CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

10th anniversary EUROPEAN CYBER SECURITY MONTH

PREVENCIÓN Y RESPUESTA PARA ATAQUES DE RANSOMWARE

En este documento, encontrará un protocolo para prevenir y responder a los ataques de ransomware y tener su empresa preparada para estas amenazas cibernéticas.

GENERALITAT VALENCIANA
Conselleria de Hacienda y Modelo Económico

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
UNIÓN EUROPEA

Actuación susceptible de ser cofinanciada por la Unión Europea a través del Programa Operativo del Fondo Europeo de Desarrollo Regional (FEDER) de la Comunitat Valenciana 2014-2020

PREVENCIÓN

Prevenir un ataque de ransomware

1. Dispositivos de software

- Supervise que todos los usuarios inicien sesión y trabajen desde una VPN.
- Asegúrese de tener un firewall instalado y funcionando activamente.
- Su organización debe aplicar actualizaciones y medidas de protección de endpoint. También se pueden combinar con listas blancas, bloqueo de ejecutables en tiempo real, etc.
- Cree un sistema antispam/antiphishing dedicado, ya sea mediante software o utilizando los dispositivos de hardware dedicados.
- El procedimiento de parches dentro de su organización debe ser muy disciplinado y las actualizaciones deben aplicarse a todas las aplicaciones y al sistema operativo, tan pronto como se detecten las vulnerabilidades y salga un nuevo parche.
- Utilice técnicas de seguridad de correo electrónico de vanguardia como DNSSEC, DANE, SPF, DKIM.

2. Soluciones de copia

- Implemente una solución de copia de seguridad sofisticada para los datos de su organización, ya sea basada en software o basada en hardware, o incluso una combinación de ambas.
- Realice pruebas periódicas tanto de sus funciones de recuperación (cuando se trata de su solución de copia de seguridad) como de sus datos en general. Todos los datos hasta varios meses atrás deben probarse regularmente para garantizar que no se vean comprometidos desde adentro al mismo tiempo que ocurre el ataque.
- Verifique si su solución de copia de seguridad cubre todos sus datos, para asegurarse de que todos se guarden y se pueda acceder a ellos en caso de que ocurra lo peor.
- También es importante que sus datos respaldados sean fácilmente accesibles en su forma de respaldo, y que sus datos estén seguros en general. Siga el principio 3-2-1: tenga tres copias de seguridad diferentes, en dos tipos diferentes de medios y mantenga una copia de seguridad fuera del sitio.

3. Métodos de prevención de robos

- Aproveche los registros del sistema para realizar un seguimiento de los movimientos de datos.
- Implemente tecnologías de encriptación de datos para sus datos en general.
- Adquiera y utilice amplias herramientas de DLP (prevención de fuga de datos).
- No olvide analizar el tráfico de su red, para buscar movimientos de datos inusuales dentro del sistema.
- Utilice el método de permisos mínimos para proteger sus bases de datos, carpetas y archivos singulares (lo que significa que no otorgue a sus usuarios ningún permiso aparte de los que necesitan para hacer su trabajo correctamente).

4. Conocimiento de los usuarios

- Simule regularmente ataques de phishing para educar a sus usuarios sobre el curso de acción a seguir, así como para probar sus propios sistemas.
- Invierta en capacitación de concienciación sobre seguridad para sus usuarios, para que sepan cómo buscar aplicaciones sospechosas y no descargarlas/ejecutarlas.
- Establezca una línea de informes y un flujo de trabajo claros y fáciles de seguir para informar sobre incidentes sospechosos. ¡Haga que sus usuarios lo sepan!

RESPUESTA

Responder a un ataque de ransomware.

1. Desconecte la fuente del ransomware

- Su primer paso siempre debe ser limitar la escala del ataque tanto como sea posible, lo que significa que debe:
    - Desenchufar todas las computadoras afectadas de la red.
    - Apagar todos los métodos inalámbricos de transmisión de datos, incluidos Bluetooth, Wi-Fi, NFC, etc.
    - Identificar todos los dispositivos que hayan sido comprometidos.

2. Determinar la escala del ataque

- Inmediatamente después de intentar limitar el alcance del ataque, es esencial averiguar la escala del daño hasta el momento, lo que significa buscar signos de encriptación inusual dentro de diferentes ubicaciones de almacenamiento, como:
    - Unidades de disco duro.
    - Ubicaciones de almacenamiento basadas en la nube (OneDrive, DropBox, Google Drive, etc.).
    - Unidades asignadas o compartidas.
    - Diferentes dispositivos de almacenamiento USB, como unidades USB, cámaras/teléfonos conectados, etc.

Diversos dispositivos de almacenamiento en red. Llame a las agencias locales de ley/policía/CERT. En algunos casos, esto puede incluso ser un requisito legal. Además, el análisis forense necesario a partir de este momento probablemente estará por encima de lo que incluso su equipo de administración puede hacer.

