SOPHOS

ATIK
Your Business Solutions

La Direttiva NIS 2

Requisiti – Effetti – Dati Chiave

Questo whitepaper è stato scritto in collaborazione con l'avvocato David Bomhard della Noerr Partnerschaftsgesellschaft mbB.

Per rispondere ad attacchi informatici sempre più frequenti e dannosi e per fare fronte all'esigenza correlata di potenziare i sistemi di difesa (inclusi quelli tecnici) contro tali incidenti, a dicembre 2022 il Consiglio dell'Unione Europea e il Parlamento Europeo hanno adottato la direttiva sulla sicurezza delle reti e dei sistemi informativi 2.0 (direttiva (UE) 2022/2555, "direttiva NIS 2"). La direttiva prevede requisiti di sicurezza informatica riveduti e più ampi in tutti gli Stati membri dell'UE. Una delle finalità più importanti di questa normativa sulla sicurezza informatica nell'UE è contribuire "al funzionamento efficace della sua economia e della sua società" (vedi la Premessa 1 della direttiva NIS 2).

Questo whitepaper è stato realizzato per fornirti informazioni sui nuovi requisiti estesi previsti dalla direttiva NIS 2 per le aziende che operano nel mercato europeo, nonché per descrivere come le soluzioni Sophos possono aiutarti a ottemperare a questi nuovi requisiti.

Whitepaper Sophos, maggio 2023

A. Antecedenti e contenuti pertinenti della direttiva NIS 2

I. Roadmap: da NIS 1 a NIS 2

Con la prima direttiva sulla sicurezza delle reti e dell'informazione (direttiva (UE) 2016/1148, "direttiva NIS 1"), adottata nel 2016, sono state effettuate le prime attività di standardizzazione a livello europeo della cybersecurity all'interno dei sistemi legali degli Stati membri dell'UE.

A dicembre 2022, il Consiglio e il Parlamento europeo hanno adottato la direttiva NIS 2, nella quale sono stati revisionati ed estesi i requisiti di cybersecurity per tutta l'UE. Poiché la direttiva NIS 2 è una direttiva e non un regolamento, non può essere applicata direttamente negli Stati membri, ma deve prima essere convertita in legge nazionale. Pertanto, gli enti di legislazione nazionali sono tenuti a modificare le proprie leggi nazionali sulla sicurezza informatica entro e non oltre il termine ultimo stabilito dagli enti di legislazione europei, ovvero il 17 ottobre 2024.

Anche se gli enti di legislazione nazionali dovessero ottemperare ai requisiti prima del termine definito, le aziende non sono tenute ad adeguarsi alle nuove disposizioni fino al 18 ottobre 2024. Ciononostante, consigliamo vivamente alle aziende di valutare attentamente i nuovi requisiti e il potenziale impatto della direttiva NIS 2 il prima possibile.

> **Esempio:**
>
> *Poiché l'ambito di applicazione della direttiva NIS 2 è più ampio rispetto alla prima direttiva e poiché sono gli enti di legislazione nazionali a implementarla, alcune aziende (o autorità) che in precedenza non erano soggette alle leggi sulla sicurezza informatica potrebbero ora essere tenute a ottemperare alla direttiva NIS 2. È essenziale che tali aziende o autorità si mobilitino il prima possibile per valutare potenziali misure di implementazione e considerare gli effetti che tali misure potrebbero avere sui processi aziendali e sulle procedure amministrative.*

II. La cybersecurity come attività di gestione

Con la direttiva NIS 2, gli enti di legislazione europei hanno confermato apertamente di ritenere che la cybersecurity e la prevenzione degli incidenti di sicurezza informatica sono responsabilità dell'alta dirigenza di tutte le aziende. Ai sensi dell'Articolo 20(1) della direttiva NIS 2, gli "organi di gestione" sono tenuti a monitorare il rispetto di misure di gestione del rischio specifiche (descritte di seguito nel punto IV.) e soprattutto possono essere ritenuti (personalmente) responsabili delle violazioni in questo ambito.

