Universitat Oberta de Catalunya

uoc.edu

Estudio del impacto de un Ransomware a una PYME

Alexandra Rodríguez Marco

Máster Universitario en Ciberseguridad y Privacidad

Privacidad

Albert Jové Canela

Cristina Pérez Solà

Diciembre de 2021

A) Creative Commons:

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio del impacto de un Ransomware a una PYME*
Nombre del autor:	*Alexandra Rodríguez Marco*
Nombre del consultor/a:	*Albert Jové Canela*
Nombre del PRA:	*Cristina Pérez Solà*
Fecha de entrega (mm/aaaa):	12/2021
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Privacidad*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ransomware, PYME*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En la sociedad actual la informática es empleada en prácticamente todos los ámbitos, para ello se gestionan grandes cantidades de datos de distintos caracteres.

Las empresas medianas y pequeñas no suelen tener medidas seguridad por el coste de implantar y mantener estas, todo esto lo conocen los cibercriminales y se aprovechan de esto para atacar y lucrarse. Un modus operandi habitual es realizar un ataque masivo, introduciéndose en las organizaciones mediante descargas por un correo o sitios web, explotando vulnerabilidades de sistemas o servicios expuestos, y de este modo alojar un programa malicioso que cifra la información, para no hacerla accesible, este programa es conocido por el nombre de Ransomware. Posteriormente, los atacantes piden un rescate para poder recuperar dichos datos y así sacar un beneficio económico, además pueden espiar, hacerse con propiedad intelectual o con información de gobiernos.

Con este estudio se quiere realizar un estudio de la situación actual de una PYME o MicroPYME para evitar ser víctima de un ataque por Ransomware o cuando ya se ha visto afectada minimizar sus consecuencias o impacto.

Abstract (in English, 250 words or less):

In today's society, computer science is used in practically all areas, for these large amounts of data of different source.

Medium and small companies do not usually have security measures for the cost of implementing and maintaining these, all this is known by cybercriminals and take advantage of this to attack and profit. A common modus operandi is to carry out a massive attack, entering organizations through email downloads or websites, exploiting system vulnerabilities or exposed services, and in this way, insert a malicious program that encrypts the information, in order not to make it accessible, this program is known by the name of Ransomware. Subsequently, the attackers ask for a ransom to be able to recover said data and thus obtain an economic benefit, they can also spy, get hold of intellectual property or information from governments.

With this study we want to carry out a study of the current situation of a SME or Micro-SME to avoid being a victim of a Ransomware attack or when it has already been affected to minimize its consequences or impact.

Agradecimientos

A mi familia, especialmente dedicado a mi padre y mi abuela.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En la actualidad la tecnología informática está siendo aplicada en práctica todos los ámbitos de la vida de las personas, como el simple hecho de pedir una cita en el sistema sanitario, realizar una compra con una tarjeta en una tienda de barrio, incluso al comunicarse con algún familiar vía Zoom. Para poder realizar todas estas acciones y muchas más, tecnológicamente se emplean equipos informáticos que usan grandes cantidades de datos. En estos equipos se alojan todo tipo de archivos con información de mayor o menor sensibilidad, como puede ser datos médicos de pacientes, datos financieros de grandes corporaciones, como los de un autónomo e incluso los intereses o debilidades de una persona.

Hoy en día, la venta de información es un negocio muy rentable, tanto para multinacionales como es Google, que vende los datos de los usuarios, como en los mercados negros, donde se vende todo tipo de información. En 2009, en el periódico El Mundo publicó una noticia, la cual se hizo eco el CCN-CERT, en esta se indicaba que en ese momento se podía pagar hasta 300 euros por los datos robados de una tarjeta de crédito o incluso 800 euros por el envío de un millón de correos basura o 'spam'[1], en mercados negros.

Es sabido que la información es poder, por ello los ciberdelincuentes han marcado como uno de sus objetivos el poder robar esta por cualquier medio, para que les reporten beneficios económicos, para obtenerla los delincuentes emplean varias técnicas y métodos, entre ellos el Ransomware.

Este consiste en una extorsión que se realiza a través de un malware que se introduce en los equipos de una organización. Este software malicioso secuestra la información de la empresa, así impide el acceso a esta cifrándola, lo que puede provocar pérdidas económicas y posibles daños reputacionales de la imagen de la organización

Según un informe del CCN-CERT[2] sobre las tendencias de las ciberamezas, ya en 2019, se emplearon dos metodologías de ataque principalmente: uno fue por Ransomware, para cifrar los discos de las víctimas y posteriormente solicitar un rescate, especialmente en campañas definidas como Human Operated Ransomware (HOR); y por otro el ataque de fraude del CEO.

En la situación actual provocada por la pandemia, las empresas se han visto obligadas en cambiar su forma de trabajar, la localización de sus empleados e inclusos sus procesos han cambiado, esta ha propiciado un ambiente en que desde las grandes empresas hasta las pequeñas se siguen viendo afectadas por este tipo de ataques, como sucedía en 2019. Ya que este afecta a todo tipo de equipos, desde ordenadores de sobremesa y portátiles, servidores web, servidores de ficheros, otros servidores e inclusive dispositivos móviles.

El escenario presente ha hecho que aflorasen las vulnerabilidades de los sistemas de la gran mayoría de las empresas, que no estaban preparadas en términos de seguridad para que su fuerza

[1] https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/125-el-mercado-negro-en-internet-mueve-unos-70000-millones-de-euros.html

[2] https://www.ccn-cert.cni.es/sobre-nosotros/centro-criptologico-nacional.html

de trabajo pudiera operar en remoto. Los delincuentes o grupos organizados han visto la oportunidad y han actuado empleando ataques cada vez más estudiados y sofisticados con el objetivo no solo de robar dinero a empresas o pedir un rescate por liberar sus recursos, sino para espiar, hacerse con propiedad intelectual o información de todo tipo de organizaciones.

Durante este último año se han visto multitud de ataques, desde grandes empresas del sector sanitario, como fue el de SegurCaixa Adeslas, el 9 de septiembre de año pasado, como también al gobierno, como en el caso del ataque al SEPE[3], el 9 de marzo de 2021, y haciéndose eco de estos casos los medios de comunicación.


El sistema informático del SEPE sufre un ciberataque

El Ministerio de Trabajo asegura que el pago de prestaciones no se va a ver afectado

EL PAÍS

Madrid - 09 MAR 2021 - 14:19 CET

Ilustración 1 - Ciberataque al SEPE[4]

Todas las organizaciones son susceptibles de ser atacadas mediante programas maliciosos, ya sea Ransomware o cualquier otro software malintencionado. Existe una falsa idea entre algunos empresarios, en especial de las pequeñas, piensan que no son objetivos y que no las atacaran, porque no son nadie importante y su información no tiene valor, por lo contrario, se está observando habitualmente este tipo de empresas están sufriendo este tipo de ataques. En muchas ocasiones, lo que sucede es que no llegar las noticias de dichos ataques a la opinión pública, en las que se ven afectadas algunas PYMEs[5] o MicroPYMEs.

El 99,8% del tejido empresarial español son PYMEs, que no creen que sean objetivo de estos delincuentes y tan sólo el 36% de estas empresas tienen protocolos básicos de seguridad según un estudio realizado por Google[6]. De las PYMEs europeas que han sido víctimas de ciberataques, solo el 40% "sobrevive" pasados seis meses del incidente, es decir, el 60% no superan los efectos causados.

Con este estudio se quiere realizar un estudio de la situación actual de una PYME o MicroPYME para evitar ser víctima de un ataque por Ransomware o cuando ya se ha visto afectada minimizar sus consecuencias o impacto.

1.2 Objetivos del Trabajo

El objetivo primordial de este trabajo fin de máster es realizar un análisis del impacto del Ransomware sobre las medianas y pequeñas empresas, para conseguir un resultado óptimo de dicho trabajo se deben cumplir los siguientes objetivos:

[3] Servicio Público de Empleo Estatal

[4] https://elpais.com/economia/2021-03-09/el-sistema-informatico-del-sepe-sufre-un-ciberataque.html

[5] http://www.iPYME.org/es-ES/DatosPublicaciones/Paginas/DefinicionPYME.aspx

[6] https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

- Objetivos del estudio:
    - Comprender y definir con claridad en que consiste un Ransomware
    - Conocer los tipos de Ransomware que afectan a las empresas,
    - Distinguir cuales son los vectores de entrada de un Ransomware en una PYME
    - Exponer y establecer cuáles son las medidas de seguridad que pueden tomar las pequeñas empresas dentro de sus capacidades.
    - Definir cuál es el protocolo de gestión de incidente de Ransomware en una pequeña empresa.
    - Conocer cuál es la legislación española aplicable en estos casos.
    - Describir los daños que puede sufrir una empresa tras sufrir un incidente de este tipo.
    - Establecer unas conclusiones tras finalizar el estudio.

- Objetivos de entrega:
    - Realizar y llevar a cabo las entregas parciales, remitirlas forma y en el tiempo correspondiente.
    - Desarrollar la memoria final del trabajo fin de máster.
    - Preparar la exposición del trabajo desarrollado y el video explicativo.

1.3 Enfoque y método seguido

Para cumplir los objetivos del este trabajo fin de máster se empleará una metodología de investigación exploratoria.

La elección de esta metodología ha sido porque los estudios exploratorios nos sirven para aumentar el grado de familiaridad con fenómenos pocos conocidos. En el caso de los ataques de Ransomware que afecte a PYMEs no existe gran cantidad de documentación, y como se ha indicado anteriormente cada día más empresas como estas se ven dañadas por estos incidentes de seguridad.

Para implementar dicho método se buscará y obtendrá información sobre la posibilidad de llevar a cabo una investigación más completa sobre esta casuística, como ejemplo por qué motivo en la actualidad tantas medianas y pequeñas empresas se ven envueltas en ataques efectivos.

Para la recolección de estos datos se empleará a su vez una investigación cualitativa y, por lo tanto, se usarán métodos de recolección de datos cualitativos en diversas fuentes, como documentos técnicos, artículos académicos, estudios específicos, entrevistas, noticias de interés, etc.; y métodos de análisis de contenido cualitativo.

Estas metodologías de investigación y recopilación de datos es la más adecuada para cumplir los objetivos de documentar y lograr entender la problemática estas pequeñas organizaciones, establecer barreras para evitar ser afectadas y encontrar posibles mitigaciones cuando ya se han visto involucradas.

1.4 Planificación del Trabajo

La planificación se encuentra en el Anexo I, página 60.

1.5 Resumen de entregas

Durante este semestre se realizarán una serie de entregas que compondrán el Trabajo Fin de Máster, los entregables son los siguientes:

- *PEC 1 - Plan de trabajo:* En este entregable se exponen las justificaciones por las que se realiza el proyecto y cuáles son los objetivos que se pretenden alcanzar. También se explica el enfoque y la metodología de la investigación para que se obtenga un resultado lo más optimo posible. Asimismo, se establece el punto de partida de este análisis y el coste.

- *PEC 2 - Entrega de seguimiento:* en esta etapa del proyecto se entregará parte de los puntos sobre los que se apoya todo el estudio, se define que es el Ransomware y cuál ha sido su evolución, incluyendo el estado presente y futuro, como también cuales son los vectores de entrada más empleados. Se realizará un análisis de los tipos de PYMEs y cuales suelen ser sus niveles de seguridad, además se investigarán algunos casos reales de ataques sufridos por estas empresas medianas. Se establecerán algunas de las medidas preventivas de seguridad para evitar posibles ataques de este tipo, y se hará una aproximación para acotar medidas para PYMEs grandes y medianas, como para pequeñas o MicroPYMEs.

- *PEC 3 - Entrega de seguimiento:* en esta entrega abordaremos cuando una PYME sufre un incidente de seguridad de este carácter, se intentará dar con apoyo con casos reales o casos próximos a la realidad que viven estas empresas. Se desarrollará con una estructura de los puntos habituales que suele tener el proceso de gestión de incidentes, incluyendo un punto importante ante la gestión que es las lecciones aprendidas y como prevenir sufrir de nuevo un ataque de este tipo.

- *PEC 4 - Memoria final:* esta es la última entrega, en donde se desarrollará los delitos que se pueden imputar a los que realizan este tipo como los que los sufren, y las sanciones que puede conllevar. Además, se planteó un punto en que se expondrán los tipos de daños que puede sufrir una empresa, como son los daños económicos por la interrupción provocada en su actividad, así como también el daño reputacional que podría causar. Por último, se obtendrán las conclusiones de todo el estudio.

- *PEC 5:* Este entregable es la preparación de la presentación y con la grabación de la exposición del proyecto, para su posterior defensa.

1.6 Estructura del proyecto

A continuación, se describe el estudio que se realizará sobre los ataques de Ransomware que puede sufrir empresas de un número bajo de empleados o de balances financieros por debajo de los 43 millones de euros[7]. La estructura del proyecto esta subdividida en varios puntos que son los siguientes:

- *Introducción*: establecemos los objetivos del estudio, así como el punto de partida del estado de las PYMEs frente a la seguridad implementada en ellas.

- *Ransomware:* Este tema engloba varios puntos, con los que se quiere exponer y definir que es un Ransomware, cual ha sido su evolución histórica y como podría ser en el futuro. Y como suele ser el vector de entrada a las organizaciones.

- *PYMEs:* En este apartado se contemplará que son las PYMEs y tipos, así mismo como la relación que tienen con la ciberseguridad, y las diversas campañas por parte de distintas organizaciones para el apoyo y concienciación que estas son también objetivos de dichos ataques.

- *Medidas preventivas antes de un ataque*: En este punto se exponen las medidas preventivas o formas que tienen los activos informáticos y humanos para prevenir la infección por un programa malicioso de este tipo.

- *Incidente – cuando se ha producido un ataque efectivo*: Se establecen los pasos a seguir para la gestión de un incidente de estas características, cuando se produce un ataque efectivo dentro de una pequeña organización.

- *Delitos asociados al Ransomware:* Se especificarán las leyes y normativas aplicables a este delito en la legislación española, tanto para los atacantes como los atacados, en el caso que haya fuga de información, como también las sanciones que conllevan.

- *Daños legales, económicos y reputacionales*: Se realizará un análisis de los daños que puede causar este incidente, tanto a nivel legal (con las multas o sanciones correspondiente), a nivel económico (por la disruptiva de la producción, sanciones económicas) como a nivel reputacional, que es el daño de la imagen que sufre dicha empresa. En alguna ocasión ha habido empresas que han podido superar el impacto del Ransomware, pero no el daño a su imagen.

- *Conclusiones:* En el último apartado de este TFM se presentarán las conclusiones a las que se ha llegado, después de haber realizado toda la investigación que se tiene como objetivo.

[7] http://www.iPYME.org/es-ES/DatosPublicaciones/Paginas/DefinicionPYME.aspx

1.7 Recursos necesarios y presupuesto del proyecto

Para llevar a cabo este proyecto se ha realizado una evaluación del tiempo y recursos que son empleados, para poder obtener los costes asociados, son los siguientes:

Recursos	Uso	Costes unitarios	Costes
Ordenador personal	Ordenador personal donde se realiza la recopilación de la información y redacción de la memoria.	700 euros	700 euros
Conexión de internet	Conexión para la recopilación de datos.	30 euros/mes	90 euros
Herramientas	Aplicación de edición de textos OpenSource	0 euros	0 euros
Analista de seguridad	Costo de las horas de un analista junior de seguridad. 280 horas para la preparación del TFM	13 euros/hora	3.640 euros
Coste total			**4.430 euros**

Ilustración 2 - Costes asociados al proyecto

2. Estudio del Ransomware en PYMEs

2.1 Ransomware

Antes de adentrarnos en cómo se pueden ver afectadas PYMEs por parte de un Ransomware. asentaremos las bases en que consiste este, cual fue, ha sido y será su evolución, así como también se verán los posibles vectores de infección para realizar un ataque de estas características.

2.1.1 ¿Qué es el Ransomware?

El término Ransomware proviene de la lengua inglesa, de la unión la palabra ransom[8], que significa rescate, y ware, que hace referencia a software[9], que es programa, es decir, se traduciría literalmente como "programa de rescate", pero también se puede denominar como "programa de secuestro".

Sobre el Ransomware se puede encontrar mucha literatura, y en esta lo definen como un software malicioso, o malware, que emplea cifrado para mantener la información de una víctima secuestrada. En este tipo de ataques, se pretende cifrar los datos críticos de un usuario u organización, para que no se pueda acceder a archivos, bases de datos, incluso aplicaciones, la clave de cifrado en estos casos solo la dispone el atacante.

Con posterioridad de la infección se exige un rescate para proporcionar acceso de nuevo a toda la información secuestrada, este rescate suele exigirse mediante una nota de rescate en donde se

[8] https://dictionary.cambridge.org/es/diccionario/ingles/ransom

[9] https://dictionary.cambridge.org/es/diccionario/ingles/software

indica la forma de pago, este habitualmente la moneda de pago suele ser Bitcoins[10]. El empleo de este tipo de moneda es muy común en los delitos cibernéticos por el anonimato y el no poder seguir las transacciones realizadas con esta.

