Ataques Cibernéticos en el Sector de Energía

La red interna de una empresa del sector energético generalmente se divide en dos áreas: Tecnología de la Información (TI): datos, información, así como aplicaciones comerciales y de escritorio; y Tecnología Operacional (TO) - equipos y procesos físicos. Estos están conectados a través de Sistemas de Control Industrial (SCI).

Históricamente, las redes TO estaban divididas porque TI y TO eran vistas como disciplinas separadas.

Esto se debe por diversas razones (mayor eficiencia, supervisión remota, asistencia de proveedores), las redes TO de energía ahora están cada vez más conectadas a las redes de TI y al mundo exterior. Los sistemas de control industrial (SCI) ofrecen mayor eficiencia y fiabilidad. La conexión entre estos sistemas tradicionalmente "aislados" brinda a los operadores un control y supervisión en tiempo real de las operaciones. Si bien estas mejoras en la conectividad del sistema han hecho avanzar drásticamente al sector energético, dicha conectividad también tiene sus inconvenientes, agregando una exposición cibernética significativa al sistema.

Las redes TO suelen estar formadas por sistemas "heredados", los cuales suelen ser obsoletos, sin parches y mucho más vulnerables. Esto se debe a la preocupación por el tiempo de inactividad operativa, costos y riesgos involucrados con la aplicación de parches a sistemas antiguos. Además, muchas redes TO carecen incluso de precauciones simples, como software antivirus, firewalls e inicios de sesión seguros.

La conexión de redes entre sí expone este déficit de seguridad. Los puntos débiles de TO son mucho más vulnerables a la amenaza de seguridad por el mal uso o falla en los sistemas. Delincuentes cibernéticos, por lo general, obtienen acceso a través del entorno de TI, explotando estas conexiones no seguras para extenderse a la red TO, lo que afecta tanto a las operaciones de negocio como a las de producción.

¿Estamos realmente en riesgo?

Interrupciones y daños físicos

Las empresas de energía extraen y transportan recursos valiosos, utilizando tecnología avanzada. Las advertencias de los gobiernos sobre ataques contra el sector de electricidad, petróleo, gas y otras infraestructuras similares siguen aumentando. Es alarmante que el sector energético también es un objetivo principal para los ataques cibernéticos por parte de estados, terroristas y otros que buscan ganancias financieras, políticas o económicas.

Cuanto mayor sea el impulso de innovar los sistemas para satisfacer la demanda de velocidad, eficiencia, control y practicidad, la vulnerabilidad del sistema incrementará para los atacantes cibernéticos.

Una violación a un sistema de control industrial crítico podría causar un impacto importante para un proveedor de energía. La pérdida de control de los equipos de generación de energía o una válvula de oleoducto debido a un ataque cibernético podría causar cortes significativos de suministro, daños físicos a la planta, un incidente ambiental o incluso explosiones. La pérdida potencial en los ingresos puede ser devastadora.

Transmisión de malware

Es común que un malware infiltrado en el sistema de la red se transmita a terceros, a través de un punto vulnerable en una red informática, creando así responsabilidades, reclamaciones y pérdidas financieras adicionales; ocasionando que las redes de los clientes y contactos de la cadena de suministro de una empresa esté en riesgo.

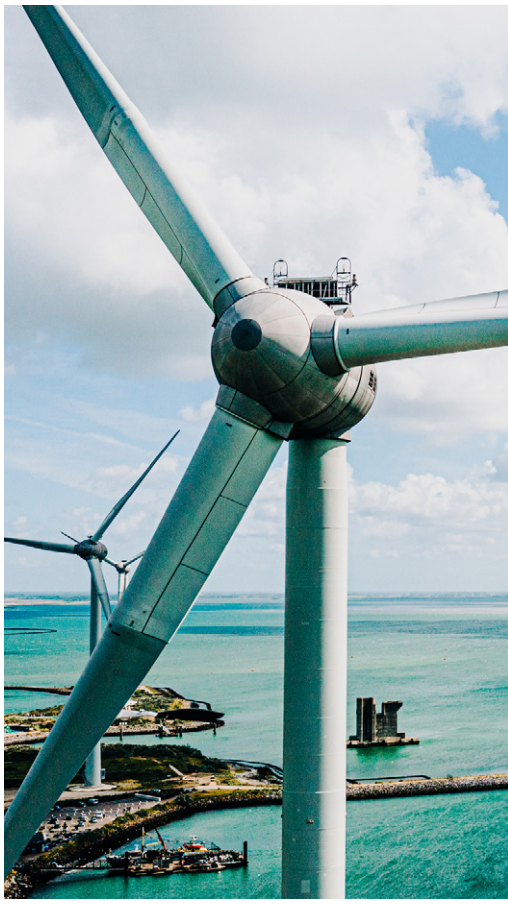
Exposición de información confidencial

Fuera de los desafíos cibernéticos específicos a los que enfrenta el sector de energía, existen riesgos adicionales que se observan en todas las organizaciones.

El alto valor de los datos dentro del sector energético aunado a la inversión relativamente baja en la gestión de activos digitales (en comparación con el sector de la salud) deja la información confidencial altamente sensible y valiosa más expuesta. Los sistemas de recursos humanos, nómina, pagos, sistemas financieros y corporativos vienen con sus propias vulnerabilidades. De hecho, la mayoría de los ataques cibernéticos siguen teniendo una motivación económica, vinculados al aumento de ataques por ransomware y los ataques relacionados con el robo de propiedad intelectual.

