Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

TÓPICOS DE SEGURIDAD PRIVADA

Rodrigo Velarde

1. CONCIENTIZACIÓN DE LA SEGURIDAD

El 17 de junio asistí al Primer Foro de "Nuevo León vs. La Delincuencia" organizado por las Cámaras Locales y el Gobierno del Estado. Con conferencistas de gran nivel, destacó Leoluca Orlando, exalcalde de Palermo, capital de Sicilia, lugar relacionado con *La Mafia*, organización criminal famosa por películas pero que existe y es un problema en la realidad.

Leoluca logró combatir exitosamente a *la Mafia*, el modelo que propuso para combatir a la Mafia es el de una carreta de dos ruedas, la rueda de la *Legalidad* (combate a la ilegalidad: policías, fiscales y jueces) y la rueda de la *Cultura* (vs. la ilegalidad).

Las dos ruedas deben de girar a la misma velocidad, de otra manera la carreta se estará moviendo en círculos. Si solo la rueda del combate gira, se podría parar el crimen no-organizado (ladrones y asaltantes callejeros) pero no a las organizaciones organizadas como la Mafia, el narcotráfico, la piratería y el terrorismo; un ejemplo de esto es el programa "Tolerancia Cero" de Rudolph Guiliani. Si solo la rueda de la cultura gira, existe el riesgo de organizar un concierto de excelente música en honor a un narcotraficante.

Cada sistema criminal necesita que no se hable de ellos, necesitan de mil personas con pistolas y un millón de personas que vivan en "la zona gris" (no hablan, no escuchan, no ven).

Antes, cuando los poco turistas que llegaban a Sicilia le preguntaban a un taxista sobre la Mafia, la respuesta era "la Mafia es un invento de los medios... aquí no existe eso".

¿Recuerdan en el 2001 y 2002 a nuestros altos funcionarios de gobierno estatal con estas declaraciones sobre ejecuciones relacionadas al narcotráfico? "son hechos aislados", "(el problema no es tan grave porque) solo se matan entre ellos", eso es vivir en la "zona gris".

La Mafia, como todas las organizaciones criminales (terrorismo, narcotráfico, etc.) son sistemas que corrompen los valores de su región. Utiliza los valores como justificación para robar, matar o traficar, los valores que corrompe la Mafia Siciliana: la familia y el honor. El terrorismo Islámico: la religión, el terrorismo Vasco o Norirlandés: el orgullo nacional, el Nazismo alemán: el respeto a las leyes (de pureza racial), ¿cuál es el valor mexicano que el crimen organizado corrompe? el valor del éxito (por cualquier medio) "el que no tranza no avanza... a mi no me van a detener".

Una vez que Leoluca empezó a mover la rueda de la *Legalidad*, gracias al trabajo de policías y jueces valientes y honestos, se puso a trabajar en la mover la rueda de la cultura, ¿como lo logró?

La paz y la legalidad son demasiado importantes para ser confiadas solamente a las fuerza militares, policíacas y judiciales, necesitamos promover con nuestras familias, amigos y compañeros, pero sobre todo con los niños, que el respeto a la ley debe ser una forma de vida, que "la legalidad es alegre y conveniente", salirnos de la "zona gris", preguntarnos a nosotros y nuestras familias todos los días: "¿que hiciste hoy para combatir al crimen?"

Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

Ahora cuando un turista (que hay muchos más) le pregunta a un taxista, la respuesta es "…lo voy a llevar a conocer las casas de los mafiosos". Las escuelas privadas niegan la inscripción a niños de familias mafiosas reconocidas.

Preguntémonos todos los días: ¿qué hice hoy para combatir la ilegalidad (mafia, narcotráfico, corrupción, piratería)?

2. INGENIERÍA SOCIAL, CONTROLANDO EL FACTOR HUMANO DE LA SEGURIDAD

Alguna persona o compañía (llamémosle "el atacante") quiere obtener cualquiera de estas cosas de su empresa:

- Planes para el novedoso producto próximo a lanzarse;
- Base de datos de clientes con sus datos de contacto e historial de consumos;
- Estrategias legales;
- Información de grandes adquisiciones o alianzas;
- Acceso al servicio telefónico para sacar llamadas de larga distancia gratis; o
- Datos personales de los ejecutivos para usarlos maliciosamente mas adelante.

¿Algo de esto lo detendrá?

- *Firewall* corporativo;
- Dispositivos de autentificación;
- Encriptación;
- Nombres codificados de servidores para dificultar el que un intruso determine que servidor puede contener la información; o
- Control de acceso restringido a nuestros edificios.

