Acronis

WHITE PAPER

Breve informativa su NIS 2 per le aziende

Cosa comportano gli standard di conformità alla NIS 2 per le aziende che operano nell'Unione Europea

Sommario

Esclusione di responsabilità:

Lo scopo di questo white paper è fornire opinioni e una comprensione dell'importanza attuale, delle implicazioni e dell'implementazione delle policy, delle procedure e delle best practice di cyber security associate alla seconda edizione della 'Direttiva sulle reti e i sistemi informatici' (NIS 2). Nella stesura del presente white paper, ci siamo basati sulla versione integrale del documento in lingua inglese pubblicato ufficialmente e reperibile nel repository EUR-Lex.[1] Abbiamo fatto ogni sforzo per garantire la massima accuratezza e completezza, ma come per tutte le questioni di questo tipo, le informazioni sono soggette a interpretazioni, revisioni e chiarimenti nel tempo. Gli autori consigliano a tutti i lettori di esaminare il materiale di origine e di consultare esperti legali e esperti in normative per trarre le proprie conclusioni.

[1] Documento 32022L255, Direttiva del Parlamento europeo e del Consiglio del 14 dicembre 2022, et al; consultato dagli autori nel dicembre 2023: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Panoramica

La direttiva NIS (Network and Information Systems) mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, a mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società.[2]

La Direttiva NIS ha svolto un ruolo significativo nella definizione delle pratiche di cyber security all'interno dell'Unione europea, certamente, e ha attirato l'attenzione a livello internazionale, ma la sua corretta implementazione ha influenzato anche le politiche di cyber security di nazioni al di fuori dell'Unione europea. Infatti, dal momento che le aziende che operano nell'Unione europea devono soddisfare i requisiti di conformità indipendentemente dalla loro sede, molte aziende soggette alla direttiva hanno semplicemente applicato pratiche di cyber security conformi come precetti in tutta la loro organizzazione.

È stata approvata una nuova versione aggiornata della NIS — NIS 2 — ed è obbligatoria la conformità ad essa entro il 17 ottobre 2024.[3] Dato l'ampio utilizzo nell'UE e la sua influenza al di fuori dei confini dell'UE, l'aggiornamento ha importanti implicazioni in termini di conformità per qualsiasi azienda che fornisca servizi a clienti residenti nell'UE.

Breve storia della NIS e NIS 2

La direttiva NIS (Network and Information Systems), precedentemente nota come direttiva UE 2016/1148, è stata adottata nel 2016 per promuovere un insieme uniforme di governance e best practice in materia di cyber security, a tutela dei cittadini e delle aziende dell'Unione europea. Gli Stati membri dell'Unione europea erano tenuti a utilizzare queste regole uniformi per creare leggi nazionali e strategie di cyber security a livello locale entro maggio 2018.

[2] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/80

[3] Briefing del Think Tank del Parlamento europeo, esaminato dagli autori nel dicembre 2023: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Punti chiave della Direttiva NIS

- **Ambito di applicazione:** si concentrava su settori settori critici come energia, trasporti e logistica, banche e finanza, sanità e settore dei servizi digitali (ad esempio, servizi di cloud computing, marketplace online e motori di ricerca).
- **Competenze nazionali:** ogni Stato membro era tenuto ad adottare una strategia nazionale sulla sicurezza delle reti e dei sistemi informatici e istituire un'autorità nazionale dedicata a tale scopo.
- **Collaborazione transfrontaliera:** è stato istituito un gruppo di cooperazione per facilitare la condivisione di informazioni strategiche e la collaborazione tra gli Stati membri dell'UE, e è stata creata una serie di team regionali di risposta agli incidenti di cyber security (CSIRT) per la risposta rapida e il coordinamento degli incidenti.
- **Requisiti di sicurezza e notifica:** tutti i settori critici e i service provider digitali erano tenuti a implementare protocolli di sicurezza standard del settore e a inviare una notifica alle autorità governative in caso di incidenti gravi.

