2024/1101

12.4.2024

ZALECENIE KOMISJI (UE) 2024/1101

z dnia 11 kwietnia 2024 r.

w sprawie skoordynowanego planu wdrożenia dotyczącego przejścia na kryptografię postkwantową

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 ([1]) (dyrektywa NIS 2),

a także mając na uwadze, co następuje:

(1) Ochrona danych i zabezpieczanie komunikacji szczególnie chronionej mają zasadnicze znaczenie dla społeczeństwa, gospodarki, bezpieczeństwa i dobrobytu Unii. Cyberbezpieczeństwo ma strategiczne znaczenie dla budowania „Europy na miarę ery cyfrowej" ([2]) i jest kluczowym celem programu polityki „Droga ku cyfrowej dekadzie" ([3]).

(2) Zarówno w strategii UE w zakresie unii bezpieczeństwa ([4]), jak i w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę ([5]) podkreślono, że szyfrowanie jest kluczową technologią służącą osiągnięciu odporności i suwerenności technologicznej oraz budowaniu zdolności operacyjnych w celu zapobiegania cyberatakom. W istocie szyfrowanie ma zasadnicze znaczenie dla świata cyfrowego celem zabezpieczenia systemów i transakcji cyfrowych, ochrony szeregu praw podstawowych, a także w celu zabezpieczenia zdolności obronnych. Wyścig, w którym różne kraje i podmioty prywatne konkurują w celu rozwijania zdolności w zakresie obliczeń kwantowych i stworzenia nowych, potencjalnie satysfakcjonujących możliwości, stanowi zagrożenie dla obecnych standardów kryptograficznych. Standardy te odgrywają decydującą rolę w zapewnianiu poufności i integralności danych, zabezpieczeniu komunikacji szczególnie chronionej oraz wspieraniu podstawowych elementów bezpieczeństwa sieci.

(3) Potencjalny rozwój w przyszłości komputerów kwantowych zdolnych do złamania stosowanych obecnie szyfrów sprawia, że Europa musi poszukiwać silniejszych zabezpieczeń, zapewniających zabezpieczenie komunikacji szczególnie chronionej i długoterminową integralność informacji poufnych, w szczególności poprzez jak najszybsze przejście na kryptografię postkwantową. Ten nowy rodzaj kryptografii usunie znane słabe punkty obecnej kryptografii asymetrycznej i zwiększy odporność na zagrożenia wynikające ze złośliwego wykorzystania komputerów kwantowych.

(4) Od ponad dziesięciu lat Komisja finansuje badania i rozwój kryptografii postkwantowej, uznając potencjalne zagrożenia, jakie obliczenia kwantowe stwarzają dla obecnej kryptografii asymetrycznej.

(5) Państwa członkowskie powinny rozważyć jak najszybszą migrację swojej obecnej infrastruktury cyfrowej i usług cyfrowych dla administracji publicznej oraz innych infrastruktur krytycznych w kierunku kryptografii postkwantowej, co doprowadzi do zasadniczej zmiany w algorytmach, protokołach i systemach kryptograficznych. Jak podkreślono w niedawno wydanej białej księdze Komisji pt. „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej" (ang. „How to master Europe's digital infrastructure needs"), wymaga to skoordynowanych wysiłków z udziałem agencji rządowych, jednostek normalizacyjnych, zainteresowanych stron z branży, naukowców i specjalistów w dziedzinie cyberbezpieczeństwa.

(6) W niniejszym zaleceniu Komisji zachęca się państwa członkowskie do opracowania kompleksowej strategii przyjęcia kryptografii postkwantowej w celu zapewnienia przejścia, które byłoby skoordynowane i zsynchronizowane między poszczególnymi państwami członkowskimi i ich sektorami publicznymi. W strategii tej należy określić jasne cele, kamienie milowe i harmonogramy prowadzące do określenia wspólnego planu wdrożenia kryptografii

([1]) Dz.U. L 333 z 27.12.2022, s. 80.
([2]) COM(2020) 67 final.
([3]) Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. (Dz.U. L 323 z 19.12.2022, s. 4).
([4]) COM(2020) 605 final.
([5]) JOIN(2020) 18 final.

postkwantowej. Powinno to doprowadzić do wdrożenia w całej Unii technologii kryptografii postkwantowej w istniejących systemach administracji publicznej i infrastrukturach krytycznych za pośrednictwem systemów hybrydowych, które mogą łączyć kryptografię postkwantową z istniejącymi podejściami kryptograficznymi lub z kwantową dystrybucją klucza.

