SOPHOS
Cybersecurity delivered.

I Principali Controlli Antiransomware E Come Sophos Ti Può Aiutare

Il ransomware è un problema in rapida espansione. Il numero di organizzazioni colpite da un attacco è quasi raddoppiato negli ultimi 12 mesi, passando dal 37% nel 2020 al 66% nel 2021. Inoltre, gli hacker sono anche diventati più abili, poiché l'anno scorso sono riusciti a cifrare i dati delle vittime nel 65% degli attacchi*.

Per bloccare il ransomware occorre prevenire sia gli attacchi con intervento umano diretto (hands-on-keyboard) più avanzati e sferrati da hacker abilissimi, sia quelli basati sul sempre più diffuso modello Ransomware-as-a-Service, che aumenta significativamente l'ambito di azione del ransomware, in quanto richiede meno competenze tecniche.

In questa guida trovi una descrizione dettagliata dei controlli di sicurezza che riducono il rischio di subire un attacco ransomware, più indicazioni su come Sophos ti può aiutare.

CONTROLLO INFORMATICO	COME SOPHOS TI PUÒ AIUTARE	DESCRIZIONE DETTAGLIATA
Individuazione proattiva delle minacce (threat hunting) per rilevare e neutralizzare gli attacchi coordinati da una mente umana, prima che il ransomware possa essere distribuito	Sophos XDR (Extended Detection and Response)	Permette alle organizzazioni di svolgere attività di threat hunting e neutralizzazione delle minacce nei propri ambienti. I rilevamenti possono provenire da endpoint, server, workload del cloud, firewall, e-mail, ambienti cloud pubblici, dispositivi mobili, Microsoft 365 e altro.
	Sophos MTR (Managed Threat Response)	Un servizio completamente gestito e disponibile 24/7 di threat hunting, rilevamento e risposta alle minacce, a cura degli esperti Sophos. I connettori compatibili con una vasta gamma di soluzioni informatiche e di sicurezza, incluso Microsoft 365, estendono la visibilità dei nostri tecnici sull'intero ambiente del cliente, per potenziare le capacità di difesa contro gli attacchi.
Blocco automatico delle minacce di ransomware, prima che possano essere distribuite	Sophos Endpoint e Sophos Workload Protection	Offrono capacità avanzate di protezione antiransomware per fermare l'intera catena di attacco, che includono: › Tecnologie di intelligenza artificiale basate sul deep learning, per bloccare sia il ransomware noto che quello mai osservato prima › Protezione antiexploit, per bloccare gli exploit e le tecniche comunemente utilizzate dai cybercriminali per diffondere malware, prelevare illecitamente le credenziali degli utenti ed eludere il rilevamento › Controllo delle applicazioni, per evitare che sui workload del cloud vengano eseguite applicazioni che potrebbero essere sfruttate dagli hacker per sferrare un attacco › Lockdown dei server, per salvare una configurazione sicura e conosciuta dei workload del cloud e isolarla in quello stato, al fine di impedire ai programmi non autorizzati di eseguirsi. › Tecnologie antiransomware, in grado di rilevare e annullare gli effetti della cifratura non autorizzata, bloccando i processi prima che possano essere infettate anche altre aree della tua rete. Prevengono sia i ransomware basati su file che quelli che sfruttano il record di avvio principale.
	Sophos Email	Analizza automaticamente tutti i processi dei file, tutte le connessioni di rete e tutte le attività dei file e del registro, per bloccare ransomware e altre forme di malware. La protezione antiphishing avanzata, la scansione degli URL e la protezione post-recapito garantiscono che solo i messaggi provenienti da mittenti sicuri possano essere recapitati nella tua casella di posta. Se lo stato dovesse cambiare dopo il recapito, il messaggio viene rimosso automaticamente.
	Sophos Firewall	Difende i sistemi da siti web compromessi e da download pericolosi, grazie a un'ispezione approfondita, basata sulle tecnologie di machine learning ed eseguita nella sandbox. I download dei file vengono analizzati per individuare qualsiasi tipo di attacco ransomware, anche se non è mai stato osservato prima.

