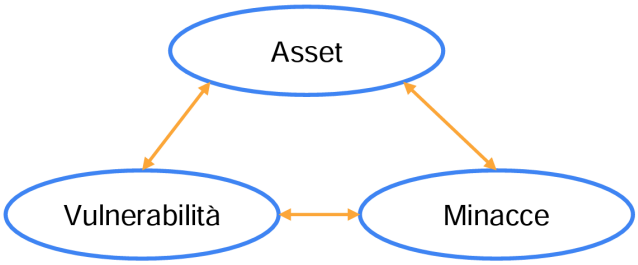
INDICE

1. **Traccia**
2. **Identificazione e valore degli asset**
3. **Analisi delle vulnerabilità**
4. **Analisi delle minacce**
5. **Conclusioni**

1. Traccia - Asset organizzativi, minacce e vulnerabilità

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 (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

Siete liberi di estendere ed ipotizzare lo scenario, il numero di asset da cui partire è a vostra scelta.

Potete utilizzare qualsiasi supporto come CVE, CVSS, tabelle NIST SP 800-30, ecc.

Obiettivo del report

Il presente report mira ad illustrare gli obiettivi dell'analisi, che includono l'identificazione e la valutazione degli asset critici, l'analisi delle vulnerabilità presenti e delle minacce potenziali, al fine di migliorare le strategie di sicurezza aziendale.

Esecuzione dei task

1. Identificazione e valore degli asset

Gli asset in un contesto di sicurezza informatica si riferiscono a qualsiasi risorsa di valore per l'organizzazione che deve essere protetta. Questi possono includere hardware fisico come computer e server, software come applicazioni e database, dati aziendali e informazioni sensibili, servizi online come l'e-commerce e l'infrastruttura di rete.

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.

È necessario svolgere un'analisi dettagliata dei processi aziendali in tutte le aree funzionali dell'organizzazione. Questo prevede interviste con il personale, revisione della documentazione esistente e delle direttive, osservazione diretta dei flussi di lavoro e raccolta dei dati online. Da questa analisi è possibile identificare i diversi asset coinvolti nel workflow dell'organizzazione.

Gli asset identificati includono:

Risorse fisiche

- Computer: circa 200 personal computer utilizzati dai dipendenti per le operazioni
- quotidiane.
- Server: 30 server che ospitano vari servizi e applicazioni.

Risorse Umane
Dipendenti (200)

Risorse immateriali/Servizi

- Sito e-commerce: un sito di e-commerce che genera un fatturato significativo per
- l'azienda.
- ERP (Enterprise Resource Planning) di gestione aziendale: un sistema ERP utilizzato per la gestione delle operazioni aziendali.
- Server di posta elettronica: un server dedicato alla gestione della posta elettronica aziendale.
- Sistema di sicurezza: un sistema di sicurezza composto da firewall, IDS (Intrusion Detection System) e SIEM (Security Information and Event Management).

Valutazione degli asset

Valutazione dell'importanza: Analizzare l'impatto di ogni risorsa sul raggiungimento degli obiettivi aziendali. Considerare fattori come la rarità, la criticità e il potenziale di crescita. Assegnare un punteggio o una classificazione a ciascuna risorsa in base alla sua importanza strategica. Nella tabella il "Valore Asset" rispecchia le conclusioni dell'analisi dell'importanza dell'asset. Attraverso l'**analisi dell'impatto** definiamo in che modo ciascun asset contribuisce agli obiettivi aziendali.

La protezione dei dati sensibili, dei brevetti e del know-how sono importantissimi per mantenere un vantaggio competitivo. I sistemi ERP integrano e automatizzano i processi aziendali chiave, come la

gestione finanziaria, la gestione della supply chain, la produzione e le vendite. PC e server sono essenziali per le operazioni quotidiane e il supporto del sito e-commerce.

Il **valore di un asset** non è solo il suo costo fisico, ma include anche il costo di sostituzione o riparazione, il valore dei dati o delle informazioni che contiene, l'impatto sulla reputazione dell'azienda in caso di perdita o compromissione.

Tabella Costo-Valore di ciascun asset

Per determinare i costi e il valore degli asset è importante considerare diversi fattori come ad esempio il costo di acquisto, i costi di gestione e di manutenzione o ammortamento, dettagliati nella tabella seguente.

