Cyber Security
NIS2

innonation.it

innonation

La Direttiva NIS2

Un passo avanti per la sicurezza informatica in Europa

Il **17 ottobre 2024**, entra in vigore la Direttiva Europea NIS 2 sulla sicurezza delle reti e dei sistemi informativi *(Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni)*, che introduce nuovi requisiti di sicurezza informatica per aziende e organizzazioni operanti in settori specifici.

Nata dalla revisione della precedente Direttiva NIS (UE 2016/1148), attuata in Italia con D.lgs. n. 65 del 18 maggio 2018, la NIS2 segna un altro importante passo verso la definizione della strategia per la Cybersicurezza dell'Unione Europea, con l'obiettivo di colmare alcune carenze e coordinare le risposte degli Stati membri in caso di incidenti di sicurezza, garantendo la continuità dei servizi essenziali e importanti

innonation

Cosa Cambia? 1/3

Espansione dei settori industriali e delle entità che rientrano nel campo di applicazione della NIS2	La direttiva NIS originaria riguardava i cosiddetti operatori di servizi essenziali come l'approvvigionamento idrico, la sanità, i trasporti e alcuni fornitori di servizi digitali. La NIS2 è stata ampliata per includere settori come quello dei servizi postali e di corriere, alimentare, dello spazio e delle acque reflue, nonché numerose medie imprese con 50 o più dipendenti e utili superiori a 10 milioni di euro.
Responsabilità di gestione	Gli organi di gestione sono responsabili dell'approvazione delle misure di gestione dei rischi di sicurezza cyber adottate dalla propria impresa, presidiandone l'attuazione, e possono essere ritenuti responsabili in caso di violazione. I membri del management sono tenuti a svolgere attività di formazione in modo da acquisire conoscenze e competenze sufficienti per poter identificare i rischi e valutare le pratiche di gestione dei rischi di sicurezza cyber e le relative ripercussioni sui servizi.

innonation

Cosa Cambia? 2/3

Rafforzamento delle misure di gestione dei rischi di sicurezza cyber

Le organizzazioni devono adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi informatici e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi.
Esistono ora dei requisiti minimi che le organizzazioni che rientrano nel campo di applicazione della NIS2 devono implementare. Questi vanno dall'uso dell'autenticazione a più fattori alla gestione degli incidenti e alle politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di sicurezza cyber. Le misure di gestione dei rischi di sicurezza cyber adottate dall'organizzazione devono essere documentate e devono essere disponibili prove dell'attuazione delle politiche in materia di sicurezza cyber. In caso di incidente informatico, le organizzazioni devono rispettare tre fasi specifiche entro un periodo di tempo limitato:

- Entro 24 ore da un attacco informatico, deve essere inviato un primo avvertimento all'autorità responsabile del proprio Paese.
- Entro 72 ore devono essere fornite ulteriori informazioni sull'incidente.
- Entro un mese deve essere disponibile un rapporto finale dettagliato sull'incidente.

innonation

Cosa Cambia? 3/3

Sicurezza della catena di approvvigionamento	La gestione dei rischi di sicurezza cyber viene ampliata per includere la sicurezza della catena di approvvigionamento. Le organizzazioni che rientrano nel campo di applicazione della NIS2 devono considerare le vulnerabilità specifiche di ciascuno dei loro fornitori diretti e fornitori di servizi al fine di prevenire o ridurre al minimo l'impatto degli incidenti della catena di approvvigionamento sui destinatari dei loro servizi e su altri servizi.
Sanzioni più elevate	I soggetti "essenziali" non conformi alla direttiva NIS2 saranno passibili di sanzioni amministrative fino a 10 milioni di euro o al 2% del fatturato totale annuo mondiale (se superiore), mentre i soggetti "importanti" subiranno sanzioni fino a 7 milioni di euro o all'1,4% (se superiore).

innonation

I Destinatari

Organizzazioni e settori interessati dalla Direttiva NIS2

La Direttiva NIS2 riguarda tutte le organizzazioni che forniscono servizi identificati come essenziali o importanti per l'economia e la società europee. Se la tua organizzazione appartiene ad una delle categorie seguenti rientra nel campo di applicazione della NIS2.

