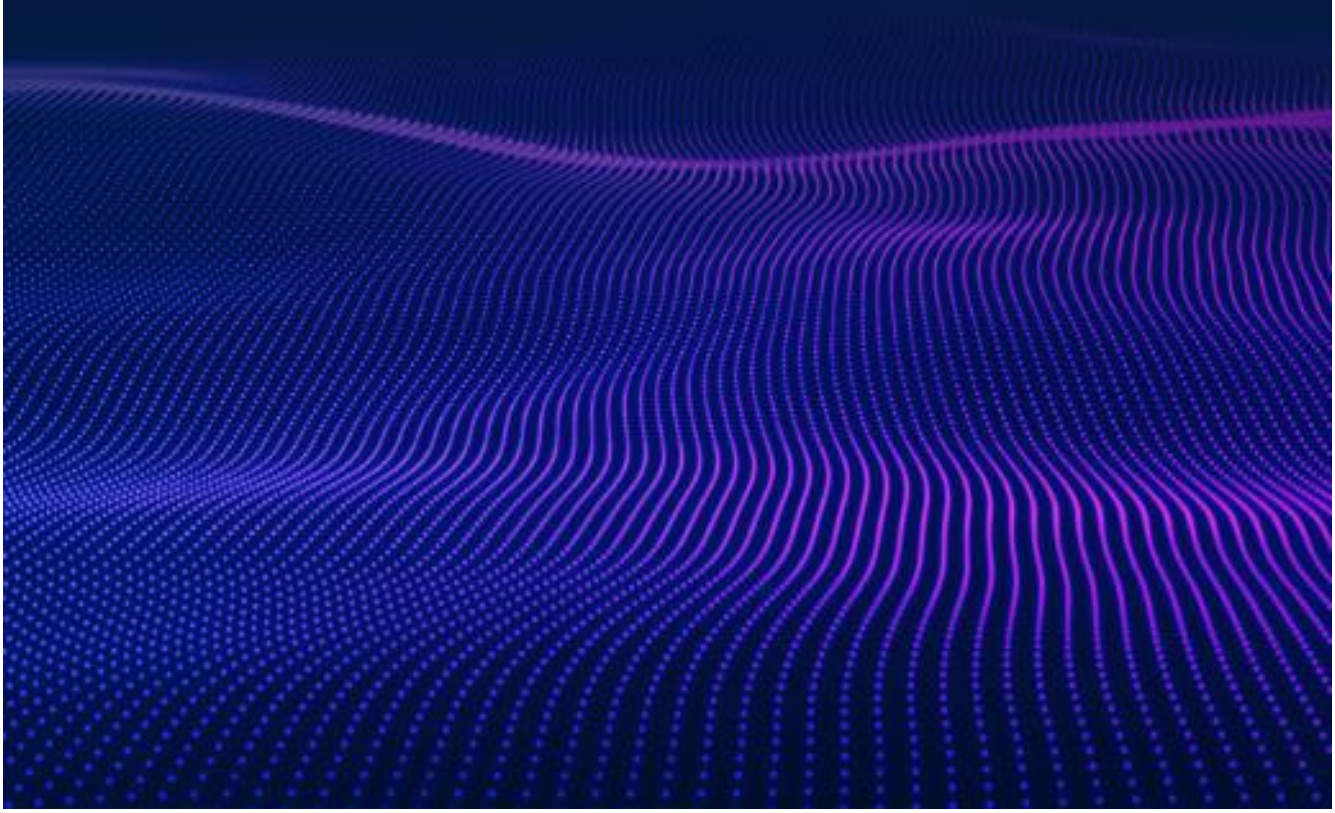
netwrix

# Soluzioni Netwrix
## Per NIS 2



# Sintesi

Il 16 gennaio 2023 è entrata in vigore la Direttiva (UE) 2022/2555, nota come NIS 2. La sua versione iniziale, la direttiva sulla sicurezza delle reti e dell'informazione (NIS), è il primo atto legislativo dell'UE in materia di cybersicurezza. Progettato per raggiungere un elevato livello di sicurezza informatica in tutti gli Stati membri, il NIS è stato recepito nelle leggi nazionali da tutti i membri, con vari gradi di efficacia e una mancanza di chiarezza per le organizzazioni interessate. NIS 2 si occupa di queste carenze, affrontando al contempo il cambiamento nel panorama delle minacce alla sicurezza informatica.

