CIBERSEGURIDAD ESENCIAL PARA PEQUEÑAS Y MEDIANAS EMPRESAS

DESCRIPCIÓN GENERAL

Numerosos reportes del sector indican que las pequeñas y medianas empresas (pymes) corren un riesgo especial de ser víctimas de los ciberdelincuentes sofisticados. De hecho, el 77 % de todos los ciberdelitos están dirigidos a pymes. Pero las limitaciones económicas dificultan que las pymes obtengan los recursos necesarios para protegerse de las amenazas avanzadas.

Uno de los cimientos básicos de la seguridad debe ser una estrategia de detección y prevención para protegerse de las amenazas avanzadas y un plan de respuesta inmediata para los incidentes imprevistos. Las galardonadas tecnologías de FireEye ayudan a detectar y detener los ataques escalonados y multivectoriales. Proporcionan información precisa y contextual a los equipos de seguridad para que ejecuten inmediatamente un plan de respuesta, ya sea por sí mismos o a través de un partner. Además, los servicios de FireEye y sus partners complementan estas tecnologías proactivas para ayudar a las organizaciones a responder a los incidentes.

Estas eficientes soluciones están diseñadas para que las pymes accedan a ellas y las utilicen con facilidad, y así puedan centrarse en el crecimiento de su negocio.

EL PROBLEMA

Los gobiernos y las grandes empresas conocen desde hace tiempo la existencia de las amenazas avanzadas y por este motivo han implementado marcos de seguridad y adoptado tecnologías gradualmente para reducir el riesgo y el impacto de las fugas de datos. Normalmente, estas organizaciones tienen un presupuesto de seguridad flexible o bien su gasto en seguridad está justificado por obligaciones legales o normativas. El problema para las pymes es que carecen de las ventajas de sus homólogos de mayor envergadura, pero se enfrentan a riesgos similares.

Aunque las noticias tienden a centrarse en las grandes brechas de seguridad, las pymes son a menudo los blancos principales de la ciberdelincuencia[1]. ¿Por qué? Porque tienen más activos (números de tarjetas de crédito, información de identidad, datos médicos, propiedad intelectual) que una persona física, pero menos seguridad que las grandes empresas, lo que las convierte en el "blanco perfecto".

A muchas pymes también las eligen como objetivo porque prestan servicios de externalización de procesos empresariales (BPO, por sus siglas en inglés) o servicios basados en la tecnología de la información (ITES, del inglés) a organizaciones más grandes. Los agresores aprovechan esta confianza, se infiltran en el eslabón más débil y después se desplazan lateralmente a un objetivo de mayor importancia. Los agresores suelen tomar el sendero de menor resistencia para alcanzar sus metas.

Las grandes empresas cada vez examinan más detenidamente su cadena de suministro para identificar a los proveedores que puedan demostrar un alto grado de diligencia en seguridad. Las pymes necesitan implementar un mayor nivel de funciones avanzadas de prevención y detección para satisfacer esos requisitos y prosperar.

A causa de su deficiente seguridad, los mensajes de correo electrónico de phishing selectivo y el ransomware son riesgos cada vez mayores para las pymes. Quizá ellas no se consideren un objetivo en sí mismas, pero la debilidad de su seguridad las convierte en blancos fáciles para la estrategia relámpago del ransomware.

Las tecnologías de seguridad tradicionales basadas en firmas son ineficientes frente a estas amenazas porque estas suelen ser polimórficas y están diseñadas intencionadamente para no mostrar firmas anteriores. Al final, las pymes tienen que abordar el riesgo de las amenazas avanzadas y el ransomware, ya que se calcula que la mitad de las pymes que sufren un ciberataque se ven obligadas a cerrar el negocio en cuestión de seis meses[2].

1 Symantec. "2015 Internet Security Threat Report" (Informe sobre las amenazas a la seguridad en Internet, 2015). Abril de 2015

2 https://staysafeonline.org/

FireEye

LA SOLUCIÓN

Para defenderse de los agresores sofisticados actuales se precisa una solución que prevenga y detecte amenazas avanzadas. Para ello, deben:

- Conocer los principales vectores de amenazas y las actividades maliciosas que tienen lugar en estos vectores.
- Detectar las nuevas amenazas, incluidos los ataques desconocidos (tipo día cero), así como las amenazas conocidas y las amenazas de consumo.
- Identificar los ataques avanzados escalonados y multivectoriales.
- Emplear información avanzada para reconocer con rapidez las amenazas graves y sus autores.

