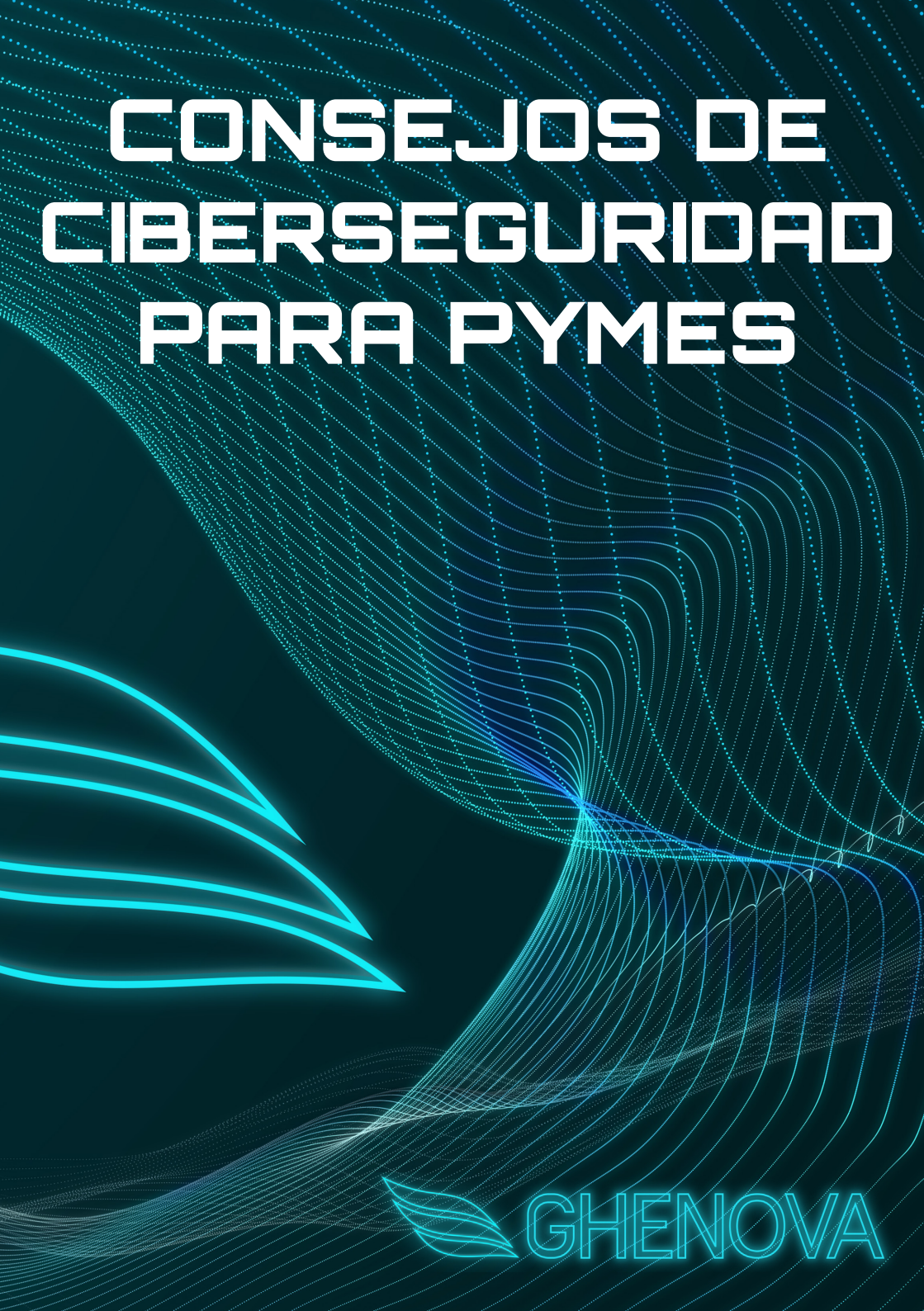
CONSEJOS DE CIBERSEGURIDAD PARA PYMES



1a edición: Junio 2023

www.ghenova.com

PRESENTACIÓN

Los avances en las tecnologías de la información (TI), su penetración en todos los campos de actividad y la conectividad a Internet han incrementado enormemente las oportunidades para las empresas.

Pero todo ello ha venido acompañado de nuevos riesgos. A medida que las empresas incorporan nuevas herramientas digitales y trasladan su negocio al ciberespacio, se incrementan las vulnerabilidades y aumenta el grado de exposición a unas ciberamenazas cada vez más numerosas y en constante evolución.

Esta guía, elaborada por Ghenova Ciberseguridad, tiene como objetivo ayudar a las pequeñas y medianas empresas a afrontar esta amenaza.

Empleando un lenguaje comprensible para todos, esta guía ayuda a entender la naturaleza del problema y a conocer las formas, en muchos casos muy simples y de bajo coste, con las que los pequeños y medianos empresarios pueden incrementar tanto la ciberseguridad de sus empresas como su capacidad para seguir operando o recuperarse en un tiempo breve en caso de un ciberataque.

También pretende convencer de que la ciberseguridad no debe verse como un gasto, sino como una fortaleza y una ventaja competitiva e, incluso, como una inversión.

Francisco Cuervas
CEO de Ghenova

ÍNDICE

INTRODUCCIÓN 3
Lo más valioso de mi empresa está en el ciberespacio 4
Existen dos clases de pymes: las que han sufrido un ciberataque y las que lo van a sufrir 6
Mi empresa es objetivo prioritario de las ciberamenazas 7
¿Conozco el perímetro de mi empresa en el ciberespacio? 8
¿Qué persigue la Ciberseguridad? 9
Transformación Digital y Ciberseguridad 10
Seguridad Física y Ciberseguridad 11
Certificaciones de empresa y Ciberseguridad 12
Evaluación inicial 14

LA AMENAZA 15
¿Quién, cómo y porqué puede atacar a mi empresa? 16
Ingeniería social 17
Phishing 18
Ataque del CEO 19
Ransomware 20
Denegación de servicio (DoS) 21
Defacement 22
Ciberespionaje 23

PREVENCIÓN, DEFENSA Y RECUPERACIÓN 25
Principios generales y buenas prácticas 26
Pólizas frente a ciberataques 42
Han atacado a mi empresa, ¿qué debo hacer? 43

¿QUÉ PUEDE HACER GHENOVA POR MI EMPRESA? 47
Portafolio de servicios 49

GLOSARIO DE TÉRMINOS 52

INTRODUCCIÓN

Lo más valioso de mi empresa está en el ciberespacio

> *No se puede acometer una transformación digital sólida y sin fisuras en una empresa sin disponer de una estrategia de ciberseguridad que la acompañe.*

Hoy en día, la gran mayoría de las empresas presentan sus productos en sus sitios en Internet, se relacionan con sus clientes a través del correo electrónico o formularios web, las transacciones comerciales se realizan a través de plataformas de pago electrónico y medios logísticos gestionados *on-line*, la atención al cliente se ha ido trasladando a *chat-bots* y gran parte del negocio se desarrolla a través de aplicaciones software que acceden continuamente a bases de datos digitales (inventario, tareas, proveedores, clientes…).

La interrupción o caída de cualquiera de estos activos o la pérdida de información sensible pueden poner en serio riesgo la continuidad de las operaciones, introducir retrasos inaceptables o provocar el incumplimiento de plazos, cobros y entregas. Sin embargo, a pesar de esta absoluta dependencia de lo digital, lo habitual es que el acceso rápido a la información y la facilidad en las comunicaciones se prioricen sobre la seguridad.

La pandemia COVID-19 ha acelerado la adopción de herramientas para posibilitar el trabajo remoto y compensar la pérdida de ingresos que suponía el impedimento a la presencialidad. En muchas ocasiones, la implantación de estas tecnologías se ha hecho de forma precipitada, sin la participación de personal especializado y sin contar con un soporte técnico adecuado, agudizando el problema. El resultado es que un gran número de pymes españolas carecen tanto de la consciencia del riesgo como de los más elementales medios de protección. Buena parte del problema radica en que todo lo relacionado con la ciberseguridad resulta opaco e incomprensible para una gran mayoría, algo que esta guía pretende remediar.

Si es usted un empresario, piense por un momento lo que para su negocio supondría la penetración de una infección de *malware*[1] que hiciera imposible el uso del correo electrónico, un *ransomware* que encriptara sus bases de datos, un ataque de denegación de servicios que impidiera el acceso a sus páginas web o el robo de información confidencial o crítica para las operaciones.

Pero es que, además, las consecuencias de un ciberataque rara vez son sólo internas. Es muy común que un incidente de este tipo se expanda con rapidez a clientes o proveedores, o que lleve aparejada la filtración de datos e información de terceros.

En resumen, sin las medidas adecuadas, un ciberataque puede poner en peligro la supervivencia de una empresa o su posición en el mercado, dañar de forma irremediable su reputación y hasta responsabilizarla legalmente frente a clientes y proveedores.

Si se adoptan medidas complejas y caras en el mundo físico para proteger un archivo o un almacén, lo coherente sería hacer lo mismo en el ciberespacio, pues el acceso no autorizado a los sistemas de la compañía puede resultar tanto o más probable que a sus instalaciones y las consecuencias aún más devastadoras.

1 Al final de la Guía se incluye un Glosario de Términos.

Existen dos clases de PYMES: las que han sufrido un ciberataque y las que lo van a sufrir

> *Todas las pymes sufrirán un ciberataque grave en los próximos 3 años. Más de un tercio de las pymes que sufran un ciberataque exitoso desaparecerán en el transcurso de los 6 meses siguientes.*

El primer paso para afrontar un problema es conocer que existe. Y uno de los factores más preocupantes que se detecta en el panorama nacional de la ciberseguridad es que las pequeñas y medianas empresas españolas no se autoperciben como objetivo de las ciberamenazas, cuando todos los análisis e informes las identifican como objetivos preferentes.

Las estadísticas demuestran que sufrir un ciberataque es sólo cuestión de tiempo. Y, generalmente, no mucho: se puede afirmar que en los próximos tres años todas las pymes sufrirán al menos un ciberataque grave.

Este ataque, de tener éxito, supondrá como promedio una pérdida en torno a los 100.000 euros. Y, en la actualidad, más de un tercio de las empresas que sufren un ciberataque exitoso quiebran en los seis meses siguientes, al no poder reponerse de las pérdidas sufridas (activos digitales irrecuperables, discontinuidad del negocio, daños reputacionales…).

Por lo tanto, las ciberamenazas constituyen uno de los principales riesgos para la supervivencia de una pyme, si no el mayor, y prepararse para tal eventualidad debería constituir una prioridad en la que debe implicarse por completo la alta dirección.

Mi empresa es objetivo prioritario de las ciberamenazas

> *Una pyme que no preste atención a su ciberseguridad tiene un futuro tan negro como una gacela coja en la sabana.*

Los leones, como las ciberamenazas, buscan saciarse a cambio del mínimo esfuerzo. Por eso acechan junto a la laguna esperando a que la gacela se acerque a beber; y eligen como víctima a la gacela más lenta o más débil.

