CyberGrant
SECURITY MADE EASY

WHITE PAPER

NIS2: la tua azienda è a rischio?

Come evitare sanzioni e rafforzare la cybersecurity

Ultimo aggiornamento 16 aprile 2026

Tutto quello che CEO, CFO, CISO e organi societari devono sapere per adeguarsi alla normativa e proteggere il business

La conformità alla direttiva NIS2

La NIS2 è stata recepita in Italia lo scorso ottobre 2024. Molte organizzazioni stanno ancora cercando di capire se rientrano nel perimetro di applicazione della direttiva e a quali requisiti rispondere, considerando anche che, ora, il **top management**, i **rappresentanti legali** e gli **organi societari** hanno **responsabilità dirette in termini di cybersecurity**.

Aggiornamento NIS2: Determinazione ACN del 13 aprile 2026

Con la Determinazione 127437, l'ACN rende operativa la NIS2 introducendo un cambio di paradigma.

- La sicurezza diventa misurabile, superando la compliance formale a favore di una resilienza dimostrabile.
- La supply chain entra al centro, con obbligo di mappare fornitori, servizi e dipendenze critiche.
- La conformità si basa su processi reali e dati verificabili, che richiedono governance, monitoraggio continuo e responsabilità diretta del management.

Non basta più dichiarare, serve dimostrare. Questo segna il passaggio da adempimento a capacità operativa.

Leggi il nostro approfondimento per sapere quello che cambia per la tua azienda con la nuova Determinazione del 13 aprile: ACN accelera sulla NIS 2, ora la resilienza si misura

Sommario

Introduzione

Cosa cambia con la NIS2

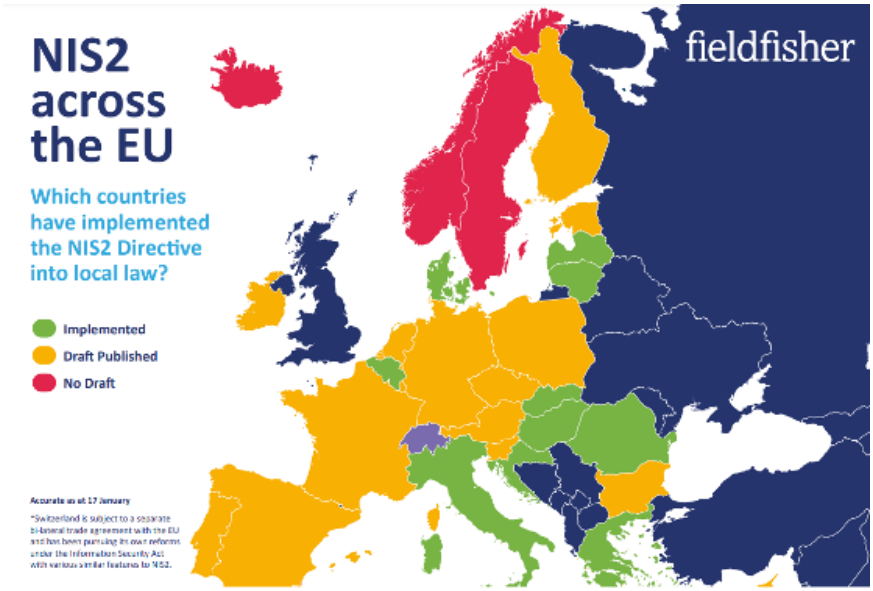
La Direttiva (UE) 2022/2555, conosciuta come Direttiva NIS 2 (Network Information Security), rappresenta una svolta importante per la cybersicurezza nelle organizzazioni europee ed è stata concepita per contrastare l'aumento delle minacce informatiche sempre più avanzate e pericolose.

La NIS2 introduce stringenti requisiti di governance, gestione dei rischi e segnalazione degli incidenti, oltre a coinvolgere un maggior numero di imprese rispetto alla versione precedente (i.e. NIS1). Inoltre, richiede **ai vertici aziendali un maggiore impegno e obblighi di controllo**. Ovvero, un ruolo attivo nella conformità, nella formazione specifica, e nella supervisione diretta sulla strategia di cybersecurity aziendale. Inoltre, **prevede sanzioni severe per il C-Leve**l, inclusa la sospensione dalle funzioni dirigenziali.

