

Controlar las fugas

Manejo de amenazas a la información confidencial

Durante los últimos cinco años, las organizaciones han experimentado un aumento en el volumen de fugas de información intencionales y no intencionales. Por ejemplo, el *software* malicioso -cada vez más sofisticado- ha revelado información confidencial fuera de la organización sin que el usuario se dé cuenta. Simultáneamente, las personas con acceso a información privilegiada o informantes han utilizado nuevos métodos para sacar conductas cuestionables a la luz pública mediante la difusión de datos confidenciales en sitios *web* como WikiLeaks.org (actualmente WikiLeaks.ch). *The New York Times* y *The Guardian* del Reino Unido han anunciado planes de crear portales similares a WikiLeaks, y seguramente habrá muchas más publicaciones que harán lo mismo. El daño residual y reputacional causado por este tipo de fuga de información es enorme.

Controlar la información confidencial dentro de una organización es todo un reto, ya que deben considerarse las amenazas internas además de las externas. La fuga de información de una red corporativa puede ocurrir deliberadamente como resultado de una acción intencional de algún colaborador, como consecuencia de un ciberataque, o inadvertidamente, por un colaborador desprevenido que llega a ser víctima de un *software* malicioso o de la ingeniería social diseñada para incitar a los usuarios para que violen las prácticas recomendadas. La ingeniería social es un medio común de los agresores para obtener información o introducir *software* malicioso en las organizaciones, ya que se aprovechan de la falta de conocimiento de los colaboradores sobre los riesgos y las prácticas de seguridad.

Es importante distinguir entre los miembros responsables de su equipo y aquellos individuos malintencionados, ya que estos tienen distintas razones para divulgar información confidencial. Debido a que los motivos de estas personas con acceso a datos confidenciales podrían variar, existen dos enfoques distintos para la implementación de controles: el enfoque conductual y el enfoque técnico.

¿Qué porcentaje de este tesoro de documentos que usted posee está relacionado con el sector privado?

"Aproximadamente la mitad".

¿Esto significa que posee información corporativa de muy alto impacto que en un momento dado podría sacar a la luz pública?

"Sí... esto podría ser un duro golpe para algunos bancos".

-Entrevista realizada por Forbes a Julian Assange, fundador y vocero de Wikileaks, el 29 de noviembre de 2010.





Es esencial que todos los colaboradores de la organización entiendan y crean en el compromiso de la compañía de realizar sus operaciones de manera ética y legal.

Enfoque conductual

Son utilizados para evitar que los individuos responsables expresen su descontento en foros públicos y que, en consecuencia, dañen la reputación de sus compañías. Los controles preventivos y correctivos de esta índole deben establecerse y aplicarse de manera congruente.

Controles conductuales preventivos

Debe empezar por asegurarse de que sus colaboradores estén informados acerca del compromiso de la compañía por actuar éticamente y con apego a la ley. La comunicación corporativa deberá ser oportuna y transparente, y tendrá que transmitir claramente las acciones que han sido emprendidas para cumplir con este compromiso.

Asimismo, deben tener pleno conocimiento sobre los procedimientos internos de escalación para revelar e informar posibles conductas ilícitas o poco éticas. Un programa manejado internamente que asegure el anonimato, la confidencialidad y respuestas adecuadas permitirá a las personas responsables contar con un medio con el que puedan cumplir sus obligaciones éticas, y dará a la compañía pie para investigar y responder a posibles violaciones de manera privada y discreta. Su compañía debe insistir en que todas aquellas personas que deseen informar sobre alguna irregularidad tendrán que utilizar esta estructura interna de denuncia. Para alentar esta práctica entre los colaboradores, debe procurar que se le dé seguimiento a todos los casos reportados.

Controles conductuales correctivos

La existencia de un proceso interno de denuncia y escalación deberá comunicarse a lo largo y ancho de la organización, y dicho proceso necesita incluir una guía para determinar en qué momento hay que aplicarlo. Esta estructura le permitirá dar seguimiento y verificar las denuncias antes de llevar a cabo cualquier tipo de acción. Es importante que las compañías tengan esta oportunidad de revisar las denuncias, ya que la divulgación de información falsa de esta índole podría representar una violación a las reglas de privacidad, dañar la reputación de la compañía o comprometer las operaciones comerciales de esta. A la vez que cumple

con diversas regulaciones para la protección de informantes, las compañías deberán también comunicar claramente que la divulgación de cualquier tipo de información relacionada con la organización que sea falsa o difamatoria tendrá como consecuencia acciones disciplinarias que podrán implicar la terminación del contrato laboral o el ejercicio de acciones judiciales.

