CIBERSEGURIDAD EN EL SECTOR ENERGÉTICO:

Riesgos y estrategias de mitigación

PROCETRADI

El **sector energético** subestima la importancia de la **ciberseguridad**, con la creencia errónea de que involucra poca tecnología y no afecta las operaciones. Sin embargo, el 97% de los profesionales de seguridad de ICS en la energía, petróleo y gas creen que es una preocupación creciente. La **transformación digital** ha llegado a todas las industrias, y con la automatización avanzada, el uso de sistemas ciberfísicos seguirá creciendo. Aunque la postura de seguridad cibernética puede no ser una preocupación inmediata, es importante comprender las implicaciones de la transformación digital en la seguridad cibernética y del **sistema de control industrial** (ICS) para modernizarse eventualmente.

Los retos de gestionar la ciberseguridad ***EN EL SECTOR ENERGÉTICO***

La infraestructura tecnológica de la mayoría de las empresas de la industria manufacturera y de suministro (incluidos los servicios públicos de energía) se puede dividir en dos categorías:

- **Sistemas de TI de la planta**
- **ICS**

Los **sistemas de TI de una planta** y los **sistemas de Ciberseguridad en infraestructuras críticas** (ICS) tienen diferentes demandas de ciberseguridad debido a su enfoque en la protección de datos versus la prevención de tiempo de inactividad y pérdida de producción. Aunque ambos son importantes en el sector energético, los ciberdelincuentes tienen diferentes enfoques para atacar cada sistema. Por ejemplo, pueden usar **ransomware** para sellar o robar datos y extorsionar a los propietarios, o pueden utilizar **ataques DDOS** para detener las operaciones de ICS y restaurarlas solo cuando se cumpla una condición. En resumen, los objetivos detrás de los ataques son los mismos, pero los enfoques son diferentes.

Clases de ciberataques en ***EL SECTOR ENERGÉTICO***

El impacto de los ataques cibernéticos lanzados sobre ICS y TI de planta se puede clasificar en tres categorías:

Pérdida de vista: donde un sistema continúa funcionando, pero ya no puede ver lo que está haciendo.

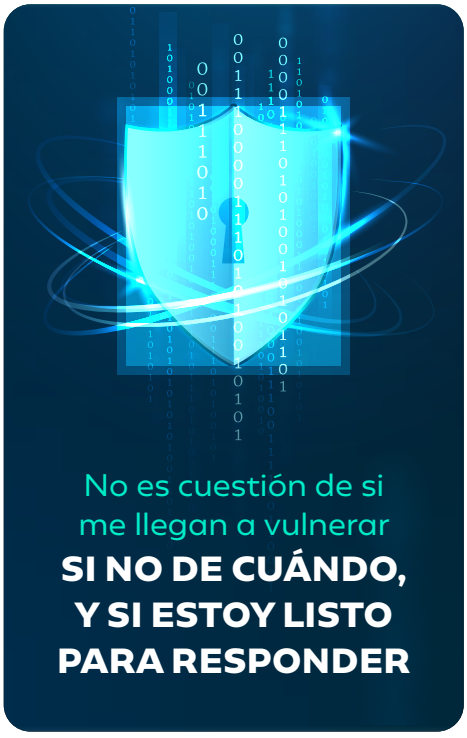
Pérdida de control: cuando un sistema es secuestrado y ya no responde a sus instrucciones o comandos.

Pérdida de seguridad: donde un sistema puede volverse tan inestable que aumenta su potencial para dañar o matar.

La pérdida de seguridad es la peor situación en la que se encuentra una empresa de servicios públicos de energía. El **ataque Tritón** de 2017 fue uno de los primeros casos en los que se envió malware para intentar causar daños o la pérdida de vidas.

Casos como estos pueden manchar las actitudes de las personas hacia la tecnología ciberfísica, incluso si, esa tecnología está diseñada para ser más eficiente energéticamente. Por ejemplo, más de un tercio de los estadounidenses, así como más del 70 % de los canadienses, están considerando comprar un automóvil eléctrico debido al deseo de conducir vehículos de bajo consumo que sean mejores para el medio ambiente. Sin embargo, muchas de esas mismas personas todavía desconfían de la idea de los autos sin conductor. Después de todo, si algo saliera mal, los resultados serían catastróficos y es posible que el conductor no pueda recuperar el control del vehículo.

Pero ¿qué **amenazas** y **riesgos** deberían preocupar más al **sector energético**? Después de todo, ya no se trata solo de una pérdida de dinero, sino también de una pérdida de vidas.



49%

Organizaciones que reconocen haber sido vulneradas en su ciberseguridad

21%

Recientemente atacadas

17%

Fallaron en un proceso de auditoría de ciberseguridad

Estrategias de mitigación de ***ATAQUES CIBERNÉTICOS***

Las empresas del sector energético ahora tienen que preocuparse por la ciberseguridad. Afortunadamente, hay algunas formas de tapar cualquier agujero en su seguridad.

Realización de evaluaciones de OT y ICS

Hacer un inventario y evaluar el estado de sus sistemas es el primer paso para asegurarlos, ya que lo ayudará a determinar la postura actual de su ciberseguridad. Esto es especialmente importante para aquellas empresas de servicios públicos que tienen equipos antiguos y tecnología operativa en el entorno. Las evaluaciones de OT e ICS pueden ayudar a identificar los riesgos de ejecutar tales sistemas y determinar qué impacto tendrá la integración de TI con ICS/OT.

Abordar la amenaza interna

Las empresas pueden evitar esto implementando controles de acceso granulares y creando una cultura de ciberseguridad en el lugar de trabajo.

Desarrollar un proceso de detección y análisis

Las empresas del sector energético deben contar con procesos robustos de detección y análisis de ciberataques. Esto debe incluir un monitoreo centrado en ICS que detecte cualquier anomalía, incluidos errores, fallas leves o, lo que es más importante, intrusiones cibernéticas.

Creación de planes de respuesta a incidentes

Esto tiene un ligero vínculo con las estrategias anteriores. Cuando ocurre una brecha, una organización debe saber cómo contenerla para mitigar el impacto. Esto también incluye estrategias de búsqueda en las que los malos actores que se han infiltrado en la red se pueden encontrar y desalojar lo más rápido posible. Además, los empleados deben saber a quién contactar e informar cuando el sistema detecta un ataque cibernético.

CONCLUSIÓN

En el **sector energético**, los líderes deben preocuparse por mantener el flujo de energía, por lo que la ciberseguridad no debería ser una preocupación adicional. El objetivo final de la **ciberseguridad** en este sector es asegurar que los ataques no tengan un impacto en el mundo real. Los ciberdelincuentes pueden estar motivados por factores distintos a lo financiero, lo que hace que la **prevención** de ataques sea crucial. A pesar de ello, existen formas de prevenir los ataques cibernéticos en el sector energético.

www.procetradi.com