Soggetti essenziali

Settore Bancario, Infrastrutture digitali (DNS, IXP, TLD, TIC), Energia, Infrastrutture dei mercati finanziari, Settore sanitario, Gestione dei servizi TIC, Pubblica Amministrazione, Spazio, Trasporti, Acqua potabile e acque reflue

Soggetti Importanti

Fornitori di Servizi Digitali, Fabbricazione, produzione e distribuzione di sostanze chimiche, Servizi postali e di corriere, Produzione, trasformazione e distribuzione di alimenti, Ricerca, Gestione dei rifiuti

innonation

Possiamo aiutarti

1. Misure di gestione dei rischi di sicurezza cyber

Ottimizzazione degli investimenti a budget limitato per aiutare la vostra organizzazione ad ottenere il massimo ritorno sugli investimenti in sicurezza

2. Igiene informatica di base

Valutazione della postura informatica e dell'igiene generale per contribuire a valutare e individuare i rischi e le lacune nei controlli di sicurezza

3. Autenticazione a più fattori o continua (MFA)

Fornire supporto strategico per la selezione, l'adozione e l'implementazione di soluzioni di autenticazione a più fattori appropriate

4. Politiche e procedure in materia di crittografia

Sviluppare modelli specifici per la creazione e il lancio di specifici moduli di formazione sulla consapevolezza degli utenti

5. Sicurezza della catena di approvvigionamento

Allineare il rischio informatico nella catena di approvvigionamento e sviluppare un approccio aziendale per analizzare e migliorare la resilienza

6. Gestione degli incidenti informatici

Analizzare la preparazione alla risposta agli incidenti e lo sviluppo di protocolli completi di risposta agli incidenti

7. Segnalazione degli incidenti informatici

Valutare le capacità e la reattività di segnalazione degli incidenti dell'impresa e progettare o adeguare le procedure esistenti di segnalazione degli incidenti per garantire l'allineamento con i nuovi requisiti normativi

8. Security in network and information systems

Ricercare sistematicamente le minacce generiche e mirate all'interno della rete e monitorare il deep e dark web per individuare minacce e risorse trapelate

innonation

Chi Siamo

Valore

Mettiamo a disposizione la nostra competenza per la progettazione, realizzazione e promozione di progetti innovativi nel settore ICT.

Conoscenza

Proviamo la cultura del trasferimento tecnologico, dell'innovazione e dell'integrazione tra università, enti di ricerca, enti pubblici e privati.

Innovazione

Offriamo servizi innovativi e tecnologicamente avanzati, grazie all'attenzione costante alla ricerca e allo sviluppo.

Cultura

Favoriamo la diffusione di modelli gestionali innovativi in grado di creare reti e sistemi integrati per la ricerca e l'innovazione.

Innovate *our nation*

La nostra crescita dipende dall' ***avanguardia della soluzione***. Ecco perché il Dipartimento di Ricerca & Sviluppo è il cuore pulsante di Innonation: perché i servizi e i prodotti che offriamo sono costruiti sulle ***esigenze del cliente***.

La nostra azienda unisce i migliori talenti del settore ICT con lo scopo di utilizzare l' ***innovazione digitale*** per ridisegnare i modelli che governano il business e ***contribuire al miglioramento della vita delle persone***.

innonation

Certificazioni

ISO 9001:2015

Processi di Qualità

Data ultimo audit: **05/04/2024**

ISO/IEC 20000-1:2018

IT Service Management

Data ultimo audit: **05/04/2024**

UNI PdR 125:2022

Parità di Genere

Data ultimo audit: **31/01/2024**

CSA STAR LEVEL ONE

SPID RAO PUBBLICO

Data ultimo audit: **11/11/2023**

CSA STAR Registry

ISO/IEC 27001:2022

Sicurezza delle Informazioni

Data ultimo audit: **05/04/2024**

ISO/IEC 27017:2015

Sicurezza per i Servizi Cloud

Data ultimo audit: **05/04/2024**

ISO/IEC 27018:2019

Protezione dei Dati Personali

Data ultimo audit: **05/04/2024**

ISO/IEC 17025:2017

Laboratorio di Prova

Data ultimo audit: **19/06/2024**

innonation

Contattaci

La tua azienda è al livello giusto per la NIS2?

Hai tempo fino al 17 ottobre 2024 per implementare le misure di sicurezza informatica richieste e garantire la piena conformità alla Direttiva NIS2.

Prenota ora una chiamata con i nostri specialisti per una consulenza personalizzata. | https://innonation.it

innonation

Connect with us

Potrai contattarci in qualsiasi momento per ricevere informazioni sul mondo Innonation.

Contattaci

innonation