Enfoque técnico: programas técnicos estratégicos

Resulta esencial contar con un programa técnico estratégico para fortalecer la seguridad a largo plazo de su organización. Este le permitirá tratar amenazas actuales y futuras, reducir el costo de las medidas de seguridad y le facilitará el manejo de incidentes de seguridad.

El primer paso en el desarrollo de un programa estratégico es identificar qué tipo de información delicada y confidencial se encuentra disponible en sus redes o para sus socios comerciales, y entender cómo se transmite dicha información a lo largo y ancho de la compañía. Un ejercicio integral de identificación y clasificación de toda la información permitirá a su compañía implementar el plan de protección más eficiente y dirigido posible. Una evaluación sobre prevención de pérdida de datos ayudará a identificar los riesgos y contribuirá al desarrollo de un plan de mejora que incluya "logros rápidos" y recomendaciones de largo plazo para reducir los riesgos de la compañía.

Se recomienda realizar periódicamente pruebas de ataque y penetración para verificar la existencia de una amplia gama de vulnerabilidades técnicas que pudieran ser aprovechadas por los colaboradores malintencionados. Dichas pruebas deberán incluir acciones relacionadas con las aplicaciones y la infraestructura, así como revisiones al código fuente. Estas evaluaciones de alcance completo pueden colaborar en la identificación de los riesgos comunes asociados con las aplicaciones y las redes, así como las "puertas traseras" que existen en el ambiente.

Por último, recomendamos llevar a cabo las acciones necesarias en contra de las amenazas futuras que el *software* malicioso y la ingeniería social pudieran representar. Realizar pruebas rutinarias es clave para combatir ataques cuyo objetivo es tener acceso a cierta información durante períodos

prolongados mediante técnicas lentas, pero seguras. Los programas de vigilancia de *software* malicioso permiten alertar a su organización sobre ataques continuos para que usted pueda detenerlos de inmediato.

Contar con una capacidad interna sustentable para detectar y responder a incidentes de seguridad cibernética, así como contratar a firmas de buena reputación que proporcionen servicios de investigación y remediación en caso de que ocurra alguna violación, le permitirá identificar y mitigar los riesgos relacionados con activos comprometidos o colaboradores que ya son víctimas de la ingeniería social.

También puede incorporar programas de prevención de la ingeniería social a sus programas de capacitación sobre seguridad, y realizar pruebas de forma periódica para monitorear la efectividad de dichos programas.

Estos deberán cubrir las propias operaciones centrales de su empresa y las de sus socios comerciales o proveedores que manejen información confidencial en representación de su organización. Finalmente, los términos contractuales no protegerán a su empresa de los daños causados por un proveedor que maneja inapropiadamente su información confidencial. Por lo tanto, resulta de vital importancia establecer y verificar controles que protejan su información confidencial sin importar su ubicación.

Medidas tácticas

Los cambios estratégicos son soluciones a largo plazo cuya implementación requiere de tiempo y cuidado; por lo tanto, muchas compañías buscan asesoría para poner en marcha su respuesta estratégica. Después de más de 15 años de proporcionar servicios de asesoría sobre seguridad, incluidas pruebas de penetración con base en las mismas técnicas que utilizan los *hackers*, Ernst & Young ha determinado que las siguientes siete medidas tácticas constituyen los cimientos más sólidos para desarrollar un programa estratégico eficaz que permita obtener el mayor rendimiento de la inversión:

1) Identificar y clasificar su información. Contar con un plan bien desarrollado de clasificación de información detallada permitirá a su compañía diseñar e implementar controles apropiados para los distintos tipos de información. Además, una política clara y bien entendida fomentará una conducta

apropiada por parte de los colaboradores y los propietarios de la información con respecto al manejo, almacenamiento y transferencia de la misma.

2) Manejar los administradores locales adecuadamente.

Los usuarios locales no deberían contar con los privilegios de un administrador local para sus terminales corporativas, como computadoras portátiles, ordenadores de escritorio o dispositivos móviles. Las cuentas de los administradores locales requerirán contraseñas robustas que no deberán utilizarse en otras máquinas.