> **Esempio:**
>
> *Ai dirigenti di un gruppo che opera nel settore automobilistico si consiglia di non limitarsi a delegare l'intera implementazione delle misure di cybersecurity, ma piuttosto di prendere l'iniziativa di supervisionare e monitorare da vicino la conformità ai requisiti legali, in quanto i membri stessi del team di dirigenza possono essere, in ultima analisi, ritenuti responsabili della violazione dei suddetti requisiti nella propria entità.*

Secondo l'Articolo 32(6) della direttiva NIS 2, queste conseguenze possono avere ripercussioni anche sugli enti della pubblica amministrazione, senza pregiudicare eventuali disposizioni nazionali dei dipendenti pubblici o di altri funzionari pubblici. A questo riguardo, le modalità di implementazione e strutturazione della responsabilità dei dirigenti devono ancora essere stabilite nel dettaglio.

III. Estensione dell'ambito di applicazione della direttiva NIS 2

1. Più settori regolamentati

La direttiva NIS 2 prevede un'estensione significativa del precedente ambito di applicazione ed è ora valida per 18 settori, sia pubblici che privati.

> **Esempio:**
>
> *La direttiva NIS 2 coinvolge un numero maggiore di settori, inclusi, ad esempio, l'industria aerospaziale e alcuni servizi critici della pubblica amministrazione.*

Poiché la direttiva NIS 2 è a livello europeo, la sua applicabilità richiede una certa correlazione con l'UE. Di conseguenza, la direttiva si applica ai soggetti che prestano i propri servizi o che svolgono attività commerciali all'interno dell'Unione europea. Un'azienda che ricopre il ruolo di semplice fornitore di un'azienda europea ma che non eroga direttamente alcun servizio nell'UE e che non svolge attività commerciali nell'UE non può essere coinvolta se non (al massimo) indirettamente nella direttiva NIS 2, attraverso misure specifiche di gestione dei rischi (vedi il punto IV.2. di seguito).

La direttiva NIS 2 riguarda i seguenti 18 settori:

SETTORI AD ALTA CRITICITÀ (ALLEGATO I DELLA DIRETTIVA NIS 2):	ALTRI SETTORI CRITICI (ALLEGATO II DELLA DIRETTIVA NIS 2):
Energia	Servizi postali e di corriere
Trasporto	Gestione dei rifiuti
Settore bancario	Fabbricazione, produzione e distribuzione di sostanze chimiche
Infrastrutture dei mercati finanziari	Produzione, trasformazione e distribuzione di alimenti
Settore sanitario	Fabbricazione
Acqua potabile	Fornitori di servizi digitali
Acque reflue	Ricerca
Infrastrutture digitali	
Gestione dei servizi TIC (business-to-business)	
Pubblica amministrazione	
Spazio	

Data l'estensione dell'ambito di applicazione, non spetta più agli Stati membri determinare quali settori debbano essere soggetti al regolamento sulla cybersecurity.

La seguente tabella mostra l'aumento dei settori che devono ottemperare alla direttiva NIS 2, rispetto alla prima direttiva NIS:

DIRETTIVA NIS 1	DIRETTIVA NIS 2
Energia	Energia
Fornitura e distribuzione di acqua potabile	Acqua potabile, acque reflue
Infrastrutture digitali	Infrastrutture digitali
Settore sanitario	Settore sanitario
Settore bancario, infrastrutture dei mercati finanziari	Settore bancario, infrastrutture dei mercati finanziari
Trasporto	Trasporto, spazio (parziale), servizi postali e di corriere
	Produzione, trasformazione e distribuzione di alimenti
	Gestione dei rifiuti
	Gestione dei servizi TIC (business-to-business)
	Pubblica amministrazione
	Fabbricazione, produzione e distribuzione di sostanze chimiche
	Industria manifatturiera
	Fornitori di servizi digitali
	Ricerca

La direttiva NIS 2 è generalmente applicabile a qualsiasi soggetto che opera nei settori elencati negli Allegati I e II, e che, in base alla terminologia del diritto europeo, raggiunge le soglie previste per definire le imprese di medie dimensioni. Di solito questo avviene quando il soggetto ha almeno 50 dipendenti o un fatturato annuo o un bilancio annuo totale superiore ai 10 milioni di EUR.