Panoramica della NIS 2

Nel dicembre 2020, la Commissione europea ha proposto importanti aggiornamenti alla Direttiva NIS originale. Questo intervento è stato probabilmente influenzato dall'accelerazione della digitalizzazione durante la pandemia e dall'aumento conseguente delle minacce informatiche e degli incidenti in tutto il mondo, che hanno evidenziato delle aree significative da migliorare. Inoltre, si è ritenuto necessario apportare alcune modifiche per risolvere alcune limitazioni e incongruenze emerse durante l'implementazione del progetto originale.

La necessità di una revisione è stata definita da:

- **Uno scenario delle minacce informatiche in evoluzione:** il numero e la sofisticazione degli attacchi informatici sono in costante aumento, per cui è necessaria una protezione più efficace e misure preventive più incisive.
- **Un'implementazione non uniforme:** l'implementazione non uniforme della Direttiva NIS nei diversi Stati membri ha generato livelli di cyber security diversi, con conseguenti falle di vulnerabilità.
- **Un ampliamento dell'ambito:** l'ambito di applicazione della Direttiva NIS originale era limitato a determinati settori e tipi di soggetti, lasciando così ampie fette di economia scoperte, senza un quadro di riferimento unificato per la cyber security.

Una delle incongruenze riguardava la discrezionalità concessa agli Stati membri in merito alle organizzazioni tenute a conformarsi. Ad esempio, è emerso che alcuni Stati membri avevano stabilito che determinati ospedali non rientravano nell'ambito di applicazione del regolamento NIS originale, mentre altri sì. A titolo di esempio, diversi Stati membri avevano interpretato che la direttiva non si applicasse alle organizzazioni più piccole, anche se queste ultime operano in settori importanti o fanno parte delle catene di fornitura di organizzazioni che invece sono soggette a obblighi specifici di conformità.

Queste incongruenze hanno creato falle nella cyber security, in cui sistemi e dati simili venivano protetti in misura diversa in scambi intersettoriali e transfrontalieri, tra altri rischi, dovuti al fatto che reti e i sistemi informatici (e quindi la necessità di una protezione dei dati formalizzata) sono diventate funzionalità centrali della vita quotidiana.

Per soddisfare queste esigenze, la NIS 2 si basa sul framework di cyber security della NIS e lo espande in modo significativo.

- **Ambito di applicazione ampliato:** la NIS 2 amplia notevolmente l'ambito, includendo più settori e tipi di soggetti, tra cui amministrazioni pubbliche e medie imprese di settori critici.
- **Requisiti di sicurezza potenziati:** la NIS 2 propone requisiti di sicurezza più rigorosi e misure di vigilanza più severe per le autorità nazionali, comprese linee guida unificate per le sanzioni.
- **Segnalazione avanzata degli incidenti:** la NIS 2 semplifica i requisiti di segnalazione degli incidenti e delinea tempistiche di segnalazione rigorose.
- **Maggior attenzione alla sicurezza della catena di fornitura:** in passato, le catene di fornitura fisiche e digitali e le relazioni tra le varie catene non venivano trattate in modo completo. La NIS 2 risolve questi problemi.
- **Condivisione delle informazioni incrementata:** incoraggia la condivisione proattiva delle informazioni relative alle minacce informatiche e agli incidenti, all'interno e all'esterno dei confini nazionali, tra agenzie, team di risposta, organizzazioni di utenti finali, service provider e, ove applicabile, con il settore pubblico.
- **Armonizzazione delle misure di sicurezza:** la NIS 2 mira a una maggiore armonizzazione delle misure di sicurezza tra gli Stati membri per ridurre le incongruenze riscontrate con la direttiva originale e colmare le lacune in materia di cyber security.

