Grupo de Trabajo: Seguridad Integral

Presentación

La Seguridad Integral todavía no es un concepto suficientemente divulgado en las Organizaciones ni en la Sociedad. Si accedemos a Internet con este término se obtienen más de 30 millones de referencias aunque casi todas ellas se refieren a la Seguridad Física, Seguridad Laboral, Seguridad Industrial, Seguridad Privada, Servicios de Vigilancia, Alarmas y protección perimetral, etc.

Algunas iniciativas relativamente recientes hablan de la convergencia entre la Seguridad Física y la Seguridad Lógica, como respuesta para la Seguridad Integral, pero en términos generales las organizaciones siguen teniendo los "distintos tipos" de seguridad, de forma dispersa y bajo departamentos separados, con metodologías y respuestas ante incidentes, heterogéneas y descoordinadas.

Pero la característica principal de los sistemas es la complejidad, sobre todo si son infraestructuras críticas, que son hoy más vulnerables que nunca ante amenazas crecientes, externas e internas. Las organizaciones además están en proceso de cambio, sujetas a legislación y regulaciones cada vez más rígidas y deben actuar en un entorno internacional y global.

Por lo tanto se debe plantear la Seguridad como un Ecosistema en el cual se deben tener conceptos sistémicos, para tener tratamientos y respuestas centralizados ante los distintos tipos de amenazas, una gestión de riesgos coherente a los distintos niveles de la organización que tenga todos los factores en cuenta y un plan de concienciación para poner de manifiesto que la seguridad "es cosa de todos" y que el problema es mundial, por lo que la organización debe prepararse adecuadamente.

Incluso con una estructura organizativa, que refleje estos objetivos adecuadamente. Ya existen organizaciones en algunos países que tienen un VP de Seguridad (sin apellidos), del cual dependen las otras "seguridades", Continuidad de Negocio, etc.

Puesto que todavía queda mucho que hacer e investigar en estos temas, este grupo de trabajo será el encargado de fomentar, desarrollar y apoyar todas las iniciativas en esa línea dentro del marco de PESI.

Objetivos

- Concepto de Seguridad Integral, como el sistema inmunológico de la Organización
- Estrategias de Ciberseguridad. Cloud y Gestión de la Cadena de Suministros
- Securización de Dispositivos de Consumo
- Horizonte de Amenazas
- Establecimiento de Buenas Prácticas
- Profundización en los conceptos GRC (Governance, Risk, and Compliance)
- Soporte con herramientas SW para GRC. Establecimiento de Funcionalidades principales, tales como la gestión integrada del riesgo, gestión de cumplimiento, gestión de incidencias, gestión de Continuidad de Negocio, etc.
- Planes de Formación y Concienciación

Líneas de Investigación y Actuación

Para conseguir los objetivos del grupo de trabajo, éste definirá distintos iniciativas que seguirán las siguientes líneas de actuación e investigación:

- Desarrollo del concepto sistémico de la Seguridad Integral
- Investigación de Amenazas Internas y Externas.
- Estudio de los posibles Cisnes Negros. Nunca se tienen en cuenta y tienen como consecuencia las mayores catástrofes ante las cuales no se tiene defensa.
- Relación y colaboración con otros organismos internacionales en el ámbito de la Seguridad de la Información, Gobernanza de la Seguridad y Estrategias de la Ciberseguridad, tales como el ISF. El World Economic Forum ha publicado recientemente un informe: *Global Risks 2012*, que examina también 50 riesgos globales importantes, mediante 5 categorías de riesgos, que puede servir de base.
- Desarrollo de planes de concienciación y formación sobre la Seguridad Integral
- Desarrollo de procedimientos y planes de contingencia flexibles para hacer las organizaciones más resilentes (La **resiliencia** o **resilencia** es la capacidad que tiene un sistema de **recuperarse frente a la adversidad** para seguir proyectando el futuro. En ocasiones, las circunstancias difíciles o los traumas permiten desarrollar recursos que se encontraban latentes y que se desconocían hasta el momento)
- Diseño y desarrollo de SW para la Gestión de Riesgos, en colaboración con empresas internacionales que ya tiene una base sobre la cual elaborar (para no re-inventar la rueda ni generar costes innecesarios)
- Participación y colaboración en foros, organizaciones y proyectos internacionales sobre la Seguridad Integral.

Retos e Hitos

A medida que el grupo de trabajo vaya avanzando en sus actividades, se irán planteando distintos hitos en línea con la estrategia establecida tanto a nivel del grupo de trabajo como de la propia plataforma. Sin ánimo de ser completa, se identifican a priori los siguientes hitos a conseguir:

- Smart Meters: Diseño del HW de dispositivos con conceptos de seguridad integrados que imposibiliten que un error de control, por parte del SW pueda causar daños. HW Physical failsafes.
- Diseño de dispositivos con “security and privacy by design”
- Tener en cuenta que los sistemas de control pueden generar disrupciones civiles masivas, disrupciones económicas y disrupciones de comunicación.
- Los dispositivos inteligentes pueden saber qué tipo de uso se les está dando y generar problemas de privacidad y protección de datos. Si la información existe, se puede acceder a ella.
- Nuevas leyes y regulaciones futuras. El diseño debe tener en cuenta los cambios para adaptarse a ellos de manera fácil, flexible y económica.

