Bitdefender

Hacked Off!

2019

Il panorama delle minacce è in costante evoluzione.

Questo stato di continuo mutamento sta aumentando la pressione sui professionisti della sicurezza informatica, che sono chiamati a identificare le debolezze organizzative e i punti deboli per combatterli efficacemente. Lo studio Hacked Off! di Bitdefender fa luce sullo stato attuale del panorama globale della sicurezza informatica, fornendo approfondimenti su come superare ogni sfida.

Non è se, ma quando!

In tutti i Paesi coinvolti nella survey

57%

Il 57% delle aziende ha subito una violazione nel 2017, 2018 o 2019.

24%

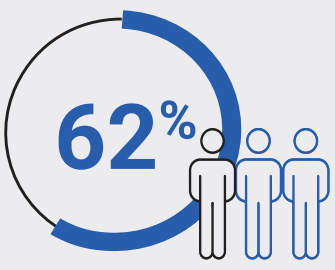
Il 24% delle aziende ha già subito una violazione dei dati nella prima metà del 2019.

36%

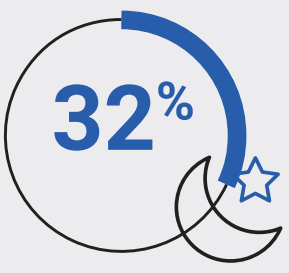
Il 36% delle aziende che non ha subito un attacco informatico ritiene sia probabile che lo stia affrontando senza saperlo.

Nessuna organizzazione è immune alle violazioni di dati!

In Italia, le minacce sono sempre all'erta, la pressione è alta e non c'è tempo per riposare



Il 62% dei professionisti di sicurezza informatica sente di non poter far fronte a un altro attacco informatico come GoldenEye o WannaCry.

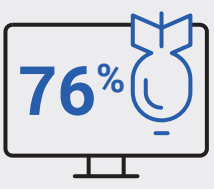


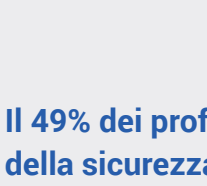
Quasi un terzo dei professionisti di sicurezza informatica (32%) sostiene di non dormire la notte preoccupandosi della sicurezza informatica della propria organizzazione.

I professionisti della sicurezza informatica sono fin troppo consapevoli dei rischi e sono sottoposti a una pressione immensa!

In Italia, mancanza di supporto, a ogni livello

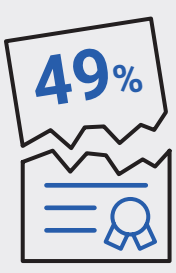
Il 76% dei professionisti di sicurezza informatica ha svelato che la propria azienda è a rischio attacco a causa della mancanza di competenze.





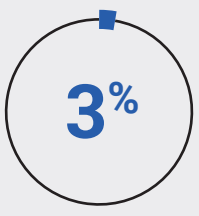
Più di un terzo dei professionisti di sicurezza informatica (38%) ha riferito che manca un supporto tecnologico adeguato.

Il 49% dei professionisti della sicurezza informatica ha anche dichiarato che il management è meno propenso a rispettare la policy di sicurezza aziendale, rifiutando o ignorando completamente le regole.



La mancanza di supporto da parte dei vertici dell'azienda è un grosso problema, poiché la causa più comune delle violazioni aziendali nel 2019 è stata proprio i soggetti esterni (33%).

È ora di cambiare



Usando i propri strumenti di sicurezza attuali, a livello globale, solo il **3% dei professionisti IT** ha riferito che il 100% degli attacchi avanzati possono essere rilevati e isolati in modo efficiente.

C'è spazio per un miglioramento e in base ai professionisti di sicurezza informatica, in Italia occorre investire maggiormente nei seguenti ambiti:

41% Analisi del traffico di rete

47% Tecnologia antimalware

34% Ricercatori di sicurezza interni / SOC

23% Rilevamento comportamentale

24% Apprendimento automatico

21% Sandox automatico

18% Sicurezza esternalizzata a MSP/MSSP

In conclusione, ai professionisti della sicurezza informatica servono i giusti strumenti, risorse e talenti per compiere il proprio lavoro fino in fondo!

Metodologia

6.000

Sono stati intervistati 6.000 professionisti di sicurezza aziendale.

Gli intervistati provenivano da **Stati Uniti, Regno Unito, Australia, Nuova Zelanda, Germania, Francia, Italia e Spagna**, e rappresentano un ampio spaccato di organizzazioni, da PMI in erba, ad aziende quotate pubblicamente e con più di 10.000 dipendenti, in una vasta gamma di settori, tra cui finanza, governo ed energia.

Il panorama globale delle minacce è in costante evoluzione.

Scopri come restare sempre un passo avanti