Le certificazioni per le aziende in materia di sicurezza informatica

La direttiva NIS2

Che cos'è la direttiva NIS2?

Proposta per la prima volta nel 2020 e implementata il 16 gennaio 2023, **NIS2 è l'acronimo di Network and Information Security 2**, ufficialmente nota come Direttiva (UE) 2022/2555. La Commissione Europea (UE) ha proposto che la NIS2 si basi sulla direttiva NIS originaria, o direttiva (UE) 2016/1148, correggendone le carenze. La direttiva NIS2 mira a migliorare la sicurezza informatica nell'UE e prepara le aziende ad essere pronte per qualsiasi potenziale minaccia informatica.
Gli Stati membri dell'UE devono recepire la direttiva NIS2 nel loro diritto nazionale entro il 17 ottobre 2024 e le misure inizieranno a entrare in vigore il 18 ottobre 2024.
Nel white paper di Eversheds Sutherland si racconta che la nuova legislazione aiuterà circa 160.000 entità a migliorare la sicurezza, rendendo l'Europa un luogo sicuro in cui vivere e lavorare.

Perché è entrata in vigore la NIS2?

Considerando l'aumento delle minacce informatiche come phishing, software dannosi e attacchi DoS, diversi governi in tutto il mondo hanno applicato normative sulla sicurezza informatica. Nell'agosto 2016, l'UE ha introdotto la direttiva NIS, un regolamento volto a migliorare la capacità degli Stati membri di gestire gli attacchi informatici. Inizialmente, l'attenzione si è concentrata sulla segnalazione degli incidenti e sull'implementazione di misure informatiche. La direttiva NIS si applicava a due gruppi: gli operatori di servizi essenziali e i fornitori di servizi digitali che erano pertinenti.
Ciononostante, la direttiva NIS iniziale ha incontrato numerosi ostacoli nel suo obiettivo di migliorare gli standard di sicurezza informatica delle nazioni dell'UE. Questi ostacoli includono implementazioni fallite, sforzi non costanti e standard/requisiti diversi. La recente digitalizzazione, accelerata dalla pandemia globale, ha inevitabilmente alimentato la crescita delle minacce informatiche. Pertanto, per affrontare meglio tali attacchi e garantire una Cyber Sicurezza uniforme in tutti gli Stati dell'UE, è emersa la richiesta di migliorare la direttiva NIS.

Qual è la differenza tra NIS e NIS2?

Come accennato in precedenza, la NIS2 è un'espansione della direttiva NIS originale. L'ultima direttiva succede alla precedente in termini di copertura più ampia, con obblighi e sanzioni più severe. Mira inoltre ad appianare la differenza nell'attuazione e nella segnalazione informatica tra gli Stati dell'UE.
Inoltre, NIS2 rafforza le normative per l'adesione alla sicurezza informatica, comprendendo la segnalazione iniziale obbligatoria degli incidenti, una gestione del rischio ampliata e un ruolo appena definito della responsabilità della sicurezza informatica di livello C.

Cosa c'è di nuovo nel NIS2?

1) Requisiti più severi

Per preparare meglio gli Stati dell'UE contro le minacce informatiche, la direttiva NIS2 ha incluso nuovi requisiti organizzativi estesi in quattro aree. Le aree sono la gestione del rischio, la responsabilità aziendale, gli obblighi di rendicontazione e la continuità aziendale.

