THE CYBER SECURITY FORUM INITIATIVE - CSFI


INFORME DE LECCIONES APRENDIDAS

# Ejercicio Tabletop: Incidente en Gasoducto

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**

- Estratega militar.
- Ejecutivos de empresas relacionadas con infraestructuras críticas.
- Ejecutivos de empresas del sector de la seguridad y las nuevas tecnologías.
- Académico universitario.
- Expertos en protección de datos.
- Cuerpos y fuerzas de seguridad del Estado.

**Observadores**

- Gestor de riesgos.
- Periodista especializado en seguridad y nuevas tecnologías
- Ejecutivos de empresas del sector de la seguridad y las nuevas tecnologías.
- Cuerpos y fuerzas de seguridad del Estado.
- Consultor de ciberestrategia

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 ejercicio se desarrolla en un escenario en el que se analizan las consecuencias de un ciberataque sobre una compañía de producción y distribución de gas cuyas instalaciones han sido catalogadas como infraestructura crítica. Los efectos de dicho ataque no se limitan al plano virtual, sino que tienen una repercusión real para la imagen y la actividad de la empresa, así como para el entorno en el que ésta se desarrolla.

Se ha convenido en que el ciberataque sea perpetrado por un ex trabajador de la compañía, que fue recientemente despedido en el marco de un expediente de regulación de empleo (ERE). El perfil de este empleado es el de un profesional con una alta cualificación técnica y profundos conocimientos acerca de la organización en cuanto al funcionamiento y sistemas informáticos, de procesamiento de datos empleados a nivel interno en la empresa, lo que le permite acceder a información sensible para la misma.

En un primer momento, el atacante aprovecha estas capacidades para introducirse en los sistemas internos de la compañía. Una vez ha conseguido acceder a los mismos, comienza a explotar vulnerabilidades técnicas de dichos sistemas desde un equipo externo ubicado en las proximidades de su residencia.

A partir de estas premisas se ha delimitado el objeto del análisis en torno al que se ha estructurado el desarrollo del ejercicio. Este último se ha dividido en tres fases, en las que se estudian cuáles son las primeras reacciones frente a los efectos del ciberataque, las decisiones que han de tomarse para controlarlo, y las medidas necesarias para impedir que puedan producirse situaciones similares en el futuro.

## 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 se tiene constancia de que la compañía se encuentra sufriendo un ciberataque, aunque por el momento no se están apreciando consecuencias de importancia, más allá de una pérdida de control sobre la presión de las válvulas del gasoducto. Las actuaciones a seguir en este momento deben centrarse en los siguientes puntos:

- Es necesario identificar, aislar y controlar el ciberataque a nivel técnico.

- Se debe identificar el plan de acción a seguir, determinando cuáles han de ser las acciones prioritarias y asignando responsabilidades. Por este motivo es recomendable contar previamente con un protocolo de actuación diseñado específicamente con el fin de hacer frente a posibles ciberataques. De este modo, se ha de buscar garantizar la seguridad de las instalaciones y los empleados y contar con herramientas, mecanismos y procedimientos de gestión de riesgos.
- La compañía debe gestionar qué información se divulga en función del impacto que esté teniendo el ciberataque, con el fin de proteger su imagen y su reputación, así como la de sus empleados. Existen discrepancias entre los expertos acerca de cuándo, cómo y cuanta información se debería comunicar.
- Aunque no hay unanimidad sobre la pertinencia de comunicar o no este ciberataque y sus efectos a la opinión pública, sí se coincide en la necesidad de informar a los organismos que procedan: cuerpos y fuerzas de seguridad del Estado, los correspondientes equipos de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés) y los correspondientes centros de protección de infraestructuras críticas.

