CYBERFERO

NIS2

Network and Information Security

Analizziamo la tua realtà per valutare la conformità alla DIRETTIVA NIS2.

https://www.cyberfero.com

Direttiva NIS2, di cosa si tratta?

La Direttiva NIS2 va ad integrarsi con le varie normative e linee guida europee in tema di protezione dati e privacy: l'obiettivo è rafforzare le misure di cybersecurity soprattutto nei settori critici e gestire le complessità della catena di approvvigionamento, instaurando un framework normativo essenziale.

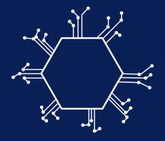
La nuova Direttiva NIS2 punta a migliorare la resilienza e le capacità di risposta agli incidenti informatici del settore pubblico e privato e si concentra, in particolare, sulla lotta alla criminalità informatica e sul miglioramento della gestione della sicurezza informatica a livello europeo e nazionale.

Le organizzazioni hanno tempo fino al 17 Ottobre 2024 per adeguarsi alla Normativa e non incorrere in sanzioni.

A chi si rivolge?

La Direttiva NIS2 si rivolge ad aziende, Istituzioni e amministrazioni appartenenti ai seguenti settori:


Mercati online


Infrastrutture digitali


Utilities


Macchine e Attrezzature


Settore bancario


Servizi postali e spedizioni


Infrastrutture mercato finanziario


Prodotti alimentari


Assistenza Sanitaria


Motori di ricerca online


Veicoli a motore


Gestione dei rifiuti


Computer ed elettornica


Trasporti


Prodotti chimici e medici


Servizi di cloud computing

La tua azienda non rientra nei settori sopra elencati?

Qualora la tua impresa operi in un ambito non esplicitamente elencato nell'elenco sopra indicato, è essenziale considerare attentamente anche la natura dei tuoi clienti. Alcuni di loro potrebbero essere soggetti a requisiti che richiedono la collaborazione con fornitori che aderiscono pienamente alle disposizioni della Direttiva NIS2.

Quali sono le sanzioni se non mi adeguo?

Gli Stati Membri possono imporre sanzioni pecuniarie ai soggetti che non sono conformi con la Direttiva.

Soggetti Essenziali

SANZIONI MASSIME A PARTIRE DA

***€10 MILIONI**

oppure

2% del fatturato mondiale annuo

*Il tetto sanzionatorio è elevabile arbitrariamente al momento del recepimento da parte del recepimento da parte del Governo.

Soggetti Importanti

SANZIONI MASSIME A PARTIRE DA

***€7 MILIONI**

oppure

1,4% del fatturato mondiale annuo

*Il tetto sanzionatorio è elevabile arbitrariamente al momento del recepimento da parte del recepimento da parte del Governo.

Cosa facciamo per la tua azienda?

Testiamo

Effettuiamo test mirati per verificare la conformità con la Direttiva NIS2, assicurando che la tua organizzazione rispetti gli standard richiesti. Utilizziamo metodologie avanzate per valutare la tua sicurezza informatica contro le minacce emergenti.

Analizziamo

Esaminiamo la tua infrastruttura di sicurezza per determinare l'adeguatezza ai requisiti della Direttiva NIS2. Attraverso un'analisi approfondita, identifichiamo vulnerabilità e rischi, fornendo un'immagine chiara della tua situazione attuale.

Indirizziamo

Identifichiamo e ti segnaliamo le carenze nella tua infrastruttura di sicurezza in relazione ai requisiti della Direttiva NIS2. Offriamo indicazioni precise su cosa migliorare per garantire la piena conformità normativa e rafforzare la tua difesa contro le minacce informatiche.

I principali obblighi per le aziende:

Gli adempimenti richiesti dalla Direttiva NIS2 riguardano i seguenti ambiti:

Gli organi di gestione devono approvare le misure per la gestione dei rischi adottate dall'Organizzazione, seguire un'adeguata formazione e garantire una formazione analoga ai propri dipendenti.

Gestione dei rischi:

I soggetti sono tenuti a adottare misure tecniche, operative e organizzative per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che i soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi.

Continuità operativa:

I soggetti devono garantire la continuità dei propri servizi e ridurre al minimo l'impatto di eventuali interruzioni attraverso misure quali la gestione del backup, il ripristino in caso di disastro e la gestione delle crisi.

Sicurezza della catena di approvvigionamento:

I soggetti sono chiamati a proteggere la propria catena di fornitura valutando le vulnerabilità specifiche dei propri fornitori e l'adeguatezza delle loro pratiche di cybersicurezza.

Segnalazione degli incidenti:

I soggetti sono obbligati a segnalare gli incidenti che abbiano un impatto significativo sulla fornitura dei propri serviziai rispettivi CSIRT o autorità nazionali competenti (preallarme entro 24 ore e notifica completa/integrativa entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo).

CYBERFERO

Da oltre 10 anni leader nel settore Cybersecurity e Sicurezza

CYBERFERO è un Managed Security Service Provider (MSSP) specializzato nella fornitura di soluzioni di sicurezza complete per aziende di tutte le dimensioni. In qualità di partner di fiducia, offriamo un'ampia gamma di servizi di sicurezza progettati per proteggere la tua organizzazione da minacce informatiche, violazioni dei dati e altri rischi per la sicurezza.

Visita il sito web

Contatti

+39 0522 1685330

https://www.cyberfero.com

info@cyberfero.com

Via Statuto 3, 42123 - Reggio nell'Emilia (RE)