N-ABLE
HEAD NERDS

Analisi della direttiva NIS 2 e impatto atteso su provider di servizi gestiti (MSP) e provider di servizi di sicurezza gestiti (MSSP)

Lewis Pope

8 settembre 2024

Sommario

Introduzione

La Network and Information Security Directive 2 (direttiva NIS 2) rappresenta un cambiamento importante nel framework legislativo dell'Unione europea che si pone come obiettivo il miglioramento della sicurezza informatica per tutti i paesi membri. Basata sulla direttiva NIS originale del 2016, la direttiva NIS 2 risolve le falle del provvedimento precedente ampliando la sua portata, imponendo l'implementazione coerente delle migliori pratiche moderne per la sicurezza informatica, rafforzando i requisiti normativi, migliorando la collaborazione tra gli stati membri e fornendo adeguati meccanismi applicativi. La presente analisi dell'impatto del nuovo provvedimento fornirà le informazioni necessarie sul contesto per aiutare i lettori a comprendere cos'è la direttiva NIS 2 descrivendone il possibile impatto sui provider di servizi gestiti (MSP), sui provider di servizi di sicurezza gestita (MSSP), qui chiamati collettivamente MSP, e sulle aziende cui queste figure si rivolgono, evidenziando le modifiche chiave, le responsabilità e le opportunità commerciali che tale direttiva introduce.

Contesto

La direttiva NIS originale è stata la prima normativa dell'Unione incentrata sul raggiungimento di un livello comune di sicurezza informatica per tutti gli stati membri. Sebbene tale provvedimento sia riuscito a innalzare gli standard di sicurezza informatica, ogni stato membro dell'Unione ha ricevuto poche linee guida e ha potuto godere della libertà di decidere come implementare i requisiti della NIS, il che ha comportato l'applicazione incoerente tra i vari paesi, una portata limitata, meccanismi congiunti inadeguati per la gestione delle crisi e altre limitazioni. La velocità della digitalizzazione, la sempre maggiore interconnessione tra i vari settori e un panorama di minacce a rapida accelerazione hanno imposto un framework collaborativo più robusto per tenere alla larga le minacce informatiche in evoluzione. La direttiva NIS 2 mira a risolvere questi problemi al fine di creare un'Unione europea più resiliente.

Date importanti

8 agosto 2016

Il Parlamento europeo e il Consiglio dell'Unione europea hanno implementato la direttiva (EU) 2016/1148 riguardante le misure per un livello di sicurezza comune più elevato per le reti e i sistemi di informazioni dell'Unione (Parlamento europeo, 2016)

8 novembre 2022

La direttiva NIS 2, precedentemente nota come direttiva (EU) 2022/2555 viene adottata dal Parlamento europeo e dal Consiglio dell'Unione europea. Da allora, ogni stato membro dell'Unione ha lavorato all'implementazione di tale provvedimento. (Parlamento europeo, 2022)

16 gennaio 2023

La NIS 2 entra ufficialmente in vigore in Unione europea e i paesi membri devono iniziare a recepirla nella propria legislazione.

17 ottobre 2024

La direttiva NIS originale (EU) 2016/1148 viene abrogata e questa è la data fissata per il recepimento definitivo della NIS 2 da parte di ogni stato membro dell'Unione (Parlamento europeo, 2022).

18 ottobre 2024

Entrano in vigore le misure imposte dalle leggi ai sensi della direttiva NIS 2.

Dopo il 18 ottobre 2024

L'obiettivo della NIS 2 è evitare un'altra situazione simile all'implementazione non coerente del precedente provvedimento, ma comunque essa prevede che ciascuno stato membro sia responsabile del suo recepimento che introdurrà i requisiti avanzati sulla sicurezza informatica in ogni paese. Poiché ogni stato membro opera ai sensi delle proprie prerogative sul recepimento della direttiva NIS 2, non sarà disponibile alcun modello universale cui attenersi che sia applicabile indistintamente a tutti i paesi dell'Unione europea. Quelli che rappresentano i requisiti in un paese potrebbero rappresentare solo linee guida consigliate in un altro, il che aggiunge ulteriori complessità per le aziende e gli MSP che operano in diversi paesi dell'UE.