1) **Gestione del rischio:** NIS2 richiede alle aziende di adottare misure di sicurezza per ridurre i rischi informatici. Alcune misure includono una maggiore sicurezza della rete e della catena di approvvigionamento, un migliore controllo degli accessi e la crittografia.
2) **Responsabilità aziendale:** Le aziende devono formare le autorità competenti per supervisionare, approvare le misure di sicurezza e affrontare e mitigare i rischi informatici.
3) **Obblighi di segnalazione:** Con la nuova direttiva entrano in vigore obblighi di comunicazione più semplici. Le entità nell'ambito della NIS2 dovrebbero essere in possesso di una tempestiva segnalazione degli incidenti. Inoltre, l'ultima direttiva impone termini di notifica specifici, come un "allarme rapido" di 24 ore.
   Le organizzazioni devono inviare un avviso all'autorità competente o al team di risposta agli incidenti di sicurezza informatica (CSIRT) entro 24 ore. Questo avviso dovrebbe comprendere ipotesi preliminari sull'incidente.
   Un report completo deve essere inviato dopo 72 ore (circa 3 giorni). Questo rapporto dovrebbe incapsulare la valutazione dell'evento, la sua gravità, gli impatti e gli indicatori di compromissione. Dopo un mese, deve essere trasmessa una relazione finale.
4) **Continuità aziendale:** La conformità NIS2 include anche la pianificazione della continuità aziendale anche a fronte di gravi incidenti informatici. Ciò include il ripristino del sistema, le procedure di emergenza e la creazione di team di risposta agli incidenti di sicurezza.

2) Copertura più ampia

La direttiva NIS ha iniziato con 7 settori considerati infrastrutture critiche, ma la nuova direttiva ne include altri 8, per un totale di 15. NIS2 divide i settori in due entità: Essential Entity (EE) e Important Entity (IE). Alcuni di questi includono infrastrutture digitali come fornitori di servizi cloud, spazio, energia, produzione, salute e finanza.

3) Misure minime

Oltre ai severi requisiti, NIS2 richiede che le organizzazioni dispongano di misure minime di sicurezza informatica. Ciò include l'esecuzione di risk assessments, l'esecuzione di backup, la formazione per la sicurezza informatica, l'utilizzo dell'autenticazione a più fattori, l'utilizzo della crittografia e dell'encryption e altro ancora.

4) Sanzioni elevate

Per promuovere sanzioni coerenti in tutti gli Stati membri dell'UE, la NIS2 ha introdotto nuove norme uniformi. Le organizzazioni dell'UE che non rispettano la direttiva NIS2 possono essere soggette a tre tipi di sanzioni. Queste sanzioni includono rimedi non monetari, sanzioni amministrative e sanzioni penali.
Le entità essenziali (Essential Entities – EE) possono incorrere in sanzioni amministrative fino a 10 milioni di euro o al 2% del loro fatturato annuo globale, a seconda di quale sia il valore più alto. Le entità importanti (Important Entities – IE) possono incorrere in una multa fino a 7 milioni di euro o all'1,4% delle loro entrate annuali, a seconda di quale sia il valore più alto.

A chi si applica la NIS2?

Insieme ai 7 settori della precedente direttiva, la NIS2 è applicabile a 15 settori, classificati come entità essenziali e importanti. La divisione si basa sulla criticità del settore e sulla dimensione organizzativa.

– Entità Essenziali (Essential Entities – EE)

NIS2 classifica 8 categorie come Entità Essenziali. Si tratta di **Energia, Trasporti, Finanza, Pubblica Amministrazione, Sanità, Spazio, Approvvigionamento idrico e Infrastrutture digitali**. NIS2 è

applicabile alle organizzazioni di questi settori con oltre 250 dipendenti, un fatturato annuo di almeno 50 milioni di euro o uno stato patrimoniale di almeno 43 milioni di euro.

– Entità Importanti (Important Entities – IE)

7 settori rientrano tra gli Enti Importanti. Sono i **servizi postali, la gestione dei rifiuti, i prodotti chimici, la ricerca, gli alimenti, la produzione e i fornitori digitali**. La NIS2 si applica alle imprese di questi settori con un numero di dipendenti compreso tra 50 e 250 e un fatturato annuo non superiore a 50 milioni di euro o uno stato patrimoniale non superiore a 43 milioni di euro.

Come prepararsi alla direttiva NIS2?

