unisys

Resiliencia cibernética empresarial

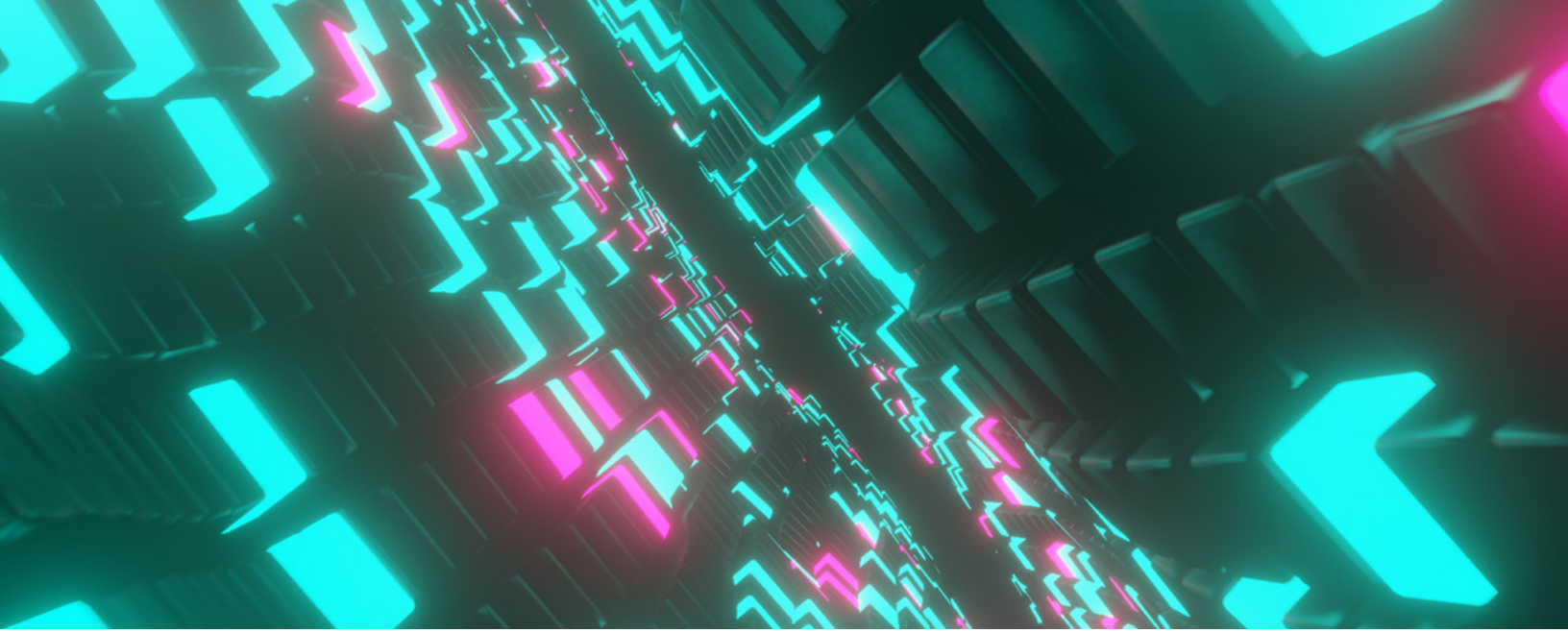
Una guía para acelerar la recuperación frente a los peores escenarios

Contenido

El valor de la ciberresiliencia empresarial

En el metro de Londres, los letreros con la leyenda *Mind the gap* advierten a los pasajeros que deben tener cuidado al pasar de la plataforma de la estación a una puerta del tren o viceversa. Esta fase de transición puede ser igual de útil a la hora de considerar las brechas de ciberseguridad y las posibles vulnerabilidades en sus estrategias de ciberresiliencia. La longevidad de la empresa se puede medir en la capacidad de su organización para hacer frente a tormentas imprevistas. La ciberresiliencia es crucial para adaptarse y responder eficazmente a las interrupciones, los riesgos y los eventos inesperados que podrían afectar las operaciones.

La resiliencia le permite mantener la continuidad, minimizar el tiempo de inactividad, recuperarse rápidamente de ciberataques y desastres, y mantener los procesos empresariales críticos funcionando sin problemas. Invertir en medidas de resiliencia puede ayudarle a proteger su reputación, generando confianza con empleados, clientes y socios, mientras demuestra su compromiso con la sostenibilidad y el crecimiento a largo plazo. Tomar estos tres pasos puede ser el inicio en el camino hacia la resiliencia.



Pasos hacia una mayor resiliencia

01 Evalúe su entorno cibernético

El camino hacia la ciberresiliencia comienza con la evaluación de su entorno operativo. Una evaluación le ofrece una comprensión exhaustiva de los riesgos de seguridad y los conocimientos necesarios para desarrollar una estrategia integral que fortalezca su organización frente a las ciberamenazas.

