SOPHOS

Lista de tecnologías, herramientas y tácticas para una protección web eficaz

Para poner en práctica una estrategia de protección web eficaz, son necesarias políticas que reduzcan la superficie susceptible a ataques, herramientas y tecnologías adecuadas para imponer dichas políticas y protección para bloquear ataques en todas las capas.

Establezca las siguientes políticas recomendadas e informe a los usuarios sobre la importancia de su papel en la seguridad de la empresa.

Lista de políticas de protección web	
Política de navegación segura	Bloquee categorías de sitios inadecuados y no deseados para reducir la exposición a las amenazas. Como mínimo, la política debe excluir las categorías siguientes: › Contenido para adultos, sexualmente explícito › Servidores proxy anónimos › Actividades delictivas, ataques informáticos › Juegos de azar › Drogas, alcohol y tabaco › Intolerancia y odio › Suplantación de identidades, fraude, correo no deseado, programas espía › Ofensivo y de mal gusto › Violencia y armas Puede controlar otras categorías adicionales para mejorar el ancho de banda y la productividad.
Política de contraseñas seguras	Siga estas pautas para imponer políticas que obliguen a crear contraseñas seguras: › Utilice contraseñas largas › Incluya números, símbolos y caracteres en mayúscula y minúscula › No utilice términos comunes del diccionario › No utilice información personal como nombres o cumpleaños › Cambie las contraseñas con frecuencia › No anote las contraseñas
Política de restricción de aplicaciones	Limite la cantidad de navegadores, aplicaciones y complementos de Internet utilizados en la empresa a un grupo estandarizado e imponga su uso como norma. › Navegador: utilice un único navegador mayoritario que sea compatible con la API de navegación segura de Google como Google Chrome, Firefox o Apple Safari › Java: a menos que necesite Java para aplicaciones web relacionadas con el negocio, desactívelo, elimínelo o limítelo a los usuarios que lo necesiten › Lector de PDF: utilice un único lector de archivos PDF mayoritario e instale todos los parches › Reproductor multimedia: evite complementos y paquetes de códecs innecesarios para los reproductores multimedia. Si es posible, utilice solamente lo que le proporciona el sistema operativo e instale todos los parches del sistema operativo › Complementos y barras de herramientas: evite complementos y barras de herramientas innecesarios en los navegadores
Política de administración de parches	Asegúrese de que las aplicaciones siguientes tienen activadas las actualizaciones automáticas siempre que sea posible y de que los usuarios aplican las actualizaciones y los parches en cuanto estén disponibles. › Navegador web › Java › Lector de PDF › Reproductor de flash

Lista de tecnologías, herramientas y tácticas para una protección web eficaz

Para imponer las políticas y ofrecer protección contra los ataques web más recientes, son necesarias las herramientas y tecnologías siguientes.

Lista de herramientas y tecnologías de protección web	
Filtrado de direcciones web	Para imponer la política de navegación segura, es necesario un filtro eficaz de direcciones web. Busque una solución que no le sature con cientos de categorías y con excepciones sencillas. La solución debería permitir a los usuarios enviar fácilmente solicitudes de excepciones y al departamento informático ocuparse de estas con unos cuantos clics.
Filtrado de sitios web maliciosos	Para protegerse contra sitios maliciosos, asegúrese de que cuenta con un filtrado por reputación eficaz. Busque una solución que se actualice en tiempo real y de un proveedor con operaciones globales de análisis de amenazas y seguimiento continuo de los sitios recién infectados.
Bloqueo de servidores proxy anónimos	Utilice tecnologías para bloquear el uso inadecuado de servidores proxy anónimos que intentan burlar el filtrado de direcciones web. Busque una solución que incluya tanto bloqueo de categorías como detección dinámica de servidores proxy anónimos en tiempo real para bloquear servidores proxy nuevos, ocultos y de creación propia.
Filtrado de correo no deseado	Asegúrese de que la solución anti-spam elegida utiliza la tecnología más reciente para bloquear mensajes de correo electrónico no deseados o inadecuados con enlaces de suplantación de identidades o maliciosos, uno de los principales puntos de entrada de los ataques web actuales.
Detección avanzada de programas maliciosos de Internet	Todo el tráfico web debería escanearse con la tecnología contra programas maliciosos web avanzados más reciente. Busque una solución que escanee todo el tráfico web (no solo los sitios peligrosos) sin afectar a la latencia ni al rendimiento. Asegúrese de que la solución elegida utiliza la tecnología más reciente (como simulación de JavaScript) para detectar amenazas ocultas o polimorfas.
Escaneado de HTTPS	Proteja uno de los principales agujeros de la protección web con una solución que escanee el tráfico cifrado. Asegúrese de que la solución no afecta al rendimiento y de que puede proteger la privacidad de los usuarios que visitan sitios de banca por Internet o financieros.
Detección de comunicación saliente	En el caso de que se produjera una infección, asegúrese de que la solución elegida puede identificar los equipos infectados presentes en la red mediante las solicitudes de direcciones web conocidas de comando y control de programas maliciosos.
Protección externa	Proteja a los usuarios que se encuentran fuera de la red corporativa con una solución que proporcione protección web de estaciones o filtrado basado en la nube. La protección web de estaciones puede integrarse en el antivirus de escritorios para administrar menos software y ofrecer protección web sin interconexiones ni redirecciones del escaneado en la nube. Busque una solución que permita administrar usuarios externos con la misma consola que utiliza para los usuarios que se encuentran en la red.
Actualizaciones en tiempo real	Asegúrese de que el sistema ofrece actualizaciones en directo sin retrasos. Las actualizaciones diarias o a cada hora de las amenazas ya no son adecuadas.
Restricción de aplicaciones	Imponga la política de aplicaciones web con las herramientas adecuadas para impedir la instalación o ejecución de aplicaciones no deseadas en las estaciones. El filtrado a nivel de las aplicaciones de la puerta de enlace de red puede ser útil para controlar el ancho de banda y la productividad, pero es importante restringir las aplicaciones en las estaciones.
Control de parches	Imponga la estrategia de parches más fácilmente con una solución que identifique y ordene por prioridad los parches de seguridad más importantes de los programas web cliente seleccionados.
Antivirus con HIPS	Elija un producto antivirus de escritorio para las estaciones con tecnología de prevención de intrusiones en el host (HIPS) incorporada. Busque una solución con reglas de HIPS recomendadas incluidas para no tener que averiguar la configuración de la protección contra amenazas más efectiva por su cuenta.

Sophos Web Protection

Además de esta lista de tecnologías importantes, asegúrese de que las funciones cuentan con el respaldo de un proveedor de seguridad informática comprometido a ofrecer la máxima protección. Busque un proveedor con operaciones globales de análisis de amenazas que vigile constantemente la aparición de amenazas nuevas y ofrezca actualizaciones instantáneas.

Asimismo, busque una solución que no solo ofrezca protección eficaz, sino que sea también fácil de implementar y administrar. La seguridad, cuanto más simple, más eficaz.

Las cinco fases del ataque de un programa malicioso

Descargar

Inscríbase en Sophos.com para realizar una evaluación gratuita

Puerta segura de enlace a Internet de Sophos
Sophos EndUser Web Protection Suite

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

Oxford (Reino Unido) | Boston (EE. UU.)

NP 10/13 NSG na