RESEÑA DE LIBRO

Guillermo Zeledón Flores

Recibido: 31 mayo, 2024 • Revisado: 21 junio, 2024 • Aceptado: 28 junio, 2024

Reseña de Libro: "The Art of Social Engineering" por César Bravo y Desilda Toska

La época post pandémica ha instalado en el mundo, y particularmente en Costa Rica, nuevas formas de asumir la organización del trabajo, el estudio, y las formas como nos relacionamos con nuestro entorno (Fait, 2022). Estamos asistiendo a una transición acelerada entre el paradigma de la presencialidad y lo material, a un estadio en que la virtualidad y lo digital llegaron para quedarse. Adicionalmente, el desafío de poder discernir entre lo factual o lo artificial que posibilita una tecnología emergente, invita al ser humano a fortalecer sus habilidades para asimilar con espíritu crítico la información que le rodea. En este contexto, dos autores radicados en Costa Rica, César Bravo y Desilda Toska, ofrecen una refrescante y rigurosa propuesta de lectura sobre lo que históricamente se ha acuñado como Ingeniería Social.

Los autores dividen su obra en tres grandes secciones:

En una primera parte, titulada **"Comprendiendo la Ingeniería Social"**, se invita al lector a hacer un recorrido para entender los fundamentos de lo que se entiende como "ingeniería social", la cual transiciona de una función "social" paralela a la de los conocimientos técnicos, a un arte de la manipulación a través de ciertas técnicas generadores de confianza. En varios de sus capítulos, los autores nos exponen la psicología que hay detrás de la ingeniería social, elementos para comprender el arte de la manipulación, repasan los 6 principios de la persuasión, desarrollan el tema de la empatía a través de los medios digitales, y generan un compendio de las técnicas actuales de las que se valen los "ingenieros sociales" para recrear escenarios de presunta confianza, y lograr que mediante la buena fe, los internautas compartan información como contraseñas, datos sensibles, números de contraseñas y cuentas bancarias, etc.

En una segunda parte, titulada **"Ataques de ingeniería social mejorados"**, los autores describen con gran precisión –producto de su formación en ingeniería–, modalidades específicas mediante las cuales los ciberdelincuentes efectúan ataques o *exploits*, es decir, incursiones no autorizadas que aprovechan las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. En esta categoría, no se habla tanto de ataques orientados a un público en general, sino que se trata de ataques dirigidos a ciertos objetivos (organizaciones, personas), y pueden contemplar ataques a bases de datos de carácter público, o ataques a través de páginas web, entre otros. Pero también, estos ataques mejorados pueden incluir descargas pagadas de sistemas de seguridad falsos, ataques basados en formatos tipo "juego", o mediante divulgación de noticas no corroboradas o deliberadamente no ciertas. En algunos casos calificados, los ataques de ingeniería social mejorados pueden variar desde extorsiones sexuales, ataques a través de la red WhatsApp, *clicks* perniciosos que pueden contener virus o provocar

Guillermo Zeledón Flores es Director Académico de Educación Ejecutiva de LEAD University. Es costarricense, graduado en Ciencias Políticas de la Universidad de Costa Rica, y Máster en Administración de Negocios con especialidad en Mercadeo de la Universidad Interamericana de Costa Rica. Posee un programa de Especialización Gerencial de ADEN Business School y la Universidad de San Francisco, California. Ha desarrollado su trayectoria profesional en las áreas de *trade marketing*, ventas, formación universitaria y capacitación técnica, tanto en compañías locales como transnacionales.

secuestro de información, o apropiación indebida de datos suministrados en las redes sociales.

Continúan los autores en esta sección que sin duda es la más abundante de su obra, haciendo una reseña sobre la tendencia de incorporación de algoritmos de inteligencia artificial para robustecer los ataques cibernéticos. Una de estas técnicas consiste en la generación de videos falsos, en donde el internauta podría contemplar a un personaje público diciendo algo que en realidad nunca sucedió, y ocasionar un caos por las supuestas declaraciones. Lo mismo puedo ocurrir con la divulgación de audios, en donde es "fácilmente reconocible" una voz, cuando en realidad podría tratarse de una simulación mediante inteligencia artificial. La lectura de todas estas modalidades de ataque resulta en no pocas ocasiones entretenida, ya que ofrecen una serie de imágenes, íconos y otros diagramas que ayudan a comprender mejor lo que de otra manera, quizás pueda resultar en un lenguaje muy técnico para el lector.

Finalizan la sección con una invitación muy estimulante, ofreciendo técnicas para poder instalar lo que denominan una "Caja de Herramientas de Ingeniería Social". La siguiente es una traducción libre, dado que el texto de momento solo se encuentra disponible en idioma inglés:

> La caja de herramientas de ingeniería social (SET, por sus siglas en inglés de ***Social Engineering Toolkit***) es un potente marco de pruebas de penetración de código abierto desarrollado por Dave Kennedy para la ingeniería social. Sirve como un marco poderoso para evaluar las vulnerabilidades presentes en el elemento humano de los sistemas de seguridad, enfatizando el papel vital que desempeñan los humanos en la protección de la información confidencial (Bravo y Toska, 2023).

