Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Se parte de la suposición en la que ostentáis el puesto de responsable de Seguridad de la Información en un centro hospitalario de referencia para una comarca.

Este centro dispone de una infraestructura tecnológica actualizada y operativa, de modo que todo el trabajo se realiza mediante equipamiento informático, dispone de **distintos servidores de base de datos, electrónica de red, servidores de dominio, equipos UTM, servidores de antivirus centralizados**, etc.

A pesar de todo, el centro es **víctima de un incidente de seguridad de tipo ransomware** que se ha introducido mediante **una memoria usb de un usuario** "descuidado". **La actuación de este ciberataque es similar a la del ya conocido WannaCry.**

Se pide que teniendo en cuenta la **Guía Nacional de Notificación y Gestión de Ciberincidentes (Capítulo 6)** ubicada en los recursos de la lección, redactéis la documentación necesaria para realizar las siguientes notificaciones del incidente al **CSIRT** de referencia:

- ➔ Notificación inicial.
- ➔ Dos notificaciones intermedias.
- ➔ Notificación final.

Recordad que en las notificaciones intermedias debe ir describiéndose las actuaciones que se van realizando para solventar el incidente y evitar su propagación.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Notificación inicial al CSIRT de Referencia

Notificar	Descripción
Código del incidente	**H-SAL-EXT-00**
Asunto	Incidente de seguridad **Ransomware** en el **H. Rascafría.**
OSE/PDS	**OSE: ciso@rascafria.com**
Sector estratégico	**SALUD**
Fecha y hora del incidente	Desconocido, en estudio.
Fecha y hora de detección del incidente	26/09/2023 a las 08:30 a.m
Descripción	A **las 8:30 a.m. del 26 de septiembre de 2023** se produjo el secuestro de aprox. un **25 %** de los equipos de puesto de trabajo de RR. HH. y ordenadores de salas de consulta. Un mensaje advertía del secuestro y exfiltración de información por el grupo ransomware **DarkHospital** exigiendo el pago de 25 Bitcoins a un monedero concreto antes de 7 días para evitar la publicación de la información exfiltrada en foros clandestinos y poder obtener la clave de recuperación de ficheros cifrados. El agente amenaza ha facilitado una url **.onion** para negociación y aporte de evidencias de la fuga.
Recursos tecnológicos afectados	Los equipos secuestrados se limitan a los **puestos de trabajo de médicos** (salas de consulta) **y RR. HH.** (son los que muestran una pantalla solicitando el rescate). Todos se encuentran en el mismo segmento de red a saber:

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

	COM -192.168.50.0/22 – segmento de puestos de trabajo de RR. HH. y personal salas de consulta. **E-HW-[SRV]-001** a **E-HW-[SRV]-069 –** Un total de 69 equipos de puesto de trabajo afectados.
Origen del incidente	Desconocido, en estudio.
Taxonomía (clasificación)	Clasificación **MUY ALTO.** Tipo de incidente: **Código dañino.**
Nivel de peligrosidad	**Muy Alto** – Distribución de malware + perdida de datos + interrupciones
Nivel de impacto	**Medio –** interrupción de los servicios superior al 20% de sistemas organización con potencial riesgo de exposición de datos sensibles de pacientes **(RGPD)** y daños reputacionales (eco mediático apreciable).
Impacto transfronterizo	**No aplica**
Plan de acción y contramedidas	Se ha pedido forense a entidad externa (SIA/INDRA) para determinar alcance real, causa raíz y fecha inicial del incidente para construir un plan de respuesta conforme a datos. **Contramedida 1:** Se ha bloqueado/aislado las comunicaciones de **COM -192.168.50.0/22** hacia el resto de la organización e Internet. **Contramedida2**: se derivan enfermos críticos a Hospital de La Paz (aquí se suspende temporalmente la atención de nuevos pacientes).
Afectación	Centro hospitalario Rascafría