ASSET	Quantità	Costo Asset	Valore Asset
PC	200	200.000 €	È elevato considerando software e licenze, manutenzione, dati sensibili, integrazione con l'infrastruttura IT aziendale (come reti, server e sistemi di archiviazione), obsolescenza tecnologica.
SERVER	30	90.000 €	Dobbiamo considerare i costi di gestione, di manutenzione, costi energetici, licenze, obsolescenza tecnologica.
IMPIEGATI	200	500.000 €/mese	Dobbiamo considerare la formazione e il costo delle certificazioni necessarie.
SITO E-COMMERCE	1	— — — —	Fatturato 10.000 €/giorno. Più elevato considerando l'impatto sulla reputazione aziendale e la perdita finanziaria in caso di interruzione del servizio.
ERP	1	30.000 €	È critico per la gestione efficiente delle operazioni aziendali e un'interruzione del servizio avrebbe un impatto negativo notevole.
SERVER MAIL	1	5.000 €	Dobbiamo considerare i costi di gestione, di manutenzione, costi energetici, licenze, obsolescenza tecnologica.
SISTEMI DI SICUREZZA	Firewall, IDS e SIEM	25.000 €	Hanno funzioni principali come la protezione dei dati aziendali, delle infrastrutture IT, delle risorse fisiche, la gestione del rischio ed il miglioramento della reputazione.

Esempio **Server Mail** con le seguenti caratteristiche:

- Sistema operativo: Windows Server
- Software di posta elettronica: Microsoft Exchange Server
- Numero di utenti: 50
- Consumo energetico: 200 watt

I costi annuali stimati per questo server mail potrebbero essere:

- **Costi di gestione:** 1.000€/anno
- **Costi di manutenzione:** 500€/anno
- **Costi energetici:** 360€/anno (costo energia elettrica 0,2 €/kWh)
- **Costi di licenze:** 2.000€/anno (licenze Microsoft Exchange Server)
- **Costo totale:** 3.860€/anno

Criticità
La determinazione della criticità di un asset o di un evento si basa su una valutazione di diversi fattori, tra cui:

- **Impatto potenziale:** La gravità delle conseguenze negative che potrebbero verificarsi in caso di incidente o malfunzionamento.
- **Probabilità di accadimento:** La likelihood che l'incidente o il malfunzionamento si verifichi.
- **Valore dell'asset:** L'importanza dell'asset per l'azienda in termini di funzionalità, dati o processi aziendali.
- **Conformità a normative:** Le implicazioni legali o regolatorie di un incidente o malfunzionamento.
- **Danno alla reputazione:** L'impatto negativo sull'immagine e sulla reputazione dell'azienda in caso di incidente o malfunzionamento.

Classifichiamo gli asset per livello di criticità:

Alto: E-commerce, ERP, PC

Medio: Impiegati, Server, Sistemi di sicurezza

2. Analisi delle vulnerabilità

Nella seguente sezione, analizzeremo le vulnerabilità che possono minacciare la sicurezza degli asset informatici identificati all'interno dell'organizzazione.

L'analisi delle vulnerabilità parte con l'utilizzo di metodi di scansione delle vulnerabilità automatizzati che esaminano i sistemi informatici alla ricerca di vulnerabilità conosciute ed eseguono una scansione delle reti aziendali, identificando le debolezze a livello di software e hardware. Successivamente, penetration testing manuali mettono alla prova la robustezza delle difese esistenti, simulando attacchi cyber contro i sistemi aziendali per scoprire vulnerabilità non ancora note o non rilevate dagli scanner automatici. Una revisione manuale delle configurazioni di sistema e del codice sorgente consente di identificare lacune potenziali nelle policy di sicurezza e nei codici di programmazione. Per avere informazioni aggiornate sulle vulnerabilità note e le specifiche soluzioni è quindi possibile consultare database pubblici di vulnerabilità (CVE, NVD) e servirsi di Vulnerability Assessment e Penetration testing.

PC

Vulnerabilità:
- Possibili attacchi via email di phishing o malware
- Vulnerabilità software per la mancanza di aggiornamenti
- Mancanza di patch di sicurezza aggiornate
- Vulnerabilità dei servizi esposti (es. HTTP, SSH)
- Password deboli o non aggiornate regolarmente
- Sistema operativo obsoleto

Raccomandazioni: È fondamentale implementare misure di sicurezza come software antivirus e firewall, nonché pratiche di sicurezza informatica come l'aggiornamenti regolari, monitoraggio delle attività degli utenti e la formazione degli utenti all'uso sicuro dei pc.

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.

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:
- Errata configurazione del software
- Possibili rischi legati alla gestione dei dati sensibili dei dipendenti e dei clienti
- Accessi non autorizzati
- Vulnerabilità nei protocolli di comunicazione e nell'accesso remoto
- Potenziali falle di sicurezza nella gestione degli account utente e dei privilegi di accesso

Raccomandazioni: È essenziale mantenere il software aggiornato con le patch di sicurezza più recenti e implementare controlli robusti sugli accessi per limitare l'accesso solo agli utenti autorizzati. La crittografia e il monitoraggio delle attività possono contribuire a rilevare e prevenire violazioni malevole.

