UCHWAŁA nr 3
RADY do SPRAW CYFRYZACJI
z dnia 14 kwietnia 2022 r.
w sprawie wzmocnienia systemu cyberbezpieczeństwa w związku z inwazją Federacji Rosyjskiej na Ukrainie, skutkującej zagrożeniem dla bezpieczeństwa sieci i systemów teleinformatycznych oraz zasobów cyfrowych RP

Na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 17 Ministra Cyfryzacji z dnia 24 czerwca 2020 r. w sprawie ustanowienia regulaminu Rady do Spraw Cyfryzacji (Dz. Urz. z 2020 r. poz. 19), uchwala się, co następuje:

W związku z eskalacją wojny rosyjskiej na Ukrainie, także w domenie cyberprzestrzeni, skutkującej realnym zagrożeniem dla bezpieczeństwa Rzeczypospolitej Polskiej, Rada do spraw Cyfryzacji uważa, że mamy do czynienia z **bezprecedensową potrzebą wzmocnienia systemu cyberbezpieczeństwa w trybie nadzwyczajnym.** Jest to postulat tym bardziej uzasadniony, gdyż od kilkunastu miesięcy notowany jest gwałtowny wzrost incydentów i cyberataków, odnotowywanych przez CSIRTy krajowe, a od 4 marca br. utrzymuje się stan alarmowy CHARLIE CRP. Stan przygotowania i odporności systemu cyberbezpieczeństwa powinien współgrać ze stanem zagrożenia oraz dynamiką rozwoju wydarzeń na arenie międzynarodowej, dlatego konieczne jest:

(1) podjęcie działań legislacyjnych i organizacyjnych wychodzących poza dotychczasowe ramy przedmiotowe i czasowe podyktowane procesem legislacyjnym w Unii Europejskiej (Dyrektywa NIS2, Dyrektywa o odporności, inne);

(2) pilne przyjęcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa;

(3) szybsze i efektywne wdrażanie postanowień uchwały nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[1];

(4) rozpoczęcie procesu zmian systemowych w obszarze cyberbezpieczeństwa RP, przygotowującego Kraj na nowe i coraz bardziej zaawansowane wyzwania w domenie cyfrowej, wynikające zarówno z erozji środowiska bezpieczeństwa międzynarodowego, jak i dynamicznej transformacji cyfrowej, rozwoju i implementacji nowych i przełomowych technologii, a także z rozwijaniem nowych zdolności w zakresie cyberataków przez państwowych i niepaństwowych aktorów.

[1] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P.2019 poz. 1037)

W związku z powyższym Rada ds. Cyfryzacji w szczególności podkreśla pilną potrzebę podjęcia następujących działań:

Rada ds. Cyfryzacji rekomenduje uwzględnienie, w ramach planów ewentualności dotyczących sytuacji kryzysowych i zagrożeń bezpieczeństwa kraju, zagrożenia potencjalnymi rosyjskimi działaniami odwetowymi za militarne, sprzętowe i informacyjne wsparcie Polski dla Ukrainy. Możliwych zagrożeń należy upatrywać w cyberatakach (w tym typu *Advanced Persistent Threats*, APT) na infrastrukturę krajów zachodnich. Szczególne ryzyko dotyczy zagrożeń związanych z naruszeniami integralności systemów OT i IT m.in. wynikających z roli czynników wewnętrznych (zagrożenia typu *Insider Threat*) w całym łańcuchu dostaw. Działania odwetowe w związku z sankcjami ekonomicznymi skutkować natomiast mogą zwielokrotnioną liczbą i skalą ataków bezpośrednio wywołujących straty finansowe Federacji Rosyjskiej, w tym z użyciem oprogramowania szantażującego (ataki typu *Ransomware*).

