DIGITAL RISK MANAGER - ALEX FIORILLO

RISK MANAGEMENT
ASSET ORGANIZZATIVI, MINACCE E VULNERABILITà

INTRODUZIONE

Un’azienda vi ha incaricato di svolgere un'analisi delle vulnerabilità e delle minacce sui propri sistemi organizzativi. L'azienda opera nel settore metalmeccanico, 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). I servizio di cui dispone sono: sito e-commerce (fatturato 10.000 €/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.

Creare un report in cui includere:
1. Identificazione e valore degli asset
2. Analisi Delle Vulnerabilità
3. Analisi Delle Minacce

1. IDENTIFICAZIONE E VALORE DEGLI ASSET

Identificazione degli asset: riconoscere e catalogare tutte le risorse possedute dall’azienda, sia tangibili (immobili, macchinari) che intangibili (brevetti, marchi, know-how). Eseguire un inventario completo e accurato, aggiornandolo regolarmente.

Attribuzione del valore: assegnare un valore monetario a ciascuna risorsa, tenendo conto della sua importanza e del suo costo. Utilizzare diverse metodologie di valutazione, come il

costo storico, il valore attuale netto o il valore di mercato. Considerare l'utilizzo di strumenti di analisi finanziaria per ottenere stima precisa del valore.

Asset (tangibili e non)

1. Hardware:
200 pc (1000€ cad.) = 200000€
30 server (3000€ cad.) = 90000€

2. Servizi:
Sito e-commerce (Fatturato giornaliero: 10000€/giorno)
ERP = 30000€
Server di posta elettronica = 5000€
Sistemi di sicurezza (firewall, IDS, SIEM) = 25000€

3. Capitale umano:
200 dipendenti = 90€/giorno

4. Immobili:
4 immobili = 1000000€

Totale valore degli asset:
Il totale effettivo del valore degli asset nel loro insieme non è realmente quantificabile in base ai dati a nostra disposizione.
Sarebbe opportune stimare anche l'importanza che ognuno di questi ha, cosa che potrebbe alterare anche drasticamente (sia in maniera positiva che negativa) il loro valore effettivo.
Prendiamo ad esempio i server, sappiamo che la macchina fisica costa all'azienda 3000€ ma non conosciamo il reale valore dei dati che contiene al suo interno, potrebbe contenere dati sensibili sugli acquirenti, sui fornitori, sui dipendenti, contratti o brevetti dei loro ingranaggi.
Questo non ci permette di effettuare una stima reale ed effettiva in quanto non conosciamo l'importanza (e quindi anche l'impatto) che quell'asset ha per l'azienda.

Inoltre non stiamo considerando, per quanto concerne soprattutto gli asset tangibili, i vari costi di ammortamento, gestione, manutenzione o il loro costo storico che sono tutti dati necessari per calcolare il loro effettivo valore di mercato al giorno d'oggi.

2. ANALISI DELLE VULNERABILITà

Vulnerabilità: debolezza nella progettazione, nell'implementazione, nell'operatività o nel controllo interno di un processo che potrebbe esporre il sistema a rischi negativi derivanti da threat events.

Analisi delle vulnerabilità: processo che permette di identificare e classificare le vulnerabilità.
La valutazione delle vulnerabilità potrebbe includere l'esame di tutti gli aspetti di un asset o capacità per determinare eventuali vulnerabilità presenti, comprese le vulnerabilità fisiche, tecniche e operative proprie dell'asset.

Per quanto riguarda le vulnerabilità dei sistemi, possiamo identificare:

PC e SERVER:
- Mancanza di aggiornamenti software regolari
- Possibili attacchi via email (phishing, malware)
- Vulnerabilità dei servizi esposti (es. HTTP, SSH)
- Password deboli o non cambiate regolarmente
- Mancanza di patch di sicurezza aggiornate

SITO E-COMMERCE:
- Vulnerabilità legate alla gestione delle sessioni utente e ai pagamenti online
- Possibili falle di sicurezza nella gestione dei dati dei clienti

ERP:
- Vulnerabilità nei protocolli di comunicazione e nell'accesso remoto
- Possibili rischi legati alla gestione dei dati sensibili dei dipendenti e dei clienti
- Potenziali falle di sicurezza nella gestione degli account utente e dei privilegi di accesso

SERVER DI POSTA ELETTRONICA:

- Vulnerabilità legate alla sicurezza delle email, inclusi attacchi phishing e spoofing
- Possibili rischi di perdita di dati sensibili attraverso email non crittografate o non protette

3. ANALISI DELLE MINACCE

Minaccia: una minaccia è una potenziale causa di un incidente indesiderato, che può produrre danni a un sistema o a un'organizzazione.

Analisi delle minacce: processo sistematico che mira a identificare tutte le minacce che hanno una ragionevole probabilità di verificarsi e quindi possono compromettere la sicurezza di un'organizzazione, di un sistema o di un asset.

Possiamo categorizzare le minacce come *interne*, *esterne* ed *ambientali.*

Minacce esterne

HACKING E ATTACCHI INFORMATICI:

- Attacchi di ransomware sui sistemi
- Furto di dati dei clienti dall'e-commerce
- Attacchi DDoS per interrompere le attività commerciali
- Possibili attacchi via email (phishing, malware)

Minacce interne

DIPENDENTI INTERNI:

- Accesso non autorizzato ai dati aziendali
- Scarso rispetto delle politiche di sicurezza informatica

ERRORI UMANI:

- Invio accidentale di email contenenti dati sensibili
- Configurazione errata dei sistemi di sicurezza

Minacce ambientali

GUASTI HARDWARE:

- Malfunzionamento dei server o dei computer a causa di componenti difettosi

DISASTRI NATURALI:

- Danni fisici agli immobili o agli impianti dell'azienda causati da calamità naturali come alluvioni, terremoti, uragani, incendi, ecc.

Esempio report riassuntivo analisi delle minacce

Minaccia	Descrizione	Vettore di Attacco	Fonte di Minaccia	Probabilità (Prima)	Controllo di Mitigazione	Costo Mitigazione	Probabilità (Dopo)
Malware Ransomware	Cripta i dati dell'organizzazione con richiesta di riscatto	Email di phishing, siti web malevoli	Attori criminali	Alta	Formazione sulla sicurezza informatica, software antivirus/antimalware, backup regolari	Medio	Bassa
Attacco DDoS	Sovraccarica i server web con traffico malevolo	Botnet di dispositivi compromessi	Hacker, Gruppi di attivisti	Media	Implementazione di un servizio di protezione DDoS, firewall applicativo web (WAF)	Alto	Bassa
Accesso non autorizzato	Hacking dei sistemi tramite sfruttamento di vulnerabilità	Rete, applicazioni web	Hacker, Insider	Media	Autenticazione a due fattori (2FA), VPN, segmentazione della rete	Medio	Bassa
Perdita di dati	Furto o esposizione di dati sensibili	Dispositivi portatili persi, insider, data breach	Insider, Hacker	Bassa	Crittografia dei dati, DLP (Data Loss Prevention), controllo degli accessi	Alto	Molto Bassa
Errore umano	Configurazioni errate, violazioni di policy di sicurezza	Azioni degli utenti interni	Dipendenti	Alta	Formazione sulla sicurezza informatica, policy di sicurezza chiare e definite	Basso	Media
Disastro naturale	Interruzione dei servizi a causa di calamità naturali	Eventi ambientali	Fonti naturali	Bassa	Backup off-site, piani di disaster recovery	Alto	Bassa