Sito e-commerce

Vulnerabilità:
- Possibili falle di sicurezza nella gestione dei dati dei clienti
- Configurazione non sicura
- Vulnerabilità legate alla gestione delle sessioni utente e dei pagamenti online
- Vulnerabilità SQL Injection

Server Mail e Sistemi di sicurezza

Vulnerabilità:
- Errata configurazione
- Vulnerabilità legate alla sicurezza delle email, inclusi attacchi phishing, spoofing e spam
- Possibili perdite di dati sensibili per assenza di adeguate misure di crittografia
- Password deboli: password predefinite, troppo brevi o vecchie

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.

Oltre alle vulnerabilità dei sistemi informatici, consideriamo le vulnerabilità delle infrastrutture fisiche come l'assenza di sistemi di allarme, videosorveglianza o controllo degli accessi o i rischi di guasti hardware e le vulnerabilità dei processi aziendali come la mancanza di procedure di sicurezza chiare e documentate o non in linea con le regolamentazioni vigenti.
I dipendenti stessi e le loro azioni sono un'importante vulnerabilità potenziale. Ad esempio la mancanza di attenzione nella distruzione dei rifiuti o la formazione insufficiente del personale sui rischi informatici e sulle procedure di sicurezza aziendale.

3. Analisi delle minacce

È fondamentale per qualsiasi azienda identificare e valutare queste minacce per poter implementare le opportune misure di mitigazione e ridurre al minimo il loro impatto.

Minacce Esterne
Threat Actors: individui malintenzionati, gruppi criminali organizzati o gruppi hacker.
Threat:

- Perdita di dati o documenti sensibili
- Furto di dati sensibili/confidenziali
- Abuso di privilegi di accesso
- Accesso non autorizzato ai sistemi aziendali o ai database
- Intercettazione di dati in chiaro
- Interruzione della comunicazione e dei servizi
- Attacchi Malware (Ransomware, Trojan), attacchi DDoS, attacchi di cross-site scripting (XSS), SQL injection
- Ingegneria sociale e phishing
- Attacchi alla Supply chain

Altri fattori esterni da considerare:

- **Cambiamenti normativi:** Nuove leggi e regolamenti possono comportare obblighi aggiuntivi per l'azienda, costi extra e potenziali sanzioni in caso di non conformità.
- **Danni alla reputazione:** Pubblicità negativa, scandali, prodotti difettosi o un servizio clienti scadente possono danneggiare la reputazione dell'azienda e non incentivare l'engagement del cliente.
- **Concorrenza:** L'ingresso di nuovi competitor sul mercato, l'innovazione da parte delle aziende già presenti e le fluttuazioni delle condizioni economiche possono rappresentare una minaccia per la quota di mercato e la redditività dell'azienda.
- **Crisi economiche**

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

- Accessi non autorizzati ai dati aziendali sensibili
- Violazioni della politica aziendale
- Scarso rispetto delle politiche di sicurezza informatica
- Sabotaggi intenzionali dei sistemi informatici

Altri fattori interni da considerare:

- **Abusi da parte dei dipendenti:** Utilizzo improprio dei sistemi aziendali, accesso non autorizzato ai dati sensibili o divulgazione non autorizzata di informazioni riservate.

- **Errori umani:** Eliminazione accidentale di dati critici, configurazioni errate dei server, password deboli, invio accidentale di email contenenti dati sensibili, configurazione errata dei sistemi di sicurezza.

Minacce Ambientali
- **Disastri naturali:** Eventi come terremoti, alluvioni, incendi o inondazioni possono causare danni alle proprietà aziendali, interruzioni delle operazioni e perdite finanziarie.
- **Guasti hardware:** malfunzionamenti dei server o dei PC

4. Conclusioni

In questo report, abbiamo presentato un'analisi approfondita delle minacce e delle vulnerabilità che l'azienda deve affrontare. L'identificazione e la valutazione degli asset critici ci hanno permesso di comprendere quali sono le risorse più esposte a potenziali attacchi. L'analisi delle vulnerabilità e delle minacce ha evidenziato i punti deboli dell'infrastruttura IT e i rischi concreti che potrebbero portare a danni finanziari, perdita di dati e reputazione.
Sono quindi necessarie misure di prevenzione, controllo e risposta agli incidenti informatici per mitigare gli effetti di eventi critici.

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

Alcuni consigli e best practice:
- Monitoraggio continuo dei sistemi
- Implementazione di piani di backup e ripristino
- Formazione dei dipendenti sulle best practice di sicurezza
- Segmentazione della rete
- Distribuzione del traffico su più dispositivi
- Implementazione di soluzioni di sicurezza come firewall, antivirus, e software di rilevamento delle minacce
- Aggiornamento regolari dei software e delle patch di sicurezza su PC e server

È inoltre essenziale elaborare procedure di emergenza per garantire la continuità operativa in caso di incidenti e produrre Disaster Recovery Plan (DRP) e Business Continuity Plan (BCP) abbinati a consulenze esterne specialistiche. Un approccio proattivo alla sicurezza informatica permetterà all'azienda di affrontare le sfide future con maggiore consapevolezza e resilienza.