GESTIÓN DE RIESGOS, LA BASE DE TODO EN CIBERSEGURIDAD:

¿Qué es? ¿Para qué y cómo emplearla?

KIPPEO
GET STARTED IN HOLISTIC SECURITY

Introducción

La gestión de riesgos cibernéticos es el proceso de identificación, evaluación y priorización de los riesgos potenciales relacionados con el uso de la tecnología, y la aplicación de medidas para mitigar o eliminar esos mismos. Esto incluye los riesgos relacionados con la violación de datos, los ciberataques, los fallos del sistema de información y otras amenazas a la seguridad e integridad de los sistemas digitales.

En los últimos años han surgido varias tendencias en materia de ciberataques:

1. Ataques de ransomware: Son un tipo de ciberataque en el que el atacante cifra los datos de la víctima y exige un rescate a cambio de la clave de descifrado. Los ataques de ransomware han aumentado significativamente en los últimos años y pueden tener graves consecuencias para las organizaciones, como pérdidas financieras, daños a la reputación y pérdida de confianza de los clientes.

2. Ataques de phishing: Estos ataques implican el uso de correos electrónicos o sitios web falsos para engañar a las víctimas para que revelen información confidencial, como credenciales de inicio de sesión o información financiera. Los ataques de phishing suelen estar muy dirigidos y pueden ser difíciles de detectar.

3. Ataques a la cadena de suministro: Estos ataques tienen como objetivo la cadena de suministro de una organización, normalmente mediante el uso de programas maliciosos que se introducen en la cadena de suministro a través de un proveedor externo. Estos ataques pueden ser particularmente difíciles de detectar y pueden tener graves consecuencias para la organización.

4. Brechas de seguridad en la nube: A medida que más organizaciones trasladan sus operaciones a la nube, se ha producido un aumento de los ataques dirigidos a los sistemas basados en la nube. Estos ataques pueden ser particularmente difíciles de detectar y pueden tener graves consecuencias para la organización.

5. Ataques al Internet de las cosas: El creciente número de dispositivos de Internet de las cosas (IoT) en uso ha provocado un aumento de los ataques dirigidos a estos dispositivos. Estos ataques pueden utilizarse para obtener acceso a la red de una organización o para interrumpir las operaciones.

Una gestión eficaz de los riesgos cibernéticos es esencial para las organizaciones de todos los tamaños, ya que las consecuencias de un incidente cibernético pueden ser graves. Estas consecuencias pueden incluir pérdidas financieras, daños a la reputación, responsabilidades legales y pérdida de confianza de los clientes.

El impacto de un ciberataque en una organización puede ser significativo y tener consecuencias de gran alcance. Según un informe de Cybersecurity Ventures, se espera que el costo de la ciberdelincuencia supere los 10,5 billones de dólares anuales en 2025.

En cuanto al impacto específico de los ciberataques en las organizaciones, algunas estadísticas recientes incluyen:

- El costo medio de una violación de datos para una pequeña o mediana empresa es de 200.000 dólares.
- El costo medio de una violación de datos para una gran organización es de 3,92 millones de dólares.
- El 60% de las pequeñas empresas que sufren un ciberataque abandonan el negocio en un plazo de seis meses.
- Los ciberataques son el tipo de delito de más rápido crecimiento en el mundo.
- Se estima que los ciberataques costaron a las empresas 1,1 billones de dólares en 2019, y se espera que esta cifra se duplique con creces hasta alcanzar los 6 billones de dólares en 2021.

Estas estadísticas demuestran el impacto significativo que los ciberataques pueden tener en las organizaciones, y la importancia de implementar medidas efectivas de gestión de riesgos cibernéticos para protegerse contra estas amenazas.

Para gestionar eficazmente los riesgos cibernéticos, las organizaciones deben adoptar un enfoque integral y proactivo. Esto comienza con la identificación y evaluación de los riesgos potenciales, y el desarrollo de estrategias para mitigar o eliminar esos riesgos.

Una gestión eficaz de los riesgos cibernéticos es esencial para las organizaciones de todos los tamaños, ya que las consecuencias de un incidente cibernético pueden ser graves. Estas consecuencias pueden incluir pérdidas financieras, daños a la reputación, responsabilidades legales y pérdida de confianza de los clientes. Para protegerse contra estos riesgos, las organizaciones deben adoptar un enfoque integral y proactivo de la seguridad.

Algunas de las mejores prácticas para gestionar los riesgos cibernéticos incluyen:

1. Implantar medidas de seguridad sólidas: Esto incluye la implementación de cortafuegos, software antivirus y controles de acceso para protegerse contra los ciberataques. También es importante actualizar periódicamente estas medidas para garantizar su eficacia frente a las amenazas más recientes.

