CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Francisco Padilla Téllez
Especialización en Seguridad Informática, Universidad Piloto de Colombia

Resumen La ciberseguridad en infraestructuras críticas ha tomado importancia toda vez que van aumentando las amenazas informáticas y exista alguna afectación para los gobiernos y sus sectores industriales, por esto se hace necesario el crear, aplicar marcos de referencia y tomar las mejores prácticas de seguridad para la protección de los activos de información y que sean el insumo principal para la generación de las estrategias de seguridad nacional.

Abstract—This paper shows some guidelines, frameworks and best practices that should be considered for the protection and assurance of computer systems that are contained in critical infrastructure.

Key Words— Cybersecurity, Critical Infraestructure, Threat, Risk, Framework, Cyberdefense, Strategy.

1. INTRODUCCIÓN

El número de incidentes informáticos ha estado en aumento y los perfiles de los atacantes han pasado a ser de individuos en búsqueda de notoriedad a grupos organizados que cuentan con grandes presupuestos e incluso intereses de los gobiernos de algunos países.

Las tecnologías de la información y las comunicaciones están en continuo cambio y evolución a sistemas basados en tecnologías abiertas de uso común en TI, su objetivo es poder tener integración de los sistemas e infraestructuras y ello conlleva a que existan un mayor número de amenazas que puedan aprovecharse de las vulnerabilidades de estos sistemas informáticos. Por ello se hace necesario que las diferentes organizaciones gubernamentales e industriales opten por tomar medidas que permitan la protección y aseguramiento de sus infraestructuras críticas.

2. DESARROLLO

La ciberseguridad es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales.

El término infraestructura crítica es empleado por los gobiernos para describir activos esenciales para el funcionamiento de la sociedad y la economía. Por tanto, la protección de las infraestructuras críticas nace debido a la consciencia que adquieren los gobiernos, de la necesidad de proteger una serie de infraestructuras necesarias para garantizar el funcionamiento de los servicios esenciales para los países.

Algunos países ya han identificado sus sectores estratégicos en los que hay infraestructuras críticas teniendo en cuenta el impacto que se puede generar si una de estas es atacada o comprometida tales como:

- Centrales y redes de energía.
- Tecnologías de la Información y las Comunicaciones.
- Sistema Financiero y Tributario.
- Sector sanitario.
- Espacio.
- Instalaciones de Investigación.
- Transportes.
- Industria Nuclear.
- Industria Química.

Gran parte de los incidentes que se producen en los sistemas de tecnologías de la información y comunicaciones son provocados por sus propios usuarios. En el caso de entornos SCADA o de carácter industrial, que a pesar de tratarse de sistemas con una criticidad elevada, ya cuentan con controles adicionales para asegurar sus componentes críticos.

Los gobiernos han encaminado esfuerzos para fortalecer la detección y determinar los tipos de amenazas que pueden afectar a sus infraestructuras críticas como las siguientes:

- Advanced Persistent Threat (APTs).
- Ingeniería Social.
- Infecciones por Malware.
- Pishing.

En la actualidad, los ciberataques y los fallos en los sistemas de las infraestructuras críticas se encuentran en el top 5 de riesgos globales según el reciente informe global risks 2012 del foro económico mundial, el cual refleja la interconexión actual entre riesgos geopolíticos, ambientales, sociales, económicos y tecnológicos donde el mayor riesgo tecnológico es el fallo de los sistemas críticos.

Con ello los gobiernos de cada país buscan establecer las medidas necesarias para la protección de estas infraestructuras y así disminuir el riesgo.

En la actualidad existen guías de buenas prácticas y marcos de referencia los cuales se pueden utilizar como insumo para la generación y aseguramiento de todos los elementos que componen estas infraestructuras críticas.

MARCO DE TRABAJO PARA SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Durante mucho tiempo ha existido la necesidad de asegurar infraestructuras críticas de ataques externos, donde ha surgido este marco de trabajo que tiene como objetivo reducir el riesgo cibernético en estas infraestructuras.

El núcleo de este marco se compone de una matriz de funciones y una matriz que muestra el nivel de aplicación de controles.

La matriz de funciones contiene las cinco funciones de seguridad cibernética de primer nivel, que son:

Conocer: Conocer e identificar qué sistemas necesitan ser protegidos, evaluar las prioridades de acuerdo a la misión de la organización y gestionar los procesos para alcanzar los objetivos según la gestión de riesgos.

Prevenir: Actividades operacionales que permiten a la organización decidir sobre las acciones a llevar adelante para garantizar una protección adecuada contra las amenazas a los sistemas empresariales y los componentes críticos de infraestructura.

