



A

Direttiva NIS2: cybersicurezza nell'UE

Capire e implementare le specifiche della NIS2

Sommario

1	Che cos'è la direttiva NIS2?	1
2	Quali sono le novità della NIS2?	2
2.1	La NIS2 estende il raggio d'azione a un numero maggiore di settori industriali e organizzazioni	2
2.2	La non conformità è costosa	2
2.3	Misure aggiuntive della NIS2	3
2.4	Responsabilità dei dirigenti in caso di violazioni.....	3
	Protezione contro le minacce informatiche: una panoramica dei requisiti NIS2.....	3
3	Chi è interessato dalla NIS2?	4
4	Misure obbligatorie	6
4.1	Stringente obbligo di registrazione.....	6
4.2	Obbligo di segnalazione degli incidenti di sicurezza.....	6
5	La gestione del rischio, il focus della NIS2.....	7
	Quali misure di gestione del rischio sono regolamentate dalla Direttiva NIS2?.....	8
6	Con baramundi alla conformità NIS2	9
7	I prossimi passi verso la conformità alla direttiva NIS2.....	10

1 Che cos'è la direttiva NIS2?

Il numero e la gravità delle minacce alla sicurezza informatica stanno aumentando in tutto il mondo, Unione europea inclusa. Le infrastrutture critiche, essenziali per il buon funzionamento di una società, sono particolarmente a rischio. Ad esempio, un attacco informatico che causa guasti alla rete elettrica potrebbe comportare l'interruzione di servizi essenziali come ospedali, sistemi di comunicazione e impianti di trattamento delle acque.

Sebbene la classificazione delle infrastrutture critiche sia diversa nei singoli paesi dell'UE, gli stati membri collaborano da tempo per migliorare la sicurezza informatica nei settori chiave attraverso la definizione di standard uniformi. Nel 2016, ad esempio, è stata introdotta una direttiva sulla sicurezza delle reti e dei sistemi informativi (Network and Information Security, NIS). La NIS richiedeva a organizzazioni di importanza critica, come ad esempio le aziende KRITIS in Germania, di aderire a una serie di standard per la sicurezza dei network e dei sistemi. La direttiva NIS definiva principi comuni e requisiti minimi, ma lasciava ai singoli stati un margine di discrezionalità in termini di modalità di implementazione.

Nel gennaio 2023, la NIS è stata sostituita dalla direttiva NIS2. Il nuovo regolamento aumenta i requisiti di sicurezza per gli operatori delle infrastrutture critiche e amplia notevolmente la platea delle organizzazioni soggette alle sue disposizioni.¹

Dagli strumenti alle pratiche per migliorare la trasparenza e la sicurezza dell'infrastruttura IT alle misure specifiche per [la gestione del rischio informatico](#), le aziende maggiormente coinvolte dovranno destinare risorse aggiuntive per allinearsi e mantenere la conformità alla Direttiva NIS2. Inoltre, come una delle più importanti novità, la NIS2 prevede il coinvolgimento, all'interno di ogni singola organizzazione, di un numero maggiore di persone oltre ai professionisti IT. Molte figure manageriali senior e dirigenziali come il Chief Information Security Officer (CISO), e vari dipartimenti, quali, ad esempio, quelli con responsabilità operative e finanziarie, contribuiranno d'ora in poi ad assicurare un'affidabile sicurezza IT. Con questo nuovo efficace approccio, il tema della sicurezza informatica e dei network assumerà un ruolo sempre più strategico nell'ambito della cultura aziendale. Le soluzioni di Unified Endpoint Management possono fornire un prezioso supporto nell'allineamento ai nuovi requisiti automatizzando numerose mansioni di routine e di sicurezza, con particolare riferimento alle organizzazioni che si ritrovano ad affrontare una carenza di lavoratori specializzati e a gestire infrastrutture IT sempre più complesse.

