Cyber[SM]

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE®

TRAVELERS

Empoderando a las organizaciones para afrontar las amenazas cibernéticas en evolución.

UNA GUÍA DE CIBERSEGURIDAD

PARA PEQUEÑAS Y MEDIANAS EMPRESAS

ÍNDICE

LA EVOLUCIÓN DE LAS AMENAZAS CIBERNÉTICAS AFECTA A LAS EMPRESAS Y ORGANIZACIONES DE TODOS LOS TAMAÑOS, SECTORES E INDUSTRIAS.

INTRODUCCIÓN

Los titulares de noticias habitualmente destacan vulneraciones de datos e intrusiones informáticas de alto perfil, y las corporaciones grandes trabajan a toda hora para contener el daño a su negocio, sus clientes y su reputación. Pero las investigaciones señalan que los delincuentes cibernéticos también atacan a las empresas y organizaciones "regulares" más pequeñas que a menudo están menos preparadas para prevenir y responder a un ataque. De hecho, la evolución de las amenazas cibernéticas afecta a las empresas y organizaciones de todos los tamaños, sectores e industrias. Ha habido un aumento constante durante los últimos cinco años en ataques dirigidos a empresas con menos de 250 empleados; ahora, más del 60 por ciento de todos los ataques dirigidos atacan a entidades pequeñas y medianas.[1]

Los expertos creen que no es una cuestión de "si" su organización sufrirá una vulneración, sino "cuándo". Solo un hacker ingenioso, un empleado descontento o incluso los registros físicos extraviados de datos de clientes o la información de propiedad exclusiva de su propia organización pueden causar enormes daños financieros y de reputación. Los costos de una vulneración de datos pueden ser asombrosos, promediando $221 por registro comprometido y $7,01 millones por vulneración de datos en los Estados Unidos en el 2016.[2] Incluso las vulneraciones relativamente pequeñas pueden incurrir en costos significativos.[3] Combinada con una reputación dañada, estas pérdidas pueden devastar a una organización desprevenida.

Con esto en mente, The Travelers Institute, la división de políticas públicas de The Travelers Companies, Inc., lanzó *Cyber: Prepare, Prevent, Mitigate, Restore*℠ (Cibernética: Preparar, Prevenir, Mitigar, Restaurar), una iniciativa educativa que convoca a la comunidad empresarial con líderes cibernéticos del sector público y privado. Trabajando con expertos en ciberseguridad, organismos gubernamentales y profesionales de la industria de seguros, *Cyber: Prepare, Prevent, Mitigate, Restore* (Cibernética: Preparar, Prevenir, Mitigar, Restaurar) le proporciona a los propietarios de negocios la información y los recursos necesarios para afrontar el desafío de la ciberseguridad.

En esta guía, ofrecemos salvaguardias fundamentales que pueden ser utilizadas por organizaciones pequeñas y medianas para mejorar su ciberseguridad. Estas salvaguardias, identificadas por los profesionales de riesgo cibernético de Travelers en el curso de ayudar a los asegurados a manejar sus riesgos de ciberseguridad, pueden ayudar a cualquier organización a estar mejor preparada, y a ser más capaz de prevenir intrusiones, mitigar los daños y restaurar las operaciones normales cuando los hackers atacan.

EN ESTA GUÍA, OFRECEMOS SALVAGUARDIAS FUNDAMENTALES QUE PUEDEN SER UTILIZADAS POR ORGANIZACIONES PEQUEÑAS Y MEDIANAS PARA MEJORAR SU CIBERSEGURIDAD.

"Al no prepararse, se están preparando para el fracaso".

– Benjamin Franklin

ESTÉ PREPARADO:

- CONOZCA SUS DATOS, SISTEMAS Y RED
- ENFOQUE SUS ESFUERZOS DE CIBERSEGURIDAD
- VALIDE SU ESTRATEGIA DE RESPALDO
- PLANEE LA RESPUESTA A INCIDENTES

PREPARAR – PREVENIR – MITIGAR – RESTAURAR

Benjamin Franklin nunca tuvo que pensar en la ciberseguridad, pero entendía una de sus piedras angulares: la preparación es crítica. En un mundo donde los recursos son limitados, debe saber qué sistemas está ejecutando, qué datos está almacenando y cómo su red está estructurada para asignar sus recursos de ciberseguridad eficazmente.

Sin embargo, no basta con implementar controles de seguridad sólidos, ya que todos sabemos que las organizaciones con una sólida seguridad pueden verse comprometidas. Por consiguiente, es importante mantener respaldos periódicos de datos importantes e implementar un plan de respuesta de incidentes para utilizarlo cuando ocurra un incidente.

Conozca sus datos, sistemas y red

Las empresas y organizaciones suelen almacenar muchos tipos de datos, utilizando una variedad de sistemas informáticos, en redes que pueden ser locales, globales o en algún lugar intermedio. Por lo tanto, el primer principio de la ciberseguridad es "conocerse a sí mismo". Sepa qué datos (y dónde) se crean, recopilan y almacenan los datos; mantenga un inventario preciso de sistemas informáticos y software; y comprenda su infraestructura de red.

Esto le permite hacer mejor lo siguiente:

- Identificar y priorizar los controles de seguridad apropiados.
- Eliminar los sistemas y el software no autorizados de su red.
- Parchear y mantener los sistemas y software existentes.
- Reconocer nuevas vulnerabilidades en los sistemas y software existentes.
- Responder más eficazmente cuando ocurra un incidente.

Hay muchos tipos de datos que se pueden encontrar en un sistema o una red, incluyendo los siguientes:

Información **m**édica **p**rotegida

(Protected Health Information, PHI)

tales como los registros de salud o médicos de los pacientes o empleados.

Información de **t**arjeta de **p**ago

(Payment Card Information, PCI)

tales como números de cuenta de tarjeta de crédito o débito.

Información de **i**dentificación **p**ersonal

(Personally Identifiable Information, PII)

tales como nombres, direcciones, números de teléfono, números de cuenta del seguro social u otra información de identificación.

Propiedad intelectual

tales como procesos de fabricación, estrategias de marketing y otros secretos comerciales.

Otra información de propiedad exclusiva

incluyendo información confidencial compartida por un socio comercial.

En muchos casos, puede ser apropiado que su organización adopte un esquema de clasificación de datos. Una cierta clase de datos puede justificar controles de seguridad más fuertes si son particularmente valiosos para la organización, si su pérdida sería particularmente perjudicial o si merecen un trato especial a raíz de las obligaciones legales o contractuales.

A continuación, se debe mantener un inventario de sistemas y software para identificar todos los dispositivos que tengan acceso a la red, incluyendo computadoras de escritorio, computadoras portátiles, dispositivos móviles, servidores, equipos de red e impresoras. El inventario debe identificar a una persona específica responsable de cada dispositivo (por nombre y cargo), así como la dirección de red y la ubicación física del dispositivo.

Las organizaciones también deben mantener un inventario de aplicaciones de software, identificando los sistemas (incluyendo servidores, estaciones de trabajo y computadoras portátiles) en los que residen.

Cualesquiera sistemas o aplicaciones que no estén autorizados deben ser investigados y eliminados.

Por último, es importante mantener información precisa sobre la estructura y topología de la red de una organización. Esta información se puede utilizar en el curso normal del negocio para asegurar que los cambios en la red sean coherentes con los controles de seguridad de red existentes. También será de gran valor en el curso de la respuesta a un incidente de ciberseguridad.

CUANDO LAS VULNERACIONES HAN RESULTADO EN RECLAMACIONES DE SEGUROS

el 14 %
de las reclamaciones involucraron la pérdida de PHI

el 27 %
de las reclamaciones involucraron la pérdida de PCI

el 45 %
de las reclamaciones involucraron la pérdida de PII [4]

Enfoque sus esfuerzos de ciberseguridad

Una vez que comprenda los datos, los sistemas y la red que trata de proteger, puede enfocarse en implementar (o mejorar) los controles de seguridad que serían más eficaces a raíz de sus necesidades y recursos específicos. (También estará mejor preparado para trabajar con un consultor de ciberseguridad, si elige hacerlo.)

