Infraestructuras Críticas: Sectores Necesitados De Un Modelo De Ciberseguridad

Carlos Gerardo Said
Decano – Facultad de Ingeniería
Universidad Católica de Salta - UCASAL, Argentina
Dirección: Facultad de Ingeniería
Ciudad Universitaria – Campo Castañares – A4400EDD – Salta – Argentina

Abstract

The proposed research aims to address the implementation and management of cyber security practices associated with information technology and operational technology regarding network environments of industrial production (SCADA-ICS). Not intended to replace other activities related to cybersecurity, programs, processes, or approaches that organizations of downstream petroleum and natural gas have implemented or intend to implement, including cybersecurity activities associated with legislation, regulations, policies, private initiatives, or the requirements for the business mission. The guidance in this research program is to complement a comprehensive cybersecurity specific areas and industries of oil and gas.

Keywords: Cyber security, Information Technology

Resumen

La investigación propuesta tiene como objetivo tratar la aplicación y la gestión de las prácticas de seguridad cibernética asociados con la tecnología de la información y la tecnología operativa en relación con los entornos de redes de producción industrial (SCADA-ICS). No pretende sustituir otras actividades relacionadas con la ciberseguridad , programas , procesos , o enfoques que las organizaciones del subsector del petróleo y el gas natural han implementado o tienen intención de poner en práctica, incluyendo las actividades de ciberseguridad asociados con la legislación, los reglamentos , las políticas, iniciativas particulares, o los requisitos propios de la misión del negocio. La orientación en esta investigación es complementar un programa integral de seguridad cibernética de las áreas específicas y en las industrias del petróleo y del gas.

Palabras claves: SCADA, ICS, Ciberseguridad, Infraestructuras Críticas

Introduccion

La industria del petróleo y la del gas son dos industrias con características similares y también individuales. Estos incluyen la exploración, recolección, producción, transformación, almacenamiento y transporte de petróleo y gas natural. El petróleo y el gas natural son almacenados en diversas partes, y se transporta a través de miles de kilómetros, por medio de tuberías, canales, ferrocarriles y rutas.

Aquellos que trabajan con SCADA (Supervisory Control and Data Acquisition) o sistemas de control industrial (ICS, Industrial Control Systems) en la industria de petróleo y gas son conscientes de la presión para aumentar la productividad y reducir costos a través de la integración de redes.

Por ejemplo, el intercambio de datos en tiempo real de las operaciones de campo con los grupos de gestión es una práctica estándar para la mayoría de las empresas. Del mismo modo, la demanda de servicios de asistencia técnica a distancia ha hecho que muchos de los sistemas de control de las tuberías se tornen accesibles a través de tecnologías basadas en Internet.

Al mismo tiempo, los propios sistemas SCADA han cambiado radicalmente. Redes propietarias han sido reemplazadas con equipos que utilizan tecnología Ethernet.

Estaciones de operador asignadas históricamente a un destino específico han sido reemplazados con equipos que ejecutan Windows ™ y el software de TI, tales como lectores de PDF y navegadores web. Estos están hoy instalados en cada centro de estación o de control.

Esto tiene un costo - muchos de los mismos problemas de seguridad que han afectado a los sistemas de negocios ahora aparecen en los sistemas SCADA.

Los sistemas de control están expuestos a amenazas de seguridad cibernética para los cuales nunca fueron diseñados.

Los ataques cibernéticos en los sistemas de automatización fueron considerados por muchos como un problema teórico hasta el descubrimiento de Stuxnet en julio de 2010. En ese momento, el mundo cambió para los proveedores de automatización, hackers, delincuentes e incluso los gobiernos.

Stuxnet fue diseñado específicamente para atacar a los productos de automatización. Es capaz de descargar la información del proceso, de realizar cambios en la lógica de los PLC, y luego cubrir sus pistas.

Empleó vulnerabilidades previamente desconocidas para difundirse. Lo suficientemente potente como para evadir las tecnologías de seguridad de última generación.

El objetivo previsto de Stuxnet fueron las centrifugadoras de enriquecimiento de uranio utilizados por Irán en su programa de armamento nuclear. Tomado el control del sistema de automatización, el malware es capaz de volver a configurar los controladores de la centrífuga, haciendo que el equipo se destruya lentamente a sí mismo.