Ma vediamo in dettaglio di che si tratta.

NIS2 è qui tra noi: cosa è necessario sapere

La scadenza del **17 ottobre 2024** per l'implementazione di NIS2 è ormai trascorsa, tuttavia, molti Paesi sono in ritardo con le loro implementazioni locali. Di seguito lo stato dell'arte del recepimento della NIS2 da parte dei Paesi europei, al 17.01.2025, come si evince dall'immagine sotto riportata.



È doveroso evidenziare che la NIS2 espande significativamente la portata della Direttiva NIS originale, includendo u**n maggior numero di settori industriali**, oltre ad una serie di controlli di sicurezza più dettagliati. Inoltre, la direttiva richiede requisiti più rigorosi per la **reportistica degli incidenti** ed intensifica le misure di applicazione e le sanzioni. Ne consegue che organizzazioni precedentemente esenti potrebbero dover implementare nuovi sistemi e pratiche di cybersecurity per essere conformi, mentre quelle già vincolate dalla precedente versione della direttiva potrebbero necessitare di rivedere e aggiornare le loro misure di sicurezza per soddisfare i nuovi requisiti.

Settori interessati

Settori “essenziali” e settori “importanti”

La direttiva NIS2, come accennato, **copre un numero più ampio di organizzazioni rispetto alla NIS1**, classificando le entità in “**essenziali**” e “**importanti**”.

Inoltre, la NIS2 fornisce anche linee guida sulle **dimensioni delle organizzazioni incluse**, estendendo il suo ambito anche a fornitori e service provider di tali entità.

Pertanto, la NIS 2 si applica principalmente a:

Servizi essenziali

- Energia
- Trasporto
- Banche
- Infrastruttura del mercato finanziario
- Sanità e servizi sanitari
- Acqua potabile
- Acque reflue
- Infrastruttura di telecomunicazione
- Pubblica amministrazione
- Spazio

Servizi importanti

- Settore postale e spedizioni
- Gestione/Trattamento rifiuti
- Settore chimico: produzione e distribuzione
- Settore alimentare: produzione, traformazione e distribuzione alimenti, i.e. inclusa grande distribuzione
- Industrie tecnologiche e ingegneristiche
- Servizi digitali
- Ricerca

\+

FORNITORI E SERVICE PROVIDER DEI:

- Servizi essenziali
- Servizi importanti

Dimensioni delle aziende coinvolte

È doveroso evidenziare che sono escluse le organizzazioni con:

< 50 dipendenti

< € 10 milioni di fatturato annuo

a meno che non siano ritenute di importanza critica o rientrino in alcuni casi, quali:

- Organizzazioni che offrono servizi attraverso reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico, o che fungono da fornitori di servizi fiduciari come registri dei nomi TLD (Top-Level Domain) e fornitori di servizi DNS (Domain Name System).
- Enti della Pubblica Amministrazione, sia a livello centrale che regionale, definiti da uno Stato membro secondo la legislazione nazionale, che forniscono servizi la cui interruzione potrebbe influenzare notevolmente attività sociali o economiche cruciali.
- Fornitore esclusivo di servizi in uno Stato membro.
- Organizzazioni la cui interruzione del servizio potrebbe incidere sulla sicurezza pubblica, sull'incolumità pubblica o sulla salute pubblica.
- Entità la cui interruzione del servizio potrebbe causare rischi sistemici, in particolare per settori con impatti transfrontalieri.
- Organizzazioni considerate critiche a livello regionale o nazionale per il settore o tipo di servizio, o per altri settori interconnessi nello Stato membro.
- Entità identificate come critiche secondo la Direttiva (UE) 2022/2557 CER (Resilienza delle Entità Critiche), conosciuta anche come direttiva sulla resilienza dei soggetti critici.

È doveroso evidenziare, altresì, che la NIS2 si applica a qualsiasi entità che fornisce servizi critici in un paese membro dell'UE, indipendentemente dalla sua ubicazione; quindi, anche alle aziende con sedi al di fuori dell'UE potrebbero essere soggette alla NIS2 senza avere una presenza fisica nell'Unione.

