

Recent Cyberattack on the Polish Energy Sector

Testimonial

Jeremi Gryka | PSE

9th E.DSO/EE-ISAC/ENCS/ENISA Cybersecurity Forum
2026-10-08
www.pse.pl



- **About PSE**
- **Attacks overview**
 - 2025-12-29 RES & CHP Operators
 - 2026-01-19 PSE
- **Analysis and follow-up**

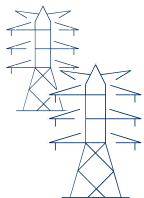
We are the Polish electricity grid Transmission System Operator



National Dispatch Centre
– main and back-up centres

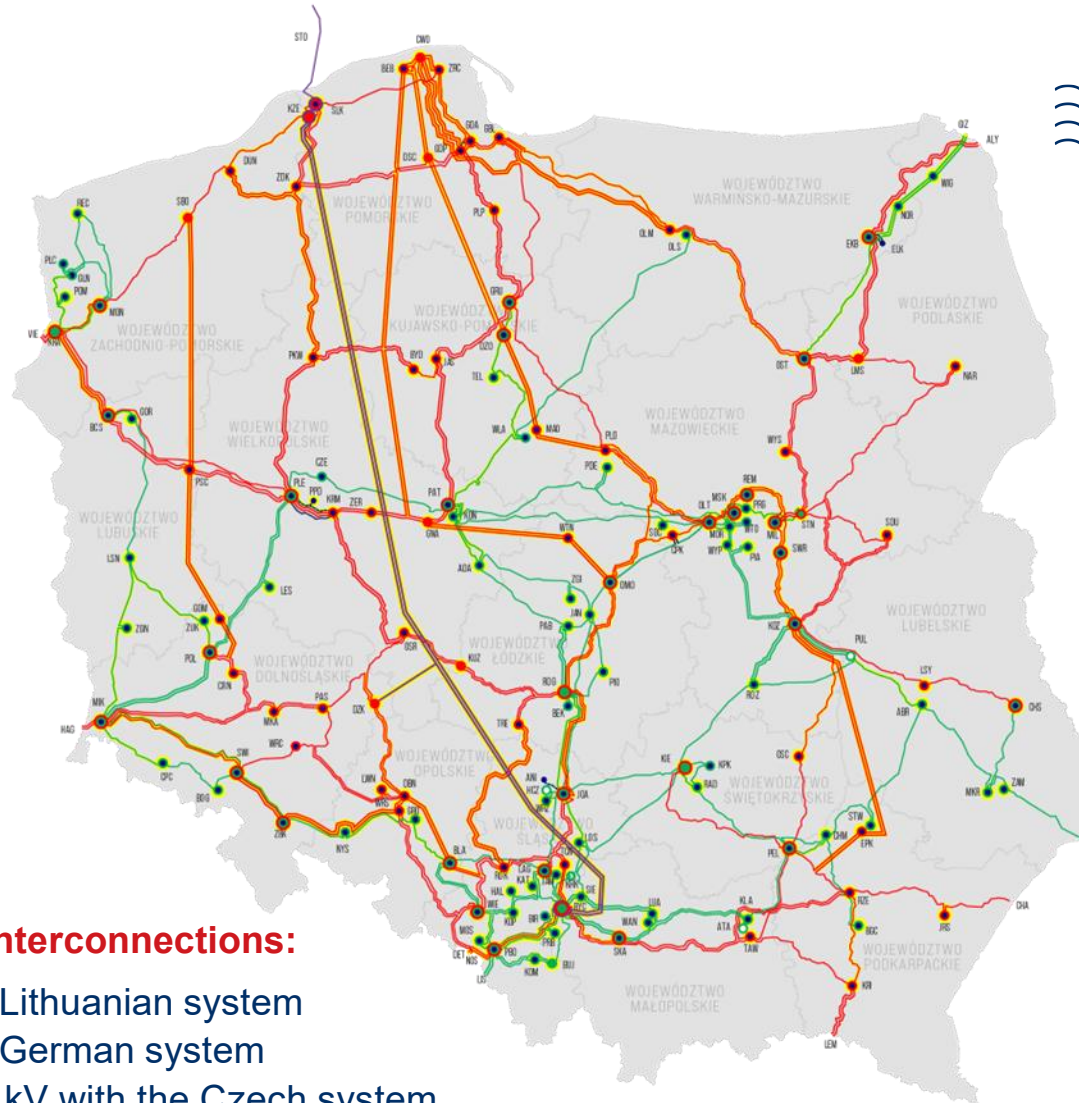


5 area divisions
- maintenance and
management of the EHV
system operation

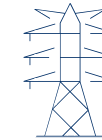


Synchronous interconnections:

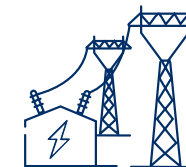
400 kV with the Lithuanian system
400 kV with the German system
400 kV and 220 kV with the Czech system
400 kV with the Slovak system
400 kV with the Ukrainian system



Submarine 450 kV DC
Poland-Sweden connection
with a length of 254 km
(of which 127 km belongs to PSE)



309 lines in operation
with **a length of 16 500 km:**
142 400 kV lines, 9 624 km
167 220 kV lines, 6 896 km