El impacto real de Stuxnet comenzó a aparecer después de que el propio malware era historia.

Gracias a la publicidad de Stuxnet, hackers y criminales descubrieron que los productos SCADA / ICS son objetivos atractivos. Estos sistemas pronto se convirtieron en blanco de elección para las divulgaciones de seguridad pública.

En 2011 ICS-CERT liberaron 104 avisos de seguridad para los productos SCADA / ICS, de 39 proveedores diferentes. Antes de Stuxnet, se habían informado sólo cinco 5 vulnerabilidades SCADA.

Lo que fue particularmente preocupante es que el código de ataque publicado para el 40% de estas vulnerabilidades. Esto significaba que los ciber-terroristas sabían dónde encontrar vulnerabilidades en SCADA/productos ICS, y tenían además el software para explotarlos.

Stuxnet también mostró al mundo el poder de un 'malware' ICS bien diseñado. Podría destruir el equipo y apagar los sistemas críticos.

En Febrero de 2011, un nuevo ataque contra la industria fue expuesto. En un documento titulado "Global Energy ciberataques: Noche del Dragón", se describe una actividad de amenaza cibernética que estaba robando datos confidenciales, como las ofertas de campos petroleros y datos de las operaciones SCADA de las empresas de energía y petroquímica.

A principios de Octubre de 2011, se anunció el descubrimiento de un nuevo troyano llamado "Duqu". Este malware dirigido utiliza en gran parte el mismo código fuente de Stuxnet.

A decir de Symantec: "El propósito de Duqu es reunir datos de inteligencia y los activos de entidades tales como: infraestructura y sistemas de empresas industriales."

A finales de octubre, Symantec dio a conocer detalles de un tercer ataque dirigido a 25 empresas que participan en la fabricación de productos químicos y materiales avanzados.

Se llamaron a estos ataques los "ataques Nitro".

Una de las vulnerabilidades más importantes de una red ICS / SCADA son los protocolos: OPC-UA, OPC-DA, ICCP, MODBUS, DNP3 entre otros.

Texto principal

La industria del petróleo y la del gas son dos industrias con características similares y también individuales. Estos incluyen la exploración, recolección, producción, transformación, almacenamiento y transporte de petróleo y gas natural. El petróleo y el gas natural son importados, así como de producción nacional, almacenados en diversas partes de la Nación, y se transporta a través de miles de kilómetros, a través de tuberías, canales, ferrocarriles y rutas.

El petróleo y gas natural están hechos de compuestos de hidrocarburos que se originan en depósitos subterráneos. El petróleo crudo es un líquido que debe ser llevado a la superficie, eliminados los gases, agua y otras impurezas, y luego transportado a las instalaciones de procesamiento (refinerías de petróleo), en los que se derivan los productos terminados.

Productos derivados del petróleo crudo incluyen gasolina, querosén, combustible de aviación, combustible diésel, combustible para calefacción, el aceite pesado, lubricantes, ceras, asfalto y gas licuado de petróleo, así como una serie de precursores petroquímicos.

Similar al petróleo crudo, el gas natural se produce, se eliminan los líquidos y otras impurezas y, a continuación, se transporta a través de oleoductos a las instalaciones de procesamiento de gas que separan los componentes más pesados del gas, dejando un producto compuesto casi enteramente de metano. A continuación, el metano se transporta como gas natural limpio para el almacenamiento a granel, los consumidores industriales y viviendas individuales.

La licuefacción del gas natural hace que una concentración más densa del gas natural y permite que el gas natural licuado (GNL) sea transportado económicamente a través de camiones/buques cisterna, en lugar de tuberías.

Aquellos que trabajan con SCADA o sistemas de control industrial (ICS) en la industria de petróleo y gas son conscientes de la presión para aumentar la productividad y reducir costos a través de la integración de redes.

Por ejemplo, el intercambio de datos en tiempo real de las operaciones de campo con los grupos de gestión es una práctica estándar para la mayoría de las empresas. Del mismo modo, la demanda de servicios de asistencia técnica a distancia ha hecho que muchos de los sistemas de control de las tuberías se tornen accesibles a través de tecnologías basadas en Internet.

