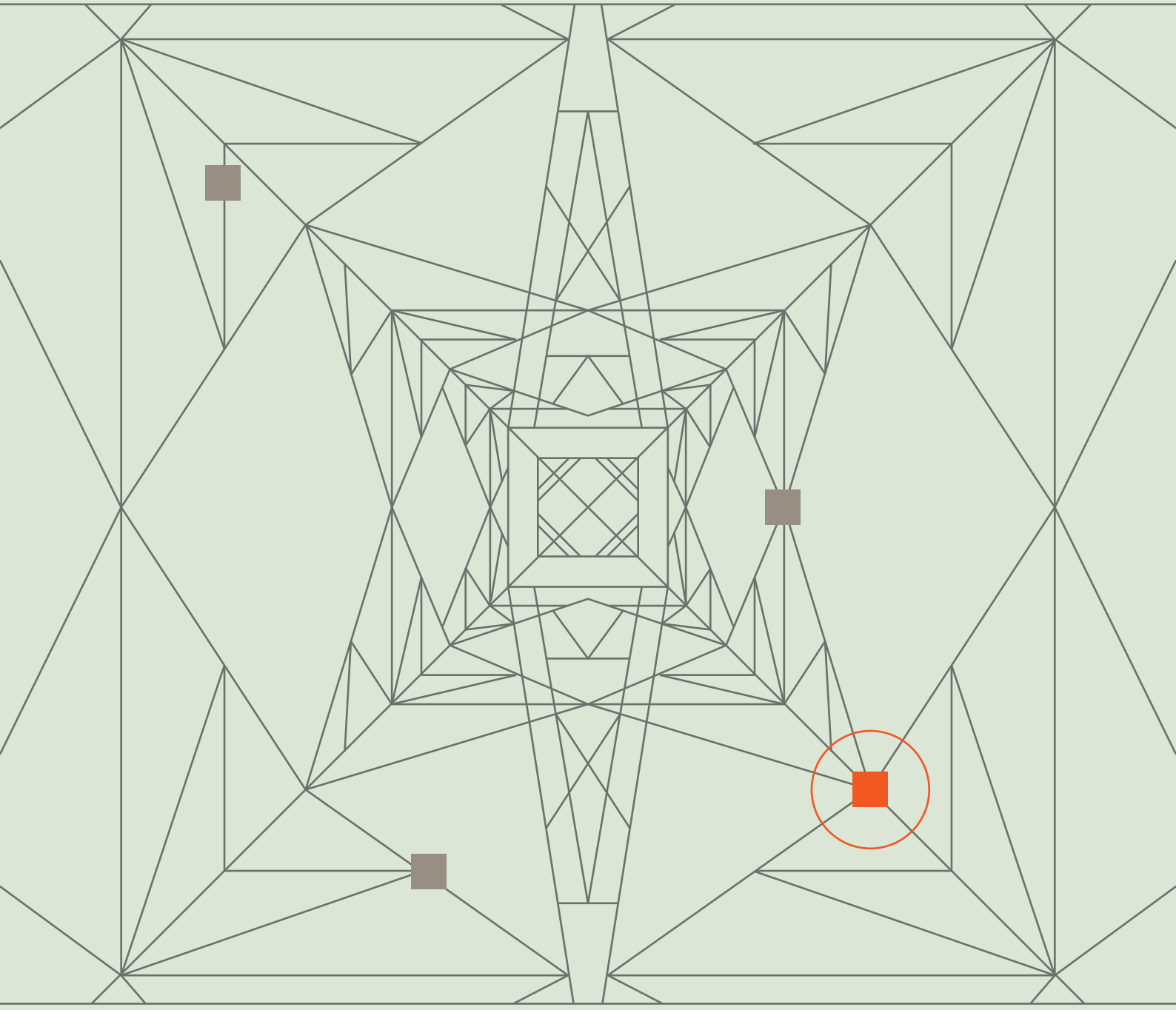
Follow-Up Analysis of the 29 December 2025 Energy Sector Incident



CERT.PL NASK

Ministry of Digital Affairs
Republic of Poland

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

CERT.PL NASK

Ministry of Digital Affairs
Republic of Poland

The Author of This Report Is

CERT Polska
(CERT.PL) – a team operating within the structures of NASK – National Research Institute, carrying out the tasks of CSIRT NASK, one of the three national-level CSIRT teams operating within Poland's national cybersecurity system.

Table of Contents

Introduction

On 29 December 2025, coordinated attacks targeted the energy sector in Poland, including 30 renewable energy facilities and a large combined heat and power (CHP) plant. These attacks were described in detail in the report published on 30 January 2026*. At the same time, another incident occurred at a smaller CHP plant supplying heat to 50,000 residents. The analysis of this incident took more than three months to complete, which is why it was not included in the initial report. To the best of our knowledge, the attack vector used in this case has not previously been observed in any known incidents.

