www.pv-magazine.es
Fecha Publicación: viernes, 05 de junio de 2026
Páginas: 4
Valor Publicitario: 2083,67 €
V. Únicos: 21069

Un ciberataque a la red eléctrica de Polonia muestra la brecha de ciberseguridad en almacenamiento

https://www.pv-magazine.es/2026/06/05/un-ciberataque-a-la-red-electrica-de-polonia-muestra-la-brecha-de-ciberseguridad-en-almacenamiento/
www.pv-magazine.es
05/06/2026

Un incidente de ciberseguridad que afectó a aproximadamente 30 instalaciones eólicas y solares en Polonia el 29 de diciembre de 2025 ha proporcionado a las aseguradoras un ejemplo real de una posible vía de ataque contra activos renovables distribuidos, permitiéndoles evaluar riesgos basados en hechos y no únicamente en modelos teóricos. El incidente implicó actividad maliciosa dirigida a infraestructuras de comunicación y sistemas de control en instalaciones energéticas distribuidas, reduciendo o interrumpiendo la visibilidad entre los activos de generación y los operadores de las redes de distribución. La generación eléctrica no fue manipulada directamente. En una planta solar o eólica, esta diferencia tiene relevancia operativa. En un sistema de almacenamiento energético con baterías (BESS), sin embargo, resulta mucho más crítica, ya que la capa de control expuesta a un atacante es la misma que gestiona la seguridad de las celdas. “La vía de ataque demostrada en Polonia —compromiso de dispositivos conectados a internet, ausencia de autenticación multifactor y reutilización de credenciales que permitieron acceder a unidades terminales remotas, relés de protección e interfaces de operación— ya se consideraba técnicamente viable”, explicó a pv magazine Tom Dryden, socio y responsable de ciberseguridad para Europa de McGill and Partners. “Lo que aportó este caso fue la confirmación de que un actor con capacidades avanzadas está dispuesto a explotar esa vía contra activos distribuidos y con intención destructiva, no únicamente financiera”. Las instalaciones afectadas continuaron generando electricidad durante el incidente. Los sistemas de almacenamiento, sin embargo, no cuentan con ese mismo margen de seguridad. La capa de control, un punto crítico para las baterías “La capa de control a la que accedería un atacante —el sistema de gestión de baterías y de energía— es también la que regula la velocidad de carga, el estado de carga y la temperatura de las celdas”, señaló Dryden. “La manipulación de esa capa no supone simplemente un problema de supervisión, sino un mecanismo directo para forzar una batería más allá de sus límites operativos seguros, con una fuga térmica como consecuencia previsible”. Desde el punto de vista asegurador, Dryden considera que este escenario de riesgo ciberfísico deja de ser un supuesto remoto para convertirse en una exposición demostrada. No porque el ataque en Polonia provocara daños físicos, sino porque confirmó que actores con capacidad ofensiva están dirigiendo sus esfuerzos hacia los activos distribuidos del sistema eléctrico. La brecha entre los seguros energéticos y los ciberseguros La respuesta del mercado asegurador se ve condicionada por la propia estructura de las pólizas existentes. Los seguros tradicionales de propiedad e infraestructuras energéticas suelen excluir los daños provocados por incidentes cibernéticos, aunque existen variaciones según las coberturas contratadas. Por su parte, los ciberseguros están diseñados para responder ante ataques maliciosos, pero no siempre cubren daños físicos. Esto significa que un operador de almacenamiento cuya instalación resulte dañada tras una intrusión en el sistema de gestión de baterías podría encontrarse con que el siniestro queda en una zona gris entre ambos tipos de pólizas. “Un incidente de fuga térmica provocado de forma maliciosa puede quedar fuera de cobertura si no se dispone de un ciberseguro específicamente diseñado para este tipo de riesgos”, explicó Dryden. Una superficie de ataque cada vez más amplia Para Charalambos Konstantinou,