2. Formar a los empleados en las mejores prácticas de ciberseguridad: Los empleados deben recibir formación sobre cómo identificar y evitar posibles amenazas, como los ataques de phishing, y cómo informar de actividades sospechosas.

3. Desarrollar y aplicar un plan de respuesta a incidentes: En caso de incidente cibernético, es esencial contar con un plan para responder rápida y eficazmente. Esto puede incluir la identificación de un equipo responsable de responder al incidente, el establecimiento de un proceso de comunicación con las partes interesadas y la identificación de los recursos y herramientas necesarios para responder al incidente.

4. Supervisar y evaluar periódicamente los sistemas y redes digitales: Las organizaciones deben supervisar regularmente sus sistemas y redes para detectar actividades inusuales o amenazas potenciales, y probar y actualizar periódicamente las medidas de seguridad para garantizar su eficacia.

5. Utilizar contraseñas seguras y aplicar la autenticación de dos factores: Las contraseñas seguras y la autenticación de dos factores pueden ayudar a proteger contra el acceso no autorizado a sistemas y redes.

Mediante la aplicación de estas mejores prácticas, las organizaciones pueden gestionar eficazmente los riesgos cibernéticos y protegerse a sí mismas, a sus clientes y a su reputación de las consecuencias de un incidente cibernético.

Además de las medidas técnicas, las organizaciones también deben contar con políticas y procedimientos para responder a incidentes cibernéticos, como violaciones de datos o ataques. Esto puede incluir disponer de un plan de respuesta a incidentes, y probar y actualizar periódicamente el plan para garantizar su eficacia.

La gestión eficaz de los riesgos cibernéticos también requiere una supervisión y evaluación continuas de los sistemas y redes digitales de la organización. Esto incluye la comprobación y actualización periódica de las medidas de seguridad, así como la supervisión de actividades inusuales o amenazas potenciales.

Existen varias normas internacionales que orientan sobre la gestión de los riesgos cibernéticos, entre ellas:

- ISO/IEC 27001: Esta norma proporciona orientación sobre el establecimiento, la implantación, el mantenimiento y la mejora continua de un sistema de gestión de la seguridad de la información (SGSI). Abarca la gestión de los riesgos para la confidencialidad, integridad y disponibilidad de la información.

- Marco de Ciberseguridad del NIST (CSF): Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), el CSF es un marco basado en el riesgo que proporciona orientación sobre la gestión de los riesgos de ciberseguridad. Ayuda a las organizaciones a identificar, proteger, detectar, responder y recuperarse de los ciberataques.

- COBIT 5: desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), COBIT 5 es un marco que proporciona orientación sobre el gobierno y la gestión de las TI empresariales. Incluye un conjunto de procesos y prácticas que pueden utilizarse para gestionar los ciberriesgos.

- ISO/IEC 27005: Esta norma orienta sobre la gestión de los riesgos para la seguridad de la información. Abarca el proceso de evaluación y tratamiento de riesgos, así como la supervisión y revisión de las actividades de gestión de riesgos.

Siguiendo estas normas internacionales, las organizaciones pueden gestionar eficazmente los ciberriesgos y protegerse de posibles amenazas.

¿Cuánto tiempo se tarda una PyME en realizar una evaluación de riesgos?

El tiempo necesario para llevar a cabo una evaluación de riesgos cibernéticos dependerá del tamaño y la complejidad de la organización, así como de los recursos disponibles para realizar la evaluación. En general, una organización pequeña con un número limitado de activos y sistemas puede ser capaz de completar una evaluación de riesgos cibernéticos en un período de tiempo más corto en comparación con una organización más grande con sistemas y activos más complejos.

Dicho esto, es importante evaluar a fondo todos los riesgos potenciales, en lugar de apresurarse a través del proceso. Una evaluación de riesgos completa y exhaustiva es crucial para gestionar eficazmente los riesgos cibernéticos.

Por término medio, una organización pequeña puede tardar varias semanas o incluso meses en completar una evaluación de riesgos cibernéticos, dependiendo del nivel de detalle y de los recursos disponibles. Los factores que pueden influir en la duración de la evaluación incluyen el número de sistemas y activos que deben evaluarse, la complejidad de la red y los sistemas de la organización, y la disponibilidad de personal para llevar a cabo la evaluación.

En general, la clave es asignar tiempo y recursos suficientes al proceso de evaluación de riesgos para garantizar que todos los riesgos potenciales se identifican y se abordan adecuadamente.

El tiempo que se tarda en realizar una evaluación de riesgos cibernéticos en una gran organización puede variar en función de una serie de factores, como la complejidad de los sistemas y redes digitales de la organización, los recursos disponibles para la evaluación y el nivel de detalle requerido en la evaluación.

¿Cuánto tiempo se tarda un gran organización en realizar una evaluación de riesgos?

