Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales

Jorge Kamlofsky[1], Gerardo Gonzalez[2] y Santiago Trigo[3]

[1] CAETI – Universidad Abierta Interamericana
Av. Montes de Oca 725 – Buenos Aires – Argentina
Jorge.Kamlofsky@uai.edu.ar

[2] Universidad Nacional de la Defensa, Facultad de Ingeniería del Ejército Argentino.
Av. Cabildo 15, Buenos Aires, Argentina
Gerardo.Gonzalez@undef.fie.edu.ar

[3] Facultad de Ingeniería, Universidad FASTA.
Gascón 3145, Mar del Plata, Argentina
SantiagoTrigo@ufasta.edu.ar

Resumen

La producción masiva de bienes se automatiza mediante los sistemas de control industrial. Estos sistemas son muy robustos y son aptos para funcionamiento contínuo. Gracias a ello, estos sistemas automatizan también, plantas de potabilización de agua, producción y distribución de energía, siderúrgicas, y sistemas de semaforización, entre otros. Es decir, automatizan muchas infraestructuras críticas. Estos sistemas no se pensaron para ser seguros. Por ello, su seguridad se basó en el aislamiento físico.

Nuevas necesidades de mayor eficiencia y productividad requieren de la integración de estos sistemas con los sistemas de administración, con nuevas tecnologías como ser: big data, internet de las cosas, inteligencia artificial, entre otras, e incluso con Internet, dejándolos expuestos a una gran cantidad de riesgos y amenazas para los que no están preparados.

En este proyecto se estudian los riesgos de ciberseguridad a los que están expuestas las infraestructuras críticas industriales. Se plantea la elaboración de una guía para mitigarlos y remediar los efectos frente a estos incidentes.

Palabras clave: seguridad en sistemas industriales, ciberseguridad en scada, seguridad de tecnologías operacionales, ciberdefensa en infraestructuras críticas.

Contexto

El proyecto presentado en este trabajo es un PDTS (Programa de Desarrollo Tecnológico-Social) aprobado por resolución del Poder Ejecutivo Nacional RS-2021-05630389. Se inició en 07/2020 y tiene una duración de tres años.

Los proyectos PDTS son considerados proyectos de interés o relevancia nacional, local o regional, y deben poseer instituciones financiadoras, adquirientes y demandantes [1].

Las instituciones que desarrollan y financian el proyecto son: la Facultad de Ingeniería de la Universidad Fasta (UFASTA), la Facultad de Tecnología Informática de la Universidad Abierta Interamericana (UAI) y la Facultad de Ingeniería del Ejército de la Universidad Nacional de la Defensa (FIE). Las instituciones adoptantes del proyecto son:

la empresa Trend Ingeniería, el Comando Conjunto de Ciberdefensa, la Dirección de Ciberdefensa del Ejército y la Facultad de Ingeniería del Ejército. Las instituciones demandantes son: La empresa Trend Ingeniería y la Dirección Nacional de Ciberseguridad.

Introducción

Desde mediados del siglo XVIII hasta la fecha las revoluciones industriales han producido una explosión demográfica. Creció fuertemente la esperanza de vida y se redujo notoriamente la pobreza. Estos cambios se lograron gracias al incremento de la disponibilidad de bienes y de alimentos, el incremento de la necesidad de mano de obra y mejoras permanentes en las condiciones sanitarias [2]. La primera revolución industrial se basó en la mecanización de la producción. La segunda (estimada desde 1870 a 1970), se caracterizó por el uso intensivo de energía (eléctrica y petróleo).

La tercer revolución industrial se basó en la incorporación de dispositivos electrónicos, informáticos y redes de comunicaciones para la automatización de la producción.

