CONSEGNA 23 APRILE S1L2

Introduzione

Un’azienda vi ha incaricato di svolgere un’analisi delle vulnerabilità e delle minacce sui propri asset 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 (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.

Obbiettivo

Creare un report in cui includere:
1. Identificazione e valore degli asset
2. Analisi delle vulnerabilità
3. Analisi delle minacce

INDICE

1. Asset value

1.1 Identificazione degli asset

Risorse fisiche:

- **PC** (200 unità)
- **Server** (30 unità)

Risorse immateriali:

- **Sito e-commerce**
- **ERP (Enterprise Resource Planning)**
- **Server di posta elettronica**
- **Sistema di sicurezza** (firewall, IDS, SIEM)
- **Dipendenti** 200

1.2 Valutazione dell'importanza

- **Analisi dell'Impatto**: Determinare come ciascun asset contribuisce agli obiettivi aziendali:
    - PC e server sono essenziali per le operazioni quotidiane e il supporto del sito e-commerce.
    - Il sistema ERP è critico per la gestione efficiente delle operazioni aziendali.
    - Brevetti e know-how sono vitali per mantenere un vantaggio competitivo nel settore.

Classificazione: Assegnare un punteggio di importanza basato su fattori quali critico, importante e non critico

Livello critico : ERP, Sito e - commerce

Livello importante : PC, server

Livello non critico: Mobili ufficio

1.3 Determinazione dei costi

Tabella di determinazione dei costi degli asset

Categoria Asset	Quantità	Costo di Acquisizione (€)	Costi di Manutenzione Annuale (€)	Ammortamento (anni)	Obsolescenza
PC	200	200.000	10.000	4	Alta
Server	30	90.000	4.500	5	Media
Sito e-commerce	1	n/a	2.000	n/a	Alta
ERP	1	30.000	1.500	5	Bassa
Server di posta	1	5.000	500	5	Media
Sistema di sicurezza	1	25.000	2.500	5	Bassa

Note sulla Tabella:

- **Costo di Acquisizione**: È il prezzo d'acquisto iniziale degli asset. Per il sito e-commerce, l'ERP e altri software, il costo può variare ampiamente a seconda della personalizzazione e delle funzionalità aggiuntive.
- **Costi di Manutenzione Annuale**: Stime per il mantenimento operativo, aggiornamenti, e supporto tecnico.
- **Ammortamento**: Il periodo di tempo su cui il valore dell'asset viene distribuito. Per hardware tecnologico come PC e server, un periodo di 4-5 anni è comune a causa dell'avanzamento tecnologico rapido.
- **Obsolescenza**: Indica quanto velocemente un asset perde il suo valore funzionale. "Alta" indica una rapida obsolescenza, spesso vista con tecnologie avanzate come i PC e i componenti e-commerce.

Dettagli Aggiuntivi

- Il sito e-commerce e l'ERP, essendo principalmente software, possono non avere un ammortamento tradizionale in termini fisici, ma possono subire deprezzamento per obsolescenza tecnologica o per cambiamenti nel mercato.
- La manutenzione del software include l'aggiornamento per mantenere il sistema sicuro e efficiente.
- Le stime potrebbero necessitare di ulteriori dettagli finanziari specifici dell'azienda per una valutazione più precisa.

1.4 Attribuzione del valore

Tabella di valutazione degli asset

Categoria Asset	Costo di Acquisizione (€)	Valore Attuale Netto (VAN)	Valore di Mercato (€)	Metodo di Valutazione Utilizzato	Note sulla Valutazione
PC	200.000	150.000	100.000	Costo storico / Deprezzamento	Obsolescenza alta
Server	90.000	70.000	45.000	Costo storico / Deprezzamento	Obsolescenza media
Sito e-commerce	n/a	400.000	450.000	Valore attuale netto	Importanza alta, crescente
ERP	30.000	50.000	55.000	Valore attuale netto	Importanza strategica
Server di posta	5.000	3.000	2.500	Costo storico / Deprezzamento	Obsolescenza media
Sistema di sicurezza	25.000	20.000	22.000	Costo storico / Deprezzamento	Importanza alla sicurezza

Metodi di Valutazione:

- **Costo Storico** : Valore basato sul costo originale di acquisizione degli asset meno l'ammortamento accumulato. Visto che l; azienda è appena aperta, il costo storico corrisponde al costo di acquisizione
- **Valore Attuale Netto (VAN)**: Calcolato proiettando i flussi di cassa futuri attesi dall'uso dell'asset e scontandoli al tasso di interesse attuale. Utilizzato per software e sistemi con impatti diretti sulle entrate.
- **Valore di Mercato**: Stima del prezzo che gli asset potrebbero ottenere se venduti nel mercato attuale.

Note sulla Valutazione:

- **PC e Server**: Valutati principalmente sul costo storico, considerando un alto tasso di obsolescenza tecnologica.
- **Sito e-commerce e ERP**: Il loro valore è principalmente derivato dai benefici economici futuri che possono generare, quindi si utilizza il VAN e il valore di mercato.
- **Sistema di sicurezza**: Importante per la protezione dei dati e delle operazioni, valutato meno del costo di acquisizione a causa della deprezzazione tecnologica, ma ancora vitale per l'operatività aziendale.

2. Analisi delle vulnerabilità

Per identificare le vulnerabilità si possono utilizzare database come il Common Vulnerabilities and Exposures (CVE) e valutare il rischio di ciascuna vulnerabilità usando il Common Vulnerability Scoring System (CVSS). Si effettueranno scansioni dei sistemi per identificare eventuali vulnerabilità conosciute.

