PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5658 di Martedì 09 luglio 2024

La Cyber Security aziendale e l'importanza della formazione

Per costruire una strategia di Cyber Security robusta, le aziende devono adottare un approccio multilivello tecnico/umanistico che include alcuni aspetti tecnici e alcuni aspetti umani.

Il 4 giugno scorso, ospedali e cliniche di Londra collegati al Servizio Sanitario Nazionale britannico (NHS) sono stati colpiti da un grave **attacco ransomware**. Lo scorso febbraio, il rivenditore europeo Pepco Group è stato bersaglio di un sofisticato **attacco di phishing** fraudolento contro la sua attività in Ungheria. Un ex dipendente di Google è stato arrestato lo scorso marzo per aver **rubato dati sensibili** e diverse tecnologie di intelligenza artificiale dall'azienda, collaborando segretamente con due società cinesi.

Questi tre casi recenti dimostrano come **errori umani e mancanze procedurali** possano esporre le aziende, anche quelle più grandi, a **gravi rischi informatici reali**.

Ogni giorno migliaia di realtà di tutto il mondo si trovano ad affrontare vari tipi di cyberattacchi, che purtroppo sembrano aumentare di anno in anno. Secondo una **statistica di Digital 360**, solo in **Italia** nel 2023 gli attacchi informatici sono stati **il 29% in più** rispetto all'anno precedente e i soggetti colpiti sono passati da 1.150 a 3.302. Secondo uno studio globale di **CyberSecurity Ventures**, si stima che **ogni 39 secondi avviene un attacco informatico**. Questo ritmo incessante non solo dimostra quanto sia pervasiva la minaccia, ma anche quanto sia facile per un attacco riuscire a penetrare difese deboli o disattente.

Questi rischi non solo mettono a repentaglio la riservatezza, l'integrità e la disponibilità dei dati aziendali, ma possono anche causare danni economici ingenti e minare la fiducia dei clienti. Un singolo attacco può costare milioni di euro, considerando il costo del downtime, le riparazioni e le possibili multe legate alla perdita di dati. Tuttavia, l'impatto reputazionale può essere ancora più dannoso, con la perdita di fiducia da parte dei clienti e la compromissione delle relazioni commerciali.

In questo contesto, la Cyber Security non è più una scelta, ma una necessità strategica.

Le aziende devono adottare un approccio proattivo e multilivello per proteggere i propri asset digitali. Questo include non solo l'implementazione di tecnologie avanzate, ma anche la **formazione continua** dei dipendenti per riconoscere e rispondere alle minacce.

Ma quindi, cos'è la Cyber Security?

La Cyber Security comprende tutte le pratiche, tecnologie e processi necessari per proteggere i sistemi, le reti e i dati aziendali da attacchi, danni o accessi non autorizzati.

Si basa su tre principi fondamentali. Il primo è la **confidenzialità**, che assicura che solo le persone autorizzate possano accedere ai dati. Il secondo è l'**integrità**, che garantisce che i dati non vengano alterati o cancellati senza autorizzazione. Infine, la **disponibilità**, che assicura che i sistemi e i dati siano sempre accessibili quando necessario.

Come creare una Cyber Security efficace

Per costruire una strategia di Cyber Security robusta, le aziende devono adottare un **approccio multilivello tecnico/umanistico** che include alcuni aspetti tecnici e alcuni aspetti umani.

Per gli aspetti tecnici, è necessario mettere in atto:

- **Tecnologie di sicurezza**: implementazione di firewall, antivirus, sistemi di rilevamento delle intrusioni e crittografia dei dati.
- **Procedure di sicurezza**: sviluppo di politiche aziendali chiare riguardo all'uso dei dispositivi, all'accesso ai dati e alla gestione delle password.
- **Monitoraggio e risposta**: utilizzo di sistemi di monitoraggio per rilevare attività sospette e avere piani di risposta agli incidenti ben definiti.
- **Backup e recupero**: regolari backup dei dati e piani di disaster recovery per garantire la continuità operativa.

Per la componente umana è necessario tener conto del fatto che spesso è l'anello più debole nella catena della sicurezza informatica. **Ecco perché la formazione dei dipendenti è fondamentale.**

Prima di tutto, è necessario **renderli consapevoli** delle varie minacce informatiche e insegnare loro a riconoscerle. Poi, devono **apprendere le migliori pratiche** per gestire le password, usare i dispositivi in modo sicuro e navigare online senza rischi. Infine, è importante **creare una cultura della sicurezza** in cui ogni dipendente si senta responsabile della protezione dei dati aziendali.

Investire nella Cyber Security aziendale non è più un'opzione, ma una necessità per proteggere il futuro dell'azienda. Una combinazione di tecnologie avanzate e formazione continua dei dipendenti rappresenta la strategia più efficace per mitigare i rischi informatici.

I corsi di formazione aziendale sulla Cyber Security di Mega Italia Media

Mega Italia Media è un partner affidabile per le aziende che desiderano rafforzare la propria sicurezza informatica attraverso corsi di formazione mirati e di alta qualità.

Nel proprio catalogo di corsi online, Mega Italia Media offre una gamma completa di **corsi specifici per la Cyber Security aziendale**, progettati per garantire che i dipendenti possano applicare immediatamente ciò che hanno imparato.

Consulta il **catalogo completo dei corsi online sulla Cyber Security**.

Ecco di seguito i titoli dei corsi proposti da Mega Italia Media:

- **Corso online - Cyber Security: Tutela dei dati e delle informazioni aziendali ? 45 minuti** (disponibile anche in lingudifendea inglese)
- **Corso online - Cyber Security - Difendersi dai crimini informatici - 1 ora**
- **Corso online - Cyber Security - La difesa olistica del sistema aziendale - 1,5 ore**
- **Corso online - Crittografia - Messaggi cifrati, segreti assicurati - 40 minuti**
- **Corso online - Ransomware - Non cadere in trappola - 30 minuti**
- **Corso online - Phishing - Guida pratica all'autodifesa - 30 minuti**
- **Corso online - Phone hacking - Manteniamo il controllo! - 30 minuti**
- **Corso online - Surface, Deep e Dark web - Cosa c'è sotto? - 30 minuti**
- **Corso online - Sicurezza e riservatezza delle informazioni aziendali - 15 minuti**

---

www.puntosicuro.it