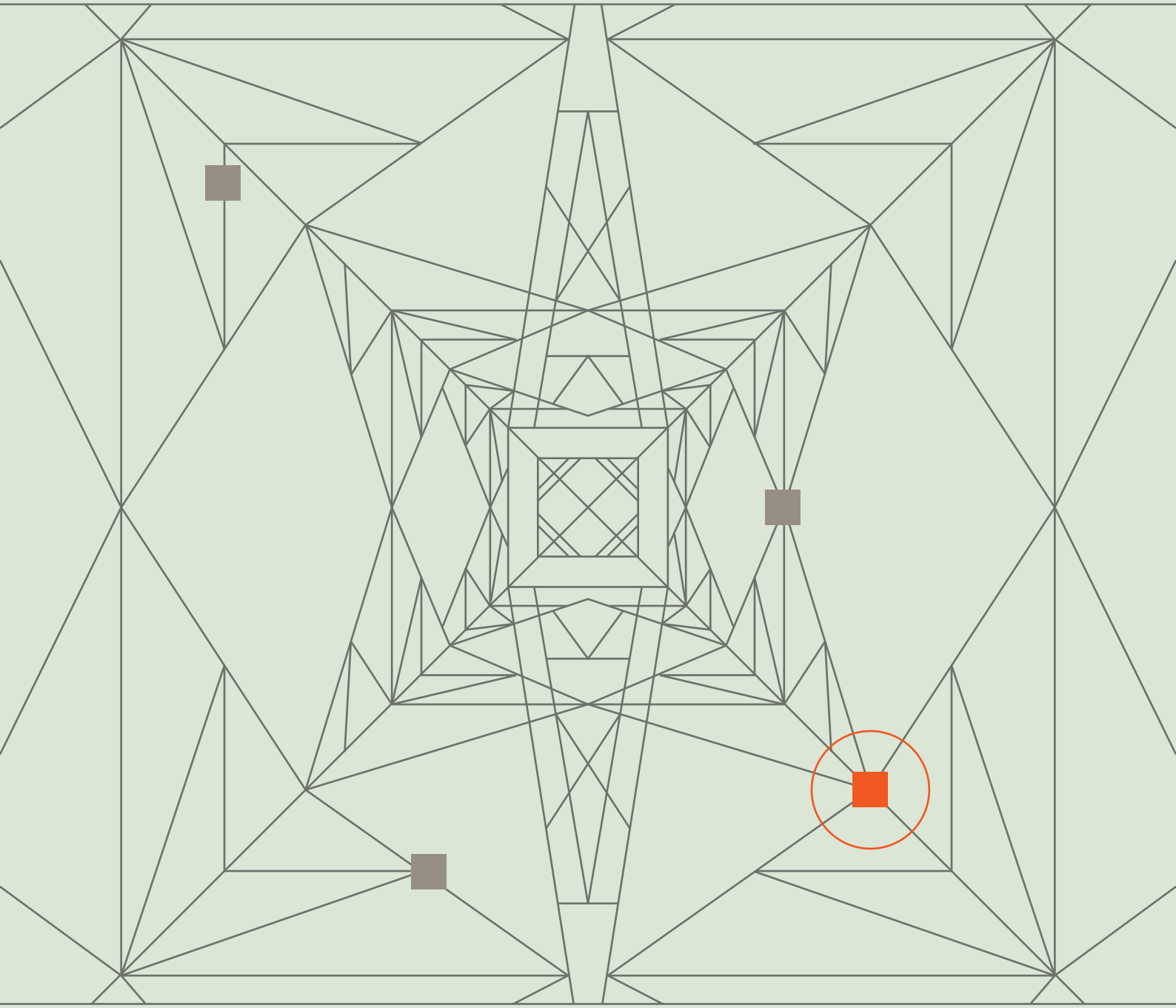
Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025



CERT.PL NASK

Ministerstwo Cyfryzacji

Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025

CERT.PL NASK

Ministerstwo Cyfryzacji

Autor raportu

CERT Polska

Zespół działający w strukturach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, jednego z trzech takich zespołów działających na poziomie krajowym w ramach Krajowego Systemu Cyberbezpieczeństwa.

Spis treści

Wstęp

29 grudnia 2025 roku doszło do skoordynowanych ataków na sektor energii w Polsce, m.in. na 30 obiektów wykorzystujących odnawialne źródła energii oraz na dużą elektrociepłownię. Opisaliśmy te ataki szczegółowo w raporcie opublikowanym 30 stycznia 2026 roku*. W tym samym czasie miał miejsce jeszcze jeden incydent – w mniejszej elektrociepłowni dostarczającej ciepło dla 50 tys. mieszkańców. Analiza tego zdarzenia zajęła ponad trzy miesiące i z tego powodu nie zostało ono opisane we wskazanym raporcie. Wektor ataku wykorzystany w tym przypadku nie był, według naszej wiedzy, dotychczas obserwowany w znanych incydentach.

