UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Gestione, valutazione e analisi del rischio cyber

Giorgio Olivieri

Giovedì 2 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Cos’è il rischio?

Definizione di rischio cyber

- Una **vulnerabilità** è una **debolezza** in un sistema informatico, una rete, una procedura o un controllo di sicurezza che può essere sfruttata da una **minaccia** per causare un danno
- Il **rischio cyber** è la **possibilità** che una minaccia sfrutti una vulnerabilità, causando un **impatto negativo** su sistemi, dati o processi

Vulnerability Assessment (VA)

- Tutti i sistemi informatici sono vulnerabili**. L'invulnerabilità è un obiettivo irraggiungibile**, pertanto la sicurezza informatica non può rendere un sistema invulnerabile ma deve gestire i rischi riducendoli ad un **livello tollerabile**
- La VA è una tecnica che consiste nell'**identificazione** e nella **misurazione** delle vulnerabilità di un determinato ambiente. E' una valutazione approfondita dello **stato di sicurezza** : solo dopo aver individuato le potenziali debolezze si è in grado di implementare le adeguate misure per ridurre o eliminare il rischio associato

Safety e Security

- La **safety** riguarda la protezione da **eventi accidentali o errori involontari** che possono causare danni a persone, beni o ambienti
- La **security** si riferisce alla protezione dei dati da attacchi deliberati o azioni malevole, quindi riguarda la sicurezza da **minacce intenzionali**
- La **cybersecurity** è una particolare branca della security che mira a garantire la protezione dei sistemi informatici a livello di **disponibilità, confidenzialità ed integrità dei dati e degli asset informatici**

Principali tipologie di attacchi

Malware

- E’ un software dannoso, cioè un programma appositamente creato per danneggiare, sabotare o accedere senza autorizzazione a dispositivi, dati o reti
- **Virus**: si attacca a file legittimi e si diffonde alla loro apertura
- **Trojan**: si presenta come un software utile al sistema ma nasconde del codice malevolo
- **Ransomware**: blocca accesso ai dati della vittima tramite un’apposita cifratura e chiede un riscatto
- **Spyware**: monitora le attività e raccoglie informazioni

Attacchi a reti e sistemi di applicazioni

- **Man-in-the-Middle**: l'attaccante si inserisce tra due interlocutori per intercettare o manipolare le comunicazioni
- **SQL Injection**: inserimento di comandi SQL malevoli nei campi input per accedere a database e rubare dati
- **Cross-Site Scripting (XSS)**: inserimento di script dannosi in pagine web per colpire altri utenti
- **Cross-Site Request Forgery (CSRF)**: costringe un utente autenticato a eseguire azioni indesiderate

Phishing & Social Engineering

- Il **phishing** è una tecnica che mira a **ingannare le persone** per ottenere dati sensibili ,spesso tramite email, SMS o messaggi falsi che imitano comunicazioni ufficiali
- Fa parte della più ampia categoria della **social engineering**, ovvero l'insieme di tecniche che sfruttano la fiducia, la fretta o la distrazione degli utenti, piuttosto che vulnerabilità tecniche
- L'obiettivo è rubare informazioni, diffondere malware o ottenere accesso ai sistemi.

Attacchi Denial-of-Service

- Gli attacchi **Denial-of-Service (DoS)** mirano a **sovraccaricare** un server, un sito web o una rete, rendendoli **inaccessibili** agli utenti legittimi
- Quando l'attacco proviene da molteplici fonti distribuite si parla di **Distributed Denial-of-Service (DDoS)**
- Comportano l'interruzione dei servizi online causando spesso perdite economiche e reputazionali

Brute Force & Credential Stuffing

- Gli attacchi **brute force** consistono nel tentare automaticamente tutte le possibili combinazioni di credenziali finché non si trova quella corretta per accedere
- Il **credential stuffing**, invece, sfrutta **credenziali rubate** da altri siti web per provare ad accedere a nuovi account, approfittando del fatto che molte persone usano le **stesse password su più servizi**.
- Sono pericolosi perché automatizzati, veloci e hanno molto successo con password deboli o riutilizzate

