Il report "Allianz Risk Barometer 2024" & i rischi informatici

"I rischi informatici sono la principale preoccupazione per le aziende a livello globale, in Italia e in molti altri paesi.
Le violazioni dei dati, gli attacchi alle infrastrutture critiche e gli attacchi ransomware sono le minacce informatiche più allarmanti per gli intervistati."

Report "Allianz Risk Barometer 2024"

I rischi informatici sono la principale preoccupazione per le aziende sia in Italia che nella maggior parte dei Paesi sviluppati. Le violazioni dei dati, gli attacchi alle infrastrutture critiche e gli attacchi ransomware sono le minacce informatiche più allarmanti per gli intervistati .

Questa è la conclusione dell'**Allianz Risk Barometer 2024**, un sondaggio annuale che domanda alle aziende di indicare i rischi che considerano più importanti.
Per la prima volta, i pericoli informatici hanno superato tutti gli altri rischi, dopo le interruzioni di attività, le crisi economiche e i cambiamenti climatici.

Le PMI sono particolarmente vulnerabili ai pericoli informatici.
Queste aziende spesso non hanno le risorse o le competenze necessarie per proteggere adeguatamente i propri sistemi informatici. Inoltre, sono più esposte alle minacce informatiche perché sono spesso prese di mira dai criminali che considerano le PMI più facili da colpire.

I motivi di questa crescente preoccupazione sono diversi.
Innanzitutto, le aziende sono sempre più dipendenti dalla tecnologia, sia per le attività quotidiane che per le operazioni critiche. Ciò le rende più vulnerabili agli attacchi informatici, che possono causare danni finanziari, danni alla reputazione e persino la perdita di dati sensibili.

In secondo luogo, le tecniche utilizzate dai criminali informatici stanno diventando sempre più sofisticate. Gli hacker stanno utilizzando l'intelligenza artificiale (AI) e altre tecnologie innovative per sviluppare attacchi più efficaci.

Cosa possono fare le aziende per **proteggersi** dai pericoli informatici?

- Adottare un approccio pro-attivo alla sicurezza informatica.

Ciò significa identificare le risorse informatiche più importanti e implementare misure di sicurezza appropriate per proteggerle.

- Investire in strumenti di rilevamento e risposta avanzati.

Il rilevamento precoce di un attacco informatico è fondamentale per limitare i danni.

- Formare i dipendenti ai rischi informatici.

I dipendenti dovrebbero essere consapevoli delle minacce informatiche e delle misure di sicurezza da adottare per proteggersi.

Inoltre rivolgersi ad aziende e consulenti tecnici specializzati nella cyber-sicurezza, come ad esempio **IPnext**, le quali sono in grado di svolgere un "assessment" della situazione e fornire la migliore soluzione che non si limiti a mettere in sicurezza l'infrastruttura presente, ma che tenga conto di mantenerla nelle condizioni richieste, all'evolvere delle possibili minacce.

Le aziende che non investono nella sicurezza informatica si espongono a rischi significativi. Un attacco informatico può avere **un impatto devastante sui risultati economici di un'azienda, sulla sua reputazione e persino sulla sua sopravvivenza.**

Link:

- Report Allianz Risk Barometer 2024

IPnext
Siamo partner tecnologici di molte imprese italiane.
Progettiamo e integriamo per loro le soluzioni ICT più evolute.
Per continuare a crescere, insieme.

- IPnext sito Web
- IPnext documentazione & soluzioni
- IPnext LinkedIn
- IPnext Newsletter “Verba Volant”

#AlliazRiskBarometer2024 #cybersecurity #PMI #IPnext #PaloAlto #AristaNetworks