Considere lo siguiente:

¿Cuál es su "tesoro real"?

Si ha adoptado un esquema de clasificación de datos, deseará implementar controles de seguridad más sólidos para el almacenamiento y la transmisión de datos que se clasifican como más sensibles.

¿Cuáles son sus vulnerabilidades?

Una evaluación de la vulnerabilidad puede ayudar a identificar puntos débiles en su ciberseguridad que merecen una mayor atención. Si su organización permite el acceso a sistemas o redes por parte de terceros, tales como contratistas o proveedores, debe entender que las vulnerabilidades de ellos se convierten en sus vulnerabilidades.

¿Cuáles son las situaciones de amenaza más probables?

Si entiende las amenazas que tienen más probabilidades de afectar a su empresa u organización, puede enfocarse en minimizar esas amenazas.

EL CUMPLIMIENTO DE UN ESTÁNDAR DE CIBERSEGURIDAD EN PARTICULAR NO ES UN REQUISITO PREVIO PARA UNA CIBERSEGURIDAD ADECUADA, PERO PUEDE SER IMPORTANTE PARA DETERMINAR QUÉ CONTROLES DE SEGURIDAD DEBEN IMPLEMENTARSE. POR EJEMPLO, LAS EMPRESAS QUE MANEJAN LA INFORMACIÓN DE TARJETA DE PAGO DEBEN CUMPLIR CON EL ESTÁNDAR DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETA DE PAGO (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD, PCI DSS).

Hay disponible gratuitamente en línea una gran cantidad de información sobre los controles de seguridad de computadoras y redes, incluyendo taxonomías integrales de controles de seguridad que pueden ayudarle a asegurar que no omita uno que sería valioso para su organización.[5]

Aquí resaltamos algunos controles de seguridad fundamentales:

Contraseñas fuertes: Casi todos los sistemas pueden configurarse para requerir que los usuarios seleccionen contraseñas que serían difíciles de comprometer para un intruso. Debe indicarse a los usuarios que no utilicen contraseñas (o variantes de contraseñas) que utilicen en otros lugares (p. ej., para controlar el acceso a cuentas de correo electrónico personal u otras de Internet).

Cortafuegos: Los cortafuegos se utilizan para permitir que solo el tráfico apropiado entre y salga de un sistema o una red. Al igual que cualquier otro control de seguridad, debe configurarse y mantenerse adecuadamente un cortafuegos para que sea eficaz. Los cortafuegos solo deben permitir el tráfico de red que sea apropiado para las necesidades del negocio o la organización. Por ejemplo, es probable que se rechacen las solicitudes de transferencia de archivos al servidor de correo electrónico de una empresa.

Antivirus: El software antivirus está diseñado para defender su red contra el software malicioso ("malware"). Para mantener una defensa eficaz, su software antivirus debe ejecutarse en segundo plano en todo momento y actualizarse continuamente. La capacidad de instalar rápidamente actualizaciones de antivirus en todos los sistemas es fundamental.

Filtrado de contenido: Los controles de filtrado de contenido restringen el material entregado por Internet a través de la web, el correo electrónico u otros medios. Permiten a una empresa u organización bloquear archivos adjuntos en correos electrónicos o materiales de sitios web que puedan incluir spyware, virus, pornografía y otros contenidos objetables. Los filtros de "spam" (correo basura), en particular, deben utilizarse para bloquear los mensajes de correo electrónico indeseados o potencialmente peligrosos.

Cifrado: Se puede emplear el cifrado para proteger los datos que su organización considere sensibles. El cifrado debe considerarse tanto para los datos almacenados ("datos en reposo") como para los datos que se trasladen o envíen a alguna parte ("datos en movimiento"). Muchos expertos en seguridad creen que los datos corren el mayor riesgo cuando están en movimiento. Siempre que los datos sensibles se transmitan externamente, considere el uso del cifrado. Además, si los datos sensibles se transmiten internamente a través de redes menos seguras, considere el uso del cifrado. Para las computadoras portátiles y los dispositivos móviles, el uso del cifrado del disco entero puede reducir significativamente los riesgos asociados con los dispositivos perdidos o robados.

Autenticación de múltiples factores (o de dos factores): Un factor de autenticación es una categoría de credencial independiente utilizado para la verificación de identidad. Los tres factores de autenticación más comunes a menudo se describen como algo que sabe (p. ej., una contraseña), algo que tiene (p. ej., un teléfono inteligente o una tarjeta de acceso) y algo que es (p. ej., los datos biométricos como las huellas dactilares). Algunas tecnologías también utilizan la ubicación (p. ej., coordenadas GPS) y la hora del día como factores de autenticación adicionales. La autenticación de múltiples factores se utiliza a menudo para procurar el control de datos sensibles o para procurar el acceso remoto a una red.

Red privada virtual (virtual private network, VPN): Una VPN es una red segura que se basa en una red subyacente más grande. En una situación común, una empresa puede proporcionar acceso remoto a la red de la empresa a través de una VPN, lo que permite a sus empleados acceder a la red de la empresa de forma segura a través del Internet público. Una VPN también se puede utilizar para proporcionar acceso limitado a parte de una red. Por ejemplo, una empresa podría utilizar una VPN para permitir a los proveedores independientes acceder a determinados sistemas o servicios en su red, sin proporcionar acceso a toda la red.

Registro de aplicaciones y redes: Muchos sistemas, aplicaciones y dispositivos de red tienen una capacidad incorporada para generar archivos de registro que reflejan el acceso y la actividad de los usuarios. Estos archivos de registro pueden ser muy útiles en caso de un incidente de ciberseguridad, particularmente para los sistemas y las aplicaciones que almacenan y manipulan información sensible.

Sistema de detección de intrusiones (intrusion detection system, IDS): Un IDS puede trabajar junto con los cortafuegos para analizar el tráfico de red y bloquear el tráfico que coincida con un patrón de ataque conocido o sospechoso.

Después de decidir los controles de seguridad que deben implementarse y en los que se debe enfocar, una organización debe documentar sus razones como parte de un plan o una estrategia de ciberseguridad global. No se puede esperar que una organización implemente todos los controles de seguridad posibles, pero debe contar con un plan razonable y documentado para proteger sus datos, sistemas y redes.

UNA ORGANIZACIÓN QUE EJECUTA UNA VERSIÓN OBSOLETA DE UN SISTEMA OPERATIVO O UNA APLICACIÓN (ES DECIR, UNA VERSIÓN PARA LA CUAL YA NO SE ESTÁN LANZANDO PARCHES Y ACTUALIZACIONES DE SEGURIDAD), DEBE HACER LA TRANSICIÓN A UNA VERSIÓN COMPATIBLE. DE LO CONTRARIO, EL SISTEMA O LA APLICACIÓN VULNERABLE DEBE Y/O PONERSE EN CUARENTENA CUIDADOSAMENTE.

Valide su estrategia de respaldo

Una de las medidas más importantes que puede tomar una organización para protegerse contra los riesgos cibernéticos es mantener respaldos periódicos y sistemáticos de los datos importantes. Una estrategia de respaldo bien diseñada protegerá contra fallas del sistema y almacenamiento, así como contra incendios o inundaciones. Además, el ransomware está en aumento. Los delincuentes cibernéticos utilizan el cifrado para "bloquear" los datos hallados en las computadoras comprometidas y exigen un pago para descifrar los datos. El mantenimiento de respaldos adecuados puede protegerle de convertirse en una víctima del ransomware más reciente.

Al evaluar su estrategia de respaldo, deseará considerar qué datos necesitan respaldarse, con qué frecuencia se deben realizar respaldos y dónde deben almacenarse los respaldos. Por ejemplo, el mantenimiento de respaldos remotos en "la nube" puede ser simple y rentable, pero es posible que los respaldos no estén disponibles inmediatamente si está caída su conexión a Internet. El costo de cualquier estrategia de respaldo en particular tendrá que ponderarse frente a la rapidez y fiabilidad con la que pueden recuperarse los datos si se dañan o destruyen.

