CIBERCRIMEN E INFORMÁTICA FORENSE: INTRODUCCIÓN Y ANÁLISIS EN EL SALVADOR

César Eduardo Vásquez Mata
Técnico en Redes Informáticas. Docente de Escuela de Ingeniería Eléctrica y Electrónica. ITCA-FEPADE Sede Central.
E-mail: cesar.vasquez@itca.edu.sv
José Mauricio Regalado González
Técnico en Redes Informáticas. Docente de Escuela de Ingeniería en Computación. ITCA-FEPADE Sede Central.
E-mail: jose.regalado@itca.edu.sv
Ricardo Salvador Guadron
Ingeniero Electricista. Director de Escuela de Ingeniería Eléctrica y Electrónica. ITCA-FEPADE Sede Central.
E-mail: rguadron@itca.edu.sv

Resumen

En este artículo se explica la situación de cibercrimen e informática forense, la importancia e interés dado por los gobiernos alrededor del mundo a este tema y un breve análisis enfocado en El Salvador a raíz de las medidas que abarcan leyes y políticas públicas referentes a ello. Finalmente se emite una crítica y conclusiones acerca del curso de la ciberseguridad en el país.

Palabras clave

Protección de datos, legislación de las comunicaciones, Leyes – El Salvador, derecho a la privacidad, derecho a la informática, cibernética.

Abstract

This article explains the situation of cybercrime and computer forensics, the importance and interest given by governments around the world to this matter and a brief analysis focused on El Salvador as a result of measures that include laws and public policies relating to it. Finally, a review and recommendations about the course of cybersecurity in El Salvador.

Keywords

Data protection, legislation of communications, Laws - El Salvador, right to privacy, right to information technology, cybernetics.

Introducción

A finales de los años noventa el mundo vivió una revolución en las comunicaciones: la Internet. Las tecnologías de la información tuvieron un auge importante en esta década, al punto que a su cierre se generó lo que conocemos como la "Burbuja punto com", el periodo en el que muchas empresas vinculadas al Internet tuvieron un alza en sus cotizaciones en la bolsa, y aunque para el año 2003 los efectos de esta burbuja derivaron en la quiebra de muchas de estas empresas, otras tantas sobrevivieron a la ola, se mantuvieron en el mercado y hoy en día resultan tener mucha influencia, no solo en los aspectos económicos, comerciales y tecnológicos, sino en la vida diaria de muchas personas.

Compañías como Facebook, Apple, Google, Amazon, Pay-Pal, Netflix, entre muchas otras, componen una parte importante del estilo de vida de muchas personas, y no solo resultan ser herramientas de ocio, sino también de trabajo e investigación. Este cambio en la dinámica social se hace obvio si tomamos en cuenta que actualmente habría más de 3 mil millones de personas conectadas a Internet, casi la mitad de la población mundial, y que el crecimiento en el número de usuarios ha sido de más de un 800% desde el año 2000 [1].

Aunque estas compañías han llevado progreso tecnológico a la humanidad con sus productos, también para los usuarios representan un riesgo, pues mucha de su información se encuentra en Internet y en las redes sociales. Para enero de 2016 se estimó que más de 2 mil millones de personas eran usuarias activas de redes sociales, lo que representa casi un tercio de la población mundial [2]. Toda esta información resulta ser valiosa en el mundo por diversas razones, esa misma importancia hace que se busque obtenerla, muchas veces, de forma ilegal, por lo que aparece la figura de cibercrimen.

Este ensayo muestra los puntos básicos en el tema y su importancia alrededor del mundo. También se muestran los avances que El Salvador ha hecho con un breve análisis acerca de su situación.

Recibido: 27/03/2017 - Aceptado: 11/06/2017

Cibercrimen

A. Los primeros pasos

El cibercrimen ocurre cuando tecnologías de la información son utilizadas para cometer o conceder una vulneración. Este tipo de figura abarca fraudes financieros, sabotaje de datos y/o redes, robo de información privada, denegación de servicio o penetración externa al sistema de información, acceso no autorizado y virus informáticos [3]. Dados estos riesgos, el cibercrimen se ha convertido en un tema de seguridad nacional en países como Estados Unidos, sobre otras amenazas como el terrorismo y el espionaje, a tal punto que en el año 2013 el FBI notificó que tres mil compañías estadounidenses habían sido víctimas de ciberintrusiones. Su importancia se hizo tal que un año después, en una investigación que hizo la firma PwC, se encontró que el 69% de los directores ejecutivos de Estados Unidos que participaron en este estudio se mostraron preocupados por el impacto de las amenazas digitales, alrededor del mundo; 49% de las personas encuestadas pensaban igual [4].

