ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

41/2016 15 de junio de 2016

David Ramírez Morán

La gestión de la información en el día a día de las TIC

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

La gestión de la información en el día a día de las TIC

Resumen:

El uso cotidiano que se hace de los sistemas de información puede dar lugar que se ponga en riesgo la seguridad de la información de las organizaciones. Existen diversas vías que no requieren ningún ataque por parte de terceros sino explotar únicamente la información que los usuarios vuelcan voluntariamente en internet. Se hace necesario despertar la conciencia acerca de la existencia de estas vías y sus diversas formas para obtener esta información, para minimizar los riesgos que pueden suponer para la seguridad de la información.

Abstract:

Common use of information systems can set the security of the information of the organizations into risk. Several ways exist that do not require any external attack but only exploiting the information users put on internet voluntarily. It is a must to wake up the conscience about the existence of these ways and the multiple forms to obtain this information to minimize the risks they can pose to the security of the information.

Palabras clave:

TIC, seguridad de la información, internet, usuarios, fugas de información.

Keywords:

ICT, information security, internet, users, data leaks.

Introducción

Las personas son consideradas en la actualidad el eslabón más débil para la seguridad de la información debido a las numerosas técnicas que se han desarrollado que aprovechan la falta de concienciación de los usuarios. La vulnerabilidad que surge de las prácticas, costumbres y, en muchos casos, falta del conocimiento de los fundamentos en que se basa el funcionamiento de los sistemas de información ha incrementado notablemente esta inseguridad. Las tecnologías de la información son herramientas indispensables cuyo ritmo de incorporación al puesto de trabajo ha ido creciendo y acelerándose, y que, a diferencia de otras tecnologías, una vez implantadas, pueden continuar siendo objeto de actualizaciones que modifican su funcionamiento. Esta característica, que constituye una virtud pues permite reducir el problema de la obsolescencia de los sistemas y, por ende, de las inversiones, se convierte, a su vez, en un arma de doble filo, pues posibilita los ataques a la seguridad de la información.

Estos ataques se pueden materializar explotando el desconocimiento de los usuarios, a los que se les pide realizar acciones cuyas consecuencias desconoce. Un usuario se enfrenta en solitario a un problema porque el software no hace lo que debe, no cumple las expectativas técnicas o su comportamiento se ha modificado respecto a versiones anteriores. A la vez, la dependencia de los técnicos informáticos ha llevado a que en muchos casos, todo aquello que se le pide al usuario en relación con la informática, lo realice de forma automática, siguiendo a rajatabla instrucciones. Se facilita de este modo que surjan y hagan mella ataques como el *phishing* por el que se envía al usuario un correo electrónico haciéndose pasar por otra persona

Técnicas de explotación de vulnerabilidades como las anteriores no son la única vía por la que la información de una organización puede verse comprometida. Todos los usuarios de sistemas de información están generando permanentemente datos que, de forma más o menos inconsciente, pueden llegar a salir de la organización a través del uso habitual que se hace de las herramientas. Abrir una página web, leer un correo electrónico o buscar un término en un buscador, además de proporcionar el servicio que esperaba el usuario, puede estar proporcionando información sobre ese usuario al dueño de la web, el remitente del correo o a la compañía que proporciona el servicio de búsqueda.

Explotación de metadatos

En 2012 el New York Times se hacía eco[1] de lo que le había ocurrido a un padre de familia en Estados Unidos frente a la empresa Target, una gran cadena de almacenes.

[1] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1

El padre había presentado una queja en la que acusaba a la empresa de incitar a su hija, menor de edad, a quedar embarazada debido a la publicidad de productos para bebés que le aparecía en la tienda online de los almacenes. Tuvo que retirar la queja y presentar sus disculpas al descubrir que su hija se encontraba efectivamente en estado de buena esperanza, hecho que los sistemas automatizados de segmentación de la publicidad habían detectado a partir de la navegación de la hija por la página web. Se trata simplemente de un ejemplo de cómo las tecnologías están permitiendo extraer información de fuentes sutiles.

Esta situación que entra dentro de lo que se puede considerar anecdótico constituye un ejemplo de cómo la información se puede explotar con fines de inteligencia cuando, por parte del receptor, existe un interés en sacarle el máximo partido posible. Las leyes de protección de la privacidad surgen ante la necesidad de proteger la intimidad y la seguridad de las personas aunque, en casos como este, no se ha vulnerado ninguna de ellas.

