PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5193 di Martedì 28 giugno 2022

Che impatto ha un attacco informatico sulla salute e sicurezza dei lavoratori?

Un documento dell'Agenzia europea per la sicurezza e la salute sul lavoro si sofferma sulla sicurezza informatica e sulla necessità di tener conto anche dell'impatto sui lavoratori nella valutazione dei rischi informatici.

Bilbao, 28 Giu ? Come ricordato in molti nostri articoli, l'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA) sta studiando in questi ultimi anni le conseguenze sul lavoro dei rapidi sviluppi della digitalizzazione, ad esempio con riferimento all' intelligenza artificiale, alla robotica e al potenziale impatto sulla salute e sicurezza sul lavoro (SSL). Studi, relazioni e ricerche che vogliono fornire ai responsabili politici dell'Unione Europea, ai datori di lavoro e alle parti sociali le informazioni necessarie sui cambiamenti nelle tecnologie digitali e sul loro impatto sulla natura e sull'organizzazione del lavoro e alle sfide emergenti che possono comportare per la SSL.

Ricordando che i costi globali della **cybersecurity** (cibersicurezza) raggiungeranno i 10500 miliardi di dollari entro il 2025, un documento si è soffermato in particolare sull'impatto della cibersicurezza sui lavoratori.

Infatti al di là dei problemi connessi al furto di dati, gli attacchi informatici possono anche mettere in pericolo i lavoratori. E le aziende che valutano i rischi dell'esposizione a questo tipo di minacce devono quindi considerare anche dei **nuovi rischi emergenti** per la salute e la sicurezza dei lavoratori.

Di questi rischi si parla nel documento (*discussion paper*) dal titolo "**Incorporating occupational safety and health in the assessment of cybersecurity risks**" (Incorporare la sicurezza e la salute sul lavoro nella valutazione dei rischi di cybersecurity). Il documento, commissionato da EU-OSHA e a cura di Isabella Corradini (Scientific director of Themis Research Center), indaga la relazione tra le minacce alla cybersecurity e la salute e la sicurezza dei lavoratori.

L'articolo presenta il nuovo documento con riferimento ai seguenti aspetti:

- Ogni azienda è a rischio di attacco informatico
- Cybersecurity: l'impatto dei cyberattacchi sulla sicurezza
- Cybersecurity: l'impatto sociale e psicologico dei cyberattacchi

Ogni azienda è a rischio di attacco informatico

Nell'introduzione del documento si ricorda che negli ultimi anni la sicurezza informatica è diventata un tema caldo per tutte le aziende di tutti i settori. La criminalità informatica sta diventando sempre più sofisticata e i **criminali informatici** sfruttano tutti i tipi di vulnerabilità per i loro attacchi.

Si sottolinea che, in un mondo sempre più digitalizzato, **ogni azienda è a rischio di attacco informatico** e il 2020 ha rappresentato uno spartiacque sia per la digitalizzazione che per le questioni di cybersecurity. Se le aziende hanno aumentato approcci organizzativi sul lavoro da remoto, soprattutto a causa della pandemia COVID-19, questo ha rappresentato anche un terreno fertile per i criminali informatici, al punto che il 78% delle organizzazioni ha registrato un aumento del volume dei cyberattacchi a causa del passaggio al lavoro da remoto.

Cybersecurity: l'impatto dei cyberattacchi sulla sicurezza

Generalmente gli attacchi informatici sono sempre stati analizzati da un punto di vista tecnologico, anche se il fattore umano rappresenta una parte altrettanto importante della questione della sicurezza informatica. E l'attenzione si è concentrata principalmente sugli aspetti economici e più raramente sulla salute e la sicurezza dei lavoratori.

Se però si pensa che i cyberattacchi in realtà possono causare infortuni, problemi psicologici o perdite di vite umane, diventa chiaro come la **valutazione del rischio informatico** e la **valutazione del rischio relativo alla salute e sicurezza** non possono essere considerate attività separate, ma devono essere eseguite insieme.