Detectar: Actividades que identifican la ocurrencia de acontecimientos adversos y que representan riesgo; y los procesos necesarios para evaluar el posible impacto de estos eventos.

Responder: Capacidad de toma de decisiones para contrarrestar un efecto cuando una amenaza se materializa.

Recuperar: Capacidad para el restablecimiento de los servicios que hayan sido desactivados o dañados como resultado de un evento indeseable.

El marco del nivel, de aplicación define tres niveles de aplicación desde tres perspectivas:

- Gerente Ejecutivo.
- Gerentes de Procesos de Negocio
- Gerentes de Operaciones.

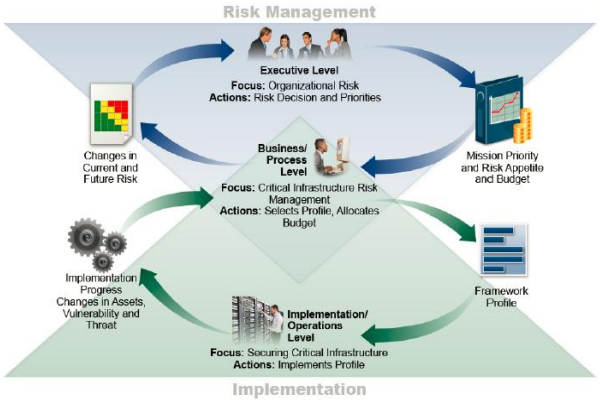

Fig 1. Describe el flujo de información y la toma de decisiones dentro de una organización.
Fuente: National Institute of Standards and Technology. 2014. Framework for Improving Critical Infrastructure Cybersecurity. Recuperado de http://www.nist.gov

El objetivo es reflejar el estado de la seguridad de la infraestructura crítica desde las perspectivas de estos roles y de esta forma determinar los riesgos.

El fin de la ciberseguridad es:

- Minimizar las vulnerabilidades en las infraestructuras críticas.
- Proteger los activos de información de la empresa/organización.
- Asegurar la continuidad del negocio y/o servicio al cliente/ciudadano.

En este marco de trabajo se encuentran los lineamientos aplicables enfocados a procesos de gobierno o a los sectores industriales de un país.

GUÍA DE ISACA DE FACTORES DE CAMBIO DE LA CIBERSEGURIDAD

En ocasiones algunas organizaciones ignoran los nuevos factores de cambio en la seguridad por lo que necesariamente TI debe ir alineada con los objetivos estratégicos del negocio pensando en las necesidades de sus usuarios, para ello existen guías de buenas prácticas en seguridad como (Transformando a la Ciberseguridad Usando COBIT 5) donde se busca la conformación de una fuerza de tarea global de ciberseguridad.

Existen tres factores de cambio donde su propósito es la de cerrar brechas de la ciberseguridad y las actividades criminales, especialmente las amenazas avanzadas persistentes y las cuales hoy en día son muy comunes, las organizaciones y gobiernos deben estar en busca constante de estos lineamientos para su aplicación y aseguramiento de infraestructuras críticas.

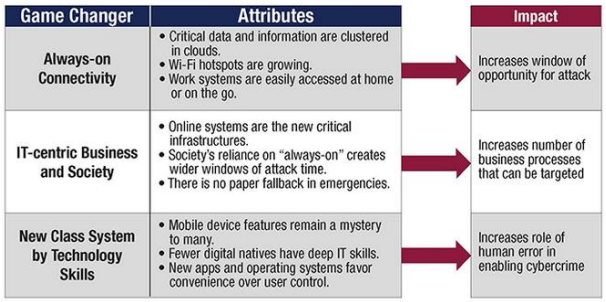

Fig. 2. Cybersecurity Game Changers
Fuente: Isaca. 2013. Guide Identifies Top Three Cybersecurity Game Changers. Recuperado de http://www.isaca.org

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Una estrategia nacional de seguridad cibernética es un plan de acciones destinadas a mejorar la seguridad y resistencia de las infraestructuras y servicios nacionales donde se establecen una serie de objetivos nacionales y las prioridades que deben alcanzarse en un plazo específico.

Es de tener en cuenta que las políticas internacionales y las estrategias nacionales de seguridad cibernética ya operan en muchos países, y están definidas como es el caso de mayoría de países Europeos y Estados Unidos con la (International Strategy for Cyberspace) publicada en mayo del 2011 naciendo con la necesidad de la protección y aseguramiento de sus infraestructuras críticas.