www.pv-magazine.es
Fecha Publicación: viernes, 05 de junio de 2026
Páginas: 4
Valor Publicitario: 2083,67 €
V. Únicos: 21069

profesor asociado e investigador principal del laboratorio SENTRY de la Universidad de Ciencia y Tecnología Rey Abdullah (KAUST), la superficie de ataque en infraestructuras energéticas digitales es escalonada. El acceso a sistemas de comunicación y unidades terminales remotas permite interrumpir operaciones o desconectar activos. La manipulación de parámetros de control puede alterar la generación eléctrica. Y un compromiso del firmware, el nivel más profundo, puede persistir incluso después de reiniciar los equipos. Konstantinou recuerda además que el protocolo de comunicaciones utilizado ampliamente en recursos energéticos distribuidos bajo la norma IEEE 1547 carece de mecanismos nativos de autenticación e integridad, una limitación estructural que ya había sido identificada en investigaciones previas. “Los actuarios no pueden valorar aquello que no pueden ver”, afirmó. Según el investigador, la verificación de la integridad del firmware podría reducir significativamente la incertidumbre asociada a estos riesgos. Limitaciones regulatorias La directiva europea NIS2 obliga a los operadores energéticos a aplicar medidas de gestión de riesgos y notificar incidentes de ciberseguridad, pero no exige explícitamente mecanismos estandarizados para verificar la integridad del firmware de los equipos. Por su parte, la futura Ley de Resiliencia Cibernética (Cyber Resilience Act) establece requisitos para proteger programas y configuraciones frente a modificaciones no autorizadas. Sin embargo, según Konstantinou, disponer de un inventario de componentes de software no permite conocer qué código se está ejecutando realmente en cada momento. Como consecuencia, la información que necesitarían las aseguradoras para evaluar adecuadamente el riesgo sigue sin estar disponible de forma estandarizada para operadores y terceros. No esperar a la regulación Los retrasos en la transposición de NIS2 por parte de varios Estados miembros han generado cierta incertidumbre regulatoria. No obstante, los expertos consideran que las empresas no deberían posponer sus inversiones en ciberseguridad. “No recomendaríamos a los operadores retrasar medidas para mejorar su resiliencia cibernética a la espera de cambios regulatorios o de una mayor madurez del mercado asegurador”, afirmó Dryden. “Las medidas necesarias para cumplir la normativa y las que permiten asegurar adecuadamente los activos son, en gran medida, las mismas”. Un mercado asegurador favorable, por ahora Pese al aumento de las amenazas, el mercado de ciberseguros sigue siendo actualmente favorable para los compradores debido a la elevada capacidad disponible frente a la demanda. Según Dryden, esta situación podría mantenerse relativamente estable durante los próximos doce meses, aunque no se descarta un endurecimiento de las condiciones si la siniestralidad continúa creciendo. Para los operadores de sistemas de almacenamiento, la recomendación pasa por evaluar el riesgo ciberfísico en función del coste real de reposición de los activos y complementar las pólizas tradicionales con coberturas específicas para riesgos cibernéticos adaptadas al sector energético. El reto de la observabilidad Según Konstantinou, la principal barrera para cerrar la brecha de visibilidad no es tecnológica, sino económica. Los fabricantes son quienes deben asumir los costes de implementar sistemas que permitan verificar la integridad de sus dispositivos, mientras que los beneficios recaen principalmente sobre operadores y aseguradoras. Sin embargo, considera que el propio mercado asegurador podría acelerar el cambio. “Si las aseguradoras ofrecen mejores condiciones a las flotas capaces de demostrar la integridad de su firmware, ese incentivo podría avanzar más rápido que la propia regulación”, señaló. El incidente de Polonia no ha modificado todavía los precios de los seguros, pero sí ha cambiado la percepción del riesgo. Como resume Dryden, el debate sobre los riesgos ciberfísicos ha pasado de ser una preocupación conceptual a convertirse en una amenaza operativa demostrada. Mientras tanto, la brecha entre cobertura aseguradora y visibilidad tecnológica continúa abierta. De ESS News

