sicurezza composto da firewall, IDS e SIEM di (25.000€).

Nella gestione del rischio, l'identificazione degli asset, l'analisi delle minacce e delle vulnerabilità avviene in contemporanea e si integrano a vicenda.



Identificazione degli Asset

Lo scopo di un documento per l'identificazione degli asset è fornire una guida dettagliata e strutturata per individuare e catalogare tutti gli asset rilevanti per un'organizzazione. Questo documento serve a garantire una comprensione chiara e completa degli asset disponibili, consentendo all'organizzazione di gestirli in modo efficace, proteggerli adeguatamente e assegnare loro le risorse necessarie per massimizzare il loro valore e mitigare i rischi associati.

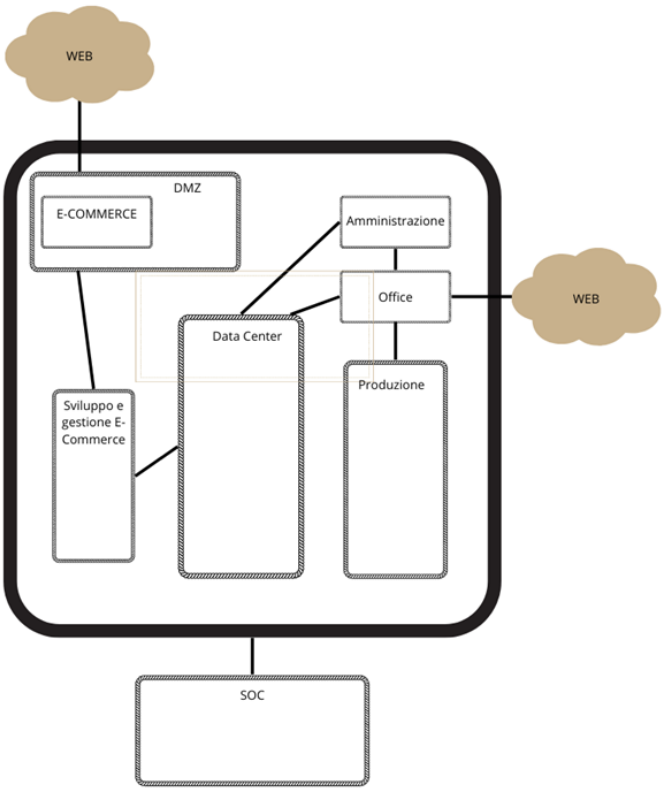
Metodologia di Identificazione degli Asset

La metodologia utilizzata per l'identificazione degli asset si basa su un approccio che coinvolge diversi metodi di raccolta dati e di collaborazione inter dipartimentale all'interno dell'organizzazione.

Da questa suddivisione sono state implementate più fasi per avere una copertura completa di tutti gli asset aziendali.

Analisi dei processi aziendali

Il team responsabile ha condotto un'analisi dettagliata dei processi aziendali in tutte le aree funzionali dell'organizzazione. Questo coinvolgeva interviste con personale chiave, revisione della documentazione esistente, osservazione diretta dei flussi di lavoro e raccolta dei dati online. Da questo lavoro è stata sviluppata una bozza dei vari reparti/flussi dell'organizzazione.



Valutazione degli Asset Fisici: Dotazioni Informatiche

Sono stati identificati e catalogati tutti gli asset fisici appartenenti alle dotazioni informatiche dell'organizzazione. Questo processo ha coinvolto un'ispezione fisica delle strutture e la revisione dei registri patrimoniali esistenti.

Grazie a questo lavoro è stato possibile classificare gli asset informatici tangibili secondo due metodologie:

- **Per processo aziendale dell'asset**
- **Per sensibilità/Riservatezza dell'asset:** vengono definiti sensibili/riservati se le informazioni presenti nell'asset sono critiche e non possono essere esfiltrate/divulgate.

La tabella seguente elenca la classificazione degli asset secondo le due metodologie riportate sopra.