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

Attack on the Second CHP Plant

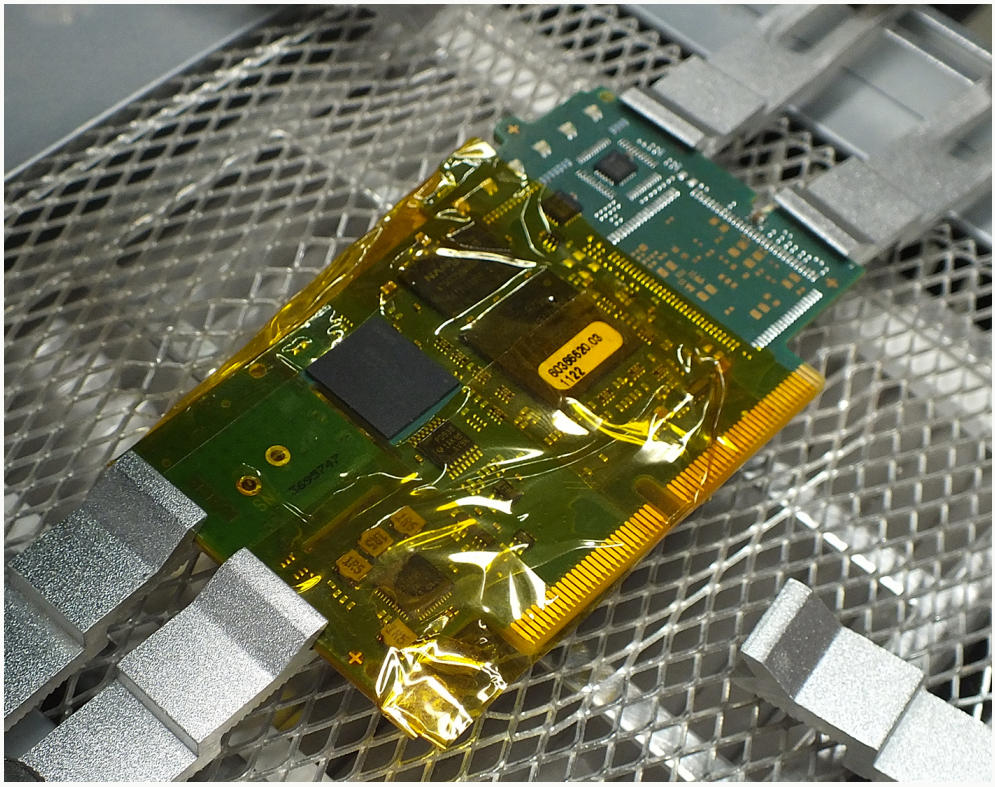
On 29 December, at approximately 7:00 a.m., the industrial control systems of a CHP plant supplying heat to approximately 50,000 residents came under attack. The attack resulted in the shutdown of a steam turbine and the water treatment system used to produce process water, leading to an interruption of the cogeneration process. Thanks to the prompt response of the plant's operators, the incident caused only a short-term outage of the installation and did not result in any disruption to heat or electricity supplies for customers.

As maintenance work was being carried out at the facility, the entity initially assumed that the process interruption had been caused by an error made by the contractor’s engineers and reported the event for informational purposes only. However, due to its awareness of other similar events, CERT Polska initiated incident handling under the assumption that the event may have resulted from a cyberattack. Further analysis confirmed this hypothesis. This case demonstrates the importance of reporting not only confirmed incidents but also unexplained failures and operational disruptions.

Based on further detailed analysis of the collected logs, investigators were able to identify the device from which the attacker had conducted their activities: a WAGO PFC200 PLC equipped with an integrated cellular modem. Unfortunately, the device had been damaged, and no data could be recovered from it despite forensic examination carried out in a laboratory.

FIGURE 1.

Preparation for desoldering the memory chip from a WAGO PFC200 device in the CERT Polska laboratory



Attacks against industrial networks initiated directly from a PLC are not among the scenarios typically observed in OT environments. Due to the lack of logs, our investigation relied on the development and testing of hypotheses. The first assumption was that the device had been inadvertently exposed to the Internet. However, an analysis of the presence of this type of device within the Polish IP address space during the relevant period ruled outInternet exposure. We subsequently obtained information indicating that the device was used to communicate with the systems of a Distribution System Operator (DSO). It was equipped with a SIM card operating within a dedicated private data transmission network (private APN) managed by the DSO.

This discovery led to a painstaking analysis that ultimately allowed us to reconstruct the attack sequence. In this report, we present the findings in chronological order; however, the actual investigative work was conducted in the reverse direction, with analysts working backward from the observed effects to identify the initial point of compromise.