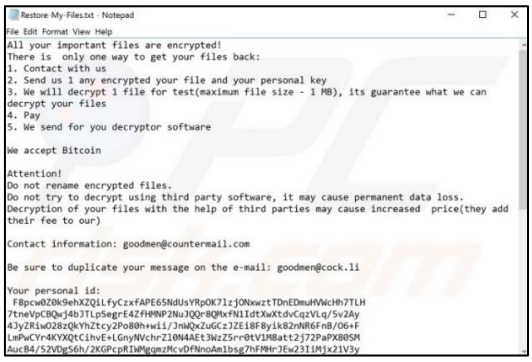


Ilustración 3 - Nota de rescate.[11]

El Ransomware a menudo está diseñado para propagarse a través de una red y en especial afectar a bases de datos y servidores de archivos, y por lo tanto puede paralizar rápidamente a toda una organización, suponiendo costosas interrupciones en las operaciones y la pérdida de información y datos críticos, incluso un daño reputacional, en ocasiones estos daños son irrecuperable para algunas organizaciones como indica el estudio realizado por Google[12].

Es una amenaza en auge, que genera miles de millones de euros en pagos a los ciberdelincuentes, provocando daños y gastos significativos para las empresas grandes y pequeñas, y de la misma manera afecta las organizaciones gubernamentales.

Para los criminales el realizar campañas de Ransomware se presenta como un modelo de negocio muy lucrativo, pudiendo ganar con ello miles de millones de dólares, como indica el FBI en su informe publicado el 02.04.2021; a continuación, se muestra la información más reseñable.

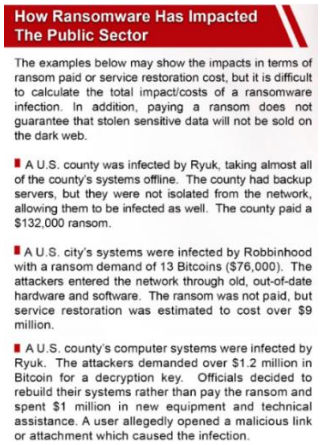


Ilustración 4 - Informe publicado por el FBI, Qué es y qué hacer acerca del Ransomware. [13]

[10] https://es.wikipedia.org/wiki/Bitcoin

[11] https://www.pcrisk.com/removal-guides/16476-lockbit-Ransomware

[12] https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

[13] https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

2.1.2 Historia, presente y futuro del Ransomware

Desde el origen del primer Ransomware han transcurrido más de 30 años, en concreto 32, por lo que este tipo de malware no es reciente, pero ha evolucionado desde entonces.

Echando la vista atrás podemos dividir la historia del Ransomware dos etapas claras, si clasificamos estos malware por el comportamiento, que sería el siguiente:

- 1ª etapa: Ransomware para el bloqueo de acceso al activo informático.

  Durante los primeros años el Ransomware empleaba la técnica de no permitir el acceso los hosts infectados hasta que la víctima podía pegar el rescate, pero sin encriptar la información. El objetivo solía ser organizaciones gubernamentales.

  Este tipo de Ransomware era muy rentable, pero entro en desuso por las autoridades podían localizar a los atacantes por el método de pago que se empleaba y los delincuentes se encontraban expuestos.

- 2ª etapa: Ransomware para el cifrado de información.

  Los últimos años, en especial a partir de 2015 se hizo popular el empleo del Ransomware que cifra la información de la víctima y el método de pago suele ser en criptomonedas. Como se ha comentado anteriormente estas proporcionan una cierta impunidad y anonimato a los criminales, por el hecho de no poder ser rastreadas las operaciones. Todas estas casuísticas han propiciado que este tipo de ataques no se lleve por un individuo, sino que se han llevados grupos del crimen organizado.

  En la siguiente gráfica basada en datos de en las estadísticas de Kaspersky Security Network, se observa en un año, de 2014 a 2015, el número de ataques se quintuplicó

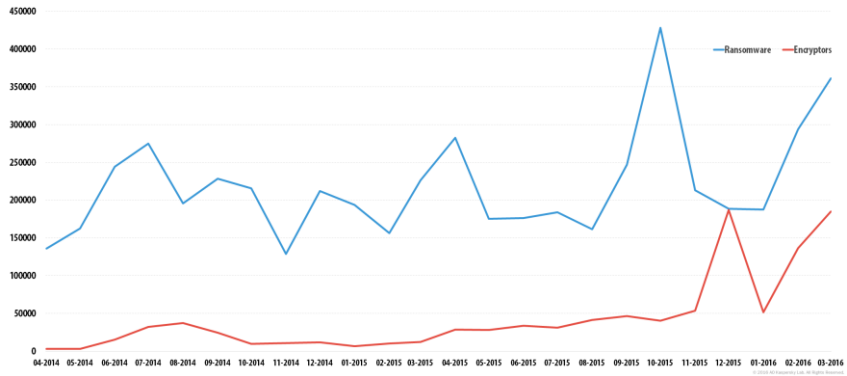


Ilustración 5 - Gráfica evolución de ataques Ransomware. [14]

  En esta etapa hay muchos modos en las que un usuario puede ser infectado, la más habitual es mediante un email con un archivo malicioso adjunto, enlaces web acortados, redes sociales, mensajes SMS o correos electrónicos de spam tradicionales.

- 3ª etapa: Ransomware dirigido.

[14] https://latam.kaspersky.com/blog/Ransomware-blocker-to-cryptor/7295/

En la actualidad se está contemplando el incremento del uso de Ransomware operados por humanos[15].

El ransomware operado por humanos es diferente, ya que son operados por un usuario u organización y el ataque se centra en una organización, de la que buscan por diversos métodos los accesos a estas.

Las características que los distinguen de los Ransomware de la etapa 1 y 2 es que incluye el robo de credenciales y un movimiento, y posteriormente despliega el Ransomware sobre activos críticos.

Ransomware es una parte del todo el ataque, porque también sustraen información para presionar en la extorsión y además antes de desplegarlo los atacantes en ocasiones borran las copias de seguridad. A parte de todo esto, los criminales preparan puertas traseras para poder volver a la organización.

2.1.3 Vectores de infección

Los criminales emplean varias de técnicas para infectar los sistemas de las víctimas con Ransomware, a esto se le denomina vector de entrada o infección. Los cuales no son distintos del resto de vectores que emplean los softwares maliciosos como pueden ser virus o troyanos.

Estas técnicas están en constante cambio y actualización, para que realmente sean más efectivas y para evadir la detección, y de este modo no puedan parar la infección.

Los ciberdelincuentes que utilizan con frecuencia las siguientes técnicas para infectar a las víctimas con Ransomware:

- *Campañas de phishing por correo electrónico*

Estas campañas consisten en que el atacante envía un correo electrónico que contiene un archivo o enlace malicioso, que está diseñado para engañar al objetivo para que interactúe con él, entonces el malware es desplegado cuando un usuario ejecuta el archivo o enlace.

Al principio de los tiempos los delincuentes emplearon estrategias genéricas de spam para distribuir su malware, por lo contrario, la tendencia actual se trata de campañas más específicas y dirigidas al nicho que se quiere atacar.

Existe una técnica en que el atacante compromete, previamente con malware, una cuenta de correo de una víctima y a partir de esta puede extender más la infección.

Un de los casos más empleados en Ransomware, es el envío de correos que contiene una posible factura, y el archivo realmente es un archivo malicioso, que no tendrá una extensión no relacionada con una factura.

A continuación, se muestra un ejemplo de un correo relacionado con el envío de una supuesta factura en formato *.ZIP.

[15] https://docs.microsoft.com/es-es/security/compass/human-operated-ransomware

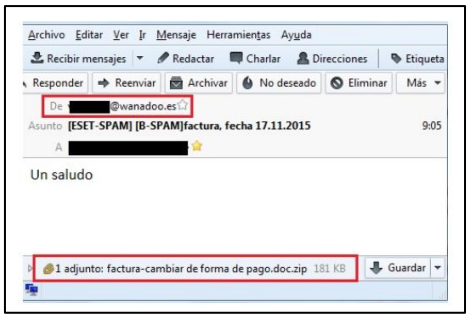


Ilustración 6 - Mensaje que contiene un archivo malicioso imitando una factura. [16]

Otro modo habitual para distribuir Ransomware es el empleo de correos haciendo se pasar por empresas de logística, entidades bancarias o administraciones publicas de gobiernos.

Uno de los ejemplos más recursivo en estos últimos años es el correo sobre la entrega de un paquete de la compañía pública Correos, como se muestra a continuación

Ilustración 7 - Mensaje suplantando a Correos con el Ransomware Locky. [17]

Para evitar este tipo de ataques sean efectivos se recomienda concienciar a los usuarios, para que no abran correos con adjuntos o enlaces que no esperen o el origen es desconocido, o incluso revisando el dominio del correo del remitente.

- *Vulnerabilidades del protocolo de escritorio remoto:*

El protocolo RDP[18] permite controlar los recursos y datos de un activo de forma remota por una conexión través de Internet.

Esta técnica consiste en explotar una vulnerabilidad del protocolo RDP, mediante de exploits, o por fuerza bruta. Un ejemplo de exploit de este protocolo sería el del CVE 2019-0708[19] (Bluekeep) entre muchos otros.

[16] https://blogs.protegerse.com/2015/11/19/facturas-falsas-propagan-Ransomware-por-correo-electronico/

[17] https://www.welivesecurity.com/la-es/2016/05/12/Ransomware-locky-falso-email-de-correos/

[18] Remote Desktop Protocol, Protocolo o Escritorio Remoto en castellano. Es una tecnología desarrollada por Microsoft y que facilita el control remoto de una computadora con Windows sin necesidad de estar delante de ella.

[19] https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-0708

El método más empleado de esta técnica es el uso de fuerza bruta, para ello el atacante usa credenciales obtenida en distintas fuentes como podría ser por un leak[20] de credenciales o incluso por la explotación de una BBDD[21].

Una vez que tienen acceso RDP, los delincuentes pueden desactivar los sistemas de seguridad para que no sea detectado e introducir cualquier malware en el sistema de la víctima.

Para evitar este tipo de ataques se recomienda una buena política de credenciales, implementar un segundo factor de autenticación y no emplear las credenciales de la organización para plataformas fuera de estas, así como también el acceso mediante una VPN.

Es habitual que en muchas ocasiones se encuentre el puerto RDP (3389) expuesto al mundo como indica el informe de Shodan.io, como se muestra en la imagen inferior, y en algunos casos dichos puertos no están configurados correctamente y suponen una puerta trasera por la cual puede entrar un ciberdelincuente.

Ilustración 8 - Datos de puertos RDP abiertos en Shodan.io.[22]

- *Vulnerabilidades de software:*

Una técnica empleada es aprovechamiento de las vulnerabilidades de los activos, habitualmente de los softwares más utilizados y de esto modo los atacantes podrían tomar el control del host de la víctima.

Un ejemplo de esta técnica es el mítico WannaCry, este aprovechaba una vulnerabilidad critica de Windows, para ello se empleaba el exploit Eternablue (CVE-2017-0144). Consistía en que la

[20] Fuga de información.

[21] Base de datos.

[22] https://www.shodan.io/search/report?query=remote+desktop

versión 1 del servidor SMB (SMBv1) acepta en varias versiones de paquetes específicos en Windows de atacantes remotos, y esto permitía ejecutar código en el ordenador en cuestión

Para evitar este tipo de ataques se recomienda una tener los SO y programas actualizados a la última versión del proveedor.

- *Otros:*

Existe otros vectores que actualmente no son tan común el uso como podría ser anteriormente, como son las descargas archivos infectados en sitios web o P2P[23], navegación en páginas web maliciosas y periféricos infectados.

2.1.3.1 Tendencia en vectores de ataque

Se puede ver una tendencia del uso de unas técnicas de distribución frente a otras de este tipo de malware.

Durante los 3 primeros meses de 2019 se ve un aumento del 63,5% del uso de ataques de vulnerabilidad de RDP frente al que había sido hasta el momento el ganador, con un 30,4%, que eran los correos maliciosos, estos datos son obtenidos por McAfee.[24]

Según los datos analizados en el artículo "Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021[25]" de Coveware.com, se obtiene que la tendencia de 2021, en la cual se ve un incremento de los ataques por el compromiso del protocolo de escritorios remotos que, por phishing, como se muestra en la siguiente gráfica.

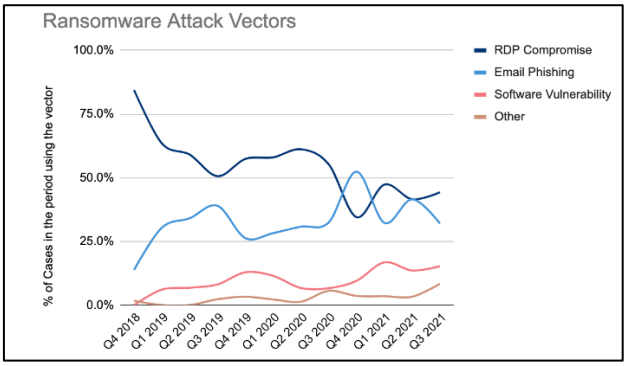


Ilustración 9 - Los vectores de ataque de Ransomware más comunes en el tercer trimestre de 2021[26]

2.2 PYMEs y ciberseguridad

En la actualidad casi cada día se pueden ver en los medios de comunicación casos en el que grandes corporaciones e inclusive gobiernos sufre ataques cibernéticos. Dichos ataques no son exclusivos de grandes empresas, sino también se ven afectadas medianas y pequeñas empresas, pero estas noticias no saltan a la palestra mediática.

---

[23] Descargas de punto a punto, como pueden ser en plataformas como uTorrent, BitTorrent, eMule, Gnutella, etc.

[24] https://hipertextual.com/2019/07/escritorio-remoto-malware-mcafee

[25] https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts

[26] https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts

Dentro que el ámbito informático, aún están sin regular algunos aspectos y aún se encuentra con falta de control, pero a nivel europeo se dispone un Reglamento en vigor, que es RGPD[27], que establece las bases para la protección de datos personales y las sanciones que conlleva en no proteger dichos datos.

El impacto que puede sufrir una organización ante un ataque de este tipo, no solo es a nivel económico, por la paralización de la actividad, la restauración al punto de partida, sino también a nivel de daño reputacional o imagen y además se suman las sanciones impuestas por RGPD, como también pueden ser por incumplimientos contractuales, cancelación de pedidos, penalizaciones por discontinuidad de servicios ofrecidos a terceros, etc. Cualquier empresa grande o pequeña tendrá que asumir todo este impacto, y se puede asumir que para una PYME esto puede ser más difícil de superar que posiblemente para una empresa grande.

En 2018, se habría registrado un total de 102.414 ataques en España, como se indica en un informe encargado por Google. Y el ataque más común en las PYME, que estas habrían sufrido, serían los incidentes de tipo Ransomware[28].

La problemática actual en muchas PYMEs en España, es que muchas de ellas no cuentan con equipos técnicos informáticos, y mucho menos con especializados en seguridad informática, para poder ser asesorados y que se ocupen de la seguridad de estas. Existe la opción, que está en auge, de externalizar estos servicios, para recibir un asesoramiento y apoyo para estas tareas.

Según datos de la Guardia Civil, la gran mayoría de los ataques cibernéticos en España se realizan a PYMEs, que son el objetivo del 70% de los ciberdelitos[29]. Esta cifra podría ser inferior de lo que en realidad es, porque no todas las empresas víctimas de ciberataques denuncia, en ocasiones evitan hacerlo por miedo a dañar su imagen.[30]

Pero, sin embargo, ser preventivos es el primer punto básico para minimizar los riesgos y es importante que la empresa tenga definidos sus planes de seguridad tecnológica.

Las PYMEs no suelen priorizar los trabajos relacionados con la ciberseguridad frente a otros, es decir, invierten pocos recursos tanto económicos, como de persona y tiempo, a estructurar sus inventarios de activos y a considerar las medidas de seguridad y estructura necesarias para prevenir ataques, en poner en marcha planes de sensibilización, concienciación y formación en seguridad a su personal, como también tener pólizas de seguros de ciberseguridad.

Las estadísticas demuestran que solo el 10% de las empresas de que tiene menos de 10 trabajadores tiene una política de seguridad y un plan de respuestas frente ataques, en cambio el

---

[27] https://www.boe.es/doue/2016/119/L00001-00088.pdf

[28] https://www.iniseg.es/blog/ciberseguridad/diagnosticando-la-ciberseguridad-en-espana/

[29] https://www.ituser.es/seguridad/2021/04/pymes-ante-el-riesgo-de-un-ciberataque-tres-cuestiones-que-tienen-que-valorar

[30] https://www.iniseg.es/blog/ciberseguridad/diagnosticando-la-ciberseguridad-en-espana/

50% de las empresas de 50-249 empleados sí que tienen establecida una política de seguridad y un plan de contingencia.[31]

En la actualidad ciberseguridad en las PYMEs españolas es reactiva. Tan solo un 36 % [32] de las PYMEs tienen protocolos básicos de seguridad, como la verificación de dos pasos para el correo de empresa, y el 30 % de las webs no disponen del protocolo https. A nivel europeo no está mucho mejor, el 60% de las PYMEs europeas que son víctimas de ciberataques desaparece en los seis meses siguientes al incidente, el coste medio del ataque ronda los 35.000 euros.

Con la difusión en los medios de comunicación se tiene una mayor conciencia a nivel global y empresaria de los riesgos de seguridad que se pueden llegar a correr. Todavía hay un largo camino por recorrer hasta conseguir concienciar a las empresas de la importancia real de su seguridad tecnológica.

Prevenir es el recurso mejor invertido que, además, será siempre dimensionado a nuestro tamaño y escala de prioridades

2.2.1 Casos reales

Como se ha indicado anteriormente los casos de ataques de Ransomware sufridos por PYMEs no llegan a los medios de comunicación, por el hecho que tiene mucha más relevancia los casos en que se ven afectadas grandes corporaciones u organismos públicos, por ello es difícil encontrar ejemplos conocidos.