* https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/

Atak na drugą elektrociepłownię

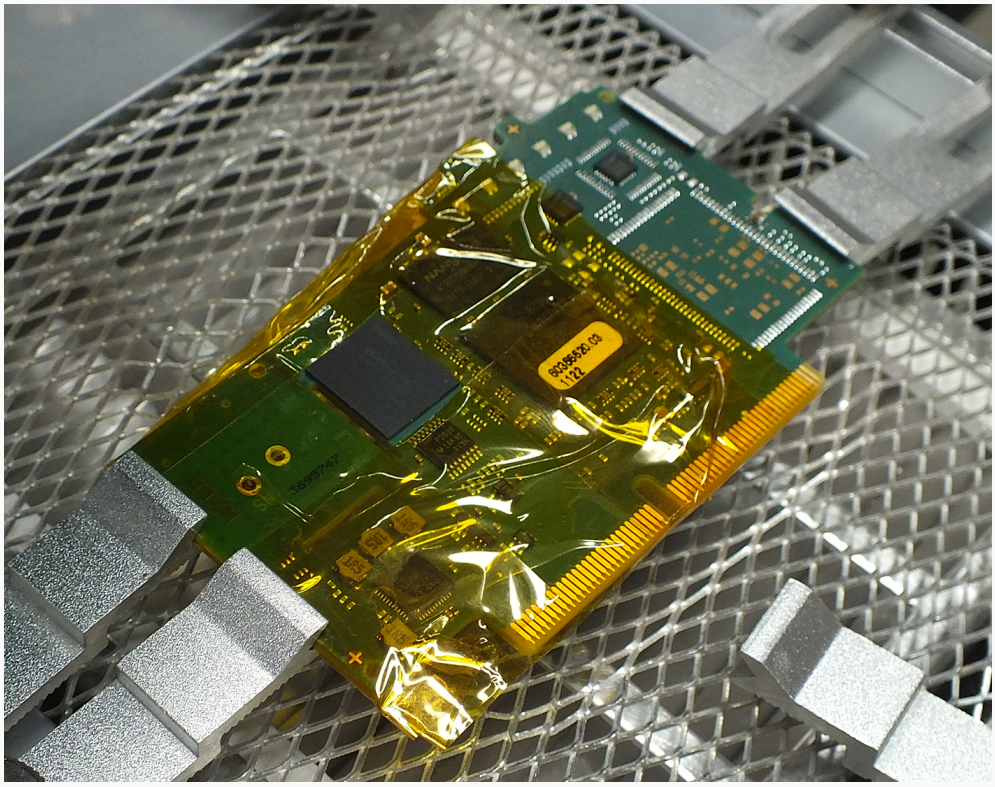
29 grudnia około godziny 7:00 doszło do ataku na systemy automatyki elektrociepłowni dostarczającej ciepło około 50 tys. mieszkańców. W wyniku ataku doszło do zatrzymania turbiny parowej oraz stacji uzdatniania wody do celów technicznych, co doprowadziło do przerwania procesu kogeneracji. Dzięki szybkiej reakcji obsługi elektrociepłowni incydent spowodował jedynie krótkotrwały przestój instalacji i nie doprowadził do przerw w dostawach ciepła do odbiorców.

W związku z pracami utrzymaniowymi prowadzonymi na obiekcie podmiot zakładał, że do zatrzymania procesu doprowadził błąd inżynierów podwykonawcy, i zgłosił zdarzenie wyłącznie informacyjnie. Jednak CERT Polska, mając wiedzę o innych podobnych zdarzeniach, podjął obsługę incydentu w kierunku ataku, a dalsza analiza potwierdziła tę hipotezę. To pokazuje, jak ważne jest zgłaszanie nie tylko potwierdzonych incydentów, lecz także niewyjaśnionych awarii.

Na podstawie dalszej szczegółowej analizy pozyskanych logów udało się wytypować urządzenie, z którego atakujący prowadził działania – był to sterownik WAGO PFC200 z wbudowanym modemem komórkowym. Niestety urządzenie zostało uszkodzone i nie udało się odzyskać z niego danych pomimo analizy w laboratorium.

RYS. 1

Przygotowanie do wylutowania pamięci z urządzenia WAGO PFC200 w laboratorium CERT Polska



Ataki na sieć przemysłową inicjowane bezpośrednio ze sterownika PLC nie należą do typowych scenariuszy obserwowanych w środowiskach OT. Z racji braku logów podjęliśmy się analizy na podstawie hipotez – pierwszą było omyłkowe wystawienie urządzenia do internetu. Jednak analiza obecności tego typu urządzeń w polskiej adresacji IP w tym okresie wykluczyła przypadkowe udostępnienie urządzenia w internecie. Natomiast pozyskaliśmy informację, że urządzenie to służyło do komunikacji z systemami operatora sieci dystrybucyjnej (OSD) i miało kartę SIM działającą w wydzielonej, prywatnej sieci transmisji danych (prywatny APN), obsługiwanej przez OSD.

To odkrycie doprowadziło nas do żmudnej analizy, która pozwoliła ustalić przebieg ataku. W tym raporcie prezentujemy analizę w formule chronologicznej, natomiast faktyczna praca analityków była prowadzona w kolejności odwrotnej.

