Ciberseguridad industrial

Ransomware en los ambientes del Oil & Gas, impacto real y estado de situación de la Argentina

Por ***Pablo Almada*** (KPGM)

Los ataques cibernéticos han llegado para quedarse y su complejidad alcanza a todas las industrias, entre ellas la del petróleo y gas.

En el último tiempo hemos escuchado casos resonantes acerca de los ciberataques al sector del Oil & Gas, por ejemplo el caso del *ransomware* de Colonial Pipeline que afectó la costa este de los Estados Unidos y provocó escasez de combustible generando un alza en los precios. Otro caso que podemos mencionar es el de *ransomware* PEMEX en 2018, que afectó al 5% de sus estaciones de trabajo o el caso de una importante empresa de energía de la Argentina que se vio afectada por este tipo de ciberataque.

Actualmente las empresas del sector, y específicamente los C-Level, están tomando conciencia de que la ciberseguridad es un riesgo adicional que se debe tener en cuenta en la gestión de las organizaciones. Los casos nombrados, demuestran como un ciberataque puede paralizar la producción, afectar la vida de los ciudadanos y,

posiblemente, materializar eventos que pongan en riesgo la vida del personal.

La masificación de este tipo de ataques conocidos como *ransomware*, que buscan por medio de un paro de producción extorsionar a una empresa para el pago de un rescate de sus operaciones, han crecido rápidamente por su efectividad, facilidad y redito económico.

La integración entre los ambientes de IT y OT brinda oportunidades interesantes para la eficiencia del negocio, pero como contrapartida, expone nuestras operaciones a riesgos para los cuales no fueron diseñadas. Esta situación se puede potenciar debido al uso de dispositivos de IIoT para el monitoreo y el uso de SCADA Cloud, entre otros. La integración entre redes IT/OT es una realidad, lo importante es hacerla de una forma cibersegura.

¿Qué pasaría si la red de operaciones se ve comprometida por un *ransomware*?

Los *ransomware*, en el 99,9% de los casos, afectan los servidores, las estaciones de operación, las estaciones de ingeniería y todo PC/servidor que posea un sistema operativo de "usuario". La afección se materializa a través del bloqueo de acceso a los equipos, es decir, los operadores no pueden operar ni visualizar el proceso industrial, los HMIS locales se bloquean, los historian pierden acceso a sus datos, se pierden las interfaces entre los sistemas corporativos e industriales y los backups, entre otros.

Asimismo, no se perdería el control de un campo o una Instalación de Superficie (IS), ya que están "controlados" por los PLC y no por los PC/servidores. Aquí surgen algunas preguntas que se podría hacer el operador/

responsable de un yacimiento o un operador/responsable de una IS:

- ¿Cuánto tiempo vamos a operar la planta a ciegas?
- ¿Qué riesgo corremos al no poder ver lo que está pasando en campo?
- ¿Podemos asegurar que todo fue pensando en nuestros Hazop?
- ¿Y nuestras matrices de seguridad?
- ¿Seguimos produciendo a ciegas o paramos todo?

En resumen, el impacto de un *ransomware* generaría pérdidas económicas, afectación de contratos (legales) y, según la importancia de la compañía en el mercado, desabastecimiento de hidrocarburo en el nivel nacional impactando a la población civil (Figura1).

¿Cómo podríamos estructurar los impuestos?

Figura 1. **Impactos físicos.**

Dejamos fuera del alcance de este documento el 0,01%, ya que solo han sido reproducidos en laboratorios y no existe evidencia de que hayan sido usados en un ciberataque. Este 0,01% de *ransomwares* afectarían los PLC. Debemos recordar que los PLC poseen un sistema operativo en tiempo real, donde nuestras lógicas de control corren en un sandbox.

¿Qué posibilidad existe de que ocurra un ciberataque de *ransonware* en un ambiente de operaciones?

Hemos escuchado en campo frases, como "Mis sistemas no se verían afectados por un *ransomware*" o "Nuestros sistemas están aislados" y podríamos escribir muchas otras similares, pero la realidad es que resulta extremadamente difícil que las operaciones no se vean afectadas por un *ransomware*.

Las redes de campo poseen múltiples puntos por donde podría infiltrarse un malware tipo *ransomware*. Por ejemplo, por las conexiones con nuestras empresas de servicios, los sistemas de control de los generadores de las IS, las cuadrillas que hacen los registros de pozos en las paradas de mantenimiento (Siemens/Rockwell/Yokogawa/etc.), entre otros. Además, tenemos nuestras propias conexiones con terceras partes, en los puntos LACT o con otras empresas operadoras que podríamos estar compartiendo datos por un tema contractual. Otro punto de entrada son las laptops que se utilizan en campo, que disponen de mínimas o nulas medidas de seguridad. A su vez, las redes corporativas presentan múltiples puntos para el intercambio de datos. Los SCADA Cloud, que hoy ya son una realidad, y como último ejemplo, la incorporación del uso de dispositivos conocidos como Internet Industrial de las Cosas (IIoT).

Cuando un *ransomware* tiene acceso a la red de control, busca equipos vulnerables que pueda usar como punto inicial de propagación. Los equipos de la red de control son extremadamente vulnerables a los *ransomware*, ya que las medidas de ciberseguridad son inexistentes, con lo cual tiene el campo libre para atacar, propagarse y esconderse para luego activarse. Asimismo, la actividad de propagación en una red de control es simple, porque su arquitectura tiende a ser plana y sin filtros por naturaleza.

