OFICINA Acelera pyme

Cidaut

CIBERAMENAZAS Y SEGURIDAD EMPRESARIAL

Financiado por la Unión Europea

red.es

Fondos Europeos

Fondo Europeo de Desarrollo Regional

"Europa se siente"

Las Oficinas Acelera pyme puestas en marcha en toda España por Red.es, entidad pública adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, cuentan en su segunda convocatoria 2022 con un presupuesto de 18.450.000 €, de los cuales Red.es aportará hasta el 80% del presupuesto subvencionable y las entidades beneficiarias el resto. Las actuaciones están financiadas con cargo al Programa Operativo Crecimiento Inteligente, Fondos Europeos de Desarrollo Regional (FEDER) del periodo de programación 2021-2027.

Tabla de contenido

1. MOTIVACIÓN

La transformación de la industria y de la sociedad en general, genera numerosas ventajas, pero también provoca una mayor exposición a determinados riesgos que se derivan de dichas facilidades de comunicación, lo cual supone un importante reto para la ciberseguridad, a la que deben dar respuesta tanto las grandes empresas como las PYMEs.

Es por ello que la importancia de la ciberseguridad en las empresas es un tema que en los últimos años está cogiendo cada vez más protagonismo. Tanto es así, que en la actualidad es un elemento diferenciador. La ciberseguridad en la industria 4.0, poco a poco, se está volviendo más importante y resulta indispensable para poder desarrollar la actividad económica de manera segura.

Así, actualmente las pymes industriales deben afrontar, como factor de competitividad y de supervivencia, la transformación digital de sus procesos de negocio.

Dicha transformación, requiere cada vez más el uso intensivo de tecnología, y de una mayor conectividad de los sistemas internamente y con el exterior, lo que redunda en un incremento del riesgo tecnológico, ya que las posibilidades de exposición de información son cada vez mayores.

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LA PYME

Cada vez es más necesaria y existe una mayor conectividad entre el mundo de Tecnologías de la Información (IT) tradicional y el mundo de Tecnologías Operacionales (OT) o de producción, que convergen en sistemas ciberfísicos con aplicaciones dispositivos y conectividad con el también llamado Internet de las cosas *IoT*.

Es fundamental que la dirección de las pymes asuma el riesgo tecnológico como un riesgo relevante para el negocio, y que hay que tratar de minimizar, al igual que otros riesgos, como el financiero, económico u operacional entre otros, ya que el ciberriesgo es transversal al negocio y afecta directamente.

Además, los ataques pueden provocar:

- Una parada total de los sistemas de la empresa, suponiendo un impacto económico incalculable.
- Cese total de la compañía si durante el ciberataque se ha perdido toda la información.

Además, estos ciberataques, cada vez más frecuentes y dirigidos a cualquier tipo de organización, están aumentando la concienciación de las organizaciones y la

ciberseguridad gana importancia en ellas. Por lo tanto, cada vez es más normal ver aumentada la inversión de las partidas relacionadas con la ciberseguridad para pymes. Pero los presupuestos de las organizaciones son finitos, por lo que es de suma importancia llevar a cabo inversiones en aspectos estratégicos de ciberseguridad IT y ciberseguridad OT, para combatir estos ciberataques.

IMPORTANCIA DE LA CIBERSEGURIDAD: ¿POR QUÉ PROTEGER TU EMPRESA?

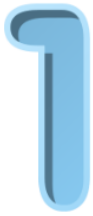
Las razones para proteger tu empresa de ciberamenazas, se pueden resumir en:

- Evitar enormes pérdidas económicas.
- Reservar la confidencialidad, integridad y disponibilidad de la información clave de tu negocio.
- Anticiparse a posibles amenazas y vulnerabilidades antes de que sucedan.

- Evitar interrumpir la producción, secuestro de datos, etc.
- Hacer frente a las amenazas de forma inmediata

2. ¿CÓMO ATACAN LOS CIBERDELINCUENTES?

