GUIA PRACTICA DE CIBERSEGURIDAD PARA PYMES

En el año 2020 hemos sufrido un cambio radical en la forma de vivir y por supuesto de trabajar, siendo el Teletrabajo una de los cambios más significativos en la Pyme.

Por eso la ciberdelincuencia está más activa que nunca incrementando exponencialmente los ciberataques. Cuando no los sufrimos directamente vemos que existen casos a nivel mundial y en España contra empresas, servicios del gobierno como el de salud, profesionales autónomos y particulares.

Tenemos que tomar conciencia de los riesgos a los que estamos expuestos de manera permanente y ser conscientes primero que nada de que también nos puede pasar a nosotros con las respectivas pérdidas de datos, tiempo y dinero que esto conlleva. La mayoría de personas no tienen sistemas de protección y tampoco toman precauciones con el uso de Internet, de sus datos personales, de su información de empresa y mucho menos de su privacidad.

Tenemos que tomar medidas de control y justificar la implantación de medidas preventivas, de control, de reducir los daños cuando se alteran, modifican o destruyen datos, archivos e información confidencial.

Estas medidas de control deben estar muy bien especificadas y que niveles de protección necesitamos implantar en nuestra infraestructura de información de la empresa y lo otro importante saber que actitudes de comportamiento debemos evitar como usuarios de sistemas informáticos y de Internet que nos vulneran ante posibles ciberataques.

Hay que entender a qué tipos de riesgos estamos expuestos y se describe una breve introducción a los principales riesgos que existen:

Phising o suplantación de identidad:
Es un tipo de estafa muy común en Internet por que los ciberdelincuentes persiguen engañarnos a través de la suplantación de identidad de una persona, empresa donde la confianza es lo que nos hace caer, lo que persiguen es manipularnos y poder obtener datos nuestros como contraseñas, información bancaria, entre otras.

Por lo general se realiza a través de correos electrónicos que contiene enlaces a páginas web de empresas de confianza como bancos, hacienda, la Seguridad Social, etc y nos llevan a páginas idénticas pero con otro destino distinto al original y engañarnos con su contenido para que dejemos nuestros datos. Otra forma es tener archivos adjuntos en los correos electrónicos con código malicioso que al ejecutarse en nuestro ordenador instala un virus.También está presente en páginas web fraudulentas que accedemos por distintas vías como Google o redes sociales.

Lo primero que hay que hacer es desconfiar del correo electrónico si no sabemos su origen, quién lo ha enviado y muchos menos descargar cualquier archivo adjunto que venga.

Ataques a contraseñas:
Los ciberdelincuentes se las arreglan para atacar y poder descifrar nuestras contraseñas y por malas prácticas generalizadas se lo ponemos bastante fácil.
Se cometen errores graves al poner una contraseña para una credencial de acceso a un recurso, servicio web, etc porque utilizamos las mismas contraseñas, además son débiles, cortas y fáciles de recordar como usar información personal como fechas de nacimiento, apuntarlas en notas o en archivos sin encriptar. Otra práctica incorrecta es usar patrones simples como por ejemplo 1234, o letras del abecedario como abcd, o contraseñas populares como admin, 1234, etc. Otra forma de este tipo de ataques es ataque por diccionario que también su objetivo es saber nuestras contraseñas realizando diferentes comprobaciones de combinación de palabras que empiezan empezando por simples y cambiando a palabras más complejas.

Dispositivos USB:
Es el medio más utilizado para usar la técnica del BadUSB, es decir el USB infectado que los atacantes colocan en sitios estratégicos como lugares públicos, o que se reciben como regalos de algo. Su objetivo es instalar software malware con el objetivo de robar nuestros datos o tomar el control de nuestro equipo, propagarse por toda la red infectando el resto de equipos.

La mejor forma de evitar esto es evitar conectar dispositivos USB donde no sabemos su origen y contenido.

Spam:
Este tipo de ciberataque es muy conocido por todos y muy incómodo de liar con él porque nos llena los buzones de correo con grandes cantidades de mensajes no solicitados o de envíos publicitarios. La inmensa mayoría tienen una finalidad de vendernos algo, pero lo hay también que contienen algún tipo de malware.