Las empresas, sobre todo en Estados Unidos, invierten cantidades exorbitantes de dinero en infraestructura de ciberseguridad por la cantidad de datos que poseen y por lo valioso, confidencial y preciado que son. En 2013 se estimó que las inversiones globales en seguridad alcanzaban los 1.7 mil millones de dólares; esto alcanzó los 2.5 mil millones en 2014 según CB Insights y se esperaba que este monto fuera superado en 2015. Para 2019 se estima que el gasto total en tecnologías de seguridad informática alcance los 108 mil millones de dólares, según la firma Gartner [5].

Cada año las amenazas de ciberseguridad se van aumentando, y aunque se han hecho esfuerzos importantes por reforzar la seguridad en sitios web, los dispositivos móviles resultan ser el nuevo foco de atención para los atacantes. Según el Reporte de Amenazas de Seguridad en Internet, aproximadamente un millón de aplicaciones, de poco más de seis millones analizadas, fueron reconocidas como software malicioso en 2014; asimismo, las vulnerabilidades de los dispositivos móviles han ido en aumento, contabilizándose 168 nuevas en ese año, superando las 127 de 2013. Una tendencia contraria a las vulnerabilidades en sitios web [6].

La información, sobre todo corporativa, resulta ser muy valiosa y cotizada, por lo que una de las formas de ataque más populares es el "spear phishing", una variante del phishing, cuya diferencia radica en personalizar el ataque con técnicas de ingeniería social, a manera que el objetivo no sospeche que está siendo víctima de un ataque [7]. De acuerdo con el Reporte de Amenazas de Internet de Symantec, aunque hay un avance en el combate de este tipo de ataque, dado el decrecimiento en el número de ataques, resulta ser sumamente común para cuestiones como el espionaje industrial; muestra de ello fue que 4 de cada 10 ataques de este tipo fueron hechos a empresas grandes, con más de 2,500 empleados [6].

B. Combate al cibercrimen en el mundo

El contemplar todas estas amenazas no es algo nuevo; desde la década de los años ochenta se ha planteado establecer legislaciones que combatan el cibercrimen, sin embargo, el punto clave en este tema es el Convenio de Budapest sobre la Ciberdelincuencia, año 2001. Y aunque existen críticas a esta convención, pues no estipula un modelo de legislación para estos delitos [8], sí define los delitos y da un esbozo de los lineamientos que tendría que seguir el país, en un esfuerzo por armonizar legislaciones entre naciones.

El Convenio sobre Ciberdelincuencia[1] reconoce los siguientes crímenes:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

- **Acceso ilícito:** acceso deliberado e ilegítimo a todo o parte de un sistema informático.
- **Interceptación ilícita:** interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas, originadas o efectuadas dentro de un sistema informático, incluyendo las emisiones electromagnéticas provenientes del mismo.
- **Ataques a la integridad de los datos:** daño, borrado, deterioro, alteración o supresión deliberada e ilegítima de datos informáticos.
- **Ataques a la integridad del sistema:** obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático.
- **Abuso de los dispositivos:** producción, comercio o intercambio de contraseñas y dispositivos que faciliten o cometan los delitos descritos anteriormente.

2. Delitos informáticos

- **Falsificación informática:** generación de datos no auténticos, por medio de la alteración, introducción, borrado

1. Disponible en: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

o supresión, con la intención de hacerles pasar como tal.

- **Fraude informático:** perjuicio patrimonial a otra persona mediante la manipulación de datos informáticos o interferencia en el funcionamiento de un sistema informático, buscando la obtención ilegítima de un beneficio económico para sí mismo o terceras personas.

Además, el Convenio reconoce delitos relacionados con la pornografía infantil, como la producción, oferta, difusión, transmisión, adquisición o posesión de pornografía infantil en sistemas informáticos o dispositivos de almacenamiento; también reconoce infracciones contra la propiedad intelectual, tentativa, complicidad y responsabilidad de personas jurídicas. Sin embargo, podría presumirse que delitos como la pornografía infantil están incluidos, dado que el uso de la tecnología computacional incrementa los casos en los que podría eludirse este tipo de delitos tradicionales, al igual que podrían tomarse el fraude y la falsificación [8]. En cuanto a los últimos delitos mencionados, el Convenio da bastante apertura para el establecimiento de legislaciones en cada uno de los países firmantes, por ello se decidió no extenderse más en dichos puntos en este artículo.

