Entendiendo la inseguridad de la información

Jeimy J. Cano Ph.D

La inseguridad informática es la característica propia de los sistemas de información actuales. Pareciera que mientras más nos esforzamos en controlar y avanzar en el entendimiento de la inseguridad, nuevas y más desafiantes vulnerabilidades aparecen.

En este contexto, donde siempre estamos "un paso atrás" de las vulnerabilidades, establecer un esquema de gestión de seguridad de la información, se transforma en una búsqueda de patrones y posibilidades para reconocer la dinámica de la inseguridad informática, lo que nos permite alcanzar mayores niveles de confiabilidad, no de seguridad.

Cuando hablamos de gestión de la inseguridad informática, debemos no solamente considerar los aspectos técnicos, conocidos por los especialistas en seguridad de la información, sino conjugar la dinámica de la industria de la seguridad, la renovación constante de las vulnerabilidades del software y la psicología del individuo. En razón a lo anterior, se sugiere que dicha gestión debe ser esa iniciativa para descubrir y comprender algunas de las relaciones que se materializan al evidenciarse una falla de seguridad.

La industria de la seguridad de la información

Revisando el segundo capítulo titulado *The security industry*, del libro de Shostack y Stewart publicado por Addison Wesley en 2008, denominado *The New School of Information Security*, se presenta de manera clara y abierta la forma como la industria

se da a la tarea de vender la distinción de seguridad de la información, tanto en el tema de productos y servicios, así como en buenas prácticas, listas de chequeo y estándares.

Dicen los autores que la industria se apalanca en las siguientes estrategias para "vender" la distinción de seguridad de la información:

** Uso del miedo e incertidumbre para crear la sensación de que estamos en el filo del abismo.*
Esta estrategia busca generar inquietud en las organizaciones frente al tema de seguridad de la información para que vean en los productos y servicios una salida encaminada a alejarse del abismo que se les ha presentado. Si bien el miedo y la incertidumbre son propios de la inseguridad de la información, también es cierto que una adecuada administración de riesgos y una cultura de seguridad organizacional nos permiten mitigar y manejar la exposición natural a las vulnerabilidades propias de la tecnología.

** Productos de seguridad de la información que son expuestos a los intrusos para que intenten quebrarlos y cuando no lo hacen, se proclaman "imposibles de hackear".*
Esta manera de vender los productos exige al fabricante ofrecer un producto de alta calidad, pero generalmente las cantidades ofrecidas por violar el sistema o comprometerlo, no son lo suficientemente motivadoras para los "reales atacantes", por lo cual esta estrategia no siempre es muy confiable. Someterse al escrutinio de terceros es una buena estrategia, pero requiere un alto nivel de participación y calidad de los evaluadores del producto.

** Productos y servicios que son utilizados por una compañía específica o una entidad del gobierno, lo cual le ofrece al proveedor una visibilidad en el mercado.*
Esta forma de mercadear la seguridad de la información es muchas veces el resultado de procesos internos de las organizaciones que generalmente son desconocidos para los terceros. Es probable que acuerdos de licenciamiento, alianzas estratégicas o poca variedad de productos sean la razón por la cual se ha adquirido el producto. Para contar con esta referencia de confiabilidad y uso del producto, lo mejor es contactar directamente a la organización para conocer en detalle el tema de contratación y uso de la misma.

** Los servicios y productos son sometidos a evaluación en revistas populares de la industria, las cuales emiten conceptos sobre los mismos.*
Aparecer como uno de los productos evaluados en una revista reconocida en la industria de la seguridad de la in-

formación es en sí misma una manera de mercadear el producto. No interesa el resultado mismo de la evaluación, el sólo hecho de haber sido seleccionado como uno de los productos que se reconocen en el mercado, ya lo hace acreedor de un prestigio importante y ha logrado el objetivo de ser considerado como una de las opciones válidas por los futuros clientes.

** Se establecen y recomiendan por parte de los proveedores y organizaciones internacionales lista de chequeo, certificaciones de negocio y modelos de control que procuran salvaguardar a las organizaciones de los más importantes peligros en temas de seguridad de la información.*
Esta estrategia, basada en la orientación de la academia, acude a nuestro lado educacional y formativo, para sugerirnos que los estudios realizados por estas empresas nos permiten ver situaciones que van más allá de las prácticas actuales y que están alineadas con las tendencias internacionales, gracias a sus amplios esfuerzos y experiencia basada en sus trabajos con sus clientes. Muchas veces los resultados de estos estudios internos que adelantan estas organizaciones, muestran apartes de la realidad y tendencias que deben ser consideradas dentro de la dinámica de las organizaciones, pero no tomadas como estudios formales, basados en consideraciones estadísticas exigentes, datos confiables o similares.