En general, es probable que lleve más tiempo completar una evaluación de riesgos

cibernéticos en una organización grande que en una pequeña, debido a la naturaleza más grande y compleja de los sistemas y redes de la organización.

Hay una serie de enfoques que las organizaciones pueden adoptar para acelerar el proceso de completar una evaluación de riesgos cibernéticos. Estos incluyen:

- Utilizar herramientas automatizadas: Hay una serie de herramientas disponibles que pueden automatizar varios aspectos del proceso de evaluación de riesgos, como el escaneo de redes en busca de vulnerabilidades.
- Utilizar una metodología de evaluación de riesgos: Existen varias metodologías de evaluación de riesgos que proporcionan un enfoque estructurado para identificar y evaluar los riesgos. Utilizar una de estas metodologías puede ayudar a garantizar que la evaluación sea exhaustiva y coherente.
- Priorizar los riesgos: No es práctico ni rentable tratar de abordar todos los riesgos potenciales. Al priorizar los riesgos en función de su probabilidad e impacto, las organizaciones pueden centrar sus esfuerzos en los riesgos más críticos.

En general, el tiempo necesario para completar una evaluación de riesgos cibernéticos en una gran organización dependerá de las circunstancias específicas de la organización y del enfoque adoptado para la evaluación.

En conclusión, la gestión del ciberriesgo es un aspecto crítico de las operaciones empresariales modernas. Al identificar y mitigar los riesgos potenciales, las organizaciones pueden protegerse a sí mismas, a sus clientes y a su reputación de las consecuencias de un incidente cibernético. Existen varias prácticas recomendadas que las organizaciones deben seguir a la hora de realizar una evaluación de riesgos cibernéticos:

1. Definir el alcance de la evaluación: Es importante definir claramente el alcance de la evaluación, incluidos los sistemas y redes que se incluirán, los tipos de riesgos que se considerarán y el nivel de detalle requerido.
2. Identificar los activos: Identifique los activos más importantes para la organización, como servidores, bases de datos y datos confidenciales, y evalúe los riesgos para estos activos.
3. Identificar las amenazas potenciales: Considere los tipos de amenazas a los que la organización tiene más probabilidades de enfrentarse, como ciberataques, violaciones de datos o fallos del sistema.
4. Evaluar las vulnerabilidades: Identifique las vulnerabilidades en los sistemas y redes de la organización que podrían ser explotadas por amenazas potenciales.
5. Evaluar el impacto de los riesgos potenciales: Evaluar el impacto potencial de los riesgos identificados, incluidas las consecuencias financieras y de reputación.
6. Desarrollar estrategias de mitigación de riesgos: Desarrollar estrategias para mitigar o eliminar los riesgos identificados, como implementar medidas de seguridad, formar a los empleados en las mejores prácticas de ciberseguridad o desarrollar un plan de respuesta a incidentes.
7. Revisar y actualizar periódicamente la evaluación: Los riesgos cibernéticos evolucionan constantemente, por lo que es importante revisar y actualizar periódicamente la evaluación para garantizar que siga siendo pertinente y eficaz.

Siguiendo estas buenas prácticas, las organizaciones pueden llevar a cabo una evaluación de riesgos cibernéticos exhaustiva y eficaz y desarrollar estrategias efectivas para mitigar o eliminar los riesgos identificados.

Cómo vemos un análisis de riesgos puede prevenir y apoyar a nuestra empresa a detectar sucesos que tengan impacto en la operación, infraestructura y economía, así como, comprender la visión general de la ciberseguridad para otras áreas que no sean exactamente de TI.

Sin embargo, muchas organizaciones aún desconocen que camino tomar para iniciarse en la ciberseguridad, por lo cual existen diferentes partners y aliados que facilitarán el comienzo para mantener optima la seguridad de la información.

En KIPPEO, a través del apoyo de profesionales y consultores, nos enfocamos en proporcionar a las empresas diferentes soluciones y herramientas para facilitar el acceso al mundo de ciberseguridad, apegándonos a las necesidades de cada usuario.

Si aún no conoce el estatus de su ciberdefensa o bien, lo conoce, pero no sabe por dónde empezar, nosotros le apoyamos a conocerlo y seremos su partner en ciberseguridad durante este recorrido con las mejores prácticas ya mencionadas anteriormente: Análisis de vulnerabilidades, pruebas de penetración, plan de continuidad de negocio, protección a su correo electrónico, CISO as a Service, entre otros.

¡No dude en ponerse en contacto con nosotros!

GESTIÓN DE RIESGOS, LA BASE DE TODO EN CIBERSEGURIDAD:

¿Qué es? ¿Para qué y cómo emplearla?

Síguenos!

www.kippeo.com

KIPPEO

GET STARTED IN HOLISTIC SECURITY