Nowa strategia UE w zakresie cyberbezpieczeństwa i nowe przepisy mające na celu zwiększenie odporności fizycznych i cyfrowych podmiotów krytycznych

Bruksela, 16 grudnia 2020 r.

Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawiają dziś nową strategię UE w zakresie cyberbezpieczeństwa. Strategia ta, jako kluczowy element kształtowania cyfrowej przyszłości Europy, planu odbudowy dla Europy i strategii UE w zakresie unii bezpieczeństwa, wzmocni zbiorową odporność Europy na zagrożenia dla cyberbezpieczeństwa i pomoże zapewnić wszystkim obywatelom i firmom możliwość pełnego korzystania z wiarygodnych i sprawdzonych usług i narzędzi cyfrowych. Niezależnie od tego, czy Europejczycy korzystają z urządzeń podłączonych do internetu, sieci elektroenergetycznej, czy też z banków, samolotów, administracji publicznej i szpitali, powinni mieć zaufanie, że są chronieni przed cyberzagrożeniami.

Nowa strategia w zakresie cyberbezpieczeństwa umożliwia również UE zwiększenie przywództwa odnośnie do międzynarodowych norm i standardów w cyberprzestrzeni oraz zacieśnienie współpracy z partnerami na całym świecie w celu promowania globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni, opartej na praworządności, prawach człowieka, podstawowych wolnościach i wartościach demokratycznych.

Ponadto Komisja przedstawia wnioski legislacyjne dotyczące zarówno cyberodporności, jak i fizycznej odporności podmiotów krytycznych i krytycznych sieci: dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa NIS lub „dyrektywa NIS 2") oraz nową dyrektywę w sprawie odporności podmiotów krytycznych. Proponowane akty prawne dotyczą wielu sektorów i mają na celu zaradzenie w spójny i komplementarny sposób obecnym i przyszłym zagrożeniom w internecie i poza nim, począwszy od cyberataków po przestępczość, czy klęski żywiołowe.

Zaufanie i bezpieczeństwo w centrum cyfrowej dekady UE

Celem nowej strategii UE w zakresie cyberbezpieczeństwa jest ochrona globalnego i otwartego internetu, a jednocześnie ustanowienie gwarancji nie tylko odnośnie do bezpieczeństwa, ale także do ochrony europejskich wartości i praw podstawowych ludności. Wykorzystując osiągnięcia ostatnich miesięcy i lat wspomniana strategia zawiera konkretne propozycje inicjatyw regulacyjnych, inwestycyjnych i politycznych w trzech obszarach działań UE:

1. **Odporność, suwerenność technologiczna oraz przywództwo**

W ramach omawianego nurtu działań Komisja proponuje reformę przepisów dotyczących bezpieczeństwa sieci i systemów informatycznych przy pomocy dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji lub „dyrektywa NIS 2") w celu zwiększenia poziomu cyberodporności krytycznych sektorów publicznych i prywatnych: szpitale, sieci energetyczne, koleje, ale także ośrodki przetwarzania danych, administracja publiczna, laboratoria badawcze, produkcja wyrobów medycznych i leków o kluczowym znaczeniu oraz pozostała infrastruktura krytyczna i usługi krytyczne muszą pozostać poza zasięgiem cyberataków w coraz szybciej zmieniającym się i złożonym środowisku zagrożeń.

Komisja proponuje również powołanie w całej UE sieci centrów monitorowania bezpieczeństwa, wspieranych przez sztuczną inteligencję (AI), która to sieć będzie stanowić prawdziwą „tarczę przed zagrożeniami dla cyberbezpieczeństwa", zdolną wykrywać odpowiednio wcześnie oznaki cyberataku i umożliwiać proaktywne działania przed wystąpieniem szkody. Dodatkowe działania obejmą specjalne wsparcie dla małych i średnich przedsiębiorstw (MŚP) udzielane w ramach centrów innowacji cyfrowych, a także zwiększone wysiłki na rzecz podnoszenia kwalifikacji siły roboczej, przyciągania i zatrzymywania najlepszych talentów w dziedzinie cyberbezpieczeństwa oraz inwestowanie w badania naukowe i innowacje, które są otwarte, konkurencyjne i działają na zasadzie doskonałości.