La tercera parte de la obra, titulada **"Protección contra ataques de ingeniería social"**, desarrolla el ciclo de vida de los ataques complejos de ingeniería social, así como una serie de consejos y mejores prácticas para proteger a las organizaciones en cada una de las etapas de los ataques. Asimismo, se efectúa una revisión de algunas leyes y regulaciones internacionales aplicables a la ingeniería social.

En palabras de los autores:

> Los ataques de ingeniería social han aumentado en sofisticación y frecuencia, y los profesionales e investigadores de seguridad han comenzado a formalizar las etapas y metodologías de los ataques de ingeniería social. Esto ha llevado al desarrollo de un marco estructurado conocido como ciclo de vida de la ingeniería social (Bravo y Toska, 2023, p. 190).

En efecto, los ataques a los sistemas informáticos no ocurren de manera casual, y pueden ser resumidos en un ciclo (Figura 1), que contempla:

Reconocimiento: recopilación de información sobre el objetivo.

Selección de objetivos: elegir con cuidado individuos o grupos para explotar.

Desarrollo de pretextos: creación de una persona creíble y digna de confianza.

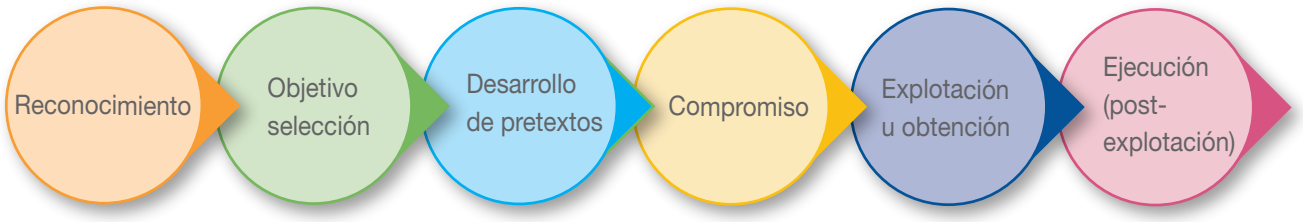
Compromiso: el atacante trabaja en construir una relación y ganarse la confianza del objetivo.

Explotación: manipulación de la víctima para realizar una pluralidad de acciones deseadas por el atacante

Obtención: la reunión discreta de información de la víctima sin pedirla explícitamente

Ejecución (post-explotación): explotación de la información obtenida o el acceso para ejecutar un ciberataque. (Bravo y Toska, 2023).

FIGURA 1. ESTILO DE VIDA DE LA INGENIERÍA SOCIAL



Fuente: Bravo y Toska, (2023)

Finalmente, dedican un apartado para ofrecer consejos para evitar ser víctima de robo e información, tales como limitar la cantidad y tipo de información que se publica en redes sociales, ajustar las configuraciones de privacidad, extremar la seguridad en "sitios" de citas, aprender a distinguir perfiles falsos, y un detalle que podría pasar inadvertido para una gran mayoría: eliminar metadatos de las imágenes, esto es, datos "invisibles" asociados a una imagen como la ubicación, hora, y otra información sensible que no se desea compartir.

CONCLUSIÓN

El uso de redes sociales, aplicaciones de comunicaciones, sistemas bancarios y otras herramientas tecnológicas que permiten multiplicidad de transacciones y expresión de estados de ánimo, ofrecen posibilidades de gran confort y bienestar para los usuarios, pero también conllevan riesgos tales como la pérdida de la privacidad, y/o el arriesgar patrimonios económicos y personales. A medida que transcurre cada capítulo, el lector descubrirá abundantes reseñas, definiciones y *modus operandi* de ciber atacantes, dispuestos a aprovechar cualquier descuido para sustraer información valiosa. Para quien nunca haya escuchado el concepto de ingeniería social, podría resultar decepcionante enterarse que académicamente se le haya asignado un nombre tan aspiracional a una actividad que en definitiva, busca fines inescrupulosos y compromete la paz y tranquilidad de las personas. Esto desde luego no es responsabilidad de los autores, y en ello considero que estriba uno de los principales logros de la obra: visibilizar un fenómeno propio de nuestros tiempos, que pone de manifiesto que hoy más que nunca, generemos información constantemente, sea que tengamos conciencia de ello o no, y esta información se ha convertido en un botín que no pocas personas están dispuestas a apoderarse para su propio beneficio. En definitiva, el arte "perverso" de quienes son capaces de invadir la intimidad de las personas y organizaciones y lucrar a partir de ello, debe alertarnos constantemente a que, sin salir de nuestra casa, nos podemos ver expuestos a situaciones que comprometen nuestra seguridad. Es digno de justicia reconocer el invalorable aporte que esta obra hace para la toma de conciencia, no solo por lo exhaustivo en el recuento y explicación de los diferentes tipos de amenazas que configuran los ataques o *exploits*, sino porque ofrece soluciones técnicas y conductuales para evitar ser víctima de estos hechos. Su lectura es más que recomendada no solo por su relevancia, sino porque denota un esfuerzo pedagógico por transmitir temas complejos de una manera muy didáctica y sencilla.

REFERENCIAS BIBLIOGRÁFICAS

Bravo, C. y Toska, D. (2023). *The Art of Social Engineering.* Packt Publising.

Fait, E. L. (2022). *Después de la pandemia: Una visión de largo plazo.* Academia de Centroamérica.