Seguridad Cibernética para Sistemas de Seguridad Industrial

Cyber Security for Industrial Security Systems

Ing. Hadrian Clark Rodríguez [1]
[1] Program Manager, Latam Airlines Group, www.latam.com

Resumen: El presente trabajo presenta algunas reflexiones relacionadas con un tema muy de actualidad, que ha ido creciendo rápidamente en los últimos años, que afecta tanto a las grandes como pequeñas empresas industriales y a los organismos gubernamentales, fuerzas armadas y de seguridad de todo el mundo. La seguridad en los sistemas de Tecnologías Operativas que hoy están siendo vulneradas, creando problemas importantes en las operaciones de las empresas y en la seguridad de los estados. Las Tecnologías Operativas se usan en diversas industrias como la aviación, generación y distribución eléctrica, servicios de suministro de agua potable, el petróleo y gas, empresas manufactureras, medios de transportes terrestres y marítimo, medios de comunicación, laboratorios de investigación avanzada, servicios públicos y privados, servicios de emergencia sanitaria, control de tráfico vehicular, etc., significando que el impacto que se produce al vulnerar la seguridad de estas actividades, especialmente aquellas críticas que pueden afectar la calidad de vida de las personas, provocando pérdidas de vidas, es muy grande como también el daño producido que genera costos y tiempos importantes para recuperar los sistemas.

Palabras claves: seguridad, cibernética, tecnología, control

Abstract: This paper presents some reflections related to a very current topic, which has been growing rapidly in recent years, affecting both large and small industrial companies and government agencies, armed forces and security forces around the world. The security of Operational Technology systems is currently being violated, creating major problems in business operations and in the security of states. Operational Technologies are used in various industries such as aviation, power generation and distribution, drinking water supply services, oil and gas, manufacturing companies, land and maritime transport, media, advanced research laboratories, public and private services, health emergency services, vehicular traffic control, etc., meaning that the impact produced by violating the security of these activities, especially those critical ones that can affect the quality of life of people, causing loss of life, is very large as well as the damage produced that generates significant costs and time to recover the systems.

Keyword: security, cyber, technology, control

1 Introducción

La tecnología operativa (OT) abarca los sistemas informáticos y de control que supervisan y gestionan las operaciones físicas de infraestructuras críticas, como plantas de energía, sistemas de transporte, instalaciones de agua y redes de distribución de gas, electricidad, sistemas de armamentos, etc. A medida que estas infraestructuras se vuelven más interconectadas y automatizadas, la ciberseguridad en el ámbito de la OT se convierte en una preocupación cada vez más apremiante, considerando que la ciberseguridad es la protección de la información digital contenida en los equipos, dispositivos y activos.

Los Sistemas de Control Industrial (ICS) interactúan con el mundo físico, que se compone de controladores (PLC), unidades de supervisión (SCADA) y computadoras conectadas por una red, componentes altamente vulnerables, ya que no funcionan de fabrica en ellos los firewalls o antivirus como en el mundo IT. En la actualidad, cuando hay una violación de la seguridad de IT, expertos en seguridad cibernética intervienen y pasan semanas para investigar y recopilar información histórica a fin de encontrar la causa raíz. Pero en el mundo OT una orden de reconfiguración enviado a un PLC fuera de un tiempo de mantenimiento o un nuevo protocolo utilizado entre dos dispositivos, por nombrar unas pocas ocurrencias posibles, estos no serán detectados como eventos anormales.

Los ataques cibernéticos a sistemas OT pueden provocar daños físicos a la infraestructura tanto pública como privada, como el sobrecalentamiento de equipos, la manipulación de válvulas o la alteración de procesos industriales. Estos daños pueden resultar costosos de reparar, tanto en lo monetario como en el tiempo que pueden demorar y ponen en peligro la seguridad de las personas, causando interrupciones masivas en los servicios esenciales, como la electricidad, el agua, el gas o el transporte, afectando a las personas en casas, escuelas, hospitales, empresas, etc. Estas interrupciones de estos servicios pueden tener un impacto muy significativo en la sociedad, en la economía y en la seguridad nacional.

2 Factores contribuyentes

La industria 4.0: La cual marcó un antes y un después en temas de ciberseguridad, tanto para las empresas estratégicas del Estado, como para las áreas de la Defensa, Gubernamentales y todas las que son principalmente las consideradas infraestructuras críticas. Hoy, la Ciberseguridad Industrial no es más una opción, es imperativa y mandataria, ya que los daños producidos resultarían irreparables, no tan solo daños físicos en las instalaciones o en la pérdida de los servicios básicos en caso de la infraestructura critica, sino también por la pérdida de la confianza y la seguridad.