2. **Budowanie zdolności operacyjnej w celu zapobiegania, powstrzymywania i reagowania**

Komisja przygotowuje, wspólnie z państwami członkowskimi w postępującym i równościowym procesie, nową wspólną jednostkę ds. cyberprzestrzeni – aby zacieśnić współpracę między organami UE i organami państw członkowskich odpowiedzialnymi za zapobieganie cyberatakom, powstrzymywanie ich i reagowanie na nie – obejmującą środowiska cywilne, dyplomatyczne, zajmujące się ściganiem przestępstw i cyberobroną. Wysoki przedstawiciel przedstawia propozycje wzmocnienia unijnego zestawu narzędzi dla dyplomacji cyfrowej, aby zapobiegać działaniom szkodliwym dla cyberbezpieczeństwa – w szczególności mającym wpływ na naszą infrastrukturę krytyczną, łańcuchy dostaw, demokratyczne instytucje i procesy – zniechęcać do nich, powstrzymywać je i skutecznie na nie reagować. UE będzie również dążyć do dalszego zacieśniania współpracy i rozwijania najnowocześniejszych zdolności w zakresie cyberobrony, w oparciu o prace Europejskiej Agencji Obrony, i zachęcać państwa członkowskie do pełnego wykorzystania stałej współpracy strukturalnej i Europejskiego Funduszu Obronnego.

3. **Rozwój globalnej i otwartej cyberprzestrzeni dzięki zacieśnionej współpracy**

UE zintensyfikuje współpracę z partnerami międzynarodowymi w celu wzmocnienia międzynarodowego porządku opartego na zasadach, wspierania bezpieczeństwa międzynarodowego i stabilności w cyberprzestrzeni oraz ochrony praw człowieka i podstawowych wolności w internecie. Przyczyni się to do rozwoju międzynarodowych norm i standardów, które odzwierciedlają te podstawowe wartości UE, poprzez współpracę z partnerami międzynarodowymi w ramach Organizacji Narodów Zjednoczonych i innych odpowiednich forów. UE będzie nadal wzmacniać unijny zestaw narzędzi dla dyplomacji cyfrowej oraz zwiększać wysiłki na rzecz budowania zdolności cyfrowych w państwach trzecich poprzez opracowanie unijnego programu budowania zewnętrznych zdolności cyfrowych. Zintensyfikowane zostaną dialogi w sprawach cyberprzestrzeni z państwami trzecimi, organizacjami regionalnymi i międzynarodowymi, a także w ramach społeczności opartej na porozumieniu zainteresowanych stron. UE utworzy również unijną sieć dyplomacji cyfrowej na całym świecie, aby promować swoją wizję cyberprzestrzeni.

UE jest zaangażowana we wspieranie nowej strategii w zakresie cyberbezpieczeństwa za pomocą bezprecedensowego poziomu inwestycji w transformację cyfrową UE na najbliższe siedem lat, za pośrednictwem kolejnego długoterminowego budżetu UE, w szczególności programu „Cyfrowa Europa” i programu „Horyzont Europa”, a także planu odbudowy dla Europy. Zachęca się zatem państwa członkowskie do pełnego wykorzystania unijnego Instrumentu na rzecz Odbudowy i Zwiększania Odporności w celu zwiększenia cyberbezpieczeństwa i dokonania odpowiednich inwestycji na szczeblu UE. Celem jest doprowadzenie do łącznych inwestycji UE, państw członkowskich i przemysłu o wartości do 4,5 mld EUR, w szczególności w ramach Centrum Kompetencji w Dziedzinie Cyberbezpieczeństwa i Sieci Ośrodków Koordynacji, a także zapewnienie, by znaczna część środków trafiała do MŚP.

