“Todas las áreas de la industria de O&G **podrían estar sujetas a un ataque cibernético”**

Para el Director de Seguridad de la empresa experta en telecomunicaciones, tanto el *upstream* como el *downstream* pueden estar en la mira de las infiltraciones.

Entrevista a ***Juan Marino***, director de Ciberseguridad de Cisco.

¿Qué es la ciberseguridad y por qué está creciendo en importancia en la industria del petróleo y del gas?

La ciberseguridad permite controlar el riesgo al que se expone la información digital, asegurando confidencialidad, integridad y disponibilidad. En la industria de O & G está adquiriendo mayor relevancia dada la creciente integración del mundo de tecnología de la información (IT) con el mundo de la Tecnología Operacional (OT), lo cual supone una expansión de la "superficie de ataque" por medios cibernéticos, que antes se encontraba limitada al mundo de IT.

En efecto, hasta ahora se realizaban ataques a la IT y las comunicaciones. ¿Desde cuándo y cómo cree que comenzaron a involucrar a la OT?

La integración de IT con OT es una tendencia creciente dadas las posibilidades de automatizar procesos, hacer controles remotos, etc., lo cual supone ganancias en productividad y agilidad. Esto abre las puertas para que los cibercriminales puedan también sacar provecho con acciones maliciosas, intentando penetrar y tomar control de redes OT sin necesidad de acceder físicamente a las mismas. Los ataques sobre OT tienen precedentes desde el ataque a redes críticas de energía con un *malware* conocido como Stuxnet que data de varios años atrás y, a partir de allí, las amenazas sobre redes críticas han crecido y claramente se están convirtiendo en uno de los problemas más serios, no solo en la industria del petróleo y del gas, sino también en cualquier industria en la que se controlan procesos críticos a través de una red de operaciones.

En el nivel geográfico, Ucrania es uno de los países que más está sufriendo ataques vinculados a la disrupción de sistemas críticos y esto crea los precedentes para actividades que luego se esparcen en otras geografías. Más reciente ha sido el ataque conocido como *Blackenergy* y la última amenaza de la que tomamos conocimiento, justamente a través de una investigación que hizo el centro de inteligencia de amenazas Cisco Talos, se denomina VPNFilter, el cual afecta al menos a 500.000 *routers* hogareños que podrían ser utilizados en cualquier momento como infraestructura para generar ataques maliciosos con objetivos críticos.

¿Qué áreas de la industria de hidrocarburos involucra principalmente? ¿Cómo pueden los piratas informáticos entrar en la red de OT? ¿Hay ejemplos extremos del daño que los hackers pueden hacer en las empresas de O & G en el mundo (parada de la planta, daños al equipo, interrupciones de servicios públicos, cierre del círculo de producción, etc.)?

Todas las áreas de la industria de O & G podrían estar sujetas a un ataque cibernético. Si pensamos en la red OT sería factible considerar los siguientes escenarios:

- Infiltración en la operación del *upstream* para exfiltrar información crítica del negocio tal como la telemetría de la producción de los pozos petroleros.
- Disrupción en la operación del *upstream* tomando control de la red industrial. Esto puede generar la interrupción de la producción o incluso provocar daños físicos sobre la planta. El caso Stuxnet es un ejemplo de *malware* con consecuencias físicas en la planta industrial
- En el negocio del *downstream* los riesgos pueden significar la interrupción del abastecimiento, la disrupción en el sistema de pagos o la exfiltración de datos de clientes y tarjetas de crédito.
- En el ámbito de IT, las empresas de la industria de O & G están sujetas, como cualquier otra compañía a la pérdida de información crítica del negocio y ataques a la disponibilidad de recursos informáticos.

¿Las víctimas de estos ataques son solo grandes corporaciones o también han llegado a compañías medianas y pequeñas de O & G?

