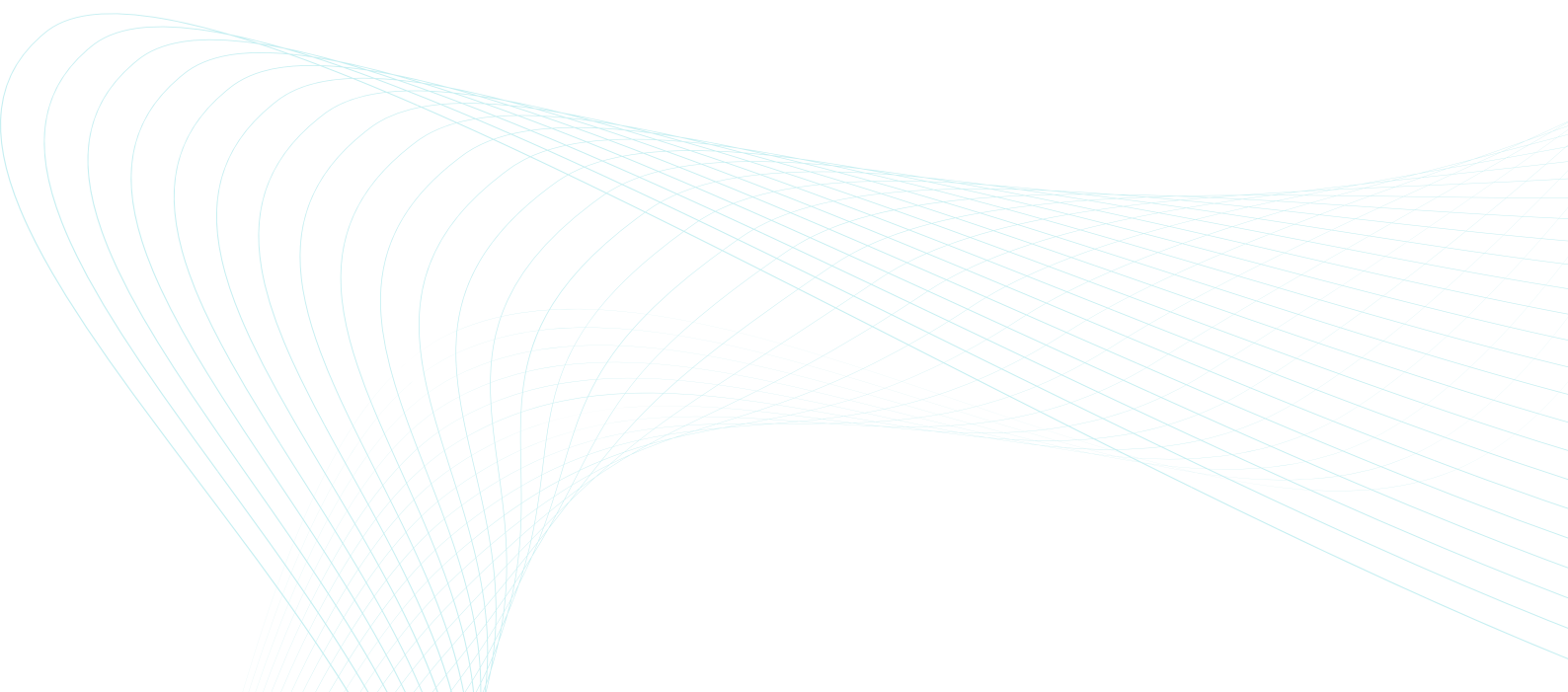


ESPLORA LA CYBERSECURITY

Tutto quello che c'è da sapere
sulla direttiva la NIS2

Contenuti

COS'E LA DIRETTIVA NIS2?	3
COSA DOBBIAMO ASPETTARCI DALLA DIRETTIVA NIS2?	4
COSA SIGNIFICHERÀ LA NIS2 PER LA TUA ORGANIZZAZIONE?	7
HAI BISOGNO DI AIUTO PER L'IMPLEMENTAZIONE DELLA NIS2?	8
CONTATTI	12
FONTI	13



Introduzione

Grazie per esserti interessato alla lettura del nostro *white paper* sulla direttiva NIS2. In questo documento tratteremo gli aspetti più importanti della direttiva NIS2.

La direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Direttiva NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (Direttiva NIS) è volta a rafforzare la sicurezza informatica nell'Unione europea (UE). La Direttiva NIS2 è stata concepita per aiutare le organizzazioni a proteggersi dalle minacce informatiche e per garantire che l'infrastruttura informatica dell'UE sia più sicura e solida.

Ora che la Direttiva NIS2 è stata finalmente pubblicata ufficialmente, gli Stati membri hanno tempo fino al 17 ottobre 2024 per recepire le sue disposizioni nella legislazione locale. In Italia, la legge di delegazione europea contenente anche la delega al Governo per emanare un decreto per implementare la NIS2, è stata approvata dal Parlamento, pubblicata in Gazzetta Ufficiale, ed è entrata in vigore il 10 marzo 2024. Si attende ora il decreto di recepimento della Direttiva NIS2.

In questo *white paper* forniremo una panoramica delle disposizioni più importanti della Direttiva NIS2 e di come si applicano. Parleremo inoltre degli obblighi che le organizzazioni hanno per conformarsi al nuovo quadro normativo e di come ESET, in collaborazione con Eversheds Sutherland per gli aspetti legali, può supportare questo processo.

Ci auguriamo che questo *white paper* sia utile alle organizzazioni che desiderano saperne di più su come proteggersi dalle minacce informatiche e su come conformarsi alla direttiva NIS2.

Cos'è la direttiva NIS2 ?

La nuova normativa dell'UE può avere un forte impatto sui requisiti di cybersecurity della tua organizzazione. "Questa direttiva europea aiuterà circa 160.000 entità a rafforzare la loro posizione in materia di sicurezza e a rendere l'Europa un luogo sicuro in cui vivere e lavorare. La legge dovrebbe anche consentire la condivisione delle informazioni con il settore privato e con i partner di tutto il mondo. Se veniamo attaccati su scala industriale, dobbiamo reagire su scala industriale", ha dichiarato il deputato olandese Bart Groothuis.

Poiché la cybersecurity è estremamente importante per la protezione della nostra società, nel 2016 l'Unione Europea (UE) ha introdotto la prima Direttiva sulla Sicurezza delle Reti e delle Informazioni (Direttiva NIS). Sebbene questa direttiva europea abbia garantito una maggiore coerenza all'interno dell'UE nel campo della sicurezza delle reti e delle informazioni, secondo il Parlamento europeo è stato necessario aumentare ulteriormente la resilienza informatica per proteggere le società. Con la crescente digitalizzazione e il gran numero di attacchi informatici, la Direttiva NIS è stata ora sottoposta a revisione e migliorata. La Direttiva NIS2 avrà un ambito di applicazione più ampio e si concentrerà su un maggior numero di settori, al fine di equiparare e aumentare la resilienza informatica delle organizzazioni negli Stati membri dell'UE.

Gestione del rischio e collaborazione:

Come farà questa nuova direttiva a garantire una migliore resilienza informatica? La Direttiva NIS2 cerca di migliorare il livello di cybersecurity negli Stati membri dell'UE in vari modi. La direttiva rafforza i requisiti di sicurezza imposti, si concentra sulla sicurezza della catena di approvvigionamento (la catena di produzione o di fornitura), razionalizza gli obblighi di segnalazione, rafforza le misure di vigilanza e introduce criteri uniformi per l'applicazione di sanzioni in tutti gli Stati membri. Vengono inoltre introdotte previsioni per la condivisione delle informazioni e per la cooperazione (inter)nazionale nel campo della gestione delle crisi.



















Ambito di applicazione soggettivo della Direttiva NIS2:

La Direttiva NIS2 riguarda un maggior numero di settori rispetto alla precedente Direttiva NIS. La Direttiva NIS identificava come destinatari della propria disciplina solo i settori della sanità, dei trasporti, bancario e delle infrastrutture dei mercati finanziari, delle infrastrutture digitali, dell'approvvigionamento idrico, dell'energia e dei fornitori di servizi digitali, lasciando agli Stati membri la possibilità di definire quali organizzazioni fossero considerate essenziali.