17 gennaio 2025

L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) si occuperà di creare e di gestire un apposito registro contenente un'ampia selezione di fornitori di servizi IT. Entro questa data, ogni stato membro dovrà imporre ai soggetti interessati di registrarsi presso le autorità competenti. I provider di servizi gestiti e i provider di servizi di sicurezza gestiti sono interessati da questo requisito.

Ritardi

Il recepimento della NIS 2 da parte dei singoli stati è stato ritardato in molti paesi a causa di diverse ragioni, quali ad esempio, l'avvicendamento dei leader politici e la complessità delle attività legate all'implementazione della direttiva tramite procedure legislative, per cui i progressi registrati sono stati diversi a seconda di ciascuno stato membro. Sebbene la direttiva sia vigente dal 16 gennaio 2023 e ai paesi dell'UE sia stato imposto di recepirla entro il 17 ottobre 2024, sono molti i paesi che non riusciranno a rispettare questa scadenza.

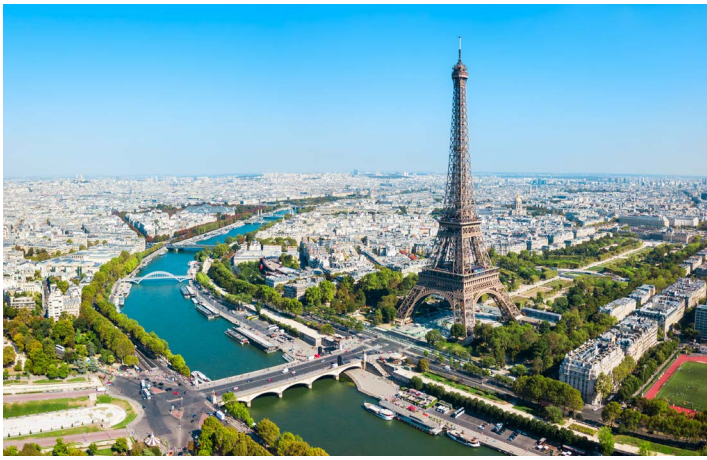
A questo punto, gli MSP e le aziende devono condurre indagini e restare informati circa lo stato del recepimento della direttiva in ogni paese membro in cui operano. Di seguito, viene fornito l'elenco non esaustivo dei paesi dell'UE che non riusciranno a rispettare la scadenza del 17 ottobre 2024 per il recepimento della direttiva.

Danimarca

Il Ministro della difesa danese ha annunciato in data 6 febbraio 2024 che il recepimento della direttiva NIS 2 avrebbe subito ritardi, spostando la scadenza agli inizi del 2025 (Forsvarsministeriet, 2024). A settembre 2024 non era disponibile alcun progetto di legge.

Francia

A settembre 2024 non era disponibile al pubblico il progetto di legge completo. Sebbene non sia stata fornita alcuna informazione dall'agenzia francese ANSSI (Agence nationale de la sécurité des systèmes d'information) circa il rispetto delle scadenze (République Française, 2024) è probabile che i soggetti essenziali e importanti interessati non sappiano cosa è previsto dalle leggi francesi anche oltre il 17 ottobre 2024.



Svezia

Il 5 marzo 2024 la Svezia ha rilasciato la relazione provvisoria circa le nuove regole per la sicurezza informatica che propone l'abrogazione dell'Information Security Act in favore del Cybersecurity Act che recepisce la direttiva NIS 2 (Bohlin, 2024). All'epoca, non erano previsti il recepimento della NIS 2 nella legislazione svedese e la relativa entrata in vigore fino al 1° gennaio 2025.

Obiettivi della direttiva NIS 2

La NIS 2 mira a migliorare la direttiva NIS precedente e ad armonizzare i framework, la legislazione e le risorse per la sicurezza informatica ponendosi quattro obiettivi principali:

Ampliare la portata delle aziende interessate

- La NIS 2 amplia le tipologie di attività e aziende interessate dalle nuove linee guida e dalle leggi successive. Ora interessa aziende importanti ed essenziali, come quelle operanti nel settore sanitario, delle utenze, della pubblica amministrazione, della gestione dei rifiuti, dei servizi digitali, della produzione alimentare e altre.

