McAfee Email Protection

Protección avanzada para buzones de correo en cualquier momento y cualquier lugar

Las empresas necesitan, ahora más que nunca, una protección avanzada del correo electrónico. Según el SANS Institute, el 95 % de los ataques a redes son el resultado directo de phishing selectivo[1]. Los usuarios siguen mordiendo el anzuelo de las técnicas de ingeniería social y los ciberdelincuentes han ampliado su repertorio para incluir otras tácticas inteligentes capaces de pillar desprevenidas incluso a las organizaciones conscientes de la importancia de la seguridad. El malware avanzado y la pérdida de propiedad intelectual corporativa son problemas cada vez mayores que pueden tener consecuencias importantes en cualquier empresa. El nivel de riesgo también puede incrementarse porque las empresas están empezando a trasladar su correo electrónico a buzones de correo alojados en la nube. Por último, la falta de flexibilidad de las soluciones de protección de correo electrónico antiguas puede obligarlas a buscar una alternativa mejor. McAfee® Email Protection es la respuesta. Esta potente solución proporciona protección frente a las amenazas de phishing selectivo en toda la empresa y viene equipada con tecnología integrada de prevención de pérdida de datos (DLP) y continuidad del correo electrónico. Gracias a las opciones de despliegue flexibles —en la nube, in situ o con la solución híbrida—, podrá implementar la seguridad del correo electrónico como y cuando lo desee.

Principales ventajas

Protección frente a ataques selectivos de phishing

- Detecta en tiempo real las amenazas de las URL maliciosas con ClickProtect.
- Se integra con McAfee Advanced Threat Defense para proteger frente al malware oculto.
- Incorpora la tecnología de prevención de pérdida de datos.

Seguridad para buzones de correo alojados

- Protección frente a ataques selectivos vaya donde vaya el correo electrónico.
- Controles de correo no deseado para el usuario final.
- Continuidad del correo electrónico.
- Funciones diferenciadas de protección frente a pérdidas de datos y cifrado.

Opciones de despliegue flexibles

- Despliegue como y cuando lo desee.
- Opciones de despliegue híbrido con administración única y consola de reportes.

Más allá de la ingeniería social: nuevas tácticas de phishing selectivo

Cuando se trata de ataques de phishing, el eslabón más débil es el usuario. El reporte *The Verizon Data Breach Investigation Report, 2014* (Reporte sobre las investigaciones de fugas de datos de 2014 de Verizon)[2] señala que casi uno de cada cinco usuarios hace clic en los vínculos de los mensajes de correo electrónico de phishing. Los ciberdelincuentes siguen aprovechándose de la vulnerabilidad de los usuarios frente a la ingeniería social, pero han dado un paso más y ahora emplean otras tácticas sofisticadas que dificultan la identificación de las amenazas del correo electrónico. He aquí algunos ejemplos:

- **URL de un solo uso:** los ciber-delincuentes eliminan las URL maliciosas en cuanto los usuarios son víctimas del phishing y se produce la infección. De este modo, la detección y el análisis forense son más difíciles, si no imposibles.
- **Infección diferida:** en algunos casos, los agresores esperan a que el mensaje de correo esté analizado, aprobado y entregado en las bandejas de entrada corporativas para soltar la carga útil en el sitio web elegido como blanco. Los empleados suelen confiar en los mensajes que reciben en el trabajo y pueden acabar haciendo clic en un vínculo malicioso.
- **Malware preparado para entornos aislados:** este tipo de código malicioso permanece latente para eludir la detección y causa estragos más adelante.

intel Security

Defensas avanzadas por capas

Protección en el momento del clic
McAfee Email Protection ofrece múltiples capas de protección para ayudarle a esquivar los ataques sofisticados del phishing selectivo y el malware sigiloso que los acompaña. Gracias al motor McAfee Gateway Anti-Malware Engine, número uno en el mercado[3], de McAfee Web Gateway, McAfee Email Protection protege frente a URL maliciosas en el momento de hacer clic y en el momento del análisis con ClickProtect, que funciona en cualquier dispositivo y en cualquier lugar para neutralizar los intentos de phishing selectivo. ClickProtect detecta y elimina las amenazas de las URL que incluyen los mensajes de correo electrónico. Busca variaciones en la intención de una URL entre el momento en que se analiza el mensaje —por inofensivo que parezca— y el instante en que el usuario hace clic en ella.