CONTROLLO INFORMATICO	COME SOPHOS TI PUÒ AIUTARE	DESCRIZIONE DETTAGLIATA
Identificazione e risoluzione delle lacune di sicurezza, ad esempio dispositivi privi di patch, computer non protetti e altro, al fine di migliorare il livello di sicurezza dell'ambiente.	Sophos XDR (Extended Detection and Response)	Identifica software e sistemi obsoleti e non supportati. Permette di accedere a tutte le applicazioni sul dispositivo, alle informazioni sulla versione, agli hash SHA256 del file, ai dati sulle patch e a vari log, ad esempio la cronologia dell'esecuzione delle applicazioni, le connessioni di rete, i processi padre/figlio ecc. Include query che mettono a confronto le applicazioni installate con dati sulle vulnerabilità disponibili on-line e query che identificano le lacune del profilo di sicurezza nelle impostazioni del registro di sistema.
	Sophos ZTNA	Concede l'accesso remoto sicuro e controllato a sistemi e applicazioni, eliminando la superficie di attacco e la capacità di movimento laterale degli hacker.
Isolamento di Remote Desktop Protocol, per impedire che venga sfruttato dai cybercriminali per ottenere accesso ai sistemi	Sophos Firewall	Permette ai team IT di gestire e isolare facilmente RDP.
	Sophos ZTNA	Abilita l'accesso remoto a RDP e altre applicazioni, senza esporre i sistemi al rischio di attacco.
	Sophos Cloud Optix	Identifica proattivamente le porte RDP esposte, grazie a valutazioni basate sugli standard di settore per la sicurezza sul cloud pubblico. La correzione guidata indica agli amministratori come risolvere i problemi dovuti agli errori di configurazione.
	Sophos XDR (Extended Detection and Response)	Rileva le connessioni RDP e registra le attività nei log. Il terminale remoto consente agli amministratori di attivare/disattivare la policy RDP. Garantisce visibilità sulla policy RDP per tutti i dispositivi gestiti, e ne individua eventuali modifiche.
Pianificazione della strategia di risposta agli incidenti informatici, per minimizzare l'impatto in caso di attacco	Sophos Rapid Response	Offre una risposta agli incidenti rapidissima, a ogni ora del giorno o della notte, a cura dei tecnici specializzati Sophos.
	Sophos MTR (Managed Threat Response)	Garantisce threat hunting, rilevamento e risposta alle minacce come servizio completamente gestito dai nostri esperti e operativo 24/7.
Corsi di formazione e sensibilizzazione di cybersecurity, con test sul phishing	Sophos Phish Threat	Promuove consapevolezza sulla protezione ed educa gli utenti, offrendo opzioni quali: simulazioni di attacchi di phishing, iscrizione automatica a corsi di formazione e sensibilizzazione sulla sicurezza, e funzionalità complete di reportistica. L'integrazione con Sophos Email permette ai team di sicurezza di identificare gli utenti che hanno ricevuto un avviso o a cui è stato proibito di visitare un determinato sito web a causa del relativo profilo di rischio, e arruolarli rapidamente in corsi di formazione.

CONTROLLO INFORMATICO	COME SOPHOS TI PUÒ AIUTARE	DESCRIZIONE DETTAGLIATA
Identificazione e mitigazione delle vulnerabilità negli ambienti cloud, per prevenire i tentativi di exploit da parte dei cybercriminali	Sophos Cloud Optix	Identifica e mitiga proattivamente le vulnerabilità di sicurezza, i ruoli IAM dotati di privilegi eccessivi e gli errori di configurazione degli accessi negli ambienti cloud pubblici, grazie all'integrazione con Amazon Inspector. I problemi di configurazione che possono essere rilevati includono: le porte delle virtual machine esposte a internet, l'abilitazione dell'accesso root remoto e la presenza di versioni vulnerabili di software installati. Riceve patch per le virtual machine Amazon, tramite l'integrazione con AWS Systems Manager. Estende la portata delle scansioni per includere le pipeline di CI/CD, grazie alla scansione degli ambienti Infrastructure-as-Code; allo stesso tempo analizza i registri dei container su Azure, AWS e Docker Hub, individuando eventuali vulnerabilità del sistema operativo.

Per parlare della tua strategia di resilienza informatica e di come Sophos può aiutarti a potenziare le tue difese antiransomware, parla con un commerciale Sophos.

** La Vera Storia Del Ransomware 2022, Sophos, un sondaggio che ha coinvolto 5.600 IT Manager in 31 paesi*

Scopri di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione.

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

© Copyright 2022. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

2022-04-08 (SB-NP)

SOPHOS