Las grandes corporaciones y la Adminsitración han comprendido hace tiempo que las ciberamenazas constituyen un riesgo de primera magnitud y la ciberseguridad ha pasado de ser un tema meramente tecnológico a asunto fundamental de la gestión de riesgos que involucra a la alta dirección. Por tal motivo, llevan años fortaleciendo sus defensas y dotándose de medios para asegurar la supervivencia y la recuperación en caso de sufrir un ataque.

Por ello, a pesar de ser víctimas muy apetitosas para las ciberamenazas, las probabilidades de éxito son muy escasas al atacar a estas presas. De ahí que las ciberamenazas hayan ido trasladando progresivamente su actividad hacia las pymes, que resultan mucho más interesantes que los simples ciudadanos en términos de negocio pero que, en su mayoría, presentan tan débiles defensas como estos.

Y, en este contexto, las pymes que no prestan atención a su ciberseguridad son como las gacelas cojas.

¿Conozco el perímetro de mi empresa en el ciberespacio?

> *Es muy frecuente que las empresas desconozcan su perímetro en el ciberespacio y dónde está ubicada y cómo está protegida su información crítica.*

Al acometer la protección de los activos digitales, es muy importante conocer con claridad su identidad, ubicación y qué personas tienen acceso a ellos. Mal puede protegerse aquello cuya existencia se desconoce o no se sabe con precisión dónde se encuentra.

Sin embargo, es muy frecuente que la dirección de la empresa desconozca la respuesta a esas preguntas, cuando no tendrían complejidad alguna aplicadas a los elementos físicos.

En una empresa pequeña, realizar un inventario de los activos digitales y establecer políticas de almacenamiento y acceso tanto a los dispositivos como a la información son tareas sencillas que suponen un primer paso absolutamente necesario para avanzar en la protección. Sin embargo, la gran mayoría no ha dado este paso ni es consciente de su importancia.

En empresas de cierta entidad, lo anterior puede no resultar tan simple, por lo que puede ser conveniente contar con algún tipo de apoyo especializado. Por tal motivo, uno de los primeros consejos ha de ser el considerar la contratación de una asistencia técnica especializada o, incluso, la creación de un departamento TIC en consonancia con el tamaño de la empresa, su dependencia tecnológica y la naturaleza de sus activos digitales

¿Qué persigue la Ciberseguridad?

> *El objetivo fundamental de la Ciberseguridad es proteger la confidencialidad de la información, así como su integridad y disponibilidad y la de los sistemas que la almacenan y gestionan.*

La Ciberseguridad tiene que ver con la información, con los sistemas y con las personas. Su objetivo fundamental es proteger la confidencialidad de la información, así como su integridad y disponibilidad y la de los sistemas que la almacenan y gestionan.

Esto significa, en lo referente a la información, protegerla de accesos no autorizados, garantizar que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, y asegurar que sólo pueda ser modificada por las personas autorizadas y que se encuentre a disposición de quienes deban acceder a ella siempre que lo requieran.

A lo anterior, hemos de sumar la autenticidad, que persigue garantizar la legitimidad del origen de la transmisión (es decir, atestiguar que el emisor de un mensaje es quien dice ser), la trazabilidad, que busca identificar de forma inequívoca al autor de cada acción, y el no repudio o irrenunciabilidad, que permite probar la participación de las partes en una comunicación, en sus dos sentidos (el no repudio en origen anula la posibilidad de que un emisor pueda negar un envío cuando el destinatario tiene pruebas de que se ha hecho; el no repudio en destino impide que el destinatario pueda alegar la no recepción de una comunicación cuando el remitente tenga pruebas de que sí fue recibida).

Transformación Digital y Ciberseguridad

> *No se puede acometer una transformación digital sólida y sin fisuras en una empresa sin disponer de una estrategia de ciberseguridad que la acompañe.*

Para un empresario puede parecer lógico y suficiente abordar la ciberseguridad únicamente desde la perspectiva del cumplimiento legal y normativo. Sin embargo, la realidad y la experiencia aconsejan tener una mayor amplitud de miras.

Digitalizar la documentación, fomentar el teletrabajo, emplear portales de venta *on-line* y mover los servicios a la nube son prácticas muy de moda y que pueden contribuir notablemente a desarrollar un negocio y a mejorar la eficiencia. Sin embargo, pueden suponer también puertas de entrada y vulnerabilidades susceptibles de ser explotadas por las ciberamenazas y, por lo tanto, un gran riesgo para los activos críticos de la empresa.

Por tal motivo, los procesos de digitalización y el desarrollo e implantación de políticas, procedimientos y medidas de ciberseguridad deben ir de la mano, para proteger adecuadamente unos activos cuya naturaleza ha cambiado.

Ciberseguridad que no debe entenderse únicamente como prevención, sino que ha de abordar también la manera de fortalecer tanto la capacidad de operar en un ambiente hostil o en condiciones degradadas (resiliencia) como la de restaurar lo dañado en el menor tiempo y de la forma más completa posible después de haber sufrido un ataque (restauración).

Seguridad Física y Ciberseguridad

> *La Seguridad Física es parte de la Ciberseguridad. Los dispositivos que almacenen o manejen información sensible o confidencial deben estar ubicados en lugares de acceso restringido y controlado.*

Los elementos físicos que forman parte de los sistemas TI constituyen una importante fuente de riesgos para una pyme. Acciones como reiniciar, detener, conectar o desconectar son algunas de las posibilidades que puede emplear un atacante potencial para lanzar un ciberataque cuando cuenta con algún tipo de acceso físico a los dispositivos de la empresa. Obviamente, esta posibilidad se acrecenta cuando el atacante forma parte de la propia organización (*insider*).

Por tal motivo, es muy conveniente que los dispositivos que almacenen o manejen información crítica, sensible o confidencial estén ubicados en lugares de acceso restringido y controlado (biometría, clave, tarjeta magnética, videovigilancia…).

En las empresas, por lo general, los aspectos de seguridad física están mucho más desarrollados y maduros que los de ciberseguridad, por lo que incluir los "activos ciber" en los planes y protocolos de seguridad física corporativos no debería de ser muy complicado. Lo importante es tenerlos bien identificados y adecuar las medidas de seguridad física a su criticidad. Así mismo, es importante incluir todos los elementos físicos de los que dependa el funcionamiento de estos activos ciber críticos, como pudieran ser la ventilación o el suministro eléctrico (esto es especialmente importante en el caso de los Centros de Proceso de Datos, CPD).

Certificaciones de empresa y Ciberseguridad

Muchas empresas, organismos y corporaciones han entendido que la ciberseguridad es un asunto de la máxima importancia. Pero si hace unos años acreditar una buena salud de la ciberseguridad corporativa podía suponer una cierta ventaja competitiva, hoy en día resulta algo absolutamente necesario para sobrevivir en el mercado. Si bien hay otras, en el ámbito empresarial español las certificaciones más demandadas en la actualidad son la conformidad con el ENS y la ISO/IEC 27001.

El **Esquema Nacional de Seguridad (ENS)** es la referencia nacional para medir el nivel de seguridad de los sistemas de información del Sector Público, de los que tratan información clasificada y de los de las entidades del sector privado cuando presten servicios o provean de soluciones al Sector Público. Fue aprobado por el Real Decreto 3/2010 y en mayo de 2022 entró en vigor una nueva versión [2].

El ENS establece unos requisitos mínimos que todo sistema de seguridad de la información debe cumplir en relación con diversos aspectos: organización, análisis y gestión de los riesgos, personal, autorizaciones y control de accesos, protección de las instalaciones, protección de la información almacenada y en tránsito, interconexiones, registro de la actividad, incidentes de seguridad y continuidad del negocio, mejora continua del proceso.

2 https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

Contempla un proceso cíclico e iterativo que se inicia con la preparación y aprobación de una política de seguridad de la entidad, al que sigue la categorización de los sistemas atendiendo a la información manejada y los servicios prestados, un análisis de riesgos y un plan de adecuación.

Existen tres niveles de exigencia para los sistemas. Los de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, mientras que los de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad. La auditoría debe ser realizada por una entidad acreditada por la Entidad Nacional de Acreditación (ENAC).

La **ISO/IEC 27001** es una norma internacional que contiene los requisitos para la implantación de un Sistema de Gestión de Seguridad de la Información, contra la que puede certificarse voluntariamente una entidad (pública o privada) mediante un proceso de auditoría realizado por un auditor certificado externo.

Se basa en el denominado "Ciclo de Deming" o PDCA - acrónimo de *Plan, Do, Check, Act* (Planificar, Hacer, Verificar, Actuar).

El ENS y la ISO/IEC 27001 difieren en su naturaleza, ámbito de aplicación, obligatoriedad y objetivos. Sin embargo, la estructura del ENS responde también al modelo PDCA-Mejora continua y ambas herramientas son compatibles y complementarias, lo que permite aprovechar gran parte del esfuerzo dedicado a la obtención de una acreditación en la consecución de la otra. En cualquier caso, para ello será fundamental el que la alta dirección de la empresa lidere el proceso y se involucre completamente en él.

Evaluación inicial

> *El primer paso para evaluar la "salud" de la ciberseguridad de una empresa debe ser conocer su estado por medio de la realización de inspecciones, test y pruebas específicamente diseñadas para ello.*

El primer paso para evaluar la salud de la Ciberseguridad de la empresa debe ser conocer el estado del paciente. Y para ello hay distintas formas de obtener la información: cuestionarios, inspecciones *in situ*, análisis de vulnerabilidades, auditorías, test de penetración…, que equivalen a las consultas médicas, análisis de sangre, electrocardiogramas, escáneres, TACs…

De esas pruebas, las hay más simples y livianas para el paciente, pero que puede que no lleguen a detectar todas las anomalías, y otras que son más concluyentes, pero que a cambio pueden resultar más intrusivas, agresivas y caras. Por lo tanto, es importante alcanzar un equilibrio que nos permita obtener la máxima información con el mínimo coste y trastorno.

El resultado será, en todos los casos, un informe del estado en el momento de la prueba y unas recomendaciones (tratamiento) para la mitigación de riesgos y corrección de deficiencias.

También, como en medicina, en ciberseguridad existen factores de riesgo. Carecer de un inventario de activos, no actualizar los sistemas, un mal uso de los dispositivos extraíbles o tener una política laxa de control de accesos serían los equivalentes a fumar, ingerir alcohol habitualmente, no tomar precauciones en las relaciones sexuales o llevar una vida sedentaria: el riesgo de que ocurra algo grave se multiplica.

LA AMENAZA

¿Quién, cómo y por qué puede atacar a mi empresa?

Una de las principales características de la ciberamenaza es su herterogeneidad. Entre los miles de individuos que hacen uso del ciberespacio con files hostiles o maliciosos, podemos encontrar desde los novatos y poco capaces *script kiddies* o *wanabees*, que utilizan herramientas y técnicas muy básicas y solo resultan preocupantes para objetivos desprotegidos, hasta las superpoderosas Amenazas Persistentes Avanzadas (APT, *Advanced Persistent Threats*, por sus siglas en inglés), generalmente asociadas al ámbito de la inteligencia o al militar, pasando por los *hackers* profesionales, las organizaciones criminales y los grupos hacktivistas.

Para una pyme, lo normal es que el grupo más peligroso lo constituyan los grupos que persiguen el beneficio económico (ciberdelincuentes), y que la forma de ataque más preocupante sea el secuestro de información (*ransomware*).

