

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Administracji
i Spraw
Wewnętrznych**

■ **PODKOMISJI STAŁEJ DO SPRAW
FUNKCJONOWANIA ZARZĄDZANIA
KRYZYSOWEGO
(NR 7)
z dnia 27 listopada 2024 r.**

Pełny zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych

– podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego (nr 7)

27 listopada 2024 r.

Podkomisja stała do spraw funkcjonowania zarządzania kryzysowego, obradująca pod przewodnictwem posła **Konrada Frysztaka (KO)**, przewodniczącego podkomisji, zrealizowała następujący porządek dzienny:

– informacja ministra cyfryzacji i dyrektora Rządowego Centrum Bezpieczeństwa na temat przeciwdziałania dezinformacji i atakom cybernetycznym na infrastrukturę krytyczną oraz podmioty strategiczne niezbędne do prawidłowego funkcjonowania państwa.

W posiedzeniu udział wzięli: **Paweł Olszewski** sekretarz stanu w Ministerstwie Cyfryzacji, **Łukasz Panas** szef Wydziału Koordynacji Działań w Cyberprzestrzeni Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni wraz ze współpracownikami, **Wojciech Demediuk** dyrektor Departamentu eZdrowia Ministerstwa Zdrowia, **Paweł Dziuba** dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Obrony Narodowej, **Mariusz Cichomski** zastępca dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji, **Adam Kachel** dyrektor Głównego Sztabu Policji Komendy Głównej Policji wraz ze współpracownikami, **Andrzej Godecki** zastępca dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, **Jarosław Pudzianowski** główny specjalista w Wydziale Ochrony Infrastruktury Krytycznej RCB, **Witold Skomra** doradca w Rządowym Centrum Bezpieczeństwa, p.o. szefa Wydziału Ochrony Infrastruktury Krytycznej, **Paweł Bernacki** starszy specjalista w Wydziale do spraw Cyberbezpieczeństwa Sektora Energii Departamentu Informatyzacji Ministerstwa Klimatu i Środowiska, **Agnieszka Lipińska** analityczka i specjalistka ds. dezinformacji NASK, oraz **Adam Ostrowski** specjalista do spraw legislacyjnych Związku Miast Polskich.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Igor Amarowicz i Anna Ornat** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł **Konrad Frysztak (KO)**:

Przepraszam za spóźnienie. Spieszę z wyjaśnieniem i usprawiedliwieniem, że po głosowaniach zatrzymał mnie pan minister Grabiec. Jeszcze raz przepraszam.

Szanowni państwo, otwieram posiedzenie podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego.

Na podstawie listy stwierdzam, że mamy kworum.

Porządek dzienny to informacja ministra cyfryzacji i dyrektora Rządowego Centrum Bezpieczeństwa na temat przeciwdziałania dezinformacji atakom cybernetycznym na infrastrukturę krytyczną oraz podmioty strategiczne niezbędne do prawidłowego funkcjonowania państwa.

Szanowni państwo, witam pana Pawła Olszewskiego, sekretarza stanu w Ministerstwie Cyfryzacji – dzień dobry, panie ministrze – wraz ze współpracownikami.

Sekretarz stanu w Ministerstwie Cyfryzacji **Paweł Olszewski**:

Sam jestem.

Przewodniczący poseł **Konrad Frysztak (KO)**:

O, cóż za zaskoczenie. Pana Kamila Basaja, starszego informatyka w Oddziale Koordynacyjnym Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, pana Mariusza Cichomskiego, zastępcę

dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji, pana Pawła Bernackiego z Ministerstwa Klimatu i Środowiska. Pozwolicie państwo, tak będzie szybciej, żebyśmy mogli przejść do rozpatrywania. Witam pana Wojciecha Demediuka, dyrektora Departamentu eZdrowia Ministerstwa Zdrowia, pana Pawła Dziubę, dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Obrony Narodowej, pana komandora Andrzeja Godeck...

Zastępca dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni Andrzej Godecki:
Godeckiego.

Przewodniczący poseł Konrad Fryszak (KO):

Godeckiego. Proszę wybaczyć. Błąd tutaj, który mamy. Zastępcę dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, pana inspektora Adama Kachela, dyrektora Głównego Sztabu Policji Komendy Głównej Policji, pana Michała Kanownika, prezesa zarządu Związku Cyfrowa Polska, panią Katarzynę Nosalską, dyrektora Centrum Rozwoju Kompetencji Ministerstwa Cyfryzacji, pana podpułkownika Łukasza Panasa, szefa Wydziału Koordynacji Działań w Cyberprzestrzeni Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, pana Jarosława Pudzianowskiego, głównego specjalistę w Wydziale Ochrony Infrastruktury Krytycznej w RCB, pana Witolda Skomrę, doradcę w RCB, pełniącego obowiązki szefa Wydziału Ochrony Infrastruktury Krytycznej, pana Bartosza Włodarczyka, starszego specjalistę w Wydziale Zarządzania Ministerstwa Klimatu i Środowiska, pana Łukasza Wojewodę, dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji. Nie ma.

Sekretarz stanu w MC Paweł Olszewski:

Tak. Zwolniłem państwa dyrektorów, mają inne obowiązki, więc będę sam na pokładzie.

Przewodniczący poseł Konrad Fryszak (KO):

To w takim razie pan minister tutaj dzisiaj będzie pewnie odpytywany. Pana nadkomisarza Piotra Zasławskiego z Komendy Głównej Policji i pana młodszego inspektora Piotra Tofiluka z KGP. Tym sposobem przywitania mamy za sobą.

Szanowni państwo, oddaję głos panu ministrowi. Bardzo proszę.

