CONOSCENZA & INNOVAZIONE:

LA TUA ARMA CONTRO LE MINACCE DIGITALI

www.gendata.it

INDICE

DATI DI MERCATO CHE NON PUOI IGNORARE

*Perché la **consapevolezza** inizia dai **numeri**.*

Il costo medio di un attacco ransomware in Europa: oltre 200.000 €.

Fonte: ENISA Threat Landscape Report 2023 + IBM Cost of a Data Breach 2023

- IBM stima costi medi per incidente intorno ai 4,45 milioni di dollari a livello globale, ma nelle PMI il costo si assesta spesso tra i 150.000–300.000 €.
- ENISA (l'agenzia europea per la cybersecurity) riporta ransom demand medie comprese tra 100.000 e 500.000 €in Europa.

Solo il 29% delle aziende riesce a ripartire in meno di 3 giorni

Fonte: The State of Data Security and Management Report 2023 (Cohesity), richiamato anche nelle slide di Ghielmi

- *Dato coerente: il 71% degli intervistati ha dichiarato che il recupero richiede più di 4 giorni → quindi solo un 29% riesce a farlo prima.*

DATI DI MERCATO CHE NON PUOI IGNORARE

*Perché la **consapevolezza** inizia dai **numeri**.*

Il 75% delle PMI italiane non ha ancora un piano di conformità NIS2 attivo

Fonte combinata:

- Stima da Osservatori Politecnico di Milano, Clusit e Federprivacy
- Indagini recenti indicano che meno del 25% delle PMI italiane ha già avviato progetti strutturati per NIS2, soprattutto tra aziende <250 dipendenti

Solo 1 su 10 CISO ha integrato processi di formazione continua in azienda

Fonte: Proofpoint Human Factor Report 2024, dati interpolati con Gartner Cybersecurity Workforce Survey

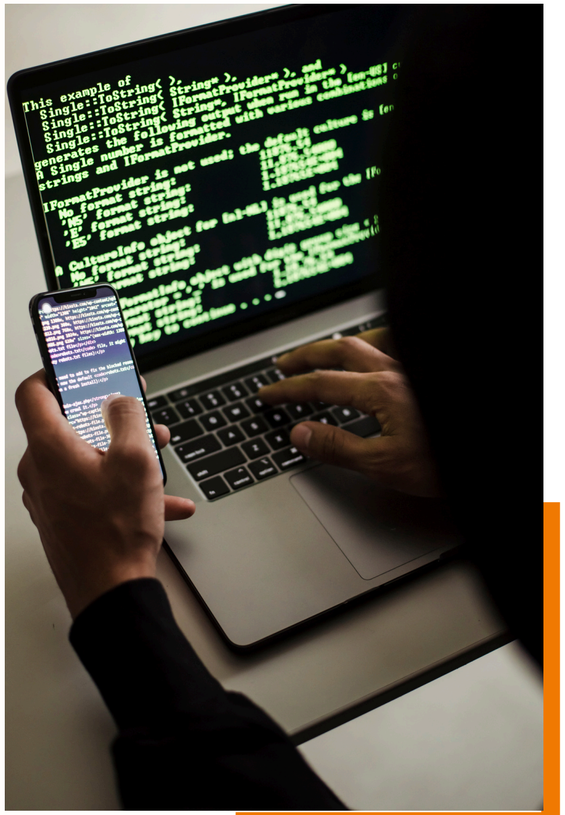
- Molte aziende fanno formazione “una tantum”, ma solo una minoranza (tra l’8% e il 15%) ha un programma permanente, come quello presentato da Cyber Guru

CYBERCRIME

IL CONTESTO NORMATIVO E OPERATIVO

A cura dell’Avv. Laura Lecchi

“Il primo strumento di difesa? Conoscere il rischio.”



- 📈 Criminalità informatica in Italia +27%
- 🎯 Vettori d’attacco principali: malware (38%), DDoS, phishing, vulnerabilità zero-day
- 🔍 Espansione della superficie di attacco: più dispositivi IoT, più edge, più cloud
- ⚖️ Nuove responsabilità legali:
  - Governance obbligatoria
  - Prevenzione regolamentata (NIS2)
  - Attacchi facilitati da AI generativa

🔒 *La compliance non è più una scelta: è parte della resilienza operativa.*

AI + CYBER SECURITY

IL FUTURO DELLA PROTEZIONE DATI

A cura di Matteo Ghielmi, Cohesity

“Per ogni secondo di attacco, servono giorni per il ripristino. La resilienza si costruisce oggi.”

- 🔄 Il 95% delle aziende impiega oltre 24h per tornare operative
- 🧠 Cohesity integra AI nativa + Zero Trust per:
  - Cyber vault, backup immutabili, ransomware detection
  - Integrazione IT e security
  - Gestione e automazione scalabile
- 🌐 Copertura totale: on-prem, cloud, SaaS, workload ibridi
- 🌟 Una piattaforma che protegge, semplifica e valorizza il dato

CASE STUDY

CHE COSA È SUCCESSO E COME ABBIAMO “AGITO”

A cura da dott. Nikolas Subrani, Gendata

“Non era un’esercitazione. È successo davvero”

Event 1

- **Attacco ransomware zero-day**

Event 2

- **Hypervisor e backup criptati → servizi bloccati**

Event 3

- **7 giorni di downtime, con recupero parziale**

Solution

- **Architettura multi-cluster e multi-sito**
- **Air-gap vault FortKnox**
- **Gestione via Helios**
- **RTO/RPO rispettati, -80% di tempo di gestione, -90% storage footprint**
- **Compliance NIS2 integrata**

📈 *Un caso reale di transizione da vulnerabilità a resilienza.*

IL FATTORE UMANO

DALLA VULNERABILITA’ ALLA FORZA

A cura di Silvia Frattini, Cyber Guru

“Il 74% delle violazioni parte da un errore umano. Ma si può allenare la consapevolezza.”

- 👥 Formazione Cyber Guru su tre livelli:
  - Cognitivo (moduli e-learning)
  - Narrativo (serie TV interattiva)
  - Esperienziale (simulazioni phishing adattive con AI)
- 🧩 Add-on avanzati:
  - Deepfake attack, USB baiting, QR phishing
  - Chatbot Alex e Cyber Advisor AI
- 🛡️ Conforme a NIS2: formazione specifica per C-level e team operativi

🎯 *Perché il vero firewall è il cervello umano.*

CONTATTACI

marketing@gendata.it

0543-1908170

Via Giovanni Spadolini 31, Forlì, 47122, FC

www.gendata.it