Sin embargo, dependiendo de otros factores, como sector de negocio en el que trabaje la pyme, proyectos en los que esté implicado, clientes, etc., puede interesar de forma eventual a actores de naturaleza diferente que busquen algún rédito en términos de propaganda o activismo político, adquirir algún tipo de ventaja competitiva, dañar la reputación de un contratista u obtener acceso a información clasificada de algún proyecto concreto. A continuación se exponen las técnicas y tipos de ataque que con mayor probabiliad puede tener que afrontar una pyme.

Ingeniería social

> *Las técnicas de ingeniería social buscan, a través del engaño, que la víctima proporcione de forma voluntaria información que posibilite un ataque posterior o realice alguna acción que lo desencadene.*

El concepto de ingeniería social engloba diversas técnicas de engaño cuyo fin es que la víctima proporcione de forma voluntaria información que posibilite un ataque posterior o realice alguna acción que lo desencadene.

Se sustenta sobre dos principios: que los usuarios constituyen el eslabón más débil de la cadena de la ciberseguridad y que la mayoría de las personas tienen una tendencia natural a ayudar a otra en problemas.

Un ingeniero social utilizará generalmente el correo electrónico, la mensajería instantánea o el teléfono para contactar con la víctima, fingiendo ser otra persona (un empleado de otro departamento u otra empresa, un técnico, un cliente…). Tratará de crear una relación de confianza y un contexto que justifique una petición, aparentemente inocua, pero que será la desencadenante o posibilitadora de una acción maliciosa posterior (por ejemplo, que la víctima facilite unas credenciales de acceso, clique un enlace o escanee un código QR).

En muchas ocasiones, el atacante utilizará información previamente obtenida (por lo general, de redes sociales) tanto para establecer la relación de confianza como para dar verosimilitud a la situación. La mayoría de ataques se apoyan en estas técnicas, por lo que es muy conveniente que los empleados estén alertados de su existencia y sean capaces de detectarlas.

Phishing

> *El* phishing *es una acción precursora cuyo nombre proviene de la palabra inglesa "*fishing*" (pesca), haciendo alusión a utilizar un cebo y esperar a que las víctimas 'muerdan el anzuelo'.*

Más que una modalidad de ataque, el *phishing* es una acción precursora y posibilitante de otras posteriores. Por lo general, se combina con otras técnicas, como la suplantación de identidad y la ingeniería social, para incrementar sus posibilidades de éxito. Emplea el correo electrónico y la mensajería SMS como vectores más frecuentes para alcanzar a las víctimas.

Generalmente, se trata de campañas masivas en las que se envían cientos y hasta miles de correos o mensajes suplantando la identidad de grandes compañías u organismos oficiales, confiando en que al menos un pequeño porcentaje caerá en el engaño.

Lo más habitual es que en la comunicación se solicite al destinatario y potencial víctima que ejecute alguna acción mediante la cual se produzca una descarga de *malware* y la correspondiente infección: por ejemplo, clicar en un enlace (normalmente, una URL recortada), escanear un código QR o ejecutar un archivo adjunto.

Cuando se dirige a una víctima concreta y previamente seleccionada, suele explotarse alguna información previa que permita ganarse la confianza del destinatario (remitente confiable, asunto de interés…) y, en este caso, se denomina *spear phishing.*

Cuando el objetivo del *spear phishing* es un alto cargo, se denomina *whaling* (de *whale*, ballena).

El ataque del CEO

> *A pesar de ser muy conocido, el denominado ataque del CEO sigue teniendo un elevado índice de éxito entre las pymes.*

El denominado ataque o fraude del CEO, es un caso especial que combina phishing e ingeniería social y, a pesar de que se supone muy conocido, tiene todavía un elevado índice de éxito, por lo que merece un tratamiento especial.

Su secuencia es la siguiente: Los criminales obtienen la identidad de un alto cargo de la empresa (por ejemplo, a través de LinkedIn). A continuación, tratan de obtener el máximo de información posible sobre su agenda (participación prevista en eventos, actos, viajes…) a través de publicaciones en redes sociales, medios de comunicación, etc., así como sobre el sector de actividad de la empresa, contactos, colaboradores, rumores sobre posibles fusiones…

El siguiente paso es la identificación de alguien de la empresa que cuente con permisos para realizar transferencias. Será a esta persona a la que se le envíe un correo electrónico en el que se suplante la identidad del CEO y en el que se exigirá el ingreso urgente y reservado de una cantidad elevada en una cuenta corriente, controlada por el estafador. Con la información obtenida en la fase anterior, el atacante tratará de construir en el correo un relato creíble en el que se reúnan unas circunstancias que, por una parte, contribuyan a que la víctima no sospeche que se trata de un engaño y, por otra, justifiquen tanto el pago sobrevenido como su urgencia y confidencialidad. Todo ello, unido a la relación de autoridad del CEO con la víctima, da lugar a que con cierta frecuencia algún empleado realice la transferencia de manera inmediata sin las debidas verificaciones.

Ransomware

> *Un ataque de* ransomware *constituye, probablemente, la amenaza más seria para la supervivencia de una pyme.*

Se trata de la modalidad de ataque más extendida en los últimos tiempos y la que más dinero mueve en el Mundo, haciendo del cibercrimen la forma delictiva más productiva, por encima del tráfico de drogas, de armas o de personas. Por su naturaleza, es la más peligrosa y potencialmente dañina para una pyme.

Utilizando técnicas muy diversas, los atacantes buscarán acceder a algún activo importante de la red víctima para, a continuación, cifrarlo y solicitar un rescate a cambio de su descifrado, generalmente en algún tipo de criptomoneda, lo que impedirá su rastreo.

Los vectores más empleados por los atacantes para llevar el malware al objetivo suelen ser el correo electrónico (*phishing e-mail*), o la infección de dispositivos USB (*baiting*) o de sitios web visitados por los empleados (*watering hole*), transmitiendo la infección a la red.

El *malware* WannaCry, atribuido a un grupo APT norcoreano y protagonista de uno de los ciberataques más mediáticos de todos los tiempos, explotaba una vulnerabilidad de Windows, que había sido descubierta unos meses atrás, y combinaba los efectos de un gusano (era capaz de propagarse automáticamente por equipos y redes sin necesidad de interacción humana) con los de un *ransomware*. Esta circunstancia propició que en las primeras veinticuatro horas de campaña consiguiera infectar a cerca de un cuarto de millón de dispositivos y se extendiera a más de un centenar de países.

Denegación de Servicio (DoS)

> *Los ataques de denegación de servicio (DoS) pueden poner en peligro los activos expuestos a Internet (sitio web, cuentas en RRSS...), paralizando los servicios a cliente y provocando daños reputacionales a la empresa.*

Los ataques de denegación de servicio (DoS, *Denial of Service*, por sus siglas en inglés) buscan que un servicio o recurso sea inaccesible a los usuarios legítimos sobrecargando los recursos computacionales del sistema atacado (por ejemplo, una página web). Una ampliación del ataque DoS es el llamado ataque de denegación de servicio distribuido, también llamado DDoS por sus siglas en inglés (*Distributed Denial of Service*), el cual se lleva generalmente a cabo sumando los recursos de cientos o miles de dispositivos, generando así un gran flujo de solicitudes que saturan el servidor objetivo, degradando su funcionamiento o dejándolo fuera de servicio.

Al principio, se utilizaron para ello ordenadores previamente infectados (*zombies*) para formar grandes redes (*botnets*) que sumaban y concentraban sus recursos contra el objetivo. La irrupción del Internet de las Cosas ha hecho que se empleen cada vez más este tipo de dispositivos, aprovechando sus, por lo general, débiles medidas de protección y malas configuraciones. Lo anterior, combinado con técnicas de reflexión y amplificación, ha permitido a los atacantes lanzar flujos de varios Terabytes por segundo contra sus objetivos.

Estos ataques, que pueden emplearse para echar abajo los activos de una empresa en Internet (páginas web, perfiles en redes sociales, etc.), pueden contratase como servicio y a muy bajo precio en la *Dark Web*.

Defacement

> *Los* defacements *equivalen a grafitis en la red. Suelen tener una motivación ideológica y buscan obtener la máxima notoriedad en apoyo a una causa y en contra de la reputación de la víctima.*

Se denomina *defacement* a un tipo de ataque mediante el cual se modifica la apariencia visual de un sitio web. Viene a ser algo así como un grafiti en la red. Se trata de un ataque típico del hacktivismo (activismo en Internet) y suele estar dirigido contra organismos oficiales, pero en muchas ocasiones sus víctimas han sido empresas y particulares que han contravenido algún aspecto relacionado con la causa ideológica que alguno de estos grupos defienda.

Persiguen la notoriedad, por lo que su éxito se mide por la repercusión mediática que consiga el ataque.

Para una pyme, tiene una especial importancia porque en muchas ocasiones suele traducirse en daños a la reputación y pérdida de clientes y volumen de negocio.

La posibilidad técnica de que ocurra está generalmente propiciada por algún error de programación de la página web, algún bug en el propio servidor o una mala administración por parte de los gestores de la web. Por tal motivo, es muy conveniente contratar el desarrollo de estos servicios a profesionales, tanto en lo referente a diseño web como al alojamiento del sitio, y someter el resultado a pruebas específicamente diseñadas para identificar y corregir las posibles vulnerabilidades y defectos de programación.

Ciberespionaje

> *Todo ciberataque responde a un patrón secuencial que se conoce como* killchain*. Los ataques cuya finalidad es el espionaje suelen contar con todas las fases. Ataques poco sofisticados o no dirigidos pueden obviar una o varias fases (en particular, el análisis del objetivo).*

Un ciberataque cuenta con varias fases diferenciadas, para cada una de las cuales existen técnicas y herramientas específicas. Un ataque poco sofisticado o masivo puede obviar alguna, pero lo normal en una campaña de ciberespionaje es que cuente con todas ellas: Reconocimiento, *Weaponization*, Entrega, Explotación, Instalación, *Command & Control* y Acciones sobre el objetivo.

En la fase de Reconocimiento el atacante tratará de obtener la máxima información posible del objetivo: identidad de personas y cargos, relaciones, direcciones IP, direcciones de correo electrónico, sistemas operativos, aplicaciones software empleadas en los sistemas, protocolos, elementos de defensa perimetral… Mucha de esta información puede obtenerse directamente de Internet o por medios pasivos, sin alertar a la víctima.

Con la información obtenida, los atacantes preparan una ciberarma a medida del objetivo (*Weaponization*), constituida por el binomio *Exploit + Payload* (partes del código del *malware* encargadas de aprovechar una vulnerabilidad del sistema y de realizar la acción maliciosa, respectivamente).

La Entrega es una parte crítica del ataque, siendo lo habitual que se apoye en técnicas de *phishing* o a través de la infección de algún dispositivo con acceso al sistema (por ejemplo, una memoria USB).

