Protege el mayor activo de la empresa: La información

El creciente uso de las nuevas tecnologías y los servicios en la nube hace que los usuarios de estos servicios deban estar correctamente formados. La presente guía pretende dar unas nociones básicas de seguridad, con las que las empresas puedan empezar a formar a sus empleados en seguridad y buenas prácticas.

Cabe resaltar también que todas las medidas descritas son absolutamente complementarias y en ningún caso son excluyentes y/o incompatibles. Será responsabilidad de la persona o empresa que decida ponerlas en práctica, hacer un correcto cumplimiento de ellas.

La seguridad informática es un proceso; por lo que es necesaria una implicación activa de las personas. Los consejos descritos en esta guía pretenden ser el iniciador para una concienciación sobre la seguridad; no obstante, existen empresas especializadas en seguridad informática que cuentan con herramientas y procedimientos con los que comprobar y mantener la seguridad adquirida por la aplicación de estos consejos; siendo recomendable que una vez detectadas las necesidades en temas de seguridad puedan ponerse en contacto con una de estas empresas, que les puedan ofrecer un sistema de protección integral.

Las empresas a día de hoy hacen un importante uso de las nuevas tecnologías, para todo tipo de procesos y mejoras de productividad. Este salto a las empresas 2.0 conlleva una serie de ventajas pero hay que tener en cuenta que también implica ciertos riesgos. Las ventajas son fácilmente identificables, agilización de procesos documentales, feedback y mayor capacidad de respuesta ante peticiones de clientes y proveedores, etc. Pero las amenazas a las que una empresa se ve expuesta por el uso de nuevas tecnologías, en ocasiones son más difíciles de identificar, especialmente cuando las personas encargadas de decidir sobre las medidas de seguridad a adoptar, no las perciben como reales o propias.

La base de esta guía pretende poner de manifiesto la concienciación y presentación de situaciones reales que pueden afectar a todo tipo de empresas y que pueden desembocar en una pérdida de dinero, imagen, credibilidad y/o clientes.

A continuación se describen una serie de consejos, agrupados temáticamente, para que sea más sencillo identificar posibles fallos de seguridad y las medidas a aplicar. Los grupos temáticos son los siguientes:

- **Contraseñas**, son el objetivo de la mayoría de ataques cibernéticos, puesto que una sola contraseña puede dar acceso a mucha información sensible de la empresa. Un claro ejemplo es la cuenta de correo de un empleado, si un atacante consigue acceso a la cuenta de un empleado, aunque este no tenga información sensible en su buzón, puede usar esta cuenta para recabar información de otros usuarios suplantando al primero.

- **Seguridad en Móviles**, con el actual uso masivo de los denominados SmatPhones, con acceso a internet, se presentan nuevas amenazas o posibilidades de fuga de información. Si un dispositivo móvil se pierde y éste era usado para temas relacionados con el trabajo, es muy sencillo acceder a toda la información que contiene, si no se toman las medidas necesarias. También es destacable la semejanza de estos dispositivos con los ordenadores PC, por lo que aunque a priori no parece posible, es necesario el uso de antivirus o software de protección para evitar la fuga de información descontrolada.

- **Servicios Online**, actualmente ya se ha tomado como algo cotidiano el uso de servicios como las redes sociales para la comunicación con los clientes, partners o proveedores. Así pues, es muy importante hacer un buen uso de estos servicios y tomar las medidas necesarias, para que sepamos en todo momento qué uso se hace de la información, que aportamos por estos medios.

- **Trámites Online**, los trámites online pueden ser desde un simple registro para solicitar un documento oficial, hasta el pago de cierto producto a través de la página web de uno de nuestros proveedores. Es muy importante conocer los riesgos a los que se expone una empresa que hace uso de servicios en internet como la banca electrónica o la compra de productos por internet. Los ataques más famosos respecto a los citados trámites, son los denominados ataques Phishing, que consisten en la suplantación de la entidad bancaria o cualquier otra entidad con la que queremos realizar el trámite. El engaño además, se completa cuando después de conseguir que

cumplimentes un formulario con tus datos de banca electrónica; por ejemplo, se realizan todas las operaciones que debería realizar el destinatario real de esos datos y hacen que el incauto no perciba el falso servicio.

