VÍDEO intypedia017es

LECCIÓN 17: DATOS PERSONALES. GUÍA DE SEGURIDAD PARA USUARIOS

AUTORA: María Goretti López Deltell

Agencia de Protección de Datos de la Comunidad de Madrid, España

BERNARDO

Hola, bienvenidos a Intypedia. En este capítulo vamos a comentar los riesgos y amenazas con los que se enfrenta la seguridad de los datos personales, desde el punto de vista de los usuarios de los mismos, que los manejan diariamente.

ESCENA 1. RIESGOS Y AMENAZAS

ALICIA

Cuando hablamos sobre peligros para la seguridad de datos personales siempre nos viene a la mente la imagen de un "hacker" experto informático que consigue infiltrarse en una red y obtener valiosa información privada. Pero aunque esto es muchas veces así, la realidad es que la mayor parte de los más famosos escándalos en seguridad de datos se producen por negligencias en el manejo de los mismos por parte de los usuarios.

BERNARDO

¡Tienes razón! Basta con repasar los últimos escándalos aparecidos en la prensa: centenares de expedientes de mujeres maltratadas dejados en la basura a la puerta de un Juzgado, pendrives con datos de decenas de miles de militares perdido en una calle de Londres, ordenador personal con miles de datos de Hacienda olvidado en un taxi u obtención fraudulenta de contraseñas de acceso mediante técnicas burdas de engaño.

De hecho podemos hablar de amenazas a la seguridad de los datos, es decir de ataques intencionados por parte de personas que pretenden acceder fraudulentamente a ellos, pero también de RIESGOS debido a malas prácticas por parte de los usuarios, que pueden dejar visibles datos protegidos sin que nadie haya ido activamente a buscarlos.

ALICIA

Los usuarios pueden llegar a ser el Talón de Aquiles de la seguridad de datos personales. En primer lugar porque son decenas de miles y están diariamente tratando esos datos. Y sobre todo porque a menudo no son conscientes de su importancia como guardianes de esa seguridad.

BERNARDO

¡En efecto! De nada sirve mantener los servidores de datos en criptas superprotegidas con los métodos más sofisticados, o utilizar técnicas criptográficas para el almacenamiento de datos, si luego se dejan listados o documentos en la papelera, se graban datos en un pendrive que luego se pierde o, como veremos enseguida, los usuarios se dejan engañar con técnicas burdas para entregar sus contraseñas.

ALICIA

Veamos cuáles son las principales amenazas y riesgos que deben enfrentar los usuarios de datos protegidos.

ESCENA 2. TÉCNICAS DE ENGAÑO O "SOCIAL ENGINEERING" Y CONTRASEÑAS

BERNARDO

En el mundo anglosajón suelen inventar palabras para conceptos nuevos que se hacen populares. Como hardware, software o hacker. Hace ya años inventaron un nuevo nombre para una técnica que, a pesar de su simplicidad, se revelaba muy útil para obtener información o acceder a datos protegidos. Se trata del "*social engineering*", que en castellano podríamos llamar "técnicas de engaño".

ALICIA

¡Pero eso es algo que ha existido siempre! Hacerte amigo de un empleado público y obtener información a través de él o ella.

BERNARDO

Sí, pero ahora no se trata de obtener directamente los datos personales, sino de obtener información que indirectamente nos pueda dar acceso a TODOS los datos de un sistema. Lo cual es mucho más peligroso. Es como obtener una copia de la llave de la caja fuerte.

ALICIA

¡Ya! Entonces es muy importante proteger las contraseñas.

BERNARDO

Los usuarios deben protegerlas como si fueran las llaves de una caja fuerte. Y de hecho lo son.

Nunca se deben dar a conocer las contraseñas, ni siquiera a otros compañeros de trabajo. Una utilización fraudulenta de nuestra contraseña personal podría comprometernos a nosotros mismos. Las contraseñas deben ser personales. Nunca deben utilizarse contraseñas comunes a todo un grupo.

ALICIA

Y además no deben ser fáciles de deducir. Hay que evitar contraseñas obvias, como “123456”, o que se puedan fácilmente deducir de nuestro perfil personal, como el nombre, fecha de nacimiento, o incluso el número de teléfono, o el nombre de los hijos, etc. ...

BERNARDO

Pero el problema es que si elegimos una contraseña complicada puede ser difícil de recordar, y acabaremos anotándola en un post-it y guardándola en el cajón de la mesa, con el riesgo de que alguien la encuentre. De hecho, esto es desgraciadamente una práctica muy común.

