Ciberseguridad industrial: La seguridad como un todo.

Si nos remontamos a unos quince años atrás, en general, los ataques cibernéticos estaban enfocados principalmente en corromper y modificar las páginas de inicio de sitios web (particularmente entidades públicas y gubernamentales, compañías multinacionales). Estas incursiones tenían como objetivo dejar un mensaje político, una idea, un germen de protesta. Era un enfoque "romántico".

Con el tiempo, en paralelo con la evolución de las redes de datos, la capacidad de procesamiento disponible y la introducción paulatina de procesos de negocio y de intercambio comercial en internet, los ciberataques han ido mutando hacia una mayor complejidad y sofisticación, de la misma forma que el enfoque también cambio: ya no reside en la protesta política-ideológica, sino que derivó en eventos de denegación de servicio (DOS), para luego evolucionar hacia un perfil lucrativo.

En general, los ciberataques actuales tienen un fin económico, ya sea por el "secuestro" de información vital para el negocio (ransomware), y que requiere de un rescate para su restablecimiento, o bien la detención de las operaciones como un trabajo "por encargo". Es decir, el ciberataque a medida del cliente que lo requiere.

Las redes industriales como objetivo.

Dentro de este contexto, el primer objetivo de este nuevo tipo de ataques fueron las redes administrativas (aquellas que interconectan servicios de oficinas), ya que eran las que se encontraban conectadas directamente a internet y, por ende, más expuestas al

mundo externo. Este perfil de ataque se ha ido modificando para incluir como objetivo a las redes industriales.

En general estas redes siempre estuvieron aisladas ya que no tenían conectividad con internet (o muy poca) debido a que su servicio estaba orientado a la operación de las líneas productivas. Sumado a esto, este enfoque se vio afectado por la hiperconectividad que venimos experimentando (ej. Industry 4.0, Internet of Things, Analíticos de datos, etc.), y potenciado por una arquitectura de redes que no fue diseñada para afrontar estos desafíos (ej. interconexión entre redes industriales y administrativa, falta de estándares de plataformas, obsolescencia de aplicativos y sistemas operativos, etc.).

En este sentido, las redes industriales se han convertido en un punto de ataque ya que es posible alcanzar el objetivo económico (ransomware), el robo de información propietaria (espionaje industrial/impacto público) y la detención del proceso productivo (delitos entre competidores). Estos eventos pueden ocasionar también, como consecuencia, la pérdida de la vida humana.

Esto es singularmente relevante ya que el compromiso de un equipo de control, por ejemplo, un PLC (Programmable Logic Controller), puede derivar en un funcionamiento no esperado de una máquina que ocasione un accidente impactando en la imagen pública de una industria estratégica (energía, manufactura crítica). Es por eso que, tras este tipo de ataques, no solamente están presentes las bandas especializadas en Cibercrimen, sino también agencias de inteligencia de gobiernos nacionales.

Ciberseguridad + Seguridad de planta = Ciberseguridad Industrial

El enfoque de seguridad industrial, entonces, tiene relevancia no solamente con el paradigma clásico de establecer procedimientos, protocolos de trabajo y controles para

la operación segura en la línea de producción –únicamente desde un enfoque físico–, sino que ahora es necesario incorporar las estrategias, herramientas y equipos de trabajo cuya misión es monitorear, analizar y dar respuesta ante eventos de Ciberseguridad.

Es importante resaltar que, sin una práctica de Ciberseguridad industrial, no es posible dar cobertura completa a los aspectos derivados del concepto de *seguridad industrial*, ya que los incidentes y accidentes –ya sea con pérdida de días, o fatales–, también pueden tener su origen en un ciberataque.

El cambio cultural.

Otro aspecto clave a considerar, en línea con los cada vez más recurrentes ataques a las redes industriales, es un proceso de cambio cultural complejo dentro del ámbito industrial que decididamente impacta sobre los procesos productivos. Este cambio, justamente, tiene sus raíces en establecer nuevos estándares y procedimientos antes desconocidos y o ignorados por las líneas productivas. Parchar servidores, monitorear el antivirus, definir estrategias de control para dispositivos en redes aisladas y gestionar la obsolescencia son solo algunos de los aspectos que pasan a ser parte de la operación cotidiana. Esto necesariamente colisiona con una formación técnica clásica que no incorpora los conceptos de ciberseguridad y que entiende que las cuestiones de conectividad y cómputo son asuntos a resolver por Sistemas (Soporte) desde una óptica coyuntural y no estratégica.

