La direttiva NIS2: cosa bisogna sapere e come prepararsi

Contenuti

Che cos'è la NIS2?

Poiché le minacce alla sicurezza informatica si evolvono e pongono rischi sempre maggiori per individui e aziende, le normative si evolvono continuamente per tenere il passo con le minacce e aumentare gli standard minimi di sicurezza. La NIS2 (Network and Information Security version 2), l'ultima direttiva dell'Unione Europea in materia, rappresenta uno sviluppo significativo in questo ambito.

Espansione e rafforzamento della direttiva NIS (2016) precedente, la NIS2 rappresenta una revisione significativa del panorama normativo dell'UE in materia di sicurezza informatica, con l'obiettivo di rafforzare il livello generale di resilienza informatica negli Stati membri e delle entità che operano con essi. La direttiva estende l'ambito di applicazione della direttiva NIS originaria, ampliando la gamma di settori e tipi di entità che ricadono sotto la sua giurisdizione, compresi quelli che si ritiene svolgano un ruolo "essenziale" e "importante" nel mercato interno dell'UE.

Per queste organizzazioni, la NIS2 rappresenta un passo avanti nella conformità alla sicurezza: si troveranno per la prima volta incluse nell'ambito di applicazione della normativa o saranno tenute a rispettare standard (e incorreranno in sanzioni) molto più elevati rispetto alla direttiva precedente.

La NIS2 introduce obblighi più significativi, richiedendo alle entità di adottare meccanismi completi di segnalazione degli incidenti, solide pratiche di gestione del rischio, misure di responsabilità aziendale e strategie efficaci di continuità operativa. È significativo che la direttiva NIS2 introduca anche conseguenze importanti in caso di non conformità, tra cui multe sostanziali e il rischio di controversie legali.

Essendo una direttiva UE, la NIS2 sarà soggetta a variazioni nell'attuazione da parte degli stati membri. Questo aggiungerà probabilmente un livello di complessità per le imprese che operano a livello transfrontaliero all'interno dell'UE. Tuttavia, il messaggio è chiaro: la preparazione non è negoziabile. Le organizzazioni di tutta l'UE devono adottare misure proattive per comprendere il regolamento, valutarne le implicazioni per le loro attività e sviluppare un piano d'azione per garantire la conformità.

Chi è interessato dalla NIS2?

La NIS2 espande in modo significativo la portata della regolamentazione rispetto alla direttiva precedente, creando una rete molto più ampia che coinvolge una serie di settori ritenuti critici per il mercato internazionale dell'UE.

Questo ampliamento non riguarda solo i settori considerati direttamente critici, ma include anche gli ambiti che fanno parte della catena di fornitura di questi settori, aumentando il numero di aziende e di settori che ora sono sottoposti a un controllo normativo.

Uno sviluppo fondamentale della NIS2 è la classificazione delle entità in due categorie: 'essenziale' e 'importante'. Questa distinzione influisce sulla portata della direttiva e sulle implicazioni per i diversi tipi di organizzazioni.

Entità essenziali

Questa categoria, riconosciuta anche come NIS, comprende settori fondamentali per il benessere sociale ed economico. Tra questi vi sono i trasporti, i servizi finanziari, la sanità e le società di servizi come i fornitori di energia.

Per queste entità, la NIS2 riafferma la loro decisività e aumenta i requisiti di conformità. Ad esempio, la segnalazione degli incidenti deve avvenire entro 24 ore: rispetto alla direttiva precedente, si tratta di un aggiornamento importante.Il cambiamento più significativo per queste aziende è l'introduzione di multe e conseguenze sostanziali in caso di non conformità. Di conseguenza, le regole sono cambiate e la posta in gioco non è mai stata così alta.

Industrie di infrastrutture essenziali o critiche:

Settore Bancario

Affari e finanza

Infrastruttura digitale

Acqua Potabile

Energia

Settore Sanitario

Pubblica Amministrazione

Spazio

Trasporto

Acque Reflue

Entità importanti

Le entità "importanti" sono una novità assoluta della NIS2, il che significa che per la prima volta la direttiva riguarderà queste organizzazioni. Settori come le infrastrutture digitali, la pubblica amministrazione e il settore manifatturiero devono adeguare e sottoporre rapidamente a audit le proprie prassi di sicurezza informatica.

Data l'ampiezza dei requisiti e le tempistiche più brevi, questo potrebbe rappresentare una sfida iniziale più impegnativa. La buona notizia per queste entità è che la direttiva impone obblighi meno stringenti rispetto a quelli per le organizzazioni classificate come "essenziali", con minori ripercussioni potenziali in caso di non conformità. Tuttavia, la necessità di prepararsi non deve essere sottovalutata.

