ARTICOLO DI ELEARNINGNEWS

Year 8 - number 292 Wednesday 05 june 2024

La Cyber Security aziendale e l'importanza della formazione

Secondo diverse ricerche, si stima che ogni 39 secondi avviene un attacco informatico. In questo contesto, la Cyber Security non è più una scelta, ma una necessità strategica.

Ogni giorno, le aziende di tutto il mondo affrontano migliaia di cyberattacchi. Dai ransomware che paralizzano le operazioni, ai phishing che compromettono i dati sensibili, fino agli attacchi da insider, la sicurezza informatica è una sfida costante.

Come puoi immaginare, oltre al danno diretto sulla redditività aziendale (mancate vendite, mancata erogazione dei servizi, perdita di clientela potenziale, eccetera), un attacco informatico può costare molto alla tua azienda anche per le attività di ripristino/ricostruzione dei dati, se non addirittura il pagamento di un riscatto per 'liberare' i tuoi sistemi.

Secondo diverse ricerche, 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 lingua 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**