White Paper

Nuova direttiva NIS2

Dati essenziali e conformità

Introduzione a NIS2

Con l'aumento della frequenza delle minacce digitali e l'evoluzione della sofisticatezza degli attacchi informatici, governi e agenzie internazionali stanno proponendo normative nuove e aggiornate per aumentare la resilienza. Quando viene introdotta una nuova normativa, può essere difficile apprenderla, analizzarla e implementarla prima della data di entrata in vigore.

Se lavori nel settore IT nell'Unione Europea (UE), saprai già che è essenziale per il tuo lavoro scoprire al più presto i dettagli della NIS2 (acronimo per Network and Information Security Directive 2, che assicura un livello elevato in tema di cibersecurity e condiviso in tutta la UE). Abbiamo pensato che potrebbe essere utile fornirti una rapida introduzione a NIS2 per dare il via al tuo percorso di implementazione, in modo da restare al passo con le normative e, soprattutto, un passo avanti agli aggressori.

© 2024 Object First. Informations confidentielles. Tous droits réservés. Toutes les marques commerciales appartiennent à leurs propriétaires respectifs.

Cos'è NIS2?

La direttiva NIS2 mira a rafforzare la sicurezza informatica negli Stati membri dell'UE e in tutte le entità che intrattengono rapporti commerciali con essi. Risponde alle crescenti minacce legate alla digitalizzazione e all'aumento degli attacchi informatici.

NIS2 amplia il campo di applicazione della direttiva NIS originaria con più settori e tipologie di soggetti che rientrano nella sua giurisdizione, compresi quelli ritenuti aventi un ruolo «essenziale» e «importante» nel mercato interno dell'UE. Introduce requisiti più consistenti, tra cui la segnalazione dettagliata degli eventi, le pratiche di gestione del rischio, le misure di responsabilità aziendale e le strategie di continuità operativa.

Rischi di non conformità

La direttiva NIS2 prevede sanzioni sostanziali in caso di non conformità, nonché la possibilità di avviare contenziosi. NIS2 impone agli Stati membri di recepire tali requisiti nella legislazione nazionale entro il 17 ottobre 2024. Anche se l'implementazione potrebbe variare leggermente, è essenziale una preparazione approfondita per tale scadenza.

È necessario comprendere proattivamente la direttiva, identificare gli impatti sulla propria organizzazione e stabilire un piano per raggiungere la conformità.

A questo punto, probabilmente ti starai chiedendo: «Qual è l'impatto su di me?», ma prima devi capire chi sei «tu» e se NIS2 ha un impatto sulla tua organizzazione.

Sono essenziale o importante?

NIS2 suddivide le aziende in due gruppi: "essenziali" e "importanti". La collocazione in questo gruppo ti aiuterà a capire in che modo NIS2 impatterà sulla tua azienda in futuro.

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati.
Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolar

Entità essenziali

NIS2 individua settori cruciali quali i trasporti, i servizi finanziari, l'assistenza sanitaria e le aziende di servizi pubblici (inclusi i fornitori di energia) come «entità essenziali», sottolineandone l'importanza per il benessere sociale ed economico. Rafforza gli obblighi di conformità, in particolare imponendo la segnalazione degli incidenti entro 24 ore, il che rappresenta un inasprimento significativo dei requisiti previsti dalla direttiva precedente. Inoltre, prevede pesanti sanzioni e gravi conseguenze in caso di non conformità, sottolineando la posta in gioco più elevata e il quadro normativo più severo che queste entità devono ora affrontare.

