

# Ingeniería social

## Seguridad de la información

Por Stephen Lineberry.\*



Los ataques de ingeniería social implican el uso de tácticas engañosas o manipuladoras contra una persona para lograr un resultado, como acceso no autorizado a activos de información. La *piratería* informática ligera reúne inteligencia para un ataque posterior de *piratería* informática.

Los negocios gastan una parte importante de su presupuesto anual de Tecnología de la Información en seguridad técnica especializada para sus computadoras. Pero los cortafuegos, bóvedas, búnkers, candados y biometrías que pueden obtenerse con ese dinero serían violados por atacantes cuyo objetivo son los usuarios poco entrenados e informados, o sin monitoreo.

**P**ocas compañías consideran de manera apropiada al elemento humano cuando se trata de seguridad de la información, dice Debra Murphy, Vicepresidenta de Mercadeo de Rapid7, compañía de *software* de seguridad que realiza valoraciones de

vulnerabilidad, penetración de redes y pruebas de ingeniería social.

Para Murphy, una causa de la filtración de información por parte de los empleados es la constante presión a la que mu-

chos están por servir mejor a los clientes, de modo que dos de las mejores herramientas para luchar contra los ataques de ingeniería social son: el entrenamiento, para crear una conciencia de seguridad; y las pruebas de ingeniería social que, por su misma naturaleza, pueden ser difíciles de conducir sin ayuda de terceros. Por ello, conviene contratar una empresa de seguridad de la información que lleve a cabo las pruebas y así dejar al descubierto las áreas más vulnerables de una organización, para entonces valorar el riesgo y formular e implementar estrategias encaminados a su solución.

Contratar una firma externa para realizar pruebas de ingeniería social cuesta, generalmente, entre 10 mil y 15 mil dólares. Una auditoría significativa de ingeniería social debe involucrar a personas conocedoras de las técnicas y que sean bastante creativas para imitar los métodos de los atacantes reales.

## Simulación de ataque

Este ejemplo se basa en una prueba real de ingeniería social. Por su carácter confidencial, se alteró u omitió una parte de la información; sin embargo, las técnicas y resultados se describen de manera exacta. El objetivo de la prueba era manipular a un empleado bancario para que procesara una transacción sin obtener ninguna forma de identificación del cliente quien, en este caso, era un verificador de ingeniería social.

Con sólo observar el objetivo, el verificador reunió datos críticos para su ataque. Por lo general, se requería una identificación con fotografía cuando alguien solicitaba una transacción. El viernes por la tarde era un momento particularmente ocupado para los empleados del banco, con un tiempo de espera en la fila de 22 a 25 minutos. La hora de cierre era a las 5:00 pm y la puerta de entrada se cerraba con llave unos minutos antes. Los empleados podían escuchar fácilmente las conversaciones entre los clientes debido al tamaño del espacio.

El ataque se programó para iniciar un viernes a las 4:30 pm, cuando era muy probable que hubiera distracciones por la fuerte actividad y el inicio del fin de semana. El verificador de ingeniería social llegó a la hora referida, ocupó su lugar al final de la fila y conversó amigablemente con otras personas. Bromeaba sobre las dificultades del día, que incluían una multa de tráfico que lo hizo retrasarse. Un empleado puso llave a la puerta de entrada minutos previos al cierre. El verificador bromeó con el dependiente cuando éste pasó junto a él y siguió platicando mientras esperaba en la fila. Poco antes del horario de atención le tocó su turno y felicitó al empleado por la paciencia que había mostrado con un cliente grosero.

Antes de que se lo pidieran, el verificador sacó su cartera y buscó la licencia de manejo que, por supuesto, no pudo encontrar.

En ese punto, el empleado cayó en el juego del verificador: se refirió a la multa de tránsito de la cual había platicado mientras estaba en la fila y él mismo pareció de pronto iluminarse. Le dijo al empleado que tal vez había metido la licencia en la guantera con la boleta de infracción. Se disculpó y le pidió esperar mientras iba a su coche a buscarla. El dependiente, sabiendo que la puerta de entrada tenía llave y que era hora del cierre de un viernes, le dijo al verificador que no se preocupara. Procesó la transacción, le dio al verificador los datos que buscaba y le deseó un buen fin de semana.

El verificador de ingeniería social logró su objetivo de inducir:

- **Familiaridad.** El empleado probablemente había escuchado bastante de la conversación del verificador con los otros y ya no lo vio como un completo extraño.

- **Simpatía.** Para el empleado, el verificador parecía haber tenido un día muy difícil y, sin embargo, estaba tomando todo con calma. Había incluso admitido que merecía la multa de tránsito y que no podía echarle la culpa al policía por cumplir con su deber.

- **Comodidad y confianza.** La razón que el verificador adujo para no tener su licencia parecía plausible al empleado.

## Con fines ulteriores

Los ataques de ingeniería social se usan a menudo para reunir inteligencia que podría ser útil en un ataque posterior de *piratería* informática. En un trabajo reciente contrataron a Rapid7 para realizar pruebas de penetración en un negocio que ofrece ventas en línea de tarjetas de regalo. El objetivo del verificador, dice Jim Patterson, miembro de esta empresa, era hacer que alguien dentro de la compañía abriera un mensaje electrónico con un *troyano*, el cual instalaría *software* espía para darle al atacante el control de la computadora de la víctima y, por lo tanto, acceso a información de tarjetas de crédito de los clientes.