A menudo tendrá sentido implementar una estrategia de respaldo "escalonada" en la que se realice un respaldo de los datos con frecuencia a una ubicación, y tal vez con menos frecuencia a una segunda ubicación. Por ejemplo, se puede utilizar un servicio de respaldo remoto para los respaldos nocturnos, realizándose una copia de respaldo adicional en un dispositivo de almacenamiento local cada semana y almacenándose en una ubicación separada y segura. Con el crecimiento del ransomware, al menos una copia de respaldo debe almacenarse sin conexión o en una parte más segura de su red.

Las copias de respaldo de los datos deben cifrarse si los datos originales justifican el cifrado. Las copias de respaldo también deben probarse periódicamente para asegurar que los datos puedan, de hecho, ser restaurados si los datos originales han sido dañados o destruidos.

Planee la respuesta a incidentes

Cada organización debe planear lo inesperado, incluyendo una vulneración de datos o un incidente cibernético. De hecho, sin un plan de respuesta a incidentes, existe una mayor probabilidad de cometer errores en la respuesta a la vulneración o al incidente; por ejemplo, al no cumplir con las leyes y reglamentaciones aplicables. Estos errores pueden causar daños a la empresa u organización que van más allá de los daños causados directamente por el ataque. Un plan de respuesta a incidentes bien diseñado hará más fácil que su organización inicie una respuesta rápida y coordinada.

EN MÁS DEL **90 %** DE LAS VULNERACIONES, EL COMPROMETIMIENTO TOMA SOLO UNOS MINUTOS O MENOS

Y EN EL **99,6 %** DE LAS OCASIONES, LOS DATOS SON FILTRADOS EN CUESTIÓN DE DÍAS.[6]

EN GENERAL, UN PLAN DE RESPUESTA A INCIDENTES DEBE INCLUIR AL MENOS LOS SIGUIENTES COMPONENTES:

1. INFORMACIÓN SOBRE LAS PERSONAS EN LA ORGANIZACIÓN QUE FORMARÁN EL EQUIPO DE RESPUESTA A INCIDENTES;

2. DIRECTRICES Y PROCEDIMIENTOS PARA AYUDAR AL EQUIPO; Y

3. INFORMACIÓN SOBRE LOS RECURSOS EXTERNOS DISPONIBLES PARA APOYAR AL EQUIPO.

El equipo de respuesta a incidentes

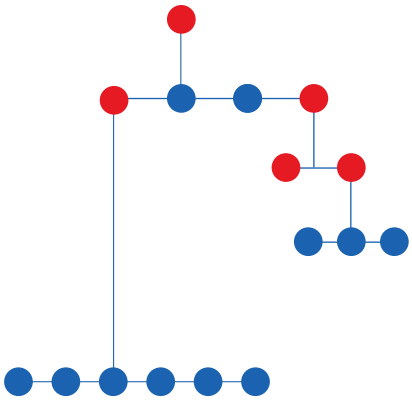
Identifique a los miembros del equipo por nombre y cargo, junto con una descripción de las funciones y responsabilidades. Un gerente experimentado, como el Director de Seguridad de la Información, debe desempeñarse como el líder del equipo para ayudar a coordinar el esfuerzo de respuesta global. Otros miembros deben incluir a representantes de las áreas de gerencia, tecnología de la información, asuntos legales, cumplimiento y relaciones públicas/relaciones con los medios de comunicación.

Procedimientos y directrices para la respuesta a incidentes

Un plan de respuesta a incidentes debería proporcionar un marco de acción para que las decisiones importantes sean consideradas con antelación y no sean tomadas bajo presión. En particular, es importante que el plan de respuesta a incidentes proporcione procedimientos y directrices sobre cuestiones difíciles, incluyendo la identificación de líneas de autoridad y obligaciones de presentación de informes internas. El equipo debe enfocarse en tomar las mejores decisiones posibles, no en averiguar cómo deben tomarse las decisiones y quién debe tomarlas.

Los procedimientos y directrices claros sobre las siguientes preguntas pueden facilitar enormemente un esfuerzo de respuesta a incidentes:

- ¿Se aplica el plan de respuesta a incidentes? No todos los incidentes de seguridad requerirán invocar el plan.
- ¿Está asegurada la empresa u organización para el incidente? Si es así, ¿cuándo se debe notificar a la aseguradora?
- ¿El equipo debe traer recursos externos? ¿Debe notificarse a las autoridades policiales? ¿Quién tendrá la responsabilidad principal de coordinar con ellos?
- ¿Cuándo se deben apagar determinados servicios o partes de la red o hacerse transiciones de ellos a los sistemas de respaldo, si están disponibles? Por ejemplo, probablemente debería haber diferentes criterios para apagar un servidor de correo electrónico y un servidor de sitio web orientado al cliente.
- ¿Qué datos, de ser extraviados o expuestos, están sujetos a las leyes de notificación de vulneración de datos? Si se requiere una notificación, ¿cuándo y cómo debe realizarse la notificación?
- ¿Qué datos, de ser extraviados o expuestos, deben informarse a los reguladores gubernamentales? ¿Y a los socios comerciales?
- ¿Debe comunicarse la información sobre el incidente a los empleados de la organización? ¿Y al público?
- ¿Cómo debe el equipo documentar el esfuerzo de respuesta de incidentes, y cómo debe preservar los registros o la evidencia que recopila durante la investigación?



Por supuesto, no será posible que un plan de respuesta a incidentes proporcione procedimientos y directrices detallados para abarcar todas las cuestiones o situaciones posibles. Los procedimientos y las directrices deben ser lo suficientemente flexibles como para aplicarse a una serie de diferentes incidentes cibernéticos, al tiempo que proporcionan una orientación más concreta para los incidentes que se consideren más probables.

Recursos externos

Dependiendo de la naturaleza y el alcance del incidente, puede ser apropiado que el equipo de respuesta a incidentes solicite la asistencia de recursos externos, tales como un "instructor de vulneraciones", un experto forense de computadoras y redes, o un consultor de gestión de crisis. La mayoría de las compañías no tienen empleados con la experiencia y el tiempo para manejar un esfuerzo de respuesta a incidentes.

En el curso del desarrollo de un plan de respuesta a incidentes, es importante identificar los recursos externos y establecer relaciones con ellos antes de que ocurra un incidente, de modo que estén preparados para brindar asistencia cuando sea necesario. También será más rentable negociar estos servicios antes de un incidente, en lugar de esperar hasta que su organización los necesite urgentemente.

Si su organización externaliza cualquier parte de su función de TI, el plan de respuesta a incidentes también debe proporcionar información de contacto para sus proveedores de TI. A menudo será necesario trabajar con sus proveedores de TI para investigar y obtener evidencia después de un incidente de ciberseguridad.

Una vez que haya implementado un plan de respuesta a incidentes, es importante probarlo regularmente; anualmente, si es posible.

Pruebas del plan de respuesta a incidentes

Estos ejercicios “prácticos” deben involucrar al equipo de respuesta a incidentes completo, y los resultados de los ejercicios deben ser puestos a la disposición de la alta gerencia. Es mejor abordar los problemas que podrían ser planteadas por la alta gerencia sobre el plan de respuesta a incidentes en relación con un ejercicio práctico, no en medio de un esfuerzo de respuesta a incidentes real.

Ayudar a prevenir los incidentes cibernéticos dañinos.