In breve, la direttiva NIS2 amplia il campo di applicazione della normativa, coprendo un maggior numero di settori e introducendo un sistema di classificazione che determina il livello dei requisiti e delle potenziali sanzioni. Per capire come prepararsi per la NIS2, le organizzazioni devono comprendere in quale classificazione rientrano per sapere cosa ci si aspetta da loro e le possibili conseguenze.

Industrie importanti:

Chimica

Digital Provider

Food

Produzione

Servizi Postali

Ricerca

Gestione Dei Rifiuti

Che cosa significa la NIS2 per le organizzazioni

Quando le organizzazioni comprendono se (e dove) rientrano nell'ambito di applicazione della NIS2, il passo successivo è quello di fare chiarezza sulle implicazioni della direttiva, compresi gli ampi requisiti organizzativi, le dieci misure minime di cybersecurity e le conseguenze specifiche in caso di non conformità.

Introduzione di conseguenze maggiori

La direttiva NIS2 introduce sanzioni molto più severe rispetto alla versione precedente. In alcuni ambiti sono state introdotte sanzioni minime, mentre in altri sono state aumentate. Vale la pena notare, tuttavia, che gli Stati membri hanno la facoltà di stabilire sanzioni ancora più elevate.

- **Entità essenziali:** Queste organizzazioni rischiano sanzioni amministrative fino a 10 milioni di euro o almeno il 2% del fatturato mondiale totale annuo dell'esercizio precedente dell'azienda a cui appartiene l'entità, a seconda di quale sia il valore più alto.
- **Entità importanti:** Per queste entità, sono previste sanzioni amministrative fino a 7 milioni di euro o almeno l'1,4% del fatturato mondiale totale annuo dell'esercizio precedente, a seconda di quale sia il valore più alto.

Requisiti organizzativi ampi

La NIS2 prevede un approccio globale alla sicurezza informatica, che comprende una serie di responsabilità organizzative:

Obbligo di diligenza

Le organizzazioni sono tenute a implementare solide misure di gestione del rischio per ridurre al minimo i rischi informatici. Ciò include la gestione degli incidenti, la protezione della catena di approvvigionamento, il miglioramento della sicurezza della rete e del controllo degli accessi e l'impiego della crittografia, ove necessario. Una parte fondamentale di questo aspetto, specificamente richiamata nella direttiva, è garantire la **continuità aziendale** in caso di incidenti informatici significativi. Questo include il ripristino del sistema, le procedure di emergenza e la creazione di un team di risposta alle crisi.

Obbligo di segnalazione

Le entità essenziali sono tenute a stabilire processi per la segnalazione tempestiva di incidenti di sicurezza significativi, con scadenze di notifica specifiche, come un sistema di "allerta precoce" di 24 ore. La NIS2 enfatizza inoltre in modo significativo la **responsabilità aziendale**, richiedendo al management un coinvolgimento attivo e la competenza in materia di misure di cybersecurity dell'organizzazione. Il management può incorrere in sanzioni in caso di violazione, tra cui la responsabilità e il potenziale divieto temporaneo di ricoprire ruoli dirigenziali.

Dieci misure minime

La direttiva delinea dieci misure minime di sicurezza informatica che le organizzazioni devono adottare per conformarsi ai suoi requisiti:

1. Condurre valutazioni del rischio e stabilire politiche di sicurezza per i sistemi informativi.
2. Sviluppare politiche e procedure che aiutino a migliorare l'efficacia delle misure di sicurezza.
3. Implementare politiche e procedure per l'utilizzo della crittografia e della cifratura, se del caso.
4. Definire un piano per la gestione degli incidenti di sicurezza.
5. Garantire la sicurezza nell'approvvigionamento, nello sviluppo e nel funzionamento dei sistemi, compresa la segnalazione delle vulnerabilità.
6. Fornire formazione sulla sicurezza informatica e mantenere le pratiche di igiene informatica di base.
7. Implementare le procedure di sicurezza per i dipendenti che accedono ai dati sensibili, comprese politiche di accesso ai dati e gestione delle risorse.
8. Gestire le operazioni aziendali durante e dopo un incidente di sicurezza, garantendo backup aggiornati e accesso ai sistemi IT.
9. Utilizzare l'autenticazione a più fattori, le soluzioni di autenticazione continua e la crittografia vocale, video e del testo.
10. Proteggere le catene di approvvigionamento, valutando le vulnerabilità e i livelli complessivi di sicurezza di tutti i fornitori.

