Universidad Miguel Hernández

Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Derecho Semipresencial.

Trabajo Fin de Grado. Ciberdelitos. Ransomware.

Curso Académico 2018/2019

María Salud Quesada Gómez

Tutor: Fernando Miró

ÍNDICE

Introducción.

Este trabajo de fin de grado trata sobre Ciberdelincuencia en general, y concretamente sobre el Ransomware y los distintos tipos de existen. Estamos ante un tipo de delito informático o actividad maliciosa que afecta tanto empresas y organizaciones corporativas como a ciudadanos y usuarios en general, y que, además, se ha convertido en un rentable modelo de negocio para los ciberdelincuentes, ya que los riesgos que corren son mínimos. España cuenta con casi 40 millones de usuarios activos, y de ellos, casi la mitad utiliza el teléfono móvil como principal acceso, conectándose habitualmente a redes sociales.

La metodología a seguir en el trabajo es la de exponer, desde un punto de vista jurídico y técnico, en qué consiste el ransomware, sus características fundamentales, los usuarios y entornos vulnerables, cómo prevenir los ataques y las recomendaciones por parte de las autoridades policiales, gobiernos e instituciones públicas y privadas cuya finalidad es la lucha contra el cibercrimen.

El Cibercrimen o los ciberdelitos son aquellos delitos que solo pueden ser cometidos usando ordenadores, redes u otras formas de tecnologías de la información y la comunicación (TIC), y por lo tanto exigen una conexión obligatoria a internet.
Incluye tales actividades como la creación y propagación de malware, piratería informática para robar datos personales o industriales sensibles y ataques de denegación de servicio para causar daño financiero y/o reputacional.

La ciberdelincuencia está provocando daños sociales y económicos cada vez más graves, que afectan a los derechos fundamentales de las personas, plantean amenazas contra el Estado de Derecho en el ciberespacio y ponen en peligro la estabilidad de las sociedades democráticas.

Los ciberdelitos denunciados superan en número a los delitos convencionales en algunos países de la Unión, el uso de los instrumentos de cifrado y anonimización con motivos delictivos va en aumento, y los ataques con programas de secuestro de archivos para pedir rescate (Ransomware) superan

en número a las amenazas que plantean los programas malintencionados como los troyanos.

De acuerdo con la más reciente Evaluación de la Amenaza del Crimen Organizado por Internet (IOCTA), el cibercrimen se está volviendo más agresivo y conflictivo. Esto se puede ver a través de las diversas formas de delito cibernético, incluidos los delitos de alta tecnología, las violaciones de datos y la extorsión sexual.

Pero no se trata solo de datos financieros, sino de datos en general, que es un objetivo clave para los ciberdelincuentes. El número y la frecuencia de las violaciones de datos van en aumento, y esto a su vez está generando más casos de fraude y extorsión.

Desde la web del Observatorio español de delitos informáticos (oedi.es) se pueden extraer las estadísticas sobre ciberdelitos del año 2016, según datos públicos analizados por el Ministerio del Interior, dan como resultado que el número de ciberdelitos fue de 66.586 totales, de los cuales:

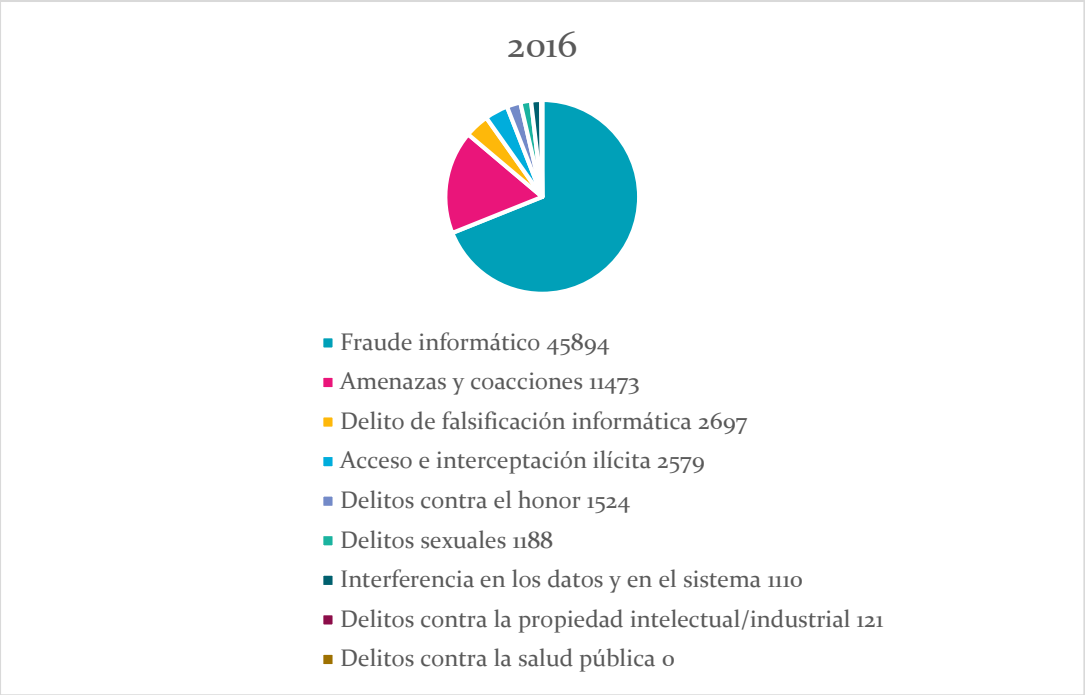

Tabla 1. Ciberdelitos en el año 2016. (1)[1]

Estos ciberataques se ven facilitados por la velocidad de Información, ya que viaja de manera instantánea, la conexión mundial, la falta de medidas y diferentes jurisdicciones crean vacíos legales, en algunos aspectos la tecnología va por delante de la legislación y la falta de Seguridad, ya que las medidas de protección se aplican una vez sucedido el incidente.

La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, resultando difícil determinar la autoría y el lugar de comisión del delito y, en consecuencia, la competencia para juzgar unos determinados hechos. De otra parte, el particular funcionamiento de los sistemas informáticos y los problemas de definición de la titularidad condicionan la atribución de responsabilidad en los delitos cometidos a través de sistemas informáticos o contra éstos. Así, el problema esencial consiste en determinar la responsabilidad jurídico-penal de los intervinientes, y esclarecer cuál es la responsabilidad de los intermediarios de servicios.

En conclusión, el ransomware es una amenaza que ha llegado para quedarse. Desde hace varios años ha ido evolucionando, utilizando métodos y algoritmos

[1] (Ministerio del Interior. Informe sobre criminalidad. , 2016; Observatorio español de delitos informáticos. , 2018)

de cifrado cada vez más complejos. Mientras esta amenaza continúe siendo una de las actividades más rentables para los cibercriminales, estos irán perfeccionando sus técnicas y adaptándose a nuevos escenarios, para los cuales hay que estar preparados.

CAPÍTULO 1: EL RANSOMWARE.

1. ¿QUÉ ES EL RANSOMWARE?

- APARICIÓN Y EVOLUCIÓN HISTÓRICA.
- TIPOS.
- LA INGENIERÍA SOCIAL COMO MÉTODO DE ATAQUE.

2. ¿CÓMO SE MATERIALIZAN LOS ATAQUES?

- QUIÉN ESTÁ DETRÁS Y SUS ROLES.
- QUÉ ARCHIVOS PUEDEN INFECTARSE.

3. HECHOS DE INTERÉS Y SU REPERCUSIÓN SOCIAL.

- CASO VIRUS DE LA POLICÍA.
- CASO GANDCRAB.
- EL PROYECTO “NO MORE RANSOM”.

1. ¿Qué es el ransomware?

El ransomware es un tipo de malware que hoy en día se está propagando de forma muy activa por internet. Este malware impide el acceso y amenaza con destruir los documentos y otros activos de las víctimas si estas no acceden a pagar un rescate.

Recordamos que el malware (virus, troyanos, etc.) es un software que si llega a los ordenadores de las víctimas, los infecta, manipulando el sistema y provocando mal funcionamiento o que realice acciones maliciosas. En el caso del ransomware, es un malware que cifra ciertos archivos o bien todo el disco duro de la víctima, bloqueándolo para impedir que el usuario acceda a sus ficheros y solicitando un rescate para recuperar el acceso al sistema y los ficheros.

El ransomware se propaga como otros tipos de malware; el método más común es mediante el envío de correos electrónicos maliciosos a las víctimas, los cibercriminales las engañan para que abran un archivo adjunto infectado o hagan clic en un vínculo que los lleva al sitio web del atacante, dónde se infectan, usando técnicas propias de **Ingeniería social**, concepto muy relevante y que más adelante profundizaremos en él.

La palabra Ransomware se forma al unir ransom (rescate) con ware (producto o mercancía).
En este caso el malware pide un rescate (ransom) a la víctima, a través de un mensaje o una ventana emergente, de ahí el nombre. Es un «secuestro virtual» de nuestros recursos por el que nos piden un rescate.

El mensaje, que suele ser intimidante, es el medio por el cual se avisa a la víctima de que la única forma de descifrar sus archivos o recuperar el sistema es mediante el pago de una cantidad de dinero virtual (normalmente **Bitcoins**[2]). Es habitual que incluyan un límite de tiempo (normalmente 72 horas) para pagar el

[2] BITCOIN: Moneda virtual o criptomoneda empleada tanto en transacciones financieras realizadas a través de ellas en el mundo virtual, así como medio de pago en caso de ciberataques. Permite el pago anónimo entre particulares.

rescate o amenacen con la destrucción total de los archivos secuestrados o con incrementar el valor del rescate si no se paga a tiempo.

Es común que el rescate se solicite a través de alguna moneda virtual como Bitcoins o que se utilicen muleros, que son intermediarios que transfieren el dinero procedente de estas actividades ilícitas (de forma voluntaria o involuntaria). Tanto las monedas virtuales como los muleros permiten al ciberdelincuente ocultarse. El precio a pagar por la recuperación suele variar entre cientos y miles de euros.

A cambio del pago, los ciberdelincuentes proporcionan el mecanismo para desbloquear el ordenador y descifrar los ficheros.

Pero no hay que olvidar que se trata de delincuentes, y por tanto no tenemos garantías de recuperar la información íntegra y sin daños, o de que vuelvan a pedirnos otro rescate, por lo que se recomienda no pagar.

También existe el riesgo de que para acceder al mecanismo de desbloqueo dirijan a la víctima a un enlace que podría a su vez contener otro malware y causar otra infección.
Es muy frecuente que los ordenadores infectados por ransomware estén también infectados con otro tipo de malware.

Aparición y evolución histórica.

Miguel Ángel Mendoza, en una publicación del 21 de agosto de 2015, hace referencia a la aparición y evolución del Ransomware[3].

Fue tal la evolución del ransomware, que hay una versión de código abierto y se puede contratar como servicio en el mercado sin tener conocimientos técnicos.

Aunque el secuestro de la información ha tomado relevancia en la actualidad y ha tenido un fuerte impacto en todo el mundo, lo cierto es que el ransomware es una amenaza que ya lleva varios años infectando dispositivos.

[3](MENDOZA, M.A, 2018)

En 1989 “PC Cyborg Troyano” reemplazaba el archivo AUTOEXEC. BAT, luego ocultaba los directorios y cifraba los nombres de todos los archivos de la unidad C, haciendo inutilizable el sistema. Por último, le solicitaba al usuario “renovar su licencia” con un pago de 189$ a una casilla de correo a nombre de PC Cyborg Corporation.

En 2005 “GPCoder” cifraba archivos con extensiones específicas, cómo documentos e información del usuario (xls, doc, txt, rtf, zip, rar, dbf, htm, html, jpg, db, etc.). Luego dejaba un archivo de texto en el escritorio con las instrucciones al usuario para el pago del rescate a cambio del programa y la clave para descifrar los archivos.

En 2010 “WinLock” Bloqueaba el equipo y desplegaba un mensaje en la pantalla, donde solicitaba al usuario enviar una cantidad de SMS Premium para desbloquearlo.

En 2012 “Reveton”, también conocido como el **“virus de la policía”**[4], que también bloqueaba el acceso al equipo, pero esta vez desplegando una pantalla con un falso mensaje de la policía nacional, o incluso del FBI. En esta pantalla le indicaba al usuario que el equipo había sido bloqueado por contener material ilegal, como pornografía infantil, software pirata o contenido con derechos de autor, por lo que debía pagar una “multa” para restaurar el acceso normal.

En 2013 “CryptoLocker” y “CryptoWall” aparecieron estos tipos de ransomware criptográfico caracterizados por utilizar cifrados asimétricos con clave pública RSA de 2048 bits; cifrar únicamente extensiones específicas de archivos de documentos, fotos e información del usuario; utilizar conexiones anónimas con el controlador del atacante a través de TOR; y ser uno de los primeros en solicitar el pago del rescate en bitcoins.

En 2015 “CTB Locker” con un comportamiento similar a Cryptolocker, se propagaba a través de un troyano que al ser ejecutado descargaba el código malicioso que cifraba los archivos del usuario. Asimismo, supo manejar muy bien

[4] (Asociación de afectados de internet. , 2018)

su credibilidad: ofrecía al usuario la posibilidad de descifrar de manera gratuita hasta cinco archivos para demostrar que podían ser recuperados.

En 2017 “WannaCryptor” se volvió popular bajo el nombre de WannaCry (en español “quieres llorar”), cifra los archivos del equipo infectado utilizando una combinación de los algoritmos AES-128 y RSA-2048, lo cual hace imposible su recuperación mediante técnicas de análisis. Sin embargo, lo que convirtió al ataque en algo realmente escandaloso fue su capacidad de propagarse por sí mismo, de manera similar a un gusano, a través de las redes de los equipos infectados, utilizando una vulnerabilidad en el protocolo de archivos compartidos de Windows.

Entre los distintos tipos de Ransomware, encontramos:

I. Ransomware que cifra los archivos.

En este tipo de ataque la comunicación entre el atacante y la víctima se realiza a través de **TOR**[5], mientras exige la transferencia de dinero. *Cryptolocker*[6]*, CTB-locker y TorrentLocker* son los más resonantes.
Estas variantes son detectadas por los productos de ESET bajo el nombre WIN 32/FileCoder.
Este Ransomware utiliza diversos algoritmos de cifrado para bloquear el acceso a los archivos del usuario. Una vez que se apodera de un sistema, se inicia el cambio en la estructura de los archivos y documentos, de manera tal que solo se podrán volver a leer o utilizar tras restaurarlos a su estado original, lo cual requiere del uso de una clave conocida únicamente por los ciberdelincuentes.
En la mayoría de los casos, el ataque afecta solo a ciertos archivos, siendo los de ofimática los más comúnmente perjudicados (documentos de texto, powerpoints, notas, etc.).
Una vez finalizada la infección, se despliega una pantalla que indica que los

[5] TOR: Es un software libre y una red abierta que ayuda a defenderse contra el análisis del tráfico, para evitar la vigilancia de la red que amenaza la libertad y la privacidad personal, las actividades y relaciones comerciales confidenciales y la seguridad del estado.
[6] Cryptolocker: Familia reciente de ransoms cuyo modelo de negocio se basa en la extorsión al usuario. Secuestra los documentos del usuario y pide un rescate por ellos, con tiempo límite para poder recuperarlos.

archivos han sido cifrados y explicando al usuario el proceso de pago de una cantidad de dinero a cambio de la clave para descifrar la información.

II. Ransomware de pantalla de bloqueo (*Lockscreen*).

Con este tipo de Ransomware no es posible usar el equipo hasta haber pagado el rescate. *Reveton* es una de las familias más encontradas en entornos virtuales.

El ransomware de tipo lockscreen impide el acceso y el uso del equipo mediante una pantalla de bloqueo, imposibilitando cualquier acción para cerrarla, abrir el administrador de tareas, los navegadores web o cualquier otra parte del sistema. En esta pantalla típicamente se muestra un mensaje donde se explica lo ocurrido y se solicita el pago de un rescate.

Dado que esta variante no cifra los archivos, en estos casos la información podría recuperarse, ya que se puede extraer el disco duro y luego limpiar el equipo de la infección.

Por esta misma razón, este malware suele utilizar engaños y trucos de ingeniería social para persuadir al usuario a que pague el rescate.

III. El ransomware en los dispositivos móviles.

Los ataques de ransomware también llega a los dispositivos móviles. En Android encontramos a SIMPLOCKER, en iOS a WireLurker, y además nuevas variantes del “Virus de la Policía”.

2. Cómo se materializan los ataques.

Los ciberdelincuentes utilizan una o varias vías para infectar a la víctima: Aprovechan agujeros de seguridad, es decir, vulnerabilidades del software de los equipos, sus sistemas operativos y sus aplicaciones. Los desarrolladores de malware disponen de herramientas que les permiten reconocer dónde están estos agujeros de seguridad e introducir así el malware en los equipos. Recientemente, algunas variedades de ransomware utilizan servidores web desactualizados como vía de acceso para instalar el ransomware.

También se están aprovechando de sistemas industriales *SCADA* conectados a internet sin las medidas básicas de seguridad, ya que conservan las mismas credenciales genéricas de acceso y administración. Por ejemplo, cada vez más equipos de aire acondicionado, impresoras de red, equipos médicos, etc. que no estaban conectados a ninguna red informática, son conectados a redes corporativas o internet sin las mínimas medidas de seguridad.