Actualmente las amenazas no están limitadas a grandes corporaciones, dada la escala y automatización del cibercrímen en el nivel global, que no distingue geografías. Podemos suponer que las grandes corporaciones son objetivos más atractivos por el valor de la información que resguardan, pero por otra parte, las organizaciones menores no suelen contar con el mismo nivel de madurez en procesos y tecnologías de ciberseguridad, lo cual las hace más vulnerables a ataques cibernéticos.

Resumen ejecutivo Reporte Anual de Ciberseguridad Cisco 2018

¿Qué pasaría si los defensores pudieran ver el futuro? Si supieran que se aproxima un ataque, podrían detenerlo o al menos mitigar su impacto y garantizar lo que necesitan para proteger a la mayoría y asegurarlos. El hecho es que los defensores pueden ver lo que está en el horizonte. Muchas pistas están ahí fuera y son obvias.

Los atacantes ya tienen la experiencia y las herramientas necesarias para derribar las infraestructuras y los sistemas críticos, paralizando así regiones enteras. Pero cuando surgen noticias sobre ciberataques disruptivos y destructivos –como los de Ucrania, por ejemplo, o los que ocurren en cualquier otro lugar del mundo–, algunos profesionales de la seguridad podrían pensar inicialmente: "El entorno de mercado/región/tecnología de nuestra compañía no era un objetivo, entonces, probablemente no estemos en riesgo".

Sin embargo, al quitarle valor a lo que parecen ser ataques lejanos, o permitir que el caos de las batallas diarias con atacantes consuma su atención, los defensores fallan al no reconocer la velocidad y la escala a la que los adversarios están reuniendo y mejorando su armamento cibernético.

Durante años, Cisco ha estado advirtiéndoles a los defensores sobre la creciente actividad de ciberdelincuencia en todo el mundo. En nuestro reciente informe anual de ciberseguridad presentamos datos y análisis de los investigadores de amenazas de Cisco y de varios de nuestros socios tecnológicos, sobre el comportamiento observado de los atacantes durante los últimos 12 a 18 meses. Muchos de los temas examinados en este informe están centrados en tres temas generales:

1. Los adversarios están llevando el malware a niveles de sofisticación e impacto sin precedentes. La evolución del malware fue uno de los desarrollos más importantes en el panorama de los ataques en 2017. La llegada de "cryptoworms" ransomware basado en la red elimina la necesidad del elemento humano en el lanzamiento de campaña de ransomware. Y para algunos adversarios, el premio no es un rescate, sino la eliminación de sistemas y datos, como lo demostró Nyetya (eliminador limpiador de malware disfrazado de ransomware). El malware de autopropagación es peligroso y tiene el potencial de acabar con Internet, según los investigadores de amenazas de Cisco.
2. Los adversarios son cada vez más expertos en la evasión y en usar como armas los servicios de la nube y otras tecnologías utilizadas con fines legítimos. Además de desarrollar amenazas que pueden evadir los entornos de sandboxing más sofisticados, los actores maliciosos están ampliando su adopción del cifrado para evitar la detección. La encriptación está destinada a mejorar la seguridad, pero también les proporciona a los actores maliciosos una poderosa herramienta para ocultar la actividad de comando y control (C2), lo que les brinda más tiempo para operar e infligir daños. Los ciberdelincuentes también están adoptando canales C2 que dependen de servicios legítimos de Internet como Google, Dropbox y GitHub. La práctica hace que el tráfico de malware sea casi imposible de identificar.

Además, muchos atacantes están lanzado múltiples campañas desde un único dominio para obtener el mejor rendimiento de sus inversiones. También están reutilizando los recursos de la infraestructura, como las direcciones de correo electrónico de los subscriptores, los números de sistema autónomo (ASN) y los servidores de nombres.

3. Los adversarios están explotando grietas en la seguridad, muchas de las cuales surgen de la expansión del Internet de las Cosas (IoT) y del uso de los servicios de la nube. Los defensores están desplegando dispositivos de IoT a un paso rápido, pero a menudo le prestan poca atención a

¿Quiénes crees que son estos atacantes?, ¿cuáles son sus propósitos?

