IDENTIFICAZIONE ASSET

AZIENDA:

- essa opera nel settore metalmeccanico, nella produzione di ingranaggi

RISORSE:

- 200 impiegati
- Web Site e-Commerce
- 200 Pc (1000 € per pc)
- 30 server (3000 € per server)
    - **SERVIZZI:**
        - e-Commerce (fatturato 10k al giorno)
        - ERP di gestione aziendale (30k mensili)
        - server di posta elettronica (5k)
        - sistema composto da, Firewall, IDS e SIEM di (25k)

ANALISI DELLE MINACCE.

MINACCE ESTERNE:

- **Hacking e attacchi informatici:** tentativi di accesso non autorizzato ai server aziendali per rubare dati o interrompere i servizi.

- **Attacchi DDoS:** sovraccarico dei server e-commerce per renderli inutilizzabili.

- **Furto di dati dei clienti:** accesso non autorizzato ai database dell'e-commerce per rubare informazioni personali o di pagamento.

MINACCE INTERNE:

- **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.

MINACCE AMBIENTALI:

- **Guasti hardware:** malfunzionamenti dei server o dei PC a causa di componenti difettosi.

- **Disastri naturali:** danni fisici agli edifici o agli impianti causati da incendi, alluvioni, terremoti, ecc.

ANALISI DELLE VULNERABILITÀ.

Vulnerabilità dei sistemi informatici:

- **Mancanza di aggiornamenti software:** mancata installazione di patch di sicurezza o aggiornamenti del sistema operativo.

- **Configurazioni di rete insicure:** porte aperte non necessarie, protocolli non sicuri.

- **Password deboli:** password predefinite o facilmente indovinabili.

Vulnerabilità delle infrastrutture fisiche:

- **Mancanza di misure di sicurezza fisica:** assenza di sistemi di allarme, videosorveglianza o controllo degli accessi.

- **Rischio di guasti hardware:** mancanza di manutenzione preventiva sui server e sui PC.

Vulnerabilità dei processi aziendali:

- **Mancanza di procedure di sicurezza documentate:** politiche e linee guida non chiare per la gestione dei dati e degli accessi.

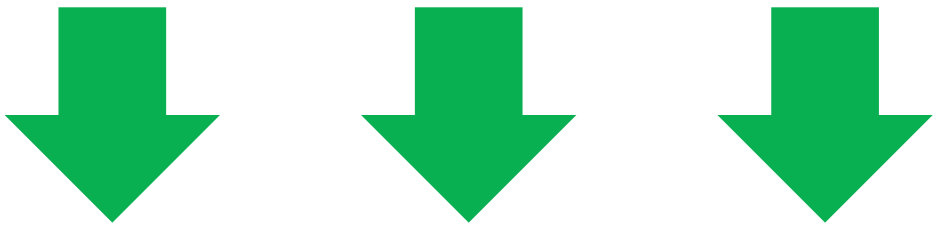
- **Formazione insufficiente del personale:** dipendenti non informati sui rischi informatici e sulle procedure di sicurezza aziendale.

PIANIFICAZIONE DELLE CONTROMISURE:

- **Implementazione di soluzioni di sicurezza informatica:** come firewall, antivirus, e software di rilevamento delle minacce.
- **Aggiornamento regolari:** dei software e delle patch di sicurezza su PC e server.
- **Miglioramento della sicurezza:** fisica degli edifici con sistemi di allarme e videosorveglianza.
- **Elaborazione di procedure:** di emergenza e backup dei dati per garantire la continuità operativa in caso di incidenti.

TABELLA CON RIFERIMENTO AL MODELLO:

- NIST 800-30R1



MINACCIA	DESCRIZIONE	PROBABILITÀ	IMPATTO POTENZIALE	LIVELLO DI RISCHIO	CONTROMISURE
Attacco informatico	Tentativo di violare la sicurezza informatica dell'azienda attraverso hacking, malware o phishing.	Alta	Elevato: compromissione dei dati sensibili, interruzione delle operazioni aziendali, danni alla reputazione.	Elevato	Implementazione di firewall, antivirus, autenticazione a due fattori, formazione del personale sulla sicurezza informatica.
Guasto hardware	Malfunzionamento o rottura di attrezzature hardware critiche per le operazioni aziendali.	Media	Moderato: interruzioni delle operazioni, perdita di dati temporanea, possibili costi di riparazione o sostituzione.	Medio	Implementazione di sistemi di backup regolari, manutenzione preventiva delle attrezzature, contratti di assistenza tecnica.
Errore umano	Azioni involontarie o non corrette da parte del personale che possono causare danni ai dati o alle operazioni aziendali.	Media	Moderato: perdita di dati, errori di produzione, interruzioni temporanee delle operazioni.	Medio	Formazione del personale, implementazione di controlli di validazione dei dati, revisione dei processi operativi.
Disastro naturale	Eventi imprevisti come incendi, alluvioni, terremoti, che possono danneggiare le strutture aziendali e le risorse fisiche.	Bassa	Elevato: danni fisici agli edifici, interruzioni prolungate delle operazioni, perdita di dati critici.	Medio	Implementazione di piani di emergenza e di continuità operativa, assicurazioni contro i danni fisici, protezione delle infrastrutture.
Accesso non autorizzato	Tentativo di accedere a dati o sistemi senza autorizzazione, sia da parte di utenti interni che esterni.	Media	Elevato: accesso non autorizzato a dati sensibili, compromissione della riservatezza e dell'integrità dei dati.	Alto	Gestione degli accessi basata sui ruoli, crittografia dei dati sensibili, monitoraggio degli accessi e delle attività.
Interruzione del servizio	Interruzione dei servizi aziendali, ad esempio a causa di problemi di rete, errori di configurazione o attacchi informatici mirati.	Alta	Elevato: perdita di entrate, danni alla reputazione, insoddisfazione del cliente.	Elevato	Implementazione di sistemi di backup e ripristino, ridondanza dei sistemi critici, monitoraggio proattivo delle reti e dei servizi.