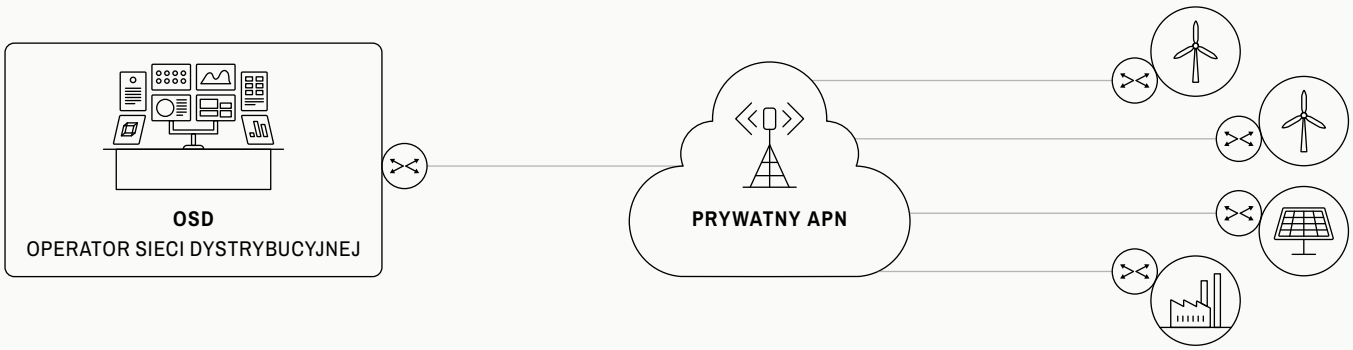
Aktywność na farmie wiatrowej

Aby zrozumieć przebieg ataku na elektrociepłownię, trzeba najpierw przypomnieć, jak przebiegały ataki na farmy wiatrowe, opisane przez nas w pierwszym raporcie. Atakiem objętych zostało ponad 30 stacji elektroenergetycznych GPO. Jest to miejsce, w którym obiekt OZE jest połączony z siecią dystrybucyjną i jej operatorem.

W każdej zaatakowanej stacji przy farmie wiatrowej było obecne urządzenie Fortigate pełniące funkcję koncentratora VPN oraz Firewalla. W każdym przypadku interfejs VPN był dostępny z sieci internet i umożliwiał logowanie na zdefiniowane w konfiguracji konta bez wieloskładnikowego uwierzytelniania. Sieci badanych obiektów często posiadały wydzielone podsieci VLAN, ale atakujący w momencie ataku posiadał uprawnienia administratora urządzenia, co prawdopodobnie zostało użyte do pozyskania poświadczeń konta VPN, które miało uprawnienia dostępowe do wszystkich podsieci.

Na stacjach – w celu zapewnienia komunikacji zapasowej lub rzadziej podstawowej – montowane są routery komórkowe. Routery te posiadają kartę SIM umożliwiającą połączenie z prywatnym APN obsługiwanym przez OSD. W ramach prywatnego APN prowadzona jest komunikacja pomiędzy systemem SCADA a sterownikiem RTU na obiekcie.

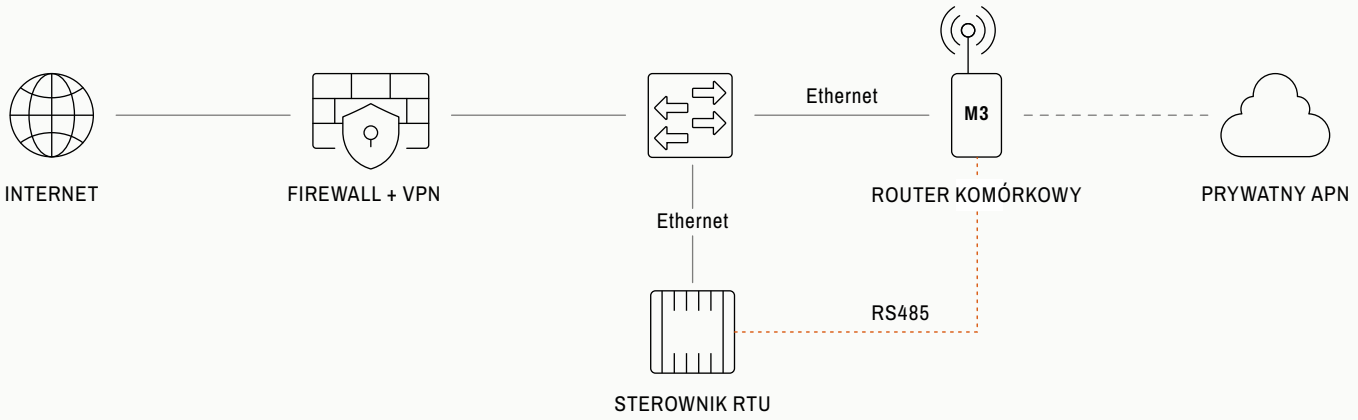
RYS. 2 **Poglądowe wykorzystanie prywatnego APN w energetyce rozproszonej**



Ważnym aspektem jest to, że OSD wymagają, aby wszelka komunikacja pomiędzy siecią teleinformatyczną OSD a sterownikiem RTU odbywała się za pomocą protokołu szeregowego, w tym wypadku DNP3.0.

