Conceptos y retos en la atención de incidentes de seguridad y la evidencia digital

Jeimy J. Cano, Ph.D*

Abstract

The continuous reports of security vulnerabilities and new ways to have access to privileged resources of our host, notice the necessity to be prepared to face a possible attack in our computational infrastructures and communications. Therefore, the organizations that would maintain high security levels, require to establish, along with the good computer security practices, computer incident response teams, strategies for the identification and harvesting of the evidence of the incident, as well as personal permanently trained in computer security. In this sense, this article offers to readers an analysis scenario to think about incident response and digital evidence.

Keywords

Atención de incidentes, evidencia digital, computacion forense, delitos informáticos, prueba en informática

Los continuos reportes de seguridad anunciando vulnerabilidades y nuevas formas de tener acceso a recursos privilegiados de nuestras máquinas, nos advierten la necesidad de prepararnos para enfrentar un posible ataque a nuestras infraestructuras de computación y comunicaciones. Estudios recientes [1,2] muestran que si bien las organizaciones han destinado recursos para modificar sus estructuras computacionales para mejorar sus condiciones de seguridad, no se han concientizado sobre la necesidad de estar preparados para enfrentar un incidente de seguridad y en menor proporción considerar procesos para recolectar evidencia de dicho incidente.

En este sentido, si bien prácticas como la administración de parches, pruebas de penetración, y evaluaciones de seguridad, entre otras, son elementos fundamentales en la valoración de la arquitectura de seguridad y su exposición a vulnerabilidades, la atención de incidentes debe ocupar un lugar privilegiado en estas prácticas, como proceso complementario y diligente de la organización para atender posibles fallas.

Un incidente de seguridad, según se define en el Internet Security Glossarry, RFC 2828, es un evento de seguridad relevante para un sistema en el cual las políticas de seguridad han sido desatendidas o traspasadas [3]. En este sentido, los incidentes generan un ambiente de desconcierto y confusión en las organizaciones, durante el cual, si no se encuentran preparadas para atender dicha manifestación de violaciones a las políticas de seguridad, múltiples desaciertos se pueden cometer y comprometer la seguridad de la organización.

* Profesor de Cátedra Departamento de Sistemas y Computación - Facultad de derecho. Uniandes.

Por tanto, las organizaciones que procuran mantener altos niveles de seguridad, requieren establecer, junto con las buenas prácticas de seguridad, equipos de atención de incidentes, estrategias para la identificación y recolección de la evidencia del incidente, así como personal permanentemente entrenado en seguridad informática y una cultura de la seguridad informática arraigada en cada uno de los procesos de la organización.

En razón a lo anterior y dado el constante crecimiento de los incidentes de seguridad y la falta de estrategias para enfrentarlos, en este artículo analizaremos tres perspectivas de la problemática de la atención de incidentes revisando lo sugerido por el RFC 2350, relacionado con la conformación de equipos de atención de incidentes y sus procedimientos, el RFC 3227 en lo relativo a la recolección y archivo de evidencia digital y las implicaciones de la Convención sobre Cybecrimen recientemente firmada por el Consejo de Europa, como iniciativa multinacional para enfrentar el incremento de conductas delictivas a través de medios electrónicos.

RFC 2350 (4)

De acuerdo con el RFC 2350, un equipo de atención de incidentes es aquel que coordina y soporta la respuesta a un incidente de seguridad que involucra y actúa en las áreas formalmente constituidas por la organización. Esto es, el grupo de usuarios, sitios, redes u organizaciones a las cuales sirve el equipo. De manera similar, este documento, establece algunas directrices sobre lo que podría catalogarse como incidente: [4, pág.17]

- Pérdida de confidencialidad de la información.
- Compromiso de la integridad de la información.
- Negación del servicio.
- Indebida utilización de servicios, sistemas o información.
- Daño a los sistemas.