La Direttiva NIS 2 è di grande importanza per gli MSP per diversi aspetti fondamentali:

- **Ambito ampliato:** a differenza della direttiva NIS originale, che si concentrava principalmente sugli operatori di servizi essenziali e sui fornitori di servizi digitali, la NIS 2 amplia il proprio ambito di applicazione per includere una gamma più ampia di soggetti. Questa espansione significa che più imprese potrebbero rientrare nei requisiti normativi della direttiva, rendendo necessario, per questi, il rispetto delle sue disposizioni.
- **Requisiti di sicurezza e conformità più rigorosi:** le imprese devono garantire che le pratiche di cyber security siano allineate agli standard avanzati definiti dalla Direttiva NIS 2. Tra questi troviamo l'implementazione di misure di sicurezza avanzate, il mantenimento di piani di incident response efficaci e il rispetto di requisiti di segnalazione più rigorosi in caso di incidenti di sicurezza per gli ambienti interni e i sistemi e dispositivi client supportati.
- **Segnalazione degli incidenti obbligatoria:** in caso di incidente di cyber security rilevante, ogni azienda dovrà segnalarlo all'autorità nazionale competente entro un determinato lasso di tempo. Il mancato rispetto di tali obblighi potrebbe comportare sanzioni.
- **Aumento della responsabilità e delle sanzioni:** il mancato rispetto della direttiva può comportare un aumento della responsabilità per le aziende, in linea con le nuove sanzioni standardizzate.
- **Maggiore attenzione alla sicurezza della supply chain:** le aziende devono garantire che i propri sistemi e servizi siano conformi e quindi meno a rischio di diventare un bersaglio o un anello di un attacco alla supply chain. Questo significa anche che devono eseguire valutazioni approfondite e regolari delle proprie attività e delle catene di fornitura IT.
- **Differenziazione e fiducia del mercato:** la conformità alla NIS 2 può rappresentare un elemento di differenziazione competitiva per un'azienda. Allineandosi a queste normative, le aziende possono aumentare la fiducia dei clienti e dei partner attuali e potenziali.
- **Standardizzazione transfrontaliera:** per le aziende che operano in più di uno Stato membro dell'UE, NIS 2 prevede un insieme di requisiti di cyber security più omogeneo. Questo aumenterà la conformità in alcune giurisdizioni dell'Unione europea, ma, soprattutto, faciliterà probabilmente gli sforzi di conformità per le aziende che servono clienti in più paesi dell'UE. Gli stati nazionali all'interno dell'UE potrebbero avere ulteriori requisiti di cyber security o differenze nelle definizioni regionali. La direttiva afferma esplicitamente che «La presente direttiva non impedisce agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione».[4] Tuttavia, ci aspettiamo che la nuova direttiva riduca notevolmente queste differenze.
- **Misure di cyber security proattive:** le aziende devono anticipare le minacce emergenti e aggiornare continuamente le proprie policy e procedure di sicurezza, ivi comprese l'automazione e l'implementazione oculata di sistemi di intelligenza artificiale (AI) e machine learning (ML) che accelerano la reattività.

[4] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/111

Elementi di rilievo della NIS 2 per le imprese

Oltre ai requisiti di conformità per i soggetti importanti e critici, la direttiva completa include istruzioni per gli Stati membri, le agenzie di polizia e gli enti regolatori dell'Unione europea. Riteniamo che tutte le aziende con sede o che operano nell'Unione europea, che forniscono servizi a clienti che operano nell'Unione europea o che stanno valutando l'espansione delle proprie attività nell'Unione europea, debbano familiarizzare a fondo con l'intera direttiva. Tuttavia, abbiamo individuato alcune clausole e i relativi requisiti che potrebbero interessare in particolare le imprese.

AI, ML, automazione e innovazione

Viene incoraggiato in particolare l'uso innovativo di tecnologie di cyber security avanzate, compresa l'AI.

> Gli Stati membri dovrebbero incoraggiare l'uso di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici, consentendo di destinare in modo più efficace risorse per affrontare gli attacchi informatici. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cibersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli strumenti automatizzati o semiautomatizzati nella cibersicurezza... [5]

L'aggiunta di un linguaggio specifico per l'AI non è una sorpresa. Sebbene l'AI sia in uso da molti anni, non era stata affrontata in modo esaustivo nella Direttiva NIS originale, perché gli strumenti di AI e ML sono diventati di uso comune e ampiamente disponibili solo negli ultimi anni. La sua inclusione nella NIS 2 è tempestiva, soprattutto considerando che gli strumenti di intelligenza artificiale sono ora disponibili anche per i criminali informatici, che possono così accelerare notevolmente la varietà, la qualità e il numero degli attacchi. Riteniamo che il modo migliore per le aziende di affrontare l'accelerazione degli attacchi sia combattere il fuoco con il fuoco, accelerando la cyber protection e le difese attive con soluzioni che distribuiscono AI, ML, automazione e innovazione continua.

