SOPHOS

Security made simple.

CHECKLIST: CÓMO PARAR RANSOMWARE

Tecnologías clave y prácticas recomendadas de seguridad

Los ataques de ransomware empiezan de dos formas principales - un correo electrónico trampa con un archivo adjunto malicioso o a través de un sitio web infectado - y luego se abren camino hasta llegar a endpoints y servidores. Para detener estos ataques, es fundamental disponer de una tecnología de protección avanzada en cada fase del ataque y combinar esta protección con buenas prácticas de seguridad del usuario.

Proteger las endpoints y servidores

Si un ransomware accede a sus sistemas, es vital bloquearlo y eliminarlo lo antes posible. Obtenga las tecnologías siguientes:

☐ Tecnología CryptoGuard (disponible en Sophos Intercept X)

Protege endpoints y servidores con una tecnología exclusiva que detiene el ransomware al instante. CryptoGuard complementa su solución de seguridad actual, bloqueando los procesos que intenten realizar cambios no autorizados en sus datos.

- Eficaz contra CryptoLocker, Locky, Zepto, Cerber y muchos más
- Protege contra el cifrado local y remoto
- Revierte los cambios de forma automática, así que no se pierden datos

☐ Prevención de vulnerabilidades (disponible en Sophos Intercept X)

Impide que el ransomware se aproveche de las debilidades en otros productos de software.

☐ Análisis de archivos y de comportamiento HIPS

Examina los componentes y la estructura de los archivos en busca de elementos maliciosos y comprueba si contienen código que intenta modificar el registro.

☐ Protección web

Escanea el contenido web para detectar si tiene código de ransomware.

☐ Detección de tráfico malicioso (MTD)

Detecta el tráfico hacia los servidores de comando y control de ransomware y lo bloquea.

☐ Restricción de aplicaciones

Limita las aplicaciones que pueden ejecutarse y puede bloquear Wscript, a menudo utilizado por los programas de ransomware.

☐ Listas blancas de apps

Establece una política de "bloqueo por defecto" en los servidores para que solo puedan ejecutarse las aplicaciones de confianza, evitando así que el ransomware logre afianzarse.

Detener las amenazas de correo electrónico

La puerta de enlace de correo es la primera línea de defensa contra correos electrónicos maliciosos que contengan ransomware. Asegúrese de que incluya:

☐ Tecnología antivirus y anti-spam

Bloquea emails con ransomware, como los archivos adjuntos maliciosos con macros, y detiene otras amenazas de correo electrónico.

☐ Protección en el momento del clic

Evita que los usuarios hagan clic en enlaces a sitios web que alojen ransomware, aunque el enlace sea seguro al entrar en la bandeja de entrada.

☐ Espacio seguro en la nube

Detecta amenazas de día cero como ransomware al realizar pruebas con archivos en un entorno seguro antes de que el usuario los ejecute.

Detener las amenazas web

La puerta de enlace web bloquea el ransomware procedente de Internet antes de que llegue a las estaciones de trabajo de los usuarios. Busque lo siguiente:

☐ Filtrado de direcciones web

Bloquea los sitios web que alojan ransomware e impide que este se comunique con sus servidores de comando y control.

☐ Filtrado web

Impone estrictos controles en tipos de archivos relacionados con el ransomware, impidiendo que se descarguen.

☐ Espacio seguro en la nube

Detecta amenazas de día cero como ransomware al realizar pruebas con archivos en un entorno seguro antes de que el usuario los ejecute.

Nueve buenas prácticas de seguridad para aplicar hoy mismo

Las buenas prácticas en seguridad TI, incluida la formación continua de los empleados, son componentes esenciales de todas y cada una de las configuraciones de seguridad. Asegúrese de seguir estas nueve mejores prácticas:

☐ Realice copias de seguridad periódicamente y guarde una copia de seguridad reciente fuera de la red y sin conexión

Guardar datos fuera de la red y sin conexión significa que el ransomware no puede acceder a ellos. Si dispone de copias de seguridad recientes, puede minimizar las pérdidas de datos.

☐ Habilite las extensiones de archivo

Al habilitar las extensiones resulta mucho más fácil detectar los tipos de archivo que usted o sus usuarios no suelen recibir habitualmente, como JavaScript.

☐ Abra los archivos JavaScript (.JS) con el Bloc de notas

Abrir un archivo JavaScript con el Bloc de notas impide que ejecute código malicioso y le permite examinar su contenido.

☐ No habilite las macros de los documentos adjuntos que reciba por correo electrónico

Muchas infecciones dependen de que usted active las macros, así que no se deje convencer.

☐ Tenga cuidado con los archivos adjuntos no solicitados

Si no está seguro, no lo abra. Si es posible, consulte al remitente.

☐ No se conceda más derechos de los que necesita

Disponer de derechos de administrador podría significar que una infección local se convierta en un desastre en la red.

☐ Plantéese instalar los visores de Microsoft Office

Estas aplicaciones de visualización le permiten echar un vistazo al documento sin abrirlo en Word o Excel.

☐ Aplique los parches con prontitud y frecuencia

Cuanto más pronto aplique las revisiones de software, menos agujeros existirán para que los explote el ransomware.

☐ Manténgase al día sobre las nuevas funciones de seguridad en sus aplicaciones empresariales

Por ejemplo, ahora Office 2016 incluye un control llamado "Bloquear la ejecución de macros en archivos de Office procedentes de Internet".

Siempre seguro con Sophos

Para detener el ransomware antes de que le detenga a usted, necesita implementar la protección adecuada. Utilice la tecnología CryptoGuard en Sophos Intercept X para evitar que el ransomware cifre sus archivos. Asegúrese también de disponer de las tecnologías anti-ransomware adecuadas en la puerta de enlace de correo, la puerta de enlace web, el firewall y los servidores para detener estas amenazas antes de que lleguen a sus endpoints. Esta combinación es la mejor manera de evitar que el ransomware secuestre sus datos y su negocio.

Para obtener más información sobre la protección contra el ransomware

visite es.sophos.com/ransomware

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Latin America
Correo electrónico: Latamsales@sophos.com

08-09-2016 CL-NA (RP)