Plan de respuesta ante incidentes ciberfísicos en una planta de tratamiento de crudo

Por ***Pablo M. Almada*** (KPMG)

El avance de los ciberataques exige a la industria energética nuevas estrategias para proteger sus instalaciones críticas. Este trabajo presenta un plan integral de respuesta ante incidentes ciberfísicos en plantas de tratamiento de crudo, combinando ciberseguridad y operación. Una guía clave para fortalecer la resiliencia y garantizar la continuidad operativa frente al *ransomware*.

Este trabajo fue seleccionado en las 3ª Jornadas de Revolución Digital para Petróleo y Gas.

Contexto del estudio

Las plantas de tratamiento de crudo (PTC) son los puntos neurálgicos de un yacimiento, ya que si se detienen por un periodo prolongado, se ven obligadas a detenerse las baterías, los pozos, las plantas de tratamiento de agua y las plantas de inyección de agua, lo que resultaría en una paralización total de la producción. Dentro de las PTC, hay múltiples activos que son controlados y operados por los sistemas de control, entre ellos se encuentran las calderas que mantienen las temperaturas de los hidrocarburos, controlan las densidades y previenen la generación de parafinas, bombas de desplazamiento, free waters, medidores másicos, entre otros, que aumentan drásticamente la complejidad de la instalación de superficie desde la perspectiva ciberfísica, pero facilita ampliamente su operación. Además, disponemos de múltiples vías de interconexión con redes corporativas para reporting interno, auditoria gubernamental, servicios de backup, acceso remoto, optimización de proceso, interfaces varias, entre otros.

Contexto situacional

Aunque la región, excluyendo EEUU, no ha visto ataques de adversarios altamente sofisticados, la paralización de servicios mediante ciberataques de Ransomware con fines puramente económicos ha ido en aumento en los últimos 5 años. Empresas de O&G de la región, como PEMEX en Mexico u otras en Argentina, han sido blanco de este tipo de ciberataques que por razones de confidencialidad y falta de obligaciones de reporte permanecen en el anonimato.

Este tipo de incidentes no solo alcanzan a las redes corporativas de una compañía, sino también a las redes de campo dando por resultado una falta de visualización y operación de los sistemas de control. El impacto de un ciberataque de esta naturaleza en ambientes corporativos es ya conocido y determinístico en comparación a un ambiente de operación. En este último, al tener una dependencia y un alto grado de cohesión entre los sistemas informáticos y el proceso tisico el impacto empieza a complejizarse.

Ante esta situación nos surgen algunas preguntas que deben ser tenidas en cuenta ya que un ciberataque es un acto deliberado y no una situación/acto no intencional como se tratan en un Hazop clásico. ¿Cuál es su efecto operativo tisico en una instalación de tratamiento de crudo? ¿Puede funcionar una instalación sin un sistema de control? ¿De qué dependemos? ¿Qué elementos tisicos operativos tengo para operar en caso de infección? ¿Qué pasa con las baterías que alimentan nuestra instalación de superficie? Habrá que tomar decisiones que estarán limitadas por el tiempo de las capacidades de operación de la instalación de superficie y la experiencia del equipo sobre el terreno que, por el momento, es cada vez más reducida debido a las capacidades de la tecnología a través de la operación remota.

El desafío principal es sumarse al proceso de contingencia operativa de la PTC dándole un enfoque de ciberseguridad. Para esto, y debido a la propia naturaleza de los sistemas de control, debemos crear un proceso de respuesta cibertisica para hacer frente al ransomware a partir de las 4 fases de respuesta a incidentes: preparación, detección y análisis, contención y erradicación, y recuperación. Cabe destacar la importancia de la preparación para fomentar la resiliencia, la detección temprana y el análisis para introducir conceptos de defensa activa, así como la contención y erradicación, la recuperación, alineada con los tiempos de inactividad operativa y las lecciones aprendidas, es crucial, ya que no siempre el plan funciona como se espera.

A continuación, se realizará una descripción a alto nivel del proceso de creación de un playbook de respuesta ante incidentes desde una perspectiva cibertisica.

Bien sabemos que el planeamiento es la piedra fundamental para acercarse al éxito de una tarea o proyecto, en este caso también lo es. En este punto, se debe lograr un conocimiento profundo de la filosotia de control de la PTC, activos, modos de operación, limites de operación cuando la PTC funciona en un modo degradado, personal en campo, sus capacidades técnicas operativas, sistemas de control que dan soporte a la operación, equipamiento tecnológico presente, inventarios tecnológicos y tisicos de los componentes, interdependencias de la PTC con las baterías, planta de tratamiento de agua, plantas de inyección, entre otros. Este último no es algo menor debido a que al paralizar una PTC se ve directamente afectado todo el funcionamiento del yacimiento, como así también los procesos de la refinería a donde se bombea el hidrocarburo post tratamiento.

