01

CIBERATAQUES ESPAÑA

AIR EUROPA

Descripción: Air Europa detectó el pasado 29 de septiembre un incidente de seguridad no autorizado con **capacidad para captar datos de tarjetas de crédito**. Este incidente se produjo entre el 22 de agosto y el 29 de septiembre, aunque no de forma consecutiva, poniendo en riesgo los datos en tránsito durante el proceso de gestión del pago, causando la **exfiltración de información relacionada con las tarjetas de crédito de sus clientes.**

Solución adoptada: Air Europa contactó con los afectados a través de un correo electrónico y recomiendaron **cancelar la tarjeta** para evitar cargos no autorizados o fraudes.

Datos o servicios comprometidos:

- Numero de tarjeta
- Fecha de caducidad
- CVV (*)

(*) Datos obtenidos de la página oficial del institucito Nacional de Ciberseguridad (INCBE)-[Actualización 30/11/2023] Air Europa informa de un ciberataque y recomienda a sus clientes cancelar su tarjeta bancaria | Ciudadanía | INCIBE

TELEPIZZA

Descripción: El grupo de **ransomware** Lockbit 3.0 publicó el pasado año **datos robados** a Food Delivery Brand, (grupo tras la marca Telepizza y otras cadenas de comida rápida) ante la **negativa** de Telepizza a pagar el rescate.

Solución adoptada: Llevaron a cabo un análisis forense para descubrir el punto de entrada, aumentaron la seguridad de la infraestructura con los proveedores y cerraron todos los **puntos vulnerables** a su juicio.

Datos o servicios comprometidos:

- Facturación de la firma en distintos países
- Contratos de trabajo de antiguos empleados (*)

(*) Datos obtenidos de la página web del diario digital español “El Confidencial” - Miles de datos internos y de exempleados de Telepizza, al descubierto tras un ciberataque (elconfidencial.com)

AYUNTAMIENTO DE CANGAS (GALICIA)

Descripción: El grupo de **ransomware** Lockbit 3.0 robó y encriptó una gran cantidad de datos relativos a la contabilidad, gestión tributaria y nóminas, que paralizó todos los programas externos del Concello. Pidieron a cambio un rescate, amenazando con vender los datos para que puedan ser utilizados en una página Tor.

Solución adoptada: Llevaron a cabo un análisis forense para descubrir el punto de entrada, aumentaron la seguridad de la infraestructura con los proveedores y cerraron todos los **puntos vulnerables** a su juicio.

Datos o servicios comprometidos:

- Desconexión de servidores de dominio
- No funcionamiento de los programas de contabilidad, gestión tributaria y elaboración de nóminas (*)

(*) Datos obtenidos de la página web del diario digital regional "El Faro de Vigo" - CIBERATAQUE AL CONCELLO DE CANGAS: Paralizados los programas externos de gestión tributaria, nóminas y contabilidad (farodevigo.es)

AGENCIA TRIBUTARIA - AEAT

Descripción: Se detectó el pasado junio una campaña de suplantación dirigida a la Agencia Tributaria, la cual está **distribuyendo malware** a través de correos electrónicos, mediante una técnica de ingeniería social llamada ***phishing***, Estos correos se están distribuyendo con dos tipos de código malicioso: Granodeiro y Mekotio, con el objetivo de infectar el dispositivo de la víctima para robar datos bancarios.

Solución propuesta por el INCIBE: Si no se ha descargado el archivo, marcarlo como spam y **eliminarlo** de la bandeja de entrada. Si se ha descargado y ejecutado se deberá **aislar el dispositivo, ejecutar un antivirus y formatear el dispositivo.**

Datos o servicios comprometidos:
- Dispositivos de los usuarios infectados (*)

(*) Datos obtenidos de la página oficial del institucito Nacional de Ciberseguridad (INCBE)- [Notificaciones fraudulentas suplantan la identidad de la Agencia Tributaria para propagar malware | Ciudadanía | INCIBE

HYUNDAI

Descripción: La multinacional de fabricación de automóviles emitió un comunicado firmando que un **tercero no autorizado había accedido a parte de la información de su base de datos.**

Solución adoptada: Hyundai notificó la incidencia a la **Agencia Española de protección de Datos** para su colaboración y **bloquearon** todos los servidores afectados, desconectándolos permanentemente de la red.

