KERBEROS

MANAGING GENERAL AGENCY

Guía de respuesta a incidentes

KERBEROS
MANAGING GENERAL AGENCY

¿Está su organización preparada para responder a un incidente cibernético?

Preparación, prevención y resiliencia frente al riesgo cibernético

Los ataques cibernéticos continúan aumentando en frecuencia y sofisticación en organizaciones de todos los tamaños y sectores.

En muchos casos, los incidentes comienzan con algo aparentemente pequeño:

un correo de phishing, una contraseña comprometida o un sistema que no fue actualizado a tiempo.

Sin embargo, cuando los atacantes logran acceso, las consecuencias pueden escalar rápidamente:

- Interrupción de operaciones.
- Robo de información sensible.
- Fraude financiero.
- Daños reputacionales.
- Notificaciones regulatorias.

Desde la experiencia de suscripción y monitoreo de riesgos de **Kerberos Re**, así como las prácticas observadas en equipos de respuesta a incidentes, existe un consenso claro:

Las organizaciones que mejor manejan un incidente cibernético comparten dos características fundamentales:

1. Controles sólidos de ciberseguridad para prevenir ataques.
2. Un plan de respuesta a incidentes claramente definido.

Este reporte presenta diez capacidades clave que los equipos de respuesta a incidentes consideran esenciales antes de que ocurra un ataque.

Parte I

Controles de seguridad que previenen la mayoría de los ataques

1. La identidad como nuevo perímetro de seguridad

Una gran proporción de incidentes cibernéticos actuales comienza con **credenciales comprometidas**.

Los atacantes ya no necesitan "hackear" sistemas complejos; con frecuencia simplemente **inician sesión utilizando contraseñas robadas**.

Las organizaciones deben implementar controles como:

- Autenticación multifactor (MFA) en todos los sistemas críticos.
- Eliminación de cuentas administrativas compartidas.
- Monitoreo de accesos y actividad sospechosa.
- Políticas sólidas de gestión de identidades.

La protección de identidades se ha convertido en uno de los controles más efectivos para prevenir accesos no autorizados.

2. Superar el modelo tradicional de perímetro

Durante muchos años, las organizaciones confiaron principalmente en:

- Firewalls.
- Redes privadas virtuales (VPN).
- Controles perimetrales.

Sin embargo, los atacantes ahora explotan con frecuencia vulnerabilidades en estos mismos dispositivos.

Las arquitecturas modernas de seguridad están migrando hacia modelos como:

- **Zero Trust Network Access (ZTNA).**
- **Secure Access Service Edge (SASE).**

Estos enfoques priorizan la verificación continua de identidades y dispositivos, en lugar de confiar únicamente en la seguridad de la red.

3. Reducir el riesgo asociado a servidores de archivos locales

Los servidores de archivos tradicionales continúan siendo un objetivo frecuente en ataques de ransomware.

Una vez que un atacante obtiene acceso a la red interna, puede cifrar grandes volúmenes de información almacenada en unidades compartidas, paralizando las operaciones de la organización.

Muchas empresas están reduciendo este riesgo migrando hacia plataformas de almacenamiento en la nube administradas corporativamente, tales como:

- Microsoft SharePoint.
- Google Workspace.
- Plataformas seguras de colaboración en la nube.

Estas soluciones ofrecen mayor control de accesos, auditoría de actividad y opciones de recuperación.

4. Gestión continua de parches de seguridad

Los atacantes suelen aprovechar vulnerabilidades para las cuales **ya existen actualizaciones disponibles**.

Sin embargo, muchas organizaciones continúan operando sistemas:

- Desactualizados.
- Sin soporte del fabricante.
- Sin parches de seguridad aplicados oportunamente.

Implementar un programa estructurado de **gestión de vulnerabilidades y actualizaciones** es una de las formas más eficaces de reducir la exposición al riesgo cibernético.

5. Copias de seguridad confiables como última línea de defensa

En incidentes de ransomware, la capacidad de restaurar información desde copias de seguridad puede determinar la rapidez de recuperación de una organización.

