Fraude informático: preguntas y respuestas con Muna Dora Buchahin Abulhosn

Mencionar su nombre significa indagar entre los "pesos pesados" del fraude en el ámbito de las tecnologías de la información y las comunicaciones. A ella nada se le escapa.

Sara Gallardo M.

A Muna Dora Buchahin Abulhosn, abogada y doctora en Derecho, entrevistadora forense certificada, especialista en anticorrupción, conferencista por todo el mundo, perito auxiliar en Criminología del Tribunal Superior de Justicia del Distrito Federal en México, con todas las acreditaciones internacionales posibles, docente y autora del libro "Auditoría forense, delitos contra la administración pública", no le cabe un título más en su hoja de vida. Son tantos, que citarlos todos le quitaría espacio a la esencia de esta entrevista: compartir con los lectores su conocimiento y vasta experiencia al frente de 450 auditorías en los ámbitos público y privado y en más de 243

dictámenes de casos presentados ante autoridades penales y administrativas en México, país donde reside y es testigo de su arduo trajinar por los laberintos de la seguridad de la información.

La más reciente noticia en su laureado camino es el premio ACFE: "*Certified Fraud Examiner of the Year Award 2016*", entre los Certified Fraud Examiner – CFE-, Examinador Certificado de Fraude, de 208 capítulos en el mundo.

Semejante perfil, no podía producir nada distinto a una serie de respuestas al cuestionario enviado por correo electrónico, acompañadas de cifras, gráficos y conceptos.

Revista Sistemas: ¿Cuál es la definición que motiva el actuar de un profesional certificado en fraude?

Muna Dora Buchahin Abulhosn: es un especialista en la prevención, detección, disuasión y la investigación de fraude ocupacional, entendido como *el uso de la propia ocupación para el enriquecimiento personal, a través del mal uso o el uso indebido de los recursos o activos de la organización, con la intencionalidad de cometer un acto ilícito.* El "Manual del Examinador" lo define como: "... todos aquellos medios complejos que el ingenio humano puede concebir y a los que recurre un individuo para sacar ventaja de otro, por medio de falsas sugerencias o por supresión de la verdad. Incluye toda sorpresa, truco, astucia u ocultamiento, y cualquier forma injusta por la que el otro es engañado". Por lo tanto, el entorno y la importancia de su actividad lo obligan a una actualización permanente para acreditar su *experticia*, las competencias y las habilidades forenses para cualquier tipo de investigación como especialista antifraude. Su actuación se rige con los más altos estándares de ética, conocimiento y experiencia que contemplan el dominio de diversas técnicas forenses, dado que el examinador de fraudes certificado (CFE) se integra en cualquier organización pública o privada, independientemente de las distintas regulaciones legales a cada país.

RS: ¿Desde su experiencia, cuáles son los fraudes informáticos más comunes?

MDBA: los más recurrentes se vinculan con el llamado "robo de identidad" en sus diversas modalidades. A través de diferentes mecanismos como el envío de correos spam, donde se le solicita al destinatario con

un correo engañoso, acceder a una liga de un sitio "conocido seguro" (el cual en realidad es una copia del original), y cuyo propósito es que el usuario ingrese datos personales (usuario, contraseña, número de tarjeta bancaria, etc.), para que éstos sean robados y utilizados posteriormente para fines ilícitos, entre ellos el mercado negro o el robo o retiro de dinero de cuentas bancarias.

También sucede que a través del envío de correo spam, se puede anexar un archivo electrónico, de tipo PDF o video o cualquier otro de uso común. Una vez que el destinatario lo abre, puede descargar un archivo (*malware*) que se instala en la computadora y una vez instalado, puede estar enviando toda la información que el usuario teclea cuando visita sitios específicos, entre los más comunes referidos a bancos.

La sofisticación de las técnicas de los defraudadores para lograr mayor impacto en sus objetivos, es permanente. Existe una variación denominada *spear-phishing*, la cual realiza envíos de correos a personas específicas (está dirigido al ataque) y son envíos de remitentes o empresas que seguramente conoce el destinatario. Ante este escenario, es fácil que la víctima crea como válido el correo y proporcione la información solicitada, ingresando a las ligas que se indican en el correo o descargando un archivo puntual. El uso indebido de los datos personales es ahora un riesgo universal inminente, en un potencial mundo de fraudes cibernéticos que ha afectado a gran número de organizaciones y ciudadanos.

RS: ¿El ambiente de la tecnología móvil, la nube y otros desarrollos similares han hecho crecer el fraude?

MDBA: en el mundo globalizado se atrae el lado oscuro de los delitos cibernéticos. Según datos del *Informe 2016 de "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?,* publicado por el Banco Interamericano de Desarrollo (BID), de una población de 125 millones de habitantes en México, el 44% tiene acceso a internet (55 millones de personas), terreno abonado para el desarrollo colectivo, al generar comunicación y mayor información en tiempo real. Pero, son mayores los riesgos tanto para los usuarios como para las empresas, por la vulnerabilidad de los sistemas operativos de los dispositivos móviles (Android, IOs o Microsoft), y de programas que pueden robar información y transmitirla para fines ilícitos.

Los modelos de servicios en la nube, entre los que se cuentan: *Software como Servicio (Software as a service – SaaS-); Plataforma como servicio*

(Platform as a Service –PaaS-) o *Infraestructura como Servicio (Infrastructure as a Service –IaaS-),* también han presentado vulnerabilidades que los delincuentes informáticos han explotado. Muchas de ellas, por el descuido del usuario al dejar sesiones remotas abiertas o accediendo desde redes no seguras, lo cual es aprovechado para accesos no autorizados y robos de información.

RS: ¿Qué tipo de entrenamiento deben tener las personas y empresas para enfrentar el fraude informático?

MDBA: desde el más alto nivel organizacional, resulta imprescindible implementar una cultura de seguridad de la información, comunicar y sensibilizar a todo el personal en línea vertical y horizontal, y no estrictamente en el sentido de "seguridad informática", sino incluir una sensibilización permanente, vinculada en las distintas áreas y con un protocolo de alerta a los posibles riesgos y vulnerabilidades, en caso de un incidente o contingencia.

La capacitación debe centrarse en modelos de seguridad de la información y normas internacionales que permitan seguir un marco de referencia, como las ISO/IEC 27001 (estándar para la implementación de un sistema de gestión de la seguridad de la información), ISO 27017 (estándar para la aplicación de controles de seguridad de información en sistemas o servicios basados en computación en nube) e ISO 27032 (Guía sobre ciberseguridad), por mencionar algunas.

Es muy importante mantener comunicación constante interna entre el personal de la organización, para conocer la recurrencia y los *modus operandi* de los fraudes informáticos. Esto servirá como insumo para actualizar las políticas de seguridad o configuraciones específicas de sistemas o la infraestructura de la organización. Estas actualizaciones deben ser permanentes y alineadas a la organización.

Debo decir que en México existen grandes oportunidades de trabajo para aquellos jóvenes que deciden estudiar estas carreras profesionales, y que hay escasez de personal en esta materia. Se asegura un futuro promisorio y lleno de actividad intensa para los talentos.

Siga la entrevista completa en el siguiente link:
http://acis.org.co/portal/content/entrevista-muna-dora-buchahin-abulhosn

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Autora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res, empresa que supera los 1800 empleados; corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros universitarios y editora de esta revista.*