Existen diferentes formas de ciberdelincuencia a las que las PYMEs, autónomos y emprendedores deben hacer frente, pero todas ellas tienen 2 aspectos en común:



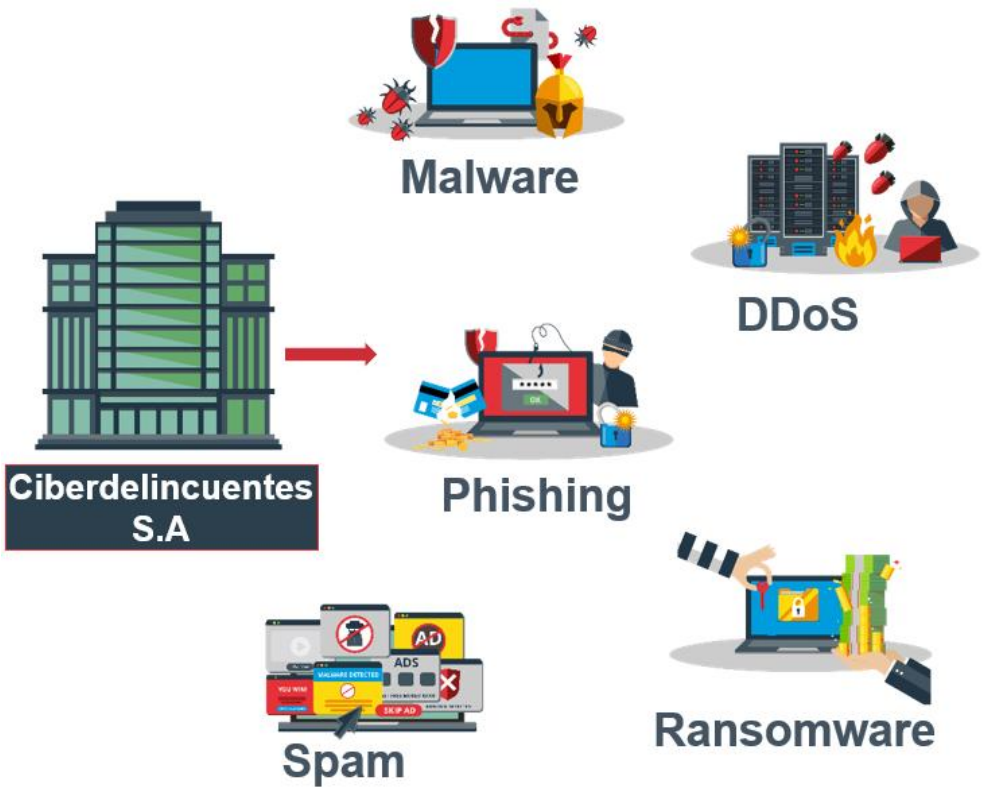
Es complicado identificar su origen

Dado que puede cometerse desde cualquier lugar del planeta y sin necesidad de estar asociada a ninguna identidad en específico, su origen suele ser incierto. Esto se dificulta más cuando la entidad atacada no cuenta con los conocimientos o recursos necesarios para hacer una investigación profunda.

Puede no ser obvio

Como muchos ciberdelitos se llevan a cabo de forma que parezcan ataques aislados, muchas veces los administradores afectados tardan en darse cuenta. Es más frecuente esta situación cuando no se cuenta con una plataforma de seguridad o de asistencia técnica que detecte las actividades inusuales de manera rápida.

A continuación, se describen las diferentes formas de ciberdelincuencia empleadas en las empresas en la actualidad, tales como Malware, Phishing, Spam, DDoS y Ramsonware (fuente: INCIBE):



Ejemplo de diferentes ciberataques sufridos por las empresas en la actualidad

En las siguientes páginas se describen las principales características de estos tipos de ciberataques:

MALWARE

Se trata de programas maliciosos diseñados para infectar dispositivos sin el conocimiento o consentimiento del usuario y realizar diferentes acciones en beneficio del atacante como, por ejemplo:

- Robar datos como credenciales e información de pago y datos personales.
- Mostrar publicidad no deseada o fraudulenta.
- Participar en una red zombi de dispositivos o *botnet*, controlada por el atacante, para realizar acciones maliciosas de forma coordinada.
- Lanzar ataques para dañar a otra empresa o entidad, como en los DDOS (ataques distribuidos de denegación de servicio).
- Descargar e instalar más *malware* en el dispositivo, y distribuirlo entre otros dispositivos.
- Minar criptomonedas, generando dinero para el atacante.
- Secuestrar el dispositivo al cifrar sus datos y dejarlo inutilizable, en el caso de un *ransomware*, exigiendo un rescate a cambio de la falsa promesa de liberarlo.