La Direttiva NIS2 introduce regole uniformi per i soggetti di medie e grandi dimensioni che operano in settori critici, come l'energia, i trasporti, la sanità e le infrastrutture digitali. Sono ora inclusi i "settori ad alta criticità", tra cui energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi ICT (B2B), pubblica amministrazione e spazio, e i "settori critici", come i servizi postali e i corrieri, la gestione dei rifiuti, i prodotti chimici, i prodotti alimentari, la fabbricazione, i fornitori di servizi digitali e la ricerca. Tutte le medie e grandi imprese di questi settori rientreranno nel campo di applicazione della normativa.

La tua organizzazione Essenziale o importante?

Le modalità di applicazione dipendono dalla categoria in cui rientra un'organizzazione. Secondo la Direttiva NIS2, le organizzazioni destinatarie delle relative previsioni possono rientrare in due categorie, e essere classificate come essenziali o importanti. La classificazione di un'organizzazione come essenziale o importante dipende dal fatto che l'organizzazione rientri in un settore critico o ad alta criticità e dalle dimensioni dell'azienda.

IN QUALE SETTORE OPERA LA TUA ORGANIZZAZIONE?	
 ENERGIA	 SERVIZI POSTALI E CORRIERI
 TRASPORTI	 GESTIONE DEI RIFIUTI
 BANCHE	 PRODUZIONE
 SANITA'	 FORNITORI DI SERVIZI DIGITALI
 ACQUA POTABILE	 RICERCA
 ACQUE REFLUE	 FABBRICAZIONE, PRODUZIONE E DISTRIBUZIONE DI PRODOTTI CHIMICI
 INFRASTRUTTURA DIGITALE	 PRODUZIONE, TRASFORMAZIONE E DISTRIBUZIONE DI ALIMENTI
 GESTIONE DEI SERVIZI ICT (B2B)	
 GOVERNO	<p>° Grande: più di 250 dipendenti e un fatturato annuo di almeno 50 milioni di euro (o un totale di bilancio di almeno 43 milioni di euro).</p> <p>° Medie dimensioni: più di 50 e meno di 250 dipendenti e un fatturato annuo non superiore a 50 milioni di euro (o un totale di bilancio non superiore a 43 milioni di euro).</p>
 AEROSPAZIALE	
 INFRASTRUTTURE PER IL MERCATO FINANZIARIO	



Le organizzazioni di medie dimensioni con meno di 250 dipendenti e un fatturato annuo fino a 50 milioni di euro (o un totale di bilancio fino a 43 milioni di euro) che operano in settori ad alta criticità sono considerate importanti, insieme ad altre organizzazioni di grandi e medie dimensioni in settori critici. Sono considerate essenziali solo le grandi organizzazioni che superano i massimali delle medie organizzazioni e che rientrano nei settori molto critici. Alcune organizzazioni sono automaticamente considerate "essenziali", indipendentemente dalle loro dimensioni, laddove un'interruzione del servizio possa avere gravi conseguenze per la società o siano il fornitore esclusivo a livello nazionale. Si tratta ad esempio di organizzazioni che forniscono reti e servizi di comunicazione pubblica, fornitori di servizi fiduciari e fornitori di servizi di registrazione di nomi di dominio di primo livello. Sul tema si attendono comunque le scelte del legislatore.

In principio, la Direttiva NIS2 non si rivolge alle piccole e microimprese che hanno meno di 50 dipendenti e un fatturato annuo inferiore a 7 milioni di euro (o un totale di bilancio inferiore a 5 milioni di euro). Tuttavia, se hanno un ruolo chiave per la società, l'economia, i settori o i servizi, gli Stati membri devono garantire che rientrino nell'applicazione di questa direttiva.

La differenza principale delle prescrizioni previste a carico rispettivamente dei soggetti essenziali e importanti riguarda le modalità con le quali viene svolta la vigilanza su di essi. Per i soggetti essenziali, principalmente operanti in settori vitali, la vigilanza sarà proattiva. Ciò significa che queste organizzazioni saranno monitorate attivamente per verificare il rispetto degli obblighi normativi. Nel caso dei soggetti importanti, la vigilanza avviene a posteriori a seguito di segnalazione.



COSA DOBBIAMO ASPETTARCI dalla Direttiva NIS2?

Lo spieghiamo sulla base di due esempi.