Al mismo tiempo, los propios sistemas SCADA han cambiado radicalmente. Redes propietarias han sido reemplazadas con equipos que utilizan tecnología Ethernet.

Estaciones de operador asignadas históricamente a un destino específico han sido reemplazados con equipos que ejecutan Windows ™ y el

software de TI, tales como lectores de PDF y navegadores web. Estos están hoy instalados en cada centro de estación o de control.

Estas nuevas tecnologías están permitiendo a las empresas implementar prácticas ágiles y rentables de negocios. Desafortunadamente, también tienen un costo - muchos de los mismos problemas de seguridad que han afectado a los sistemas de negocios ahora aparecen en los sistemas SCADA.

Los sistemas de control de la tubería están expuestos a amenazas de seguridad cibernética para los cuales nunca fueron diseñados.

Stuxnet – un generador de cambios

Los ataques cibernéticos en los sistemas de automatización fueron considerados por muchos como un problema teórico hasta el descubrimiento de Stuxnet en julio de 2010. En ese momento, el mundo cambió, no sólo para las empresas de petróleo y gas, sino también para los proveedores de automatización, hackers, delincuentes e incluso los gobiernos.

Stuxnet fue diseñado específicamente para atacar a los productos de automatización de Siemens. Es capaz de descargar la información del proceso, de realizar cambios en la lógica de los PLC, y luego cubrir sus pistas.

Empleó vulnerabilidades previamente desconocidas para difundirse. Es lo suficientemente potente como para evadir las tecnologías de seguridad de última generación.

El objetivo previsto de Stuxnet fueron las centrifugadoras de enriquecimiento de uranio utilizados por Irán en su programa de armamento nuclear. Tomado el control del sistema de automatización, el malware es capaz de volver a configurar los controladores de la centrífuga, haciendo que el equipo se destruya lentamente a sí mismo.

Stuxnet tenía un objetivo específico, pero al igual que todos los ataques, cibernéticos o convencionales hubo daños colaterales.

Varias empresas en los EE.UU. tenían los PLC que fueron reconfigurados por Stuxnet, probablemente por accidente. Ningún daño real ocurrió, pero una gran cantidad de mano y detenciones de servicios ocurrieron por esto.

Estos problemas se detuvieron; ‘soluciones’ al software y firmas de antivirus pronto condujeron Stuxnet a la extinción. Pero, el problema no termina ahí.

Stuxnet – un generador de cambios

El impacto real de Stuxnet comenzó a aparecer después de que el propio malware era historia.

Gracias a la publicidad de Stuxnet, hackers y criminales descubrieron que los productos SCADA / ICS son objetivos atractivos. Estos sistemas pronto se convirtieron en blanco de elección para las divulgaciones de seguridad pública.

En 2011 ICS-CERT liberaron 104 avisos de seguridad para los productos SCADA / ICS, de 39 proveedores diferentes. Antes de Stuxnet, se habían informado sólo cinco 5 vulnerabilidades SCADA.

Lo que fue particularmente preocupante es que el código de ataque publicado para el 40% de estas vulnerabilidades. Esto significaba que los ciber-terroristas sabían dónde encontrar vulnerabilidades en SCADA/productos ICS, y tenían además el software para explotarlos.

Stuxnet también mostró al mundo el poder de un 'malware' ICS bien diseñado. Podría robar secretos corporativos, destruir el equipo y apagar los sistemas críticos. Y mientras Stuxnet parecía haber sido creada por razones políticas, las oportunidades para la explotación empresarial eran evidentes tanto para los gobiernos como para los delincuentes.

Era cuestión de tiempo antes de que alguien decidiera reutilizar las técnicas de Stuxnet para ir tras otras víctimas.

En Febrero de 2011, un nuevo ataque contra la industria fue expuesto. En un documento titulado "Global Energy ciberataques: Noche del Dragón", se describe una actividad de amenaza cibernética que estaba robando datos confidenciales, como las ofertas de campos petroleros y datos de las operaciones SCADA de las empresas de energía y petroquímica.