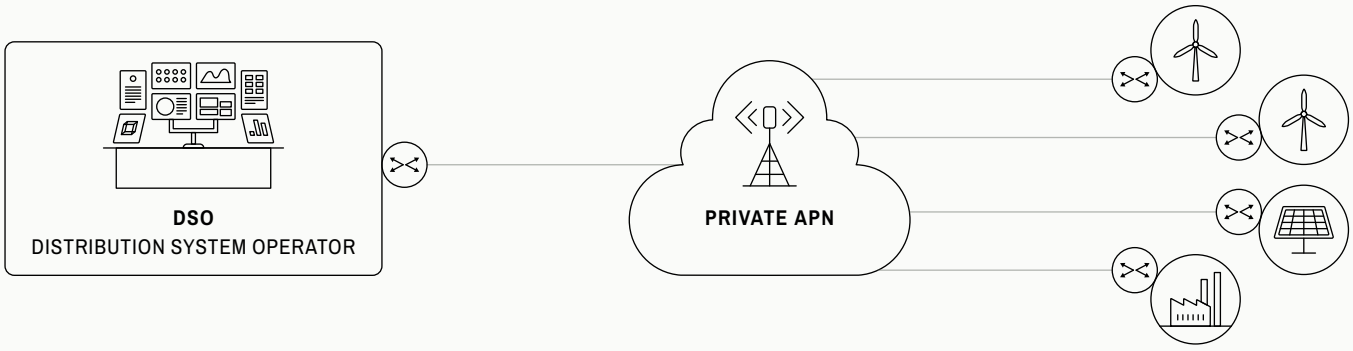
Activity at the Wind Farm

To understand the attack on the CHP plant, it is first necessary to revisit the attacks on the wind farms described in our initial report. Those incidents affected more than 30 Grid Connection Points (GCPs). A GCP is the point at which a renewable energy installation is connected to the distribution network and its operator.

Each compromised substation associated with a wind farm contained a FortiGate device functioning as both a VPN concentrator and a firewall. In every case, the VPN interface was accessible from the Internet and allowed authentication using accounts defined in the device configuration without multi-factor authentication. Although the networks of the investigated facilities often employed separate VLAN segments, the attacker had administrative privileges on the device at the time of the attack. These privileges were likely used to obtain the credentials of a VPN account that had access to all network segments.

Substations also commonly use cellular routers as a backup or, in some cases, as their primary communication channel. These routers are equipped with SIM cards that provide access to a private APN managed by the DSO. The private APN enables communication between the DSO's SCADA system and the Remote Terminal Unit (RTU) installed at the substation.

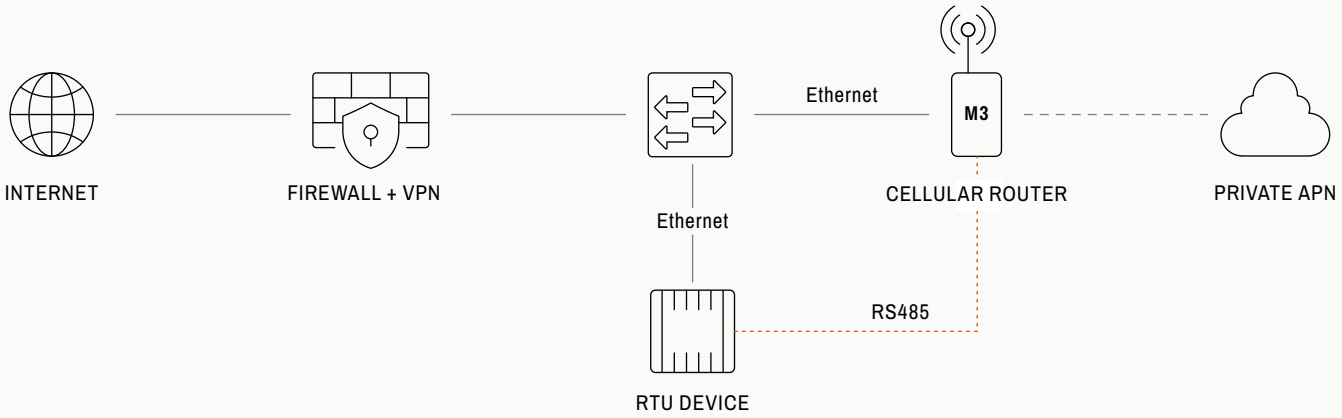
FIGURE 2. **Illustrative use of a private APN in distributed energy resources (DERs)**



An important aspect of this architecture is that DSOs require all communication between the DSO's ICT network and the RTU to take place over a serial protocol, in this case DNP3.0.

At the compromised facility, a Teltonika RUTX50 router was used, and the DSO's requirements were met. However, no requirements had been defined regarding the handling of the cellular router's administrative interface. As a result, the router was configured with two physical interfaces: a serial link connected to the RTU and a second interface, Ethernet, connected to a VLAN managed by the central firewall that had been compromised by the attacker.

FIGURE 3. **Placement of the Cellular Router Within a Segment of the Wind Farm Network**



The router model deployed at the affected facility exposes a web administration interface and an SSH service on its LAN interface by default. Upon first login, users are required to change the default password, and this step had been completed by the company that deployed the system. It was not possible to determine how the attacker obtained the new password, or whether a vulnerability in the Teltonika device had been exploited.

Through laboratory analysis of the device, an SQLite database containing selected device events, including logins to the web administration interface and via SSH, was recovered from persistent storage.