- Mapee sus activos críticos, sistemas, dependencias y todos los demás componentes de su entorno cibernético.
- Identifique amenazas de seguridad, riesgos clave y posibles vulnerabilidades de seguridad en su infraestructura digital.
- Evalúe la eficacia de las medidas de seguridad de su organización, identificando brechas o debilidades en sus defensas, incluidas aquellas que ya han provocado un compromiso no detectado o que hayan sido potencialmente explotadas.
- Utilice esta inteligencia para priorizar las áreas de mejora para abordarlas más adelante como parte de su plan estratégico.
- Integre evaluaciones continuas en su estrategia de ciberseguridad para detectar señales de alerta antes de que se conviertan en problemas.

Descubrimiento de la superficie de ataque

El descubrimiento de la superficie de ataque implica explorar todas las vías que un atacante podría utilizar para infiltrarse en sus sistemas y red. Esto incluye la detección de riesgos de seguridad y casos de TI en la sombra (shadow IT), es decir, cuando los empleados adoptan tecnología sin obtener primero la autorización de TI. Detectar a tiempo la TI en la sombra puede reducir la exposición de su organización a nuevos riesgos de seguridad y reducir el desperdicio de recursos.

02 Desarrollar una estrategia de resiliencia

Utilice los conocimientos obtenidos de la evaluación para construir una base para la resiliencia. Una estrategia eficaz implica políticas, controles y procedimientos sólidos en línea con la tolerancia al riesgo y los objetivos empresariales de su organización. La consolidación de su estrategia facilita la implementación de medidas de mitigación de riesgos, el fortalecimiento de su posición de resiliencia, la preparación para un escenario de seguridad en el peor de los casos y la estabilización de las operaciones empresariales si se llegara a producir un ataque.

Ingredientes para el éxito de la estrategia

Al desarrollar un plan integral de ciberresiliencia para proteger su organización contra las ciberamenazas, priorice la incorporación de varios componentes vitales.

- **Preparación y prevención** que reconoce que la resiliencia comienza mucho antes de que se produzca un ataque
- **Supervisión y respuesta a incidentes** que proporciona visibilidad sobre posibles ataques y minimiza el impacto en las operaciones
- **Copia de seguridad y recuperación** que restaura los datos y la funcionalidad del sistema después de un incidente
- **Continuidad del negocio** tras un ciberataque o una interrupción
- **Formación de los empleados** para educarlos sobre las mejores prácticas de ciberseguridad y fomentar una cultura consciente de la seguridad
- **Cumplimiento normativo** para alinear su estrategia de ciberresiliencia con los requisitos legales y normativos relevantes
- **Mejora continua** de las capacidades de resiliencia a través de una supervisión continua

03 Establecer fundamentos de ciberseguridad

Después de trazar su estrategia, es hora de transformar sus medidas de seguridad existentes reevaluando los protocolos, tecnologías y prácticas de seguridad actuales para abordar las amenazas y vulnerabilidades emergentes. Esto le permite proteger mejor sus activos, datos y operaciones de los ciberriesgos y las interrupciones. Otro imperativo de ciberseguridad es reforzar la preparación y las capacidades de respuesta de su organización con protocolos de respuesta a incidentes, planes de continuidad del negocio y estrategias de recuperación ante desastres.

Soluciones básicas para la resiliencia

- **Detección y respuesta gestionadas:**

  Identifique rápidamente los incidentes de ciberseguridad y minimice su impacto en las operaciones y en la postura de seguridad. La supervisión permanente y las capacidades de respuesta inmediata ayudan a proteger a su organización de forma proactiva contra ciberamenazas y ataques.

- **Detección de la superficie de ataque:**

  Obtenga una visibilidad continua de los activos expuestos, lo que permite una mitigación proactiva del riesgo, una respuesta más rápida a los incidentes y defensas ágiles a medida que el entorno y las amenazas evolucionan.

- **Ciberresiliencia, integración e innovación continua:**

  Integre a la perfección las prácticas de ciberseguridad en las operaciones, la gestión de riesgos y las estrategias de negocio de su organización. Las ciberamenazas son dinámicas, por lo que es crucial avanzar en las medidas de ciberseguridad para mantenerse a la vanguardia frente a un panorama de amenazas en constante evolución.

- **Recuperación cibernética:**

  Mantenga la continuidad del negocio y limite el tiempo en el que su organización queda sin activos críticos como el acceso a los datos y los sistemas de comunicación después de un ciberataque. Los principios y prácticas de recuperación ante desastres, como los protocolos de copia de seguridad, sirven como base para los esfuerzos de recuperación cibernética, a la vez que requieren medidas adicionales de resiliencia y protección, como el aislamiento de los sistemas afectados.

- **Recuperación ante desastres:**

  Recupérese rápidamente ante desastres nacionales, como inundaciones y terremotos, y eventos tecnológicos, como fallos de servidores, para minimizar el tiempo de inactividad y mantener los sistemas operativos. Los sólidos planes de recuperación ante desastres mantienen su negocio funcionando sin problemas después de eventos inesperados.

