www.pv-magazine.es
Fecha Publicación: viernes, 13 de marzo de 2026
Páginas: 3
Valor Publicitario: 1657,00 €
V. Únicos: 4000

PDF EN PROCESO DE ELABORACIÓN
Disculpen las molestias.

Nueva plataforma de simulación permite a operadores eléctricos entrenar frente a ciberataques

https://www.pv-magazine.es/2026/03/13/nueva-plataforma-de-simulacion-permite-a-operadores-electricos-entrenar-frente-a-ciberataques/
www.pv-magazine.es
13/03/2026

Investigadores del instituto alemán Fraunhofer FKIE han desarrollado la herramienta, denominada PowerRange, diseñada para probar estrategias de seguridad y mejorar la capacidad de respuesta ante incidentes en infraestructuras energéticas críticas. marzo 13, 2026 Emiliano Bellini Investigadores del instituto alemán Fraunhofer FKIE han desarrollado una plataforma virtual de simulación que permite a los operadores de redes eléctricas entrenarse frente a ciberataques mediante escenarios realistas y controlados. La herramienta, denominada PowerRange, está diseñada para probar estrategias de seguridad y mejorar la capacidad de respuesta ante incidentes en infraestructuras energéticas críticas. “PowerRange ha sido concebida como un cyber range flexible y escalable para redes eléctricas”, explicó Martin Serror, autor principal del estudio, a pv magazine. Según el investigador, la plataforma permite simular tanto redes eléctricas centralizadas tradicionales como sistemas energéticos descentralizados con una alta penetración de energías renovables y almacenamiento. Serror subraya que las infraestructuras renovables presentan una mayor exposición a riesgos cibernéticos que las centrales eléctricas convencionales. Estas últimas pueden aislarse con mayor facilidad de las redes de comunicación mediante sistemas de air-gap, mientras que las instalaciones renovables dependen en mayor medida de la coordinación digital y de la comunicación entre múltiples dispositivos y sistemas. En este contexto, los sistemas renovables y las infraestructuras de almacenamiento suelen presentar vulnerabilidades asociadas a accesos remotos inseguros, interfaces utilizadas para monitorización, control o mantenimiento, y actualizaciones de firmware inalámbricas (over-the-air) que carecen de mecanismos robustos de autenticación o verificación de integridad. ¿Desea reforzar y mejorar la ciberseguridad de sus activos de energía solar para protegerlos frente a las amenazas emergentes? Únase a nosotros el 29 de abril en el webinar pv magazine+ | Descifrando el primer ciberataque masivo a la infraestructura de energía solar de Europa: el caso de Polonia y las lecciones aprendidas (EN INGLÉS) Los expertos del sector analizarán situaciones reales de ciberataques, pondrán de relieve las posibles vulnerabilidades de los sistemas solares y de almacenamiento, y compartirán estrategias prácticas y viables para proteger sus activos energéticos. Los asistentes adquirirán conocimientos valiosos sobre cómo anticiparse, prevenir y responder a las ciberamenazas en el sector de la energía solar, en rápida evolución. El estudio que presenta la plataforma, titulado «PowerRange: An immersive cyber range for power grid operators», y publicado en la revista International Journal of Critical Infrastructure Protection, describe un entorno de entrenamiento inmersivo basado en el banco de pruebas de código abierto Wattson. Este entorno permite ejecutar de forma segura ataques cibernéticos complejos y aplicar contramedidas en diferentes configuraciones de redes eléctricas, integrando redes de tecnología de la información (IT) y tecnología operativa (OT) con los procesos de generación y distribución de electricidad. La plataforma amplía estas capacidades al ofrecer un entorno de formación diseñado específicamente para operadores de redes eléctricas. Entre sus funcionalidades destaca la posibilidad de aplicar medidas de seguridad en condiciones realistas, detectar debilidades operativas y entrenar a todos los niveles organizativos, desde personal de gestión hasta

www.pv-magazine.es
Fecha Publicación: viernes, 13 de marzo de 2026
Páginas: 3
Valor Publicitario: 1657,00 €
V. Únicos: 4000

