Odpowiedź branży fotowoltaicznej na wyzwania z zakresu cyberbezpieczeństwa

Rafał Kozieł
Polskie Stowarzyszenie Rozwoju Fotowoltaiki

Polskie Stowarzyszenie Rozwoju Fotowoltaiki

- Założone na początku 2022 roku
- Zrzesenie producentów i dystrybutorów wiodących marek inwerterów na polskim rynku
- Główne cele stowarzyszenia:
  - Działalność edukacyjna w zakresie instalacji fotowoltaicznych i magazynów energii
  - Promowanie najlepszych praktyk w obszarach: realizacja inwestycji, bezpieczeństwo przeciwpożarowe instalacji; cyberbezpieczeństwo
  - Doradztwo techniczne, opiniowanie projektów ustaw i rozporządzeń dotyczących OZE

PSRF

https://www.psrf.pl

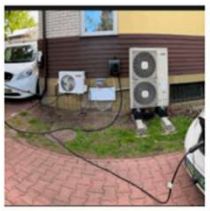
Polskie Stowarzyszenie Rozwoju Fotowoltaiki

BAZA WIEDZY

Wyświetlanie wszystkich wyników: 7

Domyślne sortowanie

Expert guide – Practical Validation of nearZEB Residential Power Supply Model with Renewable Electricity Brought into the Building Using Electric Vehicles (via V2G) Instead of the Distribution Network



Poradnik – Praktyczna walidacja modelu zasilania budynków mieszkalnych nearZEB przy użyciu energii odnawialnej dostarczanej do budynku za pomocą pojazdów elektrycznych (poprzez V2G) zamiast sieci dystrybucyjnej

Poradnik – Prosty projekt sposobem na poprawę bezpieczeństwa instalacji fotowoltaicznej

Poradnik – wymagania ppoż dla systemów magazynowania energii

Publikacja – Odpowiedź branży fotowoltaicznej na wyzwania z zakresu cyberbezpieczeństwa

Publikacja – Skrupulatne planowanie rozwoju branży fotowoltaicznej i magazynowania energii

Wytyczne – Zalecenia projektowania, dostaw, montażu, odbiorów i eksploatacji instalacji mikrogeneratorów PV instalowanych prosumentom

AKTUALNOŚCI

BEZ KATEGORII

Komplementarnia misja branży fotowoltaicznej i ciepła systemowego

Spieszymy poinformować, że Adam Kampa, Wiceprezes PSRF reprezentował nas na kongresie energetycznym DISE we Wrocławiu. Adam miał okazję omówić rolę branży PV w transformacji ciepłownictwa! Dziś mówimy o synergii elementów ...

BEZ KATEGORII

Forum dyskusyjne dotyczące magazynów energii

Członkowie Polskiego Stowarzyszenia Rozwoju Fotowoltaiki aktywnie biorą udział w wydarzeniach branżowych oraz dzielą się swoimi opiniami i doświadczeniami. Tak też było tym razem, w trakcie forum dyskusyjnego na temat magazynów ...

BEZ KATEGORII

Kontynuacja współpracy merytorycznej z dwumiesięcznikiem Nowa Energia – ekonomika magazynowania energii elektrycznej w chemicznych magazynach energii

Informujemy, że Polskie Stowarzyszenie Rozwoju Fotowoltaiki nie zwalnia tempa, gdyż w ramach kontynuacji współpracy merytorycznej, już w najbliższym wydaniu magazynu Nowa Energia pojawi się publikacja, którą opracował nasz kolega – ...

BEZ KATEGORII

Odpowiedź branży fotowoltaicznej na wyzwania z zakresu cyberbezpieczeństwa

Dziś wracamy do Państwa z pełnym wydaniem artykułu PSRF w magazynie Nowa Energia: „Odpowiedź branży fotowoltaicznej na wyzwania z zakresu cyberbezpieczeństwa". Zachęcamy do lektury zwłaszcza tych z Państwa, którzy zainteresowani ...

Transformacja energetyczna = cybernetyzacja → warstwa IT

Transformacja energetyczna / dekarbonizacja → zastosowanie rozproszonych, małych źródeł i magazynów energii.

