WISER
Wide-Impact cyber SEcurity Risk framework

# Glossario di Sicurezza Informatica per principianti

Secondo uno degli ultimi studi di EY Global Information Security Survey (GISS), in Italia sale al 97% la percentuale delle aziende che dichiarano di avere una funzione di Cybersecurity non in linea con le proprie esigenze: quasi due aziende su tre non dispongono di un programma formale e strutturato di Threat Intelligence, mentre quasi la metà non possiede metodi e strumenti tecnologici adeguati per identificare le vulnerabilità.

Questa piccola guida si rivolge alle PMI e ai team informatici delle Pubbliche Amministrazioni che spesso hanno difficoltà nella comprensione e nella gestione delle tematiche di sicurezza informatica. La guida si pone dunque come primo passo per una conoscenza approfondita delle tematiche di sicurezza in ambito informatico, a partire dalla terminologia di base.

**Cyber attacco (Cyber attack)**: sfruttamento intenzionale dei sistemi informatici, reti o infrastrutture di imprese operanti nell'ambito digitale atto a causare un danno alle stesse.

**Cyber incidente (Cyber incident)**: evento che può o potrebbe rappresentare una minaccia per apparecchi informatici, pc, dispositivi collegati ad internet, reti e sistemi, ma anche per i dati in essi contenuti, processati o trasmessi.

**Cyber Resilienza (Cyber resilience)**: la capacità dei sistemi informatici e delle organizzazioni di resistere ad attacchi informatici e, nel caso siano stati causati danni, di rispondere ad essi.

**Cyber sicurezza (Cyber security)**: la protezione dei sistemi connessi ad internet inclusi hardware, software e relative infrastrutture, dei dati in essi contenuti e dei servizi offerti da accessi non autorizzati, danni od usi impropri. In questa voce sono compresi anche danni causati intenzionalmente o accidentalmente dal gestore dei servizi nel caso quest'ultimo non abbia seguito le normali procedure di sicurezza o sia stato manipolato per aggirarle.

**Valutazione del rischio informatico (Cyber security risk assessment)** : individua le criticità e lacune in specifiche aree di rischio all'interno di una organizzazione e determina le azioni atte a colmare tali lacune e criticità. Inoltre, una corretta valutazione del rischio informatico garantisce di investire tempo e denaro nei settori giusti e di conseguenza di non sprecare risorse.

**Cyber minaccia (Cyber threat)** - qualsiasi evento in grado di compromettere tramite mezzi informatici la sicurezza, o causare danni a sistemi informativi e dispositivi connessi a Internet, tra cui hardware, software e relative infrastrutture, ai dati processati, trasmessi e contenuti su di essi e dei loro servizi.

# Tipi di attacchi e vulnerabilità

**Commodity malware** - software dannoso facilmente reperibile tramite l'acquisto o il download gratuito, che viene utilizzato a scopi malevoli da diverse entità.

**Violazione di sicurezza (Data breach)** - la trasmissione o comunicazione non autorizzata di informazioni sensibili ad una parte, solitamente esterna all'organizzazione vittima, che non è autorizzata a possedere o vedere l'informazione.

**DDoS** - attacco informatico sferrato da più computer in contemporanea finalizzato ad interrompere l'erogazione di un servizio di rete.

**Doxing** - la pratica di ricerca, o di hacking di informazioni personali di un individuo (PII) su Internet, a cui segue la loro pubblicazione.

**Malware** – software dannoso comprendente a sua volta Virus, Worm, Trojan e Spyware.

**Virus**- I virus sono programmi dannosi per computer che possono infettare la macchina su cui sono installati e diffondersi ad altri file.

**Worm** - Un worm è un programma malevolo che si replica autonomamente in modo da diffondersi ad altri computer. Spesso, il Worm utilizza una rete di computer per diffondersi, basandosi su falle di sicurezza sul computer di destinazione per accedervi. A differenza di un virus informatico, per attivarsi non ha bisogno di interagire con un programma già esistente.

**Trojan** - Un cavallo di Troia o Trojan, è un programma malevolo che viene nascosto all'interno di un'applicazione apparentemente inoffensiva, in modo da poter infettare il computer della vittima senza che questa ne sia consapevole.

**Spyware** - Uno spyware è un particolare tipo di software che una volta installato sul computer è in grado di raccogliere informazioni private legate all'utente ed alle sue preferenze.

**Phishing** – È una tipologia di truffa informatica attraverso la quale si cerca di ingannare la vittima a fornire informazioni sensibili attraverso l'uso di e-mail che sembrano provenire da una fonte attendibile o conosciuta.

**Ransomware** - Software dannoso che impedisce l'accesso degli utenti ai propri file, computer o dispositivi finché non viene pagato un riscatto in denaro.

**SMS spoofing** - Una tecnica che maschera l'origine di un messaggio SMS, sostituendo il numero di cellulare originario con testo alfanumerico. Può essere utilizzato legittimamente da un mittente in modo da sostituire il proprio numero di cellulare con il loro proprio nome e cognome, o la società di lavoro, per esempio. Oppure può essere usato in modo illegittimo, al fine di impersonare un'altra persona.

**Social engineering** – si riferisce alla manipolazione psicologica utilizzata per ingannare e manipolare le vittime in modo tale che queste divulghino informazioni personali e riservate. In genere, le azioni più comune tramite cui il Social engineering viene perpetuato comprendono l'apertura da parte della vittima di una pagina Web dannosa o di un file allegato infetto.

**Vulnerabilità** – Errori o bug presenti in programmi software che possono essere sfruttati dagli hacker per effettuare azioni malevole.

**Test di vulnerabilità** – Attività fondamentale del processo di valutazione del rischio informatico, attraverso la quale si identificano e quantificano, anche in termini di pericolosità, le vulnerabilità in un sistema. E' consigliato effettuare test di vulnerabilità con cadenza regolare data la velocità con cui attacchi e vulnerabilità possono evolversi nel corso del tempo.