Komisja dąży również do wzmocnienia przemysłowych i technologicznych zdolności UE w dziedzinie cyberbezpieczeństwa, w tym poprzez projekty wspierane wspólnie z budżetu UE i budżetów krajowych. UE ma wyjątkową możliwość połączenia zasobów własnych w celu zwiększenia swojej strategicznej autonomii i wzmocnienia przywództwa w dziedzinie cyberbezpieczeństwa w całym cyfrowym łańcuchu dostaw (w tym zbioru danych i chmury obliczeniowej, technologii procesorów nowej generacji, ultra bezpiecznej łączności i sieci 6G), zgodnie ze swoimi wartościami i priorytetami.

Cyberodporność i fizyczna odporność sieci, systemów informatycznych i podmiotów krytycznych

Należy zaktualizować istniejące na szczeblu UE środki mające na celu ochronę kluczowych usług i kluczowej infrastruktury zarówno przed ryzykiem w cyberprzestrzeni, jak i zagrożeniami fizycznymi. Ryzyko w cyberprzestrzeni w dalszym ciągu ewoluuje wraz z rosnącą cyfryzacją i wzajemnymi powiązaniami. Zagrożenia fizyczne stały się również bardziej złożone od czasu przyjęcia w 2008 r. unijnych przepisów dotyczących infrastruktury krytycznej, które obecnie obejmują jedynie sektory energii i transportu. Zmiany mają na celu aktualizację przepisów zgodnie z zasadami strategii UE w zakresie unii bezpieczeństwa, przezwyciężenie fałszywej dychotomii między tym co w internecie i poza nim oraz zerwanie z podejściem hermetycznym.

Aby zareagować na rosnące zagrożenia wynikające z cyfryzacji i wzajemnych powiązań, **dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji lub „dyrektywa NIS 2”)** będzie dotyczyć średnich i dużych podmiotów z większej liczby sektorów, stosownie do ich krytyczności dla gospodarki i społeczeństwa. Dyrektywa NIS 2 wzmacnia wymogi w zakresie bezpieczeństwa nakładane na przedsiębiorstwa, dotyczy bezpieczeństwa łańcuchów dostaw i relacji z

dostawcami, usprawnia obowiązki sprawozdawcze, wprowadza bardziej rygorystyczne środki nadzoru dla organów krajowych, surowsze wymogi w zakresie egzekwowania przepisów i ma na celu harmonizację systemów sankcji we wszystkich państwach członkowskich. Wniosek dotyczący dyrektywy NIS 2 pomoże zintensyfikować wymianę informacji i współpracę w zakresie zarządzania kryzysami w cyberprzestrzeni na szczeblu krajowym i unijnym.

Proponowana **dyrektywa w sprawie odporności podmiotów krytycznych** rozszerza i pogłębia zakres dyrektywy w sprawie europejskiej infrastruktury krytycznej z 2008 r. Obecnie uwzględniono dziesięć sektorów: energii, transportu, bankowości, infrastruktury rynku finansowego, zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, administracji publicznej i przestrzeni kosmicznej. Na mocy proponowanej dyrektywy każde z państw członkowskich przyjmie krajową strategię na rzecz zapewnienia odporności podmiotów krytycznych i przeprowadzi regularnie oceny ryzyka. Oceny te pomogą również zidentyfikować mniejszy podzbiór podmiotów krytycznych, które będą podlegać obowiązkom mającym na celu zwiększenie odporności tych podmiotów na zagrożenia inne niż ryzyko w cyberprzestrzeni, takim jak oceny ryzyka na poziomie danego podmiotu, podejmowanie środków technicznych i organizacyjnych oraz zgłaszanie incydentów. Komisja z kolei zapewni dodatkowe wsparcie państwom członkowskim i podmiotom krytycznym, na przykład poprzez opracowanie na szczeblu unijnym przeglądu zagrożeń transgranicznych i międzysektorowych, najlepszych praktyk, metod, transgranicznych działań szkoleniowych i ćwiczeń mających na celu sprawdzenia odporności podmiotów krytycznych.