En la actualidad ENISA (European Unión Agency for Network and Information Security) tiene desarrollada una guía práctica sobre el desarrollo y ejecución de estrategias nacionales de ciberseguridad la cual fue publicada en el 2012, y contiene los métodos para identificar los elementos, prácticas comunes y recurrentes de las estrategias nacionales de seguridad cibernética

Esta guía de buenas prácticas puede ser tomada como referencia por gobiernos que no tengan aún estrategias de ciberseguridad donde puedan definir los siguientes aspectos importantes para su desarrollo y aplicación:

- Alcance.
- Audiencia.
- Metodología
- Ciclo de Vida de la Estrategia de Ciberseguridad.
- Identificación de Partes Interesadas
- Desarrollo de Planes de Contingencia Nacionales.
- Establecer Cooperación Internacional.
- Establecer los Requerimientos de la Línea Base de Seguridad.
- Evaluar la Estrategia de Seguridad Cibernética Nacional.

El desarrollo de una estrategia nacional de seguridad cibernética es un esfuerzo grande que requiere la coordinación entre los diferentes actores nacionales del sector público y del privado.

LEGISLACIÓN APLICABLE

El gobierno español con el apoyo del CERT ha desarrollando leyes donde se establecen medidas para protección de infraestructuras críticas como la ley 8 del 2011 donde su objeto es establecer las estrategias y las estructuras adecuadas que permitan, dirigir y coordinar las actuaciones de los distintos órganos del estado en materia de protección de infraestructuras críticas, para mejorar la prevención, preparación y respuesta a amenazas cibernéticas.

En la legislación europea se establece la directiva 2008/114/ce del 8 de diciembre de 2008, la cual hace referencia a la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección y la de los sectores industriales.

Los países de la unión europea reunieron esfuerzos para la creación del programa europeo para la protección de Infraestructuras críticas, (PEPIC) donde allí se establece un marco legislativo para la identificación y designación de las infraestructuras críticas y también la creación de grupos de expertos para su protección y aseguramiento.

Actualmente en países de américa latina dentro de sus gobiernos existen organismos como la agencia nacional de seguridad de la que se derivan los CERT los cuales deben ser sectoriales de tal forma que los incidentes informáticos sean tipificados y haya una respuesta a estos eventos de forma más rápida y centralizada. Este equipo de respuesta ante emergencias informáticas esta alineado con las políticas de seguridad para protección de infraestructuras críticas, ya que cada sector del país esta expuesto ante las diferentes amenazas, se debe determinar los riesgos y dirigir de forma centralizada la respuesta a los incidentes de seguridad.

3. CONCLUSIONES

La ciberseguridad en infraestructuras es de gran de importancia para los gobiernos y para los diferentes sectores industriales de un país, ya que el funcionamiento del estado y procesos industriales, deben contar con el aseguramiento necesario que permita contar con controles, procesos y estrategias de seguridad que permita la reducción de riesgos y así contar con una

solida ciberdefensa de estas infraestructuras ante ataques u otros delitos informáticos latentes, aplicando los diferentes marcos de trabajo y estandares para la protección y continuidad de los procesos críticos de un estado o empresa.

4. REFERENCIAS

[1] *Framework for Improving Critical Infrastructure Cybersecurity* "National Institute of Standards and Technology", PP 12, Feb 2014, web page. http://www.nist.gov.

[2] *Guía básica de protección de Infraestructuras Críticas* "Instituto Nacional de Las tecnologías de la Información", Nov 2013, web page, http://cert.inteco.es.

[3] *National Cyber Security Strategies Practical Guide on Development and Execution*, "Agencia Europea de Seguridad de las Redes y de la Información", Dec 2012, web page, http://www.enisa.europa.eu/.

[4] *Global Risks 2012 Seventh Edition* "World Economic Forum", 2012, web page, http://www3.weforum.org.

[5] *Transforming Cybersecurity Using COBIT 5* "Systems Audit and Control Association", 2013, web page, http://www.isaca.org.

[6] *International Strategy for Cyberspace*, "The White House", May 2011, web page, http://www.whitehouse.gov.

[7] *Ley 8/2011 de Protección de Infraestructuras Críticas*, "Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)", 2011, web page www.cnpic-es.es.

[8] *COBIT 5 Guide Identifies Top Three Cybersecurity Game Changers* "ISACA", 2013, web page www.isaca.org/About-ISACA/Press-room/News-Releases/2013/Pages/New-COBIT-5-Guide-Identifies-Top-Three-Cybersecurity-Game-Changers.aspx