FIGURE 4. **Recovered logs indicating successful SSH logins to the Teltonika cellular router**

```
CONNECTIONS,37,1688315762,2025-12-18 16:36:02,Web UI,notice,Authentication was successful from HTTP 10.20.26.97
CONNECTIONS,38,1688318191,2025-12-18 17:16:31,IP Block,notice,IP (10.20.26.97) to (10.20.26.107) attempt 1/10 (ssh).
CONNECTIONS,39,1688318205,2025-12-18 17:16:45,IP Block,notice,IP (10.20.26.97) to (10.20.26.107) attempt 2/10 (ssh).
CONNECTIONS,40,1688318251,2025-12-18 17:17:31,IP Block,notice,IP (10.20.26.97) to (10.20.26.107) attempt 3/10 (ssh).
CONNECTIONS,41,1688318251,2025-12-18 17:17:31,SSH,notice,Bad password attempt for root from 10.20.26.97:55454
CONNECTIONS,42,1688318255,2025-12-18 17:17:35,IP Block,notice,IP blocking entry (10.20.26.97 -> 10.20.26.107:22) deleted.
CONNECTIONS,43,1688318255,2025-12-18 17:17:35,SSH,notice,Password auth succeeded for root from 10.20.26.97:55454
CONNECTIONS,44,1688318817,2025-12-18 17:26:57,SSH,notice,Password auth succeeded for root from 10.20.26.97:55458
CONNECTIONS,45,1688319842,2025-12-18 17:44:02,SSH,notice,Password auth succeeded for root from 10.20.26.97:55460
CONNECTIONS,46,1688334460,2025-12-18 21:47:40,Web UI,notice,Authentication was successful from HTTP 10.20.26.97
CONNECTIONS,47,1688335230,2025-12-18 22:00:30,IP Block,notice,IP (10.20.26.97) to (10.20.26.107) attempt 1/10 (ssh).
CONNECTIONS,48,1688335230,2025-12-18 22:00:30,SSH,notice,Bad password attempt for root from 10.20.26.97:55536
CONNECTIONS,49,1688335236,2025-12-18 22:00:36,IP Block,notice,IP blocking entry (10.20.26.97 -> 10.20.26.107:22) deleted.
CONNECTIONS,50,1688335236,2025-12-18 22:00:36,SSH,notice,Password auth succeeded for root from 10.20.26.97:55536
CONNECTIONS,51,1688402874,2025-12-19 16:47:54,SSH,notice,Password auth succeeded for root from 10.20.26.97:58620
CONNECTIONS,52,1688561536,2025-12-21 12:52:16,SSH,notice,Password auth succeeded for root from 10.20.26.97:38338
CONNECTIONS,53,1688576950,2025-12-21 17:09:10,SSH,notice,Password auth succeeded for root from 10.20.26.97:38340
CONNECTIONS,54,1688581633,2025-12-21 18:27:13,SSH,notice,Password auth succeeded for root from 10.20.26.97:38342
CONNECTIONS,55,1688590030,2025-12-21 20:47:10,SSH,notice,Password auth succeeded for root from 10.20.26.97:38344
CONNECTIONS,56,1688590076,2025-12-21 20:47:56,SSH,notice,Password auth succeeded for root from 10.20.26.97:38346
```

The attacker logged into the router multiple times via SSH during December 2025. Based on logs obtained from the mobile network operator, it was determined that the attacker most likely used SSH tunneling to gain access to the private APN network.

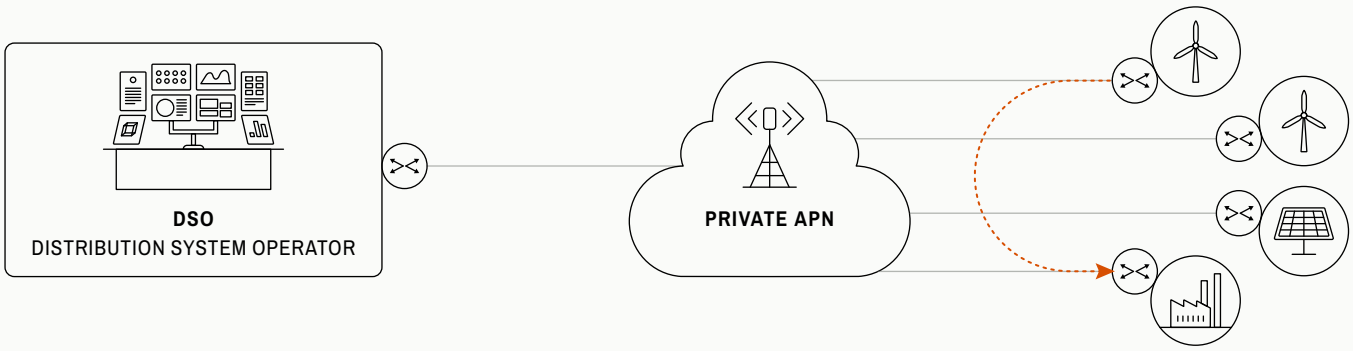
Leveraging the Private APN for Lateral Movement

Beginning on 18 December 2025, the attacker repeatedly scanned the private APN network in search of VNC and HTTP services, as well as the industrial protocols S7 and Modbus.