→ Podstawą jest sprawna komunikacja w czasie rzeczywistym

→ Bilansowanie, liczniki zdalnego odczytu

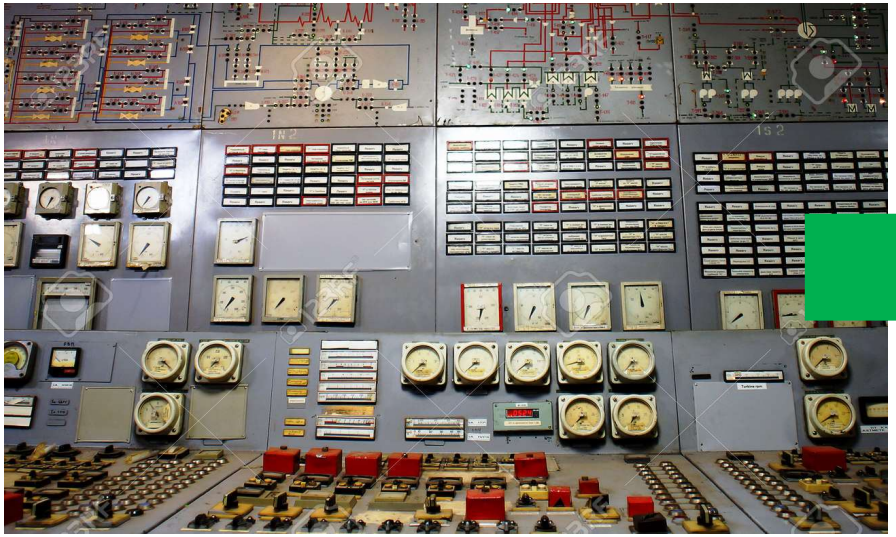
→ **Budowa ogromnego systemu informatycznego do komunikacji / wymiany danych**

Transformacja energetyczna = digitalizacja Energetyki → warstwa OT

Transformacja energetyczna → digitalizacja systemów sterowania i zarządzania przepływami mocy

→ Analogowe/mechaniczne urządzenia kontrolne zastępowane interfejsami elektronicznymi, zdalne sterowanie

→ Masowe wprowadzanie układów monitorujących i sterujących typu SCADA

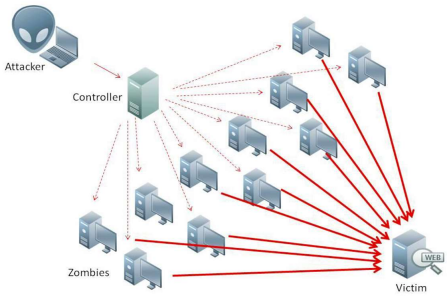


Główne rodzaje ataków

Atak na protokół komunikacyjny

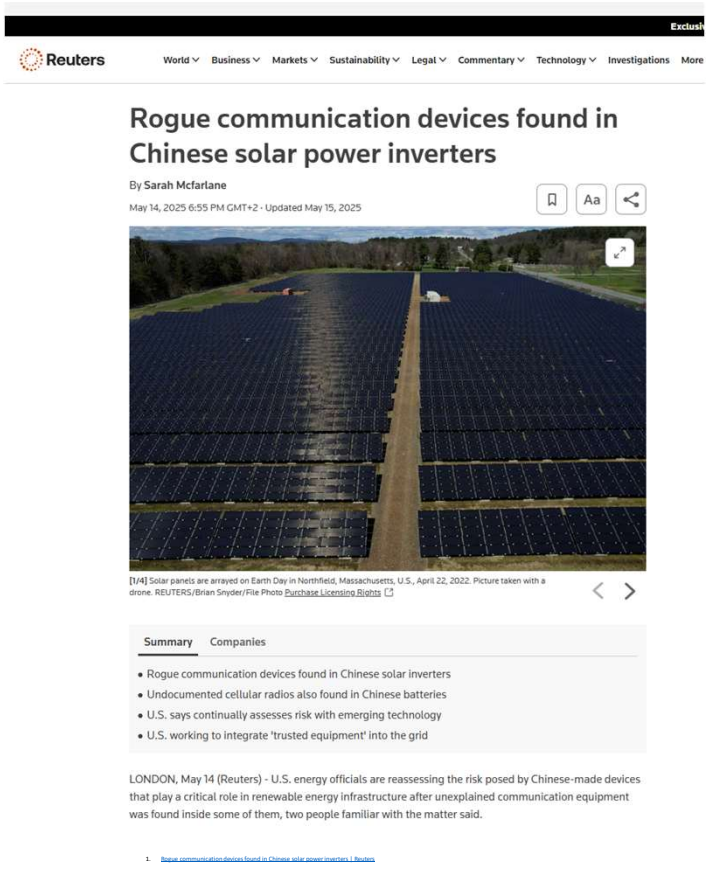
Atak na łańcuch dostaw

Atak DDoS



Atak Ransomware

Reuters – maj 2025



Reuters

World Business Markets Sustainability Legal Commentary Technology Investigations More

