# Cyber Security

## Panoramica

# Concetti di Security

# Computer Security

## Definizione

È l'insieme di misure e controlli che garantiscono **confidenzialità** (*confidentiality*), **integrità** (*integrity*) e **disponibilità** (*availability*) delle risorse dei sistemi informativi, che siano essi Hardware, Software o le informazioni stesse.

- **Confidentiality** - Le informazioni (o sistemi) confidenziali rimangono tali, pertanto non accessibili a soggetti non autorizzati.

- **Integrity** - Le informazioni e i programmi sono modificati solo con metodi autorizzati. L'integrità dei sistemi invece si riferisce allo scopo di un determinato sistema, garantendo che esso possa eseguire solo le azioni per cui è stato programmato.

- **Availability** - Garantisce che i sistemi siano disponibili, che funzionino e che il servizio che offrono non sia negato agli utenti autorizzati.

# Terminologia 1/3

## Risorse di sistema e Asset

- **Hardware** - Computer, Server, Sistemi fisici in generale, Sistemi di archiviazione, Sistemi di trasmissione
- **Software** - Sistema Operativo, Tool, Utility, Applicazioni
- **Dati** - File, Database
- **Rete** - Reti LAN (Local Area Network) e WAN (Wide Area Network), Router

# Terminologia 2/3

- **Attacco** - Qualsiasi azione volta a collezionare, distruggere o degradare i sistemi informativi o l'informazione stessa

- **Security Policy** - Criteri di sicurezza che hanno lo scopo di mantenere un determinato livello di sicurezza

- **Minacce** - Qualsiasi circostanza o evento che può impattare negativamente su un sistema informativo o un'informazione

- **Vulnerabilità** - Vulnerabilità in un sistema, processo, policy o implementazione che può essere sfruttata per un attacco.

# Terminologia 3/3

## Attacchi e provenienza

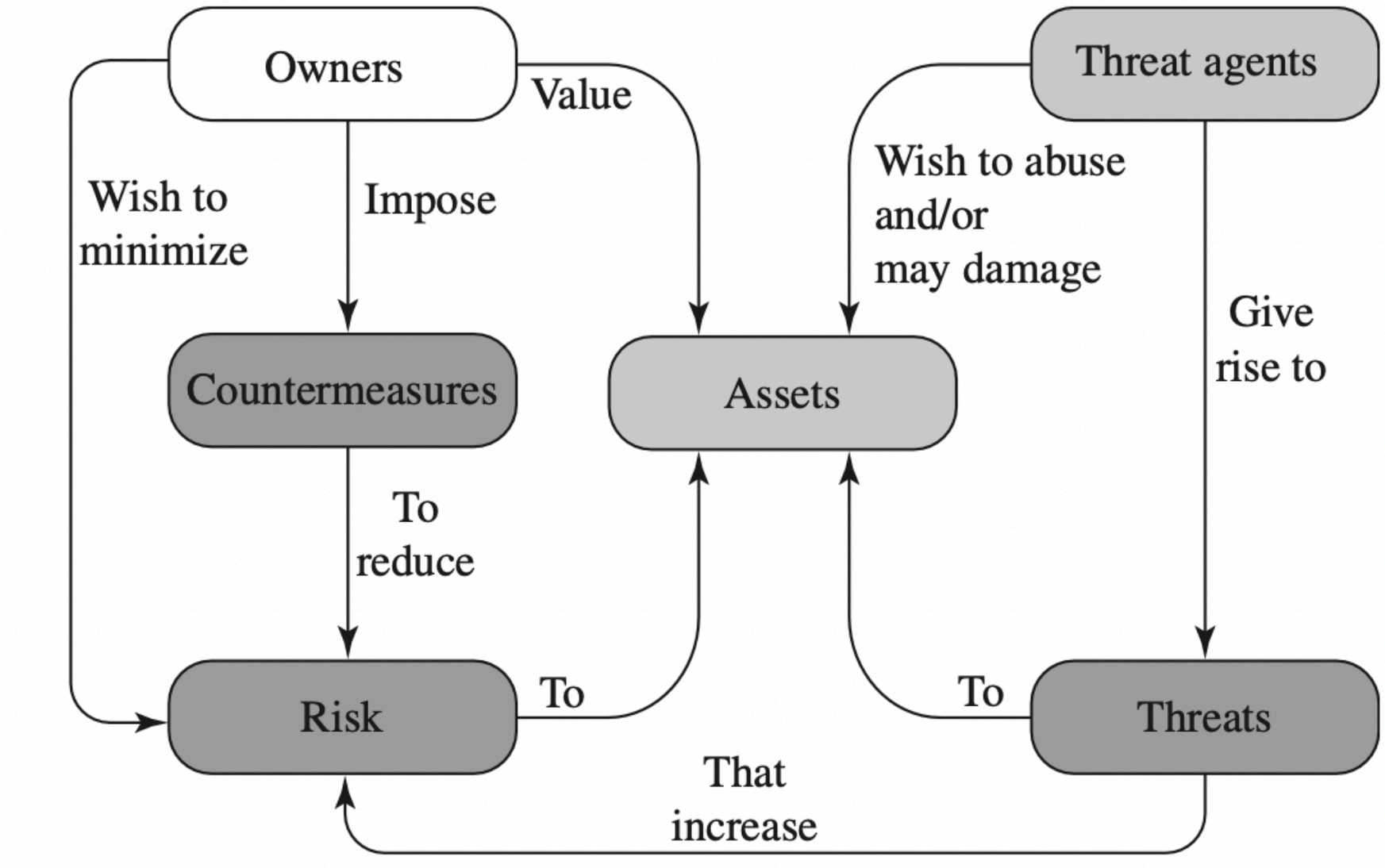
- **Attacco attivo** - Tentativo di alterare le risorse di sistema o l'operatività del sistema stesso

