

CyberSec

La BU Cybersecurity di SMI

PERCHÉ CYBERSEC

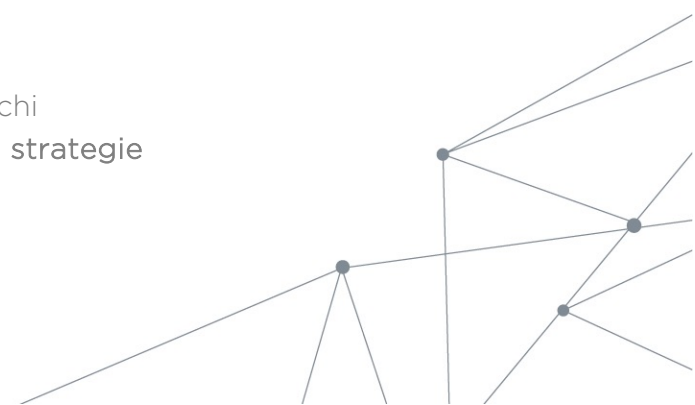
Ogni azienda, sia pubblica che privata, è costantemente minacciata da crimini informatici e atti di terrorismo cibernetico.

Dalla creazione di siti per il **phishing**, furto di **dati** e **identità personali**, all'introduzione di **virus** e **malware** nei sistemi aziendali.

Le conseguenze di tali attacchi possono essere estremamente gravi come:

- **Perdita di informazioni** critiche
- **Interruzione** dei processi di **business**
- **Danni** significativi all'**immagine** dell'azienda
- **Danneggiamenti** alle **infrastrutture** nazionali e/o di sicurezza.

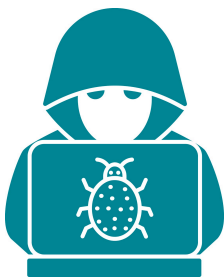
È ormai imprescindibile che le organizzazioni comprendano i rischi che le minacce cyber comportano e concentrarsi sull'**adozione** di **strategie** volte alla **riduzione** del loro **impatto**.



DATI CERTI - NON IPOTESI

ALCUNE PERCENTUALI RELATIVE AGLI ATTACCHI CYBER

- L' 82% delle applicazioni presentano **vulnerabilità**.
 - Il 75% di tutti gli attacchi rilevati su internet sono rivolti contro le **piattaforme applicative**.
 - L' 85% delle intrusioni viene **scoperto solo dopo diverse settimane**.
 - 116 **giorni** è il **tempo medio** per la risoluzione delle vulnerabilità.
 - Il **98%** dei **dati violati** provengono da **database**.
 - Il **99%** delle **intrusioni** porta alla compromissione di uno o più sistemi entro **poche ore o giorni**.
- Nello stesso intervallo di tempo si verifica spesso perdita di dati.



FONTE:
[WHITEHAT WEBSITE SECURITY STATISTICS REPORT,](#)
WINTER 2011 VERIZON 2012 DATA BREACH INVESTIGATIONS REPORT
EMA, THE RISE OF DATA-DRIVEN SECURITY, CRAWFORD, AUG 2012

BU CyberSec

AREE DI OFFERTA

OFFENSIVE SECURITY

- VA/PT Team

DEFENSIVE SECURITY

- SOC Governance, Monitoring e Management - Partner Team
- WAF
- SECDEVOPS

GRC (governance risk compliance)

- GRPR & ISO27001

