LOGRAR UNA CONCIENCIA INTEGRAL SOBRE CIBERSEGURIDAD A *EN FORMA VERTIGINOSA*

Cómo la información sobre amenazas avanzadas y un nuevo conjunto de herramientas automatizadas de FireEye están ayudando a las instituciones a reducir sus brechas de seguridad en entornos multinube.

Por el personal de FedScoop

RON BUSHAR, JEFE DE TECNOLOGÍA GUBERNAMENTAL DE FIREEYE, ha visto bastantes casos de ransomware y brechas de seguridad en los últimos 12 meses. Las escenas resultan familiares. Él y los analistas de FireEye se reunían, a fin de cooperar, con miembros del equipo de seguridad de una agencia gubernamental para evaluar con qué estaban lidiando. Por lo general, el FBI estaría allí, a veces también lo estaría el Servicio Secreto, junto con especialistas de varios proveedores de tecnología de seguridad.

En años anteriores, FireEye se asociaría con Mandiant para investigar brechas de ciberseguridad: FireEye era la compañía en la que confiaban las empresas para identificar una brecha de seguridad; Mandiant, que FireEye adquirió en 2013, era la empresa que podía indicarle quiénes eran los hackers y cómo responder. Desde entonces, los expertos en inteligencia y respuesta ante incidentes de Mandiant han respondido a decenas de miles de vulneraciones en todo el mundo.

FireEye se ha ganado la reputación de estar al tanto de las vulnerabilidades de hackeo a nivel mundial y de brindar herramientas automatizadas para detectarlas y abordarlas rápidamente. Esa reputación ha seguido creciendo con una serie de adquisiciones, incluyendo más recientemente, Verodin (que ahora se conoce como Mandiant Security Validation), un proveedor de instrumentación de seguridad, y Cloudvisory, que proporciona visibilidad de seguridad en varias nubes.

"FireEye ahora puede presentarse e implementar lo que sabemos sobre cada variante de ransomware que estamos viendo en todo el mundo y comenzar a buscarlo en minutos, independientemente de la tecnología que esté usando una institución", afirma Bushar. "De inmediato podemos decir: 'Probablemente sea este grupo. Estas son las técnicas que utilizan. Así es como entraron. Aquí es donde podemos buscar para encontrar el lugar donde implementaron su ransomware. Y esta es la mejor manera de aislar esto y hacer que sus sistemas vuelvan a estar en línea'".

Su información ya no puede tener meses ni semanas de antigüedad. Y también hay que combinarla con agilidad desde el punto de vista tecnológico y poder trabajar a escala.

RON BUSHAR,
jefe de tecnología gubernamental de FireEye

Sin embargo, Bushar reconoce que la rápida evolución de los ciberataques es solo una parte del desafío que enfrentan los funcionarios gubernamentales. También existe la presión implacable por modernizar los sistemas de TI obsoletos en medio de limitaciones de recursos de larga data.

"Las instituciones tienen el mismo problema de capacidad que todos los demás para mantener un conjunto de habilidades talentosas. Y todos tienen exceso de trabajo, ¿verdad?", dice Bushar, quien se desempeñó como exdirector adjunto del Departamento de Justicia para operaciones de seguridad antes de ocupar cargos de alto nivel en Mandiant y FireEye.

La buena noticia, manifiesta, es que una combinación de factores ahora hace posible que las instituciones logren una visibilidad mucho mayor de sus redes, en las instalaciones y en la nube, y también acorta drásticamente el tiempo que lleva detectar y bloquear amenazas potenciales.

LOGRAR UNA VISIBILIDAD GENERALIZADA

Independientemente de dónde se encuentren las instituciones en sus esfuerzos de modernización de TI, la marcha constante hacia los servicios en la nube las han obligado a transformar su manera de pensar en la seguridad.

Si bien muchas instituciones federales aún deben mantener controles perimetrales definidos de manera estática, esos controles están destinados principalmente a la prevención en vez de la detección. Migrar datos y aplicaciones a la nube exige soluciones fundamentalmente diferentes para gestionar la seguridad en un entorno distribuido, más dinámico y más diverso.