La revolución Industrial 4.0 exige la conexión a Internet de los computadores que conforman la OT (llamado también el Internet de las Cosas Industriales o IIoT), donde la proliferación de dispositivos conectados en entornos industriales aumenta la complejidad de la seguridad en OT. Los dispositivos IIoT ofrecen ventajas en términos

de monitorización y eficiencia, pero también introducen riesgos de seguridad, especialmente si no se implementan medidas adecuadas de protección.

3 La amenaza puede ser multifactorial: La guerra asimétrica, el sabotaje, el espionaje Industrial, entre otros.

Los adversarios cibernéticos pueden buscar acceder a sistemas OT para realizar espionaje industrial, robar información confidencial, robar dinero o sabotear operaciones. Estas actividades ilícitas pueden socavar la competitividad de las empresas y comprometer la integridad de las operaciones industriales.

Sin embargo, uno de los factores más preocupantes a nivel país es sin duda la amenaza de un ataque bajo la justificación de la guerra Irrestricta o Asimétrica, concepto desarrollado en el año 1999 por los coroneles del ejército de la República Popular de China, Qiao Liang y Wang Xiangsui [1], quienes introdujeron esta nueva visión en toda la esfera mundial, planteando que los conflictos se resolverán "usando todos los métodos, incluyendo fuerzas armadas o fuerzas no armadas, militares y no militares, letales y no letales, para imponer al enemigo aceptar sus propios intereses". En resumen, se amplía el concepto de la guerra a partir de las nuevas posibilidades de ejercer la violencia, las que no se limitan sólo a las operaciones militares, por tanto, la diversidad de medios que hoy se pueden utilizar en la agresión a la seguridad de una nación incluye los ataques cibernéticos a la infraestructura critica.

Algunas malas experiencias a nivel global: El caso Stuxnet, un gusano informático supuestamente creado por Estados Unidos e Israel, introducido mediante un pendrive, para atacar las instalaciones de enriquecimiento de uranio de Irán ha proporcionado pruebas de que penetrar en un sistema cerrado de control fue, sin duda, manejable. Más recientemente, el malware de la Libélula, muy similar en efectos al Stuxnet, permitió a los hackers tomar el control de sistemas industriales en Europa, poniendo en riesgo a las instalaciones energéticas, plantas nucleares y la infraestructura critica tanto en E.E.U.U. y Europa. Otro caso importante ocurrió a finales de 2014, en una fundición de acero alemana que fue el blanco de un ataque cibernético, cuando los hackers tuvieron éxito y tomaron el control total del software de producción, causaron importantes daños materiales en el sitio.

4 Vulnerabilidades Heredadas

Muchas infraestructuras críticas utilizan sistemas OT heredados que pueden carecer de las medidas de seguridad necesarias para hacer frente a las amenazas cibernéticas modernas. Las empresas que incluyen infraestructura critica en general van creciendo, mejorando, actualizándose, pero siempre sobre proyectos ya instalados, donde la gestión de estas vulnerabilidades representa un desafío constante para garantizar la protección de las infraestructuras críticas, ya que poseen más de algún equipo con menor protección para ataques cibernéticos, que lo hará más vulnerable.

5 ¿Que se requiere para una solución eficaz? Conciencia situacional + Gestión de anomalías + Seguridad

Controlar los sistemas en todo momento es el primer paso para implementar una protección eficaz. Detección de Anomalías y Gestión de Seguridad son dos campos en los cuales se trabaja a nivel mundial, aunque hay países que presentan un escaso desarrollo de estos sistemas, como el nuestro.

El sistema de protección debe cumplir con a lo menos:

1. Generar un inventario de todos los dispositivos.
2. Desarrollar un mapa visual de la red.
3. Verificar las vulnerabilidades del software
4. Que implique impacto Cero, con sensores totalmente pasivos y un diseño de Hardware que permita el llamado "Efecto Diodo". Esto último por la condición de infraestructura crítica y los protocolos de seguridad.
5. Tener un poderoso detector de anomalías que registre:
6. Conexiones inescrupulosas/comportamiento anormal del sistema/contraseñas débiles.
7. Finalmente, se lleve un registro de cambios completo; se estima que un ataque cibernético podría tomar entre 3 a 6 meses después de haber ingresado al sistema interno.

6 Desafíos futuros: "Cerrar la brecha entre OT & IT"

Aunque comparten tecnologías similares, hacer converger OT & IT es un desafío importante y un factor clave de éxito para lograr una protección eficaz. Al proporcionar un lenguaje común y ayudando a compartir la misma percepción del riesgo, ambos mundos pueden converger fácilmente. Este enfoque innovador entre tecnologías operativas (OT) y las tecnologías de la información (IT) disminuyen considerablemente esta brecha, aunque algunos expertos insisten en que la creciente integración de sistemas de tecnología de la información (IT) y tecnología operativa (OT) ha ampliado la superficie de ataque cibernético. Esta convergencia facilita la gestión centralizada, pero también introduce nuevas vulnerabilidades y desafíos de seguridad.