- **Riconoscimento dei processi critici:** Per prepararti alla direttiva NIS2, inizia identificando i processi importanti delle aziende che potrebbero essere attaccati. È necessario implementare solide misure di sicurezza per garantire la sicurezza di tali processi. Misure di sicurezza informatica di prim'ordine dovrebbero proteggere la rete e i sistemi informativi dell'azienda.
- **Anticipazione e preparazione:** Sebbene sia impossibile prevedere gli attacchi futuri, le aziende possono anticipare eventuali minacce potenziali in base alla cronologia precedente. Sulla base di questi dati, possono costruire una difesa informatica abbastanza forte da mitigare tali attacchi. Qualsiasi possibile punto vulnerabile, come i dispositivi remoti endpoint, deve essere identificato e protetto.
- **Educazione e consapevolezza:** La sicurezza informatica di un'organizzazione è responsabilità di tutti coloro che sono al suo interno. Tutti devono essere a conoscenza degli attacchi informatici, delle misure di sicurezza e dei piani di emergenza. Pertanto, la dirigenza deve assicurarsi che tutti siano ben addestrati in materia di sicurezza informatica, come per esempio sulla gestione e sulla segnalazione degli incidenti in modo tempestivo.

L'Art. 32 del GDPR

Art. 32 del GDPR: procedura obbligatoria di valutazione

In diversi punti il GDPR lascia intendere che il titolare del trattamento deve definire delle procedure per rispondere ai requisiti di protezione dei dati personali. L'unico caso, però, in cui il testo di legge parla esplicitamente di "procedura" è all'articolo sulla sicurezza del trattamento. **L'art. 32 del GDPR**, al comma 1 lettera d), richiede al titolare di definire **una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative**.

Che cosa non è la procedura dell'art. 32 del GDPR

La procedura di valutazione dell'efficacia non è né la verifica della conformità normativa **né** l'attività di controllo **prevista dall'art. 39 a carico del DPO. Non ha quindi come obiettivo quello di verificare che il trattamento dei dati avvenga nel rispetto dei requisiti di legge e non è un'attività riservata alle sole realtà che dispongano, per scelta o per obbligo, del DPO.**

Questa procedura non ha nemmeno a che vedere con l'**aggiornamento del registro dei trattamenti o dell'analisi dei rischi**, e non equivale all'esecuzione di verifiche/**audit regolari**.

A che cosa serve la procedura dell'art. 32 del GDPR?

Si tratta di un obbligo che si applica al titolare del trattamento (o al responsabile) e ha come obiettivo quello di testare, verificare e valutare l'efficacia delle misure **definite dall'organizzazione. Questo significa che:**

1) la procedura deve essere in grado di dimostrare che le misure tecniche e organizzative consentono di **raggiungere l'obiettivo di protezione dei dati personali** trattati dall'organizzazione;
2) il titolare ha la possibilità di fare un **bilanciamento** (valutazione) delle misure rispetto agli interessi e al rischio che deve gestire, per cui la procedura serve per valutare se non siano **troppo rigide o dispendiose le misure in atto o se, al contrario, non sia opportuno un loro rafforzamento**;
3) l'attività di test, verifica e valutazione deve essere effettuata con **regolarità**. Questa regolarità deve essere **definita in funzione dell'esposizione al rischio** connesso al trattamento dei dati, con una frequenza crescente al crescere dell'esposizione. Tenendo presente che quest'ultima cresce sia in funzione della tipologia e della quantità di dati trattati, sia in funzione della variabilità del contesto interno o esterno (es. rapidità con cui è necessario apportare modiche tecnologiche o documentali).