Así mismo, este documento detalla algunos de los servicios que debe proveer este equipo. En particular comenta que existen dos tipos de servicios, los directamente relacionados con la tarea de responder al incidente y los relativos a las actividades proactivas de diagnóstico y soporte de la respuesta al incidente.

En la respuesta al incidente, se establecen actividades como el reporte de valoración del incidente y verificación del mismo; de otra parte las acciones relacionados con coordinación de áreas y personal, y de manera complementaria aquellas que están relacionadas con asistencia técnica y eliminación de la vulnerabilidad, asistida con la recuperación de la información y servicios involucrados en el incidente.

En las actividades proactivas y de soporte de la respuesta al incidente, el equipo debe proveer información acerca de los posibles parches u problemas similares registrados en el pasado, establecer y sugerir herramientas que permitan una valoración más cercana del sistema o arquitectura computacional y sus vulnerabilidades. Finalmente, el equipo en este tipo de actividades proactivas debe promover y desarrollar entrenamiento y educación a los usuarios o grupos de su competencia para lograr mayor coordinación y colaboración en el desarrollo de su gestión ante un incidente.

De igual forma, en el soporte a la respuesta del incidente el equipo debe contar con formas de reporte claras y completas, con el fin de mantener una bitácora de los eventos y los procedimientos seguidos en cada uno de ellos. Dependiendo de los objetivos y servicios que ofrezca el equipo de atención de incidentes es posible utilizar múltiples formatos, unos para registrar nuevas vulnerabilidades y otros para registrar los incidentes en sí mismos.

La descripción anterior nos sugiere importantes características para considerar en la generación de un grupo de atención de incidentes, sin embargo, los procesos relativos a la recolección de evidencia no son mencionados. Esta posible ausencia, puede ser debida a que el tema de la evidencia digital no es un tópico que las

organizaciones reconozcan como crítico en la atención y seguimiento de un incidente.

RFC 3227 (5)

Sin embargo, como respuesta a esta creciente necesidad de contar con evidencia digital y adelantar procesos judiciales, se presenta el RFC 3227, que ofrece guías para la recolección y manejo de este tipo de evidencia.

De acuerdo con este documento, la idea es ofrecer a los administradores de sistemas guías para adelantar la recolección y manejo de evidencia digital relevante a un incidente de seguridad. Tal recolección representa un esfuerzo considerable de parte de los administradores, dada la carga de las labores que desarrollan y los esfuerzos de afinamiento constante de los servicios y aplicaciones de las cuales son responsables.

Si la evidencia es recogida de una manera adecuada, habrá mayores posibilidades de establecer una ruta hacia los atacantes y contar con mayores elementos probatorios en el evento de una persecución y juzgamiento del intruso.

Dentro de las principales directrices sugeridas en la guía están: [5, págs 2, 3 y 4]

- Mantenga adherencia estricta a su política de seguridad organizacional y su relación formal con el equipo de atención de incidentes y las personas responsables del campo jurídico.
- Capture la escena del incidente lo más preciso posible.
- Mantenga notas detalladas. Estas deben incluir fechas y horas. Si es posible generar un reporte automático, es decir contar con un script, que pueda ser usado para generar un archivo como parte de la evidencia.
- Establezca las diferencias entre el reloj del sistema y la hora de referencia internacional, GMT.
- Esté preparado para testificar (posiblemente años después) detallando las acciones adelantadas y en qué momento. Sus notas detalladas son vitales.
- Minimice los cambios en los datos que ha recolectado. Debe evitar la actualización de horas o fechas en archivos y directorios.
- Remueva posibles formas externas de modificación de la información
- Primero recolecte la información y luego analice sus hallazgos.
- Aunque usted necesita indicar que sus procedimientos de atención de incidentes son realizables, debe asegurar su viabilidad y funcionamiento en una crisis.
- En la revisión de cada dispositivo o mecanismo presente en el incidente, se debe seguir un acercamiento metódico para la recolección de evidencia. La rapidez y claridad es crítica para una adecuada y oportuna recolección de evidencia. Es importante efectuar este procedimiento gradualmente.
- Proceda recolectar la evidencia desde la volátil a la menos volátil:
- Registros, caché
- Tablas de enrutamiento, cache de arp, tabla de procesos, estadísticas del kernel, memoria
- Sistema de archivos temporales
- Diskettes
- Registro remoto y datos de monitoreo relevante al sistema en estudio
- Configuración física, Topología de la red
- Medios de almacenamiento
- Si usted va adelantar un análisis forense debe hacer una o varias copias bit a bit del medio de almacenamiento, con el fin de utilizar una de las copias para efectuar sus análisis, preservando el medio original.