W obiekcie, który został zaatakowany, wykorzystywano router Teltonika RUTX50 i wymagania OSD zostały uwzględnione. Natomiast nie było wymagań co do tego, w jaki sposób powinien być traktowany interfejs administracyjny routera komórkowego. Spowodowało to, że router komórkowy miał skonfigurowane dwa fizyczne interfejsy – łącze szeregowe podłączone do sterownika RTU oraz drugi, Ethernet wpięty do VLAN-u zarządzanego przez centralny Firewall, który został przejęty przez atakującego.

RYS. 3 **Umiejscowienie routera komórkowego we fragmencie sieci farmy wiatrowej**



W domyślnych ustawieniach wykorzystany router udostępnia na interfejsie LAN panel WWW oraz usługę SSH. Przy pierwszym logowaniu wymuszona jest zmiana domyślnego hasła, co zostało zrobione przez firmę wdrażającą system. Nie udało się ustalić, w jaki sposób atakujący pozyskał nowe hasło lub czy wykorzystano jakąś podatność w urządzeniu Teltonika.

Dzięki analizie urządzenia przeprowadzonej w laboratorium z pamięci trwałej udało się odzyskać bazę w formacie SQLite, zawierającą wybrane zdarzenia na urządzeniu, w tym logowania do panelu WWW oraz poprzez SSH.

RYS. 4 **Odzyskane logi wskazujące udane logowania do usługi SSH na routerze komórkowym Teltonika**

```
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
```

Atakujący w grudniu wielokrotnie logował się do routera z wykorzystaniem protokołu SSH. Na podstawie logów uzyskanych od operatora komórkowego udało się ustalić, że najprawdopodobniej atakujący wykorzystywał tunelowanie SSH w celu uzyskania dostępu do sieci prywatnego APN.

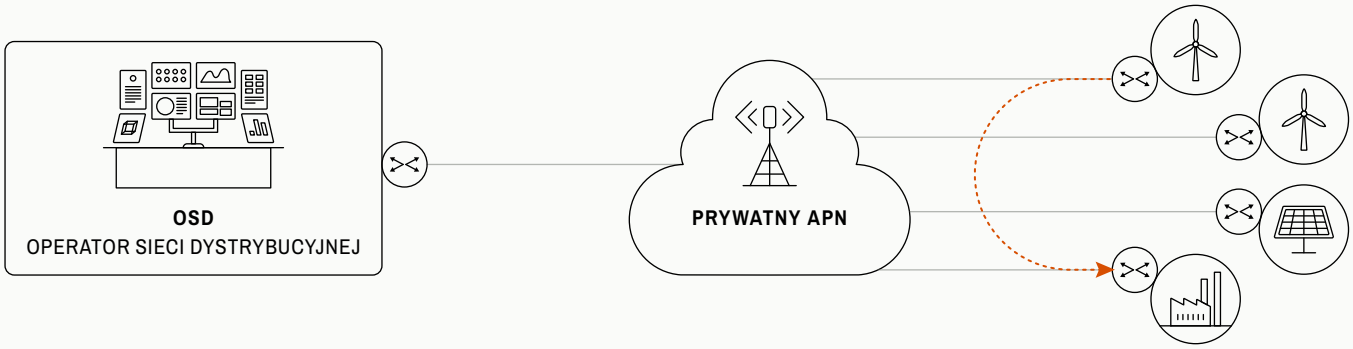
Wykorzystanie prywatnego APN do eskalacji

Od 18 grudnia 2025 roku atakujący kilkukrotnie skanował sieć prywatnego APN w poszukiwaniu usług VNC oraz HTTP, a także protokołów przemysłowych S7 i Modbus.

Jednym z urządzeń, które atakujący odnalazł w sieci prywatnego APN, był wspomniany wcześniej sterownik WAGO PFC200. Sterownik ten posiadał panel administracyjny WWW udostępniony na interfejsie WAN – dostępnym z sieci APN – i wykorzystywał domyślne poświadczenia dla konta „admin". Natomiast urządzenie to nie udostępnia w domyślnej konfiguracji usługi SSH na interfejsie WAN. Na podstawie logów od operatora komórkowego udało się ustalić, że atakujący w pierwszej kolejności korzystał z panelu WWW, a w dalszej kolejności z protokołu SSH – prawdopodobnie usługa ta została włączona z wykorzystaniem panelu webowego. Na podstawie przebiegów czasowych posiadanych logów z sieci APN oraz z sieci lokalnej elektrociepłowni stwierdzamy, że atakujący najprawdopodobniej wykorzystywał tunelowanie SSH w celu uzyskania dostępu do sieci OT elektrociepłowni.

Sterownik WAGO posiadał dostęp zarówno do systemów SCADA, jak i do segmentów sieci z urządzeniami przemysłowymi odpowiedzialnymi za sterowanie kluczowymi procesami technologicznymi.

RYS. 5 **Ścieżka ataku z farmy wiatrowej do elektrociepłowni**



Rekonesans sieci elektrociepłowni

Atakujący po uzyskaniu dostępu do sieci elektrociepłowni prowadził w okresie od 18 do 25 grudnia 2025 roku działania rozpoznawcze i mające na celu poszerzenie posiadanych dostępów.

