La ciberseguridad en el sector de la energía en el próximo invierno

Agustín Valencia

Colaborador y docente del Centro de Ciberseguridad Industrial (CCI)

Nunca antes desde la crisis del petróleo de 1973 se había afrontado un invierno con tanta preocupación a nivel mundial como el que nos espera en el de 2022-2023.

En Europa la tensión energética es máxima, como bien se indica a diario en los noticiarios. Todo el aporte de gas desde Rusia por el gasoducto Nordstream 1 se ha bloqueado, Francia ha necesitado parar buena parte de su parque de generación nuclear para inspeccionar posibles fallos de corrosión en sistemas críticos, continúan las tensiones con Argelia para enviar gas a España y la capacidad estadounidense está reducida debido a un accidente que se explicará más adelante.

Por otro lado, las fuentes renovables no han aportado tanto como se pudiera necesitar debido a la climatología y a que concentraciones puntuales de energía no siempre pueden ser evacuadas por las redes de transporte. Y esto conlleva a paradojas que se ven en las redes sociales, como ver molinos obligados a parar en condiciones de viento.

Cuando se habla de grandes accidentes siempre se habla de la teoría del iceberg, de modo que se analizan cuántas causas han ido contribuyendo de manera poco visible y que, todas juntas, han propiciado que un solo fallo más desencadenara consecuencias fatales.

Reacción en cadena

Pero ¿podría ser la ciberseguridad hacia alguno de los vectores energéticos –todos tan tensionados actualmente– la espoleta para la reacción en cadena? Sin duda, motivos hay, y aquí vamos a explicar algunos.

A nivel de amenazas, fue en los primeros meses de 2022 cuando se publicaron dos nuevas; ambas muy enfocadas contra sistemas industriales. La primera, denominada Pipedream por Dragos, describía una amenaza muy evolucionada que aglutinaba las capacidades de los ataques que han conformado la disciplina de la ciberseguridad industrial y cómo defenderse. Nos referimos a Stuxnet y a Triton, junto con capacidades de dispersión por medio de comunicaciones industriales como Modbus e incluso encriptadas como OPC-UA. Stuxnet fue pública en 2010 a raíz de los ataques a controladores Siemens en la fábrica de combustible nuclear de Natanz (Irán), así como a la modificación de láminas de SCADA y el riesgo asociado a los *pendrive* USB. Y Triton, pública en 2017, es importante por ser la primera enfocada en anular un sistema de seguridad instrumentado y en buscar daños contra instalaciones y personas y por ser capaz de anular protecciones y conseguir persistencia modificando librerías de SCADA y controladores.

> La cadena de suministro es un problema que necesita abordarse en varias dimensiones

Además, por las vulnerabilidades que explotan, los objetivos se enmarcan principalmente en los entornos de electricidad y *Oil & Gas*. Es más, la gravedad del descubrimiento hizo a la CISA estadounidense emitir una alerta en abril (AA22-103A) para que se diera prioridad a las mitigaciones recomendadas por parte del sector.

La segunda amenaza, denominada Industroyer 2, no es realmente nueva. Se trata de la evolución de Industroyer, pública en 2017 por Eset a raíz de los ataques realizados por Rusia en las infraestructuras ucranianas en las navidades de 2015 y 2016. El ataque original perseguía destruir las subestaciones de la infraestructura eléctrica aprovechando una vulnerabilidad de protecciones. Pero originalmente no se le dio gran importancia porque se infravaloraba la capacidad de los atacantes para acceder a estos sistemas mediante los protocolos de comunicaciones específicos del entorno eléctrico. Sin embargo, al ser analizado, se vio que se había diseñado para propagarse mediante más de tres protocolos específicos.

Industroyer 2 va un paso más allá. Busca la persistencia en las estaciones de operación e ingeniería de los centros de control de las empresas operadoras, al igual de Triton, pero con una especificidad adicional: se había diseñado para atacar SCADA funcionando sobre sistemas operativos Solaris, poco comunes en general pero muy específicos de algunas herramientas.

Ataques

En febrero se supo que varias terminales portuarias de aprovisionamiento de hidrocarburos de Alemania, Bélgica y Holanda se vieron afectadas por un ataque de *ransomware*. En concreto, las empresas Both Oiltanking Deutschland y Mabanaft Deutschland llegaron a declarar fuerza mayor por no poder cumplir sus compromisos de abastecimiento debido al impacto del ataque en sus infraestructuras. Incluso empresas como Shell tuvieron que modificar sus rutas para poder descargar sus barcos cisterna en otras terminales.

Análogamente, y solo basándonos en información pública, la CISA estadounidense ha difundido varios avisos para incrementar el nivel de alerta de los sistemas eléctricos del país en vista del aumento de actividad. El más sonado fue al poco de iniciarse la invasión de Ucrania por Rusia. La alerta (AA22-083A) describía técnicas, tácticas y procedimientos identificados en ataques para que las empresas de energía pudieran alimentar sus sistemas de detección y de monitorización para ayudar a incrementar la eficacia de sus centros de operaciones de seguridad. Parte de la información hacía referencia a los ataques mencionados anteriormente.