La automatización de la producción a gran escala se realiza con los ICS (del inglés: Industrial Control Systems). Los ICS consisten en sistemas de tele-mando y tele-control de procesos compuestos por autómatas industriales (según sus siglas en inglés): RTU (Remote Terminal Unit), PLC (Programmable Logic Controller), DCS (Distributed Control System) y/o PAC (Programmable Automation Controller) que pueden interconectarse [3]. A ellos se les conectan entradas y salidas, discretas y/o analógicas como ser: micro-switches, sensores de temperatura, actuadores para encendido de motores, llaves, etc. Poseen procesadores de pequeño porte. Su lógica es determinista, lo cual favorece a la alta disponibilidad, esencial en el ambiente industrial [4]. Los ICS se supervisan y controlan en tiempo real desde sistemas informáticos llamados SCADA (del inglés: Supervisory Control and Data Acquisition).

Por tratarse de tecnología que impacta físicamente sobre la operación, se denomina OT (del inglés: Operation Technology). Gracias a su robustez, automatiza procesos que requieren uso continuo: plantas de producción de vestimenta, equipos, pero también: plantas alimenticias, de potabilización de agua, de producción y distribución de energía, transporte, siderúrgicas, entre otras. Es decir, está presente en las infraestructuras críticas de naciones. Este último sub-conjunto es el objeto de análisis de este proyecto: las Infraestructuras Críticas Industriales (ICI).

Enormes diferencias tecnológicas entre IT (del inglés: Information Technology) y OT y el aislamiento físico de los SCADA les dieron a los ICS una falsa sensación de seguridad por ocultamiento [5, 6]. Desde el ataque a la central nuclear de Irán de Natanz con el malware Stuxnet en 2010 [7], la comunidad internacional mostró gran preocupación: hasta ese momento, se pensaba imposible que un malware (IT) pudiera afectar la seguridad de las infraestructuras basadas en OT. Se trabaja en soluciones [8–10].

En IT se posee gran experiencia en seguridad. Y diferentes normas (entre ellas: [11,12]) basan la seguridad en tres pilares (en orden según su importancia): confidencialidad, integridad y disponibilidad. Pero en OT, el orden de prioridades es el opuesto. Quizás por ello, no es tan sencillo implementar las soluciones de IT en el mundo OT a pesar de existir normas y estándares de seguridad (entre ellos: [13,14]). Para mostrar ello, en [15] se plantea que una

gran parte de los incidentes de ciberseguridad en sistemas OT podrían haberse evitado si se hubiera implementado algún sistema de gestión de Seguridad Informática.

Hoy, desde hace una década estamos ingresando en la cuarta revolución industrial, caracterizada por la integración de los ICS con las nuevas tecnologías: inteligencia artificial, internet de las cosas, big data, realidad aumentada y con los sistemas corporativos (IT). A esta integración se la denomina Industria 4.0 [16–18]. Esta nueva necesidad de mayor integración tecnológica expone aún más a las ICI a amenazas y riesgos: un problema de seguridad en estas instalaciones puede significar el colapso de servicios vitales para la población.

En este proyecto se propone el desarrollo de una guía para el abordaje de incidentes de ciberseguridad en las ICI que atienda a la prevención de incidentes, su remediación y análisis forense.

Líneas de Investigación, Desarrollo e Innovación

Este proyecto se desarrolla íntegramente dentro de la línea de Seguridad Informática o Ciber-Seguridad. Pretende unir los esfuerzos realizados en el tema por cada uno de los grupos de investigación.

El desarrollo del proyecto se inició con presentaciones de lo realizado en el tema por cada uno de los grupos de investigación. También realizaron presentaciones tanto demandantes como adquirientes. Continúa con reuniones de investigación donde se presentan tanto lineamientos de trabajo para los equipos de investigación, como resultados parciales obtenidos. Cada grupo por separado desarrolla las tareas asignadas.

Se considera importante que en todas las reuniones en las que participan todos los grupos de investigación, se invite tanto a demandantes como a adquirientes a conocer los pasos que los equipos de investigación realizan, de modo de corregir tempranamente algún desvío o acentuar el trabajo sobre un acierto. Además facilita el proceso de transferencias y capacitación hacia adquirientes y demandantes.