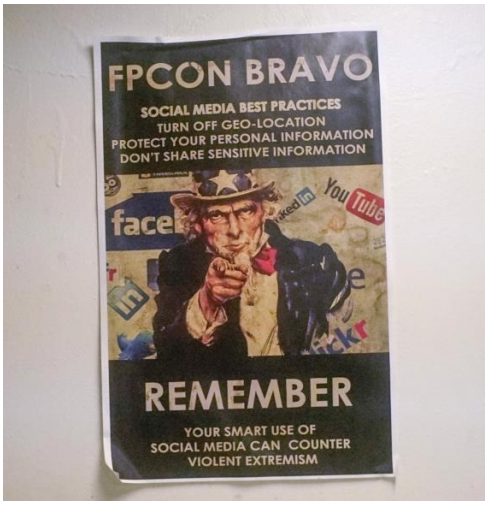
Si solo con fines comerciales se desarrolla un sistema con una complejidad tal que es capaz de detectar el embarazo de una persona, si alguien ha adquirido una consola, o si tiene un coche nuevo a partir de los patrones de navegación de los usuarios, qué no se podrá hacer cuando los fines van más allá de un exiguo margen comercial y alcanzan intereses estratégicos o de seguridad.

Por este motivo, es necesario concienciar a los usuarios de los riesgos que asumen al utilizar las herramientas que las tecnologías de la información ponen en sus manos. Es necesario hacerle consciente de que toda interacción del usuario con su ordenador puede ser información de interés para un tercero, a partir de la cual extraer inteligencia, es decir, recopilación de información que convenientemente tratada proporciona datos de interés sobre el usuario, su organización, sus intenciones…

Las redes sociales

La naturaleza de las redes sociales como trampolín de información es ampliamente conocida y no debería causar sorpresa a los usuarios la información que un tercero puede obtener a través de ellas. Es muy amplia la literatura que analiza los riesgos que pueden suponer las redes sociales para una organización. Aunque no son el objetivo de este documento, resulta imprescindible mencionarlas como una de las vías por las que pueden producirse fugas de información de la organización. Sin embargo, los usuarios, en muchos casos, no son conscientes de la cantidad real de información que están brindando con su utilización.

Para abordar los problemas de la seguridad que suponen las redes sociales se considera que una de las acciones primordiales consiste en la concienciación de los usuarios. Salía recientemente en un reportaje[2] sobre el portaviones USS Truman de la Armada de los Estados Unidos una imagen interesante en la que el «Tío Sam» se dirigía a las tropas apelando al uso apropiado de las redes sociales en un póster pegado a uno de los mamparos. En el ejército americano tienen muy presentes los riesgos que supone esta vía de fuga de información como demuestra este tipo de campañas.



Se recordaban los riesgos que entraña que tanto al enviar un mensaje como una fotografía a través de las redes sociales se pueden estar enviando también metadatos como la localización del equipo, la fecha y hora exacta de envío o la identificación unívoca del terminal desde el que se ha remitido la información. A partir de esta información no sólo es posible extraer inteligencia sobre operaciones en curso o zonas de interés, sino que también se posibilitan técnicas más graves de ataque a la seguridad de la información gracias a información como los intereses de la persona que ha enviado la información, el tipo de equipo que utiliza, etc. que pueden ser usados para otros tipos de ataque informático.

Por esta vía se veían también comprometidas las versiones oficiales de Rusia sobre la participación en los conflictos de Ucrania[3] y Siria[4], con fotografías realizadas por los soldados en los que la geolocalización delataba la presencia de tropas en la zona[5] y, en algunos casos, en ubicaciones fuera de las zonas declaradas.

Los buscadores

Estas herramientas son en muchos casos el primer punto de contacto de una persona con la solución de un problema nuevo. Tan pronto como se empieza a trabajar sobre un aspecto el usuario va a recurrir a ellos para recopilar información adicional sobre el tema. Los términos de búsqueda que introduzca en la página son información que está remitiendo, en primer lugar a la empresa del buscador, y en segundo lugar, a

[2] http://elpaissemanal.elpais.com/documentos/a-bordo-de-la-quinta-flota-estadounidense/
[3] https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine
[4] http://uaposition.com/latest-news/the-russian-army-in-syria-russian-soldiers-post-their-geotagged-photos-in-social-networks/
[5] Enrique Fojón y Guillem Colom. *Las redes sociales y sus riesgos para las Fuerzas Armadas* http://www.elmundo.es/tecnologia/2014/10/22/5447427cca474150258b456c.html

empresas que se han especializado en detectar los accesos de los buscadores para extraer estos términos de búsqueda.

