

◆ CASE STUDY · POLAND · 29 DECEMBER 2025

When “isolated” isn’t isolated.

How attackers crossed a shared private cellular network (APN) to stop a heat and power plant, and the six controls that close the gap.

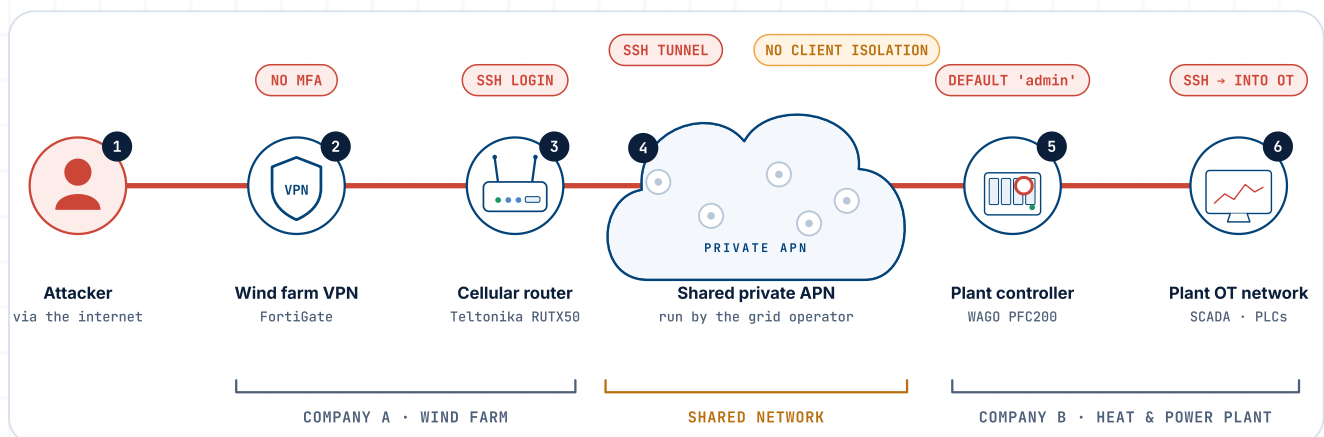


FIG 0 The attack path, from the internet to the plant’s OT network, across a private APN run by the grid operator.

◆ IN THIS BRIEF

01-02

Why remote sites are not really isolated

03

How the attack propagated, step by step

04-05

Timeline and impact on the plant

06-08

Root causes, six controls, self-check

≈30

renewable energy sites, a large and a smaller combined heat and power plant hit on one day

50,000

residents heated by the plant reached through the private APN

1st

real-world attack seen using a private APN to reach an OT network

◆ AT A GLANCE

A network that felt private, and a **direct line into OT.**

On 29 December 2025, a coordinated, destructive cyberattack hit Poland's energy sector. At one heat and power plant, the attackers did not come through the corporate network. They came over the mobile network: through a private APN that the local grid operator shared with many energy sites.

DATE	29 December 2025, early morning. Reconnaissance from 18 December.
SECTOR	Energy: around 30 wind and solar sites, a large combined heat and power (CHP) plant, and a smaller CHP plant.
ENTRY POINT	An internet-facing VPN at a wind farm, without multi-factor authentication.
ROUTE	Wind farm cellular router → shared private APN → controller at the CHP plant → plant OT network.
IMPACT	PLCs stopped and password-locked. Steam turbine and water treatment shut down; heat and power production stopped.
RECOVERY	Service restored within hours, before residents lost heat.
ATTRIBUTION	The investigation suggested an attack from an adversary country.
SOURCE	CERT Polska follow-up report (August 2026) and public reporting.

◆ THE KEY POINT

An APN, public or private, is a transport network. It is **not a security boundary.**

Why this matters to you

Most remote OT sites, from substations to pumping stations and wellheads, rely on a cellular router for telemetry, maintenance or vendor access. If that router shares a network with other sites, and sits on the same network as your PLCs, your "air gap" is a single misconfiguration away from the internet.