Datos o servicios comprometidos:

Datos personales de sus clientes:

- Correos electrónicos
- Datos de domicilios
- Números de teléfono
- Números de bastidores de vehículos (*)

(*) Datos obtenidos de la página web de la revista “ComputerHoy” - Hyundai sufre un ciberataque en España que compromete los datos de miles de clientes | Computer Hoy

HOSPITAL CLÍNIC DE BARCELONA

Descripción: El hospital Clínic de Barcelona fue víctima el pasado año de un **ataque informático tipo ransomware.** Los hackers atacaron los sistemas informáticos y publicaron los datos robados en la "Deep" y "dark" web. Se solicitó un rescate que el Gobern se negó a pagar.

Solución propuesta: Ante el aumento de ciberataques a hospitales, uno de los expertos intervinientes en el asunto indicó que hay que "recalcar la necesidad de contar con **herramientas** de análisis forense y **respuesta ante incidentes**, sistemas de autenticación multifactor, formación de usuarios, inteligencia artificial aplicada a los flujos de correo, entre otros medios, para poder prevenir este tipo de ataques"

Datos o servicios comprometidos:

- Complica acceso historiales de pacientes
- Sistema informático paralizado: suspensión de cirugías, consultas externas y analíticas(*)

(*) Datos obtenidos de la página oficial del institucito Nacional de Ciberseguridad (INCBE)- Ciberataque ransomware paraliza actividad del Hospital Clínic de Barcelona | INCIBE-CERT | INCIBE

02

CIBERATAQUES EE.UU.

UNITED STATED MARSHAL SERVICE

Descripción: El Servicio de Marshals de EE.UU (USMS), agencia federal de policía y servicio de alguaciles perteneciente al departamento de Justicia de Estados Unidos sufrió el pasado año un **ataque de ransomware y filtración de datos**, afectando a sistemas que contienen **información confidencial**. Se consideró un suceso de "suma importancia.

Solución adoptada: **Desconectaron** el sistema de la red y enviaron el informe al Departamento de Justicia para iniciar la investigación.

Datos o servicios comprometidos:

- Información de identificación de los empleados
- Declaraciones de procesos legales
- Información administrativas
- Información sobre investigaciones del USMS (*)

(*) Datos obtenidos de la página web de la revista argentina "La Nación" - El ciberataque que pone en peligro información confidencial de EE.UU. - LA NACION

UBER

Descripción: El pasado 2022 un atacante desconocido **accedió** a los sistemas informáticos de la compañía de movilidad, incluido el software de seguridad de la empresa y el dominio de Windows. Se llevó a cabo mediante **ingeniería social** contra un empleado de la compañía, pues el **usuario es el eslabón más "débil de la cadena de seguridad".**

Datos o servicios comprometidos:

- Servicios de Amazon Web
- Maquinas virtuales Vmware ESXi,
- Panel de administración de correo electrónico (*)

(*) Datos obtenidos de la página web española "Muycomputer" - https://www.muycomputer.com/2022/09/16/uber-sufre-un-ciberataque-que-compromete-sistemas-ti-criticos/

SEDENA

Descripción: El pasado 2022 se produjo una **filtración masiva** de documentos reservados de la Secretaría de la Defensa Nacional de México (SEDENA) mediante **ramsonware**. Se extrajeron 6 terabytes de **información interna y confidencial**.

Datos o servicios comprometidos:

- Información militar: actividades operativas y de inteligencia de la milicia.
- Correos electrónicos del ejército y de gobiernos extranjeros. (*)

(*) Datos obtenidos de la página web del servicio británico “BBC” - Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México - BBC News Mundo

OILTANKING DEUTSCHALAND

Descripción: La proveedora de combustible alemana sufrió en 2022 un **ciberataque** que afectó a su **capacidad de suministro**. Se desconoce a día de hoy qué tipo de método se utilizó.

Solución adoptada: Trabajaron junto con especialistas externos y con las autoridades del país. Operaron con una capacidad limitada, entrando en estado de "fuerza mayor".

Datos o servicios comprometidos:
- Inutilización de sus sistemas informáticos
- Inutilización de las cadenas de suministro principales (*)

(*) Datos obtenidos del diario digital español "El Español" - Hackean uno los principales proveedores de gas y petróleo de Alemania (elespanol.com)