Cada vez que se hace una búsqueda, se está abriendo una pequeña ventana a lo que se está gestando en el interior de la organización. Se trata de información que puede ser aprovechada cuando se cuenta con los medios necesarios para poder tratarla e integrarla. No cabe duda de que la infraestructura necesaria para poder explotar esta información es compleja aunque, con la capacidad de procesado con la que cuentan actualmente las empresas tecnológicas, no queda fuera de la potencia de cálculo instalada. Cada búsqueda, además de la información, incorpora multitud de metadatos que pueden ayudar a la integración de la información, atribuyéndola a un origen tanto de forma directa como indirecta, relacionándose con búsquedas previas.

¿Y qué tipos de asuntos pueden analizarse por esta vía? Ejemplos son muchos y diversos. Desde la interés de una empresa por la adquisición de otra hasta los intereses de un gobierno por una tecnología con la que renovar sus capacidades.

Además, los usuarios no hacen más que contribuir a estos riesgos para la seguridad de la información con prácticas que se les han ido grabando a fuego a medida que utilizan con más frecuencia los ordenadores. Una sesión de navegación actual comienza con dos pasos indisolubles para infinidad de usuarios: abrir el navegador y, en el caso de que no se abra automáticamente, invocar la página web del buscador de internet.

Toda información que se introduzca en la caja de texto del navegador está siendo recopilada por el proveedor del servicio de búsqueda y va a poder ser tratada, analizada y registrada. Es obvio que para proporcionar los resultados de la búsqueda debe tratarse esta información, pero este tratamiento solo responde a los intereses del usuario (salvando posibles intereses comerciales). El proveedor del servicio de búsqueda puede hacer tratamientos adicionales que respondan a sus propios intereses o los de terceros que usan sus servicios.

A título de ejemplo, a raíz del reciente debate entre los candidatos para las próximas elecciones generales en España, se publicaron diversos artículos[6] sobre la estadística de los términos de consulta que los internautas buscaron acerca de los candidatos durante el debate. La integración de esta información la ha elaborado el proveedor del servicio de búsqueda y constituye un servicio adicional que puede vender a costa de la información recopilada de los usuarios.

[6] http://www.europapress.es/nacional/noticia-debate-edades-mas-buscado-candidatos-google-debate-electoral-20160614143248.html

Incluso en aquellos casos en los que se conoce la dirección web de la página que se desea visitar, www.ieee.es, por ejemplo, se introducirá esta dirección en la barra de búsqueda del buscador en lugar de la propia barra de direcciones del navegador. De esta forma se está remitiendo al proveedor del servicio de búsqueda el historial completo de todas las páginas por las que se navega.

Es necesario reconocer también que esta costumbre se puede catalogar como una medida de seguridad pues el buscador, al proporcionar los resultados, priorizará aquellos de mayor fiabilidad frente a posibles páginas fraudulentas que aprovechen, por ejemplo, el uso de direcciones web similares, utilizando extensiones menos habituales como .org, .net... El precio a pagar por este filtro de seguridad son los datos que se han remitido al buscador en cuestión para que localizara la página a la que deseamos acceder.

El email

Una de las vías por las que el correo electrónico puede dar lugar a la fuga de información se basa en la funcionalidad que permite solicitar un mensaje de confirmación cuando el destinatario abra el correo. El receptor puede configurar su cliente de correo de forma que este mensaje de confirmación se envíe de forma automática, con lo que el remitente recibirá un correo de confirmación en cuanto el destinatario abra el correo. Esta información puede permitir analizar la agenda del receptor o extraer información adicional (especialmente antaño cuando la lectura del correo se hacía en un ordenador) cuándo esa persona ha vuelto a sus dependencias (oficina, domicilio, etc.) habituales. Cada vez menos usuarios activan el envío automático de las confirmaciones o autorizan manualmente su envío por lo que es un riesgo en declive. Los terminales móviles y las posibilidades de acceder al correo electrónico en cualquier momento y ubicación han reducido también este problema pues los datos de hora y ubicación ya no aportan información tan fiable o significativa.

Frente a la contramedida que su pone la configuración correcta del cliente de correo, se pueden utilizar otras técnicas con fines similares. De una forma muy sencilla es posible conseguir la funcionalidad anterior de confirmación de lectura, además de la identificación del usuario y su ubicación.