Próby uzyskania dostępu do Firewalla

Jedną z pierwszych odnotowanych aktywności były próby uzyskania dostępu do urządzenia pełniącego funkcję Firewalla oraz bramy VPN na panel WWW dostępny z sieci LAN. W tym celu podjęto próby logowania z wykorzystaniem kont „admin", „user" oraz specyficznej nazwy użytkownika powiązanej z firmą wdrażającą telemechanikę w obiektach OZE. Próby te zakończyły się niepowodzeniem, atakujący ponowił je trzy dni później, ale też bezskutecznie.

RYS. 6

Nieudane próby logowania do urządzenia pełniącego funkcję Firewalla oraz bramy VPN

```
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],[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],[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)
```

Skanowanie sieci

Atakujący nie mógł uzyskać dostępu do urządzenia brzegowego, więc rozpoczął skanowanie sieci wewnętrznej. Wśród usług, które były poszukiwane, znajdują się usługi związane z systemami automatyki przemysłowej: S7 (102/TCP), Modbus (502/TCP), CODESYS (11740/TCP) oraz monitoringu: RTSP (554/TCP). Innymi, bardziej typowymi usługami były usługi zdalnego pulpitu (RDP, VNC) i webowe (HTTP, HTTPS).

Ciekawym faktem jest, że skanowanie portów w jednej z podsieci rozpoczęto od adresu maszyny z systemem SCADA. Najprawdopodobniej atakujący mógł wytypować wartościowe cele podczas poprzedniej fazy rekonesansu. Dla kolejnej z podsieci skanowanie portów miało bardziej typowy przebieg – widoczne są próby połączeń do wszystkich dostępnych adresów z jej przestrzeni.

Opisywane skanowanie przeprowadzone zostało 21 grudnia (niedziela) – na osiem dni przed atakiem.

Pozostała aktywność w ramach rekonesansu

Następnego dnia (22 grudnia) atakujący kontynuował działania związane z rekonesansem – w logach ruchu sieciowego można zaobserwować połączenia do portów dwóch hostów, na których działały usługi zdalnego pulpitu. Najprawdopodobniej były to manualne próby znalezienia prawidłowych poświadczeń, natomiast nie stwierdzono śladów udanego połączenia.

Po kolejnych trzech dniach (25 grudnia, Boże Narodzenie) atakującemu udało się połączyć z trzema sterownikami PLC firmy Siemens za pomocą protokołu S7. Nie udało się wyjaśnić dokładnego celu tych działań. Prawdopodobny jest rekonesans sterowników przed wykonaniem działań destrukcyjnych.

Działania destrukcyjne w elektrociepłowni

W dniu 29 grudnia 2025 roku atakujący wykorzystał zdobyte wcześniej dostępy oraz wiedzę posiadaną z rozpoznania do zakłócenia działania sterowników PLC oraz innych urządzeń przemysłowych. W tym dniu aktywność atakującego w sieci elektrociepłowni rozpoczęła się około godziny 5:30, a zakończyła około godziny 10:10. Oznacza to, że działania naprawcze (okolice godziny 7:30) prowadzone przez zaatakowany podmiot rozpoczęły się jeszcze, gdy atakujący był obecny w sieci.

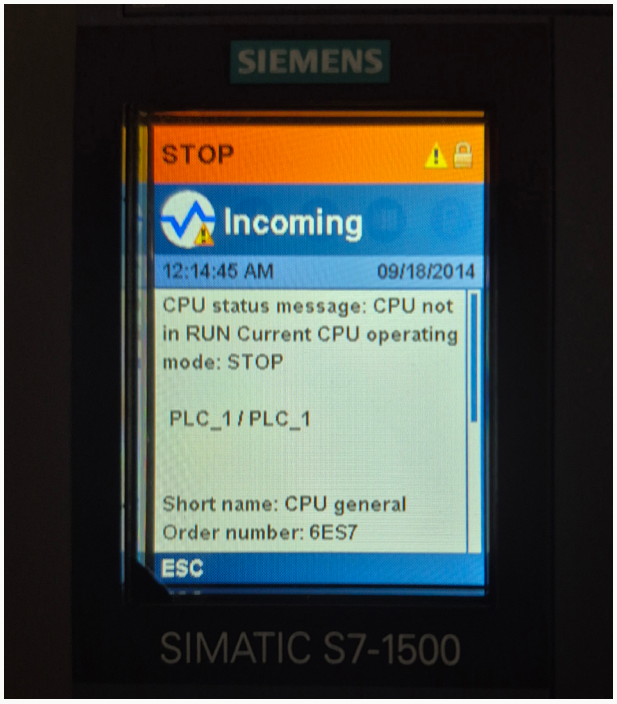
Na podstawie materiałów pozyskanych do analizy udało się zrekonstruować przybliżony przebiegu ataku.

Atak na sterowniki PLC firmy Siemens

Pierwszą czynnością atakującego w sieci elektrociepłowni po zestawieniu tunelu poprzez sterownik WAGO było nawiązanie połączenia z panelem WWW serwera SCADA, a po chwili ze sterownikiem Siemens S7-300 po protokole S7. Te same czynności powtórzono z kolejnymi sterownikami – S7-1200 oraz S7-1500. W międzyczasie były widoczne również odwołania atakującego do panelu SCADA.