Existen diferentes tipos de malware, como por ejemplo el adware (mostrando publicidad no deseada o engañosa), spyware (que recopila información personal, bancaria y de navegación), gusanos (que buscan replicarse y difundirse), troyanos (programas maliciosos con aspecto legítimo), ransomware (que secuestran el dispositivo, solicitando el pago de un rescate), botnets o redes zombi (que infectan y controlan muchos dispositivos para que lancen ataques coordinados), entre otros.

Los medios que se utilizan para este tipo de ataques son los siguientes:

- **Mensajes.** Mediante herramientas de chat, ya sean específicas o dentro de otra aplicación como una red social o, incluso, un software de CRM gratuito, mensajes de texto (SMS) o correos electrónicos, se pueden facilitar archivos o enlaces con malware para infectar un dispositivo. Además, también el propio malware puede emplear estos medios para difundirse entre los contactos.
- **Descargas de aplicaciones y archivos** normalmente desde páginas no oficiales, como por ejemplo páginas de descargas o *streaming* ilegal de archivos que se

ofrecen de forma gratuita, redes para compartir archivos entre usuarios, o aplicaciones fuera de las tiendas oficiales como Google Play, App Store, Microsoft Store, Steam, etc.

- **Memorias USB y otros dispositivos externos**. Los dispositivos de almacenamiento, como una memoria USB o *pendrive*, una tarjeta de memoria, un disco duro externo, pueden contener algún archivo infectado con un *malware*, especialmente cuando se utilizan en diferentes equipos compartidos.
- **Páginas fraudulentas y publicidad engañosa**. Una página web controlada por un ciberdelincuente podría infectar un dispositivo, lanzando una descarga de un archivo, pidiendo instalar un *plugin* o complemento, por ejemplo, con la excusa de reproducir un contenido multimedia, o simplemente aprovechando vulnerabilidades o fallos de seguridad en un navegador que no está actualizado. El malware también puede redirigir la navegación del dispositivo hacia páginas de phishing ideadas para el robo de datos, simulando ser una entidad oficial y de confianza como por ejemplo un videojuego o red social. El riesgo no se limita a los archivos ejecutables o los instaladores de aplicaciones. En ocasiones se camufla el nombre o extensión del archivo malicioso. Incluso, hay archivos aparentemente inofensivos, como los documentos de ofimática (de procesador de texto como Word, de hoja de cálculo como Excel, etc.), que también pueden contener malware.

Ejemplo de malware para acceder a dirección maliciosa (fuente: INCIBE):

Una vez se ha pulsado sobre alguno de los enlaces, se produce la descarga de un archivo .zip como el del ejemplo que se muestra a continuación. Dicho archivo contiene el *malware*, diseñado para infectar nuestro equipo.

PHISHING

El phishing es una técnica que consiste en el envío de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de entidades, redes sociales, entidades públicas, empresas reconocidas o servicios que utilizamos habitualmente, y su objetivo es obtener toda la información personal y bancaria que puedan conseguir de nosotros, como usuarios y contraseñas, direcciones, datos de tarjetas de crédito, etc., realizar un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas.

Los correos de phishing pueden suplantar a cualquier tipo de empresa o servicio. A continuación, mostramos algunos casos más frecuentes.

- **Phishing bancario**: suplantan a una entidad financiera legítima para obtener información bajo excusas como: bloqueo de cuenta, actividad sospechosa en la cuenta, cargos en cuenta, etc.
- **Phishing a entidades públicas**: suplantan a través del correo electrónico a entidades y organismos públicos bajo cualquier pretexto, como devolución de impuestos, pago multa de tráfico, obtención de ayudas, etc.
- **Phishing a entidades privadas**: captan la atención de los usuarios con asuntos y mensajes que apelan en muchas ocasiones a los sentimientos. Entre las empresas candidatas a ser suplantadas, encontramos las siguientes:
    - Compañías eléctricas
    - Tiendas y supermercados
    - Mensajería y transporte
    - Operadoras de telefonía
    - Redes sociales
    - Plataformas de videojuegos
    - Servicios de almacenamiento en la nube
    - Servicios de correo electrónico
    - Plataformas de entretenimiento

A continuación se expone un ejemplo de phishing utilizando la identidad de la Seguridad Social (fuente: INCIBE):