At first, the plant thought the outage was a contractor's mistake. **Report unexplained failures, not only confirmed incidents.**

01 • THE CONCEPT

The air gap that quietly disappears.

Substations, wind farms, pumping stations, pipelines and wellheads often sit far from the corporate network, with no fibre at all. So people assume nothing outside can reach them.

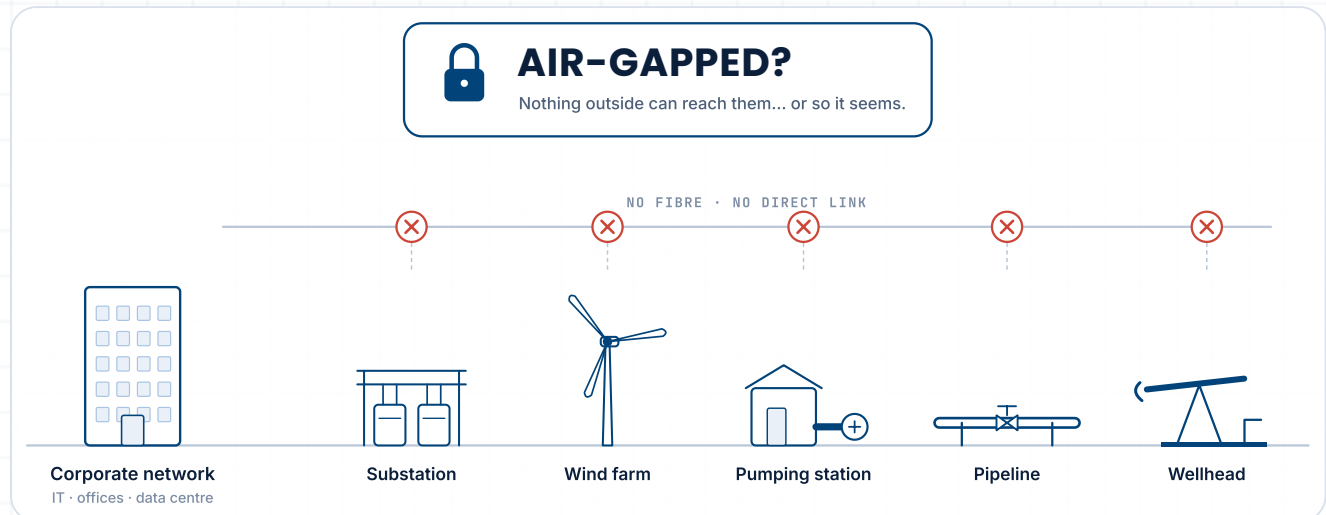


FIG 1 Remote sites with no wired link to the corporate network are often assumed to be air-gapped.

In practice, most of these sites have a **cellular router or modem**, for telemetry, remote maintenance or vendor support. That router joins the mobile network through an **APN (Access Point Name)**. The APN decides which data network the device joins, and who else is on it.

