**Consideraciones para la continuidad del negocio**

Anteriormente, aprendiste sobre cómo los equipos de seguridad desarrollan planes de respuesta a incidentes para ayudar a garantizar que exista un proceso preparado y consistente, y pueda responderse rápidamente a los incidentes de seguridad. En esta lectura, explorarás la importancia que tiene la planificación de la continuidad del negocio a la hora de recuperarse de incidentes.

**Planificación de la continuidad del negocio**

Los equipos de seguridad deben estar preparados para minimizar elimpacto que los incidentes de seguridad pueden tener en el desarrollo normal de un negocio. Cuando ocurre un incidente, las organizaciones pueden experimentar interrupciones significativas en la funcionalidad de sus sistemas y servicios, que pueden tener efectos graves, como perjuicios legales, financieros y de reputación. Las organizaciones deben utilizar la planificación de la continuidad del negocio para seguir operando durante cualquier interrupción importante.

Al igual que un plan de respuesta a incidentes, un **plan de continuidad del negocio (BCP)** es un documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa. Un BCP ayuda a las organizaciones a garantizar que las funciones comerciales críticas puedan reanudarse o restaurarse rápidamente cuando ocurre un incidente.

Los analistas de seguridad de nivel inicial no suelen ser responsables del desarrollo y las pruebas de un BCP. Sin embargo, es importante que comprendas cómo los BCP proporcionan a las organizaciones una forma estructurada de responder y recuperarse de los incidentes de seguridad.

**Nota**: Los planes de continuidad del negocio no son lo mismo que los *planes de recuperación ante desastres*. Estos se utilizan para recuperar sistemas de información en respuesta a un hecho grave, que puede ir desde fallas de hardware hasta la destrucción de las instalaciones por un desastre natural, como una inundación.

**Los impactos del ransomware en la continuidad del negocio**

Los impactos de un incidente de seguridad como el ransomware pueden ser devastadores para el funcionamiento de una organización. Los ataques de ransomware dirigidos a infraestructura crítica, como la de salud, pueden tener el potencial de causar interrupciones significativas. Dependiendo de la gravedad del ataque, pueden verse afectadas la accesibilidad, la disponibilidad y la prestación de servicios de salud esenciales. Por ejemplo, el ransomware puede cifrar datos, lo que resulta en la inhabilitación del acceso a los registros médicos y la imposibilidad de que los proveedores de atención médica accedan a los registros de los pacientes. A mayor escala, los incidentes de seguridad que tienen como objetivo los activos, sistemas y redes de infraestructura crítica también pueden comprometer la seguridad nacional y económica, y la salud y seguridad del público. La importancia de los BCP radica en que ayudan a minimizar las interrupciones en las operaciones para que se pueda acceder rápidamente a los servicios esenciales.

**Estrategias de recuperación**

Cuando se produce una interrupción debido a un incidente de seguridad, las organizaciones deben tener algún tipo de plan de recuperación operativo para resolver el problema y poner los sistemas en pleno funcionamiento. Los BCP pueden incluir estrategias para la recuperación que se centran en retomar las operaciones normales. La resiliencia del sitio es un ejemplo de estrategia de recuperación.

**Resiliencia del sitio**

La **resiliencia** es la capacidad de prepararse, responder y recuperarse de las alteraciones. Las organizaciones pueden diseñar sus sistemas para que sean resilientes y puedan continuar prestando servicios a pesar de enfrentar interrupciones. Un ejemplo es la resiliencia del sitio, que se utiliza para garantizar la disponibilidad de redes, centros de datos u otras infraestructuras cuando se produce una interrupción. Hay tres tipos de sitios de recuperación utilizados para la resiliencia del sitio:

* **Sitios calientes (Hot sites)**: Instalaciones completamente operativas que replican el entorno primario de una organización. Los sitios calientes pueden activarse inmediatamente cuando el sitio principal de una organización experimenta fallas o interrupciones.
* **Sitios tibios (Warm sites)**:Instalaciones que contienen una versión completamente actualizada y configurada del sitio caliente. A diferencia de estos, los sitios tibios no están completamente operativos y disponibles para su uso inmediato, pero pueden ponerse en funcionamiento rápidamente cuando se produce una falla o interrupción.
* **Sitios fríos (Cold sites**):Instalaciones de respaldo equipadas con parte de la infraestructura necesaria para operar el sitio de una organización. Cuando se produce una interrupción o falla, los sitios fríos pueden no estar listos para su uso inmediato y tal vez requieran trabajo adicional para poder operar.

**Conclusiones clave**

Los incidentes de seguridad tienen el potencial de interrumpir seriamente el funcionamiento de una empresa. Disponer de los planes correctos es esencial para que las organizaciones puedan seguir funcionando. Los planes de continuidad del negocio ayudan a las organizaciones a comprender el impacto que los incidentes de seguridad graves pueden tener en sus operaciones, y resultan útiles para mitigarlos de manera que las operaciones regulares puedan reanudarse.

Marcar como completo

Me gusta

No me gusta

Informar de un problema