Analicemos un caso de malware diferido en el que el agresor crea un mensaje de correo electrónico que contiene una URL aparentemente legítima para el director financiero de una empresa. La solución de seguridad del correo electrónico recibe el mensaje, lo examina, lo considera seguro y lo entrega en la bandeja de entrada correspondiente. Pero cuando el mensaje se encuentra en la bandeja del director financiero, el agresor carga el malware en la página web de destino. Si el director hace clic en el vínculo, la red de la empresa se infectará.

En el momento en el que se hace clic en la URL de un mensaje de correo electrónico, ClickProtect se pregunta: "¿Sigue siendo segura esta URL?". McAfee Gateway Anti-Malware Engine utiliza la emulación de comportamiento para reescribir e inspeccionar todas las URL distribuidas y detectar contenido web malicioso sin depender de las firmas.

Con la vista previa, los usuarios pueden ver los sitios web maliciosos de forma segura y aprender las mejores prácticas, lo que añade otra capa de seguridad y reduce el riesgo en general. El correo electrónico puede reenviarse sin riesgos y, aunque los destinatarios no tengan ClickProtect, la protección acompaña al mensaje donde quiera que vaya.

Detección y bloqueo del malware oculto
Gracias a la integración con McAfee Advanced Threat Defense, McAfee Email Protection puede detectar y bloquear el malware de tipo zero-day oculto en archivos adjuntos sospechosos antes de que el mensaje llegue a la bandeja de entrada. Esta innovadora estrategia por capas combina análisis de código estático en profundidad (ingeniería inversa) y análisis dinámicos (entorno aislado) para analizar el comportamiento real del malware. El análisis de código estático proporciona información detallada de clasificación del malware, amplía la protección frente a amenazas muy camufladas y evasivas, y permite la identificación de malware asociado aprovechando la reutilización de código. Las rutas de ejecución retardada o eventual, que no suelen procesarse en un entorno aislado dinámico, pueden detectarse gracias a la descompresión y al análisis del código completamente estático.

Prevención de pérdida de datos incorporada
En última instancia, los ataques de phishing selectivo tienen un objetivo claro: apropiarse de datos valiosos y confidenciales. McAfee Email Protection está provisto de la tecnología de nuestras soluciones DLP, líder en el mercado. Se incluyen, además, diccionarios de contenido integrado para el sector de tarjetas de pago (PCI-DSS), asistencia sanitaria, información financiera, legislación local sobre protección de la intimidad, etc., que permiten crear directivas sobre cumplimiento de normativas relacionadas con la identificación, el almacenamiento y la transmisión de datos confidenciales.

Mediante la creación y el almacenamiento de huellas digitales de documentos seleccionados, McAfee Email Protection "aprende" qué tipo de contenido debe estar controlado y protegido por las directivas. La herramienta de expresiones regulares, los diccionarios personalizables, los contadores de umbral, el análisis exhaustivo de contenidos en más de 300 tipos de documentos y las listas blancas le permiten crear e implementar directivas sobre archivos adjuntos y contenido para diferentes grupos de usuarios de la organización.

McAfee Email Protection incluye cifrado del correo electrónico integrado (push/pull) o cifrado TLS, S/MIME o PGP para el despliegue como dispositivo virtual, dispositivo físico o servidor blade, sin costo adicional.