De igual forma la guía establece algunas acciones que deben ser evitadas en el proceso de recolección de la evidencia como son: [5, págs 3 y 4]

- No apague el sistema hasta que la recolección de la evidencia se halla completado. Mucha evidencia se puede perder y el atacante puede ha-

ber alterado el proceso de inicio/apagado y las rutinas de inicio de los servicios para destruir la evidencia.

• No confíe en los programas del sistema. Ejecute programas de recolección de evidencia apropiados, que protejan adecuadamente los medios originales.

• No ejecute programas que modifiquen las fechas de acceso a todos los archivos del sistema.

• Cuando remueva dispositivos de acceso externo, note que una simple desconexión o filtro de la red puede disparar la alarma de "switches caídos" que una vez detectados pueden eliminar evidencia en la red.

Como se puede observar el RFC 3227 ofrece una guía genérica que puede ser utilizada como marco conceptual básico para incorporar en las organizaciones al crear grupos de atención de incidentes. Otros documentos relacionados sobre el manejo de evidencia digital y análisis de firmas de ataques pueden ser consultados en el portal de seguridad de SecurityFocus. [6,7]

Si bien, los documentos anteriores ofrecen un camino para enfrentar los posibles incidentes de seguridad en las organizaciones con relación a la tecnología, en el mundo legal, la problemática continúa. Particularmente, la falta de una adecuada formación en tecnología de los jueces y fiscales, y escasa legislación sobre la materia, hace que los posibles incidentes de seguridad que conlleven a daños en las propiedades de las personas jurídicas y naturales, puedan quedar en la impunidad.

Por tanto, se hace necesario que el aparato judicial desarrolle una estrategia de formación y entrenamiento para comprender la delincuencia en medios tecnológicos, con el fin de conocer las maneras de vulnerar los bienes jurídicamente tutelados y adelantar esfuerzos en la formulación de un discurso probatorio en informática, que permita a los fiscales conceptuar sin ambigüedad sobre la pertinencia y veracidad de la información en medios tecnológicos.

Convención sobre Cybercrimen

Sobre este particular la Comunidad Europea, a nivel internacional preocupada por el incremento de los ataques de seguridad y el delito informático, promovió una iniciativa que se materializó a través de la Convención sobre Cybercrimen. [8] Dicha convención agrupó a mas de 20 países de Europa y otros países como Canadá, Japón, Sur África y Estados Unidos de Norteamérica.

Esta convención cree firmemente que una lucha efectiva contra el delito informático requiere una coordinación de esfuerzos internacionales en materia criminal que permita a las diferentes naciones interactuar sin restricciones y bajo directrices claras. Así mismo, esta iniciativa internacional considera que todas acciones contra la confidencialidad, integridad y disponibilidad de sistemas de computación, así como la inadecuada utilización de redes y datos son conductas que deben ser penalizadas. Por tanto, establecer un escenario para la detección, investigación y persecución de tales personas tanto a nivel interno, en cada nación, como internacional, es una necesidad para el buen empleo de la informática y las comunicaciones en el mundo.