PREVENIR INCIDENTES:

- FORTALEZCA LOS CONTROLES DE ACCESO
- PARCHE LAS VULNERABILIDADES CONOCIDAS
- EDUQUE A SUS EMPLEADOS
- ADOPTE POLÍTICAS Y PROCEDIMIENTOS CONSCIENTES DE LA SEGURIDAD

PREPARAR – **PREVENIR** – MITIGAR – RESTAURAR

Los controles de seguridad y los planes de respuesta a incidentes son necesarios, pero no necesariamente suficientes, para una ciberseguridad adecuada. La implementación de las siguientes cuatro directrices ayudará en gran medida a su organización a prevenir eficazmente los incidentes cibernéticos dañinos:

1. Fortalezca los controles de acceso;
2. Parchee inmediatamente las vulnerabilidades de aplicaciones y sistemas;
3. Eduque a sus empleados sobre los riesgos cibernéticos y las prácticas de seguridad; y
4. Adopte políticas y procedimientos que integren las buenas prácticas de seguridad en sus operaciones comerciales.

Fortalezca los controles de acceso

Todos estamos familiarizados con las contraseñas, las cuales se encuentran entre los tipos de controles de acceso más fundamentales. Los controles de acceso más sofisticados se están convirtiendo en algo habitual. Por ejemplo, muchos bancos e instituciones financieras han empezado a requerir la autenticación de dos factores para el acceso a la cuenta en línea, y muchos teléfonos inteligentes y computadoras pueden desbloquearse usando identificadores biométricos, como huellas dactilares. La implementación juiciosa de controles de acceso más fuertes, como limitar el número de empleados con acceso a la red remota, puede ser una forma rentable de mejorar la ciberseguridad de su organización.

Incluso sin la adopción de nuevas tecnologías de control de acceso, las empresas y organizaciones pueden beneficiarse si se adhieren al principio del menor privilegio: es decir, el acceso a los datos, los sistemas y la red solo debe permitirse en la medida necesaria para la operación fluida y continua de la empresa. Alguna información puede ser accesible por todos; alguna información puede restringirse a un departamento específico; y alguna información debe ser accesible solamente por un conjunto de personal clave.

El principio del menor privilegio debe aplicarse a todos los usuarios, incluidos los administradores del sistema y otros miembros de un departamento de TI. A menudo se considera que el uso inadecuado de los privilegios administrativos es un factor que contribuye de manera importante a las vulneraciones de datos y otros incidentes cibernéticos.

En muchas organizaciones en crecimiento, los administradores de sistemas asumen numerosas funciones laborales y tienen acceso a múltiples sistemas o aplicaciones. Esto puede presentar un riesgo de seguridad si los privilegios administrativos no se controlan adecuadamente, lo que hace más fácil para un atacante obtener el control total de un sistema comprometido. Para minimizar este riesgo, se deben considerar los siguientes controles:

- No se debe permitir a los usuarios privilegios administrativos locales, incluso en computadoras proporcionadas para su uso exclusivo.
- Los miembros del personal de TI deben tener privilegios administrativos solo para sistemas o aplicaciones específicos, y solo en la medida necesaria para el cumplimiento de sus funciones.
- Los miembros del personal de TI con privilegios administrativos deben mantener cuentas separadas para el uso diario y para el uso como administrador del sistema. La cuenta de administrador no debe utilizarse para el acceso rutinario al correo electrónico o al Internet. La contraseña de la cuenta de administrador no debe compartirse, incluso con otros miembros del personal de TI, y debe ser diferente de la contraseña de la cuenta de usuario.
- Cuando deban otorgarse privilegios más amplios a un usuario o administrador del sistema para realizar una tarea específica, otorgue los privilegios solo por un tiempo limitado.

Por último, es importante incluir controles de acceso físico para los datos y sistemas sensibles. Proporcionar seguridad física al exterior del edificio puede ser un primer paso para protegerse contra el acceso a sistemas y redes no autorizado. Proteja las áreas tales como las salas de servidores, las salas de computadoras y las salas de equipos telefónicos a través de medidas de seguridad apropiadas, tales como puertas cerradas con llave y controles de entrada.

SEGUIR EL PRINCIPIO DEL MENOR PRIVILEGIO PUEDE AYUDAR A REDUCIR EL RIESGO DE LA INVOLUCRAMIENTO DE INFILTRADOS INTERNOS, UN FACTOR EN MÁS DEL 30 % DE LAS RECLAMACIONES DE SEGURO CIBERNÉTICO.[7]

Parche las vulnerabilidades conocidas

La directriz es simple: parchee sus sistemas y software. Una vulnerabilidad sin parche es uno de los métodos más fáciles y más comunes de comprometer un sistema informático o una red.

Desafortunadamente, puede haber obstáculos significativos para asegurar que todos los sistemas informáticos y aplicaciones de software en una red estén completamente parcheados. En primer lugar, en la mayoría de las redes corporativas, hay una multitud de aplicaciones que se ejecutan en una variedad de sistemas diferentes. Todas estas aplicaciones y sistemas pueden requerir parches, proporcionados por una serie de proveedores independientes. En segundo lugar, constituye una buena práctica probar los parches antes de que se implementen, en particular para los sistemas o el software que se consideran indispensables, lo cual plantea retrasos. Por último, los parches no siempre se aplican con éxito, en particular a las computadoras portátiles y otros dispositivos móviles que se desconectan con frecuencia de la red.

Estas dificultades pueden abordarse en parte mediante el uso de un sistema de gestión de parches. Ya sea que utilice un sistema de gestión de parches comercial o herramientas desarrolladas internamente, el sistema debería:

- **Ayuda a rastrear, obtener y validar los parches disponibles.**

  A medida que los distintos proveedores lanzan parches para sus productos, el sistema debe identificar qué parches se necesitan en su entorno particular y ponerlos a disposición del personal de TI para realizar pruebas y evaluaciones.

- **Permitir los parches basados en prioridades.**

  Los parches de rutina se pueden aplicar en un horario predeterminado, pero los parches críticos deben aplicarse lo antes posible.

- **Realizar informes y auditorías.**

  Si la implementación de un parche falla en cualquier parte de la red, la información sobre el error debe estar fácilmente disponible para los miembros del personal de TI.

LOS PARCHES NO SIEMPRE SE APLICAN CON ÉXITO, EN PARTICULAR A LAS COMPUTADORAS PORTÁTILES Y OTROS DISPOSITIVOS MÓVILES QUE SE DESCONECTAN CON FRECUENCIA DE LA RED.

También constituye una buena práctica que una organización analice regularmente sus sistemas y redes para detectar vulnerabilidades que el sistema de gestión de parches haya omitido.

En algunos casos, puede ser necesario continuar utilizando un sistema o aplicación con vulnerabilidades conocidas; por ejemplo, un sistema heredado con una vulnerabilidad para la cual no hay ningún parche disponible. En tal caso, el sistema vulnerable debe protegerse cuidadosamente utilizando otros medios, tales como los cortafuegos y controles de acceso estrictos.

Eduque a sus empleados

Muchos incidentes de ciberseguridad pueden atribuirse directamente a una capacitación inadecuada sobre la seguridad. Un programa de capacitación diseñado para empoderar a los empleados a reconocer las amenazas cibernéticas comunes y para notificar al personal de TI constituye una forma rentable de reducir estas amenazas.

Un programa de capacitación integral debe:

- **Enfatizar la importancia de la ciberseguridad para el éxito de la organización.** Los empleados deben entender por qué son importantes los datos, los sistemas y la seguridad. Una vulneración de seguridad puede permitir que los atacantes drenen la cuenta bancaria de una organización; pueden seguir otras repercusiones financieras y legales, tales como los costos de respuesta a incidentes, los gastos de notificación de la vulneración de datos, y la pérdida de reputación y el fondo de comercio. Si es aplicable, deben resaltarse los requisitos legales y reglamentarios para proteger ciertos tipos de datos, tales como la información médica personal (personal health information, PHI). La capacitación debe abordar la responsabilidad de cada empleado de proteger los datos, los sistemas y las redes de la organización.
- **Capacitar a los empleados para evitar riesgos de seguridad de la información.** Los riesgos pueden incluir el phishing (suplantación de identidad) y otras formas de ingeniería social, así como la gestión incorrecta de contraseñas, la navegación de Internet insegura y el uso de software no autorizado.
- **Explicar cómo proteger las computadoras portátiles, los dispositivos móviles y los medios de almacenamiento digital.** Se debe recordar a los empleados que protejan físicamente los datos y dispositivos, así como cuándo y cómo utilizar el cifrado. Las computadoras y otros activos físicos se pierden con una frecuencia de más de 100 veces que lo que son robados.[8]
- **Alentar a los empleados a informar las actividades sospechosas.** Los empleados deben ser conscientes de sus procedimientos de respuesta a incidentes y deben saber cómo informar sobre actividades sospechosas, incluyendo las llamadas telefónicas dudosas, al personal de TI o de seguridad.

