Kymatio®

White Paper - Ingeniería Social

INGENIERÍA SOCIAL, ¿ESTAMOS PREPARADOS?

KYMATIO - ACTIVACIÓN DE FIREWALLS HUMANOS

Ingeniería social, ¿qué es?

Actualmente, el campo de la seguridad de la información es altamente dinámico, en el que tanto las medidas de prevención como los métodos de ataque se encuentran en constante adaptación a los cambios del entorno. Por cada avance en materia de seguridad, los delincuentes se abren paso con la creación de nuevas formas de conseguir sus objetivos. Esto da lugar a un proceso cíclico de actualización y desarrollo continuos.

De esta forma, ante el aumento constante en la complejidad de los ataques, se genera la necesidad de desarrollar programas de protección cada vez más avanzados. No obstante, en los últimos años, en el punto de mira de los delincuentes no solo han estado los sistemas informáticos, sino que cada vez están ganando más protagonismo las personas. La razón es muy simple: en muchas ocasiones, es más fácil "hackear" un individuo que un sistema.

Esto se conoce como ingeniería social, y se trata de un método ante el cual aún no se ha conseguido dar una respuesta de protección certera. En este tipo de ataques se aprovechan de las vulnerabilidades humanas haciendo uso de diversas técnicas de manipulación (Mouton, Leenen, & Venter, 2016; Hinson, 2008; ACCISI, 2018).

La ingeniería social se define como la manipulación de personas a través del contacto directo y/o mediante tecnología, con el fin de obtener información sensible u otros datos que puedan comprometer la accesibilidad, confidencialidad y/o integridad de la misma. Puede producirse tanto en el ámbito personal como en el organizacional y, en el caso de este último, la manipulación puede producirse por parte de alguien externo o interno a la compañía.

La ingeniería social en números

No cabe duda de que este método está en auge, haciendo peligrar tanto el capital como la reputación de las organizaciones y, en muchos casos, incluso su continuidad.

El Instituto Ponemon realizó un estudio al respecto en 2020. Los resultados fueron, cuanto menos, impactantes: el 79% de las empresas que participaron admitieron haber sufrido al menos un ataque de ingeniería social. Además, en el 67% de los casos las consecuencias fueron significativas o muy significativas.

A la vista de estos resultados, cabe preguntarse si la raíz del problema podría encontrarse en el nivel de concienciación de la plantilla.
Tan solo la mitad de estas compañías proporcionan concienciación a sus empleados. Esto ya de por sí constituye un punto crítico en términos de seguridad, pero no es el único. Si la otra mitad sí está implantando programas para combatir la ingeniería social, ¿cómo puede existir un porcentaje tan alto de incidentes?

Está claro que los métodos de concienciación no están resultando eficaces, y esto es algo de lo que son conscientes las propias organizaciones: la confianza que tienen respecto a su capacidad para responder a estos ataques ha caído de un 31% a un 23% en tan solo dos años.

La forma de protegerse frente a estas amenazas debe evolucionar y cubrir nuevas necesidades, cambiando el enfoque predominante hasta ahora. Sin embargo, para poder establecer nuevas directrices, en primer lugar, es necesario comprender el problema en profundidad.

Diferentes técnicas, diferentes vectores de ataque

Los ingenieros sociales buscan manipular a las personas, a menudo por una motivación económica, y para ello pueden apoyarse en diversas técnicas para favorecer el éxito de sus ataques. Algunas de ellas son:

Phishing. Una de las más comunes. Consiste en enviar un correo electrónico, a menudo suplantando la identidad de entidades o personas de confianza, para engañar al receptor y que descargue un ejecutable, pinche en un enlace o proporcione determinada información sensible (Krombholz, Hobel, Huber & Weippl, 2015). Además, gracias al auge de las redes sociales, estas también se han convertido en un medio ampliamente utilizado para este tipo de engaños (Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019).