La convención está compuesta por cuatro capítulos: I) Uso de términos; (II) Medidas a ser tomadas a nivel interno – Ley sustantiva y procedimientos de ley; (III) Cooperación Internacional y (IV) Cláusulas finales.

En el contexto de este artículo, revisaremos algunos de los alcances de esta iniciativa en su capítulo II, en lo referente a los procedimientos de ley asociados con el cybercrimen. En lo referente a los procedimientos de ley la convención cubre: Preservación de los datos almacenados; preservación y revelación parcial del tráfico de datos; producción,;búsqueda y análisis de datos; recolección de evidencia en tiempo real e intercepción de contenido de datos y comentarios sobre la jurisdicción internacional.

La convención adopta medidas procesales tradicionales, tales como la búsqueda y análisis de

evidencia, en el nuevo ambiente tecnológico. Adicionalmente, las nuevas medidas que han sido creadas, se desarrollaron con el fin de asegurar que los procesos tradicionales de recolección de datos, mantengan su efectividad en un ambiente con evidencia tecnológica volátil. Esto requiere una reconceptualización de la evidencia física, una evidencia que es construida y analizada a través de medios electrónicos.

A continuación algunos apartes y comentarios sobresalientes del capítulo II:

Article 16 – Expedited preservation of stored computer data

(...)

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

(...)

Es parte fundamental de proceso de almacenamiento de evidencia mantener la cadena de custodia siguiendo los lineamientos establecidos por la ley sobre los períodos de almacenamiento y registro de la misma. Este aparte nos recuerda que la evidencia debe ser protegida y manejada con altos niveles de aseguramiento y con procesos claramente definidos para evitar alteraciones o modificaciones que comprometan la misma.

Article 19 – Search and seizure of stored computer data

(...)

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to :

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data; and

d. render inaccessible or remove those computer data in the accessed computer system.

(...)

En este aparte se comenta la necesidad de la existencia de una entidad competente para adelantar las labores de identificación, análisis y registro de evidencia digital, que asegure adecuados procedimientos para mantener la integridad de los datos y sus características originales. Es clave desarrollar y contar con experiencia y entrenamiento en labores forenses en informática [9,10] que permitan mayor confianza en los procesos mencionados.

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(...)

De igual forma que en el segmento anterior, esta fase nos presenta la posibilidad de obtener evidencia en tiempo real, para lo cual se involucran a los proveedores de acceso internet y sus contactos internacionales. Es importante notar en

*este aparte, la clara disposición orien*tada a un seguimiento internacional y la cooperación y *asistencia de las partes involucradas para coordinar esfuerzos en la lucha contra el delito informático.*

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

Finalmente, este aparte hace énfasis en la intercepción de información que puede ayudar a determinar serias ofensas contra una de las partes involucrada, proceso soportado en la colaboración y coordinación de esfuerzos a través de los proveedores de servicios de internet.

Conclusiones

A lo largo de este breve documento hemos revisado la problemática existente al presentarse un incidente de seguridad informática en las organizaciones, así como algunas guías para enfrentarse al reto de la evidencia digital y el manejo del incidente mismo. De igual manera hemos revisado algunos aparte de la iniciativa internacional sobre cybercrimen que de forma complementaria, nos confronta con la realidad de nuestro sistema legislativo y judicial para procesar este tipo de incidentes.

Si bien los incidentes de seguridad proponen un reto a las organizaciones en la recuperación y ajuste de sus arquitecturas de seguridad, también lo hace evidente en la definición de estrategias de recolección de evidencia. Luego, si las organizaciones no se encuentran preparadas para enfrentar estas situaciones de crisis adecuadamente, muchas fallas y desaciertos se harán evidentes comprometiendo su seguridad y de igual forma, las entidades judiciales no tendrán mayor oportunidad para establecer y procesar evidencia relevante para adelantar un proceso, ni tendrán elementos de juicio para verificar y validar dicha evidencia.