Para mostrar estos casos se emplearán los ejemplos de posibles incidentes que se pueden dar en las PYMES.

Un caso habitual de vector de infección es recibir una notificación de un servicio fiscal. Por ejemplo, la llegada de un email indicando que no se ha realizado el pago de un impuesto al completo y se impondrá un recargo, esto provocará en la víctima un interés por apelar, y el correo le instan a que descargue un formulario, lo rellene y adjunte. En dicho memento el atacante consiguió que la víctima descargara y ejecutara el malware.

El programa malicioso tendrá vía libre para cifrar los archivos y dejar las instrucciones para el rescate.

La Agencia Tributaria suele ser una entidad suplantada en campañas de correos masivos de phishing, que pueden contiene malware para infectar a los receptores. Los atacantes en ocasiones emplean la técnica explicada en el anterior párrafo para que el afectado pique, indicando que falta una parte de un adeudo, como se muestra en la siguiente imagen.

---

[31] https://www.ibercaja.es/empresas/corner-del-especialista/informacion-seguros/ PYMEs-vulnerables-ciberseguridad/

[32] "Panorama actual de la Ciberseguridad" es el estudio realizado por Google. https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf.


De: aviso@agencia.es
Fecha: 12 de enero de 2021, 9:16:30 CET
Para:
Asunto: Errores en su Declaracion de Renta

Agencia Tributaria

Estimado Contribuyente,

Se han detectado irregularidades en su declaracion jurata de Renta correspondiente al 2019.
Adjunto a este mensaje va su factura con la deferencia que debe
En caso de no realizar el pago en fecha puede incurrir en cargos y multas extras.

DESCARGAR FACTURA

Ilustración 10 - Correo suplantación de la Agencia Tributaria[33].

Por el impacto que causa a nivel social, la Agencia Tributaria tiene un apartado en su sitio web en donde se listan las campañas conocidas de suplantación[34] para avisar a los usuarios.

Como la anterior modalidad también los empleados de una PYMEs puede recibir un correo exigiendo el pago de un impuesto, que el antivirus no bloqueo, pero un usuario concienciado puede descartar el abrirlo y pagar la exigencia, como se indica en el siguiente aviso INCIBE: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-distribucion-malware-email

También se suele recibir correos de suplantación en el que se esconden enlaces o archivos maliciosos, como la propuesta de una oferta que hará mejorar la contabilidad de la empresa. Los correos electrónicos fraudulentos que se parecen a correos electrónicos de ventas masivas, pero que incluyen archivos adjuntos maliciosos destinados a parecerse a información sobre productos o servicios, pueden ser un vector de entrada.

En estos tres ejemplos anteriores se emplea las campañas de phishing como vector de entrada, y la ingeniería social. Pero como se indicó el vector de entrada que más se está popularizando es el de la vulnerabilidad o fuerza bruta del protocolo RDP.

Se han visto varias empresas pequeñas en que esta técnica ha sido el vector de entrada para el Ransomware, con los datos que muestra shodan.io acerca que el puerto 3389 es muy habitual que se encuentre expuesto. En muchas ocasiones este puerto no se está correctamente configurado o incluso si no fuera necesario deshabilitado.

Esta técnica únicamente no se está empleando con PYMEs sino también con organismos y empresas grandes, y se ha visto favorecido por el confinamiento de COVID-19.

En muchas empresas se tuvieron que habilitar los escritorios remotos para poder teletrabajar y esto fue aprovechado por los grupos criminales, por lo que han incrementado muy notablemente los ataques de fuerza bruta contra el RDP. Esto incremento se ha visto reflejado en las detecciones realizadas por las soluciones de seguridad de ESET en España como se muestra en la siguiente gráfica.

---

33 https://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/_comp_Consultas_informaticas/_Informacion_de_casos_de_Phishing_/12_01_2021_Errores_en_su_Declaracion_de_Renta.shtml

34 https://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/_comp_Consultas_informaticas/_Informacion_de_casos_de_Phishing_/_Informacion_de_casos_de_Phishing_.shtml

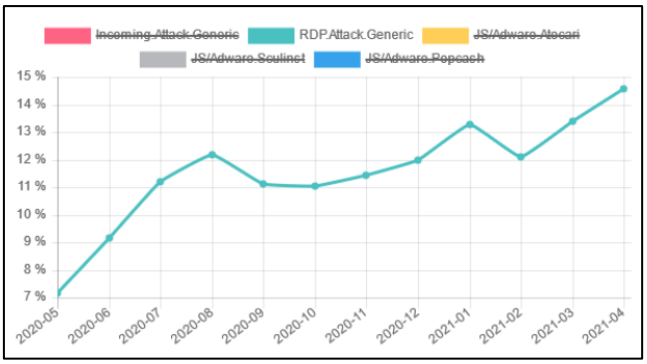


Ilustración 11 - Casos de ataques RDP en España, datos de ESET[35].

Según los datos de ESET de las fechas de cuando se producen estos ataques, se puede observar que la gran mayoría se producen durante los fines de semana. El acceso en dichos periodos tiene sentido porque es cuando no suele coincidir con el posible horario laboral de la víctima, por lo que es difícil coincidir en el logueo de víctima y atacante al mismo tiempo. A menos que se monitoricen los accesos, nadie podría darse cuenta de los accesos fuera de horario laboral y el atacante tiene libertad de poder moverse por la red corporativa.

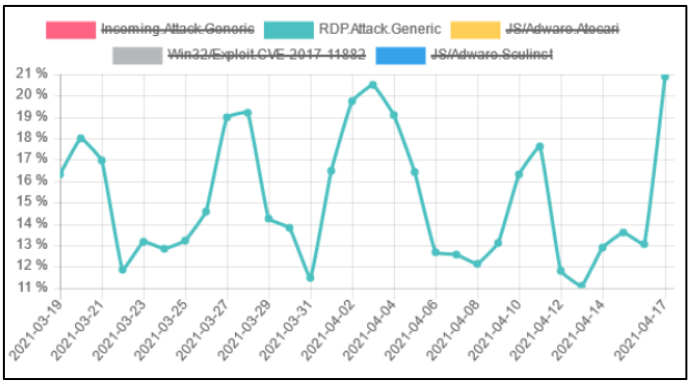


Ilustración 12 - Fechas de ataques RDP en España, datos de ESET[36].

Otro vector de infección sería la explotación de vulnerabilidades del sistema, en la actualidad aún se continúa usando las vulnerabilidades MS17-010, popularizadas por primera vez por el exploit EternalBlue y el Ransomware WannaCry

Estas vulnerabilidades sen han usado en Ransomware vigentes como Ryuk, SamSam y Satan, y algunas organizaciones no han sido parcheadas, siguen siendo puertas traseras para acceder a las organizaciones y permiten a los atacantes propagarse rápidamente de un host a otro en toda la red.

Este vector de infección se sigue dando en PYMEs en que el técnico que mantiene el sistema aun no parcheo el servidor.

2.3 Medidas ante un Ransomware

Existen dos medidas ante un Ransomware, que puede ser:

---

35 https://blogs.protegerse.com/2021/04/20/Ransomware-en-espana-incremento-de-los-ataques-a-rdp-como-puerta-de-entrada-para-los-delincuentes/

36 https://blogs.protegerse.com/2021/04/20/Ransomware-en-espana-incremento-de-los-ataques-a-rdp-como-puerta-de-entrada-para-los-delincuentes/

- Las medidas preventivas o activas: Con estas se pretende proteger y evitar la infección de los sistemas mediante el ataque de Ransomware. En los puntos del 2.3.1 y 2.3.2 de este estudio se desarrollan. Aplicar las medidas de seguridad recomendables no implica no poder ser atacado e infectado por Ransomware, pero sí que el impacto podrá ser menor que si no se dispusieran de estas.
- Las medidas reactivas de reacción o correctivas: Con estas se pretende dar respuesta y corregir los efectos causados por un ataque de Ransomware. En el punto 2.3.3, se desarrollarán las medidas reactivas ante un Ransomware en una PYME.

2.3.1 Medidas preventivas de seguridad

Las medidas preventivas que se deben tomar en todas las organizaciones para reducir el impacto de un posible Ransomware, en los puntos siguientes concretaremos en más detalle cuales podrían tomar las PYMEs, son las siguientes:

- *Copias de seguridad*

Como primera medida preventiva se recomienda realizar copias de seguridad periódicas y se debería comprobar que es posible restaurarlas. Dicha medida nos permitirá recuperar la actividad de la empresa en poco tiempo

Las recomendaciones básicas según INCIBE en cuanto a las copias de seguridad son:

- Realizar al menos tres copias de seguridad actualizadas y en distintos soportes. Si una organización ha sufrido un ataque por Ransomware se puede encontrar en tres situaciones:
  - Querer pagar el rescate para descifrar la información, no se recomienda esta opción porque ayuda a lucrase a las organizaciones criminales y no se asegura el poder desencriptar la información con la clave facilitada.
  - Recuperar la información por una backup.
  - Asumir que se ha perdido la información.
- La mejor opción de las 3 sería realizar los backups de la información y aplicar la llamada regla ‘3-2-1’. Esta consiste en realizar, al menos, tres backup de datos, dos de ellas se deberán guardar en plataformas diferentes, como pude ser una en un disco externo y otra en la nube, y la tercera en una ubicación diferente a las anteriores. A parte de todo esto, se debería comprobar que estas copias se podrían restaurar correctamente.
- Lo más recomendable es que las copias de seguridad no sean accesibles desde la red, para evitar el cifrado de todas las copias por parte de un atacante. En ocasiones no es posible que sean inaccesibles, como ocurren con los backup en la nube, por ello se recomienda que las otras copias no sean accesibles. En la actualidad hay tipo de Ransomware que buscan activamente conexiones y otros activos en su misma red, como podrían ser discos externos o USB conectados, incluso programas como OneDrive o Dropbox, para replicarse y ejecutarse automáticamente, por lo se propagan rápidamente, para así evitar el cifrado de todas las copias.
- Es conveniente seguir una política de optima de realización de backups. Para determinar la frecuencia con la que se pudieran realizar copias de seguridad es necesario efectuar un análisis del número de datos o archivos a guardar, del coste de almacenamiento, como

también de las obligaciones legales, como el cumplimiento de RGDP[37]. A modo orientativo INCIBE aconseja que sería una buena práctica realizar y conservar copias de seguridad con la siguiente frecuencia:

- Copias incrementales diarias.
- Copias totales una vez a la semana.
- Conservación de las copias totales un mes.
- Almacenamiento de la última copia del mes durante un año.[38]

- La información sensible de la empresa se recomienda que esté cifrada, como los soportes que la contienen, por motivos de seguridad y confidencialidad de esta. Si se viera involucrada en un Ransomware, el atacante robaría información cifrada, de este modo no podrá acceder a ella. Se recomienda que la clave de descifrado no esté ubicada en el mismo sitio que la información, para impedir que los delincuentes obtengan la información en claro.

- *Navegación segura*

Otra medida de seguridad es emplear VPN siempre que sea posible. Las redes privadas virtuales son un tipo de conexión de red en el que el tráfico viaja cifrado y en el que los atacantes no pueden visualizar su contenido. Además de todo esto, es recomendable que los trabajadores no se conecten a redes públicas con los dispositivos corporativos.

Estas conexiones se suelen utilizar cuando los empleados están fuera de la organización y es necesario tener acceso a documentos internos. Para que esta red sea aún más segura se podría implementar un segundo factor de autenticación para acceder a esta.

Se debe evitar el visitar sitios web de contenido dudoso, mantener actualizados los navegadores web y el sistema operativo, así como cualquier solución de seguridad que se emplee, como también la seguridad lógica. Para restringir la navegación se podría realizar desde los firewalls corporativos, algunos permiten el bloque de acceso de algunas páginas web que tenga TLD concretos. Por ejemplo en ocasiones algunos TLD de dominios son empleados para la referencia la temática del sitio web, como ocurren con páginas de pornografía que se suele asociar a TLDs como .xxx, .porn o .adult, los cuales se podrían bloquear.

- *Segmentación de la red*

La segmentación de red crea múltiples segmentos aislados dentro de una red más grande, esto puede ser de manera física o lógica, cada uno de los cuales puede tener diferentes requisitos y políticas de seguridad. Estas subredes contienen tipos específicos de aplicaciones o terminales que tienen el mismo nivel de confianza.

Esta segmentación no evita que un Ransomware la infección por Ransomware, pero sí que puede limitar la expansión de un segmento a otro, y de este modo contener el Ransomware en un segmento o los que haya afectado, es decir, aislarlo de la red no afectada.

[37] Reglamento Europeo de Protección de Datos

[38] https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

- *Segmentación de la red de máquinas virtuales*

La segmentación de redes de máquinas virtuales se emplea para la comunicación entre las máquinas virtuales, hace la función de un cortafuegos o enrutador para permitir o denegar el tráfico generado entre segmentos o niveles de una red, esto les afectas a las organizaciones que tienen una infraestructura virtualizada.

- *Protege la seguridad WIFI*

Se deberá configurar la red Wifi corporativa o la que emplee el trabajador si estuviera teletrabajando, para que el riesgo en esta sea menor. La configuración por defecto del router no siempre es la más apropiada por ello se debe configurar. El router debe incorporar un protocolo WPA entre sus medidas de seguridad.

La configuración al menos deberá contemplar la autenticación para acceder a esta, y el cifrado de datos intercambiados entre los nodos de la WLAN, por si se realizara un "man in the middle"[39] por parte de un ataquen los datos no se podrían leer.

- *Inventario de software*

Es recomendable tener un inventario de los software empleados y validados a nivel de empresa, para controlar los softwares instalados y los que se han instalado siendo inconsciente.

Los usuarios en algunas ocasiones no conocen algunos de los programas que tienen instalados en sus equipos, sin contar los que estén preinstalados en modo "valores de fabrica". En ocasiones algunas instalaciones legitimas lanzan otras instalaciones en segundo plano de otros softwares, que podrían ser maliciosas, y este comportamiento se ha visto en algunos malwares. Por ello, se recomienda el control del inventario de software, para detectar instalaciones sospechosas o no legítimas.

Una medida preventiva muy importante para evitar la instalación de software no validados es el control de los roles de usuarios, no permitiendo a un usuario general el lanzar instalaciones o permitirlas.

Las políticas de restricción del uso del software también pueden incluir controles para evitar que se ejecute malware. Algunos sistemas operativos, como Windows 10 Pro, incorporan sistemas específicos de protección contra el Ransomware.

[39] https://es.wikipedia.org/wiki/Ataque_de_intermediario

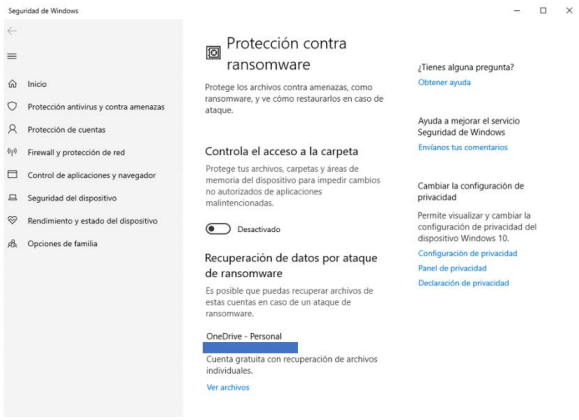


Ilustración 13 - Protección integrada contra Ransomware en Windows.

- *Actualizaciones*

Como se ha indicado en el punto de "Vectores de infección", una debilidad o vulnerabilidad puede suponer un punto de acceso para un atacante, que quiere infectar la organización con Ransomware. Por esto, es importante tener lo más actualizados posibles los sistemas que utilizas, menos vulnerabilidades tendrán y más difícil será que puedan entrar o infectar la organización.

Es recomendable que los sistemas operativos, aplicaciones y dispositivos tengan habilitada la instalación de actualizaciones de forma automática. Si emplea software a medida se debe exigir que se hayan tenido en cuenta los requisitos de seguridad y que cuentas con actualizaciones.

Una vulnerabilidad Zero-day es una vulnerabilidad que acaba de ser descubierta y que aún no existe forma de mitigarla. La amenaza es el periodo hasta que se consigue resolver o parchear dicha vulnerabilidad, y que en este tiempo los atacantes aprovechan para explotarla, como ocurrió en el caso del Ransomware WannaCry. Sin embargo, las organizaciones que tengan una buena política de actualización, también se puede ver comprometidas por la explotación de este tipo de vulnerabilidades.

- *Mínimos privilegios*

El principio básico de esta medida de seguridad es mantener los privilegios de seguridad al mínimo para que el usuario o grupo de usuarios puedan realizar su trabajo, de este modo evitar estos tengan más privilegios de los que necesitan.

Para los usuarios generales se han de emplear cuentas que tengan privilegios limitados, y no con privilegios de administrador.

El control de privilegios ayudara a la hora de permitir el acceso a ciertos directorios a los usuarios con bajos privilegios, la modificación de archivos y la ejecución. Esto proporciona una protección ante el uso indebido de los accesos a la información por parte de softwares no deseados o atacantes. Las cuentas con privilegios solo deben tenerlas los usuarios administradores.

También es aconsejable el uso de contraseñas robustas y política de contraseñas lo más seguras. Los atacantes tienen más posibilidades de acceder al sistema si las contraseñas son fáciles de descifrar.

Un método habitual usado por los atacantes es emplear ataques de fuerza bruta o de diccionario, por lo que se recomienda implantar políticas de bloqueo de credencial, como por ejemplo tener solo 3 intentos de acceso al sistema, si se falla 3 veces seguidas la cuenta se bloquea.

