Hablando de ciberseguridad parte XIII

Source:
Tomado de Cubadebate Omar Pérez Salomón

En el artículo No. 46 del Decreto-Ley No. 370, sobre “La informatización de la sociedad en Cuba”, publicado en la Gaceta Oficial Ordinaria de 4 de julio de 2019, se definen las Infraestructuras Críticas de las Tecnologías de la Información y la Comunicación como aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

Precisamente sobre este importante asunto estaremos hablando con Miguel Gutiérrez Rodríguez, Director General de Informática del Ministerio de Comunicaciones de Cuba.

- Teniendo en cuenta la definición citada, ¿cómo está organizada la protección de las infraestructuras críticas en nuestro país?

- Como se plantea en el Decreto No. 360, sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, se ha creado un Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC que tiene un conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de las infraestructuras críticas de las TIC, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como un flujo de información que abarque a todos sus integrantes.

En este momento estamos actualizando el Catálogo Nacional y el plan para la Protección de las Infraestructuras Críticas de las TIC, que tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

- ¿Mencione algunos de los sectores y actividades que poseen infraestructuras consideradas críticas?

- Para cualquier país existen sectores que son estratégicos por su impacto en la economía, en la sociedad, en la seguridad y defensa nacional. Entonces, sus redes informáticas e infraestructura se consideran críticas, tal es el caso de la Banca, telecomunicaciones, Información y Comunicación Social, energía, recursos hidráulicos, transporte, determinadas industrias, los órganos de la defensa, entre otros.

En el Decreto se estable que los jefes de estas entidades responden por la garantía de la confidencialidad, integridad y disponibilidad de los datos sobre infraestructuras críticas de las TIC a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada; además garantiza que el personal vinculado a las mismas esté capacitado para su utilización, posean compromiso político, ético y de responsabilidad social y material; así como que conozcan sus deberes y derechos específicos en relación con estas. También ejecutan las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten su funcionamiento.

- ¿Cuál fue el primer ataque cibernético conocido a una infraestructura crítica?

- Es un hito cómo en la década de 1980 se utilizó por primera vez un arma cibernética, cuando la CIA introdujo un software defectuoso en el sistema de operación del nuevo gasoducto transiberiano que debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia a países de Occidente, causando

grandes pérdidas económicas y contribuyendo al colapso de la URSS.

Así lo describió el Comandante en Jefe, Fidel Castro Ruz, en su reflexión, Mentiras deliberadas, muertes extrañas y agresión a la economía mundial:[1]

“El dossier, bajo el nombre de Farewell, llegó a la CIA (Agencia Central de Inteligencia de Estados Unidos, siglas en inglés) en agosto de 1981. Dejaba claro que los soviéticos llevaban años realizando sus actividades de investigación y desarrollo. Dada la enorme transferencia de tecnología en radares, computadoras, máquinas-herramientas y semiconductores de Estados Unidos a la Unión Soviética, podría decirse que el Pentágono estaba en una carrera armamentista consigo mismo.

“El Dossier Farewell también identificaba a cientos de oficiales de casos, agentes en sus puestos y otros suministradores de información a través de Occidente y Japón. Durante los primeros años de la distensión, Estados Unidos y la Unión Soviética habían establecido grupos de trabajo en agricultura, aviación civil, energía nuclear, oceanografía, computadoras y medio ambiente. El objetivo era comenzar a construir ‘puentes de paz’ entre las superpotencias. Los miembros de los grupos de trabajo debían intercambiar visitas a sus centros.

“Aparte de la identificación de agentes, la información más útil aportada por el Dossier la constituía la ‘lista de compras’ y sus objetivos en cuanto a la adquisición de tecnología en los años venideros. Cuando el Dossier Farewell llegó a Washington, Reagan le pidió al Director de la CIA, Bill Casey, que ideara un uso operativo clandestino del material.

“La producción y transporte de petróleo y gas era una de las prioridades soviéticas. Un nuevo gasoducto transiberiano debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia a través de Kazajstán, Rusia y Europa oriental hasta los mercados de divisas de Occidente.

Para automatizar la operación de válvulas, compresores e instalaciones de almacenaje en una empresa tan inmensa, los soviéticos necesitaban sistemas de control sofisticados. Compraron computadoras de los primeros modelos en el mercado abierto, pero cuando las autoridades del gasoducto abordaron a Estados Unidos para adquirir el software necesario, fueron rechazados. Impertérritos, los soviéticos buscaron en otra parte; se envió un operativo de la KGB a penetrar un proveedor canadiense de softwares en un intento por adquirir los códigos necesarios. La inteligencia estadounidense, avisada por el agente del Dossier Farewell, respondió y manipuló el software antes de enviarlo.

“Una vez en la Unión Soviética, las computadoras y el software, trabajando juntos, hacían operar el gasoducto maravillosamente. Pero esa tranquilidad era engañosa. En el software que operaba el gasoducto había un caballo de Troya, término que se usa para calificar líneas de software ocultas en el sistema operativo normal, que hacen que dicho sistema se descontrole en el futuro, o al recibir una orden desde el exterior.