Actualmente resulta muy difícil individualizar a los atacantes y saber desde dónde operan, dada la sofisticación en la ejecución de los ataques y la capacidad de actuar bajo radar y de forma anónima, tomando provecho de infraestructura TOR y la *deep & dark web*. Lo que sí resulta más claro es que existen varios propósitos asociados a las distintas campañas de ataque. No siempre se logra precisar el motivo exacto de un ataque determinado pero en general predominan los siguientes:

- **Motivación económica**: gran parte de los ataques están motivados por lucro a través de la venta de la información exfiltrada, o de pagos extorsivos relacionados con la recuperación de la información robada o "secuestrada".
- **Competencia desleal**: en algunos casos los actores maliciosos lucran al brindar un servicio de ataque motivado por competencia desleal.
- ***Hacktivismo***: acciones maliciosas para afectar la operación de un organismo por convicción política, social, religiosa, etc.
- **Ataques a nivel del Gobierno**: en algunos casos se especula que existen ataques vinculados con accionar deliberado a nivel de Estado como una estrategia para afectar infraestructura crítica de otros gobiernos.

Los sistemas de control tipo SCADA son utilizados por todas las compañías de petróleo y gas. ¿Qué estrategia recomienda para protegerlos contra los ataques?

Las redes SCADA y los dispositivos vinculados a la misma, como cualquier otro sistema, presentan vulnerabilidades que hay que reconocer y en función de ello, establecer una estrategia de procesos y tecnologías para minimizar el riesgo cibernético.

En la medida en que estas redes industriales se conectan con la red IT, resulta fundamental establecer una arquitectura de seguridad que permita implementar controles en distintas capas, asegurar el control de acceso y los flujos de tráfico permitidos entre cada dispositivo dentro y fuera del ámbito de la red industrial. En este sentido, Cisco propone

la seguridad de estos sistemas. Los dispositivos IoT sin parche y no monitoreados les brindan a los atacantes la oportunidad de infiltrarse en las redes. Una investigación sugiere que las organizaciones con dispositivos IoT susceptibles a ataques también parecen desmotivadas para acelerar las correcciones. Peor aún, estas organizaciones probablemente tengan muchos más dispositivos IoT vulnerables en sus entornos de TI que ni siquiera conocen.

Mientras tanto, las botnets del IoT se están expandiendo junto con el IoT y se están volviendo más maduras y automáticas. A medida que crecen, los atacantes las usan para lanzar avanzados ataques distribuidos de la negación del servicio (DDoS).

Los atacantes también aprovechan el hecho de que los equipos de seguridad están experimentando dificultades para defender los entornos de IoT y de la nube. La razón es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos.

Recomendaciones para los defensores

Cuando inevitablemente los adversarios golpean sus organizaciones, ¿estarán preparados los defensores y qué tan rápido podrían recuperarse de estos ataques? Las conclusiones del Estudio Comparativo de Capacidades de Seguridad de Cisco 2018 –el cual ofrece información sobre las prácticas de seguridad de más de 3.600 encuestados a lo largo de 26 países– muestran que los defensores tienen muchos desafíos que ganar.

Aun así, los defensores se darán cuenta que realizar mejoras de seguridad estratégicas y adherirse a las mejores prácticas y más comunes, puede reducir la exposición a riesgos emergentes, detener el progreso de los atacantes y proporcionar más visibilidad dentro del panorama de las amenazas.