Sekretarz stanu w MC Paweł Olszewski:

Dzień dobry. Witam państwa bardzo serdecznie. Dziękuję serdecznie za zaproszenie i zajęcie się niezwykle istotnym tematem. Postaram się zwięźle zaprezentować to, co w ramach Ministerstwa Cyfryzacji i nie tylko, bo pełnimy funkcję również koordynacyjną, się dzieje. Oczywiście, jeśli będą dodatkowe pytania to służę odpowiedzią. Cyberzagrożenia są dzisiaj na pierwszym froncie, jesteśmy w realnej wojnie w cyberprzestrzeni. Mówię to z pełną odpowiedzialnością. Liczba ataków rośnie lawinowo. W tym roku najprawdopodobniej, wszystko na to wskazuje, analizując trendy, przekroczymy liczbę incydentów o ponad 100 tys. obsługiwanych tylko i wyłącznie przez CSIRT NASK. Ministerstwo Cyfryzacji pełni rolę koordynacyjną wraz z Rządowym Centrum Bezpieczeństwa. Funkcjonuje połączone centrum operacyjne cyberbezpieczeństwa. Jest to miejsce, które umożliwia zarządzanie cyberbezpieczeństwem na poziomie krajowym, CSIRT-y krajowe w nich uczestniczą, służby specjalne, organy ścigania. Wymieniamy się wiedzą odnośnie do incydentów, odnośnie do zagrożeń, odnośnie do tego, co się dzieje i w jakiś sposób dzielić między siebie zadania. Realizujemy również działania dotyczące ochrony całej infrastruktury.

Mamy kilka dużych projektów, o wszystkich nie będę mówił, wymienię tylko te najważniejsze. Projekt Anty DDoS, uruchomiony w Ministerstwie Cyfryzacji, realizowany przez NASK. Dzięki temu zapewniamy ochronę centralnym organom dla bodaj 76 instytucji, o ile dobrze pamiętam, ten projekt działa niezwykle skutecznie i będzie nadal realizowany. Również realizujemy projekt CTI Cyber Intelligence, który ma na celu rozpoznawanie zagrożeń w cyberprzestrzeni. Został on zakupiony na potrzeby Ministerstwa Cyfryzacji, ale również innych instytucji. Umożliwia on m.in. obserwowanie aktywności wrogich grup APT, wykrywanie ataków, obserwowanie forów hakerskich w darknetcie, szybką analizę wycieków danych, to wszystko się na bieżąco dzieje.

Jak państwo wiedzą, również funkcjonuje powiększony w tym roku fundusz cyberbezpieczeństwa i dodatki teleinformatyczne dla specjalistów z zakresu cyberbezpieczeństwa w poszczególnych instytucjach tak, aby te zarobki były konkurencyjne. Organem pomocniczym w sprawie obsługi tych incydentów jest Zespół Incydentów Krytycznych, który jest zarządzany przez Rządowe Centrum Bezpieczeństwa, więc nie będę już wchodził w ten obszar. Pozostawię to panu dyrektorowi.

Może przedstawię jeszcze, że pełnomocnik rządu do spraw cyberbezpieczeństwa podejmuje szereg działań, wydaje komunikaty, zalecenia, rekomendacje. Dla przykładu były rekomendacje dotyczące aktualizacji niektórych produktów poszczególnych firm, które stanowiły zagrożenie, były rekomendacje dotyczące obowiązku niestosowania pewnych platform, które obsługiwały Biuletyn Informacji Publicznej, były komunikaty związane ze zwiększeniem zagrożenia atakami DDoS, oszustw komunikacji z osobami publicznymi, były zalecenia również dotyczące działań i zamierzeń, które są podejmowane w związku ze wzrostem liczby incydentów związanych z wyciekiem danych. Obserwowaliśmy na bieżąco, co się działo.

Głównie to są ataki wymierzone w łańcuchy dostaw podmiotów infrastruktury krytycznej. Na bieżąco się tym zajmujemy w ramach połączonego Centrum Operacyjnego Cyberbezpieczeństwa, analizujemy, niwelujemy ewentualne straty, więc ten obszar cyber w Polsce, dzięki szerokiej współpracy bieżącej, powiem to połączone Centrum Bezpieczeństwa obraduje co tydzień. Natomiast w sposób ciągły współpracujemy, jeśli coś się dzieje jesteśmy 24 godziny na dobę na łączach. To jest ten obszar związany z cyberbezpieczeństwem tak w dużym skrócie, bo można byłoby o tym mówić więcej, bo tak jak powiedziałem na wstępie, jeśli będą pytania to oczywiście służę odpowiedzią.

Drugi zakres tematyczny Komisji, czyli walka z dezinformacją, niezwykle ważny, istotny i trudny. Na całym świecie, jak państwo doskonale wiedzą, ten poziom dezinformacji wraz z rozwojem Internetu, komunikacji, social mediów, portali internetowych narasta, wykorzystywany jest bardzo często przez również wrogie państwa do kreowania postaw obywateli, wpływania na decyzje wyborcze, więc to jest przedmiotem naszego zainteresowania. W ramach Ministerstwa Cyfryzacji są dwie dotacje, które są realizowane przez NASK. Jedna dotacja jest związana bezpośrednio z monitoringiem treści o potencjale dezinformacyjnym. Druga dotacja, tzw. bezpieczne wybory, gdzie obsługujemy to wszystko, co dzieje się w trybach wyborczych. Na bieżąco analizowana jest infosfera, jeśli chodzi o propagandę dezinformacji i walka z tym. W 2024 r. było 45 raportów tygodniowych, tłumaczonych również na język angielski, 49 raportów w rosyjskiej przestrzeni informacyjnej, 23 raporty dotyczące obecności rosyjskich przekazów dezinformacyjnych w polskiej sferze informacyjnej, 48 raportów dotyczących dezinformacji z innych rejonów świata niż tylko Federacja Rosyjska.

Realizowaliśmy również szereg raportów ad hoc, tematycznych, związanych choćby z powodzią, związanych choćby z sytuacją na wschodniej granicy, jeśli chodzi o szczepionki, wpływ szczepionek, COVID etc., więc na bieżąco monitorujemy to, dzielimy się tą wiedzą z zainteresowanymi interesariuszami i podejmujemy działania mające zminimalizować negatywne skutki dezinformacji. Dziękuję serdecznie.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie ministrze.

Kto teraz z panów zechciałby przedstawić? RCB? Bardzo proszę. Trzeba...