Conseguir las cuentas con privilegios de administrador de acceso a los equipos mediante engaños, como el *phishing*[7] y sus variantes, o aprovechar otras debilidades de procedimiento, por ejemplo, no cambiar el usuario y contraseña por defecto, o vulnerabilidades del software. Con estas cuentas podrán instalar el software, es decir, el malware en los equipos.

Otra forma muy común y sencilla para el ciberdelincuente es el uso de la *Ingeniería social*. Por ejemplo, mediante un correo falso con un enlace o un adjunto con una supuesta actualización de software de uso común que en realidad instala el malware; o con un mensaje suplantando a un amigo o conocido con un enlace a un sitio que aloja el malware. También se utilizan estas técnicas a través de redes sociales o servicios de mensajería instantánea.

El *spam* (correo basura) que contiene enlaces web maliciosos o ficheros adjuntos como un documento de Microsoft Office o un fichero comprimido (.rar, .zip) que contienen macros o ficheros JavaS-cript que descargan el malware.

Otro método conocido como drive-by download, consiste en dirigir a las víctimas a sitios web infectados, descargando el malware sin que ellas se percaten aprovechando las vulnerabilidades de su navegador. También utilizan técnicas de malwertising o malvertizing[8].

[7] PHISING: Es uno de los métodos ms utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta´, como puede ser una contraseña o información detallada sobre tarjetas de crédito, u otra información bancaria de la víctima.

[8] Malwertising: consiste en incrustar anuncios maliciosos en sitios web legítimos. El anuncio contiene código que infecta al usuario sin que este haga clic en él.

La Ingeniería social como método de ataque.

La ingeniería social se ha utilizado en muchas áreas diferentes del crimen, y la delincuencia informática no es una excepción. Muchas compañías de seguridad en Internet destacan continuamente el factor humano como el eslabón más débil de la seguridad cibernética. Influenciar a la gente para que actúe en contra de su propio interés o el interés de una organización es a menudo una solución más simple que recurrir a software malicioso o la piratería.

Tanto la policía y la industria financiera indican que la ingeniería social continúa permitiendo a los atacantes que carecen de los conocimientos técnicos, la motivación para usarlos o los recursos para adquirirlos. Además, permite a aquellos dotados técnicamente para orquestar ataques combinados sin pasar por las dos líneas de hardware o software humanos y de defensa. Las principales amenazas identificadas en *IOCTA* (Guía IOCTA 2017, 2018)[9] *2016* son: Fraude CEO, Phising (We live security , 2018) y Fraude por adelanto de pago. Cuando los creadores de malware usan técnicas de ingeniería social, pueden atraer a un usuario desprevenido para que descargue un archivo infectado o abra un enlace a un sitio web infectado. Muchos gusanos de correo electrónico y otros tipos de malware utilizan estos métodos.

Ataques de gusanos.

El cibercriminal intentará atraer la atención del usuario hacia el enlace o el archivo infectado, y luego hacer que el usuario haga clic en él. Los ejemplos de este tipo de ataque incluyen:

1. El gusano “LoveLetter” que sobrecargó los servidores de correo electrónico de muchas empresas en 2000. Las víctimas recibieron un correo electrónico que les invitaba a abrir la carta de amor adjunta. Cuando abrieron el archivo adjunto, el gusano se copió a todos los contactos en la libreta de direcciones

[9] IOCTA (The Internet Organised Crime Threat Assessment): es una evaluación de amenazas centrada en la aplicación de la ley destinada a informar el establecimiento de prioridades para los Planes de Acción Operativos EMPACT en las tres áreas prioritarias de cibercrimen (ciberataques, explotación sexual infantil en línea y fraude de pagos).

de la víctima. Este gusano todavía se considera como uno de los más devastadores, en términos del daño financiero que infligió.

2. El gusano de correo electrónico “Mydoom”, que apareció en Internet en enero de 2004, usando textos que imitaban mensajes técnicos emitidos por el servidor de correo.
3. El gusano “Swen” se hizo pasar por un mensaje enviado por Microsoft. Decía que el archivo adjunto era un parche que eliminaría las vulnerabilidades de Windows. No es de extrañar que mucha gente tomara en serio el reclamo y tratara de instalar el falso parche, aunque realmente era un gusano.

Canales de entrega de enlaces de malware

Los enlaces a sitios infectados se pueden enviar por correo electrónico, ICQ y otros sistemas de mensajería instantánea, o incluso a través de salas de chat de Internet de IRC. Los virus móviles a menudo se entregan por mensaje de texto, por ejemplo, mediante el Whatsapp.
Cualquiera que sea el método de entrega utilizado, el mensaje generalmente contiene palabras llamativas o intrigantes que alientan al usuario desprevenido a hacer clic en el enlace. Este método de penetración en un sistema puede permitir que el malware pase por alto los filtros antivirus del servidor de correo.

Ataques de red punto a punto (P2P).

Las redes P2P también se usan para distribuir malware. Este ataque se basa en la aparición de un gusano o un virus troyano en la red P2P, al que se le pone un nombre de una manera que atrae la atención y logra que los usuarios descarguen e inicien el archivo, por ejemplo:

- AIM y AOL Password Hacker.exe
- Microsoft CD Key Generator.exe
- Play Station emulator crack.exe

En algunos casos, los creadores y distribuidores de malware toman medidas que reducen la probabilidad de que las víctimas denuncien una infección:

Las víctimas pueden responder a una oferta falsa de una utilidad gratuita o una guía que promete, por ejemplo, el acceso gratuito a Internet o comunicaciones móviles, la posibilidad de descargar un generador de números de tarjetas de crédito, un método para aumentar el saldo de la cuenta en línea de la víctima ... u otros beneficios ilegales.

En estos casos, cuando la descarga resulta ser un virus troyano, la víctima está dispuesta a evitar revelar sus propias intenciones ilegales. Por lo tanto, la víctima probablemente no denuncie la infección.

Un ejemplo esclarecedor de esta técnica fue el virus troyano que se envió a las direcciones de correo electrónico que se tomaron de un sitio web para encontrar empleo. Las personas que se habían registrado en el sitio recibieron ofertas de trabajo falsas, pero las ofertas incluían un virus troyano. El ataque se dirigió principalmente a direcciones de correo electrónico corporativas, y los ciberdelincuentes sabían que el personal que recibió el troyano no querría decirles a sus empleadores que habían sido infectados mientras buscaban empleo alternativo.

También existen métodos inusuales de ingeniería social, se trata de métodos complejos para completar sus ataques cibernéticos, por ejemplo el ocurrido en Japón, donde los ciberdelincuentes utilizaron un servicio de entrega a domicilio para distribuir los CD que estaban infectados con el spyware de Troya. Los discos fueron entregados a los clientes de un banco japonés. Las direcciones de los clientes habían sido robadas previamente de la base de datos del banco.

¿Quién está detrás?

El ransomware, como otros tipos de malware, es un negocio de bajo coste y con beneficios importantes. Debido a esto están proliferando redes de ciberdelincuentes especializadas en ransomware.
En este negocio participan además del creador del ransomware, los agentes que lo distribuyen y los servicios para recaudar el rescate.
Aprovechando las ventajas de la tecnología, los ciberdelincuentes utilizan los modelos de negocio que proporciona internet (P2P, crowdsourcing, redes de

afiliados o piramidales, inserción de publicidad, etc.), para obtener beneficio y ocultar su actividad maliciosa.

Dentro de esa estructura delincuencial, como plasma la sentencia *28/16* del Caso de la policía, funcionan como un ecosistema del cibercrimen, los miembros del grupo en cuestión se hacen cargo de las distintas funciones que abarcaban desde la creación de virus hasta el circuito económico del producto de su actividad. Entre las distintas etapas o tareas de la citada estructura podemos distinguir las siguientes:

El "ransomware coder" es la persona encargada de programar el ransomware y de ponerlo a disposición de otros miembros del grupo.
Se suele elaborar de forma expresa, ya sea para un individuo o para un grupo de afiliados, todo ello por una suma concreta de dinero o bien por un porcentaje de las ganancias ilícitas, tomando como base el número de ordenadores infectados.

El "coder" se encarga de ofrecer el código. También suelen llevar a cabo un servicio de actualizaciones diarias de dicho código, para evitar ser detectado por los antivirus o dificultar así su estudio mediante *técnicas de reversing*[10].

Los "Ransomware exploiters" se dedican a explotarlo. Establecen la infraestructura de dominios y servidores para su propagación e infección.

Los servidores de control "C&C" suelen llevar el control estadístico del número de usuarios infectados.

Los pagos de los servicios y servidores "C& C" se hacían a través de PayPal o Bitcoins.

En el “Ransomware as a Service**”**, el delincuente contacta con agentes para distribuir el ransomware. Los agentes, al igual que los muleros que cobran los rescates, pueden ser cualquier persona con conocimientos de internet.

[10] Técnicas de reversing[10]: Permiten analizar las acciones que genera el ransomware dentro del ordenador y acceder a las estadísticas generadas por los servidores de control "C&C".

Los agentes distribuyen el malware (alojándolo en sitios legítimos, mediante correos electrónicos, etc.) y si consiguen que alguien pague el rescate obtendrán una parte del mismo.
Este rescate, suele ser pagado mediante Bitcoins, para conseguir así un pago anónimo gracias a los servicios de mixing o tumbling de bitcoins, accesibles desde la red anónima *Tor*, que mezclan los fondos de distintas carteras, realizando una especie de lavado de la criptomoneda que dificulta que se pueda seguir el rastro de las transacciones.

Sin embargo, y como veremos más adelante, el pago del rescate no garantiza que vayamos a recuperar nada, ni tampoco que vayamos a recibir ataques futuros.

Las extensiones más perjudicadas son las de archivos de ofimática y multimedia como procesadores de texto, hojas de cálculo, diapositivas, imágenes, correos electrónicos, bases de datos con información sobre clientes, cuentas, etc.

3. Hechos de interés y su repercusión social.

El caso “virus de la policía”.

El Centro Europeo de Ciberdelincuencia de Europol publicó su evaluación de la amenaza “virus de la policía”[11].
Este informe tiene como objetivo aumentar el conocimiento del ransomware, así como identificar las oportunidades para la intervención policial internacional y la coordinación operativa.

El “Ransomware policía o virus de la policía” es un tipo de fraude informático utilizado por los criminales para extorsionar y obtener dinero a través del despliegue de este malware[12].
El malware deshabilita la funcionalidad de los ordenadores de las víctimas y

[11] (Evaluación amenaza "virus de la policía", 2017)
[12] (Asociación de afectados de internet. , 2018)

muestra un mensaje exigiendo el pago de un rescate para recuperar el acceso a sus ordenadores.

Los mensajes simulaban ser enviados por las Fuerzas y Cuerpos de seguridad, y acusaban a la víctima de la realización de actividades online tales como intercambio ilegal de archivos, acceder a material de abuso infantil, o visitas de sitios web terroristas.

Los criminales usaban los logotipos de las FF.CC. de seguridad para dar autoridad a sus mensajes y obligar a las víctimas a pagar rescates para desbloquear sus equipos.

Aunque el número exacto de víctimas en la Unión Europea es difícil de evaluar, se estima que millones de ordenadores han sido infectados y decenas de miles de ciudadanos han pagado las demandas de rescate. Siendo así un negocio de varios de millones de euros para los criminales involucrados.

Estas actividades cibercriminales se ven facilitadas por los foros online que proporcionan el código fuente ransomware, la infraestructura para la distribución de los servicios de malware y de lavado de dinero para cobrar las ganancias ilícitas obtenidas a través de soluciones de prepago en línea y monedas virtuales.

Con los “Ransomware Kits” los ataques pueden ser fácilmente desplegados sin necesitar a técnicos expertos.

Están surgiendo nuevas formas de ransomware que pueden tener aún más impacto en las personas y las empresas, las cuales corren el riesgo de perder permanentemente sus datos y archivos.

Sin embargo, las diversas jurisdicciones y el derecho interno de cada Estado complican las investigaciones policiales y la cooperación. Debido a esto es necesario un mejor intercambio de información entre las autoridades policiales y socios privados para luchar contra este fenómeno, ya que los cibercriminales siguen avanzando y expandiendo su grupo de víctimas, abordando nuevos mercados y dirigiéndose a diferentes sistemas operativos y dispositivos.

El jefe del Centro Europeo de Ciberdelincuencia afirmó que "*los ataques de malware en forma de ransomware están aumentando por desgracia. Se trata de una mina de oro para las organizaciones criminales, fácil de usar y difícil para las víctimas el protegerse. Todo tipo de usuarios son víctimas potenciales de este crimen, no solo los usuarios sino también las empresas y las instituciones públicas[13]".*

Caso GandCrab. *"Más de 50.000 víctimas en menos de un mes".*

El Ransomware GandCrab ya ha hecho 50.000 víctimas en todo el mundo, un gran número en Europa, por lo que es una de las formas más agresivas de ransomware en lo que va de 2018.

Se propaga a través de anuncios maliciosos publicados en sitios web comprometidos o por medio de facturas ficticias enviados como archivos adjuntos en mensajes de correo electrónico.
Una vez instalado en el ordenador de la víctima, el ransomware cifra los archivos en el sistema infectado, ofreciendo una clave de descifrado a cambio de un pago de un rescate de US $ 300 - 500 en la moneda virtual DASH.

Por primera vez en el ransomware se da uso de DASH para el pago encriptado del rescate.
Este ransomware también se ejecuta como un programa de afiliados (ransomware-as-a-service), en la que los afiliados distribuyen el ransomware, mientras que los desarrolladores GandCrab ganan una comisión por cada pago de un rescate.

Gracias a los esfuerzos de las autoridades rumanas, Bitdefender[14] y Europol, la herramienta para desencriptar los archivos está disponible de forma gratuita en "No más Ransom"[15] y en la página web de Bitdefender. Funciona para todas las versiones conocidas de la familia GandCrab ransomware. El lanzamiento de esta

[13] (Evaluación amenaza "virus de la policía", 2017)
[14] (Bitdefender, 2018)
[15] (No more ransom, 2018)

nueva herramienta es otro ejemplo de la eficacia de las asociaciones público - privadas como “No más de Ransom”, una iniciativa que abarca más de 120 socios, siendo la Policía rumana el más reciente miembro asociado.

Para prevenir la infección con ransomware, los usuarios se les recomienda mantener copias de seguridad de datos importantes, utilizar una solución de seguridad, y evitar el acceso a enlaces o archivos de correos electrónicos no solicitados. Encontrar más consejos de información y prevención sobre www.nomoreransom.org.

Proyecto “No more Ransom”.

El portal No More Ransom es una iniciativa del National High Tech Crime Unit de la policía de Países Bajos, el European Cybercrime Centre de Europol y de dos compañías de ciberseguridad (Kaspersky Lab y McAfee) con el objetivo de ayudar a las víctimas de ransomware a recuperar sus datos cifrados sin tener que pagar a los criminales. El proyecto se lanzó oficialmente el 25 de julio de 2016.[16]

Dado que es mucho más fácil evitar la amenaza que revertirla una vez un sistema se haya visto afectado, el proyecto también se dirige a educar a los usuarios sobre cómo funciona el ransomware e informar sobre qué contramedidas se pueden tomar para prevenir eficazmente una infección. Cuantas más partes apoyen el proyecto, mejores resultados se podrán obtener. Debido a este “interés general” está abierta a que se unan otras entidades, tanto públicas como privadas.

Los usuarios pueden descargar herramientas de descifrado que se han creado en base a errores de implementación de los delincuentes, ingeniería inversa de algoritmos, acciones de aplicación de la ley o datos filtrados por delincuentes en línea.
Las víctimas solo necesitan subir dos archivos cifrados y la nota de rescate para verificar si hay soluciones de descifrado disponibles.

[16] (No more ransom, 2018)

El proyecto también proporciona información de prevención y enlaces para informar el delito cibernético a las respectivas fuerzas policiales nacionales.

Los distintos tipos de ransomware descifrados han sido: Annabelle, GandCrab, LambdaLocker, NemucodAES, MacRansom, Jaff, EncrypTile, Amnesia2, Amnesia Mole, BTCWare, Cry128.

CAPÍTULO 2: La actualidad del Ransomware.

1. LEGISLACIÓN ESTATAL

- LEY PENAL EN BLANCO.
- LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.
- REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE, REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.
- RELACIÓN CON EL CIBERATAQUE DE RANSOMWARE WANNACRY.

2. NORMATIVA EN EL ÁMBITO DE LA UNIÓN EUROPEA.

- EUROPOL Y EUROPEAN CYBERCRIME CENTRE
- EC3. SIRIUS. CONVENIO DE BUDAPEST.
- INFORME SOBRE CIBERCRIMINALIDAD 2015. MINISTERIO DEL INTERIOR. CONVENIO DE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA
- INFORME DE 26 DE JULIO DE 2017. SOBRE LA LUCHA CONTRA LA CIBERDELINCUENCIA. (2017/2068(INI)).

3. GUÍAS NACIONALES E INTERNACIONALES.

- GUÍAS DE INCIBE.
- NORMATIVA COBIT 5 (SEGURIDAD DE LA INFORMACIÓN EN ORGANIZACIONES).
- NIST (SEGURIDAD DE DATOS).
- ESTÁNDARES ISO 27000

4. PROBLEMAS AL APLICAR LOS DIFERENTES TIPOS DE LEGISLACIÓN.

1. Legislación estatal.

Ley penal en blanco.

El actual Código Penal no tipifica el delito de Ransomware. Se trata de una ley penal en blanco o ley necesitada de complemento, ya que existen otros preceptos penales que contienen la pena, pero no consignan íntegramente los elementos específicos del supuesto de hecho, remitiéndose a otras disposiciones legales del mismo o inferior rango. En el caso del Ransomware estamos ante un concurso de delitos, como a continuación se explica.

