PERRY JOHNSON REGISTRARS, INC.

Resiliencia empresarial a través de la ciberseguridad

La creciente importancia de proteger a su organización y a sus clientes de las amenazas de ciberseguridad es innegable. Desde ataques de ransomware hasta el robo de datos personales, los piratas informáticos y otros malos actores pueden llegar fácilmente a todo el mundo para dañar una empresa sin levantarse de su silla. Además de la relativa facilidad de tales ataques, explotar las debilidades de la ciberseguridad también puede ser increíblemente lucrativo y rápido. En comparación con, por ejemplo, robar una tarjeta de crédito de la billetera de alguien (que se detecta rápidamente y se bloquea fácilmente), el robo de información personal a través de Internet puede permitir que el ladrón tenga nuevas tarjetas emitidas a su nombre o, en una escala mayor, una el ladrón podría apuntar a una base de datos llena de miles y miles de nombres de clientes e información de tarjetas de crédito.

Las medidas de ciberseguridad abordan las amenazas a los activos de información y los sistemas informáticos en tres áreas: confidencialidad, integridad y disponibilidad. La confidencialidad incluye los métodos por los cuales los activos y sistemas solo están disponibles para personas autorizadas y están protegidos de aquellos sin permiso. La integridad se refiere a la naturaleza completa, precisa y actualizada de los activos y sistemas. Finalmente, la disponibilidad incluye la disponibilidad inmediata de los activos y sistemas necesarios para los usuarios autorizados en cualquier momento que sea necesario.

Establecimiento de una resiliencia: El plan de ciberseguridad comienza, como con cualquier sistema destinado a reducir la amenaza de pérdida o falla, con una evaluación minuciosa del riesgo. Identificar qué medidas deben implementarse y con qué grado de intensidad sentarán las basesbase del sistema que se va a construir encima. Evalúe las amenazas y vulnerabilidades de su organización: pregunte quién, qué, por qué y cómo; escriba preguntas como: "¿Quién puede atacarnos?" "¿A qué apuntarán?" "¿Cómo obtendrán su objetivo?" Las respuestas a estas pueden ayudarlo a comenzar a identificar las debilidades. También es importante recordar que los requisitos regulatorios o contractuales también pueden influir en sus prioridades al identificar el riesgo; asegúrese de conocerlos y tómelos en consideración.

Una vez que se han identificado los riesgos, hay varias formas de responder:

- Al tratar el riesgo, puede implementar una medida (o varias medidas) para reducir la posibilidad o el impacto de dicho riesgo.
- Al terminar el riesgo, elimina el riesgo en la fuente.
- Al transferir el riesgo, transfiere la responsabilidad de dicho riesgo a otra parte, como la subcontratación a un tercero o la contratación de un seguro.
- Al tolerar el riesgo, elige retener el riesgo, quizás porque no hay una forma viable de tratarlo de manera efectiva o porque el riesgo se ha considerado aceptable.

Debido a que no existe una garantía del 100% de que una medida implementada sea efectiva cada vez que aparece una amenaza, un riesgo tratado aún debe considerarse un riesgo activo; no se eliminó, simplemente se hizo menos probable o menos dañino. Una deferencia-El enfoque en profundidad puede ayudar a abordar las "grietas en el escudo" restantes, por así decirlo, ofreciendo una protección en capas más matizada. Idealmente, cada parte de este plan presentará una variedad de desafíos diferentes para que los atacantes los superen, en lugar de que todos dependan del mismo tipo de seguridad. Un plan de seguridad es tan fuerte como su eslabón más débil; encuentre y refuerce este punto, según los tipos de atacante que parezcan más probables, y ayude a mitigar el riesgo.

Además de las tres facetas de la seguridad (confidencialidad, integridad y disponibilidad), es importante tener en cuenta tres factores de defensa que se deben cubrir: personas, procesos y tecnología. Es común que las organizaciones se centren únicamente en implementar tecnología o soluciones de software y descuiden el componente humano de un marco de seguridad. Los programas y el hardware involucrados deben ser implementados y mantenidos por personas; ¡no te olvides de ellos! Igualmente importantes son los procesos seguidos por los humanos que mantienen el marco de seguridad. Los procesos minuciosos y sólidos que están documentados y programados regularmente son cruciales. Finalmente, la tecnología es la más obvia de las tres, incluso si son imperfectas y dependen del factor humano.

La resiliencia también incluye ser capaz de manejar un incidente una vez que ocurre, y en ciberseguridad el primer paso para hacerlo es *Detectar* que se ha producido una infracción en primer lugar. Las medidas detectivescas se dividen en tres categorías:

- La detección previa al incidente puede considerarse una forma de prevención, tomando las precauciones adecuadas antes de que se produzca un ataque. Esto puede incluir análisis de vulnerabilidades o pruebas de penetración.
- La detección en tiempo real se activa cuando las medidas preventivas han fallado y un ataque ha tenido éxito. Las notificaciones automáticas, una alarma que suena en una puerta rota y otras formas de advertencia se incluyen en esta categoría.
- Desafortunadamente, la detección posterior al incidente es común, ya que muchos incidentes se descubren mucho después del hecho. A parte de la falla de seguridad, es importante ser consciente de que se produjo un ataque y fue exitoso, para poder seguir con la limitación de daños.

La respuesta a un ataque completa la resiliencia de una empresa y cubre los métodos elegidos para identificar, contener, erradicar y recuperarse de un ataque. Las lecciones aprendidas de una falla de seguridad cibernética ofrecen una oportunidad para mejorar que es tan valiosa como un sistema de seguridad sólido para comenzar.

Para obtener más información, comuníquese con PJR – llame: **(248) 358-3388** o correo electrónico: **pjr@pjr.com.**