Według relacji pracowników elektrociepłowni sterowniki zostały przełączone w tryb STOP i zabezpieczone hasłem, które uniemożliwiało zmianę ich trybu pracy oraz modyfikację oprogramowania. W rezultacie doszło do zatrzymania turbiny parowej i stacji uzdatniania wody do celów technicznych, co doprowadziło do przerwania procesu kogeneracji. W ramach czynności mających na celu przywrócenie sprawności obsługa przywróciła urządzenia do stanu fabrycznego i wgrała posiadane kopie oprogramowania. To działanie pozwoliło na skrócenie czasu awarii, ale doprowadziło również do usunięcia logów ze sterowników. Siemens ProductCERT potwierdził, że w takiej sytuacji odzyskanie logów jest niemożliwe.

RYS. 7 **Sterownik Siemens S7-1500 chwilę po ataku**



Atak na urządzenia firmy Moxa

Atakujący dokonał również zmian konfiguracyjnych na siedmiu serwerach portów szeregowych oraz trzech przełącznikach sieciowych firmy Moxa. Działania były analogicznie do tych obserwowanych na obiektach OZE. Urządzenia zostały przywrócone do ustawień fabrycznych, zmieniono hasło logowania oraz ustawiono adres IP urządzeń na nieosiągalny, np. 127.0.0.1. Spowodowało to niedostępność urządzeń, a zmiana hasła i adresu IP miała na celu opóźnienie przywrócenia sprawności. Na podstawie czasów żądań HTTP przesyłanych do każdego z urządzeń podczas przeprowadzania ataku z dużą pewnością jesteśmy w stanie określić, że działania te były zautomatyzowane.

Atak na inne urządzenia

W czasie ataku widoczne były również połączenia do paneli WWW dwóch przemienników częstotliwości z serii ACS firmy ABB. Nie udało się ustalić, jakie działania podjął względem nich atakujący.

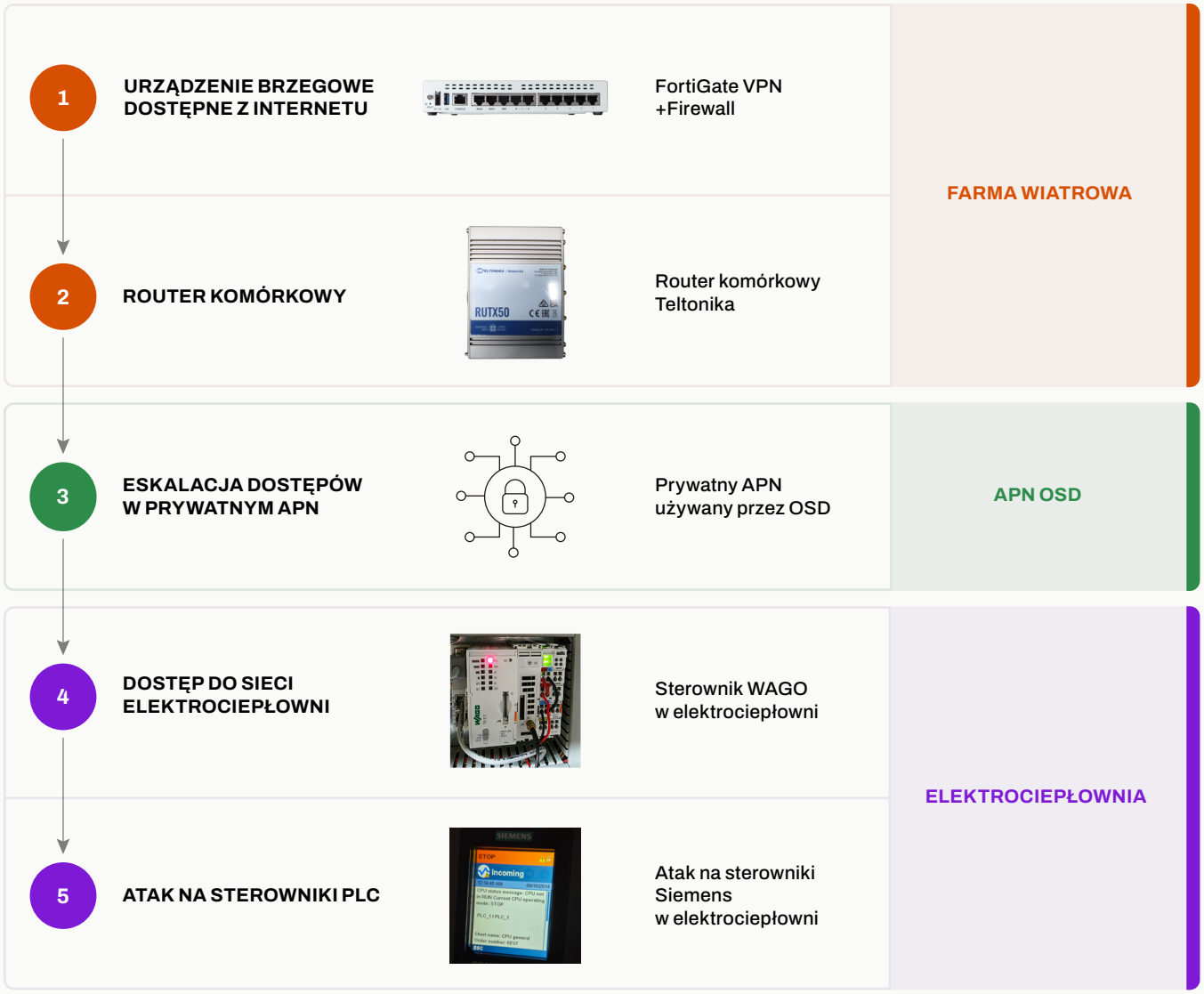
W logach ruchu sieciowego widoczne były także nieudane próby połączeń do przemienników częstotliwości Schneider Electric ATV6xx. Niepowodzenie najprawdopodobniej wynikało z niedokładnie przeprowadzonego rekonesansu – atakujący próbował łączyć się na port 80/TCP, gdy panel WWW urządzenia nasłuchiwał na innym porcie.