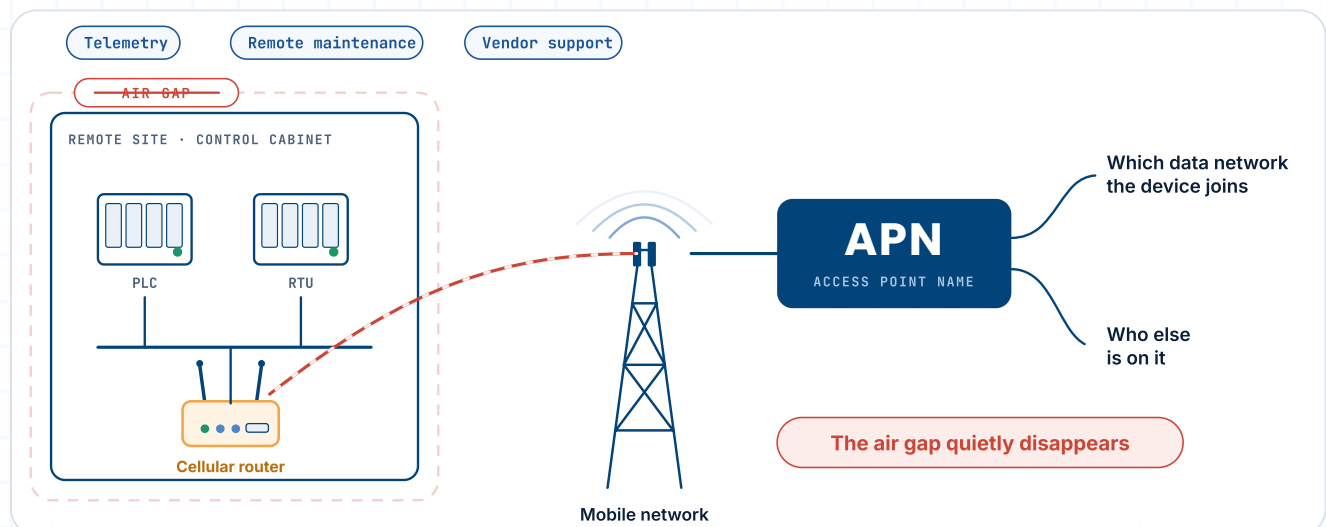


FIG 2 A cellular router in the control cabinet joins a data network through the APN. The air gap no longer exists.

02 • PUBLIC AND PRIVATE APNS

Private is not the same as isolated.

Public APN

Shared with thousands of unknown SIM cards: phones, trackers and other companies' equipment.

Private APN

Keeps outsiders out, but is still one shared network linking every site that uses it. Without client isolation, it is one flat network.

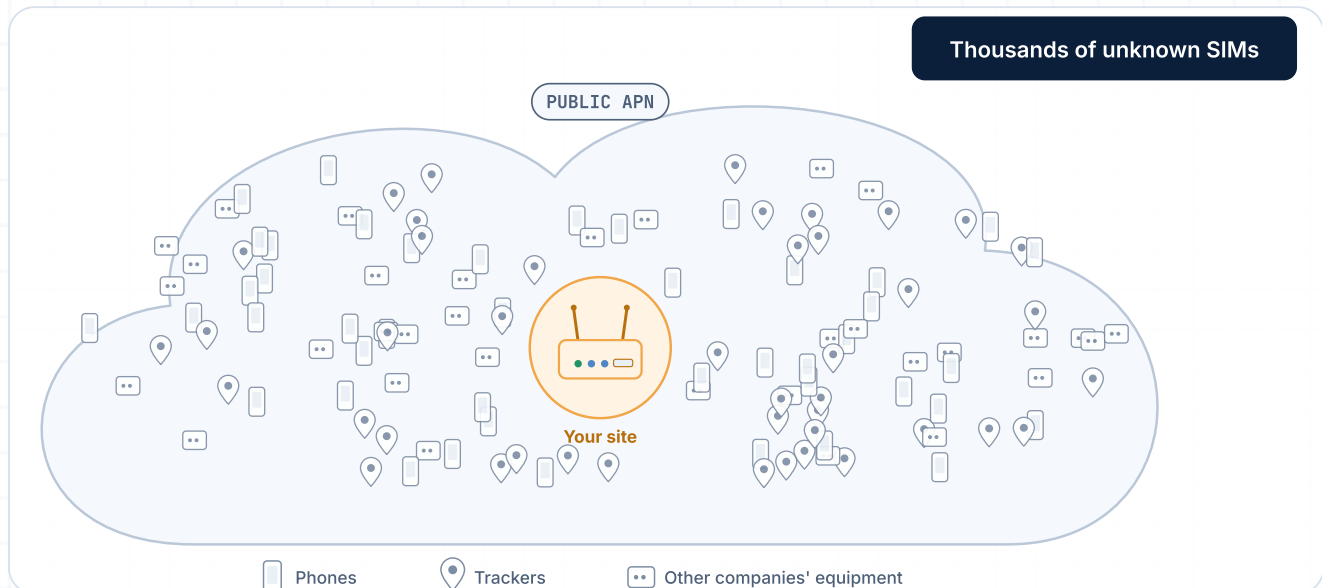


FIG 3 A public APN: your site's router shares a network with devices you do not know or control.

