LEGÁLITAS

CONSEJOS PARA PREVENIR LOS CIBERATAQUES Y CÓMO IDENTIFICARLOS

Uno de los mayores riesgos que existen para la seguridad informática, y que muchas veces pasa desapercibido, es el factor humano.

Si bien no suele suceder intencionadamente, el desconocimiento de los trabajadores o su falta de formación puede ocasionar una incidencia de seguridad. Es importante tener en cuenta que, muchas veces, **el usuario es la última barrera que se interpone entre un atacante malicioso y nuestra información.**

PARA INTENTAR PREVENIR, ENTRE LOS RIESGOS MÁS HABITUALES QUE PODRÍAN ENCONTRAR NUESTROS TRABAJADORES, IDENTIFICAMOS LOS MÁS FRECUENTES:

Ataques de ingeniería social

Es una técnica en la que los atacantes, por ejemplo, **simulando otras identidades**, intentan obtener **información privilegiada** de los trabajadores (correos electrónicos, contraseñas, nombres de responsables de departamentos...) que pueden servir para recopilar información de una empresa para su posterior ataque.

Mail Spoofing

Para robar información, igual que en el caso anterior, también se utiliza el Mail Spoofing, un tipo de ataque informático con el que el delincuente **simula ser alguien, suplantando la identidad** de alguien de dentro de la organización, con una dirección de correo electrónico legítimo, pero que en sus archivos adjuntos o en una URL especialmente creada para el ataque, **introduce código malicioso** (pequeños programas preparados para conseguir su objetivo).

Es necesario señalar que estos ataques, normalmente, no se producen de forma aislada o autónoma, sino que habitualmente se producen con posterioridad a otros ataques, o en base a otra información que se haya obtenido previamente.

Bloqueo de nuestros servicios (DOS)

Otro escenario que podríamos encontrar, aunque no necesariamente por haber sufrido un incidente de seguridad, es la **denegación de servicio (DOS)**. Un tipo de ataque que bloquearía totalmente nuestros servicios (página web, correo electrónico, teléfono...) con todas las pérdidas que ello conlleva.

Phishing | Spear Phising

Es otro tipo de ataque dentro de la categoría de Ingeniería Social que pretende aprovecharse de la **falta de formación** o concienciación. Hace uso de información recopilada previamente para crear un **entorno de confianza**. Son los ataques de Phishing, o Spear Phising, los que basándose en información previamente obtenida, intentarán robar aún más información simulando un portal o aplicación web, presumiblemente, de confianza para el usuario.

La diferencia entre pishing y spearphing es que el primero **simula entornos genéricos** en los que no haría falta demasiada información previa (portales bancarios), mientras que el segundo, el spearphising, hace uso de **información recopilada previamente** (por ejemplo, el portal web de una aplicación de uso en la empresa).

Introducción de software malicioso

Estas formas de ataque descritas anteriormente pueden provocar diferentes incidentes de seguridad en nuestra empresa, desde un robo de información puntual hasta la introducción de **software malicioso**, tipo ransomware/ cryptolocker, que provocaría que **todos nuestros archivos queden bloqueados e inaccesibles** hasta que no accedamos al pago de un "rescate" (de ahí el termino ransom) que nos soliciten para poder recuperarlos.

LEGÁLITAS

¿Quiénes son y por qué lo hacen?

Entre las motivaciones de estos ciber-criminales se puede encontrar un amplio abanico, aunque la más habitual persigue el interés económico, bien de **forma proactiva, mediante la estafa y el chantaje, o mediante el robo de información privilegiada para su venta a terceros**.

Otra posible motivación bastante habitual es el **hacktivismo**, un colectivo que justifica sus acciones amparándose en el activismo político. Este tipo de acciones se centran más en la visibilidad de sus reivindicaciones, con lo que el daño suele ser hacia la imagen corporativa de la empresa y, aunque pueda generar repercusiones colaterales en el ámbito económico, no es su principal finalidad. Un ejemplo de ataque de tipo hacktivismo es el **defacement**, por el que se modifica la apariencia corporativa de la empresa (página web, redes sociales...) para que muestre un mensaje reivindicativo.

Otros perfilesde ciberdelincuentes que pueden llegar a darse, son los de los propios trabajadores o extrabajadores (técnicos) de la empresa, quienes, descontentos, arremeten contra esta en señal de venganza. Aunque también los hay profesionales, como algunos investigadores de seguridad, que han traspasado la línea moral de su profesión para pasarse al "lado oscuro", o gente que, sin habilidades técnicas o conocimientos muy superficiales,

Prudencia, observar y vigilar sus movimientos

Después de estas nociones básicas, el mejor consejo siempre será la **prevención**. Prestar atención a los mails que recibimos, a los programas y aplicaciones que instalamos y a las webs por las que navegamos. Toda atención es poca. Permanezca alerta.

IMPORTANTÍSIMO:

- No instales en tu equipo programas que desconoces.
- No pulses en enlaces cuyo origen o destino sea desconocido. Desconfía.
- No descargues contenidos de páginas extrañas.
- Nunca facilites información confidencial, como claves personales, por correo electrónico.
- Si recibes un correo con un enlace web, que redirige a una página que te pide que introduzcas información personal o bancaria, desconfía. En muchas ocasiones se trata de emails que lo que pretenden es llevarte a una página falsa idéntica a la original para hacerse con tus datos bancarios. Recuerda que tu banco nunca te va a pedir los datos.
- Si quieres realizar cualquier tipo de operación bancaria o comercial, trata de no hacerlo desde ordenadores públicos o desde una red WIFI abierta, ya que es más fácil captar este tipo de datos. Estas redes son completamente inseguras.
- Verifica siempre quién es el verdadero remitente del correo electrónico recibido fijándote en la dirección de email e incluso copiándola en Google o Bing para comprobar si es auténtica o un fraude.
- Dispón de un filtro antispam o herramientas que bloquean el correo considerado como no deseado.
- Bajo ningún concepto introducir memorias USB de procedencia desconocida.

No olvides que...

El robo de identidad es uno de los delitos que más crece en España y en el mundo. En nuestro país, **más de 4.5 millones de personas han sido afectadas por robo de datos personales** y las pérdidas medias por uso fraudulento ascienden a **8.000 €**.