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Medios necesarios para la resolución (J-P)	Por determinar
Impacto económico estimado (si se conoce)	Aprox. **80.000€ por hora** de interrupción servicio + gastos gestión incidente + posibles sanciones.
Extensión geográfica (si se conoce)	Acotado a zona de Rascafría (Norte Madrid).
Daños reputacionales (si se conocen)	Por determinar, por el momento hay mucho ruido en medios sobre la interrupción de servicios del hospital y rumores sobre "incidente de seguridad" debido a las pantallas de chantaje que ofrece el ransomware.
Adjuntos	Se aporta captura completa del mensaje aparecido en las pantallas de los equipos afectados con la URL onion para negociación y verificación de evidencias de fuga.
Regulación afectada (ENS, RGPD, NIS, PIC, Otros)	ENS + RGPD
Se requiere actuación del FFCCSE	NO

*La notificación de la hora lo haremos en formato **UTC**

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Notificación intermedia 1 al CSIRT de Referencia

Notificar	Descripción
Código del incidente	**H-SAL-EXT-00**
Asunto	Incidente de seguridad **Ransomware** en el **H. Rascafría.**
OSE/PDS	OSE: **ciso@rascafria.com**
Sector estratégico	**SALUD**
Fecha y hora del incidente	20/09/2023 a las 13:30 a.m.
Fecha y hora de detección del incidente	26/09/2023 a las 08:30 a.m
Descripción	El forense determina que la causa raíz y compromiso inicial se debe a la inserción de un artefacto USB no autorizado por parte de un empleado de RR. HH. descuidado. Los datos del EDR instalado en puesto de trabajo y recogidos por el SIEM del hospital indican que se introdujo el USB por vez primera el 20 de septiembre 2023. Conocer esta fecha es esencial para poder determinar copias de seguridad no comprometidas (previas a la fecha origen del incidente). El ransomware presenta capacidades de tipo gusano y se propagó aprovechando vulnerabilidad CVE-2023-3299 en protocolo Microsoft DS port 445/tcp dentro del segmento de red de puesto de trabajo de RR. HH. y salas de consultas, ya que se

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

	encuentran en el mismo segmento de red. El resto de redes no se vieron afectados debido a que no se permiten otros protocolos desde la red de puesto de trabajo excepto proxy y servicios dns. El análisis de la url onion facilitada en la nota de rescate muestra que los intrusos pudieron acceder y exfiltrar información PII –expedientes médicos y CV de RR. HH.– haciendo uso de credenciales robadas a empleados médicos y/o personal de RR. HH. Si bien el acceso es únicamente de lectura –la escritura o modificación expedientes requiere un 2° factor de autenticación–
Recursos tecnológicos afectados	Los equipos secuestrados se limitan a los puestos de trabajo de médicos (salas de consulta) y RR. HH. (son los que muestran una pantalla solicitando el rescate). Todos se encuentran en el mismo segmento de red a saber: **COM** -192.168.50.0/22 – segmento de puestos de trabajo de RR. HH. y personal salas de consulta. **E-HW-[SRV]-001** a **E-HW-[SRV]-069 –** Un total de 69 equipos de puesto de trabajo afectados.
Origen del incidente	USB infectado con código malicioso (ransomware)
Taxonomía (clasificación)	Clasificación **MUY ALTO.** Tipo de incidente: **Código dañino.**
Nivel de peligrosidad	**Muy Alto** – Distribución de malware + perdida de datos + interrupciones