De Ministerio de Inclusion Seguridad Social <infoemail-@eletronica.com.br>
Asunto **Liquidacion de impuestos Ultimo aviso**
A

GOBIERNO DE ESPAÑA · MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES
Seguridad Social **Sede**Electrónica

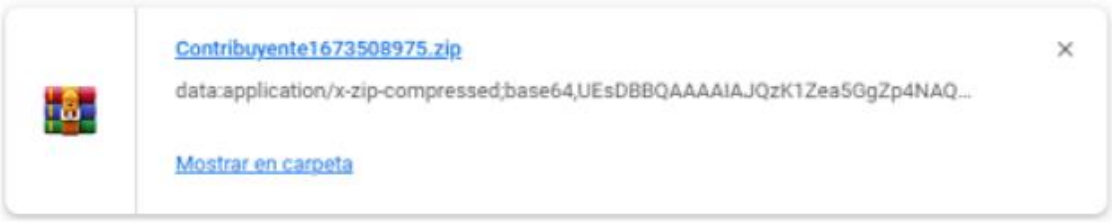
Estimado(a) Contribuyente

SeguridadSocial: Le informa que existen obligaciones,
Producto de una liquidaciÃ³n tributaria que se encuentra impaga. puede descargar
El informe generado por el **SII** en **el siguiente enlance**:

Descargar Informe

Copyright Â© Seguridad Social 2023. Todos los derechos reservados

Al pulsar en el enlace 'Descargar informe' se descarga un archivo comprimido .zip, el cual se nombra como 'ContribuyenteXXXXXXXX.zip' (donde las XXXXXX aparecen una sucesión de números que puede variar).


Contribuyente1673508975.zip
data:application/x-zip-compressed;base64,UEsDBBQAAAAIAJQzK1Zea5GgZp4NAQ...
Mostrar en carpeta

Al ejecutar el archivo, el dispositivo se habrá infectado con un troyano que podría llevar a cabo diferentes procesos fraudulentos.

SPAM

El spam hace referencia a mensajes no solicitados, principalmente de tipo publicitario, y enviados de forma masiva. La forma de envío más utilizada es el correo electrónico, pero también puede presentarse por programas de mensajería instantánea o redes sociales.

No es un problema menor; aunque se está consiguiendo reducir, se dice que más del 70% de los correos electrónicos que circulan son spam. La mayor parte del spam que circula por correo electrónico está escrita en inglés, y se origina en Estados Unidos y Asia.

Si bien hay casos de publicidad no solicitada, en la mayoría de las ocasiones, además se trata de publicidad engañosa y falsa. Su estrategia más frecuente es tentar al receptor del correo con ofertas de artículos de lujo (relojes, perfumes, smartphones), medicamentos o productos ilegales a un precio muy atractivo, inferior a su precio de mercado.

En muchas ocasiones el correo basura contiene un fichero adjunto o un enlace a una página web. Si accedemos a cualquiera de los dos es muy probable que nuestro ordenador se infecte con algún tipo de malware. El spammer busca dos cosas: nuevas direcciones de correo o infectar nuevos ordenadores que se dediquen a reenviar spam sin que sus propietarios lo sepan.

Aunque la mayor parte de los servicios públicos de correo electrónico (Gmail, Hotmail/Outlook, Yahoo!) incluyen filtros muy eficaces contra el spam, el mejor consejo es **desconfiar** de cualquier correo electrónico que recibimos de alguien **desconocido** o de alguna empresa u organización con la **que no tenemos ningún tipo de relación**. **No debemos responder a los correos, ni pinchar en los enlaces o abrir los ficheros adjuntos que acompañan al correo**.

En el spam no existe un interés especial en el receptor del correo o del mensaje. Únicamente se espera, a través de envíos masivos, que algún destinatario adquiera los productos ofrecidos y, en el peor de los casos, su equipo resulte infectado con algún tipo de virus. Pero a veces el objetivo sí se centra en quien recibe el correo.

DDoS

Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.

Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

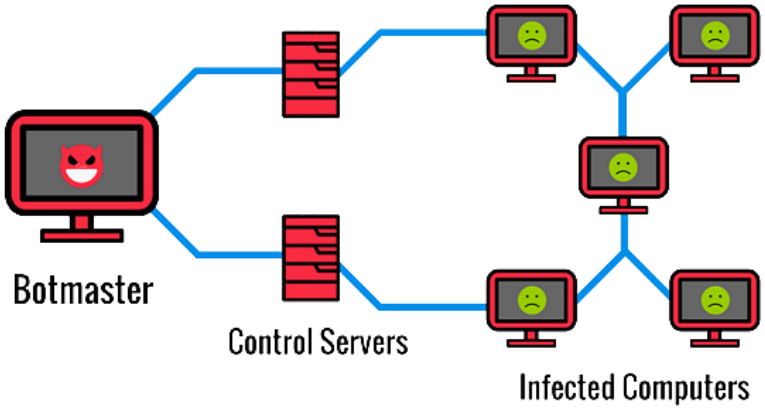
Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Destributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque.

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

En el caso de los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Los ordenadores que realizan el ataque DDoS son reclutados mediante la infección de un malware, convirtiéndose así en bots o zombis, capaces de ser controlados de forma remota por un ciberdelincuente. Un conjunto de bots, es decir, de ordenadores

infectados por el mismo malware, forman una botnet o también conocida como red zombi. La imagen siguiente ilustra la relación entre los diferentes bots y la botnet:



Obviamente, esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina.

Como hemos visto, los ataques de denegación de servicio son utilizados para inhabilitar un servicio ofrecido por un servidor, haciendo colapsar el sistema aprovechando sus vulnerabilidades. El objetivo de los ciberdelincuentes es provocar un perjuicio, tanto a los usuarios que se abastecen del servicio, como al administrador que lo ofrece, inhabilitando su funcionalidad y provocando pérdidas, tanto económicas, como de prestigio.

RAMSONWARE

Actualmente, uno de los incidentes de seguridad que más afecta a las empresas es la infección por *ransomware*, que secuestra su información y pone en peligro la continuidad del negocio.

Es un tipo de malware que se introduce en los equipos y dispositivos móviles impidiendo el acceso a la información, generalmente cifrándola, y solicitando un rescate (*ramson*, en inglés) para que vuelva a ser accesible. Después de la infección inicial, el malware intentará propagarse al resto de los sistemas conectados a la red, incluyendo unidades de almacenamiento compartidas.

El *ransomware* identifica las unidades de un sistema infectado y comienza a cifrar los archivos dentro de cada unidad. Por lo general, el software de rescate añade una extensión a los archivos cifrados, como .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault o .petya, para mostrar que los archivos han sido cifrados. La extensión de archivo utilizada es específica para cada tipo de *ransomware*. El *ransomware* se manifiesta cuando el dispositivo está infectado y ya no se puede acceder a la información.

En la mayoría de los casos la infección se produce por:

- Correos electrónicos que utilizan la ingeniería social para que la víctima descargue adjuntos infectados o acceda a un sitio web malicioso a través de un enlace.
- Ataques usando el protocolo de escritorio remoto (RDP), ya sea aprovechando alguna vulnerabilidad en el sistema o con ataques de fuerza bruta.
- Vulnerabilidades de servicios expuestos a internet (FTP, SSH, TELNET, etc.).
- Vulnerabilidades en los sistemas operativos y en navegadores que facilitan la infección al visitar sitios fraudulentos.

- Dispositivos externos infectados que se conectan a los equipos corporativos.
- Por medio de otro malware que previamente ha entrado en nuestro dispositivo.

Ejemplo de ramsonware:

Importante oleada de ransomware afecta a multitud de equipos

Fecha de publicación: 12/05/2017
Importancia: 5 - Crítica

Recursos afectados:

- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016

Descripción:

Actualizado 16/05/2017 - 12:00. Se está produciendo una infección masiva a nivel mundial de equipos tanto personales como en organizaciones, por un malware del tipo ransomware que tras instalarse en el equipo, bloquea el acceso a los ficheros del ordenador afectado y como es típico en este tipo de virus, solicita un rescate para permitir el acceso. Además en este caso, podría infectar al resto de ordenadores vulnerables de la red a la que pertenece.

3. ¿CÓMO AFECTA A LAS EMPRESAS?