Sanzioni

Le organizzazioni che non rispettano i requisiti della direttiva NIS2 saranno soggette a sanzioni rilevanti, e precisamente:

Servizi essenziali

possono incorrere in multe fino a **10 milioni di euro o il 2%** del loro fatturato annuo globale.

Servizi importanti

possono incorrere in multe fino a **7 milioni di euro o l'1,4%** del loro fatturato annuo globale.

Accountability del C-Level

È fondamentale evidenziare che la non conformità alla Direttiva NIS2 può comportare una serie conseguenze legali.

In primis, il C-Level - i.e. persone fisiche in posizioni dirigenziali, legali rappresentanti o membri degli organi societari delle organizzazioni coinvolte - **può essere considerato responsabile** se non vengono rispettati i nuovi requisiti che includono: un maggiore coinvolgimento e obblighi di controllo, un ruolo attivo nella compliance, formazione specifica per migliorare la capacità di valutare i rischi di sicurezza informatica, e supervisione diretta sulla sicurezza IT. Le sanzioni accessorie possono prevedere la sospensione dalle funzioni dirigenziali.

Inoltre, il C-Level deve anche promuovere regolarmente corsi di formazione all'interno dell'organizzazione per tutti i dipendenti. Ciò significa esercitare una leadership competente e determinata, affrontando le sfide della cybersecurity e guidando le organizzazioni verso un futuro sicuro e resiliente.

Notifica degli incidenti

La direttiva NIS2 introduce obblighi più rigidi in termini di notifica degli incidenti e, precisamente:

- **Entro 24 ore** – Una notifica iniziale alle autorità competenti o al CSIRT (Computer Security Incident Response Team), indicando se si sospetta che l'incidente sia causato da atti illeciti o dolosi o che potrebbero avere un impatto transfrontaliero.
- **Entro 72 ore** – Un aggiornamento e un'iniziale valutazione dell'incidente, fornendo informazioni in termini di gravità e di impatto, oltre a fornire gli indicatori di compromissione.
- **Su richiesta dell'Autorità o di un CSIRT**- Una relazione di aggiornamento sullo stato dell'incidente.
- **Entro un mese** (dopo la presentazione della prima relazione) - Una relazione finale comprendente, almeno: cause, impatto complessivo e misure di mitigazione implementate. Inoltre, qualora l'incidente fosse ancora in corso, i soggetti devono fornire: una relazione sullo stato di avanzamento dei lavori - a quel momento - e una relazione finale entro un mese dalla gestione dell'incidente.

> *Di fatto, le organizzazioni saranno valutate non solo per il fatto di essere state vittime di un attacco informatico, ma anche per **la qualità della loro risposta e per il livello di preparazione dimostrato**. Ne consegue che, è quanto mai fondamentale che le organizzazioni comprendano a fondo cosa comporta la direttiva NIS2 e quale impatto essa abbia su di esse.*

Requisiti della direttiva NIS2

È doveroso evidenziare che la direttiva NIS2 adotta un approccio risk-based e multi -risk (i.e. non solo rischi digitali, ma anche fisici, ambientali, oltre a quelli legate alle persone). Inoltre, introduce nuovi requisiti in quattro aree principali dell'organizzazione per potenziare la capacità dell'Europa di resistere alle minacce informatiche attuali e future. E, precisamente:

Responsabilità aziendale - Il Top Management deve essere consapevole e comprendere i requisiti della Direttiva, assumendosi la responsabilità diretta di identificare e di affrontare i rischi informatici per conformarsi ad essa.

Gestione del rischio - Le organizzazioni devono implementare misure volte a minimizzare i rischi e le loro conseguenze. Ciò comprende la gestione degli incidenti, il miglioramento della sicurezza della supply chain, la sicurezza della rete, il controllo degli accessi e la crittografia.

Segnalazione alle autorità - Le organizzazioni devono avere processi stabiliti per garantire una corretta segnalazione alle autorità competenti.

