Cybersecurity, cos’è e perché è importante per la tua azienda

La digitalizzazione è sempre più presente a tutti i livelli; ha rivoluzionato e sta continuando a rivoluzionare le nostre vite e, ovviamente, ha radicalmente trasformato il modo in cui le aziende di tutti i settori conducono le proprie attività; i vantaggi della digitalizzazione sono evidenti, ma al tempo stesso, la crescente dipendenza dalla Rete e dai software ha dato vita anche a un notevole sviluppo dei crimini informatici; ciò ha fatto sì che la cybersecurity, ovvero la sicurezza informatica, sia diventata un punto fermo per tutte le aziende, grandi o piccole che siano.

Cos’è la cybersecurity?

La cybersecurity, o cybersicurezza, è il campo dell’informatica e della tecnologia che si occupa della protezione di sistemi informatici, reti, dati e dispositivi da minacce cibernetiche, attacchi informatici e violazioni della sicurezza. Il suo obiettivo principale è quello di garantire la confidenzialità, l’integrità e la disponibilità delle risorse digitali, nonché prevenire danni e garantire che le operazioni aziendali e personali rimangano sicure e protette nell’ambiente digitale.

La cybersecurity non è un optional

Come vedremo più avanti, la cybersecurity è di vitale importanza per le aziende e non può essere considerata un optional; è per questo motivo che è fondamentale che dipendenti e collaboratori aziendali frequentino un Corso Cybersecurity che fornisca una formazione adeguata che

permetta loro di riconoscere facilmente le minacce e gli attacchi informatici più tipici; è sicuramente il modo migliore per proteggere la propria rete e i dati aziendali.

Perché la cybersecurity è importante per un’azienda?

L’importanza della cybersecurity per un’azienda può essere così schematicamente riassunta:

- **protezione dei dati sensibili:** le aziende raccolgono, elaborano e archiviano una quantità sempre maggiore di dati sensibili, inclusi dati finanziari, informazioni personali di clienti, fornitori, dipendenti, collaboratori nonché documenti relativi a strategie aziendali. Una violazione dei dati può causare danni irreparabili alla reputazione dell’azienda e potenzialmente portare a gravi conseguenze legali.
- **Continuità operativa:** un attacco informatico riuscito può causare lunghe interruzioni dell’operatività aziendale. La perdita di accesso a dati, sistemi e servizi può portare a ritardi nella produzione, a perdite finanziarie e a insoddisfazione dei clienti.
- **Protezione della proprietà intellettuale:** molte aziende investono tempo e risorse nello sviluppo di proprietà intellettuali, come brevetti, marchi e segreti commerciali. La mancanza di sicurezza informatica può rendere vulnerabili tali asset (a causa di furti informatici, violazioni ecc.).
- **Obblighi normativi:** in molte giurisdizioni, le aziende sono tenute a rispettare normative specifiche sulla protezione dei dati, come per esempio il *Regolamento Generale sulla Protezione dei Dati* (GDPR) in Europa. Le violazioni di tali normative possono comportare sanzioni finanziarie significative.
- **Affidabilità da parte dei clienti:** i clienti si fidano delle aziende con cui fanno affari relativamente alla

sicurezza delle loro informazioni personali. Una violazione dei dati può minare la fiducia del cliente, con tutte le conseguenze del caso.

- **Minimizzazione del rischio finanziario:** gli attacchi informatici possono causare costi imprevisti per affrontare le conseguenze dell'attacco, come la risoluzione delle violazioni, la riparazione dei sistemi e l'eventuale pagamento di danni a terzi colpiti.

Quali sono le principali misure di cybersecurity?

Per garantire la cybersecurity nella propria azienda, è fondamentale implementare una serie di misure e pratiche di sicurezza, tra cui si ricordano principalmente:

- **firewall e protezione antivirus:** installare firewall e software antivirus per rilevare e prevenire gli accessi non autorizzati e l'installazione di malware.
- **Aggiornamenti regolari:** mantenere tutti i software e i sistemi operativi aggiornati con le patch di sicurezza più recenti.
- **Autenticazione forte:** implementare l'autenticazione a più fattori per impedire l'accesso non autorizzato anche in caso di violazione delle credenziali.
- **Consapevolezza del personale:** formare il personale sui rischi della sicurezza informatica e promuovere comportamenti sicuri.
- **Backup dei dati:** eseguire regolarmente il backup dei dati critici e archiviarli in luoghi sicuri per la ripresa operativa in caso di attacco informatico.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cybersecurity-cose-e-perche-e-importante-per-la-tua-azienda/