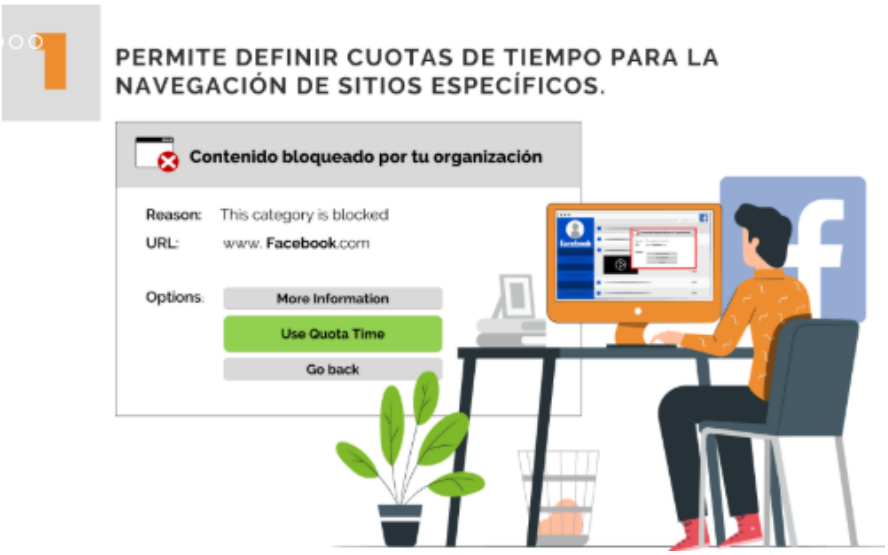
Web Security



FILTRADO DE CONTENIDO

SEGURIDAD WEB

Elimina riesgos de seguridad web como virus, programas espías y robo de identidad, ya sea para modalidad Home Office y/o Oficina. Para evitar el mal desempeño en el acceso a Internet, incrementado la productividad.

Las capacidades son:

- Filtrado de contenido: Reduce el riesgo de URLs maliciosas
- Maximiza la productividad de tus empleados
- Filtrado de trafico Cifrado (https)
- Filtrado de contenido de páginas dentro de páginas web 2.0
- DLP integrado: evita la fuga de información
- Análisis de imágenes
- Análisis forense: Reporte detallado de la actividad de los usuarios en internet
- Web Mobile: Protección a usuarios móviles

Beneficios

- Habilita un servicio de internet seguro dentro y fuera de la red corporativa
- Elimina riesgos de seguridad web como virus, programas espía y robo de identidad
- Bloqueo de contenido no apto para el negocio
- Incrementa la productividad

Seguridad de aplicaciones web

La seguridad de aplicaciones web es una rama de la Seguridad Informática que se encarga específicamente de la seguridad de sitios web, aplicaciones web y servicios web.

A un alto nivel, la seguridad de aplicaciones web se basa en los principios de la seguridad de aplicaciones pero aplicadas específicamente a la World Wide Web. Las aplicaciones, comúnmente son desarrolladas usando lenguajes de programación tales como PHP, JavaScript, Python, Ruby, ASP.NET, JSP, entre otros.

Amenazas de seguridad

Con la aparición de la Web 2.0 (El término 'Web 2.0' o 'Web social' comprende aquellos sitios web que facilitan compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web. Web 2.0 permite a los usuarios interactuar y colaborar entre sí, como creadores de contenido. La red social conocida como web 2.0 pasa de ser un simple contenedor o fuente de información; la web en este caso se convierte en una plataforma de trabajo colaborativo.) el intercambio de información a través de redes sociales y el crecimiento de los negocios en la adopción de la Web como un medio para hacer negocios y ofrecer servicios, los sitios web son constantemente atacados. Los hackers buscan, ya sea comprometer la red de la corporación o a los usuarios finales, accediendo al sitio web y obligándolos a realizar drive-by downloading.

Como resultado, la industria está prestando mayor atención a la seguridad de aplicaciones web, así como a la seguridad de las redes de computadoras y sistemas operativos.

La mayoría de los ataques a aplicaciones web ocurren a través del **cross-site scripting** (XSS es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar) e inyección SQL(es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.) El cual comúnmente resulta de una codificación deficiente y la falta de desinfección de las entradas y salidas de la aplicación web.

El Phishing(Es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace). Para

realizar el engaño, habitualmente hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.) es otra amenaza común de las aplicaciones Web. "RSA, la División de Seguridad del EMC, anuncio hoy lo hallado en su reporte sobre fraude de enero de 2013, estimando las pérdidas globales debido al phishing en $1.5 billones en 2012".

De acuerdo con el proveedor de seguridad Cenzic, las principales vulnerabilidades durante marzo del 2012 fueron:

37%	Cross Site Scripting
16%	Inyección SQL
5%	Path disclosure
5%	Ataque de denegación de servicio
4%	Ejecución de código arbitrario
4%	Corrupción de memoria
4%	Cross Site Request Forgery
3%	Violación de datos (divulgación de información)
3%	Inclusión de archivos arbitraria
2%	Inclusión local de archivos
1%	Inclusión remota de archivos
1%	Desbordamiento de búfer
15%	Otros, incluyendo inyección de código (PHP/JavaScript), etc.

Seguridad web de Cisco

Las peligrosas amenazas avanzadas se pueden ocultar a plena vista en sitios web legítimos o en publicidades emergentes atractivas. Los empleados o invitados pueden poner su organización en riesgo haciendo clic en donde no deberían. Cisco Web Security Appliance (WSA), desarrollada por Cisco Talos, lo protege bloqueando automáticamente los sitios de riesgo y comprobando sitios desconocidos antes de permitir que los usuarios lleguen a estos a través de un enlace, mejorando así el cumplimiento.

Características

Protección antes, durante y después de un ataquemonitoreo y análisis

Obtenga un monitoreo y análisis en toda la red. Cuando se produce una situación de riesgo, determine rápidamente el alcance del daño, soluciónelo y logre que las operaciones vuelvan a la normalidad.

Opciones flexibles de implementación

Ejecute la seguridad web en un equipo, como una máquina virtual, e inclusive en un router de sucursal, sin cargo adicional. Dentro de esta solución de seguridad abierta, puede escalar a medida que crece su empresa. Proteja las sucursales sin regresar el tráfico al gateway corporativo.

Análisis automatizado de tráfico entrante y saliente

Analice todo el tráfico web en tiempo real para malware tanto conocido como nuevo. Use reputación dinámica y análisis basado en comportamiento en todo el contenido web.

Control y Visibilidad de las Aplicaciones

Entérese de lo que ocurre en su red y contrólelo. Cree e implemente políticas granulares para sitios web como Facebook y LinkedIn con aplicaciones integradas. Es simple, para que pueda proteger sin retrasar la productividad o sobrecargar los recursos de TI.

Identificación rápida de ataques de día cero

Analice en busca de actividades sospechosas a través del tiempo para detectar comportamientos anormales. Use capacidades retrospectivas con Advanced Malware (AMP) for Web Security para volver el tiempo atrás y eliminar el malware en dispositivos infectados.

Textos tomados de:

https://www.vdvnetworks.com/servicios/filtrado-de-contenido/?gclid=Cj0KCQjwrIf3BRD1ARIsAMuugNvNNWkpLDXg08LPjOOk_Vw24IuserQJvhMktwRMe34W74_uXOMgK_caAmc-EALw_wcB

https://es.wikipedia.org/wiki/Seguridad_de_aplicaciones_web

https://www.cisco.com/c/es_mx/products/security/web-security-appliance/index.html#~stickynav=1