DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 20| Febrero 2022

PREVENCIÓN Y GESTIÓN DE ATAQUES *RANSOMWARE*

Í N D I C E

PREVENCIÓN Y GESTIÓN DE ATAQUES *RANSOMWARE*

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

El *ransomware* es un tipo de *malware* (*software* malicioso) que, en los últimos tiempos, está creciendo de forma exponencial. Este «secuestra» nuestros recursos, impidiendo el acceso a los mismos -habitualmente cifrándolos-, y solicita un rescate a cambio de su liberación.

El rescate se solicita, generalmente, a través de un mensaje o una ventana que emerge en el dispositivo afectado. Es habitual que se incluya un límite de tiempo para pagar el rescate y que amenacen con la destrucción total de los archivos secuestrados o con incrementar el valor del rescate si no se paga a tiempo. Asimismo, es común que el rescate se solicite a través de alguna moneda virtual como el *Bitcoin*. Un ejemplo de mensaje podría ser el siguiente:

El *ransomware* puede afectar a cualquier usuario, negocio o actividad que pueda pagar a cambio de la devolución de su información. Este está afectando a usuarios domésticos, negocios, sector público e incluso a servicios críticos como hospitales, causando pérdidas temporales o permanentes de información, interrumpiendo la actividad normal, ocasionando pérdidas económicas para restaurar los sistemas y ficheros y, en muchos casos, también daños reputacionales.

En el presente boletín, os proponemos una serie de actuaciones para conocer, prevenir y mitigar esta amenaza.

EL *RANSOMWARE* «SECUESTRA» NUESTROS RECURSOS, IMPIDIENDO EL ACCESO A LOS MISMOS -GENERALMENTE CIFRÁNDOLOS- Y SOLICITA UN RESCATE A CAMBIO DE SU LIBERACIÓN.

¿QUÉ PODEMOS HACER LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN PARA EVITARLO?

Un gran número de infecciones con *ransomware* tienen lugar por medio de ataques de ingeniería social. Esto es, los atacantes engañan a los usuarios para instalar el *malware*. Lo más habitual es que las infecciones se produzcan por alguna de las siguientes vías:

- correo electrónico con enlaces o adjuntos maliciosos;
- escritorio remoto expuesto a Internet, con credenciales poco robustas y sin mecanismos de protección;
- vulnerabilidades en el navegador web que facilitan la infección al navegar por sitios maliciosos;
- dispositivos externos infectados que se conectan a los equipos corporativos.

Para evitar el *ransomware*, sigue estas **RECOMENDACIONES:**


Mantén actualizados los sistemas operativos, navegadores y aplicaciones.


Utiliza contraseñas robustas.


Evita abrir adjuntos o clicar enlaces en correos sospechosos no esperados o no solicitados.


Evita usar redes públicas.


Comprueba que la página web en la que has entrado es una dirección segura. Para ello, ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.

UN GRAN NÚMERO DE INFECCIONES *RANSOMWARE* TIENEN LUGAR POR MEDIO DE ATAQUES DE INGENIERÍA SOCIAL. ESTO ES, LOS ATACANTES ENGAÑAN A LOS USUARIOS PARA INSTALAR EL *RANSOMWARE*.

UNA VEZ MATERIALIZADO EL ATAQUE, ¿CÓMO ACTUAMOS?

1 NO PAGAR NUNCA EL RESCATE

- Pagar no garantiza que vayamos a volver a tener acceso a los datos.
- Si pagamos, es posible que seamos objeto de ataques posteriores, pues ya saben que estamos dispuestos a pagar.
- Puede que soliciten una cifra mayor una vez hayamos pagado.
- Pagar fomenta el negocio de los ciberdelincuentes.

2 APLICAR EL PROCEDIMIENTO DE GESTIÓN DE BRECHAS DE SEGURIDAD

La detección por parte de un usuario de los sistemas de información de la Diputación de Valencia de un ataque *ransomware* o de cualquier otro suceso que suponga o pudiera suponer un incidente de seguridad deberá ser **comunicado inmediatamente** para valorar si puede catalogarse como "brecha de seguridad de los datos personales".

Tras la comunicación, se recabará **información útil** para decidir qué medidas tomar y para valorar la necesidad de notificar al centro de respuesta a incidentes de ciberseguridad, a la autoridad de control en materia de protección de datos y, en su caso, a los afectados. Asimismo, se valorará la denuncia del incidente a las Fuerzas y Cuerpos de Seguridad del Estado para que se investigue el origen del delito. Así, se puede colaborar en las labores de prevención a otras entidades y en las acciones para capturar al ciberdelincuente.

El **Delegado de Protección de Datos (DPD)** ocupará un papel muy relevante, liderando el plan de actuación en todos sus aspectos. Es importante que el DPD sea consultado tan pronto se haya detectado el incidente, lo que implicará que el usuario que lo detecte deba comunicarlo sin dilación. La actuación del DPD tendrá especial relevancia en esta fase de comunicación puesto que, entre las funciones que la normativa le atribuye, está la de actuar como punto de contacto entre el Responsable del tratamiento -la Diputación de Valencia- y la autoridad de control -la AEPD-.