Por último, los empleados también deberían recibir capacitación sobre políticas y procedimientos relacionados con la ciberseguridad. En muchos casos, explicar la justificación de las políticas restrictivas de "uso del sistema" ayudará a promover un mayor cumplimiento.

El número de campañas de spear phishing dirigidas a los empleados aumentó un 55 % en el 2015.[9]

Adopte políticas y procedimientos conscientes de la seguridad

La ciberseguridad adecuada será difícil de lograr si las políticas o los procedimientos de una empresa son descuidados: un hacker experto puede comprometer a toda una red corporativa desde un punto de apoyo obtenido en una computadora vulnerable.

Hay varias esferas en particular en las que las políticas o los procedimientos formales pueden mejorar sustancialmente la ciberseguridad:

CUANDO SE AGREGAN NUEVOS DISPOSITIVOS A UNA RED, DEBE HABER PROCEDIMIENTOS PARA ASEGURAR QUE SE CAMBIEN LAS CONTRASEÑAS PREDETERMINADAS; SE APLIQUEN PARCHES Y ACTUALIZACIONES; Y SE ELIMINEN O DESHABILITEN LOS SERVICIOS, LAS APLICACIONES Y LOS PUERTOS DE RED INNECESARIOS.

- Debería implementarse una política de "uso del sistema" para regir el uso de las computadoras y la red de la empresa u organización, incluyendo las restricciones apropiadas para el uso del correo electrónico, las redes sociales, el Internet, los dispositivos de almacenamiento externo, y los sistemas y el software no autorizados.
- También debería haber procedimientos sobre los requisitos de eliminación de información y datos sensibles, incluyendo los sistemas informáticos y dispositivos de almacenamiento que almacenan o procesan tales datos.
- El control inadecuado de los cambios en los equipos y sistemas de red puede ser una causa común de fallas de seguridad y sistemas. La falta de un procedimiento escrito crea el riesgo de que se puedan realizar cambios sin la preparación o las pruebas apropiadas. Establezca procedimientos escritos que rijan y coordinen todos los cambios en las configuraciones existentes.
- Debe haber un proceso para revocar inmediatamente el acceso al sistema y a la red cuando un empleado deja una empresa u organización, y para cambiar las contraseñas y otros controles de las cuentas compartidas, según corresponda, que el empleado puede haber conocido o accedido. También puede ser recomendable que los empleados firmen un acuerdo de confidencialidad o de no divulgación, así como una declaración al abandonar la empresa u organización expresando que no han tomado datos sensibles, de propiedad exclusiva, confidenciales u otros.

Gestión de proveedores

Las empresas y las organizaciones deben prestar atención especial a las políticas y los procedimientos relacionados con sus proveedores, ya sean de TI u otros. La ciberseguridad de una organización se verá seriamente amenazada si se proporciona acceso a los sistemas o la red de la organización a un proveedor con una ciberseguridad deficiente.

De acuerdo con el principio del menor privilegio, una organización solo debe proporcionar a un proveedor el nivel de acceso a los sistemas o la red que sea necesario para el desempeño de las responsabilidades del proveedor. Los proveedores deben estar sujetos a los mismos requisitos de contraseña que otros usuarios (o administradores del sistema, según corresponda), y no deben utilizar la misma contraseña en distintos sitios del cliente. Una vez que la organización ya no esté utilizando el proveedor, deben existir políticas y los procedimientos para asegurar que se revoquen rápidamente las credenciales y los privilegios de acceso.

Las políticas y los procedimientos de la organización también deberían garantizar que el proveedor haya adoptado prácticas de ciberseguridad sólidas, en consonancia con el nivel de acceso a los datos, los sistemas y la red suministrado al proveedor. Por ejemplo, podría ser apropiado incluir disposiciones contractuales que establezcan requisitos de ciberseguridad, acuerdos para ayudar con investigaciones, obligaciones de seguros, disposiciones de indemnización, etc. Si al proveedor se le proporciona acceso a datos sensibles, tales como la información de identificación personal, podrían ser apropiados controles adicionales, tales como requerir evaluaciones independientes de las prácticas de ciberseguridad del proveedor.

Los atacantes se están aprovechando cada vez más de las relaciones de externalización para obtener acceso a la información sensible.[10]

Los incidentes cibernéticos no tienen por qué ser catastróficos si se gestionan correctamente.

MITIGAR EL DAÑO:

- DETECTE LOS INCIDENTES TEMPRANO
- EJECUTE SU PLAN DE RESPUESTA
- OBTENGA AYUDA CUANDO LA NECESITE
- DOCUMENTE SU ESFUERZO DE RESPUESTA

PREPARAR – PREVENIR – **MITIGAR** – RESTAURAR

Los incidentes cibernéticos pueden ser inevitables pero no tienen por qué ser catastróficos si se gestionan correctamente. La detección temprana es crucial. Por lo que las organizaciones deben revisar los registros de red y seguridad con la mayor frecuencia posible. De hecho, el monitoreo continuo es un objetivo digno.

Cuando ocurra un incidente, un plan de respuesta a incidentes bien diseñado será de gran valor para guiar a la empresa u organización desde las etapas iniciales de la respuesta a incidentes: investigar, evaluar y mitigar, hasta la eventual restauración de las operaciones normales. A menudo tiene sentido que una organización busque experiencia externa, para contener los daños causados por un incidente; siempre tendrá sentido documentar las acciones tomadas durante todo el proceso de respuesta a incidentes (así como las razones para ello).

Detecte los incidentes temprano

Incluso una organización con una sólida ciberseguridad no puede asumir que su red es impenetrable. Por lo tanto, es de vital importancia detectar incidentes temprano para minimizar el daño en caso de un comprometimiento.

Afortunadamente, la mayoría de los sistemas (y muchas aplicaciones) incluyen alguna capacidad de registro o monitoreo. Los cortafuegos de red se pueden configurar para registrar el tráfico sospechoso y emitir alertas en condiciones especificadas. Casi todas las computadoras pueden configurarse para realizar un seguimiento de los intentos de inicio de sesión fallidos, lo cual es un indicador temprano de un ataque potencial. Las empresas y las organizaciones deben ser conscientes de las capacidades de registro y monitoreo que ya están disponibles; además, existen sistemas de monitoreo de red especializados que se pueden implementar para permitir un monitoreo más estrecho del tráfico de red.

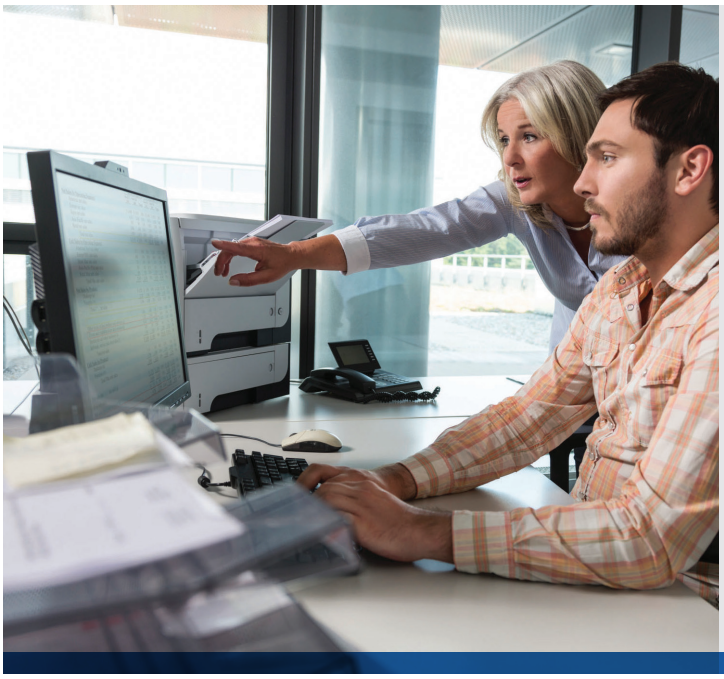
Sin embargo, generalmente no es práctico configurar todos los sistemas y aplicaciones para que registren tantos datos como sea posible. En cambio, las organizaciones deberían enfocar sus capacidades de registro y monitoreo en la protección de sus activos más valiosos. Por ejemplo, es probable que los intentos de inicio de sesión fallidos en un servidor central de base de datos se investiguen más inmediata y exhaustivamente que los intentos de inicio de sesión fallidos en la computadora portátil de un empleado promedio.