Sei un'entità essenziale se la tua azienda ha più di 250 dipendenti e un fatturato annuo di oltre 50 milioni di euro e rientra in una di queste categorie:

- Infrastruttura digitale
- Energia
- Finanza
- Salute
- Pubblica amministrazione
- Spazio
- Trasporto
- Approvvigionamento idrico (potabile e acque reflue)

Entità importanti

NIS2 introduce una nuova classificazione per le entità «importanti», e amplia il campo di applicazione della direttiva per includere per la prima volta settori come settori quali i servizi postali, la gestione dei rifiuti e la produzione manifatturiera. Questa estensione implica che questi settori debbano valutare e migliorare rapidamente le proprie misure di sicurezza informatica per conformarsi allo standard NIS2. Sebbene le entità «importanti» siano soggette a obblighi e sanzioni meno severi in caso di non conformità rispetto alle loro controparti «essenziali», non bisogna sottovalutare la sfida di soddisfare tali requisiti in tempi relativamente brevi.

Sei un'entità «importante» se la tua azienda ha più di 50 dipendenti e un fatturato annuo fino a 10 milioni di euro e rientra in una di queste categorie (ciò include anche le categorie elencate come essenziali):

- Prodotti chimici
- Alimenti
- Produzione
- Servizi postali
- Ricerca
- Gestione dei rifiuti

L'impatto di NIS2 sulla tua azienda

Se la tua attività rientra nelle categorie «essenziali» o «importanti» elencate, il passo successivo è capire cosa significa NIS2 per la tua organizzazione e quale impatto può avere su di te.

Introduzione

La direttiva NIS2 sottolinea l'importanza di una strategia approfondita per la sicurezza informatica all'interno delle realtà aziendali. Sebbene si tratti di un quadro normativo molto dettagliato raccomandiamo alle imprese interessate all'interno di uno Stato membro di prendersi il tempo necessario per leggere autonomamente gli articoli, abbiamo creato alcuni punti salienti per aiutarti a iniziare la tua valutazione, a partire dalle dieci misure minime di sicurezza informatica evidenziate nella direttiva.

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolari.

Le dieci misure di gestione del rischio per la sicurezza informatica

Una delle sezioni più critiche della direttiva è l’articolo 21, che elenca dieci misure di gestione dei rischi per la sicurezza informatica. Gli Stati membri devono garantire che i soggetti «essenziali» e «importanti» attuino misure tecniche, operative e organizzative idonee a gestire i rischi per la sicurezza delle loro reti e dei loro sistemi informativi utilizzati nelle loro operazioni o nei loro servizi. Tali misure devono prevenire o ridurre al minimo l’impatto degli incidenti sui destinatari dei servizi. Devono tenere conto delle tecnologie più recenti, degli standard pertinenti e dei costi, nonché garantire che il livello di sicurezza sia adeguato al livello di rischio. Nel valutare la proporzionalità delle misure di sicurezza, le organizzazioni devono considerare la loro esposizione al rischio, le loro dimensioni e il potenziale impatto degli incidenti. Ciò include la valutazione della gravità e della probabilità degli incidenti, nonché dei loro effetti sociali ed economici.

La direttiva NIS2 elenca dieci misure di sicurezza informatica che tutte le entità qualificate devono implementare:

1. Politiche sull’analisi dei rischi e sulla sicurezza dei sistemi informatici.
2. Gestione degli incidenti.
3. Processi di continuità aziendale, come la gestione dei backup,, il disaster recovery e la gestione della crisi.
4. Sicurezza della supply chain, inclusi gli aspetti correlati alla sicurezza delle relazioni tra ciascuna impresa e i suoi fornitori diretti o provider di servizi.
5. Sicurezza nell’acquisizione, sviluppo e manutenzione di reti e sistemi informatici, inclusa la gestione e la divulgazione delle vulnerabilità.
6. Politiche e procedure per valutare l’efficacia delle misure di gestione dei rischi relativi alla sicurezza informatica
7. Pratiche base di igiene informatica e formazione sulla sicurezza informatica
8. Politiche e procedure relative all’utilizzo della crittografia e, laddove appropriato, della cifratura
9. Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione delle risorse
10. Soluzioni di autenticazione a più fattori o autenticazione continua, comunicazioni vocali, video e testuali protette e sistemi di comunicazione di emergenza protetti nell’entità, laddove appropriato

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolari.