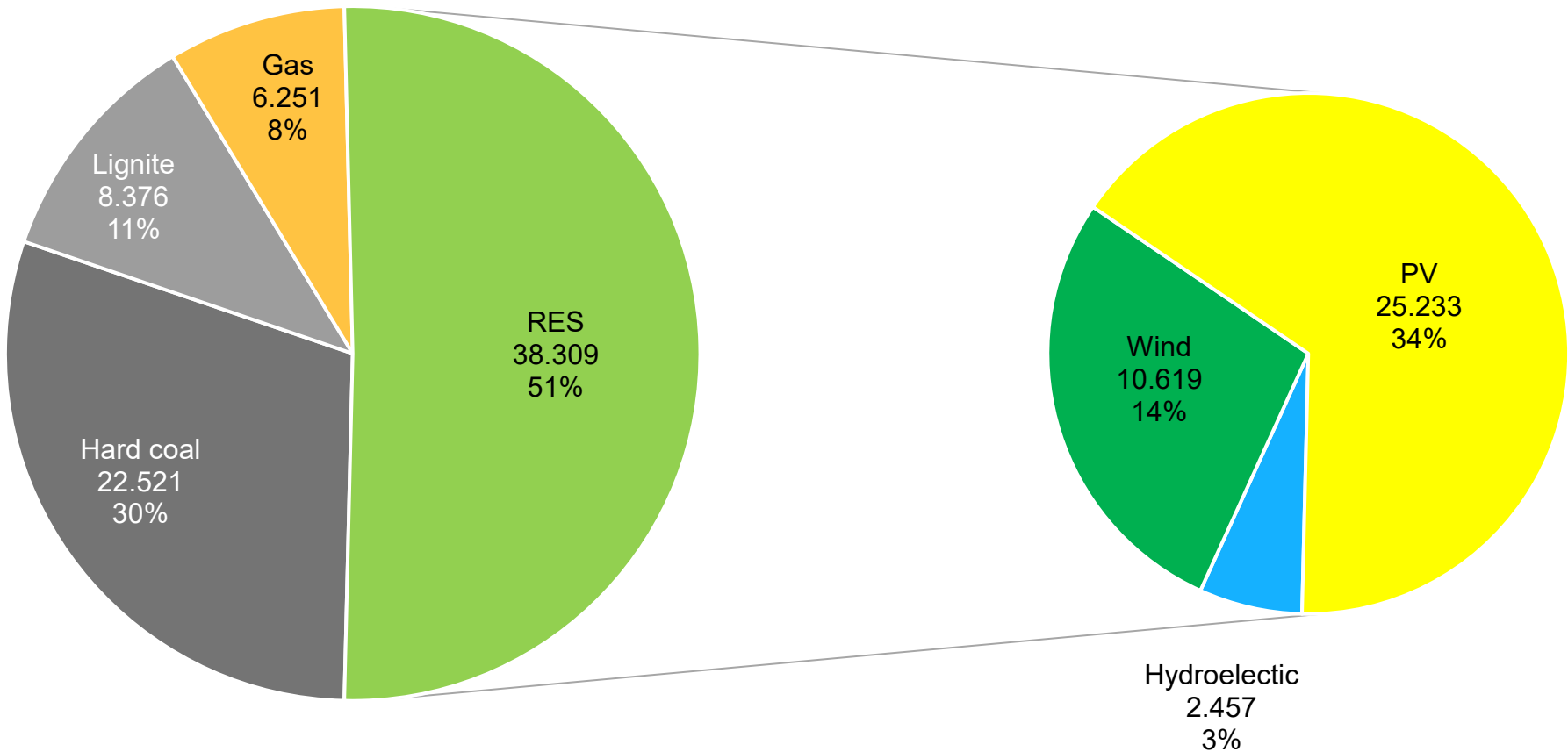


**112 extra-high
voltage (EHV)
substations**

We are the Polish electricity grid Transmission System Operator



Power generation mix – installed power in MW



Attack #1 2025-12-29

Focused cyber attack against ICT infrastructure of Polish RES & CHP operators

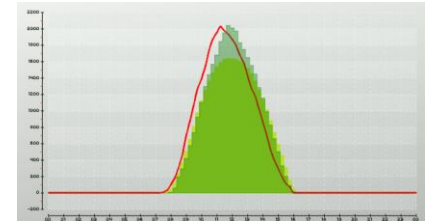
■ Calendar and environmental context

- Monday after loooong Christmas weekend, “bridge” days off for many
- Short cloudy day
- -10°C, snowstorms



■ PSE context

- No anomalies in PSE ICT systems
 - PSE was not targeted
- No anomalies at the national grid level
 - minimal PV, above average wind generation
- PSE received information on cyber problems at selected partners, but only on 2025-12-31
- Some communications issues with a few RES producers, but not exceptional

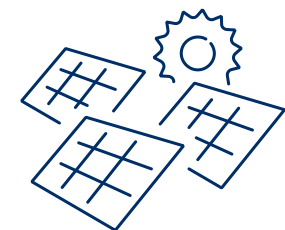
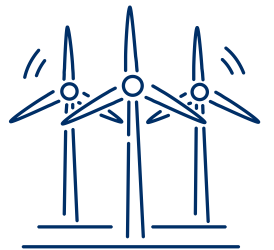


Attack #1 2025-12-29

Focused cyber attack against ICT infrastructure of Polish RES & CHP operators

■ 30 RES facilities

- 2025Q3..4: Takeover of multiple Fortinet devices serving as Internet firewalls and remote access VPN systems at the RES producers, most likely via stolen admin credentials/lacking updates
- Reconnaissance of RES internal networks
- 2025-12: Extensive scanning activity / logon attempts, preparatory reconfigurations
- 2025-12-29: Deletion of data or factory reset on RTUs/HMIs/EIDs, (rendered unusable)
- Specifically scanned for energy market devices from manufacturers widely used in Poland
 - Hitachi (corrupted firmware loaded, with faulty bootloader; files erased)
 - Mikronika RTUs and HMIs (files erased)
 - Hitachi Relion IEDs (files erased)
 - Moxa (reconfigured useless)
- Also scanned for Siemens and Sprecher devices
- Factory-reset/wipe of VPN devices (rendered unusable / traces deleted)
- NB: Some RES facilities relied on a common ICT integrator
- ***Electricity generation not affected***