Debemos establecer filtros antispam en los hostings de correos que la mayoría lo tienen, y también filtrarlos manualmente marcandolos como spam y también tener un buen antivirus que revise el correo entrante por si hay algún archivo con malware.

Ataques a las redes wifi:
Existe software para romper las contraseñas de las redes wifi y poder acceder a ella donde estarían en nuestra propia red local lo cual podrían infectar o tomar el control de nuestros dispositivos. Por eso debemos tener contraseñas seguras, largas y complicadas de descifrar, además de usar protocolos seguros de red wif, mínimo WPA2 y WPA3, jamás uses protocolo WEP muy inseguro.

También no es conveniente conectarse a redes públicas como centros comerciales, negocios y de hoteles, son redes que pueden estar hackeadas o estar accediendo a una red wifi falsa con un nombre muy similar al original. Y jamás utilices estas redes públicas si vas a intercambiar información sensible como datos bancarios o archivos de empresa, lo mejor es conectarse por Red Privada Virtual (VPN) a nuestra empresa.

Ataques DDoS:
Es un tipo de ataque a conexiones y sus siglas significan en inglés “Ataque distribuido por denegación de servicio”. Este tipo de ataque consiste en acceder a un servidor web al mismo tiempo desde muchos equipos diferentes para saturar la respuesta del servidor y deje de funcionar al no soportar el volumen de peticiones.

Normalmente se propaga desde equipos infectados con un malware con este fin. El objetivo consiste en hacer caer la web, y dependiendo del tiempo que permanezca offline aumentan sus consecuencias. Con esto consiguen que se suspendan servicios, pérdida de reputación, robo de datos o pérdidas económicas, lo cual tampoco los usuarios podrán acceder al servicio caído.

Podemos protegernos de este tipo de ataques en un Hosting con un firewall en el servidor del alojamiento web, tener actualizado el software del hosting, servicio antivirus instalado y actualizado, limitar la tasa de tráfico de manera preventiva, y un servicio de monitoreo de este tipo de ataques para que redirija el exceso de tráfico. Y por supuesto tener una buena empresa de Hosting.

Escaneo de puertos (portscan):
Este tipo de ataque es el proceso donde se escanea de manera automática los puertos de un dispositivo conectado a la red con la finalidad de saber que puertos están abiertos o si cuenta con algún protocolo de seguridad deficiente, pudiendo determinar posibles agujeros de seguridad y poder realizar sus ataques. Pueden saber información importante de los usuarios, conocer el sistema operativo de nuestro dispositivo.

Para evitar el ataque por escaneo de puertos debemos sólo abrir los puertos necesarios para los servicios que tengamos en uso, todos aquellos puertos abiertos sin ninguna función deben estar cerrados todos. Para evitar esto es muy importante contar con un buen cortafuegos o firewall que actúa como barrera y es imprescindible para la seguridad de la red de la empresa.

Ataques por virus:
Están en la categoría de malware y están diseñados para auto copiarse y propagarse a tanto dispositivos como sea posible. Pueden propagarse infectando ejecutables, pueden venir en un correo electrónico, a través de un servicio web, en dispositivos usb, en archivos adjuntos y a través de conexiones de red.

Pueden crear estragos eliminando o modificando archivos en el equipo, pueden estropear o corromper el sistema operativo también.

Lo mejor forma de protegerse de los virus es tener un antivirus profesional, tenerlo actualizada su base de datos de virus por lo que pueda eliminar o meter en cuarentena cualquier archivo con un comportamiento sospechoso y también pueda escanear cualquier archivo adjunto para descargar o que su origen no sea fiable.

Tipos de virus:

Adware:

Es un software no deseado cuyo fin es mostrar anuncios publicitarios en su pantalla, principalmente en un navegador. El adware genera beneficios para su programador y es muy incómodo su funcionamiento porque se abren pestañas, cambia la página de inicio del navegador y lo ralentiza, también puede instalar nuevas barras de navegación. Una vez que el adware está instalado hace una serie de actuaciones no deseadas donde puede analizar su ubicación, los sitios web que visita y mostrar anuncios de acuerdo a esto. El adware se puede instalar de manera legítima cuando instala una aplicación y junto con ella viene el adware y también lo instala (cuidado con los programas gratuitos). Otra forma de instalarse es navegando en un sitio web, lo cual puede aprovechar alguna vulnerabilidad del navegador y se descarga.