L'Articolo 2(2)-(5) della direttiva NIS 2 aggiunge esplicitamente al proprio ambito di applicazione certi soggetti specifici, indipendentemente dalle dimensioni. Tra questi vi sono i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, nonché certi enti della pubblica amministrazione. Per tali soggetti, il numero di dipendenti, il fatturato annuo e il bilancio annuo totale non sono fattori determinanti

> **Esempio:**
>
> *Nel settore sanitario, la direttiva NIS 2 collocherà un numero nettamente superiore di soggetti nell'ambito normativo della legislazione UE sulla cybersecurity. A differenza della direttiva precedente e delle rispettive leggi nazionali per l'implementazione, tutti i soggetti che fabbricano dispositivi medici ai sensi del Regolamento (UE) 2017/745 relativo ai dispositivi medici dovranno ottemperare ai requisiti della direttiva NIS 2; precedentemente, questi requisiti erano obbligatori solo per i fabbricanti di prodotti medicinali che superavano certe soglie, le quali venivano a loro volta stabilite dagli Stati membri.*
>
> *Di conseguenza, i soggetti che fabbricano dispositivi indossabili, ad esempio i fitness tracker, saranno tenuti a ottemperare alla legislazione UE sulla cybersecurity.*

2. Soggetti essenziali e importanti

In linea di principio, l'ambito di applicazione della direttiva NIS 2 si estende solo alle società che hanno almeno 50 dipendenti o che raggiungono un fatturato annuo o un bilancio annuo totale superiore ai 10 milioni di EUR. In alcuni casi (ad es. per i fornitori di servizi di comunicazione elettronica accessibili al pubblico), la direttiva NIS 2 si applica sempre e comunque, indipendentemente dalle dimensioni del soggetto.

La direttiva NIS 2 connette la maggior parte dei propri requisiti alla classificazione di un operatore come soggetto "essenziale" o "importante".

I "soggetti essenziali" sono:

- Soggetti che operano nei settori elencati nell'Allegato I, che superano le soglie di almeno 250 dipendenti o di un fatturato annuo oltre i 50 milioni di EUR e un bilancio annuo totale oltre i 43 milioni di EUR
- Prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni
- Fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che superano le soglie di almeno 50 dipendenti o di un fatturato annuo o un bilancio annuo totale di oltre 10 milioni di EUR
- Enti della pubblica amministrazione dell'amministrazione centrale di uno Stato membro (secondo la definizione dello Stato membro)
- Soggetti esplicitamente classificati come "essenziali" da uno Stato membro
- Soggetti identificati come critici ai sensi della direttiva (UE) CER 2022/2557
- Soggetti che, se del caso, lo Stato membro ha identificato come operatori di servizi essenziali, ai sensi della direttiva NIS 1 o della legislazione nazionale

I "soggetti importanti" sono:

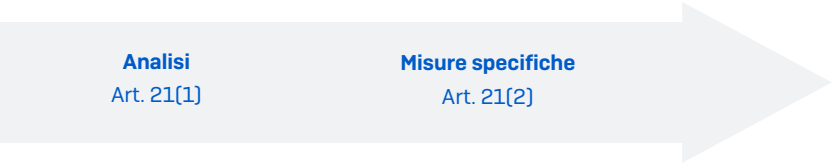
- Soggetti che operano nei settori elencati negli Allegati I o II, che non vengono considerati soggetti essenziali
- Soggetti esplicitamente classificati dagli Stati membri come "essenziali"

SOGGETTO ESSENZIALE	SOGGETTO IMPORTANTE
Settore elencato nell'Allegato I + almeno 250 dipendenti o un fatturato annuo di oltre 50 Mio di EUR e un bilancio annuo totale di oltre 43 Mio di EUR	**Settore elencato negli Allegati I e II +** almeno 50 dipendenti o un fatturato annuo o un bilancio annuo totale di oltre 10 Mio di EUR (se non già determinato come essenziale)
Casi eccezionali, ad es. enti dell'amministrazione centrale, fornitori di servizi DNS o soggetti classificati come essenziali dallo Stato membro	Casi eccezionali indipendentemente dalle dimensioni, ad es. perché classificati come importanti dallo Stato membro

IV. Obbligo centrale: azione di gestione dei rischi

La direttiva NIS 2 prescrive che i soggetti essenziali e importanti intraprendano azioni adeguate e proporzionate in ambito tecnico, operativo e organizzativo, al fine di gestire i rischi alla sicurezza della rete e dei sistemi informatici utilizzati da tali soggetti per svolgere le proprie attività o per fornire i propri servizi, nonché per prevenire e limitare l'impatto di eventuali incidenti sui destinatari dei loro servizi e su altri servizi (Articolo 21(1), direttiva NIS 2).