- **Redes P2P**, las redes punto a punto o P2P se hicieron famosas por la facilidad con la que se permitían el libre intercambio de contenidos. Esto propició que los cirber-delincuentes aprovecharan esta facilidad para usarlas como canales de distribución de software maliciosos, como pueden ser virus, troyanos o software espía. Aunque su uso no está aconsejado dentro del ámbito de la empresa todavía hay empresas que disponen de uno o varios ordenadores que tienen instalado un software de conexión a redes P2P.

Contraseñas

Las contraseñas que se usan en los distintos servicios de una empresa son el principal objetivo a la hora de intentar saltarse las medidas de seguridad de un sistema, o para acceder a información clasificada que requiera de una autenticación previa.

Los siguientes puntos describen medidas para proteger las contraseñas de posibles robos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres.
- No usar series, repeticiones o datos personales ("123456", "abcdefg").
- No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I…).
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de 8 caracteres o más.
- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
- Para quien maneje muchas contraseñas puede utilizar un gestor de contraseñas para evitar poner siempre la misma, y poder tenerlas siempre a mano.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:

- Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
- Usar un acrónimo de alguna frase fácil de recordar: Tengo tres perros podría convertirse en la contraseña Tng3Prrs
- Utiliza signos de puntuación y números para combinar las iniciales de personas u objetos de un grupo conocido como, por ejemplo, tus deportistas favoritos, amigos, películas o libros favoritos o personajes históricos. Ejemplos: Gandhi, Abraham Lincoln y Juana de Arco podrían convertirse en la contraseña: 1G,2AL,JA.

Seguridad en Móviles y Tabletas

Los teléfonos móviles se han convertido en una herramienta de trabajo imprescindible, debido a que con estos dispositivos cada vez más han ido incorporando funcionalidades que anteriormente eran exclusivas de los ordenadores; por ello, es necesario que se les apliquen unas medidas de seguridad que garanticen y protejan la información que contienen o que transmiten.

- No revelar por mensaje de texto información personal.
- Si puedes, protege tu móvil con contraseña, y activa la opción de bloqueo del teléfono cada cierto tiempo, y la solicitud de una contraseña para que se pueda desbloquear.
- Instala una aplicación de geolocalización de confianza para tratar de localizar el móvil en caso de pérdida o robo (estos programas podrían permitir controlar el móvil de forma remota, por lo que podrían ser una fuente de ataque en caso de no descargar una aplicación de confianza) o insertes una memoria externa en tu móvil sin estar seguro de que no contiene ningún virus.
- Mantén el Bluetooth apagado cuando no lo utilices, o en modo "invisible".
- Haz copias de seguridad de tu tarjeta de memoria.
- Protege tu tarjeta SIM con una contraseña (PIN).
- Antes de descargar una aplicación, lee atentamente los permisos que le das.
- No realices jailbreak (iPhone), root (Android) o modifiques el sistema operativo para "saltar" restricciones del fabricante o de la compañía.

- En caso de robo, contacta inmediatamente con tu operadora para bloquear tu tarjeta SIM.
- Apúntate el código IMEI (normalmente podrás acceder a este número pulsando en tu móvil *#06#) para indicárselo al operador en caso de robo, ya que este es como el DNI de tu teléfono.
- Mantén el software de tu móvil actualizado.
- No aceptes conexiones Bluetooth de dispositivos que no conozcas.
- No respondas a los mensajes que te envíen que te parezcan fraudulentos, ya que podrían ser números de tarificación especial.
- Si conectas tu móvil a una red Wi-fi, asegúrate de que es una red segura.
- Vigila la factura de tu teléfono, e infórmate de cualquier anomalía.
- No dejes que manipulen tu móvil en lugares que no te ofrezcan las garantías.
- En caso de robo, solicita el borrado remoto de la información si dispones de este servicio.
- No guardes el código PIN junto con el código PUK.
- Solicita autorización cada vez que un dispositivo intente establecer una conexión.
- Si es posible, instala un antivirus en el móvil, y asegúrate de que esté siempre actualizado.
- No instales aplicaciones de sitios que no son fiables.
- Intenta no mantener en tu móvil datos tuyos importantes (contraseñas, números de tarjetas, números de cuenta...)