- **Attacco passivo** - Tentativo di utilizzare le informazioni di un sistema senza alterarne le risorse

- **Attacco interno** - È un attacco iniziato all'interno del perimetro, l'attaccante (insider) ha accesso autorizzato alle risorse e/o alle informazioni

- **Attacco esterno** - Proviene dall'esterno, l'attaccante non ha accesso autorizzato ai sistemi e lo ottiene illegalmente

# Relazioni tra minacce, asset e rischio



# Minacce, Attacchi e Asset

# Minacce, Attacchi e Asset

## Definizioni

- **Minaccia** - La minaccia si concretizza nel momento in cui un sistema elabora informazioni che hanno un **valore** per un soggetto (attaccante).

- **Attacco** - Quando si ha una minaccia ed un attaccante riesce a sfruttare una vulnerabilità, si arriva all'attacco che è quella fase necessaria per ottenere accesso o informazioni dagli asset.

- **Asset** - È una risorsa, importante per il titolare della stessa e per un attaccante, e può essere un sistema di elaborazione, una rete o le informazioni trattate.

# Minacce, Attacchi e Asset

## Conseguenza alle minacce e attacchi

| Conseguenza alla minaccia | Attacco |
|---|---|
| **UNAUTHORIZED DISCLOSURE**<br>(Unauthorized entity gains data access) | • Exposure<br>• Interception<br>• Inference<br>• Intrusion |
| **DECEPTION**<br>(False Data) | • Masquerade<br>• Falsification<br>• Repudiation |
| **DISRUPTION**<br>(Interrupts/Prevents system operation) | • Incapacitation<br>• Corruption<br>• Obstruction |
| **USURPATION**<br>(Unauthorized System Control) | • Misappropriation<br>• Misuse |

# Requisiti Funzionali

# Requisiti Funzionali

Sono i requisiti necessari per permettere ai sistemi di eseguire le operazioni per i quali sono stati programmati.