El autor Álvaro Écija[17] explica como el ransomware se ha tipificado como un *delito de estafa en concurso con un delito de daños informáticos*, sin embargo, con los ordenamientos jurídicos actuales no se puede actuar con eficacia por los motivos siguientes.

El Título XIII del Código Penal trata sobre los "Delitos contra el patrimonio y contra el orden socioeconómico", y es en el capítulo VI (de las defraudaciones) sección 1, donde se tipifica este delito:

"De las estafas. Artículo 248 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno."

En el caso del ransomware, el ciberdelincuente realiza, con la intención de lucrarse, un engaño mediante el envío de un correo malicioso o archivo infectado, con la finalidad de que la víctima lo abra y su sistema sea infectado.

El artículo 248.2 es el que se centra en la comisión del delito empleando medios informáticos. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

[17] (Écija, Álvaro, 2017)

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Este artículo está abarcando los diversos actos ilícitos y con ánimo de lucro que se pueden realizar mediante el secuestro del sistema por el ciberdelincuente.

El capítulo IX del Código Penal desarrolla de los daños. Aquí se encuentra la tipificación de este delito refiriéndose al daño producido al borrar, dañar o acceder a datos informáticos, sistemas o documentos. Las penas son de presión de 6 meses a 3 años, pudiendo agravarse cuando concurran determinadas circunstancias.

"Artículo 264 1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".

2. "Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A

estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado".

3. "Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".

Artículo 264 bis 1. "Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno":

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. "Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior".

3. "Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".

El artículo 264 ter castiga a quienes produzcan, adquieran o faciliten a terceros los medios necesarios para cometer los delitos informáticos mencionados anteriormente.

Artículo 264 ter. "Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores":

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

En relación con los consumidores y la protección de sus datos, el Código Penal tipifica los delitos relativos al mercado y a los consumidores.

Este artículo podría aplicarse cuando el Ransomware infecta el sistema de una gran empresa y saca a la luz datos financieros de esta o de sus clientes. La pena impuesta por el tipo básico va de 2 a 4 años, pudiendo agravarse si el daño se agrava.

Artículo 278. 1. "El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses".

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Esta ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Para evitar o reducir al máximo las probabilidades de ser víctimas de un ataque de Ransomware, o de cualquier otro ciberdelito, esta ley establece los siguientes principios que incluyen medidas de seguridad.

- El principio de seguridad de datos, establecido en el artículo 9 de la ley, "*impone al responsable del fichero adoptar las medidas técnicas y organizativas necesarias* que garanticen la seguridad de los datos de carácter personal y eviten su *alteración, pérdida, tratamiento o acceso no autorizado"*.

- Estas medidas han sido desarrolladas en el Título VIII del Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, desarrollado a continuación.

Reglamento de desarrollo de la Ley orgánica de protección de datos. Real Decreto 1720/2007, de 21 de diciembre.

El Reglamento de desarrollo de la LOPD (RLOPD) ha regulado la materia de modo que contempla las múltiples formas de organización material y personal de la seguridad que se dan en la práctica.

Regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Lo más importante de este reglamento es la modificación algunos aspectos del régimen actual y las nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Además, incluye dos elementos de carácter general que constituyen la mayor innovación del RGPD para los responsables, y se proyecta sobre las obligaciones destinadas a las organizaciones.

El principio de responsabilidad proactiva

Este principio consiste en la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al reglamento.
Requiere que las organizaciones analicen: qué datos tratan, con qué finalidades, y qué tipo de operaciones de tratamiento llevo a cabo.
A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.
En resumen, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que llevan a cabo.

El enfoque de riesgo

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones.

Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Soluciones del RGPD a las violaciones de seguridad de los datos.

El Grupo ECIX hace referencia a las soluciones que el Reglamento General de Protección de Datos realiza con relación a las brechas de seguridad.

El RGPD define las violaciones de seguridad de los datos, conocidas como “quiebras de seguridad”, de forma muy amplia, al incluir todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Sucesos como un ataque de Ransomware, la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Obligaciones que impone el RGPD.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
La notificación ha de incluir un contenido mínimo, la naturaleza de la violación, categorías de datos y de interesados afectados, medidas adoptadas por el responsable para solventar la quiebra, y, si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Los responsables deben documentar todas las violaciones de seguridad. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias.
Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.
El RGPD añade a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.

Relación entre los datos personales y su afectación a los derechos y libertades.

Partiendo de que la valoración del riesgo de la quiebra es distinta del análisis de riesgos previo a todo tratamiento, se trata de establecer hasta qué punto el

incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados puede causar un daño en sus derechos o libertades.

⇒ Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

Se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.

Por tanto, la mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar a la notificación, dado que en esas condiciones no sería posible determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

En casos de quiebras que por sus características pudieran tener gran impacto, sí sería recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, cuando sea complejo determinar completamente su alcance. En esos casos sí es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

Cabe mencionar que la información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

En cuanto al criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

Es importante señalar que entre las obligaciones del responsable se encuentra la de elaborar un documento de seguridad, que recogerá las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente que será de obligado cumplimiento para todos aquellos con acceso a datos de carácter personal.

La notificación a los interesados no es necesaria en todos los casos.

Dicha notificación no será necesaria cuando el responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado. Tampoco cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice, o cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

Por otro lado, el RLOPD señala que las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles, básico, medio y alto, a aplicar según el tipo de datos de carácter personal a tratar.

Un ejemplo de los supuestos considerados de alto riesgo en cuanto a su tratamiento son los perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar, los tratamientos a gran escala de datos sensibles y la observación sistemática a gran escala de una zona de acceso público.

Las obligaciones a seguir en el caso de las transferencias internacionales de datos son las siguientes.

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

1. A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado
2. Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino
3. Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Análisis del RGPD y de las brechas de seguridad que produjo el ciberataque mundial de Ransomware "Wannacry".

Horacio Gómez Rey[18], realiza un análisis sobre el ciberataque de ransomware Wannacry ocurrido a escala mundial el viernes 12 de mayo de 2017, dejando sistemas de hospitales, operadoras de telecomunicaciones, y demás empresas, inutilizados.

Desde el punto de vista de protección de datos y privacidad, sin profundizar en los detalles técnicos relativos a las vulnerabilidades aprovechadas por los atacantes para penetrar en los sistemas de multinacionales y otras entidades, este ciberataque ha tenido diversas consecuencias.

El nuevo RGPD, como se ha desarrollado anteriormente, contempla la obligatoriedad de notificar una brecha de seguridad [19]cuando la misma constituya un riesgo para los derechos y las libertades de las personas físicas, dentro de las primeras 72 horas desde que acontece.

Siendo necesario que se vean envueltos datos de carácter personal y que se derive un riesgo para los derechos y libertades de los interesados.

Pero, en el caso de este tipo de ataque cuyo objeto consiste en cifrar archivos y posteriormente pedir un rescate para descifrarlos, hay que cuestionarse si

[18] (Gómez Rey, H. Ecix group. Brechas de seguridad y ransomware wannycry, 2018)

estarían realmente en riesgo los derechos y libertades de las personas físicas, y por tanto se habría producido efectivamente una violación de la seguridad de los datos personales.

En primer lugar y para verificar que se cumplen los 2 requisitos que el reglamento exige se debe acudir a la definición de violación de la seguridad de los datos personales establecida en el mismo:

"Toda violación que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos".

En base a esto, se podría afirmar que se habría producido un acceso no autorizado a dichos datos, además de una comunicación de los mismos, y se habría producido el primer requisito de la notificación de la violación de seguridad de los datos.

El segundo requisito para que sea obligatorio notificar esta violación, es que existan riesgos en los derechos y libertades de los interesados. Se deberá considerar que una violación de la seguridad de los datos entraña un riesgo para los derechos y libertades de los interesados cuando, según el RGPD, pudiera provocar daños y perjuicios físicos, materiales o inmateriales, como los siguientes:

Usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización, aspectos personales referidos al rendimiento en el trabajo, y casos en los que el tratamiento implique gran cantidad de datos personales y afecten a gran número de interesados.

No obstante, varias Autoridades Nacionales de Protección de Datos a nivel europeo tienen desarrollados diversos criterios a tener en cuenta para valorar si las brechas de seguridad son susceptibles o no de notificación, estos son:

⇒ El potencial detrimento para los datos de los interesados (agravios en los datos personales), incluyendo el agravio emocional, físico y financiero. Algunas de las formas en las que este agravio puede manifestarse son, por ejemplo, la exposición al robo de identidad a través del lanzamiento de datos identificativos que no sean públicos, como por ejemplo sus circunstancias financieras.

La probabilidad de que esto ocurra dependerá del volumen de datos envueltos en la brecha de seguridad y de la sensibilidad de los mismos, ya que existen más probabilidades de que los derechos y libertades de la persona sean dañados cuando los datos envueltos en la brecha de seguridad son sensibles, es decir, son datos personales que revelan el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Por tanto, de acuerdo con estos criterios y en relación con la brecha de seguridad provocada por Wannacry, si hay datos personales envueltos en el ciberataque, la operadora de telefonía debe notificar está violación a la AGPD así como a los interesados (que son los propios afectados), siempre en caso de que los derechos y libertades se vean perjudicados.

A nivel técnico, el ransomware, en este caso concreto el WannaCry, infecta el sistema cifrando todos los archivos y utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, distribuyéndose al resto de sistemas Windows que haya en esa misma red.

En este ciberataque de magnitud mundial, los sistemas afectados fueron Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2012 and R2, Windows 10 y Windows Server 2016.

Las soluciones que se pusieron en marcha consistieron en el seguimiento, a través de la web del Centro Criptológico Nacional, de las recomendaciones y medidas a tomar, actualizar los sistemas a su última versión, parchear según informa el fabricante a través del canal disponible en su web y aislar de la red o apagar el equipo.

Otras soluciones adicionales ante este tipo de ciberataques son las de mantener los equipos y sistemas actualizados para reducir las vulnerabilidades, formar en materia de ciberseguridad a las personas que forman parte de la organización, y tener protocolos de actuación definidos tanto preventivos, como de actuación en caso de ciberataque, como más adelante se desarrollarán y profundizará en ellas.

2. Normativa en el ámbito de la Unión Europea.

Europol y El Centro Europeo sobre la cibercriminalidad (EC3).

Debido a la carencia de legislación a nivel internacional que aborde la problemática de los ciberdelitos, instituciones como Europol, como agencia de la Unión Europea en materia policial, tiene como principal objetivo contribuir a la consecución de una Europa más segura para beneficio de todos los ciudadanos de la UE.
Para ello, en enero de 2013 se ubicó en sus dependencias, por motivos logísticos y la orientación de su trabajo a la lucha, entre otros ámbitos, de la cibercriminalidad, el Centro Europeo sobre cibercriminalidad, más conocido como EC3. A continuación se enumeran las materias más importantes en las que enfocan su lucha y trabajo con excelentes resultados:

- Cibercriminalidad cometida por grupos organizados, en especial los que generan grandes beneficios por sus actividades ilícitas, tales como el fraude on-line.
- Cibercriminalidad que cause grave daño a las víctimas, como la explotación sexual de menores on-line.
- Cibercriminalidad, incluyendo ciberataques, que afecten a las infraestructuras críticas y a los sistemas de información en la Unión Europea.

El EC3 representa a la comunidad policial de la Unión Europea en áreas de interés común como el requerimiento de R&D, gobernanza de Internet y desarrollos legislativos.

SIRIUS, la nueva creación de Europol.

Julio San José[20] hace referencia a Sirius, como plataforma creada por Europol para facilitar las investigaciones de los ciberdelitos.
Se trata de una solución práctica e innovadora creada para abordar los desafíos actuales a los que se enfrenta la aplicación de la ley en las investigaciones en Internet.

A medida que los delincuentes adoptan el modelo del Crime-as-a-Service obtienen un acceso más sencillo a herramientas y servicios para la realización de actos delictivos y las autoridades policiales se enfrentan a un completo y complejo desafío cuando realizan las investigaciones online.

Para hacer frente a este desafío y apoyar mejor las investigaciones de los Estados miembros de la UE en Internet, Europol lanzó la plataforma SIRIUS en octubre de 2017.

SIRIUS es una plataforma web enfocada a los agentes de la ley de los distintos estados miembros que permite compartir conocimientos, prácticas y experiencias en el campo de las investigaciones de ciberdelitos, con un

[20] (San José, J. "Sirius, la plataforma de Europol para facilitar las investigaciones de los ciberdelitos"., s.f.)

enfoque especial en la lucha contra el terrorismo. Ofrece un enfoque innovador de colaboración al proporcionar a los investigadores una plataforma para intercambiar rápida y eficientemente conocimientos, manuales y consejos, así como herramientas para ayudarlos a analizar la información recibida por los diferentes proveedores de servicios en línea. La plataforma también aborda otros desafíos en las investigaciones criminales, como la racionalización de las solicitudes a los proveedores de servicios en línea y la mejora de la calidad del registro receptivo.

Su principal objetivo es fomentar el codesarrollo de herramientas y soluciones que pueden respaldar las investigaciones en Internet. Con este fin, Europol organizará una reunión bianual sobre el código en su sede de La Haya, que reunirá a expertos en aplicación de la ley y en programación informática para desarrollar conjuntamente herramientas y soluciones comunes.

Convenio de Budapest. Primer Tratado Internacional en Cibercriminalidad.

El Convenio sobre cibercriminalidad o Convenio de Budapest[21], creado el 23 de noviembre de 2001 en Budapest (Hungría) y firmado por 56 Estados, entró en vigor el 1 de julio de 2004 como el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet. España ratificó este convenio el 1 de octubre de 2010.

Sin embargo, existen otras tipologías no contempladas en este convenio que interesa observar cuando los medios empleados en su comisión son las nuevas tecnologías, dado el volumen y la importancia que han adquirido y su continuo auge.

En el capítulo II del Convenio se establecen las medidas que deben adoptarse a nivel nacional, promoviendo que cada parte adoptará las medidas legislativas

[21] (Convenio de Budapest. 2001, 2001)

y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Este convenio considera "fraude informático" a *la introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático con la intención dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.*

Informe sobre cibercriminalidad del Ministerio del Interior.

Este Informe data del año 2015[22] y muestra la realidad delictiva que gira en torno a la cibercriminalidad. La información estadística que se muestra y recopila en este documento es aquella delincuencia conocida y registrada por las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra y distintos Cuerpos de Policía Local), que figura en el Sistema Estadístico de Criminalidad (SEC).

Desde el punto de vista jurídico, la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal por parte de las Leyes Orgánicas 1/2015 y 2/2015, cuya vigencia tuvo lugar a partir del día 01 de julio del pasado año, vino a regular nuevos tipos penales en el ámbito de la cibercriminalidad. Este avance legislativo ha venido dado, entre otras cosas, por la adopción de la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

La reforma del Código Penal sobre cibercriminalidad abarca tipologías penales de muy variada índole, entre ellos, se encuentran los delitos de descubrimiento y revelación de secretos, (el ciberdelito llamado sexting), de daños informáticos, de pornografía infantil, delitos contra la propiedad intelectual,

[22] (Informe sobre criminalidad. Ministerio del Interior, 2015)

delitos de terrorismo y delitos de odio.

Además, España también ratificó el *Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*, entrando en vigor en España el 1 de abril de 2015.

Además de las conductas que introduce el Convenio de Budapest, que más adelante se desarrollará, este informe recoge que la realidad criminal denota la existencia de otras categorías distintas.
Cuando los medios empleados en su comisión sean las tecnologías de la información y la comunicación (TIC), se pueden encuadrar dentro de los delitos tecnológicos las otras conductas delictivas, teniendo en cuenta el volumen y la importancia de la cifra registrada, como son los delitos contra el honor y las amenazas y coacciones, más desarrollados en el capítulo 4.

A lo largo de la serie histórica de los años 2012-2015, se aprecia un incremento de la delincuencia comprendida dentro del concepto de cibercriminalidad. En concreto, durante el año 2015, se ha conocido un total de 60.154 hechos, de los cuales el 67,9% corresponde a fraudes informáticos como las estafas y el 16,8% a amenazas y coacciones. Las diferentes categorías mantienen el mismo orden cuantitativo jerárquico del pasado año, con la excepción de los delitos de falsificación informática, que este año superan en porcentaje a los delitos contra el honor.

En el periodo 2012 a 2015 se experimenta un incremento al alza, con la excepción de las detenciones e imputaciones que casi igualan los datos del pasado año.

El porcentaje de hechos esclarecidos alcanza la cifra de un 32,2% de los hechos conocidos en 2015.

De otro lado, las victimizaciones según grupo de edad y sexo, tras los registros consignados en el Sistema Estadístico de Criminalidad (SEC), se aprecia que en 2015, los datos por grupos de edad y sexo, sitúan con mayor proporción a

los varones respecto a las mujeres, con la excepción del grupo de edad de menores, ya que en este grupo las mujeres duplican en cifras a los del sexo masculino.

Según los distintos rangos de edad determinados en relación con las detenciones e imputaciones según grupo de edad y sexo, se distingue que la mayoría de los autores de estos ilícitos penales se encuentran englobados en el grupo de edad 26 a 40 años.