La afección de los ciberataques puede llegar a ser muy considerable en las empresas, conllevando:

1. Pérdidas económicas directas que repercuten en la empresa

- Caídas en el servicio o en las cadenas de producción
- Coste de reestablecer el servicio
- Posibles indemnizaciones por denuncias de los clientes

2. Pérdidas económicas indirectas

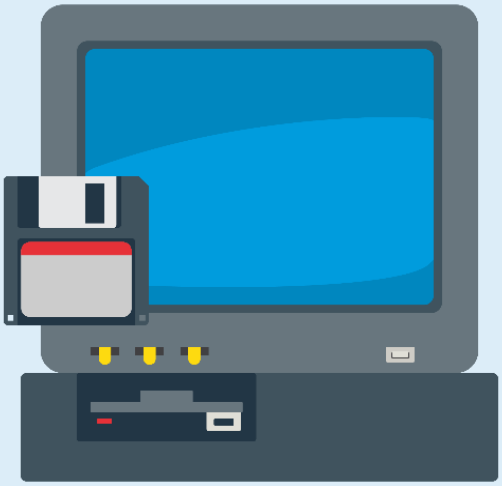
- Tiempo invertido para buscar y subsanar la brecha de seguridad, además de reestablecer los servicios
- Búsqueda e investigación para determinar fallos que han propiciado la fuga o brecha de datos

3. Pérdida de confianza y reputación

- Un grupo u organización criminal posee datos de tus clientes, proveedores, usuarios y empleados, y pueden ser utilizados para atacarlos: serán vendidos o cedidos a otras entidades para ser explotados, enviando SPAM, favoreciendo campañas de phishing, intentos de intrusión, extorsión, etc.
- Dejas al descubierto que tu organización no tiene una buena seguridad. Pueden volver a hacerlo.

4. ERRORES MÁS COMÚNES EN LAS EMPRESAS

SOFTWARE DESACTUALIZADO



Tanto los equipos operativos, como los contenidos y páginas web y los programas que se utilizan para el trabajo, deben estar debidamente actualizados a sus últimas versiones y con todos los parches de seguridad instalados.

Cualquier software desactualizado, como un sistema operativo obsoleto, sin soporte por parte del fabricante, así como el resto de aplicaciones informáticas que se utilizan, desde herramientas ofimáticas, pasando por el CRM, hasta el software de la web o las apps de los móviles, son susceptibles de tener fallos de seguridad o vulnerabilidades. Los ciberdelincuentes aprovechan estos agujeros para intentar introducirse en los sistemas.

CONTRASEÑAS POCO SEGURAS

Es una de las primeras barreras de seguridad; por lo tanto, se debe configurar para que sea difícil de romper. Se deben proteger todos los accesos posibles, tanto a dispositivos móviles como a equipos y documentación sensible. Siempre que sea posible se establecerán contraseñas elaboradas, que cuenten con múltiples caracteres, mayúsculas y minúsculas, símbolos… Y se cambien de forma periódica.

MEDIDAS DE SEGURIDAD DEFICIENTES

La información debe estar rigurosamente catalogada y ser accesible para así poder consultarla y clasificarla fácilmente según las necesidades de la empresa. Así pues, debe estar salvaguardada y controlada para evitar que algún agente externo pueda acceder a ella, modificándola o destruyéndola.

Es por ello que se recomienda que la información tenga un ciclo de vida, eliminándose de forma segura cuando deje de ser de utilidad. Pero, mientras esa información sea útil y tenga una razón de ser conservada, deberá estar protegida, siguiendo buenas pautas para ello.

A continuación, se muestran una serie de medidas básicas para la protección de este activo vital para los intereses de las organizaciones:

Control de acceso a la información

Limitar el acceso a la información es una de las prácticas más relevantes. Se debe a que cuantas menos personas tengan acceso a una información, menor es el riesgo de que esta se comprometa. Toda empresa debe seguir el principio del mínimo privilegio, es decir, un usuario debe tener acceso a la información estrictamente necesaria para realizar sus funciones. Para ello, se deben seguir los siguientes pasos:

Definir los tipos de información existentes en nuestra empresa, como pueden ser: datos, contabilidad, clientes, marketing, producción, etc.

Designar quién puede acceder a las diferentes informaciones.

Asignar quién y cómo puede autorizar el acceso a determinada información.

Copias de seguridad

La creación de copias de seguridad es un método de salvaguardas básico para la protección de la información.