Continuità aziendale - Le organizzazioni devono pianificare come garantire la continuità aziendale in caso di gravi incidenti informatici, includendo il ripristino del sistema, le procedure di emergenza e la formazione di una squadra di risposta alle crisi.

Dieci misure minime da implementare

Le organizzazioni che rientrano nel perimetro della NIS2 dovranno altresì dimostrate di avere implementato le seguenti dieci misure minime:

1. **Valutazione dei rischi e politiche di sicurezza per i sistemi informativi** - Stabilire un quadro per identificare e mitigare i rischi legati ai sistemi informativi.
2. **Politiche e procedure per valutare l'efficacia delle misure di sicurezza** - Definire metodi e procedimenti per monitorare e valutare l'efficacia delle soluzioni di sicurezza implementate.
3. **Politiche e procedure per l'uso della crittografia e, se del caso, della cifratura** - Stabilire linee guida sull'applicazione della crittografia per proteggere i dati sensibili.
4. **Piano per la gestione degli incidenti di sicurezza** - Implementare un piano dettagliato di risposta agli incidenti per garantire una reazione rapida agli eventi indesiderati, elemento cruciale per la conformità alla Direttiva NIS2.
5. **Sicurezza nell'approvvigionamento dei sistemi e nello sviluppo e nel funzionamento dei sistemi** - Stabilire criteri per la gestione e segnalazione delle vulnerabilità durante il ciclo di vita dei sistemi.
6. **Formazione** - Garantire un'educazione continua sui principi base di cybersecurity. Di fatto, educare i dipendenti e promuovere una cultura della sicurezza - attraverso corsi regolari sulla consapevolezza delle minacce e sulle migliori pratiche - li trasforma in una difesa efficace per proteggere le risorse digitali. Inoltre, la formazione dovrebbe includere anche aspetti, quali: la gestione delle password, il riconoscimento delle truffe di phishing e l'importanza di segnalare prontamente attività sospette.
7. **Procedure di sicurezza per i dipendenti con accesso a dati sensibili o importanti** - Implementare criteri chiari per l'accesso ai dati e mantenere un inventario delle risorse rilevanti per garantirne l'uso e la gestione corretta.
8. **Piano per la gestione delle operazioni aziendali durante e dopo un incidente di sicurezza** - Stabilire un piano di business continuity, disaster recovery e gestione delle crisi, con backup aggiornati, per mantenere l'accessibilità ai sistemi informatici durante e dopo un incidente.
9. **Sicurezza delle risorse umane** - Adottare misure come l'autenticazione a più fattori, la crittografia delle comunicazioni e la gestione sicura dei canali di comunicazione interna.
10. **Sicurezza delle supply chain e del rapporto tra azienda e fornitore** - Valutare regolarmente i rischi della supply chain e assicurarsi che i partner aderiscano ai requisiti della Direttiva NIS2. Ciò include la valutazione dei rischi dei fornitori, gli accordi contrattuali che definiscono le aspettative di sicurezza, oltre a una comunicazione costante con i fornitori.

Scadenze per la compliance della NIS2 in Italia

Direttive da ACN

L'Agenzia per la Cybersicurezza Nazionale (ACN) coordina l'attuazione della Direttiva NIS 2 in Italia, operando come Autorità nazionale competente. Per un'efficace implementazione, sono delineate alcune tappe essenziali. E, precisamente:

Registrazione

Dal **1° dicembre 2024**, le organizzazioni pubbliche o private con i requisiti specifici della normativa NIS 2 possono registrarsi tramite il portale dei servizi dell'ACN. In particolare:

- Entro il **17 gennaio 2025** – Registrazione per fornitori di cloud computing, data center, servizi gestiti (inclusi quelli di sicurezza) e mercati online.
- Entro il **28 febbraio 2025** - Registrazione per tutti gli altri soggetti che rientrano nel perimetro della NIS2 secondo il decreto di attuazione n.138/2024 del nostro Paese.