McAfee Email Gateway

Entornos de dispositivos virtuales y requisitos del sistema

- VMware vSphere 4.x o superior
- VMware vSphere Hypervisor (ESXi) 4.x o superior
- Procesador: dos procesadores virtuales
- Memoria virtual disponible: 2 GB
- Espacio libre en el disco duro: 80 GB

Dispositivo de hardware

- Disponible en dos modelos; se vende por separado
- También disponible en formato de servidor blade

Por tercer año consecutivo, McAfee Email Protection ha recibido **cinco estrellas en la revista SC Magazine**.

Continuidad del correo electrónico para la continuidad empresarial

Las empresas no se detienen cuando la red de correo electrónico experimenta una interrupción. Cuando se produce una caída de la red debido a desastres naturales, cortes de electricidad o trabajos de mantenimiento regulares, McAfee Email Protection ofrece opciones para mantener a los empleados, clientes, partners y proveedores conectados permanentemente. La función de continuidad del correo electrónico conserva todos los mensajes enviados o recibidos durante la interrupción, sincronizando de forma inteligente un registro exacto de toda la actividad de mensajes durante ese periodo hasta que los servidores de correo electrónico vuelven a estar disponibles.

Información y reputación de amenazas

McAfee Email Protection cuenta con otra eficaz herramienta en su arsenal, McAfee Global Threat Intelligence (McAfee GTI), el servicio de información sobre amenazas más exhaustivo del sector, que reúne y redistribuye datos en tiempo real de más de 100 millones de sensores de todos los vectores de amenazas (archivos, Web, correo electrónico y red). El análisis de reputación de McAfee GTI minimiza los riesgos porque bloquea los mensajes de correo electrónico que provienen de fuentes sospechosas, contienen vínculos de sitios web sospechosos o llevan datos adjuntos maliciosos.

Al reducir considerablemente la probabilidad de que se infiltren en la red el malware, los ataques de phishing y los ataques de amenazas persistentes avanzadas, su organización trabaja con más seguridad y disminuye la necesidad de costosas medidas de corrección.

Retos para la seguridad del correo electrónico alojado

Cada vez hay más direcciones de correo electrónico corporativo suministradas por servicios de correo electrónico alojado, como Microsoft Office 365, Google Apps for Work y otros. Muchas soluciones de correo electrónico alojadas ofrecen la seguridad como parte de sus servicios. Pero, ¿es suficiente?

Probablemente no, ya que siguen proliferando los intentos de phishing, el spam y el correo electrónico no deseado, y las funciones de seguridad incorporadas no están equipadas para impedir la filtración de datos. Además, las interrupciones del funcionamiento del correo electrónico asociadas a Office 365, por ejemplo, pueden afectar a la productividad. McAfee Email Protection protege a toda la empresa frente a los ataques selectivos de phishing y el malware avanzado durante las fases de prueba, migración y posmigración. Sea cual sea el momento y el lugar en el que se despliegue sus buzones de correo, McAfee Email Protection proporciona cobertura total y continuidad del correo electrónico.

Opciones de despliegue flexibles para ahora y para el futuro

McAfee Email Protection le proporciona la flexibilidad que necesita para desplegar la seguridad del correo electrónico como desee. Puede elegir entre la solución SaaS (software como servicio) basada en la nube, la solución in situ (dispositivo virtual, dispositivo físico o servidor blade) y la combinación híbrida de ambas. Con McAfee Email Protection, podrá desplegar la seguridad de su correo electrónico del modo que mejor se adapte a sus necesidades actuales, así como ampliarla o cambiar de modalidad en el futuro.

Independientemente de su elección, McAfee Email Protection le proporciona una única consola de administración centralizada y reportes consolidados que permiten medir fácilmente la eficacia de los programas de seguridad del correo electrónico. Las directivas se aplican tanto a los componentes de la solución basada en la nube como a los desplegados in situ.

Si desea obtener más información o iniciar una evaluación de McAfee Email Protection, póngase en contacto con su representante de McAfee o visite **www.mcafee.com/mx/products/email-and-web-security/email-security.aspx**.

1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST: *McAfee Web Gateway Security Appliance Test* (Prueba del dispositivo de seguridad McAfee Web Gateway)

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com