ARTICOLO DI ELEARNINGNEWS

Year 9 - number 327 Wednesday 26 march 2025

Cyber attacchi in crescita: l'accordo che punta sulla prevenzione

Polizia di Stato e Confindustria uniscono le forze per rafforzare la sicurezza informatica delle aziende. Ma senza formazione, nessuna difesa è davvero efficace.

Nessuna azienda è al sicuro. Negli ultimi anni, **gli attacchi informatici sono diventati sempre più sofisticati e frequenti**, colpendo indiscriminatamente imprese di qualsiasi settore e dimensione. I dati parlano chiaro: tra il 2021 e il 2022 le denunce per reati informatici presentate dalle aziende sono più che raddoppiate, passando da 5.000 a oltre 13.000, per poi assestarsi intorno alle 12.000 nel 2023.

Le tecniche utilizzate dai criminali informatici sono sempre più avanzate e mirate. Il ransomware, ad esempio, blocca i sistemi aziendali e chiede un riscatto per ripristinare i dati. Altri attacchi puntano al furto di informazioni sensibili, utilizzabili per truffe o per la vendita nel dark web. Il problema non riguarda solo le grandi aziende, che investono in soluzioni di sicurezza avanzate, ma colpisce soprattutto le piccole e medie imprese, spesso meno attrezzate per contrastare la minaccia.

L'accordo tra Polizia e Confindustria

Per rispondere a questa emergenza, **Polizia di Stato e Confindustria Brescia** hanno firmato un **protocollo d'intesa** con l'obiettivo di rafforzare la cybersecurity delle aziende. L'accordo si basa su tre azioni principali.

1. **Aumentare la resistenza cyber delle aziende**: attraverso la condivisione degli indici di compromissione, le imprese riceveranno alert tempestivi su minacce in corso, permettendo loro di rafforzare le proprie difese prima che sia troppo tardi.
2. **Definire procedure efficaci in caso di attacco**: un sistema di sicurezza non è efficace solo nella prevenzione, ma anche nella capacità di rispondere rapidamente agli incidenti. Le imprese saranno guidate su come reagire in modo efficace per limitare i danni di un attacco.
3. **Potenziare la formazione sulla sicurezza informatica**: il punto più cruciale. Come sottolineato dalla dirigente del Centro Operativo per la Sicurezza Cibernetica della Lombardia, Manuela De Giorgi, la maggior parte degli attacchi informatici si basa sulla collaborazione inconsapevole della vittima. Un semplice clic su un link fraudolento può aprire la porta a intrusioni devastanti. Nessun software di sicurezza può essere efficace se chi lo utilizza non è consapevole dei rischi e non sa riconoscere le minacce.

Il fattore umano: l'anello debole della sicurezza informatica

Gli hacker non si limitano più a cercare falle nei sistemi informatici: puntano direttamente alle persone. Tecniche di **social engineering** come il phishing e lo spear phishing mirano a ingannare i dipendenti per ottenere credenziali di accesso o installare malware. Spesso, un'e-mail apparentemente innocua o una telefonata ben studiata sono sufficienti a compromettere intere infrastrutture aziendali.

Eppure, molte imprese continuano a sottovalutare questo aspetto, concentrandosi solo sugli investimenti in software di protezione e firewall avanzati. Ma nessuna barriera tecnologica può sostituire una **cultura della sicurezza informatica diffusa in azienda**. Se i dipendenti non vengono adeguatamente formati, rischiano di essere il punto d'ingresso per un attacco, vanificando qualsiasi strategia di difesa informatica.

Questa vulnerabilità è ancora più evidente nelle piccole e medie imprese, dove la cybersecurity è spesso percepita come un costo accessorio e non come una necessità. Molte PMI non dispongono di un team IT dedicato e delegano la gestione della sicurezza a figure non specializzate, aumentando il rischio di subire attacchi devastanti. Proprio per questo, il protocollo firmato tra Polizia di Stato e Confindustria ha un valore strategico: **promuovere la consapevolezza** e fornire strumenti concreti per **proteggere il**

tessuto imprenditoriale italiano.

Cybersecurity e formazione

Se il fattore umano è il punto più vulnerabile nella sicurezza informatica, allora la **formazione diventa la prima linea di difesa**. Tuttavia, insegnare alle aziende e ai loro dipendenti come riconoscere e contrastare le minacce cyber non è semplice: servono strumenti efficaci, aggiornamenti costanti e metodologie che favoriscano l'apprendimento continuo.

In questo contesto, l'**eLearning** si rivela la soluzione ideale. I corsi online permettono alle imprese di formare il proprio personale in modo flessibile, con moduli sempre aggiornati sulle nuove minacce e modalità di attacco.

Uno degli errori più diffusi nelle aziende è considerare la cybersecurity come un problema esclusivamente tecnologico, delegandolo ai reparti IT senza coinvolgere attivamente tutti i dipendenti. In realtà, **la sicurezza informatica è una responsabilità condivisa**.

- **Dirigenti e manager**: devono conoscere le strategie di prevenzione e gestione del rischio per prendere decisioni rapide in caso di attacco.
- **Dipendenti operativi**: sono il primo bersaglio degli hacker e devono saper individuare tentativi di phishing e social engineering.
- **Team IT e sicurezza**: hanno bisogno di un aggiornamento costante su nuove minacce, vulnerabilità e strategie di difesa.

Un click sbagliato da parte di un impiegato può compromettere l'intero sistema aziendale. Proprio per questo, la formazione deve essere diffusa a tutti i livelli, creando una cultura della sicurezza informatica all'interno dell'azienda.

Mega Italia Media offre una gamma di **corsi eLearning** progettati per formare dipendenti e manager sulle **minacce informatiche**, fornendo strumenti concreti per prevenire attacchi e proteggere i dati aziendali.

I corsi includono:

- Tecniche per identificare e prevenire attacchi informatici come phishing, malware e ransomware.
- Strategie di difesa informatica per proteggere reti, dati e sistemi aziendali.
- Approfondimenti normativi sulla sicurezza informatica.

Investire nella formazione è la soluzione più efficace per ridurre i rischi e garantire la continuità operativa. **Scopri tutti i corsi**.