Doradca w Rządowym Centrum Bezpieczeństwa, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej Witold Skomra:

Zadziałało. Dziękuję, panie przewodniczący. Trochę techniki i człowiek się gubi.

Nawiązując do słów pana ministra. Owszem, prowadzimy zespół incydentów krytycznych, który w założeniach ustawowych ma niwelować spory kompetencyjne pomiędzy poszczególnymi CSIRT-ami. Przypominam, że mamy trzy podstawowe sfery: militarną, cywilną, administracja rządowa i operatorzy infrastruktury krytycznej. Ta trzecia sfera jest w domenie ABW. Na bieżąco natomiast funkcjonuje to połączone centrum i to połączone centrum działa na tyle skutecznie, że takie spory kompetencyjne, kto za co odpowiada się nie zdarzają praktycznie. Ustawodawca założył, że mogą zdarzać się sytuacje,

w której nikt nie odpowiada za zdarzenie. Mogę z całą odpowiedzialnością stwierdzić, że takich sytuacji nie ma. W ramach bieżącej współpracy te CSIRT-y na robocze ustalają, kto czym się zajmuje i bardzo często dzielą się pracami, czyli „ja rozpoznaję hardware, a ty popatrz, jak wpływa ten wyciek na funkcjonowanie innego obszaru” i często bywa tak, że formalnie incydem zajmuje się NASK, a tą warstwą głębszą zajmuje się wojsko. To działa świetnie i nie zdarzało się jeszcze, żeby trzeba było ingerować.

Natomiast jest możliwy incydent i dobrze, że takie forum działa, jest możliwe, że incydent cyber przeniesie się na stronę fizyczną – brak dostępu wody, prądu czy czegośkolwiek innego i wtedy ten zespół incydentów krytycznych może wnioskować o rządowy zespół zarządzania kryzysowego i przejście na tę warstwę decyzji politycznych. Dlatego istnienie takiego zespołu jest niezwykle istotne i bardzo potrzebne.

Jeżeli chodzi o naszą sferę oddziaływania, pan przewodniczący mnie przedstawił, odpowiadając za ochronę infrastruktury krytycznej i z tymi podmiotami głównie współpracujemy. Po pierwsze, raz do roku spotykamy się ze wszystkimi na forum wymiany informacji o sytuacji w infrastrukturze krytycznej. To jest jawne. Jawne, dlatego że ustawa dotychczasowa nie przewiduje obowiązku ochrony informacji niejawnych u operatorów IK z wyjątkiem pierwszego sektora, czyli energetyka, do tego się za chwilę odniosę. Dwa razy do roku organizujemy posiedzenia poświęcone bezpieczeństwu cyber właśnie w podmiotach infrastruktury krytycznej i współpracujemy w dziedzinie dezinformacji. Mianowicie przy Rządowym Zespole Zarządzania Kryzysowego funkcjonuje grupa zadaniowa zagrożeń hybrydowych i ten zespół hybrydowy współpracuje właśnie z NASK-iem, jeżeli chodzi o ocenę czy kampanie dezinformacyjne prowadzone w przestrzeni cyfrowej mają element czy mogą być elementem wojny hybrydowej i z drugiej strony z podobnym zespołem przy MSZ-cie w odniesieniu do spraw międzynarodowych i oddziaływania międzynarodowego, więc mamy takie trzy ośrodki, które wzajemnie wymieniają się informacjami na temat aktualnej sytuacji dezinformacyjnej.

Jeżeli chodzi o infrastrukturę krytyczną, to jesteśmy przekonani, że niektóre z tych kampanii, które trwają, a na pewno nowe się pojawiają, będą właśnie ukierunkowane na podważanie zaufania do władz i na wywoływanie niepokoju właśnie z budową nowych elementów energetycznych, głównie elektrownia jądrowa, nowe podstacje energetyczne, sieci energetyczne itd., o zmianie ewentualnej lokalizacji wiatraków nawet nie muszę wspominać, bo pamiętamy tę kampanię, gdzie wiatraki miały wywoływać raka i Bóg wie, co tam jeszcze. Tego typu działania są dla mnie rzeczą oczywistą, że wcześniej czy później się pojawiają.

Natomiast chciałbym wspomnieć o kilku problemach, których nie jesteśmy w stanie rozwiązać przy obecnym stanie prawnym i które uwzględniamy w nowelizacji ustawy o zarządzaniu kryzysowym. Pierwsza sprawa, wyciek wrażliwych danych o infrastrukturze krytycznej i operatorach infrastruktury krytycznej poprzez podwykonawców. To jest ciekawe, że podnieśliśmy poziom ochrony u operatorów IK i nie zdarzyło się, żeby bezpośrednio od któregoś z operatorów dane wyciekły i nie ma miesiąca, żeby jakieś dane dotyczące czy systemów ochrony, czy zawieranych umów, czy jakichś innych elementów, nie wyciekały od podwykonawców. Dlaczego? Dlatego, że ta informacja jest chroniona poprzez tzw. tajemnicę przedsiębiorcy, czyli ustawę o ochronie konkurencji, która jest bezsankcyjna i mówiąc brutalnie, jeżeli w zawieranej umowie z kontraktorem nie ma jakiejś potężnej kary za wyciek, to oni się nie przejmują danymi operatora infrastruktury krytycznej i to trzeba zmienić jak najszybciej. Dalej, operatorzy nie mają możliwości sprawdzania przeszłości osób, które nie są ich pracownikami i to jest drugi duży problem.

Teraz pokrótce przedstawiłbym, jakie rozwiązania przyjęliśmy w ustawie zmieniającej ustawę o zarządzaniu kryzysowym w tym obszarze dotyczącym infrastruktury krytycznej. Może przypomnę, że ta zmiana wynika z konieczności implementacji dyrektywy o odporności podmiotów krytycznych. W jednym Dzienniku Ustaw ukazały się 4 regulacje prawne, które powinny być realizowane jednocześnie. Jedna, o której wspominał pan minister, czyli dyrektywa NIS2 i stąd nowelizacja ustawy o KSC. Druga to jest właśnie dyrektywa o odporności podmiotów krytycznych, która będzie implementowana ustawą o zarządzaniu kryzysowym. Trzecia dotyczy systemu bankowego i to pominę milczeniem, bo od tego jest KNF i tam, ponieważ to jest rozporządzenie, więc nie wymaga implementacji, tylko dostosowania polskiego prawa, żeby rozporządzenie DORA było realizowane.