La recuperación de una red de control es compleja, ya que debemos empezar a reconstruir los equipos con software de naturaleza vulnerable. En la mayoría de los casos, los aplicativos de control poseen múltiples restricciones tecnológicas que nos obligan a instalarlos en sistemas operativos obsoletos, sin soporte, o en el mejor de los casos, en sistemas operativos con soporte, pero sin actualizaciones y sin sistemas antimalwares. Luego, nos enfrentamos al problema de los backups, ¿están infectados?, ¿cómo podemos saber que no lo están?

Los ciberatacantes se han dado cuenta de que pueden generar un mayor impacto si una vez que logran infiltrarse en la red, se quedan ocultos unas semanas para luego ejecutar el ataque. De esta manera, lo que se busca es afectar los backups que hayan sido tomados durante la ventana que el *ransomware* estuvo oculto. Bajo este escenario, cuando se recuperan los sistemas de control a partir de los backups tomados en la ventana, los equipos "recuperados" funcionarían durante un período entre 15 y 20 días para luego volver a activar el ciberataque de forma automática.

Por último, entre los temas que se deben gestionar en un ciberataque, tenemos que pensar cómo vamos a recuperarnos de forma segura con el *ransomware* aún presente en la red. Para ello, debemos hacernos estas preguntas: ¿cómo levantamos los equipos sin que se reinfecten?, ¿tenemos diseñada la red de forma que los activos recuperados se puedan aislar en enclaves de cuarentena? o ¿nuestros equipos de red nos permiten armar redes aisladas de cuarentena o tenemos que salir a comprar equipos e instalarlos? Este último escenario, aunque parezca irreal, ha ocurrido durante procesos de recuperación.

¿Qué acciones están tomando las empresas del sector en la región?

Debido a la masificación de ciberataques durante los últimos años, las empresas de la región han empezado a tomar acciones de protección. Empresas maduras han activado e implementado medidas, sus IS y campos se encuentran monitoreados con herramientas de ciberseguridad, además poseen esquemas de actualizaciones, accesos remotos seguros, redes segmentadas y sistemas antimalware, entre otros. Es de destacar que este tipo de empresas poseen personal específico a cargo de la gestión de ciberseguridad en OT. En cambio, existe otro tipo de empresas que tienen presente que la ciberseguridad es un tema importante, pero apuestan a que no serán blancos de un ciberataque y no priorizan la toma de medidas o personal

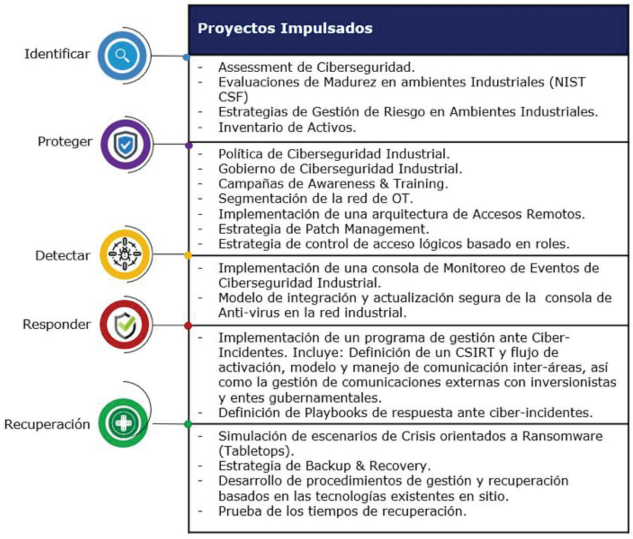

Figura 2. **Proyectos comunes.**

para contrarrestar un ataque. Este último escenario es lo mismo que decir "no pongamos válvulas de seguridad en las cabezas de pozo, ya que nunca tuvimos problemas de despresurización en las líneas de producción".

En la figura 2 se resumen los principales proyectos que actualmente ejecutan algunas compañías del sector.

Recomendaciones generales para el sector

Cada empresa tiene sus particularidades. Sin embargo, a continuación, se detallan algunas recomendaciones que no requieren ser ejecutadas de manera secuencial.

1 Contar con el apoyo del C-level para encarar un programa de ciberseguridad.
2 Contar con un equipo interdisciplinario que incluya referentes del equipo de operaciones.
3 Conocer el estado de la ciberseguridad en los ambientes de operaciones.
4 Tener un inventario de los activos de control y de las redes con atributos específicos de cyber.
5 Tener una política de ciberseguridad en ambientes industriales que haya sido creada en conjunto con los referentes de las distintas unidades de negocio de la compañía.
6 Contar con un plan de securización, alineado a la criticidad de los activos corporativos, que contenga mínimamente los siguientes puntos:
   - Estrategia antimalware.
   - Procesos de actualización de sistemas operativos.
   - Estrategia de segmentación de redes.
   - Monitoreo de redes OT.
   - Gestión de accesos lógico y accesos remotos.
   - Gestión de backups.

En conclusión, es necesario cambiar el *mindset* del personal acerca de la idea de que somos inmunes, tarde o temprano seremos blanco de un ciberataque, aun si contamos con las medidas de protección. Es clave trabajar para que cuando ocurra, el impacto sea el mínimo posible y tengamos la capacidad de recuperarnos de forma eficiente y efectiva.