Raul Pastor

Firewall

Nel compito di oggi viene richiesto di calcolare quantitativamente la perdita annuale di ogni scenario (moltiplicare asset*frequenza evento*probabilità evento):

● Inondazione sull’asset «edificio secondario»
● Terremoto sull’asset «datacenter»
● Incendio sull’asset «edificio primario» ● Incendio sull’asset «edificio secondario»

Date le seguenti tabelle:

ASSET VALORE
Edificio primario 350.000€
Edificio secondario 150.000€
Datacenter 100.000€

EVENTO ARO
Terremoto 1 volta ogni 30 anni
Incendio 1 volta ogni 20 anni
Inondazione 1 volta ogni 50 anni

EXPOSURE FACTOR
Terremoto Incendio Inondazione
Edificio primario
80% 60% 55%
Edificio secondario
80% 50% 40%
Datacenter
95% 60% 35%

● Inondazione sull’asset «edificio secondario» 1200€
● Terremoto sull’asset «datacenter» 2850€
● Incendio sull’asset «edificio primario» 10500€

PARTE 2:

1. Confidenzialità (Riservatezza)
L'obiettivo è impedire l'accesso non autorizzato ai dati sensibili.

Minacce:
Phishing e Ingegneria Sociale: Ingannare gli utenti per farsi consegnare credenziali di accesso.
Attacchi Man-in-the-Middle (MITM): Intercettazione di dati mentre transitano su reti non protette (es. Wi-Fi pubbliche).
Insider Threats: Dipendenti o collaboratori che espongono intenzionalmente o accidentalmente dati riservati.

Contromisure:
Crittografia: Proteggere i dati sia quando sono archiviati ("at rest") sia quando vengono trasmessi ("in transit").
Autenticazione a più fattori (MFA): Richiedere più prove di identità per rendere inutili le password rubate.
Controllo degli accessi (RBAC): Limitare l'accesso ai dati solo a chi ne ha strettamente bisogno per il proprio lavoro (Principio del minimo privilegio).

2. Integrità

L'obiettivo è garantire che i dati rimangano accurati, completi e non vengano alterati senza autorizzazione.

Minacce:
Malware e Ransomware: Software malevoli che modificano, criptano o eliminano file critici.
Errori Umani: Modifiche accidentali o cancellazioni involontarie di record importanti.
Manomissione dei dati: Modifica intenzionale di record finanziari o database per occultare frodi.

Contromisure:
Hashing e Firme Digitali: Utilizzare algoritmi per verificare che un file non sia stato alterato dopo la creazione.
Sistemi di Versionamento: Mantenere una cronologia delle modifiche per poter ripristinare versioni precedenti dei dati.
Audit Log: Registrare ogni modifica effettuata sui dati per identificare chi ha fatto cosa e quando.

3. Disponibilità

L'obiettivo è assicurare che i sistemi e i dati siano sempre accessibili agli utenti autorizzati.

Minacce:
Attacchi DDoS: Sovraccaricare un server con traffico falso per renderlo inutilizzabile.
Guasti Hardware e Software: Rottura di dischi rigidi, server o bug critici nel codice.
Eventi Naturali: Alluvioni, incendi o interruzioni di corrente che bloccano l'accesso fisico ai data center.

Contromisure:
Ridondanza e Failover: Duplicare i componenti critici (es. server, linee internet) in modo che uno subentri se l'altro fallisce.
Piani di Backup e Disaster Recovery: Salvare copie dei dati in luoghi sicuri ed isolati per ripristinarli dopo un incidente.
Sistemi UPS e Protezione Fisica: Utilizzare gruppi di continuità per prevenire spegnimenti improvvisi e proteggere fisicamente l'infrastruttura.