



Dicembre 2021
n°8

ASSISTENZA TECNICA

PRONTO INTERVENTO, PREVENZIONE
E MANUTENZIONE



COME GESTIRE LA SICUREZZA INFORMATICA AZIENDALE, O CYBER SECURITY

Una tematica destinata ad acquisire un ruolo
sempre più importante nelle imprese

“Le competenze degli hacker e la modalità con cui agiscono cambiano rapidamente.”



La **sicurezza informatica aziendale** è un argomento che riguarda da vicino ogni tipo di impresa. I trend parlano chiaro: nel 2020, gli attacchi cyber gravi sono **incrementati del 12 %** a livello globale e la percentuale è destinata a salire. Che i rischi vadano da un fermo della produzione o delle vendite a danni reputazionali, sapere come gestire la **sicurezza informatica aziendale** è più che mai importante.

Cyber security: cos'è?

Con il termine **cyber security**, o sicurezza informatica, si intende l'insieme di strategie, regole, comportamenti e implementazioni per gestire il rischio di attacchi informatici. In un'azienda, costruire una struttura difensiva di questo calibro è **complesso ma fattibile**. Approfondire la propria cultura in questo campo è fondamentale: vediamo insieme quali sono gli **attacchi alla cyber security aziendale** e quali modalità di protezione è possibile mettere in campo.

Attacchi informatici: cosa sapere?

Conoscere le diverse tipologie di cyber attack è importante per sapere da cosa ci si deve proteggere. Elenchiamo di seguito gli attacchi informatici più comuni e conosciuti:

- **Malware:** è un'applicazione dannosa che causa malfunzionamenti. Raccoglie dati illegalmente o li cripta per renderli inaccessibili;
- **Ransomware:** è un tipo di malware che impedisce l'accesso al sistema infettato e richiede una somma di denaro per venire rimosso. I **cryptolocker** fanno parte di questa categoria;
- **Phishing:** il phishing è una frode informatica che ha l'obiettivo di estorcere i dati sensibili e le informazioni riservate degli utenti;

- DoS: acronimo di **Denial of Service**, è un attacco che interrompe la continuità di un servizio o, in alternativa, che lo rende inaccessibile.

Quale attività è fondamentale per la sicurezza informatica?

La risposta a questa domanda è complessa, in quanto gli attacchi informatici sono in **continua evoluzione**; le competenze degli hacker e la modalità con cui agiscono cambiano rapidamente. Improvvisare soluzioni temporanee o svolgere dei controlli una tantum non rappresentano, quindi, una protezione sufficiente.

Quale attività, invece, è fondamentale per un'efficace sicurezza informatica aziendale?

Un'analisi del rischio, effettuata con il supporto di figure specializzate, è il modo migliore per riflettere sulla propria situazione e prendere provvedimenti adeguati. In linea generale, prevede di rispondere alle seguenti domande:

- A **quali rischi** sono esposto?
- Quali beni aziendali, materiali e non, possono essere **danneggiati** da un attacco informatico?
- Quali sono le **vulnerabilità** delle mie infrastrutture e come potrebbero essere sfruttate per commettere crimini informatici?

- Quali sono le soluzioni disponibili e come le integro nel mio **sistema informatico**?

La strategia stessa, inoltre, dovrà essere analizzata ciclicamente per assicurarsi che sia calibrata su esigenze reali e sui nuovi sistemi di aggressione.

Il fattore umano

Le strategie di **sicurezza informatica** aziendale che funzionano davvero prevedono anche la formazione dei dipendenti in materia. È stato rilevato, infatti, che il comportamento umano può involontariamente causare fino all'**80 %** degli attacchi informatici aziendali.

Quali sono, in generale, le buone abitudini da avere?

- Informarsi con frequenza sulle **modalità** di cyber attack, in quanto evolvono in continuazione e non farsi trovare impreparati è fondamentale;
- Navigare solo su **siti sicuri**, che si riconoscono dal lucchetto verde e dalla dicitura **https** all'inizio dell'url;
- Mantenere **aggiornati** il sistema, il browser e le app su ogni dispositivo aziendale;
- **Non aprire allegati** di email provenienti da indirizzi sconosciuti;
- **Non condividere** le password.

Cosa può fare Zen Srl per la tua **sicurezza informatica aziendale**? Possiamo fornire e configurare **dispositivi firewall** - in grado di filtrare gli accessi alla rete aziendale - e conservare, tramite il servizio di **backup remoti**, una **copia dei dati più importanti** per la tua azienda. Siamo conosciuti, inoltre, per la rapidità con cui forniamo **assistenza tecnica remota**: una veloce telefonata al nostro Help Desk ha evitato, in molti casi, che il “fattore umano” causasse gravi danni.

Hai bisogno di un partner strategico **affidabile e disponibile** per le tue attività di cyber security aziendale? Contattaci a info@zensrl.it per scoprire come possiamo supportarti!