La ciberseguridad en sistemas ciberfísicos para aplicaciones dentro de la industria 4.0

Mtro. Flores Montaño Luis Alberto
luisfloresmontano@hotmail.com
Mtra. Esther Viridiana Vázquez Carmona
evazquezc1801@alumno.ipn.mx
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo

Boletín No. 83
1o. de marzo de 2021

Resumen

La reciente expansión de la digitalización mundial, y con la creciente detección de diversos ciberataques, ha provocado que la seguridad cibernética se convierta en una prioridad nacional en muchos estados del mundo. Ambos desarrollos del conocimiento se han dado a través de la nueva revolución industrial, conocida como la cuarta revolución industrial o industria 4.0; por lo que, los recientes ciberataques, han provocado adoptar numerosas medidas de protocolos en la seguridad cibernética. Considerando los sistemas ciberfísicos, estos están basados en la seguridad, confiabilidad y disponibilidad; y, por otro lado, estos son la base de las infraestructuras esenciales, pertenecientes

Las infraestructuras esenciales están relacionadas con la prosperidad industrial y tecnológica a nivel global, así como en la seguridad nacional de diversos estados. En esta investigación se considera la consecuencia del posible efecto que se puede tener en un desarrollo cronológico de la seguridad cibernética, además se presenta un marco legislativo de seguridad, el cual es base para una de las principales herramientas de protección en la seguridad cibernética, finalmente se enfatizan y destacan sus principales características.Las infraestructuras esenciales están relacionadas con la prosperidad industrial y tecnológica a nivel global, así como en la seguridad nacional de diversos estados. En esta investigación se considera la consecuencia del posible efecto que se puede tener en un desarrollo cronológico de la seguridad cibernética, además se presenta un marco legislativo de seguridad, el cual es base para una de las principales herramientas de protección en la seguridad cibernética, finalmente se enfatizan y destacan sus principales características.

Palabras Clave: Ataque cibernético, seguridad cibernética, sistemas ciberfísicos, infraestructuras críticas, seguridad.

Summary

The recent expansion of global digitization, and with the increasing detection of various cyber attacks, has caused cyber security to become a national priority in many states around the world. Both developments of knowledge have occurred through the new industrial revolution, known as the fourth industrial revolution or industry 4.0; Therefore, recent cyberattacks have led to the adoption of numerous protocol measures in cybersecurity. Considering cyber-physical systems, these are based on security, reliability and availability; and, on the other hand, these are the basis of essential infrastructures, belonging to industry 4.0.

The recent expansion of global digitization, and with the increasing detection of various cyber attacks, has caused cyber security to become a national priority in many states around the world. Both developments of knowledge have occurred through the new industrial revolution, known as the fourth industrial revolution or industry 4.0; Therefore, recent cyberattacks have led to the adoption of numerous protocol measures in cybersecurity. Considering cyber-physical systems, these are based on security, reliability and availability; and, on the other hand, these are the basis of essential infrastructures, belonging to industry 4.0.

Keywords: Cyber attack, cyber security, cyber physical systems, critical infrastructure, security.

I Introducción

Desde la década de los 80´s se ha empezado a clasificar las infraestructuras esenciales en 6 diferentes categorías, la cuales incluyen diferentes áreas como es la industria, gestión del agua, transporte y salud. Los diversos ataques terroristas a nivel mundial han provocaron una implementación operativa de las infraestructuras esenciales, incluyendo también a los fenómenos naturales predecibles, como puede ser el caso de los huracanes, tormentas o nevadas, las cuales causan daños materiales y humanos, esto en ocasiones provoca que en muchas ocasiones sea casi imposible aplicar planes de rescate adecuados en caso de situaciones críticas en daños de las infraestructuras (por ejemplo, el suministro de agua, gas o electricidad) y que no puedan funcionar de manera adecuada.

Por lo tanto, la protección de las infraestructuras esenciales debe ser garantizada a través de un marco legislativo apropiado. Un ejemplo de esto fue la adopción de la Ley Patriota en el 2001 (en inglés PATROIT Act), con el fin de proporcionar las herramientas necesarias de interceptación y obstrucción de actos terroristas (Doyle, 2002).

