INFORMATICA FORENSE UN ALIADO EN LA ESTRATEGIA DE CIBERSEGURIDAD IMPLEMENTADA EN COLOMBIA

Robles Pallares Javier Leonardo
jleonardor@gmail.comNombre Institución
Universidad Piloto de Colombia

Resumen— Con los lineamientos de política para ciberseguridad diseñados por el Departamento Nacional de Planeación (DNP) a través del Consejo Nacional de Política Económica y Social (CONPES) en Colombia, la informática forense adquiere vital importancia y provee de herramientas técnicas, investigativas y jurídicas a los estamentos gubernamentales que tienen el compromiso de garantizar la seguridad de la información.

Índice de Términos- Informática forense, ciberseguridad, ciberataques, ciberdelito.

I. INTRODUCCIÓN

Las relaciones comerciales, económicas y culturales de los países, y las relaciones sociales de sus habitantes, dependen y se facilitan gracias a las nuevas tecnologías e infraestructuras de la información y las comunicaciones. Estas nuevas tecnologías desarrollaron un nuevo ámbito de interrelacionarnos llamado el ciberespacio, un espacio globalizado que día a día crece en relevancia política, social, económica y estratégica, lo que hace necesario articular unos lineamientos de ciberseguridad y ciberdefensa que gestione los riesgos que amenazan su funcionamiento.

La estrategia de ciberseguridad colombiana demuestra que el estado está dispuesto a enfrentar un ataque informático coordinado no solo en aspectos técnicos si no también preparados con una legislación idónea, si bien el país cuenta las leyes necesarias para la dar cumplimiento a la defensa de sus intereses y el de sus ciudadanos en el ciberespacio requiere de herramientas que le permitan prevenir, detectar, corregir los incidentes informáticos que ocurran en las entidades estatales y privadas al interior del país. En este punto la informática forense juega un papel sobresaliente pues ayudará con el material probatorio requerido para juzgar a un ciberdelincuente y brindará la posibilidad de recoger información sobre los atacantes y sus técnicas.

II. CIBERSEGURIDAD EN COLOMBIA

El impacto mundial de acciones como las creadas por grupos como Anonymous o LulzSec implicados en varias operaciones dirigidas contra las autoridades gubernamentales de orden local y nacional, Presidencia de la República, el Senado de la República, portales del gobierno y de los Ministerios de Defensa, del Interior y Justicia, y Cultura entre otros, instituciones financieras, compañías petroleras, Consejo Nacional Electoral, dejando fuera de servicio sus páginas o servicios web por varias horas.

La aparición de software malicioso (malware) con un preciso enfoque geográfico o enmarcado dentro de un sector industrial concreto y un grado de

[1]Ingeniero de Telecomunicaciones - Universidad de Pamplona.
Estudiante Especialización Seguridad Informática – Universidad Piloto de Colombia.
Estudiante Diplomado Informática Forense - Universidad Piloto de Colombia.

sofisticación cada vez mayor, con la inclusión de capacidades como identificar contraseñas, conversaciones, micrófonos, la propiedad de transformarse, replicarse y propagarse de manera automatizada; desarrollado con técnicas de criptografía avanzadas y complejas, aprovechando y haciendo uso de vulnerabilidades "zero-day" (hasta el momento desconocidas), son apenas una muestra de las nuevas amenazas y riesgos a los que estamos expuestos en el ciberespacio, el cual hoy en día se considera el quinto dominio para temas de relevancia de seguridad nacional.

La estrategia nace partiendo del hecho que el estado Colombiano no contaba con unos lineamientos o estrategia clara ante las amenazas cibernéticas, se habían realizado grandes avances a nivel legislativo con la creación de leyes como la 1273 y 1288 ambas decretadas el año 2009 estas no tenían niveles de aplicabilidad esperados, por su parte el estado no contaba con la capacidad para enfrentar las amenazas provenientes del ciberespacio, presentaba grandes debilidades y pese a que existían iniciativas gubernamentales, privadas y de la sociedad civil, para contrarrestar el efecto de las amenazas y posibles ataques cibernéticos, no había una coordinación apropiada entre las instituciones. El desarrollo de la estrategia de ciberseguridad es una respuesta para enfrentar los efectos del ciberdelito los cuales hacen parte de una realidad de defensa nacional.