Pełny przebieg ataku

W celu lepszego zobrazowania przebiegu ataku poniżej zamieszczamy podsumowanie jego kolejnych etapów.

1. Uzyskanie dostępu do urządzenia brzegowego na farmie wiatrowej oraz nawiązanie zdalnego połączenia VPN.
2. Zidentyfikowanie w sieci farmy wiatrowej routera komórkowego Teltonika RUTX50, posiadającego dostęp do prywatnej sieci APN.
3. Zalogowanie się do panelu WWW routera, a następnie do działającej na nim usługi SSH.
4. Wykorzystanie usługi SSH do zestawienia tunelu umożliwiającego komunikację z prywatną siecią APN.
5. Przeprowadzenie skanowania prywatnej sieci APN.
6. Zidentyfikowanie sterownika WAGO PFC200 z panelem WWW dostępnym za pośrednictwem interfejsu WAN.
7. Wykorzystanie domyślnych danych uwierzytelniających w celu uzyskania dostępu do panelu z uprawnieniami administratora.
8. Włączenie usługi SSH na interfejsie WAN urządzenia WAGO PFC200.
9. Wykorzystanie usługi SSH do zestawienia tunelu umożliwiającego dostęp do sieci OT elektrociepłowni.
10. Prowadzenie przez tydzień rekonesansu sieci OT elektrociepłowni.
11. Przeprowadzenie działań destrukcyjnych skutkujących zatrzymaniem turbiny parowej oraz stacji uzdatniania wody, co doprowadziło do przerwania procesu kogeneracji.

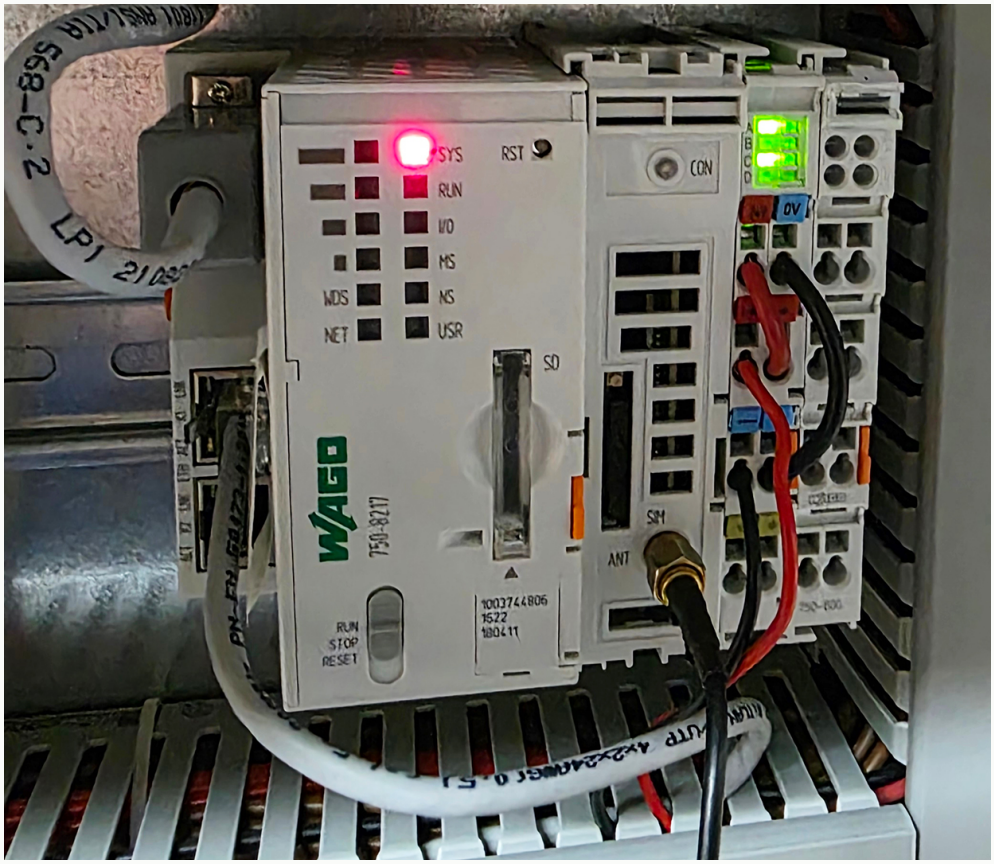
RYS. 8 — **Poglądowy schemat przebiegu ataku na elektrociepłownię z wykorzystaniem prywatnego APN**



Zacieranie śladów

Aktywność atakującego w sieci elektrociepłowni trwała blisko pięć godzin i zakończyła się dostępem do panelu WWW systemu SCADA, prawdopodobnie w celu oceny wpływu przeprowadzonych działań. Po tym atakujący uszkodził sterownik WAGO, którego używał jako bramy do sieci, poprzez uszkodzenie tablicy partycji, co uniemożliwiło jej odczyt przez urządzenie. Podmiot próbując naprawić urządzenie przywrócił je do ustawień fabrycznych, ale nie naprawiło to tablicy partycji i nie umożliwiło to ponownego uruchomienia urządzenia. W ramach analizy nie udało się odzyskać żadnych wartościowych logów z urządzenia.