** Los productos y servicios se encuentran alineados con las "buenas prácticas", las cuales representan lo que la industria y la práctica sugieren que es lo más adecuado.*
Comenta el autor que las "buenas prácticas" generalmente no toman en consideración las diferencias entre compañías, o más generalmente, entre industrias. Las "buenas prácticas" son esos discursos conceptuales que procuran establecer la dinámica propia de las organizaciones frente a sus necesidades particulares y no necesariamente son extrapolables a otras. Las "buenas prácticas", pueden ser buenas para unas organizaciones y no tan buenas para otras.

En conclusión, podemos comentar que las diferentes formas de vender la distinción de seguridad deben pasar por un filtro de evaluación de necesidades propias de la organización, la comprensión clara de la dinámica del negocio y las limitaciones propias de los productos, pues sólo así podemos advertir cómo la inseguridad de la información podrá sorprendernos, no para dejarnos "mal parados", sino para continuar aprendiendo que sólo mientras más la conocemos podemos avanzar en sistemas más confiables.

En este contexto la gestión de la seguridad debe seguirle la pista a la dinámica de la industria de la seguridad para avanzar en la comprensión de la realidad de los proveedores y sus tendencias, para ir afinando el olfato técnico hacia las soluciones más apropiadas para las organizaciones y su perfil de inseguridad de la información.

Inseguridad en las aplicaciones

De otra parte, revisando el libro de David Rice, denominado *Geekonomics. The real cost of insecure software,* nos encontramos con una serie de reflexiones del autor que nos muestran una realidad contundente sobre el costo de la inseguridad en el *software* y en las aplicaciones, y cómo los ataques a estos elementos son parte de la problemática desarrollada por el autor.

Revisando el capítulo tres titulado: *The power of weaknesses: Broken Windows and National Security*, nos encontramos con una pregunta interesante y cinco sugerencias que tratan de responder a dicho interrogante. La pregunta es: ¿Qué factores contribuyen a un crecimiento explosivo y exponencial de los ataques? Para ello, desarrolla cinco ideas al respecto, que trataremos de comentar brevemente, tanto en la posición del autor como en la práctica general de la seguridad informática.

Factor No.1. La velocidad es bendición y ruina.
Según el autor, incrementar la velocidad en la cual la gente y los negocios pueden tener las cosas, facilita de manera rápida y eficiente los métodos para cometer delitos o crímenes conocidos como fraudes o robos, ahora de una nueva forma. Esta afirmación es interesante y refuerza una vez más que las inversiones en seguridad informática son inversamente proporcionales a los datos. Es decir, mientras más volátil es la tecnología, en cuanto a sus nuevas funcionalidades y rápida obsolescencia, más eficiente se vuelve el intruso para materializar sus acciones y comprometer los datos. El no conocer el desarrollo tecnológico y estar sometido a la curva de aprendizaje para dominarlo, son factores claves para avanzar en el reconocimiento de la inseguridad tanto en las aplicaciones como en los servicios que ofrecen las organizaciones a sus clientes.

Factor No.2. Si el software hace más fácil y rápida la materialización de los delitos informáticos, la cantidad de dinero que se podría ganar en un mes, ahora sólo toma unos segundos.
Rice comenta que ahora nos enfrentamos al factor segundo, un simple incentivo financiero: ganar más dinero con menos esfuerzo. Es decir, la magnitud de las ganancias ilícitas, se están incrementando; existen can-

tidades enormes de dinero en forma electrónica que son susceptibles de fallas y asaltos que aún estamos por descubrir. Esta reflexión es desafiante y exigente al tiempo, si ahora los intrusos "saben" que requieren menos tiempo para tener dinero, pues la tecnología es su aliada; la pregunta es ¿qué estamos haciendo nosotros para hacerles la vida más difícil? Será que como a nosotros no nos ha pasado, ¿eso no ocurre?

