M2 INFORMATICA

Essere al passo con la Direttiva NIS2: Cosa devono sapere le imprese

www.m2informatica.it

Premessa

Affrontare le sfide derivanti da un panorama normativo e tecnologico sempre più complesso, insieme alle minacce in costante evoluzione, richiederà un impegno sistemico da parte delle organizzazioni per elevare il livello di sicurezza cibernetica a livello nazionale ed europeo nei prossimi anni.

L'entrata in vigore della **Direttiva NIS2** a gennaio 2023 ha introdotto nuovi obblighi di sicurezza informatica per **grandi** e **medie imprese**, sia nel settore pubblico che privato. Con il recepimento imminente da parte degli Stati Membri entro il **17 ottobre 2024**, i soggetti coinvolti saranno tenuti ad aderire a rigorosi requisiti relativi alla governance, alla continuità operativa, al controllo della catena di approvvigionamento, alla segnalazione degli incidenti e, in generale, alla gestione dei rischi.

Indice

Introduzione

A gennaio 2023, gli Stati membri dell'Unione Europea hanno ufficialmente approvato una revisione della Direttiva sulla sicurezza delle reti e dei sistemi informatici (Network and Information Systems - NIS) del 2016. Progettata come risposta a cyber attacchi ampiamente diffusi e dannosi, la **Direttiva NIS2** potenzia i requisiti di sicurezza, semplifica gli obblighi di reportistica e introduce misure di supervisione più severe, insieme a requisiti di applicazione più rigorosi. L'obiettivo della nuova Direttiva è rafforzare le difese delle entità critiche contro le vulnerabilità della supply chain, gli attacchi ransomware e altre minacce informatiche.

Tutti i 27 Stati membri dell'UE sono tenuti a ratificare la Direttiva NIS2 **entro il 17 ottobre 2024.**

Questo implica lo sviluppo di piani nazionali per la sicurezza e la formazione di team specializzati per l'implementazione.

La normativa si integra con altre leggi europee sulla protezione dei dati e della privacy, come il **GDPR** e il **Regolamento DORA**, e richiede alle organizzazioni non solo di prevenire gli attacchi informatici, ma anche di dimostrare preparazione e risposta efficace.

È imperativo che le organizzazioni comprendano appieno la **Direttiva NIS2** e la sua influenza su di loro.

La **Direttiva NIS2** ha l'obiettivo di potenziare i requisiti di sicurezza, semplificare gli obblighi di reportistica e introdurre misure di supervisione più severe, insieme a requisiti di applicazione più rigorosi, con l'obiettivo di aumentare la cybersecurity.

Gli Stati membri, tuttavia, si sono dimostrati riluttanti nell'applicare sanzioni, allocare risorse finanziarie e umane, e condividere informazioni in modo sistematico. Ciò ha contribuito a minare, da un lato, l'efficacia delle misure di cybersicurezza adottate dai soggetti in perimetro e, dall'altro, la capacità dell'UE di conseguire un adeguato livello di consapevolezza situazionale comune. Tutte queste sfide rendono ancora più cruciale l'implementazione efficace della **Direttiva NIS2**, per migliorare la sicurezza cibernetica complessiva.

Questo documento fornisce una breve panoramica della **Direttiva NIS2** e spiega come potrebbe influire sul business, fornendo anche indicazioni su come prepararsi.

Che impatto avrà la Direttiva NIS2 sulla tua organizzazione?

Va sottolineato che la **Direttiva NIS2** rappresenta un'evoluzione della **Direttiva NIS originale,** la quale aveva l'obiettivo di potenziare i livelli di cybersecurity in tutta l'Unione Europea. Le modifiche e le nuove disposizioni introdotte dalla Direttiva NIS2 mettono un forte accento sull'aspetto della preparazione, ed avrà un impatto significativo sulle organizzazioni. La **Direttiva NIS2** copre più settori, introduce controlli di sicurezza più approfonditi e impone requisiti di reportistica sugli incidenti più rigorosi.

- Le organizzazioni precedentemente esentate potrebbero dover implementare nuovi sistemi e pratiche di sicurezza informatica per adeguarsi alla **Direttiva NIS2**.
- Al contempo, le organizzazioni già vincolate dalla Direttiva originale potrebbero essere obbligate a rivedere i loro sistemi e le pratiche di sicurezza per conformarsi alla **Direttiva NIS2**.