RYS. 9 **Sterownik WAGO PFC200 po ataku**



Następnie atakujący kontynuował działania w obrębie farmy wiatrowej. Router komórkowy Teltonika RUTX50, który służył do zestawiania tuneli SSH, został przywrócony do ustawień fabrycznych* pół godziny po ostatniej aktywności w sieci elektrociepłowni. Następnie atakujący zmienił hasło administratora i ustawił adres IP urządzeń na nieosiągalny – 127.0.0.1 – w celu utrudnienia jego ponownej konfiguracji.

Atakujący na koniec obserwowanych działań przywrócił do ustawień fabrycznych urządzenie Fortigate pełniące funkcję koncentratora VPN oraz Firewalla, które było wykorzystywane jako punkt wejścia do sieci farmy wiatrowej. W przypadku wykorzystywanego modelu urządzenia i jego konfiguracji spowodowało to utratę logów.

* W wersjach RutOS starszych niż 7.07 baza zdarzeń była przechowywana w pamięci urządzenia nawet po przywróceniu go do ustawień fabrycznych w celach diagnostycznych. Dzięki temu możliwe było odzyskanie logów z urządzenia.

Podsumowanie

Opisane zdarzenie z wykorzystaniem dostępu do sieci OT za pomocą prywatnego APN było według naszej wiedzy pierwszym tego typu przypadkiem zaobserwowanym podczas rzeczywistego ataku. Jego wykonanie było możliwe m.in. z powodu błędnej konfiguracji, która pozwalała na nawiązywanie połączeń pomiędzy dowolnymi urządzeniami w ramach sieci prywatnego APN. Na podstawie przeprowadzonych ankiet z wieloma podmiotami wykorzystującymi tego typu rozwiązania stwierdzono, że w momencie ankietowania była to często spotykana konfiguracja w Polsce. Według naszej wiedzy jest to również powszechnie stosowana konfiguracja w innych krajach na świecie.

CERT Polska rekomenduje podmiotom korzystającym z rozwiązań opartych na prywatnym APN:

- Przeprowadzenie audytu konfiguracji prywatnego APN. W szczególności rekomenduje się włączenie izolacji komunikacji pomiędzy urządzeniami końcowymi korzystającymi z APN, tzw. „client isolation". Jeżeli jest konieczne dopuszczenie takiej komunikacji, należy przeprowadzić analizę ryzyka uwzględniającą możliwość przejęcia urządzenia podłączonego bezpośrednio do prywatnego APN oraz wykorzystania go do komunikacji z pozostałymi urządzeniami.

- Traktowanie prywatnego APN jako sieci niezaufanej względem sieci OT. Po stronie OT połączenie z prywatnym APN powinno podlegać segmentacji i kontroli ruchu co najmniej na poziomie stosowanym wobec korporacyjnych sieci WAN. Jeżeli sieć pozostaje poza kontrolą organizacji, w szczególności gdy organizacja nie ma wpływu na jej konfigurację ani nie posiada informacji pozwalających zweryfikować zastosowane mechanizmy bezpieczeństwa, powinna być traktowana jako sieć zewnętrzna o poziomie zaufania odpowiadającym sieci internet.

- Ścisłe ograniczenie komunikacji pomiędzy siecią OT a urządzeniem pełniącym funkcję bramy do prywatnego APN. Należy dopuścić wyłącznie połączenia niezbędne do realizacji określonych celów biznesowych i technicznych, z wykorzystaniem reguł typu „allowlist".

- Monitorowanie ruchu pomiędzy siecią OT a prywatnym APN, ze szczególnym uwzględnieniem odstępstw od zdefiniowanego profilu komunikacji przewidzianego dla tego połączenia.

- Centralne logowanie i monitorowanie zdarzeń z urządzeń będących bramą do prywatnego APN w przypadku, gdy urządzenie wspiera taką konfigurację.

- Ograniczenie do niezbędnego minimum liczby otwartych portów dostępnych na interfejsie osiągalnym z prywatnego APN. W szczególności nie należy udostępniać na nim usług administracyjnych, takich jak panel WWW, SSH lub Telnet.

- Zmianę domyślnych poświadczeń dla wszelkich usług dostępnych na urządzeniu, w szczególności do usług administracyjnych.

- Uwzględnienie prywatnych APN oraz urządzeń zapewniających dostęp do tych sieci w zakresie testów penetracyjnych, ćwiczeń red team oraz przeglądów architektury bezpieczeństwa.