INCIDENTES RELACIONADOS CON LA SEGURIDAD INFORMÁTICA

Seijas Salinas, Orquídea Manuela

GRADO EN INGENIERÍA INFORMÁTICA - Escuela Técnica Superior de Ingeniería

Contenido

Introducción

Para dar inicio al curso académico, se ha propuesto la realización de un informe, que tiene el fin de dar al alumno una oportunidad de entrar en contacto por primera vez con la seguridad informática. Se han descrito dos incidentes relacionados con la seguridad informática, en los que se han visto afectados los datos o el hardware de los sistemas.

1. Incidente 1: *Hackeo* en Equifax

Equifax es una empresa norteamericana dedicada a proveer información crediticia a nivel mundial que también proporciona soluciones de información estratégica para minimizar los riesgos financieros de las empresas.

A finales de julio de 2017, el equipo de seguridad de la empresa observó una actividad atípica en la red y se decidió investigarla y bloquearla. También se decidió hacer offline la parte de la aplicación web afectada por la actividad atípica. A través del informe interno del incidente, se descubrió una vulnerabilidad en el framework de la aplicación web, Apache Struts. En este momento, se decidió actualizar la parte afectada para arreglar el fallo de seguridad.

A principios de agosto, se decidió contratar los servicios de una compañía externa de cíber seguidad, Madiant. Esta empresa estuvo analizando la información disponible para identificar la actividad no autorizada en la red.

El ataque se realizó a través de una vulnerabilidad en Apache Struts, que fue identificada y divulgada por U.S. CERT en marzo de este año. Sin embargo, la organización Equifax no conocía esta debilidad en el momento del ataque y fue necesario realizar tareas de identificación de las vulnerabilidades de la infraestructura informática de la empresa.

Este incidente potencialmente afecta a unos 143 millones de estadounidenses, casi la mitad de los habitantes de Estados Unidos, siendo este uno de los mayores ataques informáticos sufridos en una empresa en los Estados Unidos. Han quedado a merced de los atacantes nombres, números de la seguridad social, licencias de conducir (en Estados Unidos no existe ningún tipo de identificador equivalente al DNI, por lo que la mayoría de las personas se identifican con esta documentación), entre otros. También se han comprometido aproximadamente 200.000 datos de tarjetas de crédito de estadounidenses.

En la actualidad se están tomando medidas tanto como para investigar el ataque como para resolver los errores de seguridad. Además, se ha ofrecido a los usuarios un servicio de monitorización crediticia por si se produce algún caso de robo de identidad.

2. Incidente 2: Riesgo de *hackeo* en marcapasos provoca la retirada de 500.000 marcapasos en Estados Unidos

La Administración de Alimentos y Medicinas (FDA, por sus siglas en inglés) de los Estados Unidos ha retirado alrededor de 500.000 marcapasos debido a la posibilidad de que puedan ser *hackeados* debido a su falta de ciberseguridad. Los marcapasos retirados son implantables radiocontrolados, que normalmente se colocan en pacientes con latidos irregulares, o lentos, y a pacientes que se están recuperando de un infarto.

Por el momento no se han detectado accesos no autorizados a ningún marcapasos implantado, pero la FDA informa de que la vulnerabilidad permite que un usuario no autorizado pueda acceder a un marcapasos y reprogramarlo utilizando equipamiento comercialmente disponible. Es posible encontrar marcapasos y monitores del sistema en eBay, por lo que, si una persona estuviera interesada en realizar un ataque de este estilo, le costaría entre 15 y 3000 dólares. Este ataque se podría realizar descargando la batería del artefacto deliberadamente o manipulando el marcapasos para que los latidos no fueran los apropiados para el paciente.

No se han retirado marcapasos que ya estén implantados, debido a que se trataría de un procedimiento médico peligroso e innecesario. La empresa encargada de la producción se ha encargado de emitir una actualización de su *firmware* con el fin de que el personal médico lo aplique a los pacientes que ya tienen implantados los marcapasos para arreglar los posibles fallos de seguridad.

La vulnerabilidad ha sido descubierta por MedSec, una empresa de cíber seguridad especializada en la búsqueda de debilidades en dispositivos médicos. WhiteScope también realizó una investigación y encontró unas 8000 vulnerabilidades en cuatro marcapasos diferentes de cuatro productores diferentes. En esta empresa fue donde se hizo el estudio de cuánto costaría realizar un ataque de este tipo y en dos de los marcapasos que compraron encontraron datos sin encriptar de pacientes previos.

Se cree que el riesgo de ataque es extremadamente bajo, porque para que se comprometa la seguridad de los marcapasos se tienen que dar una serie de circunstancias muy concretas. Así que la FDA solamente recomienda a los pacientes que tienen los marcapasos comprometidos que hablen con su médico en su próxima revisión para la actualización del *firmware*.

Conclusiones

En este breve informe, se han podido ver dos aproximaciones opuestas a la seguridad informática.

En el primer caso, Equifax, se ha realizado la revisión de la seguridad una vez se ha producido el incidente. Esto es así porque, trabajando con la ingente cantidad de datos con la que trabajan, probablemente presuponían que tenían la seguridad lo suficientemente controlada. Sin embargo, debido a una vulnerabilidad del framework opensource, que ya estaba registrada, se produjo un ataque a su aplicación web y, por lo tanto, a su servicio como entidad monitorizadora de crédito.

En el segundo caso, una empresa de seguridad ha expuesto el posible problema antes de que se produjera algún problema asociado a la vulnerabilidad de los marcapasos. Sin embargo, debido a lo improbablidad de este hecho, la FDA, entidad encargada en este caso, ha decidido no producir una alarma en el público: se ha limitado a retirar los marcapasos que están afectados, pero no implantados y, en el caso de que estén implantados, ha aconsejado que en la siguiente revisión rutinaria se actualice el *firmware*.

La conclusión que se extrae de estos dos incidentes es que es sumamente complicado prever cuándo o, inclusive, si se va a producir un ataque informático. Independientemente de la parte del mercado económico que se trate.

Referencias

- González, J. 2017. *Una brecha de seguridad en la financiera estadounidense permite acceder al historial de crédito de sus usuarios en el país*. http://www.eldiariomontanes.es/tecnologia/ataque-informatico-pone-20170908135054-ntrc.html [Visitado por última vez el 17/09/2017.]
- Equifax Media Relations. 2017. https://www.equifaxsecurity2017.com/ [Visitado por última vez el 17/09/2017.]
- Ibercheck Soluciones. 2017. https://www.ibercheck.com/que-es-equifax/ [Visitado por última vez el 17/09/2017.]
- Prieto M. 2017. *Equifax reconoce un ciberataque masivo que afecta a 143 millones de clientes.* http://www.expansion.com/economia-digital/companias/2017/09/08/59b23dd822601dc97c8b4655.html [Visitado por última vez el 17/09/2017.]
- Hern A. 2017. *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears.* https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update [Visitado por última vez el 17/09/2017.]
- Goodin D. 2017. *Radio-controlled pacemakers aren't as hard to hack as you (may) think.* https://arstechnica.com/information-technology/2017/05/radio-controlled-pacemakers-arent-as-hard-to-hack-as-you-may-think/ [Visitado por última vez el 17/09/2017.]