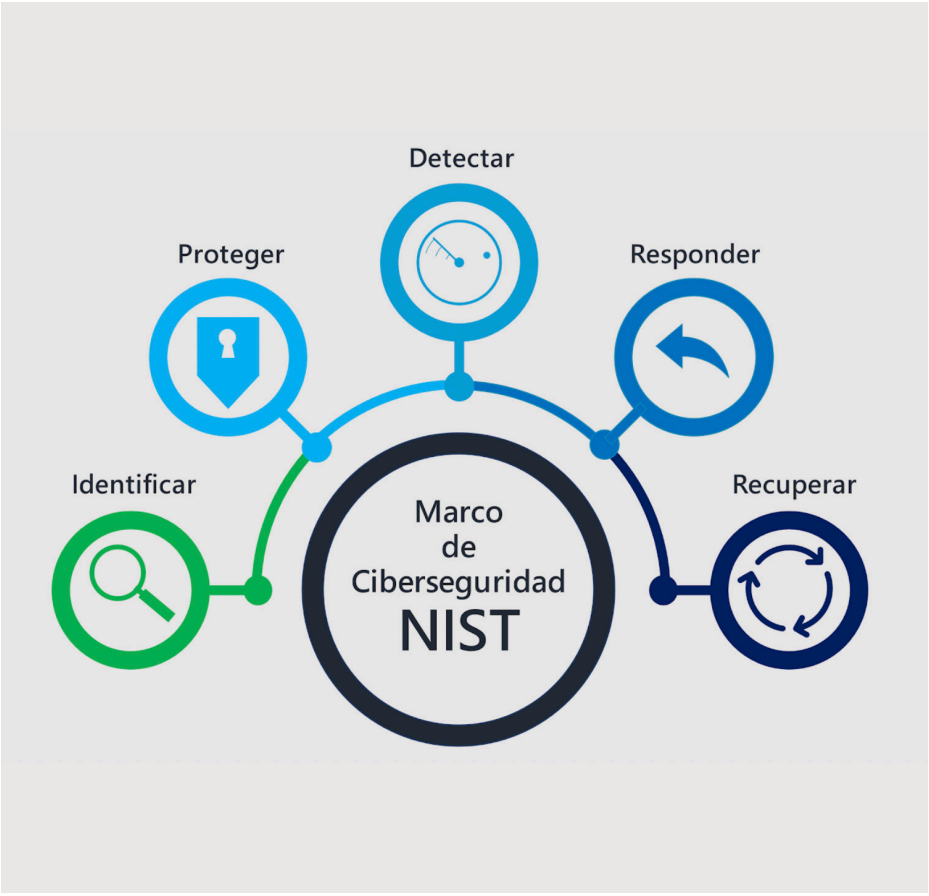
Una vez introducido el *malware*, éste se ejecuta aprovechando alguna vulnerabilidad del sistema objetivo, comenzando la instalación de diferentes módulos y elementos, como ocurre con cualquier software, tratando de no alertar a los administradores legítimos.

A continuación, se establecen las comunicaciones que permiten el control tanto del elemento infectado como del *malware*, permitiendo su actualización y asegurando su persistencia.

Los siguientes pasos son la escalada de privilegios, tratando de obtener privilegios de administrador y de administrador de dominio, el desplazamiento lateral y la expansión sigilosa, permitiendo la actuación remota sobre el sistema víctima en función de los intereses del atacante: robo y exfiltración de información, alteración de datos, etc.

PREVENCIÓN, DEFENSA Y RECUPERACIÓN

Principios generales y buenas prácticas



La siguiente selección de recomendaciones se basa principalmente en el modelo IDENTIFICAR-PROTEGER-DEFENDER-RESPONDER-RECUPERAR, propio del Marco de Ciberseguridad del NIST [3], buscando un enfoque eminentemente práctico. Su aplicación proporcionará a la empresa una sólida línea base de ciberseguridad de naturaleza preventiva y escalable.

3 Instituto Nacional de Estándares y Tecnología de los EE.UU.

Soporte documental, inventario y control de activos

Es importante contar con documentación técnica de cada sistema de la empresa, que incluya el inventario de los elementos que lo conforman y la configuración en detalle de cada uno de ellos. Esto permitirá identificar si le afectan vulnerabilidades que sean descubiertas, reducirá los tiempos para la aplicación de actualizaciones y parches y facilitará la planificación de la renovación o reemplazo de aquellos elementos próximos a finalizar su vida útil (por ejemplo, por estar anunciado el final de su soporte).

Así mismo, se deben designar responsables de llevar a cabo la comprobación periódica del inventario y de mantener actualizado el hardware y software de los diferentes sistemas.

Identificación de los activos críticos

Es conveniente identificar cuanto antes, a ser posible durante la fase de diseño, los activos críticos de la empresa, de forma que puedan diseñarse las soluciones técnicas más adecuadas para potenciar su protección y resiliencia (back-ups, redundancias de elementos o cableado, etc.).

En la identificación de activos críticos es muy importante tener en cuenta las mutuas dependencias entre los distintos elementos del sistema: un activo crítico puede depender de forma indirecta de otro que no se considera en principio crítico, pero que cambia su categoría debido a esta dependencia (por ejemplo, un sistema de refrigeración o ventilación de un elemento hardware crítico para el sistema).

Responsable de Ciberseguridad de la empresa

La normativa nacida a partir de la Directiva NIS de la Unión Europea establece una serie de obligaciones para determinadas empresas. Entre ellas, la de contar con un CISO (*Chief Information Security Officer*).

Si bien la mayoría de las pymes no están afectadas por esta normativa, se recomienda analizar la conveniencia de contar con una persona responsable de velar por la ciberseguridad corporativa y de proteger la información y los sistemas ante posibles ciberataques y fugas de datos. O, dicho de otro modo, de fomentar la seguridad de la información conforme a las posibilidades y circunstancias de cada empresa.

Durante mucho tiempo, la figura del CISO ha estado sujeta a diferentes interpretaciones y traducida a perfiles bastante heterogéneos y generalmente en un nivel muy alejado del directivo. Sin embargo, en los últimos años el CISO ha pasado de ser un profesional de perfil marcadamente técnico y completamente al margen de la estrategia empresarial a incorporarse de pleno en los procesos de negocio.

Esta circunstancia exige que el CISO aglutine unos conocimientos que engloban los niveles ejecutivo, operativo y técnico y, sobre todo, que posea la capacidad y habilidad para servir de nexo entre mundos que hablan lenguajes completamente diferentes: unos que piensan en la continuidad de negocio, la reputación o las implicaciones legales, otros que entienden de interrupciones de fabricación, retrasos de entrega o penalizaciones y otros que manejan vocablos como código ofuscado, *sniffer, keylogger, rootkit, zero-day o kerberoasting*.

En definitiva, todo empresario debería valorar la conveniencia de contar en su empresa con esa figura capaz tanto de representar de manera efectiva la posición de la organización con respecto a la seguridad de la información y la capacidad de influir en los directivos, como de identificar y evaluar las amenazas y traducir los riesgos a un lenguaje que los ejecutivos puedan entender, comprender las operaciones comerciales y los datos críticos que la organización está tratando de proteger y, al mismo tiempo, ser capaz de entender informes de seguridad complejos desde la perspectiva técnica y de traducirlos a un lenguaje entendible para el resto de equipos.

Actualizaciones y gestión de parches de seguridad

Las actualizaciones y los parches de firmware y software corrigen y resuelven problemas tanto funcionales como de seguridad. Por tal motivo, es fundamental que los sistemas operativos, programas, aplicaciones, drivers, antivirus, etc. estén siempre actualizados a su última versión y que se mantenga un registro en el que estén reflejadas todas las actualizaciones que se han llevado a cabo en el sistema y los elementos afectados.

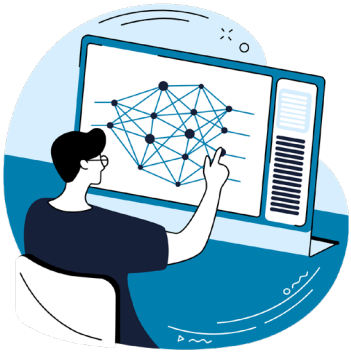
Segmentación y bastionado

La segmentación viene a ser el equivalente a la compartimentación estanca de un buque de guerra, una de las primeras medidas que se adoptan en la situación de zafarrancho de combate, y que consiste en cerrar todas las puertas y escotillas para que, en caso de un impacto o colisión, sus efectos (inundación, incendio, explosión) queden restringidos al menor espacio posible. En términos de ciberseguridad, consiste en dividir una red en varios segmentos o subredes, lo que, además de proporcionar diferentes ventajas a los administradores, permite confinar y controlar con mayor facilidad los efectos indeseables de un incidente.

Es muy conveniente que cada uno de los segmentos de red así constituidos (subredes o redes de área local) contengan únicamente los recursos específicos (ordenadores, servidores, impresoras…) necesarios para dar un servicio, y limitar los puertos, protocolos y servicios a los estrictamente necesarios. Con ello se habrán creado entornos de mínimo privilegio, que permitan controlar fácilmente su acceso, reducir la superficie de ataque y disminuir el tráfico en la red sin afectar a su rendimiento.

También es importante modificar las contraseñas por defecto en la electrónica de red *(routers* y *switches*), así como establecer un mecanismo que sólo permita la conexión a la red de equipos autorizados, asegurándose de que todos los accesos wireless están controlados y se realizan siempre a través de dispositivos autorizados y utilizando protocolos seguros.

Aislamiento de redes



Aunque no será lo habitual, es posible que por la naturaleza de su actividad o clientes alguna empresa tenga que contar con redes o sistemas que deban permanecer aislados o con acceso muy restringido.

Si este fuera el caso, durante la fase de diseño e instalación se han de detectar todas las posibles conexiones con otros sistemas y aplicar las soluciones técnicas adecuadas para cada tipo de interconexión. Han de ser objeto de especial atención las conexiones con redes públicas (fundamentalmente, Internet). Dependiendo de la criticidad de la red, esto se llevará a cabo bien mediante separación física (sin conexión) o bien con medidas de seguridad específicas que controlen dichas conexiones.

Además, es muy importante vigilar que esta situación se mantenga de forma permanente y que posibles modificaciones posteriores no la alteren. Deberá prestarse especial atención al conveniente aislamiento entre estas redes y otras de propósito general o de cortesía con las que cuente la empresa (por ejemplo, una red WiFi para visitantes). Se han dado numerosos casos de accesos no autorizados a sistemas de acceso restringido que se han conseguido a través de conexiones con este tipo de sistemas.

Estructura de seguridad de los sistemas

Se debe definir y mantener actualizada una estructura de seguridad para cada uno de los sistemas corporativos en la que se designe a los diferentes responsables y se establezcan de forma clara sus cometidos. Esta información debería estar integrada en el plan general de seguridad de la empresa.

Políticas y procedimientos

Además de las medidas técnicas para asegurar que los sistemas de la empresa estén debidamente protegidos y configurados para ser resilientes en caso de ataque, es importante también desarrollar políticas y medidas procedimentales que definan la forma en que los sistemas han de ser operados.

En particular, es muy conveniente desarrollar procedimientos operativos para determinados aspectos que tienen una acusada incidencia en la ciberseguridad, como pueden ser: el alta y baja de usuarios, las entradas y salidas de información, el acceso de terceros, la gestión de las copias de seguridad, el uso del correo electrónico, la instalación y empleo de aplicaciones, la notificación de anomalías, la gestión de incidentes de seguridad, etc.

