Guida alla Gestione del Rischio nell'Era Digitale

1. Introduzione: L'evoluzione del concetto di sicurezza

Il panorama della sicurezza informatica è in continua evoluzione a causa della corsa tra attaccanti e difensori. La sicurezza ha visto un'espansione costante della superficie di attacco e della complessità delle minacce, passando dalla protezione dei primi sistemi informatici negli anni '60 alla moderna era dell'iperconnettività.

Questa crescente interconnessione ha portato a una fusione tra sicurezza fisica e digitale. I sistemi di sorveglianza moderni, ad esempio, integrano l'intelligenza artificiale, mentre il controllo degli accessi utilizza la biometria, superando i metodi tradizionali. Questa convergenza, pur offrendo soluzioni robuste, crea anche nuove vulnerabilità, come la possibilità che un attacco digitale a un sistema di controllo possa aggirare le barriere fisiche.

2. Concetti fondamentali e modello di rischio

Per comprendere la sicurezza informatica, è fondamentale distinguere tra diversi concetti chiave:

- **Minaccia**: È un potenziale pericolo che può sfruttare una debolezza per causare danni.
- **Vulnerabilità**: Una debolezza o una lacuna nel sistema che può essere sfruttata da una minaccia.
- **Attacco**: Un tentativo deliberato di eludere i servizi di sicurezza per compromettere un sistema.
- **Rischio**: La probabilità che una minaccia sfrutti una vulnerabilità, generando un impatto negativo.
- **Contromisura** o **Difesa**: Un meccanismo o una strategia per mitigare il rischio.

3. Classificazione degli attacchi

Gli attacchi informatici si dividono in due categorie principali:

Attacchi Passivi: La sicurezza a rischio silenzioso

Gli attacchi passivi sono intrusivi, ma non modificano il sistema. L'attaccante intercetta e monitora il flusso di informazioni senza alterare i dati. Sono difficili da rilevare e la difesa si basa sulla prevenzione, ad esempio tramite la crittografia che rende i dati inutilizzabili per l'attaccante. Le due tipologie principali sono:

- **Intercettazione del contenuto**: Utilizzo di tecniche come il *packet sniffing* per catturare una copia di ogni pacchetto che transita su una rete.
- **Analisi del traffico**: Sfrutta i metadati (come l'identità degli host, la loro posizione, la frequenza e la lunghezza dei messaggi) per creare un profilo comportamentale di un utente o di un'organizzazione, anche quando il contenuto dei messaggi è cifrato.

Attacchi Attivi: Manipolazione e compromissione

Gli attacchi attivi implicano una manomissione diretta del sistema. L'attaccante altera le risorse, modifica il flusso dei dati o ne crea uno falso. Sebbene siano più facili da rilevare, la loro prevenzione è più complessa. Le categorie principali sono:

- **Mascheramento (Spoofing)**: Un'entità ne impersona un'altra per ottenere accesso o dati sensibili. Esempi includono l'*Email Spoofing* e l'*IP Spoofing*.
- **Dirottamento di sessione (Session Hijacking)**: Una forma avanzata di spoofing in cui l'attaccante ruba il cookie di sessione di un utente per assumere il controllo del suo account.
- **Modifica dei messaggi**: L'attaccante intercetta e altera il contenuto di un messaggio in transito, compromettendo l'integrità dei dati. Le contromisure includono l'uso di funzioni di *hashing* e *firme digitali* per rilevare manomissioni.
- **Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)**: Attacchi volti a rendere un sistema non disponibile per i suoi utenti legittimi, saturandone le risorse. Un attacco DDoS è più sofisticato e utilizza più sorgenti compromesse (*botnet*) per lanciare l'attacco, rendendolo più difficile da rilevare.

4. Principi di progettazione di un sistema di sicurezza

La progettazione di un sistema di sicurezza richiede più di una semplice soluzione tecnologica. È cruciale analizzare i potenziali attacchi e considerare il contesto operativo, definendo il posizionamento fisico e logico dei meccanismi di sicurezza. È inoltre essenziale gestire correttamente le informazioni segrete, come le chiavi crittografiche.

5. Fasi di lavoro e risorse utilizzate

Il progetto è stato sviluppato attraverso diverse fasi:

- **Fase 1: Analisi del Materiale**: Comprensione dei concetti di base della sicurezza, distinguendo tra attacchi passivi e attivi.
- **Fase 2: Struttura dell'Elaborato**: Creazione di una scaletta logica, partendo da concetti generali per arrivare a casi specifici.
- **Fase 3: Stesura e Revisione**: Redazione del documento, assicurandosi di mantenere un linguaggio tecnico ma comprensibile e di correggere eventuali errori.

Le risorse principali utilizzate sono state il materiale didattico ufficiale del corso "Reti di calcolatori e Cybersecurity" e "Cybersecurity". Sono stati impiegati anche modelli teorici come il **Modello ISO/OSI e TCP/IP** per contestualizzare la sicurezza all'interno dell'architettura di rete e i modelli crittografici per spiegare il funzionamento di algoritmi come **AES e RSA**.