I soggetti tenuti ad adeguarsi

La portata di applicazione della NIS2 è notevolmente più ampia rispetto alla precedente NIS, coinvolgendo un numero più esteso di soggetti e settori. A differenza della NIS, che si rivolgeva esclusivamente agli "Operatori di servizi essenziali" (OSE) e ai "Fornitori di servizi digitali" (FSD), la nuova Direttiva si estende a tutte le organizzazioni identificate come soggetti "Essenziali" o "Importanti".

MEDIE IMPRESE

Per determinare l'inclusione di un'organizzazione in una di queste categorie, viene introdotto un criterio duplice basato sulla dimensione (size-cap rule) e sul settore di appartenenza. Rientrano nel perimetro le **medie imprese**, definite come **quelle con meno di 250 dipendenti** e un **fatturato annuo non superiore a 50 milioni di euro**, o le imprese che superano i massimali delle medie imprese nei settori specificati negli allegati I e II della Direttiva.

PICCOLE IMPRESE

Anche alcune piccole imprese rientrano nel perimetro, come ad esempio quelle con **meno di 50 dipendenti** e un **fatturato annuo inferiore a 10 milioni di euro**, e le **microimprese** con **meno di 10 dipendenti** e un **fatturato annuo non superiore a 2 milioni di euro**, a condizione che svolgano un ruolo chiave per la società, l'economia o siano cruciali per particolari settori o tipi di servizi, rientrando così nell'ambito di applicazione della presente Direttiva.

Il criterio della dimensione non si applica alle Pubbliche Amministrazioni. Infatti, **sono soggette agli obblighi della NIS2 gli enti della PA centrale**, definiti conformemente al diritto nazionale di uno Stato membro, e gli **enti a livello regionale** che, in seguito a una valutazione basata sul rischio, offrono servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali ed economiche critiche. Tuttavia, **sono esentati dagli obblighi della NIS2 gli enti della pubblica amministrazione** che **operano nei settori della sicurezza nazionale**, **pubblica sicurezza**, **difesa**, **contrasto**, **prevenzione**, **indagini**, **accertamento** e **perseguimento dei reati**.

In particolare, l'Allegato I alla Direttiva stabilisce i settori considerati "ad alta criticità", mentre l'Allegato II elenca i settori ritenuti "critici".

SETTORI AD ALTA CRITICITA'

- **Energia**
- **Trasporti**
- **Settore bancario**
- **Infrastrutture dei mercati finanziari**
- **Settore sanitario**
- **Acqua potabile**
- **Acque reflue**
- **Infrastrutture digitali**
- **Gestione dei servizi TIC**
- **Pubblica Amministrazione**
- **Spazio**

ALTRI SERVIZI CRITICI

- **Servizi postali e di corriere**
- **Gestione dei rifiuti**
- **Fabbricazione, produzione e distribuzione di sostanze chimiche**
- **Produzione, trasformazione e distribuzione di alimenti**
- **Fabbricazione** (dispositivi medici, computer, autoveicoli, ecc.)
- **Fornitori di servizi digitali**
- **Ricerca**

La Direttiva NIS2 introduce requisiti più rigorosi per la cybersecurity e la gestione del rischio

L'articolo 21 della **Direttiva NIS2** impone agli Stati membri di assicurare che le entità essenziali e rilevanti gestiscano il rischio implementando sistemi, politiche e migliori pratiche efficaci che abbraccino una vasta gamma di misure e discipline di sicurezza informatica, tra cui:

- Analisi dei rischi e sicurezza dei sistemi informatici.
- Continuità operativa, come la gestione dei backup e il ripristino di emergenza.
- Pratiche di base per la cyber-igiene.
- Sicurezza della supply chain.
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione delle risorse.
- Accesso Zero Trust (autenticazione multi fattoriale, autenticazione continua).
- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi.
- Tecnologie di crittografia e cifratura.
- Gestione e reportistica degli incidenti.

"CYBER IGIENE" AI SENSI DELL'ARTICOLO 21 DELLA Direttiva NIS 2

Le strategie di cyber-igiene costituiscono il fondamento per proteggere le infrastrutture dei sistemi informatici e di rete, comprendendo aspetti come hardware, software, sicurezza delle applicazioni online e dati aziendali o utenti finali. Queste strategie includono un insieme comune di pratiche di base, quali l'aggiornamento di software e hardware, la gestione delle password, la supervisione delle nuove installazioni, la limitazione degli account di accesso a livello amministrativo e la realizzazione di backup dei dati. Tale approccio proattivo crea un quadro solido per la preparazione e la sicurezza generale in caso di incidenti o minacce informatiche.