Para eliminar el adware puede utilizar un antivirus profesional que evite su instalación o utilizar herramientas específicas para su eliminación. Evite descargar software gratuito dentro de lo posible y mucho menos de fuentes que no conozca.

Spyware:

El spyware puede infectar cualquier dispositivo, mantenerse oculto, recopilar información de nuestra actividad y dar a los ciberdelincuentes acceso a información confidencial como datos bancarios, contraseñas o descargar otros malwares e instalarlos en el equipo.

Hay spyware que son capaces de activar las webcams para vernos y también el micrófono para escucharnos sin que nos demos cuenta. El adware es un tipo de spyware, pero también existen los keyloggers que graban todas las pulsaciones de tecla y guardan esta información en un archivo cifrado, pueden obtener contraseñas, accesos a cuentas de nuestro uso.

Yo puedo saber y sospechar que tengo spyware si nuestro dispositivo va más lento de lo normal, se bloquea, en el navegador se nos cambia la página de inicio, cambio en el motor de búsqueda del navegador, aparecen ventanas emergentes, etc.

Cómo lo puedo evitar con un antivirus profesional que tenga análisis de spyware, también debo evitar descargar archivos adjuntos de correos electrónicos si n o son de confianza o inesperados, evite descargar software gratuito sino es imprescindible y de webs originales.

Troyanos:

Es un tipo de malware que muchas veces se camufla como software legítimo. Se pueden propagar por ingeniería social engañando a los usuarios para que ejecuten archivos que

contienen los troyanos en sus dispositivos, siendo una vez activados poder permitir a los ciberdelincuentes espiarte, robar tus datos confidenciales y obtener un acceso por una puerta trasera a tu sistema.

Esto pueden realizar diversos daños como eliminación, modificación, bloqueo y copia de datos y también pueden ralentizar los dispositivos infectados. Los troyanos no pueden reproducirse en otros dispositivos.

Los troyanos nos pueden afectar por diferentes tipos de acciones que realizan:

Puerta trasera (Backdoor) proporciona un control remoto del dispositivo infectado a los ciberdelincuentes, pueden realizar todo tipo de acciones con archivos, incluso reiniciar el ordenador, si son varios los equipos infectados se puede crear una red zombi con objetivos delictivos.
Rootkit están diseñados para ocultar actividades en el sistema para extender la acción de programas maliciosos y no ser detectados en el tiempo.
Troyano bancario: Están diseñados para robar datos bancarios, tarjetas de débito y crédito y sistemas de pago online.
Troyanos espía: Pueden espiar tu actividad en el ordenador mediante lo que introduces con el teclado, capturas de pantalla, etc.

Puedes protegerte de los troyanos mediante un buen antivirus profesional, también evitar ejecutar archivos dudosos, links, o utilizar dispositivos usb de dudosa procedencia.

Ransomware:
Es un tipo de malware que infecta tu ordenador e impide a los usuarios acceder a su sistema o a sus archivos personales y exige el pago de un dinero para poder acceder de nuevo a ellos. Se puede instalar principalmente a través de enlaces engañosos incluidos en un correo electrónico.

El virus le da la capacidad al ciberdelincuente de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos perdiendo el control sobre todos los datos almacenados y lanza una ventana emergente en la que pide realizar el pago de un rescate, y este pago se realiza principalmente en bitcoins (moneda virtual).

Para protegernos del ransomware debemos primero que nada tener conciencia de no ejecutar archivos de dudosa procedencia y más si vienen como archivos adjuntos en correos electrónicos, además de tener un buen antivirus profesional y siempre actualizado (evita los antivirus gratuitos, estos protegen de manera muy básica).

Otra forma de mantenernos protegidos del ransomware es tener copias de seguridad actualizadas tanto en red local como en la nube, también podemos protegernos realizando puntos de restauración frecuentes en windows o snapshots en otros sistemas. Los puntos de restauración podemos llevar el sistemas de archivos almacenados en windows a un estado anterior, por eso es importante que estén activados y que sean frecuentes. Aunque esto no es infalible en las últimas versiones de ransomware.