Suele tratarse de envíos masivos con mensajes genéricos para que, aunque el porcentaje de éxito no sea precisamente alto, la cantidad de personas que caigan víctimas del fraude sea suficientemente significativa (Salahdine & Kaabouch, 2019; Gupta, Singhal & Kapoor, 2016). Sin embargo, cuando se busca perseguir a una persona u organización en específico, los atacantes recurren al evolucionado spear phishing. Consiste en mensajes totalmente dirigidos que proporcionan datos reales como nombres o cargos para aumentar la credibilidad y facilitar así que la víctima potencial baje su guardia (Salahdine & Kaabouch, 2019).

Vishing. Su nombre proviene de voice phishing y, como indica, sus características son comunes con el phishing, a diferencia del canal utilizado. En este caso, se contacta con el objetivo a través de llamadas de teléfono para convencerle de que realice las acciones buscadas por los delincuentes (Ollmann, 2007; Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019).

Smishing. Esta técnica guarda muchas similitudes con las dos anteriores, ya que se trata de fraudes a través de mensajes de texto (Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019). Aunque en su origen se empleaban únicamente los SMS para ello (de ahí su nombre), la proliferación de las aplicaciones de mensajería instantánea como WhatsApp o Telegram abren nuevas ventanas por las que los ingenieros sociales podrían querer entrar. La utilización de enlaces maliciosos acortados o los robos de cuentas son los métodos más empleados.

Dumpster diving. No todos los ataques de ingeniería social tienen un componente tecnológico, y este es uno de esos casos. Se basa en buscar en la basura de la víctima algún tipo de información sensible o, al menos, útil para poder proseguir con el engaño más adelante (Granger, 2001; Mitnick & Simon, 2003; Krombholz, Hobel, Huber & Weippl, 2015; Salahdine y Kaabouch, 2019). Algunos ejemplos pueden ser notas con contraseñas apuntadas, horarios o informes impresos.

Shoulder surfing. A veces no hace falta llegar muy lejos para conseguir la información que se necesita: basta con mirar la pantalla del objetivo mientras se encuentra trabajando (Krombholz, Hobel, Huber & Weippl, 2015; Salahdine y Kaabouch, 2019).

Tailgating: Ocurre cuando el ingeniero social camina junto a o detrás de una persona que tiene autorización para entrar en la empresa o un área sensible de la misma para acceder a la vez en el momento que esta abra la puerta (Dey, 2016). De esta forma, el atacante conseguiría acceso a las instalaciones para dañarlas, robar información o, incluso, realizar escuchas mientras otras personas hablan de temas sensibles (Heikkinen, 2006).

Baiting. Se trata de un método algo diferente a los demás, ya que el atacante no contacta ni se acerca siquiera a la víctima. Consiste en infectar con un malware (programa malicioso) un dispositivo extraíble, como los USB, y dejarlo en un sitio donde pueda ser encontrado con facilidad (Salahdine y Kaabouch, 2019). De esta forma, en el momento en el que alguien lo recoja y lo conecte a su ordenador, el malware comenzará a hacer efecto, ya sea dañar archivos, secuestrarlos o monitorizar las acciones realizadas en el equipo.

Estas son las técnicas que utilizan los delincuentes para llevar a cabo sus ataques, pero ninguna de ellas surtiría efecto de no ser porque hay algo que incita a que la víctima actúe como se espera. Entonces, ¿cómo lo hacen?

¿Por qué funcionan los ataques?

Igual que los hackers buscan sin cesar las vulnerabilidades de los sistemas informáticos para perpetrar sus ataques, los ingenieros sociales hacen lo propio con las personas. No hay nadie que sea totalmente infalible, por lo que solo es necesario utilizar el mensaje correcto para aumentar enormemente las probabilidades de éxito.
Por tanto, cabe preguntarse cuáles son estas vulnerabilidades que tratan de explotar.

Estas aberturas no son más que nuestras motivaciones. No es necesario ir a deseos especialmente complejos, sino que se puede empezar con algo muy sencillo: ¿qué es más efectivo en nosotros, los castigos o las recompensas?

Hay personas que son especialmente sensibles al castigo; es decir, que están más motivadas por evitar consecuencias negativas que por conseguir otras positivas. Otras, en cambio, funcionan de forma totalmente contraria. Esto no quiere decir que sean excluyentes: todas las personas están felices cuando ocurre algo positivo, y a nadie le gusta que le ocurra nada malo.