ALICIA

Sí, desgraciadamente lo es. Pero hay un truco para elegir contraseñas difícilmente deducibles y que sean fáciles de recordar. Por ejemplo, todos recordamos anécdotas de nuestra vida que han sido importantes o que nos han impactado. Basta con crear la contraseña basándonos en esas anécdotas. Nadie las podrá deducir de nuestro perfil porque nadie las conoce.

BERNARDO

Y si además las aderezamos con algún número fácil de recordar, tanto mejor.

ESCENA 3. LOS DESECHOS INFORMÁTICOS Y DISPOSITIVOS PORTÁTILES

ALICIA

Otro de los peligros para la seguridad de los datos personales son la documentación obsoleta y los desechos informáticos que generan nuestros ordenadores.

BERNARDO

En efecto. Nuestros sistemas y ordenadores generan mucha basura que contiene muchísima información que debe ser protegida. Por ejemplo listados, documentos, DVDs, o incluso los propios ordenadores obsoletos cuando se retiran.

ALICIA

Los documentos obsoletos y listados fallidos nunca deben ser tirados a la basura sin destruir. Existen empresas que garantizan su destrucción por contrato y que recogen esos listados o DVDs periódicamente. Además nos proporcionan contenedores herméticos donde almacenarlos hasta que los retiran.

BERNARDO

Y por supuesto nunca debemos tirar a la basura ni entregar en donación un ordenador obsoleto que deba ser retirado sin previamente "sanitizarlo".

ALICIA

¿"Sanitizarlo"? ¡Vaya palabra! ¿Se trata de otro neologismo?

BERNARDO

Pues sí. A veces son necesarias nuevas palabras para conceptos nuevos. "Sanitizar" un ordenador es proceder a borrar todos los datos que contiene. Ten en cuenta que en el disco duro de un ordenador pueden estar grabados decenas de miles de millones de caracteres, conteniendo datos personales. Podrían estar grabadas una página de información por cada uno de los ciudadanos de España.

ALICIA

Bueno, pero eso es muy fácil, ¿no? Basta con borrar todos los ficheros del disco duro antes de retirar el ordenador.

BERNARDO

Pues no, no es tan sencillo. Cuando das la orden de borrar un archivo, por ejemplo en Windows, no se borran físicamente los datos, tan sólo se borran las cabeceras del fichero que apuntan a esos datos. Cualquiera con unos mínimos conocimientos informáticos podría acceder a ellos. Para realmente hacerlos desaparecer se deben utilizar unos programas especiales que literalmente machacan todos los datos en los discos. Esos programas se pueden encontrar fácilmente en Internet, y con ellos podemos entregar o tirar a un "punto limpio" nuestros ordenadores obsoletos sin riesgo para los datos personales que hubieran contenido.

ESCENA 4. ORDENADORES Y DISPOSITIVOS PORTÁTILES

ALICIA

Otro riesgo importante para los datos personales protegidos es el uso inadecuado de ordenadores portátiles o dispositivos de almacenamiento como los "pendrives".

BERNARDO

Sí. El riesgo en este caso es que se trata de dispositivos muy pequeños que pueden extraviarse o ser robados con mucha facilidad. Un ordenador portátil actual puede contener una cantidad

enorme de información. Y un lápiz “pendrive” puede contener decenas de Gigabytes, es decir decenas de miles de millones de caracteres, o el equivalente a decenas de millones de folios escritos.

ALICIA

Como norma nunca deberemos almacenar datos personales en dispositivos portátiles.

BERNARDO

Y si es necesario y no hay alternativa, los datos deben estar cifrados. De esa forma en caso de pérdida o sustracción nadie podrá acceder a ellos.

ALICIA

Pero cifrar datos debe ser muy complicado, ¿no?

BERNARDO

Pues no. Realmente es muy sencillo. Prácticamente todos los sistemas actuales permiten el cifrado de una forma sencilla e inmediata. Los administradores de vuestros sistemas os pueden aconsejar cómo hacerlo. El acceso a la clave de cifrado se hace mediante una frase o clave, de forma que sólo quien la conoce puede acceder a los datos.

ESCENA 5. EL CORREO ELECTRÓNICO, EL CIFRADO Y LA FIRMA ELECTRÓNICA

ALICIA

Pero si quiero enviar un mensaje cifrado a otra persona, por ejemplo por correo electrónico, ¿deberé proporcionarle esa frase o clave para que pueda descifrarlo?