Posteriormente se hicieron esfuerzos por adaptar estas legislaciones a nuevas tecnologías de la información que fueron surgiendo con los años, el más importante de ellos fue en el año 2007, realizado por la Unión Internacional de Telecomunicaciones (ITU) en Ginebra, Suiza. Este organismo, por medio de un panel de más de 100 expertos, logró establecer una serie de recomendaciones por medio de la Agenda Global de Ciberseguridad (GCA), entre las cuales se habla de adaptar legislaciones a crímenes hechos con tecnologías de VoIP o videojuegos en línea, así como también de los procesos a realizar para investigar estos hechos, e incluso contemplar legislaciones contra el spam, robo de identidad, entre otras [9]. Sin embargo, aunque se hacen muchas sugerencias a las legislaciones sobre cibercrimen, todas parten de la base de la Convención de Budapest y, en síntesis, solo recomiendan a los países añadir o contemplar otras tecnologías de la información sobre la base del Convenio de Budapest, por lo que se puede concluir que al día de hoy sigue siendo el referente para la creación de cualquier marco legal acerca de cibercriminalidad.

C. *Cibercrimen en El Salvador*

Parte de los esfuerzos de la ITU fue elaborar un índice que permitiera medir y clasificar los países del mundo según su preparación ante el cibercrimen, por lo que junto con ABI Research desarrollaron el Índice Mundial de Ciberseguridad (IMC) para 193 países Estados Miembros [2] . El IMC se centra en cinco áreas de medición con los siguientes criterios:

1) Medidas jurídicas

a) Legislación Penal
b) Reglamentación y Conformidad

2) Medidas técnicas

c) CERT/CIRT/CSIRT
d) Normas
e) Certificación

3) Medidas organizativas

f) Política
g) Hoja de Ruta de Gobernanza
h) Organismo Responsable
i) Evaluación Corporativa Nacional

4) Creación de capacidades

j) Desarrollo de Normas
k) Desarrollo Laboral
l) Certificación Profesional
m) Certificación del Organismo

5) Cooperación

n) Cooperación Interestatal
o) Cooperación entre Organismos
p) Asociaciones entre los Sectores Público y Privado
q) Cooperación Internacional

La metodología del IMC, en líneas generales, es la siguiente: cada uno de estos criterios tiene una misma ponderación, de dos puntos cada uno, y el resultado del índice viene dado por el cociente de los puntos conseguidos entre el total, que es de 34. Finalmente, el resultado del IMC oscilará entre 0 y 1.

Para el informe de 2015, cuya investigación se realizó un año antes, Estados Unidos fue el líder mundial con un IMC de 0.824, sin embargo, el continente americano no fue la región mejor calificada, ya que este puesto corresponde a Europa. América es el penúltimo continente, solo superando a África, aunque con leves diferencias con respecto a Emiratos Árabes y Comunidad de Estados Independientes (CEI).

2. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

El Salvador logró un índice de 0.206, colocándose en la posición 22 de la clasificación mundial, empatando con otros países como Venezuela, Trinidad y Tobago, Guatemala, Paraguay, entre otros. Regionalmente, El Salvador está en posición 12; a nivel centroamericano solo lo superan Panamá y Costa Rica, siendo éste el mejor posicionado dentro del área. Sin embargo, es necesario recalcar que este informe, así como otro estudio más reciente del Banco Interamericano de Desarrollo (BID), puntualizan falencias en la estructura de ciberseguridad para el país, dejando entrever que la cultura de ciberseguridad en El Salvador apenas está en una etapa inicial.

El perfil de El Salvador tanto para el informe de la ITU [3], como para el del BID [4], evidencia la intención de El Salvador por colocar la ciberseguridad como un tema de agenda nacional, además de destacar los esfuerzos por establecer una legislación específica para estos delitos, misma que no había sido aprobada en el momento en que los informes fueron publicados. Además, reconocen la existencia de un Equipo de Respuesta para Incidentes Informáticos (CIRT) o para Incidentes de Seguridad Informática (CSIRT) [5], llamado SalCERT, aunque no se pudo profundizar acerca de quienes conforman este equipo, sus responsabilidades, jurisdicción y otros detalles; el BID solamente menciona que ha tenido limitantes por temas presupuestarios.

Los puntos débiles para El Salvador pasan por la infraestructura para el tratamiento de delitos informáticos, pasando por estrategias nacionales de coordinación y organización de seguridad y defensa cibernética, aplicación de normas y estándares internacionales de ciberseguridad, educación especializada sobre el tema y cultura nacional de la importancia de la seguridad informática, entre otras áreas. Sin embargo el panorama no es desalentador, pues a nivel centroamericano, solamente Costa Rica y Panamá cuentan con estructuras más sólidas en materia de ciberseguridad, el resto de países se ve levemente superado por El Salvador. Además, se reconocen dos aspectos concretos para el país: los avances que se están haciendo en materia de legislación, bastante sólidos pese a ser un tema relativamente nuevo para el país, y la importancia que se le está dando al tema de seguridad informática, sobre todo por el sector empresarial.