Le aziende o autorità soggette alla direttiva NIS 2 devono innanzi tutto stabilire le misure necessarie, per poi implementarle in una seconda fase.



1ª Fase: analisi delle misure richieste

Il punto di partenza per valutare le misure da intraprendere in un caso specifico è l'analisi sistematica delle circostanze del singolo caso, tenendo in considerazione il fattore umano e il livello di dipendenza dalla rete e dai sistemi informativi. La proporzionalità delle misure da intraprendere viene determinata dal potenziale impatto socioeconomico di qualsiasi incidente informatico. Più possono essere gravi gli effetti, maggiore sarà l'impegno che il soggetto dovrà investire nell'implementazione delle misure di gestione dei rischi. Alla luce di tutto questo, la mancata applicazione di misure di gestione dei rischi per motivi legati ai costi andrebbe giustificata in maniera approfondita, specialmente nel caso dei soggetti essenziali.

Complessivamente, i requisiti per la gestione dei rischi si basano su un "approccio multirischio": nell'analisi non vanno inclusi solo i rischi "digitali", ma anche quelli fisici.

> **Esempio:**
>
> *Durante l'analisi delle misure di gestione del rischio necessarie, un'azienda tecnologica deve includere sia il rischio implicato da scenari di phishing o pirateria informatica, sia le implicazioni di incidenti dannosi quali furti, incendi (ad es. nel centro dati) o interruzioni della corrente elettrica.*

2ª Fase: Misure specifiche di gestione dei rischi

Come parte di un programma di gestione attiva dei rischi, i requisiti della direttiva NIS 2 includono, nello specifico, le seguenti misure:

- **Politiche:**politiche di analisi dei rischi e di sicurezza dei sistemi informatici
- **Continuità operativa:** ad esempio gestione del backup e ripristino in caso di disastro, e gestione delle crisi
- **Gestione degli incidenti:** gestione degli incidenti di sicurezza
- **Acquisto:** sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità
- **Formazione:** pratiche di igiene informatica di base e formazione in materia di cibersicurezza
- **Cifratura:** politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura
- **Catena di approvvigionamento:** sicurezza della catena di approvvigionamento (supply chain), compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
- **Efficacia:** strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza
- **Altre misure organizzative:** sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi
- **Altre misure tecniche:** uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Come conseguenza dell'obbligo di proteggere la supply chain, anche le aziende non soggette alla direttiva NIS 2 potrebbero essere coinvolte indirettamente. Persino le aziende che non hanno sede nell'UE potrebbero doversi attenere ai requisiti di azione in tema di cybersecurity, per via di un elemento della propria catena di approvvigionamento.

Esempio:

Ai sensi dell'Articolo 21(2) della direttiva NIS 2, una casa costruttrice di autovetture è tenuta a garantire la cybersecurity anche nella propria supply chain. Di conseguenza, per soddisfare l'obbligo di implementare misure di gestione dei rischi in base alla direttiva NIS 2, tale casa costruttrice potrebbe esigere (ad es. come termine contrattuale) l'applicazione di misure di cybersecurity specifiche da parte dei fornitori.

V. Standardizzazione e certificazione

La direttiva NIS 2 permette agli Stati membri di esigere il conseguimento di certificazioni e/o l'utilizzo di prodotti certificati da parte dei soggetti essenziali e importanti. Di conseguenza, per gli operatori potrebbe essere consigliabile optare per soluzioni tecniche certificate, con le quali possano dimostrare l'ottemperanza ai requisiti della direttiva NIS 2 tempestivamente e con basso impatto finanziario. La certificazione di tali prodotti è basata sui programmi europei per le certificazioni di cybersecurity, ai sensi del regolamento sulla cibersicurezza UE (Regolamento (UE) 2019/881).

La direttiva NIS 2 conferisce inoltre alla Commissione europea il potere di implementare atti delegati al fine di esigere che alcune categorie specifiche di soggetti essenziali e importanti adottino soluzioni tecniche certificate oppure ottengano un certificato corrispondente. Tuttavia, i suddetti atti delegati possono essere adottati solo qualora la Commissione abbia precedentemente identificato livelli insufficienti di cybersecurity e abbia stabilito un termine ultimo per l'implementazione.