Asset e numero di asset	Reparto	Sensibilità/Riservatezza
Computer x50	Sviluppo e gestione E-Commerce	Si
Computer x50	SOC (security operation center)	
Computer x50	Produzione	
Computer x35	Office	
Computer x15	Amministrazione	Si
Server x5	DMZ : E-commerce	
Server x25	Data Center	Si

Inventario dei Dati e delle Risorse Digitali

È stato eseguito un inventario completo di tutti i dati e delle risorse digitali dell'organizzazione, compresi dati archiviati su server, database, documenti elettronici e altre risorse digitali pertinenti. Il tutto è stato possibile con l'ausilio di un software di gestione aziendale ERP. Un ERP, acronimo di Enterprise Resource Planning (in italiano, pianificazione delle risorse aziendali), è un sistema software integrato progettato per gestire e coordinare le risorse, i processi e le informazioni all'interno di un'organizzazione.

Dati Archiviati sui Server Interni al Data Center:

Server di Database (10 server)

Risorse digitali:

- Database Clienti: Contiene informazioni sui clienti, tra cui nome, indirizzo, contatti, storico degli acquisti.
- Database Prodotti: Catalogo dei prodotti offerti dall'azienda, inclusi descrizioni, prezzi e disponibilità.
- Documenti Aziendali: Archivio di documenti aziendali, tra cui politiche, procedure, contratti e comunicazioni interne.

Server di Backup (5 server)

Risorse digitali:

- Copie di Backup dei Database: Backup giornalieri dei database principali per la sicurezza dei dati.

Server di Gestione del Contenuto (2 server)

Risorse digitali:

- blog o una sezione di contenuti editoriali

Server per applicazioni (3 server)

Risorse digitali:

- Applicazioni Aziendali: Applicazioni per lo sviluppo e gestione dell'E-commerce
- Applicazione Mobile: Applicazione mobile per la gestione degli ordini e il supporto ai clienti.
- Software di Gestione delle Vendite: Applicazione interna per la gestione delle vendite e il monitoraggio delle prestazioni.

Server di Archiviazione (5 server)

Risorse digitali:

- volume elevato di immagini dei prodotti, file multimediali e altri contenuti digitali

Dati archiviati sui server della DMZ (5 server)

Risorse Digitali:

- Sito Web: Contenuto pubblico del sito web aziendale, inclusi pagine informative, blog e risorse scaricabili.
- Portale Clienti: Area riservata ai clienti per l'accesso a informazioni personalizzate, storico degli ordini, ecc.

Valutazione dell'importanza e Determinazione dei costi

Per valutare l'importanza degli asset e determinare i costi associati, vengono utilizzati i valori forniti e le informazioni forniti dallo scenario sull'utilizzo e la sensibilità degli asset.

Valutazione dell'Importanza

Computer:

Sviluppo e gestione E-Commerce (50): Questi computer sono cruciali per lo sviluppo e la gestione dell'ecommerce, che genera un fatturato significativo per l'azienda (€10.000/giorno). L'importanza di questi computer è quindi molto alta.

SOC (security operation center) (50): Anche se non sono direttamente coinvolti nella generazione di entrate, i computer del SOC sono fondamentali per la sicurezza dell'azienda e la protezione dei dati. L'importanza è alta.

Server:

DMZ : E-commerce (5): Questi server supportano l'ecommerce e svolgono un ruolo critico nel mantenere il sito web online e funzionante. L'importanza è molto alta.

Data Center (25): Essendo nel data center, questi server ospitano probabilmente dati aziendali critici. L'importanza è alta.

Risorse digitali:

Database Clienti e Prodotti: Contengono informazioni cruciali per l'operatività dell'azienda e per la soddisfazione dei clienti. L'importanza è molto alta.

Documenti Aziendali: Contengono politiche, procedure e contratti aziendali, fondamentali per il funzionamento aziendale. L'importanza è alta.

Sito Web e Portale Clienti: Fondamentali per l'esperienza dell'utente e per le vendite online. L'importanza è molto alta.