3) Prohibir el uso de máquinas no autorizadas en su red.

El intento de conectar activos ajenos a la infraestructura corporativa es señal de que ocurre una de dos situaciones indeseables: una persona no autorizada ha entrado a las instalaciones de la compañía y se ha conectado a la red, o un colaborador ha traído un dispositivo personal a la oficina que ha conectado a la red. Los dispositivos personales no cuentan con los programas corporativos, como las actualizaciones de antivirus y de *firewalls* locales, sin los cuales los dispositivos infectados podrían propagar el *software* malicioso a toda la organización.

Los dispositivos de control de acceso a la red (NAC, por sus siglas en inglés) evitan que activos que no sean propiedad de la compañía se conecten a esta, y notifican al personal de seguridad apropiado si alguien intenta conectar activos ajenos.

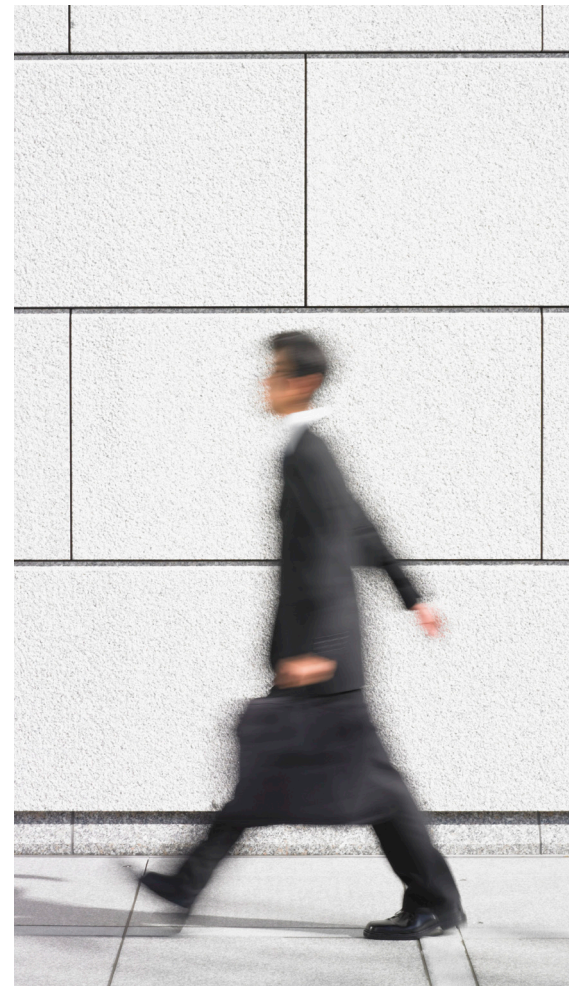
4) Impedir la fácil extracción vía medios removibles.

Las terminales deberán estar configuradas de tal manera que no permitan el uso de dispositivos removibles (CDs, memorias USB, etc.). Los dispositivos móviles como las computadoras portátiles y los celulares (*smartphones* o PDAs) tendrán que tener sus memorias completamente encriptadas, y su compañía deberá poder borrar las memorias a distancia si los dispositivos llegaran a ser extraviados o robados.

5) Contar con herramientas en modalidad de interrupción automática.

Deberá implementar herramientas de prevención de pérdida de información (DLP, por sus siglas en inglés) y configurar dicha herramienta a modalidad de "interrupción automática". En esta modalidad, si las herramientas PPI no logran verificar el contenido de la comunicación (por ejemplo, un correo

Los informantes malintencionados representan una amenaza peligrosa distinta para sus organizaciones. Estos individuos deben ser identificados rápidamente, purgados de todos los sistemas y reportados a las agencias de seguridad.



electrónico encriptado que no pueda ser leído), estas herramientas la bloquean y registran el suceso.

6) Implementar prácticas de administración de contraseñas robustas.

Las políticas de seguridad de su compañía deberán incluir el uso de contraseñas robustas y bloqueo de cuenta en caso de repetidos intentos de acceso fallidos. Los atributos de una contraseña robusta incluyen utilizar un número elevado de caracteres mínimos requeridos, evitar palabras completas, y usar letras mayúsculas y minúsculas, números y caracteres especiales (por ejemplo, símbolos o signos de puntuación). Las contraseñas deberán estar protegidas por algoritmos criptográficos robustos no reversibles.