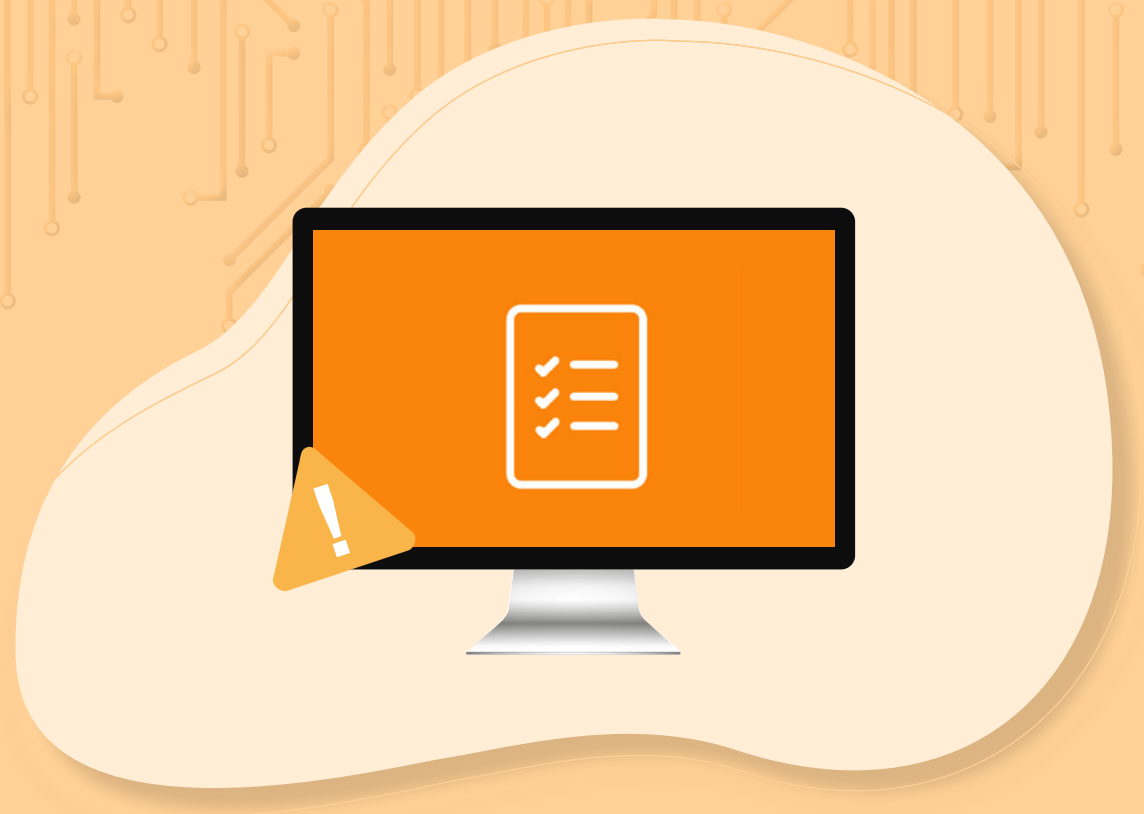
3. Averigüe si alguno de sus datos ha sido robado

- Existen diferentes métodos para hacerlo, que incluyen:
    - Por lo general, una de las indicaciones más obvias de robo de datos es algún tipo de notificación de los atacantes cibernéticos de que sus datos han sido robados.
    - Archivos inusualmente grandes con formato de archivo (.zip, .7z, etc.) que contienen datos confidenciales transmitidos a través de su red.
    - Los registros y los informes del software DLP pueden ayudar a encontrar signos de fugas de datos en alguna parte.

Es posible que pueda encontrar el malware o las herramientas que se usaron para la infección.

CHECKLIST

Qué revisar en caso de sufrir un ataque de ransomware en su organización:



Checklist

1. Restaure sus archivos desde una copia de seguridad

- Asegúrese de que se elimine el vector de ataque inicial para que no vuelva a ser atacado.
- Localice sus copias de seguridad y asegúrese de que contienen todos los archivos.
- Verifique la integridad de sus copias de seguridad y busque signos de corrupción.
- También se recomienda buscar instantáneas (si es posible) y versiones anteriores de sus archivos (si se trata de almacenamiento en la nube).
- Restaure sus archivos respaldados.
- Descubra el vector de infección y cómo cerrarlo.

2. Si está intentando descifrar sus archivos

Esto se puede intentar principalmente en casos específicos cuando es posible determinar el tipo de ransomware y hay un descifrador disponible para esa cepa específica.

- Para descifrar sus archivos, en caso de haber localizado un descifrador, solo tiene que conectar todos los medios de almacenamiento que se han visto afectados por el ransomware.
- Descubra el vector de infección y cómo cerrarlo.

3. Si no hace nada con respecto al ransomware

- Es posible que desee considerar hacer una copia de seguridad de sus archivos cifrados y no eliminarlos, por si más adelante hubiera un desencriptador para esta cepa específica.

CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana

10th anniversary EUROPEAN CYBER SECURITY MONTH

GENERALITAT VALENCIANA
Conselleria de Hacienda y Modelo Económico

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional
UNIÓN EUROPEA
Una manera de hacer Europa

Actuación susceptible de ser cofinanciada por la Unión Europea a través del Programa Operativo del Fondo Europeo de Desarrollo Regional (FEDER) de la Comunitat Valenciana 2014-2020