10 errores frecuentes de la seguridad digital de tu empresa y cómo evitarlos.

Los **ciberdelincuentes también están de vuelta por Navidad**, listos para traer carbón y malwares a su empresa. A continuación, le **contamos 10 errores comunes** y cómo evitarlos estas Navidades:

1. Facilitar las claves de apoderados a personal administrativo no autorizado.

Uno de los errores más comunes, es dar acceso a claves de apoderados a personal administrativo. Potencialmente, esto puede resultar en accesos no autorizados.

¿Cómo actuar?

Para evitar cualquier acceso no autorizado, las empresas deben contar con políticas estrictas de control de acceso, almacenando las claves de forma centralizada y controlando el acceso a las mismas siguiendo el principio del mínimo privilegio. Además, se recomienda utilizar autenticación multifactor (MFA) para accesos sensibles, garantizando que solo personas autorizadas puedan acceder.

2. Compartir credenciales por correo electrónico.

Al compartir credenciales por correo electrónico, como por ejemplo nombres de usuario y contraseñas, se expone información crítica a posibles ataques. Los atacantes pueden interceptar las comunicaciones y obtener visibilidad de todo lo que compartimos en ellas.

¿Cómo actuar?

Divida la información, enviando el nombre de usuario y la contraseña por diferentes canales de comunicación (correo electrónico, llamada, SMS, etc.). Esto reduce el riesgo de que ambas partes de las credenciales sean interceptadas simultáneamente por un ciberdelincuente. Adicionalmente, es conveniente que la contraseña proporcionada sea temporal, debiendo ser cambiada por el destinatario inmediatamente después del primer uso. Y, siempre que sea posible, se deben aplicar técnicas de cifrado de extremo a extremo en las comunicaciones.

3. Almacenar tarjetas de coordenadas de forma insegura.

Guardar tarjetas de coordenadas en medios no seguros, como fotografías en el móvil, o realizando fotocopias de ellas, aumenta el riesgo de robo de información.

¿Cómo actuar?

Para minimizar los riesgos de revelación y el uso indebido de esta información, evite hacer duplicados o extraer datos de su tarjeta de coordenadas. Mantenga siempre estas tarjetas en un lugar seguro y acceda a ellas solo cuando sea absolutamente necesario.

4. No verificar la cuenta bancaria de proveedores.

Pagar facturas sin verificar regularmente la cuenta corriente de los proveedores, puede derivar en fraudes tales como el ingreso de pagos en cuentas bancarias fraudulentas/que pertenezcan a los atacantes.

¿Cómo actuar?

Para evitar estos fraudes, es imprescindible que las empresas dispongan de procedimientos de verificación obligatoria para cualquier cambio en la cuenta bancaria de proveedores, incluyendo en los mismos la confirmación directa de los datos con una fuente confiable.

5. No confirmar cambios de cuenta bancaria por teléfono.

Es importante confirmar telefónicamente, con el interlocutor adecuado, cualquier cambio de cuenta bancaria. No hacerlo puede permitir pagos fraudulentos, ya que los ciberdelincuentes podrían haber suplantado la identidad del destinatario legítimo.

¿Cómo actuar?

Para protegerse de estos ataques, las empresas deben tener implantado un protocolo de validación por múltiples canales (por ejemplo, llamadas telefónicas, videoconferencias) antes de aceptar cambios en la información de pago.

6. Aceptar órdenes por correo sin validación previa (Fraude del CEO).

Ejecutar órdenes recibidas por correo sin verificarlas puede materializar posibles ataques de suplantación de identidad, tales como phishing o spear phishing, donde los atacantes se hacen pasar por una persona o entidad legítima para engañar a la víctima.

Estos atacantes suelen suplantar la identidad de un alto cargo, quien haciendo uso de su autoridad, traslada urgencia, rapidez y discreción en la operación sin hacer preguntas y saltándose los procedimientos habituales.

¿Cómo actuar?

Para evitarlo, las organizaciones deben contar con una política de verificación por múltiples canales para cualquier orden de acción financiera o de datos críticos recibida por correo, incluyendo mecanismos de reporte de cualquier petición que intente saltarse los cauces establecidos en dicha política, independientemente de quién sea el peticionario.

7. Usar contraseñas débiles o repetidas.

Las contraseñas poco complejas facilitan el éxito de ataques de fuerza bruta, permitiendo a los ciberdelincuentes adivinarlas. Además, la repetición de contraseñas permite a los atacantes acceder a múltiples cuentas si una credencial es comprometida, exponiendo a las empresas a brechas de seguridad y robo de información.

¿Cómo actuar?

Para mitigar estos riesgos, es esencial usar contraseñas fuertes y únicas para cada cuenta. Las empresas deben disponer de políticas robustas de control de acceso, preferiblemente combinadas con autenticación multifactor (MFA) para agregar una capa adicional de seguridad.

8. No actualizar software ni aplicar parches de seguridad.

No mantener los sistemas actualizados deja a las empresas vulnerables a ataques, ya que los ciberdelincuentes pueden explotar fallos conocidos para realizar ataques de diversa índole.

¿Cómo actuar?

Es imprescindible que las empresas implementen políticas de gestión de actualizaciones que incluyan la instalación periódica de parches de seguridad críticos. Además, es fundamental la realización de pruebas regulares de vulnerabilidades, con el objetivo de identificarlas y subsanarlas cuanto antes.

9. No realizar copias de seguridad regulares ni probar su restauración.

La ausencia de backups, o no verificar las copias de seguridad que se realizan, expone a la empresa a perder información crucial en caso de un ataque de ransomware o un fallo del sistema.

¿Cómo actuar?

Para evitar este riesgo, las empresas debe contar con políticas y mecanismos de backup periódicos. Estos backup deben verificarse mediante pruebas periódicas de restauración para asegurar la integridad de los datos respaldados.

10. No formar en seguridad digital a los empleados.

El personal sin formación /concienciación es más vulnerable a ataques de phishing y malware al carecer de los conocimientos necesarios para identificar y evitar amenazas.

¿Cómo actuar?

Las organizaciones deben contemplar en sus programas formativos la capacitación y concienciación continua en materia de seguridad digital, con acciones que expliquen cómo reconocer amenazas y enfaticen la importancia de su identificación.

En Bankinter trabajamos continuamente por su seguridad, si tiene dudas ante cualquier situación, llame a nuestro **Servicio de Atención al Fraude: 900 81 00 62**.

Además, seguimos la Directiva Europea PSD2 relativa a los servicios de pago, por eso para determinadas operaciones, le **solicitaremos una clave que enviaremos por SMS a su teléfono móvil**.

Si desea comprobar que su número de móvil está correctamente registrado, entre en **bankinter.com/empresas, y acceda a su Área de Gestión: Usuarios Perfiles Firma de Seguridad**.

bankinter.