En este sentido, se requiere un trabajo conjunto tanto, en las organizaciones como en el sistema judicial, que promueva por un lado la conformación adecuada de equipos de atención de incidentes, debidamente entrenados, con funciones y sistema de notificación bien definidos para contar una mayor capacidad de reacción y control de las situaciones críticas, conscientes de que la evidencia digital es parte fundamental de su labor. Así mismo, promover iniciativas gubernamentales que sensibilicen al aparato judicial y legislativo de la nación para desarrollar estrategias, estándares y legislaciones que promuevan el estudio y difusión del conocimiento de los delitos informáticos, para forjar un nuevo perfil de fiscales que se integren al reto de una sociedad digital.

Luego, es necesario que, además de las iniciativas anteriormente mencionadas, la academia promueva investigación y formación coherente con estas necesidades, buscando la armonización e integración de las visiones técnicas y legales que permitan el inicio de una nueva manera de avanzar en el descubrimiento de nuevas posibilidades y negocios con tecnología informática en un mundo globalizado.

Finalmente podemos concluir y sugerir que es necesario:

1. Fortalecimiento Judicial en legislación relacionada con temas informáticos.

2. Fortalecimiento en la academia e investigación integrada de temas jurídicos y técnicos.

3. Creación y entrenamiento continuo de equipos de atención de incidentes.

4. Capacitación y entrenamiento a los funcionarios del sistema jurídico en temas de informática

5. Fortalecimiento de la cultura organizacional acerca de la preparación para la atención de incidentes.

Agradecimientos

Agradecimientos especiales al Ing. Jorge Gil, M.Sc., por sus valiosos aportes y comentarios a este artículo.

Referencias

1. INFORMATION SECURITY MAGAZINE. (2001) *2001 Industry Survey*. http://www.infosecuritymag.com. October.

2. KPMG (2001) 2001 Global e-Fraud Survey. Http://www.kpmg.co.uk/kpmg/uk/direct/forensic/pubs/EFRAUD.cfm

3. SHIRLEY, R. (2000) RFC 2828: Internet Security Glossary. Network Working Group. May. http://www.rfc-editor.org/rfc/rfc2828.txt

4. BROWNLEE, N. y GUTTMAN, E. (1998) RFC 2350: Expectations for Computer Security Incident Response. Network Working Group. June. http://www.rfc-editor.org/rfc/rfc2350.txt

5. BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. http://www.rfc-editor.org/rfc/rfc3227.txt

6. WRIGHT, T. (2001) The field guide for investigating computer crime, part 7: Information Discovery – Basics and Planning. Securityfocus. http://www.securityfocus.com/focus/ih/articles/crimeguide7.html

7. KENT FREDERICK, K. (2002) Network intrusion detection signatures, part 2. Securityfocus. http://online.securityfocus.com/infocus/1534

8. COUNCIL OF EUROPE. (2001) Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

9. CANO, J. (2001) Credenciales para investigadores forenses en informática. Certificaciones y entrenamiento. Revista Electrónica de Derecho Informático. No.38. Septiembre. http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=114090

10. FARMER, D. y VENEMA, W. (1999) Computer forensic analysis Class Handouts. Http://www.fish.com/forensics/

Bibliografía

SKOUDIS, E. (2002) Counter Hack. A step by step guide to computer attacks and effective defenses. Prentice Hall.

CASEY, E. (Editor) (2002) Handbook of computer crime investigation. Academic Press.

SCHULTZ, E. y SHUMWAY, R. (2002) Incident Response. A strategic guide to handling systems and network security breaches. New Riders.

CHIRILLO, J. (2001) Hack attacks revealed. John Wiley & Sons.

MANDIA, K. y PROSISE, C. (2001) Incident Response. Investigation Computer Crime. McGraw Hill

CASEY, E. (2000) Digital evidence and computer crime. Academic Press.

GARFINKEL, S. y SPAFFORD, G. (1996) Practical Unix and Internet Security. Second Edition. O'Really & Associates.