7) Revisar y fortalecer los controles de acceso a la información y habilitadores de uso.

Al momento en que los sistemas de administración de identidad y acceso son implementados, generalmente los perfiles y accesos de los usuarios son configurados de manera amplia. Este es el momento de revisar dichos perfiles y accesos para asegurar que los colaboradores tengan acceso solo a la información que necesitan para desempeñar sus funciones de manera adecuada, y no más. Las restricciones de acceso deberán incrementarse como resultado del monitoreo para identificar actividades inusuales o sospechosas por parte de quienes tienen acceso a información confidencial.

Conclusiones

El robo de información por parte de informantes corporativos representa una amenaza real con consecuencias a largo plazo para su empresa, como la interrupción de las operaciones y un daño profundo a la reputación de la compañía. Los responsables podrían estar motivados por varios factores, incluidas la conciencia social o el deseo de obtener un beneficio personal. Las medidas preventivas deberán considerar los distintos motivos para que estas sean verdaderamente eficaces.

El problema que los colaboradores responsables revelen información delicada acerca de alguna actividad poco ética o ilícita, fuera de la jerarquía corporativa, no deberá ser tratado con hostilidad o desdén. En lugar de esto, la compañía deberá alentar a los colaboradores responsables a que levanten sus denuncias dentro de los canales autorizados y diseñados específicamente por la compañía para dicho propósito. Los colaboradores deberán estar convencidos que su organización está comprometida a erradicar cualquier comportamiento poco ético, y también que sus acciones serán reconocidas públicamente. Una vez que haya ganado la confianza de los posibles informantes, ellos se sentirán apoyados y seguros de poder levantar sus denuncias dentro de la organización, y usted evitará la publicidad negativa que acompaña a las fugas de información.

Por otro lado, los adversarios determinados representan una amenaza continua y peligrosa distinta para su organización. La prevención de pérdida de información, ataques, penetración y detección de *software* malicioso comprenden la localización, el entendimiento, la clasificación y protección de información confidencial. Capacitar a los colaboradores sobre las prácticas líderes de seguridad cibernética aumentará el grado de consciencia sobre seguridad y les brindará herramientas para combatir la ingeniería social. Contar con un programa de respuesta de incidentes robusto le permitirá reaccionar rápida y correctamente cuando eventos o individuos no previstos amenacen sus operaciones comerciales.

Ernst & Young

Aseguramiento | Asesoría | Fiscal | Transacciones

Acerca de Ernst & Young

Ernst & Young es líder global en aseguramiento, asesoría, servicios fiscales y transaccionales. A nivel mundial, nuestros 152,000 profesionales están unidos por los mismos valores y un compromiso sólido con la calidad. Marcamos la diferencia al ayudar a nuestra gente, clientes y comunidades a lograr su potencial.

Para mayor información, favor de ingresar a www.ey.com/mx/asesoria.

© 2011 Mancera S.C.
Integrante de Ernst & Young Global
Derechos reservados
Clave: TLFM001

Esta publicación contiene información en forma de resumen y, por lo tanto, su uso es solo para orientación general. No debe considerarse como sustituto de la investigación detallada o del ejercicio de un criterio profesional. Ni EYGM Limited, ni ningún otro miembro de la organización global de Ernst & Young acepta responsabilidad alguna por la pérdida ocasionada a cualquier persona que actúe o deje de actuar como resultado de algún material en esta publicación. Sobre cualquier asunto en particular, referirse al asesor apropiado.

Los puntos de vista de terceros expuestos en la presente publicación no necesariamente son los puntos de vista de la organización de Ernst & Young Global o de sus firmas integrantes. Por ende, dichos puntos de vista se deben tomar en el contexto del momento en que se expresaron.

Ernst & Young se refiere a la organización global de firmas miembro conocidas como Ernst & Young Global Limited, en la que cada una de ellas actúa como una entidad legal separada. Ernst & Young Global Limited no provee servicios a clientes.

Para obtener mayor información contacte a cualquiera de nuestros líderes de la práctica de Seguridad de la Información:

Carlos Chalico
(55) 1101 6414
carlos.chalico@mx.ey.com