En la segunda parte del escenario, el ciberataque se ha materializado ya en forma de pérdidas económicas, en daños en la infraestructura y en repercusiones negativas para la imagen sobre la compañía. Aunque por el momento dichos daños son limitados, cabe la posibilidad de sufrirse otras consecuencias mayores en un corto espacio de tiempo. Tras identificar y evaluar el ciberataque, se extraen los siguientes consejos para la dirección de la compañía, que podría tener que verse obligada a efectuar un cambio en sus prioridades en pleno ataque y a crear un gabinete de crisis para tratar de esclarecer qué ha sucedido, minimizar el impacto e identificar al autor:

- Se reitera la necesidad de tratar de mantener el control sobre todo el sistema y reforzar la seguridad de la zona de dicho sistema que se ha quedado aislada a raíz del ciberataque, y que ha sufrido la mayor parte de los daños provocados por el mismo.
- Se recomienda suspender el control informatizado de las zonas del sistema que se hayan visto afectadas o que puedan estarlo potencialmente y sustituirlo por el control manual, evitando así que el ataque dañe más aún las infraestructuras. Esto implicaría desactivar el software.
- Se debe identificar qué ha sucedido hasta el momento, cuáles son los daños estructurales y económicos sufridos y poner en marcha las gestiones necesarias para minimizar su impacto.
- Hay que priorizar los daños que pueden afectar a las vidas humanas y adoptar acciones encaminadas a minimizarlos.

En la última parte del ejercicio, una vez se constata que el causante del ataque fue un antiguo empleado descontento, se ha logrado controlar el ciberataque y recuperar el control sobre todo el sistema, se analizan las medidas que deberían adoptarse en lo que atañe a la gestión del personal de la empresa para que esta situación no llegue a reproducirse:

- Uno de los asuntos que más interrogantes plantean es el que surge en relación con los futuros despidos de empleados que tienen acceso a información sensible, con el fin de evitar nuevos casos similares.
    - Así, se plantea la necesidad de implementar de forma estricta un sistema para controlar la fuga de información, Data Loss Protection (DLP), y buscar, sobre todo, los sistemas e instrumentos que permitan tener un control total sobre posibles fugas de información.
        - Para conseguir este objetivo se sugiere el uso de un circuito cerrado de comunicaciones mediante dispositivos cifrados, comunicaciones seguras y control de dispositivos extraíbles entre otros.
        - En cuanto a la arquitectura técnica de comunicaciones, se propone controlar el envío de información corporativa a internet mediante el correo electrónico, proxies de acceso exterior o accesos remotos.
        - Se ha mencionado la existencia de empresas especializadas en el proceso de despido (Out placement), que pueden realizar una labor esencial para evitar este tipo de situaciones.
- Como consecuencia de este debate, los expertos se han centrado también en la importancia de los procesos de contratación.
        - Se recomienda realizar test e informes psicológicos.
        - Gestión detallada del personal categorizando a los empleados según el nivel de acceso a información sensible.
        - Se recomienda realizar informes pre-laborales que incluyan antecedentes profesionales y personales, como los estudios o la vida personal.
        - A su vez, se ha hecho hincapié en la necesidad de establecer acuerdos de confidencialidad entre la compañía y los empleados durante el proceso de contratación.
        - Se ha mencionado también la potencial utilidad que puede tener un sistema de vigilancia mutua equilibrado y responsable entre los empleados.

## 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 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:

**Francisco Caballero Calzada (Team Leader)**
Project Manager, S21sec

**Federico Bolívar Hernández CISA, CISM, CRISC, CGEIT, CSFI-DCOE**
**(Facilitador de la presentación TTX)**
Senior Information Security Engineer

**Ana Belén Perianes Bermúdez**
Doctoranda en Seguridad y Defensa Internacional
Experta en Seguridad en el Mediterráneo, Próximo Oriente y Oriente Medio

**Gema Sanchez**
Prof. Ciencia Política y de la Administración
Universidad Complutense de Madrid

**Mario Guerra Soto**
Ingeniero de Telecomunicación. Especialidad Telemática
Máster en Seguridad de Tecnologías de la Comunicación
Ingeniero de la Administración Pública

**Alfredo Reino, CISSP-ISSMP, CISA, CISM, GCFA, C|EH**
Security Solutions Architect
Verizon Enterprise Solutions

**Vanesa Latas Núñez**
Licenciada en Derecho
Especialista en RR.II, Diplomacia y Seguridad

**Albert Puigsech Galícia**

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

Edición: David González.