Ransomware

Gli attacchi ransomware in tutto il mondo industrializzato sono aumentati in modo drammatico dopo la pandemia, e ora coinvolgono quasi tre quarti delle aziende. [6] La direttiva riconosce esplicitamente i rischi dei ransomware, l'aumento del numero di attacchi e il nuovo modello criminale di business, la direttiva menziona il ransomware ben sette volte, tra cui:

[5] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (51); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/90
[6] "Quota annuale di organizzazioni colpite da attacchi ransomware in tutto il mondo dal 2018 al 2023", come riportato da Statista e verificato dagli autori di questo white paper a dicembre 2023: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate

> Negli ultimi anni l'Unione ha dovuto far fronte a un aumento esponenziale di attacchi ransomware, in cui i malware criptano dati e sistemi e chiedono il pagamento di un riscatto per il rilascio. La frequenza e la gravità crescenti degli attacchi ransomware possono essere determinate da diversi fattori, come i diversi modelli di attacco, i modelli criminali commerciali che considerano i «ransomware come un servizio» e le criptovalute, le richieste di riscatto e l'aumento degli attacchi contro la catena di approvvigionamento. Gli Stati membri dovrebbero sviluppare politiche, come parte delle loro strategie nazionali per la cibersicurezza, che affrontino l'aumento degli attacchi ransomware. [7]

Le piccole e medie imprese sono particolarmente sensibili rispetto ai rischi della catena di approvvigionamento. Questo è probabilmente dovuto al fatto che le organizzazioni più piccole tendono a sottovalutare il rischio. Anche se la direttiva sembra concedere ampio margine di manovra agli Stati membri per affrontare questi rischi, le best practice per la protezione dal ransomware nell'UE sono generalmente accettate, e tra queste troviamo gli aggiornamenti e applicazione delle patch per i sistemi e i software, l'uso di efficaci strumenti di rilevamento attivo e antivirus, l'impiego di filtri per i siti Web/gli URL e il mantenimento di una solida soluzione di backup e ripristino, tra le altre cose emesse da EUROPOL in concomitanza con la direttiva NIS originale. [8] Pertanto, le disposizioni sui ransomware nella NIS 2 potrebbero essere considerate come l'applicazione più omogenea delle best practice già note negli Stati membri e come garanzia di conformità in un'ampia gamma di segmenti cruciali e dimensioni organizzative.

Microimprese e piccole e medie imprese

La NIS 2 riconosce che la precedente legislazione era rivolta alle grandi organizzazioni, mentre “Le piccole e medie imprese rappresentano nell’Unione, un'ampia percentuale del mercato industriale e commerciale...” 9 Pertanto, le organizzazioni più piccole sono menzionate in modo specifico e gli Stati membri sono incoraggiati a fornire orientamenti e risorse anche a questo gruppo critico.

La NIS 2 riconosce inoltre che le organizzazioni più piccole devono affrontare sfide che non riguardano le organizzazioni più grandi, tra cui:

- Bassi livelli di consapevolezza in materia di cyber security.
- Mancanza di team adeguati o di risorse di sicurezza IT remote.
- Costi unitari più elevati per la distribuzione della cyber security a causa delle economie di scala e dell'utilizzo inefficiente delle risorse da parte del personale specializzato.

E dal momento che le piccole organizzazioni sono parti importanti delle catene di fornitura di altre aziende, queste potrebbero diventare l'anello debole, innescando un impatto a cascata sull'economia.

