Rischi e “instabilità” tecnologici nell'edizione 2019 del Global Risks Report del World Economic Forum. Parte 1

Author : Sergio Guida

Date : 29 Gennaio 2019

Le minacce informatiche e tecnologiche in rapida evoluzione sono fra i rischi più significativi, anche perché non valutiamo ancora pienamente le vulnerabilità delle società collegate in rete.

La capacità del mondo di promuovere l'azione collettiva di fronte a una crescente serie di gravi sfide ha raggiunto livelli di crisi con il peggioramento delle relazioni internazionali. Nel frattempo, un rallentamento delle prospettive economiche, causato anche da tensioni geopolitiche, sembra destinato a ridurre ulteriormente il potenziale di cooperazione internazionale nel 2019. Trasformazioni complesse - sociali, tecnologiche e legate al lavoro - stanno avendo un profondo impatto e tra le minacce globali indicate nella quattordicesima edizione del *Global Risks Report*, promossa dal *World Economic Forum* in collaborazione con Marsh & McLennan e Zurich Insurance Group, spicca il cyber risk.

Il mondo sta affrontando un numero crescente di sfide complesse e interconnesse, dal rallentamento della crescita globale e dalla persistente disuguaglianza economica ai cambiamenti climatici, alle tensioni geopolitiche e al ritmo accelerato della Quarta rivoluzione industriale.

Più precisamente, le sezioni si concentrano su cinque aree di interesse evidenziate nella *Global Risks Perception Survey* (GRPS: (1) vulnerabilità economiche, (2) tensioni geopolitiche, (3) tensioni sociali e politiche (4) fragilità ambientali e (5) instabilità tecnologiche.

Nella prospettiva decennale del sondaggio, i rischi informatici intensificano il balzo in avanti che hanno registrato nel 2018, mentre i rischi ambientali continuano a dominare le preoccupazioni degli intervistati oltre il breve termine.

Esponenti autorevoli di Marsh & McLennan, partner strategici di lunga data, hanno ribadito come il persistente finanziamento insufficiente delle infrastrutture critiche in tutto il mondo stia ostacolando il progresso, lasciando imprese e comunità più esposte ad attacchi informatici e a catastrofi naturali, non riuscendo a sfruttare al massimo le capacità di difesa.

La tecnologia continua a svolgere un ruolo profondo nel plasmare il panorama dei rischi globali per individui, governi e imprese.

Le preoccupazioni in merito alle frodi e agli attacchi informatici vengono sottolineate nel GRPS, che evidenzia anche una serie di altre vulnerabilità tecnologiche: nel 2018 ci sono state massicce violazioni di dati, si sono rivelate nuove debolezze hardware e la ricerca ha indicato i potenziali usi dell'intelligenza artificiale per progettare attacchi informatici su scala crescente.

L'anno scorso ha inoltre fornito ulteriori prove di quanto gli attacchi informatici rappresentino un rischio per le infrastrutture critiche, spingendo i paesi a rafforzare il loro screening dei partenariati transfrontalieri per motivi di sicurezza nazionale.

Nel GRPS, quello di "frode e furto massivo di dati" è stato classificato come il rischio numero quattro in termini di probabilità su un orizzonte di 10 anni, con "attacchi informatici" al numero cinque. Ciò conferma uno schema registrato lo scorso anno, con i cyber-rischi che consolidano la loro posizione accanto ai rischi ambientali nel quadrante ad alta probabilità e alto impatto del panorama globale dei rischi.

La grande maggioranza degli intervistati prevede un aumento dei rischi nel 2019 degli attacchi informatici che portano al furto di denaro e dati (82%) e all'interruzione delle operazioni (80%). L'indagine riflette come le nuove “instabilità” siano causate dall' approfondimento dell'integrazione delle tecnologie digitali in ogni aspetto della vita. Circa i due terzi degli intervistati si aspettano che i rischi associati alle notizie false e al furto di identità aumentino nel 2019, mentre i tre quinti hanno affermato lo stesso sulla perdita di privacy per le aziende e i governi.

Attacchi informatici “maliziosi” e negligenze nei protocolli di cyber-sicurezza hanno portato a violazioni massive delle informazioni personali nel 2018. Il più grande è stato in India, dove il database governativo *Aadhaar*, il più grande sistema biometrico del mondo con 1,1 miliardi di cittadini registrati, ha subito violazioni multiple che potenzialmente hanno compromesso i record di tutti gli utenti registrati. A gennaio è stato riferito che i criminali vendevano l'accesso al database a 500 rupie per 10 minuti, mentre a marzo un leak ai danni di una società di servizi pubblici permetteva a chiunque di scaricare nomi e numeri di identificazione. Altrove, violazioni dei dati personali colpivano circa 150 milioni di utenti dell'applicazione *MyFitnessPal*, e circa 50 milioni di utenti di *Facebook*.

Le cyber-vulnerabilità possono derivare da direzioni impreviste, come mostrato nel 2018 dalle minacce *Meltdown* e *Spectre*, che sfruttavano carenze nell'hardware del computer piuttosto che nel software e, potenzialmente, avrebbero potuto riguardare tutti i processori Intel prodotti negli ultimi 10 anni.

L'anno scorso abbiamo anche avuto dimostrazioni di come gli attacchi informatici possano mettere a rischio addirittura delle infrastrutture critiche. Ad esempio, a luglio il governo degli Stati Uniti ha rivelato che degli hacker erano riusciti ad ottenere l'accesso alle sale di controllo di alcune aziende di servizi pubblici. La potenziale vulnerabilità delle infrastrutture tecnologiche critiche è diventata sempre più un problema di sicurezza nazionale, tanto che la seconda

interconnessione di rischi più frequentemente citata nel GPRS 2019 è l'associazione di cyber-attacchi con l’eventuale sabotaggio di infrastrutture informatiche critiche.

Ecco perché non c'è mai stata una necessità più urgente di un approccio collaborativo e multistakeholder ai problemi globali delle “networked societies”.

Il report completo è disponibile QUI

Articolo a cura di **Sergio Guida**