Un incidente de ciberseguridad que afectó a aproximadamente 30 instalaciones eólicas y solares en Polonia el 29 de diciembre de 2025 ha proporcionado a las aseguradoras un ejemplo real de una posible vía de ataque contra activos renovables distribuidos, permitiéndoles evaluar riesgos basados en hechos y no únicamente en modelos teóricos. El incidente implicó actividad maliciosa dirigida a infraestructuras de comunicación y sistemas de control en instalaciones energéticas distribuidas, reduciendo o interrumpiendo la visibilidad entre los activos de generación y los operadores de las redes de distribución. La generación eléctrica no fue manipulada directamente. En una planta solar o eólica, esta diferencia tiene relevancia operativa. En un sistema de almacenamiento energético con baterías (BESS), sin embargo, resulta mucho más crítica, ya que la capa de control expuesta a un atacante es la misma que gestiona la seguridad de las celdas. “La vía de ataque demostrada en Polonia —compromiso de dispositivos conectados a internet, ausencia de autenticación multifactor y reutilización de credenciales que permitieron acceder a unidades terminales remotas, relés de protección e interfaces de operación— ya se consideraba técnicamente viable”, explicó a pv magazine Tom Dryden, socio y responsable de ciberseguridad para Europa de McGill and

www.pv-magazine.es
Fecha Publicación: viernes, 05 de junio de 2026
Páginas: 4
Valor Publicitario: 2083,67 €
V. Únicos: 21069

