Publicado en Madrid el 12/12/2023

Ocho formas en las que el factor humano ayuda a proteger a las empresas

Check Point Software destaca la importancia de formar e instruir al personal de las empresas en materias de ciberseguridad

Ante un panorama cada vez más acechado por las ciberamenazas, Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, considera que la tecnología juega un papel fundamental en la protección de las empresas. Sin embargo, muchas veces el factor humano se pasa por alto. Por muy sofisticados que sean los protocolos de actuación, si el personal de la empresa no tiene las herramientas necesarias para prevenir un ciberataque, todas las medidas anteriores son insuficientes.

La mayoría de los incidentes de seguridad no son solo el resultado de técnicas de piratería sofisticadas, sino que a menudo se ven favorecidos por errores humanos: caer en correos electrónicos de phishing, tener contraseñas débiles o filtrar datos de manera accidental, son algunos de los errores más frecuentes entre el personal de una empresa.

Invertir en técnicas de seguridad centradas en la formación de los empleados es esencial para evitar pérdidas financieras graves, daños en la reputación de la empresa y la pérdida de la confianza de los clientes. Ante esta situación, Check Point Software propone ocho recomendaciones para construir una defensa más sólida contra las amenazas cibernéticas basada en el factor humano:

Formación: las amenazas cibernéticas evolucionan constantemente. Los empleados deben estar formados para reaccionar ante tales amenazas y actualizar periódicamente sus conocimientos para reducir las posibilidades de un ciberataque.

Prevención contra los ataques phishing: esta es una de las formas de engaño más habituales. Los empleados son víctimas a menudo de estos correos electrónicos o mensajes que parecen auténticos y que tratan de robar información confidencial o instalar un malware. Los empleados deben estar prevenidos ante este tipo de ataques y tener en cuenta que pueden presentarse también a través de mensajes al teléfono, no solo en el correo electrónico.

Gestión de credenciales: la gestión de contraseñas es fundamental para garantizar la protección de la empresa. Se recomienda:

Adoptar un modelo de confianza cero.
Inicio de sesión único (SSO).
Autenticación de múltiples factores (MFA).
Política de bloqueo de cuenta tras varios intentos fallidos.
Cambios regulares en las contraseñas.

4. Sistemas de gestión de cambios: otra sugerencia es implementar un sistema de gestión de cambios en el que, para realizar cualquier modificación en el sistema haya que pasar por diferentes niveles de aprobación. Diversos integrantes del equipo tendrán que evaluar estos cambios, de este modo, se minimizan los errores y los riesgos que acarrean.

5. Responsabilidad: es importante mantener un diálogo abierto con los empleados sobre la importancia de la ciberseguridad y que haya comunicación sobre los riesgos potenciales de la empresa.

6. Gestión de riesgo de proveedores: a la hora de realizar colaboraciones, se debe asegurar que estas empresas también cumplen con los estándares de seguridad.

7. Marco legal: es necesario revisar el cumplimiento de las leyes de protección de datos y los estándares de la industria, así como obtener contratos legales para proteger la información sensible.

8. Plan de respuesta a incidentes: tener un plan de respuesta a incidentes es una medida eficaz e imprescindible para cualquier empresa. La vulnerabilidad ante una ciberamenaza es inevitable, por ello lo mejor es construir un plan de respuesta consistente y estar preparados para actuar lo antes posible.

"Gran parte de las empresas han sufrido ciberataques porque no han preparado al personal ni le han informado sobre los riesgos que existen. Es impresionante ver cómo empresas que han construido un sistema de protección cibernética muy sólido, son víctimas de estas amenazas por errores que cometen los empleados. La ciberseguridad se trata realmente de personas, procesos y tecnología", explica Eusebio Nieva, director técnico de Check Point Software para España y Portugal. "Las empresas tienen que formar a su equipo en materia de ciberseguridad para prevenir estos errores y evitar así graves perjuicios en su economía y su reputación".

Datos de contacto:
Everythink PR
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Software Ciberseguridad Recursos humanos Digital