**Compromiso por ransomware**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Descripción del incidente**](#_g59i8ewd3ed3) **2**

[**3. Planificación**](#_vo0jrlgaxvu6) **2**

[**4. Detección del incidente y valoración**](#_td2jbwbw5lgz) **3**

[**5. Respuesta**](#_p6wuquv52hvw) **3**

[**6. Lecciones aprendidas**](#_a08u2ws55tu3) **3**

# **2. Descripción del incidente**

Se trata de un incidente producido por ransomware, éste, cifra datos esenciales o bloquea a los usuarios el acceso a sus dispositivos hasta que paguen un rescate al atacante.

El ransomware o secuestro de datos, exige un pago o servicio tras impedir a las víctimas el acceso a sus archivos. Hoy por hoy, es uno de los tipos de ciberataque más destructivos provocando a sus víctimas pérdidas económicas, pérdida de datos confidenciales

o propiedad intelectual, posible deterioro de la reputación, interrupción de las operaciones, disminución de la productividad, coacción o extorsión.

La mejor forma de protegernos ante un ransomware es evitar que penetre en el entorno.

Existen diferentes tipos de ransomware, siendo estos: Locker ransomware, Scareware, Crypto ransomware, etc…

# **3. Planificación**

El ransomware se introduce como infección secundaria cuando la seguridad de un sistema ya se ha vulnerado mediante diferentes tipos de malware. Por ello debemos centrarnos en la prevención y la detección.

* Hacer copias de seguridad de los datos más importantes y almacenarlas en un módulo diferente de los sistemas de archivos principales.
* Contar con software especializado, actualizado, seguro y de calidad.
* Formar y concienciar a los empleados..
* Separar los módulos de red para limitar la propagación..

# **4. Detección del incidente y valoración**

Usualmente podemos identificar que estamos siendo víctimas de un ataque ransomware ya que los datos de los discos se encuentran cifrados o bien por los distintos sistemas o tecnologías de detección y monitorización que posea la empresa.

# **5. Respuesta**

Lo más importante tras sufrir un incidente de ransomware es, evitar por todos los medios que se infecten más dispositivos o que se propague a diferentes sectores de la empresa. Es conveniente bloquear estos equipos de la red y desconectarlos de su suministro eléctrico.

Lo siguiente es restaurar el funcionamiento de la empresa a través de copias de seguridad almacenadas o equipos de reemplazo ya configurados y preparados para continuar con la actividad productiva, minimizando así las pérdidas.

# **6. Lecciones aprendidas**

Debemos analizar si la respuesta al incidente ha sido ágil y proporcionada

Analizadas todas las cuestiones concluimos abordando todas aquellas propuestas de mejora o cambios a realizar para que el incidente no vuelva a repetirse y de hacerlo seamos capaces de reaccionar de forma más eficaz.

Referente a las lecciones aprendidas podemos decir con certeza que lo más importante es evitar brechas de seguridad, poseemos diferentes métodos para conseguirlo, podemos resumirlos en:

1. Limitar el acceso a la información.
2. Contraseñas seguras y dinámicas o implementar doble factor de autenticación.
3. Proteger el correo electrónico.
4. Realizar copias de seguridad y borrados seguros.
5. Almacenamiento modular en la nube, en Red y local.
6. Contratar servicios de seguridad integral y mantener las actualizaciones al día.
7. Monitorizar las conexiones.