SOPHOS
Cybersecurity delivered.

Principales controles contra el ransomware y cómo puede ayudar Sophos

El desafío que representa el ransomware no deja de crecer. La proporción de organizaciones afectadas por el ransomware prácticamente se ha duplicado en doce meses: del 37 % en 2020 al 66 % en 2021. Los adversarios también han tenido más éxito a la hora de cifrar los datos, ya que el 65 % de los ataques del año pasado* comportaron el cifrado de datos.

Detener el ransomware requiere esfuerzos para prevenir tanto los ataques manuales directos perpetrados por adversarios expertos como el modelo de creciente éxito de ransomware como servicio, que amplía significativamente el alcance del ransomware al reducir el nivel de los conocimientos necesarios para desplegar un ataque.

Esta guía detalla los principales controles de ciberseguridad que minimizan la exposición al ransomware y su impacto y cómo puede ayudar Sophos.

Principales controles contra el ransomware y cómo puede ayudar Sophos

CIBERCONTROL	CÓMO PUEDE AYUDAR SOPHOS	INFORMACIÓN DETALLADA
Búsqueda de amenazas proactiva para detectar y neutralizar ataques dirigidos por humanos antes de que se despliegue el ransomware	Sophos XDR (detección y respuesta ampliadas)	Permite a las organizaciones la búsqueda y la neutralización de amenazas en su entorno. Las detecciones pueden proceder de endpoints, servidores, cargas de trabajo en la nube, firewall, correo electrónico, entornos en la nube pública, dispositivos móviles, Microsoft 365, etc.
	Sophos MTR (Managed Threat Response)	Servicio totalmente gestionado de búsqueda, detección y respuesta a amenazas 24/7 por parte de un equipo de expertos de Sophos. Conectores a una gama de soluciones de seguridad y de TI, incluyendo Microsoft 365, que amplían la visibilidad de nuestros operadores en todo el entorno del cliente, lo que incrementa sus capacidades de defensa contra ataques.
Bloqueo automático de amenazas de ransomware antes de que puedan desplegarse	Sophos Endpoint y Sophos Workload Protection	Proporciona capacidades avanzadas de protección contra el ransomware que interrumpen la cadena de ataque en su conjunto, incluyendo: › Inteligencia artificial basada en Deep Learning para prevenir ransomware tanto conocido como desconocido. › Protección de exploits para bloquear los exploits y las técnicas usadas para distribuir malware, robar credenciales y eludir la detección. › Control de aplicaciones para bloquear la ejecución de aplicaciones en cargas de trabajo en la nube que podrían ser usadas por los adversarios para lanzar ataques. › Server Lockdown, que toma una configuración válida conocida de las cargas de trabajo en la nube y bloquea ese estado para impedir la ejecución de programas no autorizados. › Tecnología antiransomware que detecta y revierte cifrados no autorizados, cerrando procesos antes de que puedan propagarse por la red. Protege tanto contra el ransomware basado en archivos como de registro de arranque maestro.
	Sophos Email	Analiza automáticamente todos los procesos de archivos, la actividad de archivos, la actividad del registro y las conexiones de red para bloquear el ransomware y otras formas de malware. La protección avanzada contra phishing, el escaneado de direcciones URL y la protección posentrega aseguran que solo lleguen a su bandeja de entrada remitentes seguros y, si el estado de amenaza de los mensajes entregados cambia, estos se eliminan automáticamente.
	Sophos Firewall	Protege de los sitios comprometidos y las descargas maliciosas con avanzado Machine Learning e inspección en espacios seguros para las descargas de archivos a fin de identificar incluso ataques de ransomware nuevos y desconocidos.