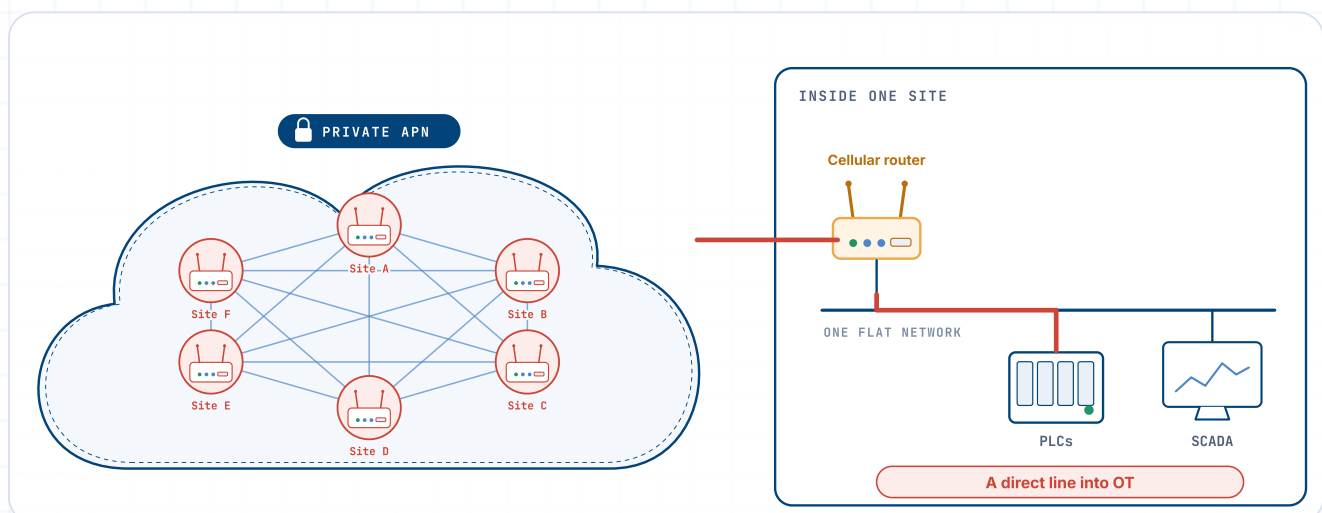


FIG 4 A private APN without client isolation: a weakness at one site reaches every other site, and, through a router on the same LAN as the PLCs, the OT network itself.