Migliorare la resilienza informatica

- La NIS 2 impone l'implementazione di requisiti di sicurezza informatica più rigidi in una più ampia serie di settori, ma tali requisiti non presentano nulla di nuovo, piuttosto enfatizzano l'importanza dell'implementazione delle prassi di base per la sicurezza, di un'adeguata gestione dei rischi, della sicurezza della supply chain, della segnalazione degli incidenti e della responsabilità maggiore.

Ridurre le incoerenze

- Armonizzando i requisiti di sicurezza e di segnalazione degli incidenti in tutta l'Unione europea, la direttiva NIS 2 mira a ridurre le incoerenze, a introdurre misure di sicurezza uniformi, gli obblighi di segnalazione e l'applicazione di sanzioni potenziali per favorire partecipazione e cooperazione.

Migliorare la consapevolezza congiunta della situazione

- La NIS 2 sottolinea l'importanza di migliorare le capacità collettive di prepararsi e di rispondere a incidenti di sicurezza su ampia scala tramite una maggiore condivisione delle informazioni e la definizione chiara delle responsabilità tra gli stati membri. La condivisione delle informazioni dal settore privato fino ai centri di fusione, ai CSIRT o ad altri soggetti responsabili di coordinare gli eventi informatici sarà fondamentale per permettere all'Unione di prepararsi e di rispondere al meglio agli eventi.

Ampliare portata e copertura dei settori

La NIS 2 elimina la distinzione tra operatori dei servizi essenziali (OES) e fornitori di servizi digitali (DSP) e la sostituisce con le classificazioni di soggetti essenziali e soggetti importanti. Questo approccio inclusivo interessa un ventaglio più ampio di settori e servizi critici per la società e le funzioni economiche.

Soggetti essenziali

Si tratta di aziende le cui operazioni sono ritenute critiche per il benessere e la sicurezza pubblica. Vengono sottoposte a controlli più severi e devono rispettare in modo proattivo le misure di sicurezza informatica previste dalla NIS 2. I soggetti essenziali includono settori quali:

- Energia (elettricità, gas, petrolio)
- Trasporti (aerei, ferroviari, marittimi, stradali)
- Infrastrutture dei mercati bancario e finanziario
- Sanità (ospedali, prestatori di cure)
- Fornitura e distribuzione di acqua potabile
- Gestione delle acque reflue
- Infrastrutture digitali (punti di scambio internet, provider di servizi DNS, servizi di cloud computing)

Soggetti importanti

Si tratta di aziende che erogano servizi non fondamentali, ma comunque vitali per il funzionamento della società e dell'economia. Tali aziende sono soggette al rispetto dei requisiti di sicurezza informatica ma subiscono la supervisione reattiva delle autorità competenti. I soggetti importanti includono settori quali:

- Servizi postali e corrieri
- Gestione dei rifiuti
- Produzione, lavorazione e distribuzione alimentare
- Produzione di merce fondamentale (prodotti farmaceutici, dispositivi medicali, sostanze chimiche)
- Servizi digitali (marketplace online, motori di ricerca, social network)

Armonizzazione minima

L'articolo 5 della direttiva NIS 2 (Parlamento europeo, 2022) aggiunge qualche incertezza riguardo ai soggetti che operano nei paesi dell'UE che non hanno completato il recepimento della direttiva o non hanno ancora rilasciato progetti di legge in merito all'implementazione prevista della NIS 2. Gli stati membri avranno la libertà di implementare i requisiti per livelli maggiori di sicurezza informatica rispetto a quelli imposti dalla direttiva stessa. Questo potrebbe portare a situazioni in cui i soggetti interessati dalla NIS 2 vengono presi alla sprovvista quando lo stato membro di riferimento introduce normative più severe rispetto a quanto atteso.

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

L'articolo 20 della direttiva (Parlamento europeo, 2022) impone il rafforzamento della rete di CSIRT originariamente stabilita dalla direttiva NIS originale del 2016. La rete di CSIRT è una rete collaborativa finalizzata a migliorare lo scambio di informazioni, a favorire la fiducia e ad agevolare la cooperazione tra gli stati membri. L'obiettivo principale di tale rete è migliorare la gestione degli incidenti informatici transfrontalieri, garantendo una risposta coordinata alle minacce che interessano più stati membri. L'ENISA gioca un ruolo fondamentale nel supportare tale rete, poiché provvede al suo supporto a livello di attività di segreteria, tecniche e di coordinazione.