Odnosząc się do systemu bankowego, tu jest ciekawa zmiana. Do tej pory system bankowy pilnował, żeby nie był objęty żadnymi innymi regulacjami, nie mógł być uznawany za infrastrukturę krytyczną. W tej chwili się to zmienia. System bankowy będzie takim samym sektorem infrastruktury krytycznej, jak wszystko inne, z pewnymi wyłączeniami, będzie podlegał tym samym regulacjom, ale to szczegół.

Wróćmy do tej implementacji dyrektywy CER. Formalnie mieliśmy czas do 17 października tego roku na wdrożenie dyrektywy. Do dzisiaj proces legislacyjny ukończyły 4 kraje. Formalnie zakończenia procesu nie zgłosił żaden, taką informację mam z zeszłego tygodnia ani jeden kraj nie dał sobie z tym rady. Te kraje, które w ogóle zdążyły w terminie implementować ustawę na ogół nie miały wcześniej rozwiniętego systemu ochrony infrastruktury krytycznej, stąd było im łatwiej. Jeżeli ktoś to ma zrobione dobrze, a my jesteśmy jednym z 4 najlepiej chroniących infrastrukturę, to ci mają gorzej. Prosty przykład, my mamy 11 systemów infrastruktury krytycznej. Dyrektywa mówi o 11 sektorach infrastruktury krytycznej. Pozornie się zgadza. Jak dodamy 11 do 11, okazuje się, że trzeba 16, żeby nie burząc tego, co mamy, wdrożyć w pełni dyrektywę. To jest jeden z przykładów.

Co zamierzamy zrobić? Po pierwsze, upoważnić wojewodów do wskazania infrastruktury krytycznej, czyli wracamy w nieco zmienionej formie do idei lokalnej infrastruktury krytycznej, wprowadzić pojęcie potencjalnej infrastruktury krytycznej tak, żeby kryteriami objąć to, co jeszcze nie jest budowane, a jest na deskach kreślarskich. Elektrownia atomowa to jest numer 1, farmy wiatrowe to jest numer 2. Warunki bezpieczeństwa powinny być zapewnione na desce kreślarskiej, a nie dopiero, jak ten obiekt powstanie.

Dalej, wymaganie zdolności do przetwarzania informacji niejawnych, chociażby na poziomie „zastrzeżone”, tym najniższym, jakie obowiązuje, ale tak żeby dane dotyczące elementów bezpieczeństwa były chronione ustawą o ochronie informacji niejawnych, a nie ustawą o ochronie konkurencji. Zmieniamy sposób ochrony tychże informacji. Dotychczasowe zalecenia co do sześciu obszarów bezpieczeństwa zamierzamy wydać w formie rozporządzenia, czyli będą prawem powszechnie obowiązującym.

Co do incydentów, zamierzamy wprowadzić to w sposób zintegrowany z raportowaniem w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, czyli w oparciu o system S46. Jak już mamy incydent, to już wszyscy wiedzą o tym, że się coś stało i tu nie ma co ukrywać, tym bardziej, że odbiorcy będą i tak musieli jakieś działania mitygujące podjąć. Chcemy też zmienić sposób nadzoru i kontroli. Do tej pory wyglądało to tak, że zatwierdzaliśmy plany ochrony infrastruktury krytycznej i dalej nie było wiadomo, co się z tym dzieje. Teraz będzie to raport najwyższego kierownictwa o stanie ochrony obiektu czy usługi kluczowej na tym wyższym poziomie, poparty audytem bądź wewnętrznym, bądź zewnętrznym, ministrowie dostaną narzędzie w postaci możliwości zobowiązania podmiotu do przeprowadzenia audytu na własny koszt przez wskazaną firmę. Koniec końców to, czego nie było do tej pory w ustawie, czyli rozdział kary. Za niewykonywanie obowiązków związanych z ochroną infrastruktury krytycznej i usług kluczowych przewidujemy kary. Może nie tak dolegliwe, jak przewidywane w ustawie o KSC, ale niemniej chcemy powiązać działania najwyższego kierownictwa w dziedzinie ochrony infrastruktury i usług kluczowych właśnie z możliwością ukarania, zwłaszcza jeżeli dojdzie do incydentu. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Czy ktoś jeszcze z państwa chciałby coś uzupełnić? Nie widzę. Czy są zatem jakieś pytania od posłów? Bardzo proszę, pani posłanka Nowogórska.

Posel Urszula Nowogórska (PSL-TD):

Szanowny panie przewodniczący, szanowni państwo, mam takie pytanie: wspominał pan, że było kilka incydentów wynikających z ujawnienia danych wrażliwych przez firmy podwykonawcze. Proszę mi powiedzieć, czego dotyczyły tak naprawdę te informacje ujawniane? Czy to były dane techniczne, czy dane ludzkie i ile takich incydentów było w ostatnim czasie? Na przykład w ciągu ostatnich 3 lat. Bardzo dziękuję.

Doradca w RCB, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej Witold Skomra:

Danych z ostatnich 3 lat to nie mam. W tym roku, incydentów, w których zaszyfrowano dane i je pobrano – więc nie wiemy, co się z nimi stało – mieliśmy co najmniej 4. One

dotyczyły zarówno danych osobowych, jak i danych technicznych. Mam na myśli dane systemów sterowania przemysłowego, z firm ochroniarskich np. wpływały dane dotyczące kamer, dotyczące sposobu ochrony danego obiektu, systemów kontroli wejścia itd., więc w tym roku takich przypadków, gdzie podejrzewamy, że dane zostały pobrane mieliśmy co najmniej 4. Przynajmniej o takich wiemy.