Una vez finalizado el relevamiento cibertisico, debemos enfocarnos en definir los equipos de respuestas que estarán formados por operadores, instrumentistas, personal de tecnología de la operación, CSIRT (usualmente el corporativo), personal de soporte, personal de redes, CISO y resto del personal que son parte de los comités de incidentes como el gerente/líder de la PTC, legales, comunicaciones, entre otros. Es importante involucrar este equipo en el proceso de creación de plan de respuesta ante incidentes ya que ellos nos darán una mirada realista y de usabilidad del proceso en cuestión.

Luego, para abordar el proceso de manera realista debemos realizar un análisis Hazop cibernético, donde se interpreta el análisis de peligros y operabilidad (Hazop) desde la perspectiva de un ciberataque, con el objetivo de identificar y priorizar posibles riesgos y vulnerabilidades de ciberseguridad en los sistemas/redes y de safety en los procesos físicos.

Además, con esto logramos comprender cuáles serían las implicaciones si nuestra PTC fuera afectada por un ataque de ransomware y el gap de ciberseguridad que debemos abordar para proteger nuestra instalación de superficie.

Una vez identificados los riesgos y gaps de ciberseguridad debemos fortalecer los ambientes operativos con el objetivo de:

1) Minimizar la probabilidad de ocurrencia.
2) Minimizar el impacto desde la perspectiva cibertisica.
3) Minimizar los tiempos de recuperación.
4) Contar con capacidades de detección temprana.
5) Contar con herramientas tecnológicas de contención y erradicación en los puntos adecuados.
6) Tener proceso de backup y restore eficiente y eficaces a ataques tipo ransomware.
7) Otros.

Una vez fortalecidos los ambientes operativos debemos desarrollar un plan de respuesta a incidentes, esto incluye la creación de un documento formal que describa los pasos a seguir al responder a un incidente de ciberseguridad, incluido un plan de comunicación, roles y responsabilidades y escalamientos. Este plan debe contener múltiples procedimientos que alcanzan a las distintas fases del proceso de respuesta ante incidentes ciber tisicos. Ellos son:

1) Procedimientos de identificación: el equipo de respuesta a incidentes identifica y confirma la ocurrencia de un incidente de ciberseguridad. Por lo general, esto implica monitorear y analizar el tráfico de red, los registros y otros indicadores de compromiso para detectar actividad maliciosa.
2) Procedimientos de contención: una vez que se confirma un incidente, el equipo de respuesta trabaja para contener el impacto y evitar más accesos no autorizados o daños a los sistemas y equipamiento tisico. Esto puede implicar aislar los sistemas y redes afectados, cerrar cuentas comprometidas, aislamiento de las instalaciones de superficie, entre otros.
3) Procedimientos de erradicación: el equipo de respuesta trabaja para eliminar la causa del incidente de ciberseguridad y eliminar cualquier acceso no autorizado o malware de los sistemas. Esto puede implicar parchear vulnerabilidades, restaurar desde copias de seguridad o eliminar código malicioso de los sistemas afectados. Este punto es muy importante debido a que tenemos una posible intervención de las terceras partes que nos dan soporte para recuperar los sistemas.
4) Procedimientos de recuperación: una vez contenido el incidente y erradicada la causa, la atención se centra en restaurar las operaciones y sistemas. Esto puede implicar restaurar sistemas a partir de copias de seguridad, reconfigurar la configuración de red e implementar medidas de seguridad adicionales para evitar incidentes futuros.
5) Procedimientos de lecciones aprendidas: deben incluir, al menos de manera general, los procesos para llevar a cabo una revisión posterior al incidente con el fin de identificar áreas de mejora en el plan de respuesta a incidentes, en los controles de seguridad y en la capacitación, utilizando la experiencia adquirida durante el incidente.

Finalmente, luego de armar todo el plan de respuesta ante incidentes, se debe realizar capacitaciones y simulacros: esto implica capacitar y probar periódicamente al equipo de respuesta a incidentes y al plan para garantizar la preparación y eficacia en caso de un incidente de ciberseguridad real.

Para concluir, las soluciones aquí planteadas han sido probadas e implementadas en una de las PTC mas importantes del país como así también en el ciclo combinado de generación eléctrica en base a gas mas grande del país.

Buscá todo sobre el shale en nuestra web

Shale en ARGENTINA

IAPG
INSTITUTO ARGENTINO DEL PETRÓLEO Y DEL GAS

LOS NO CONVENCIONALES | OPORTUNIDAD | QUIMICOS | SISMICIDAD | USO DEL AGUA

www.shaleenargentina.org.ar

El sitio del IAPG destinado especialmente a los hidrocarburos de reservorios no convencionales, como *shale gas* y *shale oil*.

Pensada como herramienta útil para toda la comunidad, especializada o no, que quiera conocer con mayor profundidad lo relativo a estos reservorios y al *fracking* o estimulación hidráulica, así como los aspectos que generan mayores cuestionamientos: el uso del agua, la protección de los acuíferos, el uso de químicos, etcétera.

Toda la información de los expertos y las últimas noticias.

¡Y además, la posibilidad de consultar interactivamente a un experto sobre cualquier aspecto relacionado con el shale en la Argentina!

/company/iapg /IAPGinfo /IAPG_Info /iapginfo