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)