Attack #1 2025-12-29

Focused cyber attack against ICT infrastructure of Polish RES & CHP operators



■ A large Combined Heat and Power plant

- 2025Q2..Q4: Compromise of Active Directory system. Reconnaissance and credentials gathering. Foothold and access for attack
- 2025-12-29: AD mechanisms used to attempt to wipe ~140 workstations – unsuccessful, stopped by EDR (canary mechanism).
- Successful destruction of data on servers.
- Wiper malware + multiple living-off-the-land techniques
- ***Electricity generation not affected***

■ Cloud Services used by victims of above attacks

- Credentials obtained on-premises used to access cloud services
- Microsoft 365 accounts with access to Exchange, Teams, SharePoint
- Accessed files and messages with technical info re OT network & SCADA systems work

Attack #1 2025-12-29

Focused cyber attack against ICT infrastructure of Polish RES & CHP operators

■ Not-so-private GSM APN configuration

- Some (RES & fossil) energy production facilities connect to DSO via a common dedicated APN
- APN configuration allowed lateral movement between facilities
- GSM router compromised at one of the RES facilities via its management interfaces
- 2025-12: intensive scanning of the APN IP network



■ A small Combined Heat and Power plant

- 2025-12-18: Initial access to a WAGO PLC with GSM adapter configured for the above APN
- Reconnaissance of CHP internal networks + unsuccessful attacks on internal firewall
- 2025-12-29: Siemens PLC ordered STOP + password assigned
 - Steam turbine and water treatment stopped
 - CHP personnel restored config from backup, restarted the process
- Moxa (reconfigured useless), ABB devices accessed, Schneider device attack attempted, but failed
- WAGO device used for initial access damaged
- Initial disturbance during the attack taken as a result of engineering error during recent maintenance
- ***Heat and electricity generation affected (short term – not visible to customers)***