El año 2011 el gobierno nacional, encabezado por del Departamento Nacional de Planeación (DNP) consciente de la problemática descrita anteriormente y del aumento de la capacidad delincuencial en el ciberespacio, aprobó, a través del Consejo Nacional de Política Económica y Social (CONPES) el documento denominado "*lineamientos de política para ciberseguridad y ciberdefensa 3701*" del 14 de julio de 2011, con la divulgación de estos lineamientos Colombia se convierte en el primer país de Latinoamérica en adoptar una estrategia para prevenir y enfrentar delitos cibernéticos.

Este documento traza como objetivo central de esta política el fortalecimiento de la capacidad del país para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito del ciberespacio, a su vez, define tres objetivos específicos:

1. Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas, para proteger la infraestructura crítica nacional.
2. Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa
3. Fortalecer el cuerpo normativo y de cumplimiento en la materia.

xDentro de los lineamientos de política para ciberdefensa y ciberseguridad se precisó la creación del colCERT como el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, prestando soporte y asistencia a los demás organismos; así como proveer información de inteligencia informática. La misión central del colCERT es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del estado Colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. Adicionalmente se crean los siguientes dos organismos:

- CCP: Equipo que designó la Policía Nacional, el cual se encarga de dar respuesta operativa a los delitos cibernéticos. El CPP tiene dentro de su estructura el Comando de Atención Inmediata Virtual también llamado CAI Virtual, quien recibe toda la información y reportes por parte de ciudadanos, colaboradores y víctimas de delitos cibernéticos. Esta entidad ya es una realidad.
- CCOC: Concebido para fortalecer las capacidades técnicas y operativas a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de

protocolos de ciberdefensa; así como desarrollar capacidades de neutralización y reacción ante incidentes informáticos. El CONPES recomienda que este en cabeza de las fuerzas militares.

La preparación en seguridad informática de esta nueva "fuerza" se plantea de una manera gradual. En una primera fase se capacitan a los funcionarios que estén directamente involucrados en la atención y manejo de incidentes cibernéticos y luego se extenderá a otras instituciones del Gobierno y al sector privado, con el apoyo de los ministerios de Educación y de las Tecnologías de la Información.

III. INFORMATICA FORENSE

Con el establecimiento de una estrategia de ciberseguridad, la creación de organismos de coordinación y ejecución anteriormente descritos, y una legislación que soporta estos procesos, se hace necesario contar con mecanismos que permitan:

- Conocer del accionar de grupos o personas relacionadas con delitos informáticos que puedan perturbar el curso normal de las actividades que se realizan en el ciberespacio, operaciones que pueden ser financieras, civiles, gubernamentales, etc.
- Realizar la reconstrucción de un evento delictivo de un modo legítimamente admisible ante las instancias legales.

Dichos mecanismos son sustentables a través de la informática forense la cual por medio de la aplicación del método científico y técnicas analíticas permiten la obtención de la mayor cantidad de información digital de un incidente informático para su posterior análisis, a esta información recolectada se le conoce con el nombre de evidencia digital.

Debido a la importancia que en su momento empezaba a tomar la informática forense el grupo de países industrializados, denominado G8 estableció unas recomendaciones para el tratamiento de las evidencias digitales:

- Todos los principios generales de procedimientos y técnicas forenses deben ser aplicados cuando se manipulen pruebas digitales.
- Cuando sea necesario que una persona tenga acceso a una prueba digital original, dicha persona debe estar formada para ese propósito.
- En la manipulación de pruebas digitales, las acciones que se lleven a cabo no deben alterar dicha prueba.
- Toda actividad relativa a la recogida, acceso, almacenamiento, o transferencia de pruebas digitales debe ser completamente documentada, conservada y disponible para su estudio.
- Cada persona es responsable de todas las acciones tomadas con respecto a la prueba digital mientras dicha prueba esté a su cargo.
- Cualquier institución o grupo, que sea responsable de la recogida, acceso, almacenamiento, o transferencia de una prueba digital, es responsable de cumplir y hacer cumplir estos principios.