Del análisis de la relación de las diferentes tipologías delictivas por las que las personas han sido objeto de la detención/imputación se detecta que las estafas, amenazas, la pornografía de menores y descubrimiento y revelación de secretos han tenido mayor incidencia entre los detenidos/imputados de sexo masculino.
Además, se aprecia que las estafas, amenazas, injurias y usurpación de estado civil predominan entre los responsables de sexo femenino.

La mayoría de los detenidos/imputados por ciberdelincuencia son de nacionalidad española, concretamente un 85,7%.
Entre los detenidos/imputados de nacionalidad extranjera son los originarios de Rumanía, Marruecos, Colombia, y Nigeria los que aglutinan mayor número de casos.

El colectivo de los detenidos/imputados de 26 a 40 años realiza con mayor frecuencia los delitos de fraudes informáticos y amenazas y coacciones.

Convenio de Ciberdelincuencia del Consejo de Europa.

Este convenio[23] tiene como objetivos aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional debido a los profundos

[23] (Convenio de Ciberdelincuencia del Consejo de Europa, 2010)

cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas.

En relación con las medidas que deberán adoptarse a nivel nacional, establece en su artículo 2 “sobre el Acceso ilícito”, que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Por otro lado, en relación al “fraude informático”, establece que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Informe de 26 de julio de 2017 sobre la lucha contra la ciberdelincuencia. (2017/2068(INI)).

Este informe se basa en una serie de consideraciones generales a través de las cuales desarrolla un análisis sobre la lucha contra la ciberdelincuencia.

En relación con el Ransomware y ciberdelitos similares, destaca que el acusado aumento de los casos de secuestro de archivos para pedir rescate, de las redes de robots informáticos y de interferencia no autorizada en sistemas informáticos repercute en la seguridad de las personas, en la disponibilidad y la integridad de sus datos personales, así como en la protección de la privacidad, las libertades fundamentales y la integridad de las

infraestructuras críticas, incluidas, entre otras, el suministro de energía y electricidad y las estructuras financieras, como los mercados bursátiles.

Insiste en la necesidad de racionalizar las definiciones comunes de ciberdelincuencia, guerra cibernética, ciberseguridad, acoso cibernético y ciberataque, a fin de garantizar una definición jurídica común que compartan las instituciones y los Estados miembros de la Unión.

Subraya que la lucha contra la ciberdelincuencia debe consistir ante todo en proteger y reforzar las infraestructuras críticas y otros dispositivos conectados a la red, y no solo en ejecutar medidas represivas.

Reitera la importancia de las medidas jurídicas tomadas a nivel europeo con objeto de armonizar la definición de los delitos relacionados con ataques contra sistemas de información, así como con la explotación sexual de menores en línea, y obligar a los Estados miembros a establecer un sistema para el registro, la producción y la puesta a disposición de datos estadísticos sobre estos delitos a fin de combatirlos con mayor eficacia.

Insta a los Estados miembros que aún no lo hayan hecho a que transpongan y apliquen de manera rápida y adecuada la Directiva 2011/93/UE relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. Pide a la Comisión que controle estrictamente y garantice su aplicación plena y efectiva, y que informe de sus resultados de manera oportuna al Parlamento y a la comisión competente.
Destaca que debe dotarse a Eurojust y Europol de recursos suficientes para mejorar la identificación de las víctimas, luchar contra las redes organizadas de delincuentes sexuales y acelerar la detección, el análisis y la remisión de material sobre abuso infantil tanto en línea como fuera de línea.

Deplora que la mitad de las empresas de Europa hayan sufrido, al menos, un incidente de ciberseguridad y que los ciberataques contra empresas a menudo no se detecten o denuncien.
Recuerda que varios estudios estiman que los ciberataques tienen un coste significativo para la economía mundial; considera que la obligación de

comunicar las violaciones de la seguridad y de compartir información sobre los riesgos introducida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 contribuirá a atajar este problema al brindar apoyo a las empresas, en particular a las pymes.

Destaca que el carácter constantemente variable del panorama de ciberataques plantea a todas las partes interesadas graves problemas jurídicos y tecnológicos; considera que las nuevas tecnologías no deben considerarse una amenaza, y reconoce que los avances tecnológicos en materia de cifrado mejorarán la seguridad global de nuestros sistemas de información, por ejemplo, al permitir a los usuarios finales proteger mejor sus datos y comunicaciones; señala, sin embargo, que aún existen graves deficiencias en la seguridad de las comunicaciones y que técnicas como el «encaminamiento cebolla» (onion routing) y las redes ocultas pueden ser utilizadas por usuarios malintencionados, en especial por terroristas y autores de delitos sexuales contra menores, piratas informáticos patrocinados por terceros Estados no amistosos u organizaciones políticas o religiosas extremistas con fines delictivos, en concreto para ocultar sus actividades o identidades ilícitas, lo que dificulta sobremanera las investigaciones.

Expresa gran preocupación por el reciente ataque mundial con programas de secuestro de archivos para pedir rescate (Ransomware WannaCry anteriormente desarrollado), que parece afectar a decenas de miles de ordenadores de casi cien países y a numerosas organizaciones, incluido el Servicio Nacional de Salud (NHS) británico, la víctima de mayor relevancia de este ataque con código malicioso; reconoce, en este contexto, la importante labor de la iniciativa «No More Ransom» («no más pago de rescates»), que ofrece más de cuarenta herramientas de descifrado gratuitas que permiten a las víctimas de estos ataques en todo el mundo descodificar sus equipos afectados.

Subraya que las redes ocultas y la Red Thor también ofrecen un espacio libre para que periodistas, activistas políticos y defensores de los derechos humanos de determinados países puedan evitar la detección por parte de autoridades estatales represoras.

Observa que el recurso por parte de redes delictivas y terroristas a instrumentos y servicios de ciberdelincuencia sigue siendo escaso; destaca, no obstante, que esta situación probablemente cambie, en vista de los nexos crecientes entre el terrorismo y la delincuencia organizada y la amplia disponibilidad de armas de fuego y precursores de explosivos en las redes ocultas.

Condena rotundamente toda interferencia del sistema acometida o dirigida por un país extranjero o por sus agentes con el fin de perturbar el proceso democrático en otro país.

Subraya que las peticiones transfronterizas de intervención de nombres de dominio, retirada de contenidos y acceso a los datos del usuario plantea grandes desafíos que exigen medidas urgentes, habida cuenta de lo mucho que está en juego; destaca, en este contexto, que los marcos internacionales en materia de derechos humanos, que se aplican en línea y también fuera de línea, representan un importante hito a escala mundial.

Pide los Estados miembros que velen por que las víctimas de ciberataques personales puedan disfrutar plenamente de todos los derechos consagrados en la Directiva 2012/29/UE, y que doblen sus esfuerzos en relación con la identificación de víctimas y los servicios centrados en las víctimas, también mediante el apoyo continuado al grupo de trabajo sobre identificación de víctimas de Europol; pide asimismo a los Estados miembros que, en cooperación con Europol, creen con carácter de urgencia plataformas conexas a fin de garantizar que todos los usuarios de internet sepan cómo pedir ayuda en caso de ser objeto de actividades ilegales en línea; pide a la Comisión que elabore un estudio relativo a las implicaciones de la ciberdelincuencia transfronteriza sobre la base de la Directiva 2012/29/UE.

Subraya que la evaluación iOCTA de 2014 de Europol alude a la necesidad de contar con instrumentos jurídicos más eficientes y eficaces, teniendo en cuenta las actuales limitaciones del proceso del tratado de asistencia judicial mutua (MLAT, por sus siglas en inglés), y defiende una mayor armonización de la legislación en la Unión, cuando proceda.

Destaca que la ciberdelincuencia socava gravemente el funcionamiento del mercado único digital, en la medida en que mina la confianza en los prestadores de servicios digitales, compromete las transacciones transfronterizas y perjudica gravemente los intereses de los consumidores de servicios digitales.

Hace hincapié en que las estrategias y medidas en materia de ciberseguridad solo serán adecuadas y eficaces si se basan en los derechos y libertades fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión y en los valores fundamentales de la Unión.

Insiste en la acuciante y legítima necesidad de proteger las comunicaciones entre particulares y entre particulares y entidades públicas y privadas, con el fin de evitar la ciberdelincuencia; destaca que un cifrado sólido puede contribuir a satisfacer esta necesidad; hace hincapié, asimismo, en que limitar el uso o debilitar la fortaleza de las herramientas criptográficas creará vulnerabilidades que podrán explotarse con fines delictivos, y reducirá la confianza en los servicios electrónicos, lo que, a su vez, dañará por igual a la sociedad civil y a la industria.

Pide un plan de acción para la protección de los derechos de la infancia en el ciberespacio, tanto en línea como fuera de línea, y recuerda que las fuerzas de seguridad deben prestar especial atención a los delitos contra menores en el marco de la lucha contra la ciberdelincuencia; resalta a este respecto la necesidad de reforzar la cooperación judicial y policial entre los Estados miembros y con Europol y su Centro Europeo de Ciberdelincuencia (EC3) para prevenir y combatir la ciberdelincuencia, en particular, la explotación sexual de menores en línea.

Insta a la Comisión y a los Estados miembros a poner en marcha todas las medidas jurídicas necesarias para luchar contra el fenómeno de la violencia en línea contra las mujeres y el ciberacoso; pide a la Unión y a los Estados miembros, en particular, que aúnen fuerzas para crear un marco de delitos penales que obligue a las empresas de internet a eliminar el contenido ofensivo, degradante y humillante, o a poner fin a su divulgación; pide asimismo que se prevea apoyo psicológico para mujeres víctimas de violencia en internet y para niñas objeto de ciberacoso.

Y por último, destaca que los contenidos ilícitos en línea deben ser eliminados sin demora con las debidas garantías procesales; hace hincapié en el papel que desempeñan las tecnologías de la información y la comunicación, los prestadores de servicios en internet y los proveedores de alojamiento en internet a la hora de garantizar la eliminación rápida y eficiente de contenido ilegal en línea a petición de las fuerzas de seguridad competentes.

3. Guías nacionales e internacionales.

Instituto Nacional de Ciberseguridad de España. INCIBE.

El Instituto Nacional de Ciberseguridad de España (INCIBE) es una sociedad dependiente del Ministerio de Energía, Turismo y Agenda Digital, a través de la Secretaría de Estado y para la Sociedad de la Información y Agenda Digital (SESIAD).
Es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

El CERT de Seguridad e Industria es el centro de respuesta a incidentes de ciberseguridad operado por INCIBE. Trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, aumentar la ciberresiliencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo.

La misión de INCIBE es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.

La visión de INCIBE es conseguir sus objetivos mediante el compromiso de profesionales altamente cualificados, comprometidos con sus proyectos y capaces de generar valor e innovación de forma continua.
La dinamización del sector TIC, desde una perspectiva de igualdad de oportunidades, generando nuevos negocios y oportunidades para clientes, proveedores y profesionales.
El soporte a los ciudadanos, empresas, administraciones, RedIRIS junto con sus instituciones afiliadas y sectores estratégicos, todos ellos claves para un desarrollo de las nuevas tecnologías con un alto impacto social.
Y la generación de inteligencia en ciberseguridad como medio necesario para el desarrollo de tecnologías y conocimiento a aplicar en nuevas herramientas y estrategias.

Todo esto llevado a cabo con transparencia y excelencia, tanto en la aptitud y en la actitud de sus profesionales, así como en la ejecución de los proyectos. Con vocación de servicio público. Mantenimiento del espíritu innovador y de la

búsqueda de la excelencia en los proyectos que se abordan, maximizando el valor ofrecido. Con la sostenibilidad como valor ético y criterio de desempeño que involucra los aspectos económicos, sociales y medioambientales de la actividad. Y con un espíritu de integración, apoyo y cooperación con todos los agentes relevantes en ciberseguridad, reforzando las capacidades nacionales en seguridad.

Control Objectives for Information and related Technology. COBIT.

Autores como Sue Milton[24], Joanne Karczewska[25] y Francisco Cuesta Martínez[26], hacen una aproximación desde distintos puntos de vista y ámbitos donde el marco de trabajo COBIT se aplica y se desarrolla.
COBIT (Control Objectives for Information and related Technology) es un framework o marco de trabajo de buenas prácticas para el gobierno de las tecnologías de la información que proporciona un conjunto de herramientas de apoyo a los gestores de dichas tecnologías (TI).
La aplicación de COBIT garantiza el cumplimiento de las normativas del sector y aumenta la eficiencia y eficacia de las TI, ya que integra procesos y recursos de otros estándares y metodologías como ITIL y algunas normas ISO.
De este modo, ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI, un elemento que juega un papel de vida o muerte para las empresas.

COBIT Tiene una orientación hacia el proceso y un fuerte enfoque en el control más que en la ejecución. Para lograr los objetivos, COBIT ayuda a saber el qué, más que el cómo.

Fue creado por ISACA (Information Systems Audit and Control Association) y por el ITGI (IT Governance Institute). Sus ediciones han sido:

[24] (Milton, S. Cómo Cobit 5 puede ayudar a reducir la probabilidad y el impacto de las 5 amenazas cibernéticas más importantes"., s.f.)
[25] (Karczewska, J. Cobit 5 y el Reglamento General de Protección de Datos., s.f.)
[26] (Cuesta Martínez, F. Cobit 5, marco de negocio para la seguridad de la información., s.f.)

1. “Auditoría” [COBIT1] en el 1996.
2. “Control” [COBIT2] en el 1998.
3. “Administración” [COBIT3] en el 2000.
4. “Gobierno de TI” [COBIT4] en el 2005 (con una nueva versión en el 2007, COBIT 4.1.
5. “Gobierno Corporativo de TI” [COBIT5] en el 2012.

La nueva versión, “Un marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa”, amplía la anterior e incorpora las últimas ideas en técnicas de gestión y gobierno empresarial, además de proporcionar nuevos principios, prácticas, herramientas y modelos ampliamente aceptados para incrementar el valor de las TI en la organización.

Para entender en qué ayuda COBIT y cuál es su enfoque es interesante conocer los cinco principios por los que se rige. Estos son, satisfacer las necesidades de los stakeholders, cubrir la organización en todos sus ámbitos, aplicación de un framework único e integrado, habilitar un enfoque holístico y separación entre el gobierno y la gestión.

COBIT 5 y el reglamento RGPD 2016/679 del Parlamento Europeo y el Consejo del 27 de abril de 2016, sobre la protección de personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

La autora Joanna Karczewska[27] lleva a cabo el análisis de este reglamento, vigente desde el 25 de mayo de 2018, con el objetivo de contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, así como contribuir al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, y al bienestar de las personas físicas.
Por lo que respecta a la tecnología de la información involucrada en las

[27] (Karczewska, J. Cobit 5 y el Reglamento General de Protección de Datos., s.f.)

organizaciones europeas, es conveniente el marco COBIT para encontrar inspiración adicional en relación con el gobierno y gestión de TI empresarial (GEIT).

El Reglamento RGPD requiere que el responsable del tratamiento implemente las políticas de protección de datos apropiadas.

Cuando se desarrollan nuevos procedimientos relativos al tratamiento de datos personales o se revisan los actuales, las buenas políticas, como se recomienda en el marco de COBIT 5, deben ser efectivas, para alcanzar el fin establecido, eficientes, para garantizar que los principios del reglamento RGPD se implementen en la forma más eficaz y no invasivas, es decir, que resulten lógicas para quienes deben cumplirlas y que no tendrían que crear una resistencia innecesaria.

Además, debe haber un mecanismo para proporcionar un fácil acceso a esas políticas a todas las partes interesadas, y las partes interesadas deberían saber dónde encontrar esas políticas.

En cuanto a la seguridad, el artículo 32 del reglamento RGPD establece que los responsables y encargados del tratamiento deben garantizar implementando las medidas técnicas y organizacionales necesarias teniendo en cuenta las últimas innovaciones disponibles; los costes de implementación; y la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos de distinta probabilidad y gravedad para los derechos y las libertades de las personas físicas. Estas medidas deberían incluir el uso de seudónimos y el cifrado de los datos personales, la capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y los servicios de tratamiento operativos, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de que ocurra un incidente físico o técnico y un proceso para llevar a cabo de forma regular la evaluación, la prueba y el análisis de la eficacia de las medidas técnicas y organizacionales para garantizar la seguridad del tratamiento.

Otro cybersecurity framework. NIST.

Autores como David Eduardo Acosta[28] hacen referencia a NIST, como Marco de Trabajo de Ciberseguridad (NIST Cybersecurity Framework) que garantiza la gestión coordinada de los controles de seguridad de forma óptima, escalable e integrable, aprovechando lo mejor de cada uno de los marcos de trabajo (como COBIT, ISO, etc.) así como las mejores prácticas y metodologías de la industria y la experiencia de cientos de voluntarios para establecer una línea de trabajo consistente y práctica que aborde los riesgos de ciberseguridad actuales.

Los objetivos de NIST, en relación con las amenazas y ataques que sufren las infraestructuras críticas son:

1. Identificar estándares de seguridad y guías aplicables de forma trasversal a todos los sectores de infraestructuras críticas
2. Establecer un lenguaje común para gestionar riesgos de ciberseguridad
3. Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio
4. Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos
5. Establecer criterios para la definición de métricas para el control del desempeño en la implementación
6. Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad
7. Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares

[28] (Acosta David, E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST., s.f.)

8. No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.

Amenazas y ataques a infraestructuras críticas.

Una infraestructura crítica se define como un activo, sistema o parte localizados en los Estados miembros esencial para mantenimiento de funciones sociales vitales, salud, seguridad, económico o social de las personas, y su interrupción o destrucción tendría un impacto significativo en el Estado miembro donde ocurra, como resultado de la falta de mantenimiento de esas funciones.

