Ambito di applicazione del Decreto n. 138/2024 1/2

Tre criteri definiscono quali organizzazioni devono conformarsi alla Direttiva NIS 2 e al Decreto NIS

Direttiva NIS2 – In estrema sintesi

- Rafforza la cybersecurity nell'UE ampliando i settori coinvolti e gli obblighi per enti pubblici e privati.
- **Impone** misure di gestione del rischio, sicurezza della supply chain e formazione del personale.
- Obbligo di notificare rapidamente gli incidenti significativi (entro 24/72 ore).
- Responsabilità diretta del top management e sanzioni fino a 10 M€ o 2% del fatturato.

CRITERIO GEOGRAFICO

L'organizzazione fornisce servizi o svolge attività in un paese UE

CRITERIO MERCEOLOGICO

Se l'organizzazione opera in uno dei 18 settori specificati nella Direttiva NIS 2 e nel Decreto NIS

CRITERIO DIMENSIONALE

Se l'organizzazione ha più di 50 dipendenti e un fatturato superiore a 10 milioni di euro

La NIS2 come "Dieta Forzata" per le Aziende

Tutti in questa stanza sappiamo che mangiare esclusivamente nei fast food distrugge la salute. Non serve una laurea in medicina per capirlo. Eppure, il settore del fast food fattura miliardi. Perché? Perché tra la conoscenza di un rischio e l'azione per evitarlo c'è di mezzo la natura umana.

Una dieta **fallisce** se il paziente mangia insalata solo quando il medico lo guarda.

Allo stesso modo, la **NIS2** fallisce se l'ingegnere applica le patch solo per evitare la multa. La regola serve a creare il perimetro, ma è la cultura che ci permette di viverci dentro.

Il Fattore Umano vs Tecnica

Secondo voi è più probabile che un'azienda venga bucata perché un hacker ha 'inventato' un attacco geniale mai visto prima (Zero-Day) o perché qualcuno ha lasciato una password di default o non ha patchato un server per mesi?"

Report di fine 2025*

- *Fattore umano*: **60%**
- *Sfruttamento vulnerabilità Sw*: cresciuto del **34%** rispetto lo scorso anno
- *Ransomware*: **44%** ma il **64%** non ha pagato
- *Terze parti*: coinvolgimento raddoppiato da **15%** del 2024 al **30%** del 2025

Fattore Umano

- Circa il 60% delle violazioni include ancora un errore umano (non solo cadere nel phishing, ma anche errori di configurazione o smarrimento di credenziali).

Vulnerabilità:

- Lo sfruttamento delle vulnerabilità software è cresciuto del 34% rispetto all'anno scorso. In particolare, i dispositivi "edge" (VPN, router, firewall stessi) sono diventati i bersagli preferiti

Ransomware

- Il ransomware è presente nel 44% delle violazioni, ma la notizia vera è che il 64% delle aziende vittime ha rifiutato di pagare il riscatto.

Supply Chain

- Il coinvolgimento di fornitori o partner esterni nelle violazioni è raddoppiato, passando dal 15% al 30%.

* Fonte Verizon (link)

Cosa fa Sinelec per aumentare la sicurezza

Migliorare la postura di sicurezza di un'azienda non è un progetto con una data di inizio e una fine, ma un **percorso di maturazione continua.**

Formazione:

- Tecnici
- Operatori di esercizio
- Management

Vulnerability Assessment:

- analisi continua delle vulnerabilità,
- non per puntare il dito ma per migliorare.

Security Operation Center (SOC):