## Cosa è cambiato e cosa c'è di nuovo con NIS 2?

NIS 2 sostituisce la direttiva NIS iniziale (NIS 1), attuata nel 2016. A seguito di una revisione obbligatoria del suo predecessore, NIS 2 mira ad affrontare le carenze individuate. Lo fa fissando tre obiettivi generali.

Il primo obiettivo è quello di aumentare il livello di cyber-resilienza di un insieme più ampio di imprese attive nell'Unione europea. Lo fa definendo ulteriormente le capacità di gestione del rischio informatico richieste per essere in atto nelle organizzazioni coperte da NIS 2. Si tratta di quelle organizzazioni che hanno più di 50 dipendenti e con un fatturato o un bilancio superiore a 10 milioni di euro nella gamma ampliata di settori. Inoltre, per questo obiettivo, NIS 2 definisce le regole di sicurezza applicabili e centralizza questo aspetto in modo che le stesse regole si applichino in tutta l'UE, eliminando un mosaico frammentato di implementazioni NIS1 negli Stati membri dell'UE.

Il secondo obiettivo è quello di affrontare nello specifico tale frammentazione, in quanto la NIS 2 ridurrà le incoerenze nei settori già coperti. Lo farà allineando:

i) L'ambito di applicazione de facto
ii) Le esigenze di segnalazione degli incidenti di sicurezza
iii) Le disposizioni applicabili agli organismi nazionali di vigilanza
iv) Le capacità richieste dalle autorità di una nazione nel campo della sicurezza informatica

Il terzo obiettivo è quello di aumentare la consapevolezza situazionale facilitando gli accordi di condivisione delle informazioni, in modo che tutte le entità interessate e, se necessario, anche altre entità, si scambino informazioni pertinenti sulla cybersicurezza. Questa condivisione di informazioni su minacce, vulnerabilità, TTP, IoC e altri è una novità in NIS 2 ed estende gli obblighi di segnalazione, che sono stati ulteriormente allineati rispetto a NIS1.

NIS 2 deve essere recepito nelle leggi nazionali degli Stati membri dell'UE entro il 17 ottobre 2024, il che lascia all'organizzazione circa 21 mesi per verificare il proprio stato e migliorare ove richiesto.

# Chi è interessato?

In breve, se un soggetto privato nell'UE ha più di 50 dipendenti e realizza un fatturato superiore a 10 milioni di EURI, è molto probabile che sia incluso e debba essere preparato per la conformità NIS 2.

Il numero di organizzazioni che rientreranno nella direttiva NIS 2 è sostanzialmente superiore a quello di NIS1. NIS 2 richiede che le entità essenziali e importanti adottino le misure necessarie per conformarsi e per essere in grado di soddisfare i requisiti di notifica stabiliti. Esiste un limite massimo definito nel NIS 2, in base al quale le organizzazioni di grandi e medie dimensioni dei 18 settori elencati sono coperte da esso. Secondo i regolamenti dell'UE, un'impresa di medie dimensioni è definita come avente più di 50 dipendenti e più di 10 milioni di euro di fatturato e/o volume di bilancio, mentre una grande impresa è al di sopra dei massimali di un'impresa di medie dimensioni (250 dipendenti, 50 milioni di euro di entrate, 43 milioni di euro di bilancio).

I 18 settori sono (essenziale) energia, trasporti, banche, infrastrutture del mercato finanziario, salute, acqua potabile, acque reflue, infrastrutture digitali, servizi ICT, pubblica amministrazione, spazio e servizi postali e di corriere (importanti), gestione dei rifiuti, produzione manifatturiera e distribuzione di prodotti chimici, produzione, trasformazione e distribuzione di alimenti, produzione, fornitori digitali e ricerca.

# Cosa devono fare le entità interessate?

Da un punto di vista tecnico, operativo e organizzativo, il nucleo della NIS 2 è negli articoli 21 e 23 in quanto definiscono le misure che devono essere messe in atto presso un'entità coperta e l'obbligo di segnalazione da adempiere da parte dell'entità coperta nel caso in cui si verifichi un incidente. L'articolo 34 disciplina le ammende inflitte qualora un ente essenziale o importante violi le disposizioni degli articoli 21 e 23.