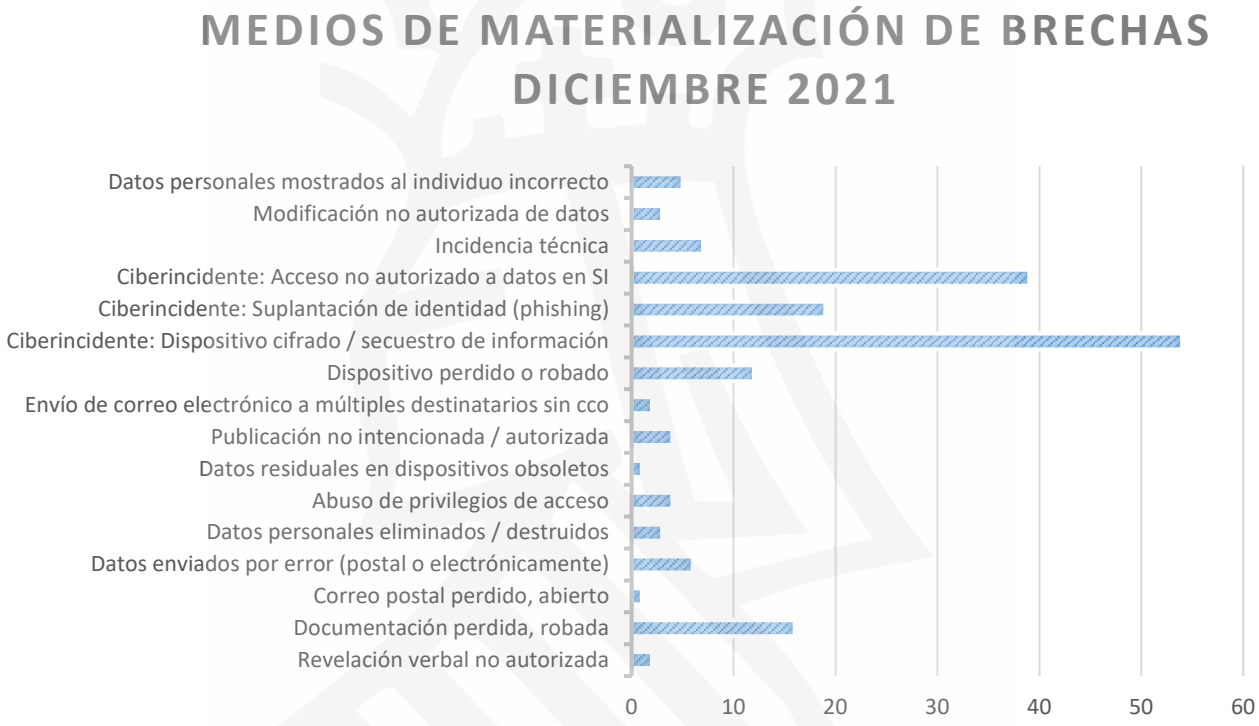
Es importante que se genere **documentación de todo el proceso** de detección, contención y respuesta, y que se custodien las evidencias.

Te animamos a que revises el boletín de protección de datos remitido en el mes de abril de 2021 **(Boletín nº 10): *"Análisis, gestión y comunicación de las brechas de seguridad en el contexto del RGPD".***

EL USUARIO DE LOS SISTEMAS DE INFORMACIÓN DE LA DIPUTACIÓN QUE DETECTE UN *RANSOMWARE* O CUALQUIER OTRO SUCESO QUE SUPONGA O PUDIERA SUPONER UN INCIDENTE DE SEGURIDAD, DEBERÁ COMUNICARLO INMEDIATAMENTE A LA PERSONA DESIGNADA A TAL EFECTO O, EN SU DEFECTO, AL RESPONSABLE DE LA INFORMACIÓN

BRECHAS DE SEGURIDAD NOTIFICADAS A LA AEPD POR *RANSOMWARE*

La Agencia Española de Protección de Datos (AEPD) publica, con periodicidad mensual, un informe que resume las principales características de las notificaciones de brechas de seguridad recibidas. En todos los informes publicados a lo largo de 2021 han destacado las brechas de seguridad provocadas por ciberincidentes consistentes en el cifrado de dispositivos y secuestro de la información (*ransomware*). En el informe de diciembre de 2021 -el último publicado hasta la fecha-, la Agencia señala que las brechas de datos personales causadas por ciberincidentes de tipo *ransomware* continúan siendo las más notificadas.



EN 2021, LA MAYOR PARTE DE LAS BRECHAS DE SEGURIDAD NOTIFICADAS A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS FUERON PROVOCADAS POR AGENTES EXTERNOS A LAS ORGANIZACIONES, SIENDO LOS CIBERINCIDENTES PROVOCADOS POR EL SECUESTRO Y CIFRADO DE LA INFORMACIÓN (*RANSOMWARE*) LOS MÁS HABITUALES.

¿PUEDEN SANCIONAR A LA DIPUTACIÓN POR SER VÍCTIMA DE ESTE TIPO DE ATAQUES?