Obbligo di segnalazione

Un tema ricorrente nell’intera direttiva NIS2 è l’importanza della segnalazione. Le entità «essenziali» sono tenute a predisporre procedure per segnalare rapidamente incidenti significativi di sicurezza informatica, con scadenze specifiche per la segnalazione, incluso un sistema preliminare di «allerta precoce» attivo 24 ore su 24.

NIS2 sottolinea inoltre l’importanza della responsabilità aziendale, richiedendo che il management si impegni attivamente e comprenda gli sforzi dell’organizzazione in materia di sicurezza informatica. I manager potrebbero essere penalizzati per violazioni della sicurezza, rischiando di incorrere in responsabilità e persino in divieti temporanei di ricoprire posizioni manageriali.

Penali

Le nuove norme della Direttiva NIS2 sono molto più severe rispetto al passato e in alcuni casi introducono multe più elevate o del tutto nuove.

Tuttavia, i paesi dell Unione Europea possono decidere di imporre sanzioni ancora più elevate, se lo desiderano. Le aziende considerate «essenziali» devono essere pronte ad incorrere in sanzioni fino a 10 milioni di euro o al 2% dei loro ricavi annui complessivi conseguiti nell’ultimo anno, a seconda di quale sia l’importo più alto. Le aziende considerate «importanti» potrebbero incorrere in multe fino a 7 milioni di euro o all’1,4% dei loro ricavi complessivi conseguiti l’anno precedente, a seconda di quale sia l’importo più alto.

Ma non è finita qui

Queste tre sezioni illustrano un’ampia gamma di aspettative contenute nella direttiva NIS2; tuttavia, non si tratta di un elenco esaustivo. Invitiamo tutte le aziende che operano nell’Unione Europea a esaminare l’intera direttiva e i relativi requisiti con i propri team e a comprendere appieno le aspettative e le implicazioni di questa imponente normativa.

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolari.

Come Object First può essere di aiuto

NIS2 rappresenta un'evoluzione estremamente importante nella regolamentazione della sicurezza e potrebbe rappresentare un notevole passo avanti per garantire la conformità nei data center di entità «importanti» ed «essenziali». Oltre a scrivere questa guida introduttiva, abbiamo pensato di ampliare alcuni dei nostri consigli per aiutarti a raggiungere in modo efficiente i tuoi obiettivi NIS2.

Resilienza dei dati Zero Trust

La sezione 89 dell'introduzione della direttiva NIS2 menziona le imprese che adottano lo Zero Trust per migliorare il loro livello di sicurezza complessivo. Zero Trust è un insieme di principi essenziali per garantire la sicurezza delle app e delle infrastrutture di produzione. Tuttavia, non considera il software di backup e lo storage di backup come parte del suo modello di maturità complessivo.

L'anno scorso, Veeam e Numberline hanno pubblicato la loro ricerca su Zero Trust Data Resilience (ZTDR).
Si tratta di un approccio completo alla protezione dei dati che estende i principi di sicurezza Zero Trust all'ambiente di backup di un'organizzazione. Introduce elementi critici quali la separazione tra software di backup e archiviazione di backup, zone di resilienza multiple e archiviazione di backup immutabile e crittografata. Questo approccio riduce al minimo i rischi, rafforza la protezione dei dati e aumenta il livello di sicurezza di un'organizzazione. Comprendere ZTDR è fondamentale per le organizzazioni poiché fornisce un quadro solido per proteggere i propri dati dalle minacce informatiche, in particolare dagli attacchi ransomware e di esfiltrazione dei dati. Offre un'alternativa più sicura ai modelli di sicurezza tradizionali per quanto riguarda la protezione dei dati e dovrebbe essere parte della checklist di ogni amministratore per quanto riguarda la preparazione a NIS2. Per maggiori informazioni su ZTDR, leggi il nostro whitepaper.