Miglioramenti alla rete di CSIRT ai sensi della NIS 2

- Fiducia e cooperazione avanzate: il nuovo framework imposto dalla NIS 2 dà la priorità non solo alla risposta agli incidenti, ma fornisce anche misure quali la divulgazione coordinata delle vulnerabilità, garantendo che i CSIRT risolvano potenziali minacce prima che queste si trasformino in incidenti su larga scala.
- Coordinamento degli incidenti: i CSIRT hanno l'obbligo di comunicare in modo più efficace e di divulgare informazioni in tempo reale durante gli incidenti critici, riducendo al minimo i ritardi nelle risposte.
- Ruolo avanzato di ENISA: il coinvolgimento dell'ENISA nella rete di CSIRT è fondamentale. Oltre a fornire attività di segreteria, l'ENISA funge da centrale di coordinamento degli incidenti e contribuisce ad armonizzare gli sforzi degli stati membri durante incidenti di sicurezza informatica complessi.

Banca dati europea delle vulnerabilità

Secondo l'articolo 12 della direttiva NIS 2 (Parlamento europeo, 2022) i CSIRT devono fungere da coordinatori per la divulgazione delle vulnerabilità. Inoltre, tale articolo prevede anche la creazione di una banca dati europea delle vulnerabilità. L'ENISA ha il compito di sviluppare e gestire una banca dati europea delle vulnerabilità. Tale banca dati è stata concepita per permettere ai soggetti e ai relativi fornitori di sistemi di rete e informazioni, che rientrino o meno nell'ambito di applicazione della direttiva NIS 2, di divulgare e registrare le vulnerabilità note al pubblico.

L'obiettivo principale di questa banca dati è assicurare trasparenza e sicurezza. Questo impegno include la pubblicazione di linee guida, raccomandazioni e analisi per aiutare i CSIRT dell'Unione europea ad adottare politiche di divulgazione coordinata (ENISA, 2024).

Segnalazione degli incidenti

L'articolo 41 della direttiva NIS 2 indica in modo dettagliato che le procedure di segnalazione degli incidenti che coinvolgono i soggetti essenziali e importanti saranno obbligatorie. Venuti a conoscenza di un incidente, i soggetti interessati avranno 24 ore per inviare un avviso preventivo iniziale a un team CSIRT o alle autorità competenti, in base a quanto previsto presso lo stato membro in cui tale soggetto opera e nella giurisdizione dello stato membro in cui si verifica l'incidente. Entro 72 ore dall'incidente, dovrà essere prodotta una notifica più dettagliata ed, entro 1 mese, un report finale (Parlamento europeo, 2022).

Tali tempistiche saranno comuni a tutti i paesi dell'UE una volta completato il recepimento della direttiva NIS 2, ma potrebbero essere previsti ulteriori requisiti diversi da paese a paese circa la necessità di informare il pubblico generico sugli eventi significativi che si verificano. Potrebbero inoltre essere imposti ulteriori requisiti di segnalazione a seconda della natura dell'incidente. Se i dati personali vengono esposti a seguito di una violazione dei dati, sarà necessario notificare le parti interessate, ai sensi del Regolamento generale per la protezione dei dati.

Implicazioni per gli MSP

Gli MSP ricoprono un ruolo cruciale nell'ecosistema di sicurezza informatica, poiché erogano i propri servizi ai soggetti essenziali e importanti. Ai sensi della direttiva in oggetto, gli MSP saranno obbligati a un esame più minuzioso e subiranno una maggiore pressione per dimostrare la dovuta cura e diligenza ai soggetti interessati e agli enti normativi. Questo significa che gli MSP che erogano servizi ai soggetti importanti o essenziali devono assicurarsi che le proprie prassi e politiche in materia di sicurezza informatica rispondano ai nuovi requisiti più severi della direttiva e rispettino le leggi implementate dai singoli stati membri dell'UE. Inoltre, gli MSP devono prepararsi a valutazioni complete della sicurezza della supply chain, poiché le relative pratiche influiscono in modo diretto sull'approccio alla sicurezza informatica dei relativi clienti.