Posel Urszula Nowogórska (PSL-TD):

Pytanie uzupełniające, jeżeli mogę, panie przewodniczący. Proszę mi powiedzieć, czy dostrzegł pan jakieś związki przyczynowo-skutkowe z przekazaniem informacji wrażliwych a ewentualnymi niepokojącymi zdarzeniami, które się zdarzały w odniesieniu do tej infrastruktury albo do tych przekazanych danych. Były takie zdarzenia?

Doradca w RCB, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej Witold Skomra:

Nie, czegoś takiego nie zaobserwowaliśmy. Te grupy, które się włamywały, żądały zwykle okupu. Jak grupa żąda okupu, to jest to jeszcze w miarę bezpieczne, bo gorzej, jeżeli się ktoś włamał, pobrał dane i nie zażądał okupu, bo to znaczy, że miał inne cele ukryte. Natomiast tak całkiem nie możemy być spokojni, bo nie jest wykluczone, że ten kto żąda okupu tych danych już komuś nie sprzedał wcześniej. Nawet przewidujemy sytuację, w której ktoś żąda okupu tylko po to, żeby zamaskować rzeczywisty cel, bo o co innego mu chodziło. Nie mieliśmy takiego przypadku, żeby powiązać wyciek danych z późniejszymi działaniami.

Natomiast oczywiście wszyscy użytkownicy są natychmiast informowani, że potencjalnie ich dane mogły wyciec i że powinni zmienić system organizacji, hasła dostępowe i wszystko, co jest związane z funkcjonowaniem systemu bezpieczeństwa, ale podkreślam, ciągle reagujemy post factum, a zabezpieczenie przed, oparte o tajemnicę przedsiębiorstwa jest za słabe i powinno być jak najszybciej zmienione.

Sekretarz stanu w MC Paweł Olszewski:

Jeśli mogę, panie przewodniczący, uzupełnić odpowiedź.

Przewodniczący poseł Konrad Fryszak (KO):

Tak, oczywiście. Bardzo proszę, panie ministrze.

Sekretarz stanu w MC Paweł Olszewski:

Uzupełniając, tych ataków i zaszyfrowania, m.in. wycieku danych jest zdecydowanie więcej, nie mówię tylko o infrastrukturze krytycznej, bo tyczy się również i samorządów, i tyczy się przedsiębiorstw, więc nie możemy skupiać się tylko i wyłącznie na 4 incydentach, bo tych incydentów jest zdecydowanie więcej, o czym też już wcześniej mówiłem.

Bardzo ważny wątek, o którym zaczął mówić pan dyrektor, a mianowicie wyciek danych i czy były one w jakikolwiek sposób wykorzystywane. Tu muszę się nie zgodzić z panem dyrektorem. Były wycieki danych, które były wykorzystywane, opinia publiczna o tym wiedziała, a mianowicie wyciek danych przez atak hakerski z Polskiej Agencji Antydopingowej, wyciekły bardzo istotne dane wrażliwe sportowców, które później zostały wykorzystane i tu nawiązuję też do dezinformacji jako drugiego punktu posiedzenia Komisji, zostały wykorzystane właśnie celem dezinformacji, to znaczy opublikowano w momencie olimpiady pomieszanie prawd, półprawd i kłamstw na bazie rzeczywistego wycieku danych, więc ta mechanika w taki sposób bardzo często wygląda.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję.

Teraz pan poseł Ściebiorowski.

Posel Łukasz Ściebiorowski (KO):

Dziękuję. Panie przewodniczący, pani minister, szanowni goście, są też widoczne różne kampanie, chyba w ostatnim czasie nawet gdzieś mi taka telewizyjna dotycząca dezinformacji mignęła i chyba to też jest dobry kierunek, żeby uświadamiać społeczeństwo, że nie każda informacja podawana, nawet zwłaszcza, w Internecie, może być prawdą i to jest istotne.

Mam też pytanie, bo pan minister tu już wspomniał, zahaczył o samorząd, a o to właśnie chciałbym zapytać, czy przede wszystkim te zdarzenia, które odbywają się na poziomie

samorządów, na poziomie lokalnym, dotyczące dezinformacji, ataków już też na ich infrastrukturę, też są do państwa obligatoryjnie zgłaszane? Czy macie od razu przepływ informacji, że takie się zdarzają i czy też tutaj współpracujecie z samorządami raz w celu zwrócenia uwagi, na co oni mają zwracać uwagę? Oni mają też swoje służby, swoich informatyków, którzy to wyłapują, ale zakładam, że na poziomie centralnym jest to bardziej profesjonalne czy powinno być, więc macie państwo większe narzędzia. Czy jest tutaj współpraca z samorządem w tym zakresie? Czy one się też zwracają same o wsparcie w zakresie tej dezinformacji i zapobieganiu tym atakom? Gros tych informacji dotyczących obywateli jest też tam w różnych urzędach, instytucjach, więc zakładam, że też samorządy powinny tutaj jak najbardziej być wyczułone na to. Dziękuję.

Sekretarz stanu w MC Paweł Olszewski:

Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję.

Pan minister? Bardzo proszę.

Sekretarz stanu w MC Paweł Olszewski:

Tak, przeprowadziliśmy, to znaczy jesteśmy w trakcie realizacji szerokiej kampanii reklamowej, że tak to nazwę, informacyjnej, edukacyjnej, zarówno w telewizji, rozgłośniach radiowych, na poziomie krajowym, regionalnym, telewizjach kablowych. Teraz państwo obserwują jeden wariant tej kampanii. Zaraz będą jeszcze dwa kolejne, równoległe są też cykle zarówno w radiu, jak i w telewizji takie edukacyjne. Podjęliśmy współpracę z 17 rozgłośniami regionalnymi Polskiego Radia, gdzie współfinansujemy program dotyczący higieny cyfrowej i kompetencji cyfrowych, rozwoju kompetencji cyfrowych, cyberbezpieczeństwa, więc ten walor, jeśli chodzi o cyberbezpieczeństwo i dezinformację, walor edukacyjny jest niezwykle istotny, bowiem bardzo często najsłabszym ogniwem jest człowiek i jego podatność. Stąd tutaj edukacja jest absolutnie kluczowa.