La exposición de información confidencial podría dar lugar a los siguientes costos directos y daños a terceros:

- Daños a terceros asociados con la divulgación inadvertida de secretos comerciales.
- Gastos de defensa asociados a reclamaciones por parte de terceros.
- Reclamaciones de clientes y otras personas por el costo de reconstruir los sistemas afectados.
- Investigación forense de la violación.
- Asesoramiento legal y costos de relaciones públicas.
- Requisitos regulatorios. Si bien las multas solo estarán cubiertas por una póliza de seguro si son asegurables por ley, los costos de responder a una solicitud regulatoria de información generalmente están cubiertos por una póliza de seguro de Cyber.



Casos de estudio

Estudios muestran que los delincuentes cibernéticos están apuntando al sector energético. Los atacantes, a través de SCI comprometidos, están obteniendo cada vez más acceso a refinerías de petróleo, redes eléctricas y presas hidroeléctricas. Los ejemplos recientes de pérdidas demuestran cómo los ataques cibernéticos están causando cada vez más interrupciones del negocio más allá de las redes de TI.

Conexión TI/TO

En enero de 2020, un empleado de una instalación de gas natural descargó inadvertidamente un malware a una computadora haciendo click en un enlace en un correo electrónico de phishing, el individuo recibió un mensaje fraudulento con características que hacían creer que era un mensaje proveniente de una fuente de confianza.

Esto le dio al atacante acceso a la red de TI de la instalación. Debido a que la compañía carecía de una segmentación adecuada entre sus redes de TI y TO, esto permitió que el ataque por ransomware se propagara: el atacante pudo infiltrarse en la red e impactar los activos en ambos entornos.

Aunque el impacto operacional se limitó a una instalación, se requirió el cierre de toda la tubería en instalaciones físicamente separadas debido a las dependencias de transmisión de la tubería.

Amenaza de los datos

Una empresa energética portuguesa (EDP) sufrió un ataque de ransomware en abril de 2020. El grupo de atacantes cibernéticos conocido como Ragnarok golpeó a la empresa de servicios públicos con sede en Lisboa y su unidad de energía eólica, robando hasta 10TB de datos con la amenaza de filtrar los datos robados si no se pagaba el rescate de $10.9 millones.

La empresa, que suministra energía a más de 11 millones de clientes con presencia en 19 países, tenía 20 días para pagar a los delincuentes cibernéticos para asegurarse de que los datos no se publicaran o se eliminaran.

En julio de 2020, EDP Renewables North America confirmó que el ataque había afectado a su empresa matriz y que "los atacantes habían obtenido acceso no autorizado a al menos cierta información almacenada en los propios sistemas de información de la compañía".

La compañía ofreció a los clientes un año de protección de identidad sin costo alguno. La vicepresidenta y gerente general de la firma de seguridad cibernética industrial Tripwire, Kristen Poulos, comentó sobre el ataque que parecía haber sido contenido para comprometer la información confidencial. Poulos declaró: "aunque eso es un desafío importante en sí mismo, si tales ataques penetraran en el espacio TO (debido a la segmentación inadecuada entre TI y TO), podrían infectar sistemas críticos para la producción de energía como al interfaz hombre-máquina y estaciones de trabajo de ingeniería. Afortunadamente, este no parecía ser el caso.

Seguro de Cyber

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su organización. Es vital salvaguardar los sistemas de una empresa para permitirle proteger sus actividades, clientes, reputación e ingresos. Es fundamental reconocer las vulnerabilidades particulares en todo el sector energético.

Un ataque cibernético puede tener ramificaciones de gran alcance. Comprender estos riesgos y mitigarlos de manera proactiva es clave.

A menudo, las empresas son susceptibles a los ataques. Al comprender los riesgos que conlleva la conectividad digital, las empresas pueden implementar controles para reducir la probabilidad de un ataque cibernético y, si tiene éxito, identificar y gestionar el ataque de manera oportuna y eficiente.

Una técnica importante de mitigación de riesgos es la transferencia del riesgo al seguro. Contrariamente a la creencia popular, las pólizas tradicionales no siempre están diseñadas para responder a un incidente cibernético. De hecho, en los últimos años, las aseguradoras han tomado medidas específicamente para excluir la cobertura relacionada con un ataque cibernético de sus pólizas. Contar con una cobertura afirmativa de Cyber es vital.

Una parte fundamental de una póliza de protección de datos independiente son los servicios de respuesta a incidentes, hacer frente a pérdidas propias, asesoramiento forense y legal de TI, así como consultores de relaciones públicas y gestión de crisis para mitigar el daño a la reputación de la empresa.

En Lockton, nos especializamos en programas de seguros amplios y complejos para compañías del sector de energía. Nuestro programa de seguros se adapta a las necesidades de la organización lo que garantiza una cobertura adecuada para todas las líneas de negocio. Esta experiencia en el sector energético nos da una excelente exposición a los hábitos de compra cibernética.

Las empresas del sector energético dependen de una serie de sistemas tecnológicos para mantener sus negocios en funcionamiento.

Nuestro equipo de expertos en riesgos cibernéticos trabajará con usted para crear una solución personalizada que proteja y asegure su negocio exactamente donde lo necesite, garantizando que los riesgos cibernéticos se integren en su proceso de gestión de riesgos para que los sistemas tecnológicos recuperen la máxima eficiencia lo antes posible. Recuperar la confianza es vital.

Para mayor información:

Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com

Moisés García
ProFin México
moises.garciab@lockton.com