También es recomendable realizar una eliminación o deshabilitar cuentas que no son necesarias, por ejemplo, empleados que ya no pertenecen ya a la organización.

Como también se aconseja que no se emplee notas para apuntar credenciales corporativas, en el mercado existen varios gestores de contraseñas para guardarlas sin que sean apuntadas a la vista de cualquiera.

- *Exposición*

Uno de los principios básico de la seguridad es el de mínima exposición, por lo que se debe reducir la exposición al exterior de la red de la empresa, como la información, que los servicios que no sean necesarios tenerlos expuestos sean deshabilitados o bloquear el acceso a estos desde el exterior.

Para evitar la exposición una exposición innecesaria es recomendable separar los servidores accesibles desde el exterior, por ejemplo, las páginas web corporativas, de los servidores privados de nuestra organización, por ejemplo, los servidores que contienen la base de datos con la información de clientes y proveedores.

- *RDP*

Como se ha visto anteriormente, el tener expuesto el protocolo de acceso remoto puede suponer un vector de entrada muy atractivo para un atacante.

Las recomendaciones para aumentar el posible fracaso de una infección por un ataque de este protocolo serían:

  - Deshabilitar el protocolo si no es necesario el acceso.
  - Implantar el uso de una red VPN, además de esto el poder emplear un segundo factor de autenticación, como también la utilización de una política de contraseñas robustas.

- *Firewall*

Los cortafuegos o firewalls son sistemas de seguridad capaz de establecer reglas para bloquear o permitir conexiones de entrada o salida a las redes de una organización.

En estos configuraremos lo que está permitido y lo que no, como el tipo de conexión o si son entrantes o salientes, incluso a que equipos o segmento de red afecta, también se pueden bloquear direcciones IP y dominios. En el mercado existen firewalls privativos e incluso OpenSource, que puede ser implantado en cualquier empresa.

- *NIDS/NIPS*

En algunas ocasiones los propios cortafuegos incluyen lo que se denomina NIDS (sistema de detección de intrusos red) e NIPS (sistema de prevención de intrusos en red), estos se tratan de dos sistemas que ayudarán a mantener segura la red interna de nuestra empresa mediante un control pasivo y activo.

Es importante esta tecnología para prevenir el ataque e impacto de este sobre toda la corporación que está siendo monitorizada.

- *HIDS/HIPS*

Al igual que el NIDS e NIPS, existe unos sistemas de seguridad dirigidos a la protección en el mismo host, que son HIDS (Host Intrusion Detction System) e HIPS (Host Intrusion Prevention System) estos se tratan de dos sistemas que monitorizan la detección basada en host y la prevención.

Como el en el caso anterior son importantes estas tecnologías para prevenir el ataque e impacto a nivel host.

- *Antivirus*

Disponer de un antivirus habilitado, actualizado y correctamente configurado puede prevenir distintos tipos de ataques, entre ellos algunos Ransomware. Los antivirus han evolucionado y en la actualidad son los llamados EPP (Endpoint Protection Platform), es decir, es una solución de seguridad diseñada para detectar y bloquear amenazas a nivel de dispositivo. Estos realizan varias funciones, como pueden ser: la de antivirus, la de antimalware, prevención de intrusiones (IPS), prevención de fugas de datos (DLP), prevención de exploits y tecnología anti-Ransomware.

La evolución más avanzada de los tradicionales antivirus es el EDR[40] (Endpoint detection and response). Se trata de una herramienta que proporciona monitorización y análisis continuo del dispositivo y la red, el objetivo de esta es identificar, detectar y prevenir APT (amenaza persistente avanzada).

- *Vacunas antiransomware*

En la actualidad también se disponen de soluciones de seguridad que funcionan como vacunas contra código dañino de tipo Ransomware, como es microCLAUDIA[41].

Esta es el centro de vacunación del CCN-CERT, basado en el motor de CLAUDIA[42], se trata de un agente que se instala en los activos, de sistema Windows, el cual proporciona protección contra malware de tipo Ransomware.

MicroCLAUDIA no es una solución única para proteger de este tipo de ataques, sino que se trata de una solución complementarias a los EPP o EDR. Aunque es un desarrollo del CCN-CERT para organismos, también está disponible para empresas privadas[43].

- *Proxy*

El Proxy Web de una organización tiene la funcionalidad del control del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, etc. Esto permite gestionar algún tipo de tráfico que no se desea recibir en la organización, mediante la configuración de este sistema; como podría ser tráfico de países desde los que suelen realizar ataques, dominios de origen TOR, dominios de TLD especiales y usualmente usados para contener malware, etc.

---

[40] Recurso para combatir las amenazas avanzadas y responder a incidentes en los puntos finales de la red.

[41] https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html

[42] https://www.ccn-cert.cni.es/soluciones-seguridad/claudia.html

[43] https://s2grupo.es/microclaudia.html

- *DMZ*

Una recomendación es disponer una red DMZ, una zona desmilitarizada (demilitarized zone) o red perimetral, se trata de es una red local que se ubica entre la red interna de una organización y una red externa.

Al igual que la red interna, la DMZ es una parte de la empresa expuesta al exterior por lo que debe estar especialmente controlada y monitorizada, es recomendable instalar detectores de intrusos, debe configurar y proteger los servidores que la componen, y estos estar actualizados lo máximo posible.

En esta red podrían estar los siguientes equipos de una organización:

- Servidores de correo y servidores de correo web.
- Servidores de VPN.
- Servidores DNS.

Si se ha externalizado la infraestructura o el mantenimiento de esta, se debe incluir un acuerdo de nivel de servicio que garantiza la mínima exposición, ello conllevara menos riesgo a la organización.

- *Configuración del correo*

El correo electrónico es una de las principales vías de entrada de correos sospechosos de poder ser fraudulentos, contener adjuntos con malware o enlaces maliciosos. Por este motivo, estos deben configurarse para mantener unas medidas de segura, las básicas serían las siguientes:

- Filtros de spam: Evitara el recibir algunos emails de phishing. Algunos proveedores de dominio aplican por defecto un filtro de spam, suponiendo un ahorro en coste y tiempo para algunas organizaciones.»
- Filtro de email spoofing o suplantación de correo electrónico, para ello se puede la autenticación de correos entrantes por protocolo.
- Antivirus: este se debe encargar de escanear los correos entrantes como salientes para detectar amenazas y filtrar ficheros potencialmente maliciosos» Deshabilitar las macros de los ficheros de Office o de cualquier otra
- Desactivar la visualización en formato HTML en las cuentas de correo críticas, como podrían ser los altos cargos de la empresa, o a disposición del público para contactar con la empresa. El formato html permite programas escritos en Java, que pueden hacer que se salta las medidas de seguridad para redirigir al usuario a una página maliciosa y acabe infectando el sistema.
- Para abrir los correos sospechosos se recomienda hacer una sandbox[44], como podría ser Cuckoo Sandbox[45], de código abierto. En este se puede lanzarle cualquier archivo sospechoso para ser analizado, dentro de un entorno realista pero aislado

[44] Traducido como caja de arena, se emplea para ejecutar archivos sospechosos de forma segura, aislados del resto de su equipo.

[45] Cuckoo Sandbox - Automated Malware Analysis

- *DLP*

Las soluciones DLP[46] se utilizan en el proceso de monitorización de sucesos que pueden ocasionar la exfiltración de información. Disponer de un sistema como este supone el detectar las fugas de información y archivos confidenciales, esto es importante, ya que la tendencia actual las infecciones por Ransomware se produce una fuga antes del cifrado.

En muchas ocasiones una organización no sabe que ha sido afectada por un Ransomware, hasta que no lee el aviso de rescate o ve los ficheros cifrados y con extensiones no habituales. Por ello detectar la fuga de información podría suponer el parar el ataque y que la información no fuera cifrada.

- *Extensiones de ficheros*

No se debería ocultar las extensiones de los ficheros, para así poder fijarse siempre en las extensiones de los archivos recibidos y comprobar si son coherentes con el nombre, así como identificar los archivos ejecutables que no deberían serlos.

Por ejemplo, si un usuario recibe un archivo "factura.pdf.exe", y si esta opción no está habilitada en su sistema, vería el nombre del archivo "factura.pdf" y posiblemente no sospechara.

- *LOGs*

Se recomienda guardar logs[47] del uso de ficheros y del acceso externo a los dispositivos perimetrales, que permite poder investigar cualquier posible incidencia o incidente, y si se ha de denunciar se pueden aportar pruebas para justificar ante la justicia o seguro.

- *Concienciación y formación de los usuarios*

En la entrevista realizada a Guillermo Rodríguez Suárez, senior manager de Risk Advisory de Deloitte, en el medio Computing.es, indica:

"El 90% de los ataques, según datos de diferentes estudios, que se producen en una compañía tienen su origen en fallos, descuidos, negligencias o actos deliberados de los empleados."[48]

Por ello es muy importante la existencia de planes de formación y concienciación a nivel corporativo, que marquen unas líneas de actuación para todos los empleados de la empresa en materia de seguridad informática.

Fujitsu, en colaboración con el Observatorio de la Industria 4.0, realizo un estudio con grandes empresas dedicadas al entorno industrial, y en este se determinó que solo el 64% de las organizaciones encuestadas capacitaron a sus empleados para prevenir el Ransomware.[49]

---

[46] Data Loss Prevention.

[47] Un log ("registro", en español) es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

[48] https://www.computing.es/seguridad/opinion/1115211002501/sensibilizacion-del-empleado-clave-seguridad-de-compania.1.html

[49] https://www.computing.es/seguridad/noticias/1125950002501/64-de-organizaciones-capacitan-empleados-prevenir-Ransomware.1.html

En ocasiones, se le da una formación de concienciación a los empleados, pero esto no es suficiente, ya que se trata de un proceso de aprendizaje lento y costoso, y se debería reforzar de forma habitual y mantener la información de seguridad para que estén al día.

Las formaciones para concienciar a los empleados es una de las medidas que menos se invierte en la actualidad, pero es un factor primordial para evitar este tipo de ataques y varias entidades dedicadas a la ciberseguridad facilitan formaciones, como son:

- INCIBE tiene un video tratando el tema de la concienciación informática, disponible en el siguiente enlace: https://www.incibe.es/protege-tu-empresa/kit-concienciacion.
- Existe un proyecto impulsado por CSIRT[50] de la Comunidad Valenciana para el apoyo en la concienciación de todos los ciudadanos, PYMEs y Administraciones Públicas de la Comunidad Valenciana, disponible en el siguiente enlace: https://concienciat.gva.es/.

- *Auditar*

Una medida preventiva sería auditar los sistemas corporativos, como puede ser escanear los equipos con antimalware actualizado y que se realice periódicamente.

También es recomendable realizar periódicamente una auditoría a las infraestructuras, para comprobar que todas las medidas anteriormente recomendadas se cumplen. Estas pruebas las han de pasar personal cualificado, si la empresa no dispone de él, siempre puede solicitar a personal externo.

Para la prevención frente al Ransomware se tiene que tener especial consideración los siguientes aspectos:

- protección antivirus, antispam y de filtrado de contenidos;
- administración de permisos de usuarios y accesos a servicios;
- seguridad de los dispositivos móviles;
- gestión automatizada de actualizaciones y parches;
- detección de vulnerabilidades;
- monitorización del uso de los recursos informáticos y de red; y
- monitorización y análisis de eventos de seguridad en tiempo real (SIEM).

Las pruebas que se puede pedir para comprobación que el nivel de seguridad es el correcto para que ante un ataque el riesgo sea bajo, son las siguientes:

- test de penetración;
- auditoría de red;
- auditoría de seguridad perimetral;
- auditoría web;
- auditoría forense, esta se realizaría si se sufrió un incidente de ciberseguridad.

[50] CSIRT (Computer Security Incident Response Team) o CERT (Computer Emergency Response Team) se tratan de equipos de respuesta ante incidentes de seguridad informáticas.

- *Plan de respuesta a incidentes*

Otra medida preventiva es disponer con un plan de contingencia y de respuesta ante incidentes, para una organización pueda estar preparada en caso de que ocurra.

Ilustración 14 - Fases de respuesta ante incidentes[51].

En el caso de producirse un incidente, es esencial contar con un procedimiento claro de actuación que evite pérdidas de tiempo y económicas innecesarias, además de sistemas de recuperación y contramedidas. En este estudio, esto lo desarrollaremos con más profundidad para un incidente provocado por un Ransomware en una PYME, y sus consecuencias.

En este plan se contemplará quien será el encargado gestionara el incidente, donde está la documentación esencial para gestionarlo y quien es el responsable. Además, se determinarán el tipo de incidente en la etapa de detección y análisis, en las de contención, resolución y recuperación, se ha de conseguir pasar de nuevo a la actividad, y en la última etapa que es el cierre de incidente, se debe documentar todo lo ocurrido y aplicar las lecciones aprendidas.

2.3.2 Medidas de seguridad - PYME

El estudio realizado por la empresa norteamericana, Coveware[52], especializada en la recuperación y eliminación de Ransomware, arroja el Ransomware sigue siendo un gran un problema para las pequeñas empresas.

En el tercer trimestre de 2021, casi el 44% de los ataques afectaron a las empresas con entre 101 y 1.000 empleados, frente al 38% en el segundo trimestre, esto sugiere que los objetivos de los cibercriminales están cambiando, prefieren atacar a empresas más pequeñas que a grandes corporaciones.

---

[51] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_Ransomware.pdf

[52] https://www.coveware.com/about

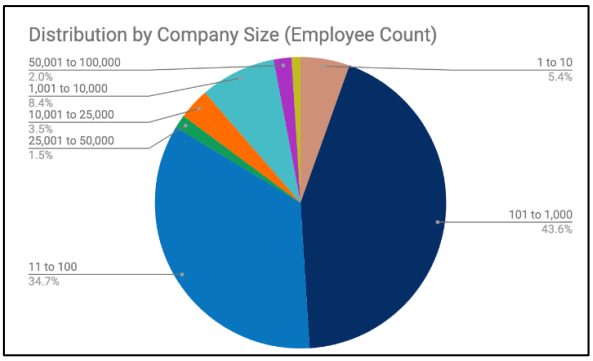


Ilustración 15 - Distribución de las empresas según el número de víctimas de Ransomware en el tercer trimestre de 2021[53].

Este estudio también indica que las empresas se pueden enfrentan 22 días de interrupción de la actividad.

Este cambio de tendencia a atacar a PYMEs por parte los grupos especializados en Ransomware, es decir, que los grupos que emplean el modelo RaaS[54] no intenten atacar a grandes corporaciones; se puede deber al riesgo que corren estos grupos criminales cuando atacan a entidades muy grandes, como en el caso del ataque al oleoducto Colonial. El impacto que produjo esta infección tubo una respuesta nacional del gobierno norteamericano, que conllevara se pusiera el punto de mira en los grupos cibercriminales, y esto supone un riesgo para su modelo de negocio, por ello se puede pensar durante el tercer trimestre han cambiado los objetivos.

Uno de los primeros Ransomware como servicio (RaaS) fue en 2018, con el Ransomware GandCrab. RaaS es un modelo de negocio, en que un grupo o un usuario desarrolla un conjunto de herramientas de Ransomware, y por otra parte otro grupo compran o se suscriben a estas para lanzar ataques. Por esto, usuarios con poca experiencia pueden llevar a cabo ataques complejos, y esta facilidad a conseguido que crezca el número de plataformas RaaS, a su vez, es una de las causas del aumento de los ataques masivos de Ransomware.

Las empresas medianas y pequeñas no son tan importantes y no pueden pagar grandes rescates, pero son más rentables a la hora de atacar y pueden proporcionar un pago considerable si dicha empresa no tiene las medidas de seguridad conveniente y no dispusiera de las copias de seguridad de la información, es decir, no tuviera modo de recuperar la información.

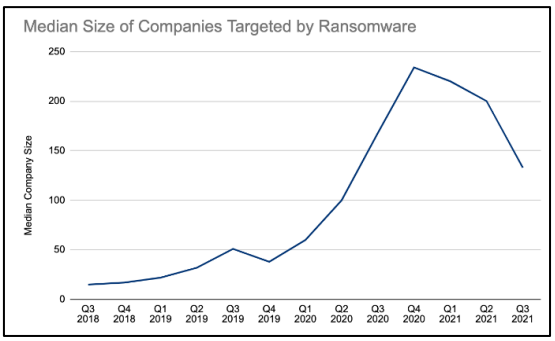


Ilustración 16 - Tamaño de las empresas afectadas por el Ransomware en el tercer trimestre de 2021[55].

[53] https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts

[54] https://www.checkpoint.com/cyber-hub/threat-prevention/Ransomware/Ransomware-as-a-service-raas/

[55] https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts

Como muestra la gráfica de abajo, los métodos rentables de vector de ataque, son el RDP y los correos de phishing, siguen para las organizaciones más pequeñas.

Esta situación se puede deber a que las organizaciones más pequeñas tengan recursos limitados para tener expertos en seguridad de TI, y no se esté contemplando las vulnerabilidades del protocolo RDP.

En relación a los ataques de correos de phishing posiblemente se den en mayor media en las PYMEs por el hecho de no disponer de servicios de filtrado de correo electrónico, por el coste económico que suponen. Dichos filtros podrían mitigar el riesgo de un ataque de phishing y que la empresa acabe sufriendo una infección.

De esta gráfica se puede extraer que a medida que los criminales quieren atacar a empresas más grandes, los vectores de ataque deben ser mucho más sofisticados, por ello emplean como vector de infección una vulnerabilidad de software, la cual requiere una especialización del atacante.