Ellos deben considerar:

- Implementar herramientas en la primera línea de defensa que puedan escalar, como las plataformas de seguridad de la nube.
- Confirmar que se adhieren a las políticas y a las prácticas corporativas para el parcheo de aplicaciones, sistemas y dispositivos.
- Emplear la segmentación de la red para ayudar a reducir las exposiciones a los brotes.
- Adoptar herramientas de monitoreo de procesos Endpoint de próxima generación.
- Acceder a datos y procesos de inteligencia de amenazas de una manera más precisa y oportuna, que permitan que esos datos sean incorporados a la supervisión y al evento de seguridad.
- Realizar análisis más profundos y más avanzados.
- Revisar y practicar los procedimientos de respuesta de seguridad.
- Realizar a menudo una copia de seguridad de datos y hacer pruebas de procedimientos de restauración –procesos que son críticos en un mundo de cyptoworm ransomware de movimiento rápido basados en la red– y de armas cibernéticas destructivas.
- Revisión de pruebas de eficacia de terceros respecto de tecnologías de seguridad para ayudar a reducir el riesgo de ataques a la cadena de suministro.
- Llevar a cabo un análisis de seguridad del microservicio, del servicio en la nube y de los sistemas de administración de aplicaciones.
- Revisar los sistemas de seguridad y explorar el uso del análisis del SSL y, en caso de ser posible, el descifrado SSL tan pronto como sea posible.

Los defensores también deberían considerar la adopción de tecnologías de seguridad avanzadas que incluyan el aprendizaje automático y las capacidades de la inteligencia artificial. Con un malware ocultando su comunicación dentro del tráfico web encriptado y personas malintencionadas enviando datos confidenciales a través de sistemas corporativos en la nube, los equipos de seguridad necesitan herramientas más efectivas para prevenir o detectar el uso del cifrado para ocultar actividades maliciosas.

Sobre el reporte

El Reporte Anual de Ciberseguridad de Cisco 2018 presenta los últimos avances en la industria de seguridad diseñados para ayudar a las organizaciones y a los usuarios a defenderse contra los ataques. También se observan las técnicas y estrategias que utilizan los adversarios para romper esas defensas y evadir la detección.

En el informe se destaca, asimismo, las principales conclusiones del Estudio Comparativo de Capacidades de Seguridad de Cisco 2018, que examina la postura de seguridad de las empresas y sus percepciones acerca de su preparación para defenderse de los ataques.

Puede descargarse gratuitamente aquí: *https://www.cisco.com/c/es_ar/products/security/security-reports.html#~download-the-report*

servicios de consultoría y soluciones para poder crear la estrategia de ciberseguridad adecuada y establecer los procesos y tecnologías necesarios para un control eficaz.

En términos de tecnologías, las siguientes son algunas de las más importantes:

- **Control de acceso a la red basado en identidad**: utilizando la red como *enforcer* con *Identity Services Engine*.
- **Análisis de comportamiento de la red basado en flujos**: utilizando la red como sensor para detectar los flujos normales y anormales dentro de la red IT y OT.
- **Sistemas de prevención de intrusiones**: analizando tráfico IP y protocolos de red industrial para detectar y prevenir la explotación de vulnerabilidades.
- **Sistemas de Firewall**: para la segregación de las capas de red IT y OT, de acuerdo con modelo Purdue, estableciendo zonas de distintos niveles de seguridad y definiendo tráfico, puertos y aplicaciones permitidas entre cada zona.

Los *boardings* de las empresas ¿tienen conciencia la dimensión de este riesgo?, ¿cuáles son sus consejos para las empresas de hidrocarburos que aún no han entendido la gravedad de esta amenaza?

Entiendo que hay una falsa percepción de que la red industrial es segura o que está exenta de ataques cibernéticos. Es importante crear conciencia sobre las amenazas reales que existen en la medida que se comienza a conectar el mundo IT con OT. Por otra parte, para que se pueda establecer y ejecutar una estrategia de ciberseguridad que atraviese todas las áreas de la organización resulta importante muchas veces realizar cambios de estructura organizacional promoviendo una mayor integración entre áreas y una mejor gobernanza en materia de ciberseguridad.

Referencias

Informe Anual de Ciberseguridad 2018, Cisco: *https://www.cisco.com/c/es_ar/products/security/security-reports.html#~download-the-report*