Ingeniería social en la práctica: descubriendo debilidades en la seguridad del factor humano en entornos sanitarios

Julián Gómez[1[0000-0002-3157-1469]], Miguel Á. Olivero[2[0000-0002-6627-369]], Julián A. García-García[2[0000-0003-2680-1327]], María J. Escalona[2[0000-0002-6435-1497]]

[1]Entelgy Innotec Security, Madrid, España
[2] Departamento de Lenguajes y Sistemas Informáticos, Sevilla, España
molivero@us.es

Resumen. La ciberseguridad es un conjunto de procedimientos y herramientas que permite proteger los recursos tanto de la empresa como de sus usuarios. Además, en un contexto industrial los sistemas contienen información sensible sobre su contexto. Con el auge del teletrabajo los ciberdelincuentes tienen nuevas oportunidades de ataque ya que toda la comunicación laboral es digital. Esto supone que los ataques de ingeniería social sean una herramienta clave para que el atacante gane acceso a recursos delicados de la empresa. Para evaluar la seguridad del factor humano se han diseñado 4 ataques con el objetivo de conseguir información que podría comprometer la seguridad de los sistemas de una clínica de salud. Los ataques incluyen suplantación de identidad y engaño para desafiar la ingenuidad del equipo de desarrollo. Los resultados han descubierto las debilidades que presenta el equipo humano y permite crear un plan de formación como mecanismo de seguridad preventivo para proteger de ataques de ingeniería social de un atacante malicioso.

Keywords: Ciberseguridad, Factor Humano, Ingeniería Social, Salud.

1 Contexto

La ciberseguridad se engloba en un campo trasversal que se extiende más allá de la informática guardando estrecha relación con otras disciplinas como el derecho, la legislación, y las fuerzas de seguridad y control. La ciberseguridad es un requisito indispensable para mantener la calidad de un sistema ya que permite proteger los recursos tanto de la empresa como de sus usuarios. Los datos que se almacenan en los sistemas industriales contienen además información sensible de su contexto: información médica, propiedad intelectual, secretos de estado o de industria.

Se estima que para el año 2025 el gasto contra el cibercrimen a nivel mundial suponga unos 10,5 billones de dólares al año, es decir un coste de 20 millones de dólares cada minuto [1]. De acuerdo con EnigmaSoftware [2], España está en el puesto 6 de la lista de los 20 países con más cibercrimen. Además, la reciente situación de pandemia, con el auge del teletrabajo, ha ayudado a incrementar esta cifra que ha aumentado en un 25 %, según se recoge en periódicos nacionales [3]. La Information Systems Audit Control Association (ISACA) publica periódicamente el estado del arte respecto a la

ciberseguridad. En el informe de 2022 [4] ISACA concluyó que la mano de obra en ciberseguridad es, y será, escasa debido a las exigencias que involucra la formación de un profesional.

En este contexto, se realiza una auditoría de seguridad al factor humano que participa en el desarrollo evolutivo de un sistema médico ya en producción llamado iMedea. iMedea es un sistema de gestión clínica que está desarrollado por la empresa G7innovation cuyo principal macro-usuario es una clínica de reproducción asistida. El objetivo del proyecto es identificar aquellos puntos débiles que permitan establecer una línea de formación en ciberseguridad para los desarrolladores.

2 Seguridad en el factor humano

La empresa con la que se ha colaborado almacena datos clínicos de sus pacientes que son altamente sensibles según las leyes de protección de datos (p.ej., LOPD y RGPD). Por ello es absolutamente necesario hacer auditorías de seguridad tempranas de los nuevos desarrollos.

El sistema ofrece ciertas garantías a sus usuarios dada la inaccesibilidad a sus recursos desde el exterior, ya que el acceso está acotado a la red interna de la clínica. No obstante, aunque el software sea seguro, el factor humano supone un eslabón débil. Se necesita analizar la seguridad del factor humano mediante análisis y explotación de vulnerabilidades de los desarrolladores del sistema que pudieran facilitar el acceso a usuarios no autorizados. Esta debilidad se acentúa debido a la situación de teletrabajo en la que los desarrolladores necesitan acceso a una red restringida.

Además, considerando el impacto que puede suponer para la industria, existen varios estudios académicos que proponen mecanismos para medir y cuantificar el impacto del factor humano en la ciberseguridad (p.ej., [5], [6]).

Entrenar a los humanos supone una gran ventaja a la seguridad del sistema, ya que es debido a la arbitrariedad del humano que el personal de una empresa se convierte en el punto de entrada para muchos atacantes. De este modo se propone ejecutar una batería de ataques controlados de ingeniería social que ayuden a identificar las necesidades de formación en ciberseguridad.

3 Metodología

La seguridad del sistema puede ser evaluada desde las primeras etapas de desarrollo estudiando la seguridad del factor humano. Un factor humano capaz de resistir ataques de ingeniería social aporta un extra a la seguridad del producto y por tanto a su calidad final. Existen una gran cantidad de técnicas de ataques para estos propósitos [7], aunque debido a la naturaleza del teletrabajo algunas de ellas que requerían ser ejecutadas en físico, como el tailgaiting o el dumpster diving, estaban limitadas. Por otro lado, se evitan otras como el scareware para que la ejecución de este proyecto no interfiera con el trabajo habitual de las víctimas.

De este modo se planifican 4 ataques de ingeniería social involucrando 4 técnicas distintas para estudiar la capacidad defensiva del equipo de desarrollo. El

procedimiento comienza con el atacante conociendo nombre y email de los desarrolladores y qué puesto ocupan. Este tipo de información puede encontrarse en redes sociales como LinkedIn [8].