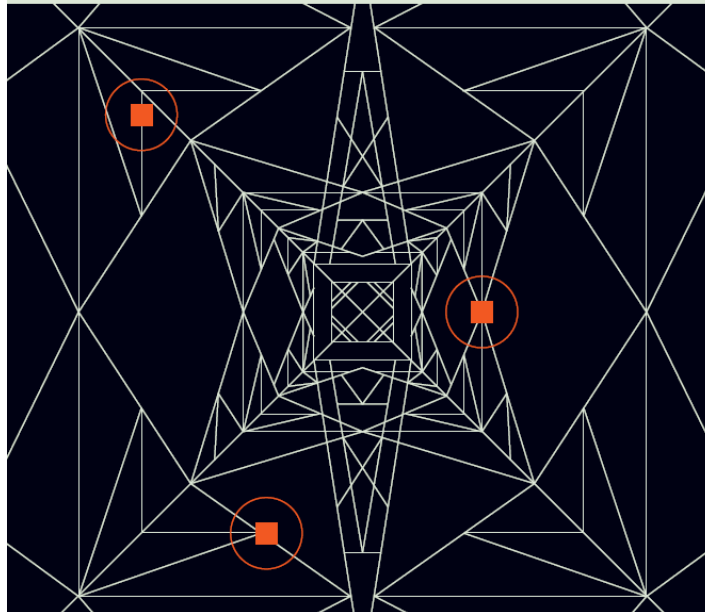


Polish National CSIRT reports on the Attack #1 activities

Originally published on 2026-01-30, with a follow-up on 2026-08-08



Energy Sector Incident Report – 29 December

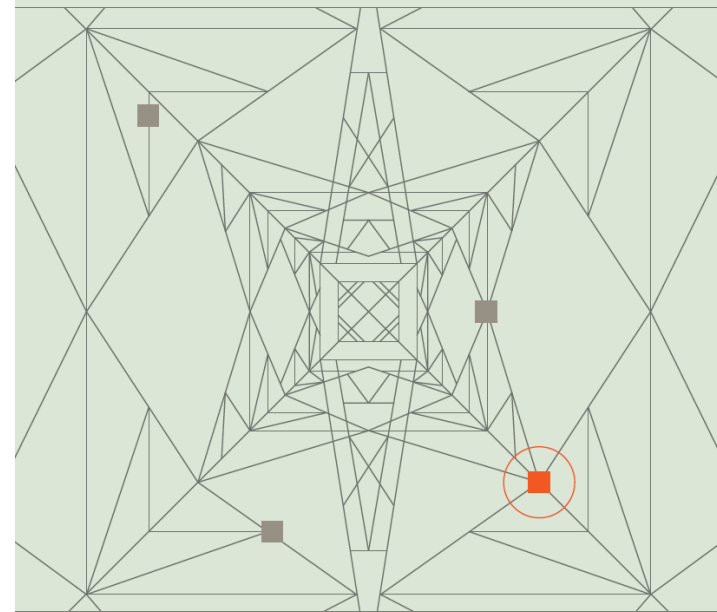


CERT.PL
NASK

Ministry of Digital Affairs
Republic of Poland

<https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/>

Follow-Up Analysis of the 29 December 2025 Energy Sector Incident



CERT.PL
NASK

Ministry of Digital Affairs
Republic of Poland

<https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/>



Attack #2 2026-01-19

DDoS attack on www.pse.pl

- **PSE ICT systems were targeted**

- One (PSE on-site) web server targeted and rendered unavailable to the Internet for minutes.
- Attack source: an international botnet