Inspecciones y auditorías

De forma periódica, conviene llevar a cabo la inspección y auditoría de los sistemas por parte de personal especializado. Estas inspecciones han de contemplar aspectos de seguridad física, políticas y procedimientos operativos, y descubrimiento de vulnerabilidades, y deben generar como producto principal un informe que contenga una propuesta de medidas correctivas que resulten adecuadas para la mitigación de las deficiencias y vulnerabilidades encontradas.

Podría ser conveniente, además, someter a pruebas de penetración y a una revisión exhaustiva de las medidas de seguridad a aquellos sistemas considerados críticos.

Intercambio de información

Cuando la empresa tenga una entidad importante y así lo recomiende la naturaleza de los proyectos en los que esté implicado o la de sus clientes, puede ser conveniente establecer canales de cooperación con aquellos organismos de la Administración (por ejemplo, con el INCIBE-CERT, el CCN-CERT o algún CERT autonómico) y del ámbito privado con los que se pueda compartir información sobre amenazas, muy especialmente indicadores de compromiso y vulnerabilidades. Esto permitirá tanto mejorar las medidas preventivas como anticipar posibles ataques.

Control y seguridad de las aplicaciones

Los programas y aplicaciones software pueden tanto implicar vulnerabilidades explotables como constituir un vector de entrada de *malware* al sistema (esto último es especialmente aplicable a muchas aplicaciones para dispositivos móviles). Por tal motivo, es muy recomendable llevar a cabo la normalización de los equipos, para limitar sus funcionalidades a las estrictamente necesarias, restringir la instalación de aplicaciones únicamente a aquellas autorizadas por el responsable del sistema y configurarlas para que se ejecuten con el mínimo de privilegios que sea posible.

El correo electrónico merece una especial atención por ser uno de los principales vectores de ataque. Por ello, es importante limitar las herramientas y programas de correo electrónico autorizados e incidir en este aspecto en las acciones de concienciación, fomentando la alerta ante correos de los que desconozca el remitente y evitando la ejecución de archivos o ficheros de remitentes desconocidos. Otra medida valiosa es proporcionar unas instrucciones básicas para los usuarios que orienten su actuación ante la recepción de correos sospechosos.

Seguridad en la cadena de suministro y seguridad de terceros

En los últimos años se han incrementado de forma muy notable los ataques a través de la cadena de suministro. Estos ataques son muy difíciles de prevenir y detectar al comprometer directamente a proveedores externos, socios o clientes.

Entre las técnicas empleadas destaca el *tampering* o inserción intencionada de vulnerabilidades o código malicioso embebido en el hardware o software, que puede producirse en cualquiera de las etapas entre la fabricación y la instalación del elemento manipulado en el sistema objetivo (durante el diseño, desarrollo, fabricación, ensamblado, almacenamiento o transporte).

Hoy en día, los proveedores de servicios en la nube contemplan tres modalidades: software como servicio, plataforma como servicio e infraestructura como servicio (SaaS, PaaS e IaaS, respectivamente, por sus siglas en inglés). Obviamente, la tendencia creciente entre las empresas de trasladar a nubes de terceros desde sus centros de datos hasta las aplicaciones y el que, en consecuencia, toda la información operativa, aplicaciones, servidores y copias de seguridad estén depositados fuera de la empresa tiene sus implicaciones en ciberseguridad, especialmente cuando sus soportes físicos se encuentran ubicados fuera del territorio nacional.

Por ello, es importante que los elementos hardware y software y servicios asociados, especialmente aquellos que se empleen en los sistemas críticos de la empresa, procedan de proveedores de garantía y cuenten con un soporte técnico fiable y algún tipo de certificación de cibereseguridad (ISO/IEC 27001, ENS, etc.).

Algunas formas de reducir el riesgo son utilizar productos de fabricantes reputados, proveedores de servicios y medios de distribución de confianza o utilizar precintos, sellos y embalajes a prueba de manipulaciones.

Registro de actividad

Para poder detectar patrones anómalos y llevar a cabo investigaciones forenses en el caso de un incidente, los sistemas se deben configurar para que almacenen determinados registros (eventos del sistema, logs de acceso, logs de errores) que sean generados por los diferentes elementos de la red o del sistema (sistema operativo, estaciones de trabajo, antivirus, dispositivos de protección perimetral, impresoras, bases de datos…). Para ello, es preciso también dotar al sistema de una capacidad de almacenamiento adecuada en función del volumen de logs que se prevé manejar.

Control de privilegios

Los privilegios de administración sobre los equipos deben estar limitados a sus administradores y las cuentas de administración deben ser utilizadas exclusivamente para este cometido, por lo que los administradores deben emplear cuentas sin privilegios cuando accedan al sistema para tareas que no requieran un acceso privilegiado.

Los usuarios no deberían poder llevar a cabo por su cuenta modificaciones del hardware o del software, como pudiera ser el empleo o instalación de programas, equipos y dispositivos no autorizados, la modificación de configuraciones, el uso de dispositivos USB no inventariados, etc.

Así mismo, se debería limitar a lo indispensable las personas autorizadas a introducir y extraer información en el sistema y valorar la conveniencia de inhabilitar los puertos USB y lectores de CD/DVD de determinados equipos.

Seguridad física y del entorno

Se recomienda valorar la conveniencia de que el entorno físico de ciertos sistemas, incluyendo su cableado, puntos de acceso y zonas de cobertura wireless, dispongan de alguna medida de control de acceso físico. Por ejemplo: videovigilancia, acceso por clave o tarjeta o acceso por biometría (huella dactilar, reconocimiento facial, retina...).

Esto es especialmente importante en aquellas zonas o instalaciones a las que puedan acceder personas ajenas a la compañía. Así mismo, es conveniente contemplar procedimientos y medidas para la supervisión y acompañamiento de personal de otras empresas que haya de acceder a los sistemas o áreas restringidas.

Tampoco se debería permitir la conexión de elementos ajenos al sistema (portátiles, periféricos, dispositivos de almacenamiento extraíble, etc.), ni siquiera para tareas de mantenimiento o reparación, si no cuentan con autorización expresa de la persona responsable del sistema. En particular, las tareas de mantenimiento de sistemas críticos deberían ser realizadas usando preferentemente equipos bajo el control y la supervisión del responsable del sistema.

Análisis de riesgos

Se debe buscar siempre un equilibrio razonable entre seguridad y funcionalidad. El nivel de riesgo que se acepte asumir en una red o sistema corporativo debe establecerse sobre esta premisa.

En función de la naturaleza de la red o sistema en cuestión, puede resultar conveniente llevar a cabo un análisis de riesgos, entendido como el proceso sistemático e iterativo que permite estimar la magnitud de los riesgos a los que está expuesto, teniendo en cuenta las medidas de seguridad implantadas y midiendo su efectividad. De no ser aceptable el resultado, exigirá la aplicación de medidas adicionales, denominadas salvaguardas.

Para su realización existen muy diversas metodologías y herramientas, algunas de ellas específicamente asociadas a las certificaciones de seguridad de la información vistas anteriormente.

Protección perimetral

La protección perimetral debe aplicarse a todo elemento del sistema que tenga alguna conexión con el exterior, en especial cuando esa conexión se produce con algún elemento ajeno a la empresa, como puede ser alguna red pública o Internet.

En el caso de las estaciones de trabajo, por lo general contarán con la posibilidad de enviar o recibir correo electrónico y navegación web. Lo ideal es que todas ellas tengan un software antivirus instalado y actualizado y que cuenten con cortafuegos locales adecuadamente configurados.

En función de la entidad de la red corporativa o del sistema y de la criticidad de los activos, deberá considerarse la instalación adicional de elementos y dispositivos específicos de defensa perimetral, como cortafuegos, sistemas de prevención y detección de intrusiones (IDS/IPS), de prevención de pérdida de datos (DLP), para detectar y bloquear la conexión de dispositivos no autorizados (NAC), sistemas anti-spam, proxies web, recolección centralizada de logs, etc.

Control lógico de accesos

Así mismo, deben existir controles para el acceso a las redes y sistemas de la empresa (protocolos y servicios autorizados), al sistema operativo, a las aplicaciones y a la información (carpetas de red, etc.).

El acceso a los sistemas y aplicaciones debe estar basado en el principio de la "necesidad de conocer/acceder", de forma que solo tengan acceso al activo en cuestión aquellas personas que lo necesiten para realizar su trabajo o cometido.

Es muy recomendable establecer para ello controles de doble factor (por ejemplo, contraseña + token). En el caso de usar mecanismos de control de acceso basados en usuario y contraseña, se recomienda establecer una política que defina el tamaño, complejidad (combinación de caracteres alfanuméricos, especiales, etc.) y periodicidad de cambio (por ejemplo, cada varios meses).

En las actividades de concienciación debe incidirse en la importancia de utilizar contraseñas robustas, de protegerlas debidamente y de no compartirlas nunca. Así mismo, se debe evitar utilizar la misma contraseña para diferentes sistemas o aplicaciones.

Una medida cada vez más empleada para evitar los inconvenientes que todo esto genera son los gestores de contraseñas. También es muy importante que aquella información de la empresa que sea considerada crítica sea almacenada cifrada y esté disponible únicamente para los usuarios autorizados.

Gestión de incidentes

Si la naturaleza y tamaño de la compañía así lo aconseja, se debería disponer de un procedimiento de actuación ante incidentes de ciberseguridad.

En dicho procedimiento debería describirse qué se entiende por incidente de ciberseguridad y cómo y a quién habrán de notificarse y escalarse, en caso necesario.

También debería identificar a los responsables de tomar las medidas de respuesta necesarias y la secuencia y naturaleza de éstas, que deberían contemplar, como mínimo: 1) la valoración inicial; 2) la recuperación de los sistemas y la información; 3) la investigación del incidente; y 4) la implementación de acciones correctivas.

Planes de continuidad

Así mismo, es conveniente desarrollar planes que prevean el mantenimiento de los servicios ante un incidente de ciberseguridad, bien por los mismos medios o por otros alternativos, de manera que se reduzca el impacto en las operaciones de la empresa.

Para ello se deberán contemplar las causas potenciales de incidente, su naturaleza y probable alcance y determinar, en cada caso, qué sistemas resultarán esenciales para mantener las operaciones o servicios y qué medios alternativos podrían utilizarse para dar continuidad a las operaciones, así como las limitaciones a las que la empresa se verá sometida.

Estos planes deberían ser revisados con cierta frecuencia y actualizados según sea necesario. Además, conviene practicarlos con regularidad mediante simulacros que permitan evaluar los diferentes aspectos: comunicación, coordinación, disponibilidad de recursos, validez de los procedimientos y capacidad de respuesta.

Asistencia técnica especializada

En función de la naturaleza de la empresa, servicios y productos que ofrezca y entidad y criticidad de los sistemas corporativos, puede resultar conveniente disponer de medios para la asistencia técnica remota (o *in situ*, llegado el caso), que permitan auxiliar al personal de la empresa en aspectos técnicos que puedan exceder sus conocimientos y capacidades.

En las grandes corporaciones, es frecuente que este servicio sea suministrado por un departamento específico de la propia compañía, pero en el caso de las pymes lo habitual es que lo proporcione una empresa especializada contratada para tal fin.

