PROTOKÓŁ z XXVII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 7 marca 2025 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

Otwarcie Posiedzenia – p. Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Pani Przewodnicząca powitała członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości.

System e-CzasPL - w kontekście wyzwań synchronizacji czasu – Pan Krzysztof Silicki, RdC/NASK; Pan Maciej Gruszczyński, Kierownik Laboratorium Nowych Technologii Czasu i Długości w Głównym Urzędzie Miar oraz Pan Tomasz Widomski, Członek Rady Nadzorczej Elproma oraz krajowy delegat MC KPRM do ITU – Dyskusja.

Pan Krzysztof Silicki wskazał, że pierwsza część posiedzenia została poświęcona tematyce synchronizacji czasu wszystkich systemów teleinformatycznych, które nie mogłyby działać bez synchronizacji. Nawiązał do Uchwały Rady ds. Cyfryzacji w sprawie dystrybucji i synchronizacji czasu, a także odporności infrastruktur krajowych odpowiedzialnych za dostarczanie czasu urzędowego, wiarygodnych informacji o czasie z systemów nawigacji satelitarnej i połączeniu oraz synchronizacji wszystkich elementów dla korzyści systemów wymagających takiego działania.

Pan M. Gruszczyński na wstępie wskazał na problemy związane z synchronizacją czasu, która jest katalizatorem różnych procesów w informatyce i cyfryzacji państwa. Przedstawił tło zagadnienia czasu w systemach IT omawiając przykłady, m.in. panel systemu nawigacyjnego na samolotach transatlantyckich jednego z producentów, gdzie w nocy z 6 na 7 kwietnia 2019 r. wyświetlała się data 22 sierpnia 1999 r. – zdarzenie powodujące uziemienie samolotów, opóźnienia w starcie, co przekładało się na wymierne straty z uwagi na odszkodowania. Efektów tego zdarzenia było więcej – oddziaływanie na wszelkiego rodzaju zautomatyzowane stacje badawcze mierzące pływy na morzach, ale także systemy zarządzające *smart city* czy dostępem do Internetu w miastach. Pan M. Gruszczyński wspomniał o przyczynie - *GPS week number rollover* – zdarzeniu wiązanym z architekturą systemu GPS (przepełnienie licznika czasu transmitowanego w depeszy nawigacyjnej z systemu nawigacji satelitarnej, czyli afekt związany z nieprawidłowym podaniem informacji o czasie).

Zastosowań synchronizacji czasu z wykorzystaniem GPS jest obecnie bardzo dużo, a infrastruktura krytyczna jest podatna na błędy tego rodzaju, zarówno nieintencjonalne, jak i celowe cyberataki. Pan M. Gruszczyński wskazał rolę GUM w utrzymywaniu UTC(PL) na podstawie ustawy o czasie urzędowym na obszarze Rzeczypospolitej Polskiej[1], zgodnie z

[1] Ustawa z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz.U. 2004 nr 16 poz. 144)

którą Prezes GUM jest organem uprawnionym do utrzymywania czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) oraz do rozpowszechniania sygnałów tych czasów. Poinformował, że GUM zbudował nowoczesny kampus laboratoryjny w Kielcach, gdzie zostaną rozwijane zegary optyczne, ale posiada także podstawowe zegary atomowe. W Warszawie znajdują się zegary utrzymywane przez GUM oraz przez jednostki współpracujące w ramach stworzonej sieci – w przypadku dużej awarii fizycznej w głównej lokalizacji, jeden z ośrodków mógłby przejąć funkcję centrum utrzymania skali czasu urzędowego obowiązującego w Polsce, z uwagi na stałe porównywanie za pomocą technik satelitarnych i fizycznych połączeń światłowodowych. Przedstawiciel GUM wspomniał, że z synchronizacji czasu korzysta: telekomunikacja, energetyka, rynki finansowe, inteligentne miasta, transport czy TV.

Podstawowym celem projektu e-CzasPL były takie fundamenty jak zakup sprzętu redundantnego (zegarów atomowych), które w przypadku awarii jednej jednostki mogą kierować funkcję na działające jednostki; automatyzacja procesu obsługi awarii i przerw; wydajnościowy klaster dystrybucji czasu urzędowego o zwiększonej niezawodności. Pan M. Gruszczyński przedstawił także schemat systemu generowania skali czasu urzędowego.

W dalszej części wypowiedzi przedstawiono nowe e-usługi publiczne w ramach projektu e-CzasPL. Jednym z ważniejszych serwisów to e-Czas Monitor, który służy jego użytkownikom do dodatkowego potwierdzenia zgodności czasu i synchronizacji względem UTC(PL) z wykorzystaniem techniki NTP – czyli serwis „audytu czasu" oraz autentyfikacji.

Serwis e-Czas PTP jest przeznaczony dla wymagających odbiorców usługi synchronizacji do wiarygodnego źródła czasu i częstotliwości za pomocą połączeń światłowodowych i techniki PTP.

Serwis e-Czas On-line pozwoli wyświetlić, na dowolnym urządzeniu mobilnym, zegar synchronizowany z czasem urzędowym obowiązującym na terytorium RP. Wspomniano również o polskim systemie DCF – czyli serwisie e-Czas Radio. Jest to serwis emitowania kodowanych cyfrowych sygnałów czasu na falach długich, przy wykorzystaniu fali nośnej 225 kHz Programu Pierwszego Polskiego Radia, z nadajnika znajdującego się na terytorium Polski (technika podobna do systemu DCF77, ale oparta na modulacji fazy sygnału), co powoduje powstanie ogólnodostępnej możliwości zsynchronizowania z czasem urzędowym na obszarze RP dowolnego urządzenia odmierzającego czas wykorzystując tanie, energooszczędne i nieskomplikowane urządzenia odbiorcze. Wykorzystanie tej techniki pozwala na zsynchronizowanie do czasu urzędowego na obszarze RP wielu urządzeń odmierzających czas z dokładnością kilku lub kilkunastu milisekund. System jest dodatkowym (redundantnym) źródłem informacji o czasie dla użytkowników znajdujących się na terytorium Polski. Sygnały wzorcowe generowane są w oparciu o moduł stabilnej częstotliwości oparty na wysokostabilnych rubidowych wzorcach częstotliwości znajdujących się w Radiowym Centrum Nadawczym (RCN) w Solcu Kujawskim. Aktualnie na polskim rynku istnieją firmy, które produkują odbiorniki tego sygnału radiowego.

Pan Tomasz Widomski swoją wypowiedź rozpoczął od gratulacji dla Rady za podjęcie uchwały w sprawie dystrybucji i synchronizacji czasu. Od tego momentu w NTP Pool w polskiej strefie zauważono 100 % wzrost liczby serwerów w tej grupie – to serwery anonimowe utrzymywane przez wolontariuszy, wśród nich są serwery GUM, Elpromy, Orange. Sieć NTP Pool bywa źródłem pewnych manipulacji – istnieje możliwość zarówno prowadzenia cyberataków z poziomu tej sieci jak i uodparniania. Korzystają z niej użytkownicy Linux, ruterów oraz urządzenia IoT. Istnieje obawa, że 50% obecnej puli polskich serwerów to „serwery zatrute" z uwagi na możliwość stworzenia serwerów pozornie dobrze wyglądających i reprezentujących prawidłowy czas, jednak kiedy zostaną zaakceptowane w tej grupie, to wybranym adresom IP (wybranych do zaatakowania systemów IT) mogą podawać czas fałszywy, który będzie niewłaściwy nie tylko na poziomie mikrosekund, lecz na poziomie kilku dni. Takie działanie spowoduje brak dostępu do części usług IT, m.in. unieważnienie uwierzytelnionych elektronicznie transakcji, które będą sprzeczne w znaczeniu prawnym, z uwagi na zaburzenia chronologii prawdziwych zdarzeń, ale może wprost prowadzić do znaczącego obniżenia funkcjonalności, a nawet poważnej awarii technicznej. W dalszej części wypowiedzi Pan T. Widomski wskazał, że największym infrastrukturalnym odbiorcą NTP Pool jest między innymi kolej – gigantyczna infrastruktura, szczególnie wrażliwa ze względu na konieczność zapewnienia głębi logistycznej w przypadku konfliktu kinetycznego, a praktyczne znaczenie użycia NTP Pool właśnie wtenczas odgrywa szczególną rolę, co Pan T. Widomski zilustrował przykładami z innych państw i wyjaśnił. Wspomniał o spostrzeżeniach z obszaru Pool, gdzie zauważono pewne powiązania ekonomiczne/kryzysowe wraz ze wzrostem puli serwerów publicznych w niektórych krajach.

Wskazano dwa sposoby manipulowania synchronizacją w zakresie wyłącznie systemów informatycznych odpowiedzialnych za zarządzanie wnętrzem infrastruktury krytycznej tych obszarów, które wymienia Dyrektywa NIS 2: telekomunikacja, energetyka oraz transport. Instrumentami cyberataku desynchronizacji są: *jamming* i *spoofing* GPS na serwery NTP. Drugim elementem jest zatrucie NTP Pool. W każdym przypadku antidotum zagrożeń jest synchronizacja do GUM.

Pan T. Widomski wskazał, że atak na czas i synchronizację polega obok bezpośredniej bardzo niebezpiecznej (w dobie manipulacji sygnałami GPS) desynchronizacji rozproszonej struktury IT/OT będącej składową każdej ważnej dla gospodarki państwa infrastruktury krytycznej opisanej dyrektywą NIS2 na zaburzeniu chronologii zapisów *log.* Gdy zostanie zaburzona chronologia, w przypadku dużej, rozproszonej po całej Polsce sieci energetyki, nie będzie można dotrzeć do przyczyny zdarzenia. Podkreślił, że nie mniej istotna jest też kwestia badania opóźnień co dot. wszelkich nowych technologii jakie oprą się na szóstej generacji telekomunikacji oraz same będą spełniać techniczny rygor *low-latency networking.*

W toku dyskusji zapytano o możliwości promocji rozwiązań GUM w Europie oraz na świecie oraz o miejsca, w których znajdują się polskie produkty. Pan T. Widomski odpowiedział, że generalnie polskie produkty można spotkać w każdym dobrze funkcjonującym laboratorium metrologii czasu na świecie. Z dużym powodzeniem podejmowane są próby dotarcia do

krajów Azji. Firma Elproma odpowiada tam za synchronizację całych infrastruktur najnowszej energetyki *Smart Grid* – dwukierunkowego przemysłu energii stanowiącego *de facto* klucz do rozwiązania problemów obniżenia kosztów energii, z uwagi na brak utraty energii na przesyle. Ponadto, drogi pomiędzy źródłem, a odbiorcą są najkrótsze - jest to dynamiczne zarządzanie połączeniem – warunek konieczny efektywnego zarządzania dystrybucją energii elektrycznej, co jest nie mniej ważne od dołączania nowych źródeł jej wytwarzania.

W podsumowaniu Pan T. Widomski wyróżnia dwa rodzaje nowych cyber-zagrożeń desynchronizacją IT/OT: (1) zakłócanie GPS przez *jamming* i *spoofing GNSS*; (2) „zatrucie" POOL.NTP grupy publicznych serwerów NTP w Polskiej strefie. Jako antidotum powyższych zagrożeń podkreślił odpowiednio (Ad 1.) używanie czasu urzędowego UTC(PL) z Głównego Urzędu Miar RP za pośrednictwem naziemnym dystrybucji państwowym systemem eCzasPL; (Ad 2.) zwiększenie liczby kontrolowanych przez Państwo i synchronizowanych do UTC(PL) serwerów publicznych NTP krajowej strefy, co jest wnioskiem Uchwały Rady ds. Cyfryzacji w sprawie dystrybucji i synchronizacji czasu.

Zwrócono uwagę, że już pięciominutowa desynchronizacja Microsoft Active Directory (AD) uniemożliwia uwierzytelnienie Kerberos użytkowników, odmawiając dostępu do sieci, a nawet budynków i serwerowni. Pięciosekundowa desynchronizacja może destabilizować pracę VPN. Rozproszone bazy danych SQL i ich archiwizacja wymagają milisekundowej dyscypliny zgodnego czasu. Pan T. Widomski zauważa, że problem desynchronizacji jest przedmiotem międzynarodowej dyskusji na forum ITU (grupa WP-7A, obraduje przy ONZ w Genewie) i sprawy te są traktowane z niepokojem i powagą, ponieważ są niszowe i wymagają wsparcia państwa.

W dalszej części dyskusji, członkowie Rady zastanawiali się nad rekomendacjami w formie apelu do CSIRTów sektorowych o stosowanie konkretnego typu rozwiązań/wzorca z zakresu synchronizacji w kontekście cyberbezpieczeństwa bądź szerszym, ponieważ zjawisko zakłóceń dotyczy wszystkich sektorów gospodarki. Pani Przewodnicząca zaproponowała stworzenie stanowiska w tej sprawie skierowanego do Ministra Cyfryzacji – Pełnomocnika Rządu ds. Cyberbezpieczeństwa o szersze rekomendacje, a także rozważenie usankcjonowania prawnego tego zakresu na dalszym etapie.

Informacja na temat prac dotyczących Krajowego Planu na rzecz Energii i Klimatu – Pan Wojciech Racięcki, Dyrektor Departamentu Strategii i Analiz w Ministerstwie Klimatu i Środowiska.

Pan Dyrektor W. Racięcki wskazał, że w Ministerstwie Klimatu i Środowiska trwają prace nad dużym dokumentem strategicznym – Krajowym Planem na rzecz Energii i Klimatu. Dokument przedstawia dekarbonizacje całej polskiej gospodarki. To parasolowy program opisujący transformację Polski do 2040 r. z ustawieniem parametrów i celu na 2030 r.

Pan Dyrektor przybliżył treść dokumentu, który zawiera trzy fundamentalne kwestie: trajektorie transformacyjne, czyli wyliczenia w jaki sposób dekarbonizują się poszczególne

obszary – dekarbonizacja do roku 2030 – obniżenie do 50% emisji dwutlenku węgla, do 2040 r. do 70% emisji. Ponadto ilość energetyki – wzrost o ok. 2,3 gigawaty rocznie mocy wytwórczych OZE, magazyn energii, biometanownie, termomodernizacja budynków – pierwszy obszar opisujący trajektorie modelowanych zmian, biorąc pod uwagę wszystkie uwarunkowania Polski, możliwości implementacyjne oraz najbardziej sensowny miks energetyczny. MKiŚ ma na celu zrealizowanie trzech priorytetów znajdujących się w tym programie: obniżenie kosztów energii, produkcja energii z polskiego terytorium dla uzyskania bezpieczeństwa energetycznego oraz rozwój gospodarki.

Drugim segmentem są wszystkie działania, które trzeba w Polsce wykonać dla zrealizowania planu. Większość działań to działania energetyczne – dekarbonizacja przemysłu czy rolnictwa, ale także wątek w zakresie cyberbezpieczeństwa oraz cyfryzacji. Trzeci obszar to finansowanie całego procesu stanowiące gigantyczne wyzwanie.

Mając na uwadze sam obszar transformacji, to MKiŚ nie zajmuje się wprost tematami związanymi z digitalizacją czy cyfryzacją, jednak obecnie nie ma procesów, jakie miałyby zaistnieć w zakresie jakichkolwiek działań na większą skalę bez cyfryzacji. Jest kilka działań, które w dużej mierze dotykają aspektów cyfrowych. Biorąc pod uwagę ilość koniecznych mocy wytwórczych w źródłach OZE czy fotowoltaice oraz procesów inwestycyjnych, w dokumencie jest założenie cyfryzacji/standaryzacji tych procesów. Potrzeba dobrego zorganizowania/zaprojektowania działań, ale także całej infrastruktury informatycznej, która jest w stanie to wszystko zbudować. MKiŚ prowadzi obecnie konsultacje ze wszystkimi resortami z uwagi na wieloaspektowość obszaru zawartego w dokumencie.

Pan Dyrektor omówił działania zawierające element cyfrowy. Pierwszy z nich to Krajowy Punkt Kontaktowy do spraw odnawialnych źródeł energii, polegający na stworzeniu punktu OSS (One Stop Shop) obsługi procesów inwestycyjnych tzn. aby gmina, gdzie transformacja w dużej mierze będzie się odbywała, miała jeden koordynacyjny ośrodek posiadający pełną wiedzę co do sposobu wykonania tej transformacji (sposób prowadzenia modernizacji budynków, budowanie mocy wytwórczych, uwarunkowania ustawowe) - będzie wsparciem dla procesów oraz prowadzącym procesy inwestycyjne, jeżeli inwestor wyrazi na to chęć. Dla prawidłowego funkcjonowania systemu potrzebne są narzędzia cyfrowe, by dobrze zaimplementować jego pracę. Z tym działaniem skojarzone jest działanie digitalizacji i standaryzacji procesów inwestycyjnych dla transformacji energetyczno-klimatycznej – z uwagi na dużą ilość procesów inwestycyjnych należy zestandaryzować umowy pomiędzy stronami. Planowane jest stworzenie jednego zasobu kompetencyjnego będącego bazą, sterowaniem i wsparciem dla procesu. Ponadto, potrzebne jest narzędzie symulacyjne/optymalizacyjne – symulator systemu energetycznego miasta, który będzie pomocnym narzędziem obliczeniowym dla samorządów.

Pan Dyrektor wspomniał o działaniach związanych z uporządkowaniem bazy emisyjności i świadectw energetycznych budynków. Bazę audytów energetycznych prowadzi Ministerstwo Rozwoju i Technologii. Planowane jest powstanie w tej bazie pewnych algorytmów wyznaczających sposoby modernizacji budynków. Kolejną poruszoną kwestią było

cyberbezpieczeństwo w elektroenergetyce. Pan Dyrektor zwrócił się z zapytaniem do członków Rady w jaki sposób zapewnić cyberbezpieczeństwo w systemach energetycznych.

Jeden z członków Rady zauważył, że sama transformacja energetyczna to także olbrzymie wyzwanie cyfryzujące - zarządzanie zarówno procesem transformacji jak i w kolejnym etapie zarządzanie całością. Konieczne jest opracowanie od podstaw niektórych systemów.

Poruszono temat m.in. elektrowni wodorowych. Dyskutowano o sposobach produkcji energii. Jeden z członków Rady powrócił do tematu cyberbezpieczeństwa. W aspekcie systemowym w nawiązaniu do nowelizacji ustawy o KSC – większa ilość sektorów zostaje zdefiniowana jako kluczowe lub ważne – organ właściwy w danym sektorze będzie miał obowiązek powołania tzw. CSIRTu sektorowego. Ponadto, organ właściwy może kreować specyficzną dla danego sektora rzeczywistość przepisów w zakresie cyberbezpieczeństwa, pozostającą bez kolizji z Dyrektywą NIS 2 i ogólnymi zasadami zawartymi w ustawie. Miliony tzw. liczników dwukierunkowych są kupowane po najniższej cenie bez wymogów co do cyberbezpieczeństwa. Istotne są działania na poziomie organu właściwego, by procesy wdrażać teraz, a nie po zapisaniu strategii. W modelach/narzędziach teleinformatycznych do sterowania dynamicznym przepływem będzie potrzebna sztuczna inteligencja oraz algorytmy samouczące się.

Pani Przewodnicząca zaproponowała zorganizowanie spotkania w formie online z Panem Dyrektorem W. Racięckim w celu szczegółowego omówienia dokumentu i zgłoszenia ewentualnych uwag przez Radę.

Kolejne dwa posiedzenia będą dotyczyć tematyki treści w Internecie – trwają prace nad agendą spotkań Rady. Z pewnością omówiony zostanie temat Rozporządzenia CSAM. Jedno z kwietniowych posiedzeń będzie dotyczyło tematyki *Healthcare* i europejskiej przestrzeni danych. Dyskutowano także na temat nowelizacji ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Zamknięcie posiedzenia.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Katarzyna Chałubińska-Jentkiewicz
2. Andrzej Dulka
3. Agnieszka Gryszczyńska
4. Agnieszka Jankowska – Przewodnicząca
5. Jolanta Jaworska
6. Michał Kanownik
7. Katarzyna Kopczewska
8. Janusz Kosiński
9. Anna Beata Kwiatkowska
10. Jarosław Mojsiejuk
11. Krzysztof Silicki
12. Patrycja Staniszewska
13. Katarzyna Szymielewicz
14. Robert Trętowski
15. Sławomir Wojciechowski

Zaproszeni goście:

16. Maciej Gruszczyński, Kierownik Laboratorium Nowych Technologii Czasu i Długości w Głównym Urzędzie Miar
17. Tomasz Widomski, Członek Rady Nadzorczej Elproma, krajowy delegat MC KPRM do ITU
18. Wojciech Racięcki, Dyrektor Departamentu Strategii i Analiz w Ministerstwie Klimatu i Środowiska

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

19. Karolina Taczalska, Biuro Ministra w MC
20. Joanna Gójska, Biuro Ministra w MC