Si può presumere che in futuro gli Stati membri definiranno, come minimo, gli obblighi corrispondenti. Le aziende devono pertanto seguire attentamente il processo trasformativo di questa autorizzazione in legge, in modo da procurarsi con adeguato anticipo le certificazioni o i prodotti certificati richiesti.

La direttiva NIS 2 prescrive inoltre agli Stati membri di promuovere l'uso di standard europei e internazionali, nonché di specifiche tecniche per la protezione della rete e dei sistemi informativi (ad es. ISO/IEC 27001). Questi standard assumeranno dunque un'importanza ancor più centrale ai sensi della direttiva NIS 2.

VI. Sanzioni pecuniarie per le violazioni

La direttiva NIS 2 prescrive agli Stati membri dell'UE l'obbligo di predisporre sanzioni pecuniarie in caso di violazione dell'Articolo 21 (misure di gestione dei rischi, vedi sopra) e dell'Articolo 23 (obblighi di segnalazione per gli incidenti di sicurezza significativi) della direttiva NIS 2. La direttiva NIS 2 definisce inoltre i valori minimi per il limite massimo delle sanzioni pecuniarie:

SOGGETTI ESSENZIALI	SOGGETTI IMPORTANTI
Sanzioni amministrative pecuniarie fino a 10 milioni di EUR oppure **2% del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.**	Sanzioni amministrative pecuniarie fino a **7 milioni di EUR** oppure **1,4% del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.**

Ciascuna sanzione pecuniaria deve essere aggiunta alle misure di vigilanza e implementazione che un'autorità competente potrebbe imporre nell'eventualità di una (potenziale) violazione.

Esempio:

> *Ai sensi dell'Articolo 32(5) della direttiva NIS 2, gli Stati membri sono tenuti, quando implementano la direttiva, a dotare le autorità competenti di poteri che possono essere intesi come "ultima ratio". Nell'eventualità in cui non venga osservata la conformità alle misure di vigilanza, l'autorità responsabile per l'implementazione della direttiva NIS 2 può richiedere ad altre autorità competenti oppure organi giurisdizionali di impedire temporaneamente che i membri incaricati a svolgere attività di gestione svolgano attività di gestione nel soggetto. Così facendo, gli enti di legislazione europei enfatizzano il principio della cybersecurity quale "attività di gestione" (vedi sopra).*
>
> *La situazione è simile nel settore pubblico: sebbene certe misure di implementazione enunciate dalla direttiva NIS 2 siano esplicitamente non applicabili agli organismi della pubblica amministrazione (ad es. le autorità), verranno applicate le regole di responsabilità per dipendenti pubblici e funzionari pubblici (responsabilità civile) in vigore nello Stato membro.*

All'alta dirigenza di soggetti significativi e importanti si consiglia pertanto di analizzare attentamente e tempestivamente il proprio obbligo di intraprendere azioni di gestione dei rischi, al fine di evitare sanzioni pecuniarie pesanti in caso di violazione.

È ancora da definire se gli organismi della pubblica amministrazione che rientrano ora nell'ambito della direttiva NIS 2 debbano anch'essi essere soggetti a sanzioni pecuniarie. Ai sensi dell'Articolo 34(7) della direttiva NIS 2, spetta ai singoli Stati membri stabilire se e in che misura le entità amministrative debbano essere soggette a sanzioni amministrative pecuniarie.