- **Scansione dei PC e Server**: Utilizzare strumenti di vulnerability scanning per identificare vulnerabilità note nei sistemi operativi e nelle applicazioni installate.
- **Analisi del sito e-commerce e del server ERP**: Verificare la presenza di vulnerabilità nel software del server web, nelle applicazioni e-commerce e ERP, specialmente quelle legate a SQL Injection, XSS, e altre vulnerabilità web comuni.
- **Server di posta elettronica**: Analizzare per problemi di configurazione, come cifratura debole, e vulnerabilità di software come quelle riportate nei CVE recenti.
- **Sistema di sicurezza**: Controllare le configurazioni e gli aggiornamenti di firewall, IDS e SIEM per assicurare che siano privi di vulnerabilità note.

2.1 classificazione delle vulnerabilità / 27005 ANNEX D

Possiamo classificare le vulnerabilità per comprendere meglio la natura, le caratteristiche e il potenziale impatto delle diverse vulnerabilità , stabilire la priorità di intervento e allocare le risorse in modo efficiente.

PC e Server

- **Vulnerabilità Hardware**:
  - Insufficiente manutenzione o installazione errata.
  - Suscettibilità a umidità, polvere, variazioni di temperatura o variazioni di tensione.
  - Archiviazione non protetta e mancanza di controllo delle configurazioni.
- **Minacce Hardware Correlate**:
  - Deterioramento o distruzione fisica dell'hardware.
  - Furto di dati attraverso il furto fisico di media.
  - Interruzioni dovute a fenomeni meteorologici o perdite di alimentazione.

Sito e-commerce e ERP

- **Vulnerabilità Software**:
  - Software distribuito su larga scala potrebbe avere vulnerabilità note.
  - Interfacce utente complesse possono portare a errori nell'uso.
  - Manutenzione del software e gestione delle patch inadeguate.
- **Minacce Software Correlate**:
  - Abuso dei diritti (come i diritti amministrativi ottenuti illegittimamente).
  - Corruzione dei dati attraverso attacchi mirati.

Server di Posta Elettronica

- **Vulnerabilità Software**:
  - Gestione scadente delle password.
  - Mancanza di tracciamento delle attività (audit trail).
  - Utilizzo di software non aggiornato o nuova versione senza sufficiente testing.
- **Minacce Software Correlate**:
  - Spamming o phishing.
  - Interferenza o abuso dei diritti di accesso.

Sistema di Sicurezza (Firewall, IDS, SIEM)

- **Vulnerabilità di Rete**:
  - Architettura di rete insicura.
  - Comunicazioni non protette e traffico sensibile non criptato.
  - Single point of failure nella rete di sicurezza.
- **Minacce di Rete Correlate**:
  - Eavesdropping (intercettazioni) e spionaggio remoto.
  - Saturazione del sistema informativo e fallimento delle attrezzature di telecomunicazione.

3 Analisi delle minacce / NIST SP 800-30

Basandoci sul framework fornito dalla NIST SP 800-30 e sulle informazioni relative all'azienda metalmeccanica fornite, possiamo estrapolare una valutazione delle minacce per alcuni asset aziendali:

Asset: 200 PC e 30 Server

Minacce Potenziali:

- **Malware e Ransomware:** Potrebbero crittografare dati vitali, interrompendo le operazioni aziendali.
- **Attacchi di rete:** Gli attacchi DoS/DDoS potrebbero mirare ai server per interrompere le operazioni di produzione e di e-commerce.
- **Accesso fisico non autorizzato:** Potrebbe portare al furto o al danno fisico dei dispositivi.

Valutazione della Minaccia:

- **Frequenza:** Elevata per malware e ransomware, media per attacchi di rete, bassa per accesso fisico non autorizzato.
- **Impatto:** Elevato in termini di perdita di dati e interruzione delle operazioni.
- **Gravità del Rischio:** Elevata data la potenziale interruzione significativa delle attività aziendali.

Asset: Sito e-commerce

Minacce Potenziali:

- **Intrusioni Web:** Come SQL injection o cross-site scripting (XSS) che possono compromettere i dati dei clienti.
- **Furto di identità digitale:** Rubare le credenziali degli utenti per commettere frodi.
- **Fishing e ingegneria sociale:** Per ottenere accesso ai sistemi interni tramite credenziali di dipendenti.

Valutazione della Minaccia:

- **Frequenza:** Elevata per le intrusioni web e il phishing.
- **Impatto:** Elevato a causa del potenziale danno reputazionale e della perdita di reddito.
- **Gravità del Rischio:** Elevata, considerando l'importanza dell'e-commerce per i ricavi giornalieri.

Asset: ERP (Enterprise Resource Planning)

Minacce Potenziali:

- **Interruzioni del servizio:** Gli attacchi DoS/DDoS potrebbero rendere inaccessibile l'ERP.
- **Violazioni dei dati:** Accesso non autorizzato ai dati finanziari e operativi sensibili.
- **Errore umano:** Configurazione errata o uso improprio potrebbe portare a perdite di dati.

Valutazione della Minaccia:

- **Frequenza:** Media per violazioni dei dati, bassa per interruzioni del servizio e errori umani.
- **Impatto:** Elevato a causa della centralità dell'ERP nelle operazioni aziendali.
- **Gravità del Rischio:** Media, l'impoverimento dei dati potrebbe avere conseguenze a lungo termine sulla gestione aziendale.