El nivel de especialización del vector de ataque y el del criminal que realiza el ataque, aumentan los costes de este, por ello estos van dirigidos a empresas más grandes para obtener mayor rentabilidad.

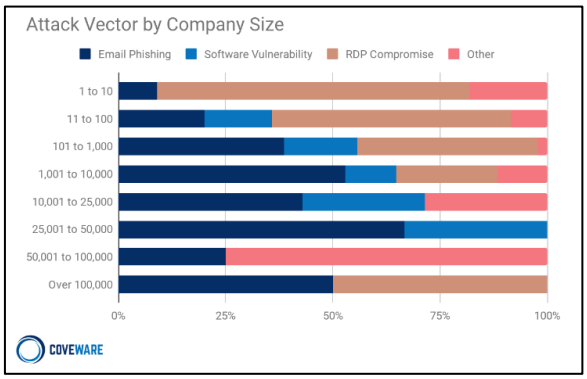


Ilustración 17 - Vectores de ataque más comunes utilizados por las 3 principales variantes de Ransomware en el tercer trimestre de 2021 [56]

En la actualidad, las grandes empresas dependen de las TIC, pero no solo ellas, sino también las PYMEs, que constituyen más del 99% del tejido empresarial europeo.

Las empresas medianas y pequeñas presentan más carencias en el ámbito IT, lo cual aumente el riesgo de sufrir un incidente, y no lograr recuperarse. El porcentaje de PYMEs que han sufrido en alguna ocasión una brecha de seguridad es el 74% de estas.

Estas empresas en su gran su mayoría no disponen de medidas de ciberseguridad, aunque como se ha indicado dependen del ámbito IT. Las PYMEs se enfrentan a siete obstáculos que necesitan superar para protegerse y garantizar la continuidad de sus negocios ante un ataque de Ransomware:

- Desconocimiento sobre los estándares de seguridad de la información aplicables. En muchos casos, las PYMEs desconocen cuales son los estándares que deben aplicar para poder cumplir lo requerimientos de la seguridad de la información. Por ejemplo, un bufet pequeño de abogados que quiere digitalizar todo su archivo y tenerlo disponible para

[56] https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts

consulta, y no conocen cómo almacenar dicha información y las medidas de seguridad que deben aplicar.

- Presupuesto y recursos limitados. El presupuesto destinado a seguridad de la información es un gran impedimento para implantar estándares, para realizar estas tareas es necesario personal especializado y el coste de este no es trivial para una PYME.
- Preferencias en la inversión. La dirección de una PYME tiene como objetivo invertir los esfuerzos en ser competitivos en su ámbito de negocio y no en ciberseguridad. Por ello, las preferencias de la dirección no están alineada con la disminución del riesgo de sufrir un ataque, y no perciben la ventaja competitiva frente a la competencia que podría dar reforzar la seguridad.
- Percepción equivocada acerca de los objetivos de los ciberataques. La idea que los grupos criminales solo atacan a grandes corporaciones está muy extendida, pero a lo largo de este estudio se ve como la tendencia actual es a infectar pequeñas y medianas empresas.
- No contribución en el proceso de desarrollo de los estándares. Las empresas grandes suelen ser las impulsoras de esos estándares y se ajustan a sus procesos, por lo contario no se ajusta a los de las PYMEs y para estas es costoso el asumirlas técnicamente y económicamente.
- Carencia de personal-capacidad de ciberseguridad. En estas empresas es difícil asignar roles y responsabilidades de seguridad de la información, porque no tienen personal con capacidades. Un tercio de las empresas españolas indican que no disponer de suficiente personal para dedicar tiempo a la ciberseguridad[57].
- Gestión de riesgos. La evaluación del riesgo de la seguridad de la información apenas es conocido por las PYMEs, por lo que muchas no lo evalúan este tipo de riesgo. Consecuencia de esto, no perciben el riesgo de no disponer de un plan de continuidad ante un incidente de seguridad.

Las medidas que deberían cumplir las PYMEs en la medida de lo posible serían las citadas en el punto 2.3 de este análisis, pero ante los problemas que podría tener para alcanzar todos los hitos, se podría recomendar que alcanzaran las siguientes medidas para reducir el impacto en caso de sufrir un Ransomware, estas son:

- Mantener siempre los sistemas operativos de los dispositivos actualizados hasta su nivel más reciente de parcheado y facilitado por el proveedor.
- Disponer de un antivirus actualizado, aunque una mejor opción sería de disponer un EPP (Endpoint Protection Platform) y EDR [58](Endpoint detection and response).
- Realizar copias de seguridad periódicas de todas las máquinas e información más crítica, y que sea necesaria para el trabajo.
- Tomar medidas frente a la exposición de documentos y los RDP.
- Se debe deshabilitar todos aquellos servicios que vienen activados por defecto en los sistemas operativos, pero que no son necesario para realizar las labores empresariales.

[57] https://www.bankia.es/es/bankademia/ PYMEs-y-autonomos/ PYMEs/invertir-ciberseguridad-negocio

[58] Recurso para combatir las amenazas avanzadas y responder a incidentes en los puntos finales de la red.

- Implementar protecciones sofisticadas de análisis, detección y bloqueo de tráfico malicioso, como podría ser un Firewall OpenSource, como lo son PfSense[59], Untangle Firewall[60] o OPNSense[61].
- Concienciación y formación del personal en seguridad informática.

2.3.3 Medidas reactivas - Incidente

Con las medidas reactivas de reacción o correctivas como se ha comentado anteriormente se pretende dar respuesta y corregir los efectos causados por un incidente de seguridad, en este caso de estudio, el incidente es de Ransomware.

Ante un incidente se debe aplicar la gestión ante de incidentes de seguridad de la información, esta se trata de un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible[62].

El proceso de gestión de incidentes se compone de distintas fases, todas ellas son necesarias, pero algunas pueden estar incluidas como parte de otras o abordarse de manera simultánea.

Ilustración 18 - Gestión de incidentes según la guía CCN-STIC-817 [63]

2.3.3.1 Preparación

Como se indicó en el punto 2.3 una de las medidas activas sería disponer de un plan de contingencia ante un incidente, que en el cual están sentadas las bases de quien y como se llevará a cabo proceso para lograr la recuperación lo más rápidamente. En otras palabras, en este se habrá definido el Equipo de Respuesta, la utilización de las herramientas y recursos necesarios para sobrevivir a un incidente.

Pero como se ha comentado con anterioridad, solo el 10% de las empresas con menos de 10 trabajadores tiene una política de seguridad y un plan de respuestas frente ataques, y el 50% las

[59] https://www.pfsense.org/

[60] https://www.untangle.com/untangle-ng-firewall/free-trial/

[61] https://opnsense.org/

[62] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

[63] https://www.ccn-CERT.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

de 50-249 trabajadores[64]. Por ello, se dará el caso, en un gran número de PYMEs, de no tener disponible un plan de contingencia o frente a desastres para poder abordar este tipo de incidentes.

Lo que conllevará que se deba aplicar una gestión ante incidentes sin un plan de contingencia establecido, para ello varias organizaciones tienen a disposición equipos para intervenir, así como documentación con sugerencias como actuar en dichos casos, como es INCIBE con el documento "Ransomware: Una guía de aproximación para el empresario".[65]

Como preparación ante un incidente, se debería establecer algunas pautas cuando se sufra uno, como pueden ser:

- Que los responsables de seguridad de la información mantengan una reunión cuando se declare un incidente.
- Se debe avisar a la Dirección de la empresa e ir informándola de los avances.
- El comité de crisis de la organización es el que deberá gestionar la situación y aplicar los planes dispuestos previamente.
- Se debe realizar una primera valoración del estado de la red, equipos, activos y servicios que componen la red.
- Se debe tener documentado el diagrama de la arquitectura de los sistemas informáticos.
- Los activos deben estar inventariados, para saber qué datos y servicios críticos pueden estar comprometidos.
- Documentar un listado de proveedores y clientes que pueden verse afectados e identificar quien deben ser notificados.
- Y en cuando se identifique un incidente de este tipo realizar un comunicado para empleados, proveedores y cliente, ante el peligro de propagación.

2.3.3.2 Identificación

En el plan de contingencia se tendrá definido cual es actividad normal que permitirá detectar actividades sospechosas, que sean el indicio de estar sufriendo o haber sufrido un incidente. Además, marca las pautas a seguir para llegar a obtener las evidencias que puedan ser presentadas en una denuncia ante las autoridades.

El primer paso de este plan es la identificación de que se ha sufrido o se está sufriendo un Ransomware. Aunque en ocasiones, los ataques de Ransomware se detectan cuando se descubre la nota de rescate o cuando ya se han cifrado archivos. Por lo cual, la velocidad de la detección de Ransomware es fundamental, para así combatirlo antes que se pueda propagar por las redes y cifren datos esenciales de la empresa.

Cuando se obtiene los indicios que se está sufriendo o se ha sufrido un incidente hay que catalogar que tipo y criticidad. El Ransomware se clasifica como Compromiso de la información y de tipo de Modificación no autorizada de información, como se puede ver en el Anexo II.

---

[64] https://www.ibercaja.es/empresas/corner-del-especialista/informacion-seguros/ PYMEs-vulnerables-ciberseguridad/

[65] https://www.incibe.es/protege-tu-empresa/guias/Ransomware-guia-aproximacion-el-empresario

Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.

Ilustración 19 - Clasificación de incidentes de seguridad Guía de Seguridad de las TIC

Para establecer el impacto de un incidente se puede consultar el Anexo III, basada en la Guía de Seguridad de las TIC del CCN-CERT.

Una vez que se declara un incidente de seguridad y su nivel de criticidad, se recomienda documentar toda la información relativa al mismo de la manera más completa posible a medida que se realizan acciones, como pueden ser entre otros:

- las acciones realizadas,
- las comunicaciones,
- los datos suministrados,
- los tiempos.

2.3.3.3 Contención

Cuando se sospecha que un equipo está infectado de este tipo de ataque se debería aislar del resto de activos de la corporación. Ya que es necesario contener la propagación del código dañino por la red, este puede consistir tanto en cifrado de carpetas compartidas, documentos esenciales, como movimientos laterales a otros equipos de la organización que se tenga visibilidad desde el activo infectado, etc.; para de este modo evitar que un posible atacante remoto pueda seguir con su actividad maliciosa dentro de la organización. Si esto no se contuviera, el atacante podría seguir exfiltrando información, para después forzar el pago de la extorsión a cambio que no se haga pública, la posibilidad del despliegue de puertas traseras, como también la eliminación de evidencias.

Para conseguir esto, se debe desconectar de la red, tanto física como lógica, y de cualquier tipo de conexión con otros dispositivos. Por ejemplo, existen Ransomware de tipo cryptoworms[66], que buscan activamente conexiones y otros activos en su misma red para replicarse y ejecutarse automáticamente, por ello se propagan rápidamente, un ejemplo fue el Ransomware ZCryptor[67], que se vio por primera vez en 2016.

Si la PYME que ha sufrido el incidente, no tiene una segmentación de las subredes efectiva, se podría dar el caso en que el atacante podría tener el acceso todo el parque de activos y poder acceder a cualquier información de la organización. Se puede rediseñar la segmentación de la red a nivel de Firewall, si se dispone, para poder contener subredes en caso de más activos afectados y añadir más cortafuegos.

[66] https://hals.com.mx/cryptoworm-Ransomware-puede-distribuirse/

[67] https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-Ransomware-pasado-presente-y-futuro/

Para la contención es recomendable cambiar inmediatamente todas las contraseñas y de cuentas online, por si el atacante tuviera acceso a ellas. En la fase de erradicación, cuando se haya eliminado el Ransomware, se deben cambiar estas de nuevo.

Es clave la velocidad con la que se actúa para contener la infección y evitar un impacto mayor en la organización. Del mismo modo, la intervención a todos los niveles dentro de la PYME, desde el equipo técnico hasta la alta Dirección, también influye en la pronta resolución del incidente.

2.3.3.4 Comunicación del incidente

Como se ha indicado anteriormente en estos casos se debe actuar con prontitud, tanto para la contención, como el aviso a los responsables de la organización. También es un paso fundamental la rápida notificación de un ciberataque de estas características al CERT de referencia, para la resolución del incidente y la minimización de sus impactos.

Con la publicación del RD 43/2021[68], los operadores críticos, operadores de servicios esenciales y proveedores de servicios digitales tienen la obligación de notificar sus incidentes a la autoridad competente respectiva, a través del CSIRT de referencia.

Aunque en el caso de las PYMEs que no estén englobadas en ese tipo de operadores, pueden denunciar al CERT de INCIBE. En ese caso, se debe aportar una captura de la pantalla con la nota de rescate y dos archivos cifrados por el Ransomware (sin información sensible, con formato Word o Excel y ocupen menos de un MB). De este modo se podrá analizar el Ransomware y así mantener información a la organización.

Cuando la PYME no sea un operador crítico, ni operador de servicios esenciales y ni proveedores de servicios digitales podrá denunciar ante:

- Grupo de delitos telemáticos de la Guardia Civil[69].
- Brigada de Investigación Tecnológica de la Policía Nacional[70].

A la hora de presentar la denuncia ante los cuerpos de seguridad, se debe tener claro los puntos fundamentales de la cronología del ataque, que serán:

1. Fecha exacta y hora aproximada de cuando tuvo conocimiento de la infección.
2. Acciones anteriores al conocimiento de la infección.
3. Acciones previas inmediatas al conocimiento de la infección.
4. Cantidad de rescate solicitada y dirección de la cuenta de Bitcoin del ciberdelincuente, esta información suele estar en la nota de rescate.
5. Si se contactó con los delincuentes, y por qué vía se realizó. Aportar información acerca de este, si por ejemplo se hizo a través de correo electrónico, se deberá aportar los correos originales con las cabeceras, para poder determinar la trazabilidad.
6. Se puede aportar las pruebas del equipo informático infectado.

[68] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

[69] https://www.gdt.guardiacivil.es/webgdt/enlaces.php

[70] https://www.policia.es/_es/denuncias.php

Por otra parte, si hay una brecha de datos personales[71], en el artículo 33 del RGPD se establece la obligación por parte del responsable del tratamiento de datos de notificar a la autoridad de control competente, la Agencia Española de Protección de Datos (AEPD) en un plazo máximo de 72 horas, a menos que sea improbable que la brecha constituya un riesgo para los derechos y libertades de las personas físicas. Esto se puede denunciar telemáticamente, a través del siguiente enlace: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/nbs/procedimientoBrechaSeguridad.jsf

Según indica la AEPD, un 10% de las notificaciones de brechas de seguridad, recibidas entre 25 de mayo de 2018 (fecha de aplicación del RGPD) y el año siguiente, están provocadas por el cifrado de equipos mediante algún tipo de Ransomware.

2.3.3.5 Investigación

En ocasiones la entrada de Ransomware puede haber sido por varias vías e incluso que esté alojado en varios activos de la organización, aunque no se muestre indicios en algún sistema.

Tras la fase de contención, se debe determinar cuántos y qué equipos han sido afectados, como los hubiera utilizado el atacante para pivotar por la red o como para cifrar su información, o incluso realizar modificación o eliminación de esta.

Si antes de la contención se ha podido obtener el volcado de memoria del proceso malicioso, en esta fase de la gestión del incidente se podría investigar.

Durante la fase de investigación, tanto el análisis forense como el análisis de las muestras de malware se puede realizar al mismo tiempo. Este último análisis es esencial para definir la amenaza, las capacidades que tiene dicho malware, la persistencia que puede tener en un sistema y si es un malware conocido, o es una nueva variante o completamente nuevo.

Para saber si el malware es conocido o no, se pueden emplear herramientas de reconocimiento de Ransomware, como es Crypto-Sheriff[72] perteneciente a la iniciativa NomoreRansom[73], en la que está involucrada la EUROPOL.

Para realizar el análisis forense será necesario clona el disco de activo o activos afectados, si es completa será mejor. Para comprobar que el clonado es correcto. los hashes del dispositivo original como el clonado deben ser el mismo.

El siguiente paso sería comprobar el grado de cifrado de los datos, por lo que será necesario conecta el clon del disco duro del equipo afectado a otro ordenador en un entorno aislado, es decir, sin conexión a ninguna otra red o internet.

---

[71] Brecha de datos personales o violación de la seguridad de los datos personales es todo aquel incidente de seguridad que provoque la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

[72] https://www.nomoreransom.org/crypto-sheriff.php

[73] https://www.nomoreransom.org/es/index.html

Cuando se monte la imagen forense como un disco esclavo y se analice, se pueden encontrar dos tipos de escenarios:

- Que se haya cifrado o eliminado la tabla de particiones del sistema.
- Que no se haya cifrado la tabla de particiones y se podrá ver la estructura de directorios

Cuando se obtenga la estructura de directorios se ha de recolectar la siguiente información:

- Sistema operativo
- Listar los usuarios del sistema y consultar la actividad del usuario víctima, cual han sido sus últimos movimientos y que archivos ejecutados más recientes.
- También se deberá comprobar el registro de eventos del sistema operativo. Si se dispone del SO Windows, se puede comprobar los logs de eventos de Windows, para analizar los inicios de sesiones dentro del sistema, con código 4624[74], por ejemplo, si el delincuente accede con un usuario de forma remota a la maquina afectada para extraer información esencial.

Cuando se ha analizado la información obtenida anteriormente, se tiene una mayor visión de lo que sucedió, y se pude determinar el incidente e infección si se produjo por archivo descargado de internet (vía email o web) o de forma remota (explotación de una vulnerabilidad o RDP).

