Gestión de brechas cibernéticas

Forensic & Integrity Services (Forensics)

Ayudamos a nuestros clientes a prevenir y gestionar efectivamente amenazas cibernéticas de alto impacto para su organización.

¿Sus sistemas informáticos se han visto afectados?

Un ataque cibernético puede dañar la operación de un negocio, al permitir que terceros puedan tomar el control de su infraestructura tecnológica o permitirles acceso a su información electrónica afectando su estado financiero, pérdida de información importante de la organización y dejando la reputación de las empresas en juego, es decir, inmiscuyéndolas en acciones legales de parte de los organismos de control internacionales.

Los delincuentes tienen como objetivo la información comercialmente sensible, propiedad intelectual e infraestructura de red crítica. Estas amenazas pueden provenir de atacantes que se encuentran tanto dentro como fuera de su organización.

Alguno de estos abusos de vulnerabilidades pueden parecer inofensivos y otros mucho más perjudiciales y maliciosos en sus intentos. Sin embargo, cualquier intrusión en sus sistemas informáticos puede generar multas reglamentarias, gastos operativos, daños a la reputación y pérdida de ventajas competitivas. Ninguna organización desea que su información confidencial se negocie o se filtren a la luz pública.

Muchos proveedores tecnológicos están creando productos para ayudar a contrarrestar estas amenazas. Las empresas ya implementan herramientas sofisticadas de detección de virus, sistemas de detección de intrusos y dispositivos de prevención de fugas de datos. A pesar de estas soluciones, las brechas de alto perfil y dañinas continúan publicándose en la red.

El impacto potencial del cibercrimen requiere que la seguridad de la información sea vista como un riesgo de negocio y no como un simple asunto de TI. Cada vez más, la alta dirección está involucrada en la estrategia de prevención, ya que las autoridades hacen que las empresas y sus líderes rindan cuentas por la seguridad de los datos y el gobierno de la información de sus clientes y empleados.

El costo que las brechas cibernéticas causan a la economía anualmente se estima en 445,000 MDD[1]. Debido a que los negocios de todas las industrias son víctimas de algún tipo de ciberataque, todos los niveles del negocio desde la alta dirección, gerencia ejecutiva, áreas de gestión de riesgos, el área jurídica, unidades de operativas y sobre todo tecnologías de la información (TI) son afectadas profundamente.

[1] De acuerdo con un reporte de la compañía de seguridad McAfee

EY
Construyendo un mejor entorno de negocios

Un nuevo desafío

Nuestra experiencia muestra que la mayoría de las empresas ya entienden la necesidad de una solución de ciberseguridad efectiva, pero son conscientes de que tales controles y tecnologías por sí solos no pueden eliminar por completo la amenaza.

A menudo, se instalan dispositivos de seguridad de red para detectar intrusiones y monitorear la fuga de datos. Estos se utilizan para defenderse de amenazas ampliamente conocidas, pero no son en sí mismas una defensa viable contra un atacante motivado.

Aun cuando las empresas a nivel mundial han incrementado la prioridad e inversión a la ciberseguridad, el enfoque es proteger la información mediante la prevención de intrusiones. Desafortunadamente, el nivel de amenaza actual es tan alto que solo es cuestión de tiempo para que cualquier organización sufra una brecha de seguridad significativa.

Cuando se descubren fugas, se solucionan de inmediato sin realizar una investigación completa del ataque. Esto puede dejar a otras partes de la red en peligro y expuestas, ya que nunca se descubre el alcance completo de la filtración.

Para abordar adecuadamente estas complejas brechas, es necesario que las compañías construyan un marco de respuesta robusto y centralizado como parte de la estrategia empresarial de gestión de riesgos, pero también deben considerar:

- ¿Cómo determinar si los atacantes sobrepasan las defensas de seguridad?
- ¿Qué se puede hacer si ya ocurrió un ataque?

Un enfoque forense proactivo puede ayudar a su organización a responder a incidentes complejos que pueden haber violado su seguridad. Esto ayudará a reducir la cantidad de tiempo en que una red está expuesta, mitigando el daño o la pérdida de datos que pueda resultar de esto y aumentar la probabilidad de atrapar al atacante.

¿Cómo EY puede ayudarle?

Nuestro enfoque

Nuestro equipo de investigación de crimen cibernético está compuesto por profesionales forenses y de seguridad de TI que trabajan con investigadores corporativos con alta experiencia. A menudo investigamos y respondemos a incidentes de brechas de seguridad, pero nosotros aconsejamos a los clientes que adopten un enfoque más proactivo.

Un programa centralizado de respuesta a brechas cibernéticas (CBRP, por sus siglas en inglés), es el punto focal que reúne a todas las partes interesadas que deben colaborar para resolver una brecha de ciberseguridad.

Nuestros equipos se centrarán en la investigación de su infraestructura de TI para encontrar cualquier evidencia de robo de datos o intrusión.

Nuestros servicios

EY puede ayudarle desde la investigación forense hasta la asistencia en litigios, trabajar con reguladores, organismos legales y agencias de seguridad e inteligencia nacional. Tenemos el prestigio, el nivel y la experiencia que usted necesita para responder y recuperarse de una brecha cibernética de una manera integral.