Cyber protection attiva

La NIS 2 incoraggia la distribuzione e l'implementazione di una cyber protection attiva. La direttiva definisce la “protezione attiva” come segue:

> Anziché reagire, la protezione informatica attiva consiste nel prevenire, individuare, monitorare, analizzare e attenuare in maniera attiva le violazioni della sicurezza della rete... La capacità di condividere e comprendere in modo rapido e automatico informazioni e analisi riguardanti le minacce, segnalazioni di attività informatiche e azioni di risposta è fondamentale per consentire un'unità di sforzi al fine di prevenire, individuare, affrontare e bloccare con successo gli attacchi informatici nei confronti dei sistemi informatici e di rete. [10]

In altre parole, le organizzazioni e gli Stati membri conformi sono invitati a implementare misure di cyber security in grado di rilevare e risolvere tempestivamente gli attacchi e gli incidenti, ovvero nelle fasi iniziali e prima che si verifichino interruzioni dei sistemi, danni o perdita di dati. Questo implica funzionalità di sicurezza avanzate, tra cui l'EDR (Endpoint Detection and Response). Per fortuna, oggi esistono soluzioni EDR progettate per essere accessibili e facili da implementare per le PMI e le microimprese. Parleremo di questo argomento nella parte finale del presente documento.

[7] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizioni generali (54); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/90

[8] “Tips & advice to prevent ransomware from infecting you electronic devices", guida EUROPOL, 16 novembre 2016, esaminata dagli autori per la stesura del presente report nel dicembre 2023:
https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices

[9] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizioni generali (56); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/90-91

[10] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizioni generali (57); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/91

Requisiti per le segnalazioni degli incidenti

Le nuove regole per la creazione di report degli incidenti saranno applicate una volta che la NIS 2 sarà in vigore. Riconoscendo che una segnalazione tempestiva comporta benefici in termini di arresto della diffusione delle minacce informatiche e riduce i rischi a breve termine, sarà necessario presentare un "rapporto iniziale" all'UE e agli enti degli Stati membri per qualsiasi incidente grave che coinvolga soggetti essenziali e importanti, nel più breve tempo possibile. La direttiva riconosce inoltre il valore della creazione di report una volta che saranno state eseguite la risposta e la correzione, complete di informazioni forensi e investigative dettagliate. Pertanto, la NIS 2 prevede un quadro di segnalazione in più fasi richiesto a tutti gli enti interessati da un incidente.[11]

- **Preallarme:** deve essere presentato "senza indebito ritardo e comunque entro 24 ore".
- **Notifica dell'incidente:** deve essere presentata "senza indebito ritardo e in ogni caso entro 72 ore".
- **Relazione finale:** deve essere presentata "senza indebito ritardo e in ogni caso entro un mese".

Per le imprese è importante sapere che la direttiva riconosce l'obbligo di risposta e correzione in caso di attacco informatico, stabilendo un'eccezione ai requisiti di tempistica delle notifiche.

> Gli Stati membri dovrebbero garantire che l'obbligo di presentare tale preallarme, o la successiva notifica dell'incidente **non sottragga le risorse del soggetto notificante alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie, per evitare che gli obblighi di segnalazione degli incidenti sottraggano risorse alla gestione della risposta agli incidenti o compromettano altrimenti gli sforzi dei soggetti a tale riguardo**.[12]