Le organizzazioni dovranno affrontare diverse aree volte a proteggere le reti e i sistemi informativi e gli ambienti fisici in cui operano. Queste aree sono (secondo la direttiva NIS 2 §21):

i) politiche in materia di analisi dei rischi e sicurezza dei sistemi informativi;
ii) gestione degli incidenti;
iii) continuità operativa, come la gestione del backup e il ripristino di emergenza e la gestione delle crisi;
iv) sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti le relazioni tra ciascuna entità e i suoi fornitori diretti o prestatori di servizi;
v) sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi, compresa la gestione e la divulgazione delle vulnerabilità;
vi) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
vii) pratiche di base sull'igiene informatica e formazione sulla sicurezza informatica;
viii) politiche e procedure relative all'uso della crittografia e, se del caso, della crittografia;
ix) sicurezza delle risorse umane, politiche di controllo degli accessi e gestione delle risorse;

x. l'uso di soluzioni di autenticazione a più fattori o di autenticazione continua, comunicazioni vocali, video e di testo protette e sistemi di comunicazione di emergenza sicuri all'interno dell'entità, se del caso.

In caso di incidente con un impatto significativo sull'organizzazione, deve dare un preavviso entro 24 ore ed entro 72 ore deve presentare una notifica di incidente che contiene una valutazione iniziale che include la gravità e l'impatto, nonché gli indicatori di compromissione, se già disponibili.

Nel complesso, NIS 2 enfatizza le capacità di un'organizzazione di prevenire, rilevare, rispondere e mitigare incidenti e rischi utilizzando framework riconosciuti e tecnologie all'avanguardia. Inoltre, alle entità interessate può essere richiesto di acquistare solo prodotti e servizi delle tecnologie dell'informazione e della comunicazione (TIC) certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza.

# Cosa si può ottenere con le soluzioni Netwrix?

NIS 2 comprende requisiti di sicurezza avanzati relativi alla gestione degli incidenti e delle crisi, gestione e divulgazione delle vulnerabilità, politiche e procedure per valutare l'efficacia delle misure di gestione del rischio di sicurezza informatica, pratiche di igiene informatica di base e formazione sulla sicurezza informatica, l'uso efficace della crittografia e la sicurezza delle risorse umane, politiche di controllo degli accessi e gestione delle risorse.

Un'organizzazione considerata essenziale o importante secondo NIS 2 probabilmente deve migliorare tutti e tre i livelli, la governance e la sicurezza dei dati, la governance e la sicurezza delle identità, nonché il modo in cui governa e protegge la propria infrastruttura.
Per evitare che si verifichi un incidente o che si verifichi un rischio informatico, un'azienda deve essere in grado di enumerare cosa c'è, quali sistemi esistono e la loro rispettiva posizione di sicurezza, chi utilizza questi sistemi in quale circostanza (uso privilegiato o regolare) e quali dati sono accessibili da tali identità. Deve governare le identità degli utenti, essere consapevole dei dati che gestisce e decidere se questi dati sono sensibili e richiedono la crittografia..

Saranno necessari controlli tecnici e organizzativi per rilevare un incidente o per individuare potenziali percorsi di attacco che rappresentano un rischio di compromissione. Anche le alterazioni indesiderate alle identità devono essere rilevate, essendo un indicatore di compromissione, mentre devono essere monitorate anche le modifiche ingiustificate all'integrità e allo stato rafforzato di un sistema.
Risposte automatizzate e personalizzabili agli attacchi in corso contribuiranno a ridurre al minimo l'impatto e supporteranno i requisiti di segnalazione stabiliti in NIS 2.

Le soluzioni Netwrix rispondono a un'ampia gamma di queste esigenze, come illustrato nel diagramma seguente:


Insieme al Cyber Security Framework (CSF) del NIST, le soluzioni Netwrix consentono e supportano organizzazioni di tutte le dimensioni per governare e gestire dati sensibili, identità privilegiate e utenti normali. I rischi per le identità, come i percorsi di attacco ai dati sensibili utilizzando account privilegiati, sono essere affrontati automaticamente. Le soluzioni aiutano a gestire la postura di sicurezza dell'infrastruttura IT di un'organizzazione trovando e correggendo le vulnerabilità, migliorando così l'igiene informatica di base di un'azienda.