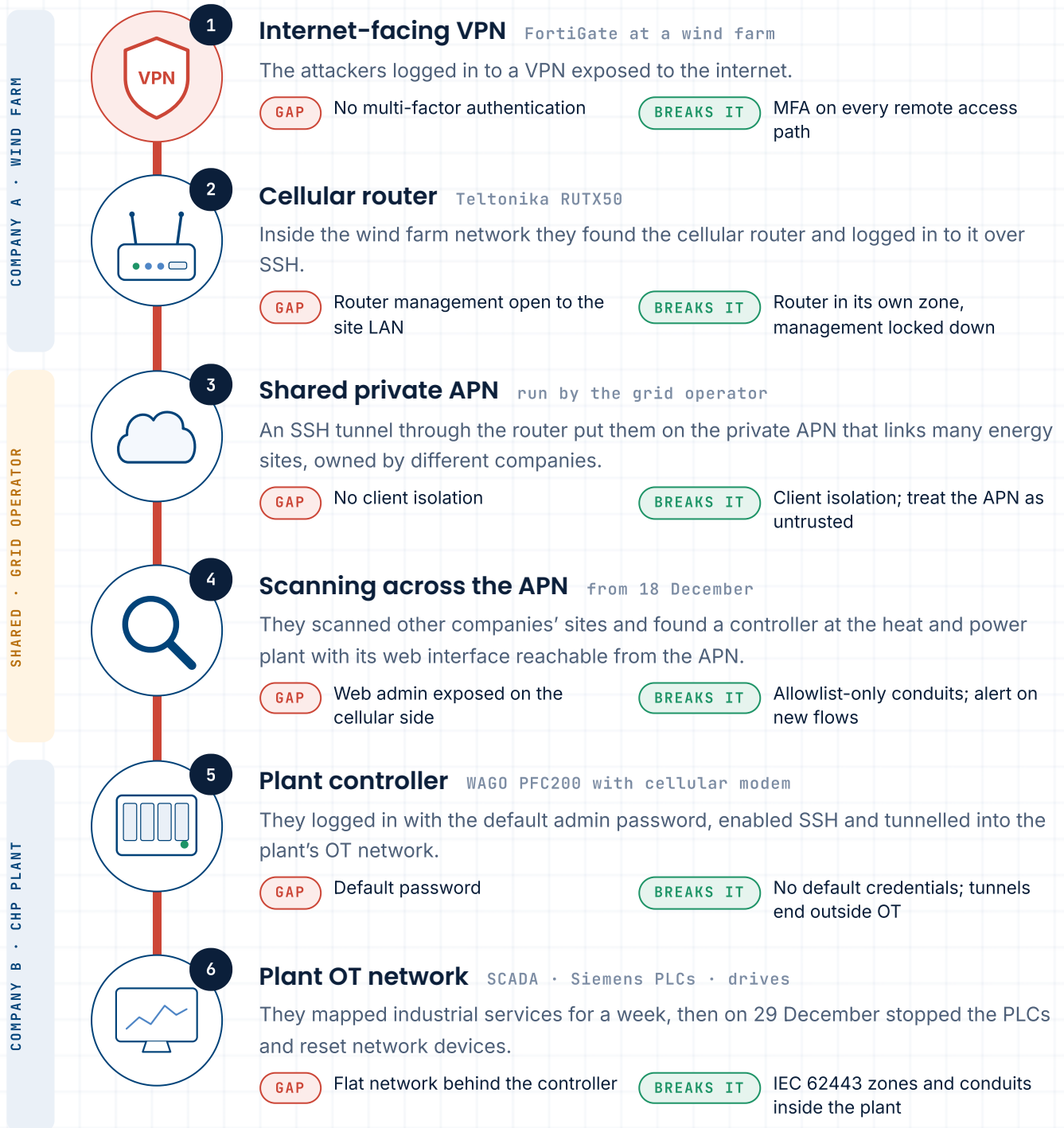
REMEMBER

Treat every APN as untrusted, the same as the internet.

03 • HOW THE ATTACK PROPAGATED

Six steps from the internet to the plant floor.

Each step crossed a boundary that someone assumed was safe. Each one could have been broken by a single, well-understood control.



04 • TIMELINE

Eleven days, mostly unseen.