Rada ds. Cyfryzacji rekomenduje, aby rząd RP we współpracy z ABW oraz ekspertami do spraw bezpieczeństwa sieci i systemów IT i OT, w tym - z polskich firm ICT, przeprowadził **kompleksowy i pilny przegląd bezpieczeństwa technicznego i operacyjnego** obiektów infrastruktury krytycznej. Przegląd ten powinien uwzględniać ryzyka wynikające z roli podmiotów trzecich, czyli dostawców usług w całym łańcuchu dostaw, zgodnie z podejściem „know your supplier”[2]. W pierwszej kolejności takie przeglądy należy przeprowadzić w sektorze energetycznym, dostaw innych krytycznych mediów (np.: wody), transportowym i służby zdrowia. W razie stwierdzonych nieprawidłowości, wyniki przeglądu powinny uruchamiać w trybie nadzwyczajnym dodatkowe i uzupełniające działania związane z zarządzaniem ryzykiem oraz zwiększaniem bezpieczeństwa i odporności tychże sieci i systemów. W szczególności mając na uwadze ostatnio występujące przypadki awarii, wynikające z działania systemów dystrybucji czasu, Rada rekomenduje, aby systemy lokalnej dystrybucji czasu były synchronizowane do systemu Głównego Urzędu Miar, działającego na podstawie przepisów opublikowanych w Rozporządzeniu Ministra Gospodarki, Pracy i Polityki Społecznej w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL)[3], a w przypadku braku łączności z GUM, do serwerów NTP opartych na satelitach europejskich GALILEO i/lub GALILEO+GPS. Jednocześnie należy zadbać, aby nie synchronizować się względem rosyjskiego systemu GLONASS i chińskiego BEIDOU. W szczególności, należy nie synchronizować się do serwerów publicznych nieznanego pochodzenia, a przede wszystkim zadbać o nieużywanie tzw. systemu automatycznego przydzielania serwerów.

[2] Adekwatną metodologię przedstawił na przykład National Institute of Standards and Technology, U.S. Department of Commerce w lutym 2021 r. w dokumencie Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.

[3] Rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 19 marca 2004 r. w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) (Dz. U. 2004 nr. 56 poz. 548)

Rada ds. Cyfryzacji rekomenduje podjęcie przez rząd RP pilnych **działań poprawiających koordynację operacyjną i świadomość sytuacyjną** w obszarze cyber-zagrożeń. Ich celem powinno być pogłębienie współpracy i wymiany informacji o atakach i incydentach w cyberprzestrzeni między wszystkimi podmiotami odpowiedzialnymi za system cyberbezpieczeństwa. W tym celu powstać powinny CSIRTy sektorowe (zgodnie z rekomendacją Rady w zakresie ograniczenia kradzieży tożsamości oraz cyberataków wykorzystujących polską infrastrukturę z 14 kwietnia 2022 r.) oraz Operacyjne Centra Bezpieczeństwa (*Security Operations Center*, SOC) w kluczowych dla bezpieczeństwa i odporności kraju podmiotach publicznych i prywatnych. Należy również uwzględnić potrzebę koordynacji działań na najwyższym szczeblu politycznym, na przykład w formule tzw. pokoju wojennego (war room), na wypadek wystąpienia zmasowanego cyberataku na sieci i systemy teleinformatyczne lub incydentu bezpieczeństwa. War room umożliwi Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni, szefom służb, ministrom (a w przypadkach nadzwyczajnych także Prezydentowi RP) podejmowanie decyzji i reagowanie na bieżące zagrożenia, wspieranie się wiedzą i informacjami przekazywanymi na bieżąco przez CSIRTy i specjalistów cyberbezpieczeństwa. Odpowiednią infrastrukturą i zapleczem do zorganizowania takiego centrum dowodzenia dysponuje aktualnie Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni.

Rada ds. Cyfryzacji rekomenduje podjęcie przez rząd **działań regulacyjnych o charakterze „ad hoc”**, uzupełniających regulacje związane z wprowadzonym stopniem alarmowym CHARLIE-CRP (i innymi w skali CRP). Regulacje te powinny dawać zarówno możliwość (poprzez zmiany w zakresie stosowania Prawa Zamówień Publicznych), jak i odpowiednią zachętę do podjęcia przez "instytucje utrzymujące kluczowe systemy IT" (przede wszystkim operatorów usług kluczowych), ale także szereg innych firm i instytucji, **pilnych działań zwiększających zdolność, nie tylko organizacyjną** (o której mówi *de facto* rozporządzenie do ustawy), **ale także techniczną, do ochrony sieci i systemów IT**. Należy bowiem pamiętać, że „poziom zabezpieczeń jest ściśle związany ze skalą inwestycji w cyberbezpieczeństwo”.