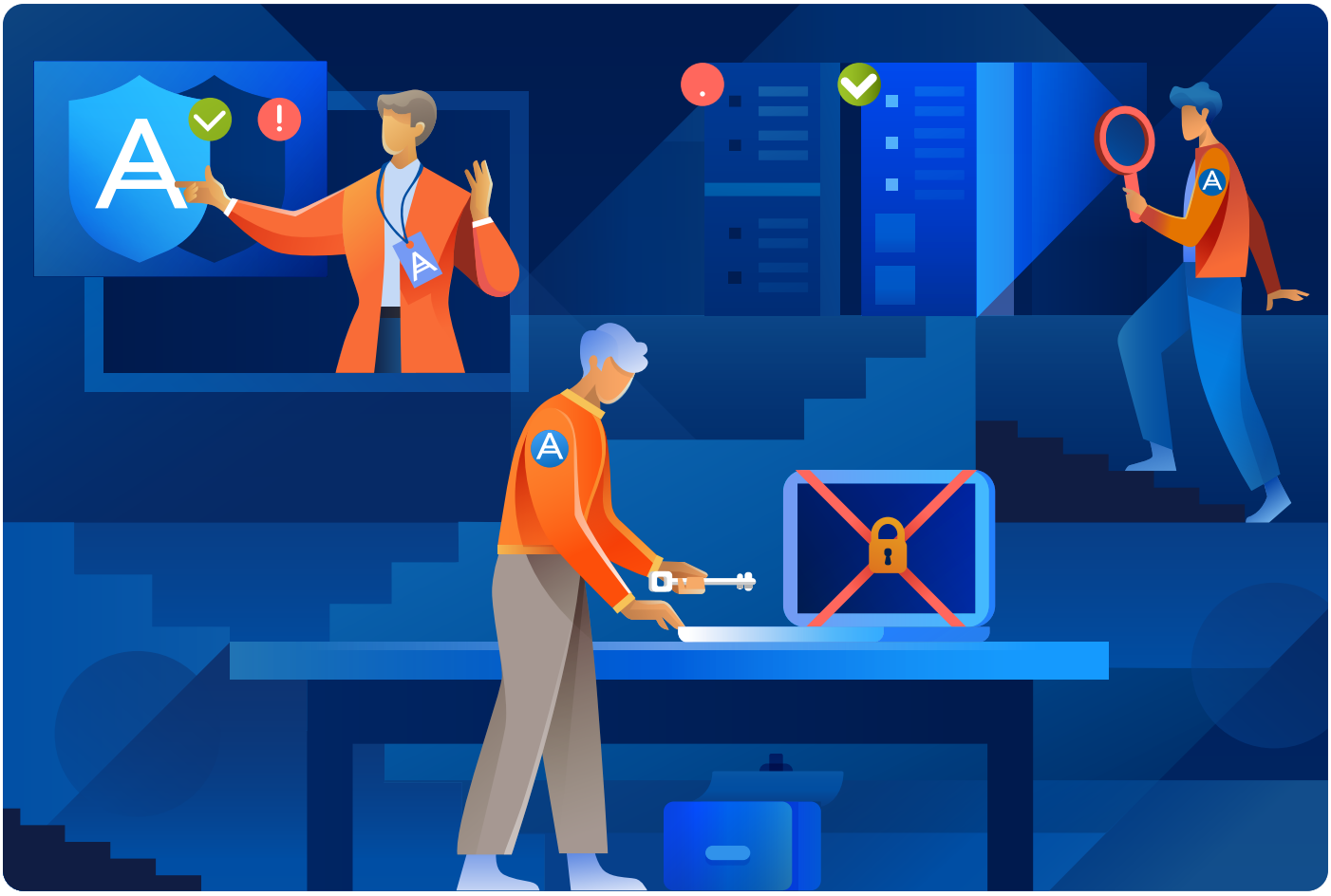
Inoltre, gli Stati membri sono tenuti a semplificare il processo di presentazione di report tempestivi, mettendo a disposizione sistemi online per facilitarne le procedure di creazione e per standardizzare i requisiti per la stesura.

> ...gli Stati membri dovrebbero fornire mezzi tecnici quali un punto di ingresso unico, sistemi automatizzati, moduli online, interfacce di facile utilizzo, modelli e piattaforme dedicate per l'uso dei soggetti, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione della presente direttiva, per la comunicazione delle pertinenti informazioni da segnalare".[13]

Infine, è importante notare che quando si sospetta che un incidente di sicurezza sia collegato a un'attività criminale grave di qualsiasi tipo ai sensi della normativa UE o nazionale, le organizzazioni sono tenute a segnalare l'incidente anche alle autorità competenti, compreso un eventuale coordinamento con EUROPOL, agevolato dal Centro europeo per la lotta alla criminalità informatica e dall'ENISA.[14]

Le imprese trarranno vantaggio dalla standardizzazione e dalla definizione dei requisiti di creazione di report e dalla creazione di meccanismi formalizzati per la creazione dei report digitali.