La registrazione consente all'ACN di censire gli operatori nei settori NIS2 e di fornire supporto durante l'implementazione degli obblighi, attraverso azioni di monitoraggio e di assistenza. Il sito dell'ACN contiene informazioni sui settori e i sottosettori coperti dalla normativa e su come **determinare se un'organizzazione è classificata come "essenziale" o "importante"**

- Entro il 15 aprile 2025 - ACN notificherà se i soggetti registrati rientrano nell'elenco NIS2 e pubblicherà gli obblighi di notifica degli incidenti e le misure di sicurezza da adottare.
- Dal **15 aprile al 31 maggio 2025** - I soggetti essenziali e importanti devono comunicare/aggiornare tramite il Portale dei servizi di ACN alcune informazioni fondamentali per permettere i controlli.

Altre scadenze

- dal 1° maggio al 30 giugno - I soggetti comunicano/ aggiornano tramite il Portale dei servizi di ACN **l'elenco delle proprie attività** e dei propri servizi.
- **1° gennaio 2026 - I soggetti NIS2 dovranno iniziare a notificare gli incidenti ed aggiornare annualmente le informazioni sui propri servizi.**
- Entro **ottobre 2026** – I soggetti NIS2 dovranno **completare l'implementazione delle misure di sicurezza** informatica di base e garantire la sicurezza della supply chain.

Inoltre, a livello di area europea, ogni Paese dovrà considerare anche queste scadenze:

- Entro il 17 aprile 2025 - Gli Stati membri stabiliscono un elenco di entità essenziali e importanti, nonché di entità che forniscono servizi di registrazione di nomi di dominio. Gli Stati membri riesaminano e, ove opportuno, aggiornano tale elenco regolarmente e, almeno ogni due anni, in seguito.
- Entro il 17 aprile 2025 e successivamente ogni due anni – Le Autorità competenti notificano alla Commissione e al gruppo di cooperazione il numero di entità essenziali e importanti per ciascun settore.
- **Entro il 17 ottobre 2027 e successivamente ogni 36 mesi** - La Commissione riesamina il funzionamento della presente direttiva e ne riferisce al Parlamento europeo e al Consiglio.

NIS2 e CIA Triad

La NIS 2 sottolinea l'importanza di proteggere i sistemi di rete e informativi per garantire la CIA Triad. Le tre lettere che compongono l'acronimo "CIA Triad" rappresentano i concetti di: **Riservatezza (Confidentiality), Integrità (Integrity) e Disponibilità (Availability).** È opportuno sottolineare il significato di ciascun elemento della triade.

Riservatezza

La riservatezza può essere violata attraverso vari metodi. Tra questi vi sono gli **attacchi diretti**, in cui un aggressore tenta di accedere a sistemi non autorizzati, oppure cerca di infiltrarsi in applicazioni o database al fine di sottrarre o modificare dati. Tali attacchi possono impiegare tecniche come gli attacchi Man-In-The-Middle (MITM), in cui l'aggressore si inserisce nel flusso di comunicazioni per intercettare, per rubare o per alterare le informazioni.

Altre strategie di spionaggio di rete mirano a **ottenere le credenziali di accesso**, e talvolta, gli aggressori cercano di acquisire i privilegi di sistema più elevati per ottenere ulteriori autorizzazioni.

È doveroso evidenziare che non tutte le violazioni della riservatezza sono intenzionali. Errori umani o controlli di sicurezza insufficienti possono anche essere causa di compromissioni. Ad esempio, qualcuno potrebbe non proteggere adeguatamente la propria password per una postazione di lavoro o per un'area riservata, condividerla con altri, o consentire a qualcuno di vedere il proprio login durante l'inserimento.

Inoltre, un utente potrebbe non crittografare correttamente una

comunicazione, permettendo a un aggressore di intercettare le informazioni. Ancora, un ladro potrebbe anche rubare un hardware, i.e. un computer o un dispositivo usato per il login, per accedere a dati riservati.

La riservatezza comporta gli sforzi di un'organizzazione per garantire che i dati rimangano confidenziali o privati. Per raggiungere tale obiettivo, è necessario controllare l'accesso alle informazioni, prevenendo la condivisione non autorizzata dei dati in modo sia intenzionale sia accidentale, oltre ad impedire l'accesso alle risorse importanti a chi non ha le dovute autorizzazioni. Inoltre, per contrastare le violazioni, è possibile: classificare ed etichettare i dati sensibili; implementare politiche di controllo degli accessi; crittografare le informazioni; adottare sistemi di autenticazione multifattoriale (Multi Factor Authentication - MFA); considerare l'architettura Zero Trust. Ancora, è consigliabile garantire che tutti i membri dell'organizzazione ricevano la formazione e le conoscenze necessarie per identificare ed evitare i potenziali pericoli.