- **Respuesta a incidentes de ciberseguridad:**

  Contenga los ciberataques para evitar que se propaguen y causen daños adicionales a los sistemas y datos de su organización. La respuesta a incidentes protege sus datos y restablece la producción de los sistemas afectados.

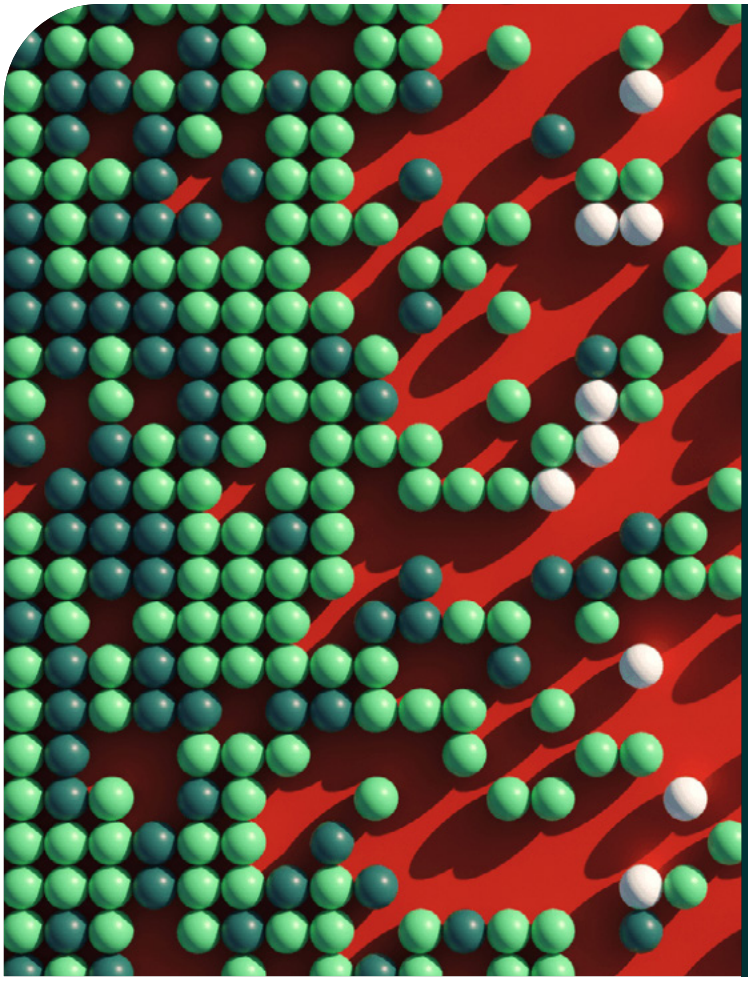
Ventajas de la ciberresiliencia empresarial

Adoptar un enfoque resiliente, especialmente cuando prioriza la prevención de riesgos, ofrece varias ventajas que refuerzan la ciberseguridad de su organización. Estos beneficios contribuyen a crear un marco sólido para la resiliencia que facilita la superación de posibles desafíos.

- **Identificación de riesgos:** Comprenda los riesgos de su organización para adaptar sus estrategias de resiliencia a la hora de mitigar eficazmente posibles vulnerabilidades.
- **Gestión de riesgos:** Abordar y mitigar los riesgos estratégicamente para la resiliencia y la continuidad durante las interrupciones.
- **Prevención de riesgos:** Reduzca la probabilidad de ataques exitosos que puedan afectar a las operaciones empresariales.
- **Mayor flexibilidad:** Gane agilidad a la hora de evolucionar con las circunstancias cambiantes y adapte su enfoque para abordar los riesgos emergentes y mitigar las amenazas, con un impacto mínimo en las operaciones.
- **Preparación mejorada:** Prepare a su organización para diversos escenarios, incluidas las ciberamenazas y los fallos del sistema, con herramientas y estrategias para responder eficazmente a las interrupciones.

Cómo puede ayudar Unisys

Los expertos en ciberseguridad de Unisys pueden guiar sus esfuerzos para mejorar la resiliencia empresarial en todas las etapas de su recorrido de seguridad, desde la evaluación inicial hasta la gestión continua. Nuestros servicios integrales le permiten desarrollar y mantener sus capacidades de resiliencia.



Soporte integral:

Benefíciese de la experiencia en la identificación de riesgos, la determinación de herramientas para mitigarlos, la creación de infraestructuras resilientes y la gestión eficaz de las operaciones.

Soluciones a medida:

Obtenga soluciones adaptadas a las necesidades específicas de su organización, la infraestructura de TI actual y futura, los desafíos únicos y los requisitos empresariales..

Monitorización continua::

Obtenga visibilidad sobre posibles amenazas o interrupciones en las operaciones empresariales con la supervisión continua de los sistemas.

.

¿Podría su ciberresiliencia ser más fuerte?

Visite unisys.com o póngase en contacto con nosotros para programar una consulta con nuestros expertos hoy mismo.

unisys

unisys.com

08/26 7094-12721