B. I prodotti Sophos per gli operatori di soggetti essenziali e importanti

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
Capo IV, Articolo 20, Governance		
2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.	**Formazione e certificazioni Sophos**	I corsi di formazione e le certificazioni aiutano Partner e Clienti a ottenere tutti i vantaggi delle implementazioni di sicurezza Sophos; offrono inoltre accesso a personale esperto, dotato di competenze e conoscenze aggiornate in materia di best practice di sicurezza.
	Sophos Phish Threat	Offre simulazioni di attacchi informatici di phishing e corsi di formazione e sensibilizzazione per gli utenti finali delle organizzazioni. I corsi trattano un'ampia selezione di argomenti, da lezioni introduttive su phishing e cybersecurity, fino a informazioni importanti sulla prevenzione della perdita dei dati, sulla protezione con password e molto di più.
Capo IV , Articolo 21, Misure di gestione dei rischi di cibersicurezza		
2. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete... in base a: a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;	**Sophos Intercept X** **Sophos Intercept X for Server**	Offre tecnologie innovative quali deep learning e funzionalità antiexploit e antihacking, integrate nel rilevamento del traffico dannoso, con l'aggiunta di dati di intelligence sulle minacce al fine di prevenire, rilevare e correggere le minacce con estrema facilità su tutti i dispositivi e tutte le piattaforme.
	Sophos Firewall	Sfrutta le tecnologie di machine learning leader di settore di Sophos (incluse in SophosLabs Intelix) per identificare immediatamente i più recenti tipi di ransomware e minacce sconosciute, prima ancora che riescano a infiltrarsi nella rete. Garantisce protezione avanzata dai più recenti attacchi di tipo drive-by e dal malware web mirato; inoltre, offre filtri per URL, siti malevoli e applicazioni web, più filtri basati sul cloud per la protezione degli utenti remoti.
	Sophos Cloud Optix	Monitora e rileva eventuali deviazioni dagli standard di configurazione, prevenendo, rilevando e correggendo automaticamente le modifiche accidentali o intenzionalmente malevole della configurazione delle risorse.
	Funzionalità Synchronized Security nei prodotti Sophos	Condivide dati sulla telemetria e sullo stato di integrità, rendendo possibile l'isolamento coordinato dei dispositivi infetti e abilitando il rilevamento del malware e la correzione dei problemi su server, endpoint e firewall. Questa sinergia consente di bloccare anche gli attacchi più avanzati.
	Sophos Managed Detection and Response (MDR)	Rilevamento e risposta alle minacce 24/7, per identificare e neutralizzare gli attacchi informatici più avanzati che le tecnologie, da sole, non sono in grado di bloccare.
2. b) gestione degli incidenti;	**Sophos Managed Detection and Response (MDR)**	Monitora costantemente i segnali provenienti dall'intero ambiente di sicurezza, incluse le tecnologie per rete, e-mail, firewall, gestione delle identità, endpoint e cloud. Ci consente di rilevare e rispondere in maniera tempestiva e precisa ai potenziali eventi di cybersecurity. Il servizio completo di incident response (IR) è incluso come componente standard, per garantire protezione 24/7 a cura dei nostri esperti di IR. Include reportistica e Root Cause Analysis complete. Il nostro tempo medio necessario per rilevare, indagare e rispondere alle minacce è di soli 38 minuti.
	Servizio Sophos Rapid Response	Offre assistenza tempestiva, grazie all'azione di un team di esperti di incident response che identificano e neutralizzano le minacce attive nella tua organizzazione.
	Synchronized Security nei prodotti Sophos	Condivide dati sulla telemetria e sullo stato di integrità, rendendo possibile l'isolamento coordinato dei dispositivi infetti e abilitando il rilevamento del malware e la correzione dei problemi su server, endpoint e firewall.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	PERCHÉ È UTILE
2. c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	**Sophos Managed Detection and Response (MDR)**	Garantisce il rispetto dei requisiti di protezione delle informazioni nell'ambito della gestione della continuità operativa, grazie al rilevamento e alla risposta 24/7 degli incidenti di sicurezza nell'intero ambiente informatico, sfruttando competenze umane avanzate e tecnologie di intelligenza artificiale all'avanguardia.
