Ciberseguridad, la gran lección que nos apura a aprender la pandemia

Por ***Diego Taich,*** *Managing, Director de Consultoría en Ciberseguridad & IT de PwC Argentina y* ***Ezequiel Mirazon****, socio de PwC Argentina, líder de la práctica de Energía, Minería y Utilities.*

El ciberdelito ha aumentado a ritmo sostenido en los últimos años y, a partir de la pandemia COVID-19, su incremento fue exponencial. Se prevé que esta tendencia se mantendrá igual en la pospandemia.

La industria de O&G se caracteriza por utilizar gran cantidad de activos físicos, hacer uso extensivo de mano de obra y contar con una infraestructura muy automatizada. Por ende, si ciertos ciber-riesgos se materializan, podrían derivar en situaciones preocupantes en la operación diaria e incluso en grandes pérdidas.

Muchas compañías de la industria están fuertemente identificadas con una nación y forman parte de las "infraestructuras críticas" de cada país, por lo tanto se encuentran eventualmente sujetas a amenazas originadas en "hacktivistas" (personas con una fuerte ideología respecto a temas ecológicos, políticos, sociales, etc., que realizan actividades de *hacking*), *cyberwar* (naciones que atacan a otras a través del ciberespacio) y ciberterrorismo.

Otro componente particular de la industria de O&G es la combinación de varias tecnologías que apoyan la operación (OT) como sistemas de control y automación e *Internet of Things* (IoT): uso de cámaras, sensores, geo localizadores, etc., con las tecnologías más tradicionales (IT) y las del consumidor (teléfonos móviles, tabletas, dispositivos *contact-less*, etc.). Todas terminan confluyendo en la organización y, por lo tanto, son potenciales escenarios de riesgo frente a los ciberataques. Sumado a ello, existen situaciones en las cuales, debido a la baja general del consumo que enfrenta la industria desde hace unos meses, las empresas han reducido sus costos y, en algunos casos, han despedido o licenciado a empleados, entre ellos a los que protegen los sistemas de control industrial que se utilizan para la operación del negocio.

Los analistas estiman que desde el comienzo de la pandemia se ha producido un incremento muy fuerte solamente en ataques de *phishing* (engaño realizado para obtener información o infectar un sistema con *malware*) o *spear-phishing* (*phishing* dirigido a un individuo o grupo de individuos en particular) en la industria. Asimismo, los ataques de *ramsomware* (secuestro de datos, que usualmente son liberados a cambio del pago de una recompensa) aumentaron 9 veces desde febrero de 2020 a la fecha. Por

otra parte, el *spoofing*, suplantación y/o el robo de identidad (vía whatsapp, mail, etc.) también han crecido y suele producir un daño muy relevante para las organizaciones, que derivan en fraudes, pérdidas financieras, etc., y para las personas (daño en la imagen, económicos, etc.).

El incremento del ciberdelito se encuentra apalancado en diversos factores por: (a) trabajo remoto masivo, con la utilización –en muchos casos– de herramientas informáticas inseguras para comunicarse y/o transferir información; (b) intensificación del uso del ciberespacio mediante canales de *e-commerce*, medios de pago y/o billeteras digitales; (c) fuerte aumento del *phishing*; y (d) cambios en la fuerza laboral (rotación de personal, despidos, etc.) y en la cadena de abastecimiento (bajas de proveedores y también aparición de nuevos) que, si no son acompañados por adecuados procedimientos de actualización de los permisos de accesos a los activos de la información, pueden generar una brecha de seguridad.

Si bien es cierto que las empresas de O&G en la Argentina no han sufrido el mismo nivel de ataques de ciberterrorismo y/o "cyberwar" que empresas similares en otras regiones, también se encuentran sujetas a las mismas amenazas que otras compañías de parte de grupos organizados y hackers que lanzan ataques de *phishing*, *malware* y *ramsomware* (secuestro de datos que usualmente son liberados a cambio del pago de una recompensa) esperando fugar información y obtener dinero.

Para aquellas compañías reguladas se debería considerar también que una brecha de seguridad puede resultar en severas sanciones para la organización y sus directivos. La SEC ha identificado las amenazas a la ciberseguridad como un riesgo relevante y, por lo tanto, las empresas que son reguladas por dicho organismo deben contemplarlas como prioritarias a la hora de planificar y hacer inversiones. En varios países que cuentan con leyes estrictas de protección de los datos de las personas físicas, si lo que se vieran expuestos fueran datos de tipo personal de los empleados, proveedores u otros almacenados, la empresa y eventualmente algunos de sus funcionarios podrían también ser pasibles de recibir serias sanciones.

En este contexto, las empresas de la industria deberían considerar los siguientes aspectos:

- El modelo de defensa perimetral (tomado de los utilizados durante la época medieval para proteger los castillos), en el cual se utilizan medidas para asegurar "las 4 paredes" de la organización, ya no provee una cobertura integral, ya que los empleados y contratistas están operando en gran parte desde afuera de las oficinas. Por lo tanto, no es suficiente poseer solo el *firewall* que protegía esas cuatro paredes. Contemplando esta situación, los modelos de seguridad están cambiando a un esquema de "cero confianza", que se basa fundamentalmente en realizar inspecciones detalladas de los intentos de acceso a los datos de la organización (versus protección del perímetro).

Personas:

- Proteger y reforzar la función de ciberseguridad en las empresas. En particular para la industria de O&G, salvaguardar las funciones que resguardan los sistemas de control y automación.
- Entrenar a los empleados y contratistas sobre los posibles ciberataques y cómo deberían reaccionar.

Procesos:

- Fortalecer y expandir el monitoreo de incidentes pensando en un esquema activo 7x24.
- Actualizar los Planes de Continuidad del Negocio. Los procedimientos de gestión de crisis y respuesta a incidentes se deben poder ejecutar por una fuerza de trabajo remota.
- Foco en la seguridad de las terceras partes.

Tecnología:

- Acelerar el *patching* de sistemas críticos.
- Soportar y asegurar las herramientas para el trabajo remoto.
- Aplicar autenticación robusta.
- Acelerar la virtualización de dispositivos.
- En particular para la industria de O&G, establecer y mantener una adecuada segmentación entre las redes de IT, OT e IOT, haciendo un escrutinio detallado del tráfico que fluye entre dichas redes y los pedidos de accesos a datos y dispositivos.

Las empresas enmarcadas en la industria de O&G deberían revisar sus estrategias de ciberseguridad para poder proteger adecuadamente sus activos críticos en la nueva normalidad, con el objetivo de ser más resilientes y evitar o minimizar pérdidas económicas, impactos en la operación y daños en la imagen y reputación.