El soporte elegido para almacenar la copia de seguridad debe ser fiable. Hay tres variables para tener en cuenta a la hora de crear la copia de seguridad:

- Analizar con un software integral de seguridad la información de la que se va a realizar la copia, de los sistemas y de los repositorios donde se encuentra.
- Deben hacerse pruebas de restauración periódicas con el fin de garantizar que no haya problemas en caso de tener que recuperar la información.
- Debe llevarse un control de los soportes de copia mediante un etiquetado y registro de la ubicación de los soportes.

5. ¿QUÉ PUEDEN HACER LAS EMPRESAS PARA PROTEGERSE? 10 PAUTAS CLAVE

A continuación se exponen varias acciones que los responsables de las empresas pueden llevar a cabo para mejorar la ciberseguridad de sus empresas:

1. Capacitar a los empleados para que confíen, pero verifiquen

Como regla general, los empleados solo deben tener acceso a los recursos y la información necesarios para realizar sus funciones laborales. Para determinar esto, una empresa necesita saber cómo se utilizan los datos, sistemas, dispositivos, etc. y con qué propósito.

Siempre que sea posible, las empresas deben crear perfiles de usuario, es decir, cuentas que limiten el acceso a recursos específicos dentro de la empresa. Cuando esto no es posible, la siguiente mejor opción es establecer restricciones y proteger con contraseña el acceso a carpetas o archivos como parte de la funcionalidad de los sistemas operativos.

La clave para limitar el acceso también es cancelar el acceso una vez que un empleado deja la empresa. Esto mitiga el riesgo de amenazas internas.

2. Instalar un software antivirus y antimalware confiable y mantenerlo actualizado

La solución más común para protegerse contra el malware es un software antivirus. Los sistemas operativos Microsoft Windows y Mac ya tienen un software antivirus integrado que funciona bien contra la mayoría de las amenazas y que tiene la funcionalidad básica para detectar y eliminar malware, cuando están actualizados. A pesar de las ventajas de estos programas integrados, los atacantes tienen amplias oportunidades para diseñar programas de malware para eludir estas defensas. En cualquier caso, es una buena práctica incluir protección antivirus adicional en los dispositivos de TI de la empresa y asegurarse de que se actualice de manera regular.

3. Usar cortafuegos de red y revisarlos periódicamente

Los cortafuegos o “firewalls” son dispositivos o programas que controlan el flujo de información o tráfico entre redes (tráfico de red) desde una red externa a la empresa, dentro de la red interna de la empresa, o entre dispositivos con diferentes configuraciones de seguridad. Los cortafuegos

se pueden integrar en el enrutador proporcionado por el proveedor de servicios de Internet (ISP, por sus siglas en inglés) o en programas antivirus específicos. Un cortafuegos es una defensa esencial para una empresa. Según el nivel de riesgo empresarial, las empresas deben considerar si actualizar los cortafuegos y complementarlos con otras soluciones, como aquellas que cifran el tráfico o monitorean de cerca la información intercambiada con y dentro de la red empresarial.

4. Elegir contraseñas seguras y cambiarlas con frecuencia

Las contraseñas simples de una sola palabra que se usaban en el pasado ya no son un medio efectivo para proteger una cuenta. Los atacantes ahora tienen herramientas capaces de descifrar contraseñas en una hora o menos. Una práctica más segura es desarrollar contraseñas con frases cortas que contengan números y caracteres especiales mixtos para que las contraseñas sean más complejas, largas y difíciles de adivinar.

Las contraseñas siempre deben ser complejas, guardarse en un lugar seguro, mantenerse confidenciales y cambiarse regularmente.

5. Utilizar la autenticación multifactor

La autenticación multifactor requiere que los usuarios proporcionen dos o más medios de verificación para obtener acceso a una cuenta, aplicación o sistema. Puede ser una combinación de una contraseña u otra información específica del usuario legítimo y un código generado y enviado por el sistema (por correo electrónico, mensaje de texto o llamada telefónica) al usuario.

6. Actualizar el software de manera regular

Con las actualizaciones, los desarrolladores solucionan problemas, como vulnerabilidades de seguridad conocidas de aplicaciones, programas o sistemas operativos. Estas actualizaciones deben instalarse lo antes posible. Las empresas deben tener en cuenta que los desarrolladores solo pueden corregir las vulnerabilidades conocidas.

7. Cifrar todos los datos confidenciales

El cifrado de datos hace que el contenido sea legible solo para aquellos que tienen las claves o contraseñas para abrir o descifrar los datos. Se pueden cifrar archivos individuales o dispositivos completos, incluyendo las unidades en la nube.

