THE CYBER SECURITY FORUM INITIATIVE - CSFI

INFORME DE LECCIONES APRENDIDAS

Ejercicio Tabletop: Interrupción de Comunicaciones a Consecuencia de un Ciberataque

6 de mayo 2013, Madrid España | www.csfi.us

Índice

1. Introducción

CSFI ha completado recientemente el desarrollo del ciberejercicio Tabletop (TTX), tras varios meses de trabajo llevado a cabo por miembros del proyecto en diferentes localizaciones de toda España. El propósito de este ejercicio práctico es poner en relieve la necesidad de fomentar la colaboración entre diversas áreas profesionales y de conocimiento, con el fin de fortalecer la concienciación acerca de la importancia de la seguridad cibernética para la comunidad internacional.

La perspectiva multidisciplinar a partir de la cual se ha concebido y realizado el ejercicio ha llevado a que tanto los roles de experto como en los de observador hayan sido desempeñados por profesionales de diferentes ámbitos:

Expertos	**Observadores**
– Ejecutivos de empresas del sector de la seguridad y las nuevas tecnologías. – Académicos universitarios. – Periodistas especializados en seguridad y nuevas tecnologías. – Expertos en protección de datos. – Cuerpos y fuerzas de seguridad del Estado	– Ejecutivos de empresas del sector de la seguridad y las nuevas tecnologías. – Académicos universitarios. – Periodistas especializados en seguridad y nuevas tecnologías. – Expertos en protección de datos. Cuerpos y fuerzas de seguridad del Estado

El día 6 de mayo se desarrolló el primer ejercicio de tipo “Tabletop” realizado por CSFI en España que desde su inicio, en diciembre de 2012, hasta su presentación, ha sido llevado a cabo por profesionales españoles de procedencia multidisciplinar. En dicha presentación se ha expuesto paso por paso a un grupo de expertos y observadores de diversos perfiles profesionales el desarrollo de un ciberataque en un escenario ficticio creado a tal efecto. En cada una de las tres partes en que se divide la exposición, se solicita al panel de expertos que intervengan y expongan sus decisiones tal y como si el escenario estuviera ocurriendo en realidad.

2. Breve descripción del escenario

El escenario creado para el ejercicio se basa en los efectos que tiene la interrupción de las comunicaciones telefónicas y a raíz de internet en una región determinada. Este problema se deriva de un ataque cibernético a las infraestructuras de distribución del principal operador de telefonía e internet en la zona. Dicho ataque ha sido perpetrado por un grupo anarquista que pretende desacreditar al gobierno del Estado al que pertenece la región afectada, que se encuentra sumido en una profunda crisis económica, política y social.

El corte de comunicaciones tiene lugar coincidiendo con la celebración de una huelga general en todo el país, y ha sido previamente anunciado por los atacantes a través de las redes sociales con el fin de desinformar a los ciudadanos y a los medios de comunicación, haciendo creer que los culpables pueden haber sido los sindicatos convocantes. El grupo continuará con esta estrategia durante la duración del ataque, tratando de hacer llegar su mensaje a todas las otras zonas en las que internet continúa funcionando, mientras que el gobierno, la prensa y la empresa afectada empezarán a reaccionar.

El objeto del análisis que se realiza a lo largo de las tres partes en que se divide el ejercicio consiste en las dimensiones comunicativas del ataque, así como la actuación que seguirán en esta línea el gobierno y los periodistas.

3. Lecciones aprendidas en el ejercicio

De las opiniones expuestas por los expertos y observadores se extraen las siguientes ideas:

Tras exponer el escenario del ciberejercicio y quedar de manifiesto que lo ocurrido es consecuencia de un ciberataque (si bien esto no se habría comprobado todavía por parte del gobierno y las fuerzas y cuerpos de seguridad del Estado en el escenario que se ha planteado), se ha constatado que la actuación a seguir en esta fase por el Gobierno debe centrarse en una serie de puntos:

- El gobierno debe tener un plan de acción listo para ser activado en situaciones similares. Debe actuar frente a un ciberataque como si se tratara de cualquier otro tipo de crisis.
- Se debe concretar el nivel de actuación, teniendo en cuenta si el que toma decisiones es la autoridad de la región, o bien de la nación. Tiene que haber un plan de actuación de nivel Superior para todo el país, no sólo para la región afectada. Hay que medir los tiempos, localizar a los

responsables no es urgente y no debe hacerse con prisas, Las investigaciones llevan su tiempo y se hacen mal bajo presión.