Cuando se producen ataques en infraestructuras críticas, se suelen producir por sofisticados ataques en vulnerabilidades que aparecen en los sistemas de control industrial (ICS) y control de supervisión y sistemas de adquisición de datos (SCADA) en empresas como las centrales eléctricas y la industria pesada.

El ataque de WannaCry de mayo de 2017 anteriormente explicado es un excelente ejemplo de esto, hospitales paralizados en el Reino Unido, perturbación en las redes ferroviarias de Alemania y Rusia, empresas de telecomunicaciones en España y Portugal, empresas petroquímicas en China y Brasil, etc.
Cabe destacar el número creciente de ataques de ransomware contra hospitales, instituciones y compañías de transporte, causando interrupciones serios agravios para los usuarios.
Los ataques más comunes contra las infraestructuras críticas en la Unión Europea eran los ataques DDoS.

ISO 27001 en el ámbito de las organizaciones y empresas.

Agustín López Neira[29] y Javier Ruiz Spohr[30] hacen referencia a ISO 27001 en el ámbito de las organizaciones y empresas.

[29] (López Neira, A. Ruiz Spohr, J. "ISO 27000"., s.f.)
[30] (López Neira, A. Ruiz Spohr, J. "ISO 27000"., s.f.)

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.
Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada, esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

Una de las mayores ventajas de ISO 27001 es que las empresas pueden certificarse por ella, esto significa que una empresa puede demostrar a sus clientes, socios, accionistas, agencias gubernamentales y otros que pueden mantener su información segura.

Existen diferentes estándares incluidos en la familia de ISO 27000, entre ellos:

ISO 27000 que contiene el vocabulario en el que se apoyan el resto de normas. Es similar a una guía/diccionario que describe los términos de todas las normas de la familia.

ISO 27001 es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar.

ISO 27002 se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles.

ISO 27003 es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

ISO 27004 describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.

ISO 27005 es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.

ISO 27006 es un conjunto de requisitos de acreditación para las organizaciones certificadoras.

ISO 27007 es una guía para auditar SGSIs. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

4. Problemas al aplicar los diferentes tipos de legislación.

En el ámbito del cibercrimen y los ciberdelitos se plantea una dificultad común al resto de ciberproblemas que se pueden dar en internet.
Es un ciberproblema que afecta a las personas y empresas en el ciberespacio, para el cual no existe un ordenamiento jurídico aplicable, ni existe un tribunal competente capacitado para juzgar los actos cometidos.
Los ciberdelitos no tienen un lugar claro y territorial donde se producen, por este motivo con los ordenamientos jurídicos actuales no se puede actuar con eficacia.

Con todo, esta ciberconducta puede ser perseguible en aquellos ordenamientos en los que se pueda identificar un lugar de origen de la conducta y un autor.
En los casos de Ransomware, esta conducta se ha tipificado como un delito de estafa (artículo 248 y siguientes del Código Penal) en concurso con un delito de daños informáticos (artículo 264 del Código Penal), entre otros, como anteriormente se ha desarrollado.

Pero de cara al futuro se deben superar las barreras territoriales que condicionan a los ordenamientos jurídicos a aplicarse a un territorio concreto delimitado por fronteras físicas.

Las dificultades que enfrentan las fuerzas del orden que operan legalmente en la *deep web* es evidente, con muchas jurisdicciones restringidas por su legislación nacional. Se necesita un enfoque armonizado en este aspecto en toda la Unión Europea, que existan unos estándares de seguridad para aquellos sistemas operativos que manejan sistemas e infraestructuras críticos, transportes, redes eléctricas o tráfico aéreo.

Por lo tanto, es necesario contar con disposiciones destinadas a proteger las infraestructuras y la seguridad de la red y de los sistemas de información para alinear y centrar las capacidades de seguridad cibernética en todos los Estados miembros de la Unión Europea y garantizar intercambios eficientes de información y cooperación.

CAPÍTULO 3: Perfil de las víctimas del delito.

1. PERFILES DE RIESGO.

   - CÓMO AFECTA A LOS USUARIOS Y A LOS ENTORNOS CORPORATIVOS.

2. CONSECUENCIAS Y RECOMENDACIONES.

3. ACCIONES QUE SE OFRECEN A NIVEL POLICIAL.

   - INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA).

4. PROTECCIÓN.

   - PRODUCTOS ANTIMALWARE.

1. Perfiles de riesgo.

Cómo afecta a las empresas y entornos corporativos.

ESET Latinoamérica[31] hace referencia a cómo afecta el Ransomware a las empresas y a los entornos corporativos.

Partiendo de que la información es un activo muy valioso para las empresas, si se compromete su disponibilidad puede implicar grandes y negativas consecuencias. Esta es la principal razón por la cual muchos ataques de ransomware están orientados a infectar archivos e información de empresas y corporaciones.

Asimismo, la mayoría de las empresas trabajan con redes compartidas de información, lo que hace que una infección pueda propagarse rápidamente a través de la red, infectando no solo las estaciones de trabajo de los empleados, sino también los servidores y bases de datos de la compañía, donde muchas veces se aloja la información crítica y sensible.

Existen determinados riesgos específicos a tener en cuenta: En primer lugar, tenemos que mencionar las pérdidas financieras, particularmente en casos donde la información que se pierde está compuesta de datos privados de clientes a quienes se debe resarcir y/o indemnizar de alguna manera. En el mismo sentido, si los archivos afectados son patentes o fórmulas de ciertos productos, esto podría derivar en la interrupción completa o parcial del negocio.

En esta misma línea, hay compañías que concentran su trabajo en servidores en la nube, y si estos resultan infectados y no se cuenta con un plan de continuidad para seguir trabajando fuera de línea, el correcto funcionamiento del negocio también se verá afectado.

El riesgo a la marca también compromete directamente el prestigio, la solidez y hasta credibilidad de una compañía.
Aunque es difícil de medir el dinero neto que podría perderse, sí puede verse

[31] (Eset Latinoamerica. 2015, s.f.)

en la percepción de los usuarios o clientes, ya que, si pierden la confianza en la marca, recuperarla es muy complicado.

Por otro lado, está el tema de la responsabilidad legal y las obligaciones que tiene una compañía en base a cómo son las leyes de protección de datos en los países donde opera.

En caso de perder información, se deben pagar multas e indemnizaciones a quienes resulten víctimas del ataque por los daños y consecuencias negativas que el ataque pueda desencadenar.
Aunque no es recomendable pagar el rescate, muchas veces resulta más perjudicial la pérdida de la información que ceder ante al atacante.

En el caso de las empresas, no solo deben considerar el valor en sí de la información que se perdió o ya no está disponible, sino también los costes indirectos que son muchas veces mayores y que implican detener las operaciones, no proporcionar los servicios, demorar las actividades o cualquier otra consecuencia que afecte la continuidad del negocio.

Todo esto se produce mediante el recurso a las técnicas de ingeniera social. Se trata de técnicas mediante las cuales el ciberdelincuente realiza un reconocimiento, establecimiento, contacto, confianza y manipulación para obtener su objetivo, es decir, el infectar el sistema de la víctima.

En el caso de las empresas y corporaciones, el primer paso es intentar reunir toda la información posible sobre la empresa que le pueda ser útil para conocer a su víctima, información como listados de empleados y teléfonos, departamentos, ubicación, proveedores, etc.

A continuación, selecciona a una víctima, que suele ser un empleado o algún colaborador de la empresa, y trata de establecer una relación que le permita ganarse su confianza utilizando la información obtenida, como su banco de confianza, la empresa de mantenimiento informático, una situación particular, etc.

Una vez se ha ganado su confianza, manipula a su víctima para obtener la información que necesita. Esta información puede ser en forma de credenciales, información confidencial, etc., o conseguir que realice alguna acción por él como instalar un programa, enviar algunos correos, hacer algún ingreso, etc.

Estas técnicas para conseguir la confianza y manipular a la víctima son diversas y se aprovechan del respeto a la autoridad, cuando el atacante se hace pasar por un responsable o por un policía; de la voluntad de ser útil, ayudar o colaborar que se aprecia en entornos laborales y comerciales; del temor a perder algo, como en los mensajes que tienes que hacer un ingreso para obtener un trabajo, una recompensa, un premio, etc.; de la vanidad, cuando adulan a la víctima por sus conocimientos, su posición o sus influencias; apelando al ego de los individuos al decirles que ha ganado un premio o ha conseguido algo y que para obtenerlo tienen que realizar una acción que en otro caso no harían o creando situaciones de urgencia y consiguiendo los objetivos por pereza, desconocimiento o ingenuidad de la víctima.

Por último, tras conseguir su objetivo se apartan sin levantar sospechas. En ocasiones destruyen las pruebas que puedan vincularles con alguna actividad delictiva posterior que ejecuten con la información obtenida, como por ejemplo accesos no autorizados si obtiene credenciales, publicación de información, etc.

Cómo reconocer un ataque de ingeniería social

Para evitar el ransomware, o cualquier tipo similar de ataque realizado mediante ingeniería social, hay que desconfiar de cualquier mensaje recibido por correo electrónico, SMS, WhatsApp o redes sociales en el que se le coaccione o apremie a hacer una acción ante una posible sanción.

Como pautas generales, para evitar ser víctima de fraudes de tipo ransomware es recomendable no abrir correos de usuarios desconocidos o que lo hayan solicitado, lo mejor es eliminarlos directamente y no contestar en ningún caso

a estos correos.
Revisar los enlaces antes hacer clic, aunque sean de contactos conocidos.
Desconfiar de los enlaces acortados o utilizar algún servicio para expandirlos antes de visitarlos.
Desconfiar de los ficheros adjuntos, aunque sean de contactos conocidos.
Es muy importante tener siempre actualizado el sistema operativo y el antimalware, y en el caso del antimalware compruebar que está activo.
Por último, hay que asegurarse de que las cuentas de usuario de los empleados utilizan contraseñas robustas y no tienen permisos de administrador.

Las políticas de Backpus empresarial.

Antes de comenzar con el proceso de backup es fundamental determinar qué información será respaldada, ya que no toda la información posee el mismo valor.

Esto se puede lograr valorando los datos y estableciendo cuáles tienen mayor relevancia según las preferencias personales, el tipo de trabajo que se haga con dichos datos, o incluso el objetivo o utilidad que tengan.
Existen tres aspectos que deben ser analizados a la hora de clasificar la información y establecer una política de backup.

Criticidad, que consiste en determinar qué información es importante respaldar. Tener en cuenta toda la información que utiliza la empresa diariamente para funcionar, así como también aquella que debe conservar para futuras consultas. Es importante entender que realizar un backup requiere un coste y esfuerzo, por lo que es importante determinar cuál es la información que realmente vale la pena resguardar.

Periodicidad, no se puede perder de vista la frecuencia con la cual se modifican los datos. Existe información dinámica e histórica y es importante entender la diferencia entre cada una para determinar cada cuanto tiempo se realizará el resguardo de información. Existen diferentes tipos de backup: Completo, Diferencial o Incremental. Cada uno tiene sus beneficios en cuanto a coste,

esfuerzo y periodicidad, por lo que es recomendable saber cada cuanto se requiere resguardar la información para elegir el que mejor se ajuste a las necesidades.

Medio, es el tipo de soporte que se elija para resguardar la información, como un disco rígido, cintas, medios ópticos, la nube, etc., dependerá de la cantidad de información que deba guardar, la periodicidad con la que se haga el backup y de la accesibilidad que se requiera. Además, se debe considerar que el espacio físico en donde se guarde el soporte de respaldo también debe estar protegido.

Factores de propagación.

Las formas de propagación del ransomware son muy similares a las de cualquier otro archivo malicioso.

Los vectores de infección más comunes son los mensajes engañosos de correo electrónico.
Un método típico de infección de ransomware es a través de un correo electrónico falso, que habitualmente asegura provenir de una empresa conocida, una entidad bancaria o una agencia gubernamental. Estos correos engañan al usuario para lograr que descargue un archivo, ya sea adjunto en el correo o a través de un link a la web.
Estos archivos maliciosos suelen ser troyanos que aparentan ser documentos de texto o imágenes inofensivas, pero al abrirlos descargan el ransomware que finalmente bloquea el equipo o los archivos del usuario. Por esta razón, siempre se recomienda no abrir archivos adjuntos ni ingresar a links de correos electrónicos desconocidos o no esperados.

También son vectores de propagación importantes las descargas de archivos en redes p2p o sitios de software pirata.
Muchos de estos sitios o archivos prometen software gratuito o cracks para evadir verificaciones de licenciamiento. Sin embargo, lejos de ser gratuitos,

pueden infectar el equipo del usuario para obtener algún tipo de rédito económico, por ejemplo, mediante el pago de un rescate. Asimismo, este tipo de programas suele solicitar que se deshabilite la protección antivirus, por lo que les resulta aún más sencillo infectar el equipo. En ambos casos, ya sea a través de un correo electrónico falso o una página maliciosa, el atacante requiere de la intervención del usuario para descargar y ejecutar el archivo malicioso, y para lograr engañarlos se vale de la ingeniería social. Por lo tanto, la precaución y educación en seguridad informática es clave ante estos casos.

Sin embargo, también existen muchos códigos maliciosos que se propagan por sí mismos, sin la intervención del usuario, aprovechando las vulnerabilidades de los sistemas o aplicaciones que no se encuentran actualizados.

Muchas variedades de ransomware traen consigo un exploit que aprovecha dichas vulnerabilidades para poder ejecutar el código en el equipo, copiar así el ransomware y ejecutarlo.
En estos casos, es muy común la propagación a través de equipos vulnerables conectados en la misma red. Cuando el código malicioso logra infectar uno de los sistemas, automáticamente comienza a reproducirse en los demás equipos expuestos.

Este fue el caso de la familia WannaCryptor, explicado con anterioridad, que utilizaba un exploit conocido como *EternalBlue* para explotar una vulnerabilidad en el protocolo SMB, es decir, de archivos compartidos, que permitía la ejecución de código en un equipo remoto.
De esta forma, el ransomware lograba copiarse y ejecutarse a través del puerto 445 por todas las máquinas vulnerables conectadas a la red. Otras variantes de ransomware, como *Reveton*, utilizaban una vulnerabilidad de Java para explotar los navegadores que se conectaban a una página web infectada y ejecutar el código que bloqueaba el equipo.
Es por esto por lo que mantener los sistemas actualizados constantemente puede evitar infecciones.

2. Consecuencias y recomendaciones-

Los ataques de Ransomware contra empresas están creciendo porque los cibercriminales saben que las organizaciones tienen más posibilidades de pagar debido a que los datos afectados suelen ser más sensibles y vitales para su continuidad. Además, puede que a veces sea más caro restaurar los datos mediante copias de seguridad que pagando el rescate.

El ransomware es muy fácil de monetizar. Más allá de infección inicial, todo lo que el atacante tiene que hacer es cobrar el rescate, y mediante el uso de monedas como Bitcoin, el lavado y su monetización es muy simple.

Además, la naturaleza del ataque de ransomware implica que pueda llegar a muchos objetivos y puntos de información en los que el ciberdelincuente esté interesado una vez ha penetrado en el sistema.

Las víctimas son diversas, desde objetivos financieros habituales, hasta entidades como hospitales, instituciones, Gobiernes, infraestructuras críticas y servicios.

La población en general también es su objetivo, las pequeñas y medianas empresas, que a menudo carecen de los recursos para salvaguardar sus datos y redes, también son objetivos clave.

El éxito y la demanda de ransomware experimentó un aumento del 750% de 2015.
El modelo de negocio para ransomware también ha evolucionado. Los desarrolladores de los primeros tipos de ransomware lo produjeron para su propio uso, pero ahora variantes como *Satan o Shark* se pueden ejecutar como programas de afiliación, proporcionando ransomware-as-a-service.

El aumento en el ransomware también se refleja en los informes de este año, ya que en casi todos los Estados miembros informan sobre el crecimiento de los casos de Ransomware.

A lo largo de 2016, las amenazas emergentes destacaron en comparación con el informe del año anterior. *Locky y Cerbe* son los ransomwares más utilizados.

Otros ransomwares, como *CTB-Locker, Cryptowall, Crysis, Teslacrypt, Torrentlocker y Zepto* también fueron reportados, pero estos aparecen localizados en países específicos.

Recomendaciones.

En caso de ser víctimas de un ciberataque de Ransomware, hay que mantener el sistema operativo y el software actualizado en todo momento. Asegurarse de que el software antivirus está activo y también se mantiene hasta la fecha.
Comprobar cuidadosamente antes de abrir archivos adjuntos ya que pueden contener el malware.

Es vital hacer copias de seguridad de manera regular en los sistemas y almacenarlos en un lugar seguro, preferiblemente fuera de línea.

Reportar el incidente a la policía y llamar a un experto para eliminar el malware o buscar consejo en la web de los proveedores de seguridad de confianza.

3. Acciones que se ofrecen a nivel policial.

Dentro de las normas básicas de seguridad que se ofrecen para los usuarios, destaca la confidencialidad de la información como factor fundamental.

1. Se debe proteger la información propia o confiada a terceros, evitando su envío no autorizado al exterior mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

2. Se debe guardar, por tiempo indefinido, la máxima reserva en cuanto a los datos, documentos, metodologías, claves, análisis, programas y demás información a la que se tenga acceso.

3. En el caso de entrar en posesión de información que no sea de difusión pública, en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

4. Los usuarios sólo pueden acceder a aquella información para la que tienen permisos explícitos, en función de las labores que desempeñan, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no tengan autorización.

