TECNOTREND

CÓMPUTO FORENSE: EL CSI DEL CIBERESPACIO (ENSAYO)

Mtro. Hugo Navarro Espínola

Maestro en Ingeniería de Sistemas Electrónicos y Computacionales, entre las certificaciones con las que cuenta se mencionan Certified Information Systems Security Professional, Certified Information Systems Security Manager, Certified Information Systems Auditor, Certified Ethical Hacker, Computer Hacking Forensic Investigator, entre otras. Más de 20 años de experiencia en Administración de Tecnologías de la Información y Telecomunicaciones. Actualmente, es Director General de Red Team Security.

Palabras clave

Delito digital, ataque cibernético, evidencia digital, cadena de custodia.

Introducción

Según el estudio “2016 Norton Cyber Security Insights” (Symantec Corporation, 2016) tan solo en México hubo pérdidas de 5.5 billones de dólares y 22.4 millones de usuarios afectados por algún tipo de delito digital en dicho año. Esto da una idea de la magnitud del problema a la que se está enfrentando México y por qué es necesario estar preparados para lidiar con circunstancias que apenas hace unos años no solo no existían, sino que eran impensables.

Así bien, según Steve Hailey del Cybersecurity Institute define el cómputo forense de la siguiente manera:

Es la ciencia que trata de la localización, extracción y análisis de los diferentes tipos de datos de diferentes dispositivos en los cuales los especialistas los interpretan para que sea útil en un proceso legal. (Recuperado de Marcella, 2010)

Año 2017 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Planteamiento

Para comprender el alcance del cómputo forense es necesario primero entender tres cuestiones fundamentales:

1. ¿A qué dispositivos se les puede aplicar el cómputo forense?
2. ¿Cuáles son los escenarios donde podemos aplicar el cómputo forense?
3. ¿Por qué se usan las computadoras para cometer delitos?

Atendiendo a la primera pregunta, la respuesta es más simple de lo que uno pudiera imaginarse; el cómputo forense se puede aplicar a cualquier dispositivo electrónico que posea memoria para almacenar algún tipo de información que después de algún incidente pueda ser preservada, identificada, extraída y analizada y documentada.

Respondiendo a la segunda pregunta, lo más importante es entender que existen 3 escenarios donde se puede encontrar evidencia digital en un delito, dichos casos pueden manifestarse cuando:

1. Cuando un dispositivo electrónico fue utilizado como herramienta para cometer un delito. Un ejemplo de este escenario pudiera ser la computadora que utiliza un delincuente cibernético para vulnerar la seguridad de la página Web de un banco.

2. Cuando un dispositivo electrónico contiene evidencia de algún delito. En este escenario, una computadora que guarda fotografías que contienen pornografía infantil es un buen ejemplo.

3. Cuando un dispositivo electrónico es el objetivo o blanco de un delito. Una página web atacada es un ejemplo claro de este escenario.

Año 2017 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Haciendo referencia a la tercera pregunta, generalmente imaginamos que la masificación de Internet y la hiperconectividad son los únicos responsables de que actualmente las computadoras sean usadas para cometer delitos, pero la respuesta va más allá:

1. Cometer un delito con una computadora en ocasiones puede ser extremadamente rápido
2. La evidencia electrónica es muy volátil
3. Da la sensación de ser anónimo
4. En muchas ocasiones es difícil aplicar la ley o, bien, la ley no tiene el incidente tipificado como delito
5. Se requiere tener conocimientos especializados para dar con el culpable

Exposición de Tesis y Argumentación

Uno de los puntos fundamentales para poder perseguir un delito o crimen digital consiste en trabajar en un proceso lo suficientemente sólido como para que la evidencia digital tenga admisibilidad; es decir, que pueda ser considerada como una evidencia válida en un proceso legal.

Si bien no hay una receta única que nos indique todos los pasos a seguir, existen una serie de procesos clave que pueden aplicarse de manera general (Marcella, 2010):

1. Identificación
2. Colección o extracción de la evidencia
3. Preservación
4. Interpretación o análisis

Año 2017 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Conclusiones

El cómputo forense en la actualidad adquiere especial importancia en virtud de que cada vez dependemos más del uso de la tecnología como parte de nuestra vida cotidiana y, por lo tanto, cada vez crece más la posibilidad de que un dispositivo electrónico pueda contener evidencia digital con valor probatorio en un proceso legal.

El punto más importante a entender es que no solo es necesario conocer las técnicas y herramientas para extraer y analizar la información digital, es igual o inclusive más importante, asegurarnos de que la evidencia digital sea admisible. De nada sirve que podamos exponer en un caso legal cierta evidencia, si no podemos demostrar que esta no ha sido alterada.

Referencias

Marcella Albert J. and Doug Menendez. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. Aurebach Publications, 2010.

Symantec Corporation. Norton Cybersecurity Insights 2016 Report, 2016 consultado en https://us.norton.com/cyber-security-insights

Año 2017 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203