La tecnología es importante y necesaria dentro del esquema de seguridad de la información de una empresa, este esquema o cadena se completa con el eslabón del factor humano; o sea, las prácticas de seguridad llevadas a cabo por personas, no por tecnología, ¿cuál es el eslabón más débil de esta cadena? el eslabón humano. No hay tecnología en el mundo que evite un ataque de ingeniería social; debido a ello, la seguridad no debe verse como un producto sino un proceso. No es un problema de tecnología, es un problema de administración y de gente, la ingeniería social es exitosa cuando las personas no siguen las buenas prácticas de seguridad.

Una definición simple de un ingeniero social es: aquél que obtiene información sensible de una compañía haciéndose pasar por otra persona para simplemente pedir la información.

Las compañías que se dedican a conducir pruebas de penetración reportan que sus intentos de ingresar a los sistemas computacionales por medio de la ingeniería social son casi 100% exitosos.

La única manera efectiva de mitigar la amenaza de la ingeniería social es a través de la concientización combinado con reglamentos que regulen el comportamiento de los empleados. El primer paso es reconocer que existe gente sin escrúpulos que usarán el engaño para manipularnos psicológicamente y obtener la información que buscan.

Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

Las seis variantes más usadas por los ingenieros sociales:

1) Autoridad

El atacante tratará de hacerse pasar por un ejecutivo de alto nivel o alguien que trabaja para un ejecutivo de alto nivel.

2) Caer bien

A través de la conversación, el atacante logra conocer un pasatiempo o interés de la victima o podrá decir que es del mismo pueblo o escuela, o tener los mismos objetivos o ideas. El atacante también tratará de imitar el comportamiento de sus víctimas, para obtener empatía a través de la similitud.

3) Reciprocidad

Se recibe llamada de un supuesto empleado de informática para avisarnos que varias máquinas han sido infectadas por un nuevo virus y nos da información de cómo prevenirlo; hecho esto, la persona nos pide que probemos un nuevo software que sirve para cambiar contraseñas. Como nos acaban de ayudar, se nos dificulta el negarnos a ayudar de vuelta y caemos en la trampa de dar nuestras contraseñas. Técnica usada por la gente que pide limosna pero primero te da un pequeño obsequio (estampita de la virgen).

4) Consistencia

El atacante contacta a un nuevo empleado y le recuerda el compromiso que tiene de cumplir con la Política de Seguridad de la Información. Después de discutir varias prácticas de seguridad, el atacante pregunta al empleado por su contraseña para “verificar el cumplimiento con la práctica de escoger contraseñas difíciles de adivinar”, la víctima le contesta pues quiere cumplir con las políticas de seguridad.

5) Validación social

El atacante llama diciendo que está conduciendo una encuesta y nombra a otras personas en el departamento que ya han cooperado con él, la víctima, creyendo que la cooperación por otros valida la autenticidad del pedido, acuerda cooperar. El solicitante pregunta una serie de datos entre ellos su usuario y contraseña.

6) Escasez

El atacante envía correos afirmando que las primeras 100 personas que se registren en el nuevo sitio *web* de la compañía ganarán boletos gratis para la nueva gran película, al entrar al sitio se pide que proporcione su correo y que escoja un contraseñas. Es usual que los correos de compañías sean los mismos que los usuario y la mayoría de la gente por comodidad usan el misma contraseña en todos los sistemas.

Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

Para evitar lo anterior, procedimientos para ayudar al empleado que recibe una solicitud por cualquier medio como teléfono, correo o fax para determinar si la solicitud y la persona haciéndola, son legítimos.

Verificar que la persona es quien dice ser y su estatus laboral:

- Identificador de llamadas: verificar si la llamada es interna y que el nombre y extensión concuerden con la identidad del solicitante;
- Regresar la llamada: colgar y buscar el nombre del solicitante en el directorio de la compañía, hablarle y verificar la historia;
- Confirmación de su conocido: colgar y preguntar al jefe directo del solicitante o algún empleado de su confianza por la identidad y estatus laboral del solicitante;
- Reconocimiento de voz: no acceda a la petición si no reconoce la voz de la persona; y
- Presencia: solo acceda a la petición si se lo piden en persona y te muestran identificación vigente de la empresa.

Determinar que la persona está autorizada a recibir la información específica o que puede hablar para solicitar cierta acción nuestra ("*need-to-know*"):

- Revisar listas de usuarios autorizados para esa información;
- Solicita a su Gerente o al Gerente del solicitante por la autorización para cumplir con la solicitud.
- Preguntar al dueño de la información si el solicitante tiene el "*need-to-know*";
- Verificar que la supuesta compañía del solicitante tenga una relación estratégica, de socio o proveedor con nuestra empresa;
- Verificar la identidad y estatus laboral del solicitante hablando a su supuesta empresa; y
- Verificar que el solicitante haya firmado un contrato de confidencialidad con nuestra empresa.