Por tanto, teniendo en cuenta las limitaciones físicas y las limitaciones de interacción que se imponen, los cuatro ataques planificados son:

Ataque 1: Videollamada con trabajador en prácticas. Este ataque usa la técnica de *pretexting*. Se ejecutará sobre un desarrollador novel ya que, debido a su inexperiencia, se le supone el eslabón más débil. El pretexto a usar es que el atacante también es recién llegado a la empresa, pero aún no le han resuelto algunas dudas. (p. ej., ¿Dónde tenéis alojado el código?, ¿Tenéis una base de datos?, ¿Puedes pedirle al Project Manager que me dé correo corporativo?, ¿Tenéis fecha de entregas?).

Ataque 2: Project Manager. En este ataque se mezclan técnicas de *pretexting*, *speah phising*, i*mpersonation*, y *whaling*. En este caso se adquiere un dominio similar al usado por los trabajadores de la empresa con el objetivo de poder mandar emails suplantando la identidad sus jefes. Los empleados recibirán un email de dominio "@g7i**n**ovation" en vez de "@g7i**nn**ovation" en el que supuestamente una figura de autoridad (el Project Manager) les pedirá información confidencial. Estos ataques que involucran la suplantación de identidades serían puestos en conocimiento de las personas suplantadas para que dieran su consentimiento.

Ataque 3: Reunión en persona con desarrollador. Para el cuarto ataque se creará una identidad falsa con rol de desarrollador y se solicita información sensible a una figura de autoridad. El pretexto a usar es que somos nuevos en la empresa y aún no conocemos los procedimientos. En el ataque se involucran técnicas de *pretexting*, *speah phising*, e *impersonation.*

Ataque 4: PDF falso. El último ataque suplanta la identidad de una figura de autoridad y viene presentado con el pretexto de una reestructuración de equipo dentro de la empresa. Este mensaje, que pretende ser alarmista, irá acompañado de un archivo *.exe* camuflado en un supuesto *.pdf* que debería contener las instrucciones de dicha reestructuración. Este ataque implica técnicas de *pretexting*, *speah phishing* y *whaling*.

4 Resultados, conclusiones y trabajo futuro

La ejecución de los ataques sobre el equipo de desarrollo se ha llevado de forma secuencial accediendo desde el eslabón más débil hasta la suplantación de figuras de autoridad. Esto ha permitido obtener información clave sobre la empresa que, de haber sido atacada por un atacante real, le habría supuesto un riesgo crítico.

Ataque 1: Videollamada con trabajador en prácticas. Información extraída: Estructura general del sistema, metodología de trabajo, carpetas compartidas, archivo Excel con información de procesos internos de migración de base de datos, código fuente. Además, pudo observarse el repositorio donde estaba alojado el código, y mostró un token de acceso SSH.

Ataque 2: Project Manager. Este ataque no extrajo información. Se conoce del fracaso del ataque ya que la víctima contactó con la persona suplantada por otros medios para verificar el mensaje sospechoso.

Ataque 3: Reunión en persona con desarrollador. El ataque fue exitoso ya que la víctima creyó que la identidad falsa era un estudiante con una beca de prácticas de formación. La víctima aceptó concertar una reunión presencial para explicar de forma general cómo se trabaja en la empresa. Sin embargo, el ataque de la reunión fue cancelado a petición de la propia empresa para no interferir con la agenda de la víctima.

Ataque 4: PDF falso. Algunas de las victimas abrieron el archivo, a pesar de que los antivirus detectaban el archivo como un virus, ignorando todos los avisos. En este caso, sin embargo, algunas de las víctimas sí detectaron que el archivo podría ser un virus, y avisaron a los demás para detener la cadena.

Tras estudiar los resultados de los cuatro ataques, se identificaron debilidades del factor humano que permite a la empresa diseñar una formación en materia de ciberseguridad. Principalmente el desconocimiento de cómo se componen los grupos de trabajo, jerarquías y políticas de compartición de información sensible. De este modo, el equipo de desarrollo puede también garantizar la seguridad de su sistema también contra ataques de ingeniería social.

Como trabajo futuro se creará una formación para concienciar a los desarrolladores de la responsabilidad que implica acceder al código y se planifica una evaluación de la formación. Dicha evaluación consistirá en ejecutar ataques similares que ayuden a comprobar la efectividad de la formación como mecanismo de seguridad.

Bibliografía

1. The Most Significant Cyber Attacks from 2006-2020, by Country. VisualCapitalist. 2021. URL: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/
2. Top 20 Countries Found to Have the Most Cybercrime. EnigmaSoftware. URL: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
3. Los ciberataques a empresas crecen un 25% a causa de la pandemia. La Vanguardia. URL: https://www.lavanguardia.com/economia/20210503/7424172/ciberataques-empresas-crecen-25-causa-pandemia.html
4. State of Cybersecurity 2022. ISACA. URL: https://www.isaca.org/go/state-of-cybersecurity-2022/
5. B.M. Bowen, R. Devarajan, S. Stolfo, (2011). «Measuring the human factor of cyber security». *IEEE Int. Conf. on Technologies for Homeland Security* (HST). 230-235. DOI: 10.1109/THS.2011.6107876.
6. A. Tiwari, U. Daniel, A.H. He, (2019) «Human factor security: evaluating the cybersecurity capacity of the industrial workforce». *Journal of Systems and Information Technology*. DOI: 10.1108/JSIT-02-2018-0028.
7. F. Mouton, L. Leenen, H.S.Venter, (2016) «Social engineering attack examples, templates and scenarios». *Computers & Security, 59, 186-209*
8. M. A. Olivero, A. Bertolino, F. J. Domínguez-Mayo, M. J. Escalona, I. Matteucci, (2020). «Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life». *Journal of Information Security and Applications*, *52*, 102492.