Los correos electrónicos inicialmente transportaban únicamente texto plano e imágenes como documentos anexos que había que abrir con otra aplicación. Para poder enviar correos electrónicos con diferentes fuentes o con imágenes integradas, esto ha cambiado. Actualmente un correo electrónico es a todos los efectos una página web en la que es posible incluir fuentes de letra, enlaces a contenidos y, lo que es más importante, enlaces a imágenes que serán cargadas automáticamente por el cliente de correo. Las imágenes ya no llegan al destinatario como un fichero gráfico

sino que aparecen en el correo electrónico como un enlace. Cuando el programa de correo va a mostrarlo, identifica el enlace y accede a la dirección de internet indicada en el enlace para descargar la imagen. El dueño del servidor puede detectar estas peticiones y determinar así que un correo electrónico en el que aparecía un enlace a la imagen ha sido leído por el destinatario. Este es el motivo por el que se está deshabilitando en muchos entornos la carga automática de las imágenes incluidas en los correos electrónicos.

Un paso más en la monitorización de la actividad del usuario se produce con los enlaces que aparecen en los correos electrónicos. Estos enlaces pueden tener una función de monitorización. Para ello, en cada uno de estos enlaces se incluye una cadena de caracteres que identifican unívocamente al destinatario del correo electrónico. Así, además de poder determinar si un destinatario al que se había enviado el email ha abierto el correo, también es posible determinar si ese usuario distribuye correos electrónicos que recibe a otros usuarios o si varias personas consultan ese correo electrónico. De esta forma se pueden identificar grupos de interés, grupos de trabajo o personas que guardan algún tipo de relación entre sí.

Conclusiones

La capacidad de analizar información está creciendo exponencialmente por el efecto combinado de la mayor potencia de cálculo de los sistemas y el creciente interés en el análisis y fusión de datos de muy diversa naturaleza para generar información. Las estrategias comerciales cada vez hacen un uso más extensivo de estas tecnologías, lo que está dando lugar al crecimiento de la inversión en la investigación para la creación de nuevos sistemas más rápidos, más inteligentes y más automatizados.

Es necesario despertar en el usuario la conciencia de que es un generador de información y que cada acción que desarrolla puede constituir un dato a partir del cual un sistema automático puede extraer información. Por tanto, es necesario que a la hora de navegar sea consciente de cuántos de estos datos está proporcionando a terceros externos a la organización, como pueden ser empresas de buscadores, páginas web, emisores de correo electrónico…

Empiezan a percibirse señales de que las actividades de difusión y concienciación están empezando a mostrar sus efectos positivos. Recientemente, la Fiscalía francesa saltaba a la prensa porque en su labor de instrucción de un caso obligó a utilizar un único ordenador completamente desconectado de internet para la elaboración de la documentación del caso, ante el temor de que algún tipo de información se filtrase a

internet.[7]

En el contexto del individuo, el uso abusivo de estas capacidades de obtención, tratamiento y explotación de información se encuentra limitada por la legislación con la que cuentan un número creciente de países en relación con la protección de datos. No obstante, con la debida anonimización de los datos, es posible obtener información estadística de gran relevancia sobre la población que incluso para las instituciones gubernamentales puede ser difícil de recabar por cuestiones legislativas o regulatorias.

Sin embargo, en lo que respecta a la información de las organizaciones, esta no se encuentra protegida por la legislación, por lo que es posible para los proveedores de servicios elaborar perfiles, por ejemplo, de los términos de búsqueda de los empleados de una organización, o de qué enlaces abren de los correos publicitarios que se les remiten.

La capacidad al alcance de los proveedores también plantea el problema de a quién se proporciona esta información. En el caso de los buscadores, por ejemplo, hay varios proveedores en el mercado entre los que destacan los de origen americano, ruso o chino. A día de hoy es el usuario el que decide unilateralmente qué buscador utilizar aunque en un futuro no sería descartable la imposición de limitaciones a cuál pueden utilizar los empleados de la organización para minimizar los riesgos de fuga de información. En esta línea es destacable que en el seno de la Unión Europea no se cuenta con ningún proveedor de este tipo de servicios por lo que existe actualmente una dependencia de proveedores externos para una funcionalidad que se está convirtiendo en imprescindible.

David Ramírez Morán
Analista del IEEE

[7] http://www.elmundo.es/tecnologia/2016/06/01/574ee53122601d420e8b4672.html