“Con el objetivo de afectar las ganancias de divisas provenientes de Occidente y la economía interna de Rusia, el software del gasoducto que debía operar las bombas, turbinas y válvulas había sido programado para descomponerse después de un intervalo prudencial y resetear ?así se califica? las velocidades de las bombas y los ajustes de las válvulas haciéndolas funcionar a presiones muy por encima de las aceptables para las juntas y soldaduras del gasoducto.

“El resultado fue la más colosal explosión no nuclear e incendio jamás vistos desde el espacio. En la Casa Blanca, funcionarios y asesores recibieron la advertencia de satélites infrarrojos de un extraño evento en medio de un lugar despoblado del territorio soviético.

El NORAD (Comando de Defensa Aeroespacial Norteamericano) temía que fuera el lanzamiento de misiles desde un lugar donde no se conocía que hubiera cohetes basificados; o quizás fuera la detonación de un dispositivo nuclear. Los satélites no habían detectado ninguna pulsación electromagnética característica de las detonaciones nucleares".

- Otras infraestructuras críticas como las plantas nucleares de Irán o la red eléctrica de Venezuela han sufrido ataques cibernéticos.

- Así es. La aparición del gusano Stuxnet hizo más lento el funcionamiento de los motores de enriquecimiento de uranio de la central nuclear iraní de Bushehr, con el objetivo de retrasar el programa nuclear con fines pacíficos de Irán, pero atacó además a redes de varios países. El 60% de los ordenadores infectados se encontraban en ese país. Circuló en redes globales desde marzo del 2010 y el diario The New York Times hizo público el 16 de enero de 2011, opiniones de expertos militares y de Inteligencia norteamericanos, donde reflejaron que la central nuclear de Dimona (al sur de Israel) se convirtió en un laboratorio para examinar y ensayar el virus Stuxnet.

Se trató de un ataque particular y sofisticado, perpetrado por un equipo con acceso a abundantes recursos financieros, un elevado nivel de preparación y un profundo conocimiento técnico diseñado para espiar sistemas infectados, inutilizar plantas y causar daños en ambientes industriales.

- ¿Computadoras conectadas a redes informáticas de Cuba también fueron infectadas?

- El 13 de julio de 2011 se detectó la presencia del Stuxnet en redes cubanas. A partir de un estudio realizado por la empresa Segurmática, se conoció que este programa maligno instaló dos drivers o controladores, firmados digitalmente con un certificado de la compañía Realtek, significando que el autor tuvo acceso a la llave privada de este certificado, un secreto supuestamente muy bien guardado. El análisis realizado sobre esta cuestión por la empresa estadounidense Symantec, situó a Cuba en el lugar 14 de los países con más ordenadores infectados.

- ¿Qué valoración le merece las afectaciones a la red eléctrica de Venezuela ocurrido en marzo de 2019?

- En el artículo, "Venezuela bajo ataque: 7 apuntes sobre el shock eléctrico", publicado en el sitio Misión Verdad, se dan a conocer algunos elementos importantes de este sabotaje:

"Esta vez no hubo un ataque a subestaciones o a líneas de transmisión eléctrica, como se había ensayado en distintas ocasiones con anterioridad, según manuales de sabotaje de la CIA contra la Nicaragua sandinista de los 80, ya desclasificados.

"Cabe acotar que el software usado (llamado Scada) en el Sistema de Control Automatizado (SCA) que operativiza el funcionamiento de los motores es el creado por la empresa ABB, que desde hace años no trabaja en el país.

Esta empresa ABB, que en Venezuela trabajó como Consorcio Trilateral ABB (ABB Venezuela, ABB Canadá, ABB Suiza), diseñó un proyecto de modernización del Guri a finales de la década pasada, durante el gobierno de Hugo Chávez, en el que describe a profundidad tanto el sistema atacado como la organización básica del Guri.

"El analista geopolítico Vladimir Adrianza Salas, en entrevista con Telesur, relaciona el ataque con el consorcio. Explicó que el embalse del Guri requiere un sistema de control que técnicamente se llama sistema scada, el cual no es otra cosa que un sistema de supervisión, control y requisición de datos que permite, desde la perspectiva informática, controlar todos los elementos de generación de energía.

Si saboteas esto, saboteas el funcionamiento. Pero para sabotear esto necesitas dos cosas: o debes tener acceso desde afuera o debes tener complicidad interna para modificar los procesos.

“Precedentes de este tipo se encuentran en países atacados o presionados directamente por Estados Unidos, como Irak y el Líbano, donde los apagones fueron sistemáticos y de forma consecutiva, uno tras otro durante decenas de horas.

Las réplicas en la interrupción del suministro de energía responderían a estas secuencias de ofensivas que ya han sido experimentadas en otros contextos de guerra asimétrica e irregular”.

Por supuesto, se impone estudiar al detalle estas experiencias y adoptar las medidas necesarias para impedir ataques cibernéticos de esta naturaleza o de otro tipo.

[1] Fidel Castro Ruz: “Mentiras deliberadas, muertes extrañas y agresión a la economía mundial”, 18 de septiembre de 2007, Granma Digital.