Ciberseguridad

RAFAEL PALACIOS Y JAVIER JARAUTA. PROFESORES DE SEGURIDAD EN EL PROGRAMA DE INGENIERÍA DE TELECOMUNICACIÓN DEL ICAI. UNIVERSIDAD PONTIFICIA COMILLAS DE MADRID

Concienciar en seguridad, la **asignatura pendiente**

Ciberseguridad es el término moderno relativo a la seguridad informática, que hace más énfasis en la posibilidad de que la seguridad se vea comprometida mediante accesos realizados desde Internet, que es actualmente lo más habitual. Durante 2016, España se enfrentó a más de 100.000 ciberataques, el doble que el año anterior y cinco veces más que en 2014. Esta escalada de incidencias hace aumentar la preocupación y en todos los sectores crece la conciencia de una necesidad de invertir en seguridad.

ES por esta razón por lo que se calcula que para 2020 habrá cerca de 700.000 empleos sin cubrir en materia de ciberseguridad en Europa, y por lo tanto las universidades (como Comillas en los programas de Ingeniería de Telecomunicación) se esfuerzan en preparar profesionales con la mejor formación en estos aspectos que el mercado nacional e internacional está demandando masivamente.

Los aspectos más importantes que se deben tener en cuenta en ciberseguridad son:

- Seguridad de las aplicaciones.
- Seguridad de la información (protección de los datos).
- Seguridad de la red de comunicaciones.
- Seguridad operacional de los procesos de negocio.
- Resiliencia y planes de recuperación y continuidad de negocio en caso de desastre.
- Educación y concienciación de usuarios.

Los ataques se producen al explotar una vulnerabilidad de una aplicación informática, o del software a nivel de sistema operativo, o bien por robo y suplantación de identidad. El objeto de los ataques puede ser la denegación de servicio (hacer que el sistema no funcione), el robo de información valiosa (Ej. espionaje, robo de credenciales, información para extorsión) o alteración de información (Ej. destrucción de información, cifrado para ransomware, etc.).

Vulnerabilidades

La seguridad de las aplicaciones y la seguridad de la información están directamente relacionadas con las vulnerabilidades del sistema. Auditar el código de las aplicaciones, aplicar los parches de seguridad y mantener los sistemas actualizados, así como mantener una cierta redundancia de equipos (en función de la criticidad del sistema) son las acciones más efectivas para mejorar la seguridad en estos aspectos.

Shutterstock / Brian A. Jackson

Ciberseguridad

Una buena configuración de la red, así como un plan operacional, son medidas que permiten detectar y reaccionar contra un ataque, como también minimizar la capacidad de propagación. Son por lo tanto mecanismos que hay que definir e implantar previamente, para minimizar las consecuencias de un ataque cuando este se produzca. Un buen ejemplo es un firewall empresarial (o un router en casa) que protege de determinados ataques desde Internet hacia los equipos personales, que pueden estar protegidos aunque tengan alguna vulnerabilidad no parcheada. Otro buen ejemplo es tener la red segmentada, de manera que cuando un ordenador infectado se conecta a la red (o un móvil infectado se conecta a la red WiFi) no propaga la infección a todos los demás dispositivos. Un ejemplo de medidas operacionales de seguridad, es la decisión en invertir en equipos o medidas especiales de seguridad para proteger mejor aquellos sistemas que se consideren más críticos.

Los planes de recuperación y de continuidad de negocio, no protegen ni evitan los ataques. Están pensados exclusivamente para recuperarse de los ataques, o también de incidentes fortuitos que también se pueden producir y pueden llegar a ser catastróficos. A la capacidad de recuperarse lo antes posible ante un incidente, hoy en día se le denomina Resiliencia. El ejemplo más sencillo de este tipo de medidas es la copia de seguridad. La información de todo tipo, por ejemplo las fotografías o documentos importantes, se pueden perder o verse alteradas por múltiples razones: ataques de malware, fallos en aplicaciones que gestionan la información, errores humanos por despiste, o ataques humanos intencionados (por suplantación de identidad). Cuando ya se ha perdido la información, la única manera de recuperarla suele ser acudir a la copia de seguridad que debe estar actualizada y almacenada en un equipo independiente. Siempre resulta paradójico que la mayoría de los usuarios gastan más dinero en la funda del móvil, que en pagar el almacenamiento icloud para mantener un backup del móvil que es automático, completo, actualizado y en servidores fiables de la nube. Si el móvil se cae al suelo, a lo mejor la funda lo puede salvar; pero si finalmente se rompe, se cae al agua, lo roban, o el niño le borra las fotos, el backup es nuestro único aliado.