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Nivel de impacto	**Medio –** interrupción de los servicios superior al 20% de sistemas organización con potencial riesgo de exposición de datos sensibles de pacientes **(RGPD)** y daños reputacionales (eco mediático apreciable).
Impacto transfronterizo	**No aplica**
Plan de acción y contramedidas	Una vez determinada la fecha inicial del compromiso se puede aplicar recuperación ante desastres a partir de backups no comprometidos. Se han restaurado un 20 % de los equipos afectados. Contramedia1: Se ha aplicado la última actualización a los sistemas para corregir la vulnerabilidad detectada. Contramedida2: Se aplica cortafuegos local para evitar futura propagación de gusanos/amenazas similares. Contramedida3: Se mantiene el bloqueo/ aislamiento de las comunicaciones del segmento COM -192.168.50.0/22 hacia el resto de la organización e Internet en tanto se limpie todos los sistemas. Los equipos restaurados ya no se ven afectados por la vulnerabilidad. Contramedida4: aún se derivan enfermos críticos a Hospital de La Paz, aunque RR. HH. ya está funcionando a un **50 %.** Contramedida5: cambio de credenciales todo el personal de RR. HH. y salas de consulta.
Afectación	Centro hospitalario Rascafría

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Medios necesarios para la resolución (J-P)	Por determinar
Impacto económico estimado (si se conoce)	Aprox. 80.000€ por hora de interrupción servicio + gastos gestión incidente + posibles sanciones por informes médicos y CVs de empleados en foros clandestinos, DNIs, y otra documentación PII).
Extensión geográfica (si se conoce)	Acotado a zona de Rascafría (Norte Madrid).
Daños reputacionales (si se conocen)	Potenciales daños a la reputación del hospital y equipo responsable.
Adjuntos	Se aporta informe forense facilitado por SIA/INDRA
Regulación afectada (ENS, RGPD, NIS, PIC, Otros)	ENS + RGPD
Se requiere actuación del FFCCSE	NO

*La notificación de la hora lo haremos en formato **UTC**

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Notificación intermedia 2 al CSIRT de Referencia

Notificar	Descripción
Código del incidente	**H-SAL-EXT-00**
Asunto	Incidente de seguridad **Ransomware** en el **H. Rascafría.**
OSE/PDS	OSE: **ciso@rascafria.com**
Sector estratégico	**SALUD**
Fecha y hora del incidente	20/09/2023 a las 13:30 a.m.
Fecha y hora de detección del incidente	26/09/2023 a las 08:30 a.m
Descripción	Se ha restaurado un **70 %** de los equipos afectados. Se ha detectado la publicación de la información exfiltrada en el sitio de fugas **(leak's site de DarkHospital) en red TOR.** Se comprueba que son 13 GB con archivos que contiene datos PII (pasaportes, DNIs, CVs y expedientes médicos de personalidades).
Recursos tecnológicos afectados	Los equipos secuestrados se limitan a los puestos de trabajo de médicos (salas de consulta) y RR. HH. (son los que muestran una pantalla solicitando el rescate). Todos se encuentran en el mismo segmento de red a saber: **COM -192.168.50.0/22** – segmento de puestos de trabajo de RR. HH. y personal salas de consulta.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

	E-HW-[SRV]-001 a E-HW-[SRV]-069 – Un total de 69 equipos de puesto de trabajo afectados. **S-INFO** – expedientes médicos y CVs.
Origen del incidente	USB infectado con código malicioso (ransomware)
Taxonomía (clasificación)	Clasificación **MUY ALTO.** Tipo de incidente: **Código dañino.**
Nivel de peligrosidad	**Muy Alto** – Distribución de malware + perdida de datos + interrupciones
Nivel de impacto	**Medio –** interrupción de los servicios superior al 20% de sistemas organización con potencial riesgo de exposición de datos sensibles de pacientes **(RGPD)** y daños reputacionales (eco mediático apreciable).
Impacto transfronterizo	**No aplica**
Plan de acción y contramedidas	Se ha recuperado la información exfiltrada y se ha **notificado antes de las 72** h a las personas cuya información PII ha quedado expuesta en foros clandestinos. Contramedida1: se pagará un **plan de monitorización de identidad para detectar potenciales escenarios de suplantación de identidad** haciendo uso de la información exfiltrada. Contramedida2: se fuerza el **uso de llaves criptográficas FIDO2** también para el acceso a consulta desde salas médicas y RR. HH. Contramedida3: se publica **nota de prensa** para paliar posible daño reputacional.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Afectación	Centro hospitalario Rascafría
Medios necesarios para la resolución (J-P)	Por determinar
Impacto económico estimado (si se conoce)	Aprox**. 80.000€** por hora de interrupción servicio + gastos gestión incidente + posibles sanciones por informes médicos y CVs de empleados en foros clandestinos, DNIs, y otra documentación PII).
Extensión geográfica (si se conoce)	Acotado a zona de Rascafría (Norte Madrid).
Daños reputacionales (si se conocen)	Daños a la reputación del hospital y equipo responsable, posibles denuncias colectivas.
Adjuntos	Se aporta **informe forense facilitado por SIA/INDRA**
Regulación afectada (ENS, RGPD, NIS, PIC, Otros)	ENS + RGPD
Se requiere actuación del FFCCSE	NO