	Sophos Intercept X **Sophos Intercept X for Server**	Offre tecnologie innovative quali deep learning e funzionalità antiexploit e antihacking, integrate nel rilevamento del traffico dannoso, con l'aggiunta di dati di intelligence sulle minacce al fine di prevenire, rilevare e correggere le minacce con estrema facilità su tutti i dispositivi e tutte le piattaforme. Include la capacità di ripristinare i file alla loro versione originale in seguito a un'eventuale compromissione da parte di ransomware o di un attacco al record di avvio principale. Fornisce opzioni dettagliate di correzione, grazie alla capacità di eliminare codice malevolo e annullare le modifiche dannose applicate dal malware alla chiave di registro.
	Sophos Cloud Optix	Monitora gli account AWS, Azure e GCP alla ricerca di servizi di archiviazione sul cloud nei quali non sono abilitati i backup pianificati, fornendo istruzioni per la correzione del problema.
2. d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	**Sophos Intercept X with XDR**	Offre un sistema di difesa contro le minacce introdotte da fornitori terzi, che agisce in profondità e che protegge i sistemi con tecnologie di intelligenza artificiale, prevenzione degli exploit, protezione basata sui comportamenti, antiransomware e molto di più. Inoltre, la potente funzionalità XDR consente di identificare automaticamente le attività sospette, di attribuire la giusta priorità agli indicatori di compromissione e di cercare rapidamente potenziali minacce su endpoint e server.
	Sophos Managed Detection and Response (MDR)	Offre opzioni di threat hunting e correzione delle minacce a cura di tecnici esperti, nell'ambito di un servizio completamente gestito. Gli specialisti Sophos sono operativi 24/7 e lavorano instancabilmente per individuare, confermare e risolvere proattivamente le minacce e gli incidenti della supply chain.
	Sophos ZTNA	Difende la tua organizzazione dagli attacchi alla supply chain che cercano di sfruttare l'accesso dei fornitori ai tuoi sistemi interni, con una protezione basata su controlli estremamente granulari degli accessi. Prima di concedere l'accesso alle risorse, questa soluzione basata sul cloud convalida l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri. Autentica le richieste provenienti da Partner attendibili, indipendentemente da dove siano situati.
2. e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;	**Sophos Managed Detection and Response (MDR)**	I nostri esperti di threat hunting monitorano e conducono indagini sugli avvisi provenienti dalla rete. Utilizzano il firewall e gli strumenti di sicurezza per rete, cloud, e-mail ed endpoint per identificare e analizzare eventuali attività sospette, nonché per garantire la protezione dei dati personali, ovunque si trovino. Sophos NDR genera dati di alta qualità e pratici da usare; le informazioni vengono raccolte dall'intera infrastruttura di rete e utilizzate per ottimizzare le difese informatiche. Sophos MDR risponde proattivamente alla divulgazione delle vulnerabilità da parte del Cliente. Non appena riceve la notifica, viene avviata un'indagine completa che cerca tracce di attività di exploit. Se necessario, Sophos MDR provvede a correggere l'incidente e offre consulenza su come incrementare la sicurezza dell'ambiente e prevenire tentativi di exploit in futuro. Per rispondere all'indagine sulla divulgazione delle informazioni, viene fornito un report completo, compilato da esperti umani.
2. f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	**Sophos Managed Detection and Response (MDR)**	Indaga e valuta 24/7 i potenziali rischi di sicurezza nell'intero ambiente, utilizzando i dati di intelligence sulle minacce leader di settore forniti da Sophos X-Ops per identificare i livelli di rischio e assegnare la giusta priorità alle attività di risposta.
2. g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	**Formazione e certificazioni Sophos**	I corsi di formazione e le certificazioni aiutano Partner e Clienti a ottenere tutti i vantaggi delle implementazioni di sicurezza Sophos; offrono inoltre accesso a personale esperto, dotato di competenze e conoscenze aggiornate in materia di best practice di sicurezza.
	Sophos Phish Threat	Offre simulazioni di attacchi informatici di phishing e corsi di formazione e sensibilizzazione per gli utenti finali delle organizzazioni. I corsi trattano un'ampia selezione di argomenti, da lezioni introduttive su phishing e cybersecurity, fino a informazioni importanti sulla prevenzione della perdita dei dati, sulla protezione con password e molto di più.
2. h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	**Sophos Central Device Encryption**	Protegge dispositivi e dati con cifratura completa del disco per Windows e macOS. Verificando lo stato di cifratura, è possibile dimostrare la conformità.
	Sophos Email **Sophos Firewall**	Offre cifratura TLS e supporto di SMTP/S, nonché un portale completo di cifratura con push e opzionalmente con pull.
	Sophos Mobile	Implementa la cifratura dei dispositivi e monitora la conformità ai criteri di cifratura.

