Cyberbezpieczeństwo w UE: Komisja proponuje utworzenie wspólnej jednostki ds. cyberprzestrzeni, aby lepiej reagować na incydenty na dużą skalę zagrażające naszemu bezpieczeństwu

Bruksela, 23 czerwca 2021 r.

Komisja przedstawia dziś wizję utworzenia nowej **wspólnej jednostki ds. cyberprzestrzeni**, która zajmie się rosnącą liczbą poważnych cyberincydentów mających wpływ na usługi publiczne, przedsiębiorstwa i obywateli w całej Unii Europejskiej. Zaawansowane i skoordynowane działania w dziedzinie cyberbezpieczeństwa stają się coraz bardziej potrzebne, ponieważ liczba, skala i skutki cyberataków rosną, co w dużym stopniu wpływa na nasze bezpieczeństwo. Wszystkie właściwe podmioty w UE muszą być przygotowane do wspólnego reagowania i wymiany informacji na zasadzie potrzebnego, a nie ograniczonego, dostępu.

Wspólna jednostka ds. cyberprzestrzeni została ogłoszona po raz pierwszy przez przewodniczącą Ursulę **von der Leyen** w wytycznych politycznych. Celem zaproponowanej dziś jednostki jest zgromadzenie zasobów i wiedzy fachowej dostępnych w UE i jej państwach członkowskich, aby skutecznie zapobiegać masowym cyberincydentom i cyberkryzysom, powstrzymywać je i reagować na nie. Społeczności zajmujące się cyberbezpieczeństwem, w tym społeczności cywilne, organy ścigania, dyplomacji i cyberobrony, a także partnerzy z sektora prywatnego, zbyt często działają oddzielnie. Dzięki wspólnej jednostce ds. cyberprzestrzeni uzyskają one wirtualną i fizyczną platformę współpracy: właściwe instytucje, organy i agencje UE wraz z państwami członkowskimi będą stopniowo budować europejską platformę na rzecz solidarności i pomocy w celu przeciwdziałania cyberatakom na dużą skalę.

Zalecenie w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni stanowi ważny krok w kierunku ukończenia europejskich ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa. Jest to konkretny rezultat strategii UE w zakresie cyberbezpieczeństwa i strategii UE w zakresie unii bezpieczeństwa, przyczyniający się do bezpiecznej gospodarki cyfrowej i społeczeństwa cyfrowego.

W ramach tego pakietu Komisja przedstawia dziś sprawozdanie z postępów poczynionych w ostatnich miesiącach w ramach strategii w zakresie unii bezpieczeństwa. Ponadto Komisja i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili pierwsze sprawozdanie z realizacji strategii w zakresie cyberbezpieczeństwa, zgodnie z wnioskiem Rady Europejskiej, a jednocześnie opublikowali piąte sprawozdanie z postępów we wdrażaniu wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r. oraz wspólnego komunikatu z 2018 r. w sprawie zwiększenia odporności i wzmocnienia zdolności reagowania na zagrożenia hybrydowe. Ponadto Komisja wydała decyzję w sprawie ustanowienia biura Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w Brukseli, zgodnie z aktem o cyberbezpieczeństwie.

Nowa wspólna jednostka ds. cyberprzestrzeni służąca zapobieganiu cyberincydentom na dużą skalę i reagowania na nie

Wspólna jednostka ds. cyberprzestrzeni będzie działać jako platforma zapewniająca **skoordynowaną reakcję UE** na cyberincydenty i cyberkryzysy na dużą skalę, a także oferująca **pomoc** w usuwaniu skutków tych ataków. Obecnie w UE i państwach członkowskich działa wiele podmiotów zaangażowanych w różne dziedziny i sektory. Chociaż sektory są zróżnicowane, spotykają się one często z tymi samymi zagrożeniami – stąd potrzeba **koordynacji, dzielenia się wiedzą, a nawet wczesnego ostrzegania**.

Uczestnicy zostaną poproszeni o zapewnienie zasobów operacyjnych na potrzeby wzajemnej pomocy w ramach wspólnej jednostki ds. cyberprzestrzeni (tutaj można zapoznać się z listą proponowanych uczestników). Wspólna jednostka ds. cyberprzestrzeni umożliwi uczestnikom wymianę najlepszych praktyk, a także informacji w czasie rzeczywistym na temat zagrożeń, które mogą pojawić się w obszarach ich działania. Będzie również **pracować na szczeblu operacyjnym i technicznym** w celu realizacji unijnego planu reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, w oparciu o plany krajowe, ustanowienia i mobilizacji unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa, ułatwienia przyjmowania protokołów wzajemnej pomocy między

uczestnikami, ustanowienia krajowych i transgranicznych zdolności w zakresie monitorowania i wykrywania, w tym centrów monitorowania bezpieczeństwa (SOC) oraz w innych obszarach.