Obblighi

A differenza della Direttiva originaria, i requisiti di cybersecurity della **Direttiva NIS2** si applicano non solo alle organizzazioni che operano all'interno della sua definizione estesa di "critica" e ai loro dipendenti diretti, ma **anche ai subappaltatori** e **ai fornitori di servizi che collaborano con loro**.

Con l'adozione della Direttiva da parte degli Stati Membri, **le organizzazioni saranno tenute a conformarsi a rigorosi requisiti**, che possono essere categorizzati in cinque macro-aree:

- **governance**
- **continuità operativa**
- **presidio della catena di fornitura**
- **segnalazione e gestione degli incidenti**
- **misure per la gestione dei rischi per la cybersicurezza**

GOVERNANCE

I vertici delle entità essenziali e rilevanti, come il Consiglio di Amministrazione, sono incaricati di approvare le misure di gestione dei rischi e possono essere considerati responsabili in caso di violazione. Parallelamente, gli organi di gestione sono tenuti a fornire formazione periodica ai propri dipendenti per trasmettere conoscenze e competenze adeguate.

CONTINUITÀ OPERATIVA

Nella gestione dei rischi secondo la Direttiva, si pone un'attenzione speciale sulla continuità dei servizi e la riduzione dell'impatto delle interruzioni, mediante misure come il backup, il ripristino in caso di disastro e la gestione delle crisi.

PRESIDIO DELLA CATENA DI FORNITURA

Un ulteriore aspetto cruciale riguarda la capacità delle organizzazioni di assicurare la sicurezza della propria catena di approvvigionamento, considerando le vulnerabilità specifiche dei fornitori diretti e dei fornitori di servizi, nonché le loro pratiche di sicurezza informatica.

SEGNALAZIONE E GESTIONE DEGLI INCIDENTI

Le entità essenziali o rilevanti sono tenute a segnalare agli specifici CSIRT o alle autorità nazionali competenti qualsiasi incidente che influisca in modo rilevante sulla fornitura dei loro servizi. Ai sensi dell'articolo 23, un incidente è considerato significativo se:

a. "Provoca o può provocare una grave interruzione operativa dei servizi o perdite finanziarie significative per il soggetto coinvolto."

b. "Influisce o può influire su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli."

MISURE PER LA GESTIONE DEI RISCHI

La Direttiva NIS 2 impone l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate ai rischi di cybersecurity, seguendo un approccio multirischio. Queste misure includono:

- L'autenticazione a più fattori.
- La crittografia.
- L'implementazione di pratiche di igiene informatica di base e di sviluppo sicuro.
- Il potenziamento della sicurezza delle risorse umane.
- L'adozione di strategie di controllo dell'accesso e di gestione degli attivi.

Segnalazione e gestione degli incidenti

La Direttiva NIS2 introduce obblighi più rigidi per la reportistica sugli incidenti

Le entità critiche devono ora:

- Dare notifica iniziale di un incidente di sicurezza significativo entro 24 ore dal rilevamento.
- Fornire una valutazione iniziale dell'incidente entro 72 ore dal rilevamento.
- Creare un report finale dettagliato entro un mese dal rilevamento.

Sanzioni

La Direttiva NIS2 impone sanzioni onerose

I criteri adottati per stabilire l'importo delle sanzioni rispecchia quello di altre normative europee come, ad esempio, il Regolamento Europeo per la Protezione dei Dati Personali (GDPR):

- In caso di non conformità rispetto all'adozione delle misure di gestione dei rischi di cybersicurezza e/o agli obblighi di segnalazione degli incidenti, i soggetti essenziali possono incorrere in sanzioni "pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo."

- Per le medesime violazioni, i soggetti importanti possono incorrere in sanzioni "pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo."

Prepararsi alla Direttiva NIS2

Gli Stati membri hanno tempo fino a **ottobre 2024** per ratificare la **Direttiva NIS2**. Ci sono azioni concrete che possono essere intraprese già oggi per prepararsi alla Direttiva NIS2, rispetto a quando gli Stati membri ne avranno ratificato le normative.