CIBERCONTROL	CÓMO PUEDE AYUDAR SOPHOS	INFORMACIÓN DETALLADA
Identificación y cierre de brechas de seguridad para reforzar su entorno, por ejemplo, dispositivos sin parchear, equipos no protegidos, etc.	Sophos XDR (detección y respuesta ampliadas)	Identifica software y sistemas obsoletos y sin soporte. Proporciona acceso a todas las aplicaciones en el dispositivo, información de versiones, hashes de archivo SHA256, información de parches y sus registros, incluyendo el historial de ejecución de la aplicación, las conexiones de red, los procesos principales/secundarios, etc. Incluye consultas para cotejar las aplicaciones instaladas con la información de vulnerabilidades online, y consultas para identificar las debilidades en la posición de seguridad en la configuración del registro.
	Sophos ZTNA	Posibilita un acceso remoto seguro y granular a sistemas y aplicaciones, eliminando la superficie de ataque y la posibilidad de que los ataques se puedan mover lateralmente.
Bloqueo del protocolo de escritorio remoto para evitar que adversarios puedan usarlo para obtener acceso	Sophos Firewall	Permite a los equipos de TI administrar y bloquear de forma sencilla el protocolo de escritorio remoto (RDP).
	Sophos ZTNA	Permite acceso remoto seguro a RDP y otras aplicaciones sin exponer estos sistemas a un ataque.
	Sophos Cloud Optix	Identifica proactivamente puertos RDP expuestos mediante evaluaciones de seguridad en la nube pública. La remediación guiada proporciona instrucciones a los administradores sobre cómo solventar estos errores en la configuración de seguridad.
	Sophos XDR (detección y respuesta ampliadas)	Detecta conexiones RDP y registra la actividad. Terminal remoto que permite a los administradores activar/desactivar la política RDP. Proporciona visibilidad de la política RDP en todos los servicios administrados y detecta cambios en la misma.
Planificación de la respuesta a ciberincidentes para minimizar el impacto en caso de ataque	Sophos Rapid Response	Proporciona una respuesta a incidentes 24/7 ultrarrápida proporcionada por especialistas de Sophos.
	Sophos MTR (Managed Threat Response)	Proporciona un servicio totalmente gestionado de búsqueda, detección y respuesta a amenazas 24/7 por parte de un equipo de expertos.
Formación de concienciación sobre ciberseguridad y pruebas de phishing	Sophos Phish Threat	Mejora la concienciación en materia de seguridad y forma a los usuarios con simulaciones de ataques de phishing, formación automatizada de sensibilización sobre la seguridad y generación de informes exhaustivos. La integración con Sophos Email permite a los equipos de seguridad identificar de forma eficiente y agilizar la formación de los usuarios a los que se ha avisado o impedido que visiten un sitio web debido a su perfil de riesgo.

CIBERCONTROL	CÓMO PUEDE AYUDAR SOPHOS	INFORMACIÓN DETALLADA
Identificación y mitigación de vulnerabilidades en entornos en la nube para evitar que los adversarios puedan aprovecharlas	Sophos Cloud Optix	Identifica y mitiga proactivamente las vulnerabilidades de seguridad, los roles de IAM con demasiados privilegios y los errores de configuración en los accesos a la red en entornos en la nube pública con integración para Amazon Inspector, incluyendo la exposición de puertos de equipos virtuales a Internet, la habilitación de inicios de sesión root remotos o la instalación de versiones de software vulnerables. Recibe el estado de los parches para los equipos virtuales de Amazon con integración en AWS Systems Manager. Amplía los escaneados de seguridad a los procesos de CI/CD con escaneado de infraestructura como código a la vez que analiza los registros de contenedores en Azure, AWS y Docker Hub en busca de vulnerabilidades del SO.

Para hablar sobre su ciberresiliencia y cómo Sophos puede ayudarle a reforzar sus defensas contra el ransomware, póngase en contacto con un representante de Sophos.

** El estado del ransomware 2022, Sophos, encuesta a 5600 profesionales de TI en 31 países*

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización.

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su empresa estarán protegidos de forma eficaz por productos con tecnologías de inteligencia artificial y Machine Learning.

2022-04-08 (SB-NP)

SOPHOS