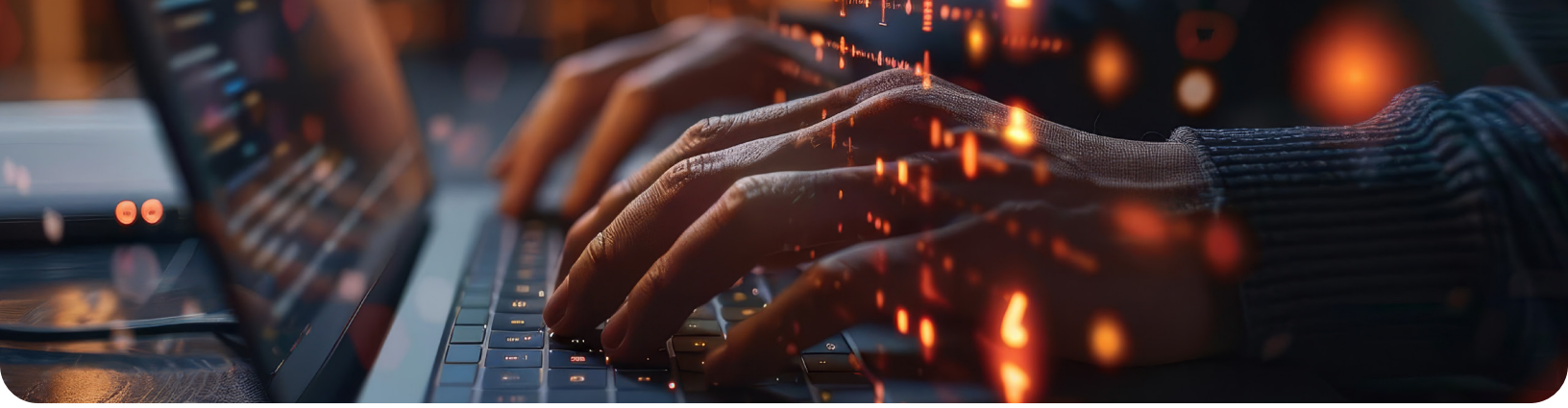
No caiga en estas ciberamenazas

Una guía completa

Los ciberdelincuentes son cada vez más sofisticados y las empresas de todos los tamaños corren riesgos. Ya sea por medio de correos electrónicos de phishing diseñados para robar credenciales de inicio de sesión, ataques de ransomware que bloquean el acceso a los datos o vulnerabilidades en dispositivos conectados, las ciberamenazas tienen consecuencias devastadoras. Comprender estas amenazas y tomar medidas proactivas para la protección de su empresa puede ayudar a evitar costosas violaciones de seguridad, tiempos de inactividad y daños a la reputación. Esto es lo que necesita saber.



1. Ataques de phishing por IA

Los ciberdelincuentes utilizan la inteligencia artificial (IA) para crear correos electrónicos de phishing muy convincentes, lo que dificulta más que nunca detectar los mensajes fraudulentos. Estos ataques engañan a los empleados para que revelen información confidencial, como contraseñas o detalles financieros, o descarguen malware en sus sistemas.

Los riesgos

- Violaciones de datos: El robo de credenciales puede dar lugar a accesos no autorizados a datos confidenciales de la empresa.
- Pérdidas económicas: Las estafas de phishing pueden dar lugar a transacciones fraudulentas, fraude con transferencias bancarias o infecciones de ransomware.
- Daño ala reputación: Una violación de datos puede erosionar la confianza de los clientes y partners.

¿Sabía usted que?

Los ataques de correo electrónico aumentaron 293 %, ya que los ciberdelincuentes siguieron utilizando herramientas con IA, como WormGPT y FraudGPT.

(Fuente: Informe de Ciberamenazas de Acronis, Primer Semestre de 2024)

Cómo proteger su empresa

- Capacite a sus empleados: Entrene regularmente a su equipo para que identifique intentos de phishing, verifique los remitentes de los correos electrónicos y denuncie los mensajes sospechosos.
- Implemente filtros de seguridad del correo electrónico: Las herramientas avanzadas de filtrado ayudan a detectar y bloquear los correos de phishing antes de que lleguen a las bandejas de entrada.
- Tenga un plan de respuesta ante incidentes: Prepárese con una estrategia clara para responder a los ataques de phishing y mitigar los daños rápidamente.
- Utilice la autenticación multifactor (MFA): Al añadir un nivel de seguridad adicional, se dificulta a los atacantes el acceso a las cuentas, incluso si las contraseñas se ven comprometidas.

2.
Ataques de cadena de suministro

Un ataque de cadena de suministro ocurre cuando los ciberdelincuentes eligen como destino a un proveedor o suministrador de terceros para obtener accesibilidad a su empresa. Si uno de sus proveedores de servicios se ve comprometido, sus datos, operaciones y sistemas operativos podrían correr peligro.

Los riesgos

- Violaciones de datos: Un proveedor comprometido podría exponer datos confidenciales de clientes o de la empresa.
- Interrupciones operativas: Los ciberataques a proveedores pueden provocar tiempos de inactividad e interrupciones comerciales.
- Impacto legal y financiero: Las empresas podrían enfrentar multas o acciones legales si los datos de los clientes se ven comprometidos debido a una débil seguridad de su cadena de suministro.

¿Sabía usted que?

Se espera que el costo de los ataques al software de la cadena de suministro aumente de USD$46,000 millones en 2023 a USD$138,000 millones en 2031.

