elmec

NIS2 | DA OBBLIGO A VANTAGGIO

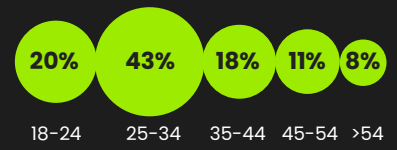
Proteggere il business

Il nostro manifesto

- BUONGIORNO!
- FIRMA
- FORMAZIONE
- SEMPLICEMENTE AFFIDABILI

1006
Dipendenti

- **733** tecnici
- **34** anni di età



1.836
certificazioni

- **312** conseguite nel ‘25

215M €
Fatturato complessivo

- **65,5%** servizi ricorrenti
- **98,7M €** investimenti /3Y

+50
Anni di storia

+1.700
Clienti attivi

100%
Proprietà italiana

28.405
Ore di formazione

- **86%** tecnica
- **14%** altro

I nostri servizi

		PRODUTTIVITÀ	RISPARMIO	PROTEZIONE
SERVIZI UTENTI	Supporto utenti	$$	-	1
	DaaS	$$	1	-
	Sicurezza informatica	-	-	3
SERVIZI DATA CENTER	Gestione Data Center	-	1	2
	Gestione Cloud	-	1	2
	Sicurezza informatica	-	-	3
	Connettività	$$	1	-
RIVENDITA	Tecnologia	$	2	-
	Licenze software	-	3	-
	Apple	$$	1	-
	Ricondizionato	$	3	-
	Fotovoltaico	$$	2	-

IL PERCHÉ CONVIENE

Avete sentito cos’è l’obbligo.
Vi mostro perché conviene.

Tre attacchi reali gestiti dal nostro team. Stesso ingresso, esiti molto diversi.

1 ogni 21,5 sec
un tentativo di attacco bloccato: 678 milioni nel 2025.

1 account su 4
ha la password senza scadenza; il 6% è già sul dark web.

Fonte: Data Gathering CybergON 2026 (dati 2025 sui sistemi monitorati)

CASO 1 — AZIENDA DI DISTRIBUZIONE, PIÙ SEDI

L’errore che si poteva evitare

IL PERCORSO DELL’ATTACCO

1. INGRESSO
Un vecchio account del firewall, mai dismesso e senza secondo fattore, usato con credenziali rubate.

2. MOVIMENTO INTERNO
Furto delle credenziali di dominio e diffusione sui server, senza log centralizzati a dare l’allarme.

3. IMPATTO
Cifratura dei dati e richiesta di riscatto, con minaccia di pubblicazione.

COSA AVREBBE RICHIESTO LA NIS2

Autenticazione a più fattori e controllo degli accessi (art. 24)
Registrazione e analisi dei log (art. 24)

COM’È ANDATA

Nessun riscatto pagato, produzione mai ferma, sistemi ripristinati in giornata.

CASO 2 — GRUPPO INDUSTRIALE MULTINAZIONALE

Il colpo che non si poteva prevedere

IL PERCORSO DELL'ATTACCO

1. INGRESSO
Una falla del firewall ancora senza correzione: nessuna patch disponibile, nessuna disattenzione.

2. MOVIMENTO INTERNO
Per giorni l'attaccante si sposta tra i server, fino all'ambiente di virtualizzazione.

3. FERMATO QUI
Il rilevamento gestito 24/7 individua l'intrusione e la risposta la blocca prima della cifratura.

IL PRESIDIO CHE HA FATTO LA DIFFERENZA

Gestione e trattamento degli incidenti (art. 24)
Non puoi prevenire una falla sconosciuta. Puoi accorgertene e fermarla.

COM'È ANDATA

Un solo server isolato per poche ore, invece del blocco totale dell'infrastruttura.

CASO 3 — GRUPPO ALIMENTARE

Quando mancano le fondamenta

IL PERCORSO DELL'ATTACCO

1. INGRESSO
Un accesso VPN senza secondo fattore, già forzato un mese prima e rimasto aperto.

2. MOVIMENTO INTERNO
Vulnerabilità note e non aggiornate sul sistema di backup, usato dall'attaccante come arma.

3. IMPATTO
Dati esfiltrati e poi pubblicati sul dark web.

I PRESIDI NIS2 CHE MANCAVANO

Autenticazione a più fattori (art. 24)
Gestione vulnerabilità e backup sicuro (art. 24)

COM'È ANDATA

Stesso ingresso degli altri due. Senza le fondamenta, il danno si è compiuto.

IL FILO ROSSO

Stesso ingresso. Stesso furto. Esiti diversi.
La differenza? I presidi. Che hanno un nome: NIS2.

Autenticazione forte art. 24
MFA e gestione degli accessi: mancavano in tutti e tre i casi.

Rilevamento e risposta art. 24
Dove c'era, l'attacco è stato visto e fermato in tempo.

Vulnerabilità e backup art. 24
Patch e backup protetti: la differenza tra ripartire e finire sul dark web.

La NIS2 non è un adempimento burocratico.

È l'elenco delle fondamenta che separano la continuità dal blocco. Investirci significa più resilienza, più fiducia di clienti e fornitori, e una posizione migliore anche di fronte all'assicurazione.

3,31 milioni di € — il costo medio di una violazione dei dati in Italia. Fonte: IBM Cost of a Data Breach Report 2025

DALL'OBBLIGO ALLA PRATICA

I requisiti NIS2, piano operativo

FONDAMENTA

Continuità, dati e infrastruttura

- **Managed Infrastructure**
- **Secure Backup**
- **Business Continuity & Disaster Recovery**
- **Data Center e IaaS**
- **Gestione asset e device (DaaS, UEM)**
- **Identity & Access Management**

DIFESA

Rilevare, rispondere, prevenire

- **SOC 24/7 e XDR/SIEM**
- **Incident Response**
- **Vulnerability & AD Audit, Pen Test**
- **Mail & Network Security, Awareness**

GOVERNANCE

Vedere e dimostrare

MyElmec

Un'unica dashboard: stato sicurezza, vulnerabilità, alert del SOC, patch e asset.

- **Referente CSIRT esterno** (art. 25)
- **Assessment & Gap Analisi**

Non un progetto da avviare da zero:
dare valore a quanto già implementato e prevedere un piano di miglioramento.

IN SINTESI

La sicurezza non è un costo da subire.
È un vantaggio competitivo da scegliere.

GRAZIE

A PRESTO

www.elmec.com

Headquarter:
via Pret, 1 – 21020 Brunello (VA)

Vieni a trovarci! Prenota uno Study Tour.

+39 0332 802 111

elmec@elmec.it

L'impatto ambientale per noi è importante.

Per questo abbiamo scelto lo sfondo nero.

Consumo energetico di una presentazione su laptop (1 ora):

- Sfondo chiaro: **~10–30 Wh***
- Sfondo scuro: **~5–20 Wh***

Risparmio energetico stimato: ~5–15 Wh

* Valori indicativi basati su misurazioni generiche su diversi dispositive.