Sin embargo, esta preferencia existe, y viene determinada por el cerebro. Es a lo que se denomina Sistema de Inhibición Conductual (BIS) y Sistema de Activación Conductual (BAS), presentes en todas las personas (Gray, 1981). A pesar de que depende de la situación, todos tenemos una tendencia. Por ejemplo, cuando alguien ofrece una recompensa sin ningún tipo de consecuencia negativa, nadie la rechazaría. No obstante, ante situaciones más complejas que tienen tanto pros como contras, la balanza no siempre se inclina hacia el mismo lado en función de quién las esté valorando.

Además de esta distinción básica, hay otros factores que entran en juego. A pesar de que se tratan de motivaciones menos sencillas, también tienen su base en la psicología (Eysenck, 1970; Costa y McCrae, 1992), y nacen de la combinación de distintas características de las personas, como su nivel de emocionalidad ante las diversas situaciones o la orientación hacia los demás.
Así, se identifican cinco grandes grupos de motivaciones a las que apelan los ingenieros sociales para perpetrar sus ataques, a saber:

1. **Altruismo.** Es el deseo de ayudar a otras personas. Un supuesto compañero que se encuentra en un apuro, una persona con las manos llenas que parece querer entrar en la oficina, una petición de ayuda directa para una buena causa... Cualquiera de estos pretextos puede ser utilizado para llevar a cabo un engaño, en el que caerán más aquellas personas con una mayor orientación hacia los demás.
2. **Temor.** Infundir miedo es una de las técnicas preferidas por los delincuentes, y tiene que ver con lo anteriormente mencionado sobre la sensibilidad al castigo. Solo hay que introducir en el mensaje una consecuencia indeseable en caso de que no se sigan las instrucciones para que un gran porcentaje de personas se plantee, como poco, hacer caso de lo que se les dice.
3. **Curiosidad.** Se trata de apelar a la parte contraria: las recompensas. Solo con apelar a hechos curiosos o que puedan reportar algún tipo de beneficio basta para que se valore aceptar lo que se propone, como ofrecer algo gratis.
4. **Autoridad.** Hay personas para las que es muy importante seguir las normas y cumplir con peticiones directas de aquellas que tienen cierta autoridad. La obediencia a este tipo de figuras es algo natural para muchos, lo que hace fácil ser víctima de un ataque en el que se suplante la identidad de alguna de ellas.
5. **Autoestima.** Querer preservar nuestro sentimiento de valía es algo importante para todos, si bien más para unas personas que para otras. Por eso, cuando alguien reconoce nuestras aptitudes o, por el contrario, sentimos que las atacan, nace una necesidad de sacar a relucir lo mucho que valemos. Esto hace que se abra un nuevo vector de entrada a los ingenieros sociales que decidan utilizar este factor para conseguir sus objetivos.

Al igual que ocurre con el Sistema de Inhibición Conductual y el Sistema de Activación Conductual (la sensibilidad al castigo o al refuerzo, respectivamente), cada persona presentará una de estas vulnerabilidades en mayor medida, aunque tampoco quiere decir que no pueda presentar las demás.

Además de estas, existen una serie de técnicas empleadas para aumentar la **persuasión**; es decir, para aumentar las probabilidades de que el atacante consiga que la víctima actúe según sus planes. Estas técnicas las explica Cialdini en su libro Influencia: la Psicología de la Persuasión (1984), en el que él mismo admite: "Toda mi vida he sido un poco ingenuo. Desde que tengo memoria, me han engañado con facilidad los sermones de todo tipo de vendedores, recaudadores de fondos, representantes de empresas y similares. (...) Con una frecuencia inquietante, siempre me he encontrado en posesión de alguna suscripción a revistas no deseadas o con entradas para fiestas de los trabajadores de mantenimiento". Normalmente se utilizan como apoyo a las anteriores, y son:

1. **Simpatía.** Tendemos a aceptar las peticiones de aquellos que nos caen bien, por lo que, en muchas ocasiones, los atacantes tratarán de causar una buena impresión en la víctima.
2. **Reciprocidad.** "Hoy por ti, mañana por mí" es un mantra muy extendido entre la población, hasta el punto de ser casi una norma no escrita. Por eso, cuando alguien hace algo por nosotros, nos sentimos obligados a corresponder de alguna forma.
3. **Compromiso.** Mostrar un compromiso o, al menos, una previa actitud favorable hacia lo que se pide, hace que las probabilidades de actuar en consecuencia aumenten.
4. **Sanción social.** Ante situaciones de incertidumbre, cuando no sabemos qué hacer, nos fijamos en el comportamiento de los demás. Esto es porque buscamos ser aprobados por otras personas, por lo que, si nos presentan una petición que socialmente estaría bien vista (como ayudar a alguien), es más probable que aceptemos.
5. **Autoridad.** Ya se ha comentado anteriormente: cuando la petición proviene de alguien con cierta autoridad sobre nosotros, tenderemos a obedecer. Esto es algo que ya Milgram, en 1963, estudió en su laboratorio. El experimento consistió en pedir a los participantes que proporcionaran descargas eléctricas, cada vez de mayor voltaje, a otra persona si no contestaba correctamente a las preguntas que se le realizaban. Las descargas no eran reales, pero esto es algo que los participantes no sabían. Incluso cuando el supuesto voltaje era tan alto como para amenazar la vida de la otra persona, la mayor parte de los participantes aplicó la descarga cuando la figura de autoridad (el responsable del experimento) se lo pidió.
6. **Escasez.** Cuando nos ofrecen algo durante un tiempo limitado, muchas personas sienten el impulso de hacerse con ello mientras aún pueden. Esto es porque no quieren quedarse sin ello más adelante, o porque buscan formar parte de ese círculo exclusivo que se ha hecho con el producto. En cualquier caso, está claro que las probabilidades de actuar según nos piden aumenta en el momento en el que nos ponen un plazo para ello.

A todas estas reglas y características personales es preciso sumarles algo más: la situación en la que se encuentra cada uno. Si bien es un tema a tratar en posteriores análisis, cabe destacar que el entorno tiene una gran influencia en las personas, ya que nuestra capacidad de razonamiento no es igual bajo una situación de estrés que en una distendida, por ejemplo.

¿Estamos preparados?

Los ingenieros sociales son conscientes de las diferentes técnicas y de nuestras vulnerabilidades, aprovechándose de ellas para conseguir sus objetivos. Por esa razón es importante que nos conozcamos a nosotros mismos para poder detectar en qué tipo de situaciones podemos estar más expuestos a un engaño.

No se trata de una solución fácil, mucho menos en el plano organizacional, en el que muchas personas aún desconocen el alcance y los peligros de la ingeniería social. Sin embargo, de lo que no cabe duda es de que los enfoques actuales no son suficientes para frenar el avance de estos ataques, y esto se debe al bajo nivel de personalización de los programas de concienciación.

Tal y como se ha explicado a lo largo del documento, no todas las personas tienen las mismas motivaciones. Por esta razón se hace necesario un programa que atienda a las necesidades de cada individuo de forma particular y personalizada.

Concienciación personalizada, simulaciones dirigidas, capacitación sobre cómo funciona la ingeniería social y cómo podemos protegernos cada uno de nosotros conociendo nuestras propias vulnerabilidades... ese es el camino hacia el éxito si queremos ir un paso por delante de los atacantes.

Solo así se podremos activar nuestros firewalls humanos, protegiendo tanto nuestra información personal como la de la organización.

Sobre Kymatio

Kymatio es una solución SaaS que automatiza la concienciación de los empleados y la evaluación de su estado de alerta de forma desatendida y personalizada, al tiempo que proporciona una herramienta de gestión de riesgo asociado al elemento humano, con métricas, evolución en el tiempo y planes de acción.

Utilizando la neuropsicología y la ciberseguridad como base de su tecnología, la IA de Kymatio interactúa con las personas, ofreciéndoles una concienciación personalizada y adecuada a sus necesidades, manteniendo el nivel de alerta y fortaleciendo las áreas en las que pueden ser más vulnerables.