L'azienda energetica BrightEnergies, con 500 dipendenti, si è già trovata in passato a dover far fronte agli adempimenti di sicurezza a seguito dell'introduzione della prima direttiva NIS. Nella legislazione locale sulla sicurezza delle reti e delle informazioni, il settore a cui apparteneva ("energia") è sempre stato classificato come un fornitore di importanza vitale. L'attuale direttore Lennard, ai tempi dell'applicazione della direttiva NIS non operava ancora presso la BrightEnergies, ma è venuto comunque a conoscenza del fatto che esiste una documentazione interna aziendale di quali misure e processi sono stati adeguati o rinnovati in quel periodo. Nel 2022, ha appreso che sarebbe stata rilasciata una nuova normativa: la Direttiva NIS2. In questa nuova normativa, un'azienda energetica è considerata un "soggetto essenziale". Con l'introduzione della direttiva NIS2, sono state apportate diverse modifiche. Poiché le aziende del settore energetico spesso vengono colpite da attacchi informatici, Lennard ora vuole fare tutto il possibile per garantire che BrightEnergies non venga colpita. Il rispetto dei requisiti posti dalla direttiva NIS2 deve avere quindi la massima priorità.



L'azienda Waste2Resource che si occupa di trattamento e riciclaggio dei rifiuti in passato non rientrava nell'applicazione della direttiva NIS o di altre normative di cybersecurity. Negli ultimi anni, tuttavia, è diventato più chiaro che anche un'azienda che operi in questo settore può trovarsi a dover affrontare un attacco informatico: nel 2021 un loro concorrente è stato chiuso per giorni a causa di un ransomware che ha impedito ai camion della spazzatura di circolare. Il team IT di Waste2Resource ha accolto con positività l'introduzione della direttiva NIS2, anche se è consapevole del fatto che ci sia ancora molto lavoro da fare. Il team, guidato dal neo CISO Kayleigh, è attualmente impegnato nell'analisi dei rischi; in ogni caso, il CISO e il suo team sanno già che la propria azienda è considerata un soggetto importante ai sensi della direttiva NIS2 e di dover quindi far fronte a un dovere di attenzione e a un obbligo di segnalazione reattiva.

Obblighi e implicazioni

La Direttiva NIS2 richiede che anche soggetti operanti in altri settori rispetto a quelli identificati ai sensi della Direttiva NIS, adottino requisiti di cybersecurity più ampi. Tra le altre cose, è richiesta l'implementazione di adeguati sistemi di backup, lo svolgimento di analisi dei rischi, il costante controllo della catena di approvvigionamento e l'obbligo di segnalazione degli incidenti che possano avere impatti significativi. I vertici delle organizzazioni destinatarie della normativa saranno responsabili della conformità della propria organizzazione alle disposizioni della Direttiva NIS2.

Questo nuovo approccio rappresenta un grande passo per molte organizzazioni, grandi o piccole che siano. Sia il governo che le organizzazioni dovranno assumersi maggiori responsabilità. Questo avrà anche conseguenze finanziarie: per le aziende che non sono ancora coperte dalla Direttiva NIS2 si prevede un aumento massimo del budget ICT del 22%, e per le aziende già destinatarie delle previsioni della Direttiva NIS, un aumento fino a un massimo del 12%. Anche gli oneri amministrativi aumenteranno. Resta da vedere se questa spesa aggiuntiva per l'ICT sarà remunerativa e darà alle aziende vantaggi competitivi grazie al livello più elevato di cybersecurity.

Si prevede comunque che l'applicazione di adempimenti più stringenti e sanzioni più severe previsti dalla Direttiva NIS2 favorirà certamente un'economia digitale più sicura nell'Unione europea e una maggiore protezione dai cyberattacchi.

Cosa significherà la NIS2 per la tua organizzazione?

Come accennato in precedenza, la Direttiva NIS2 differenzierà due categorie: soggetti essenziali e importanti, laddove in precedenza si distingueva solo tra organizzazioni vitali che rientravano nella NIS e organizzazioni non vitali. Tutti i settori e le organizzazioni che rientreranno nella NIS2 sono di grande importanza per la collettività. Se queste organizzazioni non potessero più svolgere il loro ruolo, si creerebbero gravi problemi per la società.

Gli attacchi informatici possono avere un impatto significativo, non solo sulle organizzazioni ma anche sulla società civile. Ecco alcuni esempi di attacchi importanti:



NotPetya

La diffusione del ransomware NotPetya nel 2017, che ha causato interruzioni tra cui la chiusura del porto di Rotterdam.