Asset	Importanza	Priorità
Computer (Sviluppo e gestione E-Commerce)	Alta	Alta
Server DMZ per l'E-commerce	Alta	Alta
Database Clienti	Alta	Alta
Database Prodotti	Alta	Alta
Documenti Aziendali	Alta	Alta
Risorse Digitali (Sito Web, Portale Clienti, Archivio)	Alta	Alta
Server nel Data Center	Alta	Alta
Computer (Amministrazione)	Media	Media
Computer (SOC)	Media	Media
Altri server e risorse digitali	Bassa	Bassa

Determinazione dei Costi

Per determinare i costi associati, consideriamo il costo di acquisto e i costi di manutenzione annui per ogni asset:

Computer e Server:

Costo di acquisto per computer: €1000/pc * numero di computer.

Costo di acquisto per server: €3000/server * numero di server.

Risorse digitali:

Costo del software ERP: €30.000.

Costo del server di posta elettronica: €5000.

Costo dei sistemi di sicurezza: €25.000.

Asset	Quantità	Valore Unitario	Totale
Computer	200	€1000	€200.000
Server	30	€3000	€90.000
Risorse digitali			
- Software ERP	1	€30.000	€30.000
- Server di posta elettronica	1	€5000	€5000
- Sistemi di sicurezza	1	€25.000	€25.000

Costi di Manutenzione:

Costi di manutenzione annui per pc, server, software ERP, server di posta elettronica, e sistemi di sicurezza.

Costi di manutenzione annui per i computer:

- €500/pc * numero di computer.

Costi di manutenzione annuali per i server:

- €1500 * numero di server.

Costi di smaltimento annui per i server:

- €700/server * numero di server.

Costi di smaltimento annui per i computer:

- €200/pc * numero di computer.

Costi di manutenzione annui per l'ERP:

- €5000

Costi di manutenzione annui per i sistemi di sicurezza:

- €5000

Asset	Costi di Manutenzione	Costi di Smaltimento Annuo
Computer	€140.000 (€500/pc * 200 + €200/pc * 200)	€40.000 (€200/pc * 200)
Server	€43.500 (€1500 * 30 / 2 + €700/server * 30)	€21.000 (€700/server * 30)
Software ERP	€5.000	-
Server di posta elettronica	-	-
Sistemi di sicurezza	€5.000	-

Analisi delle vulnerabilità

Nella seguente sezione, analizzeremo le vulnerabilità che possono minacciare la sicurezza degli asset informatici identificati all'interno dell'organizzazione. Attraverso questa analisi, faremo presente le potenziali vulnerabilità che possono compromettere la sicurezza degli asset e forniremo raccomandazioni per mitigare tali rischi e proteggere l'integrità, la riservatezza e la disponibilità delle risorse aziendali.

L'analisi delle vulnerabilità degli asset può avvenire da fonti diverse, come i database pubblici di vulnerabilità (CVE, NVD), vulnerability Assessment, Penetration testing ed altre.

Computer:

- **Vulnerabilità:** Le vulnerabilità software per la mancanza di aggiornamenti possono esporre i computer a rischi di sicurezza.

- **Raccomandazioni:** È fondamentale implementare misure di sicurezza come software antivirus e firewall, nonché pratiche di sicurezza informatica come l'aggiornamento regolare del software, monitoraggio delle attività degli utenti e l'istruzione degli utenti sull'uso sicuro dei computer.

Server:

- **Vulnerabilità:** I server possono essere vulnerabili ad attacchi informatici mirati, accessi non autorizzati e malfunzionamenti hardware o software. I server che ospitano dati sensibili, come quelli nel Data Center, sono particolarmente a rischio.

- **Raccomandazioni:** È fondamentale implementare misure di sicurezza avanzate come crittografia dei dati, controllo degli accessi e monitoraggio continuo dei server. È inoltre consigliabile eseguire regolarmente patch e aggiornamenti per proteggere contro le vulnerabilità note.