5. Todos los soportes de información que vayan a ser reutilizados o causen baja por cualquier motivo, deberán antes ser tratados para eliminar la información que contienen, de manera que resulte imposible su recuperación.

6. Los usuarios precisan disponer de un único acceso autorizado (identificador de usuario y contraseña o tarjeta criptográfica con certificado digital) y son responsables de toda actividad relacionada con el uso de su acceso autorizado.

7. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista o al alcance de terceros.

8. Los usuarios no deben dejar su tarjeta criptográfica sin custodia o prestarla a terceros.

9. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

10. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y comunicar la correspondiente incidencia de seguridad.

11. Si un usuario pierde su tarjeta criptográfica debe comunicarlo de modo inmediato.

12. Los usuarios deben utilizar contraseñas seguras: Las contraseñas han de tener un tamaño mínimo de 8 caracteres y se recomienda que incluyan algún carácter especial (tipo @, #, +, etc.) que las protejan en mayor grado contra ataques. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables al usuario

(nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

Las contraseñas deberán cambiarse, siguiendo requerimientos del sistema informático, a intervalos de tiempo establecidos (como máximo cada 45 días y en intervalos no inferiores a 15 días).

Los usuarios serán responsables de toda acción realizada en los sistemas informáticos con su usuario de sistema o tarjeta criptográfica y certificado digital, por lo que deberán procurar que nadie conozca sus contraseñas.

13. El usuario debe desconectarse de todas las sesiones con aplicaciones antes de apagar su equipo o impresora, no dejando a la vista documentos que puedan contener datos de carácter reservado o personal.

Internet Organised crime threat assessment. (IOCTA). Evaluación de la Amenaza de Delincuencia Organizada de Internet.

La evaluación de la amenaza de delincuencia organizada de Internet (en adelante, IOCTA) del año 2017[32] fue elaborada por un equipo de analistas estratégicos de Europol con contribuciones de los Estados miembros, el cibercrimen de la Unión Europea Taskforce (EUCTF), los proyectos de análisis de Europol, Cyborg, Terminal y Twins, así como el equipo de Cyber Intelligence y el equipo SOCTA, a través de encuestas estructuradas, entrevistas y talleres moderados. Esto se ha mejorado con investigación de fuentes abiertas e información del sector privado, incluida la Recomendación de EC3 Grupos, Eurojust, ENISA, CERT-EU, el EBF y la comunidad CSIRT. Estas las contribuciones han sido esenciales para la producción del informe.

La Evaluación de la Amenaza de Delincuencia Organizada de Internet (IOCTA) es producida por Centro Europeo de Ciberdelincuencia (EC3) en Europol. Su objetivo es informar a los tomadores de decisiones a nivel estratégico,

[32] (Guía IOCTA 2017, 2018)

político y táctico en la lucha contra el delito cibernético, para dirigir el enfoque operativo para la aplicación de la ley de la UE.

La IOCTA 2017[33] contribuye al establecimiento de prioridades para la acción operativa de 2018 en las tres subáreas de la prioridad del cibercrimen: ciberataques, fraudes y explotación sexual infantil en línea, así como otros delitos.

La IOCTA 2017[34] enfoca las tendencias y desarrollos relativos a las áreas de los determinados ciberdelitos.

Además, el informe trata otros temas transversales que influyen o afectan en el ámbito de los ciberdelitos, como el uso delictivo de la Deep Web y la ingeniería social.

El informe también examina algunos de los desafíos comunes para la correcta aplicación de la ley. Este informe proporciona una actualización sobre las últimas tendencias y el impacto actual del cibercrimen dentro de Europa. Cada capítulo proporciona una visión general sobre la aplicación de la ley, las amenazas y el desarrollo del cibercrimen, basado en las experiencias de los investigadores de los delitos cibernéticos y su funcionamiento en otros sectores. Se basa en aportaciones de socios procedentes de la industria privada y académica.
Los informes buscan resaltar los riesgos futuros y las amenazas emergentes y proporcionar recomendaciones para alinear y fortalecer los esfuerzos conjuntos de la UE en la aplicación de la ley y sus socios en la prevención y lucha contra el cibercrimen.

La oficina de Coordinación Cibernética (OCC).

La OCC[35] es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad. Depende funcionalmente de la Secretaría de

[33] (Guía IOCTA 2017, 2018)
[34] (Guía IOCTA 2017, 2018)
[35] (Oficina de Coordinación Cibernética. , 2018)

Estado de Seguridad y orgánicamente del CNPIC (Centro Nacional de Protección de Infraestructuras Críticas).

Proporciona las capacidades de coordinación técnica entre el CERTSI y los órganos subordinados de la Secretaría de Estado de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado en lo que respecta a las competencias propias del Ministerio del Interior en el campo de la ciberseguridad y mantiene personal técnico permanentemente integrado en la estructura del CERTSI.

El CERT de Seguridad e Industria (CERTSI_).

El CERT[36], es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Industria, Energía y Turismo y del Ministerio del Interior. Por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015, el CERTSI_ es el CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas.

Operado técnicamente por INCIBE (Instituto Nacional de Ciberseguridad), y bajo la coordinación del CNPIC e INCIBE, el CERTSI_ se constituyó en el año 2012 a través de un Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado.

4. Protección.

Productos antimalware.

Se trata de herramientas destinadas a la protección de sistemas informáticos, independientemente de que sean servidores, ordenadores, tablets,

[36] (Capacidad de respuesta a incidentes de seguridad de la información del MIET, 2018)

smartphones o cualquier otro dispositivo, frente a cualquier tipo de software malicioso, comúnmente conocido como malware, que pudiera afectarles, es decir, estas herramientas detectan y eliminan aquellas aplicaciones o archivos que identifica como malware[37].

El software malicioso tiene como objetivo dañar o modificar el dispositivo para controlarlo o robar la información. Para tratar de infectarlo, los ciberdelincuentes harán uso de multitud de técnicas, como la ingeniería social y utilizarán distintas vías de entrada, como páginas web, correos electrónicos con archivos adjuntos, dispositivos de almacenamiento, etc. Existen diversos tipos de productos antimalware:

⇒ **Antivirus.** Son las herramientas que tienen como objetivo detectar y eliminar virus. Con el avance de Internet, estas herramientas han evolucionado. Actualmente, podemos encontrar programas avanzados que no solo buscan detectar y eliminar virus, sino que son capaces de bloquear, desinfectar y prevenir la infección de archivos.

⇒ **Antiadware.** En este caso se trata de herramientas antimalware destinadas a detectar anuncios publicitarios no deseados o la instalación de aplicaciones que contienen este tipo de amenaza. El adware puede, por poner un ejemplo, llegar a cambiar la configuración del navegador para redirigirnos a sitios web concretos que no hayan sido solicitados por parte del usuario.

⇒ **Antispyware.** Este tipo de herramientas están centradas en la lucha contra programas que tienen como fin utilizar el marketing o la publicidad y que suelen acabar en los ordenadores de los usuarios como por ejemplo, al acceder a páginas web maliciosas o al instalar software no oficial.

⇒ **UTM, Appliance (Unified Threat Management).** En español, “Gestión Unificada de Amenazas”. Se trata de dispositivos de seguridad que proveen

[37] (INCIBE. Productos antimalware. , 2018)

de varias funciones de seguridad en un único producto, es decir, que suelen incluir funciones de antivirus, antispam, firewall, etc.

Estas herramientas detectan todo tipo de amenazas, como virus, ransomware, troyanos, spyware, etc. Permiten realizar análisis en tiempo real y planificar, configurar y realizar análisis periódicos automáticos.

Las herramientas antimalware pueden utilizarse en multitud de ámbitos, desde un puesto de trabajo de un único usuario, hasta para la protección de una organización completa.

Además, es recomendable incluirlas en cualquier sistema informático, ya sean servidores, ordenadores de sobremesa o portátiles, tablets, smartphones, etc. En los escenarios donde hay un uso intensivo de Internet, o intercambio frecuente de ficheros, serán más que necesarios.
Por lo tanto, hay que tenerlas siempre presente y no esperar a que el malware haga acto de presencia en las empresas o corporaciones para hacer uso de este tipo de herramientas.

Capítulo 4. El Ransomware y otros delitos relacionados.

1. EN RELACIÓN CON LOS DERECHOS FUNDAMENTALES.

- VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD, HONOR Y PROPIA IMAGEN.

2. EN RELACIÓN CON LOS DELITOS PATRIMONIALES.

- VULNERACIÓN DELITO PROPIEDAD Y ESTAFA Y SU COMPARACIÓN.

3. RELACIÓN CON OTROS TIPOS DE DELITOS SEGÚN LA LEGISLACIÓN ESPAÑOLA.

- *ACCESO E INTERCEPTACIÓN ILÍCITA.*
- *INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA.*
- *FALSIFICACIÓN INFORMÁTICA.*
- *FRAUDE INFORMÁTICO.*
- *DELITOS SEXUALES.*
- *CONTRA LA PROPIEDAD INDUSTRIAL E INTELECTUAL.*
- *CONTRA EL HONOR.*
- *DELITOS CONTRA LA SALUD PÚBLICA.*
- *AMENAZAS Y COACCIONES.*

1. En relación con los derechos fundamentales.

Vulneración de los derechos fundamentales a la intimidad, honor y propia imagen.

Los autores Alfredo García López[38], José Cuervo Díez[39] y Eva Muñoz Deiros[40] hacen referencia en sus publicaciones a la relación entre la vulneración de tales derechos y el ataque de Ransomware.

El derecho a la protección de datos es un derecho fundamental recogido en el artículo 18 de la Constitución Española, norma suprema de nuestro ordenamiento jurídico, y protege la intimidad y privacidad del ciudadano respecto al uso y vulneración de sus datos personales, es decir, de cualquier dato que identifique o pueda identificar a una persona física concreta, y también datos de carácter personal, por ejemplo, los vídeos y las fotografías.

La protección del derecho a la protección de los datos personales viene regulada, en vía civil y administrativa, por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y por el Reglamento que la desarrolla, el Real Decreto 1720/2007, de 21 de diciembre, además del Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos), desarrollado anteriormente.

No obstante, el derecho a la protección de datos también está protegido en vía penal. Así, el apartado 2 del artículo 197 del Código Penal castiga a quien cometa delitos relativos a las infracciones del derecho fundamental a la protección de datos, concretamente:

Las mismas penas (penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses) se impondrán al que, sin estar autorizado, se apodere,

[38] (García López, A. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. , 2016)
[39] (Cuervo Díez, J. Delitos informáticos. Protección penal de la intimidad., 2014)
[40] (Muñoz Deiros, E. Delitos contra la protección de datos. , 2018)

utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Por tanto, la protección de datos protege la intimidad y privacidad del ciudadano frente a una intromisión o vulneración de su derecho fundamental a la protección de datos.

Sin embargo, esta tipificación ha sido muy criticada por los autores ya que, según la doctrina, la regulación civil y administrativa sobre la protección de datos es suficiente, y la tipificación de la vulneración de este derecho como delito, complica la determinación de la conducta penal.

En conclusión, el derecho a la protección de datos está protegido en vía civil, administrativa y vía penal, pero ésta última vía, atendida la gravedad de sus consecuencias (penas privativas de libertad) solo es aplicable en última ratio, cuando no sea posible acudir o garantizar nuestro derecho a través de las vías civil y/o administrativa.

2. En relación con los delitos patrimoniales.

Vulneración del derecho a la propiedad y estafa[41].

En el capítulo VI del Código Penal, “de las defraudaciones”, en la sección 1, se tipifica el delito de estafa:

Artículo 248 1. “Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”.

[41] (Oficina de Coordinación Cibernética. , 2018)

Esto hace referencia al engaño o manipulación que sufre la víctima mediante las técnicas de ingeniería social aplicadas por el ciberdelincuente para lograr así su objetivo.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Este artículo especifica que el engaño y el lucro se obtienen a partir de la utilización de medios informáticos, programas informáticos y semejantes, para cometer el delito.

3. En relación con otros tipos de delitos según la legislación española[42].

A través del Observatorio español de delitos informáticos (oedi.es) se desarrollan otros tipos de delitos relacionados con el Ransomware.

Acceso e interceptación ilícita[43].

El Código Penal español, regula en los artículos 197 a 201 el descubrimiento y revelación de secretos, por un lado, y en los artículos 278 a 286 los delitos relativos al mercado y los consumidores.

[42] (Oficina de Coordinación Cibernética. , 2018)
[43] (Oficina de Coordinación Cibernética. , 2018)

Estamos ante un tipo de hecho de descubrimiento y revelación de secretos, de acceso ilegal informático y de otros accesos ilícitos que afectan al mercado y a los consumidores por las consecuencias negativas que tiene dicho acceso.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Interferencia en los datos y en el sistema.

El Código Penal español regula en los artículos 263 a 267 y 625.1 la interferencia en los datos y en el sistema y los daños informáticos.

Se trata de un tipo de hecho de daños derivados del ataque informático.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Falsificación Informática[44].

El Código Penal español regula el delito de falsificación informática en los artículos 388, 389, 399 bis, 400 y 401.

Se trata de un tipo de hecho de falsificación de moneda, sellos y efectos timbrados, fabricación y tenencia de útiles para falsificar y la usurpación del estado civil.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P,

[44] (Oficina de Coordinación Cibernética. , 2018)

páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Fraude Informático[45].

El Código Penal español regula en los artículos 248 a 251 y 623.4. el delito de fraude informático.

Se trata de un tipo de hecho relativo a la estafa bancaria, estafas con tarjetas de crédito, débito y cheques de viaje, así como otras estafas.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Delitos Sexuales[46].

El Código Penal español regula en los artículos 181, 183.1, 183.bis,184, 185, 186, 189 los diferentes delitos sexuales.

Los tipos de hecho son relativos al exhibicionismo, provocación sexual, acoso sexual, abuso sexual, corrupción de menores e incapacitados, pornografía infantil y el delito de contacto mediante tecnología con menores de 13 años con fines sexuales.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P,

[45] (Oficina de Coordinación Cibernética. , 2018)
[46] (Oficina de Coordinación Cibernética. , 2018)

páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Contra la propiedad industrial e intelectual[47].

El Código Penal español regula en los artículos 270 a 277 y 623.5 los delitos contra la propiedad intelectual y contra la propiedad industrial.

El tipo de hecho es el relativo a delitos contra la propiedad industrial y contra la propiedad intelectual.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Contra el Honor[48].

El Código Penal español regula en los artículos 205 a 210 y 620.2 los delitos contra el honor.

El tipo de hecho es relativo a los delitos de calumnias e injurias.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Delitos contra la salud pública[49].

[47] (Oficina de Coordinación Cibernética. , 2018)
[48] (Oficina de Coordinación Cibernética. , 2018)
[49] (Oficina de Coordinación Cibernética. , 2018)

El Código Penal español regula en los artículos 359 a 371 los delitos contra la salud pública.

El tipo de hecho es el relativo a los delitos de tráfico de drogas y otros delitos contra la salud pública.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Amenazas y coacciones[50].

El Código Penal español regula en los artículos 169 a 172 y 620 los delitos de amenazas y coacciones.

El tipo de hecho es el relativo a los delitos de amenazas, amenazas a grupo étnico, cultural o religioso y las coacciones.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

[50] (Oficina de Coordinación Cibernética. , 2018)

CAPÍTULO 5: Soluciones al problema.

1. CÓMO EVITARLO. PREVENCIÓN.

2. PROBLEMA DE EDUCACIÓN Y CONCIENCIACIÓN. LA VÍCTIMA NO DENUNCIA.

3. FORMACIÓN Y RECICLAJE DE LOS PERFILES DE RIESGO.

4. RECOMENDACIONES A SEGUIR EN CASO DE SER VÍCTIMAS DEL CIBER ATAQUE.

1. Cómo evitarlo. Prevención.

Existen diversas guías sobre cómo prevenir ser víctimas de este tipo de ciberataque, entre ellas, encontramos la Guía Eset[51] y la Guía de INCIBE[52].

Son diversas las medidas para evitar ser víctimas de un ciberataque de Ransomware y limitar sus daños, entre ellas encontramos medidas dirigidas a los sistemas, ya que deberían ser resistentes ante un ataque y poder recuperarse rápidamente cuando ocurre este ocurre, por ejemplo, si se tienen servicios públicos como un servidor Web, Correo, o alguna aplicación en Internet y está conectado a la red Interna, en la misma red de los usuarios de la empresa sin ninguna restricción esto es un grave error, ya que si cualquier servicio público es comprometido desde Internet o desde la red Interna que sería lo más probable, el atacante podrá ingresar a otros servicios de la red Interna sin ningún problema.

Para evitar casos así, es recomendable que los servicios públicos estén en una red independiente de la red interna como una DMZ para servicios públicos o una DMZ para Proveedores. Políticas de firewall tanto de entrada como de salida de tráfico. Registros de logging activado para identificar y revisar intentos de intrusión. Y aseguramiento del mismo servicio público a nivel del servidor como un hardening del servidor.

Otra medida muy importante para evitar ser víctimas de un ciberataque de Ransomware es la de realizar copia de seguridad, ya que contar con un sistema de recuperación de datos impide que una infección de ransomware pueda destruya los datos para siempre.

Es recomendable crear dos copias de seguridad, una para ser almacenada en la nube (se pueden usar servidores de servicio que realicen automáticamente copias de los archivos) y otra en un dispositivo físico, como un disco duro portátil, memoria USB, otro equipo portátil, etc.
Es importante desconectarlos del PC cuando se haya realizado la copia.