Factor No.3. Otro factor que contribuye al explosivo crecimiento de los ataques es el volumen de vulnerabilidades reportadas en el software.
El autor afirma que estas vulnerabilidades ofrecen a los atacantes un sin fin de formas para explotar y vulnerar los sistemas de todos los tipos y sabores, desde aplicaciones corporativas como Oracle y PeopleSoft (ahora parte de Oracle), hasta computadores de uso en casa como Apple OS X y Windows. En este punto el autor dice que con este escenario, es difícil imaginar por qué no existen más personas involucradas con el cibercrimen. Este factor no sólo requiere un reclamo a los proveedores del *software* y sus estrategias de aseguramiento de calidad de *software*, sino a nosotros los usuarios que "no reportamos" los eventos que puedan ser extraños o fuera del funcionamiento normal. Los atacantes se valen de nuestra "ignorancia" para avanzar y generar la incertidumbre requerida para que sus acciones pasen desapercibidas.

Factor No.4. Las soluciones de seguridad para proteger el software de ciberataques son sustancialmente más complejas de configurar correctamente o requieren una importante cuota de "cuidado y alimentación" para asegurar su eficiencia.
El autor sugiere que la configuración y afinamiento permanente de los mecanismos de seguridad -particularmente habla de los *firewalls*-, exige una complejidad propia del mismo y conocimiento de las interacciones para mantenerlo funcionando adecuadamente. Esta afirmación de Rice, apunta precisamente al esfuerzo continuado que requiere la seguridad, a la constante evolución de las infraestructuras y a las maneras como los atacantes desafían las nuevas propuestas de seguridad y control. La inseguridad de la información es dinámica y parte de nuestra labor es tratar de seguir el rastro y por qué no, encontrarnos con ella para entenderla y desafiarla.

Factor No.5. El quinto factor es la falta de coordinación transnacional de los agentes gubernamentales para tratar el tema del delito informático.

Rice argumenta que a menos que dos naciones no compartan normas o

acuerdos sobre control, persecución y judicialización de los temas de crímenes informáticos, los atacantes seguirán manteniendo su estatus de "intocables", lo cual no envía un buen mensaje a los ciudadanos de los países. Esta connotación del autor, marca un punto importante en el tema de los ataques en Internet y las implicaciones jurídicas del asunto. Por un lado, los abogados y juristas deben avanzar en la era del *Electronic Compliance*, lo cual implica comprender los riesgos derivados del cruce entre tecnologías, leyes y mercados, como una manera de profundizar en las normas y estrategias para comprender el delito informático y las relaciones entre el mundo *offline* (mundo real) y el mundo online (virtual) y, por otro, los técnicos y especialistas en seguridad informática (o sencillamente apasionados por el tema) deben avanzar no sólo en la identificación de las vulnerabilidades y sus posibilidades, sino en la comprensión y entendimiento de la inseguridad como esa propiedad inherente a los objetos y que requiere una mente que "piense en el margen", "sin restricciones" y de manera creativa.

Estos cinco factores si bien no son los únicos para analizar la pregunta formulada por Rice, sí establece un referente base de análisis no técnico, que permite a ilustrados tecnológicos y a personas corrientes, visualizar un aspecto de una realidad emergente que poco a poco nos toca y que, cuando queramos entender, no sea demasiado tarde, pues ya la realidad supera a lo que hoy llamamos historias de ciencia ficción.

La psicología de la seguridad de la información

Comenta Shostack y Stewart en su libro que un verdadero profesional de la seguridad de la información toma mejores decisiones analizando los incidentes de pérdidas de datos, dado que allí encuentra lecciones que la inseguridad le sugiere y no solamente en el reclamo justo de la administración por la pérdida de los mismos.

Esta posición algo extraña, dado que el responsable de la seguridad se expone todo el tiempo por cuenta de la inseguridad, en este sentido, resulta todo un acierto revisar la perspectiva de la seguridad desde la visión psicológica y de percepción de la misma.

La seguridad es una sensación, una manera de percibir un cierto nivel de riesgo. Algunas personas son más propensas al riesgo, mientras que otras son más conservadoras. Mientras las primeras gustan del desafío y la vida en los límites, las otras, buscan medir sus pasos y analizar sus posibilida-

des antes de actuar. Cualquiera que sea el perfil, los dos buscan siempre confrontar la inseguridad para sacar el mejor provecho de ella, bien sea para obtener mayores dividendos en un negocio o salvar incluso su vida.