(7) W celu skutecznego przejścia na kryptografię postkwantową skoordynowany plan wdrożenia kryptografii postkwantowej powinien zawierać wykaz działań, które mają zostać podjęte przez państwa członkowskie, w tym uwzględnienie algorytmów kryptografii postkwantowej, wraz z jasnym harmonogramem poszczególnych etapów i kamieni milowych, z uwzględnieniem ich współzależności, a także zainteresowanych stron, które należy włączyć w ten proces.

(8) W celu zharmonizowanego wdrożenia kryptografii postkwantowej w całej Unii niezbędne jest opracowanie wspólnych norm europejskich oraz opracowanie ram celem określenia i wyboru algorytmów kryptografii postkwantowej, które mają być stosowane w sieciach i usługach cyfrowych w całej Unii. Dzięki aktywnemu uczestnictwu naukowców finansowanych przez UE Unia już teraz wspiera opracowywanie i testowanie algorytmów kryptografii postkwantowej, które mogłyby zostać przyjęte jako normy w ramach międzynarodowych procesów selekcji kryptografii postkwantowej. W niniejszym zaleceniu Komisji zachęca się państwa członkowskie do ścisłej współpracy na szczeblu UE z unijnymi ekspertami w dziedzinie cyberbezpieczeństwa, grupą współpracy ds. bezpieczeństwa sieci i informacji oraz Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w zakresie oceny i wyboru odpowiednich algorytmów kryptografii postkwantowej oraz ich przyjmowania jako norm UE na potrzeby zharmonizowanego wdrażania w całej Unii.

(9) Państwa członkowskie i Unia powinny nadal aktywnie współpracować ze swoimi międzynarodowymi partnerami strategicznymi przy opracowywaniu międzynarodowych norm w zakresie kryptografii postkwantowej w celu zapewnienia przyszłej interoperacyjności komunikacji.

(10) Po jego uzgodnieniu przez państwa członkowskie skoordynowany plan wdrożenia kryptografii postkwantowej powinien służyć jako model dla określenia krajowych planów przejścia na kryptografię postkwantową lub, w przypadku gdy istnieją już plany krajowe, ich dostosowania do wspólnego skoordynowanego planu wdrożenia kryptografii postkwantowej.

(11) Aby zapewnić postępy w realizacji celów niniejszego zalecenia, Komisja zamierza ściśle monitorować działania podejmowane w odpowiedzi na to zalecenie. Zachęca się zatem państwa członkowskie do przedkładania Komisji, na jej wniosek, wszystkich istotnych informacji, których dostarczenia można zasadnie oczekiwać, w celu zapewnienia takiego monitorowania. Na podstawie uzyskanych w ten sposób informacji i wszystkich innych dostępnych informacji Komisja oceni skutki niniejszego zalecenia i ustali, czy konieczne są dodatkowe kroki, w tym zaproponowanie wiążących aktów prawa Unii.

(12) Niniejsze zalecenie w sprawie kryptografii postkwantowej opiera się na celach polityki określonych w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę w celu poprawy pełnego bezpieczeństwa i odporności unijnej infrastruktury cyfrowej i usług cyfrowych dla administracji publicznej oraz innych infrastruktur krytycznych; służy realizacji celów jednolitego rynku cyfrowego oraz wspólnego komunikatu w sprawie europejskiej strategii bezpieczeństwa gospodarczego 10919/23 ([6]); a także uwzględnia zagrożenia dla bezpieczeństwa fizycznego i cyberbezpieczeństwa infrastruktur krytycznych oraz zagrożenia zidentyfikowane w ramach niedawno przeprowadzonej oceny ryzyka dla technologii kwantowych ([7]). Niniejsze zalecenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej (art. 7, 8 i 11) oraz w europejskiej konwencji praw człowieka (art. 8 i 10), które nakładają na rządy obowiązki działania celem zminimalizowania ryzyka bezprawnego dostępu do informacji i ich kontroli, co wymaga ochrony i promowania technologii kryptograficznych,

([6]) https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/en/pdf
([7]) JOIN(2023) 20 final.

PRZYJMUJE NINIEJSZE ZALECENIE:

1. ZAKRES I CELE

Celem niniejszego zalecenia jest wspieranie przejścia na kryptografię postkwantową, aby chronić infrastrukturę cyfrową i usługi cyfrowe dla administracji publicznej i innych infrastruktur krytycznych w Unii poprzez umożliwienie państwom członkowskim:

1) określenia skoordynowanego planu wdrożenia kryptografii postkwantowej mającego na celu zsynchronizowanie wysiłków państw członkowskich na rzecz opracowania i wdrożenia krajowych planów przejścia na kryptografię postkwantową przy jednoczesnym zapewnieniu interoperacyjności transgranicznej;

2) wspierania oceny i wyboru odpowiednich unijnych algorytmów kryptografii postkwantowej z pomocą ekspertów w dziedzinie cyberbezpieczeństwa, a następnie przyjmowania takich algorytmów jako norm unijnych, które należy wdrożyć w całej Unii w ramach skoordynowanego planu wdrożenia kryptografii postkwantowej;

3) wprowadzenia odpowiednich i proporcjonalnych środków w celu przygotowania się do tego przejścia.