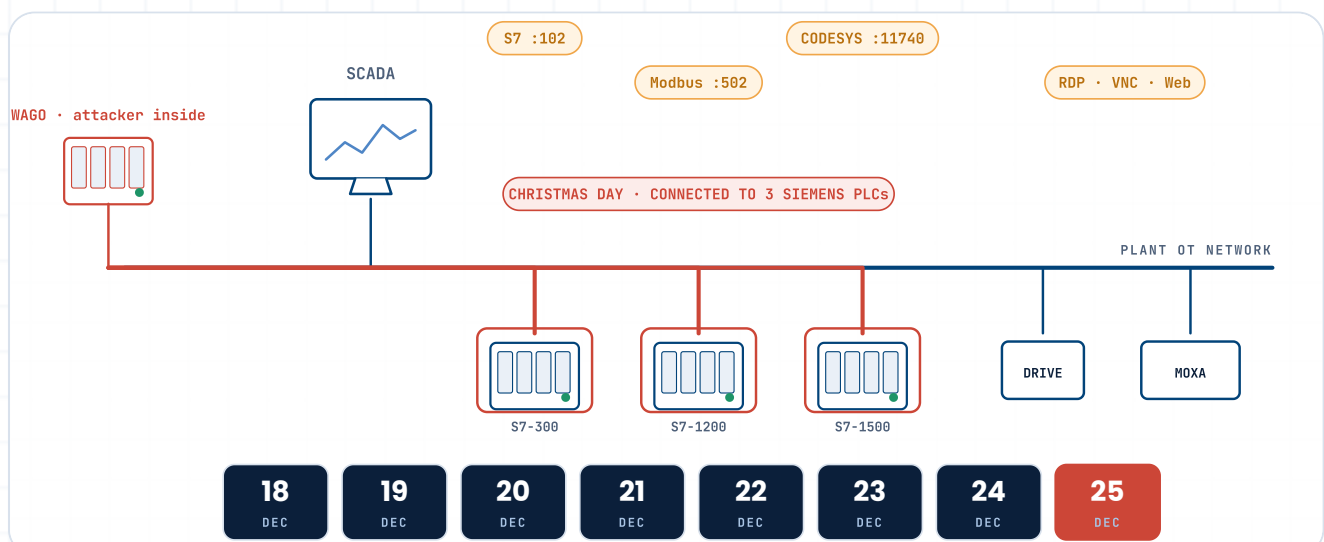
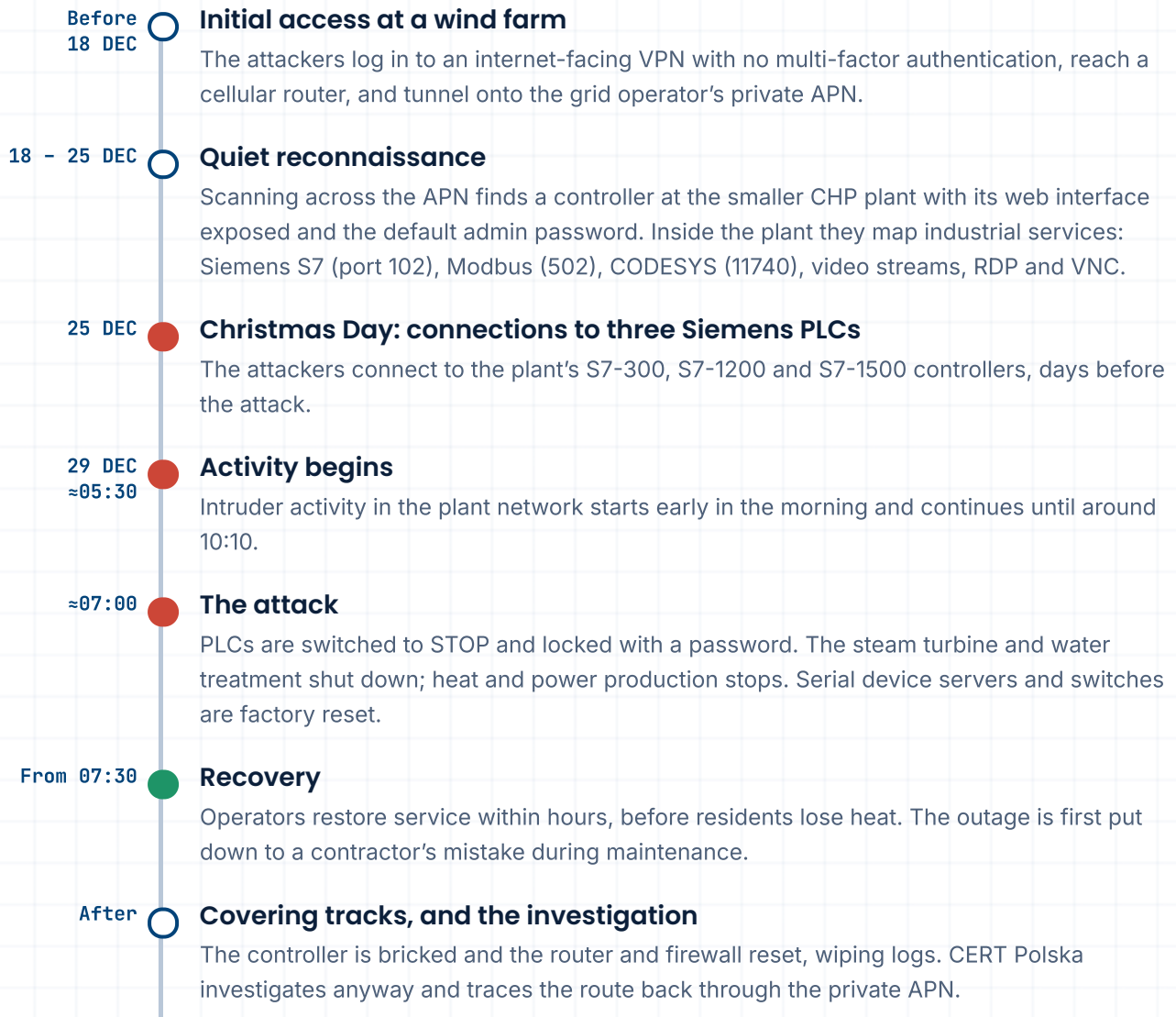