Se puede dividir al proyecto en las siguientes etapas: la evaluación de riesgos de seguridad informática en los sistemas de automatización industrial, la elaboración de recomendaciones para mitigar los riesgos en los sistemas de automatización industrial y sugerencias para la actuación para dar respuesta a incidentes y análisis forense en sistemas de automatización industrial.

Resultados y Objetivos

Este proyecto es desarrollado por tres grupos de investigación de distintas instituciones académicas. Cada grupo de investigación posee resultados previos en el tema:

El proyecto de la UAI se denomina “Ciberseguridad en los Sistemas de Control Industrial: Clave para la Ciberdefensa de las Infraestructuras Críticas” y está dirigido por el Lic. Jorge Kamlofsky desde 2015. Los resultados de este proyecto pueden consultarse en [19].

Por parte de la FIE, el proyecto de investigación denominado Infoscopia: es una interesante propuesta que trata el tema de estudio. Está dirigido por el CN Ing. Cesar Cicerchia. Más detalles del proyecto pueden obtenerse en [20].

Por el lado de UFASTA, el laboratorio Infolab posee varios resultados en temas de Ciberseguridad e Informática Forense. Se pueden consultar resultados en el sitio del Info-lab[1].

[1]Sitio del Info-lab: https://info-lab.org.ar

La presentación de este proyecto generó la firma de convenios de colaboración en temas de investigación entre las entidades académicas, cuyo alcance se amplía más allá del PDTS y comienza a plasmarse en acciones concretas como ser: intercambio docente, interconsultas en investigación, dirección conjunta de tesis, entre otros.

El proyecto busca desarrollar una guía para el abordaje de incidentes de ciberseguridad en infraestructuras críticas industriales.

El proyecto tiene el objetivo principal de desarrollar una guía basada en tres aspectos básicos: los riesgos de seguridad en las infraestructuras críticas industriales, su mitigación y respuesta utilizando para ello el análisis forense.

Esta guía permitirá trabajar tanto ex ante (prevención) como ex post (actuación, remediación, análisis forense) en el abordaje de incidentes de ciberseguridad en infraestructuras que requieren una gestión de extrema seguridad, por su condición de criticidad para la propia organización y la población en general; especialmente, en instalaciones industriales del Estado o de empresas que brindan servicios esenciales (agua, energía, comunicaciones, combustibles, etc).

Formación de Recursos Humanos

El proyecto está dirigido por el Ing. Santiago Trigo. Los co-directores del proyecto son: el Esp. Lic. Jorge Kamlofsky por parte de la UAI y el Ing. Gerardo González por parte de la de la FIE.

Para la FIE, este proyecto se apuntala en la gran importancia que tiene la *concientización y formación* en ciberseguridad para todas las personas involucradas, en especial para los profesionales, en procesos industriales, Tecnología de la operación e Internet de las cosas (IoT). Además, la aplicación directa en el escenario de Infraestructuras Críticas para todos los sectores esenciales del país y sobre todas las cosas en la reducción de riesgos cibernéticos y mejora en la seguridad en general de los procesos del mundo IT, OT e IoT. Para UFASTA, este proyecto le permite que su equipo de trabajo continúe con el desarrollo de servicios y productos sobre esta temática en proyectos futuros que den continuidad a la Línea de Investigación y Desarrollo en Ciberseguridad. Para la UAI, por su lado, este proyecto permite avanzar en las investigaciones en curso acerca de la ciberseguridad en entornos industriales. En particular, Jorge Kamlofsky se encuentra cursando un Doctorado y se espera que los resultados obtenidos del proyecto colaborarán con el desarrollo de su Tesis Doctoral.

El grupo de investigadores está conformado por: Bruno Constanzo, Hugo Curti, Juan Alberdi, Gonzalo Ruiz de Angeli y Leandro Ferrari por UFASTA; Enrique Belaustegui, Pedro Hecht, Claudio Milio y Oscar Romero por UAI y Pablo Croci, Matias Luzuriaga, Nicolás Díaz País, Rafael Olivieri, Juan Ignacio Raffo Triacca e Ignacio Omaechevarría por FIE. Cada uno de ellos son docentes de las instituciones mencionadas y adquirirán conocimientos específicos en el tema los cuales podrán ser transmitidos a los alumnos.

