LA TUA AZIENDA E' PRONTA PER NIS2?

Estensione del perimetro

La direttiva NIS2 estende gli obblighi di cybersecurity a un numero molto più ampio di organizzazioni, incluse molte imprese della filiera digitale e industriale.
Molte aziende potrebbero rientrare nel perimetro senza esserne consapevoli.
Questa checklist ti aiuta a verificare se la tua organizzazione è pronta.

Non solo tecnologia: serve una governance strutturata

La NIS2 non riguarda solo aspetti tecnici di sicurezza IT.
Richiede infatti procedure organizzative, gestione del rischio, policy interne e responsabilità chiare a livello aziendale.
Una corretta impostazione della compliance consente di ridurre il rischio di sanzioni e rafforzare la resilienza dell'organizzazione.

Una checklist per guidare la roadmap

La checklist è consultabile a partire dalla pagina seguente

NIS2

Come usare questa checklist

La checklist non sostituisce una valutazione completa di compliance NIS2. Serve per verificare rapidamente se nella tua organizzazione sono già presenti alcune delle principali misure richieste dalla normativa.

Hai identificato formalmente quali sistemi informativi e di rete sono "rilevanti"?

Occorre identificare i sistemi che sorreggono i servizi per cui il soggetto rientra nel perimetro NIS2.

La tua valutazione del rischio include non solo i cyber-attacchi, ma anche minacce fisiche, ambientali e della supply chain?

Le minacce da identificare non sono solo informatiche ma anche fisiche, ambientali e della catena di fornitura.

Hai mappato le dipendenze da partner esterni (manutentori IT, fornitori di connettività o cloud) che accedono ai tuoi sistemi critici?

L'accesso ai sistemi da parte di partner esterni rappresenta un rischio della supply chain che va mappato e gestito.

I permessi degli utenti sono limitati a quanto strettamente necessario per la mansione svolta e le funzioni sono separate per evitare conflitti d'interesse?

Occorre applicare il principio del minimo privilegio: ogni utente deve avere accesso solo alle risorse e funzioni necessarie per il proprio ruolo.

CeFor SEAC
cefor.formazione@seac.it
https://www.cefor-formazione.it

NIS2
Checklist

È implementata l'autenticazione a più fattori (MFA) per tutti gli accessi da remoto e per le utenze con privilegi elevati?

L'MFA è un sistema di sicurezza fondamentale per impedire accessi non autorizzati dall'esterno.

I dati sensibili sono cifrati sia quando memorizzati su dispositivi portatili (laptop, smartphone) sia durante la trasmissione verso l'esterno?

I dispositivi portatili possono essere smarriti o rubati: per questo motivo la cifratura dei dati rappresenta una protezione essenziale, analoga alle misure di sicurezza fisica utilizzate per le infrastrutture critiche centrali.

I locali che ospitano i server o gli apparati di rete rilevanti sono protetti da accessi fisici non autorizzati (badge, videosorveglianza)?

La protezione fisica degli spazi server è parte integrante della sicurezza NIS2, al pari delle misure informatiche.

Esiste un processo per disabilitare l'auto-esecuzione dei supporti rimovibili (USB) e per garantire aggiornamenti di sicurezza regolari?

È importante verificare e gestire i supporti rimovibili prima che possano introdurre dati nei sistemi aziendali. Parallelamente, l'aggiornamento costante di software e sistemi rappresenta una ulteriore misura fondamentale per prevenire vulnerabilità e incidenti di sicurezza.

CeFor SEAC
cefor.formazione@seac.it
https://www.cefor-formazione.it

NIS2
Checklist

Esiste un processo in grado di rilevare tempestivamente un accesso anomalo o un incidente di sicurezza sui sistemi critici?

I sistemi più critici per l'organizzazione devono essere costantemente monitorati per individuare accessi anomali o incidenti informatici. Il monitoraggio continuo e l'analisi dei log di sicurezza sono tra le misure richieste dalla direttiva NIS2.

In caso di incidente grave (ransomware o guasto ambientale), esiste un piano documentato e testato per ripristinare i servizi critici in tempi certi?

Occorre essere dotati di un piano per ripristinare l'operatività con tempistiche che non incidano significativamente sui servizi critici.

Come interpretare i risultati

Hai risposto "SÌ" a meno di 5 domande

- La tua organizzazione potrebbe non essere pronta ai requisiti NIS2.

Hai risposto "SÌ" a un numero di domande tra 5 e 8

- Alcuni aspetti di sicurezza sono presenti, ma potrebbero essere necessari interventi di adeguamento.

Hai risposto "SÌ" a tutte le domande

- Hai già implementato molte delle misure richieste dalla normativa!

CeFor SEAC
cefor.formazione@seac.it
https://www.cefor-formazione.it

Hai completato la checklist. E ora? Scopri il corso

NIS2: obblighi, sicurezza e compliance

Il corso analizza gli obblighi NIS2 per soggetti essenziali e importanti, le misure tecniche e organizzative richieste e la gestione degli incidenti.
Un percorso pratico per comprendere gli obblighi NIS2 e impostare correttamente il percorso di adeguamento per il **raggiungimento della compliance**

Vuoi capire davvero cosa richiede la NIS2?

Nel corso analizzeremo:

- I settori che rientrano nel perimetro della NIS 2
- Il Dlgs 138/2024: la consapevolezza dell'Organo di vertice in materia di cybersecurity;
- Le misure di sicurezza di base.

Iscriviti ora

SHOP.SEAC.IT

Visita lo shop Seac per scoprire il programma completo e le date disponibili.

CeFor SEAC

cefor.formazione@seac.it
www.cefor-formazione.it