Rastreando la inseguridad de la información

Jeimy J. Cano, Ph.D, CFE

Al revisar los recientes estudios de tendencias en inseguridad informática se advierten proyecciones que demandan reflexiones y acciones por parte de los encargados de la seguridad de la información en las organizaciones. Ignorar estas nuevas trayectorias y manifestaciones de la inseguridad y su aprovechamiento por parte de las organizaciones criminales es debilitar la resistencia del diseño de sus modelos de seguridad de la información vigentes.

De acuerdo con los estudios realizados por TrendMicro [EVERS, J. 2007] los criminales, la delincuencia organizada está ofreciendo altas sumas de dinero por fallas en sistemas como Windows XP (US$75000), Windows Vista (US$50000) para luego utilizarlas como herramientas y estrategias de ataque contra las organizaciones con fines diversos: espionaje, negación del servicio, extorsión o robo.

Esta situación combinada con el hecho de que los ataques más frecuentes se materializan en el web, dado que es el punto de mayor interacción con el usuario final y donde existe menor concientización sobre los temas de seguridad, establece una ruta crítica para modelar, planear, materializar y ejecutar acciones que vulneren las defensas vigentes en las organizaciones.

De igual forma el informe de 2006 de IBM Xforce [IBM INTERNET SECURITY SYSTEMS 2006] presenta resultados interesantes que complementan las afirmaciones efectuadas previamente:

• Aproximadamente el 50% de los sitios web contienen códigos maliciosos diseñados para infectar navegadores web y ofuscar sus ataques. Aproximadamente el 30% de ellos cifran sus conexiones y descargas.

• El 88.4% de todas la vulnerabilidades del 2006 pueden ser materializadas de manera remota.

• Más del 95% del *phishing* vía correo electrónico, se basó en correos con HTML embebido.

Considerando estos datos y sumado a ello el hecho de que, actualmente en muchas de las investigaciones forenses en informática se requiere examinar datos en sistemas aún conectados y activos, lo cual aumenta la posibilidad de la alteración de la evidencia volátil que se recolecte, tenemos un escenario donde todas las dudas razonables se resolverán a favor del acusado.

Este aparente estado de indefensión e incertidumbre técnica y jurídica, es la mejor excusa para repensar nuestras estrategias en seguridad de la información, no como una forma de reparar daños y ajustar infraestructuras de cómputo, sino como una función de inteligencia para revisar la resistencia de nuestros modelos de seguridad frente a situaciones críticas; así mismo, utilizando esta misma idea, para profundizar en el análisis de vulnerabilidades y fallas para identificar allí sus rastros y huellas, avanzando en la caracterización de los intrusos y sus métodos.

Cibercrimen, terrorismo en línea y la administración de justicia

Como lo muestran las tendencias anteriores, las fallas de seguridad no sólo impactan el contexto tecnológico y organizacional, también trascienden y desafían los ordenamientos jurídicos y las instituciones que soportan la administración de justicia.

Esta cambiante realidad tecnológica y la creciente habilidad (capacidad de aprendizaje) que tienen los intrusos sobre las mismas, alteran las estrategias procedimentales y legales para procesar esas posibles conductas criminales.

Por un lado, no existe un acuerdo internacional sobre lo que se puede entender por “computer crime” o “cyber crime” o delito informático. [REYES, A., O’SHEA, K., STEELE, J., HANSEN, J., JEAN, B. y RALPH, T. 2007, cap. 2] Diferentes tendencias abogan por diferentes frentes: la creación de un ordenamiento legislativo específico, la adecuación del ordenamiento jurídico actual para el tema tecnoló-

gico y los que sugieren una postura intermedia. De otra parte, tenemos los procesos de investigaciones electrónicas o informáticas realizadas por investigadores o peritos informáticos, cuyos procedimientos, herramientas y formación aún son objeto de revisión y homogenización.

Si bien las herramientas forenses disponibles a la fecha, muestran altos niveles de confiabilidad, la administración de justicia requiere un proceso de concientización, formación y entrenamiento sobre cómo la delincuencia organizada, en permanente aprendizaje, se ha actualizado y perfecciona día a día sus estrategias para limitar las actuaciones de la justicia frente a sus acciones.

Complementario a este escenario, recientemente las naciones industrializadas, han llamado la atención de los riesgos a los cuales se encuentra expuesta su infraestructura crítica nacional, la cual se encuentra articulada con tecnologías de información, particularmente en lo concerniente a Internet.

Douglas Maughan, miembro del Directorio de Ciencia y Tecnología, del Departamento de Seguridad Nacional de los Estados Unidos, afirma que: "Los atacantes pueden llegar a nuestros negocios y sistemas del gobierno a través del laberinto de redes interconectadas por Internet". [KREBS, B. 2007] Podríamos agregar a esta afirmación, que sólo es cuestión de tiempo, paciencia y perseverancia.