Para muchas organizaciones, tendrá sentido utilizar un sistema de gestión de eventos de incidentes de seguridad (security incident event management, SIEM), ya sea implementado internamente o proporcionado por un proveedor. Este sistema funciona como un recurso centralizado para recopilar, supervisar y analizar registros de red y otra información relacionada con la seguridad. Mediante el uso de un SIEM, las organizaciones pueden reducir enormemente el riesgo de que se pierdan los primeros indicadores de un comprometimiento.

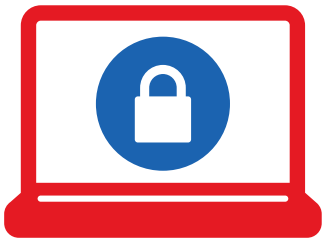
Ejecute su plan de respuesta

Cuando una organización se ve afectada por un incidente cibernético, a menudo hay una multitud de preguntas sin respuesta sobre lo sucedido, cuál será el impacto y qué hacer a continuación.

Con el fin de responder estas preguntas, su equipo de respuesta a incidentes debe enfocarse en lo siguiente: investigar el incidente, evaluar su impacto y mitigar cualquier daño. Estas tareas a menudo deben emprenderse simultáneamente, en medio de una situación que cambia rápidamente, con información incompleta y a veces inexacta. En estas circunstancias difíciles, un plan de respuesta a incidentes bien diseñado ayudará al equipo a tener éxito al delinear las áreas de responsabilidad, facilitar el intercambio de información e identificar los directrices o procedimientos pertinentes. Por ejemplo, al decidir si se debe utilizar a un consultor forense de computadoras y redes durante la investigación.



NOTIFIQUE A SU COMPAÑÍA DE SEGUROS INMEDIATAMENTE DESPUÉS DE QUE SE DESCUBRA UN INCIDENTE. EL SEGURO CIBERNÉTICO PUEDE AYUDAR A LAS EMPRESAS AL PROPORCIONAR ACCESO A UN INSTRUCTOR DE VULNERACIONES, CONSULTORES FORENSES Y OTROS PROFESIONALES DE LA COMUNIDAD DE SEGURIDAD DE DATOS.



Investigue el incidente

Es probable que la investigación de un incidente cibernético sustancial, como mínimo, determinando cómo se llevó a cabo el ataque, qué sistemas se vieron comprometidos y qué datos han sido extraviados o expuestos, requiera tiempo y experiencia sustancial. Estas investigaciones típicamente implican:

- Preservar, recopilar y analizar registros de aplicaciones, sistemas y redes que puedan tener evidencia relacionada con el ataque.
- Identificar las vulnerabilidades de software o hardware que se utilizaron para facilitar el ataque.
- Identificar los cambios no autorizados a los sistemas de la red, incluyendo la instalación de software malicioso ("malware"), tales como keyloggers (registradores de teclas) o troyanos de acceso remoto.
- Determinar qué datos, si los hubiere, fueron robados o expuestos, incluyendo las contraseñas u otros controles de seguridad que pudieran haberse comprometido.

La investigación puede tener que incluir los dispositivos de red tales como cortafuegos y routers, no solo las computadoras y los servidores conectados a la red. Cualquier evidencia significativa obtenida durante la investigación debe preservarse adecuadamente, preferiblemente en consulta con un abogado.

La investigación también puede implicar entrevistas de empleados, contratistas u otros terceros que puedan haberse visto afectados por, o de otra manera puedan haberse implicado en, el incidente. La información obtenida a través de tales entrevistas debe constatarse por escrito, y las entrevistas de terceros deben realizarse preferiblemente solo en consulta con un abogado.

Evalúe el impacto

El impacto de un incidente cibernético se evaluará típicamente en muchas dimensiones: el número de sistemas afectados; la cantidad de datos perdidos (ya sea medida según el volumen de los datos o el número de víctimas cuyos datos fueron robados); la magnitud de la pérdida financiera; el efecto en las operaciones de una empresa u organización; y la dificultad prevista de la recuperación del incidente, por mencionar algunos.

Estas evaluaciones serán requeridas por la alta gerencia y también serán requeridas por el equipo de respuesta a incidentes para tomar decisiones sensatas en coyunturas críticas. Por ejemplo, el plan de respuesta a incidentes puede especificar que un consultor forense de computadoras y redes debe contratarse si el número de sistemas afectados supera un determinado umbral, o si ciertos tipos de datos (tales como la información de tarjeta de pago) han sido robados o expuestos.

En particular, el impacto de un incidente cibernético que implique la pérdida de datos se verá afectado en gran medida por el tipo de datos involucrados. Por ejemplo, la pérdida de datos de cuentas de clientes probablemente dará lugar a un esfuerzo de respuesta diferente a la pérdida de los datos propios de la empresa u organización. Siempre que un incidente cibernético implique la pérdida o incluso la pérdida potencial de datos, un abogado debe estar estrechamente involucrado en el esfuerzo de respuesta a incidentes.

Mitigue cualquier daño

Una vez que se comprenda la naturaleza y el alcance del ataque, el equipo de respuesta a incidentes puede avanzar hacia la recuperación y restauración de los datos y sistemas perdidos o dañados. Sin embargo, si el ataque está causando daños continuos a la organización, puede que sea necesario tomar medidas para mitigar ese daño incluso antes de que finalice la investigación de incidentes y la evaluación del impacto.

El impulso inmediato podría ser "cancelarlo", es decir, hacer todo lo posible por interrumpir el ataque, como desconectar todos los sistemas que se sabe han sido comprometidos. En algunos casos, esta puede ser una respuesta apropiada.

Sin embargo, deben tenerse en cuenta otros factores antes de decidir "cancelarlo".

En primer lugar, la táctica puede ser ineficaz. Es bien sabido que los atacantes intentarán incrustarse en una red comprometida, de modo que la inhabilitación de una o varias computadoras comprometidas simplemente hará que los atacantes se desplacen a otra parte de la red. La participación en un esfuerzo de mitigación "pisar un cuero seco" puede distraer al equipo de respuesta a incidentes de ejecutar un plan de recuperación y restauración más integral.

En segundo lugar, cancelarlo puede impedir la investigación. Si los atacantes han comprometido un sistema donde se almacenan datos cifrados, puede ser más importante monitorear sus actividades para saber si los atacantes han sido capaces de descifrar los datos que apagar el sistema inmediatamente.

Por último, un esfuerzo de mitigación realizado a toda prisa, sin la planificación y consideración suficiente, podría causar daños a una empresa u organización. Por ejemplo, puede que no tenga sentido apagar el servidor de correo electrónico de una empresa, si un hacker solo ha obtenido acceso limitado al servidor sin obtener acceso a los correos electrónicos.

En lugar de cancelarlo, puede ser preferible mitigar el daño participando en una estrategia de contención, bloqueando las partes de la red que los atacantes aún no han comprometido, o bloqueando los puntos de salida al reconfigurar los cortafuegos para limitar estrictamente el tráfico saliente.

Puede ser difícil para un equipo de respuesta a incidentes investigar, evaluar y mitigar los daños causados por un incidente cibernético significativo. Por lo tanto, a menudo es apropiado que la organización apoye al equipo con recursos externos.