Zabezpieczenie sieci następnej generacji: sieci 5G i kolejne generacje

W ramach nowej strategii w zakresie cyberbezpieczeństwa zachęca się państwa członkowskie, przy wsparciu Komisji i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), do zakończenia wdrażania unijnego zestawu narzędzi w zakresie 5G zapewniającego kompleksowe i obiektywne podejście oparte na analizie ryzyka w odniesieniu do bezpieczeństwa sieci 5G i przyszłych generacji sieci.

Według opublikowanego dzisiaj sprawozdania na temat wpływu zalecenia Komisji w sprawie cyberbezpieczeństwa sieci 5G oraz postępów we wdrażaniu unijnego zestawu środków ograniczających ryzyko od czasu sprawozdania z postępu prac z lipca 2020 r. większość państw członkowskich jest już na dobrej drodze do wdrożenia zalecanych środków. Państwa członkowskie powinny teraz dążyć do zakończenia wdrażania tych środków do drugiego kwartału 2021 r. i zapewnić, by stwierdzone ryzyko zostało odpowiednio ograniczone w sposób skoordynowany, w szczególności z myślą o zminimalizowaniu narażenia na dostawców wysokiego ryzyka i uniknięciu zależności od tych dostawców. Komisja określa dziś również główne cele i działania zmierzające do prowadzenia dalszych skoordynowanych prac na szczeblu UE.

Wypowiedzi członków kolegium komisarzy:

Margrethe **Vestager**, wiceprzewodnicząca wykonawcza do spraw Europy na miarę ery cyfrowej, powiedziała: *Europa jest zdecydowana działać na rzecz transformacji cyfrowej naszego społeczeństwa i gospodarki. Musimy zatem wspierać ten proces za pomocą inwestycji na niespotykanym dotychczas poziomie. Transformacja cyfrowa nabiera tempa, ale może zakończyć się sukcesem tylko wtedy, gdy obywatele i firmy będą mieli pewność, że skomunikowane produkty i usługi, z których korzystają, są bezpieczne.*

Josep **Borrell**, wysoki przedstawiciel, powiedział: *Międzynarodowe bezpieczeństwo i stabilność w większym stopniu niż kiedykolwiek zależą od globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni, w której przestrzega się praworządności, praw człowieka, wolności i demokracji. Dzięki dzisiejszej strategii UE staje na wysokości zadania jeśli chodzi o ochronę swoich organów, obywateli i firm przed globalnymi zagrożeniami dla cyberbezpieczeństwa oraz jeśli chodzi o sprawowanie przywództwa w cyberprzestrzeni, zapewniając wszystkim możliwość czerpania korzyści z internetu i korzystania z technologii.*

Margaritis **Schinas**, wiceprzewodniczący do spraw ochrony naszego europejskiego stylu życia, stwierdził: *Cyberbezpieczeństwo jest centralnym elementem unii bezpieczeństwa. Nie istnieje już rozróżnienie na zagrożenia w internecie i poza nim. To co cyfrowe i fizyczne jest obecnie ze sobą nierozerwalnie powiązane. Przedstawiony dziś zestaw środków pokazuje, że UE jest gotowa wykorzystać wszystkie swoje zasoby i wiedzę fachową, aby przygotować się na zagrożenia fizyczne i zagrożenia dla cyberbezpieczeństwa i reagować na nie z taką samą determinacją.*

Thierry **Breton**, komisarz do spraw rynku wewnętrznego, powiedział: *Zagrożenia dla cyberbezpieczeństwa ewoluują szybko, są coraz bardziej złożone i mogą istnieć w różnych warunkach. Aby zapewnić ochronę naszych obywateli i infrastruktury, musimy zaplanować nasze działania. Odporna i niezależna europejska tarcza przed zagrożeniami dla cyberbezpieczeństwa pozwoli nam wykorzystać naszą wiedzę fachową do szybszego reagowania, ograniczenia*

potencjalnych szkód i zwiększenia naszej odporności. Inwestowanie w cyberbezpieczeństwo oznacza inwestowanie w zdrową przyszłość naszych środowisk internetowych i w naszą strategiczną autonomię.