Rogue communication devices found in Chinese solar power inverters

By Sarah Mcfarlane

May 14, 2025 6:55 PM GMT+2 · Updated May 15, 2025

[1/4] Solar panels are arrayed on Earth Day in Northfield, Massachusetts, U.S., April 22, 2022. Picture taken with a drone. REUTERS/Brian Snyder/File Photo Purchase Licensing Rights

Summary Companies

- Rogue communication devices found in Chinese solar inverters
- Undocumented cellular radios also found in Chinese batteries
- U.S. says continually assesses risk with emerging technology
- U.S. working to integrate 'trusted equipment' into the grid

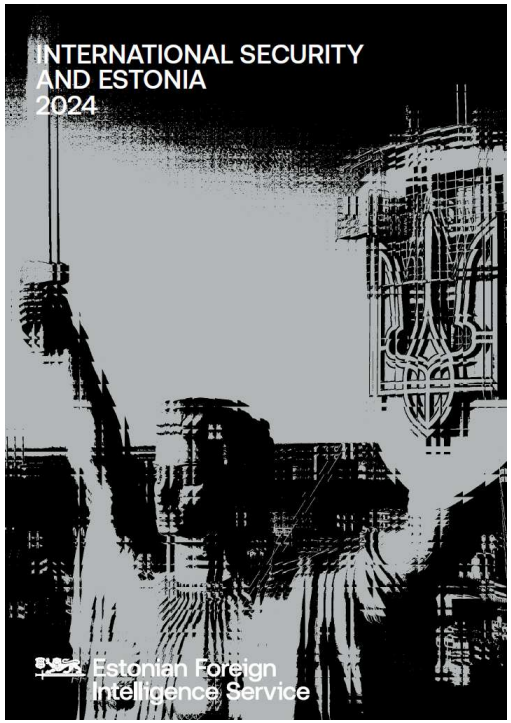
LONDON, May 14 (Reuters) - U.S. energy officials are reassessing the risk posed by Chinese-made devices that play a critical role in renewable energy infrastructure after unexplained communication equipment was found inside some of them, two people familiar with the matter said.

1. Rogue communication devices found in Chinese solar power inverters | Reuters

Główne ustalenia:

- W USA odkryto podejrzane urządzenia komunikacyjne w niektórych chińskich falownikach , których nie było w oficjalnej dokumentacji produktów.
- Ujawnione urządzenia (np. ukryte modemy komórkowe) **mogą umożliwiać zdalny dostęp do sprzętu, omijając zabezpieczenia typu firewall**.
- Stwarzają ryzyko zdalnego wyłączenia lub zmiany ustawień falowników, co mogłoby prowadzić do destabilizacji sieci energetycznych, uszkodzenia infrastruktury, a nawet szeroko zakrojonych blackoutów.

Ostrzeżenia z innych państw



PVTECH

SUBSCRIBE TO PREMIUM SIGN IN

News Industry Updates Premium Manufacturing Markets & Finance Power Plants Features Marl

NEWS

Lithuania to block Chinese inverters with cybersecurity legislation

By Will Norman

November 13, 2024

Power Plants, Balance of System, Grids, Projects

Europe

LATEST

- SolarEdge battery closures to enable focus on 'core solar' and 'solar-tied batteries', says CEO (NEWS)
- GPG Australia secures AU$2.3 billion financing for renewable energy portfolio (NEWS)
- Avangrid, PGE sign 120MW PPA backed by Meta data centre (NEWS)
- Transmission grid congestion could hinder renewable power deployment in Spain – DNV (NEWS)
- Voltalia appoints new

Facebook Twitter LinkedIn Reddit Email

SolarPower Europe has already said enhanced cybersecurity requirements should be introduced for components such as inverters. Image: BayWa r.e.

