SEGURIDAD DE CATEGORÍA EMPRESARIAL PARA PEQUEÑAS Y MEDIANAS EMPRESAS

DESCRIPCIÓN GENERAL

La mayoría de las empresas emplean protocolos de correo electrónico y web para sus actividades comerciales. Por este motivo, la mayoría de los ciberataques comienzan precisamente en estos protocolos. Una protección eficaz detecta e impide ataques conocidos, así como otros avanzados y desconocidos. Las galardonadas tecnologías de FireEye detectan y detienen de forma precisa los ataques multifase y multivectoriales. Dotan a los equipos de seguridad de herramientas eficaces que mejoran la eficiencia operativa gracias a la generación de un número significativamente inferior de falsos positivos. Estas valiosas 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.

FireEye fue la primera empresa en utilizar esta tecnología para detectar ataques avanzados desconocidos, aunque inicialmente solo la desplegaron grandes empresas. Sin embargo, los ataques de los ciberdelincuentes afectan a empresas de todos los tamaños. Las pequeñas y medianas empresas (pymes) reconocen que no son inmunes y que la protección frente amenazas avanzadas es fundamental para su infraestructura de seguridad.

DESAFÍOS DE SEGURIDAD

Las pequeñas y medianas empresas se enfrentan a un gran número de desafíos de seguridad, en parte por la naturaleza dinámica de las ciberamenazas y en parte por la forma en que las pymes intentan poner en práctica la administración de la seguridad dentro de la empresa.

Los desafíos en relación a las amenazas actuales derivan, por lo general, de la falta de visibilidad sobre la seguridad en toda la empresa. Las tecnologías tradicionales de detección y prevención del perímetro que dependen de firmas no consiguen identificar los ataques actuales. Los ciberdelincuentes utilizan técnicas para modificar la reveladora firma de malware de manera que aparezca solamente una vez dentro de una empresa concreta. En muchos casos, el malware ni siquiera está implicado en los ataques.

En cuanto al centro de operaciones de seguridad, la dificultad radica en que las pymes reciben a menudo demasiadas alertas de seguridad, que precisan la acción de personal de recursos humanos del que carece. Muchas alertas son en realidad falsos positivos y los analistas pierden el tiempo investigando problemas que no son de seguridad. Un número excesivo de falsos positivos también puede ocultar los verdaderos positivos que requieren acción inmediata para mitigar el impacto.

Además, existen otras complicaciones. Para investigar las alertas, las pymes deben contratar personal con la adecuada experiencia en seguridad. En la mayoría de las empresas, el encargado de la seguridad forma parte del departamento de TI, lo que genera conflictos de intereses. Es posible que las pymes que aplican un enfoque de defensa por capas deban lidiar con un gran número de herramientas de tecnología de seguridad, cuya administración puede no ser la adecuada, estar en manos de proveedores de servicios de seguridad o sencillamente ser inexistente. En el mejor de los casos, esto puede suponer un costo excesivo y en el peor, puede generar una importante exposición a riesgos. Estos desafíos están todos conectados: las pymes deben controlar los costos y, al mismo tiempo, administrar con poco personal muchas herramientas de seguridad que generan demasiadas alertas.

FireEye

LA SOLUCIÓN

La solución de FireEye combina Network Security Essentials (NXE) e Email Threat Prevention Cloud (ETP) para proteger a las empresas frente a las amenazas web y del correo electrónico[1]. Esos dos vectores son responsables del 90 % de los ciberataques. La solución 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 estas tecnologías de FireEye. Ayuda a identificar los ataques avanzados multifase y las amenazas combinadas que se extienden en múltiples vectores 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. El motor Cloud MVX permite ver esta relación, de manera que 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 permite además identificar y bloquear ataques posteriores que utilizan tácticas, herramientas y procedimientos similares.

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

Network Security Essentials

Network Security Essentials es una solución de seguridad de la red, plug-and-play y asequible, que puede desplegarse en menos de 60 minutos para minimizar el riesgo de sufrir costosos ataques.

Además del motor patentado y sin firmas Cloud MVX, Network Security Essentials incluye la tecnología Intelligence-Driven Analysis (IDA) que identifica y bloquea las amenazas conocidas y desconocidas. IDA es un grupo de motores contextuales basados en reglas que detectan y bloquean la actividad maliciosa en función de la inteligencia más reciente sobre máquinas, agresores y víctimas. Un sistema de prevención de intrusiones (IPS) detecta ataques comunes mediante la comparación con firmas convencionales, y proporciona protección frente al riskware para bloquear spyware y adware. A diferencia de los firewalls convencionales o de última generación, los IPS autónomos o el software antivirus, Network Security Essentials detecta con gran precisión tanto los ataques conocidos como los desconocidos, mientras mantiene una tasa de falsos positivos mínima. Esto permite a los equipos de seguridad centrarse en las alertas que realmente importan.

Opciones de implementación flexibles

Network Security Essentials requiere un dispositivo on-premise virtual o físico que puede desplegarse en línea o en modo de solo supervisión. Network Smart Node, el dispositivo on-premise, puede desplegarse en distintas ubicaciones, desde el perímetro de la red principal a las oficinas remotas o las sucursales —dondequiera que haya acceso directo a Internet. La imagen de máquina virtual descargable (Figura 1) es conveniente, porque es asequible y fácil de desplegar. Network Smart Nodes utiliza tecnología Intelligence-Driven Analysis y detección IPS basada en firmas, para identificar y proteger frente a la actividad sospechosa. Estos componentes emplean una conexión cifrada para enviar objetos sospechosos que requieren un análisis más exhaustivo al servicio Cloud MVX de la nube privada de FireEye. El servicio Network Smart Node y Cloud MVX también está disponible como dispositivo de hardware integrado (Figura 2). FireEye recomienda la opción de 50 Mbit/s para pequeñas empresas y la de 100 Mbit/s para las medianas.