FIG 5 Inside the plant: reconnaissance from the compromised controller, then connections to three PLCs on Christmas Day.

◆ 05 • IMPACT

Stop the process, **then slow the recovery.**

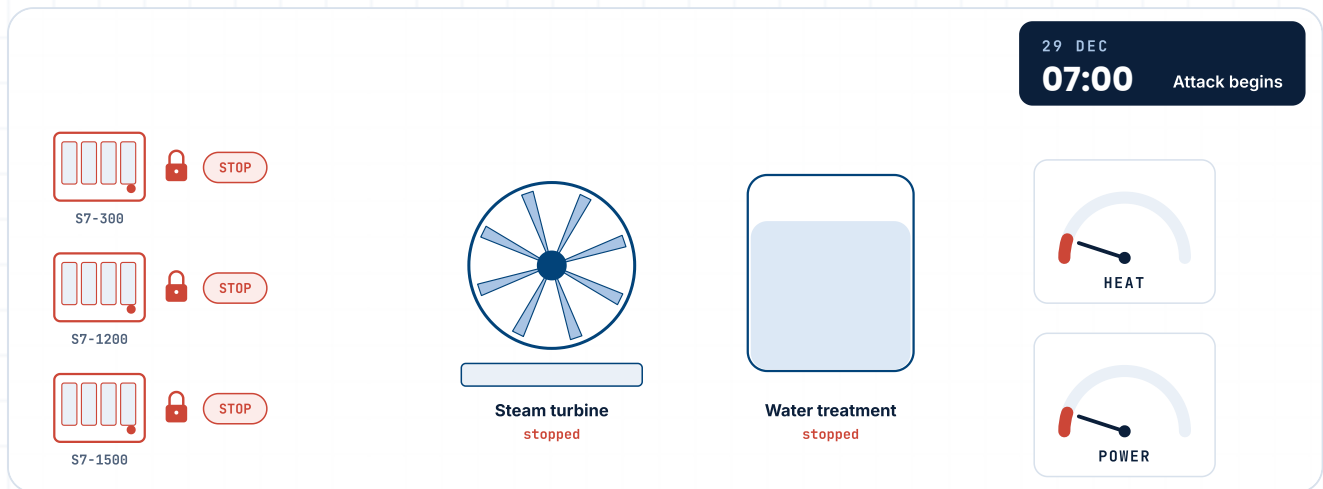


FIG 6 29 December, around 07:00: PLCs set to STOP and locked; the steam turbine and water treatment stop; heat and power output falls.