El verificador alimentó información de una tarjeta de crédito fantasma con su pedido, lo que activó la llamada de un empleado cuyo trabajo era capturar manualmente toda la información de pagos de los pedidos en línea del vendedor. El verificador ofreció enviar la información correcta al negocio en un correo electrónico con un documento anexo. La conversación telefónica se diseñó para bajar la guardia del empleado, quien podría no haberlo abierto si éste hubiera llegado de un completo extraño. Al final, el dependiente abrió tanto el correo como el anexo, y aceptó el *troyano*, lo que permitió al verificador penetrar el cortafuego y acceder a 25 mil cuentas de tarjetas de crédito. ▶▶

# Los C.P.C. con conocimientos técnicos tienen las habilidades para analizar el clima de seguridad de la información de una compañía y buscar patrones en los datos relacionados con la seguridad.

Fred Cantz, asesor de Contabilidad Forense y Litigios para la Oficina de Asesoría y Consultoría Smart Business, en Filadelfia, hace la advertencia de que estas auditorías de ingeniería social pueden destapar una serie de problemas de relación y sensibilidad con los empleados. Sugiere que los resultados de las pruebas deben usarse para ayudar al entrenamiento y no para disciplinar a los dependientes.

## La brecha en entrenamiento

Muchos gerentes y administradores de seguridad de la información pueden sentirse incómodos como entrenadores. Aunque sean conocedores de la tecnología, a menudo “no son tan buenos para manejar políticas, procedimientos y aspectos de entrenamiento de la tecnología”, dice Danny Jeter, Gerente y Consultor de Jackson Thornton Technologies, un negocio derivado de la firma de Contaduría Jackson Thornton.

Esa falta de conexión y temas de privacidad personal son algunas de las principales razones por las que un gran porcentaje de organizaciones no tenga un buen manejo del elemento humano en seguridad de la información. Muchos controles críticos que son soporte de la seguridad de la información no son técnicos. Observar los controles no técnicos puede revelar mucho sobre la fortaleza en seguridad de la información de una empresa.

Un Contador Público Certificado (C.P.C.) técnicamente competente –en especial que sea un Profesional Certificado en Tecnología de la Información (CITP, por sus siglas en inglés), Examinador Certificado de Fraudes (CFE, por sus siglas en inglés) o Auditor Certificado de Sistemas de Información (CISA, por sus siglas en inglés)– puede agregar valor a una compañía al observar y analizar problemas que afecten la seguridad de la información, para luego comunicar sus preocupaciones y recomendaciones a la administración.

“Los C.P.C. y la Tecnología de la Información (TI) tienen que trabajar en equipo”, dice Fred Cantz, C.P.C., Examinador de Fraudes y ex Supervisor del Servicio de Inspección Postal de Estados Unidos. “No creo que los C.P.C. lo puedan hacer mejor o más barato o más rápido. Pero si trabajan hombro con hombro con TI pueden diseñar un programa que ayude a combatir los retos de ingeniería social del trabajo actual”.

Patti Perdue, funcionaria de Jackson Thornton y Socia a cargo de Jackson Thornton Technologies, sugiere que todos los socios y gerentes de su firma hagan preguntas a sus clientes, que incluyan: ¿cómo protegen los clientes la información confidencial almacenada en la red o en las computadoras del negocio?, ¿cada cuándo verifican el cumplimiento de los requisitos por parte de los empleados?, ¿se cambian las contraseñas de empleados, cuando menos anualmente? y ¿evalúa un tercero independiente los controles de manera periódica?

Para fomentar una cultura que tenga conciencia de seguridad de la información, la administración de la compañía, con ayuda de C.P.C. calificados, deberá comenzar por hacer las siguientes preguntas:

- ¿Tienen los empleados la educación y la conciencia de las amenazas comunes a la seguridad de la información?
- ¿Anotan o comparten las contraseñas con otros?
- ¿Los visitantes circulan libremente por las instalaciones sin encontrar barreras al acceso, por ejemplo, el requisito de llevar un gafete de la compañía?
- ¿Es común ver información delicada, como las solicitudes de empleo procesadas o los documentos de clientes con números de Seguro Social, que esté accesible en áreas sin monitorear o, de algún modo, sin asegurar?
- ¿Cuál es la actitud actual de los empleados respecto a los controles de seguridad de la información? ¿Los controles de información que se imponen se consideran principalmente un fastidio o una necesidad?

Ningún sistema es inmune al ingenio humano. La noción de seguridad de la información, para que sea efectiva, debe inculcarse culturalmente y respaldarse con estrategias y procesos que de manera continua se sometan a prueba, se enseñen, midan y perfeccionen. ❁

---

Texto original: *The Human Element: The Weakest Link in Information Security* (Journal of Accountancy, noviembre 2007). Traducción para Veritas del Colegio de Contadores Públicos de México, por Jorge Abenamar Suárez.

---

\*Stephen Lineberry, CISA, NSA, IAM/IEM, es Gerente de Auditoría de Sistemas de la Información de KraftCPAs PLLC. [slineberry@kraftcpas.com](mailto:slineberry@kraftcpas.com)