ARTICOLO DI ELEARNINGNEWS

Year 6 - number 212 Wednesday 20 july 2022

Attacchi informatici: quali impatti sulla salute e sicurezza dei lavoratori?

L'Agenzia europea per la sicurezza e la salute sul lavoro analizza la sicurezza informatica in relazione all'impatto sui lavoratori nella valutazione dei rischi informatici.

L'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA) studia, tra gli altri fattori, le conseguenze della digitalizzazione sulla salute e sicurezza sul lavoro per fornire ai decision maker europei, ai datori di lavoro e alle parti sociali le informazioni necessarie sulle sfide emergenti in materia.

I costi globali della **cybersecurity** raggiungeranno i 10.500 miliardi di dollari entro il 2025. Il problema non è circoscritto alle perdite dovute al furto di dati; vi sono, infatti, nuovi **rischi emergenti** per la salute e la sicurezza dei lavoratori. Ma quale è l'impatto della cibersicurezza sui lavoratori?

Secondo il report "**Incorporating occupational safety and health in the assessment of cybersecurity risks**" a cura di Isabella Corradini (Scientific director of Themis Research Center), ogni azienda (indipendentemente dal settore di appartenenza) è a rischio di attacco informatico, soprattutto dopo la rapida evoluzione digitale portata dal 2020. Infatti, dal 2020 il 78% delle organizzazioni ha registrato aumenti nel volume di cyberattacchi a causa del passaggio al lavoro da remoto. Inoltre, la criminalità informatica sta diventando sempre più sofisticata e i criminali informatici sfruttano tutti i tipi di vulnerabilità per i loro attacchi.

L'impatto dei cyberattacchi sulla sicurezza

Gli attacchi informatici non hanno solo una componente tecnologica o economica: il fattore umano e la sicurezza dei lavoratori rappresentano parti importanti della questione.

Infatti, i cyberattacchi possono causare infortuni (anche gravi o gravissimi, fino alla perdita della vita) e problemi psicologici (ansia, frustrazione). Per questo motivo, la **valutazione del rischio informatico** e la **valutazione del rischio salute e sicurezza** devono essere eseguite insieme.

Ecco le possibili conseguenze di un attacco informatico, a livello organizzativo, umano e ambientale.

Alcuni esempi?

- Un attacco informatico in un'acciaieria tedesca nel 2014 è riuscito a spegnere il forno con il rischio di creare un evento critico per la sicurezza dei lavoratori;
- Nel 2017 negli USA, la Food and Drug Administration (FDA) ha richiamato 465.000 pacemaker a causa di vulnerabilità di sicurezza a eventuali cyberattacchi;
- In Iran, un cyber attacco ha avuto come obiettivo il controllo di centrifughe utilizzate per l'arricchimento dell'uranio.

Senza contare che gli attacchi hacker rivolti a apparecchiature con segnali wireless possono creare problemi di controllo di veicoli o macchinari.

L'impatto sociale e psicologico dei cyberattacchi

I cyberattacchi possono avere conseguenze sociali (come la perdita di fiducia nella tecnologia digitale), ma anche psicologiche (ansia, rabbia e depressione).

A seconda del contesto, i lavoratori coinvolti da cyberattacchi possono sentire un carico di colpevolezza, confusione o frustrazione molto o addirittura troppo elevato da gestire; si pensi al caso di fuga di informazioni digitali in banca.

Infatti, le ricerche sulla "**vittimizzazione da crimine informatico**" evidenziano esperienze negative sia per le aziende che per gli individui. Non stupirà pensare che, quando le organizzazioni subiscono attacchi ransomware, i team coinvolti subiscono danni alla fiducia professionale nell'azienda stessa.

L'**errore umano** (apertura di e-mail di phishing o cattiva gestione delle password) è considerato **la causa principale del 90% delle violazioni della sicurezza informatica** e può esporre le organizzazioni a gravi conseguenze, come l'installazione di software dannoso nella rete aziendale.

Per formare i lavoratori (tutti coloro che usano sistemi informatici nell'attività lavorativa) a prevenire gli attacchi informatici dal punto di vista umano, il corso online " **Cyber Security - Tutela dei dati e delle informazioni aziendali**" della durata di 1 ora è un validissimo strumento.

Per quanto riguarda gli errori umani, è importantissimo considerare i fattori psicologici coinvolti negli incidenti di cybersecurity:

- il 52% dei lavoratori ha maggiori probabilità di commettere errori quando è stressato,
- il 43% quando è stanco,
- il 26% quando si sente esaurito (stress o burnout).