In che cosa consiste questa procedura

Per chi ha famigliarità con i sistemi di gestione, può essere utile paragonare la procedura dell'art. 32 del GDPR all'attività di monitoraggio mediante indicatori di prestazione**. Si tratta quindi di individuare degli aspetti che si ritengono essere capaci di rappresentare lo stato della situazione nel tempo, di avere in ogni istante il polso della situazione.**
Gli indicatori sono valori numerici espressi in termini relativi (percentuali) in modo che si possa valutare un dato evento in funzione della massa complessiva di dati/eventi che si stanno considerando. Per ciascun indicatore vengono definiti dei valori di riferimento **rispetto ai quali risulti possibile stabilire se la situazione procede in modo sostenibile o se si stanno registrando degli scostamenti potenzialmente problematici.**

Un esempio di indicatore

La sicurezza informatica è un aspetto importante di ogni realtà aziendale. La scelta dei sistemi informatici **è il primo passo per la protezione dei dati personali trattati digitalmente. Testarne, verificarne e valutarne l'efficacia significa in questo caso valutare** quanti tentativi di hackeraggio il sistema è stato capace di rilevare, affrontare e impedire**. Così facendo, oltre a dimostrare che il processo di gestione della privacy è effettivo, si può anche rilevare la causa di un eventuale problema, distinguere tra** problematiche strutturali **(es. in caso di incapacità del sistema di neutralizzare gli attacchi)** e problematiche di investimento **(es. in caso di una spesa ingente rispetto al numero di attacchi registrati), aggiustando il tiro delle misure tecniche e organizzative messe in atto.**

La certificazione ISO/IEC 27001:2022

ISO 27001: definizione e contenuto

La certificazione ISO 27001 è uno standard internazionale che definisce le migliori pratiche per un sistema di gestione della sicurezza delle informazioni (SGSI)**. Questo articolo ti guiderà attraverso tutto ciò che devi sapere sulla ISO 27001, dai suoi vantaggi alla sua implementazione.**

Che cos'è la ISO/IEC 27001

ISO 27001 è uno standard che descrive come creare, mantenere e sviluppare un sistema di gestione della sicurezza delle informazioni (in inglese ISMS, Information Security Management System**). È promosso dalla** ISO (International Organization for Standardization) **e dalla** IEC (International Electrotechnical Commission) **e si compone di un insieme di best practices per la sicurezza delle informazioni che hanno l'obiettivo di proteggere i dati dei clienti e garantire la sicurezza delle informazioni.**
Questa norma fornisce un approccio completo alla sicurezza delle informazioni, coprendo tutti gli aspetti, dai documenti digitali a quelli cartacei, dalle apparecchiature hardware alle competenze del personale.

Perché ottenere una certificazione ISO 27001?

L'implementazione del framework di sicurezza delle informazioni specificato nella norma ISO/IEC 27001 ti aiuta a:

- ridurre la vulnerabilità alla crescente minaccia degli **attacchi hacker**
- rispondere ai rischi di **cybersecurity** in evoluzione
- fornire un framework gestito centralmente che protegge tutte le informazioni in un unico luogo
- garantire che beni come bilanci, proprietà intellettuale, dati dei dipendenti e informazioni affidate da terze parti rimangano integri, confidenziali e disponibili all'occorrenza
- proteggere le informazioni in tutte le forme, incluso il formato cartaceo, basato su cloud e dati digitali
- preparare persone, processi e tecnologia in tutta la tua organizzazione ad affrontare rischi legati alla tecnologia e altre minacce
- risparmiare denaro aumentando l'efficienza e riducendo le spese per la tecnologia di difesa inefficace

Quali sono i principi dell'ISO/IEC 27001

I tre principi dell'information security su cui si basa il framework ISO/IEC 27001 sono conosciuti come la triade CIA:

- **Confidentiality – confidenzialità**: solo le persone autorizzate possono accedere alle informazioni detenute dall'organizzazione
- **Information integrity – integrità delle informazioni**: i dati che l'organizzazione utilizza per perseguire i suoi affari o mantiene al sicuro per altri sono conservati in modo affidabile e non vengono cancellati o danneggiati
- **Availability of Data – Disponibilità dei dati**: l'organizzazione e i suoi clienti possono accedere alle informazioni ogni volta che è necessario, in modo che gli scopi aziendali e le aspettative dei clienti siano soddisfatti.