- En las declaraciones que se hagan es fundamental decir la verdad, no toda la verdad por si hay datos no contrastados, pero sí la veracidad de los hechos, dejando aparte hipótesis y líneas de investigación, ya que decir la verdad, o al menos parte de ella, tiene repercusiones positivas a la larga. Lo más importante es transmitir credibilidad, evitando la alarma social. Así, el gobierno debe tratar de tranquilizar a los ciudadanos explicándoles que por ahora no conoce las causas del ataque, solo sus efectos, pero que cuenta con un plan de actuación y gestión de crisis. Dicho Plan debe comunicarse desde un punto de vista del ciudadano para no crear alarmas innecesarias, ya que un plan de crisis presentado tal cual puede crear esas alarmas.
- La importancia de esta primera comunicación es muy alta. El gobierno debe dotarse de un portavoz para informar a la prensa. Debe proporcionar información veraz pero no toda la información por seguridad. Hay que mantener la calma, no convertirse en parte del problema. El interlocutor debe ser de rango medio, no un ministro, y ser siempre la misma persona. En principio ya están definidas las funciones y composición de las portavocías de los gobiernos. Deben contar lo que les cuentan a ellos, pero sin entrar en detalles técnicos. También deben evitar discordancias con el discurso de la empresa atacada.
- En las declaraciones públicas ante los medios de comunicación es necesario insistir en el mensaje de que se está colaborando con las fuerzas y cuerpos de seguridad del Estado (FCSE). En este sentido, es importante no facilitar muchos datos, pues una vez expuestos los medios de comunicación preguntan y persiguen esas líneas de actuación, lo que genera presión en la investigación con posibles efectos negativos por parte de la acción de las FCSE.
- Es fundamental tener en cuenta que, ante una crisis de esta magnitud, se dará por parte del gobierno una “lectura política de los hechos”. Lo que se diga por parte de los técnicos, tendrá o no que ver con los datos facilitados.
- Las preguntas claves que hay que saber responder son: ¿Cuál es el impacto real de esta situación? ¿Cuándo es noticia?; y una vez conocido por el Gobierno, ¿cuándo preguntarán los medios?, con el fin de evitar posibles filtraciones. Es imprescindible fomentar la colaboración público-privada y la ayuda a la población por medio de datos o pistas, así como poner en marcha mensajes a través de redes sociales y activar de inmediato acciones de monitorización y vigilancia.

Por lo que respecta a la actuación de los medios de comunicación:

- En primer lugar, no se les considera infraestructura crítica.

- En muchos casos, tenderán a enfocar los hechos desde un punto de vista “amarillista”, buscando datos y enfocando las noticias en función de sus intereses para generar atención y audiencia. Los periodistas deben ser responsables e ir contándolo evitando el pánico.
- La prensa debe contactar con medios locales y con ayuda de una unidad móvil ir sacando información del comité de huelga, de la empresa, y de los ciudadanos. Esa información la debe investigar/contrastar. También deben de tratar de obtener más información del gobierno.
- Hay que recurrir a periodistas especializados en telecomunicaciones para que su información sea veraz.
- Es necesario controlar cómo se comunica en las redes sociales, ya que puede ser algo imposible de gestionar. Se debe nombrar un moderador que monitorice y vigile las redes.

En la segunda fase del escenario, una vez los autores han reivindicado su responsabilidad en el ataque, el gobierno debe seguir las siguientes líneas a la hora de emitir mensajes:

- Ofrecer mensajes lo más concretos y específicos posible a la hora de informar a los ciudadanos; es necesario restablecer la normalidad e impedir rumores, si bien esto puede incluir no descartar otras hipótesis en las líneas de investigación. Deben darse mensajes más concretos sobre la credibilidad de la autoría, las medidas para paliar el impacto, los consejos y planes de actuación individuales a seguir y el alcance confirmado del problema. Además, es fundamental hacer ver que se está evitando la extensión del ataque a otras zonas, que hay una investigación en marcha y actuar de alguna manera para evitar las alarmas. Es urgente evitar el pánico, por lo que se recomiendo focalizar los mensajes en las comunicaciones que no se han visto afectadas, frente a las que sí han quedado interrumpidas.
- Respecto al mensaje de los atacantes, se recomienda No nombrar la cuenta de twitter, ni descartar ninguna hipótesis y hablar sólo de supuesta autoría, para así evitar dar notoriedad al grupo anarquista.

En lo que respecta a los medios a utilizar para transmitir estos mensajes, hay que tener en cuenta que:

- La aparición de las noticias relacionadas con el ataque en la prensa causará un “efecto llamada” de otros medios.
- Una de las claves radica en utilizar, junto con los medios tradiciones (radio, periódicos y televisión) las redes sociales y controlar los mensajes a través de ellas.
- Tiene que haber información constante del portavoz del gobierno, para contrarrestar así los rumores que aparezcan en la prensa. Dar información pertinente en cada momento. Es preferible emitir muchos comunicados y minimizar las ruedas de prensa.