Rada ds. Cyfryzacji rekomenduje, aby rząd uzupełnił załącznik do Rozporządzenia Rady Ministrów w sprawie **wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym**[4] poprzez uwzględnienie w nim następujących typów przedsiębiorstw: operatorzy usług kluczowych z ust. o cyberbezpieczeństwie, podmioty które świadczą usługi przetwarzania danych na rzecz obiektów infrastruktury krytycznej, podmioty odpowiedzialne za prowadzenie i bezpieczeństwo kluczowych systemów informatycznych państwa oraz Centrów Przetwarzania Danych, w tym przetwarzających dane podmiotów publicznych, uczelni i podmiotów prywatnych. Uszczegółowieniu wynikającemu z transformacji cyfrowej gospodarki i instytucji państwa, powinien ulec także przedmiotowy zakres rozporządzenia.

Rada ds. Cyfryzacji rekomenduje, aby rząd rozwinął działania w zakresie cyberobrony, na przykładzie działań podejmowanych aktualnie przez rząd Ukrainy, który stworzył Cyber Ligę

[4] Rozporządzenie Rady Ministrów z dnia 3 listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz.U. 2020 poz. 1647)

realizującą działania wspierające obronę cyberprzestrzeni. **Rozwój i wsparcie istniejącej Polskiej Obywatelskiej Cyberobrony** integrującej cyberspecjalistów, powinny być prowadzone równolegle do działalności Cyberkomponentu w Wojskach Obrony Terytorialnej i Zespołu Działań Cyberprzestrzennych (ZDC), które stanowić mają kuźnię kadr dla Wojsk Obrony Cyberprzestrzeni.

Rada ds. Cyfryzacji rekomenduje stworzenie realnego partnerstwa publiczno-prywatnego z polskim sektorem firm cybersecurity, w tym zintegrowanych w ramach Polskiego Klastra Cyberbezpieczeństwa, które mogłoby wzmacniać system cyberbezpieczeństwa kraju, a także wymieniać się wiedzą i budować rekomendacje dla dalszego rozwoju sektora. Tym samym **Rada ds. Cyfryzacji rekomenduje**, aby rząd poprzez rozpoczęcie efektywnej współpracy między państwem a polskim sektorem ICT i cyberbezpieczeństwa, aktywnie **wspierał budowę polskich zdolności cyberofensywnych i cyberobronnych w wymiarze technologicznym**, przeznaczając na ten cel większą i odpowiednią pulę środków finansowych mających na celu stworzenie silnego sektora cyberbezpieczeństwa, jako filaru rozwoju gospodarczego i bezpieczeństwa kraju.

Rada ds. Cyfryzacji rekomenduje, aby w ramach działań zmierzających do zwiększenia bezpieczeństwa cyberprzestrzeni, uwzględnić także **potrzebę fizycznego bezpieczeństwa infrastruktury cyfrowej i zasobów cyfrowych państwa**, w tym poprzez zabezpieczenie kluczowych zasobów informatycznych i informacyjnych na wypadek zmasowanego cyberataku, ataku militarnego, a nawet zajęcia części terytorium Polski. W przypadku fizycznej utraty lub nieodwracalnego uszkodzenia kluczowych zakresów danych, przetwarzanych na terenie Polski, państwo zostanie pozbawione możliwości prawidłowego funkcjonowania w obszarach utraty lub uszkodzenie danych. Szczegóły rekomendacji znajdują się w załączniku 1.

Rada ds. Cyfryzacji rekomenduje, aby docelowo w związku z potrzebami wynikającymi z realizacji zadań przewidzianych w Strategii Cyberbezpieczeństwa oraz z ustawy o Krajowym Systemie Cyberbezpieczeństwa, a także z realizacji wszystkich koniecznych działań zmierzających do zapewnienia bezpieczeństwa cyberprzestrzeni w sektorze cywilnym, powołana została Narodowa Agencja Cyberbezpieczeństwa NAC jako państwowa agencja wykonawcza, podlegająca bezpośrednio Prezesowi Rady Ministrów.

NAC powinna jako „parasol" integrować dotychczas rozproszone w ramach administracji publicznej kompetencje, wiedzę i zasoby w przedmiotowym obszarze, a także dążyć do uzupełnienia ich poprzez budowę nowych zdolności i kompetencji.

Działania te powinny być szczególnie prowadzone w zakresie:

- **podniesienia sprawności Krajowego Systemu Cyberbezpieczeństwa oraz jego uelastycznienia,**
- **dodatkowych działań w zakresie cyberbezpieczeństwa na zlecenia uprawnionych organów - w sytuacji wystąpienia potrzeby ich realizacji;**

- **zbudowania krajowego systemu certyfikacji cyberbezpieczeństwa w modelu publiczno-prywatnym (w tym nowych technologii - 5G, IoT, cloud computing)**
- **koordynacji kluczowych projektów państwa, zapewniając spójność standardów oraz wymagań cyberbezpieczeństwa;**
- **zwiększenia kompetencji technicznych i technologicznych państwa w zakresie analizy, diagnozy i atrybucji ataków, w tym poprzez utworzenie centralnego laboratorium cyberbezpieczeństwa i inżynierii wstecznej,**
- **opracowania kryteriów i metod oceny bezpieczeństwa kluczowych systemów ICT;**
- **zwiększenia zdolności koordynacji incydentów cyberbezpieczeństwa w sektorze cywilnym;**
- **zbudowania kompetencji i praktyki w zakresie tworzenia technologii i rozwiązań dla cyberbezpieczeństwa we współpracy z polskimi firmami ICT.**

Rada ds. Cyfryzacji podkreśla, że istotne jest także jak najpilniejsze wdrożenie zaleceń przedstawionych w formie rekomendacji załączonych do niniejszej uchwały oraz opublikowanych w terminie wcześniejszym dokumentów:

- **Uchwała nr 1 Rady do Spraw Cyfryzacji** z dnia 31 stycznia 2022 roku w sprawie powołania Centralnego Biura Zwalczania Cyberprzestępczości.
- **Uchwała nr 2 Rady do Spraw Cyfryzacji** z dnia 3 lutego 2022 roku w sprawie dystrybucji i synchronizacji czasu.

Załączniki:

1. Rekomendacja stworzenia „cyfrowej ambasady RP" w celu zapewnienia suwerenności cyfrowej i bezpieczeństwa informacyjnego państwa oraz jego cyfrowych zasobów
2. Rekomendacja w sprawie walki z dezinformacją jako zagrożeniem cyberbezpieczeństwa Państwa
3. Rekomendacja w przedmiocie utworzenia systemów łączności strategicznej związanych z zapewnieniem bezpieczeństwa w cyberprzestrzeni RP
4. Rekomendacje w zakresie ograniczenia kradzieży tożsamości oraz cyberataków wykorzystujących polską infrastrukturę

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone na posiedzeniu Rady do Spraw Cyfryzacji. Projekt Uchwały nr 3 wraz z załącznikami został poddany głosowaniu w dniu 14 kwietnia 2022 r. W głosowaniu wzięło udział 13 członków Rady, z czego oddano:

- 13 głosów „za" przyjęciem uchwały wraz z załącznikami,
- 0 głosów „przeciw" oraz
- 0 głosów „wstrzymuję się".

Uchwała nr 3 Rady do Spraw Cyfryzacji została przyjęta 14 kwietnia 2022 roku w głosowaniu jawnym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Andrzej	Dulka	za
2.	Agnieszka	Gryszczyńska	za
3.	Michał	Kanownik	za
4.	Janusz	Kosiński	za
5.	Karol	Krawczyk	za
6.	Anna Beata	Kwiatkowska	za
7.	Mirosław	Maj	za
8.	Dariusz	Milka	za
9.	Józef	Orzeł	za
10.	Bolesław	Piasecki	za
11.	Paweł	Śniatała	za
12.	Robert	Trętowski	za
13.	Mateusz	Tykierko	za

Przewodniczący Rady

Józef Orzeł

/-podpisano elektronicznie/