One of the devices discovered by the attacker within the private APN network was the WAGO PFC200 controller mentioned earlier. The controller exposed a web-based administration interface on its WAN interface, which was reachable from the APN network, and it was configured with the default credentials for the "admin" account. However, SSH was not enabled on the WAN interface in the device's default configuration. Based on logs obtained from the mobile network operator, it was determined that the attacker initially accessed the device through the web administration interface and subsequently used SSH, suggesting that the SSH service was likely enabled through the web interface. The correlation of timestamps from logs collected within the APN network and from the CHP plant's local network indicates that the attacker most likely used SSH tunneling to gain access to the plant's OT network.

The WAGO controller had connectivity to both the SCADA systems and network segments containing industrial devices responsible for controlling key operational processes at the CHP plant.

FIGURE 5. **Attack Path from the Wind Farm to the Combined Heat and Power Plant**



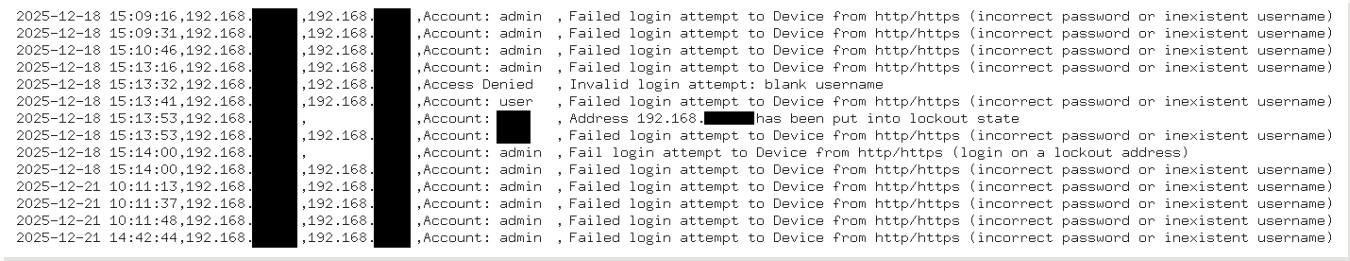
Reconnaissance of the CHP Plant Network

After gaining access to the CHP plant's network, the attacker conducted reconnaissance activities and efforts aimed at expanding their level of access between 18 and 25 December 2025.

Attempts to Access the Firewall

One of the first recorded activities involved attempts to gain access to the device serving as both a firewall and a VPN gateway through its web administration interface, which was accessible from the LAN. To achieve this, login attempts were made using the account names "admin", "user", and a specific username associated with the company responsible for deploying telecontrol systems at renewable energy facilities. These attempts were unsuccessful. The attacker repeated them three days later, but again without success.

FIGURE 6. **Unsuccessful login attempts against the device functioning as a firewall and a VPN gateway**



```
2025-12-18 15:09:16,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:09:31,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:10:46,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:13:16,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:13:32,192.168.[redacted],192.168.[redacted],Access Denied   , Invalid login attempt: blank username
2025-12-18 15:13:41,192.168.[redacted],192.168.[redacted],Account: user   , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:13:53,192.168.[redacted],[redacted],Account: [redacted]   , Address 192.168.[redacted]has been put into lockout state
2025-12-18 15:13:53,192.168.[redacted],192.168.[redacted],Account: [redacted]   , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-18 15:14:00,192.168.[redacted],[redacted],Account: admin  , Fail login attempt to Device from http/https (login on a lockout address)
2025-12-18 15:14:00,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-21 10:11:13,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-21 10:11:37,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-21 10:11:48,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
2025-12-21 14:42:44,192.168.[redacted],192.168.[redacted],Account: admin  , Failed login attempt to Device from http/https (incorrect password or inexistent username)
```

Network Scanning

Unable to gain access to the perimeter device, the attacker proceeded to scan the internal network. Among the services targeted during this activity were several commonly associated with industrial automation systems, including S7 (102/TCP), Modbus (502/TCP), CODESYS (11740/TCP), as well as video surveillance: RTSP (554/TCP). Other, more conventional targets included remote access services such as RDP and VNC, along with web services accessible over HTTP and HTTPS.

One noteworthy observation is that port scanning within one of the subnets began with the IP address assigned to the SCADA system. This suggests that the attacker may have identified high-value targets during an earlier reconnaissance phase. In another subnet, the scanning activity followed a more typical pattern, with connection attempts observed against all reachable addresses within the address range.

The scanning activity described above took place on 21 December, a Sunday, eight days before the attack.

Other Reconnaissance Activity

The following day, 22 December, the attacker continued reconnaissance activities. Network traffic logs show connections to ports on two hosts running

remote desktop services. These were most likely manual attempts to identify valid credentials; however, no evidence of a successful connection was found.

Three days later, on 25 December (Christmas Day), the attacker successfully established connections to three Siemens PLCs using the S7 protocol. The exact purpose of these activities could not be determined. The most likely explanation is that the attacker was conducting reconnaissance of the controllers in preparation for subsequent destructive actions.