Por otro lado, en Europa, debido a los atentados terroristas del 2004 y 2005 en las capitales de España y Reino Unido respectivamente, han provocado que los poderes legislativos promulguen leyes de protección para las infraestructuras esenciales contra el terrorismo. Por lo que en el año 2005 la Unión Europea desarrolló una estrategia para combatir el terrorismo (Lynch, 2005). Por otro lado, se creó el mecanismo de protección civil dentro de este territorio con el fin de coordinar y utilizar eficientemente capacidades de los estados europeos en situaciones de crisis (Lynch, 2005). En cuanto a situaciones de ciber terrorismo, el primer ciberataque de proporciones nacionales tuvo lugar en 2007 en Estonia el cual desencadenado una crisis de operación en la infraestructura de sistemas computacionales.

II Ciberseguridad

Implementar una infraestructura de ciberseguridad en un estado implica definir una serie de estrategias como pueden ser un marco legislativo adecuado políticas apropiadas, normas específicas, formación de habilidades para futuros expertos, la colaboración con instituciones en los dominios, implementación de tecnología avanzada y moderna, el desarrollo de capacidades específicas para concientizar a la sociedad civil, así como sistemas educativos acerca de buenas prácticas en la ciberseguridad, todo esto con el fin de garantizar la seguridad cibernética, acerca de esta última (Lewis, 2006).

Debido al desarrollo acelerado de los procesos de automatización, las tecnologías recientes de comunicación en el área de ciberseguridad se han convertido de suma y vital importancia en la defensa de la vida humana y materiales, por lo tanto, es importante evitar la expansión y proliferación de amenazas o ciberataques.

Acorde con el exsecretario de Defensa de Estados Unidos, Leon E. Panetta (Sherling, 2014), "Un ciberataque perpetrado por estados nacionales o por grupos extremistas violentos podrían ser tan destructivos como los terroristas en los ataques del 11 de septiembre".

Un ciberataque a la red es una acción ofensiva, en contra de la voluntad de algunas personas u organizaciones en sus respectivas computadoras o dispositivos personales, redes informáticas o en infraestructuras con el fin de infiltrarse, robar información o destruirlos.

Existen dos tipos de ciberataques (Lin, 2009): uno llamado indiscriminado o no destructivos que únicamente sirven para extraer secretos de información personal, como es el caso de los virus Petya, WannaCry, Red October; y por otro lado, también se tienen los destructivos, los cuales están orientados a organizaciones o empresas, tal es el caso de la eliminación de información Wi-Fi, el virus Shammon que actúa en las estaciones de trabajo destruyendo la comunicación de servicios por parte de las empresas atacadas; otro ejemplo que se tiene en cuenta en esta clasificación es el Stuxnet, el cual se encargó de la destrucción de la infraestructura nuclear de Irán basada en un gusano malware; adicionalmente se tienen las guerras cibernéticas (en inglés cyberwarfare), las cuales son clasificadas como ataques destructivo utilizado un medio espionaje, un ejemplo de esto es la guerra entre Corea del Sur y Japón en el año 2010,

También se tiene los conocidos espionajes gubernamentales, un ejemplo de esto fue en el 2007, el cual se llevó a cabo a la infraestructura de redes a el gobierno de Estonia (Méndez & Cesar, 2014), otro ejemplo de esto es un ataque a computadoras de los Estados Unidos para el área militar, en la Cumbre del G20. Los espionajes corporativos conocidos que se tienen en consideración son los servicios de guardia de una empresa belga; en donde hubo robo de credenciales y direcciones de correos electrónicos en servidores web otro ejemplo es el ataque a los servidores de correo de Yahoo que tuvo lugar desde el 2012 al 2014. Y finalmente se tienen los robos de información financiera como es el caso de las tarjetas de crédito; como es el caso de las tarjetas MasterCard y Visa en el año 2012.

Cabe mencionar que las características jerárquicas del resguardo de la Información y los sistemas de tecnología de las comunicaciones (TICs), se encuentran en el siguiente orden:

1. Confidencialidad
2. Integridad
3. Disponibilidad.

Este tipo de estrategia concede que el acceso no autorizado sea repudiado, asegurando así la información. Por lo tanto, en las TICs, la información y la confidencialidad son las principales prioridades.

Retomando el ataque al sistema industrial que tuvo lugar en Irán, específicamente en una planta de enriquecimiento de combustible, fue a través del virus informático conocido como Stuxnet en el año 2010. Dicho virus provocó un ataque autónomo (a Siemens en 325 y controladores 417), es decir, sin acceso a Internet. Por lo tanto, los controladores industriales estaban colocados en un área física, entregando así el control de señales a un equipo básico (por ejemplo, máquinas turbo, motores, etc.), y posteriormente capturando las señales de retroalimentación de los transductores (Office for Information Security, 2016). Adicionalmente la función adicional de los controladores industriales era monitorear el flujo del proceso. A pesar de tener sistemas computacionales, los ataques a los controladores industriales pueden causar lesiones a personas u operadores (Office for Information Security, 2016)

Como ejemplo de esto es importante destacar que la era de la información, también debería crecer basándose en Sistemas ciberfísicos (por sus siglas CPS). Cabe destacar que la modernización de lo industrial en los procesos debe basarse en elementos principales con características más seguras.