FUENTE:

Kevin D. Mitnick, *"El Arte de la Decepción"*.

3. ¿QUÉ ES MEJOR, LA DISUASIÓN O LA DETECCIÓN?

En una exposición de equipos de la Sociedad Americana para la Seguridad Industrial (ASIS por sus siglas en Inglés) se podían encontrar distribuidores de equipos enfocados al robustecimiento de la seguridad, entre ellos sobresalía un proveedor que ofrecía cámaras antigrafitti. Estas cámaras detectan los movimientos propios de la elaboración de graffiti, toman fotografías del evento y tienen la capacidad de enviarlas vía correo electrónico a la policía, pueden a su vez enviar mensajes de texto a teléfonos celulares dando aviso del evento.

Los efectos adversos del graffiti sobre los negocios son tremendos, llegando a 12 billones de dólares en Estados Unidos, el vandalismo hace sentir al cliente que el lugar es inseguro y que se encuentra deteriorado.

Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

Mientras pareciera que esta tecnología pudiera solucionar este grave problema de vandalismo, la realidad es que las cámaras son malas para disuadir a los criminales; es decir, el acto vandálico tiene que suceder para que la cámara lleve a cabo su función, al final del día, las cámaras antigrafiti no servirán para detener el crimen.

Existe una disciplina llamada, *Criminal Prevention Through Environmental Design* (Prevención del Delito a través de Diseño Ambiental) por sus siglas en inglés CPTED, cuya finalidad es la construcción de espacios que reduzcan la probabilidad de actividad criminal. Esto mediante la iluminación, señalización u otros métodos. Retomando el ejemplo del graffiti, la creación de superficies oscuras, dispares o de poca lubricidad de tal forma que sean inadecuadas para el graffiti, tiende a disuadir a los criminales.

Si la disuasión es más eficiente para disminuir los incidentes criminales, ¿por qué la detección es tan popular?

Desafortunadamente los métodos de disuasión son más complicados de entender y ejecutar que los de detección, ¿qué es más sencillo: apuntar las cámaras hacia los muros y esperar mensajes de texto? o ¿evaluar espacios por nivel de riesgo y aplicar la mezcla idónea de técnicas para detener y limpiar el graffiti?

La disuasión es menos satisfactoria para el ser humano que la detección desde un punto de vista psicológico, especialmente en el clima actual de (in)seguridad, el instinto punitivo parece, de alguna manera, más placentero.

Nos gusta el crimen y el castigo, se nos dificulta ver que la prevención es más efectiva que la detección y el castigo, tal vez ha llegado el momento de invertir menos en perseguir criminales y más en perseguir al crimen.

4. ADMINISTRACIÓN DE LA SEGURIDAD

En la última década en México (y desde antes en otros países) las empresas han cambiando su forma de ver a los Departamentos de Seguridad.

El Departamento de Seguridad (o de Prevención de Pérdidas o de Protección) ha dejado atrás la imagen de ser sólo un grupo de guardias, alarmas y cámaras, y ahora es percibido como un aliado para lograr los objetivos del negocio.

Los profesionistas de seguridad requieren interactuar con varias áreas, incluyendo las de sistemas electrónicos; de construcción de inmuebles; de desarrollo de políticas y procedimientos; de asuntos legales y laborales; de instalaciones y mantenimiento; de selección de personal; de logística; de ventas masivas; de cobranza; de auditoria; y de comunicación, entre otros.

Además de los conocimientos de seguridad, estos profesionistas deben poseer habilidades para la planeación, la negociación y la comunicación, también deben manejar la contabilidad, ya que sus unidades son vistas como centros de provecho a través de la documentación de ahorros por reducción de robos, daños y respuesta a emergencias.

Archivos de Criminología, Criminalística y Seguridad Privada

Reserva de Derechos: 04-2011-040811150700-102
ISSN 2007-2023
Director: Wael Sarwat Hikal Carreón

Las estrategias básicas de prevención:

- Seguridad física (barreras, controles de acceso, CCTV, alarmas, oficiales de seguridad);
- Capacitación y concientización de colaboradores;
- Investigación de incidentes y persecución jurídica de ofensores; y
- Administración del riesgo (de delitos).

En la medida que se dé más énfasis a las medidas preventivas (planeación, procedimientos, concientización, capacitación) sobre las reactivas (manejo de incidentes, investigación), los resultados serán más efectivos y los ahorros mayores.

En lo personal, considero que las herramientas principales del área son la capacitación, concientización y comunicación para lograr una de las misiones principales del área: “que cada colaborador sea quien brinde y supervise la seguridad de la empresa”.