A. Evidencia Digital

Cuando la evidencia digital se compara con su homóloga (evidencia documental) quedan claras varias diferencias, la evidencia digital es "frágil" pues permite la realización de copias no autorizadas de la misma, borrar, alterar sin dejar rastros de la realización de estas actividades, la volatilidad de la información al momento de un incidente informático es otro gran inconveniente que presenta este tipo de evidencia por el riesgo que implica perder información relevante para la investigación que se esté realizando.

Las pruebas digitales deben entenderse como material probatorio básico que requieren una revisión detallada sobre cómo se debe realizar la creación, recolección, custodia y cómo se presentan en una causa judicial o una investigación al interior de una empresa para aportar con precisión factores que ayuden la toma de decisiones en relación al incidente investigado. En ese orden de ideas se debe contar con el conocimiento técnico de los medios electrónicos y técnicas forenses y probatorias.

La debe tener especial cuidado en cada una de las etapas por la que pasa una evidencia cuando será utilizada en un proceso judicial o al interior de una organización, si no se llevan a cabo los procedimientos correctamente el resultado será que cualquier evidencia obtenida durante el proceso no podrá utilizarse en la investigación, carecerá de todo credibilidad y estarán bajo un manto de duda.

La adquisición de una evidencia digital será en la mayoría de los casos la primera actividad en una actividad forense. Se debe contar con la preparación adecuada y las herramientas correctas, cualquier error puede provocar la contaminación o pérdida de la evidencia y esto puede causar la inadmisibilidad en la corte en un eventual juicio.

Mantener y preservar la información una vez se ha obtenido de los dispositivos investigados es de vital importancia y se debe realizar un procedimiento denominado cadena de custodia, en el cual se informen los traslados, posesión y quienes tuvieron accesos a las pruebas. La cadena de custodia debe cumplirse desde la adquisición de la prueba hasta su posterior presentación en los estrados judiciales.

En la realización del análisis forense de cada una de las evidencias recolectadas es fundamental contar con las herramientas adecuadas así como el conocimiento, experiencia e intuición del investigador. Un error en estos procedimientos puede alterar la prueba y la deja inaceptable.

Como se puede observar, en la informática forense la evidencia digital desarrolla un papel fundamental ya que para poder demostrar un supuesto se debe contar con todos los elementos de prueba que respalden la forma como se dio el incidente y permitan responder 6 preguntas clave: Qué, Quién, Cómo, Cuándo, Dónde y Por qué.

Por esa razón es muy importante que se cumplan cabalmente todos los procedimientos en la obtención y manejo de la evidencia ya que su confiabilidad representa nuestro único elemento de prueba para demostrar algo.

B. El aliado

La informática forense se transforma en un aliado de la ciberseguridad en la medida en que los organismos implementen sistemas para conocer los vectores de ataques, herramientas utilizadas por los atacantes y objetivos buscados. Estos objetivos son posibles con la implementación de ambientes configurados y controlados por estas organizaciones del estado con el único fin de que sean atacados por delincuentes. Estos sistemas son mejor conocidos como HoneyPots, al hacer un uso extendido de estas trampas digitales se lograran detectar e investigar ataques reales en ambientes preparados para tal fin, esto conlleva a que nuestros especialistas estén en preparación continua sin que este comprometida infraestructura critica del país como los sistemas de control industrial encargadas de las estaciones de bombeo, sistemas eléctricos, sistemas ICS o Scada, etc.