Nuestro equipo está compuesto por profesionales de ciberseguridad, investigadores, personal con alto conocimiento en cómputo forense, profesionales de *eDiscovery*, contadores forenses, analistas de contratos gubernamentales, economistas y examinadores de fraude certificados, además de personas con cargos previos como directores de cumplimiento y ética, auditores de gobierno, fiscales y reguladores.

Contamos con más de 60 centros de tecnología forense a nivel global y podemos ofrecer servicios con recursos de nuestra red en todos los países donde EY se encuentra presente.

¿Qué podemos encontrar?

Somos capaces de determinar la información potencialmente comprometida mediante una variedad de métodos, incluyendo:

- Análisis de información y registros forenses
- Detección de IOC en sistemas posiblemente vulnerados
- Detección de información posiblemente comprometida por el atacante
- Detección de filtración en progreso a través de las conexiones de red
- Recuperación y análisis de respaldos en los sistemas que fueron atacados y dañados

El análisis inicial nos permitirá identificar más flujos de trabajo para investigaciones adicionales. Por ejemplo:

- Evidencia del uso de *software* de acceso remoto de fuentes no autorizadas
- Indicadores de la presencia de *malware* activo
- Conexiones persistentes a otros países o entidades no autorizadas
- Flujo de datos del *back channel* dentro/fuera de su organización
- Indicadores de recolección de datos por parte de los empleados o de los que abandonan su organización
- Acceso no autorizado al sistema y a los datos

Además de estos indicadores, frecuentemente descubrimos otros hallazgos que se relacionan con su seguridad de TI o el régimen de gobernanza de la información, que incluyen:

- Limitaciones en las políticas de seguridad existentes
- El almacenamiento de datos confidenciales en áreas no protegidas (*webmail*, almacenamiento en la nube, etc.)
- Uso inapropiado de los recursos de TI

Investigación cibernética

Nuestros servicios de investigación forense incluyen el análisis de registros, análisis forense de dispositivos y sistemas, análisis de tráfico y registros de red en vivo.

Estos resultados pueden usarse para desarrollar y afinar otros aspectos del plan de respuesta cibernética. Una brecha cibernética compleja requiere una investigación exhaustiva para la recuperación y remediación de la información, así como todas las acciones legales asociadas.

Trabajamos con nuestros clientes al desarrollar conjuntamente un enfoque de investigación personalizado para cada asunto legal, incluyendo áreas específicas de investigación y posibles procedimientos, recursos experimentados, tiempos, productos de trabajo y presupuesto; adaptamos nuestros procedimientos a los requisitos legales y normativos específicos de cada país involucrado en la investigación.

Gestión de brechas cibernéticas

Un programa centralizado de respuesta a brechas cibernéticas efectivo tiene que incluir a las partes interesadas y los factores clave en una brecha de alto impacto.

El plan de respuesta no solo supervisa el proceso de identificación, adquisición, preservación de evidencia, análisis forense de datos y evaluación del impacto; sino que también puede redireccionar el enfoque de la investigación basándose en análisis de patrones de hechos.

Cibernética forense

Desarrollamos un enfoque de muestreo de redes para generar indicadores de que una filtración pudo haber ocurrido. Esto está en contraste con una auditoría tradicional de TI o una prueba de vulnerabilidad, que se enfoca en debilidades potenciales a ataques comunes y bien publicitados. Nuestro diagnóstico de brechas cibernéticas se centra en los ataques dirigidos que están diseñados para superar las defensas.

Inicialmente, revisaremos su arquitectura de red y tomaremos muestras de artefactos forenses donde sabemos que pueden residir los indicadores de ataques cibernéticos. Típicamente, tales artefactos incluyen una muestra del tráfico de la red, registros de servidores y dispositivos, así como la selección de artefactos forenses de sistemas informáticos o servidores clave.

Este proceso de captura de datos está diseñado para reducir el soporte requerido para sus equipos de TI y no es probable que tenga un impacto significativo en el rendimiento de su infraestructura.

Después de la recopilación, utilizamos una variedad de pruebas forenses manuales y automáticas, tecnologías de minería de datos y la experiencia de nuestro personal para resaltar indicadores de actividad potencialmente sospechosa.

Remediación y recuperación de datos

Si las brechas cibernéticas resultan en destrucción o corrupción de datos, EY puede proporcionar servicios de recuperación de datos de varios tipos entre borrados, dañados, perdidos o inaccesibles que puedan haber resultado de un ciberataque. Esto incluye recuperar pérdidas de ambientes en cualquier sistema operativo y trabajar con equipos de respuesta para restaurar servicios.

Un componente importante para la planeación de la remediación tras una brecha cibernética implica fortalecer la postura de seguridad de la organización, así como aplicar controles sobre las brechas encontradas durante la investigación realizada.

Contactos

Ignacio Cortés Castán
MBA, CFE, ReFor | Socio Líder Regional de *Forensic & Integrity Services* | EY Latam Norte
ignacio.cortes.castan@mx.ey.com

Juan Ramírez Valdespino
Gerente Senior | *Forensic & Integrity Services* | EY México
juan.ramirezvald@mx.ey.com