Jeśli chodzi natomiast o współpracę z samorządem, tak, współpracujemy z samorządem, tak, dofinansowujemy samorząd. Ponad 1,5 mld zł zostało przeznaczone na cyberbezpieczny samorząd. Praktycznie wszystkie samorządy w Polsce aplikowały o te środki i je otrzymają. W ramach KPO również będziemy komunikowali niedługo właśnie na forum Ministerstwa Cyfryzacji we współpracy z samorządami, marszałkami województw, ale również z wojewodami kolejne programy dotyczące samorządu, finansowania, współfinansowania tej odporności cybernetycznej samorządu, ale również i rządu. Prawdą jest to, co pan poseł powiedział, o ile instytucje państwowe szczebla centralnego można powiedzieć są w miarę dobrze zabezpieczone, choć to nie można powiedzieć, że w 100%, bo nikt nie jest w 100% zabezpieczony, bo jeszcze jest ten czynnik stricte ludzki, o tyle poziom samorządowy, w zależności od wielkości jednostki samorządu terytorialnego, umówmy się, wygląda różnie i mamy absolutnie na radarze to, tak kolokwialnie powiem, że samorząd wymaga bezwzględnie wsparcia i również własnego zaangażowania, bowiem dane, które są tam zgromadzone i funkcje, które samorząd pełni, mają istotne znaczenie dla funkcjonowania każdego z nas.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję.

Pan przewodniczący Lechowicz, bardzo proszę.

Poseł Piotr Lachowicz (KO):

Mam takie tylko pytanie czy też takie przemyślenie w stosunku do tego, co mówił pan dyrektor, jeśli chodzi o podwykonawców, bo rozumiem, że tam najwięcej było wycieków informacji i różnego rodzaju danych. W związku z tym słuszny kierunek, to znaczy, że tam trzeba wprowadzić klauzulę z zakresu ochrony informacji niejawnnej. Proponowałbym tylko, żeby to było minimum zagadnienia jednak, jeśli chodzi o klauzulę „poufne”, dlatego że w ustawie o ochronie informacji niejawnnych mamy taki dział, który się nazywa bezpieczeństwo przemysłowe i on mówi, że dokumentem potwierdzającym zdolność do ochrony informacji niejawnnych o klauzuli „poufne” lub wyższej jest świadectwo bezpieczeństwa przemysłowego, więc dobrze, żeby taki podwykonawca takie świadectwo miał. Natomiast

jeśli jest to działalność jednoosobowa to to jest oczywiście poświadczenie bezpieczeństwa, tylko trzeba założyć, że te przepisy mówią, że w przypadku, gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone” świadectwo nie jest wymagane. To jest wszystko w art. 54 ustawy o ochronie informacji. Dlatego moim zdaniem to dopuszczenie do dokumentów zastrzeżonych wymaga tylko i wyłącznie zgody szefa jednostki, więc taka moja uwaga, że słuszny kierunek, ale tutaj zastanawiałbym się nad podniesieniem klauzul do „poufnych”. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Troszeczkę idąc wspólnie tutaj z panem przewodniczącym, chciałbym zwrócić uwagę na to, że poza kwestią bezsprzeczną dla mnie, czyli wymaganie od podwykonawców konieczności posiadania poświadczenia bezpieczeństwa oczywiście na odpowiednim poziomie i to wydaje się dosyć proste, uważam, że to można nawet aktem rozporządzenia wprowadzić, to również zmusić dostawców infrastruktury krytycznej do tego, by w umowach zawierali wysokie kary z podwykonawcami za ujawnienie takich danych. To jest coś, co wydaje się dosyć łatwe do wprowadzenia, a to będzie wtedy powodowało wyższą dbałość tych podwykonawców o przestrzeganie tych tajemnic i o odpowiednią higienę, nazwijmy to, szeroko pojętą w sieci, żeby te dane były w odpowiedni sposób chronione i zabezpieczone.

Mam jeszcze dodatkowe pytanie do pana ministra i do pana dyrektora, do szanownych państwa, dosyć szerokie wydaje się, ale ile zdarzeń ze sfery tej cyber wypłynęło i wpłynęło na zdarzenia w sferze fizycznej. Czy możecie to jakoś w ostatnich miesiącach, latach spróbować nakreślić, ile takich zdarzeń i jakich gałęzi to dotyczyło, w jaki sposób się to przełożyło na działania fizyczne? Może pan minister.

Sekretarz stanu w MC Paweł Olszewski:

Pytanie jest w istocie szerokie. To zależy, jak oceniamy. To, co czasami się wydaje, że wypłynęło i nie zostało wykorzystane, zostało zaszyfrowane, nie znaczy, że jutro nie będzie odszyfrowane i nie będzie wykorzystane. Dzisiaj niektóre mechanizmy szyfrowania są takie, że nie są do odszyfrowania, ale jak wejdziemy w erę kwantową i będziemy mogli zaszyfrowywać w czasie rzeczywistym, to będzie istniała potencjalna szansa i ryzyko równoległe do tego, że będzie można odszyfrowywać, więc bardzo trudno jednoznacznie na to pytanie odpowiedzieć. Oczywiście, jeśli są wykradzione dane firm, to każdy może być dotknięty. Nie jestem w stanie, nie mam w głowie teraz statystyk, które te działania były skuteczne, które nie były skuteczne. O części możemy nawet nie wiedzieć, jeśli chodzi o prywatne podmioty, bowiem bardzo często zdarza się, że ci, którzy wykradają dane bądź szyfrują serwery, żądają okupu i nie mamy o tym wiedzy czy dany podmiot zapłacił ten okup, czy go nie zapłacił. Taka statystyka, żeby była wiarygodna wydaje mi się – chyba, że pan dyrektor ma inne odczucia – ale nie jesteśmy w stanie takiej wiarygodnej statystyki zrobić, fotografii rzeczywistości wszystkich podmiotów, które zostały zaatakowane.