Puesto que la legislación salvadoreña sobre cibercrimen es uno de los puntos destacables para el país, se debe hacer un breve análisis al respecto. Al observar la Ley Especial contra los Delitos Informáticos y Conexos es notoria la influencia del Convenio de Budapest, pues los delitos que reconoce este tratado son igualmente reconocidos por el Gobierno de El Salvador, los cuales se mencionaron anteriormente en este artículo.

Situaciones como el fraude y la falsificación informática, accesos ilícitos o ataques a sistemas informáticos, entre otras, son bien definidas en las leyes salvadoreñas, además de ello también se contemplan los ataques de denegación de servicio, el uso fraudulento de tarjetas inteligentes, interceptación de transmisiones de sistemas informáticos, el robo de identidad y el comercio de credenciales de acceso a equipos informáticos o datos personales. Sin embargo, no se toma en cuenta el uso de sistemas informáticos con respecto a los derechos de autor y la propiedad intelectual, siendo este un punto endeble en la legislación. Sumado a ello, otro punto que no retoma esta ley es con respecto al derecho procesal y la forma en que las autoridades reaccionarían ante un delito informático.

A nivel centroamericano, El Salvador tiene intenciones de construir una estructura de combate al cibercrimen, un punto muy fuerte es la recién publicada Ley Especial contra los Delitos Informáticos y Conexos. Sin embargo su preparación general para el combate al cibercrimen no sale tan bien evaluada como Panamá o Costa Rica, por el hecho que El Salvador recién ha incorporado en su agenda nacional el tema de delitos informáticos, a diferencia de estas otras naciones, que ya establecieron su legislación correspondiente y se incorporaron a tratados internacionales, como Panamá, suscrito al Convenio de Budapest desde 2014, y determinaron, organizaron y forjaron instituciones que se encargarían de delitos informáticos, delimitando tareas y responsabilidades asesorándose de otros organismos especializados.

Para El Salvador, el camino del combate al cibercrimen empieza, pero dista de convertirse en un tema de nación; se dio un paso importante con la Ley Especial contra los Delitos Informáticos y Conexos, pero quedan tareas pendientes para el país para establecer una verdadera cultura de seguridad informática, lo que conlleva aspectos de educación, creación de instituciones, políticas públicas, infraestructura, reacción ante el cibercrimen, el derecho procesal de estos delitos y su forma de investigación, como es el caso de la informática forense.

3. Global Cybersecurity Index & Cyberwellness Profiles (pp. 182-183)
4. Cybersecurity: Are We Ready in Latin America and The Caribbean? – 2016 Cybersecurity Report (pp. 74-75)
5. Both terms could take as equals, and every report uses each one, but they are no synonymous, there are differences but this paper won't go deeper in that. For more information, consult the next source: http://www.networkworld.com/article/2328305/lan-wan/certs-and-cirts--homonyms-but-not-synonyms--part-1.ht

La informática forense es una ciencia moderna que permite reconstruir lo que sucedió en un sistema tras un incidente de seguridad. Este análisis puede determinar quiénes, desde donde, cómo, cuándo y qué acciones realizó un intruso para ocasionar un incidente de seguridad en el sistema [10]. Para manejar e implementar este análisis de forma eficiente debe existir una cultura de seguridad informática, dado que resulta determinante conocer el entorno tecnológico, usos y configuración en empresas e instituciones para realizarlo [11].

El Salvador ha dado un paso importante con la reciente aprobación de la Ley Especial contra los Delitos Informáticos y Conexos, la cual define la clasificación de los cibercrímenes, pero omite muchos de los elementos más importantes en la presentación de la evidencia en informática forense dado que la Ley no explica el proceso científico que se debe seguir para la aceptación de esta evidencia en una corte judicial. Un proceso aceptado y descrito en la Ley podría ser una herramienta perfecta para que no se pudiera refutar la veracidad de los elementos encontrados en la inspección del sistema, como afirman muchos autores, los fundamentos de una investigación radican en la determinación de una cadena de custodia donde información crucial tiene un primer contacto con el equipo de inspección.

Para ello se recurre al modelo de Casey, que determina el proceso para examinación de evidencias digitales enlistando los siguientes pasos [12]:

1. Identificación.
2. Conservación, Adquisición y Documentación.
3. Clasificación, Comparación e Individualización.
4. Reconstrucción.