Disruptive Actions at the CHP Plant

On 29 December 2025, the attacker leveraged the access previously obtained, as well as the knowledge gained during the reconnaissance phase, to disrupt the operation of PLCs and other industrial devices. On that day, the attacker's activity within the CHP plant network began at approximately 5:30 a.m. and continued until around 10:10 a.m. This indicates that the recovery activities undertaken by the affected entity at approximately 7:30 a.m. commenced while the attacker was still present in the network.

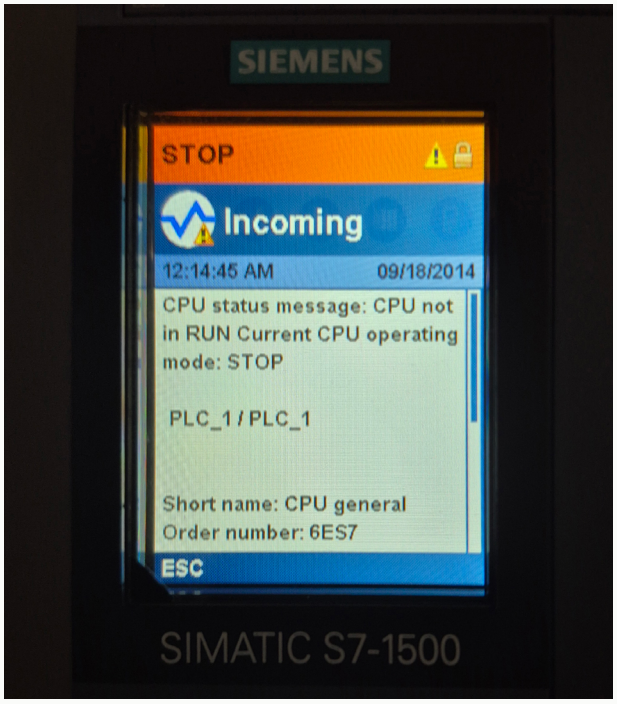
Based on the artifacts collected during the investigation, it was possible to reconstruct the approximate sequence of the attack.

Attack on Siemens PLCs

The attacker's first action within the CHP plant network after establishing a tunnel through the WAGO controller was to connect to the SCADA server's web interface and, shortly thereafter, to a Siemens S7-300 PLC using the S7 protocol. The same sequence of actions was then repeated against additional controllers – an S7-1200 and an S7-1500. Throughout this period, further interactions with the SCADA interface were also observed.

According to statements provided by CHP plant personnel, the PLCs were switched to STOP mode and protected with a password that prevented changes to their operating state and modification of the control logic. As a result, the steam turbine and the water treatment system used to produce process water were shut down, leading to an interruption of the cogeneration process. As part of the recovery efforts, the operators restored the affected devices to their factory settings and reloaded the available backups of the controllers' logic. This approach helped reduce the duration of the outage but also resulted in the deletion of logs stored on the controllers. Siemens ProductCERT confirmed the logs could not be recovered.

FIGURE 7. **Siemens S7-1500 PLC shortly after the attack**



Attack on Moxa Devices

The attacker also made configuration changes to seven Moxa serial device servers and three Moxa network switches. These actions were consistent with those previously observed at the renewable energy facilities. The devices were restored to their factory settings, the login password was changed, and the IP addresses assigned to the devices were modified to unreachable values, such as 127.0.0.1. As a result, the devices became inaccessible, while the changes to the password and IP configuration were intended to delay recovery efforts. Based on the timing of the HTTP requests sent to each device during the attack, it can be concluded with a high degree of confidence that these actions were automated.

Attacks Against Other Devices

During the attack, connections to the web administration interfaces of two ABB ACS series variable frequency drives were also observed. It was not possible to determine what actions, if any, were performed by the attacker on these devices.