Linee guida principali e impatto sugli MSP

La NIS 2 introduce diversi requisiti chiave per i soggetti interessati che potrebbero influire in maniera più diretta su alcuni MSP di maggiori dimensioni, ma tutti gli MSP per procura potrebbero essere interessati dalla direttiva per le tipologie di clienti cui si rivolgono.

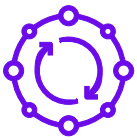
Gestione dei rischi di sicurezza informatica

I soggetti devono adottare misure complete di sicurezza informatica, quali analisi dei rischi, risposta agli incidenti, sicurezza della supply chain, adeguata protezione dei dati e gestione delle vulnerabilità. Tali misure sono state concepite per essere proporzionali all'esposizione e alla gravità dei rischi di tale soggetto. Per quanto riguarda gli MSP, anche se non vengono menzionati direttamente nella direttiva NIS 2, essi saranno classificati come soggetti essenziali o importanti a seconda delle tipologie di clienti cui si rivolgono e del recepimento della NIS 2 da parte dello stato membro in cui operano.

Segnalazione degli incidenti

Gli MSP devono sviluppare piani completi di risposta agli incidenti, che includano anche protocolli chiave per la segnalazione alle autorità nazionali e alle parti interessate. L'approccio in più fasi relativo alla segnalazione degli incidenti ai sensi della NIS 2 impone agli MSP di disporre di robusti meccanismi di rilevamento e risposta agli incidenti. Le segnalazioni iniziali vanno inviate entro 24 ore dal rilevamento, seguite poi da report dettagliati da inviare entro 72 e da un report finale da produrre entro un mese.

Viste le tempistiche ridotte per la produzione di tali report, gli MSP dovranno prendersi il tempo necessario per implementare una procedura dettagliata, pianificata e sperimentata prima che sorga la necessità di inviare una segnalazione. Qualora si verifichi un incidente che riguarda l'MSP o uno dei relativi clienti, ci sarà poco tempo per rivolgersi a un consulente legale e ai soggetti interessati prima di eseguire la segnalazione. A causa delle rigide sanzioni introdotte dalla NIS 2, ogni minuti conta. Gli MSP non possono permettersi di indovinare cosa segnalare e a chi, né di perdere tempo prezioso quando le risorse sono sotto pressione e l'attenzione è labile durante la segnalazione di un incidente.



Collaborazione e condivisione delle informazioni

La NIS 2 incoraggia la collaborazione e la condivisione delle informazioni tra i soggetti interessati e i paesi membri. Gli MSP dovranno partecipare ai forum di settore, alle organizzazioni finalizzate allo scambio di informazioni e conoscenze in ambito sicurezza informatica (ISAC), sfruttare le risorse dell'ENISA e collaborare con le autorità competenti nel proprio paese per migliorare le proprie capacità di intelligence delle minacce e di risposta agli incidenti. Tale approccio collaborativo può aiutare gli MSP a restare al passo con le minacce emergenti e le best practice della sicurezza informatica.

Supervisione e applicazione avanzate

La NIS 2 rafforza i poteri di supervisione e applicazione delle autorità nazionali, in particolare per i soggetti essenziali. Tali poteri includono la possibilità di condurre ispezioni, audit e scansioni di sicurezza a campione e di imporre sanzioni e altre pene per mancata conformità. Nel caso dei soggetti importanti, tali azioni di applicazione e di indagine potrebbero sopraggiungere a seguito della segnalazione di un incidente.

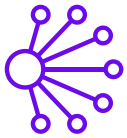
Questo con ogni probabilità significa che gli MSP saranno soggetti a un livello di valutazione cui non sono abituati. Attenendosi alle best practice, alle linee guida e ai framework riconosciuti, gli MSP possono prepararsi al meglio a eventuali incontri con enti normativi o investigativi.

Sanzioni

La direttiva armonizza il regime sanzionatorio in tutta l'Unione europea, con multe per i soggetti essenziali fino a 10 milioni di € o al 2% del volume di affari complessivo e 7 milioni di € o l'1,4% per i soggetti importanti (Parlamento europeo, 2022). Gli MSP dovranno dare assoluta priorità alla compliance alle normative NIS 2, implementando ad esempio servizi e procedure allineati ai severi framework di sicurezza informatica, conducendo audit interni e conservando record dettagliati delle proprie prassi di sicurezza informatica. La mancata conformità non solo espone gli MSP a sanzioni economiche, ma anche al rischio di danni alla propria reputazione, oltre che alla perdita della fiducia dei clienti.