Al mismo tiempo, proporciona a las organizaciones visibilidad en tiempo real sobre el riesgo humano en función de distintas métricas como el nivel de concienciación, las funciones y acceso a la información, el nivel de bienestar, respuesta a simulaciones o análisis de cuentas expuestas en brechas.

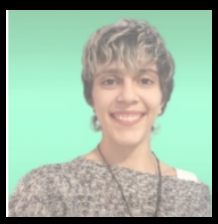
Para saber más, contacta con nosotros en **contact@kymatio.com** o pídenos una reunión en **https://calendly.com/kymatio**

Sobre las autoras

Andrea Zamorano
https://www.linkedin.com/in/andrea-zamorano/

Cyberpsychology Manager en Kymatio, investiga el lado humano de la ciberseguridad y desarrolla los algoritmos necesarios para que la plataforma sea capaz de medir con precisión los factores implicados, de forma que se pueda evaluar el riesgo y presentar las recomendaciones personalizadas en función de las necesidades de cada uno. También es docente en la Escuela de Inteligencia Económica de la UAM (La_SEI) como experta en perfilado indirecto de personalidad. Es psicóloga de formación, habiendo estudiado en la Universidad Autónoma de Madrid, y posteriormente se graduó del Máster en Inteligencia Económica y Relaciones Internacionales por La_SEI. También cuenta con un título de Experto en Organización y Recursos Humanos por la Universidad Autónoma de Madrid.

Sara Dorado
https://www.linkedin.com/in/sara-dorado/



Trabaja como Neurostrategist en Kymatio, desarrollando la base científica que sustenta la validez y efectividad de la herramienta destinada a detectar las vulnerabilidades y necesidades personalizadas de los usuarios. Además, también es experta en perfilado indirecto de la personalidad y analista de inteligencia en la Escuela de Inteligencia Económica (La_SEI), donde también hace funciones de docencia. Se graduó en psicología por la Universidad Autónoma de Madrid (UAM) y completó sus estudios con el Máster en Análisis e Investigación Criminal por el Instituto de Ciencias Forenses y de la Seguridad (ICFS).

Referencias

- ACCISI. (2018). Seguridad informática-Hacking ético. Conocer el ataque para una mejor defensa (4ª edición). Barcelona: Ediciones Eni.
- Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Four Most Famous Cyber Attacks for Financial Gains. International Journal of Engineering and Advanced Technology, 9(2), 2131-2139.
- CERT Insider Threat Center. (2013, September 30). The Latest CERT Research of Unintentional Insider Threats: Social Engineering. Software Engineering Institute, Carnegie Mellon University. Retrieved from: https://insights.sei.cmu.edu/insider-threat/2013/09/-the-latest-cert-research-of-unintentional-insider-threats-social-engineering.html
- Costa, P. T., y McCrae, R. R. (1992). Four ways five factors are basic. Personality and individual differences, 13(6), 653-665. doi: 10.1016/0191-8869(92)90236-I
- Dey, P. K. (2016). Prashant's algorithm for password management systems. International Journal of Engineering Science, 2424.
- Eysenck, H. J. (1970). The structure of human personality (3.ª Ed.). Londres: Mathuen.
- Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18.
- Gray, J. A. (1981): A critique of Eysenck's theory of personality. En A model for personality (pp. 246-276). Berlin: Springer.
- Gupta, S., Singhal, A., & Kapoor, A. (2016) A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA2016), pp. 537-540. Doi: 10.1109/CCAA.2016.7813778.
- Heikkinen, S. (2006). Social engineering in the world of emerging communication technologies. In Proceedings of Wireless World Research Forum (pp. 1-10).
- Hinson, G. (2008). Social engineering techniques, risks, and controls. EDPAC: The EDP Audit, Control, and Security Newsletter, 37(4-5), 32-46.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
- Milgram, S. (1963). Behavioral study of obedience. The Journal of abnormal and social psychology, 67(4), 371.
- Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. Indianapolis: John Wiley & Sons.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209.
- Ollmann, G. (2007). The vishing guide. Retrieved from InfoSec Writers: http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf
- Ponemon Institute (2020). Seventh Annual Study: Is Your Company Ready for a Big Data Breach?
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. Doi: 10.3390/fi11040089
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.