Analisi delle Vulnerabilità della Rete:

- **Vulnerabilità:** La rete può essere esposta a rischi di intercettazione dei dati, accessi non autorizzati e configurazioni non sicure. Le password deboli, la mancanza di patch e la cattiva configurazione dei dispositivi di rete possono aumentare il rischio di compromissione della sicurezza.

- **Raccomandazioni:** È importante implementare password robuste, applicare patch di sicurezza regolarmente e configurare correttamente i dispositivi di rete. Le tecnologie di crittografia, i firewall e il monitoraggio delle attività di rete possono aiutare a mitigare i rischi e proteggere la sicurezza della rete aziendale.

Software ERP:

- **Vulnerabilità**: Il software ERP può essere vulnerabile a violazioni della sicurezza dei dati, accessi non autorizzati e perdita di integrità dei dati. Le vulnerabilità nel software potrebbero essere sfruttate per ottenere accesso non autorizzato ai dati aziendali sensibili.

- **Raccomandazioni:** È essenziale mantenere il software ERP aggiornato con le patch di sicurezza più recenti e implementare controlli rigorosi sugli accessi per limitare l'accesso solo ai dipendenti autorizzati. La crittografia dei dati sensibili e il monitoraggio delle attività degli utenti possono contribuire a rilevare e prevenire violazioni della sicurezza.

Server di posta elettronica e Sistemi di sicurezza:

- **Vulnerabilità:** I server di posta elettronica e i sistemi di sicurezza potrebbero essere soggetti ad attacchi di phishing, spam e altre minacce informatiche. Le vulnerabilità nella configurazione e nel software possono esporre questi sistemi a rischi di sicurezza.

- **Raccomandazioni:** È consigliabile implementare filtri antispam e anti-phishing per proteggere il server di posta elettronica. Inoltre, è importante monitorare costantemente i sistemi di sicurezza e applicare aggiornamenti regolari per mitigare i rischi di sicurezza.

-

Analisi delle minacce

Nel contesto dell'infrastruttura informatica dell'organizzazione, diverse minacce possono compromettere la sicurezza degli asset identificati. Queste minacce possono provenire da fonti esterne o interne e rappresentare un rischio significativo per l'integrità, la riservatezza e la disponibilità dei dati e delle risorse aziendali.

Le minacce avverse possiamo distinguerle a sua volta tra minacce esterne ed interne.

Minacce Informatiche Esterne

Threat Actors: individui malintenzionati, gruppi criminali organizzati o hacktivisti.

Threat:

- Ransomware
- MALWARE: virus, Trojan o altri programmi dannosi.
- Attacchi DDoS (Distributed Denial of Service)
- Attacchi di Cross site scripting (XSS)
- Attacchi di SQL injection

I server esposti pubblicamente, come quelli utilizzati per l'e-commerce e il server di posta elettronica, possono essere particolarmente vulnerabili a tali attacchi.

Oltre agli attacchi informatici, l'organizzazione deve anche considerare i potenziali disastri naturali, come incendi, alluvioni e terremoti, che possono compromettere l'integrità e la disponibilità dei dati e delle risorse aziendali. La pianificazione della continuità operativa e il disaster recovery sono cruciali per mitigare gli effetti di tali eventi e garantire la continuità delle operazioni aziendali.

Minacce Interne

Threat Actors: dipendenti, fornitori, appaltatori o altri soggetti autorizzati possono abusare delle proprie credenziali per scopi fraudolenti o dannosi.

Threat: Queste minacce possono includere

- accessi non autorizzati ai dati aziendali sensibili
- violazioni della politica aziendale
- sabotaggi intenzionali dei sistemi informatici

Anche se meno comuni rispetto alle minacce esterne, le minacce interne possono avere un impatto significativo sulla sicurezza aziendale.

Altre minacce potenziali possono derivare dalla mancanza di consapevolezza e formazione del personale, che può rendere l'organizzazione vulnerabile a violazioni della sicurezza causate da errori umani o comportamenti non sicuri. La mancanza di controllo degli accessi e di procedure di sicurezza efficaci può anche esporre l'organizzazione a rischi legati alla violazione della riservatezza e alla perdita di dati sensibili.