La participación de alumnos de las tres instituciones se considera de gran importancia y está prevista mediante el desarrollo de tesinas de grado, de especialización y tesis de maestría y doctorado, además está prevista la participación de alumnos en prácticas de laboratorio, y pasantías, entre otros.

Referencias

[1] Argentina.gob.ar. “Banco Nacional de Proyectos de Desarrollo Tecnológico y Social”, (2021). Disponible en: https: // www.argentina.gob.ar / ciencia / banco-pdts / criterios-de-los-proyectos. [Consultado: 20/02/2020].

[2] Montagut Contreras, Eduardo. “La transición demográfica en la Revolución Industrial”, Los ojos de hipatía, ISSN: 2341-0612, (2017)

[3] Miguel. “¿DCS, PLC, PAC o RTU?,” Control Real Español, (2015). Disponible en: https: // controlreal.com / es / dcs - o - plc – o – pac – o - rtu/. [Consultado: 8/03/2017].

[4] Romero Mestre, H. “Çiberseguridad en sistemas de control industrial o ICSs.” Trabajo Final de Master. Incibe, UOC, URB, Universitat Autonoma de Barcelona, (2018).

[5] Courtois, N. "The dark side of security by obscurity, and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime." IACR Cryptology ePrint. 137, (2009).

[6] Menezes, A., Van Oorschot, P., Vanstone, S. "Handbook of applied cryptography”. CRC press, (1996).

[7] Englert, M. ”Cyber meets nuclear Stuxnet and the cyberattacks on Iranian centrifuages." Deutschen Physikalischen Gesellschaft, (2013).

[8] Corvalan, F. "Seguridad de Infraestructuras Críticas: Visión desde la Ciberdefensa." III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, (2015).

[9] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. and Timorin, A. Industrial control systems vulnerabilities statisttics." Kaspersly Labs, (2016).

[10] Sajid, N., Patel, S. and Patel, D. ”Assessing and augmenting SCADA cybersecurity: A survey of techniques." Computers and Security 70, (2017): 436-454.

[11] ISOTools. ”ISO 27001." (2015). Disponible en: https:// www.isotools.org / normas / riesgos-y-seguridad / iso-27001 [Consultado: 20/02/2021].

[12] NIST. "Special Publication 800 - 30, revision 1." Information Security. National Institute of Standards and Technology, U.S. Departament of Commerce, (2012).

[13] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M. and Hahn, A. "Guide to Industrial Control Systems (ICS) Security." NIST. Special Publication 800 / 82, revision 2. U.S. Departament of Commerce, (2015).

[14] ISA. “New ISA/IEC 62443 standard specifies security capabilities for control system components”, (2018). Disponible en: https: // www.isa.org / intech-home / 2018 / september-october / departments/new-standard-specifies-security-capabilities-for-c. [Consultado: 20/02/2021].

[15] Kamlofsky, J., Colombo, H., Sliafertas, M. y Pedernera, J. "Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas." III Congreso Nacional de Ingeniería Informática / Sistemas de Información (CONAIISI 2015), ISSN: 2346-9927. (2015).

[16] Lasi, Heiner, et al. "Industry 4.0." *Business & information systems engineering* 6.4 (2014): 239-242.

[17] Bartodziej, C.J. “The Concept Industry 4.0”, BestMasters, DOI 10.1007/978-3-658-16502-4, (2017)

[18] Xu, Li Da, Eric L. Xu, and Ling Li. "Industry 4.0: state of the art and future trends." *International Journal of Production Research* 56.8 (2018): 2941-2962.

[19] Kamlofsky, Jorge, et al. "Ciberseguridad en los sistemas de control industrial: clave para la ciberdefensa de las infraestructuras críticas." XXI Workshop de Investigadores en Ciencias de la Computacion WICC, (2019).

[20] Liporace, Julio César, et al. "Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional–infoscopia–." XXI Workshop de Investigadores en Ciencias de la Computación WICC, (*2019)*.