National Cyber and Information Security Agency

NÚKIB

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Business ID No.: 05800226
Data box ID: zzfnkp3

File ref. No.:
350-647/2025-E
Reference No.:
6159/2025-NÚKIB-E/350

Brno, September 3, 2025

WARNING

The National Cyber and Information Security Agency, registered office: Mučednická 1125/31, 616 00 Brno (hereinafter the "Agency"), pursuant to Section 12(1) of Act No. 181/2014 Coll., on cyber security and on amendments to related acts, as amended (hereinafter the "Cyber Security Act"), issues the following

Warning

of cyber security threat consisting of

1. the transfer of system and user data to the People's Republic of China, to the territories of People's Republic of China´s Special Administrative Regions or to entities based in the territories of the People's Republic of China or its Special Administrative Regions, and
2. the remote administration of technical assets carried out from the territories of the People's Republic of China, People's Republic of China´s Special Administrative Regions or by entities based in the territories of the People's Republic of China or its Special Administrative Regions.

1. Źródło: Raport Estońskiej Służby Wywiadu Zagranicznego https://raport.valisluureamet.ee/2024/en/
2. Źródło: Aktualizacja litewskiego Prawa Energetycznego https://www.pv-tech.org/lithuania-to-block-chinese-inverters-with-cybersecurity-legislation/
3. Źródło: NUKIB, EN_2025-09-03_warning.pdf

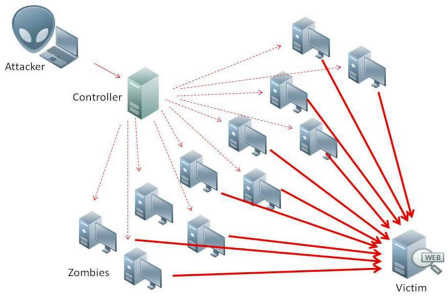
PURF

Główne rodzaje ataków

Atak na protokół komunikacyjny

Atak na łańcuch dostaw

Atak DDoS



Atak Ransomware

Ataki na energetykę z przeszłości

USA, 2003 rok

Wirus „Slammer" wprowadzony do sieci w elektrowni jądrowej David-Bess; atak typu DDoS zablokował system nadzorujący chłodzenie reaktora; konieczność wyłączenia awaryjnego na kilka godzin[1];

Ukraina, 2015 rok

Wprowadzenie złośliwego programu BlackEnergy do sieci operatora, wyłączenie stacji elektroenergetycznych, uruchomienie programu KillDisk opóźniającego możliwość zlokalizowania i usunięcia problemu; 230 tys odbiorców bez energii przez ponad 6h[2]

USA, 2021 rok

Atak na system przesyłowy paliw Colonial Pipeline, spowodował zablokowanie dostaw do okolicznych miast i panikę wśród mieszkańców po kilku dniach trwania awarii. Hakerom zapłacono okup w wysokości 4.5mln USD w walucie Bitcoin.

Niemcy, 2022 rok

W lutym 2022 r. cyberatak ma dostawcę internetu satelitarnego Viasat sparaliżował komunikację z 11 GW niemieckich turbin wiatrowych, niejako „przy okazji" ataku wymierzonego w ukraiński wojskowy system łączności[3]

Europa i USA – codziennie!

Tylko przez pierwsze 4 miesiące wojny na Ukrainie, Microsoft wykrył próby włamania do ponad 130 organizacji rządowych i firm energetycznych (najwięcej w USA i Europie Zachodniej, w tym w Polsce); ich celem była m.in. próba destabilizacji infrastruktury technicznej[4]. Ogólny wzrost o 220% rok do roku

1. CIRE.PL – Cyberataki na energetykę są coraz częstsze
2. Energetyka.Plus - Cyberbezpieczeństwo infrastruktury krytycznej – energetyka na celowniku hakerów
3. Satellite cyber attack paralyzes 11GW of German wind turbines – pv magazine International (pv-magazine.com)
4. „Defending Ukraine: Early Lessons from the Cyber War" Microsoft

Możliwe skutki przejęcia kontroli nad urządzeniami - skala MIKRO

Ok. 23 GW mocy zainstalowanej PV w Polsce

W tym prawie 12 GW – mikroinstalacje prosumenckie

Kradzież wrażliwych danych

Sfałszowanie rzeczywistych uzysków z instalacji

Poznanie rozkładu pomieszczeń i „zwyczajów" domowników – zaplanowanie włamania do budynku

Destabilizacja pracy układów BMS w magazynach energii – możliwość „zdalnego" wywołania pożaru!