La seguridad esencial de FireEye combina FireEye Network Security (NX) Essentials y FireEye Email Threat Prevention Cloud (ETP) para proteger a las organizaciones de las amenazas que llegan a través de la Web y el correo electrónico. Estos dos vectores de amenazas suman el 90 % de los ciberataques. La solución de seguridad esencial ayuda a optimizar el presupuesto de seguridad identificando únicamente los problemas de seguridad graves sin la distracción de los falsos positivos, que comprometen la escala y la inmediatez de la respuesta a incidentes.

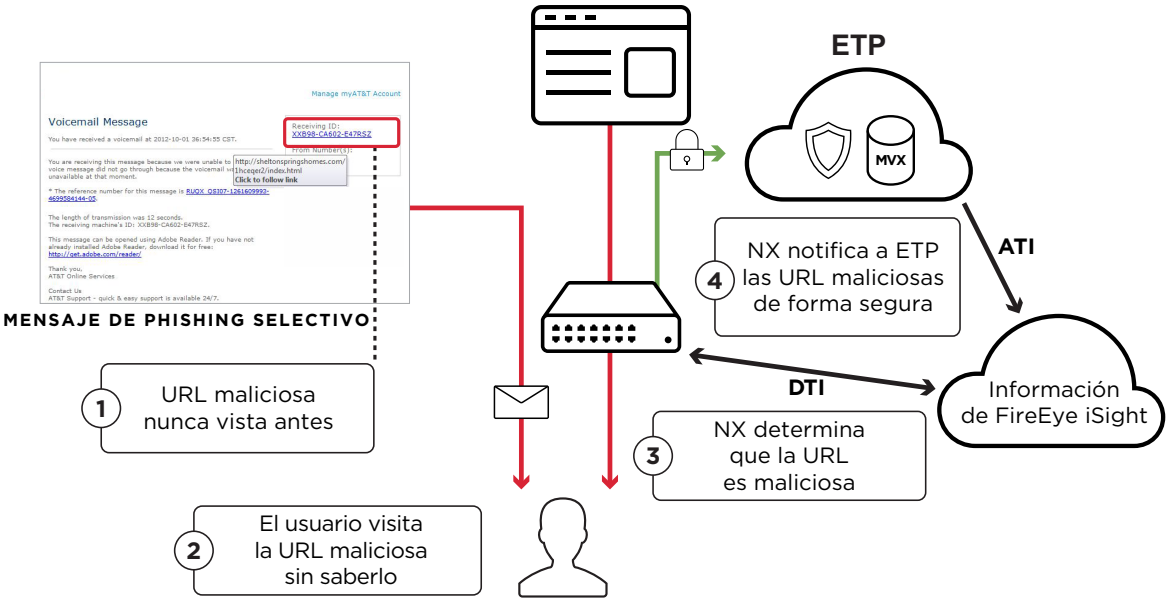
El potente motor FireEye Multi-Vector Virtual Execution™ (MVX) es el alma de las tecnologías de FireEye. Ayuda a identificar los ataques avanzados escalonados y las amenazas combinadas que se extienden en múltiples superficies de ataque, incluidos la Web y el correo electrónico, y que no parecerían maliciosas si se observaran aisladas.

Para identificar la avanzadilla de numerosos ataques multivectoriales es imprescindible correlacionar las URL maliciosas con los mensajes de correo electrónico de phishing selectivo, como muestra la Figura 1. Al ver esta relación, las organizaciones comprenden también la relación entre dos eventos y bloquean automáticamente las etapas posteriores del ataque, como la tentativa del agresor de transferir los datos robados a través de la Web. Esta visibilidad también permite identificar y bloquear ataques posteriores que utilizan tácticas, herramientas y procedimientos similares.

La solución de seguridad esencial ayuda a las organizaciones a reaccionar con más rapidez ante las amenazas con información contextual práctica. También permite a las pymes estirar un presupuesto de seguridad limitado y reducir el gasto operacional al consolidar el despliegue tecnológico, bloquear automáticamente los ataques críticos y generar alertas de alta calidad para minimizar los esfuerzos inútiles.

Con un grado elevado de automatización y eficiencia, esta solución permite a las organizaciones simplificar el despliegue y la administración diaria de la seguridad de la red y del correo electrónico, así como mejorar su nivel de seguridad.

FIGURA 1. CORRELACIÓN MULTIVECTORIAL ENTRE NETWORK SECURITY ESSENTIALS Y EMAIL THREAT PREVENTION



TECNOLOGÍA DE DETECCIÓN Y PREVENCIÓN

Network Security Essentials

FireEye Network Security Essentials es una solución de seguridad de la red, asequible y conectable directamente, que puede desplegarse en menos de 60 minutos. Reduce al mínimo el riesgo de las costosas brechas de seguridad al detectar y detener los ciberataques conocidos y desconocidos basados en la red. Utiliza el motor MVX para analizar el tráfico web y detectar exploits, archivos ejecutables de malware y llamadas multiprotocolo salientes. También incluye un sistema de prevención de intrusiones (IPS) con comparación con firmas convencionales para detectar los ataques comunes y proporciona protección contra el riskware para bloquear el spyware y el adware. A diferencia de los firewalls convencionales o de última generación, los IPS autónomos o los antivirus (AV), Network Security Essentials detecta con gran precisión tanto los ataques conocidos como los desconocidos, mientras mantiene una tasa de falsos positivos mínima.

Seguridad del correo electrónico: Email Threat Protection Cloud (ETP)

El correo electrónico suele ser la avanzadilla de las brechas de seguridad importantes. FireEye ETP es un software como servicio (SaaS) que analiza el correo electrónico en busca de phishing selectivo y de virus o amenazas de spam típicas.

Al simplificar el despliegue con una oferta basada en la nube, ETP utiliza la tecnología MVX patentada para prevenir proactivamente los ataques avanzados por correo electrónico. También proporciona protección antispam y protección antivirus en línea. ETP puede proteger los buzones de correo electrónico tanto in situ como en la nube.

Información sobre amenazas

La información sobre amenazas de FireEye basada en la nube aprovecha nuestro acceso exclusivo a los datos de sensores desplegados en todo el mundo y acompaña a las alertas de la solución FireEye. La información, actualizada cada 60 minutos, incluye nuevos perfiles de malware, exploits de vulnerabilidades y amenazas descubiertas. Complementa al motor MVX con la analítica basada en la nube y con tecnologías de aprendizaje automático para detectar las amenazas avanzadas.

FireEye Dynamic Threat Intelligence (DTI) informa cada hora de los datos intercambiados de manera anónima sobre las amenazas de la Web, el correo electrónico y los archivos, datos que se recopilan a través de la red mundial de la nube FireEye. Esta información garantiza la detección y el bloqueo de los ataques más recientes que FireEye ha detectado en su red global de clientes. DTI está disponible con Network Security Essentials.

FireEye Advanced Threat Intelligence (ATI) proporciona abundantes datos sobre los adversarios y las víctimas recopilados por analistas y equipos de respuesta a incidentes. Como resultado, las alertas de ataque de FireEye pueden incluir valiosa información contextual, como la identidad posible de los autores de amenazas, sus motivaciones probables y los detalles del malware. Con todo ello, la solución gana en eficiencia para detectar los ataques de día cero muy selectivos y el malware conocido, y ayuda a los profesionales de la seguridad a anticiparse y detener a los autores de amenazas. ATI se suministra de forma estándar con ETP.

Opciones de despliegue

La solución de seguridad esencial puede desplegarse en línea para obtener un mayor control y respuesta en tiempo real a la hora de detener los ataques en curso, como muestra la Figura 2.