Considerando pues, la realidad de la inseguridad de la información misma que no puede evitarse, debemos propender por aumentar la resistencia de nuestros sistemas para hacerle más exigente la ruta del laberinto a los atacantes, bien sea confundiéndolo en la suya o mejor aún, descubrir sus estrategias para lograr sus objetivos.

Los rastros, las investigaciones y la mente del enemigo

La materialización de una falla de seguridad, al igual que un delito tradicional, deja evidencia de lo que ocurrió; algunas veces clara e identificable, otras no.

Afirma un criminalista e investigador forense en informática chileno que *"No existe crimen perfecto, sino investigación imperfecta"*, en este sentido, la gran responsabilidad y el inmenso reto de los investigadores forenses en informática, demanda un entrenamiento dinámico y una mentalidad de intruso, para recabar las pruebas requeridas encaminadas

a evidenciar sus movimientos y para procesarlos por sus acciones.

De acuerdo con los resultados de los estudios efectuados por el *National Law Journal* publicados en septiembre de 2005, sobre la identificación y recolección de evidencia digital [NELSON, S., OLSON, B y SIMEK, J. 2006, pág. xvi] en procesos jurídicos norteamericanos, se establecen una serie de tendencias que merecen reflexiones y acciones concretas por parte de todos los actores vinculados con las acciones delictivas en medios tecnológicos:

• US$ 4.6 billones, fue la cantidad de dinero que compañías norteamericanas invirtieron internamente en 2005 para analizar correos electrónicos.

• Más del 50% de las evidencias son correos electrónicos.

• US$ 1.2 billones, fue la inversión de compañías norteamericanas en servicios externos de identificación, recolección y análisis de evidencia digital.

• 62%, la cifra de empresas que dudaron que ellas podían presentar sus registros electrónicos como confiables y exactos.

• 80%, la cantidad de asesores jurídicos que no están familiarizados con los temas de evidencia digital ni con

los cambios efectuados al código de procedimiento civil norteamericano sobre la información almacenada en forma electrónica.

Si bien los rastros o evidencias electrónicas son cada vez más invisibles en las infraestructuras de cómputo, también es un hecho que los procesos legales y procedimientos judiciales no cuentan con la experiencia y técnicas jurídicas requeridas para armonizar las actuaciones y sentencias de los jueces.

En esta encrucijada se hace necesario un *"pare y reflexione"* que invite a todas las partes para buscar propuestas interdisciplinarias que permitan comprender las diferentes variables de un fenómeno, que no es exclusivamente jurídico ni técnico, procedimental ni gubernamental, sino sistémico: la criminalidad informática.

La mente de los intrusos no es un mito o un asunto inalcanzable para los investigadores en materias forenses. Existen años de investigación acumulada que nos permiten visualizar preferencias e inclinaciones de los atacantes para perfilar sus acciones. No obstante lo anterior, sus métodos y estrategias han variado, concientes de que pueden distorsionar, borrar, o dejar evidencia de sus actividades. Esta última variante, se hace evidente en las investigaciones en informática pues saben que los analistas forenses estarán tras los bits o bytes que puedan vincularlo con la investigación.

Los recientes avances en técnicas de evasión de investigaciones forenses en informática, denominados técnicas anti-forenses [CANO 2007], nos muestran cómo los intrusos luego de efectuar sus acciones, deliberadamente tienen un procedimiento para manipular y distorsionar la escena del incidente, con el fin de que el investigador encuentre lo que él quiere que encuentre y llegue a conclusiones que pueden no ser las correctas.

Esta tendencia actual, nos advierte que hay que redoblar los esfuerzos académicos y científicos en las técnicas de investigaciones con el enfoque señalado, no sólo para comprender los hechos en medios informáticos o electrónicos, sino establecer rutinas de verificación de la escena del crimen para validar posibles manipulaciones intencionales de los atacantes, antes de entrar a recabar las evidencias del caso.

Reflexiones finales

Rastrear y comprender la inseguridad informática son competencias y habilidades actuales, que los profesionales en seguridad informática como los investigadores forenses deben desarrollar para avanzar, tanto en el diseño de sistemas de información e infraestructuras más resistentes y recuperables, como en investigaciones menos imperfectas y más confiables.

Así como plantea Ackoff [2007, pág.35] que *"los buenos docentes producen profesionales escépticos que construyen sus propias preguntas y encuentran mejores respuestas",* se requieren investigadores y profesionales en seguridad informática y cómputo forense que en forma constante reten de manera inteligente los horizontes establecidos por los proveedores de tecnologías de información y los estándares conocidos, pues sólo así es posible evidenciar el rastro de la inseguridad de la información.