PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5732 di Martedì 12 novembre 2024

Cybersecurity e rischio burnout: 5 consigli per prevenirlo

Il burnout colpisce sempre più professionisti della Cybersecurity, esponendo le aziende a maggiori rischi. Scopri come prevenirlo con alcune semplici pratiche per migliorare il benessere lavorativo.

Con l'aumento delle minacce informatiche, sempre più **professionisti nel campo della Cybersecurity** si trovano a dover gestire un carico di lavoro insostenibile, che porta ad un esaurimento emotivo e fisico definito con il termine "**burnout**". Questo fenomeno non riguarda però solo il benessere dei singoli lavoratori: infatti, può aumentare il rischio di errori che possono mettere in pericolo la sicurezza delle organizzazioni.

La realtà del burnout nella Cybersecurity

Il burnout è una condizione di stress cronico che si manifesta con una condizione di estrema stanchezza percepibile sia a livello fisico che mentale, sensazione di distacco dal lavoro e ridotta efficacia professionale. Secondo un **rapporto di Bitdefender**, nota società di software antivirus e di sicurezza informatica, circa il **70% degli specialisti in sicurezza informatica** si trova sull'orlo del crollo, e il **64% di questi professionisti** sta attivamente cercando un nuovo lavoro per sfuggire alla pressione crescente.

La pandemia ha contribuito ad aggravare questa situazione, con un aumento del **600% degli attacchi informatici** dall'inizio del 2020. L'incremento esponenziale delle minacce ha sovraccaricato i professionisti della Cybersecurity, che devono essere sempre vigili e pronti a intervenire rapidamente. Questo stato di allerta costante ha un impatto diretto non solo sulla salute mentale degli esperti, ma anche sulla loro capacità di mantenere alte le prestazioni.

L'aumento degli attacchi cyber ha inoltre incrementato l'interesse dei criminali verso infrastrutture critiche, come ospedali e reti energetiche. Un errore umano, anche minimo, potrebbe dunque aprire la porta a devastanti conseguenze per aziende e settori pubblici.

Le cause principali di burnout nella Cybersecurity

Le cause del burnout nel settore della Cybersecurity sono molteplici e interconnesse. Un **rapporto di Gartner** ha identificato diverse ragioni principali per cui i professionisti del settore soffrono di stress cronico:

1. **Volume di lavoro insostenibile**: il sovraccarico di lavoro è indicato come la causa principale di burnout dal **90% dei professionisti della sicurezza informatica**. Molti si trovano a gestire numerosi progetti con scadenze serrate, un fattore che contribuisce direttamente al loro stress.
2. **Aumento delle minacce globali**: il **60% dei leader aziendali** ritiene che l'espansione delle minacce a livello globale, legata a questioni geopolitiche e nuove forme di attacchi, sia una delle principali cause dello stress nei team di sicurezza.
3. **Carenza di risorse e supporto**: le risorse limitate sono un altro elemento che contribuisce al burnout. Molte organizzazioni non forniscono ai loro team di sicurezza informatica il supporto adeguato, costringendoli a lavorare in

condizioni di stress continuo.
4. **Pressione costante e responsabilità elevate**: i professionisti della Cybersecurity sanno che un solo errore può avere conseguenze devastanti. Questa pressione costante porta a un aumento del carico di responsabilità che non è facile da gestire, specialmente senza un supporto adeguato.
5. **Cultura aziendale inadeguata**: spesso le aziende non promuovono una cultura del benessere che possa mitigare lo stress. Questo crea un ambiente di lavoro tossico, dove il burnout diventa inevitabile.

5 consigli pratici per prevenire il burnout nella Cybersecurity

Per affrontare e prevenire il burnout nel settore della Cybersecurity, è fondamentale che i professionisti e le aziende adottino strategie concrete. Ecco cinque consigli pratici per gestire meglio il carico di lavoro e mantenere un equilibrio tra vita lavorativa e privata:

1. **Promuovere una cultura del benessere aziendale**: le organizzazioni devono creare una cultura aziendale che ponga l'accento sul benessere dei dipendenti. Politiche flessibili, programmi di supporto psicologico e momenti di pausa strutturati possono aiutare a ridurre lo stress. L'importanza del **team building** non dovrebbe essere sottovalutata, specialmente in contesti ad alta pressione come la Cybersecurity.
2. **Automatizzare e delegare**: automatizzare i processi ripetitivi e noiosi attraverso software specifici può liberare tempo prezioso per attività più critiche. Allo stesso tempo, delegare compiti a membri del team meno sovraccarichi può alleggerire la pressione.
3. **Supporto e formazione continua**: le aziende devono **investire nella formazione** non solo per migliorare le competenze tecniche dei loro team, ma anche per fornire strumenti di gestione dello stress. Programmi di coaching e mentoring possono essere particolarmente utili nei momenti di crisi.
4. **Favorire un bilanciamento tra vita privata e lavoro**: i professionisti della Cybersecurity devono essere incoraggiati a prendersi pause regolari e a mantenere un sano equilibrio tra lavoro e vita privata. Le aziende possono facilitare questo processo promuovendo orari flessibili e lo smart working.
5. **Costruire team coesi e comunicativi**: un team coeso e ben comunicante è più resiliente allo stress. I leader devono favorire una comunicazione aperta, permettendo ai membri del team di esprimere le loro preoccupazioni senza timore di ritorsioni.

L'importanza della sicurezza informatica e la formazione

Il burnout nel settore della Cybersecurity rappresenta un problema che va oltre il benessere individuale, influenzando direttamente la sicurezza delle organizzazioni. Un team esausto e sovraccarico è più incline a commettere errori, aumentando il rischio di violazioni e attacchi informatici. Questa connessione tra benessere psicofisico e sicurezza aziendale rende fondamentale l'investimento non solo in tecnologie avanzate, ma anche nel supporto continuo per i professionisti della Cybersecurity.

In questo contesto, la **formazione continua** ha un ruolo chiave. Non basta affidarsi solo a tecnologie sofisticate per garantire la protezione dai cyberattacchi: è altrettanto cruciale che i dipendenti siano costantemente aggiornati sulle nuove minacce e sulle migliori pratiche di sicurezza. Un training regolare può **aiutare a ridurre gli errori umani**, che rappresentano una delle principali cause di violazioni di sicurezza. La formazione in ambito Cybersecurity consente ai dipendenti di riconoscere i segnali di pericolo e di agire tempestivamente per prevenire incidenti informatici.

Alice Gugliotta

Fonte: eLearningnews

www.puntosicuro.it