Dane na koniec września 2025; Źródło: Moc zainstalowana fotowoltaiki w Polsce | Wrzesień 2025

Możliwe skutki cyberataków - skala MAKRO

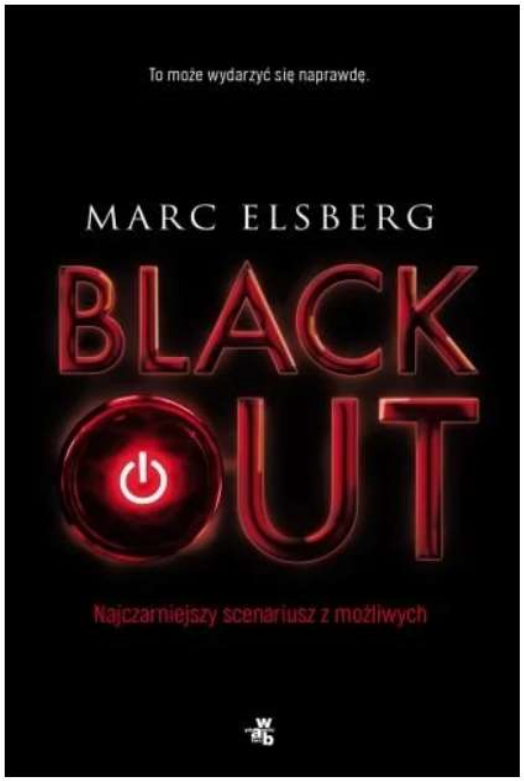
Eksperci szacują, że nagłe, niekontrolowane wyłączenie 3 GW generacji może zdestabilizować sieć na obszarze Polski!

Kim są napastnicy, których musimy się obawiać?

Atakujący na zlecenie obcych krajów i rządów!

Mają odpowiednie: zasoby, motywację, umiejętności

Fikcja literacka czy realny scenariusz?



Marc Elsberg „Blackout”

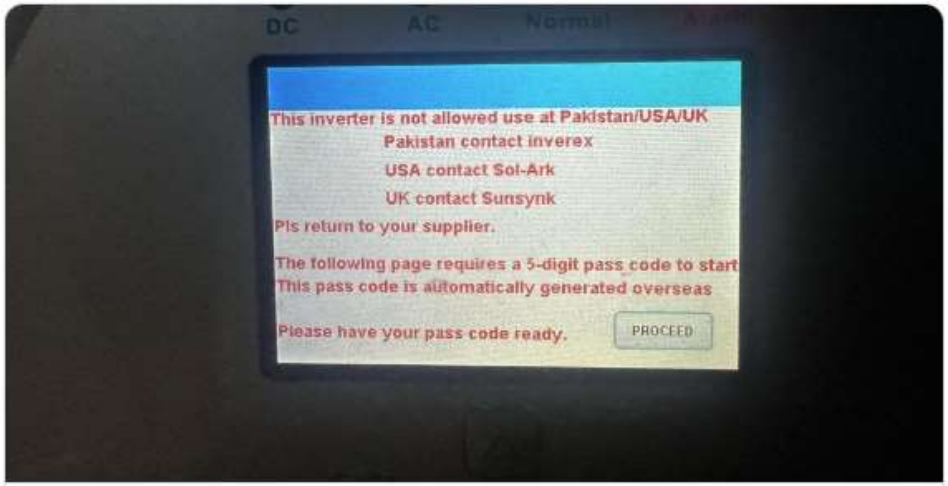
1. Masowe, jednoczesne odłączenie znacznej liczby odbiorców w kilku krajach poprzez wykorzystanie liczników inteligentnych (smart meter)
2. Zainfekowanie wirusami oprogromowania SCADA jednego z czołowych dostawców software – sfałszowane odczyty pomiarowe i brak możliwości sterowania elektrowniami i aparaturą rozdzielczą
3. Fizyczne niszczenie infrastruktury – linie i stacje elektroenergetyczne

Najgorszy scenariusz...

Źródło: [Deye deaktiviert Solar-Wechselrichter in USA, UK und PakistanBorns IT- und Windows-Blog]

derek the solarboi
@solarboi.com
+ Follow

Seemingly at the drop of a hat the morning of Friday, Nov 15th, Deye-branded inverters across the US were intentionally bricked.