I vantaggi del miglioramento continuo con l'ISO 27001

L'ISO 27001 garantisce un miglioramento continuo dei sistemi di gestione della sicurezza delle informazioni. Questo significa che le aziende certificate devono dimostrare di migliorare continuamente il loro ISMS. Ogni anno, queste aziende devono partecipare a un processo di revisione esterna mentre ogni tre anni si svolge una revisione della certificazione per mantenerne la conformità.

Quali sono i controlli più importanti previsti dall'ISO 27001?

I controlli più importanti variano a seconda delle peculiarità dell'organizzazione. Tuttavia, l'ISO 27001 fornisce indicazioni precise su diritti di proprietà intellettuale, salvaguardia delle registrazioni del sistema organizzativo, protezione dei dati e tutela della privacy**, politica documentata e suddivisione delle responsabilità per la sicurezza delle informazioni, sensibilizzazione e formazione del personale, rendicontazione degli incidenti e gestione della business continuity.**

Conclusione

L'ISO 27001 è uno standard fondamentale per la gestione della sicurezza delle informazioni. Con il suo aiuto, le aziende possono proteggere le informazioni dei clienti, rispettare i requisiti legali, espandere il business e proteggere la loro reputazione. Implementare un ISMS secondo l'ISO 27001 richiede un impegno significativo, ma i benefici che ne derivano sono enormi**.**

In che modo Azienda Digitale può aiutare la tua organizzazione con le certificazioni

Azienda Digitale informatica e servizi in partnership/collaborazione con aziende specializzate nelle soluzioni di sicurezza informatica e infrastrutture, assiste le aziende nell'acquisire le certificazioni menzionate in questo documento, dall'Art 32 del GDPR alla direttiva NIS2, alla ISO 27001, offrendo una suite completa di soluzioni di sicurezza. Questi includono:

- Test di sicurezza informatica White Box, Grey Box e Black Box
- Zero Rischi - Test non invasivi, Operazioni non intrusive
- Test periodici, personalizzabili in base alle vostre esigenze
- Test su Applicazioni web, reti aziendali, indirizzi IP pubblici
- Verifica degli hash delle password
- Conformità agli standard di classificazione CVE/CWE/CVSS
- Report con dettagli delle vulnerabilità
- Rapporto dettagliato sulle criticità rilevate
- Test Verificato da Certified Penetration Tester
- Report accettato come prova documentale ISO/IEC 27001:2022
- Certificazione valida per Art .32 GDPR
- Certificazione valida per la direttiva NIS2

L’integrazione di questi servizi fornisce un solido ecosistema di sicurezza. Questa integrazione è in linea con i requisiti delle certificazioni rilasciate da enti competenti e accreditate per una gestione completa del rischio. Essa aiuta le aziende a ottenere informazioni in tempo reale su potenziali rischi come vulnerabilità, errori di configurazione e password deboli, che sono obiettivi primari per le minacce informatiche.
Utilizzando i servizi e le nostre soluzioni offriamo un rilevamento preciso e rapido delle minacce. La natura interconnessa di questi servizi consente una risposta automatizzata e coordinata, riducendo significativamente l’impatto degli incidenti di sicurezza e supportando l’enfasi posta dalla direttiva NIS2, GDPR e ISO/27001 sulle strategie di sicurezza proattive e reattive.
Le tecnologie a disposizione migliorano anche il rilevamento delle minacce correlando i dati tra diversi livelli di sicurezza, fornendo un contesto dettagliato per gli eventi della rete. Questa funzione è anche fondamentale per adempiere agli obblighi di comunicazione completi delle certificazioni rilasciate, mentre gli strumenti di segnalazione integrati aiutano a generare i report necessari per la conformità delle normative di legge.

Siamo disponibili per maggiori informazioni o per organizzare video call con i responsabili della Cyber Security che effettueranno i test.

CORRADO CORBELLA

AZIENDA DIGITALE
INFORMATICA E SERVIZI
&
DIGITAL MARKETING

AZIENDA
DIGITALE
INFORMATICA E SERVIZI
&
DIGITAL MARKETING