8. Mantener seguro el sitio web de la empresa

La mejor manera de proteger este activo crítico depende de las propiedades técnicas del sitio, el ecosistema de IT en el que se administra y dónde se guarda o aloja el sitio.

9. Mantener copias de seguridad de toda la información

Actualmente, la mayoría de las empresas dependen en gran medida de los datos y los sistemas IT. Al planificar la seguridad cibernética y crear copias de seguridad, las organizaciones deben comprender cómo funcionan los sistemas y deben priorizar las copias de seguridad para la información más confidencial y los sistemas críticos.

Se recomienda guardar copias de seguridad de manera local, en unidades o medios externos, en un servicio en la nube o en un escenario híbrido usando almacenamiento local y en la nube.

10. La seguridad física es parte de ciberseguridad

Los activos físicos de IT representan una cantidad significativa de riesgo. Conectar, desconectar, reiniciar y cargar son algunas de las muchas acciones que un atacante puede realizar para facilitar o lanzar un ataque cibernético cuando tiene acceso físico a los dispositivos empresariales. Las computadoras con la información empresarial más confidencial deben guardarse en un lugar seguro, como un gabinete u oficina cerrados. Las empresas deben asegurarse de que los dispositivos industriales conectados requieran llaves para funcionar. Para determinar qué dispositivos son críticos, como mínimo, una empresa debe saber qué dispositivos tiene, para qué se utilizan y el tipo de información que se almacena en ellos. Es probable que la mayoría de las empresas ya cuenten con protocolos de seguridad física sólidos, y las medidas requeridas dependen del tipo de empresa y su ubicación. Lo importante es incluir los ciberactivos en la seguridad física del negocio.

6. FUTURO MÁS CERCANO: RETOS PARA LA SEGURIDAD

Los retos más actuales a los que se enfrenta la ciberseguridad son los siguientes:

PREOCUPACIÓN POR LA GESTIÓN DE RIESGOS

Mientras los responsables de seguridad de las empresas manifiestan su preocupación por el nivel de ciberresiliencia de las compañías en la gestión integral de riesgos, entre los líderes de los negocios no le asignan la misma relevancia.

Es por ello que se hace necesario promover la concienciación sobre los riesgos y la inversión para luchas contra ellos.

ESCASEZ DE TALENTO ESPECIALIZADO

El déficit de personal especializado en ciberseguridad se triplicó en los últimos años en un contexto de mayor demanda de talento para hacer frente a estos retos.

TECNOLOGÍAS EMERGENTES, FOCO DE NUEVOS RIESGOS

La irrupción masiva de la inteligencia artificial generativa en el último año se ha convertido en una de las principales preocupaciones de los ejecutivos, ya que se considera que esta tecnología ofrece una gran oportunidad para los ciberatacantes para para potenciar actividades como el phishing y la difusión de información errónea.

Para luchar contra ello, las organizaciones deben comprender mejor el impacto de las nuevas tecnologías que adopten, como la IA generativa, desde la perspectiva de la ciberresiliencia.

ECOSISTEMA CIBERNÉTICO PROBLEMÁTICO

Las cadenas de suministro plantean el desafío de lograr una mayor colaboración entre las diferentes organizaciones para lograr un entorno de operación seguro. Más de la mitad de las empresas no piden pruebas sobre protocolos de ciberseguridad en las cadenas de suministro. Incluso, dos de cada cinco compañías que ha sufrido ataques en el último año lo atribuyen a terceros.

Sin embargo, la colaboración entre empresas puede ser al mayor activo para un futuro digital seguro, resiliente y confiable.

REFERENCIAS

- www.incibe.es
- European Union Agency for Cybersecurity. https://www.enisa.europa.eu
- https://www.incibe.es/ciudadania/formacion/mooc/privacidad
- https://c1b3rwall.policia.es/
- https://www.incibe.es/empresas/blog/las-principales-vulnerabilidades-de-una-pyme-en-materia-de-ciberseguridad
- https://www.incibe.es/empresas/formacion/ciberseguridad-para-micropymes-y-autonomos
- https://www.aeiciberseguridad.es/index.php/Biblioteca_23
- https://www.revistasice.com/index.php/BICE/article/view/7457
- https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf

Fondo Europeo de Desarrollo Regional

"Europa se siente"