Seguridad del correo electrónico: Email Threat Prevention Cloud

El correo electrónico se utiliza a menudo para iniciar importantes ataques. FireEye ETP es un software como servicio (SaaS), basado en la Web, que analiza el correo electrónico en busca de phishing selectivo, o de virus o spam general. ETP utiliza tecnología patentada Cloud MVX para prevenir de forma proactiva ataques avanzados por correo electrónico. También proporciona protección antispam y protección antivirus en línea, y puede proteger tanto buzones de correo on-premise como en la nube mediante el despliegue en línea o solo en modo de solo supervisión.

Inteligencia sobre amenazas

Las alertas de la solución de FireEye se complementan con inteligencia sobre amenazas de FireEye basada en la nube. La información, actualizada cada 60 minutos, incluye nuevos perfiles de malware, exploits de vulnerabilidades, inteligencia sobre adversarios y víctimas, y amenazas descubiertas. Complementa al motor Cloud MVX con la analítica basada en la nube y con tecnologías de aprendizaje automático para detectar las amenazas avanzadas. Como resultado, las alertas de FireEye pueden incluir información contextual crítica, como la identidad posible de los autores de amenazas, sus motivaciones probables y los detalles del malware, a fin de ayudar a los profesionales de la seguridad a detectar y detener los ataques desconocidos (de día cero) muy selectivos y el malware conocido.

[1] Verizon 2015 Data Breach Investigations Report (Informe sobre las investigaciones de fugas de datos de 2015)

CONFIGURACIONES DE MUESTRA

Los factores a tener en cuenta a la hora de montar una solución son los siguientes: el número de buzones de correo electrónico que se van a supervisar, el volumen de tráfico de red que atraviesa el sistema, el entorno virtualizado o físico, la adopción de servicios a través de la nube y el nivel de concienciación sobre ciberseguridad de los directivos y el consejo de administración. FireEye y sus socios pueden ayudarle a elegir o diseñar una solución que se ajuste a sus necesidades, basada en estas configuraciones de muestra.

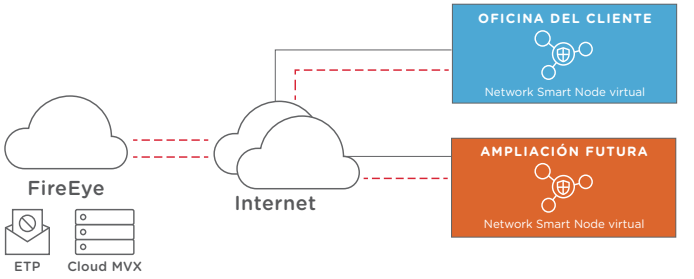

FIGURA 1. ETP CLOUD Y CLOUD MVX CON DISPOSITIVOS VIRTUALES

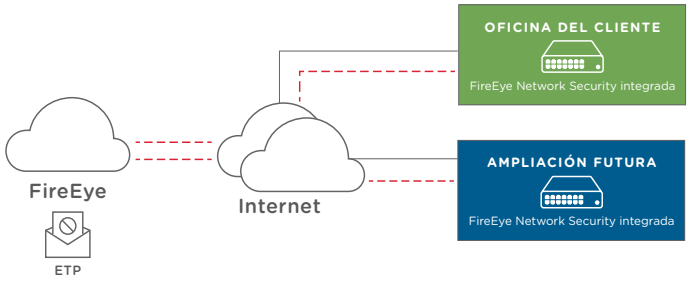

FIGURA 2. ETP CLOUD Y DISPOSITIVOS FÍSICOS DE INTEGRATED NETWORK SECURITY

	PEQUEÑAS N.º 1	PEQUEÑAS N.º 2	MEDIANAS N.º 1	MEDIANAS N.º 2
TIPO DE DESPLIEGUE	**VIRTUAL/NUBE**	**DISPOSITIVO FÍSICO**	**VIRTUAL/NUBE**	**DISPOSITIVO FÍSICO**
Número de empleados	200 - 250	200 - 250	450 - 550	450 - 550
Tráfico de red	50 Mbit/s	50 Mbit/s	100 Mbit/s	100 Mbit/s
Solución de muestra propuesta	ETP, 200 - 250 sistemas Virtual NX1500 Cloud MVX	ETP, 200 - 250 sistemas 2500NXE1 integrado	ETP, 450 - 550 sistemas Virtual NX2500 Cloud MVX	ETP, 450 - 550 sistemas 2500NXE2 integrado

PRÓXIMOS PASOS

Las pymes son el objetivo de preferencia para los agresores avanzados, debido a que cuentan con medidas de seguridad insuficientes, debido en gran parte a las limitaciones de recursos y a una menor concienciación sobre las amenazas. Para contribuir al crecimiento de su empresa y reducir riesgos, es fundamental mantener un nivel excelente de seguridad. Y para ello, se requiere confianza en el estado de seguridad, así como en el programa, las herramientas y los procesos de seguridad.

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

ACERCA DE FIREEYE, INC.

FireEye® es el líder en seguridad como servicio basado en la inteligencia. FireEye, que funciona como una extensión escalable y flexible de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina innovadoras tecnologías de seguridad, inteligencia sobre amenazas a nivel de nación-estado y los servicios de consultoría de Mandiant® de fama mundial. FireEye tiene más de 5000 clientes en más de 67 países, incluidas más de 940 empresas de la lista Forbes Global 2000.

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

www.FireEye.com