FIGURA 2A. DESPLIEGUE DE NETWORK SECURITY ESSENTIALS EN LÍNEA

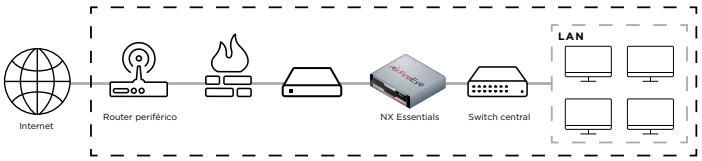
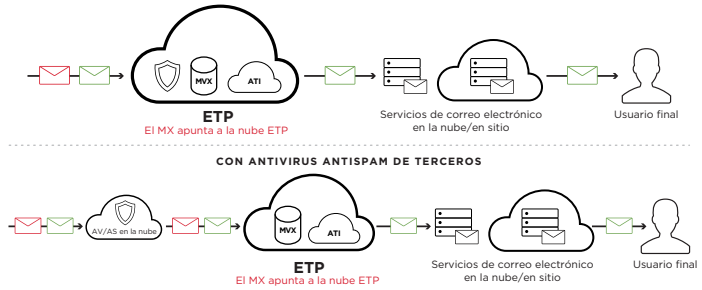


FIGURA 2B. DESPLIEGUE DE EMAIL THREAT PREVENTION EN LÍNEA



Algunas organizaciones prefieren empezar por un enfoque más conservador, por lo que también puede desplegarse en modo de prevención o de solo supervisión (modo BCC en ETP), como muestra la Figura 3. En este despliegue se monitoriza el tráfico en busca de actividades maliciosas y se genera un reporte, pero no hay ningún mecanismo automatizado de prevención. FireEye o nuestros partners pueden ayudarle a escoger y desplegar la opción que mejor se ajuste a sus necesidades.

FIGURA 3A. DESPLIEGUE DE NETWORK SECURITY ESSENTIALS FUERA DE BANDA (SPAN/TAP)

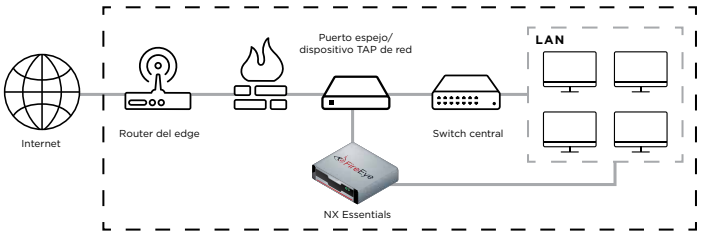
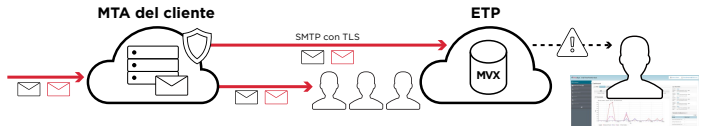


FIGURA 3B. MODO BCC - EMAIL THREAT PREVENTION



PREPARACIÓN PARA BRECHAS DE SEGURIDAD

Recuerde que la detección y la prevención solo resuelven la mitad del problema. Es igualmente importante analizar y responder al impacto técnico, legal, económico y de relaciones públicas de un incidente imprevisto. FireEye recomienda encarecidamente establecer un plan de respuesta, idealmente con un partner de seguridad. FireEye y sus partners ofrecen servicios para desarrollar un plan de respuesta, validarlo e investigar los incidentes.

PRÓXIMOS PASOS

Las pymes son el objetivo de preferencia para los agresores avanzados, porque a menudo tienen medidas de seguridad deficientes debido en gran parte a la limitación de recursos y a un menor conocimiento de las amenazas. Para poder dedicarse al crecimiento de su negocio y minimizar el riesgo, es recomendable que cuenten con un nivel de seguridad esencial. Esto incluye tecnologías y procesos de seguridad diseñados para protegerse y responder a los ciberdelincuentes sofisticados actuales. En última instancia, le darán más confianza en su nivel de seguridad.

Para informarse sobre las soluciones de FireEye diseñadas para detectar y prevenir los ataques avanzados, así como para preparar un plan adecuado de respuesta en caso de ataque, visite www.FireEye.com o póngase en contacto con su representante de ventas local.

ACERCA DE FIREEYE

FireEye protege los activos más valiosos del mundo frente a los ciberdelincuentes actuales. Nuestra combinación de tecnología, información y experiencia ayuda a eliminar el impacto de las brechas de seguridad. La comunidad FireEye Global Defense Community está formada por 4400 clientes repartidos por 67 países, incluidas más de 250 empresas del índice Fortune 500.

Para más información sobre FireEye, visite:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com