Przewodniczący poseł Konrad Fryszak (KO):

OK. Bardzo dziękuję. Chyba, że pan dyrektor będzie chciał uzupełnić?

Doradca w RCB, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej Witold Skomra:

Nie, my też nie mamy takich dokładnych danych, musimy się posiłkować późniejszymi postępowaniami, jakie CSIRT-y prowadzą, jakie typy plików zostały wykradzione. Mamy różne przykłady, na przykład firma, która miała bardzo, bardzo, bardzo wrażliwe dane dotyczące wręcz obywateli, a wyciągnięto od niej dane dotyczące sytuacji finansowej, obrotów finansowych i jej pracowników, czyli to, co firma miała najcenniejsze w ogóle nie zostało pobrane. Prawdopodobnie włamywacze nie wiedzieli, co tam jest ważne i po omacku złapali to, co im się wydawało, za najcenniejsze i dające szansę na szantaż.

Natomiast, jeżeli wyciekły dane techniczne na przykład systemów sterowania, to nie wiemy, czy ktoś kiedyś tego nie użyje właśnie do zdalnego przesterowania urządzeń, a ponieważ to wycieka na przykład od serwisantów danej firmy, to może to dotyczyć praktycznie dowolnego podmiotu w kraju, który używa sterownika firmy takiej czy innej. Nawet, jeżeli dzisiaj takich danych twardych nie mamy, to istnieje potencjalne zagrożenie takich działań w przyszłości.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Jeszcze mam pytanie dodatkowe do panów z policji, ponieważ mam wiedzę o kilku zdarzeniach, które były zgłaszane. Czy panowie macie wiedzę, nie tak dawno, bo w poprzedniej kadencji powoływaliśmy CBZC, o tym, jaką ilość oni spraw prowadzili, jakiego charakteru są to zgłoszenia i czy CBZC może się pochwalić jakimiś ważnymi osiągnięciami w tej materii? O tym jednym, o którym słyszałem, nie chciałbym mówić.

Zastępca dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji Mariusz Cichomski:

Panie przewodniczący, szanowni państwo, jeśli mogę, to oddam głosu przedstawicielowi CBZC już bezpośrednio, przedstawimy dane.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo proszę.

Naczelnik Wydziału Nadzoru i Koordynacji Centralnego Biura Zwalczania Cyberprzestępczości Komendy Głównej Policji Piotr Tofiluk:

Panie przewodniczący, szanowni państwo, jako CBZC przyjęliśmy na początku zasadę, że sprawy szczególnie skomplikowane i te, które dotyczą incydentów, tak jak państwo już wspomnieli, ataków, mam tu na myśli ataki typu DOS, DDoS, tudzież ataki ransomware, gdzie głównym elementem jest zaszyfrowanie danych, żądanie okupu, chociaż nie zawsze, też widzimy od samego początku, że mamy tendencję wybitnie wzrostową. Jeżeli chodzi o jakieś liczby, którymi operujemy, na pewno, jeżeli chodzi o ataki ransomware od samego początku, od kiedy postaviliśmy, prowadziliśmy bądź prowadzimy 180 postępowań przygotowawczych. W tym roku było do nas zgłoszonych ponad 70 takowych spraw i one są w prowadzeniu. W niektórych przypadkach może niekoniecznie zostali ustaleni sprawcy odpowiedzialni za ten atak, ale którzy mają związek z tym atakiem, pełnią rolę na przykład księgowych, bo tu trzeba też mieć jasno określoną sytuację, że niejednokrotnie zajmują się tym grupy przestępcze o charakterze międzynarodowym. Oczywiście ten czynnik wschodni jest gdzieś zawsze z tyłu wspominany i osoby odpowiedzialne niejednokrotnie nie kryją się z tym, żeby wywodzić się z krajów byłego Związku Radzieckiego.

Jeżeli chodzi o ataki DDoS, one są w trochę mniejszej liczbie aniżeli ransomware. Tu takowych postępowań mieliśmy 23 od samego początku, od kiedy funkcjonujemy. W chwili obecnej prowadzimy ich 9.

Natomiast tu były wspomniane sprawy związane z wyciekami danych, o których już tu niektórzy z państwa wspominali. Tego w 2024 r. było naprawdę sporo. Nie za każdym razem posiadaliśmy wiedzę czy te dane zostały w jakikolwiek sposób wykorzystane, a skala ich wykorzystania może być różna, od zwykłych spraw związanych z oszustwami do wykorzystania tych danych do różnych celów, zarówno przestępczych, jak i skierowania podejrzenia na taką osobę, że jest odpowiedzialny na przykład za kaskadowe powiadomienia o alarmach bombowych czy w jakikolwiek inny sposób wykorzystania tych danych. Z mojej strony w chwili obecnej to tyle. Jeżeli mają państwo pytania bardzo chętnie odpowiem.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję.

Pan minister, bardzo proszę.

Sekretarz stanu w MC Paweł Olszewski:

Chciałbym uzupełnić, po pierwsze, podziękować CBZC, bo współpraca w ramach połączonego centrum operacyjnego cyberbezpieczeństwa z Policją w tym zakresie jest de facto ciągła. Dwa, statystyki, które są publiczne, one czasami zakłamują rzeczywistość, bowiem to, co dzieje się w sieci, jest wykrywane, realizowane przez CBZC, później w statystykach jest odzwierciedlone jako inne przestępstwo, choć było realizowane bezpośrednio przez CBZC, bo dotyczyło infosfery, a kwalifikacja czynu była na podstawie przepisów i kwalifikacje i później w statystyce było to odzwierciedlone, więc tu te statystyki dotyczące CBZC są niedoszacowane, bo gros roboty właśnie ta jednostka wykonuje. Tu wielkie podziękowania.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję.

O głos prosiła pani posłanka Nowogórska.

