

Perché le PMI italiane sono tra le più colpite dal cybercrime



Nel 2022, le PMI italiane sono state costantemente nel mirino degli hacker. Mai come oggi, un'azienda italiana che guarda al futuro ha la necessità di investire in soluzioni di sicurezza informatica all'avanguardia.

Cybercrime in Italia: il 2022 è stato l'anno nero per le PMI

I dati relativi al cybercrime non mentono: nel 2022 **le PMI italiane sono state le più colpite dagli hacker** in Europa. La percentuale degli attacchi indirizzati alle imprese con un fatturato inferiore a 250 milioni di euro ha toccato addirittura l'80%, con il 51% dei bersagli rappresentato da organizzazioni con meno di 100 dipendenti.

È quanto emerge dall'analisi del Soc & Threat Intelligence Team di Swscan, che ha effettuato lo studio considerando solamente le aziende esposte in rete a seguito del mancato pagamento di un riscatto. Le PMI sono quindi un bersaglio facile, spesso costretto a cedere ai ricatti degli hacker per riprendere l'operatività del proprio business.

Una categoria impreparata

Perché gli hacker prendono di mira soprattutto le aziende di questa dimensione? Principalmente a causa di una **generale disinformazione** riguardo alle conseguenze dirette di un *data breach*. Le PMI non investono a sufficienza nella cybersicurezza e si trovano impreparate di fronte a una minaccia informatica concreta.

In secondo luogo, il tema della cybersecurity è tuttora un **argomento delicato per moltissime imprese italiane**, che non possiedono esperti di cybersecurity tra le proprie file e non istruiscono il personale in materia. Questa mancanza di formazione rende più facile la vita agli hacker, che possono perpetrare gli attacchi con facilità grazie a sistemi automatizzati e all'intelligenza artificiale.

L'importanza di affidarsi a esperti per gestire la cybersecurity

Per un'azienda che vuole evolversi nel tempo, investire nella sicurezza informatica è fondamentale. Gli attacchi informatici sono sempre più complessi; pertanto, è necessario affidarsi a un **partner IT specializzato** non solo nella risposta a un attacco informatico e nelle fasi post-incident, ma anche nella prevenzione e nella ricerca di informazioni sulle minacce emergenti.

Questo tipo di approccio "ibrido" richiede la combinazione di **competenze in ambito security e sistemistico**, grazie alle quali un esperto può qualificare gli eventi malevoli e intervenire in modo efficace. È inoltre necessaria una sorveglianza costante e un continuo studio delle dinamiche della dimensione cyber affinché l'azienda possa affrontare il futuro al meglio.

Il valore aggiunto dell'approccio ibrido di ACS

Ermanno Furlan e Mauro Gottardi, rispettivamente Head of Cybersecurity e Head of Sales di ACS Data Systems, interverranno nell'ambito del Forum ICT Security per illustrare i vantaggi di un approccio ibrido che integra la collaborazione tra esperti in cybersecurity e sistemisti.

ACS Data Systems, azienda attiva da molti anni nel settore IT

e con sedi in tutto il Triveneto, offre soluzioni efficaci per consentire alle aziende di occuparsi unicamente del proprio business. Grazie a un **SOC dedicato** e a servizi in ambito Cybersecurity, IT Infrastructure, Modern Work e Digital Signage, ACS Data Systems promuove l'innovazione tecnologica delle aziende giorno dopo giorno.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/perche-le-pmi-italiane-sono-tra-le-piu-colpite-dal-cybercrime/>