MEDIDAS DE PROTECCIÓN PARA LA PYME:

Hay diferentes niveles de protección que debemos tener en cuenta para que podamos estar protegidos ante un ataque de malware y poder tener siempre la empresa operativa.

Nivel 0: Educación del usuario
Este nivel es para el usuario de equipo cliente el cual el usuario es el primero quien debe tener conciencia de que su actitud frente al uso del ordenador y de su interacción con Internet le ayudarán a prevenir de posibles infecciones y engaños el cual permita que se realicen ataques de malware.

Debe tener en cuenta de:

- Utiliza contraseñas seguras complicadas y largas, es decir contraseñas que contengan letras mayúsculas y minúsculas, números y caracteres especiales admitidos. Utiliza contraseñas con un mínimo de 8 caracteres y más mucho mejor.
- No uses información personal para crear contraseñas, utiliza la nemotecnia que consiste en crear alguna frase que sepas que acontezca algún sentido y de allí podrás deducir la contraseña requerida.
- Evita conectarte a redes wifi públicas o desconocidas y utiliza siempre de lo posible conexiones VPN si trabajas de manera remota.
- Haz backups de seguridad de tus datos de trabajo o personales de tu equipo de trabajo.
- No compartas información personal en páginas web o servicios web que no confies.
- Al usar el navegador utiliza webs seguras (https), utiliza certificados digitales donde sea requerido.
- Descarga archivos de sitios web oficiales de aplicaciones y utilidades para tu ordenador, huye de lo gratuito a menos que sea una utilidad esencial para trabajar.
- Mantén el sistema operativo de tu ordenador actualizado, junto con el navegador web, el antivirus profesional y las aplicaciones de uso cotidiano.

- Ten una actitud preocupante en cuanto a tu privacidad, no la descuides ni tampoco la regales, es tu protección ante ciberamenazas.
- Desconfía de los correos electrónicos no solicitados o de origen desconocido y que además tengan archivos anexos que no sabemos lo que contienen, simplemente elimínalos o marcarlos como spam.
- No accedas a conexiones de Internet si no son conexiones seguras (https) hoy en día esto ya es un estándar web, evita visitar webs sospechosas.
- Limpia tus datos de navegación Internet de tu navegador, es mejor eliminar cookies, archivos temporales y demás rastros de navegación, hazlo con frecuencia.

Nivel 1: Equipos cliente y servidores
En esta parte están los equipos de trabajo de los usuarios debemos tener cuidado sobre todo al descargar archivos sospechosos de origen desconocido, como una de las fuentes de infección de malware principal.

En los servidores de datos debemos hacer énfasis en las medidas de protección porque aquí tendremos los datos sensibles de la empresa y donde las copias de seguridad periódicas y automáticas son la mejor manera de protegernos ante un posible ataque de ransomware.

Podemos tener medidas de prevención importantes en los equipos:
- Tener actualizado el sistema operativo a las últimas actualizaciones de seguridad importantes.
- Tener actualizadas las aplicaciones de trabajo principales.
- Tener un antivirus profesional instalado y actualizado y que cubra todos los posibles peligros de infección tanto de virus, ransomware, navegación web, correos electrónicos, etc. (olvídate de los antivirus gratuitos, son muy básicos, no es suficiente).
- Tener un cortafuegos local, si es el del antivirus mucho mejor que el de windows.
- Conectarse únicamente a los recursos de red que correspondan al usuario y puesto de trabajo.
- Haz una copia de seguridad de tus datos locales y ojalá que sea automática gestionado mejor por un software de backups.
- Si el equipo es un portátil nunca conectarse a redes wifi públicas y siempre por VPN a la empresa.
- En el servidor de la empresa tener a los usuarios bien segmentados en los accesos a los recursos del servidor, es decir a qué carpetas pueden acceder de acuerdo a su puesto de trabajo y estatus en la empresa y siempre con contraseñas seguras.
- Tener para el servidor un antivirus profesional para este tipo de sistema operativo el cual detecte el malware avanzado, detecte amenazas de manera proactiva y responda automáticamente, que pueda controlar que se puede ejecutar en el servidor y qué no, además que nos envíe notificaciones de intentos no autorizados. Y que tenga principal énfasis en la protección antiransomware para evitar el secuestro del servidor.
- Backups de seguridad automáticas periódicas en red local y con especial énfasis en la nube.