Servicios online

Con el auge de las redes sociales, y la facilidad de acceso desde ordenadores que no son el nuestro, hay que tener en cuenta los siguientes consejos:

- Si entras en alguna cuenta de un servicio online (gmail, facebook, twitter...) desde un ordenador ajeno, asegúrate siempre de cerrar sesión cuando termines, y nunca hagas que recuerde los datos de usuarios o contraseñas, o que mantenga abierta la sesión.
- Comprueba que no miren tus contraseñas mientras las escribes.
- Fíjate bien en los permisos que das a las aplicaciones cuando les das acceso en tu red social favorita.

- Evita dar información en las redes sociales sobre en que lugar estás en cada momento, cuando te vas de viaje, o hacia donde estas yendo en ese momento.
- En las redes sociales, deja ver tu perfil solamente a las personas que has aceptado.

Trámites online

Actualmente es cada vez más común realizar trámites por internet, como son compras o solicitud de documentos. Cuando dichos trámites son de una cierta importancia, es necesario que compruebes las siguientes medidas:

- Protege tu ordenador regularmente (mantén tu software actualizado, antivirus, cortafuegos...).
- Nunca le envíes a nadie tus datos financieros por correo electrónico.
- No te conectes a redes WiFi desconocidas y sin protección.
- Si dispones de DNI electrónico y tu banco te lo permite, accede a tus cuentas a través del DNIe.
- Si tienes la opción, utiliza un teclado virtual (mediante el ratón) para poner tu clave.
- No guardes las contraseñas de acceso a tus datos bancarios en el navegador (Internet Explorer, Firefox o Chrome), ni tampoco en cualquier otra parte del ordenador.
- A la hora de pagar online, o entrar en la página de tu banco, comprueba que la página web sea segura, la dirección debe empezar por https (esto significará que os datos viajarán cifrados), además en la dirección de la página podrás ver un candadito verde.
- Mantén un registro de tus transacciones online.
- Infórmate sobre el sitio antes de comprar.
- Lee la política de privacidad.
- Asegúrate de que la dirección está bien escrita (en ocasiones los estafadores intentan suplantar las páginas utilizando direcciones similares y creando páginas idénticas).
- Proporciona sólo la información imprescindible para la operación.
- Verifica la legitimidad del sitio web (pueden enviarte mensajes fraudulentos suplantando la identidad de tu banco y pidiéndote la contraseña por diversas razones, antes cualquier sospecha ponte en contacto con tu banco o comercio).
- Al terminar asegúrate de cerrar tu sesión.
- Intenta no usar ordenadores públicos para ese tipo de gestiones.

Redes p2p

El software P2P o de intercambio de ficheros tuvo su auge hace unos años con la aparición de programas como el eMule, dicho software permite el libre intercambio de fichero a grandes velocidades.

Este tipo de software conlleva una serie de riesgos por los cuales se puede infectar toda una red informática si no se hace un correcto uso de ellos, puesto que este software no hace ninguna comprobación de seguridad de la autenticidad del emisor de fichero ni de la veracidad de los mismos, por lo que a menudo es una fuente de virus y software malicioso. Para protegerse de los peligros que conlleva el software P2P se deben llevar a cabo las siguientes medidas de seguridad:

- No utilizar redes p2p en tu empresa, podrías comprometer datos sensibles.
- Configurar adecuadamente los archivos a los que tiene acceso el programa p2p. No sería el primer caso en que alguien acaba compartiendo todo su disco duro on-line.
- Visualizar inmediatamente el archivo descargado. Muchas veces son "fakes" (archivos cuyo nombre indica otra cosa) con pornografía infantil. En tal caso, denuncia inmediatamente y sigue las instrucciones de las autoridades para borrar el fichero.
- Nunca descargues software por redes p2p, cuyo origen no puedas comprobar. Muchas veces el software viene modificado con troyanos que permitirían acceder de manera remota a tu ordenador.
- Como en cualquier otro software, mantenlo actualizado constantemente.
- Presta atención a las extensiones de los ficheros que descargues (un vídeo nunca lleva la extensión .exe).
- No utilices el programa p2p en una cuenta con permisos de administrador.
- Analiza siempre con un antivirus el software descargado.
- Modifica el nombre de las carpetas de descarga ya que muchos códigos maliciosos buscan rutas fijas para replicarse.

Miquel Ramon Ortega i Tido

CTO (Director Tecnologías de la Información), Sofistic Telematic Security, S.L