En la última fase del ejercicio, habiéndose restablecido ya la normalidad, el gobierno debe seguir varios pasos para recuperar la confianza de la ciudadanía:

- Es imprescindible para mantener su autoridad que transmita que el que la hace la paga. En el corto plazo debe capturar y juzgar a los culpables.
- También hay que resaltar que la colaboración ciudadana es esencial, y tratar de incrementar los bajos niveles de dicha colaboración, así como transmitir que todo se puede volver a controlar gracias a los planes de actuación.
- Además, es necesario exaltar los resultados positivos, pero afrontando la vulnerabilidad manifiesta que se ha puesto de relieve con el ataque, por lo que se recomienda decir que se va trabajar en lo que sea, pero sin hacer promesas, así como reconocer que había cosas que no se estaba haciendo bien e incluso plantearse la posibilidad de depurar responsabilidades (dimisiones). También es muy importante canalizar las consecuencias, crear una oficina de atención a los afectados, informar sobre las investigaciones y recalcar que todo está solucionado.
- Por último, resulta esencial repetir mensajes positivos, acerca de la resolución de la crisis, la coordinación entre departamentos y la eficacia de las acciones de las FCSE. El mensaje a comunicar es que “podría haber sido peor si no se hubiera puesto en marcha un plan de estas características”.

Para conseguir este objetivo, el gobierno tendrá que vencer una serie de problemas y dificultades:

- La confianza debería haberse mantenido (no perdido), y en todo caso habría que afianzarla. Hay que hacerse la pregunta, ante un ciberataque que ha durado un período relativamente corto, sobre si todo ha acabado o si se van a producir nuevos ataques.
- Se debe evitar que la gran mayoría del sector de las telecomunicaciones en la región, y en el país, esté en manos de un solo operador, lo que puede dar pie a una intervención del mismo.
- La posibilidad de que haya que anular algunos mensajes en las redes sociales reabre el debate sobre la censura y sobre la posibilidad de que la ley pueda ser reformada para que se permitan limitaciones temporales de derechos de los ciudadanos durante la duración de la crisis.
- Se plantea la necesidad de constituir un departamento de seguridad nacional que evalúe lecciones aprendidas y mejore los planes.
- También se debe buscar el máximo consenso entre los medios, el gobierno y la oposición, para no hacer dudar al ciudadano.

4. Conclusiones finales

A modo de conclusión, han destacado las siguientes debilidades en el ámbito de la ciberseguridad:

- Es imprescindible una toma de conciencia del problema por parte de la sociedad, así como de la dificultad de abordar este tipo de ciberincidentes y ciberataques en el mundo real.
- No se conoce ni las vulnerabilidades ni las oportunidades
- Muchos ataques contra la ciberseguridad quedan impunes debido a la falta de castigo. Si no existen sanciones legales o se adoptan medidas que impliquen consecuencias reales para los autores de este tipo de ataques, estos podrán seguir cometiéndolos sin temer las consecuencias que les puedan acarrear las posibles penas que se les puedan imponer.

5. Comentarios sobre el desarrollo y la metodología del ejercicio

- Los expertos y observadores que han participado en el Ciberejercicio TTX valoran de un modo especialmente positivo las perspectivas multidisciplinares que se han seguido en el análisis de los dos escenarios.
- También se muestran muy satisfechos con el formato, que consideran enriquecedor, y resaltan su interés por volver a realizar un análisis similar sobre el impacto de los ciberataques en otras áreas temáticas. En este sentido, subrayan que el proceso de articulación de respuestas frente a un ciberataque es similar a los que se plantean para solucionar otras crisis y problemas.

6. Equipo Responsable de la Elaboración del Escenario

A CSFI le gustaría agradecer el trabajo realizado durante este ciberejercicio a las siguientes personas, que con su gran esfuerzo y dedicación han contribuido a la creación de los escenarios:

David González (Team Leader)
Periodista. Investigador en Relaciones Internacionales, Seguridad y Defensa

Elena Matilla Rodríguez (Facilitadora de la presentación TTX)
Senior Information Security Consultant, Isdefe

Dr. Igor Sobrado
Committer, The OpenBSD Project

Gabriel Cortina
Director Comercial. Grupo ATENEA, Seguridad y Defensa

Adolfo Hernández
Gerente de seguridad de la información de Ecix Group. Miembro de THIBER-ICFS.

Enrique Fojón
Ingeniero Superior en Informática. Miembro de THIBER,una iniciativa del Instituto de Ciencias Forenses y de la Seguridad (ICFS) de la Universidad Autónoma de Madrid

Amal-Abu Warda Pérez
Abogada. Investigadora en Relaciones Internacionales

Ramón Miralles López
Cyber exercises expert in the CEI list from ENISA

David Scarlatti
Voluntario CSFI

Lydia Kostopoulos, PhD (Coordinadora del Ciberejercicio)
Cyber Security Forum Initiative (CSFI)

Edición: David González