Claves para fortalecer la Ciberseguridad Industrial

Existen una serie de aspectos a atender para poder establecer una práctica de Ciberseguridad Industrial eficaz y sustentable:

- **Creación de un área especializada** para identificar, evaluar y responder ante eventos de Ciberseguridad Industrial. Es necesario que el equipo esté compuesto por diferentes perfiles con habilidades en diversos ámbitos del problema (Ej. redes, dispositivos de control, etc.). Esto permite potenciar la capacidad y eficacia del equipo.

- **Definición de una arquitectura de Ciberseguridad** que, mínimamente, incluya:
    - **Estructura de monitoreo centralizado**. De acuerdo a la definición de la norma ISA/IEC 62.443 en su Requerimiento Fundacional número 6 "Timely Response to Incidents" [1] establece la necesidad de identificación, análisis y respuesta oportuna ante eventos de ciberseguridad que sucedan en el ámbito industrial. Para implementar este concepto, el esquema deseable es contar un SOC (Security Operations Center) que apliqué un monitoreo 24x7 de la actividad dentro de la red industrial. Ver Figura 1.

[1] La norma ISA/IEC 62.443 define siete Requerimientos Fundacionales (FR). El Nro. 6 –FR 6– establece mecanismos para la respuesta oportuna ante incidentes.

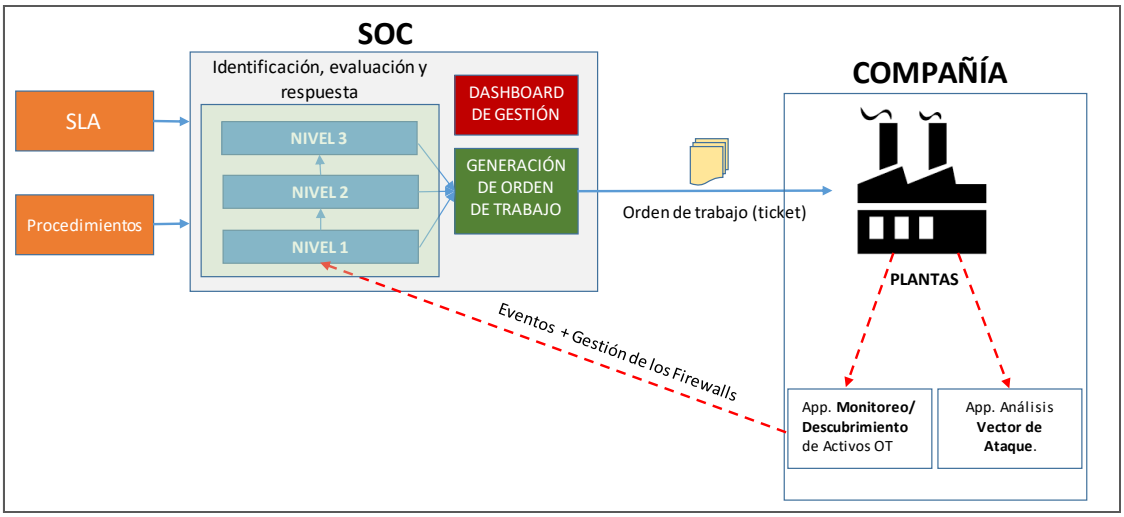

Figura 1.