En la Ley Especial contra los Delitos Informáticos y Conexos salvadoreña, estos pasos o cualquier proceso de investigación, no están definidos. Esto puede considerarse un punto débil en la estructura de ciberseguridad en el país.

"Caso Troll Center [6]

A principios de 2016, el tema de ciberseguridad tuvo un lugar en la agenda política nacional con un incidente conocido como "El caso Troll Center". No fue claramente un fraude, pero sí un ataque que demostró vulnerabilidades en la infraestructura de red de dos de los periódicos más importantes en El Salvador.

Más allá de las consecuencias políticas y mediáticas, el tratamiento de las autoridades en todo el caso mostró falencias. El procesamiento de las evidencias informáticas y tecnológicas involucradas no fue del todo claro, y la ausencia, en ese entonces, de una Ley Especial contra los Delitos Informáticos y Conexos, impidió que este caso se abordara de una manera técnica y bajo un marco legal sólido.

Conclusiones

Aun cuando El Salvador ha hecho esfuerzos relevantes por la construcción de una estructura de ciberseguridad, existen puntos omitidos. La Ley Especial contra los Delitos Informáticos y Conexos es una herramienta importante en el combate al cibercrimen, pero necesita mejorar mediante revisiones graduales, adaptándose a las últimas tecnologías de la información y contemplando otras existentes.

El Gobierno de El Salvador no ha establecido instituciones públicas dedicadas al manejo de la ciberseguridad y/o combate al cibercrimen; existe una diferencia importante entre El Salvador y otros países desarrollados, por lo tanto, sería un descuido no tratar el tema de ciberseguridad como una política pública.

Existe una deficiencia en la discusión técnica por parte del Gobierno y la adopción de correctos y definidos procedimientos de investigación y la toma de acciones legales contra el cibercrimen, omitiendo cosas como la recolección de datos y la custodia de los mismos y los sistemas incorporados bajo estándares internacionales.

El Salvador debe establecer una cultura de ciberseguridad donde todos los habitantes conozcan el riesgo de los ciberataques y su prevención, dado el creciente uso de las tecnologías de la información. En tal sentido, el aspecto educacional es necesario y debe ser definido como una política pública.

6. Información de este caso disponible en: http://www.elsalvador.com/articulo/sucesos/como-funciona-troll-center-92943

Referencias

[1] Miniwatts Marketing Group, "World Internet Users Statistics and 2015 World Population Stats", Miniwatts Marketing Group, 2015. [Online]. Available: http://www.internetworldstats.com/stats.htm. [Accessed: 8 -Abr- 2016]

[2] S. Kemp, "Global Social Media Statistics 2016", we Are Social, 2016. [Online]. Available: http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.
[Accessed: 8 -Abr- 2016]

[3] J. Vacca, "Occurrence of cyber crime", Computer Forensics: Computer Crime Scene Investigation, Massachusetts, Charles River Media, 2002, p. 56.

[4] PwC, "US State of Cybercrime Survey", 2014. [Online]. Avalilable: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf. [Accessed: 13 -Abr- 2016]

[5] Fortune, "Cyber Security Investing Grows, Resilient to Market Turmoil – Fortune", Reuters, 2015. [Online]. Available: http://fortune.com/2015/09/23/cyber-security-investing/. [Accessed: 13 -Abr-2016]

[6] "Internet Security Threat Report", 2015. vol. 20 [Online]. Avalilable: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf. [Accessed: 15-Abr-2016]

[7] K. Zetter, "Hacker Lexicon: What are phising and spear phishing? WIRED" Wired, 2015. [Online]. Available: https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/
[Accessed: 29 -Abr-2016]

[8] S. Brenner, "The Council of Europe's Convention on Cybercrime", Cybercrime: Digital Cops in a Networked Enviroment, pp. 207-220, 2007.

[9] S. Schjolberg, "Report of Chairman of HLEG" 2007. [Online]. Available: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.
[Accessed: 10 -May- 2016]

[10] H. Rifa Pous, J. Serrra Ruiz y J. L. Rivas López, "Análisis forense de sistemas informáticos", Catalunya: Universidad Oberta de Catalunya, 2009.

[11] M. Gómez, "Profesiones", 2009. [En línea]. Disponible en: http://www.profesiones.org/var/plain/storage/original/application/eedc949a2016ed79702dbdfba-5db9433.pdf. [Accedido: 03 -jun- 2016]

[12] S. Ó Ciardhuáin, "An Extended Model of Cybercrime", vol. 3. No. 1, 2004. [Online] Available: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-EA5C3E93CC575FA.pdf.
[Accessed: 3 -Jun- 2016]