Obtenga ayuda cuando la necesite

Hay muchos expertos y consultores externos que pueden ayudar a una empresa u organización a responder eficazmente a un incidente cibernético. Debe incluirse una lista de estos recursos externos en el plan de respuesta a incidentes, junto con directrices y políticas que ayudarán al equipo de respuesta a incidentes a determinar cuándo deben movilizarse los recursos externos.

Estos recursos incluyen:

Un "instructor de vulneraciones" y otro abogado externo. Un instructor de vulneraciones experimentado puede proporcionar orientación a lo largo del esfuerzo de respuesta a incidentes, particularmente en temas relacionados con la privacidad, los requisitos de notificación y el cumplimiento normativo. Además, los aspectos del esfuerzo de respuesta a incidentes llevados a cabo bajo la dirección de un instructor de vulneraciones pueden ser protegidos mediante el privilegio en caso de un litigio futuro.

Un experto forense en computadoras y redes. El uso de un experto forense externo es necesario si el personal de TI interno no tiene la capacidad o la experiencia para investigar el incidente, el cual puede requerir el análisis de malware o el examen de registros detallados de tráfico de red. También puede ser recomendable utilizar un experto forense externo si el incidente puede dar lugar a litigios.

Un consultor de gestión de crisis. Un consultor de gestión de crisis experimentado puede ayudar a la organización a minimizar cualquier daño de reputación que pueda resultar del incidente.

Autoridades policiales. Si hay razones para creer que se ha cometido un delito, puede ser apropiado remitir el asunto a las autoridades policiales. Pocos ataques cibernéticos ocurren aisladamente; a partir de la investigación de incidentes similares o relacionados, las autoridades policiales pueden proporcionar información sobre las herramientas y técnicas que se utilizaron para llevar a cabo el ataque. Si el ataque fue motivado financieramente, las autoridades policiales pueden estar mejor posicionadas para rastrear el dinero que fue robado, según corresponda.

Documente su esfuerzo de respuesta

A lo largo del esfuerzo de respuesta a incidentes, es importante documentar las medidas tomadas por el equipo de respuesta a incidentes. Esto ayudará a asegurar que su organización sea más capaz de identificar las lecciones aprendidas, de responder a cualquier investigación legal o normativa futura, y de conciliar cualquier cambio realizado en sus sistemas o redes después de que haya pasado urgencia del esfuerzo de respuesta a incidentes. El plan de respuesta a incidentes debe incluir formularios u otra orientación que ayuden a asegurar el mantenimiento de registros adecuado.

A veces, puede ser apropiado que un abogado se involucre en documentar el esfuerzo de respuesta a incidentes, ya que esto puede permitir que la organización afirme una reclamación de privilegio sobre los materiales en caso de un litigio futuro.

Recorra el camino a la recuperación.

RESTAURAR LAS OPERACIONES NORMALES:

- REPARAR, RESTAURAR Y REEMPLAZAR
- SIGA MONITOREANDO
- COMUNIQUE EFICAZMENTE
- IMPLEMENTE LAS LECCIONES APRENDIDAS

PREPARAR – PREVENIR – MITIGAR – **RESTAURAR**

Después de evaluar la situación, su organización estará preparada para recorrer el camino a la recuperación: reparando las vulnerabilidades; restaurando los sistemas y datos perdidos o dañados; y reemplazando contraseñas, claves de cifrado y otros controles comprometidos.

A lo largo del camino, será importante seguir monitoreando sus sistemas y redes para detectar señales de que los atacantes pueden haber evadido sus esfuerzos para eliminarlos. También será importante proporcionar información precisa sobre el incidente, siempre que sea apropiado, a las partes interesadas, ya sean empleados, socios comerciales, reguladores u otros.

Por último, su organización puede beneficiarse del incidente identificando y aplicar las lecciones aprendidas a partir de un examen cuidadoso del incidente y del esfuerzo de respuesta a incidentes.

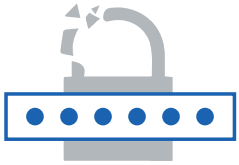
Reparar, restaurar y reemplazar

En última instancia, el objetivo de su esfuerzo de respuesta a incidentes es eliminar a los atacantes de su red y volver a las operaciones normales. Para ello, debe hacer lo siguiente:

- **Repare las vulnerabilidades.** En la mayoría de los casos, el equipo de respuesta a incidentes habrá tratado de eliminar las vulnerabilidades a medida que se hayan descubierto en el transcurso de la investigación. Las vulnerabilidades restantes que comprometan la seguridad de la red deben abordarse en esta etapa, ya sea mediante parches u otros métodos. Si no ha sido posible identificar las vulnerabilidades utilizadas por los atacantes y repararlas, el esfuerzo de recuperación podría resultar inútil.

- **Restaure los sistemas y datos perdidos o dañados.** Será mucho más fácil restaurar los datos de una copia de respaldo que volver a crear los datos perdidos o dañados. Al restaurar un sistema comprometido, el método preferido es volver a crear la imagen del sistema operativo y de las aplicaciones a partir de una imagen limpia. Si esto no es posible, se debe tener cuidado de asegurar que todos los cambios no deseados en el sistema hayan sido identificados y reparados. De lo contrario, una "puerta trasera" instalada por los atacantes podría utilizarse para volver a infectar el sistema y la red.

- **Reemplace los controles comprometidos.** Este paso final es crucial, pero a menudo se pasa por alto. Cuando los atacantes hayan comprometido un sistema o una red, a menudo pueden obtener información sobre los controles de seguridad, tales como contraseñas y claves de cifrado, que pueden utilizarse en ataques posteriores. El equipo de respuesta a incidentes debe analizar los controles de seguridad que pueden haber sido comprometidos, no solo los controles de seguridad que efectivamente hayan sido comprometidos.



Las contraseñas son robadas o expuestas en casi la mitad de todas las brechas de datos.[11]

Siga monitoreando

Es importante monitorear la red estrechamente durante todo el esfuerzo de respuesta a incidentes. Es igualmente importante que el monitoreo continúe durante un tiempo incluso después de que se crea que el esfuerzo de recuperación ha finalizado. Los atacantes a menudo reaccionarán a las medidas tomadas por el equipo de respuesta a incidentes, y el monitoreo estrecho de la red puede proporcionar información sobre los objetivos de los atacantes y cómo operan.

Lo que es más importante, el monitoreo continuo de la red ayudará a asegurar que el esfuerzo de recuperación haya tenido éxito. Debe suponerse que los atacantes, habiendo logrado una vez un punto de apoyo en una red, habrán tomado medidas para incrustarse aún más a fin de garantizar el acceso a la red incluso después de que se les haya negado el punto de comprometimiento inicial.

Dependiendo del alcance y la duración del incidente, puede ser recomendable realizar un análisis de vulnerabilidad de los sistemas y la red de la empresa u organización. Esto puede ser útil para asegurar que cualquier cambio realizado durante el esfuerzo de respuesta a incidentes no haya introducido nuevas vulnerabilidades, y también puede proporcionar una garantía adicional de que el esfuerzo de respuesta haya sido efectivamente exitoso.

Comunique eficazmente

Al responder a un incidente cibernético, puede ser muy difícil determinar qué información debe comunicarse tanto interna como externamente, ya que la información disponible sobre el incidente puede ser incompleta y no fiable. Proporcionar información que más tarde resulte inexacta puede perjudicar significativamente la reputación de la organización a los ojos de sus clientes y accionistas, y también puede invitar al escrutinio de los reguladores gubernamentales. Por lo tanto, es fundamental que la organización haya formulado una estrategia de comunicación eficaz antes de que ocurra un incidente cibernético.

Al comunicarse con la alta gerencia, es importante que el equipo de respuesta a incidentes proporcione la mayor información confiable posible sobre el alcance del incidente, su impacto potencial en la organización y la duración prevista del esfuerzo de respuesta. Es preferible que esta información sea transmitida a través de uno o varios puntos de contacto designados, con suerte identificados en el plan de respuesta a incidentes, y no a través de comunicaciones ad hoc e informales con diferentes miembros del equipo de respuesta.