especialistas en IT y operadores de sala de control. El sistema incorpora además un Centro de Control Virtual (VCC) que proporciona interfaces intuitivas y sincronizadas entre varios usuarios. A través de este entorno, los operadores pueden visualizar el estado de la red, emitir órdenes de control y realizar estimaciones del sistema en tiempo real. PowerRange permite reproducir distintos tipos de ciberataques habituales en infraestructuras críticas, como reconocimiento de red, movimiento lateral dentro del sistema, escalado de privilegios, ataques de denegación de servicio (DoS), ataques man-in-the-middle (MITM) o inyección de datos falsos. Los instructores pueden combinar diferentes ataques mediante módulos configurables y adaptar los escenarios dinámicamente en función de las decisiones tomadas por los participantes. La plataforma también modeliza los elementos de la red eléctrica mediante nodos y conexiones, representando activos energéticos, interconexiones y parámetros operativos. A través de configuraciones basadas en reglas, los usuarios pueden ajustar variables como el nivel de controlabilidad, la observabilidad del sistema o la complejidad del escenario, generando simulaciones que posteriormente pueden exportarse a configuraciones compatibles con Wattson. El equipo de investigación llevó a cabo dos sesiones piloto de formación con operadores profesionales. Según los resultados preliminares, los participantes experimentaron inicialmente dificultades relacionadas con el flujo de información y la familiarización con las herramientas, pero progresivamente lograron coordinar respuestas eficaces frente a los incidentes simulados. Los participantes destacaron especialmente el valor de los escenarios realistas, la experiencia práctica y la comunicación entre equipos. Los investigadores concluyen que los programas de entrenamiento periódicos permiten mejorar la aplicación práctica de las medidas de ciberseguridad y favorecen la coordinación entre los distintos actores implicados en la operación del sistema eléctrico. Además, subrayan que el factor humano sigue siendo un elemento clave para reforzar la resiliencia de las infraestructuras energéticas. En relación con el papel de las energías renovables, Serror señala que la naturaleza distribuida de estos activos puede aumentar la resiliencia general del sistema eléctrico frente a ataques dirigidos, ya que la afectación de un número limitado de instalaciones no suele comprometer la estabilidad global. Sin embargo, advierte de que el uso generalizado de componentes idénticos —como inversores o sistemas de control— puede generar vulnerabilidades sistémicas si un fallo común es explotado de forma coordinada. Los investigadores prevén además que los ciberataques dirigidos al sector energético continúen aumentando en los próximos años, en línea con el incremento registrado recientemente en incidentes contra infraestructuras críticas. No obstante, también advierten de que los ataques físicos y las acciones de sabotaje, como las observadas en el conflicto de Ucrania, pueden resultar incluso más disruptivos cuando se combinan con ofensivas cibernéticas coordinadas. Este contenido está protegido por derechos de autor y no se puede reutilizar. Si desea cooperar con nosotros y desea reutilizar parte de nuestro contenido, contacte: editors@pv-magazine.com. Popular content Investigadores del instituto alemán Fraunhofer FKIE han desarrollado la herramienta, denominada PowerRange, diseñada para probar estrategias de seguridad y mejorar la capacidad de respuesta ante incidentes en infraestructuras energéticas críticas. marzo 13, 2026 Emiliano Bellini Investigadores del instituto alemán Fraunhofer FKIE han desarrollado una plataforma virtual de simulación que permite a los operadores de redes eléctricas entrenarse frente a ciberataques mediante escenarios realistas y controlados. La herramienta, denominada PowerRange, está diseñada para probar estrategias de seguridad y mejorar la capacidad de respuesta ante incidentes en infraestructuras energéticas críticas. “PowerRange ha sido concebida como un cyber range flexible y escalable para redes eléctricas”, explicó Martin Serror, autor principal del estudio, a pv magazine. Según el investigador, la plataforma permite simular tanto redes eléctricas centralizadas tradicionales como sistemas energéticos descentralizados con una alta penetración de energías renovables y almacenamiento. Serror subraya que las infraestructuras renovables presentan una mayor exposición a riesgos cibernéticos que las centrales eléctricas convencionales. Estas últimas pueden aislarse con mayor facilidad de las redes de comunicación mediante sistemas de air-gap, mientras que las instalaciones renovables dependen en mayor medida de la coordinación digital y de la comunicación entre múltiples dispositivos y sistemas. En este contexto, los sistemas renovables y las infraestructuras de almacenamiento suelen presentar vulnerabilidades asociadas a accesos remotos inseguros, interfaces utilizadas para monitorización, control o mantenimiento, y actualizaciones de firmware inalámbricas (over-the-air) que carecen de mecanismos robustos de autenticación o verificación de integridad. ¿Desea reforzar y mejorar la ciberseguridad de sus activos de energía solar para protegerlos frente a las amenazas emergentes? Únase a nosotros el 29 de abril en el webinar pv magazine+ | Descifrando el primer ciberataque masivo a la infraestructura de energía solar de Europa: el caso de Polonia y las lecciones aprendidas (EN INGLÉS) Los expertos del sector

