PENTESTERRA

NIS2 CYBER GAP ASSESSMENT

NIS2 non è più un problema del prossimo trimestre

Una valutazione tecnica della cybersicurezza e dello stato di conformità della tua organizzazione rispetto alle misure dell'Articolo 21(2) di NIS2 - basata su evidenza reale, non su un'autovalutazione ottimistica.

COS'È NIS2, IN BREVE

NIS2 è la direttiva europea sulla cybersicurezza: fissa requisiti minimi di sicurezza informatica (cyber) per migliaia di aziende in tutta l'UE, nei settori critici e nella loro catena di fornitura. Che tu ci pensi oggi o tra un anno, prima o poi la tua azienda dovrà comunque adeguarsi - per legge, con o senza sanzioni.

€10M / 2%

Sanzione massima per i soggetti essenziali: 10 milioni di euro o il 2% del fatturato globale, il valore più alto

D.lgs. 138/2024

Il decreto italiano di recepimento NIS2, già in vigore

Già attive

Le prime sanzioni NIS2 sono già state comminate in UE

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO, l'IT manager o il responsabile compliance di un'azienda di medie o grandi dimensioni che rientra nel perimetro di NIS2 - per la prima volta, o senza che nessuno ne sia del tutto certo: energia, trasporti, sanità, infrastrutture digitali, manifatturiero, o fornitore critico di uno di questi settori.

COSA È SUCCESSO

Il recepimento italiano di NIS2 (**D.lgs. 4 settembre 2024, n. 138**) è già in vigore, l'ACN ha pubblicato le **Linee guida NIS - specifiche di base**, e in altri Stati membri le prime sanzioni sono già state comminate. Un cliente, un partner o un ente regolatore potrebbe chiederti domani una prova di conformità - e oggi non sai con certezza cosa mostrare.

IL PROBLEMA

Non sai, controllo per controllo, a quali misure di cybersicurezza dell'Articolo 21(2) la tua organizzazione risponde davvero oggi. Le informazioni esistono, ma sono sparse tra scansioni di sicurezza, test di penetrazione fatti mesi fa, e la memoria di chi in azienda "se ne occupa" di cyber.

PERCHÉ FA MALE

Sanzioni fino a 10 milioni di euro o il 2% del fatturato globale per i soggetti essenziali (7 milioni di euro o l'1,4% per i soggetti importanti), possibili ispezioni ACN, un contratto che rischia di saltare perché un cliente chiede evidenza di conformità e tu hai solo una checklist compilata a mano - e nessuna prova concreta da mostrare quando conta davvero.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, controllo per controllo, cosa è soddisfatto, cosa è parziale e cosa manca - con un'evidenza tecnica reale allegata a ogni risposta, non una dichiarazione ottimistica che nessuno ha verificato.

LA SOLUZIONE

Il **NIS2 Technical Gap Assessment & Report** di Pentesterra: una valutazione strutturata su tutte le misure dell'Art. 21(2)(a)-(j), con verifica di applicabilità guidata per settore, paese e dimensione aziendale, e compilazione automatica dei controlli tecnici a partire da scansioni di vulnerabilità, penetration test, OSINT e monitoraggio dell'esposizione esterna.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo questionario di autovalutazione, e non stiamo parlando di un parere legale. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. Molti dei tuoi concorrenti diretti si stanno già rivolgendo a noi. E il gap assessment non si ferma a una checklist cartacea: dove possibile, i controlli tecnici vengono auto-compilati dall'evidenza già raccolta da vulnerability scanning, penetration test, OSINT ed External Exposure Assessment - con mappatura automatica anche verso ISO 27001, DORA, GDPR, SOC 2 e NIST CSF, cross-standard, così un secondo audit non riparte da zero.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con copertura di tutte le misure dell'Art. 21(2)(a)-(j) e riferimento diretto alla base giuridica italiana (D.lgs. 138/2024, ACN Determinazione 379907/2025 e le Linee guida NIS - specifiche di base). Se emergono gap, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test di rete, formazione e simulazioni di phishing.

13

Framework supportati sulla stessa base di evidenza: NIS2, GDPR, ISO 27001, DORA e altri

5

Fonti di evidenza automatica: scansioni, pentest, OSINT, External Exposure, DevGuard

1 click

Pacchetto completo per l'auditor: questionario, evidenza, gap report

COSA RICEVI

- ✓ Un punteggio di readiness indicativo, con il conteggio dei controlli soddisfatti, parziali e mancanti
- ✓ Un gap report prioritizzato - i controlli su cui un auditor si sofferma di più sono segnalati per primi
- ✓ Una matrice di controllo esportabile in XLSX
- ✓ Un report dei gap editabile in DOCX, pronto per il tuo consiglio o per il tuo auditor
- ✓ Un pacchetto completo per l'auditor in un click: questionario, evidenza tecnica e gap report insieme

COME FUNZIONA

1

Verifichiamo l'applicabilità

Settore, paese, dimensione aziendale - ti diciamo subito se e come NIS2 si applica a te.

2

Raccogliamo l'evidenza

I controlli tecnici vengono verificati con prova allegata, senza che tu debba fare nulla.

3

Completiamo insieme il resto

Ti guidiamo nelle poche domande organizzative che restano da rispondere.

4

Ti consegniamo il report

Un PDF completo con i gap prioritizzati, pronto per l'auditor o per il tuo consiglio.

Scopri dove si trova davvero la tua organizzazione rispetto a NIS2

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi la tua valutazione NIS2 →

info@pentesterra.com · pentesterra.com/solutions/compliance