A principios de Octubre de 2011, se anunció el descubrimiento de un nuevo troyano llamado "Duqu". Este malware dirigido utiliza en gran parte el mismo código fuente de Stuxnet.

A diferencia de Stuxnet, es un ladrón de información y no parece apuntar directamente a los sistemas de PLC. Sin embargo, de acuerdo con Symantec: "El propósito de Duqu es reunir datos de inteligencia y los activos de entidades tales como: infraestructura y sistemas de empresas industriales ... Los atacantes están buscando información, tales como documentos de diseño que podrían ayudarles a montar un ataque futuro en diversas industrias, incluyendo los sistemas de control e instalaciones de las industrias ".

A finales de octubre, Symantec dio a conocer detalles de un tercer ataque dirigido a 25 empresas que participan en la fabricación de productos químicos y materiales avanzados.

Se llamaron a estos ataques los "ataques Nitro", Symantec reportó: "El propósito de los ataques parece ser el espionaje industrial, la recolección de propiedad intelectual para obtener ventaja competitiva."

Una de las vulnerabilidades más importantes de una red ICS / SCADA: los **protocolos**.

- **OPC-UA**
- **OPC-DA**
- **ICCP**
- **MODBUS**
- **DNP3**

Qué podemos intentar hacer?

- Incluir evaluaciones de seguridad como parte de los procesos de mantenimiento periódico. (Estas evaluaciones deben ser específicas para la industria, y es el objetivo de esta propuesta de investigación)
- La implementación de estos cambios mejorará la postura de "defensa en profundidad" para cualquier tubería ICS / SCADA y ayudará a proteger las operaciones contra el espionaje cibernético.
- Se necesita una mejor seguridad SCADA con urgencia; esperar el próximo 'malware' puede ser demasiado tarde.

Propuesta de investigación

La investigación propuesta tiene como objetivo tratar la aplicación y la gestión de las prácticas de seguridad cibernética asociados con la tecnología de la información y la tecnología operativa en relación con los entornos en los que operan .

No pretende sustituir otras actividades relacionadas con la ciberseguridad , programas , procesos , o enfoques que las organizaciones del subsector del petróleo y el gas natural han implementado o tienen intención de poner en práctica, incluyendo las actividades de ciberseguridad asociados con la legislación, los reglamentos , las políticas, iniciativas particulares, o los requisitos propios de la misión del negocio.

La orientación en esta investigación es complementar un programa integral de seguridad cibernética de las áreas específicas.

Planteo de la investigación

Repetidas intrusiones cibernéticas en organizaciones de todo tipo ponen de manifiesto la necesidad de mejorar la seguridad cibernética. Las amenazas cibernéticas siguen creciendo y representan uno de los riesgos operativos más serios que enfrentan las organizaciones modernas. La seguridad de la sociedad y económica depende del funcionamiento confiable de la infraestructura crítica frente a esas amenazas.

No solo es una cuestión de protección de la infraestructura crítica (como concepto abstracto), la economía depende de la operación sustentable de organizaciones de todo tipo. Un modelo de ciberseguridad específico para la industria del Petróleo y Gas puede ayudar las organizaciones de dicha categoría a evaluar y mejorar sus programas de seguridad cibernética.

Lo enunciado nos hace presumir la existencia de características diferenciales y/o únicas para las mencionadas industrias.

El modelo propuesto debe poder utilizarse para:

- Fortalecer las capacidades de ciberseguridad en el subsector del gas y el petróleo.
- Permitir a las organizaciones evaluar y comparar de manera consistente y repetitiva sus capacidades de ciberseguridad.
- Compartir conocimientos, mejores prácticas y referencias, como un medio para mejorar las capacidades de ciberseguridad.
- Permitir a las organizaciones dar prioridad a las acciones e inversiones para mejorar la ciberseguridad.

El modelo debe ser desarrollado para proporcionar una conducta descriptiva, no prescriptivo, orientación para ayudar a las organizaciones a desarrollar y mejorar sus capacidades en términos de ciberseguridad.

Como resultado, las prácticas sugeridas en el modelo deben estar en un nivel de abstracción de modo que pueden ser interpretados por las organizaciones de diversas estructuras, funciones y tamaños.