Riprendiamo dal documento una tabella relativa al rischio di cybersecurity e alle possibili conseguenze:

Table 2: The variety of impacts for cybersecurity risk management

Categories	Impacts
Organisation	Economic damages (such as less production related to service unavailability, loss of market share or loss of competitive advantage)
	Reputation damage (damaged stakeholders' trust)
	Other economic aspects (such as cyber insurance)
Workers	Physical injuries (such as loss of lives deriving from a failure of a cyber-physical system)
	Mental health injuries (such as anxiety or frustration)
	Impact on personal rights (privacy violation deriving from data breaches)
	Personal economic damage
Other related organisations	Damage due to a disruption of global supply chain interconnections
Environment	Impact on the natural environment (such as land polluted due to a cyber incident)

Adapted from Couce-Vieira et al. 2020

Si indica che i cyberattacchi possono mettere a rischio non solo il patrimonio informativo di un'organizzazione, ma anche la **salute fisica e mentale dei lavoratori**, ad esempio quando gli hacker attaccano le infrastrutture critiche o prendono il controllo dei dispositivi tecnologici.

Ad esempio nel 2014 in Germania c'è stato un cyberattacco in un'acciaieria e gli aggressori sono riusciti a spegnere il forno con il rischio di creare un evento critico per la sicurezza dei lavoratori. Inoltre nel 2017 la Food and Drug Administration (FDA) statunitense ha richiamato circa 465.000 pacemaker a causa di vulnerabilità di sicurezza a eventuali cyberattacchi.

Gli attacchi informatici ai sistemi di controllo industriale rappresentano dunque una pericolosa minaccia per la vita umana (nel documento si riporta un esempio di cyberattacco per il controllo di centrifughe iraniane utilizzate per l'arricchimento dell'uranio). Si possono poi creare problemi con veicoli o macchinari che possono diventare non controllabili a causa di segnali wireless interrotti o di attacchi da parte di hacker.

Nel documento sono riportati molti altri esempi che riguardano i rischi per la sicurezza dei lavoratori e della popolazione.

Cybersecurity: l'impatto sociale e psicologico dei cyberattacchi

Veniamo, infine, all'**impatto sociale e psicologico**.

Si indica che i cyberattacchi possono avere sia conseguenze sociali, ad esempio la perdita di fiducia nella tecnologia digitale, che psicologiche, come **ansia, rabbia e depressione**.

Ad esempio i lavoratori che sono coinvolti da cyberattacchi possono sentirsi colpevoli, confusi o frustrati, soprattutto in caso di fuga di informazioni digitali e la rilevanza di questi impatti dipende anche dall'ambiente coinvolto. Ad esempio, in un istituto finanziario, dove le conseguenze di una violazione dei dati possono essere più gravi rispetto ad altri luoghi di lavoro, il danno psicologico per i lavoratori può essere maggiore.

Si indica che le ricerche sulla "**vittimizzazione da crimine informatico**" evidenziano varie esperienze negative sia per le aziende che per gli individui. Ad esempio, quando le organizzazioni subiscono attacchi ransomware, i team ne risentono in termini di danni alla fiducia professionale.

Il documento riporta poi utili considerazioni sull'**errore umano**, considerato **la causa principale del 90% delle violazioni della sicurezza informatica**.

Questi errori, come l'apertura di e-mail di phishing o una cattiva gestione delle password, possono esporre le organizzazioni a gravi conseguenze, come l'installazione di software dannoso nella rete aziendale.

E per quanto riguarda questi errori, è importante considerare i fattori psicologici coinvolti negli incidenti di cibersicurezza: il 52% dei lavoratori ha maggiori probabilità di commettere errori quando è stressato, il 43% quando è stanco e il 26% quando si sente esaurito.

Per non parlare del fatto che i professionisti della cybersicurezza sperimentano un alto livello di stress o burnout proprio per il lavoro di prevenzione e mitigazione dei cyberattacchi.

Infine si osserva come la dimensione cyber influisca anche sui **fenomeni di violenza**.

Il cyberbullismo, ad esempio, è la forma più conosciuta di molestia online con l'obiettivo di umiliare, perseguitare e controllare una persona utilizzando mezzi digitali. E le molestie online possono produrre gravi effetti psicosomatici, sociali e mentali.

In definitiva, conclude il documento, la gestione della cybersecurity non deve essere ridotta a una mera protezione tecnologica di sistemi e informazioni. In considerazione del fatto che i cyberattacchi possono avere ripercussioni anche sulla salute e sulla sicurezza dei lavoratori, le organizzazioni dovrebbero adottare un **approccio olistico alla cybersecurity**.

RTM

Scarica il documento da cui è tratto l'articolo:

Agenzia europea per la sicurezza e la salute sul lavoro, "Incorporating occupational safety and health in the assessment of cybersecurity risks", discussion paper in lingua inglese, a cura di Isabella Corradini (Scientific director of Themis Research

Center), edizione 2022.

www.puntosicuro.it