¹ Per prendere visione del testo completo della Direttiva:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555>

2 Quali sono le novità della NIS2?

La NIS2 rafforza in modo significativo e amplia le disposizioni già previste dalla direttiva NIS del 2016, con particolare riferimento alle seguenti aree chiave:

- Include più settori industriali e definisce le “Entità essenziali” e le “Entità importanti”
- Introduce una sorveglianza più attenta e sanzioni più severe in caso di non-conformità
- Coinvolge direttamente e assegna alle figure dirigenziali senior la responsabilità della compliance
- Aumenta gli obblighi di rendicontazione
- Definisce regole di sicurezza obbligatorie che le aziende devono attuare e documentare regolarmente, con maggiore attenzione alla gestione del rischio

2.1 La NIS2 estende il raggio d'azione a un numero maggiore di settori industriali e organizzazioni

Le misure di sicurezza informatica dovranno essere implementate da una platea molto più ampia di aziende. Complessivamente, la nuova direttiva si rivolge alle organizzazioni di 11 settori “essenziali” e 7 “importanti”. La classificazione di un'azienda all'interno delle due diverse categorie dipende dal settore assegnato e dalla dimensione dell'attività (si veda Capitolo 4).

2.2 La non conformità è costosa

In caso di inadempienza alle disposizioni della Direttiva NIS2, le aziende rischiano di incorrere in multe severe. Le organizzazioni dei settori importanti, incluse quelle operanti nella produzione di generi alimentari, servizi digitali, o nell'industria chimica e manifatturiera saranno soggette a sanzioni fino a 7 milioni di euro o all'1,4% del fatturato annuale. Per le organizzazioni dei settori essenziali, come trasporti, finanza, energia e infrastrutture digitali, le sanzioni potranno ammontare fino a 10 milioni di euro o al 2% del loro fatturato annuale. Per le inadempienze gravi, gli importi potranno essere innalzati fino a 20 milioni di euro o al 4% del fatturato annuale complessivo. I trasgressori potranno inoltre essere soggetti a sorveglianza governativa per assicurare la conformità, come interventi di supervisione reattiva a seguito di un incidente avvenuto presso le aziende classificate come importanti o di supervisione proattiva con monitoraggio continuo per le organizzazioni essenziali.

2.3 Misure aggiuntive della NIS2

Le aziende interessate dalle disposizioni NIS2 saranno inoltre tenute all'implementazione di misure di sicurezza IT più severe e su scala più ampia, con enfasi sulla gestione del rischio e sulla sicurezza della catena di approvvigionamento. Altri requisiti includono regolari penetration test, sistemi per la segnalazione degli incidenti di sicurezza, e l'implementazione di misure attive per mettere in sicurezza network e sistemi. Le organizzazioni dovranno riportare gli incidenti all'interno del proprio paese o a livello dell'UE, se necessario, in base alla gravità dell'accaduto.

2.4 Responsabilità dei dirigenti in caso di violazioni

Fra gli aspetti più importanti della NIS2 troviamo le misure che assegnano una responsabilità personale ai senior manager e ai dirigenti per gli incidenti di sicurezza derivanti da grave mancanza di conformità o negligenza. I manager delle organizzazioni soggette alla direttiva NIS2 devono monitorare l'implementazione delle misure di sicurezza informatica, mentre gli amministratori delegati e gli altri dirigenti parteciperanno regolarmente a un programma di formazione sulla gestione del rischio cibernetico, e acquisiranno le conoscenze e le competenze necessarie ad assicurare alla propria organizzazione conformità costante e resilienza informatica.

Protezione contro le minacce informatiche: una panoramica dei requisiti NIS2

- Linee guida ("policy") per la gestione del rischio e la sicurezza delle informazioni
- Gestione del rischio per prevenire, rilevare e gestire gli incidenti di sicurezza
- Continuità operativa basata sul backup, sul disaster recovery e sulla gestione delle crisi
- Sicurezza della catena di fornitura e misure per l'approvvigionamento sicuro di sistemi informatici e di rete
- Specifiche per la valutazione e la gestione dei rischi informatici
- Specifiche per la crittografia
- Controllo degli accessi tramite autenticazione multi-fattore e single sign-on
- Misure per la sicurezza delle comunicazioni vocali, video e testuali