2017



Mandemakers gr. & VDL

Durante gli attacchi ransomware a Mandemakers Groep e VDL, le operazioni di queste organizzazioni sono state gravemente interrotte.

2021



Bakker Logistiek

A seguito dell'attacco alla Bakker Logistiek, i supermercati hanno registrato una carenza di formaggio per diversi giorni.

2021



Kaseya

L'attacco al fornitore di software Kaseya ha consentito ai criminali informatici di accedere ai sistemi di migliaia di aziende.

2021

Obbligo di diligenza e segnalazione

Tutti i soggetti essenziali o importanti - dovranno tra l'altro:

- predisporre e implementare policy di analisi del rischio e sicurezza dei sistemi informativi
- prestare attenzione alla gestione delle crisi e alla continuità operativa in caso di incidente informatico
- garantire la sicurezza della catena di approvvigionamento
- garantire la sicurezza della rete e dei sistemi informativi
- far uso della crittografia e della cifratura
- predisporre e implementare policy e procedure per la valutazione dell'efficacia delle misure di gestione del rischio
- formare adeguatamente il proprio personale.

La Commissione europea si riserva il diritto di definire ulteriormente le modalità di intervento mediante decisioni delegate e di esecuzione e di ampliarle con misure aggiuntive. Gli Stati membri potranno quindi imporre misure specifiche, tenendo conto delle circostanze nazionali e settoriali. L'obbligo di segnalazione si applicherà anche a tutte le organizzazioni che rientrano nell'ambito di applicazione della Direttiva NIS2. L'obbligo di segnalazione comporta che le organizzazioni interessate devono riferire l'incidente all'autorità designata entro 24 ore dal momento in cui ne sono venute a conoscenza, poi notificare entro 72 ore, e preparare una relazione finale entro un mese.

NIS2 in breve



IMPORTANTE

Organizzazioni medie attive in uno degli 11 "settori ad alta criticità" o organizzazioni di medie e grandi dimensioni attive in uno dei 7 "settori critici".



ESSENZIALE

Grandi organizzazioni attive in settori "ad alta criticità".



DOVERE DI DILIGENZA

- mantenere un adeguato livello di educazione alla sicurezza informatica e di formazione in materia
- valutare il rischio per la sicurezza dei sistemi informativi
- prestare attenzione alla gestione delle crisi e alla continuità operativa in caso di incidente informatico grave
- garantire la sicurezza della catena di approvvigionamento
- garantire la sicurezza della rete e dei sistemi informativi, compresa la risposta e la comunicazione delle vulnerabilità

- garantire la sicurezza delle risorse umane, le policy di accesso e la protezione degli asset digitali
- uso della crittografia e della cifratura
- inserimento o applicazione dell'autenticazione a più fattori e/o della comunicazione interna sicura
- policy e procedure per la valutazione dell'efficacia delle misure di gestione del rischio

Monitoraggio reattivo (dopo l'incidente)

Monitoraggio proattivo (anche al di fuori degli incidenti)



OBBLIGO DI COMUNICAZIONE (IN 3 FASI)

- preallarme entro 24 ore
- notifica dell'incidente entro 72 ore
- rapporto finale dopo un mese (o rapporto sullo stato di avanzamento in caso di incidente in corso)

Sanzione amministrativa per mancato rispetto dell'obbligo di diligenza o di segnalazione:

- una sanzione pari nel massimo ad almeno **7.000.000 di euro**
- o ad almeno l'**1,4% del fatturato annuo globale dell'esercizio precedente**, a seconda dell'importo più alto.



Sanzione amministrativa per mancato rispetto dell'obbligo di diligenza o di segnalazione:

- sanzione pari nel massimo ad almeno **10.000.000 di euro**
- o ad almeno il **2% del fatturato globale annuo dell'esercizio precedente**, a seconda dell'importo più alto.

Inoltre, le autorizzazioni possono essere temporaneamente sospesi o una persona fisica, come l'amministratore delegato, può essere temporaneamente sospesa.