Unijny ekosystem cyberbezpieczeństwa jest szeroki i zróżnicowany. Dzięki wspólnej jednostce ds. cyberprzestrzeni powstanie **wspólna przestrzeń** współpracy między różnymi społecznościami i obszarami, co umożliwi wykorzystanie pełnego potencjału istniejących sieci. Jest to kontynuacja prac rozpoczętych w 2017 r., kiedy przyjęte zostało zalecenie w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę – tak zwany plan działania.

Komisja proponuje budowanie wspólnej jednostki ds. cyberprzestrzeni w drodze **stopniowego i przejrzystego procesu** obejmującego cztery etapy. Współodpowiedzialne za ten proces będą państwa członkowskie i różne podmioty aktywne w tym obszarze. Celem jest operacyjność wspólnej jednostki ds. cyberprzestrzeni do 30 czerwca 2022 r. oraz ukończenie jej tworzenia rok później – 30 czerwca 2023 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) będzie w fazie przygotowawczej pełnić rolę sekretariatu. Wspólna jednostka będzie powstawać w bezpośrednim pobliżu biur agencji w Brukseli oraz biura CERT-UE – zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE.

Inwestycje niezbędne do utworzenia wspólnej jednostki ds. cyberprzestrzeni zostaną zapewnione przez Komisję, przede wszystkim w ramach programu „Cyfrowa Europa”. Środki finansowe będą służyć budowie fizycznej i wirtualnej platformy, ustanowieniu i utrzymaniu bezpiecznych kanałów komunikacji, a także poprawie zdolności wykrywania. Dodatkowe wkłady, zwłaszcza w rozwój zdolności państw członkowskich w zakresie cyberobrony, mogą pochodzić z Europejskiego Funduszu Obronnego.

Zapewnienie Europejczykom bezpieczeństwa w internecie i poza nim

Komisja przedstawia dziś sprawozdanie z **postępów** poczynionych w ramach strategii UE w zakresie unii bezpieczeństwa, której celem jest zapewnienie Europejczykom bezpieczeństwa. Wraz z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa Komisja przedstawia również pierwsze sprawozdanie z realizacji nowej strategii UE w zakresie cyberbezpieczeństwa.

Komisja i wysoki przedstawiciel przedstawili **strategię UE w zakresie cyberbezpieczeństwa** w grudniu 2020 r. Dzisiejsze sprawozdanie podsumowuje postępy poczynione w ramach każdej z **26 inicjatyw** określonych w strategii i odnosi się do niedawnego zatwierdzenia przez Parlament Europejski i Radę Unii Europejskiej rozporządzenia ustanawiającego **centrum kompetencji w dziedzinie cyberbezpieczeństwa i sieć ośrodków koordynacji**. Dzięki proponowanej dyrektywie w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (zmienionej dyrektywie w sprawie bezpieczeństwa sieci i informacji – NIS 2) osiągnięto zadowalające postępy we wzmacnianiu ram prawnych służących zapewnieniu odporności usług kluczowych. Jeżeli chodzi o **bezpieczeństwo sieci łączności 5G**, większość państw członkowskich czyni postępy we wdrażaniu unijnego zestawu narzędzi 5G, i posiada już lub jest bliska ukończeniu ram służących nakładaniu odpowiednich ograniczeń na dostawców 5G. Wymogi dotyczące operatorów sieci ruchomych zostaną wzmocnione dzięki transpozycji Europejskiego kodeksu łączności elektronicznej, zaś Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, ENISA, przygotuje propozycję dotyczącą europejskiego programu certyfikacji cyberbezpieczeństwa sieci 5G.

W sprawozdaniu podkreślono również postępy poczynione przez wysokiego przedstawiciela w zakresie propagowania **odpowiedzialnego zachowania państw w cyberprzestrzeni**, w szczególności poprzez przyspieszenie ustanawiania programu działania na szczeblu Organizacji Narodów Zjednoczonych. Ponadto wysoki przedstawiciel rozpoczął **przegląd ram polityki w zakresie cyberobrony** w celu poprawy współpracy w zakresie cyberobrony i prowadzi z państwami członkowskimi analizę doświadczeń w celu udoskonalenia unijnego zestawu narzędzi dla dyplomacji cyfrowej oraz określenia możliwości dalszego wzmocnienia współpracy w tej dziedzinie w ramach UE i na świecie. W opublikowanym również dziś sprawozdaniu Komisji i wysokiego przedstawiciela w sprawie postępów poczynionych w przeciwdziałaniu zagrożeniom hybrydowym podkreślono, że od momentu ustanowienia wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym – odpowiedzi Unii Europejskiej z 2016 r., działania UE od początku pandemii koronawirusa wspierały wzmocnienie **orientacji sytuacyjnej**, **odporności w sektorach krytycznych**, **właściwego reagowania** i **usuwania skutków** rosnących zagrożeń hybrydowych, w tym dezinformacji i cyberataków.