El modelo debe probarse con entidades del sector privado, público o mixto, para validar que proporcionaría información valiosa para la evaluación y para recoger retroalimentación que permita su mejora, y en un posterior estadío, autocorrección.

Los **Dominios** específicos que deberían ser atendidos por el programa de Gestión de la Ciberseguridad (orientado a las industrias del gas y el petróleo) son:

- Gestión de Riesgos.
- Identificación de Activos y Gestión de la Configuración.
- Gestión de las Identidades y Administración de Accesos.
- Gestión de las Amenazas y Vulnerabilidades.
- Análisis del Contexto y su Gestión.
- Gestión del Intercambio de Información y las Comunicaciones.
- Eventos y Respuesta a Incidentes, Continuidad de la Operación.
- Cadena de Suministro y Gestión de las Dependencias Externas.
- Gestión de la Fuerza Laboral.
- Gestión del Programa de Ciberseguridad.

Cada dominio debe entenderse como una agrupación lógica de las prácticas de seguridad cibernética.

Cada uno de los dominios del modelo debería contener un conjunto estructurado de prácticas de seguridad cibernética.

Cada conjunto de prácticas representa las actividades que una organización puede llevar a cabo para establecer la capacidad y madurez en el dominio.

Por ejemplo, el dominio de Gestión de Riesgos es un conjunto de prácticas que una organización puede llevar a cabo para establecer y madurar su capacidad de gestión del riesgo de la seguridad cibernética.

Trataremos los aspectos que proponemos incluir en el 'framework' o marco de referencia para la 'Gestión de Riesgos' en ciberseguridad, aplicada a las industrias en cuestión (petróleo y gas)

- Desarrollo de una estrategia de gestión del riesgo empresarial que identifica su tolerancia y la estrategia para la evaluación, respuesta y seguimiento de los riesgos de ciberseguridad.
- Determinación de un consejo de administración el cual revisa esta estrategia con una determinada frecuencia (o ante la aparición de amenazas, vulnerabilidades no previstas y de potencial alto impacto) para asegurarse de que permanece alineada con los objetivos referidos a la ciberseguridad, de la organización.
- Determinación del riesgo para poder cumplir con las prestaciones de servicios esenciales. Su identificación y documentación.
- Gestionar un registro de riesgos para asegurarse de que son monitoreados y se generaron respuestas en forma oportuna; seguimiento e identificación de tendencias.
- Gestión de un diagrama de arquitectura de red que identifica los activos críticos y muestra cómo están conectados y cuáles están expuestos a Internet. Recursos como servidores Web que tienen solicitudes de Internet se consideran en mayor riesgo que aquellas que no lo hacen.
- Los activos digitales que dan soporte a los de mayo exposición (por ejemplo un servidor de base de datos detrás de un servidor Web , están en el segundo nivel de riesgo y así sucesivamente.
- El diagrama de red debería incluir activos como los firewalls y dispositivos de detección de intrusiones (IPSs, UTM, IPSs NG, etc..), por ello el riesgo básico de un activo se definiría en función de cómo está protegido basado en los controles de seguridad.
- El riesgo final para cada activo surgirá de combinación de la importancia del activo en la prestación de los servicios esenciales y su exposición sobre la base de las redes y arquitecturas de ciberseguridad.

Para todos los aspectos mencionados identificaremos las políticas, procedimientos y técnicas, para luego parametrizar y aplicar los mismos a una empresa específica.

Veamos ahora los aspectos mínimos que debería incluir un 'framework' o marco de referencia para la 'Gestión de amenazas y vulnerabilidades' en ciberseguridad, aplicada a las industrias en cuestión (petróleo y gas)

- Examinar los tipos de amenazas a las que normalmente responde la organización, incluyendo software malicioso, ataques de denegación de servicio, y los ataques de grupos ciber activistas.
- Desarrollar y documentar el perfil de amenaza de la organización en todas sus áreas/sectores/actividades.
- Identifica r fuentes confiables de información que permitan la identificación de amenazas de forma rápida y estar en condiciones de consumir y analizar la información sobre amenazas publicadas por fuentes tales como los CERT, Centros de intercambio de información y de análisis (ISAC), Sistemas de Respuesta de Emergencia y Control de la Ciber-Industria, de forma tal de iniciar una respuesta eficaz.
- Hacer uso del Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST), el Common Vulnerability Scoring System (CVSS) para identificar los impactos potenciales de las vulnerabilidades de software conocidas. Esto permitiría a la organización priorizar las actividades de mitigación y reducción de riesgo/impacto de acuerdo con la importancia de las vulnerabilidades.

