NEXTVISION
Ciberseguridad Inteligente

RANSOMWARE

¿Tu organización está preparada para enfrentarse a esta amenaza?

nextvision.com

Te decimos cómo actuar en cada fase para no sufrir ante un ataque

PREVENÍ

- Mantené tu **antimalware** actualizado con tecnología Machine Learning y activá el IPS de tu solución.
- Tené un **Firewall** activo con reglas y políticas de seguridad.
- Instalá **tecnología Antispam** que te permita bloquear correos sospechosos y archivos adjuntos ejecutables.
- Usá un **filtro web** para evitar los sitios comprometidos.
- Adoptá **políticas de grupo (GPO)** para controlar la ejecución de programas.
- Mantené al día la instalación de **parches de seguridad** de los programas que usás para evitar la explotación de vulnerabilidades.
- Aplicá **restricción de cuentas y derechos administrativos**.
- Implementá un sistema de prevención de intrusiones **(IPS)** .

¡Educá! La mejor prevención es concientizar a tus empleados en el uso prudente de Internet.

DETECTÁ

- Implementá Tecnología **Sandbox** para explotar posibles vulnerabilidades de programas en un ambiente aislado.
- Usá un sistema de detección de intrusiones **(IDS)** para estar alerta ante actividades sospechosas en tu red.
- Integrá Tecnologías de **Análisis de Comportamiento** para detectar procesos anómalos en tiempo real.
- Usá la **correlación de eventos** para tener un contexto más amplio de las actividades en la red y poder responder mejor ante posibles ataques.

SI SE ACTIVÓ UN ATAQUE...

RESPONDÉ DE INMEDIATO

- **Consultá el Plan de Contingencia (si existiera en la organización)**
- **Aislá la amenaza**
  - Remové el Ransomware con las nuevas firmas de tu Antimalware actualizado.
    - ¡Ojo! No vas a poder desencriptar los archivos infectados.
  - Recuperá los archivos secuestrados con tu Backup: te recomendamos tener un soporte físico para tu backup, ya que los respaldos en la nube pueden ser afectados ante un ataque.

SI SE ACTIVÓ UN ATAQUE...

COMUNICATE CON EXPERTOS EN CIBERSEGURIDAD

- Evaluá el riesgo de propagación junto con ellos.
- Enviáles la nota de rescate recibida y un ejemplo de archivo encriptado (de ser posible)

¡NO PAGUES EL RESCATE!

No existen garantías de que podrás recuperar tus datos y estás alimentando organizaciones cibercriminales.

DESPUÉS DEL ATAQUE ...

ASEGURÁ LA CONTINUIDAD DE LA OPERACIÓN

- Garantizá siempre el acceso remoto a los sistemas.
- Contá con **Backup confiable**
  - Hacé verificaciones periódicas.
  - **Duplicá tu Backup** y tu alojamiento de **cintas en sitios externos**.
- Chequeá que el ambiente productivo esté protegido contra amenazas similares.
- **Mantené actualizada la documentación de:**
  - Red
  - Servicios de infraestructura
  - Políticas de autenticación
  - Servicios de seguridad
  - Plan de Contingencia y procedimientos

¡El Ransomware no solo infecta los endpoints!

Todos los dispositivos pueden ser afectados:

- Tablets
- Celulares
- Servidores
- Máquinas virtuales
- Dispositivos con firmwares
- IOT

TENÉ EN CUENTA

- El 97% de los ataques se pueden evitar con controles de seguridad estándar (Fuente: Verizon)
- Un 43% de las víctimas de Ransomware son organizaciones (Fuente: Symantec)
- El Email es el primer vector de ataque (Fuente: Kaspersky)
- Solo el 37% de las empresas reconoce tener un plan de respuesta ante un ataque informático (Fuente: Informe PwC 2017)

La mejor manera de empoderar tu organización ante las ciberamenazas es la:

Ciber Resiliencia

Una organización ciber resiliente es capaz de adaptarse y responder ante las amenazas. Administra los riesgos, puede recuperarse de forma ágil y mantener la operación en caso de haber sufrido un ataque.

NEXTVISION

Ciberseguridad Inteligente

AYUDAMOS A GESTIONAR LOS RIESGOS DE CIBERATAQUES DE MANERA INTELIGENTE

El 97% de los ataques son controlables con una buena administración de las herramientas tecnológicas y educación de los usuarios.

Erradicamos la improvisación, priorizando correctamente los activos a proteger para mantener la continuidad del negocio.

PROMOVEMOS UNA CULTURA CIBERSEGURA

Ayudamos a transformar los hábitos de toda la organización con programas integrales, para que todos los colaboradores cuiden la información crítica y activos digitales del negocio.