Nivel 3: Seguridad en la red local
Redes Wifi:
Las redes Wifi son muy cómodas de instalar por la ausencia de cables pero son bastante vulnerables para recibir ataques maliciosos dentro de su rango de cobertura.

Los posibles ataques que podemos sufrir en una red Wifi son ataques por denegación de servicio (DoS) que incapacita a la red wifi a través de peticiones masivas de servicio al punto de acceso haciendo que el sistema sea incapaz de responder a tantas peticiones. Otro ataque es por fuerza bruta haciendo uso de contraseñas posibles intentando averiguar las claves criptográficas que dan acceso a la red Wifi, está es la más común para robarnos acceso Wifi desde el exterior.

Existen una serie de medidas lo cual podemos mejorar la seguridad Wifi y reducir la posibilidad de un hackeo:

- Controlar el perímetro de cobertura de acceso Wifi de nuestra infraestructura de red inalámbrica, permitiendo ubicar estratégicamente los puntos acceso Wifi.
- Normalmente la política de acceso Wifi se hace a través de una sola clave compartida para todos los usuarios, siendo una mejor forma de autenticación es utilizando un servidor para las autenticaciones lo cual es un método más seguro donde cada cliente Wifi dispondrá de sus propias credenciales de acceso.
- Tener una política de contraseñas segura donde deben ser largas y contengan letras mayúsculas, minúsculas, números y caracteres especiales.
- Podemos tener una red Wifi para la empresa y otra red Wifi para personal externo a la empresa.
- Podemos establecer un horario de uso del Wifi dentro de un rango de horas de trabajo y apagarlo en las horas nocturnas.

Red general:
El router

- El router de la red debe tener un cortafuegos profesional donde todos los puertos deberán estar cerrados a excepción de los necesarios.

- La contraseña de acceso al router no debe ser la que trae de fábrica, cambiala.
- Cambia el nombre SSID del Wifi.
- Cambia la contraseña del Wifi por una segura y larga.
- Utiliza cifrado WPA2 cómo mínimo y ojalá WPA3.
- Actualiza el firmware del router cuando esté disponible.
- Desactiva el WPS (Wifi Protected Setup) que facilita la conexión de dispositivos con el router y acceder a la red.
- Si podemos tener un rango de asignación de Ip reducida (DHCP) sería mucho mejor, y los equipos de la red utilizar Ips fijas.
- Deshabilita la administración remota del router, sólo desde la red interna.
- Sólo usa redireccionamiento NAT de los puertos estrictamente necesarios y todo lo demás cerrados.

Red física:

- Mantén actualizado el hardware de la red (switches, routers, cortafuegos, puntos de acceso wifi, etc).
- Cortafuegos para **seguridad perimetral** que ofrecen una serie de medidas para una seguridad completa a la red:

1. Antivirus para puerta de enlace.
2. Gestión de control de contenidos.
3. Control y visualización de aplicaciones en tiempo real.
4. Sistema de Red Privada Virtual (VPN).
5. Cortafuegos inteligente.
6. Prevención de intrusos.
7. Anti-spam y anti-spyware.
8. Filtro para tráfico desde la red local a Internet evitando navegar por URLs peligrosas o no autorizadas.

- Si puedes tener un switch gestionable definiendo redes virtuales (VLAN) para mejorar la seguridad de la red local.

Teletrabajo

El Teletrabajo al final ha despegado en España debido al Covid-19 que ha impulsado su uso en las empresas, es una alternativa bastante interesante por los beneficios que aporta al trabajador y también para la empresa. El Teletrabajo implica que nuestra infraestructura de red tenga cambios importantes y prepararnos para acceder desde remoto a los recursos del servidor y de red.

Hay que implementar una serie de medidas tanto en la infraestructura de red y de servidor en la empresa y también en los clientes remotos que se conectarán desde Internet, todo esto para prepararlo para el Teletrabajo.