[11] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (83); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/96
[12] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (84); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/96
[13] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (86); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/96
[14] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (101 - 104); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/99-100



Sanzioni e altre conseguenze per mancata conformità

In generale, la NIS 2 non richiede esplicitamente agli Stati membri di emanare leggi o imporre sanzioni penali o civili a singoli individui in caso di mancato rispetto delle norme.[15] Tuttavia, ciò non significa che la NIS 2 non abbia poteri di applicazione.

- Anche se gli Stati membri non sono “obbligati” a imporre sanzioni civili o penali, ciò non significa che un sottoinsieme di Stati membri non decida di farlo nell'ambito della discrezionalità loro concessa dalla direttiva.[16]
- La NIS 2 incoraggia l'imposizione di sanzioni amministrative. In quanto tali, le entità non conformi possono essere a rischio finanziario e organizzativo.[17]
- La NIS 2 autorizza le "autorità competenti" (Stati membri e relative agenzie nazionali) a sospendere le certificazioni e le licenze e/o a richiedere la sospensione di alcune o tutte le attività e/o operazioni di soggetti che non siano conformi, inclusa anche, nei casi estremi, l'intera azienda.[18]
- Nel caso di istanze con “dimensioni” o impatto transnazionali, gli Stati membri e le rispettive agenzie possono cooperare e fornire “assistenza reciproca” per quanto riguarda la condivisione delle informazioni e l'applicazione delle normative.[19]

Il messaggio è chiaro. Sebbene possano esserci alcune differenze tra i vari Stati membri dell'UE per quanto riguarda le sanzioni, le penali e le altre misure che possono essere adottate, è comunque necessario rispettare le normative. I soggetti non conformi mettono a rischio la propria attività.

[15] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizione generale (128); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/105
[16] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizioni generali (131); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/105
[17] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizione generale (129); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/1050
[18] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizione generale (133); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/106
[19] “Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio”, disposizioni generali (135); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/106

Riassunto

La Direttiva NIS originale, concepita e lanciata nel 2016, è stata in gran parte considerata un successo; tuttavia, l'applicazione pratica della NIS negli ultimi anni ha rivelato delle incongruenze e delle limitazioni specifiche che ne hanno compromesso l'efficacia. Inoltre, il panorama delle minacce informatiche è in continua evoluzione, la pandemia ha accelerato la trasformazione digitale e l'introduzione di nuove tecnologie, come l'AI, ha messo in luce la necessità di un aggiornamento.

La NIS 2 contiene modifiche e ampliamenti significativi dei requisiti originali per correggere queste carenze, e tali modifiche hanno ripercussioni sulle aziende e sui clienti da queste serviti, tra le quali:

- **Ambito esteso:** l'ambito include ora un'ampia gamma di soggetti, tra cui aziende più piccole (qualunque azienda con 50 o più dipendenti o un fatturato annuo di almeno 10 milioni di euro), le aziende di settori designati come "essenziali" (energia, sanità, trasporti e acqua) e le aziende di settori designati come "importanti" (manifatturiero, alimentare, gestione dei rifiuti e servizi postali).
- **Requisiti di sicurezza e conformità più rigorosi:** le aziende devono garantire che le pratiche di cyber security siano allineate agli standard avanzati definiti dalla Direttiva NIS 2.