Revisando los análisis de Shostack y Stewart sobre estudios realizados en el Reino Unido sobre niveles de accidentalidad de tránsito, basados en el uso o no de frenos más confiables como son los ABS, se encuentran conclusiones desafiantes que nos deben invitar a reinventar nuestra perspectiva de la seguridad de la información en los individuos.

Luego de hacer seguimiento de las personas participantes en el estudio durante un año se encontró que el nivel de accidentalidad no disminuyó, pero lo interesante fue que las personas que tuvieron mayores niveles de siniestralidad fueron aquellos que tenían los frenos más confiables, es decir los ABS. Este paradójico resultado lo explican los autores con una teoría que denominan teoría de compensación del riesgo. Dicha teoría dice que "a medida que las personas se sienten más seguras con las medidas de seguridad, más propensas a los riesgos se vuelven". En el caso particular del estudio, se concluye que los conductores con frenos ABS se sentían más seguros y por tanto manejaron de manera más agresiva.

Esta interesante conclusión, nos sugiere elementos que hasta ahora hemos ignorado frente al modelaje de la seguridad de la información. Por un lado, nos invita a establecer esos perfiles de riesgo propios de cada persona, que nos permite establecer mecanismos de control que, no lo limiten en su hacer y le permitan hacer su trabajo con flexibilidad; pero al mismo tiempo, reconocer en el entorno corporativo la "falsa sensación de seguridad" que sugieren los constantes ejercicios de aseguramiento, para mantener una posición proactiva en el tema.

Incorporar en los diseños de seguridad de la información estas conclusiones, nos permite comprender la inseguridad como una función de la percepción y tendencias humanas por el riesgo, lo cual nos lleva a visualizar la configuración de controles y seguridades, que por un lado permitan un libre actuar de las personas en contornos de protección mínimos requeridos y por otro, le permitan al individuo recordar su responsabilidad en el uso de la información dentro y fuera de la organización.

La psicología de la seguridad informática debe estar animada por la constante evolución de la percepción

del individuo sobre la protección de los activos, como una manera de incorporar en la gestión de la inseguridad, esa variable que impacta los resultados propios del responsable de la seguridad y su reporte a la alta gerencia: ser más o menos vulnerables.

Conclusiones

La industria de la seguridad, la constante evolución de las vulnerabilidades y la psicología de la seguridad son componentes que interrelacionados nos permiten avanzar en el reto de conocer la inseguridad de la información, no para llegar a comprenderla totalmente, sino para reconocer en sus tendencias y conexiones una forma para mejorar nuestras estrategias de preparación y respuesta a incidentes.

Avanzar en la gestión de la seguridad de la información, es conquistar nuestro temor natural por la inseguridad, por la materialización de los riesgos. Mientras un riesgo no sea una oportunidad para desaprender del entorno y repensar nuestras medidas de seguridad, la inseguridad de la información será un escenario desconocido donde la industria, las vulnerabilidades y el individuo se matizan y se esconden al lente del responsable de la seguridad.

Aceptar el riesgo de gestionar la inseguridad de la información, es esa competencia que el responsable de la seguridad debe desarrollar, no para incrementar los niveles de confiabilidad de los datos u aplicaciones, sino la forma concreta y real para destruir el paradigma de la "falsa sensación de la seguridad", ese que está siempre vigente y latente como el caso de los frenos ABS.

Referencias

RICE, D. (2008) Geekonomics. The real cost of insecure software. Addison Wesley.
SHOSTACK, A. y STEWART, A. (2008) The New School of Information Security. Addison Wesley.

Jeimy J. Cano, Ph.D. *Ingeniero de Sistemas y Computación de la Universidad de los Andes, graduado del Magíster en Ingeniería de Sistemas y Computación de la misma universidad y Doctor en Filosofía de la Administración de Empresas de Newport University, California en los Estados Unidos. Diplomado en el Sistema Penal Acusatorio y los profesionales de la seguridad por la Universidad Militar Nueva Granada. Se ha desempeñado como profesor de cátedra en la Facultad de Ingeniería de la Universidad de los Andes en el área de la seguridad informática y la computación forense, así como de la Facultad de Derecho de la misma universidad, donde hace parte del GECTI – Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática. Es actualmente miembro de la Red Iberoamericana de Criptología y Seguridad de la Información – CriptoRED (http: // www.criptored.upm.es) y Miembro Senior del IEEE.*