A la hora de contratar estos servicios es importante analizar los tiempos de respuesta y horarios del servicio de asistencia que mejor se adapten a las condiciones de la empresa.

Concienciación (el cortafuegos humano)

Los usuarios participan en la mayor parte de los incidentes de seguridad. Así, por ejemplo, la vía de entrada de un *ransomware* a una pyme estará casi siempre asociada al elemento humano. Por lo tanto, el conseguir que los empleados estén concienciados del riesgo, tengan comportamientos responsables y se mantengan alerta frente a esta posibilidad es una de las formas más eficaces de prevención frente a las ciberamenazas.

Para ello, es muy conveniente desarrollar campañas periódicas de concienciación que permitan a todos los niveles de la organización conocer las formas de actuación de las ciberamenazas y desarrollar comportamientos y actitudes de "ciberhigiene". Así mismo, es conveniente distribuir boletines especiales o alertas ante amenazas en curso que puedan afectar a la empresa tan pronto como sean detectadas.

En el alcance de estas campañas y cursillos conviene tener en cuenta aspectos tales como la naturaleza de la amenaza y sus formas de actuación, con especial atención a las técnicas de ingeniería social, y sus implicaciones sobre el uso del correo electrónico, el empleo de credenciales de acceso y contraseñas, la utilización de dispositivos de almacenamiento extraíbles, la navegación web, el uso corporativo de dispositivos personales (BYOD) o el manejo de información sensible. Además, debido a la pérdida progresiva de estanqueidad entre los ámbitos laboral y personal, conviene incluir otros asuntos, como puede ser el uso responsable de las redes sociales.

Una técnica de probada eficacia es la de condicionar el acceso de los nuevos empleados a los recursos TIC corporativos a la previa superación de un examen que englobe todos estos aspectos.

Copias de seguridad

La opción de desencriptar los archivos cifrados como medida reactiva ante un ataque de ransomware debe ser descartada por resultar prácticamente imposible. Así mismo, el pago del eventual rescate no garantiza la recuperación de los archivos.

Por lo tanto, la forma más segura de minimizar el impacto de un ransomware exitoso es la realización de copias de seguridad o back-ups con la mayor frecuencia que se pueda.

En la medida de lo posible se debe intentar cumplir la regla del 3-2-1: disponer de tres (3) copias de seguridad, almacenadas en dos (2) medios distintos, de los cuales uno (1) debe ser un medio externo. Así mismo, se debe considerar la conveniencia del cifrado de la información sensible y de los back-ups almacenados.

Existe la posibilidad de automatizar las tareas de back-up. De no contarse con una solución automática, la empresa debería presupuestar el tiempo para crear de forma manual copias de seguridad completas teniendo en cuenta el nivel de tolerancia a la pérdida de datos que sea de aplicación. Los sistemas operativos más empleados (Microsoft, Apple) ofrecen funciones de copia de seguridad que pueden utilizarse como punto de partida.

Obviamente, las copias de seguridad deben permanecer cifradas y off-line y estar protegidas también contra otros tipos de incidentes, como pueden ser incendios o inundaciones. Además, hay que tener en cuenta que pueden corromperse o dañarse y que los medios de almacenamiento pueden quedar obsoletos, por lo que es conveniente diversificar las tecnologías empleadas.

Lo habitual en toda empresa es que la información crítica se reparta entre diferentes departamentos (contabilidad, diseño, ventas, recursos humanos, etc.). También es muy normal que estos departamentos no dispongan de medios estandarizados (por ejemplo, porque cuenten con dispositivos con diferentes sistemas operativos) o que estos no sean compatibles entre sí o que no estén interconectados.

En esos casos, las opciones pasan por disponer de una infraestructura IT capaz de trabajar con los diferentes tipos de dispositivos o que el back-up se realice en manual, que suele ser lo más frecuente.

Pólizas frente a ciberataques

En los últimos años, coincidiendo con la explosión de las ciberamenazas, un buen número de compañías de seguros ha incluído en su oferta de productos la cobertura frente a ciberataques.

Este tipo de pólizas cubre las pérdidas que provienen de los efectos de un ciberataque, como puede ser una interrupción de los servicios ofrecidos por la empresa o la filtración de datos de los clientes.

El contar con estos seguros nunca debería suponer un abandono de las medidas de ciberseguridad, sino considerarse únicamente como una herramienta cuya finalidad se limita a la mitigación de los daños económicos. Hay que entender que el seguro no elimina el riesgo ni cubre por lo general todas las consecuencias y costes derivados del incidente. En particular, es muy probable que no tenga efecto alguno sobre los daños reputacionales y en ningún caso permitirá recuperar la información dañada o comprometida.

En cualquier caso, si el empresario opta por esta medida, debe considerar cuidadosamente el perfil de riesgo específico y adaptarlo a sus circunstancias. Así, por ejemplo, si se trata de una empresa de reparto, debería atender especialmente a todo lo que pueda suponer retraso o impedimentos en la entrega de la mercancía y no atender a otros aspectos sin impacto potencial.

42

Han atacado a mi empresa, ¿qué debo hacer?

Asunto de la alta dirección

Lo primero que se debe entender es que, a pesar de sus connotaciones técnicas, que serán incomprensibles para la gran mayoría, un ciberataque tiene que involucrar por completo a la alta dirección, porque habrá decisiones que tengan que ser tomadas al más alto nivel. Todos deben ser conscientes de que puede estar en juego la supervivencia de la empresa y que decisiones tomadas en el nivel técnico pueden tener consecuencias muy graves de naturaleza empresarial.

Al mismo tiempo, son muchas las facetas que han de ser tenidas en cuenta y que pueden presentar fricciones entre sí. Principalmente, la restauración de los servicios, la comunicación del incidente y sus aspectos legales.

Continuidad de las operaciones

Ante un ciberataque, puede ser necesario apagar dispositivos y echar abajo sistemas empresariales; por ejemplo, para impedir la propagación del malware a través de redes corporativas.

En estos primeros momentos, lo conveniente es que las empresas sigan los consejos del CISO, del Director del Departamento TI de la empresa o de los proveedores de los servicios de ciberseguridad de la compañía, según sea el caso. En cierta medida, tiene paralelismo con lo que ocurre en un accidente en el mundo físico: las primeras acciones están siempre encaminadas a auxiliar y estabilizar a los heridos, resultando en esos momentos muy secundario la preservación de la escena o identificar al culpable.

Atajada la propagación, el siguiente paso recomendable, aunque no siempre posible, es el de identificar el origen del ataque (vector de entrada, paciente cero, vulnerabilidad explotada…) para evitar que pueda reproducirse.

Conseguido lo anterior, la forma más simple y rápida de restaurar la situación a un estadio similar al existente antes del ataque y reanudar las operaciones suele ser la de cargar la información contenida en las copias de seguridad. Obviamente, a menor tiempo transcurrido desde la realización de la copia, menor impacto.

No obstante, los pasos exactos para restaurar las operaciones dependerán en cada caso de la naturaleza del incidente, de la empresa y de la información involucrada, por lo que no pueden darse unas directrices de aplicación universal.

Estrategia de Comunicación

Sufrido un ataque con impacto relevante, una acertada estrategia de comunicación puede resultar fundamental para mantener la confianza de clientes e inversores, proteger la reputación de la compañía y hasta minimizar las posibles responsabilidades legales.

Para ello, existen guías, entre las que destaca la elaborada por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon [4].

Puede resultar muy conveniente tener trabajada y diseñada la estrategia a seguir, con el apoyo de expertos y sobre las casuísticas más probables, a modo de árbol de decisión. También contribuirá a una mejor gestión el llevar periódicamente a cabo ejercicios en los que se plantee su aplicación y que involucren a la alta dirección, a fin de evitar errores que pueden nacer de la improvisación, la urgencia y la inexperiencia, llegado el momento.

Unos de los aspectos más críticos es la comunicación con clientes e inversores. La experiencia demuestra que la divulgación pronta y sincera de lo ocurrido, el asesoramiento de expertos y la coordinación con los organismos que correspondan desde el momento en que se tenga conocimiento del ataque (por ejemplo, con el INCIBE-CERT), pueden contribuir muy positivamente a la protección de los intereses de los diversos afectados y a reducir el impacto.

Por otra parte, habrá ocasiones en las que las notificaciones no sólo sean obligatorias, sino que, además, deban ajustarse a ciertos requisitos legales o reglamentarios (por ejemplo, cuando afecten a la Ley de Protección de Datos o a la prestación de servicios esenciales), por lo que éste ha de ser unos de los primeros aspectos que debe contemplar el referido árbol de decisión. Los formatos, plazos y procedimientos que deban de cumplir estas notificaciones deben estar previamente identificados.

Por lo general, los siguientes aspectos deberán ser tenidos en cuenta en los comunicados a clientes e inversores:

- Explicación clara, sencilla y veraz de lo ocurrido.
- Activos e información dañada o comprometida.

4 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816

- Posibles impactos sobre clientes y proveedores y asesoramiento al respecto.
- Leyes o reglamentos que sean de aplicación.
- Agencias y organismos que pueden estar implicados.
- Acciones adoptadas y que se prevén adoptar.
- Punto de contacto para consultas o aclaraciones.
- Medios por los que se mantendrá actualizada la información

Mención aparte requieren las comunicaciones en redes sociales, cuyos efectos, aunque por lo general muy volátiles, son siempre muy difíciles de predecir y controlar. Por tal motivo, lo normal es que los comunicados para las redes deban diferir de los dirigidos a clientes e inversores. En cualquier caso, se deberá procurar que los directamente afectados sean los primeros en recibir la información. Por otra parte, esto no siempre será posible, pues habrá casos en los que las redes sociales se hagan eco de lo sucedido antes de que los clientes e inversores puedan ser informados. Puede ser lo más probable en el caso de un defacement o un ataque de denegación de servicio, e, incluso, de un ransomware si los empleados lo divulgan irresponsablemente a través de sus cuentas particulares (motivo por el cual conviene incluir esta casuística en las actividades de concienciación).