Sol-Ark OEM disables all Deye inverters in the US
Seemingly, at the drop of a hat the morning of Friday, Nov 15th, Deye-branded inverters across the US were intentionally bricked.
solarboi.com

Werbung

← Cybervorfälle: Sauter-Cumulus (Gebäudeautomation), Fefe-Blog, US-Internetanbieter
Interpol Operation Serengeti führt zu 1.006 Festnahmen →

Deye deaktiviert Solar-Wechselrichter in USA, UK und Pakistan

Publiziert am 27. November 2024 von Günter Born

[English]Kritisches Thema, was mir bereits die Tage untergekommen ist und die Gefahr von IT-Abschaltungen durch Hersteller oder Staaten illustriert. Der chinesische Hersteller Deye, auch in deutschen Balkonkraftwerken und Solaranlagen-Installationen mit Wechselrichtern vertreten, hat zum 15. November 2024 solche Geräte in den USA, in Großbritannien, in Pakistan, sowie in einigen anderen Ländern abgeschaltet. Da sind die Solaranlagen tot!

Suchen
Suchen

Blogs auf Borncity
Borncity.com Startseite
Borns IT- und Windows Blog
Born's Tech and Windows World

Bücher-Blog
Günnis Seniorentreff 50+
Mein Reiseblog
Mein Japan-Blog
E-Scooter-Blog

Spenden
Den Blog durch Spenden unterstützen.

Regulacje prawne

Ustawa KSC - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Główny dokument regulacyjny w zakresie cyberbezpieczeństwa obowiązujący w Polsce

Prace nad CRA

Do końca 2024 spodziewane uchwalenie ostatecznego kształtu dyrektywy na poziomie UE

Ustawa o Krajowym Systemie Certyfikacji Cyberbezpieczeństwa

Implementacja rozporządzenia UE 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa.

Tworzy ramy prawne system certyfikacji, wzajemnego honorowania w UE… nie ustanawia OBOWIĄZKOWEJ certyfikacji

Implementacja NIS 2 w prawie krajowym

„Deadline" na wprowadzenie dyrektywy NIS 2 do prawa krajowego (w przypadku Polski – aktualizacja KSC) mija 17.10.2024

JUŻ PRZEKROCZONY → Nowelizacja dalej w procedowaniu !!!

Ustawa KSC

Wdrożenie do polskiego prawa m.in. dyrektywy NIS

2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027

Dyrektywa NIS

Pierwsza dyrektywa europejska ustanawiająca regulacje i wytyczne w zakresie cyberbezpieczeństwa

Dyrektywa NIS 2

Styczeń 2023 – uchwalenie dyrektywy na poziomie UE

Rozporządzenie DORA

Styczeń 2025 – zaostrzenie wymogów bezpieczeństwa cyfrowego, dotyczy sektora finansowego i ICT

Implementacja **CRA** w prawie krajowym (plan)

NIS 2 i aktualizacja KSC

- Wprowadzenie definicji podmiotów kluczowych i ważnych wraz ze stosownymi wymaganiami
- W Polsce: pomysł wprowadzenia do ustawy definicji **Dostawcy Wysokiego Ryzyka**

Znaczenie bezpieczeństwa w OZE

Ryzyko cyberzagrożeń w OZE

Fotowoltaika/źródła OZE mogą być podatne na cyberataki, które mogą destabilizować system elektroenergetyczny.

Zalecane standardy bezpieczeństwa

Ważne jest stosowanie urządzeń zgodnych z europejskimi normami ETSI EN 303645 i ISO 27001.

Wzrost zagrożeń i geopolityka

Globalne napięcia i wydarzenia jak wojna na Ukrainie uwypukliły ryzyko paraliżu kluczowych usług przez cyberataki i presję polityczną.

Edukacja uczestników rynku

Szkolenia są kluczowe, by zmniejszyć ryzyko nieautoryzowanego dostępu do instalacji PV.

Kluczowe działania na przyszłość

Działania ochronne użytkowników

Zmiana domyślnych haseł i regularne aktualizacje oprogramowania minimalizują ryzyko ataków.

Rozważny dobór dostawców

Do udziału w rynku powinni być dopuszczeni wyłącznie zweryfikowani, wiarygodni dostawcy – szczególnie w infrastrukturze krytycznej

Wdrażanie regulacji i certyfikacji

Realizacja dyrektyw i krajowych programów certyfikacji wzmacnia ochronę infrastruktury krytycznej.

Raz jeszcze - EDUKACJA

Dziękuję za uwagę!

mgr inż. Rafał Kozieł
koziel@sma.de
+48 881 979 158

https://www.psrf.pl