**Introduzione al Cyber-risk**

*Tempo stimato*: 10’

*Obiettivi di apprendimento*

Alla fine di questa sezione sarai in grado di

* Conoscere cos’è il Cyber-risk
* Comprendere i fattori contribuiscono al Cyber-risk
* Distinguere i concetti di minaccia, vulnerabilità, *exploit* e attacco cyber

Il termine ***cyber-risk*** si riferisce alla possibilità di **danno** (perdita finanziaria, interruzione di servizio o danno reputazionale) subito da un’organizzazione a seguito di un malfunzionamento dei suoi sistemi informatici causato da un agente ostile. 

La consapevolezza del cyber-risk è cresciuta rapidamente negli ultimi anni a causa sia dell’aumentata dipendenza dai servizi digitali da parte delle aziende che dal crescente numero di incidenti cyber di alto profilo. Il cyber-risk è indicato per la prima volta (con il 39% delle risposte) come il primo fattore di rischio per le aziende a livello globale nel *Allianz Risk Barometer* nel 2020, relegando l’Interruzione del Business (con il 37% delle risposte) al secondo posto.

Comprendere e valutare i fattori che contribuiscono al cyber-risk è il presupposto indispensabile alla pianificazione di azioni tese a mitigarlo. Tali fattori sono le minacce, le vulnerabilità e l’impatto.

Le **minacce** (*threats*, in inglese) possono essere portate da una molteplicità di **agenti ostili**(*threat actors*), quali ad esempio, nazioni, criminali (singoli o organizzati in gruppi), attivisti (ad es. il gruppo *anonymous*), o un dipendente infedele (*insider*). Molteplici possono essere le motivazioni che guidano gli agenti ostili: profitto, obiettivi politici o ideologici, spionaggio governativo o aziendale, finalità militari, per citarne alcuni.

Le **vulnerabilità** sono difetti delle infrastrutture tecnologiche, delle procedure o dei processi aziendali che consentono l’esecuzione di comportamenti indesiderati nelle infrastrutture informatiche. Gli agenti ostili **sfruttano** (*exploit*) le vulnerabilità per lanciare **attacchi cyber**. L’**impatto** è la conseguenza di un attacco cyber, quali la perdita finanziaria, il danno reputazionale, l’interruzione del servizio, la sottrazione di segreti industriali, e la divulgazioni di dati sensibili.

L’impatto è normalmente legato alla violazione di una o più delle proprietà di **confidenzialità** (confidentiality), **integrità** (*integrity*) e **disponibilità** (*availability*) delle **risorse digitali** (*digital assets)* dell’organizzazione. La confidenzialità si riferisce all’esigenza di restringere l’accesso alle informazioni ad un insieme ristretto di soggetti autorizzati, l’integrità alla garanzia che i dati siano accurati e affidabili, la disponibilità alla garanzia che i dati o i servizi siano accessibili e quindi fruibili al personale autorizzato.

Tabella 1. - Minacce Cyber: Tipologia, Impatto e Frequenza

(Tratto da <https://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf>)

|  |  |  |  |
| --- | --- | --- | --- |
| **Categoria** | **Azioni** | **Impatto** | **Frequenza** |
| Stati-nazione | Attacchi cyber alle infrastrutture critiche (produzione/distribuzione energia elettrica; sistema finanziario) | disservizi su vasta scala | molto rara |
| Organizzazioni criminali (anche su procura di stati-nazione) | furto di segreti industriali | perdita di competitività | molto rara |
| Gruppi criminali | furto o estorsione di denaro | perdita finanziaria; danno reputazionale | molto comune |
| Attivisti | furto di denaro a organizzazioni finanziarie; interruzione del servizio | perdita finanziaria; danno reputazionale | moderatamente comune |
| Dipendente Infedele | furto di denaro; distruzione o alterazione dei dati; interruzione di servizio | perdita finanziaria; danno reputazionale | raro |

Ad esempio, un sistema informatico con una vulnerabilità nei meccanismi di autenticazione (ad esempio, utilizzo di password facilmente prevedibili) può consentire l’accesso a dati sensibili a utenti non autorizzati e quindi ad una violazione della confidenzialità. Una vulnerabilità nel processo di pagamento delle fatture può esporre un’azienda a frodi da parte di un impiegato infedele (violazione dell’integrità). Infine, una vulnerabilità nel controllo degli accessi ai locali di un’azienda può consentire ad un attaccante di danneggiare le infrastrutture di calcolo o di comunicazione rendendo così indisponibili i servizi informatici utilizzato o offerti dall’azienda (violazione della disponibilità).

Anche se l’accesso non autorizzato alle infrastrutture dell’organizzazione è una minaccia concreta (ancorché sottovalutata), gli attacchi vengono più frequentemente condotti da remoto, sfruttando vulnerabilità nei servizi informatici utilizzati dall’organizzazione per penetrarli. Le statistiche evidenziano che anche la semplice posta elettronica è un efficace **vettore di attacco** grazie al quale gli attaccanti possono raggiungere i loro obiettivi iniettando **software malevolo** (*malware*)che, sfruttando una o più vulnerabilità, compie il danno per cui è stato progettato.