En el ámbito del sector público, el Reglamento (UE) 2016/679, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) permite a los Estados establecer sus propias normas para regular su régimen sancionador. En el caso de España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) contempla para determinadas categorías de responsables o encargados del sector público la sanción de **APERCIBIMIENTO**, acompañada de las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción. Asimismo, ha de tenerse en cuenta el **DAÑO REPUTACIONAL** que la sanción causaría a la entidad.

En caso de ser víctima de un ataque tipo *ransomware*, la Diputación de Valencia podría ser sancionada por no contar con medidas técnicas y organizativas adecuadas para evitar o minimizar el impacto de este tipo de ataques, por no gestionar adecuadamente el incidente una vez materializado el mismo o por no notificar la brecha a la autoridad competente o a los interesados, según la valoración del riesgo realizada.

¿Cómo podemos evitar la sanción?

- De manera **previa al incidente**, debemos contar con **medidas técnicas y organizativas para evitar o minimizar el impacto**.
- Debemos seguir **el procedimiento** para afrontar incidentes de este tipo.
- Con **posterioridad al incidente**, debemos aplicar **medidas adicionales para minimizar el impacto.**
- Debemos **denunciar los hechos** ante las Fuerzas y Cuerpos de Seguridad del Estado.
- Debemos **generar documentación de todo el proceso** de detección, contención y respuesta y custodiar las evidencias ante una brecha de seguridad.
- Debemos realizar un **informe final sobre el incidente**.
- Debemos **notificar la brecha a quien corresponda**, según la valoración del riesgo realizada.

EN CASO DE SER VÍCTIMA DE UN ATAQUE TIPO *RANSOMWARE*, LA DIPUTACIÓN DE VALENCIA PODRÍA SER SANCIONADA POR NO CONTAR CON MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADECUADAS PARA EVITAR O MINIMIZAR EL IMPACTO DE ESTE TIPO DE ATAQUES, POR NO GESTIONAR ADECUADAMENTE EL INCIDENTE UNA VEZ MATERIALIZADO EL MISMO O POR NO NOTIFICAR LA BRECHA A LA AUTORIDAD COMPETENTE O A LOS INTERESADOS, SEGÚN LA VALORACIÓN DEL RIESGO REALIZADA.

MATERIAL COMPLEMENTARIO

- Brechas de seguridad: protégete ante el *ransomware* (Blog AEPD). Consulta este enlace.
- Brechas de datos personales (AEPD). Consulta este enlace.
- Informe de notificaciones de brechas de seguridad durante diciembre de 2021 (AEPD). Consulta este enlace.
- Expediente Nº: E/03575 (AEPD). Consulta este enlace.
- Procedimiento Nº: E/01783/2020 (AEPD). Consulta este enlace.
- Procedimiento Nº: E/08454/2019 (AEPD). Consulta este enlace.
- Ayuda *ransomware* (Blog INCIBE). Consulta este enlace.
- *Ransomware:* guía de aproximación (INCIBE). Consulta este enlace.
- Que no te secuestren el ordenador: medidas para evitarlo (Blog INCIBE). Consulta este enlace.
- Medidas de seguridad contra *ransomware* (CCN). Consulta este enlace.
- "Mi organización ha sido víctima de un ataque *ransomware,* ¿cómo debo actuar?" (Blog Asociación Española para la Calidad -AEC). Consulta este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) sanciona a una entidad por implantar un sistema de control horario por reconocimiento biométrico de huella dactilar sin haber realizado previamente una Evaluación de Impacto**. El Consorcio ESS Bilbao decidió en 2019 implantar un sistema de fichaje por reconocimiento de huella dactilar. De la documentación obrante en el expediente, la AEPD no encontró evidencia de la realización de la evaluación de impacto de protección de datos, por lo que sancionó a la entidad con apercibimiento, por una infracción del artículo 35 del RGPD.

Consulta la resolución en este enlace.

- **La Secretaría de Estado de Digitalización e Inteligencia Artificial crea la web de la "Oficina del Dato".** En 2020 se creó la Oficina del Dato, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Sus principales líneas estratégicas son las del diseño, coordinación y seguimiento del modelo de referencia arquitectónico para fomentar la recolecta, gestión e intercambio de datos públicos. En la nueva web podrás encontrar información al respecto.

Consulta la web en este enlace.

- **La Autoridad Catalana de Protección de Datos (APDCAT) emite un Dictamen sobre la conformidad con la normativa de protección de datos del uso del certificado COVID en Cataluña y el requerimiento del DNI por parte de los establecimientos.** Concluye la autoridad que la exigencia del certificado COVID en los términos expuestos y que han sido autorizados por el Tribunal Superior de Justicia de Cataluña, no puede considerarse contraria a la normativa de protección de datos personales. Igualmente, cuando sea exigible este certificado, la exigencia de exhibición del anverso del DNI a efectos de verificar la identidad resultaría compatible y proporcionado de acuerdo con la normativa de protección de datos personales.

Consulta el Dictamen en este enlace.