Preservación de evidencias versus restauración de sistemas

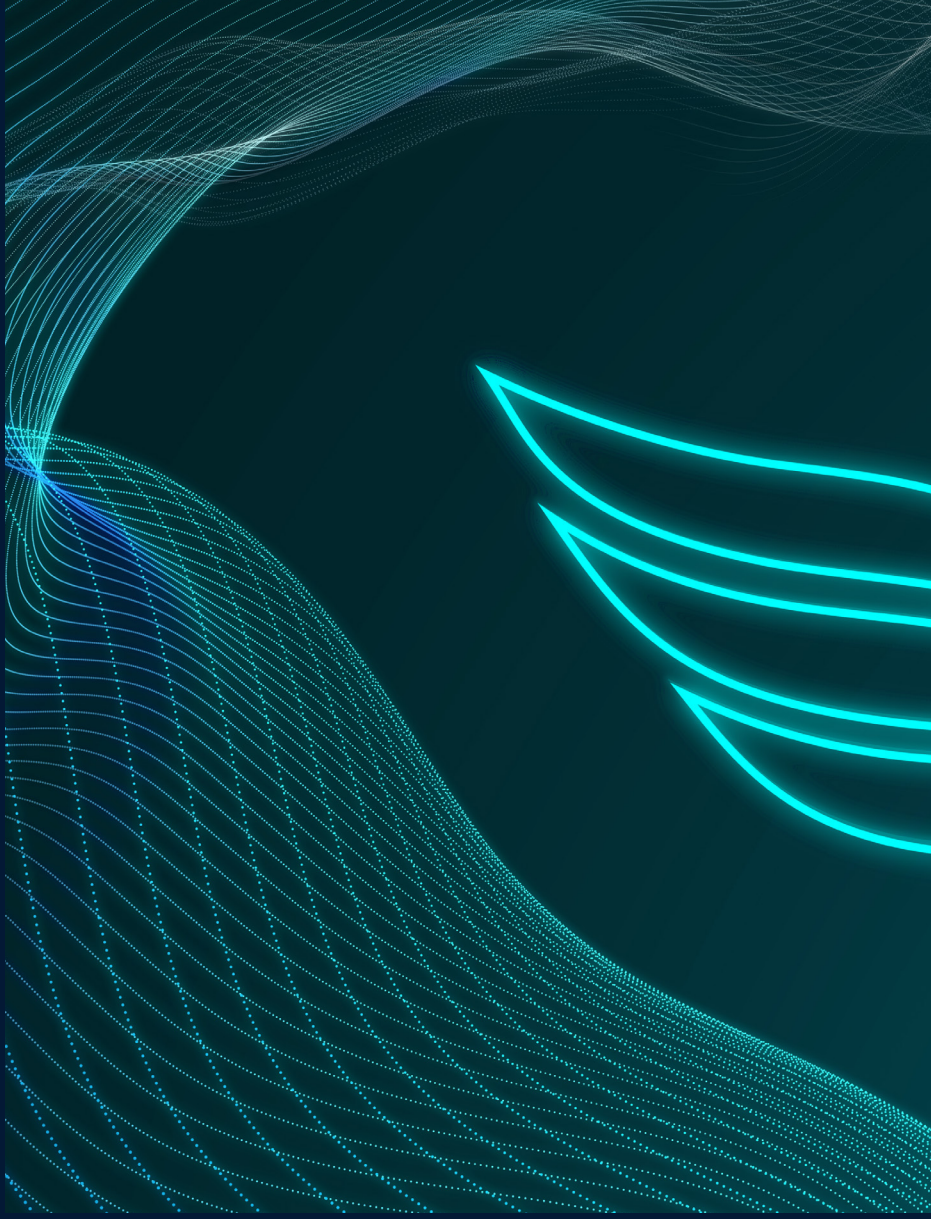
Todo incidente tiene diferentes aspectos que deben ser tenidos en cuenta y que habrá que valorar llegado el momento, pues es posible que den lugar a conflictos de intereses.

Así, por ejemplo, es posible que determinadas acciones encaminadas a la restauración de los sistemas afectados puedan poner en riesgo la localización o preservación de evidencias fundamentales para identificar la autoría del ataque. De ser una decisión interna de la compañía, debería ser tomada al máximo nivel, con el correspondiente asesoramiento directivo de las partes afectadas. En caso de que el incidente haya sido denunciado, será algo que deba plantearse de inmediato a los equipos de los Cuerpos y Fuerzas de Seguridad del Estado sobre los que recaiga la responsabilidad de la investigación.

Lecciones aprendidas

Una vez reestablecida la normalidad en los servicios y sistemas afectados, resultará muy conveniente analizar todo lo acontecido, a fin de evaluar la eficacia y oportunidad de la respuesta y gestión del incidente en todas sus facetas. Ello implica considerar los aspectos técnicos (vulnerabilidad explotada, detección, mecanismos de contención aplicados y su eficacia, resiliencia, plan de restauración, recursos empleados frente a recursos que hubieran sido necesarios…), los del proceso de toma de decisiones (primeras comunicaciones, tiempos, cadena de mando, ciclo de decisión, coordinación, claridad y delimitación de las responsabilidades, validez y calidad de los asesoramientos, relación con las agencias y organismos…), comunicación (oportunidad y efectividad de los comunicados, punto de contacto, responsabilidades…), económicos (costes de las medidas adoptadas, costes derivados de la pérdida de operatividad, penalizaciones, seguros, etc.) o legales (prontitud, precisión y alcance del cumplimiento normativo, infracciones, etc.).

Los objetivos de este proceso son, por una parte, evitar que un incidente similar pueda volver a producirse, y, por otra, mejorar la respuesta en todas sus facetas, lo cual puede tener que ver tanto con incorporar equipamiento adicional, como con contratar personal especializado, revisar los procedimientos de control de acceso o mejorar la concienciación de los empleados, entre otras muchas medidas.



¿QUÉ PUEDE HACER GHENOVA POR MI EMPRESA?

Desde su creación, GHENOVA CIBERSEGURIDAD identificó a las pymes como el conjunto al que se debían orientar prioritariamente sus servicios, al confluir en ellas la falta de madurez en ciberseguridad, el interés prioritario de las amenazas, las imposiciones de la nueva normativa y las crecientes exigencias en materia de ciberseguridad que demandan los clientes. Por todo ello, este nuevo departamento ha tenido desde su concepción una especial vocación hacia el desarrollo de servicios a medida de las pymes, asegurando el acompañamiento en todos los pasos de la ciberseguridad.

Nuestros servicios abarcan el asesoramiento en la elección de las soluciones y tecnologías más adecuadas al tamaño y naturaleza de la empresa, el soporte en el desarrollo de políticas, planes y procedimientos de seguridad de la información, el asesoramiento y apoyo para la obtención de certificaciones de empresa (ISO/IEC 27001, ENS…), la realización de análisis de vulnerabilidades, pruebas de penetración controladas y auditorías, la implantación de las medidas de mitigación más adecuadas, abarcando los diferentes activos de la compañía (redes IT/OT, páginas web, nube, cuentas en redes sociales, etc.), el desarrollo de campañas y medidas de concienciación frente a las ciberamenazas o la formación básica en materia de ciberseguridad.

Nuestros profesionales entienden perfectamente las preocupaciones y dudas de los empresarios acerca de todo lo relacionado con la ciberseguridad y buscarán, sobre la base de una atención personalizada, cercana y de confianza, la respuesta más adecuada, rápida y eficiente a las necesidades que su empresa puede tener en esta materia.

La ciberseguridad en una pyme es tanto o más importante que la seguridad física y que ha de contemplarse como una rentable inversión que proporciona fortaleza y ventajas competitivas y que constituye un factor esencial para la supervivencia.

PORTFOLIO DE SERVICIOS DE CIBERSEGURIDAD

Consultoría y análisis

Ayudamos a las empresas a definir su alcance y huella en el ciberespacio.

Diseñamos las mejores estrategias de Ciberseguridad según su casuística, validando o proponiendo mejoras en su Arquitectura de Sistemas y Redes, evaluando sus despliegues e incluso los conocimientos del personal de la empresa, siempre bajo los principios de “Zero trust” y “Security by design”.

Gestionamos la selección e implantación de elementos que eleven su capacidad de defensa y respuesta.

Ofrecemos servicios de optimización y soporte evolutivo, y en caso de necesidad, generamos la documentación necesaria para los Planes Corporativos en materia de ciberseguridad.

En concreto, las soluciones que proporcionamos en relación a consultoría y análisis son:

1. Análisis y gestión de riesgos

- Análisis de Arquitecturas de Seguridad
- Análisis de riesgos y vulnerabilidades
- Modelización de amenazas
- Diseño de estrategias de ciberseguridad

2. Proyectos de implantación

- Diseño y soporte a la implantación de Arquitecturas de Seguridad
- Soporte a la selección e implantación de elementos de Seguridad
- Optimización de configuraciones de seguridad (soporte evolutivo)

3. Planes, procesos y procedimientos

- Procedimiento de Gestión de ciberincidentes
- Planes de Continuidad de Negocio
- Procesos de actualización, parcheado y bastionado

Auditorías y pruebas activas

Con nuestra gama de servicios de auditoría y pruebas buscamos los siguientes objetivos:

- Reducir riesgos.
- Detectar y eliminar vulnerabilidades.
- Actualizar las medidas y procedimientos de ciberseguridad.
- Garantizar la seguridad de la información y el cumplimiento de las normativas de aplicación.
- Aumentar la confianza de empleados y clientes.
- Demostrar ante autoridades y en procesos de licitación una adecuada Gestión en materia de Ciberseguridad

1. Auditorías externas

- Preparación y soporte (ISO 27001, ENS, ….)
- Adecuación a Normativas

2. Ciberseguridad preventiva

- Hacking Ético y pruebas de penetración (Pentesting)
- Auditoría web
- Auditoría de redes
- Simulación de Ataques
- Seguimiento de vulnerabilidades y estrategias de remediación

Concienciación y formación

La concienciación y la formación son componentes fundamentales del marco de ciberseguridad en la Empresa, y se convierten en la mejor arma para la primera línea de defensa, los propios empleados formados y sabiendo como actuar ante posibles amenazas.

1. Servicios de formación

Conferencias, charlas, seminarios , píldoras formativas, Ciber ejercicios, Presencial y remoto.

2. Servicios de concienciación

Diseño de estrategias de Concienciación y cultura de ciberseguridad en la Empresa.

GLOSARIO DE TÉRMINOS

Análisis de vulnerabilidades: Proceso de búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (arquitecturas, configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación para subsanar las deficiencias encontradas y evitar ataques a los sistemas o reducir su impacto.

Antivirus: Programa diseñado para detectar o identificar código malicioso, a fin de prevenir o contener incidentes.

APT: Acrónimo de *Advanced Persistent Threat*, amenaza persistente avanzada. Término que se aplica a un tipo de ciberamenaza caracterizada por contar con importantes recursos (financieros, técnicos, humanos y de infraestructura) que la capacitan para llevar a cabo ataques y campañas sigilosas y prolongadas, especialmente diseñadas a medida del objetivo y generalmente con fines de espionaje o sabotaje.

Ataque de diccionario: Procedimiento para ruptura de contraseña que consiste en probar grandes volúmenes de contraseñas obtenidas de bases de datos construidas a partir de robos masivos de credenciales, combinaciones de palabras y diversas variantes.

Ataque de fuerza bruta: Procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la correcta. Este proceso puede tardar mucho tiempo (años, siglos) en completarse si la contraseña es lo sucicientemente larga y compleja, por lo que suele combinarse con un ataque de diccionario.

Auditoría de seguridad: Es el proceso de evaluación, llevado a cabo por profesionales en tecnologías de la información (TI), de la madurez de un sistema, empresa u organización, con el objetivo de identificar, enumerar y describir las vulnerabilidades que pudieran ser explotadas, evaluar el riesgo real e identificar soluciones para su mitigación .

Backup: Copia de seguridad de ficheros o aplicaciones con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños por cualquier casusa. Los dispositivos más empleados para ello son discos duros, discos ópticos, USB o DVD, aunque también es común su realización mediante servicios basados en la nube.

Baiting: Técnica de ataque que consiste en abandonar un USB infectado en algún lugar en que pueda ser localizado por una persona con acceso a la red o sistema objetivo. Se basa en que la curiosidad de muchas personas las lleva a conectar el dispositivo encontrado en su ordenador personal o en el de su puesto de trabajo.