El C&C, "comand and control" o C2, es el conjunto de servidores y otros dispositivos que son usados por los atacantes para controlar el malware. Cuando se identifica el archivo malicioso, se debería extraer y analizar en un entorno controlado para poder determinar a que C&C[75] se conecta e intentar establecer si la clave de cifrado es siempre la misma. Para determinar ambas se puede realizar mediante:

- Un análisis de los paquetes de red, este facilita la detección el C&C y las conexiones que realiza.
- Un volcado de memoria RAM, este consiste en crear un archivo que contiene la información que se encuentra en la memoria principal en el momento en que el archivo malicioso comienza a cifrar los datos de la computadora

Con el análisis de toda esta información se debe redactar un informe detallados con los resultados y conclusiones.

A parte de realizar el clonado para conservar las pruebas originales, se podrán realizar las pruebas de recuperación sobre este clon y así evitar alterar el original si no funcionaran correctamente. En ocasiones no hay modo de recuperar los datos en el momento, pero es posible que en el futuro sí que haya.

2.3.3.6 Erradicación

Tener una correcta política de backups es uno de los métodos de prevención más efectivos en este tipo de ataques, en especial para empresas que no pueden destinar numerosos recursos en sus medidas de seguridad. Cuando un Ransomware llega encriptar los datos de una PYME, y el ataque

[74] https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624

[75] https://es.wikipedia.org/wiki/Mando_y_control_(malware)

es lo suficientemente agresivo para que no queda otro modo de recuperar los datos que sea el pago del rescate, la recuperación mediante backup es la única solución.

Se debe rediseñar la red si no es óptima, y segmentarla en distintas redes para particionar y separar entornos. Como también, se debe proceder a actualizar todos los sistemas de la organización y controlar todos los servicios expuestos, en especial el RDP, que pueden ser vulnerables a un ataque.

En ocasiones los atacantes cuando se encuentra dentro de un activo emplean herramientas como es Mimikatz[76]. Esta permite obtener credenciales locales y de dominio cacheadas en el equipo infectado. Si las credenciales cacheadas en el equipo infectado son las mismas en el resto del dominio, se puede considerar que todos los equipos han sido potencialmente comprometidos. Por esto se han de cambiar las credenciales del dominio, además se deben eliminar usuarios con privilegios de administración que pudieran haber sido creados por el atacante.

Durante esta fase se aplicará el concepto de red limpia, que consiste en una red interna dentro de la red principal y aislada por un firewall, esta contendrá los equipos que se han ido revisando y limpiado, esto evita las reinfecciones.

2.3.3.7 Recuperación

Después de un incidente de este tipo, que puede implicar el cifrado y borrado de activos críticos dentro de una PYME, es necesario establecer el alcance del impacto sufrido, la evaluación de la información a recuperar y que afectación a supuesto para los servicios.

En ocasiones gran parte de la información que ha sido cifrada podrá ser recuperada, usando copias de seguridad aisladas que no se hayan visto afectadas o a través de copias obtenidas con técnicas de forense. Además, en la fase de recuperación de la actividad, es necesario reconstruir los servicios esenciales de la organización que fueron dañados. En este momento se puede hacer instalaciones limpias y seguras, y que permitan la monitorizarlas para aumentar la seguridad en la organización.

Se pueden dar varios escenarios cuando se proceda a restaurar los datos, estos son:

a) Backup completo del activo afectado, si hay una buena política de backups (puede ser tanto físico, como lógico o en la nube) y las copias no se han visto afectadas, solo será necesario desinfectar el equipo y a continuación restaurar la copia de seguridad. Para la desinfección se podría restaurar el equipo a los valores predeterminados de fábrica, formateando el activo o eliminando sus instancias de almacenamiento si están en la nube, también se podría desinfectar mediante la utilización de un antivirus e incluso borrando los archivos de forma manual.[77]

b) Datos descifrados, si no se dispone de backups para la restauración, pero sí que se tiene la clave de cifrado. En el mercado existen varias herramientas para el reconocimiento de,

[76] https://www.cynet.com/network-attacks/mimikatz/

[77] https://www.avast.com/es-es/c-how-to-remove- Ransomware-pc#gref

como es Crypto-Sheriff[78] perteneciente a la iniciativa NomoreRansom[79], avalado por la EUROPOL. Este tipo de herramientas puede facilitar claves de descifrado, con las cuales se podrían recuperar los datos y restaurar la copia después de desinfectar el host.

c) Copias de seguridad de Windows, si el sistema de ficheros del sistema operativo cuenta con shadow copy o snapshot, que mantienen copias de versiones anteriores de ficheros. Se debe localizar una copia previa a la infección, por ello es importante realizar un buen análisis forense para tener la cronología del incidente, y restáurala. Cabe la posibilidad de no disponer todos los datos, ya que las copias no tienen por qué coincidir en el tiempo con momentos antes del inicio del ataque. Después de la desinfección se puede instalar la copia de seguridad más reciente anterior al incidente.

d) Datos recuperados con herramientas forenses, en algunas ocasiones se disponen de programas forenses que son capaces de recuperar algunos ficheros originales borrados por el Ransomware.

e) Datos cifrados, si no existe solución, se recomienda conservar los datos por si en algún momento se publica una solución de desencriptado para este ataque.

2.3.3.8 Lecciones aprendidas

Este tipo de incidentes para una empresa mediana o pequeña ponen de manifiesto que invertir en seguridad es una necesidad. Como también es necesario apostar por un equipo de seguridad preparado, en medida de las posibilidades de cada empresa, puede ser propio o externo, y con los medios materiales adecuados.

También, ante estos ataques se pone de manifiesto las carencias de conocimiento de ciberseguridad por parte de los empleados, como la no conciencia de lo que las empresas tienen expuesto al exterior y la falta de una política de actualización de los sistemas.

Es indispensable disponer un sistema de seguridad como Firewalls, copias de seguridad, segmentación de las redes, políticas de roles, antivirus, SIEM, etc. para poder proteger y poder dar una rápida respuesta, como también retomar cuanto antes sea posible la actividad.

A parte, que los empleados estén concienciados, como también se disponga de un equipo de seguridad, es preciso que la alta dirección este concienciada ante situaciones de esta índole.

Como se ha indicado en varias ocasiones, este tipo se puede propagar muy rápidamente por lo que se debe de disponer de herramientas que permitan detectar con la mayor celeridad posible, es

[78] https://www.nomoreransom.org/crypto-sheriff.php

[79] https://www.nomoreransom.org/es/index.html

decir, que se pueda atajar en una fase temprana un posible incidente crítico. También, se puede disponer de herramientas que actúen como vacunas ante un taque de Ransomware.

Ante este tipo de incidentes, se debe proceder con mucha cautela para evitar una reinfección, se debe controlar todo el parque en medida de lo posible, como las posibles puertas traseras pueda haber desplegado el atacante.

Disponer de un equipo entrenado es un punto fundamental para determinar el éxito en la resolución del incidente, según estudio de Accenture el período de inactividad promedio cercano a los 12 días[80], si se dispusiera de un equipo sin experiencia el tiempo promedio podría ser superior.

Las empresas medianas y pequeñas tienen que seguir madurando en el ámbito de la seguridad informática para evitar incidentes de seguridad, que afecten gravemente al servicio que prestan, y acaben formando parte del 60% de las PYMEs Europeas que no sobreviven después ser víctimas.

2.4 Consecuencias de un ataque de Ransomware

Existe por parte de los organismos públicos campañas para advertir y concienciar del impacto de ataque de este tipo sobre su organización y la perdida de la información de esta, los daños que pueden sufrir pueden llegar abarcar mucho más que los que pueden pronosticar la gran mayoría de empresas.

La gravedad de las consecuencias puede variar también del tiempo que se tarde en recuperar la actividad, el impacto no es el mismo si se tardar en acceder a la información 2 días que si fueran 20 días. Cuanto más se tarda en poder continuar con la actividad mayores son los efectos en las pérdidas económicas, en el daño en la imagen o reputación, la productividad que se vio afectada y las sanciones que puede conllevar.

Las consecuencias aparte de tener unas implicaciones económicas de forma directa, impactando a los clientes, o indirecta, repercutiendo en la imagen de la empresa, algunas implican una modificación en la cultura de la organización, dependiendo de cómo se vea afectada por el ataque.

Cuando una organización se ve afectada por una infección por Ransomware, las consecuencias que puede llegar a sufrir serán las siguientes:

- La responsabilidad penal o civil.
- El daño económico.
- El daño a la reputación de la organización.

La siguiente imagen representa gráficamente el efecto cascada de riesgos y daños que supone el sufrir una brecha de seguridad, el análisis de estos se abordara en los siguientes puntos.

---

[80] https://www.accenture.com/_acnmedia/PDF-155/Accenture-Respuesta-y-Recuperacion-Ante-El-Ransomware.pdf

Ilustración 20 - Efecto cascada de un ciberincidente[81].

2.4.1 Delito y sanciones

Cuando una empresa sufre un ataque de tipo Ransomware, tanto los atacantes como los atacados puede incurrir en delitos e incumplimientos que suponen multas o sanciones.

Los ciberdelincuentes que realizan dicho ataque se les puede atribuir la conducta típica del delito de daños y sabotajes que prevé Código Penal, el cual está tipificado en el art. 264[82]. En este se castiga el daño, el deterioro, la modificación, la eliminación o el hacer inaccesible datos informáticos, programas o documentos, sin autorización. Este puede tener penas prisión desde los 6 meses hasta los 3años.

Además, el art 264.2 agrava las penas en el caso de comisión de los hechos delictivos en el marco de una organización criminal, cuando se hayan causado daños de especial gravedad, o cuando se hayan visto afectados los intereses generales; con llevando penas de prisión de dos a cinco años y multa de 10 veces del perjuicio ocasionado.

Como se ha apuntado anteriormente las empresas que fueron dañas con este tipo de ataques, pueden enfrentarse en este tipo de siniestros por reclamaciones de sus propios clientes, tanto por responsabilidad civil contractual, como también puede ser por terceros afectados por la sustracción de información.

Con respeto a responsabilidad civil, la cual se tipifica en el art.1.101 del Código Civil, la indemnización de los daños y perjuicios por incumplimiento de contrato siempre estará sujeto a que se produzca un daño, negligencia o morosidad.

En el caso de la afección de terceros por la sustracción de información, sobre la empresa podrá recaer la responsabilidad civil extracontractual, los artículos que garantizan esta responsabilidad son art.1.902 y art.1089 del Código Civil. El primer artículo hace referencia a que la persona que cause un daño por acción u omisión mediante culpa o negligencia, está obligado a reparar dicho daño causado a otra persona. Y el segundo artículo establece que las obligaciones pueden nacer

[81] https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf

[82] https://www.conceptosjuridicos.com/codigo-penal-articulo-264/

de la ley, los contratos y cuasi contratos, los actos y omisiones ilícitos o en los que intervenga culpa o negligencia.

Mediante estos dos artículos contemplaran los daños que se puedan causar a terceros por la sustracción de información personal que la empresa estuviera gestionando, con el principio de que la empresa no debe causar daños a terceros, para ello debería adoptar las medidas de seguridad necesarias y actuar con un nivel de diligencia adecuado.

Si en el ataque de Ransomware se vieran afectados datos personales, la empresa puede incurrir en responsabilidad legal como consecuencia del incumplimiento de lo impuesto en la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD). Esta establece los requisitos y obligaciones en materia de protección de datos en empresas sobre cómo proceder con la información personal, así como los derechos que asisten a usuarios[83]. En el artículo 82 del RGPD se dispone la obligación de establecer políticas preventivas y realizar análisis de impacto, en la actual ley vigente las indemnizaciones se dividen en muy graves, graves y leves (artículos 71 y siguientes LOPDGDD).

En el artículo 34 de RGPD se establece que cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará dicha violación al interesado sin dilación indebida. Por ello, la dilación en la comunicación de un ciberataque es el motivo más común por el que la AEPD puede sancionar a una empresa. Esta ha establecido un plazo con un límite de 72horas desde que se tuvo conocimiento para que lo comunique.

La demora en notificar una brecha de datos personales puede estar causada en ocasiones por la falta de conocimiento acerca de cómo proceder en estos casos, o inclusive la carencia de un protocolo o plan de actuación para abordar esa situación en el caso de que se ocasione.

Desde la AEPD se subraya que "La empresa debe establecer quién y qué acciones se ejecutarán en el caso de que se produzca una brecha de seguridad. Cuando sucede, el responsable del tratamiento de los datos debe poner en marcha el plan de actuación, concretando las tareas que le permitan resolver la brecha y recopilar toda la información sobre ella"[84].

Aparte de la causa ya comentada, otro motivo por el cual la agencia multe en el supuesto de sufrir ciberataque puede deberse a que la organización no haya tomado las medidas adecuadas, según el criterio de la AEPD, para evitar el robo de los datos personales.

En 2021, la AEPD, multó a Air Europa con 600.000 euros por un ciberataque que sufrió en 2018, en este se vio comprometida información personal y bancaria de clientes. Aunque hay sanciones que puede llegar a los 20,5 millones de euros e incluso a 22 millones, como en los casos de los ataques a Hoteles Marriot y a British Airways. Sin embargo, existen casos en que las empresas no son sancionadas, porque cumplieron con los requisitos que impone la agencia, que son la pronta notificación y que la organización disponía de medidas preventivas para minimizar el impacto de la brecha, como fue el caso de Mapfre, en agosto de 2020[85].

[83] https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/

[84] https://www.xataka.com/pro/cuando-sufrir-hackeo-sale-doblemente-caro-que-casos-ciberataque-puede-acabar-multa-agencia-proteccion-datos

[85] https://www.xataka.com/pro/cuando-sufrir-hackeo-sale-doblemente-caro-que-casos-ciberataque-puede-acabar-multa-agencia-proteccion-datos

Las empresas deberían contar con un "Compliance[86] Penal relativo al Derecho de las TIC", por el cual se pueda encontrar todos los posibles riesgos existentes dentro de ella, y de este modo establecer el control para preservar los equipos y los datos de posibles ataques, en el caso opuesto se incurrirá a delitos penales; como podrían ser los establecidos en el art 264 del código penal, daño informático, y el art.197 CP, revelación de secretos.

Debido a esto, los afectados por sustracción o uso indebido de la información como resultado de un incidente de seguridad, pueden exigir responsabilidad legal a la empresa que gestionaba sus datos, ya que le han ocasionado un perjuicio. Por ello, son esenciales las herramientas para protección de esta información, como también la concienciación y el debido cumplimiento de las medidas de seguridad por parte de los empleados de la organización, porque gran parte de los riesgos se producen por errores en el tratamiento de datos por parte de los empleados.

En el código penal español no está contemplado el pago del rescate por parte de la empresa afectada como un delito, pero podría tener consideración ética en que pagarlo una contribución a subvencionar el cibercrimen. En un caso extremo una organización, que decidiera pagarlo, podría llegar ser acusada de colaborar con el blanqueo de capitales o la financiación del terrorismo, y esto derivaría en una exigencia de responsabilidad por favorecer a una banda u organización criminal.

En el caso de Estados Unidos se puede cometer un delito federal, y se podrá imponer sanciones por el pago del rescate, el organismo encargado de ello es OFAC (Oficina de Control de Activos Extranjeros). En todos los casos de pago del rescate no supone una sanción, solo se sancionará en los casos que dicho pago se realice a personas o regiones bloqueadas por las leyes estadounidense.

2.4.2 Daño económico

La pérdida temporal o permanente de la información sensible o confidencial tiene efectos de alto impacto en una empresa, que pueden ser desde la disrupción hasta un daño permanente al negocio.

En la actualidad, el tiempo importa, cómo se indicó anteriormente. Si una compañía no puede desempeñar sus actividades de forma adecuada, la noticia puede extenderse y llegar a sus clientes e inclusos competidores, que podría aprovechar la coyuntura, como si se hace público puede ser suficiente para dañar la imagen de la empresa de forma permanente.

Así como la pérdida de información puede llevar también a la revelación de información confidencial, lo que podría incluso derivar en sanciones y demandas, como por ejemplo cuando se vulnera el RGPD, viéndose involucrados datos personales.

El Ransomware puede ser costoso para las empresas que son víctimas de ellos, y habitualmente solo se tienen en cuenta los costes de la pérdida de negocios, el rescate pagado, y los honorarios de los consultores, entre otros, también hay impactos financieros menos conocidos.

[86] El compliance se trata de establecer un seguido de pautas, políticas y procedimientos destinados a garantizar una correcta organización de la compañía, su objetivo es el de cumplir con la normativa legal aplicable. Se trata de un concepto que ha adquirido mucha importancia en los últimos tiempos, sobre todo en el ámbito penal. La implementación de sistemas de compliance debidamente acreditados puede llegar a eximir la responsabilidad penal a la persona jurídica en cuestión (Ley 1/2015).