- Servers withstood the attack, no restarts needed, thanks for network level mitigation by the ICP provider
- No other anomalies were observed. No impact on the core operations, or even e-mail.

- **Two waves**

- **Wave 1: 5 minutes - ~150Mbps**

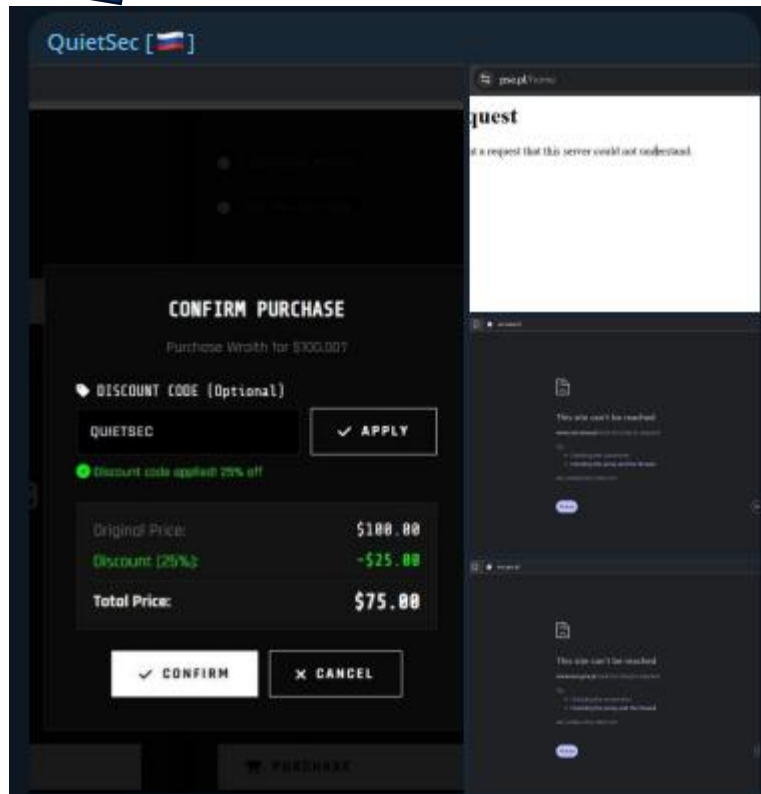
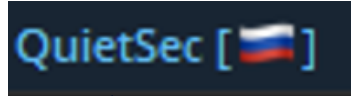
- Alarm raised, webserver defences deployed, services remained available
- No external mitigation needed

- **Wave 2: 12 minutes - ~400Mbps**

- Alarm raised, service rendered unavailable
- Mitigation with the support of the ISP provider employed successfully
- Attack continued with quickly decaying intensity for another hour

Attack #2 2026-01-19

DDoS attack on www.pse.pl



Открываем огонь по русофобской Польше ❌

Polskie Sieci Elektroenergetyczne (PSE) – оператор национальной трансмиссионной сети (высоковольтные линии и передача энергии).