# Requisiti Funzionali

## Requisiti di sistema

| | |
|---|---|
| **Access Control** | Limitare l'accesso alle informazioni e ai sistemi al solo personale autorizzato |
| **Awareness and Training** | Spiegare al personale i rischi associati alla sicurezza. Effettuare training periodico circa le minacce alla propria organizzazione |
| **Audit and Accountability** | Tracciare e monitorare le azioni degli utenti per permettere analisi in caso di attacco. Il tracciamento è necessario anche per rispondere a leggi nazionali ed internazionali |
| **Certifications, Accreditations, and Security Assessments** | Effettuare degli assessment periodici sui sistemi e sulle reti per garantire l'efficacia dei controlli di sicurezza in essere |
| **Configuration Management** | Stabilire e mantenere una baseline delle configurazioni, mantenendo un inventario dei sistemi e delle configurazioni |

# Requisiti Funzionali

## Requisiti di sistema

| | |
|---|---|
| **Contingency Planning** | Stabilire, mantenere ed implementare piani per la risposta alle emergenze. |
| **Identification and Authentication** | Identificare gli utenti che hanno accesso ai sistemi e autenticarli per verificarne l'identità |
| **Incident Response** | Stabilire un quadro operativo per le azioni di incident handling considerando preparazione del personale, detection, analisi e piani di recovery post-incident |
| **Maintenance** | Effettuare manutenzione periodica sui sistemi informativi aziendali |
| **Media Protection** | Proteggere le informazioni nei media, sia digitali che cartacei. Limitare l'accesso ai soli utenti autorizzati. Distruggere le informazioni non più necessarie prima di riutilizzare/ gettare un media. |

# Requisiti Funzionali

## Requisiti di sistema

| | |
|---|---|
| **Physical and Environmental Protection** | Limitare l'accesso fisico alle strutture e ai sistemi. Tracciare gli accessi autorizzati. Struttura la rete e i sistemi per prevenire disastri dovuti a causa maggiore (es. incendi) |
| **Planning** | Sviluppare e documentare piani di sicurezza per i sistemi aziendali, descrivere i controlli di sicurezza in essere |
| **Personnel Security** | Le persone che ricoprono ruoli di responsabilità rispondono a criteri di sicurezza per quelle posizioni. Trasferimenti e licenziamenti devono rimuovere gli accessi non più necessari |
| **Risk Assessment** | Effettuare Risk Assement periodici per mitigare i rischi |
| **System and Services Acquisition** | Allocare sufficienti risorse per rispondere adeguatamente ai requisiti di sicurezza |

# Requisiti Funzionali

## Requisiti di sistema

| | |
|---|---|
| **System and Communication Protection** | Monitorare, controllare e proteggere le comunicazioni aziendali all'esterno del perimetro. Promuovere la sicurezza delle informazioni nei sistemi considerando il design dell'architettura e lo sviluppo software |
| **System Information Integrity** | Identificare, riportare e correggere le vulnerabilità dei sistemi quanto prima. Monitorare gli alert di sicurezza e rispondere con adeguate azioni e misure di sicurezza |

# Principi fondamentali di Security Design

# Principi fondamentali di Security Design

| | |
|---|---|
| **Economy of mechanism** | Progettare un design semplice aiuta a ridurre la superficie di attacco, perché saranno presenti meno vulnerabilità rispetto ad un'architettura più complessa. |
| **Fail-safe default** | Gli accessi dovrebbero essere autorizzati per richiesta di permesso e non per esclusione. Se l'implementazione è fatta per esclusione si rischia di avere accessi autorizzati per errore, senza notarlo. |
| **Complete mediation** | L'accesso deve essere concesso da un sistema ad hoc, senza l'utilizzo di cache (pertanto con dati aggiornati). L'implementazione completa di questo controllo richiederebbe un controllo continuo anche dopo l'apertura di un file. |
| **Open design** | Il design di un meccanismo di sicurezza dovrebbe essere aperto, permettendo così ad altri ricercatori di sicurezza di verificare la bontà dei controlli in essere. |