La aplicación de inteligencia artificial (IA) y el análisis avanzado de datos en entornos OT proporciona beneficios en términos de optimización y toma de decisiones. Sin embargo, la seguridad de estos sistemas es crucial, ya que la manipulación de datos o el sabotaje pueden tener consecuencias catastróficas en infraestructuras críticas.

7 Algunos avances en Chile

7.1 Leyes y normativas: Publicación de leyes/ Creación de Ministerio/ otros

Ley N°21.663, Marco De Ciberseguridad [2]. Esta ley tiene por objeto regular la normativa general aplicable a las acciones de ciberseguridad de los organismos del Estado, ya sea entre ellos o con entidades privadas. Fue promulgada el 26-mar-2024 y publicada el 08-abr-2024

Ley N°21.459, Establece Normas Sobre Delitos Informáticos y sus sanciones [3]. Actualiza la normativa nacional para adecuarlas al Convenio de Budapest del 2004 [4],

y facilitar la persecución de los delitos informáticos a través de las fronteras internacionales. Fue promulgada el 09-jun-2022 y publicada el 20-jun-2022.

Decreto 83. Promulga el Convenio sobre Ciberdelincuencia, promulgado el 28 de agosto del 2017. [5]

7.2 Entidades relacionadas:

La Agencia Nacional de Ciberseguridad (ANCI), creada en marzo del 2024, organismo rector de la ciberseguridad en Chile, encargado de regular, fiscalizar y sancionar a todos los organismos públicos y privados que presten servicios esenciales.

El Consejo Multisectorial, mientras que se mantiene el Comité Interministerial de Ciberseguridad

La Red de Conectividad Segura del Estado

El Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática Nacional (CSIRT) y el mismo organismo para la Defensa Nacional, que son los organismos estatales encargados de coordinar la respuesta a incidente de ciberseguridad de efecto significativo en el país y apoyar técnicamente a los organismos del Estado en los incidentes que afecten su capacidad de operación.

7.3 Desarrollos:

Se ha iniciado un trabajo en conjunto con la USACH, Departamento de Tecnologías Industriales, preparando personas en este ámbito mediante el Diplomado en Ciberseguridad de Redes, que se efectúa todos los años; con la Facultad de Ingeniería de la USACH que está preparando una segunda versión del CYBERSEC CHILE 2024 [6], con la Universidad de Lyon y con SENTRYO, empresa francesa perteneciente a CISCO, especialista en IIoT.

En la fotografía se aprecia a un estudiante de la Facultad Tecnológica de la USACH en una presentación en el Seminario Scada Security Summit.

Conclusiones

Chile no tiene, a nivel país, un desarrollo en este ámbito, los Estados Unidos y los países europeos nos llevan mucha ventaja, en estos países ya trabajan con un I-SOC, integrando ambos mundos el IT y el OT; los antivirus, los cortafuegos y otras herramientas o programas similares son solamente medidas de prevención muy limitadas para operaciones específicas, pero no para la protección industrial ni menos a la gestión total de la seguridad tanto pública como privada. En Chile no se tiene experiencia en Ciber Ataques Industriales, por lo menos es lo que se piensa, porque no hay herramientas ni antecedentes que lo confirmen, la frase que más se ocupa hoy para sensibilizar a los gobiernos es "Ya no es cuestión de si sucederá… la cuestión es ¿Cuándo sucederá?"

La ciberseguridad en tecnología operativa es un aspecto fundamental para garantizar la resiliencia y la seguridad de las infraestructuras críticas de un país. Las tendencias emergentes, como la convergencia IT/OT y la adopción de IIoT y IA, presentan oportunidades y desafíos en materia de seguridad. Es crucial que las organizaciones, tanto públicas como privadas, que gestionan infraestructuras críticas implementen medidas de seguridad robustas y estén eficientemente preparadas para hacer frente a los riesgos cibernéticos en constante evolución para proteger mejor los activos y dispositivos a escala.

Referencias

[1] Liang, Qiao y Xiangsui, Wang (1999). La guerra más allá de los límites. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1106936

[2] Ley 21.663 (2024). Recuperado de https://ciberseguridad.gob.cl/noticias/ley-marco-de-ciberseguridad-es-publicada-en-el-diario-oficial/

[3] Ley 21.459 (2022). Recuperado de https://ciberseguridad.gob.cl/noticias/nueva-ley-de-delitos-informaticos-entro-en-vigor/

[4] Convenio de Budapest (2047). Recuperado de https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/

[5] Decreto 83. (2017). Promulga Convenio sobre la Ciberdelincuencia. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1106936

[6] Congreso Cybersec 2024. (2024) Recuperado de: https://fing.usach.cl/es/congreso-cybersec