Luego está la cuestión de mantenerse al día con lo que el Mayor General Earl Matthews (Fuerza Aérea de EE. UU., retirado), Vicepresidente de estrategia de Mandiant Security Validation denomina "deriva del entorno".

"Los sistemas y aplicaciones de TI cambian a diario. Se están implementando nuevas aplicaciones; se actualizan las herramientas; el equipo se reemplaza", manifiesta Matthews. "Si todo su entorno de TI cambia todos los días, la pregunta que se debe responder es la siguiente: ¿Están actualizados sus sistemas de control de seguridad y cómo tiene la certeza de ello?"

La respuesta comienza con cerrar la brecha de visibilidad, insiste Martin Holste, jefe de tecnología para la nube de FireEye.

"Todo depende de la visibilidad" en un entorno distribuido, afirma. "Es la base esencial para cualquier estrategia de seguridad de la nube, ya sea que la estrategia gire en torno a la garantía de cumplimiento, la búsqueda de amenazas, la gestión corporativa de políticas o la corrección de riesgos".

Y lo que es más importante, "las instituciones también deben ampliar su capacidad para detectar y responder a las amenazas en forma vertiginosa, especialmente cuando migran a la nube", expresa.

Lograr esa visibilidad sigue siendo una gran dificultad y una necesidad urgente para la mayoría de las empresas: el 43% de los profesionales de ciberseguridad en múltiples sectores, incluido el gobierno, indicó que la "visibilidad en la seguridad de la infraestructura" es un punto débil clave que enfrentan actualmente, según un Informe de seguridad de la nube 2020 de Cyber Security Insiders.

Según Holste, la visibilidad integral de la seguridad de la infraestructura requiere múltiples formas de visibilidad simultáneamente. Incluye contar con lo siguiente:

- **Un inventario completo de todos los activos relevantes en todo momento.** Sin un inventario actual e histórico de todos los activos incluidos en el alcance, las auditorías de cumplimiento y los análisis de seguridad arrojarán resultados incompletos o engañosos.

- **Detalles contextuales sobre el estado actual de cada activo.** Sin visibilidad del contexto de todos y cada uno de los activos, y sin la capacidad de buscar esos detalles cuando sea necesario, no hay significado ni validez para conceptos como la garantía de cumplimiento y la detección de anomalías.
- **Registro histórico completo de eventos de seguridad para cada activo**. Sin la visibilidad del comportamiento real de las cargas de trabajo y los usuarios, no hay forma de confirmar que las políticas de gestión corporativa estén funcionando o que los perpetradores nefastos no poseen ya parte de su infraestructura.

Según Holste, la solución Cloudvisory integrada de FireEye brinda a las instituciones la capacidad de sondear más profundamente en varios entornos de nube, así como cargas de trabajo en contenedores, en busca de posibles vulnerabilidades y amenazas. También funciona con una amplia gama de tecnologías de seguridad y todos los proveedores de nube líderes. Y proporciona a los usuarios controles automatizados y reglas de políticas que se pueden entregar a toda velocidad para que las instituciones puedan ajustar continuamente sus políticas de seguridad a medida que sus operaciones continúan evolucionando en el futuro.

Siempre que un desarrollador pone en marcha un nuevo servicio en la nube, debería poder centralizar fácilmente la telemetría, dando a los analistas la capacidad de ir a una única ubicación para revisar el estado de seguridad de todos los servicios en la nube.

ADAPTAR LA SEGURIDAD A UNA FUERZA DE TRABAJO REMOTA

Justo cuando muchos equipos de seguridad empresarial se estaban acostumbrando a gestionar la seguridad en entornos de TI distribuidos, de repente tuvieron que lidiar con una fuerza de trabajo recientemente distribuida.

Eso significó no solo adaptar sus controles de detección y supervisión de seguridad, para adaptarse a un aumento repentino en la cantidad de empleados que trabajan de forma remota, sino también tener que realizar esas funciones de seguridad de manera remota. Tener un conjunto sólido de herramientas de análisis y detección, que puede supervisar y hacer cumplir las políticas de seguridad, detectar nuevos tipos de vulnerabilidades y que puede distinguir entre cambios en el comportamiento y el comportamiento inusual, se ha vuelto más importante que nunca.