www.pv-magazine.es
Fecha Publicación: viernes, 13 de marzo de 2026
Páginas: 3
Valor Publicitario: 1657,00 €
V. Únicos: 4000

analizarán situaciones reales de ciberataques, pondrán de relieve las posibles vulnerabilidades de los sistemas solares y de almacenamiento, y compartirán estrategias prácticas y viables para proteger sus activos energéticos. Los asistentes adquirirán conocimientos valiosos sobre cómo anticiparse, prevenir y responder a las ciberamenazas en el sector de la energía solar, en rápida evolución. El estudio que presenta la plataforma, titulado «PowerRange: An immersive cyber range for power grid operators», y publicado en la revista International Journal of Critical Infrastructure Protection, describe un entorno de entrenamiento inmersivo basado en el banco de pruebas de código abierto Wattson. Este entorno permite ejecutar de forma segura ataques cibernéticos complejos y aplicar contramedidas en diferentes configuraciones de redes eléctricas, integrando redes de tecnología de la información (IT) y tecnología operativa (OT) con los procesos de generación y distribución de electricidad. La plataforma amplía estas capacidades al ofrecer un entorno de formación diseñado específicamente para operadores de redes eléctricas. Entre sus funcionalidades destaca la posibilidad de aplicar medidas de seguridad en condiciones realistas, detectar debilidades operativas y entrenar a todos los niveles organizativos, desde personal de gestión hasta especialistas en IT y operadores de sala de control. El sistema incorpora además un Centro de Control Virtual (VCC) que proporciona interfaces intuitivas y sincronizadas entre varios usuarios. A través de este entorno, los operadores pueden visualizar el estado de la red, emitir órdenes de control y realizar estimaciones del sistema en tiempo real. PowerRange permite reproducir distintos tipos de ciberataques habituales en infraestructuras críticas, como reconocimiento de red, movimiento lateral dentro del sistema, escalado de privilegios, ataques de denegación de servicio (DoS), ataques man-in-the-middle (MITM) o inyección de datos falsos. Los instructores pueden combinar diferentes ataques mediante módulos configurables y adaptar los escenarios dinámicamente en función de las decisiones tomadas por los participantes. La plataforma también modeliza los elementos de la red eléctrica mediante nodos y conexiones, representando activos energéticos, interconexiones y parámetros operativos. A través de configuraciones basadas en reglas, los usuarios pueden ajustar variables como el nivel de controlabilidad, la observabilidad del sistema o la complejidad del escenario, generando simulaciones que posteriormente pueden exportarse a configuraciones compatibles con Wattson. El equipo de investigación llevó a cabo dos sesiones piloto de formación con operadores profesionales. Según los resultados preliminares, los participantes experimentaron inicialmente dificultades relacionadas con el flujo de información y la familiarización con las herramientas, pero progresivamente lograron coordinar respuestas eficaces frente a los incidentes simulados. Los participantes destacaron especialmente el valor de los escenarios realistas, la experiencia práctica y la comunicación entre equipos. Los investigadores concluyen que los programas de entrenamiento periódicos permiten mejorar la aplicación práctica de las medidas de ciberseguridad y favorecen la coordinación entre los distintos actores implicados en la operación del sistema eléctrico. Además, subrayan que el factor humano sigue siendo un elemento clave para reforzar la resiliencia de las infraestructuras energéticas. En relación con el papel de las energías renovables, Serror señala que la naturaleza distribuida de estos activos puede aumentar la resiliencia general del sistema eléctrico frente a ataques dirigidos, ya que la afectación de un número limitado de instalaciones no suele comprometer la estabilidad global. Sin embargo, advierte de que el uso generalizado de componentes idénticos —como inversores o sistemas de control— puede generar vulnerabilidades sistémicas si un fallo común es explotado de forma coordinada. Los investigadores prevén además que los ciberataques dirigidos al sector energético continúen aumentando en los próximos años, en línea con el incremento registrado recientemente en incidentes contra infraestructuras críticas. No obstante, también advierten de que los ataques físicos y las acciones de sabotaje, como las observadas en el conflicto de Ucrania, pueden resultar incluso más disruptivos cuando se combinan con ofensivas cibernéticas coordinadas. Este contenido está protegido por derechos de autor y no se puede reutilizar. Si desea cooperar con nosotros y desea reutilizar parte de nuestro contenido, contacte: editors@pv-magazine.com. Popular content