(Fuente: Gartner, junio de 2024)

Recomendaciones para su empresa

- Evalúe a sus proveedores: Asegúrese de que los proveedores externos sigan protocolos de ciberseguridad estrictos antes de concederles acceso a sus sistemas.
- Limite el acceso: Conceda a los proveedores solo el nivel mínimo de accesibilidad necesario para realizar su trabajo y revise periódicamente los permisos.
- Incluya cláusulas de ciberseguridad en los contratos: Exija a los proveedores que mantengan altos estándares de seguridad.
- Realice auditorías de seguridad de manera regular: Evalúe la postura de seguridad de su cadena de suministro y corrija las vulnerabilidades.

3.
Ransomware como servicio (RaaS)

Los ataques de ransomware están en aumento y los ciberdelincuentes están facilitando que cualquiera, incluso personas con poca experiencia en tecnología, pueda lanzar ataques devastadores. Este modelo, conocido como Ransomware como Servicio (RaaS), permite a los atacantes rentar herramientas de ransomware y obtener ganancias por los pagos de rescate.

Los riesgos

- Pérdida de datos: Los delincuentes cifran sus archivos y exigen un pago para liberarlos.
- Tiempo de inactividad operativo: Las empresas pueden verse obligadas a detener sus operaciones, lo que puede provocar pérdidas financieras.
- Sin garantía de recuperación: incluso si se paga el rescate, no hay garantía de que se vayan a restaurar los datos.

¿Sabía usted que?

Se reportaron 1,048 casos públicos de ransomware en el primer trimestre de 2024, 23 % más que el año anterior.

(Fuente: Informe de Ciberamenazas de Acronis, Primer Semestre de 2024)

Cómo proteger su empresa

- Realice copias de seguridad de sus datos con regularidad: Almacene las copias de seguridad en ubicaciones externas seguras y pruebe procedimientos de recuperación.
- Capacite a sus empleados: Capacite a su equipo para reconocer las amenazas de ransomware y evitar hacer clic en enlaces o archivos adjuntos sospechosos.
- Mantenga el software actualizado: Aplique parches a las vulnerabilidades de los sistemas operativos, las aplicaciones y los complementos.
- Utilice la segmentación de conexión a redes virtuales: Restrinja la propagación del malware separando los sistemas críticos de otras áreas de la red.

4. Vulnerabilidades del Internet de las cosas (IoT)

Los dispositivos conectados, como las cámaras inteligentes, los termostatos y los sensores industriales, mejoran la eficiencia, pero también introducen riesgos de seguridad. Muchos dispositivos del IoT tienen configuraciones de seguridad débiles, lo que los convierte en objetivos fáciles para los hackers.

Los riesgos

- Violaciones de datos: Los hackers pueden aprovechar las vulnerabilidades del IoT para acceder a sus sistemas.
- Redes comprometidas: Los dispositivos comprometidos se pueden utilizar para lanzar ciberataques a gran escala.
- Riesgos de seguridad física: Los delincuentes pueden manipular cerraduras inteligentes o sistemas de seguridad.

¿Sabía usted que?

En 2022 se produjeron 112 millones de ciberataques a dispositivos IoT, contra 32 millones de 2018.

(Fuente: EC-Council, julio de 2024)

Cómo proteger su empresa

- Segmente su red: Mantenga los dispositivos IoT en una red separada de sus sistemas empresariales críticos.
- Actualice el firmware de los dispositivos: Instale parches de seguridad y actualizaciones con regularidad.
- Supervise la actividad: Configure alertas para detectar comportamientos anormales en los dispositivos conectados.
- Utilice contraseñas seguras: Cambie las credenciales predeterminadas y utilice contraseñas únicas y complejas para cada dispositivo.

5.
Amenazas internas

No todas las ciberamenazas provienen de hackers externos, sino que algunas se originan dentro de la propia organización. Ya sea un empleado descontento que busca venganza o uno que hace clic accidentalmente en un enlace de phishing, las amenazas internas son tan peligrosas como los ataques externos.

Los riesgos

- Fugas de datos: La información confidencial de la empresa puede quedar expuesta o ser robada.
- Sistema comprometido: Los empleados con acceso a sistemas críticos pueden causar daños intencionales o no intencionales.
- Daño a la reputación: Una violación de la seguridad causada por un empleado puede dañar la confianza y credibilidad de su empresa.

¿Sabía usted que?

Casi 25 % de las amenazas internas tienen un fin malicioso, como sabotaje, robo de datos y fraude.

(Fuente: Forbes, octubre de 2024)

Cómo proteger su empresa

- Proporcione capacitación de seguridad periódica: Prepare a sus empleados en las mejores prácticas de ciberseguridad.
- Limite el acceso a los datos confidenciales: Solo dé acceso en caso necesario.
- Supervise la actividad interna: Utilice herramientas de seguridad para detectar comportamientos anormales.

Proteja a su empresa de las ciberamenazas

La ciberseguridad es un desafío creciente, pero no tiene por qué enfrentarlo solo. Nuestros expertos le ayudan a evaluar los riesgos, implementar defensas sólidas y brindar protección a su empresa contra amenazas en constante evolución. Póngase en contacto con nosotros hoy mismo para hablar de cómo podemos ayudarle a proteger la seguridad de su empresa:

Cubical
Correo: soporte@cubical.ec
Teléfono: +59325142100
http://www.cubical.ec