Sebbene i requisiti generali e le dieci misure minime diano alle aziende una buona indicazione su dove indirizzare le proprie politiche per prepararsi alla NIS2, come per ogni normativa, il diavolo si nasconde nei dettagli. È essenziale rivedere completamente la direttiva o collaborare con un partner che ne conosca i dettagli. In particolare, la sfida di monitorare le variazioni tra i diversi Stati membri sarà fondamentale per garantire la conformità, soprattutto per le aziende che lavorano in diversi Paesi europei.

Fare ordine

Le organizzazioni devono prepararsi in modo proattivo mentre la direttiva NIS2 prende forma nell'Unione Europea. Questa sezione illustra i passi fondamentali da compiere.

Comprendere la direttiva

Come per la maggior parte dei progetti aziendali, è necessario iniziare con un piano dettagliato e valutare ciò che attualmente è in atto e dove è necessario arrivare.

Campo di applicazione e classificazione - Iniziate determinando se la NIS2 si applica alla vostra organizzazione e, in caso affermativo, se siete classificati come entità "importante" o "essenziale". Ciò determinerà l'entità dei requisiti da soddisfare.

Revisione e audit - Esaminate accuratamente i requisiti della NIS2 e le dieci misure minime. Verificate il vostro assetto attuale, i processi e la tecnologia di cybersecurity rispetto a questi standard per identificare le aree da migliorare.

Ottenete il coinvolgimento

I team IT e di conformità non possono soddisfare i requisiti della NIS2 da soli: è necessario un lavoro di squadra. Dalle fasi iniziali di pianificazione a quelle di revisione e manutenzione, assicuratevi che tutte le parti interessate abbiano un posto al tavolo.

Collaborazione tra team - L'implementazione delle misure e dei processi di sicurezza necessari richiede la collaborazione e il coinvolgimento di tutti i livelli dell'organizzazione. Il sostegno della leadership

è fondamentale per avviare il cambiamento e perché la NIS2 affida alla direzione aziendale la responsabilità della cybersecurity. I team IT, di sicurezza e operativi devono inoltre collaborare per implementare efficacemente le misure di sicurezza, backup e crittografia.

Formazione organizzativa - Oltre alla leadership, l'adesione alla NIS2 implica la formazione dell'organizzazione per aggiornare le pratiche di sicurezza in linea con la misura minima 6. È fondamentale che questa formazione non sia un'azione una tantum, ma un processo continuo che aiuti a mantenere la consapevolezza delle responsabilità a lungo termine, che si evolva nel tempo e che permetta di inserire efficacemente i nuovi dipendenti.

Obbligo di diligenza

Per soddisfare i requisiti dell'"obbligo di diligenza" della NIS2 è necessario un audit approfondito del rischio di sicurezza in tutta l'organizzazione. Questo include l'archiviazione dei dati, l'accesso ai dati, la sicurezza e la scansione delle vulnerabilità.

Gestione e igiene dei dati - Garantite buone pratiche di gestione dei dati, come l'etichettatura dei dati, la loro localizzazione appropriata, l'archiviazione sicura e i backup. È importante estendere l'obbligo di diligenza anche ai backup. Ciò include la disponibilità di backup immutabili (che non possono essere presi di mira o modificati da attacchi come il ransomware) e la conservazione di più copie dei dati in caso di errori.

Misure di sicurezza - Valutate e garantite costantemente l'adozione di misure di sicurezza adeguate, soprattutto per il personale che accede a dati sensibili o importanti. Incorporate framework zero-trust, crittografia e cifratura e garantite che tutti i sistemi (di terze parti e di prima parte) siano sicuri e sottoposti a regolari scansioni delle vulnerabilità. Implementate solide misure di sicurezza per i fornitori della catena di fornitura e adottate l'autenticazione a più fattori, ove opportuno.

Risposta agli incidenti

La NIS2 richiede un piano completo per gli incidenti di sicurezza che includa il mantenimento delle operazioni e della continuità durante e dopo un incidente. Pertanto, le aziende devono disporre di un team dedicato alla risposta agli incidenti che comprenda gli stakeholder delle diverse unità aziendali per definire un solido processo di risposta agli incidenti sul quale svolgere esercitazioni regolarmente.

Rilevamento delle minacce - Il rilevamento tempestivo degli incidenti, come gli attacchi ransomware che possono violare i sistemi con largo anticipo, è fondamentale. Investite in funzionalità di rilevamento delle minacce, monitoraggio, avvisi e rilevamento di malware per individuare gli incidenti il prima possibile.

Strategia di backup - Assicuratevi che vengano realizzati backup aggiornati, concentrandovi sui dati mission-critical. Si consiglia di seguire la Regola d'oro del backup di Veeam 3-2-1-1-0, che prevede l'esistenza di tre copie dei dati su due diversi supporti, con una copia fuori sede e una da mantenere isolata dall'accesso, immutabile o offline, puntando a zero errori nella verifica del backup e del ripristino.