Al decidir si se debe comunicar, cuándo se debe comunicar, y qué información debe comunicarse, a terceros, incluyendo al público, considere lo siguiente:

Factores a considerar:

¿La información sobre el incidente ya se ha divulgado al público o está a punto de serlo?
Si es así, probablemente obra en el mejor interés de la organización hacer una declaración pública para mantener la confianza de sus clientes y socios comerciales, y posicionarse como la fuente de información autorizada. Si es probable que la información sobre el incidente se divulgue al público, por ejemplo, si el incidente implica una pérdida de datos que debe informarse en virtud de una ley de notificación de vulneración de datos, es importante hacer una declaración pública.

¿Qué información confiable, si la hubiera, está disponible?
Durante las primeras etapas de un esfuerzo de respuesta a incidentes, puede no haber mucha información confiable en absoluto. En ese caso, si se debe hacerse una declaración pública, es de esperar que la organización pueda divulgar cuándo el incidente fue descubierto por primera vez, demostrar que ha empezado a investigar rápidamente, incluyendo cooperar con los organismos de aplicación de la ley o involucrar a investigadores externos, y describir las medidas correctivas para los terceros afectados, tales como los servicios de monitoreo de crédito.

Notificación de vulneración de datos

Siempre que se hayan perdido datos como resultado del incidente, será necesario determinar si la notificación de la vulneración es exigida por las leyes y reglamentaciones federales o estatales. Actualmente, 47 de los 50 estados tienen estatutos que exigen la notificación en diversas circunstancias cuando se produce una vulneración de datos. También hay situaciones en las que las leyes y reglamentaciones federales exigen la notificación, por ejemplo, la pérdida de información médica personal puede regirse por la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA).

Consulte con un abogado al desarrollar su estrategia de notificación para asegurarse que su notificación sea oportuna y completa. Conserve copias de todas las notificaciones que se envían, así como las respuestas recibidas.

Obligaciones de presentación de informes

Además de notificar a las personas cuyos datos pueden haber sido comprometidos, hay circunstancias en las que las vulneraciones de datos deben informarse a las autoridades estatales o federales. Por ejemplo, algunas leyes estatales exigen que se realice un informe al procurador general del estado (o a un funcionario similar) cuando cualquier ciudadano del estado tiene derecho a la notificación de vulneración de datos, pero otras leyes estatales no lo exigen. Los reguladores federales pueden esperar informes cuando la información médica personal ha sido vulnerada, cuando los contratistas y subcontratistas de defensa hayan sido comprometidos, y en otras situaciones.

Si una obligación de presentación de informes está potencialmente implicada en un incidente de ciberseguridad, su organización debe consultar con un abogado y comunicarse con la autoridad estatal o federal apropiada en el proceso de respuesta a incidentes. Aunque la investigación del incidente siga estando incompleta, es importante que la organización demuestre que entiende sus obligaciones de presentación de informes y que está tomando medidas oportunas y apropiadas para responder al incidente.

Implemente las lecciones aprendidas

Después de recuperarse de un incidente cibernético, es importante identificar y aplicar cualquier lección que se pueda aprender. Al examinar tanto el incidente como el esfuerzo de respuesta a incidentes, una organización tiene una valiosa oportunidad de mejorar su capacidad para protegerse y responder a los futuros incidentes cibernéticos.

El proceso de revisión debería incluir a los miembros del equipo de respuesta a incidentes, así como al personal (empleados o consultores externos) que no participó en el esfuerzo de respuesta a incidentes. Puede ser muy útil que el proceso de revisión sea facilitado por un gerente experimentado que no haya participado directamente en el esfuerzo de respuesta. Como mínimo, la revisión debe abarcar las siguientes preguntas:

REVISE LAS SIGUIENTES PREGUNTAS DESPUÉS DE UN INCIDENTE CIBERNÉTICO:

- ¿Se necesitan cambios adicionales en los controles de seguridad de la organización, más allá de aquellos ya realizados por el equipo de respuesta a incidentes? ¿Deben cambiarse o modificarse en el futuro las medidas correctivas que se implementaron bajo presión del tiempo?
- ¿Algún cambio en las políticas de ciberseguridad de la organización reduciría la probabilidad o gravedad de los futuros incidentes cibernéticos? ¿Algún cambio en las prácticas empresariales de la organización en su conjunto (p. ej., en relación con la información que se recopila o almacena) reduce la probabilidad o gravedad de los futuros incidentes cibernéticos?
- ¿Algún cambio al plan de respuesta a incidentes de la organización permitiría que el equipo de respuesta a incidentes respondiera de un modo más rápido y eficaz en el futuro?
- ¿Se utilizaron y gestionaron bien los recursos externos?
- ¿Se comunicó oportunamente la información apropiada a la alta gerencia?

MÁS INFORMACIÓN

Siempre hay oportunidad para que una empresa u organización mejore su ciberseguridad. Ciertamente, a medida que evoluciona el panorama de amenazas, las organizaciones deben perseguir la mejora continua, o bien arriesgarse a convertirse en la próxima víctima de la delincuencia cibernética.

The Travelers Institute espera trabajar con las empresas y organizaciones para ayudar a que nuestro mundo digital sea una fuente de gran oportunidad, no de riesgos incontrolables.

Para obtener más información acerca de ***Cyber: Prepare, Prevent, Mitigate, Restore*** (Cibernética: Preparar, Prevenir, Mitigar, Restaurar), visite travelersinstitute.org/cyber o envíe un correo electrónico a institute@travelers.com. Puede encontrar recursos cibernéticos adicionales en travelers.com/cyber.

ACERCA DE THE TRAVELERS INSTITUTE

Travelers estableció The Travelers Institute como un medio de participar en el diálogo de políticas públicas sobre asuntos de interés para el sector de seguros de siniestros de propiedad, así como de la industria de servicios financieros de manera más amplia. The Travelers Institute se basa en la experiencia de la industria de la alta gerencia de Travelers y la experiencia técnica de sus profesionales de riesgo, y otros expertos, para proporcionar información, análisis y recomendaciones a los formuladores de políticas públicas y reguladores.

NOTAS

[1] Symantec Corp., Informe de amenaza de seguridad de Internet de 2016, abril de 2016, volumen 21. https://resource.elq.symantec.com/LP=2899

[2] Ponemon Institute, Estudio sobre el costo de la vulneración de datos de 2016: Estados Unidos. http://www-03.ibm.com/security/data-breach/

[3] NetDiligence, Estudio sobre las reclamaciones cibernéticas de 2015. https://www.allclearid.com/business/resource/2015-netdiligence-cyber-claims-study/

[4] Ibíd.

[5] Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST), Controles de seguridad y privacidad para los sistemas y las organizaciones de información federal, Publicación especial del NIST 800-53 Rev. 4 (abril de 2013). http://www.nist.gov/manuscript-publication-search.cfm?pub_id=917904

[6] Verizon, Informe de investigaciones sobre la vulneración de datos de 2016. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[7] NetDiligence, Estudio sobre las reclamaciones cibernéticas de 2015. https://www.allclearid.com/business/resource/2015-netdiligence-cyber-claims-study/

[8] Verizon, Informe de investigaciones sobre la vulneración de datos de 2016. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[9] Symantec Corp., Informe de amenaza de seguridad de Internet de 2016, abril de 2016, volumen 21. https://resource.elq.symantec.com/LP=2899

[10] M-Trends 2016, Mandiant, a FireEye Company, febrero de 2016. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

[11] Risk Based Security, Inc., Tendencias de la vulneración de datos de 2015. https://www.riskbasedsecurity.com/2015-data-breach-quickview/

TRAVELERS INSTITUTE® | TRAVELERS

travelersinstitute.org

The Travelers Institute, 700 13th Street NW, Suite 1180, Washington, DC 20005