Las copias de seguridad deben cumplir con ciertas características clave:

- Almacenamiento fuera de la red principal.
- Protección contra modificaciones (backups inmutables).
- Pruebas periódicas de restauración.

Las organizaciones que cuentan con respaldos confiables suelen tener mayor capacidad para recuperar sus sistemas sin depender de pagos de rescate.

Parte II

Preparación para responder a un incidente cibernético

Incluso con controles de seguridad robustos, ningún sistema es completamente inmune a incidentes.

Por ello, la preparación para responder eficazmente a un evento cibernético es fundamental.

6. Definir roles y responsabilidades de respuesta

Durante un incidente, las decisiones deben tomarse con rapidez.

Las organizaciones deben identificar con anticipación a los responsables clave del proceso de respuesta, incluyendo:

- Líder de respuesta a incidentes.
- Responsables de tecnología o seguridad.
- Asesores legales o de cumplimiento.
- Responsables de comunicaciones.
- Proveedores de servicios claves.

Una estructura clara de liderazgo reduce la confusión, facilita la coordinación y hace eficiente los tiempos de respuesta.

7. Establecer canales seguros de comunicación

En algunos incidentes, los sistemas de correo electrónico o colaboración pueden verse comprometidos.

Por esta razón, es recomendable establecer **canales alternos de comunicación y redundacia**, tales como:

- Plataformas seguras de mensajería.
- Listas de contactos de emergencia.
- Protocolos de comunicación fuera de línea.

Estos mecanismos deben probarse periódicamente para asegurar su funcionamiento. Las buenas prácticas en estándares de continuidad de negocio sugieren que sea mínimo una vez al año.

8. Clasificar incidentes según su severidad

No todos los eventos de seguridad requieren la misma respuesta.

Las organizaciones pueden establecer niveles de severidad, por ejemplo:

Bajo: Intentos de phishing detectados.
Medio: Detección de malware en dispositivos.
Alto: Ransomware o compromiso de sistemas críticos.

La clasificación permite escalar incidentes de forma proporcional y eficiente.

9. Documentar procedimientos de respuesta

Un plan de respuesta a incidentes debe incluir procedimientos claros para escenarios comunes, tales como:

- Ataques de phishing.
- Infecciones de malware.
- Ransomware.
- Fuga o pérdida de información.
- Ataques de denegación de servicio.

Asimismo, es recomendable mantener un inventario actualizado de las herramientas de seguridad disponibles para detección, investigación y contención de incidentes.

10. Identificar socios externos de respuesta

En muchos casos, responder a un incidente cibernético requiere apoyo externo especializado.

Entre los proveedores que pueden participar se encuentran:

- Proveedores de tecnología de servicios homólogos.
- Firmas de análisis forense digital.
- Asesores legales especializados en incidentes.
- Consultores de comunicación de crisis.
- Aseguradoras de riesgo cibernético.

Mantener actualizada la información de contacto y los protocolos de escalamiento permite acelerar la respuesta cuando ocurre un incidente.

Construyendo resiliencia cibernética

La resiliencia frente al riesgo cibernético no depende únicamente de evitar ataques.

También implica contar con las capacidades necesarias para:

- Detectar incidentes rápidamente.
- Contener amenazas.
- Recuperar operaciones de forma eficiente.

Las organizaciones que combinan **controles sólidos de seguridad con una preparación adecuada de respuesta** tienden a experimentar:

- Menores pérdidas financieras.
- Menor impacto operativo.
- Recuperación más rápida.

Sobre Kerberos Re

Kerberos Re es una agencia de suscripción especializada en riesgos de **Cyber y Technology E&O** en América Latina.

Además de capacidad de reaseguro, apoyamos a aseguradoras y corredores mediante:

- Análisis de riesgo cibernético.
- Monitoreo continuo de exposición digital.
- Conocimiento de suscripción especializado.
- Educación y concientización sobre riesgos cibernéticos.

Nuestro objetivo es contribuir al fortalecimiento de la **resiliencia cibernética en la región**.

KERBEROS

MANAGING GENERAL AGENCY