25 DE ABRIL DE 2024

SOLUCIONS DE CIBERRESILIENCIA

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

1. ¿Qué se podría haber hecho para haberlo detectado? Busca una herramienta real de detección para cada incidente indicando una pequeña descripción de sus funciones. 2

Infección por Ransomware. 2

Fuga de Información. 2

2. ¿Cómo se podría haber evitado? Indica al menos 3 medidas de seguridad que se podrían haber implantado para evitar cada uno de ellos. 2

Infección por Ransomware. 2

Fuga de Información. 2

3. ¿Que medidas de contención se pueden aplicar? Indica al menos 1 medida de contención para cada incidente 3

Infección por Ransomware. 3

Fuga de Información. 3

4. ¿Qué respuesta ciberresiliente se debe establecer para permitir la continuidad del negocio si vuelve a producirse? Establece una serie de pasos/medidas (plan de respuesta) para poder seguir trabajando si se vuelve a producir el mismo incidente para cada uno de los tipos de incidentes seleccionados. 3

Infección por Ransomware. 3

Fuga de Información. 3

1. ¿Qué se podría haber hecho para haberlo detectado? Busca una herramienta real de detección para cada incidente indicando una pequeña descripción de sus funciones.

Infección por Ransomware.

Utilizar soluciones de seguridad para endpoints como Crowdstrike Falcon.

Esta herramienta utiliza inteligencia artificial para detectar comportamientos inusuales en el dispositivo final que puedan indicar la presencia de ransomware.

Fuga de Información.

El uso de sistemas de prevención de pérdida de datos como Elasticsearch.

Estas herramientas monitorean y analizan el tráfico de la red y el almacenamiento de datos para detectar patrones que puedan indicar la fuga de información confidencial.

2. ¿Cómo se podría haber evitado? Indica al menos 3 medidas de seguridad que se podrían haber implantado para evitar cada uno de ellos.

Infección por Ransomware.

- **Configurando Firewalls y sistemas de detección de intrusiones (IDS/IPS),** para bloquear el tráfico malicioso conocido y prevenir la descarga de malware.
- Implementar **filtros de correo electrónico** para bloquear correos maliciosos y archivos adjuntos sospechosos que puedan contener ransomware.
- Mantener el software y los **sistemas operativos actualizados** con los últimos parches de seguridad para mitigar las vulnerabilidades explotadas por el ransomware.

Fuga de Información.

- Implementar **políticas de acceso y privilegios** para restringir el acceso. Así limitar el riesgo de fuga de información.
- **Encriptar datos confidenciales**, tanto en reposo como en tránsito.

- Realizar **auditorías periódicas de acceso** para identificar actividades inusuales o sospechosas que puedan indicar una posible fuga de información.

3. ¿Que medidas de contención se pueden aplicar? Indica al menos 1 medida de contención para cada incidente

Infección por Ransomware.

- Desconectar el dispositivo infectado de la red para evitar la propagación a otros sistemas.

Fuga de Información.

- Bloquear el acceso a la información comprometida y tomar medidas para recuperar o eliminar los datos filtrados.

4. ¿Qué respuesta ciberresiliente se debe establecer para permitir la continuidad del negocio si vuelve a producirse? Establece una serie de pasos/medidas (plan de respuesta) para poder seguir trabajando si se vuelve a producir el mismo incidente para cada uno de los tipos de incidentes seleccionados.

Infección por Ransomware.

- **Respuesta inmediata**: Desconectar de la red el dispositivo infectado y notificar al equipo de seguridad del incidente.
- **Aislamiento y análisis**: Analizar la naturaleza y el alcance de la infección para determinar si se trata de un ataque aislado o si se ha extendido a otros sistemas.
- **Restaurar desde copia de seguridad**: Restaurar datos afectados a partir de copias de seguridad limpias y seguras para restaurar la funcionalidad normal del sistema.

Fuga de Información.

- **Identificación de la fuente**: Determinar cómo ocurrió la filtración de información y qué datos se vieron comprometidos.

- **Prevención y recuperación:** Bloquear el acceso a datos comprometidos y tomar medidas para restaurar o eliminar la información divulgada.
- **Notificación y mitigación**: Notificar a las partes afectadas sobre la violación de información y tomar medidas para mitigar cualquier daño potencial, como proporcionar servicios de monitoreo de crédito o cambiar la contraseña.