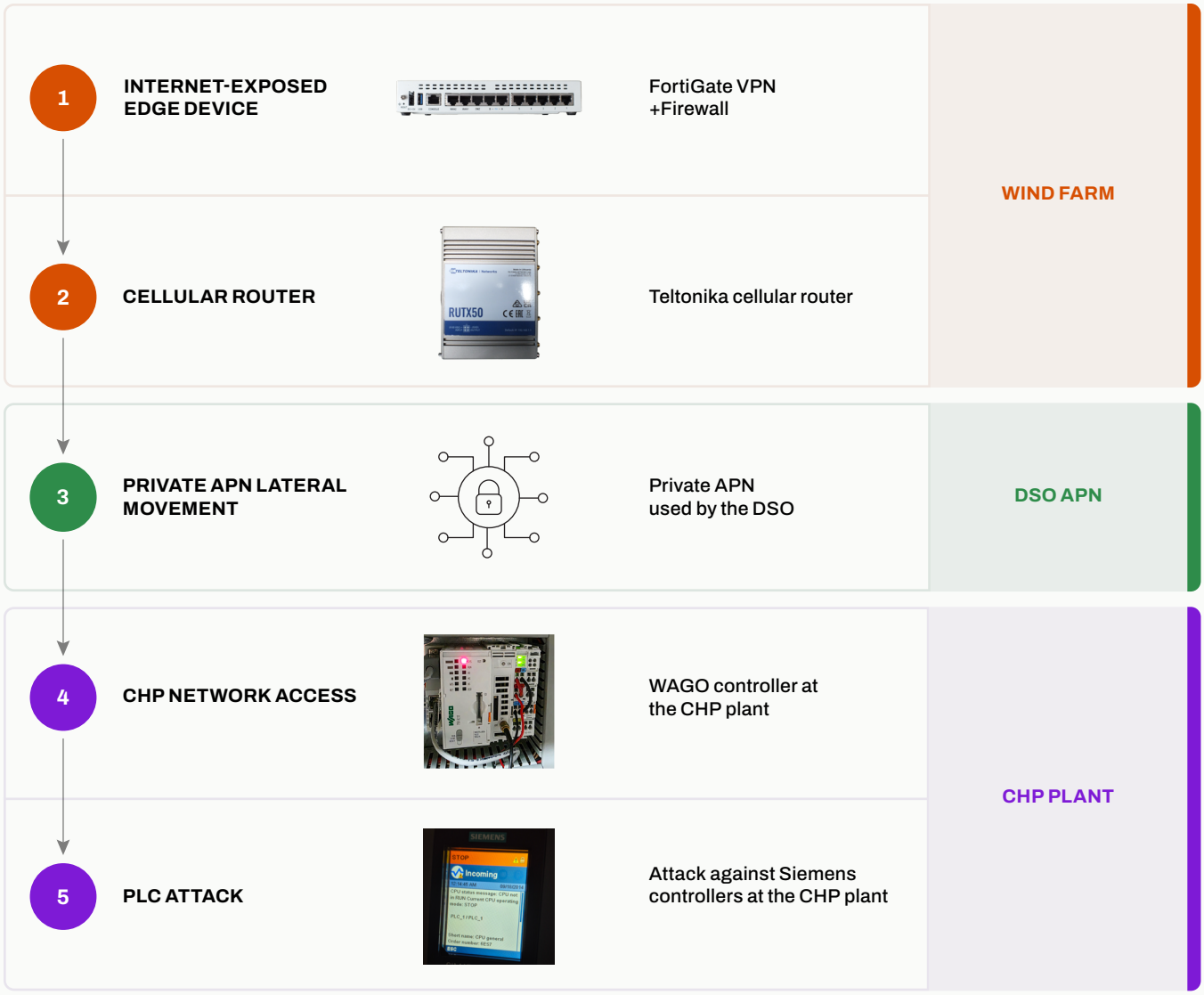
Network traffic logs also revealed unsuccessful attempts to connect to Schneider Electric ATV6xx variable frequency drives. The failure was most likely the result of incomplete reconnaissance, as the attacker attempted to connect to port 80/TCP while the devices' web administration interfaces were listening on a different port.

Full Attack Sequence

To better illustrate the progression of the incident, a summary of the successive actions performed by the attacker is provided below.

1. Access to a perimeter device at a wind farm was obtained, and a remote VPN connection was established.
2. A Teltonika RUTX50 cellular router was identified within the wind farm network.
3. The router's web administration interface was accessed, followed by login to the SSH service running on the device.
4. The SSH service was used to establish a tunnel enabling communication with the private APN network.
5. The private APN network was scanned.
6. A WAGO PFC200 controller exposing a web administration interface via its WAN interface was identified.
7. Default credentials were used to gain administrative access to the web interface.
8. The SSH service was enabled on the WAN interface of the WAGO PFC200 device.
9. The SSH service was used to establish a tunnel providing access to the CHP plant's OT network.
10. Reconnaissance of the CHP plant's OT network was conducted over the course of a week.
11. Disruptive actions were carried out, resulting in the shutdown of the steam turbine and the water treatment system used to produce process water, leading to an interruption of the cogeneration process.