Maggiore carico per la conformità

Gli MSP dovranno aderire a misure di sicurezza informatica più stringenti e ai requisiti di segnalazione, implementando anche strategie complete per la gestione dei rischi, conducendo regolari valutazioni sulla sicurezza e assicurando una rapida segnalazione degli incidenti.



Dovuta diligenza circa la supply chain

La NIS 2 si focalizza sulla sicurezza della supply chain e ciò significa che gli MSP devono valutare e mitigare i rischi associati ai propri fornitori e partner. Questo prevede il completamento di valutazioni complessive dei rischi, l'implementazione di requisiti di sicurezza contrattuali e il monitoraggio continuo dell'approccio alla sicurezza informatica della propria supply chain. Gli MSP devono adottare un approccio proattivo alla sicurezza della supply chain, oltre che audit e valutazioni regolari dei fornitori di terze parti.

Poiché sono parte della supply chain di molti soggetti essenziali e importanti, anche gli MSP saranno oggetto di valutazioni scrupolose e dovranno dimostrare l'implementazione di robuste prassi di sicurezza informatica; potrebbe essere loro richiesto di produrre le prove della conformità ai clienti.

Responsabilità del management

La direttiva NIS 2 pone obblighi diretti sul management dei soggetti interessati perché garantisca la conformità alle misure di sicurezza informatica, ad esempio, una regolare formazione e sensibilizzazione sulla sicurezza informatica, adeguate misure di gestione dei rischi di sicurezza e la potenziale responsabilità personale per la mancata conformità. Gli MSP devono assicurare che il comparto management senior sia avvezzo ai principi della sicurezza informatica e che sovrintenda attivamente ai programmi di conformità, sottolineando la necessità di uno sviluppo professionale continuo e di un'adeguata formazione per la dirigenza.

Il management senior interno alle varie attività di MSP sarà direttamente responsabile per la compliance legata alla sicurezza informatica. Questo necessita di un approccio cosiddetto top-down alla sicurezza informatica, con i dirigenti senior attivamente coinvolti nella gestione dei rischi e nell'applicazione dei criteri.

Opportunità commerciali

Nonostante il maggiore carico relativo alla conformità, la direttiva presenta significative opportunità commerciali per gli MSP. I soggetti obbligati a conformarsi alla NIS 2 cercheranno MSP affidabili con comprovata esperienza in materia di sicurezza informatica. Gli MSP che investono nell'implementazione di robusti framework di sicurezza informatica possono guadagnare un vantaggio competitivo e attrarre nuovi clienti. È più probabile che nel corso dei prossimi anni i potenziali nuovi clienti cerchino assistenza per la direttiva e le normative a essa associate piuttosto che per una stampante che non funziona.

Suggerimenti strategici per gli MSP

Per superare le complessità e capitalizzare le opportunità presentate dalla NIS 2, gli MSP devono considerare le seguenti strategie:

1. **Migliorare le funzionalità di sicurezza informatica**
   Investi in avanzati strumenti e tecnologie di sicurezza informatica, aggiorna regolarmente le procedure di sicurezza e implementa robusti programmi per la gestione dei rischi per stare al passo con le minacce emergenti.
2. **Sviluppare programmi di conformità completi**
   Implementa robusti programmi di conformità corrispondenti alle linee guida dettate dalla NIS 2, come piani dettagliati di risposta agli incidenti, regolari audit di sicurezza e documentazione completa delle prassi per la sicurezza.
3. **Coinvolgere il comparto management senior**
   Fai in modo che questo reparto sia attivamente coinvolto nelle iniziative per la sicurezza informatica, tramite una regolare formazione e aggiornamenti tempestivi per informarlo circa le ultime minacce e i requisiti di conformità. Questo vale per gli MSP come per i relativi clienti. Secondo la NIS 2, il management e l'alta dirigenza sono responsabili in modalità probabilmente ignote e sta agli MSP informare questi comparti. Gli MSP devono utilizzare a proprio vantaggio questa nuova pressione esterna per favorire l'adozione dei servizi di sicurezza informatica.
4. **Identificare i clienti essenziali e quelli importanti**
   Classifica gli attuali clienti e prepara opportune campagne di marketing o programmi di promozione appositamente per loro. Se i clienti che si classificano come soggetti essenziali o importanti non hanno ancora discusso con il proprio MSP della direttiva NIS 2, essi non sono forse a conoscenza dei requisiti di conformità ancora da implementare o probabilmente si sono già rivolti ad altri fornitori. Se l'MSP non tiene sotto controllo questo aspetto, probabilmente lo farà qualcun altro.
5. **Rafforzare la sicurezza della supply chain**
   Conduci un'adeguata dovuta diligenza circa fornitori e partner, stabilendo chiare aspettative in materia di sicurezza informatica e integrandole nei contratti che sottoscrivi e negli accordi sul livello di servizio. Gli MSP devono inoltre prepararsi al fatto che anche i clienti esistenti e potenziali facciano lo stesso. Prepara un'adeguata documentazione e falla controllare dal tuo consulente legale, così che sia pronta quando ti occorre. La necessità di giorni o settimane per preparare la documentazione non sarà un punto a favore per l'MSP e potrebbe comportare la perdita del cliente.

6. **Sfruttare a proprio vantaggio le opportunità commerciali**
   Metti in evidenza la conformità alla NIS 2 nelle campagne di marketing e commerciali per diventare un partner affidabile per i soggetti che vogliano rispettare i requisiti della NIS 2.

7. **Favorire la collaborazione all'interno del settore**
   Partecipa ai forum e collabora con altri MSP ed esperti di sicurezza informatica, condividendo approfondimenti e best practice per migliorare l'approccio generale alla sicurezza.

Conclusioni

La direttiva NIS 2 rappresenta un miglioramento sostanziale del framework per la sicurezza informatica in UE. Per i provider di servizi gestiti comporta complessità da un lato, ma anche opportunità commerciali. Migliorando in modo proattivo le capacità di sicurezza informatiche, sviluppando programmi completi di conformità e collaborando con il settore, gli MSP non solo potranno conformarsi alla direttiva, ma anche sfruttarla come vantaggio competitivo sul mercato. Via via che le minacce informatiche continuano ad evolvere, gli MSP che danno priorità alla sicurezza informatica saranno pronti a supportare adeguatamente i clienti e a contribuire alla creazione di un ecosistema digitale più sicuro.

La presente analisi sottolinea il ruolo essenziale ricoperto dagli MSP nel panorama informatico e mette in luce l'importanza di adattarsi ai nuovi requisiti normativi per assicurare una crescita e un successo continui. L'adozione della NIS 2 non rappresenta un mero ostacolo normativo, ma un vero e proprio stimolo per gli MSP, che con essa dovranno migliorare le proprie prassi di sicurezza informatica e diventare partner affidabili per i propri clienti.

Riferimenti

- Bohlin, C.-O (5 marzo 2024) Nya regler om cybersäkerhet, SOU 2024:18. Recuperato da Regeringskansliet: https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf
- ENISA (12 giugno 2024) Another step forward towards responsible vulnerability disclosure in Europe. Recuperato dall'Agenzia dell'Unione europea per la cibersicurezza: https://www.enisa.europa.eu/news/another-step-forward-towards-responsible-vulnerability-disclosure-in-europe
- Parlamento europeo (6 luglio 2016) Direttiva 2016-1148 - EN - EUR-Lex. Recuperata da EUR-Lex: https://eur-lex.europa.eu/eli/dir/2016/1148/oj
- Parlamento europeo (2022, 12 27) EUR-Lex - 02022L2555-20221227 - EN. Recuperata da EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227
- Forsvarsministeriet (6 febbraio 2024) Implementation of NIS2 Directive is Delayed. Recuperato da AmCham Denmark: https://amcham.dk/news/implementation-of-nis2-directive-is-delayed/
- République Française (30 aprile 2024) Transposition Nationale. Recuperato da MonEspaceNIS2 BÊTA: https://aide.monespacenis2.cyber.gouv.fr/fr/article/quel-est-le-calendrier-global-de-la-transposition-de-la-directive-144kxte/

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e a espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore. n-able.com/it

---