A continuación, se enumerarán algunos de los gastos que impactan en las finanzas de la empresa afectada, estos podrían ser:

- La pérdida temporal o permanente de información sensible o confidencial.
- Costes de la preparación de la demanda por extorsión, si se realiza la demanda correspondiente por parte de profesionales se deberá tener en cuenta este costo.
- Costos de contratar expertos para ayudar con las negociaciones, en ocasiones se acude a expertos para realizar la negociación entre los ciberdelincuentes y las víctimas, aunque en otras ocasiones este rol es asumido por algún responsable de la organización atacada.
- Coste del pago del rescate, en ocasiones los atacantes piden un primer rescate y posteriormente pide un segundo para no hacer públicos los documentos robados. También se debe añadir que, aunque se pague el rescate, las probabilidades de recuperar todos sus datos son escasas según el estudio publicado por Sophos[87]. De media, las empresas que pagaron el rescate recuperaron solo el 65 % de los archivos cifrados, es decir, que un tercio de la información queda no accesible.
- Costes de la notificación de violación de datos a la AEPD; en ocasiones la notificación de la violación de datos debe de ir precedido de un informe del posible alcance de la brecha. Y si se llega a sancionar, también se debe añadir los gastos de defensa por multas y sanciones de los organismos reguladores
- La investigación del ciberataque, si tiene profesionales cualificados debería contar con las horas de trabajo empleada por estos. En otras ocasiones la empresa no tiene profesionales cualificados para realizar esta tarea, por ello externaliza la labor, se debe contemplar el gasto añadido, además se dan situaciones que el personal interno deben dar apoyo al equipo externalizado para algunas tareas, esto también supone un coste adicional.
- Costes de restauración de la información, en ocasiones no se tiene en cuenta dichos gastos, que engloba un equipo de personas que se dedican a dicha tarea y no suele ser una tarea inmediata, dependerá también de la cantidad de información a recuperar.
- Los gastos de interrupción del negocio, a parte de estos se de contemplar los beneficios que se dejaron de ganar en el tiempo transcurrido para volver a una actividad normal.
- El aumento de las tarifas del seguro contra riesgos cibernéticos[88], si la organización dispone de un tipo de seguro vera que una consecuencia de un ataque de este tipo será el aumento de las tarifas. Y los montantes recuperados de las pólizas podrían no ser tan altos como se esperaba.
- Costes por responsabilidad de civil por incumplimiento de contratos, la responsabilidad por pérdida de datos de carácter personal o riesgos de privacidad y la defensa judicial, tanto de clientes como de terceros, estos vienen asociados a posibles acusaciones contempladas en el punto 2.4.1.
- Perdida de la confianza del cliente, no solo se debe contemplar en el ámbito reputacional, sino a nivel económico, aunque es difícil de cuantificar, pero puede ser un problema importante. Es posible que los clientes no puedan acceder a diversos servicios que la empresa victima ofrece, como las ventas o cualquier otra función en el negocio, lo que genera pérdida de ventas, frustración de clientes potenciales y clientes, inclusive incumplimientos de contratos. Esta pérdida de confianza no solo afecta a los clientes

[87] https://secure2.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of- Ransomware-2021-wp.pdf

[88] https://www.turboseguros.com/blog/seguros-ciberneticos/seguros-contra-riesgos-ciberneticos/

existentes que se ven afectados, sino también a los potenciales, como proveedores, así como también prestadores de servicios.

- Evaluación de riesgos por parte de los socios, cuando una empresa es atacada, las organizaciones que se asocian a esta, como clientes o partners, deben evaluar cómo están en términos de riesgo y si cumple unos estándares. Esto hace que aumenten los costes para cumplir con las condiciones y estándares exigidos por los socios.
- Perdida de la confianza de trabajadores cualificados, como sucede con los socios pueden tener una sensación de desconfianza, esto también puede suceder con los trabajadores. Este tipo de ataques puede generar dudas de la continuidad en la organización, como también el desgaste podría involucrar habilidades técnicas difíciles de encontrar, como las relacionadas con la seguridad, el análisis de datos u otras áreas. El coste de encontrar personal cualificado puede ser alto.

Las consecuencias podrían provocar una modificación en la cultura de la organización, esto podría suponer una mayor conciencia ante la ciberseguridad de la organización, por lo que habría que añadir un coste a corto o medio plazo de la implantación de algunas medidas preventivas de seguridad explicadas en el punto 2.3.2. Por ejemplo, en la actualidad el 80% de los ciberincidentes en las empresas se deben a errores humanos, como se ha indicado una medida preventiva muy eficaz sería la concienciación de los empleados, para poder evitar en mayor medida este tipo de infecciones.

Como se ha indicado anteriormente, un ataque de Ransomware puede llegar a ser paralizante para una PYME, tanto financiera como operativamente, y este podría tener consecuencias duraderas.

En ocasiones cuando se no dispone la información porque esta encriptada, el tiempo que transcurre supone unas pérdidas altas para las empresas, por ello se plantea el pago de los rescates para agilizar la vuelta a la productividad, durante estos últimos años el dinero exigido por los delincuentes se ha disparado.

Según indica el Informe de amenazas de Webroot BrightCloud de 2021, a finales de 2018, el pago promedio de Ransomware era de 6.733 dólares, pero en 2019, la cifra había aumentado un 1100 por ciento, a 84.116 dólares, este no ha parado de aumentar, llegando a un máximo de 233.871 dólares en el último trimestre de 2020.

Como se ha explicado anteriormente la inactividad de una empresa que sufrió un Ransomware puede generar grandes pérdidas, también dependiendo del tiempo hasta restaurar la actividad. Como ejemplo de ello está el caso del Universal Healthcare Services[89], en que se vio afectado por un ataque de este tipo en septiembre de 2020, y tardó tres semanas en poder resolver el incidente y esto le costó una pérdida de 67 millones de dólares.

Según estudio realizado por la empresa EQUUS HOLDINGS INC Information[90] indica que los costes de recuperación suponen una media de 10 veces el coste del pago del rescate. También afirma que, tras la recuperación del incidente, muchas de las empresas que se vieron comprometidas no se sienten fuera de peligro, por ese motivo y dependiendo de la complejidad de los datos, su recuperación incluso puede extenderse hasta 12 meses.

[89] https://www.cyberscoop.com/tardigrade-bio-isac-coronavirus-biomanufacturing-bioeconomy/

[90] https://www.eqh.com/

El informe de Datto de 2020[91] sobre ciberseguridad orientado a Ransomware indica que el coste de tiempo de inactividad para las PYMEs aumento un 486% respecto al de 2018. Esto es debido al incremento de los costes de recuperación y del tiempo empleado, ya que actualmente los ataques son más complejos y sofisticados. En este estudio también se apunta que el gasto también se ve incrementado cuando las empresas son dependientes de herramientas de respaldo obsoletas.

Al igual que el estudio realizado por EQUUS HOLDINGS, este también destaca que los costes de inactividad superan con creces la demanda del rescate inicial, pero por lo contrario es que este valora en 50 veces más el coste de la inactividad frente a la cuantía exigida en el rescate.

Según este informe evalúa un coste de rescate promedio de 5.600 dólares, y estima un importe promedio de 274.200 dólares por el tiempo de inactividad

Ilustración 21 - Comparación de costes del rescate e inactividad de una empresa afectada[92].

También se extrae de este, que el 91% de los proveedores de servicios administrados apuntan que los clientes que disponen un plan de recuperación ante desastres y continuidad del negocio, tienen menos probabilidades de experimentar un tiempo de inactividad significativo debido a una infección por Ransomware. Y tambien se señala que 4 de cada 5 pequeñas empresas que tienen dichos planes puede recuperarse de un ataque de este tipo dentro de unas 24 horas.

En el último informe realizado por Sophos[93] con relación a los ataques Ransomware, en 2021, con datos de empresas pequeñas y medianas empresas de entre 100 y 5000 empleados, de las cuales 150 son empresas españolas, arroja costes más elevados que en el anterior estudio.

En este se indica que el coste medio del rescate durante 2021 para empresas de 100 a 1000 empleados es de 107.694 dólares, y para empresas de 1001 a 5000 empleados alcanzo los 225.588 dólares.

En este también se evalúa el coste medio de las consecuencias del ataque de Ransomware, en 2021 fue de 1,85 millones dólares, más del doble del coste medio que del 2020, este fue de 761.106 dólares. El coste medio de la remediación en España es de 600.000 dólares en 2021.

2.4.3 Daño reputacional

El haberse visto afectado por un Ransomware puede tener un alto impacto para una PYME, desde la disrupción hasta un daño permanente. Y el tiempo que una compañía no puede realizar su actividad de forma adecuada, importa, y las noticias de la situación pueden llegar a sus clientes y

[91] https://www.xantrion.com/wp-content/uploads/Datto-Ransomware-and-the-Cost-of_Downtime.pdf

[92] https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf

[93] https://secure2.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-Ransomware-2021-wp.pdf

la publicidad negativa puede afectar de forma tan crítica que dañe la imagen de forma irremediable.

En la actualidad un riesgo que cada día se tiene más en cuenta es el reputacional, como se ve en el informe realizado por KPMG[94] sobre riesgos en abril de 2019. En este sitúa al riesgo reputacional en cuarto puesto, por encima del riesgo de ciberseguridad, en la clasificación de los 5 riesgos que más preocupan a los CEOs en España, durante 2018.

2018		2017		2016		2015	
1	Vuelta al proteccionismo/ territorialismo (*)	1	Riesgo operacional	1	Riesgo de ciberseguridad	1	Riesgo estratégico
2	Riesgos climáticos y medioambientales	2	Riesgo de tipo de interés	2	Riesgo con terceros	2	Riesgo operacional
3	Riesgos de tecnologías disruptivas y emergentes	3	Nuevos hábitos de clientes	3	Riesgo de talento	3	Riesgo de la cadena de suministro
4	Riesgo reputacional	4	Riesgo de ciberseguridad	4	Riesgo regulatorio	4	Riesgos de tecnologías disruptivas y emergentes
5	Riesgo de ciberseguridad	5	Riesgo de fraude	5	Riesgos de tecnologías disruptivas y emergentes	5	Riesgo de talento

Ilustración 22 - Clasificación de los 5 riesgos que preocupan a los CEOs de España[95].

Este viene incentivado especialmente a que hoy en día las redes sociales contribuyen a difundir en segundos cualquier noticia. Este riesgo es difícil de gestionar por su naturaleza subjetiva, ya que se basa en expectativas y percepciones de usuarios, y cambiante, y además compleja de cuantificar el riesgo.

En ocasiones cuando se sufre un incidente de seguridad la forma de actuar de las PYMEs es de forma reactiva, tanto en el ámbito de la ciberseguridad como en el reputacional. Y habitualmente se abordad como un caso de gestión de crisis de comunicación, que es algo puntual, y una monitorización constante de lo que se piensa/habla de la organización. El riesgo reputacional requiere una gestión y vigilancia constantes.

Como se ha indicado anteriormente el riesgo reputacional resulta complicado de medir, ya que no genera pérdidas directas, como ocurre con riesgos más tradicionales, pero puede tener una gran repercusión en las finanzas de la empresa.

A parte de los costes económicos mencionados en el punto anterior, se debería contemplar el coste del daño reputacional que pudiera sufrir. Además de las inversiones en marketing y relaciones públicas para abordar de forma reactiva el incidente, si la PYME no contara ya con un equipo para solventar dichas competencias. El objetivo de dicho equipo será recuperar la pérdida de confianza.

En la actualidad, existe una tendencia de emplear el Ransomware operado por humanos, que suele ser empleado en ataques grande. En este aparte de cifrar los datos, también se suele amenazar a las victimas con filtrar los datos confidenciales robados, estos suelen ser publicados en las plataformas controladas por estas bandas, de este modo intentan presionar a las víctimas con causar un daño hacia la reputación de la organización, si no pagasen.

Según un estudio realizado por Deloitte de 2016[96], los costes asociados con la gestión de las comunicaciones externas o el monitoreo de la marca después de un incidente, realizado las cuatro

[94] https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf

[95] https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf

[96] https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Los-riesgos-ocultos-de-un-ciberataque.pdf

semanas inmediatamente después de este puede ser de unos 400.000 dólares de promedio. Si, por lo contrario, lo que se requiere es monitorizar y reparar los posibles daños, el coste estimado de forma conservadora podrá alcanzar el millo de dólares al año.

3. Conclusiones

3.1 Conclusiones

El ransomware, ha sido uno de los principales protagonistas entre los ataques de ciberseguridad en los últimos años, y en especial este 2021, afectando a todo tiempo de empresas, pero en especial las pequeñas y medianas que son las que más se han visto afectadas, según datos de la Guardia Civil, un total del 70%.

Análisis de tendencias de cuál es el acceso un Ransomware en una PYME, muestra comúnmente es mediante un RDP expuesto al mundo, sin ningún tipo de control, y los correos de phishing. Y el motivo de estos dos vectores sean los más empleados, es que no es necesario un operador con grandes conocimientos para lanzar el ataque, y como el rescate a estas organizaciones pequeñas o medianas no puede ser muy elevado, ya que sería imposible abordar el coste. Por ello, son los más numerosos, dado que son los que más ajustan al nicho de mercado y las bandas criminales obtienen beneficios.

La educación en ciberseguridad por parte de las PYMEs habitualmente es baja, como se ha demostrado con datos estadísticos a lo largo de este estudio, pero la seguridad informática ha de pasar de ser actor secundario, o incluso en ocasiones inexistente, a convertirse en un elemento fundamental de la estrategia corporativa, cuya gestión debe planearse y ejecutarse mediante un enfoque general alineada con los objetivos estratégicos.

De ahí la necesidad un plan de contingencia, para planificar y anticiparse cómo actuar ante los incidentes, y no sólo emplear medidas reactivas, porque el tiempo de resolución supone una disrupción de la actividad de la empresa y puede llegar a tener unos costes elevados, por la dilatación en tiempo para lograr resolverlo, y a consecuencia de esto dañe irremediablemente la continuidad de organización. El tener un plan aumenta la resiliencia de las corporaciones desde las grandes hasta las más pequeñas.

Tan importante es saber que se debe hacer cuando se sufre un ransomware, como es disponer de unas medidas preventivas de seguridad que salvaguarden, en medida de lo posible, del impacto de un Ransomware. En estas medidas juega un papel muy importante el factor humano, el tener una plantilla de empleados concienciados y que siguen unas directrices de seguridad, implica un riesgo menor de sufrir un incidente, ya que estos participan en todos los procesos de funcionamiento de una organización

El disponer de un plan de acción, el implantar medidas preventivas, el tener una plantilla concienciada, no evita que las PYMEs puedan sufrir un ataque de Ransomware, pero sí que contribuye a que el daño sea menor y la disrupción sea la más corta posible. Las grandes empresas tienen embebida la seguridad de su negocio, y saben que invertir en ella a la larga les supone un

ahorro y puede que les ofrezca ventajas frente a competidores, esto debería suceder por igual en las PYMEs.

A pesar de tener buenas medidas preventivas y de protección, la PYME se puede convertir en víctima de un ataque de Ransomware, debería realizar una gestión de incidente lo más pronta posible, ya que el poder de infección de este es muy rápido. Para esto ayuda mucho el disponer del anteriormente mencionado plan de acción, tener un equipo experto y entrenado en ciberseguridad, además es esencial tener una política de copias de seguridad de sistemas y datos adecuada. Si no se dispone de un equipo con esas cualidades, siempre se puede externalizar. Las estadísticas indica que el pago del rescate no garantiza la recuperación de los sistemas e información cifrada, de ahí la importancia de los backups.

Cuando se sufre un ataque de Ransomware habitualmente se estiman los costes técnicos, la de la inactividad y el coste del rescate, si se contempla el pago, pero el sufrir un incidente de este tipo acarrea muchas implicaciones tanto legales (penales y civiles), sanciones o multas, como financieras (multitud de costes de diversos tipos) y reputacionales (tiene un impacto económico), que puede ser 10 veces mayor que el coste del rescate o inclusive más.

Ante el hecho de haber sufrido una infección por Ransomware y resolverla, no significa que el trabajo y la recuperación se hayan finalizado, porque después de cualquier incidente se debe llevar una serie de diligencias para aplicar las lecciones aprendidas, si estas no se acometen se seguirá siendo vulnerable.

3.2 Objetivos superados

Después del desarrollo del presente estudio se ha logrado superar con los siguientes objetivos:

- Comprender y definir en que consiste un Ransomware: este objetivo se logra exponiendo las características que posee el Ransomware, con ese fin se define qué es este programa malicioso y se desarrolla brevemente su evolución. Para conseguir este objetivo se ha utilizado una metodología exploratoria, esta sirve para aumentar el grado de conocimiento de este ataque.
- Conocer los tipos de Ransomware que afectan a las empresas: este propósito se consigue analizando las tendencias actuales de tipos de ataques de Ransomware, para ello se definen los vectores de entrada y se analiza la evolución de los últimos meses. Para conseguir este objetivo se ha utilizado una metodología investigación cualitativa, esta sirve para documentar y lograr entender como es el acceso a estas pequeñas organizaciones.
- Distinguir cuales son los vectores de entrada de un Ransomware en una PYME: este objetivo se consigue analizando los vectores de infección más comunes que se utilizan en el Ransomware para introducirse las organizaciones o equipos informáticos. Para alcanzar el objetivo se utiliza una metodología exploratoria que permite conocer el comportamiento para poder entrar en las empresas.
- Exponer y establecer cuáles son las medidas de seguridad que pueden tomar las PYMEs dentro de sus capacidades: este objetivo se alcanza explicando las medidas de seguridad, en este caso preventivas, que pueden aplicar las organizaciones de este tipo. Para conseguir este objetivo se utiliza una metodología exploratoria que permite analizar las acciones y herramientas que permiten salvaguardar las organizaciones, en medida de lo posible, de los Ransomwares.

- Definir cuál es el protocolo de gestión de incidente de Ransomware en una PYME: con este objeto se pretende desarrollar las medidas de seguridad reactivas y las acciones que debe realizar una mediana o pequeña empresa, para contener la infección y los pasos a seguir para lograr retornar a la actividad, con el menor impacto sobre ella. Para conseguir este objetivo se utiliza una metodología exploratoria y cualitativa, que permiten analizar las acciones a realizar que facilitan la recuperación de organización tras un incidente de este tipo.