Además, en febrero se avisó de un incremento de ataques de *ransomware* por medio de *pendrives* USB y en septiembre se emitió un aviso de que una vulnerabilidad de Windows (CVE-2010-2568) explotada por Stuxnet volvía a situarse entre las más explotadas. Pensemos que esta última es propia de equipos Windows XP y Windows 7, así como de Windows Server 2003 y 2008.

Dentro de las sospechas de ataques y relacionado con las vulnerabilidades no mitigadas, debemos señalar el accidente de junio en Estados Unidos. En concreto, la planta de Freeport sufrió una explosión en una de sus líneas de licuefacción de gas, y que suponía el 20 por ciento de toda la capacidad de producción de gas natural licuado del país y que se estaba destinando a Europa. Todavía se investiga si pudo haber alguna relación con causas de ciberseguridad. De hecho, la empresa SecurityScorecard reveló tras el accidente que la planta presentaba varias vulnerabilidades explotables desde el exterior, sugiriendo la posibilidad de haber podido lanzarse un ataque como el de Triton, pero sin confirmar si efectivamente habían sido explotadas.

¿Qué se está haciendo?

Obviamente, las empresas energéticas no son ajenas a todas estas situaciones. Afrontan grandes retos tanto para mitigar vulnerabilidades de equipos obsoletos, pero que no pueden ser reemplazados fácilmente ni en plazos cortos, como para poder mejorar los mecanismos de coordinación de respuesta ante incidentes o de las amenazas implícitas en las cadenas de suministro que conforman ecosistemas tan complejos.

En relación con la cadena de suministro, hay también una gran preocupación porque es un problema que necesita abordarse en varias dimensiones. Ya desde el inicio de la pandemia se ha evidenciado cuán débil es nuestro sis-

tema ante cambios bruscos y cómo la reactivación súbita de la actividad no ha hecho sino empeorar una situación que, más de un año después, sigue sin haberse solucionado. Quizás el caso de los *chips* y su impacto en la automoción pueda ser el ejemplo más claro. En el caso energético está afectando tanto al suministro del gas como a los planes de digitalización en marcha y a la creciente preocupación por posible *malware* embebido en dispositivos inteligentes o controladores.

El precedente del ataque a Solarwinds evidenció cómo de profundo puede ser un ataque de estas características; y el de Colonial Pipeline hizo ver que los impactos cruzados de los ataques podían llegar a parar una nación. De hecho, este último propició que se promulgara en 2021 la orden ejecutiva 14028 "para mejorar la ciberseguridad de la nación" estadounidense. Y en mayo de 2020, el NIST publicó un estudio del avance de la seguridad de la cadena de suministro de *software*. La lectura de este es recomendable, aunque no se puede extraer un claro titular de cómo estamos y de qué hace falta mejorar claramente.

En cuanto a la respuesta ante incidentes, se habla de la necesidad de aproximaciones sectoriales, pero también de colaboración público-privada de modo que haya intercambios de información muy específicos que puedan contener información fácilmente accionable por los operadores y evitando falsos positivos. Esto es lo deseable, pero no es fácil de conseguir. Tengamos en cuenta que gran parte de la inteligencia de amenazas se obtiene de los grandes actores de la ciberseguridad, pero que la medición del impacto de estas la tienen los organismos públicos. Unos organismos que, a su vez, intercambian información con las infraestructuras críticas en relaciones confidenciales, dificultando una transición más abierta a nivel sectorial.

En Europa, organizaciones como ECSO o First están siendo muy activas en estas cuestiones. ECSO, además, comenzó en junio una iniciativa para aglutinar a CISO y promover el intercambio de información. Dentro del ámbito de la energía, los puntos más relevantes son los relativos a la integración IT-OT, a la Directiva NIS 2 y al Código de Red de Ciberseguridad.

Y por el lado estadounidense, cabe resaltar la Ley sobre ataques a infraestructuras críticas (de marzo) y las obligaciones de las empresas para reportar ataques en plazos de 72 horas.

> Debemos temer ataques hacia las infraestructuras de energía en los próximos meses

Para finalizar

En definitiva, ¿debemos temer ataques hacia las infraestructuras de energía en los próximos meses? Por supuesto, pero no más que desde el inicio de la invasión de Ucrania.

¿Somos más vulnerables que antes? El ecosistema en sí es más vulnerable por lo tensionado del mismo, pero a nivel de ciberseguridad han mejorado las capacidades de *Threat Intelligence*. Quizás el mejor ejemplo es Ucrania y cómo se han conseguido frenar prácticamente todos los ciberataques dirigidos contra sus infraestructuras, que no han faltado.

Aun así, ¿podemos bajar la guardia? Claro que no. Los países siguen en niveles altos de alerta, conscientes de que un ataque exitoso en algún segmento de una cadena tan tensionada puede tener grandes efectos para la sociedad. Confiemos en que las Fuerzas y Cuerpos de Seguridad, así como los distintos organismos implicados, puedan seguir desempeñando su labor como hasta ahora mientras se sigue avanzando en los planes de seguridad y resiliencia de estas grandes organizaciones.