Medidas para el Teletrabajo en la empresa:

- Tener una lista de los usuarios autorizados para conectarse remotamente con sus claves de acceso, donde las contraseñas deberán ser seguras.
- La infraestructura de red protegida con los mecanismos para el servidor, monitorización de la red, routers seguros, antivirus profesional, seguridad perimetral, backups automáticos y periódicos.
- Tener un servidor para conexiones de red privada virtual (VPN) donde estén registrados los usuarios permitidos y con sus certificados de acceso.
- Tener determinado que aplicaciones va a usar el usuario remoto y su entorno de escritorio remoto del cual accede en el servidor.
- Tener a los usuarios informados sobre políticas de ciberseguridad de la empresa.
- La información de la empresa debe estar siempre en el perímetro de control de la información de la empresa y más si son datos sensibles.

Medidas a aplicar en el cliente de acceso Remoto:

- En el equipo local del usuario remoto tener su software actualizado (sistema operativo), antivirus, etc).
- Tener un antivirus profesional y nada de antivirus gratuitos.
- Conectarse siempre a través de Red Privada Virtual (VPN) a los recursos de red de la empresa.
- El usuario debe estar autorizado con sus credenciales de acceso seguras.
- Cada usuario debe tener limitados los privilegios de acceso a recursos de red de la empresa.
- Si se accede a Escritorio Remoto que sea a través de VPN únicamente.
- Evitar conectarse remotamente a la empresa por redes públicas por el riesgo que esto conlleva.
- El usuario debe aplicar las políticas de ciberseguridad de la empresa en su propio entorno de trabajo remoto.

Ransomware:

Este es el virus que considero el más problemático actualmente en la empresas, infectando dispositivos y pidiendo un rescate económico a cambio de volver los datos a su estado original después de encriptarlos.

La forma más común de infectarnos con este

malware es a través del Phising con un mensaje generalmente por correo electrónico donde nos piden que descarguemos un archivo infectado y a través de un engaño el cual podemos caer.

- La primera forma de protegernos ante posibles ataques de ransomware es educar al usuario de qué precauciones debe tener y dudar de cualquier mensaje que pueda ser sospechoso de phishing.
- Jamás debemos descargar un archivo de algún mensaje o correo electrónico el cual desconocemos su procedencia si no es de confianza.
- Evita navegar por páginas web que puedan descargar malware, por lo general páginas de descargas de software pirata, películas y demás.
- Nunca se debe pagar un rescate que los ciberdelincuentes reclaman, no hay garantías de que se pueda recuperar la información.
- Tener un antivirus profesional que contenga protección anti ransomware en sus protecciones.
- Backups de seguridad periódicos tanto en red como en la nube, haciendo principal énfasis en backups en la nube.
- Si detectamos un comportamiento extraño en nuestro equipo proceder a desconectarlo inmediatamente de la red de datos o wifi y apagarlo por la vía rápida tirando del cable de alimentación, aunque suene drástico pero es por rapidez anulando el dispositivo el cual puede seguir infectando otros dispositivos a través de la red de la empresa.
- En la empresa tener la red segmentada (VLAN) por grupos de usuarios, departamentos, etc y así evitar la propagación del ransomware.
- Tener un dispositivo de Seguridad Perimetral que tenga antivirus en la puerta de enlace.
- En los correos electrónicos tener activados desde los servidores de correo los antivirus que escanean los correos entrantes y salientes, filtro antispam.
- Crea puntos de restauración periódicos de tu sistema operativo y automáticos, esto podría ayudar a una recuperación si se detecta de manera temprana.
- Desactiva el protocolo RDP de tu equipo si no lo usas, que es el protocolo de Escritorio Remoto de Windows y evitas que ciberdelincuentes puedan acceder remotamente a tu equipo.
- Y lo más impòrtante jamás pagues un rescate.

Está **Guía Práctica de Ciberseguridad para Pymes** esperamos que te sea útil y puedas evitar incidentes informáticos desagradables.

INTELLIGENIUS INFORMATICA
www.intelligenius.org
Tels: 606 257 290 - 638 239 349