7 PASOS PARA REALIZAR PRUEBAS EXHAUSTIVAS DE SISTEMAS CIBERNÉTICOS

Adoptar un enfoque proactivo para la seguridad cibernética es mucho menos costoso que lidiar con las consecuencias de una violación de seguridad cibernética. De acuerdo con Cybersecurity Ventures, además del daño a la reputación que podría resultar de una violación, se estima que el delito cibernético cueste un total de $ 6 billones en todo el mundo para 2021. Evaluar su riesgo cibernético es misión crítica, va mucho más allá de una auditoría de cumplimiento. ¿Qué pasos puede seguir para realizar pruebas exhaustivas a los sistemas y así detectar riesgos cibernéticos?

1. REALIZAR UNA EVALUACIÓN INTEGRAL DE RIESGOS

Revise las funciones de su negocio que contienen los activos más valiosos, y esto no solo incluye la información confidencial y de negocio de los clientes. Considere sus operaciones y dónde la interrupción del negocio sería perjudicial. Por ejemplo, no todos los piratas informáticos tienen una motivación financiera, es posible que quieran detener su cadena de suministro para limitar la productividad. Una vez que haya establecido todas las áreas de riesgos, desde las financieras hasta las operativas y de reputación, puede comenzar a abordarlas una por una según sus objetivos comerciales.

2. EJECUTE UNA PRUEBA DE PENETRACIÓN

¿Sabe cómo está expuesta su infraestructura de red y los sistemas de información? Para salvaguardar sus sistemas cibernéticos, debe encontrar la forma de entrar del pirata informático. Si un pirata informático puede localizar un medio de entrada o evitar las características de seguridad, todo su sistema es vulnerable. Simule ataques contra su red para descubrir debilidades desconocidas, tanto internas como externas. Sin embargo, tenga en cuenta que esta prueba finaliza una vez que se encuentra un punto de entrada, dejando abierta la posibilidad de otras exposiciones desconocidas.

3. EJECUTE UN ANÁLISIS DE VULNERABILIDAD

En un banco, la bóveda puede ser el premio principal, pero no es la única consideración. Debe ser estratégico con respecto a la colocación de guardias de seguridad, vigilancia de salida y protección de cajones bancarios. Un análisis de vulnerabilidad es crítico ya que le permite enfocarse en una visión completa de los sistemas de su organización y probar cada punto de acceso potencial y debilidad. Luego, identifique el parche correcto.

4. SOLICITE UNA EVALUACIÓN DE ATAQUE CIBERNÉTICO DEL SISTEMA DE CORREO ELECTRÓNICO

Dos de los ciberataques más notables en la historia reciente, WannaCry y NotPetya, se lanzaron por correo electrónico malicioso. Dado el crecimiento dramático de los ataques cibernéticos que tienen lugar a través del correo electrónico, es esencial una evaluación de diagnóstico avanzada y profunda del sistema de correo electrónico de una organización. Estas pruebas separadas pueden detectar amenazas de malware que pueden pasar desapercibidos.

5. IMPLEMENTE UNA CAMPAÑA DE SPEAR-PHISHING

¿Alguna vez recibió un correo electrónico frenético de su jefe a altas horas de la noche? Ahora imagine que un pirata informático está realmente detrás de ese correo electrónico, haciéndose pasar por su jefe. Los ataques de spear-phishing son intentos altamente selectivos para asegurar la información confidencial y han demostrado ser efectivos. Es vital evaluar el nivel de conciencia cibernética de los empleados de su organización en todos los niveles para reducir las instancias de vulnerabilidades humanas.

6. EXAMINE LA RELACIÓN CON SUS PROVEEDORES

Incluso si los sistemas de su organización están protegidos, todos sus proveedores externos, desde socios comerciales y conexiones B2B hasta proveedores de mantenimiento y servicios de catering, también son puntos de acceso. Las relaciones con terceros deben verse como una extensión de su negocio y mantenerse con los mismos estándares. Asegúrese de que cada proveedor tenga el nivel adecuado de acceso a sus datos y que se examinen sus políticas de privacidad de datos y prácticas de cumplimiento.

7. EVALUAR, REANUDAR Y REPETIR

Los riesgos cibernéticos cambian y maduran tan rápido como lo hace la tecnología. Para mantener los sistemas seguros, es fundamental que evalúe continuamente los controles de ciberseguridad y realice estas pruebas anualmente, y este no es un proyecto estrictamente para el CIO o la función de TI. Proteger su negocio de una catástrofe es una responsabilidad compartida. Depende de la comunicación adecuada de las estrategias y planes de seguridad cibernética, y de una comprensión profunda por parte del Comité la administración y los líderes empresariales responsables de la supervisión.

Las pruebas exhaustivas de sistemas Cibernéticos son una tarea sustancial. ¿Tiene los recursos para hacerlo usted mismo? Una certificación de Controles de Sistema y Organización (SOC), por sus siglas en inglés, puede ayudarlo a encontrar y cerrar brechas en controles de seguridad cibernética y agregar credibilidad a su programa de gestión de riesgos.

CONTACTO

RAMSÉS INZUNZA
Socio Nacional de Consultoría de Riesgos
ramses.inzunza@bdomexico.com

OSCAR JARAMILLO
Gerente Senior de Consultoría en Ciberseguridad y Transformación Digital
oscar.jaramillo@bdomexico.com