[18] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (128); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/105
[19] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (131); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/105
[20] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (129); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/105
[21] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (133); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/106
[22] "Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio", disposizioni generali (135); 27 dicembre 2022, (EN) Gazzetta ufficiale dell'Unione europea, L 333/106

- **Creazione di report obbligatoria:** le aziende devono rispettare i requisiti di creazione di report obbligatori in tre fasi.
- **Aumento della responsabilità e delle sanzioni:** il mancato rispetto della direttiva può comportare un aumento della responsabilità per le aziende, con conseguente pagamento di sanzioni amministrative e sospensione di licenze e certificazioni, tra le altre sanzioni.
- **Maggiore attenzione alla sicurezza della catena di fornitura:** le aziende devono eseguire valutazioni approfondite e regolari delle proprie attività e catene di fornitura IT.
- **Differenziazione e fiducia nel mercato:** la conformità alla NIS 2 può rappresentare un elemento di differenziazione competitiva per le aziende.
- **Standardizzazione transfrontaliera:** per le aziende con clienti in più Stati membri dell'UE, la NIS 2 fornisce un insieme di requisiti di sicurezza informatica più omogeneo.
- **Misure di cyber security proattive:** la NIS 2 incoraggia l'adozione di approcci proattivi alla cyber security, compreso l'impiego oculato di intelligenza artificiale (AI), machine learning (ML) e automazione, che accelerano la reattività.

La NIS 2 è entrata in vigore nel gennaio 2024 e richiede di conformarsi entro il 17 ottobre 2024. Il mancato rispetto di tali obblighi può comportare l'applicazione di penali amministrative, la sospensione di licenze e certificazioni e altre sanzioni potenzialmente dannose per le imprese e i loro clienti.

Piuttosto che rappresentare un cambiamento rispetto alla Direttiva originale, la NIS 2 rappresenta un ampliamento e una precisazione che può aiutare le aziende a operare in modo più sicuro, riducendo i tempi di inattività e le perdite subite a causa degli attacchi informatici e quindi proteggendo in modo più efficace le informazioni sensibili dei clienti di cui sono in possesso, sia nell'UE che altrove.

Conclusione - Considerazioni finali

Questo white paper è stato redatto da Acronis per aiutare la comunità delle imprese a orientarsi nel mutato panorama normativo in materia di cyber security e protezione dei dati. La piattaforma Acronis include funzionalità di protezione e ripristino dei dati strettamente integrate con funzionalità di cyber security, per aiutare le aziende a costruire la resilienza digitale necessaria per soddisfare gli standard di conformità, come la NIS 2.

Questa piattaforma, Acronis Cyber Protect, offre:

- Il backup più sicuro e il ripristino più rapido con tecnologie anti-ransomware integrate, che eliminano le lacune nella difesa delle aziende.
- Funzionalità di sicurezza complete, tra cui il rilevamento e la risposta ottimizzata e prioritaria degli endpoint (EDR) e il filtraggio automatico degli URL, che aiutano ad evitare costosi tempi di inattività.
- Monitoraggio e gestione remota integrata degli endpoint, con vulnerability assessment e gestione delle patch automatizzata.

Le aziende che desiderano approfondire come Acronis Cyber Protect possa aiutarle a ottemperare ai requisiti di conformità alla NIS 2 possono richiedere una prova gratuita di 30 giorni, oppure una consulenza gratuita con un architetto delle soluzioni Acronis.

Informazioni su Acronis

Acronis, leader globale nella Cyber Protection, fornisce soluzioni che integrano nativamente funzioni di Cyber Security, protezione dei dati e gestione degli endpoint, progettate per i Managed Service Provider (MSP), le piccole e medie imprese (PMI) e i team IT aziendali. Altamente efficienti, le soluzioni Acronis consentono di identificare, prevenire, rilevare, rispondere e correggere le minacce informatiche più recenti e di avviare il ripristino con minime interruzioni, garantendo integrità dei dati e continuità operativa. Acronis offre la soluzione di sicurezza più completa sul mercato per gli MSP, grazie alla sua capacità unica di soddisfare le esigenze di ambienti IT diversi e distribuiti.

Acronis è una società svizzera fondata a Singapore nel 2003, con 45 sedi in tutto il mondo. Acronis Cyber Protect Cloud è disponibile in 26 lingue e in più di 150 paesi, ed è utilizzata da oltre 20.000 Service Provider per proteggere più di 750.000 aziende. Per ulteriori informazioni, visita il sito www.acronis.com.

Acronis

Maggiori informazioni su **www.acronis.com**