Las recientes incorporaciones dentro de la plataforma de análisis FireEye Helix ahora hacen posible, por ejemplo, identificar más rápidamente el comportamiento anormal de inicio de sesión de VPN, según Gregory Smith, gerente sénior de mercadotecnia de productos de FireEye. Las organizaciones que adoptan conjuntos de productividad en la nube, como Office 365, pueden establecer una línea de base y detectar comportamientos inusuales automáticamente.

Sin embargo, Bushar dice que responder a las ciberamenazas sigue siendo una cuestión complicada y cada vez más compleja.

“Se necesita de una combinación de experiencia y conocimiento del entorno de amenazas, en tiempo real, así como de la infraestructura de TI y la forma en que ha evolucionado con el tiempo. Su información ya no puede tener meses ni semanas de antigüedad. Y también hay que combinarla con agilidad desde el punto de vista tecnológico y poder trabajar a escala”, afirma.

Reconoce los méritos de la división Mandiant Threat Intelligence de FireEye, que puede identificar cuáles son los perpetradores con más probabilidades de interesarse en una empresa determinada, por ayudar a los jefes de seguridad de la información a preparar mejor sus defensas. Además, Mandiant Security Validation brinda a los jefes de seguridad de la información herramientas de instrumentación para ayudar a gestionar e informar los riesgos de seguridad a los directores y proporcionar una justificación más clara para las inversiones en TI y seguridad.

“Todo depende de la visibilidad en un entorno distribuido. Las instituciones también deben ampliar su capacidad para detectar y responder a las amenazas en forma vertiginosa, especialmente cuando migran a la nube”.

MARTIN HOLSTE,
jefe de tecnología para la nube de FireEye,

ECOSISTEMA DE FIREEYE

El ecosistema de FireEye combina tecnología y experiencia para lograr el mejor nivel de seguridad a través de un conjunto completo de capacidades de detección, protección y respuesta. Esto incluye soluciones de seguridad de red, endpoint, correo electrónico y de la nube en una plataforma de operaciones de seguridad, Helix. El ecosistema también incluye una plataforma de instrumentación de seguridad, Mandiant Security Validation, que mide, prueba y mejora continuamente la eficacia de la ciberseguridad. Por último, los servicios de Mandiant Consulting, Managed Defense y Threat Intelligence refuerzan a las organizaciones mediante los recursos y el conocimiento necesarios para responder y proteger a las organizaciones contra las amenazas más avanzadas.

Fuente: FireEye

Pero el objetivo real, dice, es brindar visibilidad y conocimientos de manera que los clientes de FireEye puedan actuar en consecuencia.

"Si habla con cualquiera que esté trabajando en el espacio de información sobre amenazas", resalta Bushar, "la queja número uno no es que la gente no esté brindando suficiente información, sino que brinda demasiada información.
Pero lo segundo que dicen es: 'No puedo consumirlo de una manera que me sea útil', o no saben qué hacer necesariamente con la información. Lo que estamos tratando de hacer ahora con nuestra función de información es ir más allá de los informes legibles por humanos, que aún son útiles, y aplicar esa inteligencia en forma vertiginosa... pero hacerlo de una manera que realmente permita el análisis proactivo y predictivo".

"En un alto nivel, realmente estamos tratando de habilitar, de la manera más rápida y fluida posible, todo lo que sabemos y aprendemos sobre los adversarios: sus herramientas, técnicas, motivaciones e intenciones, y hacer llegar eso a nuestros clientes de la forma en que quieren consumirlo, en forma vertiginosa", manifiesta Bushar.

Obtenga más información sobre el conjunto completo de capacidades de detección, protección y respuesta de FireEye con soluciones de seguridad para red, endpoint, correo electrónico y en la nube, así como una plataforma de operaciones de seguridad, Helix, y nuestros servicios Mandiant Security Validation, Mandiant Consulting, Managed Defense y Threat Intelligence.

fedscoop FIREEYE