Integrità

Significa garantire che i dati siano affidabili e non manomessi. Di fatto, l'integrità si mantiene solo se i dati sono autentici, accurati e affidabili. La compromissione dell'integrità può essere sia intenzionale sia accidentale. L'integrità, se le procedure e le protezioni aziendali sono inadeguate, può essere compromessa senza che vi sia una responsabilità individuale.

Inoltre, per proteggere l'integrità dei dati, si possono utilizzare tecniche, quali: l'hashing, la crittografia, i certificati digitali; le firme digitali. Ancora, per quanto riguarda i siti web, è importante affidarsi ad autorità di certificazione affidabili per garantire ai visitatori di accedere al sito corretto.

Un metodo per verificare l'integrità è il non ripudio dei dati che implica che le informazioni trasmesse siano corredate da una firma digitale o associate a un sistema di verifica che consenta a chiunque di dimostrare in modo inequivocabile la paternità di un'azione.

Disponibilità

È importante evidenziare che, anche se i dati sono riservati e integri, diventano inutili se non sono accessibili a chi ne ha bisogno, sia all'interno dell'organizzazione sia tra i clienti e gli stakeholder. Pertanto, è essenziale che sistemi, reti e applicazioni siano operativi come previsto e al momento giusto.

Inoltre, è fondamentale che le persone autorizzate possano accedere tempestivamente alle informazioni necessarie, tenendo conto che eventi come interruzioni di corrente, disastri naturali, alluvioni o tempeste di neve possono causare l'indisponibilità dei dati e impedire l'accesso fisico agli uffici. Inoltre, atti di sabotaggio, quali attacchi DoS o ransomware, possono compromettere ulteriormente la disponibilità delle informazioni. Pertanto, le organizzazioni, per garantire la disponibilità, possono implementare reti, server

e applicazioni ridondanti da attivare quando i sistemi primari falliscono o non sono disponibili. SI consiglia, altresì, di aggiornare regolarmente software e sistemi di sicurezza per ridurre il rischio di malfunzionamenti e nuove minacce. Infine, i backup e i piani di disaster recovery - che devono essere regolarmente testati e verificati - sono cruciali per ripristinare la disponibilità dei dati rapidamente a fronte di eventi dirompenti.

US regulation vs NIS 2: vi sono corrispondenze?

la NIS2 e CSF2 sono molto simili in quanto adottano un approccio risk-based

L'UE ha adottato varie direttive e normative – tra cui la NIS2 - per rafforzare la cybersecurity delle infrastrutture critiche, mentre gli **Stati Uniti non dispongono di un quadro normativo unificato**, basandosi principalmente su normative settoriali che variano da stato a stato.

Tuttavia, è doveroso segnalare che lo scorso gennaio 2024 il NIST (National Institute for Standards and Technology) ha pubblicato la nuova versione del Cyber Security Framework 2 (CSF2) che ha lo scopo di migliorare il livello di cybersecurity delle organizzazioni statunitensi. È doveroso evidenziare che **la NIS2 e CSF2 sono molto simili** in quanto adottano un approccio risk-based; inoltre, l'identificazione delle risorse, delle vulnerabilità, delle minacce e la conseguente mitigazione del rischio sono gli elementi fondamentali di entrambe.

Una certa similitudine esiste anche per quanto riguarda la **SEC S-K** che è entrata in vigore nel dicembre 2023, con un impatto **sulle società quotate presso la SEC nel mercato statunitense**.

Sia la SEC S-K sia la NIS2 riguardano la cybersecurity e la conformità ai rischi informatici, ma hanno obiettivi diversi. Ovvero: la SEC S-K affronta la necessità di informativa aziendale e governance del rischio informatico per le società quotate in borsa; mentre la NIS2 si concentra sui rischi di cybersecurity e sulla protezione delle infrastrutture critiche.