Botnet: Conjunto de dispositivos (denominados *bots*) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas, como envío de spam, ataques de DDoS, etc. Las botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés Command & Control) al que se conectan los bots para enviar información y recibir comandos. Existen también las llamadas botnets P2P que se caracterizan por carecer de un servidor C&C único.

BYOD: Acrónimo de *Bring Your Own Device* (trae tu propio dispositivo). Modalidad política empresarial muy extendida que consiste en que los empleados utilicen con fines laborales sus propios dispositivos personales (portátiles, tabletas, móviles…) y cuenten con acceso a recursos de la empresa, tales como correos electrónicos, bases de datos y archivos en servidores. También se le conoce como *Bring Your Own Technology*, BYOT, (trae tu propia tecnología) para abarcar no solamente a los dispositivos sino también al software. Si bien tiene grandes ventajas en términos de conectividad y productividad, desde el punto de vista de la ciberseguridad supone un importante incremento del riesgo para las empresas que debe ser debidamente gestionado.

CERT: Acrónimo de *Computer Emergency Response Team*; equipo de expertos responsables de la respuesta ante incidencias de seguridad que se producen en redes y sistemas TIC. Por lo general, un CERT lleva a cabo otras muchas actividades, tanto preventivas como proactivas y reactivas, abarcando aspectos de concienciación, asesoramiento, auditoría, asistencia técnica, inteligencia, formación, monitorización o gestión de incidentes, entre otros.

Ciberataque: Ataque en o a través del ciberespacio con la finalidad de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno informático o infraestructura, destruir la integridad de los datos o acceder a información controlada.

Ciberejercicio: Actividad orientada al adiestramiento y la evaluación del estado de preparación de un individuo, equipo, empresa, sector o país, frente a la acción de las ciberamenazas con el fin de mejorar la respuesta, cooperación y coordinación.

Ciberseguridad: Actividad, proceso, capacidad o estado mediante el cual los sistemas TIC y la información contenida en ellos están protegidos contra daños, uso o modificación no autorizada.

CISO: Acrónimo de Chief Information Security Officer (oficial principal de seguridad de la información). Es el responsable máximo en lo relativo a planificación, desarrollo, control y gestión de las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información de la organización dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad, actuando de nexo entre el nivel técnico y la alta dirección.

Cloud computing: Disponibilidad a demanda de los recursos del sistema informático, especialmente el almacenamiento de datos y la capacidad de cómputo, sin una gestión activa directa por parte del usuario. En lugar de depender de un servicio físico instalado, se tiene acceso a una estructura donde el software y el hardware están virtualmente integrados. Establece su arquitectura a partir de una fragmentación entre aplicación informática, plataforma y hardware, posibilitando tres modalidades de entrega.

Contraseña: Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.

Criptomoneda: Moneda digital en la que las transacciones se verifican y los registros se mantienen por un sistema descentralizado que utiliza criptografía en lugar de una autoridad centralizada. Las más populares son Bitcoin,Ethereum, Cardano, Solana, Litecoin y Monero.

CSIRT: Acrónimo de Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas, que se suele usar en Europa como sinónimo y en lugar del término protegido CERT, que está registrado en EE.UU. por CERT Coordination Center (CERT/CC).

Defacement: Tipo de ataque contra un sitio web mediante el cual se modifica su apariencia visual. Se trata de un ataque típico del hacktivismo propiciado generalmente por algún error de programación de la página web, algún bug en el propio servidor o una mala administración por parte de los gestores de la web.

Denegación de servicio distribuida (DDoS, por sus siglas en inglés): Forma de ciberataque en la que el atacante hace que el activo víctima (dispositivo, sitio web, red) no esté disponible para sus usuarios mediante la saturación de los recursos.

Dirección de Protocolo de Internet (IP, por sus siglas en inglés): Etiqueta numérica que identifica de manera lógica y jerárquica a todo dispositivo conectado a la red que utilice el protocolo de Internet.

Doble factor de autenticación (2FA): Esquema en el que a una autenticación simple se le añade otro factor, como puede ser un código enviado a un móvil o una huella dactilar, por lo que resulta más seguro.

Exploit: Secuencia de comandos utilizados para, aprovechando un fallo o vulnerabilidad, provocar un comportamiento no deseado o imprevisto con el fin de acceder al sistema de forma ilegítima, obtener permisos de administración y ejecutar algún tipo de acción maliciosa sobre él.

Fintech: Tecnologías digitales utilizadas para brindar servicios financieros y de pago.

Hacktivista: Persona que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología, con el fin último de lograr sus propósitos políticos. Para ello suelen emplear los *defacements*, redirecciones, ataques de denegación de servicio (DoS), robo y exposición de información privilegiada o parodias de sitios web.

Hacking ético: Actividad que consiste en tratar de violar la seguridad de un sistema informático, con autorización previa de su propietario, para encontrar agujeros de seguridad, deficiencias o errores y que estos puedan ser corregidos antes de que sean explotados con fines maliciosos. Su alcance va más allá que el del *pentesting*, puesto que no solo contempla las defensas del sistema, sino que también pone a prueba al "equipo defensor", por lo que puede incluir, por ejemplo, el uso de técnicas de ingeniería social aplicadas a los usuarios o administradores del sistema.

Información de identificación personal (PII, por sus siglas en inglés): Información del cliente que está vinculada o puede vincularse a la identidad de una persona y que tiene especial tratamiento legal y normativo.

Información personal confidencial (SPI, por sus siglas en inglés): PII cuyo compromiso tiene un mayor riesgo de causar daños financieros, de reputación o personales.

Ingeniería social: Conjunto de técnicas de engaño enfocadas a que los usuarios de sistemas/servicios TIC faciliten datos de interés para los atacantes (credenciales de acceso, información sobre los sistemas o servicios instalados, etc.).

Insider: Atacante que pertenece a la propia organización y que, por lo tanto, tiene un acceso privilegiado a los sistemas objetivo y a la información que manejan o almacenan.

Internet de las cosas (IoT): Objetos cotidianos (como sistemas de seguridad, luces, refrigeradores, sensores, equipos industriales, etc.) con capacidad de conectarse a Internet, y enviar y recibir datos.

Inyección SQL: Tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

Keylogger: Tipo de *malware* espía que se encarga de capturar y enviar al exterior las pulsaciones del teclado. Existe también en modalidad hardware.

LOPDGDD: Acrónimo de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, ley española en la que se transpone el reglamento europeo de Protección de datos o RGPD, mediante la cual se regula el tratamiento de los datos de carácter personal, garantizando a los usuarios un mayor control sobre el uso que se hace de los datos por parte de empresas u organismos oficiales, entre otros.

Malware: Software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio conjunto de programas maliciosos: virus, gusanos, troyanos, *backdoors, spyware*, etc.

***Man-in-the-Middle* (MitM):** Ciberataque que interrumpe o modifica de manera ilegal los datos a medida que se transmiten entre dos partes legítimas, con frecuencia por Wi-Fi no seguro u otra infraestructura de red.

MDM: Acrónimo en inglés de Mobile Device Management; en español, gestión de dispositivos móviles. Implementación que permite administrar de forma remota, combinada y escalable, teniendo en cuenta las políticas e infraestructura de la organización, las aplicaciones y configuraciones de los dispositivos móviles corporativos, con el propósito de aumentar su compatibilidad, seguridad y funcionalidad, simplificando las labores de gestión de los administradores.

NAC: Acrónimo en inglés de Net Acces Control (NAC); en español, control de acceso a la red. Tecnología que permite controlar de forma muy granularizada los dispositivos que se conectan a una red, permitiendo establecer políticas de gestión de los dispositivos y detectar en tiempo real los intentos de conexión no autorizados.

Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente, son desarrollados por el fabricante tras la detección de una vulnerabilidad y pueden instalarse de forma automática o manual por parte del usuario.

Phishing: Técnica de engaño, por lo general ejecutada mediante correo electrónico o mensaje instantáneo en combinación con técnicas de suplantación de identidad o spoofing, que persigue que la víctima lleve a cabo alguna acción (clicar un enlace, leer un código QR) que posibilite o desencadene el ataque.

Plan de continuidad: Conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencia destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

Prueba de penetración o *pentest*: Ataque controlado y autorizado a un sistema con el objetivo de encontrar vulnerabilidades. Implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad. Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad. Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica.

Ransomware: Tipo de malware que impide o limita el acceso de los usuarios a su sistema, ya sea bloqueando la pantalla del sistema o los archivos de los usuarios, hasta que se pague un rescate, generalmente en criptomoneda para dificultar su rastreo.

Red privada virtual (VPN, por sus siglas en inglés): Método que emplea encriptación para brindar acceso seguro a un dispositivo remoto a través de Internet.

RGPD: Acrónimo de Reglamento General de Protección de Datos, regulación de la Unión Europea introducida en 2016 orientada a la protección de los datos personales de las personas físicas por parte de organizaciones e instituciones que operan en la Unión Europea, así como del procesamiento, almacenamiento o destrucción que éstas realizan de dicha información personal y las consecuencias y sanciones en caso de que se produzca su filtración o pérdida.

Rootkit: Tipo de malware que permite un acceso continuo y con privilegios de administrador al dispositivo víctima, manteniendo su presencia oculta al control de los administradores legítimos.

Suplantación de identidad (o *spoofing*): Adopción de una falsa identidad para la remisión de mensajes fraudulentos con apariencia real y legítima con el fin de engañar a los destinatarios de forma que faciliten algún tipo de información o ejecuten alguna acción de interés para el atacante.

Tampering: Inserción intencionada de vulnerabilidades o código malicioso embebido en el hardware o software. Puede producirse en cualquiera de las etapas entre la fabricación y la instalación del elemento manipulado en el sistema objetivo; es decir, durante el diseño, desarrollo, fabricación, ensamblado, almacenamiento, transporte o instalación.

Vulnerabilidad: También conocida como "agujero de seguridad". Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente, por medio de un exploit). Cuando se descubre, el desarrollador del software o hardware afectado tratará de ponerle solución desarrollando y diseminando una actualización de seguridad del producto, conocida como parche.

***Watering hole* (abrevadero):** Técnica en la que el atacante infecta una página web legítima, que conoce que es accedida con frecuencia por personas pertenecientes al objetivo al que se dirige la acción (empresa, organización), con el fin de que queden infectados al visitarla. Su nombre procede de la técnica de caza del león, que permanece agazapado frente a la charca a la que, antes o después, la gacela tendrá que acercarse para beber.

Zero-day: Vulnerabilidad en un sistema o programa informático que es únicamente conocida por determinados atacantes y resulta desconocida para los fabricantes y usuarios, por lo que no existe un parche de seguridad para solucionarla.

XSS: Vulnerabilidad en algunas páginas web en las que se produce interacción con el usuario y cuyo nombre procede del acrónimo en inglés de (Cross-site Scripting). Dado que los sitios web dinámicos dependen de la interacción del usuario, si no está bien programado, el atacante puede encontrar la forma de insertar en algún formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Una vez realizado el ataque XSS, el atacante puede ejecutar muy diversas acciones (cambiar la configuración del servidor, secuestrar cuentas, interceptar comunicaciones…) de forma inadvertida para el administrador.

GHENOVA