En general, cuando se está en búsqueda de este tipo de herramientas, se deben enfocar prestaciones relacionadas con el descubrimiento de los activos OT, el inventario derivado y cómo "conversan" estos activos entre sí (justamente para detectar comportamientos anómalos). Junto con esto, tener la posibilidad de conocer las distintas vulnerabilidades de los dispositivos bajo monitoreo. De la misma forma, se requieren capacidades para poder evaluar todo el input de activos dentro un contexto del vector de ataque presente, es decir, en cuantos pasos un atacante puede tomar control en base a las vulnerabilidades identificadas y los controles presentes (ej. Firewalls, estrategia de antivirus, configuración del acceso remoto, etc.). Esto permite simular los distintos escenarios de ataque y, de esta manera, priorizar las actividades de remediación derivadas. Ver Figura 2.

Vector de ataque

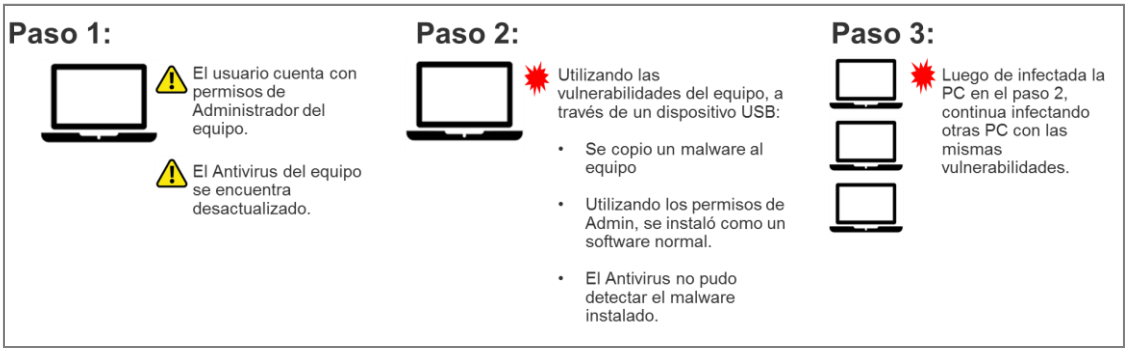

Figura 2.

- **Segregación de redes**. Es recomendado separar los mundos IT-OT. Esto permite establecer un control del flujo de la información entre zonas de acuerdo a lo establecido por la norma ISA/IEC 62.443 en el FR 5, "Restricted Data Flow". Para esto, es necesario implementar la segregación de las diferentes zonas de forma física o lógica, haciendo foco particularmente en las redes críticas de control (alto impacto). Ver Figura 3.

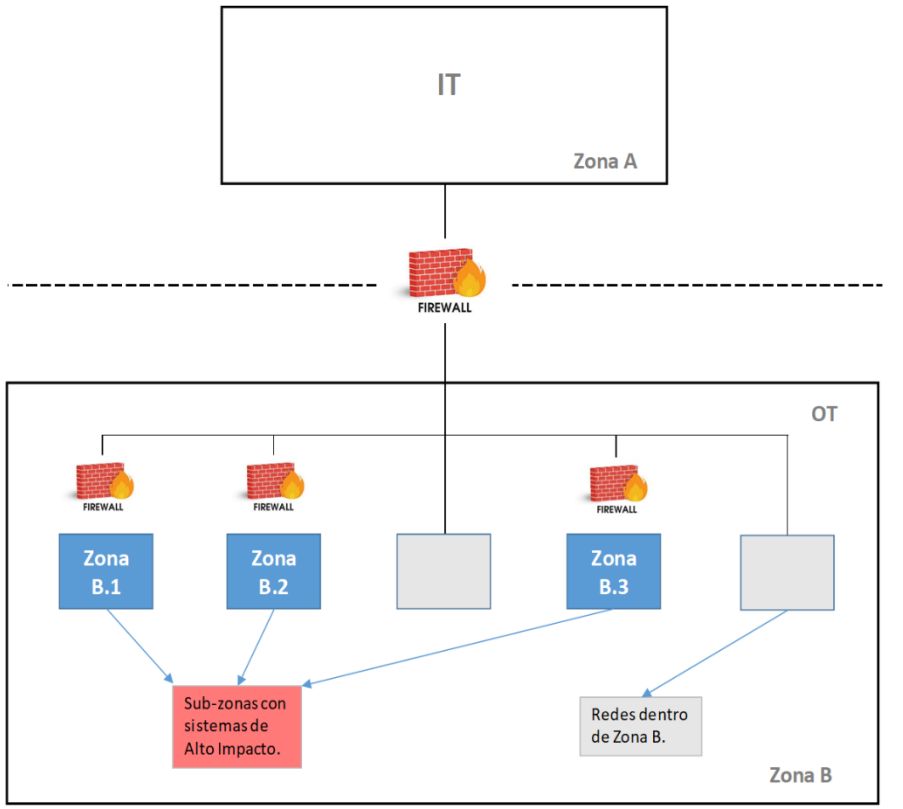

Figura 3.