3 Chi è interessato dalla NIS2?

La direttiva NIS2 amplia notevolmente la platea delle organizzazioni e dei settori industriali soggetti ai requisiti estesi di sicurezza informatica. Le “Entità essenziali”, ritenute di importanza cruciale per il funzionamento dell’economia e della società, includono organizzazioni operanti nei seguenti settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi informativi e della comunicazione, pubblica amministrazione e industria aerospaziale. Le “Entità importanti” sono organizzazioni attive in settori ad alto rischio ma che possono avere un’infrastruttura di rilevanza meno critica rispetto alle Entità essenziali. Includono organizzazioni operanti in settori quali servizi postali e corrieri, gestione dei rifiuti, di produzione di prodotti di importanza critica come farmaci, dispositivi medici e beni industriali, produzione e distribuzione di sostanze chimiche, produzione, lavorazione e distribuzione di generi alimentari, servizi digitali, ricerca e formazione.

Anche la dimensione delle aziende è un fattore determinante per l’inclusione nelle categorie di attività “Essenziali” o “Importanti”. Le organizzazioni essenziali includono medie e grandi imprese con 50 o più dipendenti o un fatturato annuale superiore ai 10 milioni di euro. Tuttavia, alcune aziende con meno di 50 dipendenti o un fatturato inferiore ai 10 milioni di euro all’anno sono soggette alla NIS2 se operanti in settori considerati di importanza critica per la sicurezza nazionale e a livello del territorio dell’UE. Solitamente, le entità importanti includono organizzazioni con 250 o più dipendenti e un fatturato annuale di oltre 50 milioni di euro o un bilancio annuale complessivo superiore a 43 milioni di euro. Infine, la classificazione dipende dall’implementazione della direttiva da parte dei singoli paesi.

Indipendentemente dal settore o dalla dimensione, alcune aziende interessate ignorano il fatto che la NIS2 riguarda anche le catene di approvvigionamento. Le aziende che intrattengono relazioni commerciali con organizzazioni clienti interessate dalla direttiva dovranno pertanto ugualmente allinearsi alla NIS2.

Secondo le stime, oltre 100.000 aziende aggiuntive in Europa saranno soggette alle nuove disposizioni. Il codice NACE può essere utilizzato per verificare se un’organizzazione è interessata² dalla direttiva e a quali obbligazioni è soggetta. Come parte della direttiva NIS2, la direzione di ciascuna organizzazione dovrà effettuare tale analisi di impatto entro ottobre 2024 per essere in regola.

² Per maggiori informazioni sui codici NACE:
https://ec.europa.eu/competition/mergers/cases/index/nace_all.html

Aziende che soddisfano due dei tre criteri dimensionali:

un'azienda può essere classificata all'interno di una delle classi delle piccole e medie imprese se raggiunge il numero di dipendenti (50 dipendenti a tempo pieno, FTE), e uno dei due criteri finanziari.

Company Category	FTE (Annual Work Units)	Annual Turnover	Annual Balance Sheet
Medium-sized	≤ 250	≤ 50 Mil EUR	≤ 43 Mil EUR
Small	≤ 50	≤ 10 Mil EUR	≤ 10 Mil EUR
Micro	≤ 10	≤ 2 Mil EUR	≤ 2 Mil EUR

Esempio:

Una società giuridicamente indipendente con 49 dipendenti a tempo pieno, un fatturato annuale di 11 milioni di euro e un bilancio complessivo di 9 milioni di euro può essere classificata come piccola impresa, in quanto impiega meno di 60 dipendenti e soddisfa uno dei due criteri finanziari. Se la società cresce, e impiega 49 collaboratori full-time, con un fatturato annuo di 11 milioni di euro e 10 milioni di euro di patrimonio netto complessivo, rientrerà nella categoria delle medie imprese e nell'ambito di applicazione della NIS2.

4 Misure obbligatorie

La NIS2 stabilisce due obblighi di rendicontazione per le aziende interessate. Il primo riguarda la registrazione, mentre il secondo la segnalazione degli incidenti di sicurezza. Se necessario, questi devono essere implementati immediatamente.