È emergenza alla BrightEnergies. Un aggressore è entrato nella rete, nessuno sa come sia stato possibile e cosa si sia dovuto fare in quel momento e il CISO non è raggiungibile! Tutti sono in subbuglio e lo specialista IT Menno prende in mano le redini della situazione in attesa dell'arrivo del CISO. Entro 24 ore invia un avviso preventivo all'RDI. Insieme al consulente esterno, vengono cercati diligentemente i backup dell'azienda. Questi vengono trovati e l'organizzazione sa come prevenire conseguenze peggiori, perché ha accesso ai suoi dati importanti. Ciononostante, l'azienda rimane inattiva per alcuni giorni, con tutte le conseguenze che ciò comporta. Un mese dopo l'incidente, una descrizione dettagliata, le misure di mitigazione e la causa principale saranno riportate in un rapporto finale. Il fatto che tutto non fosse così ben organizzato nel campo della sicurezza ha aperto gli occhi al direttore Lennard. Questa crisi ha gravi conseguenze per l'azienda BrightEnergies.



Waste2Resource sta affrontando un attacco ransomware, proprio come il suo concorrente nel 2021. Grazie ai processi che il CISO Kayleigh ha voluto documentare, il team IT può ripristinare rapidamente un backup recente. Poco meno di 24 ore dopo, l'organizzazione è di nuovo operativa. Grazie agli sforzi compiuti per conformarsi ai requisiti di NIS2, il danno non è troppo grave. Kayleigh ha dimenticato solo una cosa: l'allarme preventivo. Fortunatamente, uno dei suoi compagni di squadra l'ha avvertita all'ultimo momento che l'allarme preventivo deve essere effettuato entro 24 ore. "Non dimenticare di programmare la notifica aggiornata e finale!", dice la collega di Kayleighs prima di andare a casa.

Minacce informatiche significative

Nella direttiva NIS2 sono state stabilite regole più severe per la segnalazione degli incidenti con conseguenze gravi. Le organizzazioni devono inoltre segnalare ogni minaccia informatica significativa che incontrano e che potrebbe portare a un incidente significativo. Per quanto riguarda il concetto di cybersecurity, la NIS2 è in linea con la definizione di cybersecurity e di certificazione informatica dell'Unione Europea. Un incidente è considerato significativo se provoca un'interruzione operativa significativa o perdite finanziarie per l'organizzazione o se potrebbe causare danni materiali o immateriali significativi a persone o organizzazioni.

Notifiche volontarie

Le organizzazioni che non rientrano nell'ambito di applicazione della direttiva NIS2 possono segnalare volontariamente incidenti significativi, minacce informatiche o quasi incidenti. L'autorità di vigilanza segue la procedura di segnalazione. Non dovrebbero essere imposti obblighi aggiuntivi in caso di notifiche volontarie.

Ambito di applicazione degli obblighi

La Commissione europea può fornire ulteriori indicazioni sulle informazioni, il formato e il processo di segnalazione sia per gli incidenti ad alto impatto che per le minacce informatiche. La portata degli obblighi può quindi essere estesa.

Multe e sanzioni

Il dovere di diligenza e l'obbligo di segnalazione comportano anche una forma di applicazione per garantire l'effettivo rispetto delle norme. A tal fine, le autorità disporranno di varie misure di vigilanza e risorse.

'La sicurezza informatica e la resilienza sono diventate una tematica da consiglio di amministrazione grazie alla NIS2. Oltre alle modalità di applicazione comuni - tra cui multe, sanzioni e l'effetto di diffamazione dell'opinione pubblica - è in gioco la responsabilità personale e la sospensione degli amministratori. I giorni della non conoscenza e della delega sono finiti.'

Eversheds Sutherland

Sanzioni Minime

La direttiva NIS2 contiene un elenco obbligatorio di sanzioni, tra cui ispezioni in loco, controlli di sicurezza, scansioni di sicurezza, richieste di informazioni e richieste di accesso ai dati. Alcune sanzioni sono uguali per tutti i Paesi, altre no, come le sanzioni per violazioni gravi. In questi casi, i Paesi stessi devono garantire sanzioni efficaci, proporzionate e dissuasive. Anche il tipo di sanzione (penale o amministrativa) è determinato dal Paese stesso. Le sanzioni devono essere adeguate alla gravità e alla natura della violazione e devono tenere conto di fattori quali il danno causato, la cooperazione con l'autorità competente e altre circostanze.

