ENGINEERING
INFOGRAPHICS

La sfida della cyber resilience nei settori strategici

Gestire la sicurezza digitale oggi non è solo una questione di conformità: significa costruire fiducia, garantire continuità operativa e accelerare la competitività.

La **direttiva NIS2** introduce un nuovo livello di responsabilità per le imprese: dal **retail** al **manifatturiero**, al **pharma**, ogni settore strategico deve mettere al primo posto la **sicurezza informatica**, per garantire beni e servizi essenziali e la tenuta economica del comparto. La **cyber resilience** non è un aspetto tecnico ma, per la sua rilevanza, è una questione di **governance strategica** che impone al management un ruolo diretto, una gestione strutturata dei rischi, il monitoraggio della supply chain e l'obbligo di segnalare tempestivamente gli incidenti entro 24 ore.

Key Insights

worldwide ransomware

63%

2025: manifatturiero il più esposto, business continuity decisiva

NIS2 rende strategici software sicuro e cyber resilience per ridurre i fermi e proteggere la fiducia dei mercati.

cybercrime globale

10,29 trilioni

di dollari nel 2025: Europa tra i principali target

Con NIS2, le aziende diffondono competenze, aumentano la consapevolezza dei rischi, rafforzano la resilienza e prevengono incidenti.

+183 mila aziende

colpite da cyberattacchi alla supply chain nel 2024

NIS2 rafforza la sicurezza della supply chain con analisi dei rischi e mitigazione delle vulnerabilità.

SOURCE: STATISTA

Una security posture solida richiede processi, strumenti, governance e capacità di risposta.

In settori come il **manifatturiero**, significa rafforzare IT/OT e processi digitali, mentre per il **pharma** adottare un approccio multirischio e garantire conformità.

Ruoli e responsabilità

Definire chiaramente compiti e responsabilità del management e dei team di sicurezza, garantendo governance, accountability e capacità di risposta agli incidenti.

Gestione dati e servizi

Proteggere dati e servizi digitali adottando misure tecnologiche e organizzative adeguate, con controlli costanti e procedure di monitoraggio per garantirne riservatezza, integrità e disponibilità.

Gestione fornitori

Valutare e monitorare costantemente i fornitori lungo la supply chain, con particolare attenzione al settore farmaceutico, dove la sicurezza è critica per la tutela di processi e conformità normativa.

Our Approach

Adottiamo un approccio olistico alla sicurezza IT, offrendo **servizi di cybersecurity integrati e multilivello** per proteggere organizzazioni dagli attacchi informatici.

Con un portfolio modulare e in continua evoluzione di **soluzioni best-of-breed**, contribuiamo alla protezione degli information asset lungo l'intero stack tecnologico, garantendo una postura resiliente capace di salvaguardare infrastrutture, dati e applicazioni business critical.

- **Gap assessment** per definire priorità e modello di governance
- **SGSI e soluzioni integrate** per proteggere asset e processi
- **Consulenza** per audit, controllo dei fornitori e rispetto delle normative internazionali
- **Percorsi formativi** per rafforzare cultura della sicurezza e responsabilità

Our Partnership

pikered

Con **Pikered**, parte del nostro ecosistema di partners, offriamo il **Breach Attack Simulation (BAS)** che, integrato al nostro Red Teaming, permette di testare attacchi mirati e monitorare le difese IT, garantendo una visione completa della sicurezza.

Dal rischio alla resilienza: preparati con BAS

- Simula attacchi reali e verifica in modo continuo l'efficacia delle tue difese IT
- Individua le vulnerabilità per proteggere il tuo business
- Rafforza la continuità operativa