2. SKOORDYNOWANY PLAN WDROŻENIA DOTYCZĄCY PRZEJŚCIA NA KRYPTOGRAFIĘ POSTKWANTOWĄ

4) W niniejszym zaleceniu zachęca się państwa członkowskie do koordynowania działań na szczeblu Unii za pośrednictwem specjalnego forum państw członkowskich. W tym celu Komisja zaleca, aby państwa członkowskie korzystały z istniejących na szczeblu Unii struktur w dziedzinie cyberbezpieczeństwa i utworzyły podgrupę w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji. W skład takiej podgrupy mogliby wchodzić przedstawiciele krajowych agencji ds. bezpieczeństwa i eksperci w dziedzinie cyberbezpieczeństwa, w szczególności z krajowych organów ds. cyberbezpieczeństwa i ENISA. Podgrupa ta mogłaby zapraszać do udziału w swoich pracach przedstawicieli odpowiednich zainteresowanych stron, takich jak organy doradcze organizacji publicznych, podmioty z branży, usługodawcy i operatorzy, w celu gromadzenia i wymiany informacji na temat przejścia infrastruktury cyfrowej i usług cyfrowych dla administracji publicznej i innych infrastruktur krytycznych na kryptografię postkwantową w różnych sektorach, koordynowania ich wysiłków na szczeblu krajowym oraz opracowania skoordynowanego planu wdrożenia kryptografii postkwantowej, zgodnie z unijnymi regułami konkurencji i unijnymi przepisami o ochronie danych.

5) Ta podgrupa ds. kryptografii postkwantowej powinna rozważyć odpowiednie, skuteczne i proporcjonalne środki służące określeniu i skoordynowaniu opracowywania skoordynowanego planu wdrożenia kryptografii postkwantowej. Podgrupa ds. kryptografii postkwantowej powinna zaangażować się w dyskusje z innymi właściwymi organami, takimi jak Europol, NATO lub inne organy, aby uniknąć powielania wysiłków i zapewnić spójne podejście w obliczu pojawiających się wyzwań.

6) W tym celu zachęca się państwa członkowskie, by wkrótce po opublikowaniu niniejszego zalecenia ustanowiły taką podgrupę ds. kryptografii postkwantowej zgodnie z decyzją wykonawczą Komisji (UE) 2017/179 ([8]) oraz wyznaczyły reprezentujących je ekspertów, którzy powinni ściśle współpracować z Komisją i którym należy powierzyć zadanie określenia i opracowania skoordynowanego planu wdrożenia kryptografii postkwantowej.

7) Skoordynowany plan wdrożenia kryptografii postkwantowej powinien być dostępny po upływie dwóch lat od opublikowania niniejszego zalecenia, po czym nastąpi opracowanie i dalsze dostosowanie planów przejścia na kryptografię postkwantową poszczególnych państw członkowskich, zgodnie z zasadami określonymi w skoordynowanym planie wdrożenia kryptografii postkwantowej.

3. DZIAŁANIA NA SZCZEBLU UNII

8) Komisja we współpracy z ekspertami z państw członkowskich będzie okresowo monitorowała i oceniała całość prac.

([8]) Decyzja wykonawcza Komisji (UE) 2017/179 z dnia 1 lutego 2017 r. ustanawiająca procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 28 z 2.2.2017, s. 73).

9) W tym celu Komisja może zwrócić się do przedstawicieli państw członkowskich o przedłożenie wszystkich istotnych informacji, których dostarczenia można zasadnie od nich oczekiwać, w celu zapewnienia monitorowania postępów osiągniętych w opracowywaniu takiego skoordynowanego planu wdrożenia kryptografii postkwantowej oraz skuteczności takich środków.

10) Na podstawie przekazanych w ten sposób oraz wszystkich innych dostępnych informacji Komisja oceni opracowane środki i funkcjonowanie sieci przedstawicieli państw członkowskich oraz ustali, czy konieczne są dodatkowe działania, w tym zaproponowanie wiążących aktów prawa Unii.

4. **PRZEGLĄD**

11) Państwa członkowskie powinny współpracować z Komisją w celu oceny skutków niniejszego zalecenia najpóźniej trzy lata po jego opublikowaniu w celu określenia odpowiednich dalszych działań. Ocena ta powinna uwzględniać wyniki prac złożonej z ekspertów krajowych podgrupy ds. kryptografii postkwantowej.

Sporządzono w Brukseli dnia 11 kwietnia 2024 r.

W imieniu Komisji
Thierry BRETON
Członek Komisji