<https://www.pse.pl/>

— официальный сайт PSE (оператора сети).

❌ Check-host:

<https://check-host.net/check-report/373aa273kcf0>

Agencja Rynku Energii S.A. (ARE) – Польское агентство энергетического рынка (статистика, рыночные данные).

<https://www.are.waw.pl/en>

— официальный сайт ARE (Agency for the Energy Market).

❌ Check-host:

<https://check-host.net/check-report/373aa650k35b>

Urząd Regulacji Energetyki (URE) – Энергетическое регулирующее управление Польши (регулятор рынка электроэнергии и газа).

<https://www.ure.gov.pl/en/>

— официальный сайт регулятора польского энергетического рынка (тарифы, лицензии, правила).

❌ Check-host:

<https://check-host.net/check-report/373aaa15k7a1>

❤️ Атакуй с нами через Areshun.com !

При покупке подписки QuietSec действует скидка!
Успей!

QuietSec | бот для обратной связи - @QuietSeccontact_bot



98 edited 20:00

"We open fire against the
russophobic Poland"

Organizations targeted at
the same time:

- PSE
- URE - Polish national energy regulator
- ARE - Polish national energy market agency

"Attack with us on com!
There is a discount on
'QuietSec' subscriptions.
Hurry!"

Observations

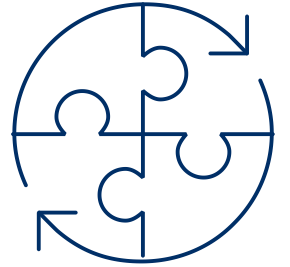
- **Characteristics of the attacks**
 - Long term of pre-positioning / reconnaissance / set-up / dormant presence
 - 2025-12-29 activities were merely a "detonation"
 - AI and automation extensively used in the preparation and execution
 - Digital arson: no attempt to take control, only destruction
- **First event of such precision, extent and selectivity in Poland, clearly distinguishing it from previous incidents.**
 - The national electricity grid overall unaffected
 - A test of Poland's reactive capabilities? A demonstration of intent?
- **Root causes in simple, routine hygiene gaps**
 - Default passwords
 - Same passwords in multiple places, even for admin access
 - Neither MFA nor smart card in remote access
 - Lacking critical updates / vulnerable equipment exposed to the internet
 - Inadequate separation of OT from IT networks, DOS APN and the Internet
 - Insecure configurations (unnecessary services, firmware update security features not enabled, APN)
- **...being removed as part of follow-up activities across the industry**



Follow-up

■ Reaction

- Incident reporting was fragmented and delayed, cooperation suffered initially
- National level CSIRTs involved deeply and effectively after a short delay
- Good cooperation with the vendors
- Analysis and recovery took ~~weeks~~ months



■ Quick and rich information exchange

- Extensive media coverage, multiple direct comments of Polish government officials
- PSE informed European partners through ENTSO-E channels – including in response to queries
- Wide communication of the detailed incident report by CERT Polska, also in EN (2026-01-30 + 2026-08-08)

■ Tabletop blue team exercise based on the report findings was organized

■ Recommendations and regulations

- Ministry of Digital Affairs published a set of recommendations addressing root causes and key problems on 2026-01-19
- Increased resolve in the implementation of the NIS2/NCCS in the Polish law (passed by the parliament on 2026-01-23, signed into law 2026-02-19, in force since 2026-04-03)
- A few days later a recommendation addressing a CISCO vulnerability issued by the Ministry (~binding)

■ Positive signals on the establishment of Energy Sector National CSIRT at PSE

Jeremi Gryka | Jeremi.Gryka@pse.pl | PSE