Shutterstock / Alexander Yakimov

«La seguridad de las aplicaciones y la seguridad de la información están directamente relacionadas con las vulnerabilidades del sistema»

Educación y concienciación

Por último, la educación y concienciación de los usuarios en materia de seguridad es siempre la «asignatura pendiente», tanto en las empresas como a nivel personal. Desde hace muchos años, y actualmente de manera creciente, las técnicas relativas a engañar a los usuarios, que se conocen con el nombre de ingeniería social, son una manera muy sencilla de saltarse la mayoría de las medidas y protecciones de seguridad tecnológicas y organizativas.

Engañando a los usuarios se puede conseguir que rellenen sus credenciales (usuario y contraseña) en una página web que es controlada por el atacante, o que ejecuten un programa o abran un documento que contiene código malicioso, o que visiten una determinada página web, que consigue inyectar código malicioso por medio de una vulnerabilidad del navegador o uno de sus plugins (Flash, Java, sharepoint, etc). En todos estos casos el código malicioso se ejecutaría con el nivel de privilegios del usuario, que muchas

veces es el nivel de administrador del sistema. La mayor parte de estos engaños llegan camuflados en forma de correos electrónicos o también en mensajes tipo SMS o Whatsapp. También hay páginas web que incitan a instalar plugins que supuestamente permiten «ver» el contenido correctamente o con mejor rendimiento, pero estos plugins pueden ser software malicioso que queda instalado en el navegador tomando parcialmente su control.

Otro método de ataque basado en usuarios son los ataques «dirigidos» que recopilan información sobre un usuario particular que esté publicada en redes sociales, o credenciales que hayan sido previamente robados en otros sistemas (Ej. Yahoo, LinkedIn), de manera que se pueda conseguir suplantar a la víctima para lanzar un ataque en su nombre o utilizando su nivel de privilegios dentro de una organización.

También es posible robarle la identidad en multitud de sistema, ya que existen herramientas que prueban un usuario y contraseña de manera automática en los servidores más populares de redes sociales, correo electrónico y web, de manera que las personas que utilizan la misma contraseña en varios servicios, y además la contraseña no es lo suficientemente robusta, resultan especialmente vulnerables.

Software malicioso

Hoy en día, la mayor parte del software malicioso que consigue instalarse en un ordenador o un dispositivo móvil, permanece escondido sin que el usuario lo detecte; es la manera de continuar recopilando información de la víctima y de quedar al servicio del ciber-delincuente para realizar cualquier tarea o ataque. Según el «Estudio sobre la Ciberseguridad y Confianza en los hogares españoles» de 2016, elaborado por El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), aunque el 75% de los ordenadores tienen instalado algún antivirus, más del 50% tienen algún tipo de malware sin que el usuario sea consciente. Asimismo se encontraron infecciones en el 15% de los dispositivos Android analizados mediante la aplicación Pinkerton de Hispasec.

> «El uso de nuestros datos personales es una preocupación creciente en la sociedad»

El uso de nuestros datos personales es una preocupación creciente en la sociedad. Cada vez existe más sensibilización por la naturaleza de los datos que se están recogiendo sobre nuestra actividad diaria, nuestros hábitos de consumo, y los detalles sobre el uso que hacemos de las nuevas tecnologías. Esta información se está utilizando cada vez más para realizar publicidad dirigida; pero teniendo en cuenta lo que acabamos de comentar sobre ataques dirigidos, es fácil imaginar el tipo de uso que se da a esta información personal cuando cae en manos de los atacantes. Un aspecto muy novedoso del nuevo Reglamento General de Protección de Datos, (Reglamento UE 2016/679 de 27 de abril de 2016) y en la nueva directiva europea NIS para la seguridad en redes y sistemas de información (Directiva UE 2016/1148 de 6 de julio de 2016) es la obligatoriedad de comunicar las incidencias de seguridad. Se descubren ciberataques a diario, pero las entidades afectadas se apresuran en corregir las vulnerabilidades sin comunicar la incidencia. Esta manera de actuar protege la imagen de estas entidades, pues no se hace público su ataque, pero en cierto modo deja desprotegido al usuario que no es consciente de que sus datos o sus claves puedan estar siendo explotados por los atacantes.

Shutterstock / Canbedone