BERNARDO

No es necesario. Una cosa es cifrar unos datos para que nadie excepto yo o quien conozca la frase o clave pueda acceder a ellos, y otra es cifrarlos para que sólo los pueda leer el destinatario. En el primer caso se trata de lo que se llama cifrado simétrico: una sola clave sirve para cifrar y descifrar. En el segundo caso se utiliza el llamado cifrado asimétrico, que por cierto es uno de los inventos más importantes de las últimas décadas, y que es el que permite, entre otras cosas, el comercio por Internet.

ALICIA

¿En qué consiste ese maravilloso invento del cifrado asimétrico? ¿Tan importante es?

BERNARDO

Importantísimo. Sirve no sólo para cifrar mensajes dirigidos a terceros sin necesidad de entregarles nuestra clave, sino que también son la base de la firma electrónica y la autenticación de personas en Internet.

ALICIA

¿Y cómo funciona?

BERNARDO

Mira. Mediante una fórmula matemática que sería complicado de explicar aquí, se generan dos claves, indisolublemente unidas, llamadas clave pública y clave privada. Cada individuo tiene una pareja de esas claves. La clave privada o secreta está guardada en su ordenador y protegida por una frase que sólo él conoce, o protegida por el acceso al propio ordenador. En cambio su clave pública la puede conocer todo el mundo, y de hecho suele publicarse en directorios como si fuera un número de teléfono.

Y ahora viene lo más importante: lo que se cifra con la clave pública sólo puede descifrarse con su pareja privada, y viceversa.

ALICIA

Sí, pero sigo sin entender el mecanismo.

BERNARDO

Muy sencillo. Si quiero enviar un mensaje cifrado a alguien basta con que busque su clave pública en un directorio y lo cifre con ella. Sólo el destinatario con su clave privada podrá descifrarlo. De esa forma no hace falta que nos intercambiemos ninguna clave como ocurre en cifrado simétrico.

ALICIA

¿Y la firma electrónica?

BERNARDO

Es un poco más complicado. Nuestro sistema de correo obtiene un “picadillo” (o hashing en inglés) de nuestro mensaje, y ese picadillo o resumen lo cifra con nuestra clave privada y lo añade como firma al mensaje, que puede ir o no cifrado para el destinatario.

Cuando el receptor quiere confirmar que el mensaje proviene de nosotros, basta con que descifre el picadillo añadido con nuestra clave pública, vuelva a generar un picadillo con el mensaje recibido y compare los dos resultados. Si coinciden es que ese mensaje ha sido indudablemente enviado por nosotros.

Además todo es muy fácil de realizar con los programas de correo actuales. Todo lo hacen ellos. Lo único que debemos tener es nuestra pareja de claves, que también generan los propios sistemas, y en todo caso registrarlas en una entidad certificadora de claves, como la Fábrica Nacional de Moneda y Timbre en España, Verisign u otras a nivel mundial.

ALICIA

¡Qué interesante resulta todo esto! ¿Dónde puedo conocer más cosas sobres esas funciones de hash o picadillo que me hablas y de los sistemas de cifra simétrica y asimétrica?

BERNARDO

Alicia, si deseas profundizar en estos dos tipos de sistemas de cifrado y conocer sus algoritmos, fortalezas y debilidades, te recomiendo veas las lecciones 2 y 3 de Intypedia. Para las funciones hash o de picadillo, tienes la lección 14 de Intypedia dedicada exclusivamente y en profundidad a este tema.

ALICIA

Así haré, gracias.

ESCENA 6. EL DOCUMENTO DE SEGURIDAD

ALICIA

Veo que el papel de los usuarios en la protección de datos personales es muy importante.

BERNARDO

Sí, muy importante. El que los usuarios puedan conocer los riesgos y amenazas y cómo prevenirlos es vital para la protección de datos personales.

ALICIA

¿Dónde pueden los usuarios encontrar estas normas?

BERNARDO

En el Web de la Agencia de Protección de Datos de la Comunidad de Madrid hay un capítulo dedicado a todas estas normas. Pero además cada Responsable de Fichero de datos personales debe proporcionar a los usuarios un Documento de Seguridad adecuado a cada fichero concreto, que debe contener todas las recomendaciones y normas de comportamiento que aseguren la protección de los datos personales del fichero.

ALICIA

Qué interesante. Creo que por hoy es suficiente. En la página web de Intypedia tienes más información sobre esta lección. ¡Hasta pronto!

BERNARDO

¡Adiós!

Guión adaptado al formato intypedia del documento desarrollado por Dña María Goretti López Deltell, de la Agencia de Protección de Datos de la Comunidad de Madrid, España.

Madrid, España, enero de 2013

http://www.intypedia.com