- **Control de acceso remoto** a dispositivos de la red industrial. La implementación de una "red de salto" desde la *iDMZ* [2] de cada planta permite un mejor control de los accesos externos a través de un único punto de entrada y de salida. Adicionalmente, es posible aplicar granularidad en los permisos de acceso (ej. acceso a una IP/Servicio en particular) siguiendo el principio del *menor privilegio* [3]. Este concepto de controlar el acceso remoto a la red es planteado por la norma NIST 800-53 en su función "Proteger", como así también en el estándar COBIT 5 –APO13.01, DSS01.04, DSS05.03.

- **Estrategia de remediación**. En base a las distintas vulnerabilidades/desvíos identificados, se deben aplicar remediaciones realizando una aproximación prioritaria basada en el riesgo.

- **Investigación y desarrollo (relacionamiento con vendors)**. Se deben contemplar las nuevas tecnologías de dispositivos industriales seguros y el roadmap de adopción en la línea productiva. Esto requiere el análisis de la obsolescencia y un relacionamiento planificado con proveedores de Nivel 1 (Sensores, PLC, instrumentos, etc.).

---

[2] iDMZ (Industrial Demiliarized Zone) refiere a una red local controlada que establece servicios y control de acceso entre dos redes (en este caso, IT/OT).
[3] La norma ISA/IEC 62.443, lo establece como "principio básico que sostiene que a los usuarios (humanos, procesos de software o dispositivos) se les debe asignar la menor cantidad de privilegios de acuerdo con sus deberes y funciones asignados.".

- **Trabajo conjunto entre los distintos actores (Governance)**. Es necesario que la efectividad del equipo se potencie mediante la coordinación inter-área. Esto permite que la respuesta ante los eventos de Ciberseguridad no penalice la estabilidad de los sistemas de planta, y de esta manera, de mayor previsibilidad a la planificación de la producción.

En resumen, para poder establecer una práctica de seguridad industrial eficaz y sustentable, es necesario un enfoque global sobre la seguridad de planta asignando la misma relevancia a los eventos de ciberseguridad. Es crítico poder delinear un diseño de ciberseguridad industrial teniendo en cuenta los aspectos relevantes: monitoreo, análisis y respuesta, la segregación de las redes y un esquema de remediación a medida.

Asimismo, se debe gestionar el proceso de cambio cultural para introducir los conocimientos y dinámicas particulares que permitan establecer gradualmente una visión estratégica del problema, y en paralelo, empoderen a los equipos industriales para afrontar el trabajo diario bajo este nuevo paradigma.

Todo esto debe ser moderado y gestionado bajo un esquema de Governance que habilite y potencie el trabajo coordinado entre áreas de diferentes incumbencias.

Si bien estas son simplemente algunas notas que resumen –a modo de ejercicio general– un camino hacia el establecimiento de una práctica eficaz, medible y sustentable de ciberseguridad industrial, lo clave es comprender que la gestión de la seguridad es una tarea que exige un esfuerzo continuo y sostenido en el tiempo para comprender y aceptar el cambio, ya que lo relojes vuelven a cero todos los días.

Bibliografía.

- International Society of Automation (ISA), (2013), ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels.
- National Institute of Standards and Technology (NIST), (2020), SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations
- International Organization for Standardization (ISO), (2013), ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements.
- Information Systems Audit and Control Association (ISACA), (2019), COBIT 5 – Control Objectives for Information Technologies.
- Bachrach, E. (2014), *En Cambio*, 2da. Ed., Buenos Aires, Sudamericana.