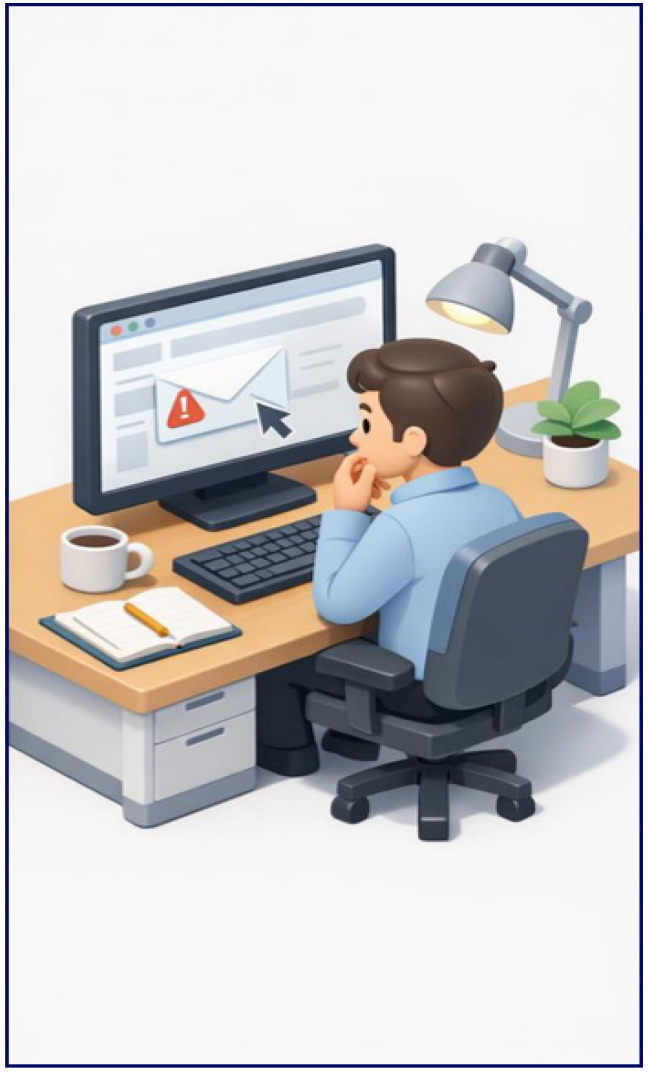
- monitoraggio continuo,
- analisi di eventi e log,
- correlazione e risposta agli incidenti.

Non esistono sistemi sicuri al 100%, esistono sistemi controllati

Nel mese di Marzo il monitoraggio ha rilevato 1.287 attività sospette di cui il 60% riconosciuto come «falso positivo» il restante 40% ha la seguente incidenza:

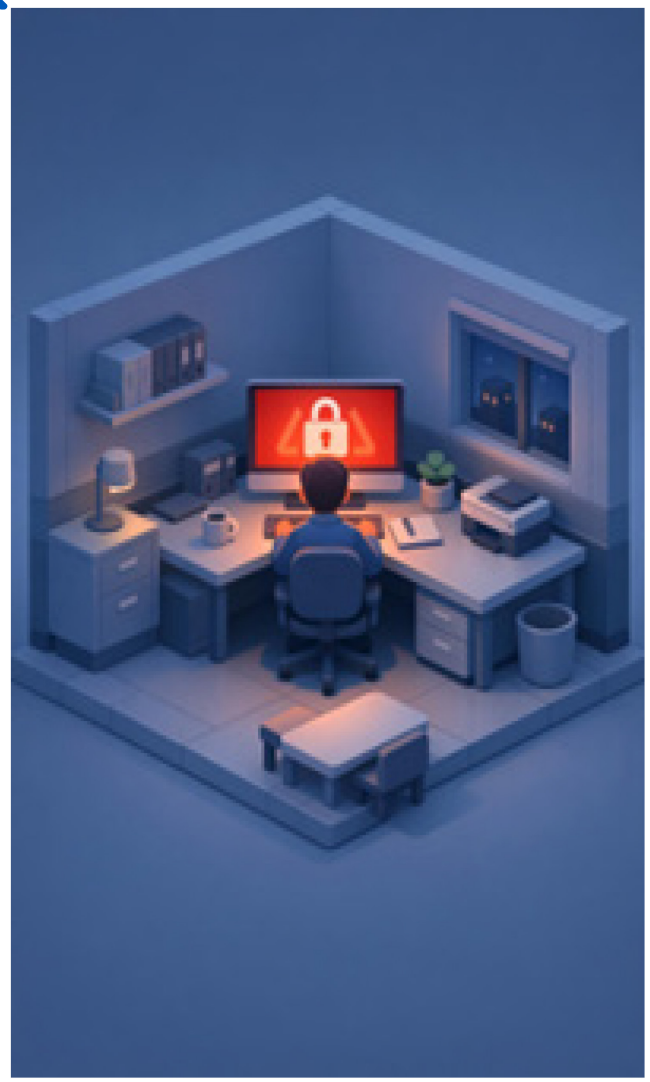
[redacted]

E adesso? I primi 5 minuti di una crisi cyber



Siete il CTO di una startup.

Ricevete un'email di riscatto alle 3 del mattino.

Cosa fate nei primi 5 minuti?

La tecnologia non risolve tutto serve **affidarsi al processo**. "*la sicurezza è un processo, non un prodotto*" [cit. Bruce Schneier]