Metodología

Desarrollo del modelo propuesto, el cual debe poder utilizarse para:

- Fortalecer las capacidades de ciberseguridad en el subsector del gas y el petróleo.
- Permitir a las organizaciones evaluar y comparar de manera consistente y repetitiva sus capacidades de ciberseguridad.
- Compartir conocimientos, mejores prácticas y referencias, como un medio para mejorar las capacidades de ciberseguridad.
- Permitir a las organizaciones dar prioridad a las acciones e inversiones para mejorar la ciberseguridad.

El modelo debe ser desarrollado para proporcionar una conducta descriptiva, no prescriptivo, orientación para ayudar a las organizaciones a desarrollar y mejorar sus capacidades en términos de ciberseguridad.

Como resultado, las prácticas sugeridas en el modelo deben estar en un nivel de abstracción de modo que pueden ser interpretados por las organizaciones de diversas estructuras, funciones y tamaños.

El modelo debe probarse con entidades del sector privado, público o mixto, para validar que proporcionaría información valiosa para la evaluación y para recoger retroalimentación que permita su mejora, y en un posterior estadío, autocorrección.

Deben desarrollarse las estrategias básicas para todos los dominios enumerados (hemos desarrollado brevemente en esta ponencia dos de ellos, a título de clarificar la propuesta).

Conclusion

No es posible en el estado actual emitir conclusiones. Podemos mencionar lo siguiente (http://www.energyglobal.com/downstream/special-reports/29052015/How-can-SCADA-security-be-improved-for-oil-and-gas-companies-089/): **"De acuerdo con el informe recientemente lanzado, 2015 - Informe Anual de Amenazas de Seguridad - DELL, los ataques a redes SCADA están en aumento. El informe encontró que en 2014 el número de ataques contra Sistemas de Control y Adquisición de Datos (SCADA) se duplicó en comparación con el año anterior. La mayoría de estos ataques se produjeron en Finlandia, el Reino Unido y los EE.UU., probablemente debido al hecho de que en estos países los sistemas SCADA tienen más probabilidades de estar conectado a internet. El Informe de Dell se produce después de los hallazgos de los EE.UU.".**

Nuestro país (Argentina) carece de un marco de seguridad para estas infraestructuras esenciales para una nación. La región latinoamericana adolece de la misma falencia. El desarrollo de un marco como el propuesto, y su aplicación en la industria es esencial hoy y crecerá su necesidad día a día en virtud de la cantidad de ataques a redes ICS-SCADA (infraestructuras críticas).

References:

DHS ICS-CERT] Department of Homeland Security. (2012, May). Industrial Control Systems Cyber Emergency Response Team. http://www.us-cert.gov/control_systems/ics-cert/

DHS ICSJWG] Department of Homeland Security. (2012, May). Industrial Control Systems Joint Working Group. May 2012. http://www.us-cert.gov/control_ systems/icsjwg/

DHS PCII] Department of Homeland Security. (2012, May). Who can access Protected Critical Infrastructure Information (PCII). http://www.dhs.gov/files/programs/gc_1193089801658.shtm

DOE 21 Steps to Improve Cyber Security of SCADA Networks. U.S. Department of Energy and the President's Critical Infrastructure Protection Board. (n.d.). 21 Steps to improve cyber security of SCADA networks. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

FIRST Forum of Incident Response and Security Teams (FIRST). (2012). CSIRT case classification (Example for enterprise CSIRT). http://www.first.org/_assets/resources/guides/csirt_case_classification.html

NIST Framework National Institute of Standards and Technology. (2012). NIST framework and roadmap for smart grid interoperability standards, Release 2.0 http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf