WSPÓLNA REPREZENTACJA ZWIĄZKOWA

Poznań, 04 czerwca 2025 r.

Zarząd ENEA Operator Sp. z o.o.

Szanowni Państwo,

Związki zawodowe działające w Enea Operator Sp. z o.o. wyrażają głębokie zaniepokojenie planowanym przeniesieniem zadań z obszaru bezpieczeństwa, w tym cyberbezpieczeństwa środowiska OT (ang. Operational Technology) sieci dystrybucyjnej, do spółki Enea Centrum Sp. z o.o. Po szczegółowej analizie przepisów prawa krajowego, unijnego oraz zaleceń sektorowych stwierdzamy, że planowana zmiana niesie poważne ryzyko naruszenia prawa, zasad bezpieczeństwa narodowego, osłabienia ochrony infrastruktury krytycznej oraz utraty kluczowych kompetencji Enea Operator jako Operatora Usługi Kluczowej (OUK).

Kluczowe argumenty

1. Zgodność z prawem i obowiązki OUK

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa (UKSC, Dz.U. z 2022 r. poz. 1863):

- Art. 8 UKSC: OUK jest zobowiązany do wdrożenia systemu zarządzania bezpieczeństwem informacji,
- Art. 9 UKSC: OUK wyznacza osobę odpowiedzialną za kontakt z CSIRT i nadzoruje dokumentację,
- Art. 10 UKSC: OUK opracowuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego,
- Art. 15 UKSC: OUK zapewnia regularne audyty bezpieczeństwa systemu informacyjnego.

Przepisy te jednoznacznie wskazują, że odpowiedzialność za cyberbezpieczeństwo spoczywa na OUK i nie może być przekazana innemu podmiotowi bez spełnienia rygorystycznych warunków formalnych, technicznych i nadzorczych. Zgodnie z Rozporządzeniem Ministra Cyfryzacji z 4 grudnia 2019 r. (Dz.U. 2019 poz. 2479), struktury cyberbezpieczeństwa muszą być podporządkowane OUK lub działać na podstawie formalnej umowy, zapewniającej realną kontrolę nad zadaniami.

Enea Centrum, jako podmiot świadczący usługi administracyjne i handlowe dla wielu spółek Grupy Enea, nie posiada udokumentowanego doświadczenia ani certyfikacji (np. ISO/IEC 27001) w zakresie usług cyberbezpieczeństwa świadczonych dla podmiotów infrastruktury krytycznej, ich systemów SCADA i środowisk OT. Struktura własnościowa, wynikająca z art. 7 Kodeksu spółek handlowych (odrębność prawna spółek), uniemożliwia Enea Operator skuteczny nadzór nad zadaniami przekazanymi do Enea Centrum, co narusza zasadę niewydelegowalnej odpowiedzialności OUK.

2. Ryzyka systemowe i konflikt interesów

Zgodnie z Zaleceniem Komisji Europejskiej 2019/553, operatorzy w sektorze energii muszą zapewnić niezależność struktur bezpieczeństwa i unikać konfliktu interesów między obszarami komercyjnymi a kluczowymi. Przeniesienie funkcji bezpieczeństwa środowiska OT do struktur Departamentu Teleinformatyki Enea Centrum stworzy konflikt interesów między działem IT a zespołem cyberbezpieczeństwa OT, wynikający z różnic w priorytetach i metodach zabezpieczania systemów IT (skoncentrowanych na

dostępności i poufności danych) oraz OT (priorytetyzujących ciągłość działania sieci dystrybucyjnej, bezpieczeństwo osób i mienia). Może to prowadzić do:

- Presji na zespół OT, by dostosował się do metod IT lub nie zgłaszał uwag do działań IT w środowisku OT, dotychczas korygowanych przez Biuro Cyberbezpieczeństwa Enea Operator, co wymagało dodatkowych działań zabezpieczających.

- Opóźnień w reagowaniu na incydenty, np. atak na systemy SCADA, wynikających z bariery rozdzielności spółek KSH, co może skutkować przerwami w dostawach energii i naruszeniem Rozporządzenia Ministra Energii z 2 marca 2018 r. (Dz.U. 2018 poz. 515) w sprawie standardów technicznych sieci elektroenergetycznych.

- Osłabienia ochrony systemów OT, kluczowych dla procesów dystrybucyjnych uznanych za usługę kluczową w rozumieniu UKSC, poprzez dezaktualizację wiedzy zespołu OT na temat środowiska sieci dystrybucyjnej.

- Braku bezpośredniego nadzoru nad infrastrukturą w kontakcie z Wydziałami Telemechaniki i Zabezpieczeń Oddziałów Dystrybucji Enea Operator, co zwiększa ryzyko niezidentyfikowania incydentów na wczesnym etapie i opóźnień w usuwaniu ich skutków.

- Zawężenia zadań zespołu cyberbezpieczeństwa Enea Operator do monitorowania i reagowania na zdarzenia, bez realizacji innych obowiązków UKSC, takich jak zarządzanie podatnościami czy aktualizacja dokumentacji, wymagających specjalistycznej wiedzy o środowisku OT.

3. Naruszenie obowiązków dokumentacyjnych, audytowych i RODO

Enea Operator wdrożył system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001 oraz plan ciągłości działania zgodny z ISO 22301. Przeniesienie zadań do Enea Centrum bez:

- Audytu zgodnego z ISO/IEC 27001 w zakresie świadczenia usługi cyberbezpieczeństwa,

- Dokumentacji ochrony infrastruktury zgodnej z ISO 22301,

- Aktualizacji Polityki Bezpieczeństwa Informacji i planu BCP,

narusza obowiązki wynikające z art. 10 UKSC oraz Rozporządzenia RM z 16 października 2018 r. (Dz.U. 2018 poz. 2080).

Ponadto, przeniesienie funkcji bezpieczeństwa może naruszać art. 32 RODO, który wymaga odpowiednich środków technicznych i organizacyjnych do ochrony danych przetwarzanych w systemach OT. Brak formalnej zgody UODO na takie przeniesienie grozi sankcjami administracyjnymi.

Niewywiązanie się z tych obowiązków naraża Enea Operator na sankcje (art. 48 UKSC), ryzyko zakwestionowania audytów przez Ministerstwo Klimatu i Środowiska oraz naruszenie wymogów Urzędu Regulacji Energetyki dotyczących niezawodności dostaw energii. Dodatkowo, zmiana generowałaby nieuzasadnione koszty związane z ponownym audytem i dostosowaniem procesów w Enea Centrum, podczas gdy Enea Operator posiada już odpowiednie kompetencje i struktury.

4. Uzasadnienie społeczne i organizacyjne

Związki zawodowe, reprezentując interesy pracowników i dbając o bezpieczeństwo firmy, wskazują na:

- Ryzyko obniżenia efektywności zarządzania incydentami: Brak bezpośredniego dostępu do danych i specjalistów w Enea Operator może opóźnić reakcję na incydenty, szczególnie w sytuacjach kryzysowych.

- Ryzyko w sytuacjach kryzysowych: Brak wewnętrznej struktury reagowania uniemożliwi skuteczne działanie w przypadku awarii systemów krytycznych, takich jak SCADA.
- Utratę kompetencji strategicznych: Przeniesienie funkcji bezpieczeństwa pozbawi Enea Operator kluczowych specjalistów i know-how, co osłabi pozycję firmy jako OUK.
- Degradację znaczenia OUK: Przekazanie zadań do Enea Centrum obniży rolę Enea Operator w Grupie Kapitałowej, co może wpłynąć na stabilność zatrudnienia i morale pracowników.

Konsultacje przeprowadzone przez związki zawodowe z pracownikami, w szczególności z działów bezpieczeństwa i IT, wskazują na szerokie poparcie dla utrzymania funkcji bezpieczeństwa w strukturze Enea Operator. Pracownicy wyrażają obawy dotyczące utraty kompetencji, obniżenia standardów bezpieczeństwa oraz potencjalnych zagrożeń dla stabilności zatrudnienia.

Postulaty

W związku z powyższym, związki zawodowe wzywają Zarząd Enea Operator do:

1. Natychmiastowego wstrzymania wszelkich prac organizacyjnych i formalnych związanych z przeniesieniem zadań z obszaru bezpieczeństwa do Enea Centrum.
2. Ujawnienia podstawy prawnej, analizy ryzyka oraz opinii organów nadzorczych (MKiŚ, CSIRT, URE, UODO) uzasadniających planowane zmiany.
3. Przeprowadzenia niezależnego audytu zgodności planowanego przeniesienia z wymogami UKSC, RODO, norm ISO/IEC 27001 i ISO 22301 oraz wytycznymi ENISA, sfinansowanego przez Enea SA, przed podjęciem jakichkolwiek działań.
4. Zapewnienia niezależności obszaru cyberbezpieczeństwa OT Enea Operator od struktur IT Enea Centrum, aby umożliwić skuteczny nadzór nad działaniami IT w środowisku OT.
5. Zapewnienia zespołowi OT stałego dostępu do aktualnej wiedzy o środowisku OT Enea Operator, niezbędnego do realizacji obowiązków UKSC, co byłoby utrudnione w przypadku przeniesienia zespołu do innego podmiotu KSH lub ograniczenia jego funkcji wyłącznie do SOC.
6. Optymalizacji procesów poprzez przeniesienie zadań 1. linii SOC (np. monitorowanie podstawowych alertów i wstępna analiza incydentów) do Enea Centrum, przy zachowaniu w Enea Operator funkcji 2. i 3. linii SOC (np. analiza zaawansowanych incydentów, zarządzanie podatnościami OT), co pozwoli wykorzystać całodobowy tryb pracy SOC Enea Centrum przy utrzymaniu specjalistycznej wiedzy dotyczącej środowiska OT Enea Operator, z natury niepowtarzalnego.

Zastrzegamy możliwość wystąpienia z oficjalnym zawiadomieniem do Ministra Klimatu i Środowiska, Urzędu Ochrony Danych Osobowych, Urzędu Regulacji Energetyki oraz innych właściwych instytucji w przypadku kontynuowania opisanych działań.

Apel do Zarządu Enea SA i Rady Nadzorczej Enea Operator

Zwracamy się do Zarządu Enea SA, jako właściciela obu spółek, oraz Rady Nadzorczej Enea Operator o podjęcie działań zapewniających zgodność planowanych zmian z prawem i interesem Grupy Enea. Prosimy o uwzględnienie ryzyk dla bezpieczeństwa narodowego, stabilności dostaw energii oraz interesów pracowników. W szczególności apelujemy o przeanalizowanie wpływu przeniesienia funkcji bezpieczeństwa na pozycję Enea Operator jako Operatora Usługi Kluczowej oraz na stabilność funkcjonowania sieci dystrybucyjnej.

Oczekujemy odpowiedzi na niniejsze pismo w terminie 14 dni od daty jego otrzymania oraz rozpoczęcia dialogu z przedstawicielami związków zawodowych w celu wypracowania rozwiązania chroniącego interesy Enea Operator, jej pracowników oraz bezpieczeństwa infrastruktury krytycznej.

Z poważaniem,

MZZP GK Enea
Signed by / Podpisano przez:
Janusz Andrzej Śniadecki
Date / Data: 2025-06-04 11:24

SOLIDARNOŚĆ
Elektronicznie podpisany przez Krzysztof Nawrocki
Data: 2025.06.04 10:32:58 +02'00'

Janusz Pydo
MOZ ZZIT ENEA
2025.06.04 11:35:30+02'00'

Signed by / Podpisano przez:
Sylwester Starzyk
Date / Data: 2025-06-04 10:47

Bogusław Konrad Malak
Elektronicznie podpisany przez Bogusław Konrad Malak
Data: 2025.06.04 10:58:25 +02'00'

Do wiadomości:

Rada Nadzorcza Enea Operator Sp. z o.o.
Rada Nadzorcza Enea S.A.
Zarząd Enea S.A.