- Conocer cuál es la legislación española aplicable en estos casos: para conseguir este propósito se ha supervisado los principales artículos del Código Civil y Penal Español, así como también LOPD, con los que se pueden ver afectados los atacantes, y con especial atención con los que pueden incurrir una organización afectada tras un incidente de dichas características. Se continúa con el uso de una metodología cualitativa, para lograr comprender el alcance que puede conllevar las conductas delictivas, la responsabilidad penal y civil e incluso multas y sanciones.

- Describir los daños que puede sufrir una empresa tras sufrir un incidente de este tipo: con este objetivo se pretende estudiar los costes tanto financieros como reputacionales, que también repercuten en costes económicos, y el impacto que pueden tener. Para lograr este objetivo se aplica una metodología exploratoria que permite enumerar unos posibles costes a tener en cuenta cuando se sufre un incidente de este tipo.

3.3 Trabajo futuro

Las posibles líneas de trabajo podrían ser:

- Realizar un plan de acción detallado para una PYME, no sería necesario que fuera una entidad real, podría ser ficticia, y posteriormente valorar las acciones y realizar una evaluación de costes si se viera afectada por un Ransomware, es decir llevar a cabo el plan.
- Realizar un estudio de la evolución y tendencias de posibles tipos y vectores de ataques que pueda adoptar el Ransomware.

4. Glosario

Phishing: es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

PYME o MicroPYME: es empresa pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y número de trabajadores. Según el Ministerio de Industria, Comercio y turismo estas se clasifican mediante unos límites financieros y el número de empleados, como se muestra en la siguiente tabla.

Categoría de empresa	Efectivos	Volumen de negocio	Balance general
Mediana	<250	<= 50 millones EUR	<= 43 millones EUR
Pequeña	<50	<= 10 millones EUR	<= 10 millones EUR
Micro	<10	<= 2 millones EUR	<= 2 millones EUR

RaaS: es un modelo de negocio, en que un grupo o un usuario desarrolla un conjunto de herramientas de Ransomware, y por otra parte otro grupo compran o se suscriben a estas para lanzar ataques. Por esto, usuarios con poca experiencia pueden llevar a cabo ataques complejos, y esta facilidad a conseguido que crezca el número de plataformas RaaS, a su vez, es una de las causas del aumento de los ataques masivos de Ransomware.

Ransomware: es una extorsión que se realiza a través de un malware que se introduce en los equipos de una organización. Este software malicioso secuestra la información de la empresa, así impide el acceso a esta cifrándola, lo que puede provocar pérdidas económicas y posibles daños reputacionales de la imagen de la organización.

Ransomware operado por humanos: Se tratan de ataques que dependen de actores humanos que pueden aprovechar fácilmente su conocimiento sobre la administración del sistema y las configuraciones erróneas de seguridad de la red para contrarrestar cualquier defensa cibernética. Los actores humanos también son más adaptables y pueden realizar un reconocimiento completo de su objetivo antes de iniciar el ataque. Estos acceden a la organización mediante algún software malicioso, que se emplea para robar datos confidenciales, como datos bancarios, contraseñas y otras credenciales que los ciberdelincuentes utilizan para aumentar el nivel de privilegios en una computadora. Y posteriormente lanzan el ransomware e incluso también otros malwares. Habitualmente para presionar a las víctimas para que paguen los rescates amenazan con hacer pública la información.

5. Bibliografía

LIBROS CONSULTADOS:

- Iria da Cunha. <<El trabajo de fin de grado y de máster. Redacción, defensa y publicación>>. Editorial UOC (Oberta UOC Publishing, SL). ISBN: 978-84-9064-391-4. Junio 2016

WEBS CONSULTADAS:

- https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_Ransomware.pdf - Visitado el 15 de septiembre de 2021.
- https://www.softeng.es/es-es/blog/balance-2020-de-los-ciberincidentes-en-espana-proyeccion-para-el-2021.html - Visitado el 26 de septiembre de 2021.
- https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf - Visitado el 26 de septiembre de 2021.
- http://www.iPYME.org/es-ES/DatosPublicaciones/Paginas/DefinicionPYME.aspx - Visitado el 27 de septiembre de 2021.
- https://metodologadelainvestigacinsiis.blogspot.com/2011/10/tipos-de-investigacion-exploratoria.html - Visitado el 27 de septiembre de 2021.
- https://inversionesdalport.com/tipos-de-metodologia-de-la-investigacion/ - Visitado el 27 de septiembre de 2021.
- https://cuadernosdeseguridad.com/wp-content/uploads/2020/10/Informe-Ciberamenazas-Tendencias-2020.pdf - Visitado el 27 de septiembre de 2021.
- https://www.mcafee.com/enterprise/en-us/security-awareness/Ransomware.html Visitado el 27 de septiembre de 2021.
- https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf Publicado 02.04.2021 Visitado el 27 de septiembre de 2021
- https://www.avast.com/es-es/c-what-is-Ransomware Visitado el 27 de septiembre de 2021.
- https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-Ransomware-pasado-presente-y-futuro/ Visitado el 5 de Octubre de 2021.
- https://www.coveware.com/blog/2021/10/20/Ransomware-attacks-continue-as-pressure-mounts Visitado el 5 de Octubre de 2021
- https://www.welivesecurity.com/la-es/2012/07/26/infografia-dorkbot-mas-de-80-000-bots-en-latinoamerica/ Visitado el 6 de Octubre de 2021
- REVETON Ransomware Spreads with Old Tactics, New Infection Method - TrendLabs Security Intelligence Blog (trendmicro.com) Visitado el 5 de Octubre de 2021
- FBI Cybercrime Division Ransomware Removal Guide (bleepingcomputer.com) Visitado el 1 de Octubre de 2021
- https://www.avast.com/es-es/c-what-is-Ransomware Visitado el 8 de Octubre de 2021

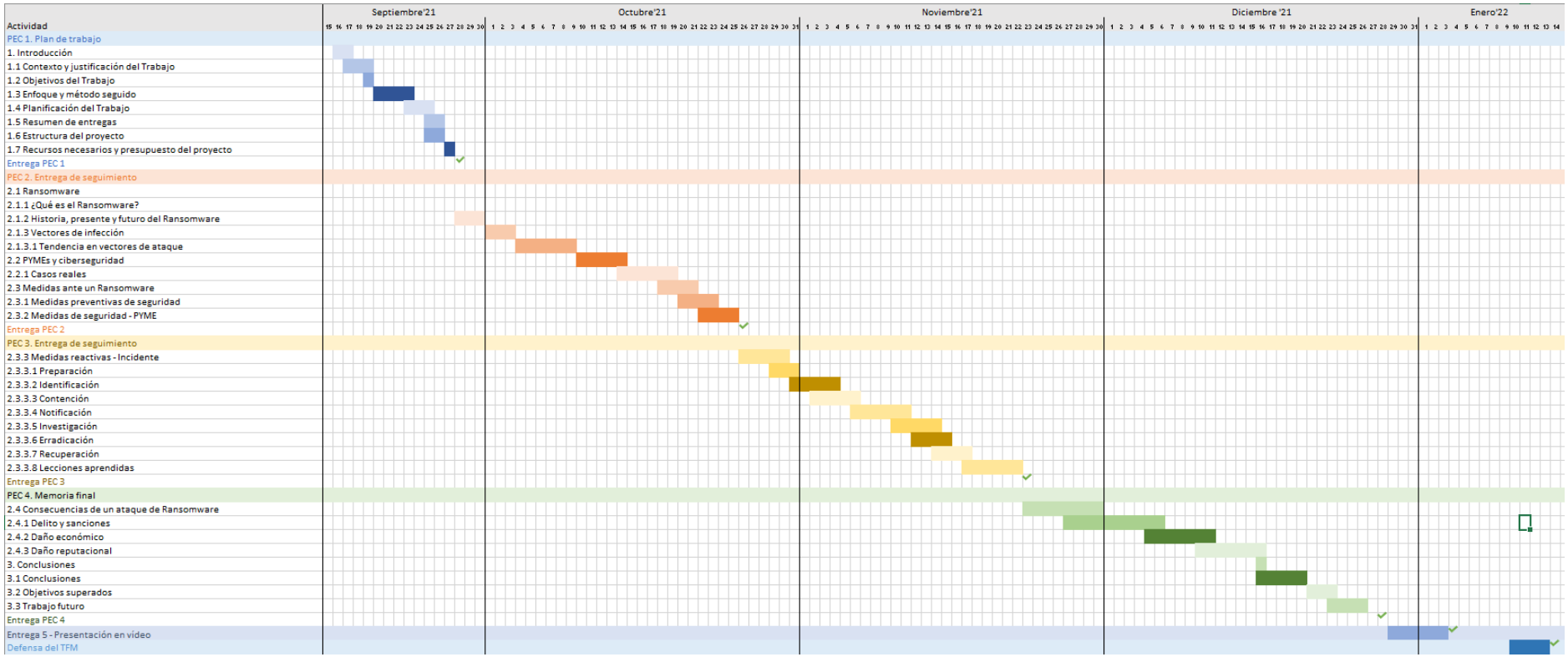
- https://www.europapress.es/economia/noticia-ciberataque-gss-interrumpe-atencion-cliente-telefono-canal-isabel-ii-20210921182641.html Visitado el 8 de Octubre de 2021
- Exploit: ¿sabes qué es y cómo funciona? - Panda Security Visitado el 10 de Octubre de 2021
- https://latam.kaspersky.com/blog/Ransomware-desafio-para-empresas-a-pesar-que-ataques-disminuyeron-un-56-en-2021/22896/ Visitado el 15 de Octubre de 2021
- https://jaymonsecurity.com/Ransomware-escritorio-remoto-rdp/ Visitado el 15 de Octubre de 2021
- https://www.xataka.com/seguridad/cuando-empresa-sufre-ataque-Ransomware-me-llaman-para-solucionarlo-dificil-lucha-malware-momento Visitado el 15 de Octubre de 2021
- https://www.hiscox.es/blog/como-puedo-proteger-mi-empresa-del-Ransomware Visitado el 15 de Octubre de 2021
- https://diedos.com/2021/03/05/que-es-el-seguro-cibernetico-todo-lo-que-necesita-saber-sobre-lo-que-cubre-y-como-funciona/ Visitado el 15 de Octubre de 2021
- https://latam.kaspersky.com/blog/how-scammers-hook-smb/19121/ Visitado el 17 de Octubre de 2021
- https://revistabyte.es/ciberseguridad/el-Ransomware-polizas-de-seguros/ Visitado el 19 de Octubre de 2021
- https://www.hornetsecurity.com/es/knowledge-base/Ransomware/encuesta-de-ataques-de-Ransomware-1-de-cada-5-empresas-es-victima/ Visitado el 20 de Octubre de 2021
- Cómo se emplea el escritorio remoto para infectar con malware (hipertextual.com) Visitado el 16 de Octubre de 2021
- La evolución del Ransomware: desde los bloqueadores a los cifradores | Blog oficial de Kaspersky Visitado el 21 de Octubre de 2021
- El flujo financiero del Ransomware | Blog oficial de Kaspersky Visitado el 21 de Octubre de 2021
- ¿Cuál es la solución de seguridad más eficaz contra el Ransomware? | Blog oficial de Kaspersky Visitado el 21 de Octubre de 2021
- Ransomware: Desafío para empresas a pesar que ataques disminuyeron un 56% en 2021 | Blog oficial de Kaspersky Visitado el 21 de Octubre de 2021
- https://www.ibercaja.es/empresas/corner-del-especialista/informacion-seguros/PYMEs-vulnerables-ciberseguridad/ Visitado el 22 de Octubre de 2021
- https://spinbackup.com/blog/Ransomware-backup-strategy/ Visitado el 23 de Octubre de 2021
- https://www.ituser.es/seguridad/2021/10/estas-son-las-barreras-que-convierten-a-las- PYMEs-en-vulnerables-en-ciberseguridad Visitado el 24 de Octubre de 2021
- Los atacantes de Ransomware bajan el cambio a la caza 'a mitad del juego' en Q3 (coveware.com) Visitado el 24 de Octubre de 2021

- https://www.kpmgimpulsa.es/blog/ciberseguridad-para- PYMEs_Visitado el 24 de Octubre de 2021
- https://www.redeszone.net/tutoriales/seguridad/mejores-firewall-open-source-proteger-red/ Visitado el 10 de Noviembre de 2021
- https://www.incibe-CERT.es/blog/Ransomware-medidas-preventivas-ii Visitado el 11 de Noviembre de 2021
- https://www.ccn-CERT.cni.es/informes/informes-ccn-CERT-publicos/2877-ccn-CERT-ia-11-18-medidas-de-seguridad-contra-Ransomware/file.html Visitado el 11 de Noviembre de 2021
- https://www.darkreading.com/attacks-breaches/how-to-negotiate-with-Ransomware-attackers Visitado el 13 de Noviembre de 2021
- https://www.ccn-CERT.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html Visitado el 14 de Noviembre de 2021
- https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/nbs/procedimientoBrechaSeguridad.jsf Visitado el 14 de Noviembre de 2021
- https://www.incibe-CERT.es/FAQ-RD_43-2021#estoy-obligado-a-notificar-incidentes-a-quien-como-que-cuando Visitado el 17 de Noviembre de 2021
- https://www.gdt.guardiacivil.es/webgdt/home_alerta.php Visitado el 17 de Noviembre de 2021
- https://www.policia.es/_es/denuncias.php Visitado el 17 de Noviembre de 2021
- https://www.emerita.legal/blog/penal/estafas/ataque-Ransomware-denunciar-delito-informatico-d13076/ Visitado el 10 de Noviembre de 2021
- https://www.adslzone.net/reportajes/seguridad/grupo-delitos-telematicos/ Visitado el 17 de Noviembre de 2021
- http://sedici.unlp.edu.ar/handle/10915/65216 Visitado el 20 de Noviembre de 2021
- https://www.tecnozero.com/antivirus-y-anti-Ransomware/que-es-un-edr/ Visitado el 20 de Noviembre de 2021
- https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html Visitado el 28 de Noviembre de 2021
- https://www.muycanal.com/2021/09/24/ Ransomware-costes Visitado el 28 de Noviembre de 2021
- https://www.orbit.es/cuanto-cuesta-un-ataque- Ransomware/ Visitado el 28 de Noviembre de 2021
- https://www.dealerworld.es/pubs/dw420/index.html?page=40 Visitado el 29 de Noviembre de 2021
- https://www.ontek.net/un-riesgo-oculto-del- Ransomware-la-inactividad/ Visitado el 30 de Noviembre de 2021
- https://www.ibm.com/downloads/cas/EV6NAQR4 Visitado el 30 de Noviembre de 2021
- https://www.webroot.com/blog/2021/04/21/ Ransomware-bec-and-phishing-still-top-concerns-per-2021-threat-report/ Visitado el 30 de Noviembre de 2021

- https://www.reale.es/es/empresas/ciber-seguridad Visitado el 06 de diciembre de 2021
- https://www.xantrion.com/wp-content/uploads/Datto-Ransomware-and-the-Cost-of_Downtime.pdf Visitado el 06 de diciembre de 2021
- https://secure2.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-Ransomware-2021-wp.pdf Visitado el 06 de diciembre de 2021
- https://ideas.llorenteycuenca.com/2021/03/ciberriesgos-y-reputacion-pautas-para-anticiparse/ Visitado el 10 de diciembre de 2021
- https://www.hispacolex.com/blog/blog-derecho-seguros/que-responsabilidad-legal-pueden-tener-la-empresa-y-los-empleados-ante-un-ciberataque/ Visitado el 15 de diciembre de 2021
- https://www.globalpoliticsandlaw.com/2021/05/23/ciberataque/ Visitado el 15 de diciembre de 2021
- https://www.eleconomista.es/legislacion/noticias/11214563/05/21/El-precio-de-pagar-el-rescate-a-los-hackers-delito-por-colaboracion-con-banda-criminal.html Visitado el 17 de diciembre de 2021

6. Anexos

Anexo I. Planificación del Trabajo



Anexo II. Tabla de la clasificación de los ciberincidentes.

CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
Contenido abusivo	**Spam**	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	**Sistema infectado**	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	**Explotación de vulnerabilidades conocidas**	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	**Compromiso de cuenta con privilegios**	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad	**DoS (Denegación de servicio)**	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	**Acceso no autorizado a información**	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante Ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	**Criptografía débil**	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para
		la reflexión o amplificación de ataques DDoS. Ej: DNS openresolvers o Servidores NTP con monitorización monlist.

	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Anexo III. Tabla de los criterios de del nivel del impacto de un ciberincidente.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
CRÍTICO	Afecta apreciablemente a la Seguridad Nacional.
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a una Infraestructura Crítica.
	Afecta a sistemas clasificados SECRETO.
	Afecta a más del 90% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.
	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual.
	Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
MUY ALTO	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
	Afecta a un servicio esencial.
	Afecta a sistemas clasificados RESERVADO.
	Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
	Daños reputacionales a la imagen del país (marca España).
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.
	Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual.
	Extensión geográfica superior a 3 CC.AA.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	Afecta a más del 20% de los sistemas de la organización.
	Interrupción en la presentación del servicio superior al 5% de usuarios.
	El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
	Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual.
	Extensión geográfica superior a 2 CC.AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

BAJO	Afecta a los sistemas de la organización.
	Interrupción de la prestación de un servicio.
	El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona.
	Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual.
	Extensión geográfica superior a 1 CC.AA.
	Daños reputacionales puntuales, sin eco mediático