[51] (Guía Eset Ransomware 2017, s.f.)
[52] (INCIBE. Ransomware, una guía de aproximación para el empresario, s.f.)

Otras de las medidas básicas es usar un buen software antivirus para proteger el sistema del ransomware. No desactivar la detección mediante heurísticas ya que esto ayuda a capturar muestras de ransomware que aún no hayan sido detectadas formalmente.

Mantener el software del PC actualizado, y cuando el Sistema Operativo o aplicaciones se actualicen a una nueva versión hay que instalarlas.

No fiarse de nada, ya que cualquier cuenta puede estar comprometida y enlaces maliciosos pueden ser enviados desde cuentas en redes sociales de amigos, compañeros o desde juegos online.
No abrir nunca archivos adjuntos desde emails de alguien desconocido. Los cibercriminales a menudo distribuyen correos electrónicos falsos que simulan ser notificaciones legítimas remitidas desde servicios de almacenamiento en la nube, bancos, policía o agencias de recaudación de impuestos que incitan a pulsar enlaces maliciosos para instalar malware en los ordenadores y sistemas, esto se conoce como 'phishing'.

Activar la opción de mostrar las extensiones de los archivos en el menú de configuración de Windows. Esto hace mucho más fácil detectar archivos potencialmente maliciosos.
Mantenerse alejado de extensiones como ‘.exe’, ‘.vbs’ y ‘.scr’, ya que los estafadores pueden usar varias extensiones para camuflar un fichero malicioso como un video, una foto o un documento.

En caso de descubrir algún proceso sospechoso en el ordenador, hay desconectarlo inmediatamente de internet o de otras conexiones en red, como el WIFI de casa, para prevenir que la infección se propague.

Los técnicos deben velar por que los sistemas empleados se hallen actualizados de forma que al menos dispongan de la protección que el fabricante ha suministrado vía actualización de los parches o definición de virus.

Se deben observar reglas de uso adecuado de los medios para preservar las tres dimensiones de la seguridad de la información que son la confidencialidad,

la integridad y la disponibilidad de los datos, si el cumplimiento no es por parte de todos, estas dimensiones pueden verse afectadas. Confidencialidad: Exfiltración, publicación de información a quien no debiera verla. Integridad: Alteración, modificación de la información, caso de ransomware. Disponibilidad: Denegación, impedir el acceso a la información, caso de los Ataques que saturan los sistemas, ataques de Denegación de Servicio (DOS) o bien si son a gran escala Ataques Distribuidos de Denegación de Servicio (DDOS).

En las empresas y corporaciones.

1. No emplear los medios de la oficina para otra cosa que no sea el cometido del puesto de trabajo.
2. Comunicar un incidente cuando se produzca mediante los cauces establecidos y si estos no existen mediante cualquier medio al alcance.
3. No abrir correos sospechosos o que tengan algo que los haga sospechosos, como, por ejemplo: texto extraño o contenido poco habitual, el cuerpo del mensaje “pide dinero” o pide algo no habitual como que se realice un acceso a su web. Otro ejemplo, es un correo de publicidad con un ZIP anexo, oferta novedosa o mail del banco: “estamos actualizando la información debe acceder a su cuenta e introducir su número de cuenta”. Los bancos nunca piden el número de cuenta, lo único que piden son el identificador de acceso y la clave que debe ser oculta. Si un banco pide que le envíes la clave en texto, hay que llamar al banco.

4. No ejecutar programas que “aparecen” en la web tipo: “instale esto y le permitiremos bajar el archivo” o “su pc es vulnerable, escanéelo ahora con este programa”, “llame a este 908 para bajar…” ya que suele tratarse de malware.

En caso de que dicha prevención falle, se debe reaccionar:

[53] (INCIBE. Ransomware, una guía de aproximación para el empresario, s.f.)

Si se recibe un mail y al abrir el adjunto la pantalla parpadea o bien el adjunto de Office no se abre o bien se abre y el Excel/Word se cierra a continuación, es posible que haya sido infectado. En ese caso se debe avisar a los equipos de soporte.

Detener un ataque es muy difícil, así que la empresa debe tener procedimientos robustos de detección, supervisión y corrección, la capacidad de informar sobre todas las sospechas y agilidad a la hora de responder.

En los hogares y entornos no profesionales o corporativos.

Se vuelve a hacer hincapié en la prevención. Unificar la información personal en una carpeta (Mis Documentos, Mis Imágenes…), para facilitar la copia de seguridad, si se tiene la información dispersa en el disco duro hacer un Backpus será más complejo.
Es recomendable comprar un disco duro externo y hacer copia de los datos a este medio externo.
Establecer una rutina de actualización de la información, éstas acciones tienen que tener continuidad, tener un backup de hace 3 años puede que no me sirva de nada, por tanto, a la hora de establecer un proceso de copia debe establecerse una rutina de actualización, cada día, cada semana o cada mes.
Revisar que Windows Update o el sistema operativo utilizado esté al día, si no es así actualizar el equipo.
Y actualizar Antivirus/Malware en todos los equipos.

Es importante explicar a todos los usuarios del PC que no deben abrir correos sospechosos, ni deben ejecutar programas que aparecen en el web tipo “instale esto y le permitiremos bajar el archivo” o “su pc es vulnerable, escanéelo ahora con este programa”, suele ser malware. Usar un bloqueador de elementos emergentes en los navegadores. Usar UAC (Control de cuentas de usuario de Windows).

Si la prevención falla, se debe reaccionar de manera eficaz, si ve que la información ya no está disponible o bien los archivos cambian de nombre o bien el equipo se queda colgado, es posible que tenga un malware cifrando la

información. En ese caso se debe apagar el equipo y buscar asesoramiento para restaurar la información, evaluar hasta dónde ha llegado o bien probar la solución de la infección completa.
También se puede restaurar la información desde el punto de restauración anterior y revisar que la información se halle actualizada.
Si ya han infectado del todo y al abrir cualquier archivo aparece el mensaje de aviso del Ransomware para proceder al pago, se debe en lugar en pagar, buscar soluciones ya existentes en www.nomoreransom.org, web que más adelante se desarrollará.

2. Problema de educación y concienciación. La víctima no denuncia.

En España, el número de denuncias de Ransomware es inferior al del número de víctimas (500.000 es el número estimado de víctimas del Ransomware Cryptolocker), lo que quiere decir que la gente no denuncia, siendo fundamental para poder perseguir el delito policial y judicialmente.

Se puede denunciar este tipo de ataques por teléfono, por internet o en comisaría, en las instancias de la guardia civil o de la policía nacional, los cuales cuentan con unidades especializadas en delitos informáticos y fraudes a través de internet. Además de otros organismos internacionales y supranacionales, como Europol, Interpol, etc.

Los usuarios vulnerables son los que están desinformados, aquellos que no están alertas si reciben un correo falso, que creen que el ransomware es un tema de películas o que los incidentes de seguridad ocurren únicamente en gobiernos y grandes corporaciones multinacionales.
La mayoría de las infecciones de ransomware requieren, de la intervención del usuario: ya sea para descargar un archivo, ingresar a un link malicioso, abrir un documento o realizar el pago creyendo algún engaño.
El factor de ingeniería social es clave para el éxito de la infección.

Por lo tanto, otro punto importante en la prevención es la educación y concientización de los usuarios. Estar informado sobre cómo actúan las

amenazas, cuáles son los engaños que utilizan para infectar a los usuarios, de qué forma se propagan y cómo prevenirlas son algunos de los conocimientos que evitarán que un empleado sea infectado.
Una buena campaña de concientización no se logra con acciones esporádicas, por el contrario, es necesario una educación periódica y constante. La clave es no centrarse en un solo recurso, sino aprovechar cualquier oportunidad para educar. No solo se logra la concientización mediante charlas y cursos explicando los riesgos y las medidas de seguridad, además, se puede complementar con recordatorios periódicos de buenas prácticas, un boletín de noticias de actualidad, guías y manuales de configuraciones de privacidad y seguridad, o incluso videos y posters con consejos prácticos.

Medidas de concienciación para protegerse.

Es fundamental contar con una solución integral de seguridad que pueda detectar y bloquear amenazas conocidas de manera temprana. Actualizar aplicaciones y componentes del sistema operativo a su última versión, ya que el ransomware aprovecha vulnerabilidades. Los correos electrónicos son una importante fuente de propagación, por eso es importante evitar divulgar la dirección, revisar al remitente, cuidarse de ofertas tentadoras, verificar si se trata de un correo dirigido y filtrar los archivos ejecutables. Educar al personal para que no sucumba ante las técnicas de ingeniería social que se utilizan como puerta de entrada para la infección. Una adecuada política de backup asegurará la restitución de bases de datos y la continuidad del negocio incluso en las peores circunstancias.

Recomendaciones de Europol.

Partiendo de que el Ransomware una estafa diseñada para generar enormes ganancias para los grupos delictivos organizados, para prevenir y minimizar

los efectos del ransomware, el centro europeo de ciberdelincuencia de Europol aconseja tomar las siguientes medidas[54].

Actualizar el software regularmente. Muchos malware son el resultado de que los criminales explotan errores en el software (navegadores web, sistemas operativos, herramientas comunes, etc.). Mantenerlo actualizado puede ayudarlo a mantener seguros los dispositivos y archivos.

Usar software antivirus, instalar y mantener actualizado el software antivirus y de firewall en los dispositivos puede ayudar al ordenador a mantenerse libre de cualquier tipo de malware. Revisar siempre los archivos descargados con el antivirus.

Buscar y descargar software solo de webistes de confianza. Utilizar fuentes oficiales y sitios web recomendados para mantener el software parcheado con las últimas versiones de seguridad, y usar siempre la versión oficial de software.

Hacer una copia de seguridad regularmente de los datos almacenados en el ordenador. Copias de seguridad de datos completas ahorrarán mucho tiempo y dinero al restaurar el ordenador, incluso cuando se ve afectado por un ataque de ransomware.

Reportarlo, es decir, comunicar cuando se es víctima de ransomware, inmediatamente a la policía y al procesador de pagos involucrado. Cuanta más información se le dé a las autoridades, más eficazmente se podrá interrumpir la infraestructura criminal.

Consultar al proveedor de antivirus sobre cómo desbloquear y eliminar la infección del dispositivo. Existen numerosos sitios web y blogs oficiales con instrucciones sobre cómo eliminar de forma segura este tipo de malware de los dispositivos electrónicos. Es muy recomendable consultar www.nomereransom.org para verificar si ha sido infectado con una de las variantes de ransonware para las cuales hay herramientas de descifrado disponibles sin cargo.

[54] (Guía Europol. Ransomware, what you need to know. , 2016)

Lo que se debe evitar hacer.

Se debe evitar hacer clic en archivos adjuntos, banners y enlaces sin saber su verdadero origen, ya que lo que parece una publicidad o imagen inofensiva puede redirigir al sitio web desde el que se descarga el software malicioso. Lo mismo puede suceder al abrir archivos adjuntos en correos electrónicos recibidos de fuentes desconocidas.

Instalar aplicaciones móviles de proveedores o fuentes desconocidas. Hay que descargar siempre desde recursos oficiales y de confianza. En la configuración de los dispositivos Android, mantener siempre desactivada la opción "Fuentes desconocidas" y la opción "Verificar aplicaciones" marcada.

Dar algo por hecho. Si un sitio web advierte sobre software obsoleto, controladores o códecs (programas que codifican y decodifican los datos) instalados en el ordenador, no confiar plenamente en ellos. Para los delincuentes es muy fácil falsificar logotipos de empresas y software. Una búsqueda rápida en la web puede indicar si el software está realmente desactualizado.

Instalar o ejecutar software no confiable o desconocido. No instalar programas o aplicaciones en el ordenador si no se sabe de dónde vienen, ya que algunos tipos de malware instalan programas en segundo plano que intentan robar datos personales.

No pagar el dinero del rescate, ya que pagar no garantiza que el problema se resuelva y que se podrá volver a acceder a los archivos. Además, se apoya de esta manera el negocio de los ciberdelincuentes y el financiamiento de sus actividades ilegales.[55]

La complejidad de la solución ante un ataque de Ransomware.

[55] (Guía Europol. Ransomware, what you need to know. , 2016)

El ransomware está en auge, hay más de 50 familias de este malware en circulación actualmente y está evolucionando rápidamente. Con cada nueva variante se mejora el cifrado y se incorporan nuevas características.

Una de las razones por las que es difícil encontrar una solución es debido a que el cifrado en sí no es dañino. Realmente es una buena herramienta y muchos programas legítimos la utilizan.

El primer malware criptográfico utilizaba un algoritmo de clave simétrica, con la misma clave para cifrar y descifrar. La información corrupta podía ser descifrada con éxito normalmente mediante la ayuda de compañías de seguridad. Con el tiempo, los cibercriminales empezaron a utilizar algoritmos de cifrado asimétricos que utilizan dos claves diferentes, una pública para cifrar los archivos, y una privada necesaria para el descifrado.

El troyano *CryptoLocker* es uno de los ransomware más famosos, que utiliza también un algoritmo de clave pública. Cuando un ordenador es infectado se conecta con un panel de control para descargar la clave pública. La clave privada sólo la tienen los criminales que escribieron el software CryptoLocker. Normalmente, la víctima no tiene más de 72 horas para pagar el rescate antes de que la clave privada se borre para siempre, y resulta imposible descifrar ningún fichero sin esta clave.

Así que lo primero que hay que tener en cuenta es la prevención. La mayoría de los antivirus incluyen algún componente que ayuda a identificar el ataque de un ransomware en etapas tempranas de la infección, impidiendo la pérdida de información sensible. Es importante para los usuarios asegurar que esta funcionalidad está activada en el antivirus.

Es posible en determinados casos descifrar los archivos que fueron cifrados por el Ransomware cuando los autores del malware realizaron errores de implementación, haciendo posible romper el cifrado. Éste fue el caso del ransomware *Petya* y *CryptXXX*.
Cuando los autores del malware se sienten culpables por sus acciones y publican las claves, o una clave maestra, como en el caso de TeslaCrypt.

O cuando la policía captura servidores con claves y las comparten. Un ejemplo es *CoinVault*.

A veces pagar el rescate también funciona, pero no existe garantía de que realizar el pago permita descifrar tus archivos. Además, con esta acción se apoya el modelo de negocio de los criminales y en consecuencia se está coopera para que más gente se esté infectando con ransomware.

El número de usuarios que se han visto atacados por ransomware es inmenso, con unos 718.000 usuarios afectados entre abril de 2015 y marzo de 2016, esto significa que ha multiplicado su impacto x 5,5 veces comparado con el mismo periodo de tiempo en 2014-2015.

La policía no puede combatir el cibercrimen, y el ransomware en particular, por sí misma. Y los investigadores de seguridad no pueden hacerlo sin el soporte de las fuerzas del orden. La responsabilidad de combatir el ransomware está compartida entre la policía, los Gobiernos, Europol y las compañías de seguridad IT, y requiere un esfuerzo conjunto.

Herramientas de protección.

Si bien el ransomware pareciera ser la amenaza “de moda” en los últimos tiempos, son muchos los tipos de amenazas que se están propagando y afectando a los usuarios. Ya sea que se trate de un troyano, un gusano, un bot o el mismo ransomware, una buena herramienta integral de seguridad es capaz de prevenir la infección.

El término “antivirus” quedó acuñado en el subconsciente colectivo, este tipo de herramientas han evolucionado y pasaron de detectar solamente virus informáticos hasta convertirse en soluciones de seguridad completas, que proveen muchas otras funcionalidades como firewall, filtros de email y antispam, antiphishing o escaneo de memoria, entre otras, que dan una protección integral al sistema y permiten navegar seguro en el contexto actual de amenazas.

Por último, es importante actualizar regularmente los sistemas y aplicaciones, ya que muchas amenazas aprovechan vulnerabilidades no corregidas para propagarse por la red. Si bien esta tarea puede llegar a ser aburrida y rutinaria, existen herramientas de gestión de parches y actualizaciones que simplifican notablemente el trabajo.

Es importante destacar que ante una infección, la posibilidad de recuperar la información y la forma de hacerlo dependerá del tipo de amenaza específica.

En general, en los casos del tipo lockscreen es posible recuperar el acceso al sistema limpiando la infección o restaurando el equipo. Además, en estos casos, si los archivos no son cifrados es posible recuperarlos del disco afectado.
Sin embargo, en algunas variantes especialmente aquellas que afectan dispositivos móviles, el bloqueo no permite la recuperación del equipo, por lo que la única solución terminará siendo un reseteo de fábrica, borrando toda la información. En el caso de los filecoders la recuperación puede ser más complicada.

En la mayoría de los casos, un buen software de seguridad tendría que ser capaz de quitar el ransomware del equipo, los archivos seguirán cifrados. En algunas familias de ransomware, especialmente las que utilizan el cifrado simétrico y guardan la clave dentro del código malicioso, es posible recuperar los archivos utilizando la herramienta específica de descifrado. Sin embargo, los archivos que fueron atacados por un tipo más sofisticado de ransomware, como Cryptolocker, son imposibles de descifrar sin la clave correcta. En cualquier caso, si ocurre una infección es recomendable limpiar el equipo de la infección, ya sea utilizando una herramienta de seguridad o reinstalando el sistema, y luego recuperar la información y los archivos mediante un respaldo limpio.

[56] (Guía Europol. Ransomware, what you need to know. , 2016)

Pagar el rescate no es garantía de recuperar los archivos.