L'articolo 21 della NIS 2 stabilisce un elenco di compiti da attuare sotto forma di "misure tecniche, operative e organizzative per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi" in uso da parte delle entità interessate, laddove l'attuazione dovrebbe tenere conto anche delle "norme europee e internazionali più avanzate e, se del caso, pertinenti". La seguente tabella suddivide le misure elencate in singoli elementi e abbina ciascuna di esse alle rispettive soluzioni Netwrix.

| Articolo | Compiti e responsabilità come definiti al § 21 del NIS 2 | Funzionalità Netwrix e rispettive soluzioni | Selezione di standard e raccomandazioni europei e internazionali correlati * |
|---|---|---|---|
| §21.2.a | politiche di analisi dei rischi | Le soluzioni Netwrix supportano l'implementazione delle policy, fornendo strumenti pertinenti per identificare, proteggere, rilevare, rispondere e recuperare dai rischi di sicurezza informatica. L'effettivo sviluppo di tali politiche esula dalla nostra portata. | ENISA Risk Management/Risk Assessment (RM/RA) Framework<br>NIST Risk Management Framework RMF (and NIST SP 800-39, NIST SP 800-37, NIST SP 800-30) |
| §21.2.a | politiche di sicurezza dei sistemi informatici; | | ISO27001 family of standards<br>NIST CSF in combination with NIST 800-53 |
| §21.2.b | gestione degli incidenti | Soluzioni Netwrix per Privileged & Identity Access Management, Protezione Ransomware e Active Directory Security permettono di gestire qualsiasi incidente. | ISO 27036-2:2023<br>NIST SP 800-61 |
| §21.2.c | continuità operativa, come la gestione del backup | Le soluzioni Netwrix per Data Governance e Data Access Governance indirizzano vari aspetti della continuità aziendale, in particolare per i componenti centrali dell'infrastruttura IT di un'organizzazione | ISO 27040:2015<br>NIST SP 800-209 |
| §21.2.c | continuità operativa, come il ripristino in caso di disastro | | ISO 27031:2011<br>NIST SP 800-184 |
| §21.2.c | continuità operativa, come gestione delle crisi | | ISO 22301:2019<br>NIST SP 800-34 |
| §21.2.d | Sicurezza della supply chain security, compresi gli aspetti relativi alla sicurezza delle relazioni tra ciascuna entità e i suoi fornitori diretti o service provider | La sicurezza della catena di approvvigionamento è affrontata dalla soluzione Netwrix per la gestione degli accessi privilegiati e delle identità | ENISA Interoperable EU Risk Management Framework<br>NIST SP 800-161<br>*(see §21.2.a - Risk Analysis as well)* |

| Articolo | Compiti e responsabilità come definiti al § 21 del NIS | Funzionalità Netwrix e rispettive soluzioni | Selezione di standard e raccomandazioni europei e internazionali correlati * |
|---|---|---|---|
| §21.2.e | sicurezza delle reti e dei sistemi informativi: acquisizione, sviluppo | Soluzioni Netwrix per Ransomware Protection abilitano la sicurezza delle reti e dei sistemi informativi controllandone lo stato quando vengono messi in funzione, mantenendo uno stato sicuro e rafforzato durante il funzionamento e aiutano a identificare vulnerabilità e configurazioni errate che influiscono sul livello di sicurezza. Netwrix aderisce inoltre a standard comuni di divulgazione delle vulnerabilità per le proprie soluzioni e prodotti. | ENISA Security Guide for ICT Procurement and ENISA Procure Secure<br>EU Cyber Resilience Act<br>IEC 62443-4-1<br>NIST SP 800-218 - Secure Software Development Framework (SSDF |
| §21.2.e | sicurezza delle reti e dei sistemi informativi: manutenzione | | NIST SP 800-137<br>NIST SP 800-123<br>NIST SP 800-100 |
| §21.2.e | sicurezza delle reti e dei sistemi informativi: gestione e divulgazione delle vulnerabilità | | ENISA Coordinated Vulnerability Disclosure Report<br>ISO 29147:2018<br>NIST SP 800-216 |
| §21.2.f | politiche per valutare l'efficacia delle misure di gestione del rischio di cybersecurity | Le soluzioni Netwrix supportano tali politiche, fornendo strumenti rilevanti per identificare, proteggere, rilevare, rispondere e recuperare dai rischi di sicurezza informatica. | ENISA National Cybersecurity Assessment Framework (NCAF) Tool<br>NIST SP 800-55 |
| §21.2.f | strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza | Le soluzioni Netwrix per la protezione contro i ransomware valutano tali misure attraverso l'audit dello stato di sicurezza di un sistema, verificandone la postura di sicurezza. | Mitre Att@ck Framework<br>*(and a.m. resources on policies)* |