# Principi fondamentali di Security Design

| | |
|---|---|
| **Separation of privilege** | È una pratica secondo la quale è necessario avere diversi permessi per accedere ad una risorsa (es. MFA). |
| **Least privilege** | Ogni processo ed ogni utente deve operare usando il minimo indispensabile dei privilegi necessari ad eseguire una determinata azione. |
| **Least common mechanism** | L'implementazione deve evitare l'utilizzo di funzioni in comune tra diversi utenti. Così si riduce il numero di comunicazioni non volute. |
| **Psychological acceptability** | Implica che i meccanismi di sicurezza non interferiscano con le attività dell'utente e rispettino gli standard definiti da chi fornisce gli accessi. |

# Principi fondamentali di Security Design

| | |
|---|---|
| **Isolation** | 1. Sistemi ad accesso pubblico isolati dai dati/sistemi critici<br>2. Processi e file degli utenti isolati gli uni dagli altri se non esplicitamente concessi<br>3. L'accesso ai sistemi di sicurezza deve essere isolato |
| **Modularity** | Le funzioni di sicurezza sono separate e l'architettura è modulare |
| **Layering** | Utilizzo di livelli multipli di sicurezza indirizzando persone, tecnologia e operations. Il fallimento di un livello di sicurezza non compromette interamente la protezione del sistema |

# Superficie di Attacco

# La superficie d’Attacco dipende dalla raggiungibilità e dalla possibilità di sfruttare le vulnerabilità di un sistema

# Superficie di Attacco

## Categorie

**Network**: Vulnerabilità presenti nella rete aziendale, nella wide-area network, o internet. Si considerano anche le vulnerabilità di protocollo.

**Software**: Vulnerabilità nelle applicazioni, librerie o nel Sistema Operativo.

**Human**: Vulnerabilità create dalle persone, che siano dipendenti, esterni, o errori umani (es. aprire un allegato).

# Strategie di Sicurezza

# Strategie di Sicurezza

- Security Policy
- Security Implementation

# Strategie di Sicurezza

## Security Policy 1/2

La prima fase della definizione delle strategie di sicurezza è la definizione delle “**Security Policy**”, che non sono altro che documenti informativi che indirizzano un problema di sicurezza cercando di mitigarlo.

Alcuni esempi di policy di sicurezza possono essere: cambio password ogni 90 giorni, utilizzo di Multi Factor Authentication per l’accesso ai sistemi

# Strategie di Sicurezza

## Security Policy 2/2

Nella fase di disegno delle policy è importante considerare questi due aspetti fondamentali:

- **Facilità di utilizzo** - Introdurre una policy per la gestione delle password che richieda il cambio obbligatorio ogni 15 giorni e che la lunghezza sia almeno di 20 caratteri va contro questo principio, per quanto i vantaggi di Security che ne derivano siano notevoli. Bisogna trovare il giusto compromesso tra usabilità e sicurezza.
- **Costo della sicurezza** - Se il costo della sicurezza è maggiore del costo di un eventuale incidente, allora è stato sbagliato qualcosa. Dobbiamo sempre considerare il rischio relativo al sistema/dato da proteggere e bilanciarlo con un corretto livello di sicurezza.

# Strategie di Sicurezza

## Security Implementation 1/2

### PREVENTION

Nessun attacco riesce, ovviamente si tratta di una situazione ideale.

Ad esempio cifrando il traffico preveniamo che questo venga letto, ma l’algoritmo di cifratura può essere debole.

### DETECTION

Un sistema IDS (Intrusion Detection System) è in grado di rilevare un’intrusione in un sistema o nella rete.

# Strategie di Sicurezza

## Security Implementation 2/2

### RESPONSE

È la fase di risposta ad un attacco, intesa come mitigazione.

Ad esempio se mi effettuano un attacco DoS posso mitigarlo con CDN e Firewall.

### RECOVERY

Un esempio di recovery è l'utilizzo di un sistema di backup che mi permetta di ripristinare lo stato del sistema ad uno stato funzionante.

# Standard

# Standard

- NIST - National Institute of Standards and Technology
- ISO - International Organization for Standardization