Leggi il whitepaper

Archiviazione dati di backup immutabile

Sorprendentemente, il termine immutabilità non è menzionato nella direttiva NIS2. L'aspetto più importante della protezione dei dati è la capacità di ripristino; con l'archiviazione immutabile, la probabilità di ripristino è molto più alta. Oggi la maggior parte degli attacchi prende di mira innanzitutto l'infrastruttura di backup per eliminare la possibilità di ripristino e garantire il pagamento del riscatto. Le misure di cybersecurity dell'Articolo 21, già citate, menzionano direttamente i requisiti di protezione dei dati, l'igiene della sicurezza informatica e la crittografia. Tuttavia, tutti questi elementi possono essere violati e distrutti. Al contrario, un target di archiviazione immutabile conforme alle best practice ZTDR, come l'impossibilità di accedere al root, un'architettura intrinsecamente segmentata dal software di backup e un'archiviazione che sfrutta il blocco degli oggetti S3 in modalità di conformità, contribuiranno ad aumentare la resilienza a fronte di un attacco.

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolari..

Raggiungere gli obiettivi dei tempi di ripristino

La direttiva contiene numerose affermazioni sull’importanza di una strategia di ripristino, tra cui un piano di ripristino reattivo e la sperimentazione di simulazioni di ripristino prima che si verifichi un cyberattacco.. Raccomandiamo a tutte le organizzazioni interessate dalla normativa NIS2 di prendersi il tempo necessario per valutare i propri attuali ambienti di protezione dei dati e di eseguire scenari di ripristino di prova per valutare meglio i propri reali obiettivi di punto di ripristino (RPO) e obiettivi di tempo di ripristino (RTO). Comprendere quanto indietro si dovrà andare per il ripristino, insieme al tempo necessario per recuperare i dati, è un aspetto fondamentale della reattività richiesta da NIS2.

Scopri Ootbi

(Immutabilità pronta all’uso)

Object First si propone di aiutare tutti i clienti Veeam nell’UE a garantire che i loro archivi di backup superino gli standard NIS2. Ecco perché Object First ha creato Ootbi, il miglior storage per Veeam. A prova di ransomware e con immutabilità preconfigurata, Ootbi di Object First offre uno storage di backup sicuro, semplice e potente, progettato appositamente per Veeam. Il dispositivo può essere inserito nel in rack, impilato installato e avviato in 15 minuti.

Ootbi aiuta gli amministratori Veeam a implementare un’architettura Zero Trust Data Resilience per backup e ripristini indistruttibili. Grazie alla sua architettura «secure by design», Ootbi garantisce che i dati di backup di Veeam rimangano immutabili e non richiede alcuna competenza aggiuntiva in materia di sicurezza da parte dell’utente finale.

Conclusione

La direttiva NIS2 è in corso di attuazione: il 17 ottobre 2024 sarà recepita dagli Stati membri. Come per qualsiasi mandato importante, ciò richiederà uno sforzo notevole da parte di molte persone all’interno di organizzazioni «importanti» ed «essenziali» per garantire che non vengano multate per non conformità. La formazione sarà sempre un primo passo fondamentale per soddisfare le esigenze di una legislazione come questa. Se sei interessato dalla direttiva NIS2, prenditi il tempo necessario per leggerla integralmente e assicurarti che la tua organizzazione sia consapevole delle implicazioni. Anche se inizialmente questa iniziativa potrebbe rivelarsi destabilizzante, ne varrà sicuramente la pena, in quanto contribuirà a ridurre le attività criminali dannose.

© 2024 Object First. Informazioni riservate. Tutti i diritti riservati. Tutti i marchi di fabbrica sono di proprietà dei rispettivi titolari.

OBJECT FIRST

objectfirst.com ↗

Tutti i collegamenti di questo documento sono disponibili qui: