Leo Simonovich
Vicepresidente y director global
de Industrial Cyber and Digital Security en Siemens

"La energía es el sector más elegido cuando se trata de ciberataques"

El proceso de transición energética que se ha iniciado en todo el mundo no está exento de las amenazas de los ataques cibernéticos. De hecho, para Leo Simonovich se trata del sector más expuesto. ¿Corre peligro esta transformación de nuestro sistema energético debido a los cibertaques?

Sin duda puede haber una mayor reticencia a acometer una transición energética hacia la digitalización por parte de las empresas debido al aumento del riesgo de sufrir un ciberataque. Pero las compañías deben perder ese miedo y entender que la conectividad propia de la digitalización del sistema energético nos conduce a un mayor conocimiento a la hora de actuar frente a esos ciberataques porque el aislamiento en sí mismo no es sinónimo de la reducción del riesgo", asegura el experto de Siemens, para quien "a medida que la automatización y la digitalización se han hecho más frecuentes en el sector de la energía, los ciberataques cada vez más sofisticados en sus activos operativos están aumentando de manera similar".

Pregunta: ¿Qué retos plantean para Siemens las amenazas derivadas de la ciberseguridad, tanto en relación con la propia empresa como con sus clientes?
Respuesta: En principio la conectividad siempre suscita, tanto en la propia compañía como en nuestros clientes, un cierto temor por el aumento del riesgo que conlleva. Pero en realidad, esta conectividad más que riesgo nos proporciona a todos un mayor conocimiento e información.

El problema radica en que la relación entre conectividad y seguridad no siempre se entiende bien. Las empresas a menudo temen que el aislamiento de sus sistemas reduzca su superficie de ataque y, por lo tanto, su vulnerabilidad. Sin embargo, la conectividad crea infinitas oportunidades para optimizar las operaciones. Y le da a una organización una mayor visibilidad de sus activos y operaciones, y, por lo tanto, una mayor capacidad para detectar y responder a un ataque. Además, la conectividad proporciona la transparencia necesaria para detectar y tomar medidas. Lo que consigue que un sistema sea vulnerable, pero a la vez más seguro.

Concretamente, un estudio reciente realizado por el Instituto independiente Ponemon descubrió que el 69% de todos los ataques provienen del interior de la compañía. Por ejemplo, el código malicioso se entrega a través de un vendedor no consciente de lo que hace o un de un empleado deshonesto. En estas circunstancias, aislar sistemas uno del otro no funcionaría. Por lo que el aislamiento en sí mismo no es sinónimo de la reducción del riesgo.

P: ¿Cuáles son las claves para una correcta coordinación entre las distintas áreas de una compañía como Siemens en materia de ciberseguridad?
R: Concretamente, la estrategia de Siemens para responder a las necesidades de nuestros clientes y también dentro de nuestra propia compañía es construir un equipo que provenga de las mejores compañías de tecnología operativa (OT) para respaldar nuestro servicio de seguridad administrado por OT. Un equipo especializado capaz de ofrecer a los clientes una solución integral que defienda su huella digital completa frente a las amenazas cibernéticas persistentes y altamente sofisticadas.

Por eso en Siemens nos hemos asociado con Darktrace para la detección de intrusiones en redes de velocidad de máquina, con PAS Global por su capacidad única de proporcionar visibilidad de sistemas de control industrial (ICS), y ahora con Tenable, para asegurar que los clientes tengan confianza, disciplina y agilidad para mejorar su seguridad y resiliencia.

Con la amplia experiencia de Siemens en tecnología operativa y el liderazgo de Tenable en seguridad cibernética, esta asociación global está excepcionalmente preparada para fortalecer las defensas en la infraestructura crítica y otras organizaciones que dependan de los sistemas industriales.

P: ¿Cuáles son los principales riesgos a los que se expone el sector eléctrico cuando hablamos de ciberseguridad?

R: Nuestro mundo está más conectado que nunca. Billones de dispositivos inteligentes generan, recopilan y almacenan cantidades masivas de datos. Y las empresas reconocen cada vez más que la capacidad de acceder a estos datos puede ayudarles a mejorar sus propias operaciones y rendimiento. Más aún si se trata de plantas de generación eléctrica donde los datos pueden mejorar el rendimiento de las plantas, generadores, centrales y turbinas, y reducir también los costes de energía. Pero al mismo tiempo, la mayor conectividad de una empresa también hace que sus sistemas sean más vulnerables a las amenazas cibernéticas cada vez más sofisticadas. A medida que la automatización y la digitalización se han hecho más frecuentes en el sector de la energía, los ciberataques cada vez más sofisticados en sus activos operativos están aumentando de manera similar. De hecho, la energía es el sector más elegido cuando se trata de ciberataques. Y las consecuencias de un ataque además pueden ser catastróficas para la economía, el medio ambiente y nuestra seguridad.

P: ¿Existen plantas de generación de energía que por su tipología (nuclear, ciclos combinados, hidroeléctricas, plantas renovables, etc.) sean más vulnerables a los ciberataques?

R: Todas las plantas de generación eléctrica que están conectadas pueden ser susceptibles de ser atacadas por delincuentes cibernéticos. Por eso en Siemens trabajamos con nuestros clientes para centrarnos primero en los fundamentos. Esto significa adoptar un enfoque basado en el riesgo, comprender los activos que tienen, que son los más vulnerables, fortalecerlos y luego monitorear todo su entorno operativo. La seguridad informática integral enfatiza no solo en cómo prevenir, sino también en cómo responder a un ataque. Esto significa brindar madurez a su empresa cibernética.

P: ¿Qué repercusión puede tener el incremento de los ciberataques sobre el proceso de transición energética que debe afrontar el sector energético en todo el mundo?

R: Sin duda puede haber una mayor reticencia a acometer una transición energética hacia la digitalización por parte de las empresas debido al aumento del riesgo de sufrir un ciberataque. Pero las compañías deben perder ese miedo y entender que la conectividad propia de la digitalización del sistema energético nos conduce a un mayor conocimiento a la hora de actuar frente a esos ciberataques porque, como he dicho anteriormente, el aislamiento en sí mismo no es sinónimo de la reducción del riesgo.

P: El pasado 23 de diciembre de 2015, Ucrania vivió un grave ciberataque que consiguió tomar el control de los sistemas de tres de las principales distribuidoras regionales de electricidad. ¿Cree que es posible un episodio similar en otros países europeos?

R: Aunque ha habido una conciencia cada vez mayor de la importancia de la seguridad cibernética tras el ataque Wannacry ransomware, considerado como el mayor ciberataque en la historia, los ataques contra el OT digitalizado se han multiplicado por seis en los últimos años y ahora representan el 30% de todos los ciberataques. Y las brechas en esta esfera tienen un impacto mucho mayor. La realidad en el entorno actual es que la probabilidad de que algún tipo de brecha ocurra en cualquier organización del mundo es del 100% ◂◂