III. Marco legislativo relacionado con dominio de ciberseguridad

El desarrollo de la ciberseguridad, sistemas ciberfísicos y de las infraestructuras esenciales están fuertemente relacionados con la adopción de leyes, estrategias y estándares específicos por cada nación. En países como Rumania, las bases de la ciberdefensa en las infraestructuras esenciales se instalaron en el 2011, a través de la Ley de identificación y designación de infraestructuras. En ese

mismo año, se creó el Centro Nacional de Respuesta a Ciber Incidentes (también conocido como CERT-RO); así como la Estrategia Nacional de protección de infraestructuras; posteriormente 2 años después la estrategia de seguridad cibernética; estás últimas con el fin de aumentar la seguridad de las personas y la seguridad cibernética de las TICs, con el fin de solidarizar la ciberdefensa (Plesanu, 2014), así como para prevenir o limitar la ciber incidentes.

Una de las estrategias de la Unión Europea es tomar las medidas necesarias para lograr un alto nivel de seguridad de las infraestructuras de información en un solo mercado digital. Así, la directiva conocida como NIS (en inglés Network Internet Security) proporciona requisitos para la creación de un marco de legislación en el campo de la ciberseguridad por los países de la Unión Europea.

En México las estrategias de seguridad cibernética que involucran a los sistemas ciberfísicos surgen en el marco del Plan Nacional de Desarrollo (PND) 2013-2018; la cual, su idea es aumentar la digitalización en México, para que con ello se maximice su impacto económico, social y político en beneficio de la calidad de vida de las personas, sin embargo, actualmente aún existe un grave letargo en (Miguel et al., 2019):

1. Materia archivística. Falta de Organización documental en muchas dependencias.
2. Aplicación de Tecnologías. No existe inclusión de esquemas de preservación digital.
3. Lagunas legales. Referentes a la protección de datos personales en posesión de los sujetos obligados.
4. Ciberseguridad y Vigilancia tecnológica. Falta de medidas de protección en las administraciones.

En el 2019, la ley de ciberseguridad es adoptada para garantizar la protección cibernética en la Unión Europa mediante un esquema de certificados para asegurar el cumplimiento de los estándares de productos, procesos o servicios de ciberseguridad (Kasper & Antonov, 2019). Este tipo de leyes tienen la responsabilidad de garantizar la seguridad; para lograr esto es necesario proteger las infraestructuras, y coordinarlas a través de un mecanismo de programas, planes y procedimientos operacionales. Básicamente, como ya se mencionó las infraestructuras esenciales garantizan el funcionamiento básico de un país (Kasper & Antonov, 2019).

Una infraestructura esencial se comprende tanto de partes física como de tecnologías de la información (TI) partes sin las cuales no se podría defender un Estado, por lo que el bienestar de los ciudadanos se vería afectado, poniendo en peligro el orden público, la seguridad y el funcionamiento de las estructuras de control de algún país. En otras palabras, la infraestructura esencial proporciona servicios vitales a la sociedad (Kasper & Antonov, 2019). Garantizar la protección de la infraestructura esencial es un proceso basado en la identificación y evaluación de amenazas, por lo que, implementar un plan de protección basado en el análisis de riesgo y un seguimiento de la eficiencia lograda en base a la evaluación de resultados, puede llegar a ser de grana utilidad.

IV. Sistemas ciberfísicos

Incrementar la seguridad de las infraestructuras esenciales desde el punto de vista técnico, los métodos de modelado, las técnicas de control específicas se vuelven cada vez más desafiantes. La base para la realización de infraestructuras esenciales consiste en los sistemas ciberfísicos (CPS). Un CPS integra tres tecnologías: computación, comunicación, y control (también se conoce como 3C) (Zhou et al., 2017); estos sistemas combinan las capacidades informáticas y de comunicación con dispositivos físicos como pueden ser sensores o actuadores.