Inoltre, la SEC S-K è naturalmente focalizzata sulla trasparenza finanziaria, sulla governance aziendale e sulla rilevanza degli incidenti e dei rischi per proteggere gli investitori.

LaNIS2, invece, si concentra sulla cyber resilience, imponendo controlli di sicurezza, segnalazione degli incidenti e gestione del rischio per le infrastrutture critiche, oltre a perseguire l'armonizzazione della cybersecurity in tutta l'UE in termini di servizi critici.

Come CyberGrant può supportare la compliance alla NIS2 della NIS2 in Italia

CyberGrant
SECURITY MADE EASY

Cyber Gran Inc. - una società americana con sede a Menlo Park, California - offre sul mercato le soluzioni RemoteGrant e FileGrant che possono supportare le organizzazioni a raggiungere la compliance di diversi requisiti della direttiva NIS2. E, precisamente:

Gestione del rischio

La NIS2 richiede un approccio proattivo nella gestione del rischio e nella protezione dei dati.

FileGrant Enterprise - Offre crittografia avanzata e gestione degli accessi per prevenire intrusioni e migliorare la protezione.

RemoteGrant - Fornisce monitoraggio continuo, il blocco di malware e di ransomware, la protezione in tempo reale contro exploit e vulnerabilità, grazie a scansioni regolari per rilevare le vulnerabilità nei sistemi endpoint, oltre a fornire aggiornamenti e patch correttivi.

Monitoraggio e risposta alle minacce

La NIS2 richiede un monitoraggio costante delle minacce e risposte rapide alle violazioni, oltre ad essere in grado di garantire la business continuity.

FileGrant Enterprise - Monitora gli accessi ai documenti in tempo reale e permette una revoca rapida per prevenire ulteriori danni.

RemoteGrant - Esegue la registrazione continua delle attività e dei log sugli end-point, oltre ad inviare notifiche delle attività non autorizzate. Inoltre, è dotato di un'avanzata tecnologia di rilevamento delle minacce, sfruttando 75 antivirus per identificare in tempo reale attività di phishing e altre minacce.

Protezione contro accessi non autorizzati

La NIS2 richiede che le organizzazioni siano in grado di limitare gli accessi non autorizzati ai dati critici.

FileGrant Enterprise - Offre crittografia robusta e anti-screen capture, oltre a controlli specifici sui ruoli, per impedire l'accesso non autorizzato.

RemoteGrant - Permette di implementare politiche di controllo degli accessi basate sui ruoli e supporta l'uso di IP autorizzati. Inoltre, implementa procedure di MFA e limita gli accessi diretti ai dispositivi.

Segnalazione degli incidenti

La NIS2 richiede la segnalazione rapida degli incidenti e la garanzia della business continuity.

FileGrant Enterprise - Permette l'identificazione rapida di violazioni e si integra con sistemi aziendali di monitoraggio per l'invio di notifiche.

RemoteGrant - Fornisce log dettagliati per l'analisi di eventi e dispone di policy di segnalazione secondo diversi livelli di priorità.

Protezione della condivisione dei dati

La NIS2 richiede la protezione dei dati critici durante il trasferimento e la conservazione.

FileGrant Enterprise - Utilizza una crittografia sofisticata per proteggere i file, rendendoli accessibili solo agli utenti autorizzati e impedendo qualsiasi forma di copia non autorizzata.

RemoteGrant: - Utilizza una serie di policy di controllo delle condivisioni, bloccando il trasferimento di file in sessioni remote per impedirne le esfiltrazioni.

CyberGrant Inc. vuole essere a fianco delle aziende, di ogni settore e di ogni dimensione, offrendo le proprie soluzioni in grado di trasformare l'approccio alla cybersecurity e alla gestione dei dati da un onere a un investimento per crescere, per generare un vantaggio competitivo e per adempiere agli obblighi normativi in materia di sicurezza dei dati e di cybersecurity alla base della direttiva NIS2.

A cura di **Federica Maria Rita Livelli**

www.cybergrant.net