1. Identifica, valuta e affronta i tuoi rischi. Gli organi di gestione di entità essenziali e importanti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate con un approccio onnicomprensivo per tutti i pericoli, in modo da gestire i rischi alla sicurezza dei sistemi informatici, di rete e dell'ambiente fisico.

2. Valuta la tua postura di sicurezza. Una valutazione della sicurezza può aiutare a identificare i punti deboli, come le password non gestite o gli account configurati in modo errato o inattivi, suscettibili di furto di credenziali.

3. Adotta misure per proteggere gli accessi privilegiati. Gli attaccanti possono sfruttare gli account privilegiati per orchestrare gli attacchi, abbattere le infrastrutture critiche e interrompere i servizi essenziali. La Direttiva NIS2 consiglia alle entità critiche di limitare l'accesso agli account amministrativi e di ruotarne regolarmente le password.

4. Rafforza le tue difese antiransomware. Gli attacchi ransomware sono costosi e debilitanti nonché una delle preoccupazioni principali per le autorità di regolamentazione dell'UE e una delle principali motivazioni alla base della Direttiva NIS2. Introduci soluzioni di sicurezza e best practice per una difesa proattiva contro il ransomware. Utilizza le soluzioni di sicurezza dei privilegi sugli endpoint per applicare il principio del privilegio minimo, controllare le applicazioni e potenziare le soluzioni antivirus di ultima generazione (NGAV) e di rilevamento e risposta sugli endpoint (EDR).

5. Passa a un architettura Zero Trust. Le architetture di sicurezza tradizionali basate sul perimetro di rete, concepite per difendere i confini della rete aziendale, non sono adatte al mondo dei servizi cloud e della forza lavoro ibrida. Adotta un approccio Zero Trust implementando diversi livelli di difesa come l'accesso con privilegio minimo, l'autenticazione continua e l'analisi delle minacce per convalidare tutti i tentativi di accesso.

6. Monitora la tua supply chain. Gli attacchi alla supply chain sono una delle principali preoccupazioni degli organi di regolamentazione dell'UE e una delle principali motivazioni alla base della Direttiva NIS2.

7. Formalizza il tuo piano di risposta agli incidenti. La Direttiva NIS2 richiede una reportistica più rapida sugli incidenti, con una prima segnalazione da effettuare entro 24 ore dall'incidente stesso. Verifica che la tua organizzazione sia preparata. Riesamina i tuoi processi di notifica degli eventi, raccolta di informazioni e reportistica.

8. Istruisci il tuo personale. La formazione sulla cybersecurity e la cyber-igiene è fondamentale per la Direttiva NIS2. Aumenta i tuoi sforzi per migliorare la consapevolezza informatica e promuovere una cultura incentrata sulla sicurezza.

Passaggi successivi

Essendo una Direttiva, la NIS2 deve essere recepita negli ordinamenti nazionali degli Stati Membri. È essenziale valutare il livello attuale di conformità rispetto ai requisiti espressi nel testo della Direttiva.

Alcuni obblighi specifici per le organizzazioni coinvolte saranno definiti dettagliatamente dai singoli Stati Membri durante il processo di recepimento, tenendo conto delle peculiarità dei contesti nazionali. La scadenza per il recepimento è fissata **entro il 17 ottobre 2024**.
Tuttavia, molti degli aspetti che le organizzazioni dovranno affrontare sono già individuabili nel testo della Direttiva. Pertanto, è consigliabile che non solo le organizzazioni direttamente coinvolte, ma anche quelle facenti parte della loro catena di fornitura, inizino fin da subito ad esaminare, da un lato, la pertinenza della Direttiva al proprio contesto e, dall'altro, ad avviare l'implementazione dei requisiti che richiedono più tempo o per i quali vi è maggiore impreparazione.

Scadenza
entro il
17 ottobre 2024

Le misure che possono essere adottate già da oggi includono:

1. Verificare se la propria Organizzazione rientri già nel perimetro di applicabilità della Direttiva;
2. Valutare il proprio livello di conformità attuale rispetto ai requisiti esplicitati nel testo della Direttiva;
3. Identificare eventuali lacune e pianificare i necessari interventi migliorativi;
4. Informare il personale competente, inclusi gli organi di gestione, sugli obblighi imposti dalla Direttiva e sulle azioni di adeguamento pianificate dall'Organizzazione.

Via Brandizzo, 20
10099 San Mauro T.se (TO), Italia

Telefono: (+39) 011 22 38 774
Fax: (+39) 011 27 30 938