Estas trampas brindan variados beneficios, a continuación se nombraran los más representativos:

- Atraer atacantes a sistemas informáticos que se asemejan a infraestructuras reales, lo que ayudara a tener conocimiento de los patrones de ataques, perfilar atacantes, detección de nuevos malware y de realizar posibles individualizaciones de atacantes.

- Permitirá comprobar la seguridad de una nueva plataforma desarrollada, lo cual ayudara a conocer posibles vulnerabilidades antes de salir a producción.
- Realización de estadísticas de ataques que puedan ser fácilmente compartidas con CERT de otros países sin poner en riesgo información de seguridad nacional (No se está revelando información secreta)
- Permite definir tendencias respecto de las actividades del atacante, activación de sistemas tempranos de alarma, predicción de ataques e investigaciones criminales.

Los CERT a nivel mundial que realizaron la implementación de estos sistemas encontraron como su principal desventaja la insuficiente documentación y la necesidad de técnicos altamente capacitados. En este último punto surge la principal inquietud. ¿Están las universidades preparando los expertos en seguridad que los organismos del estado y el sector privado requieren o tendrán estos que seguir contratando a aquellos de los que antes se defendían?

IX. CONCLUSIONES

- En la capacitación especializada en seguridad de la información y las líneas de investigación de ciberdefensa y ciberseguridad deben trabajar el sector gubernamental y la academia para la formulación, creación y puesta en marcha de contenidos actualizados al alcance de las personas interesadas de acceder a las mismas.

- Es necesario cerrar la brecha y el vacío jurídico por parte de los ingenieros y la policía, y la falta de capacidades técnicas entre los abogados, para cumplir y/o formular las leyes necesarias; convirtiendo la rama legal y la técnica en ramas complementarias

- Este es un reto colectivo, que no solo involucra a las organizaciones estatales y las personas que son objetivos permanentes de los ciberdelincuentes por sus actividades. Es un desafío para la sociedad, el estado, los administradores de justicia, jueces y fiscales, que deben estar preparados no sólo en el conocimiento de las leyes y la jurisprudencia, sino en el correcto conocimiento del contexto tecnológico, informático y de cómo estos recursos ayudan a realizar actividades delictivas.

- No sirve de nada que los organismos creados realicen todos los procesos de investigación si al finalizar una investigación las pruebas obtenidas no tendrán una validez o peso legal debido a las carencias de las leyes.

- El escaso conocimiento en el área por parte de las organizaciones, jueces, fiscales y abogados. Este factor es importante ya que muchos de los delitos o incidentes informáticos no se denuncian debido a que se asume que será costoso el proceso y al final no se tendrán resultados.

- Los organismos de justicia deben iniciar un proceso de concientización pues muchos de los jueces mantienen una verdadera resistencia al cambio, lo que conlleva al rechazo de pruebas o evidencia obtenida digitalmente.

REFERENCIAS

[1] Departamento Nacional de Planeación Documento CONPES 3701Lineamientos de Politica para Ciberseguridad y Ciberdefensa [en línea]. Julio 14 de 2011

[2] Centro Cibernético Policial. CAI Virtual – Policía Nacional de Colombia [en línea]. Disponible en <http://www.ccp.gov.co/>

[3] Cano, Jeimy. (2003). Admisibilidad de la evidencia digital. De lo conceptos legales a las implementaciones

técnicas. En GECTI. Derecho de Internet & Telecomunicaciones. Universidad de los Andes – Legis

[4] HONEYPOTS, MONITORIZANDO A LOS ATACANTES. Observatorio de Seguridad de la información. INTECO. Marzo 16 de 2010

[5] DIGITAL EVIDENCE AND COMPUTER CRIME. Eoghan Casey, Academic Press. Londres, 2004.

[6] El peritaje informatico y la evidencia digital en Colombia. Conceptos, retos y propuestas. Grupo de Estudios en Internet. Ediciones Uniandes. Mayo 2010

[7] G8 Proposed Principles For The Procedures Relating To Digital Evidence; International Organization on Computer Evidence (IOCE); <http://www.ioce.org>. Marzo de 1998