La realidad es que recuperar los archivos no está garantizado. Si se cuenta con la clave maestra se van a poder descifrar todos los documentos, no obstante, conseguir la clave sin ceder ante el pago de los cibercriminales es lo complejo. Si bien existen variantes de cryptolockers para las cuales es posible descifrar y recuperar los archivos afectados, en la mayoría de las ocasiones esto resulta casi imposible, sobre todo si el algoritmo es fuerte; la clave no puede ser obtenida a partir del código del malware; y las claves maestras son únicas para cada víctima y funciona solo para un equipo[57].

3. Formación y reciclaje de los perfiles de riesgo.

En cuanto a los fabricantes, es importante hablar sobre el "Zero Day", que se trata de las vulnerabilidades de los programas desconocidas para su fabricante, por tanto, no han podido emitir un parche que la subsane. Esto supone estar desprotegidos contra ellas ya que son desconocidas para los equipos que administran los sistemas. Ante estas vulnerabilidades las protecciones más efectivas son el aislamiento, es decir, cortar internet, o bien la concienciación, es decir, sospechar de un correo extraño o no solicitado. De esta forma evitamos, por ejemplo, que un archivo se copie entre todos los ordenadores vulnerables de una red. Este es el caso de WannaCry.

La RansomSociety.

Es la sociedad secuestrada por la amenaza de este tipo de acciones, cada día hay más preocupación por la "amenaza digital", se han visto robos de información que han influido en resultados electorales, países que abandonan las máquinas para hacer el recuento de sus elecciones "analógicamente"

[57] (Guía Europol. Ransomware, what you need to know. , 2016)

(Holanda) por miedo a intervenciones de un tercero. Ataques a infraestructuras críticas con éxito.
La amenaza existe, y más desde que ha pasado a tener plan de negocio. Conviene recordar que la “industria” del malware mueve miles de millones de euros actualmente, por tanto, hay negocio y hay gente dispuesta a beneficiarse de este mercado.

Amenazas futuras y su desarrollo.

Incluso antes del brote de WannaCry, el ransomware ya estaba establecido para tomar el escenario central en términos de amenazas de malware.
La escala y la amplia superficie del ataque WannaCry fue sin precedentes, ya que muy pocos fueron los países que no se vieron afectados.
El aspecto positivo de esto es la generación de un despertar global, concienciar sobre la amenaza en todo el mundo y crear una oportunidad para que los problemas de seguridad de las TI (Tecnologías de la información) sean tomados más en serio por empresas y organizaciones, incluida la necesidad de mejorar la gestión de parches y vulnerabilidades.

La seguridad cibernética es una industria en crecimiento, y dentro de Europa es probable que las primas de seguros aumenten a 8.900 millones de euros en 2020 desde alrededor de 3.000 millones de euros en la actualidad.

Hay un evidente riesgo de seguridad cibernética fomentando la necesidad de suscribir seguros para tener así alguna garantía, ya que los riesgos son inevitables, sobre todo en el caso de aquellas empresas y organizaciones que dependen de estos seguros para cubrir pérdidas potenciales en lugar de invertir en acciones preventivas medidas.

Un elemento clave ocurrido tanto en el ataque de WannaCry y el ataque de Petya/NotPetya fue la inclusión de la auto-propagación o la funcionalidad 'gusano' dentro del malware, creando lo algunos se refieren a como un 'ransomworm'. Si bien esto no fue la primera vez que esto se ha hecho, es el

ejemplo más exitoso de su implementación, y una táctica que probablemente se repetirá en futuras amenazas.

Los troyanos bancarios no figuraban en gran medida en los informes policiales del año 2016, sin embargo, su desarrollo e innovación no cesa de aumentar. Como se informó en años anteriores, hay poco en el camino del malware completamente nuevo, ya que los desarrolladores se centran en las variantes ya existentes, como la variante Zeus Panda, o la variante Dyre Trickbot, o malware híbrido que combina aspectos de otras variantes exitosas, como Goznym que toma prestado tanto del troyano bancario Gozi como del Nymaim descargador.

Los ataques sofisticados contra las infraestructuras críticas europeas son una amenaza real. Sin embargo, los ataques, tanto directos como indirectos, contra infraestructuras críticas utilizando el ataque cibernético comúnmente disponible herramientas como booters/stressers parecen ser mucho más probable y más fáciles de detectar.

Si bien estos ataques pueden no ser tan dañino como derribar una red eléctrica, pueden causar la interrupción severa y el colapso de servicios clave. La directiva de seguridad de la información de red (NIS) establece las soluciones de ciberseguridad en los sectores críticos, requiriendo identificar a los operadores de estos sectores para tomar las medidas apropiadas y proporcionadas para gestionar los riesgos que plantea la seguridad de sus redes y sistemas de información, incluida la necesidad de notificar incidentes significativos. Como tal, se espera que la directiva NIS tenga un impacto fuerte y positivo en la ciberseguridad de las infraestructuras críticas.

Conclusiones y opinión personal.

Se debe llevar a cabo una regulación y tipificación exhaustiva de los diferentes delitos informáticos que han surgido debido a la evolución de la informática y del crimen a través de estos medios.

La concienciación de los usuarios, de los ciudadanos que hacen uso de internet en sus hogares, y de las empresas y organizaciones, tanto públicas como privadas, es necesaria para prevenir y saber actuar en caso de ser víctimas de cualquier ataque o ciberdelito.

Se deben adoptar medidas que frenen a los posibles autores de dichos delitos, así como sanciones a tales conductas.

Poner a disposición todo tipo de herramientas y formación necesaria para difundir así técnicas de prevención y protección. Además de hacer hincapié en denunciar en el plazo más breve posible en caso de ser víctimas de cualquier ciberataque.

Concienciar de que el pago del rescate solo consigue incentivar más a los ciberdelincuentes, ya que saben que es un método cómodo, seguro y eficaz de conseguir dinero, información, dañar la imagen y reputación de empresas y particulares, etc.

Y, por último, dar a conocer y difundir en qué consisten las técnicas de ingeniería social, ya que el factor humano es el eslabón más débil en la seguridad de la información.

Personalmente, opino que el continuo auge de los ciberdelitos y los graves perjuicios que causa a la población son un asunto de suficiente entidad como para que estén en el foco de la actualidad con más intensidad y protagonismo del que goza hoy en día, que es prácticamente nulo.

Tras realizar el trabajo, considero que estamos ante una alarma social que está pasando desapercibida porque gran parte de la población todavía no es

consciente de los riesgos a los que está expuesta mientras hace uso de sus dispositivos.

La cifra de víctimas y de ataques que se llevan a cabo a diario, junto al volumen de capital económico ilícito que obtienen y manejan los ciberdelincuentes, puede derivar en graves problemas sobre todo para los usuarios domésticos, ya que los profesionales de la informática, los usuarios con conocimientos avanzados y las empresas y corporaciones conocen el riesgo real y grave al que están expuestos.
Empresas como Facebook pagan cantidades millonarias a quienes detecten cualquier agujero de seguridad en sus servicios y aplicaciones, ya que son conocedores de que cualquier filtración de datos podría hacerles desaparecer como red social (Facebook tiene $300.000 *millones* de valoración bursátil).

Internet y las nuevas tecnologías forman parte de nuestra vida diaria desde edades cada vez más tempranas, por tanto, considero que sería una buena técnica de prevención el introducir en el sistema educativo una asignatura que tratara las nuevas tecnologías y los riesgos a los cuáles nos exponemos con su uso, destacando sus beneficios y sobre todo sus aspectos negativos, para así ser conscientes de que todos los usuarios de internet somos víctimas potenciales de cualquier malware.

Considero que, realizando un esfuerzo conjunto entre el Gobierno, las fuerzas y cuerpos de seguridad y los profesionales de la seguridad informática se pueden prevenir y disminuir en gran medida las infecciones a los sistemas y dispositivos que en muchas ocasiones los propios usuarios instalamos de manera inconsciente.

Además de víctimas nos convertimos en una especie de cómplices de los ciberdelincuentes por pagar el rescate que nos solicitan ya que solo favorecemos la continuidad de sus ataques.

Por último, creo que se debe motivar a la población a que denuncie, ya que la mayoría de las infecciones no se ponen en conocimiento de la policía ni de las autoridades judiciales. Las víctimas prefieren sufrir las consecuencias del delito

e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial, y esto dificulta el conocimiento preciso del número de delitos cometidos y con ello la planificación de las adecuadas medidas legales sancionadoras o preventivas.

BIBLIOGRAFÍA

GARCÍA LÓPEZ, A. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Publicado el 20 junio de 2016. Disponible en: http://www.alfredogarcialopez.es/penal-4/

MAEZTU, D. “Tipificación penal del ransomware”. Publicado el 12 de mayo de 2017. Disponible en: http://www.derechoynormas.com/2017/05/tipificacion-penal-del-ramsomware.html

PLATAFORMA DE AFECTADOS POR EL VIRUS DE LA POLICÍA. [Consulta: mayo 2018]. Disponible en: https://asociacionafectadosinternet.es/plataforma-de-afectados/plataforma-virus-de-la-policia/

NIST Cybersecurity Framework vs ISO 27001. A través de ¿Cybersecurity Framework o ISO 27001? Publicado el 24 de febrero de 2018. Disponible en: http://noticiasseguridad.com/seguridad-informatica/cybersecurity-framework-o-iso-27001/ y https://blog.segu-info.com.ar/2018/03/nist-cybersecurity-framework-vs-iso.html

MENDOZA, M.A. La evolución del ransomware: del ochentero PC Cyborg a un servicio en venta. Publicado el 21 de agosto 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

ESET Latinoamérica. 28 de Julio de 2015. ¿Qué es el ransomware y cómo afecta a los entornos corporativos? [Consulta: Mayo 2018]. Disponible en: https://www.welivesecurity.com/la-es/infographics/que-es-el-ransomware-y-como-afecta-a-los-entornos-corporativos/

DEFINICIONES GLOSARIO. Disponible en: https://www.welivesecurity.com/la-es/glosario/

NO MORE RANSOM. 2018. [Consulta: Mayo 2018] Disponible en: https://www.nomoreransom.org/es/ransomware-qa.html

INFORME DE LA UNIÓN EUROPEA SOBRE CIBERDELINCUENCIA. 26 DE JULIO DE 2017. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0272+0+DOC+XML+V0//ES

CUESTA MARTINEZ, F. COBIT 5: Marco de negocio para seguridad de la información. Publicado el 30 de septiembre de 2015. Disponible en: https://riunet.upv.es/handle/10251/56417?show=full

REGLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, 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 ESOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

ACOSTA DAVID, E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST.- CISSP Instructor, CISM, CISA, CRISC, CHFI Instructor, CEH, PCI QSA, OPST, BS25999 L. A. Publicado el viernes, 23 de diciembre de 2016. Departamento de Consultoría Disponible en: http://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

KARCZEWSKA, J. CISA. COBIT 5 y el reglamento RGPD. COBIT Focus. Publicado el 29 de marzo de 2017. Disponible en: http://blog.isecauditors.com/search?q=ransomware y http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-the-gdpr-spanish.aspx

NEIRA LÓPEZ, A. Lead Tutor y Técnico especialista en formación desarrolla e imparte programas en Diseño y Mejores Prácticas en la gestión de los Data Center. Auditor jefe de certificación para ISO 27001, ISO 20000, ISO 22301

(BS25999) con acreditaciones ENAC, UKAS e itSMF, así como, esquemas de evaluación de disponibilidad (TIER) y eficiencia energética (CEEDA) para Data Center.
SPOHR RUIZ, J. Ingeniero de Telecomunicación, CISA, Lead Auditor ISO 27001 y ISO 22301 (BS25999). Lead Tutor ISO 27001. Auditor jefe de certificación de ISO 27001. Auditor Jefe de Calidad de Servicio y Calidad de Facturación en operadores de telecomunicaciones, según Orden Ministerial ITC/912/2006.
Disponible en: www.iso27000.es

MILTON, S. CISA, CGEIT. “COBIS FOCUS”. Publicado el 3 de abril de “017. Cómo COBIT 5 puede ayudar a reducir la probabilidad y el impacto de las 5 amenazas cibernéticas más importantes. Disponible en: http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-can-help-reduce-the-likelihood-and-impact-of-the-top-5-cyberthreats-spanish.aspx

GUÍA IOCTA 2017. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi-2NrPxq3cAhWS-aQKHdAiApwQFggoMAA&url=https%3A%2F%2Fwww.ccn-cert.cni.es%2F%3Fid%3D4795%3Aguia-sobre-la-seguridad-en-redes-inalambricas%26start%3D44&usg=AOvVaw1xek8bd6n-D_bEKW2HWXtI

GUÍA REGLAMENTO DE PROTECCIÓN DE DATOS 2018. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiss-Lmxq3cAhVN3qQKHcT0C34QFggpMAA&url=https%3A%2F%2Fwww.aepd.es%2Fmedia%2Fguias%2Fguia-rgpd-para-responsables-de-tratamiento.pdf&usg=AOvVaw3RkIeEY6tPqxPw5aA_79j_

INCIBE. Productos antimalware. Publicado el 05/06/2018. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/protegiendo-nuestra-empresa-productos-anti-malware?utm_campaign=empresas&utm_medium=twitter&utm_source=post

GÓMEZ REY, H. Abogado del Área Governance, Risk and Compliance de Ecix. “Brechas de seguridad y ransomware wannacry”. Disponible en: https://www.ecixgroup.com/brechas-seguridad-nuevo-reglamento-general-proteccion-datos-proposito-del-ransomware-wannacry/

ÉCIJA, Á. Ecix Group. Publicado en Madrid el 12 de mayo de 2017. “Ransomware delito de estafa en concurso con delito informático”. Disponible en: https://cincodias.elpais.com/cincodias/2017/05/12/legal/1494614621_922741.html

CUERVO ÁLVAREZ, J. Delitos informáticos: Protección Penal de la Intimidad. 1 de enero de 2014. Disponible en: http://www.informatica-juridica.com/trabajos/delitos-informaticos-proteccion-penal-de-la-intimidad/#5.%20CONDICIONES%20OBJETIVAS%20DE%20PERSEGUIBILIDAD.%20ART.

MUÑOZ DEIROS, E. Delito contra la protección de datos. Disponible en: https://evamunoz.es/delito-contra-la-proteccion-de-datos-habeas-data/

OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS. 2018. [Consulta: Mayo 2018].

Disponible en: http://oedi.es/

INFORME CRIMINALIDAD 2015 DEL MINISTERIO DEL NITERIOR. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjl-faCx63cAhWS6qQKHaW5C4cQFggpMAA&url=http%3A%2F%2Fwww.interior.gob.es%2Fdocuments%2F642317%2F1204854%2FAnuario-Estadistico-2015.pdf%2F03be89e1-dd38-47a2-9ce8-ccdd74659741&usg=AOvVaw2L6JS4Mg6kNi0QUo2n3JUO

SAN JOSÉ, J. “SIRIUS, la plataforma de Europol para facilitar las investigaciones de los ciberdelitos”. Disponible en: https://derechodelared.com/2017/11/02/sirius/

RTVE.es / EFE. 01.02.2018. *“Los españoles pasan más de cinco horas diarias conectados a internet”.* [Consulta: junio 2018]. Disponible en: http://www.rtve.es/noticias/20180201/espanoles-pasan-mas-cinco-horas-diarias-conectados-internet/1671382.shtml

ANEXO. Glosario de términos.

TOR: Tor es un software libre y una red abierta que lo ayuda a defenderse contra el análisis del tráfico, una forma de vigilancia de la red que amenaza la libertad y la privacidad personal, las actividades y relaciones comerciales confidenciales y la seguridad del estado.

BITCOIN: Se trata de una moneda virtual (criptomoneda). Se emplea tanto en transacciones financieras realizadas a través de ellas en el mundo virtual, así como medio de pago en caso de ataques.

Cibercrimen: Actividad delictiva organizada que implica el uso de herramientas informáticas y se basa en Internet para su ejecución. El objetivo es obtener beneficios, por lo general financieros. Delitos tales como el phishing, scam o robo de identidad son considerados cibercrimen, como así también todos los recursos y actores que forman parte de su circuito criminal.

Ciberdelincuente: Persona que comete cibercrimen.

Deep Web: Conjunto de sitios web y bases de datos que forman parte de Internet, pero que escapan (de manera deliberada o no) a la indexación de los motores de búsqueda, y que por tanto se consideran de difícil acceso.

Ingeniería Social: Conjunto de técnicas utilizadas para engañar a un usuario a través de una acción o conducta social. Consiste en la manipulación psicológica y persuasión para que voluntariamente la víctima brinde información personal o realice algún acto que ponga a su propio sistema en riesgo. Suele utilizarse este método para obtener contraseñas, números de tarjetas de crédito o PIN, entre otros.

Phishing: uno de los métodos ms utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta´, como puede ser una contraseña o información detallada sobre tarjetas de crédito, u otra información bancaria de la víctima.

Malwertising: se trata de anuncios donde **los atacantes ocultan en la publicidad el código malicioso** y no es necesario hacer click o descargarlo para infectarse.

Cryptoware: Es la encriptación del ransomware, se ha convertido en la amenaza de malware más intensa, eclipsando el robo de datos malware y troyanos bancarios. Con el criptoware convirtiéndose una amenaza clave para los ciudadanos y las empresas, la aplicación de la ley y la industria de seguridad de internet ha respondido rápidamente y en concierto, con prevención y conciencia campañas y asistencia técnica, y operaciones dirigidas los grupos criminales y la infraestructura involucrada.