| Articolo | Compiti e responsabilità come definiti al § 21 del NIS | Funzionalità Netwrix e rispettive soluzioni | Selezione di standard e raccomandazioni europei e internazionali correlati * |
|---|---|---|---|
| §21.2.g | pratiche di igiene informatica di base | I nostri set di soluzioni per Privileged & Identity Access Management, Ransomware Protection e Active Directory Security forniscono una gamma completa di pratiche di igiene informatica di base a un'organizzazione. | IT-Grundschutz (Germany)<br>Cyber Essentials / CE plus (UK)<br>Guide d'hygiène informatique (FR)<br>NIST SP 800-53 Rev. 5<br>NISTIR 7621 Rev. 1<br>NIST 1800 series of guides |
| §21.2.g | formazione in materia di cybersicurezza | Non esistono soluzioni Netwrix che affrontino questo aspetto. | ENISA European Cybersecurity Skills Framework (ECSF)<br>NIST NICE Framework |
| §21.2.h | politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura | Soluzioni Netwrix per Data Governance e Data Access Governance supportano tali politiche e procedure, fornendo strumenti pertinenti per identificare, proteggere, rilevare, rispondere e recuperare dai rischi di sicurezza informatica, in particolare quelli relativi ai dati. | ISO27001 family of standards<br>NIST SP 800-175A |
| §21.2.h | politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura | | ENISA - Recommended cryptographic measures - Securing personal data<br>NIST SP 800-175B |
| §21.2.i | sicurezza delle risorse umane | Non esistono soluzioni Netwrix che affrontino questo aspetto. | ENISA's AR-in-a-Box<br>NIST SP 800-50 |
| §21.2.i | strategie di controllo dell'accesso | Le nostre soluzioni per Privileged & Identity Access Management e Active Directory Security forniscono una gamma completa di strumenti per sviluppare e implementare policy e meccanismi di controllo degli accessi. | ISO 29146:2016<br>NISTIR 7316 and NISTIR 7874<br>NIST SP 800-192 |

| Articolo | Compiti e responsabilità come definiti al § 21 del NIS | Funzionalità Netwrix e rispettive soluzioni | Selezione di standard e raccomandazioni europei e internazionali correlati * |
|---|---|---|---|
| §21.2.i | gestione degli asset | Le soluzioni Netwrix per Identity Access Management, Ransomware Protection e Active Directory Security si occupano della sicurezza delle risorse, offrendo il controllo su "chi, cosa, quando, perché" viene utilizzato un asset e sulla sua postura di sicurezza | ISO 19770 family of standards<br>NIST SP 1800-5 |
| §21.2.j | l'utilizzo di soluzioni di autenticazione a più fattori o di autenticazione continua | Le nostre soluzioni per Privileged & Identity Access Management e Active Directory Security prevedono l'autenticazione just-in-time, MFA e i relativi controlli di accesso. | NIST SP 800-63B<br>ISO TR 29156:2015 |
| §21.2.j | l'uso di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità, se del caso | Le soluzioni Netwrix per Ransomware Protection hanno un gioco limitato, cioè per verificare che la crittografia sia effettivamente in uso, con la forza richiesta. | NIST SP 800-45<br>NIST SP 800-177 |

* Le risorse elencate sono un punto di partenza per ulteriori ricerche su una comprensione più profonda dei compiti e delle responsabilità menzionati. Alcune delle risorse menzionate affrontano molte delle attività richieste.

# Informazioni su Netwrix

Netwrix semplifica la sicurezza dei dati. Dal 2006, le soluzioni Netwrix semplificano la vita dei professionisti della sicurezza consentendo loro di identificare e proteggere i dati sensibili per ridurre il rischio di violazione e di rilevare, rispondere e recuperare dagli attacchi, limitandone l'impatto. Più di 13.000 organizzazioni in tutto il mondo si affidano alle soluzioni Netwrix per rafforzare la loro postura di sicurezza e conformità in tutti e tre i principali vettori di attacco: dati, identità e infrastruttura.

Per ulteriori informazioni su Netwrix, visita www.netwrix.it.

**Corporate Headquarters:**
6160 Warren Parkway, Suite 100, Frisco, TX, US 75034 (USA)
**Telefono:** +39 02 947 53539 **EMEA**: +44 (0) 203-588-3023
netwrix.com/social