Coordinador Subgrupo Metodologías: Rafael Rodríguez de Cora (CALS)

Subgrupo: Ciberseguridad de los Sistema de Control Industrial

Los Sistemas de Control Industrial (SCI, en adelante) son fundamentales para nuestra sociedad y economía, puesto que buena parte de las Infraestructuras Críticas nacionales e internacionales residen sobre los mismos. Sin embargo el alcance de la Ciberseguridad de los SCI va más allá de las propias Infraestructuras Críticas, extendiéndose a la casi total generalidad del tejido empresarial, no sólo en el ámbito industrial, sino en cualquier sector productivo ya que finalmente, las infraestructuras TIC que los sustentan están a su vez soportadas por SCI que controlan el entorno físico en el que residen (torres de refrigeración, controles de acceso físico, gestión energética de edificios, etc.).

Teniendo todo esto en cuenta, cabe prestar la atención adecuada a la protección de los SCI. Los aspectos de seguridad física y laboral han venido teniéndose en cuenta desde hace años, sin embargo no su Ciberseguridad, la protección de estos sistemas, su adecuado diseño, implantación y por supuesto, monitorización, lo que ha llevado a una desatención absoluta en la gestión del riesgo correspondiente.

Nuestra sociedad y economía es hoy en día totalmente vulnerable a través de las nuevas amenazas que se ciernen sobre los SCI: Stuxnet, DuQu, Denegaciones de Servicio, ataques terroristas, amenazas persistentes avanzadas, etc. tienen y pueden tener impactos en nuestras vidas y sociedades que difícilmente podíamos imaginar hasta hace unos meses.

Por ello, se hace totalmente necesario el estudio, análisis y desarrollo de todo un marco de trabajo en torno a la Ciberseguridad de los SCI. Este grupo de trabajo será el encargado de fomentar, desarrollar y apoyar todas las iniciativas en esa línea dentro del marco de PESI.

Objetivos

- Establecer una conciencia de la situación (situational awareness) de la Ciberseguridad de los SCI
- Fomentar la concienciación y formación en el ámbito de la Ciberseguridad de los SCI
- Fomentar, desarrollar y respaldar la creación de Estrategias, Buenas Prácticas, Planes y Guías Nacionales y Europeas de Ciberseguridad de los SCI
- Fomentar la colaboración público privada, nacional e internacional
- Mejorar las capacidades en Ciberseguridad de los SCI de Gobiernos, Entidades Públicas, Fabricantes, Empresas, Universidades y Centros de Investigación.
- Posicionar a nuestro país en el ámbito internacional de la Ciberseguridad de los SCI
- Fomentar la inclusión de los paradigmas de “Security & Privacy by Design” en los SCI, Redes, Arquitecturas, Servicios y Proyectos asociados
- Fomentar actividades para la mejora de la comunicación y mutuo conocimiento entre el personal de SCI y TIC
- Fomentar la Investigación en Ciberseguridad de los SCI
- Fomentar y apoyar la implementación de las Smart Grid como una oportunidad para la Investigación, desarrollo e implementación de la Ciberseguridad de los SCI

Líneas de Investigación y Actuación

Para conseguir los objetivos del grupo de trabajo, éste definirá distintos iniciativas que seguirán las siguientes líneas de actuación e investigación:

- Desarrollo de una base de conocimiento y foro de discusión sobre la Ciberseguridad de los SCI que permita contar con la información más actualizada a nivel internacional.
- Desarrollo de planes de concienciación y formación sobre Ciberseguridad de los SCI
- Relaciones Internacionales: fomentar y apoyar la participación de profesionales y organizaciones españolas en el plano internacional posicionando así a nuestro país en un nivel más alto en la Ciberseguridad de los SCI
- Desarrollo de documentación de alto nivel en Español e Inglés (todos los contenidos deberían ser desarrollados en ambos idiomas) sobre Ciberseguridad de los SCI
- Apoyo en el desarrollo de una Estrategia Nacional de Protección de los SCI
- Desarrollo y establecimiento de marcos de colaboración público privada en la Ciberseguridad de los SCI
- Participación e influencia en programas nacionales e internacionales de investigación en Ciberseguridad de los SCI
- Relación y colaboración con otras asociaciones profesionales, organizaciones y medios en el ámbito de la Ciberseguridad de los SCI (ejemplo: ISA, ENISA, ISACA, Automatización e Instrumentación, etc.)
- Participación y colaboración en foros, organizaciones y proyectos sobre Smart Grid

Hitos

A medida que el grupo de trabajo vaya avanzando en sus actividades, se irán planteando distintos hitos en línea con la estrategia establecida tanto a nivel del grupo de trabajo como de la propia plataforma. Sin ánimo de ser completa, se identifican a priori los siguientes hitos a conseguir en el periodo inicial 2012-2013:

- Estudio sobre la Ciberseguridad de los SCI en España
- Estudio sobre la Ciberseguridad Smart Grid en España
- Disponibilidad de Base de Conocimiento y Foro de Discusión sobre Ciberseguridad de los SCI
- 1er Jornada Nacional sobre Ciberseguridad de los SCI: debería ser “coorganizada” con otras entidades del ámbito industrial de cara a reflejar la aproximación conjunta de los mundos SCI y TIC
- Presentación del Grupo de Trabajo y establecimiento de relaciones con distintos grupos de trabajo y foros existentes a nivel internacional y nacional, tanto en el ámbito de la Ciberseguridad de los SCI, como en el ámbito industrial en sí mismo.
- Disponibilidad de Marco de Relación Público Privada tipo para la Ciberseguridad de los SCI en España

Coordinador Subgrupo Metodologías: Samuel Linares (Intermark)