Cyber Article

Interrupción de CrowdStrike IT y Ciberdelincuencia

Los empleados y equipos que siguen afectados por la interrupción son un objetivo prioritario para los ciberdelincuentes. He aquí cómo mitigar los riesgos…

La caída de CrowdStrike en julio de 2024 dejó a innumerables usuarios de TI paralizados con una «pantalla azul de la muerte». Aunque la interrupción provocó el caos en todas partes, desde los escritorios de las oficinas hasta la facturación en los aeropuertos, también dejó a las organizaciones expuestas a un mayor riesgo por parte de los ciberdelincuentes.

Aunque CrowdStrike ha publicado desde entonces una solución, es crucial gestionar el riesgo inmediato y creciente de phishing y ciberactividad maliciosa revisando y reforzando cada línea de ciberdefensa.

Los ciberdelincuentes siguen aprovechando el phishing y otros medios para engañar a los usuarios y distribuir contenido malicioso bajo la apariencia de ofrecer asistencia técnica.

Tanto los sistemas informáticos como las personas son vulnerables a la hora de prevenir o controlar un ciberataque, por lo que conviene comprobar la eficacia de estas líneas de defensa principales.
Y, aunque se haya restablecido el acceso para el 100% de los empleados, los ciberdelincuentes también pueden hacerse pasar por equipos de asistencia técnica de TI haciendo referencia a números de ticket de TI y compartiendo URL maliciosas.

Línea de Defensa No. 1: Las personas

Sus empleados son su primera línea de defensa contra los ciberdelincuentes. Hágales conscientes de la creciente amenaza del phishing e indíqueles que estén atentos a cualquier actividad sospechosa. Esto podría adoptar la forma de correos electrónicos inesperados, correos electrónicos con nombres de dominio desconocidos o falsos, o incluso el uso de comunicaciones a través de otros canales, como las redes sociales (por ejemplo, LinkedIn).

Realizar un ejercicio de phishing simulado con los empleados le ayudará a evaluar hasta qué punto su plantilla gestiona el riesgo. Pondrá de relieve el nivel de defensa de sus empleados, así como las lagunas de conocimientos o comportamientos que pueden abordarse con formación adicional.

Con una plantilla en alerta máxima, así como con el refuerzo de los mensajes que muchos empleados habrán aprendido a través de los módulos de formación, aumentará la posibilidad de detectar la amenaza al primer intento: a través de su personal.

INTERNAL USE ONLY

Línea de Defensa No. 2: Tecnología

Sin embargo, las personas cometen errores. Las soluciones tecnológicas de detección adecuadas ayudarán a redirigir el contenido malicioso lejos de sus empleados, o incluso a capturar la amenaza después de que un empleado haga clic por error en un enlace malicioso.

Las soluciones de detección deben estar presentes tanto en el tráfico del correo -para filtrar los mensajes antes de que lleguen a los buzones de los usuarios- como en el punto final del usuario, cuando ya es casi demasiado tarde y se ha ejecutado un archivo malicioso. Incluso con esta tecnología instalada, es importante comprobar periódicamente su eficacia. Esto es especialmente aconsejable teniendo en cuenta el aumento de las amenazas a la ciberseguridad tras la interrupción de CrowdStrike. Una auditoría técnica puede identificar cualquier vulnerabilidad existente en la tecnología de detección, lo que permite el llamado «endurecimiento tecnológico», es decir, un proceso que revisa la configuración y reduce o mitiga estas vulnerabilidades.

Un ejercicio de pruebas de penetración, que es otro método para identificar vulnerabilidades en su sistema de ciberseguridad, también puede validar si existen controles técnicos adecuados y eficientes.

Este ejercicio de prueba puede incluso ampliarse para las organizaciones que se benefician de una supervisión continua de las ciberamenazas y las brechas a través de un Centro de Operaciones de Seguridad (SOC). De este modo se evaluarán las capacidades de supervisión, alerta y bloqueo de su SOC.

Interrupción de CrowdStrike: Lecciones aprendidas

Si este incidente ha sido perturbador para su organización, se le presenta una oportunidad de oro para reforzar su ciberseguridad. Considere cómo podría mejorar sus procedimientos de preparación ante crisis y sus planes de continuidad de negocio para gestionar incidentes importantes en el futuro. Aunque la interrupción de CrowdStrike no fue causada por un ciberataque, sirve como recordatorio de la importancia de la resiliencia empresarial desde arriba.

Además de tomar las precauciones de ciberseguridad mencionadas anteriormente, a continuación puede encontrar una serie de áreas que puede desear considerar para mitigar o reducir su exposición y/o el impacto de un evento futuro similar:

1) Revisar los procedimientos existentes de prevención, respuesta y apoyo en caso de interrupciones a gran escala.

2) Revise y actualice los procedimientos de inactividad para operaciones clave. Revise en consecuencia los planes de comunicación de crisis, los procesos de respuesta a incidentes y los planes de gestión de continuidad de negocio/recuperación de desastres informáticos.

3) Asegurarse de que los empleados clave de la organización disponen de las competencias, la formación y los recursos necesarios en relación con los procedimientos de respuesta y recuperación y participan en las pruebas de los sistemas de la empresa.

4) Colaborar con colegas uniéndose a redes de inteligencia sobre amenazas y participando en grupos de inteligencia sobre amenazas específicos del sector para compartir conocimientos y mantenerse informado sobre las amenazas emergentes y las mejores prácticas.

INTERNAL USE ONLY

Ciberresiliencia en Zurich Resilience Solutions

Estamos dispuestos en ayudar a su empresa a prepararse y responder a eventos que pueden causar una interrupción significativa del negocio y pérdidas financieras, como interrupciones y ciberataques.

Nuestro equipo global de Ciberresiliencia puede ayudarle a establecer, u optimizar, sus planes de gestión de crisis y continuidad de negocio auditando los procesos y tecnologías existentes, así como proporcionando soluciones de monitorización 24/7 (SOC) para defenderse de los ciberataques.

Si desea más información sobre cómo podemos ayudar a su organización a alcanzar la madurez cibernética, póngase en contacto con nosotros en: cyber.resilience@zurich.com.

Para más información sobre nuestras soluciones y experiencia, visite nuestra página web Zurich Resilience Solutions | Zurich Aseguradora Mexicana

INTERNAL USE ONLY

Zurich Insurance Company Ltd

Mythenquai 2, CH-8002 Zurich – Switzerland

www.zurich.com

The information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its subsidiaries (hereinafter 'Zurich') as to their accuracy or completeness.

Some of the information contained herein may be time sensitive. Thus, you should consult the most recent referenced material.

Information in this document relates to risk engineering / risk services and is intended as a general description of certain types of services available to qualified customers. It is not intended as, and does not give, an overview of insurance coverages, services or programs and it does not revise or amend any existing insurance contract, offer, quote or other documentation.

Zurich and its employees do not assume any liability of any kind whatsoever, resulting from the use, or reliance upon any information, material or procedure contained herein. Zurich and its employees do not guarantee particular outcomes and there may be conditions on your premises or within your organization which may not be apparent to us. You are in the best position to understand your business and your organization and to take steps to minimize risk, and we wish to assist you by providing the information and tools to assess your changing risk environment.

In the United States of America, risk services are available to qualified customers through Zurich Services Corporation and in Canada through Zurich Risk Services as also in other countries worldwide, risk engineering services are provided by different legal entities affiliated with the Zurich Insurance Company Ltd as per the respective country authorization and licensing requirements.

©2017 Zurich Insurance Company Ltd

e1a413404eed56ea02d64d33c65d5873f229d4283452a3dfa24dcc7a21d82fac