Posel Urszula Nowogórska (PSL-TD):

Tak jest. Bardzo dziękuję, panie przewodniczący. Zacznę może od tego, że bardzo się cieszę, że coraz lepszymi instrumentami dysponujemy jako państwo w celu zabezpieczenia danych i przeciwdziałania wyciekaniu tych danych czy też ewentualnej obrony w tym zakresie. Bardzo mnie zaniepokoił jeden fakt, o którym powiedział pan dyrektor w czasie swojej wypowiedzi, tej drugiej uzupełniającej. Mianowicie powiedział pan, że zdarzają się wycieki danych technicznych, które dotyczą na przykład zdalnych sterowników, które są montowane w różnego rodzaju typach urządzeń, również w takich urządzeniach, które odgrywają znaczącą rolę w zakresie działalności dotyczącej bezpieczeństwa również państwa.

Tutaj chciałabym zapytać, kieruję to pytanie również do pana, który reprezentuje stronę wojskową, czy jeżeli zdarzają się tego typu wycieki danych i mogą one mieć potencjalny wpływ na powstanie zagrożenia państwa czy też transportu materiałów, które mają znaczenie strategiczne dla państwa, czy w takich sytuacjach rozpoczyna się współpraca i przeciwdziałanie, jeżeli chodzi o działalność w zakresie Kontrwywiadu Wojskowego, Policji i innych służb w naszym państwie? Jak to się w ogóle technicznie odbywa?

Sekretarz stanu w MC Paweł Olszewski:

Jeśli mogę, przepraszam...

Przewodniczący poseł Konrad Fryszak (KO):

Pan minister, tak.

Sekretarz stanu w MC Paweł Olszewski:

W połączonym centrum operacyjnym cyberbezpieczeństwa, tak jak powiedziałem, są służby specjalne, jest DKWOC, jest CBZC, są przedstawiciele wszystkich CSIRT-ów, jak trzeba, w zależności od tego, z jakimś incydentem mamy do czynienia, dopraszani są przedstawiciele CSIRT-ów sektorowych, więc ta współpraca i koordynacja, jeśli chodzi o realizację i pomoc w eliminowaniu skutków incydentów jest ciągła, stała i regularna. Tak jak powiedział pan dyrektor, dzielimy się obowiązkami i zadaniami. Nawet jeśli różne są sytuacje i jeśli nawet dotyczy się to CSIRT-ów MON, który realizuje DKWOC, to też umiemy ocenić, kto jakimi zasobami dysponuje i wzajemnie się wspomóc. Myślę, że takiej koordynacji, jak w tym obszarze, to naprawdę trudno w Polsce szukać.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Czy są jeszcze... Pan dyrektor, bardzo proszę.

Doradca w RCB, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej Witold Skomra:

Wyjaśniając wątpliwości pani poseł, formalnie rzecz biorąc, obowiązuje zasada, że system sterowania przemysłowego powinien być galwanicznie odizolowany od Internetu i bez fizycznej obecności serwisanta na miejscu nie powinno dochodzić do jakiegokolwiek ujawniania danych. To jest teoria. Praktyka w firmach jest taka, że dyrektor do spraw finansowych chce wiedzieć, ile części zostało zużytych do produkcji dzisiaj po to, żeby zoptymalizować zakupy i on chce wiedzieć, ile danych przepłynęło przez sterownik, więc formalnie tego nie wolno robić, ale bardzo często spotykamy się z sytuacjami, w których jednak dane ze sterowników są pobierane i przetwarzane w systemach już IT, czyli przetwarzania danych, a nie systemów sterowania przemysłowego. Mogę powiedzieć tak, formalnie rzecz biorąc jest to dobrze zabezpieczone, ale życie mówi, że może niekoniecznie.

Druga sprawa, na którą chciałbym zwrócić uwagę, dotknęła pani bardzo delikatnego problemu, mianowicie podmioty cywilne realizujące usługi na rzecz sił zbrojnych formalnie podlegają pod CSIRT NASK, a nie pod wojsko. W związku z powyższym, jeżeli służby wojskowe sygnalizują problem wycieku danych, braku ochrony czy innych, musimy się dzielić zadaniami i to centrum operacyjne, o którym pan minister mówił, jest właśnie tym miejscem, gdzie trzeba podzielić zadania. Skoro jest to zadanie na styku

cywilno-wojskowym, to kto robi którą rzecz, żeby było to spójne. To jest jeden z poważniejszych problemów. Wiemy, jak wyglądają transporty na Ukrainę i kto je realizuje. Mieliśmy naprawdę najprzeróżniejsze przypadki, jak np. w rejonie Jasionki nieznany adwersarz próbował włamywać się do skrzynek pocztowych wszystkich firm, które miały wystawioną ofertę na niskopodwoziówki albo ciężarówki, albo cokolwiek innego, im mniejsza firma, tym lepiej, bo będzie słabiej zabezpieczona, a być może dowiemy się, co ona wozi, gdzie i w jakich terminach. To jest więc taki styk, który właśnie szczególnie wymaga współdziałania w ramach tego wspólnego centrum.

Przewodniczący poseł Konrad Frysztak (KO):

Pan przewodniczący Lachowicz jeszcze z dodatkowym pytaniem.

Poseł Piotr Lachowicz (KO):

Może nie z pytaniem, tylko chcę tutaj powiedzieć, że pani poseł Urszula Nowogórska taki ważny problem poruszyła, bo to chodzi też o sterowniki, o kontrolę różnego rodzaju. O ile skrzynki pocztowe to jest jeszcze pół biedy, ale gorzej, jeśli jest zewnętrzna ingerencja na przykład w transport kolejowy, który wiezie uzbrojenie lub amunicję w danym momencie jakimś krytycznym, który oby nie nastąpił i jest to ingerencja bez zgody zarówno przewoźnika, jak i właściciela, jak i producenta. Później są awantury różnego rodzaju, mamy takie przypadki w kraju, dosyć są znane. Dziękuję uprzejmie.

Przewodniczący poseł Konrad Frysztak (KO):

Bardzo dziękuję. Jeśli nie ma innych pytań, nie ma innych oświadczeń, stwierdzam, że na tym wyczerpaliśmy porządek dzisiejszego posiedzenia podkomisji.

Dziękuję wszystkim państwu za obecność i do zobaczenia.