Risposta e recupero - Sviluppate processi per la segnalazione e la comunicazione degli incidenti durante un incidente. Per quanto riguarda il ripristino, è necessario disporre di processi di disaster recovery per garantire la continuità aziendale. I backup affidabili sono fondamentali, ma un solido processo di ripristino che includa la pianificazione del ripristino in un ambiente separato e sicuro è essenziale per ridurre al minimo i tempi di inattività e i costi associati.

Pianificazione strategica degli ambienti di ripristino - È fondamentale che le organizzazioni prendano in considerazione i loro ambienti di ripristino. Spesso non è possibile effettuare il ripristino nello stesso ambiente in cui si è verificato l'incidente. È essenziale pianificare in anticipo un ambiente di ripristino separato e sicuro. Ad esempio, nel bel mezzo di un incidente di sicurezza non è il momento di integrare per la prima volta un nuovo cloud provider!

Esplorare la NIS2 con Veeam

Con l'introduzione della Direttiva NIS2 da parte dell'Unione Europea, le aziende di vari settori devono rafforzare le loro pratiche di cybersecurity e resilienza.

Ovunque le imprese rientrino nel campo di applicazione della direttiva, prepararsi sarà una nuova sfida: le entità "importanti" navigano in queste acque per la prima volta. Le entità "essenziali", invece, devono soddisfare requisiti ancora più severi rispetto al passato. Nonostante le differenze nell'attuazione dei dettagli e dei requisiti da parte dei diversi Stati membri dell'UE, i principi generali della NIS2 sono abbastanza coerenti da consentire alle organizzazioni di iniziare a prepararsi fin da ora.

Sebbene sia facile considerare questo tipo di obblighi normativi come un inconveniente o un peso, le organizzazioni dovrebbero accettarli. Le pratiche e i requisiti definiti nella NIS2 sono fondamentali per proteggere le aziende dalle crescenti minacce informatiche: le aziende devono orientarsi verso tali pratiche se non fanno già parte del loro assetto di sicurezza.

In che modo Veeam può aiutare

Soddisfare i requisiti della NIS2 è una missione che coinvolge tutta l'organizzazione, da cima a fondo. Per molte aziende, questo richiederà l'implementazione di una serie di nuovi processi e tecnologie.

Anche se non è una soluzione miracolosa, Veeam Data Platform è ben posizionata per aiutare le entità a soddisfare i vari requisiti della NIS2, in particolare per quanto riguarda l'igiene dei dati, la reportistica e l'auditing, il backup dei dati e il disaster recovery. Veeam Data Platform comprende Veeam Backup & Replication, Veeam Recovery Orchestrator e Veeam ONE for Monitoring and Alerting, offrendo una solida base per la protezione delle risorse digitali e il potenziamento della resilienza informatica.

- **Veeam Backup & Replication:** Protegge i dati da perdite e minacce fornendo backup e repliche affidabili per tutti i carichi di lavoro.
- **Veeam Recovery Orchestrator:** Assicura il rapido ripristino dei servizi critici con il disaster recovery automatizzato, la pianificazione e i test.
- **VeeamONE:** Fornisce monitoraggio avanzato, reportistica e pianificazione della capacità per l'ambiente di backup Veeam, migliorando la vostra capacità di mantenere la continuità aziendale e di soddisfare i requisiti di conformità.
- **Veeam Security & Compliance Analyzer:** Garantisce un ripristino efficace con scansioni automatizzate, sfruttando il rafforzamento dell'infrastruttura e le best practice di protezione dei dati.
- **Veeam Threat Center:** Evidenzia le minacce, identifica i rischi e misura il punteggio di sicurezza del vostro ambiente.

Le soluzioni di Veeam sono progettate per essere una parte vitale della vostra cassetta degli attrezzi per la cybersecurity, aiutando la vostra organizzazione ad affrontare le complessità della conformità alla NIS2. Tuttavia, la preparazione per la NIS2 va oltre le capacità di un singolo fornitore: richiede l'impegno per una formazione continua sulla cybersecurity, l'adozione di best practice e la volontà di investire nelle tecnologie e nei processi necessari per proteggersi dalle minacce in evoluzione.

Parla con un esperto Veeam oggi stesso per comprendere come Veeam può aiutare la vostra organizzazione a conformarsi alla NIS2. Scopri come le soluzioni di protezione e gestione dei dati di Veeam possono rafforzare il vostro assetto in materia di cybersecurity, garantire la conformità alla NIS2 e salvaguardare il futuro della tua organizzazione di fronte alle minacce informatiche emergenti.