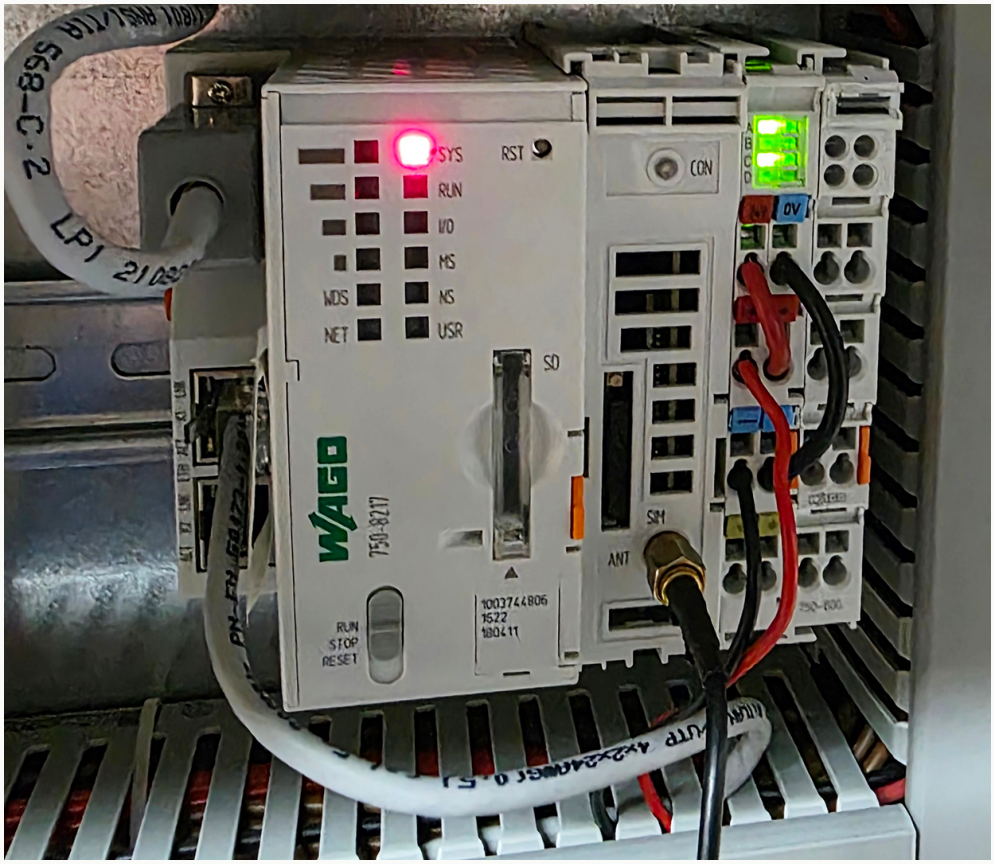
FIGURE 8. **Illustrative diagram of the attack against the CHP plant leveraging a private APN**



Covering Tracks

The attacker's activity within the CHP plant network lasted for nearly five hours and concluded with access to the SCADA system's web administration interface, most likely to assess the impact of the actions carried out. The attacker then damaged the WAGO controller that had been used as a gateway into the network by corrupting its partition table, preventing it from being read by the device. In an attempt to restore the controller, the affected entity performed a factory reset; however, this did not repair the partition table and the device remained unable to boot. No valuable logs could be recovered from the device during the investigation.

FIGURE 9. **WAGO PFC200 controller after the attack**



The attacker subsequently continued operations within the wind farm environment. The Teltonika RUTX50 cellular router that had been used to establish SSH tunnels was restored to its factory settings* approximately 30 minutes after the last observed activity in the CHP plant network. The attacker then changed the administrator password and set the device's IP address to an unreachable value, 127.0.0.1, likely to impede its reconfiguration.

As the final observed action, the attacker restored the FortiGate device serving as both the VPN concentrator and firewall to its factory settings. This device had been used as the initial entry point into the wind farm network. Given the model of the device and its configuration, this action resulted in the loss of logs.

* In RutOS versions earlier than 7.07, the event database was retained in the device's storage even after a factory reset for diagnostic purposes. This made it possible to recover logs from the device during the investigation.

Summary

To the best of our knowledge, the incident described in this report, which involved gaining access to an OT network through a private APN, was the first observed instance of this attack vector being used in a real-world cyberattack. Its execution was made possible, among other factors, by a misconfiguration that allowed connections to be established between arbitrary devices within the private APN network. Based on surveys conducted with multiple entities using this type of solution, it was determined that such a configuration was commonly encountered in Poland at the time the surveys were carried out. To the best of our knowledge, similar configurations are also widely deployed in other countries around the world.

CERT Polska recommends that entities using solutions based on private APNs:

- Conduct an audit of their private APN configuration. In particular, enabling client isolation between end devices connected to the APN is recommended. Where such communication is required, a risk assessment should be performed that considers the possibility of a device directly connected to the private APN being compromised and subsequently used to communicate with other devices on the network.

- Treat the private APN as an untrusted network in relation to the OT environment. On the OT side, connectivity to the private APN should be subject to network segmentation and traffic controls at least equivalent to those applied to corporate WAN connections. If the network remains outside the organization's control, particularly where the organization has no influence over its configuration and lacks the information necessary to verify the security mechanisms in place, it should be treated as an external network with a trust level equivalent to that of the Internet.

- Strictly limit communications between the OT network and the device acting as the gateway to the private APN. Only connections required to support defined business and technical functions should be permitted, using allowlist-based rules.

- Monitor traffic between the OT network and the private APN, with particular attention paid to deviations from the defined communication profile expected for the connection.

- Implement centralized logging and monitoring of events generated by devices serving as gateways to the private APN, where such functionality is supported.
- Minimize the number of open ports accessible via interfaces reachable from the private APN. In particular, administrative services such as web management interfaces, SSH, or Telnet should not be exposed.
- Change default credentials for all services available on devices connected to the private APN, especially administrative services.
- Include private APNs and the devices providing access to them within the scope of penetration tests, red team exercises, and security architecture reviews.

CERT.PL
NASK

Ministry of Digital Affairs
Republic of Poland