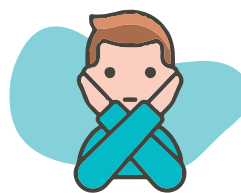
Sanzioni amministrative

In sostituzione o in aggiunta alle altre misure, possono essere imposte sanzioni amministrative pecuniarie, a seconda delle circostanze del caso. Nell'imporre una sanzione amministrativa si devono prendere in considerazione gli stessi elementi delle altre sanzioni. Le violazioni possono essere punite con sanzioni amministrative fino a 10 milioni di euro o al 2% del fatturato mondiale annuo dell'azienda, se superiore. Le autorità di vigilanza locali devono sviluppare le proprie politiche per l'imposizione di sanzioni pecuniarie.



SANZIONI

Come minimo, la direttiva NIS2 impone multe fino a 10 milioni di euro o al 2% del fatturato globale totale.



SOSPENSIONI

Le persone che ricoprono ruoli di autorità o di gestione possono essere sospese.



BrightEnergies deve affrontare sanzioni dopo l'attacco ransomware. In quanto entità essenziale, è obbligata a disporre di una sicurezza all'avanguardia. Il CISO viene sospeso e all'azienda viene richiesto il pagamento di una multa salata. Il direttore Lennard conclude che la sicurezza è ora una priorità assoluta per i team IT e vuole implementare soluzioni di sicurezza avanzate per prevenire proattivamente gli attacchi.



Fortunatamente, Waste2Resource evita le sanzioni. L'incidente ha aperto gli occhi a Kayleigh, che si reca dall'amministratore delegato e fa presente che con un po' più di budget pensa di poter garantire la sicurezza dell'organizzazione in maniera ancora più efficiente. Sebbene l'amministratore delegato riconosca la gravità dell'accaduto, è già abbastanza soddisfatto: "soddisfiamo perfettamente i requisiti, non è vero?", Kayleigh ottiene un leggero aumento del budget per contribuire a rafforzare ulteriormente la sicurezza.

Insieme per un futuro resiliente

La NIS2 garantirà inoltre l'istituzione di una rete europea di organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) per fornire supporto e coordinamento in caso di attacco informatico su larga scala nell'UE. Gli esperti insisteranno anche sulla collaborazione e sull'apprendimento reciproco tra gli Stati membri, al fine di distribuire suggerimenti e aumentare la fiducia reciproca.

HAI BISOGNO DI AIUTO con l'implementazione della NIS2?

Ecco cosa può fare ESET per la tua organizzazione. Come fornitore europeo nel campo delle soluzioni di sicurezza digitale, siamo felici di collaborare con te e aiutarti con le problematiche relative al NIS2 o alla sua implementazione.

Possibilità che offriamo nel campo del NIS2:

- Condivisione delle conoscenze attraverso i nostri canali, come Digital Security Guide o il nostro blog aziendale
- i nostri specialisti sono sempre disponibili a rispondere alle tue domande
- fornire soluzioni di sicurezza che contribuiscono alla conformità

Ecco cosa può fare Eversheds Sutherland per la tua organizzazione

Eversheds Sutherland, tra i primi 10 studi legali a livello mondiale, fornisce consulenza e soluzioni legali a una base di clienti internazionali che comprende alcune delle più grandi multinazionali del mondo. Il nostro team altamente integrato, interdisciplinare e profondamente collaborativo in materia di privacy fornisce una consulenza completa, mirata al business e tempestiva in una delle aree del diritto in più rapida evoluzione.

Possiamo aiutarti a interpretare l'impatto della NIS2 sulla tua attività e ad attuare strategie pragmatiche per la conformità. Troviamo modi innovativi per semplificare la complessità, per rendere più agevole l'amministrazione e per mettere la tua azienda a prova di futuro.

In caso di attacco informatico, il nostro team ha una lunga esperienza nel supportare i clienti globali nei loro progetti di conformità e nella risposta agli incidenti. Il nostro sistema di gestione dei progetti, unico nel suo genere, ci permette di fornire servizi legali complessi, multinazionali attraverso punti di contatto chiari e semplici.

VUOI AVERE MAGGIORI INFORMAZIONI?

Contatta il nostro **TEAM**
per ricevere supporto!

marketingitaly@eset.com

Sources:

<https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN>

[https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/
cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken](https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken)

EVERSHEDS
SUTHERLAND



Digital Security
Progress. Protected.