4.1 Stringente obbligo di registrazione

Le entità coinvolte dovranno inviare le seguenti informazioni all'autorità competente di ciascun paese, entro al massimo tre mesi dalla classificazione iniziale o rivista NIS2: ragione sociale, forma giuridica, numero di registro delle imprese, indirizzo, informazioni di contatto (ad inclusione di email, telefono, intervalli di indirizzi IP), settore o sotto-settore di pertinenza e la lista degli stati membri UE in cui opera l'azienda. Le modifiche ai dati sopra indicati dovranno ugualmente essere immediatamente comunicate. La mancata o tardiva registrazione, unitamente a un ritardo nella comunicazione di eventuali modifiche, sono considerati reati amministrativi nella maggior parte degli stati membri.³

4.2 Obbligo di segnalazione degli incidenti di sicurezza

Le aziende interessate dalla direttiva NIS2 hanno l'obbligo di informare tempestivamente l'autorità competente nel caso in cui si verifichi un "incidente grave di sicurezza" che abbia causato o con la potenzialità di causare un impatto significativo sulla loro operatività o perdite finanziarie. La segnalazione è inoltre richiesta per gli incidenti che hanno provocato o con la potenzialità di causare gravi danni materiali o di altro genere ad altre persone.

L'implementazione degli obblighi di notifica avviene secondo diverse modalità a livello dei singoli stati, e i vari contesti devono quindi essere esaminati singolarmente. La Germania, ad esempio, ha introdotto una delle versioni più complesse:

- Un rapporto iniziale deve essere stilato entro 24 ore dalla scoperta dell'incidente. Qualsiasi sospetto di atto illecito o effetti transfrontalieri devono essere ugualmente indagati.
- Al più tardi dopo 72 ore, occorre presentare un rapporto sulla valutazione iniziale della gravità, dei potenziali effetti e di qualsiasi indicatore di compromissione (IoC).
- Su richiesta dell'Ufficio federale, dovrà inoltre essere inviato un report provvisorio.
- Infine, entro al massimo un mese dalla presentazione del primo report, dovrà essere inviata una relazione finale, che dovrà necessariamente includere una descrizione dettagliata dell'incidente, della tipologia di minaccia o di causa sottostante, l'indicazione delle azioni di rimedio iniziali e continuative implementate, e qualsiasi eventuale effetto transfrontaliero.

³ Per accedere al portale di rendicontazione e informazione BSI, l'agenzia governativa della Repubblica federale di Germania responsabile per la sicurezza informatica: <https://mip2.bsi.bund.de/>.

5 La gestione del rischio, il focus della NIS2

Una gestione globale del rischio è il punto cardine della nuova direttiva NIS2. In generale, i requisiti NIS2 stabiliscono che le misure di gestione del rischio corrispondano agli standard applicabili più aggiornati, al livello di esposizione, alla dimensione dell'organizzazione, e alla probabilità e gravità degli incidenti di sicurezza. Devono inoltre prendere in considerazione potenziali impatti a livello sociale ed economico. Le organizzazioni che non implementano le misure di gestione del rischio, o non provvedono in modo corretto o entro la tempistica prevista, commettono una violazione delle disposizioni della Direttiva.

In una fase iniziale, per molte aziende l'attuazione della NIS2 richiede l'introduzione di un gran numero di misure tecniche e organizzative. La Direttiva assegna inoltre un ruolo di rilievo all'igiene informatica e alle pratiche di prevenzione degli incidenti. Anche se non esiste un unico strumento in grado di soddisfare tutti i requisiti NIS2, la maggior parte delle aziende utilizza già una gamma di soluzioni di sicurezza IT che possono aiutarle a raggiungere la compliance. Tra queste, possiamo citare le soluzioni per il controllo degli accessi al network e il monitoraggio, [la gestione dei client e l'unified endpoint management](#) (UEM).

Gli strumenti di automazione di un sistema UEM possono efficacemente supportare le aziende ad uniformarsi a numerosi requisiti della direttiva NIS2, a cominciare da un [inventario](#) completo dell'hardware e del software. È importante prendere in considerazione tutte le tipologie di dispositivo, ad inclusione dei controller e dei dispositivi di rete, oltre ai computer e agli apparecchi mobili. Il [Software Asset Management](#) e la gestione delle risorse hardware costituiscono la base di partenza per soddisfare alcuni dei requisiti NIS2, come la trasparenza, l'analisi del rischio e la sicurezza informatica generale.

Le funzionalità dell'UEM includono inoltre strumenti preziosi per procedure di manutenzione e protezione automatizzate e affidabili degli endpoint, come la gestione delle [vulnerabilità](#) e degli aggiornamenti, la crittografia dei dischi rigidi, l'autorizzazione o il blocco di liste di software e un sistema di ticketing per una rapida risoluzione dei problemi.

Quali misure di gestione del rischio sono regolamentate dalla Direttiva NIS2?

- **Policy:** introduzione di linee guida per la gestione del rischio e l'implementazione di misure di sicurezza IT
- **Gestione degli incidenti:** individuazione e gestione degli incidenti di sicurezza
- **Continuità operativa:** gestione del backup, disaster recovery e gestione della crisi
- **Catena di approvvigionamento:** misure per la sicurezza degli approvvigionamenti, della manutenzione e dell'operatività dei sistemi informatici e delle reti
- **Efficacia:** specifiche per valutare i rischi informatici e implementare misure appropriate
- **Corsi di formazione:** programmi di formazione periodica sulla sicurezza informatica per i dirigenti e i dipendenti
- **Sicurezza dei dati:** specifiche di crittografia per tutte le aree chiave
- **Personale:** protezione dei dati delle risorse umane
- **Controllo degli accessi:** monitoraggio e registrazione dell'attività di accesso al network
- **Gestione degli asset:** regole, procedure, metodi e strumenti del Sistema di gestione della sicurezza informatica (ISMS) allineati allo standard [ISO 27001](#).
- **Autenticazione:** impiego di autenticazione multifattore (MFA) e single sign-on (SSO)
- **Comunicazione:** crittografia per comunicazioni vocali, video e testuali
- **Responso di emergenza:** impiego di sistemi sicuri di comunicazione di emergenza

6 Con baramundi alla conformità NIS2

Sei responsabile dell'IT di un'azienda interessata dal NIS2? Allora baramundi può aiutarti a soddisfare i nuovi requisiti di cybersicurezza per la tua azienda. La Baramundi Management Suite copre i seguenti ambiti della direttiva NIS2 con le seguenti funzioni:

Articolo 21 Misure di gestione del rischio nel settore della cybersicurezza

Gli Stati membri assicurano che [...] gli enti adottino misure [...] adeguate per gestire i rischi per la sicurezza delle reti e dei sistemi informatici [...] e per ridurre al minimo l'impatto degli incidenti di sicurezza [...].

a) Concetti relativi all'analisi del rischio e alla sicurezza dei sistemi informatici;

- **baramundi Vulnerability Scanner**
- **baramundi Inventory**
- **baramundi OT-Inventory**
- **baramundi Network Devices**
- **baramundi Update Management & Managed Software**

f) i concetti e le procedure per la valutazione dell'efficacia delle misure di gestione del rischio nel settore della cybersicurezza

- **baramundi Vulnerability Scanner**
- **baramundi Update Management & Managed Software**

h) concetti e procedure per l'uso della crittografia e, qualora necessario, della cifratura;

- **baramundi Endpoint Security**
- **baramundi Disk Protection & File Protection (powered by Drivelock)**

i) Sicurezza del personale, concetti di controllo degli accessi e gestione degli asset

- **baramundi Defense Control**

Una soluzione UEM efficace come la [baramundi Management Suite](https://www.baramundi.com) non solo offre protezione dalle sanzioni, ma previene anche costose interruzioni. La conformità alle linee guida NIS2 non è quindi solo un obbligo di legge, ma anche un contributo fondamentale alla sicurezza e alla resilienza dell'azienda.