*La notificación de la hora lo haremos en formato **UTC**

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Notificación FINAL al CSIRT de Referencia

Notificar	Descripción
Código del incidente	**H-SAL-EXT-00**
Asunto	Incidente de seguridad **Ransomware** en el **H. Rascafría.**
OSE/PDS	OSE: **ciso@rascafria.com**
Sector estratégico	**SALUD**
Fecha y hora del incidente	20/09/2023 a las 13:30 a.m.
Fecha y hora de detección del incidente	26/09/2023 a las 08:30 a.m
Descripción	Se restablece **el 100 % de los equipos afectados**. Se finaliza la derivación de enfermos a 3º hospitales. Se da por cerrado el incidente.
Recursos tecnológicos afectados	Los equipos secuestrados se limitan a los puestos de trabajo de médicos (salas de consulta) y RR. HH. (son los que muestran una pantalla solicitando el rescate). Todos se encuentran en el mismo segmento de red a saber: **COM** -192.168.50.0/22 – segmento de puestos de trabajo de RR. HH. y personal salas de consulta. **E-HW-[SRV]-001** a **E-HW-[SRV]-069 –** Un total de 69 equipos de puesto de trabajo afectados.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

	S-INFO – expedientes médicos y CVs.
Origen del incidente	USB infectado con código malicioso (ransomware)
Taxonomía (clasificación)	Clasificación **MUY ALTO.** Tipo de incidente: **Código dañino.**
Nivel de peligrosidad	**Muy Alto – Distribución de malware + perdida de datos + interrupciones**
Nivel de impacto	**Medio –** interrupción de los servicios superior al 20% de sistemas organización con potencial riesgo de exposición de datos sensibles de pacientes **(RGPD)** y daños reputacionales (eco mediático apreciable).
Impacto transfronterizo	**No aplica**
Plan de acción y contramedidas	Se ha contratado un ciberseguro para coberturas ante futuros posibles incidentes. Se ha bloqueado el acceso a dispositivos USB no registrados previamente vía despliegue de política sobre los sistemas operativos. Se publica nota de prensa dando por finalizado el incidente.
Afectación	Centro hospitalario Rascafría
Medios necesarios para la resolución (J-P)	Por determinar
Impacto económico estimado (si se conoce)	Aprox. 80.000€ por hora de interrupción servicio + gastos gestión incidente + posibles sanciones por informes médicos y CVs de empleados en foros clandestinos, DNIs, y otra documentación PII).
Extensión geográfica (si se conoce)	Acotado a zona de Rascafría (Norte Madrid).

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Daños reputacionales (si se conocen)	Daños a la reputación del hospital y equipo responsable, posibles denuncias colectivas.
Adjuntos	Se aporta informe forense facilitado por SIA/INDRA
Regulación afectada (ENS, RGPD, NIS, PIC, Otros)	ENS + RGPD
Se requiere actuación del FFCCSE	NO

*La notificación de la hora lo haremos en formato **UTC**