Principali normative

GDPR

- Il **GDPR** (Regolamento UE 2016/679) è la normativa europea in vigore dal 25 maggio 2018, che disciplina la **protezione dei dati personali** dei cittadini dell'Unione Europea
- Tutela i **diritti** e **libertà fondamentali** degli interessati
- Garantisce un **uso lecito, trasparente e sicuro** dei dati personali
- Richiede che le aziende e organizzazioni adottino **misure tecniche adeguate**

- La CIA Triad è un modello per valutare e implementare le misure tecniche richieste dal GDPR
- **Riservatezza**: solo le persone autorizzate possono accedere ai dati
- **Integrità**: dati accurati, completi e non modificati in modo improprio
- **Disponibilità**: dati e sistemi accessibili quando necessario agli utenti

NIS2

- La **NIS2** (Direttiva UE 2022/2555) è la normativa europea che rafforza la **cybersicurezza delle reti e dei sistemi informativi** nei settori critici.
- Impone un **approccio strategico e proattivo** alla sicurezza informatica per garantire la continuità dei servizi essenziali
- Il principale obiettivo è aumentare la **resilienza digitale** di aziende e pubbliche amministrazioni che erogano servizi **essenziali o importanti** per la società e l'economia

Cyber Risk Management

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Contesto di applicazione

- Il cyber risk management è l’anello di congiunzione tra tecnologia e sicurezza
- Ormai è una priorità strategica per aziende, enti pubblici e organizzazioni di ogni dimensione
- Volta a prevenire o limitare danni causati da attacchi malevoli , errori o guasti tecnici

Fasi chiave

- Identificazione di minacce e vulnerabilità
- Valutazione del rischio
- Mitigazione con misure tecniche e organizzative
- Monitoraggio e miglioramento continuo
- Piano di risposta e recovery

Gestione del rischio

- Comprende tutte le azioni necessarie per ridurre o controllare i rischi emersi
- E’ un **processo continuo** supportato da monitoraggio e revisione periodica per garantire continuità operativa

Analisi del rischio

- Si identificano i **beni da proteggere**
- Si cercano le **minacce** esistenti e quelle potenziali
- Si valutano gli **impatti** che l'organizzazione potrebbe subire dalle minacce in termini di **probabilità di accadimento** e relativo danno potenziale (**gravità**). Questi dati vengono poi utilizzati nella fase di valutazione

Valutazione del rischio

- Obiettivo è **quantificare o descrivere qualitativamente i rischi** così da dare priorità a determinate **azione correttive**
- Per ogni rischio identificato si pianificano delle misure volte a **eliminare o ridurre il rischio ad un livello accettabile**

Stima del rischio

Come si stima

- E’ un’attività difficile ma necessaria per la gestione dei rischi
- E’ una combinazione di molteplici fattori
- Si considerano la probabilità di subire un attacco, la vulnerabilità all’attacco e il valore del danno nel caso in cui l’attacco abbia successo
- Esistono diversi tipologie di valutazione

Metodi qualitativi

- Si sfruttano una serie di metodi, principi e regole basati su categorie o livelli non numerici
- Sono facili da comprendere e comunicare, rapidi da realizzare ed economici
- Sono molto soggettivi e quindi è spesso difficile fare delle comparazioni dei rischi in modo preciso ed attendibile
- Tra i più diffusi c’è la matrice di rischio che combina probabilità ed impatto per classificare il rischio

Metodi quantitativi

- Si sfruttano una serie di metodi, principi e regole basati su categorie o livelli numerici su base statistica e matematica
- Sono oggettivi ed estremamente precisi
- Forniscono risultati rigorosi, ripetibili e riproducibili
- La stima dei fattori può richiedere alti costi a livello economico e temporale
- A volte difficile da comunicare agli stakeholder

- Un aspetto fondamentale di questi metodi è ottenere una stima oggettiva delle probabilità
- Sono metodi che spesso utilizzano simulazioni Monte Carlo , un insieme di tecniche statistiche per modellare fenomeni complessi o incerti e ottenere dei risultati approssimati con una serie di simulazioni casuali
- Si adattano bene a modelli con molte variabili e molte incertezze

Grazie per l’attenzione