W ciągu ostatnich sześciu miesięcy podjęto również istotne kroki w ramach **strategii UE w zakresie unii bezpieczeństwa** w celu zapewnienia **bezpieczeństwa w naszym środowisku fizycznym i cyfrowym**. Wprowadzono przełomowe przepisy UE, które zobowiążą platformy internetowe do usuwania w ciągu jednej godziny treści o charakterze terrorystycznym, o których poinformują je organy państw członkowskich. Komisja zaproponowała również **akt o usługach cyfrowych**, w którym przedstawiono zharmonizowane przepisy dotyczące usuwania nielegalnych towarów, usług

lub treści w internecie, a także nową strukturę nadzoru nad bardzo dużymi platformami internetowymi. We wniosku zajęto się również kwestią podatności platform na wzmacnianie szkodliwych treści lub rozpowszechnianie dezinformacji. Parlament Europejski i Rada Unii Europejskiej uzgodniły tymczasowe przepisy dotyczące **dobrowolnego wykrywania niegodziwego traktowania dzieci w celach seksualnych w internecie przez dostawców usług komunikacyjnych**. Trwają również prace nad **lepszą ochroną przestrzeni publicznej**. Obejmuje to wspieranie państw członkowskich w zarządzaniu zagrożeniem stwarzanym przez drony oraz poprawę ochrony miejsc kultu i dużych obiektów sportowych przed zagrożeniami terrorystycznymi. Celowi temu poświęcono program wsparcia o wartości 20 mln euro. Aby jeszcze lepiej wspierać państwa członkowskie w zwalczaniu poważnej przestępczości i terroryzmu, w grudniu 2020 r. Komisja zaproponowała również rozszerzenie mandatu Europolu – Agencji UE ds. Współpracy Organów Ścigania.

Wypowiedzi członków kolegium komisarzy:

Margrethe **Vestager**, wiceprzewodnicząca wykonawcza ds. Europy na miarę ery cyfrowej, powiedziała: *Cyberbezpieczeństwo jest podstawą cyfrowej i połączonej Europy. W dzisiejszym społeczeństwie reagowanie na zagrożenia w sposób skoordynowany ma zasadnicze znaczenie. Wspólna jednostka ds. cyberprzestrzeni przyczyni się do osiągnięcia tego celu. Razem możemy dokonać znaczących zmian.*

Josep **Borrell**, Wysoki Przedstawiciel Unii do spraw Zagranicznych i Polityki Bezpieczeństwa, stwierdził: *Wspólna jednostka ds. cyberprzestrzeni to bardzo ważny krok w kierunku ochrony rządów, obywateli i przedsiębiorstw europejskich przed globalnymi cyberzagrożeniami. Jeśli chodzi o cyberataki, wszyscy jesteśmy podatni na zagrożenia i dlatego współpraca na wszystkich szczeblach ma kluczowe znaczenie. Żaden podmiot nie jest wystarczająco duży, żeby czuć się bezpiecznie. Musimy się bronić, ale też dawać przykład innym, promując globalną, otwartą, stabilną i bezpieczną cyberprzestrzeń.*

Margaritis **Schinas**, wiceprzewodniczący do spraw ochrony naszego europejskiego stylu życia, stwierdził: *Niedawne ataki z użyciem oprogramowania typu ransomware powinny służyć jako ostrzeżenie, że musimy bronić się przed zagrożeniami, które mogłyby wpłynąć na nasze bezpieczeństwo i europejski styl życia. Dziś nie możemy już rozróżniać między zagrożeniami w internecie i poza nim. Musimy połączyć wszystkie zasoby, aby pokonać ryzyko w cyberprzestrzeni i zwiększyć nasze zdolności operacyjne. Budowanie zaufanego i bezpiecznego cyfrowego świata, opartego na naszych wartościach, wymaga zaangażowania wszystkich stron, w tym organów egzekwowania prawa.*

Thierry **Breton**, komisarz ds. rynku wewnętrznego, dodał: *Wspólna jednostka ds. cyberprzestrzeni jest podstawowym elementem naszej ochrony przed rosnącymi i coraz bardziej złożonymi zagrożeniami dla cyberbezpieczeństwa. Określiliśmy jasne etapy i harmonogramy, które umożliwią nam razem z państwami członkowskimi konkretną poprawę współpracy w zakresie zarządzania kryzysowego w UE, wykrywania zagrożeń i szybszego reagowania. Jest to jednostka operacyjna będąca elementem europejskiej tarczy chroniącej przed zagrożeniami cybernetycznymi.*