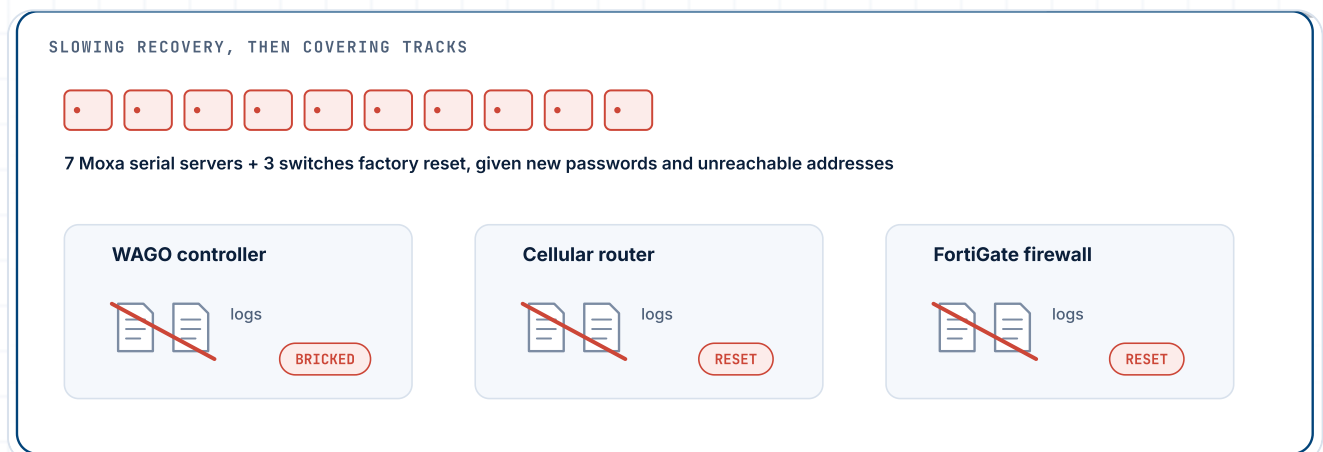


FIG 7 Devices reset to slow recovery, then evidence destroyed on the way out.

PROCESS

- ◆ Siemens S7-300, S7-1200 and S7-1500 PLCs set to STOP and password-locked
- ◆ Steam turbine and water treatment shut down
- ◆ Variable-speed drives accessed

RECOVERY AND EVIDENCE

- ◆ 7 serial device servers and 3 switches factory reset, left unreachable
- ◆ The plant controller bricked
- ◆ Cellular router and firewall reset, wiping their logs

◆ 06 • ROOT CAUSES

Four gaps, all preventable.

01

Remote access exposed to the internet

...without multi-factor authentication.

02

Default passwords left on devices

...including a controller reachable from the APN.

03

No isolation between devices on the APN

...so sites of different companies could reach each other.

04

Weak separation between APN and OT

...the cellular link led straight into the plant network.

◆ 07 • SIX CONTROLS THAT CLOSE THE GAP

01

Treat the APN as untrusted

Public or private, handle every APN like the internet: nothing on it is trusted by default.

02

Isolate devices on the APN

Ask your carrier or grid operator for client isolation, so connected sites cannot reach each other.

03

Segment the site

Put the cellular router in its own zone, with allowlist-only rules into OT, following IEC 62443 zones and conduits.

04

Harden remote access

Require MFA on every VPN and remote session, and remove default passwords from every device.

05

Encrypt the link

Run an IPsec or VPN tunnel end to end over the cellular link, terminating outside the OT zone.

06

Monitor and test

Alert on new devices and traffic flows, and include APNs and cellular routers in penetration tests.

◆ CERT POLSKA'S MAIN RECOMMENDATION

Treat the private APN as an untrusted network, the same as the internet.

◆ 08 • QUICK SELF-CHECK

Could this path exist **in your plant?**

If you tick any of these, your cellular links need review.

☐

Devices on our APN, public or private, can reach each other.

[REVIEW](#)☐

There is no encrypted tunnel over the cellular link.

[REVIEW](#)☐

The cellular router sits on the same network as the PLCs.

[REVIEW](#)☐

Remote access works without MFA, or default passwords remain.

[REVIEW](#)☐

No one can say who last reviewed the router's configuration.

[REVIEW](#)

◆ THE LESSON

Audit the path, **not just the perimeter.**

Cellular and APN path review

Every remote link mapped, tested and owned.

Remote access hardening

MFA, brokered vendor access, no default credentials.

Zones and conduits design

IEC 62443 segmentation that holds under pressure.

OT monitoring and testing

Alerts on new devices and flows; APNs in scope.