7 I prossimi passi verso la conformità alla direttiva NIS2

La tempistica è un aspetto di importanza cruciale per chiunque sia responsabile dell'informatica nelle organizzazioni interessate dalla direttiva NIS2. Attualmente, e mentre i paesi UE introducono o aggiornano i requisiti nazionali specifici, occorre provvedere a fasi di pianificazione e implementazione tempestive e approfondite, unitamente a una regolare revisione di misure di sicurezza informatica conformi. Raccomandiamo i seguenti, prossimi passi:

1. **Iniziate con un'analisi di impatto:** effettuate un'analisi d'impatto per classificare la vostra azienda in base ai codici NACE e alla direttiva NIS2. Questo accorgimento fornisce la base per la pianificazione e l'implementazione di misure conformi alla direttiva.
2. **Coinvolgete attivamente la direzione nel processo NIS2:** spiegate ai dirigenti il potenziale impatto di una mancata o tardiva compliance e informateli sui vantaggi di un'implementazione proattiva. Descrivete in che modo la NIS2 può rafforzare la resilienza informatica della vostra azienda e migliorarne la reputazione nel lungo termine.
3. **Pianificate le misure di gestione del rischio:** effettuate un'analisi completa delle lacune per individuare le aree suscettibili di intervento e le misure mirate necessarie per migliorare la sicurezza informatica. Identificate, inoltre, le soluzioni di automazione IT idonee a liberare risorse preziose da impiegare nell'implementazione delle misure necessarie e nello svolgimento delle mansioni informatiche in corso.
4. **Definite e lanciate il vostro progetto di implementazione NIS2:** avviate un progetto di implementazione dedicato, passo-passo, per assicurare una puntuale compliance. Includete il progetto nei piani di budget e nella pianificazione del personale.
5. **Completate la registrazione e preparate i processi di reporting:** definite i processi per effettuare la registrazione secondo le tempistiche richieste e preparate le procedure di reporting necessarie nell'eventualità in cui si verifichi un grave incidente di sicurezza. Testate e simulate i processi di reporting in modo da essere in grado di agire con rapidità ed efficienza in caso di emergenza.
6. **Impostate il monitoraggio normativo:** definite un sistema di monitoraggio per essere aggiornati su normative attuali, nuove o proposte già da una fase iniziale. Analizzatele con attenzione e valutate il loro impatto sulla vostra azienda.
7. **Assegnate un'alta priorità alla formazione:** nella sola Germania, tre milioni di manager e dipendenti dovranno essere formati ogni anno sulla NIS2. L'autorità competente di ogni paese fornirà costantemente informazioni specifiche sui requisiti di formazione.

Impossibile negarlo: la NIS2 richiede un approccio severo alla sicurezza informatica e un'implementazione tempestiva e coerente di misure appropriate di sicurezza IT. È un tema che i dirigenti aziendali e i professionisti IT devono prendere molto seriamente, e non solo per il rischio di sanzioni amministrative, finanziarie o addirittura penali in caso di violazioni o negligenze. La compliance con la NIS2, infatti, può rafforzare, a livello globale, la sicurezza e la resilienza informatica della vostra organizzazione, indicare il suo impegno verso una solida sicurezza e le misure per prevenire dannosi attacchi cibernetici. Una soluzione UEM efficace riveste un ruolo cruciale nell'aiutare i team IT a raggiungere e a mantenere la compliance, riducendo allo stesso tempo il rischio di mancata conformità.

Volete saperne di più?

Potrete trovare maggiori informazioni su come utilizzare l'automazione UEM per supportare la compliance NIS2, migliorando allo stesso tempo la sicurezza e l'efficienza IT, visitando il nostro sito web <https://www.baramundi.com/> o contattandoci per programmare una consulenza personalizzata. Vi invitiamo anche a provare in prima persona le nostre soluzioni UEM: basterà registrarsi per ottenere una versione di prova, completa di tutte le funzionalità e gratuita per i primi 30 giorni, della baramundi Management Suite su <https://www.baramundi.com/en/management-suite/>.

Non vediamo l'ora di conoscervi!

Contattateci!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com