Ylva **Johansson**, komisarz do spraw wewnętrznych, powiedziała: *Zwalczanie cyberataków jest coraz większym wyzwaniem. Organy ścigania w całej UE mogą najlepiej stawić czoła temu nowemu zagrożeniu poprzez koordynację działań. Wspólna jednostka ds. cyberprzestrzeni pomoże funkcjonariuszom policji w państwach członkowskich dzielić się wiedzą fachową. Wesprze to budowanie zdolności organów ścigania do przeciwdziałania tym atakom.*

Kontekst

Cyberbezpieczeństwo jest priorytetem Komisji i podstawą cyfrowej i połączonej Europy. Wzrost liczby cyberataków podczas kryzysu związanego z koronawirusem pokazał, jak ważna jest ochrona systemów ochrony zdrowia i opieki, ośrodków badawczych i innej infrastruktury krytycznej. Potrzebne są zdecydowane działania w tej dziedzinie, aby dostosować gospodarkę i społeczeństwo UE do przyszłych wyzwań.

UE jest zaangażowana w realizację nowej strategii UE w zakresie cyberbezpieczeństwa za pomocą bezprecedensowego poziomu inwestycji w transformację ekologiczną i cyfrową UE za pośrednictwem długoterminowego budżetu UE na lata 2021–2027, w szczególności programu „Cyfrowa Europa" i programu „Horyzont Europa" a także planu odbudowy dla Europy.

Jeśli chodzi o cyberbezpieczeństwo, nasza ochrona jest tak silna jak nasze najsłabsze ogniwo. Cyberataki nie kończą się na fizycznych granicach państw. Zacieśnienie współpracy, w tym współpracy transgranicznej, w dziedzinie cyberbezpieczeństwa jest zatem również priorytetem UE: w ostatnich latach Komisja przewodziła kilku inicjatywom na rzecz poprawy zbiorowej gotowości i

ułatwiała ich realizację, zaś wspólne struktury UE wspierały już wcześniej państwa członkowskie, zarówno na poziomie technicznym, jak i operacyjnym. Dzisiejsze zalecenie w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni stanowi kolejny krok w kierunku ściślejszej współpracy i skoordynowanego reagowania na cyberzagrożenia.

Jednocześnie wspólna unijna reakcja dyplomatyczna na szkodliwe działania w cyberprzestrzeni, znana jako zestaw narzędzi dla dyplomacji cyfrowej, zachęca do współpracy i propaguje odpowiedzialne zachowania państw w cyberprzestrzeni, umożliwiając UE i jej państwom członkowskim stosowanie wszystkich środków w ramach wspólnej polityki zagranicznej i bezpieczeństwa, w tym sankcji, w celu zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania ich i reagowania na nie.

Aby zapewnić bezpieczeństwo w środowisku fizycznym i cyfrowym, w lipcu 2020 r. Komisja przedstawiła strategię UE w zakresie unii bezpieczeństwa na lata 2020–2025. Koncentruje się ona na obszarach priorytetowych, w których UE może wnieść wartość dodaną strategia wspiera państwa członkowskie w zwiększaniu bezpieczeństwa wszystkich mieszkańców Europy poprzez: walkę z terroryzmem i przestępczością zorganizowaną, zapobieganie zagrożeniom hybrydowym i ich wykrywanie oraz zwiększanie odporności infrastruktury krytycznej, oraz promowanie cyberbezpieczeństwa i wspieranie badań naukowych i innowacji.

Dodatkowe informacje

Zestawienie informacji: Wspólna jednostka ds. cyberprzestrzeni

Infografika: Ekosystem cyberbezpieczeństwa w UE

Zalecenie w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni

Pierwsze sprawozdanie z postępów w realizacji strategii UE w zakresie cyberbezpieczeństwa

Decyzja w sprawie utworzenia biura Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w Brukseli

Drugie sprawozdanie z postępów w realizacji strategii UE w zakresie unii bezpieczeństwa (zob. również załącznik 1 i załącznik 2)

Piąte sprawozdanie z postępów we wdrażaniu wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r.

Komunikat prasowy: nowa strategia UE w zakresie cyberbezpieczeństwa i nowe przepisy mające na celu zwiększenie odporności fizycznych i cyfrowych podmiotów krytycznych

Strategia UE w zakresie unii bezpieczeństwa

IP/21/3088

Kontakty z mediami:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Zapytania od obywateli: Serwis Europe Direct – tel. [00 800 67 89 10 11] lub e-mail

Related media

Read-out of the College meeting / press conference by Margaritis Schinas, Vice-President of the European Commission, and Thierry Breton, European commissioner, on building a Joint Cyber Unit