Partners. “Lo que aportó este caso fue la confirmación de que un actor con capacidades avanzadas está dispuesto a explotar esa vía contra activos distribuidos y con intención destructiva, no únicamente financiera”. Las instalaciones afectadas continuaron generando electricidad durante el incidente. Los sistemas de almacenamiento, sin embargo, no cuentan con ese mismo margen de seguridad. La capa de control, un punto crítico para las baterías “La capa de control a la que accedería un atacante —el sistema de gestión de baterías y de energía— es también la que regula la velocidad de carga, el estado de carga y la temperatura de las celdas”, señaló Dryden. “La manipulación de esa capa no supone simplemente un problema de supervisión, sino un mecanismo directo para forzar una batería más allá de sus límites operativos seguros, con una fuga térmica como consecuencia previsible”. Desde el punto de vista asegurador, Dryden considera que este escenario de riesgo ciberfísico deja de ser un supuesto remoto para convertirse en una exposición demostrada. No porque el ataque en Polonia provocara daños físicos, sino porque confirmó que actores con capacidad ofensiva están dirigiendo sus esfuerzos hacia los activos distribuidos del sistema eléctrico. La brecha entre los seguros energéticos y los ciberseguros La respuesta del mercado asegurador se ve condicionada por la propia estructura de las pólizas existentes. Los seguros tradicionales de propiedad e infraestructuras energéticas suelen excluir los daños provocados por incidentes cibernéticos, aunque existen variaciones según las coberturas contratadas. Por su parte, los ciberseguros están diseñados para responder ante ataques maliciosos, pero no siempre cubren daños físicos. Esto significa que un operador de almacenamiento cuya instalación resulte dañada tras una intrusión en el sistema de gestión de baterías podría encontrarse con que el siniestro queda en una zona gris entre ambos tipos de pólizas. “Un incidente de fuga térmica provocado de forma maliciosa puede quedar fuera de cobertura si no se dispone de un ciberseguro específicamente diseñado para este tipo de riesgos”, explicó Dryden. Una superficie de ataque cada vez más amplia Para Charalambos Konstantinou, profesor asociado e investigador principal del laboratorio SENTRY de la Universidad de Ciencia y Tecnología Rey Abdullah (KAUST), la superficie de ataque en infraestructuras energéticas digitales es escalonada. El acceso a sistemas de comunicación y unidades terminales remotas permite interrumpir operaciones o desconectar activos. La manipulación de parámetros de control puede alterar la generación eléctrica. Y un compromiso del firmware, el nivel más profundo, puede persistir incluso después de reiniciar los equipos. Konstantinou recuerda además que el protocolo de comunicaciones utilizado ampliamente en recursos energéticos distribuidos bajo la norma IEEE 1547 carece de mecanismos nativos de autenticación e integridad, una limitación estructural que ya había sido identificada en investigaciones previas. “Los actuarios no pueden valorar aquello que no pueden ver”, afirmó. Según el investigador, la verificación de la integridad del firmware podría reducir significativamente la incertidumbre asociada a estos riesgos. Limitaciones regulatorias La directiva europea NIS2 obliga a los operadores energéticos a aplicar medidas de gestión de riesgos y notificar incidentes de ciberseguridad, pero no exige explícitamente mecanismos estandarizados para verificar la integridad del firmware de los equipos. Por su parte, la futura Ley de Resiliencia Cibernética (Cyber Resilience Act) establece requisitos para proteger programas y configuraciones frente a modificaciones no autorizadas. Sin embargo, según Konstantinou, disponer de un inventario de componentes de software no permite conocer qué código se está ejecutando realmente en cada momento. Como consecuencia, la información que necesitarían las aseguradoras para evaluar adecuadamente el riesgo sigue sin estar disponible de forma estandarizada para operadores y terceros. No esperar a la regulación Los retrasos en la transposición de NIS2 por parte de varios Estados miembros han generado cierta incertidumbre regulatoria. No obstante, los expertos consideran que las empresas no deberían posponer sus inversiones en ciberseguridad. “No recomendaríamos a los operadores retrasar medidas para mejorar su resiliencia cibernética a la espera de cambios regulatorios o de una mayor madurez del mercado asegurador”, afirmó Dryden. “Las medidas necesarias para cumplir la normativa y las que permiten asegurar adecuadamente los activos son, en gran medida, las mismas”. Un mercado asegurador favorable, por ahora Pese al aumento de las amenazas, el mercado de ciberseguros sigue siendo actualmente favorable para los compradores debido a la elevada capacidad disponible frente a la demanda. Según Dryden, esta situación podría mantenerse relativamente estable durante los próximos doce meses, aunque no se descarta un endurecimiento de las condiciones si la siniestralidad continúa creciendo. Para los operadores de sistemas de almacenamiento, la recomendación pasa por evaluar el riesgo ciberfísico en función del coste real de reposición de los activos y complementar las pólizas tradicionales con coberturas específicas para riesgos cibernéticos adaptadas al sector energético. El reto de la observabilidad Según Konstantinou, la principal barrera para cerrar la brecha de visibilidad no es tecnológica, sino económica. Los fabricantes son quienes deben asumir los costes de implementar

www.pv-magazine.es
Fecha Publicación: viernes, 05 de junio de 2026
Páginas: 4
Valor Publicitario: 2083,67 €
V. Únicos: 21069

sistemas que permitan verificar la integridad de sus dispositivos, mientras que los beneficios recaen principalmente sobre operadores y aseguradoras. Sin embargo, considera que el propio mercado asegurador podría acelerar el cambio. “Si las aseguradoras ofrecen mejores condiciones a las flotas capaces de demostrar la integridad de su firmware, ese incentivo podría avanzar más rápido que la propia regulación”, señaló. El incidente de Polonia no ha modificado todavía los precios de los seguros, pero sí ha cambiado la percepción del riesgo. Como resume Dryden, el debate sobre los riesgos ciberfísicos ha pasado de ser una preocupación conceptual a convertirse en una amenaza operativa demostrada. Mientras tanto, la brecha entre cobertura aseguradora y visibilidad tecnológica continúa abierta. De ESS News