REQUISITI DELLA DIRETTIVA NIS 2	SOLUZIONE SOPHOS	COME AIUTA
2. i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;	**Sophos Managed Detection and Response (MDR)**	Gli esperti di threat hunting monitorano e mettono in correlazione l'attività dei sistemi informativi nell'intero ambiente di IT security, identificando e svolgendo indagini sulle attività sospette. Inoltre, esaminano regolarmente i record di attività dei sistemi informativi, ad esempio: log di controllo e di accesso, nonché report di accesso e di tracciabilità degli incidenti di sicurezza.
	Sophos Firewall	La sensibilizzazione degli utenti in tutti gli ambiti del nostro firewall regola ogni aspetto relativo ai criteri e alla reportistica del firewall. Pertanto, garantisce pieno controllo a livello di utente sulle applicazioni e sull'uso della larghezza di banda e di altre risorse della rete.
	Sophos Central	Tiene aggiornati gli elenchi di accesso e le informazioni sui privilegi degli utenti. Applica procedure volte a garantire la revoca dei diritti di accesso qualora i singoli utenti non dovessero più soddisfare le condizioni necessarie per ottenere l'accesso (ad es. perché cambiano ruolo all'interno dell'azienda o perché si dimettono).
	Sophos ZTNA	Permette di ottenere livelli superiori di sicurezza e maggiore agilità durante i cambiamenti di ambiente, semplificando e velocizzando il processo di registrazione e rimozione delle autorizzazioni per utenti e dispositivi. Prima di garantire accesso ad applicazioni e dati, convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri.
	Sophos Cloud Optix	Gestione dell'inventario quando si utilizzano provider di servizi cloud multipli, con monitoraggio continuo delle risorse e visualizzazione completa della topologia e del traffico della rete.
2. j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.	**Sophos Firewall**	Supporta opzioni flessibili per l'autenticazione a più fattori, inclusi i servizi directory, per l'accesso ad ambiti di sistema fondamentali.
	Sophos ZTNA	Prima di garantire accesso ad applicazioni e dati, convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità ai criteri.
	Sophos Central	Utilizza l'autenticazione a due fattori per proteggere gli account degli amministratori e quelli con privilegi elevati.
	Sophos Cloud Optix	Monitora gli account AWS/Azure/GCP, individuando gli accessi da parte di account di utenti root e utenti IAM nei quali l'autenticazione a più fattori è disattivata, per permetterti di risolvere il problema e garantire la conformità alle normative.
Capo IV, Articolo 23, Obblighi di segnalazione		
4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente: una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda: ***una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;***	**Sophos Managed Detection and Response (MDR)**	Non appena riceve la notifica, viene avviata un'indagine completa che cerca tracce di attività di exploit. Se necessario, Sophos MDR provvede a correggere l'incidente e offre consulenza su come incrementare la sicurezza dell'ambiente e prevenire tentativi di exploit in futuro. Per rispondere all'indagine sulla divulgazione delle informazioni, viene fornito un report completo, compilato da esperti umani.
4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente: d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda: ***(ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;***	**Sophos Managed Detection and Response (MDR)**	Sophos MDR indaga e valuta 24/7 i potenziali rischi di sicurezza nell'intero ambiente, sfruttando i dati di intelligence sulle minacce leader di settore forniti da Sophos X-Ops. La Root Cause Analysis completa svolta da Sophos MDR permette di potenziare la sicurezza dell'ambiente e di aggiornare le strategie e i piani di risposta, in modo da integrare le informazioni ottenute.
	Sophos XDR	Non si ferma al livello degli endpoint, ma va oltre, raccogliendo dati approfonditi da origini quali rete, e-mail, cloud e dispositivi mobili, per fornire una prospettiva più ampia dello stato di cybersecurity; inoltre, offre la possibilità di approfondire le analisi dove necessario. I dati raccolti da tutti i prodotti vengono inoltrati al Sophos Data Lake e questo ti permette di rispondere rapidamente a domande critiche per l'organizzazione; potrai inoltre correlare eventi provenienti da varie origini e intraprendere azioni basate su decisioni più informate. Puoi ad esempio effettuare un confronto incrociato con le informazioni relative alla rete e ottenere una prospettiva più ampia dell'incidente o di quello che è accaduto sui dispositivi che sono stati compromessi in un attacco.

2023-05-23 IT-WP (NP)

SOPHOS

Atik Srl | Via Giovanni Cimabue, 35 | 20851 - Lissone (MB) - Italy
www.atik.it | +39 02 39198473 | commerciale@atik.it