Los principales pilares de un CPS son la seguridad, confiabilidad y disponibilidad, unos ejemplos de los sistemas CPS pueden ser:

–Las redes de comunicaciones

–Ciber sistema distribuido

–Sistemas físicos

Cabe mencionar que los sistemas CPS contienen hardware y software de componentes distribuidos, relacionados con los entornos que utilizan redes a través de sistemas físicos. En la parte del software se incluyen programas para procesar, filtrar y almacenar información. Adicionalmente los sistemas CPS son esencialmente sistemas distribuidos en tiempo real, escalables y confiables; de ahí la importancia de ser seguro.

V. Infraestructuras esenciales

Las infraestructuras esenciales (CI) proporcionan servicios básicos cómo pueden ser telefonía, transporte o energía y servicios públicos. Los circuitos integrados constan de sistemas de control y control de las redes dentro de las CI, estás deben de garantizar la seguridad de los procesos industriales.

Distintos ataques o desastres naturales o intencionales a las infraestructuras tienen un efecto en cascada, que provocan interrupciones en los servicios de suministro de agua potable o de telecomunicaciones (las cuales son dependientes de la energía),

Las prioridades de las CI son contrarias a la de los sistemas TICs:

1. Disponibilidad
2. Integridad
3. Confidencialidad

Este orden garantiza que la información está siempre disponible para asegúrese de que el servicio se mantenga tanto como sea posible.

VI. Conclusiones

Este documento es el preámbulo en el contexto del desarrollo, de la adopción por muchos estados para un plan de desarrollo de inteligencia. Por otro lado, está orientado hacia el marco legislativo sobre protección de las infraestructuras críticas de uno o más estados.

Este tipo de infraestructuras son vitales para la existencia de un estado moderno. El papel actúa como una gran advertencia de la actual estrategia ofensiva sostenida por las organizaciones criminales, y la importancia de difundir el conocimiento de sistemas ciberfísicos en la academia, con el propósito de desarrollar una cultura de ciberseguridad en todos los dominios como social, económico, médico, transporte, industria, entre otros, con el fin de prevenir y defenderse de todo tipo de ataques. Además, los ataques a infraestructuras industriales o esenciales, o ataques a ordenadores, pueden causar no solo daños materiales, sino también lesiones del personal técnico, o pérdidas de vidas humanas.

Finalmente, se proporciona información sobre la ciberseguridad, en la infraestructura esencial de los sistemas ciberfísicos, como es el caso de los marcos legales para el desarrollo de herramientas y sistemas que puedan garantizar la defensa y protección, y así tener una incursión histórica en los ataques a los que son sometidos.

Referencias y recursos electrónicos

1. Doyle, C. (**2002**). *CRS Report for Congress Received through theCRS Web The USA PATRIOT* Act : A Sketch. 3162.

2. Kasper, A., & Antonov, A. (**2019**). *Discussion Paper Towards Conceptualizing EU Cybersecurity Law.* http://www.zei.de

3. Lewis, J. A. (**2006**). *Cybersecurity and Critical Infrastructure Protection.*

4. Lin, H. S. (**2009**). *Offensive Cyber Operations and the Use of Force* http://www.microsoft.

5. Lynch, A. (**2005**). *LEGISLATING WITH URGENCY-THE ENACTMENT OF THE ANTI-TERRORISM ACT*ACT [NO 1] http://www.chiefminister.act.

6. Méndez, V., & Cesar, J. (**2014**). *La ciberdefensa en Colombia.* http://geektheplanet.net/5642/juan-manuel-

7. Miguel, J., Fonseca, C., Mx, M. C., & Zavala Juárez, B. **2019**). *CIBERSEGURIDAD Y VIGILANCIA TECNOLÓGICA: UN RETO PARA LA PROTECCIÓN DE DATOS PERSONALES EN LOS ARCHIVOS AUTORES.* https://www.eumed.net/rev/tlatemoani/index.html

8. Office for Information Security, F. (**2016**).RECOMMENDATION: IT IN PRODUCTION BSI Publications on Cyber-Security Industrial Control System Security. http://ics-cert.us-cert.gov/Recommended-Practices

9. Plesanu, T. (**2014**). *Strategic Changes in Security and International Relations. In PROCEEDINGS* (Vol. 3). https://www.researchgate.net/publication/321490744

10. Sherling, M. ((**2014**). *The Likely Regulators? An Analysis of FCC Jurisdiction over Cybersecurity* http://www.mcafee.com/us/

11. Zhou, P., Zuo, D.-C., Hou, K.-M., Zhang, Z., & Shi, H.-L. (**2017**). *A Light-weight Multilevel Recoverable Container for Event-driven System: A Self-healing CPS Approach.*