Ylva **Johansson**, komisarz do spraw wewnętrznych, powiedziała: *Nasze szpitale, systemy odprowadzania ścieków, czy infrastruktura transportowa są tylko tak silne, jak ich najsłabsze ogniwa; zakłócenia w jednej części Unii mogą mieć wpływ na świadczenie podstawowych usług w innym miejscu Unii. Aby zapewnić sprawne funkcjonowanie rynku wewnętrznego i źródła utrzymania osób mieszkających w Europie, nasza kluczowa infrastruktura musi być odporna na zagrożenia obejmujące na przykład klęski żywiołowe, ataki terrorystyczne, wypadki i pandemie, takie jak ta, której doświadczamy obecnie. Moja propozycja dotycząca infrastruktury krytycznej temu właśnie służy.*

Dalsze działania

Komisja Europejska i wysoki przedstawiciel zobowiązują się do wdrożenia nowej strategii w zakresie cyberbezpieczeństwa w nadchodzących miesiącach. Komisja i wysoki przedstawiciel będą regularnie przedstawiać sprawozdania na temat poczynionych postępów oraz udzielać pełnych informacji Parlamentowi Europejskiemu, Radzie Unii Europejskiej i zainteresowanym stronom, a także angażować wspomniane instytucje i strony we wszystkie istotne działania.

Do Parlamentu Europejskiego i Rady należy obecnie przeanalizowanie i przyjęcie proponowanej dyrektywy NIS 2 oraz dyrektywy w sprawie odporności podmiotów krytycznych. Po uzgodnieniu treści proponowanych dyrektyw, a następnie ich przyjęciu, państwa członkowskie będą musiały transponować te dyrektywy w ciągu 18 miesięcy od ich wejścia w życie.

Komisja będzie dokonywać okresowych przeglądów dyrektywy NIS 2 oraz dyrektywy w sprawie odporności podmiotów krytycznych oraz składać sprawozdania z funkcjonowania tych aktów prawnych.

Kontekst

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

W nowej strategii Unii Europejskiej w zakresie cyberbezpieczeństwa proponuje się włączenie cyberbezpieczeństwa do wszystkich elementów łańcucha dostaw oraz dalsze połączenie działań i zasobów UE na czterech płaszczyznach związanych z cyberbezpieczeństwem – rynkiem wewnętrznym, egzekwowaniem prawa, dyplomacją i obronnością. Strategia ta czerpie z unijnej strategii Kształtowania cyfrowej przyszłości Europy i strategii UE w zakresie unii bezpieczeństwa oraz opiera się na szeregu aktów prawodawczych, działań i inicjatyw wdrożonych przez UE w celu wzmocnienia zdolności w zakresie cyberbezpieczeństwa i zapewnienia cyberodporności Europy. Wspomniane akty, działania i inicjatywy obejmują strategię w zakresie cyberbezpieczeństwa z 2013 r., która została poddana przeglądowi w 2017 r., oraz przedstawioną przez Komisję Europejską agendę bezpieczeństwa na lata 2015-2020. Nowa strategia Unii Europejskiej w zakresie cyberbezpieczeństwa uznaje również rosnące wzajemne powiązania między bezpieczeństwem wewnętrznym i zewnętrznym, w szczególności w ramach wspólnej polityki zagranicznej i bezpieczeństwa.

Pierwszy ogólnounijny akt prawny o cyberbezpieczeństwie – dyrektywa NIS, która weszła w życie w 2016 r. – przyczynił się do osiągnięcia wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w całej UE. W ramach swojego kluczowego celu politycznego, jakim jest Europa na miarę ery cyfrowej, Komisja ogłosiła w lutym bieżącego roku przegląd dyrektywy NIS. Akt UE o cyberbezpieczeństwie, który obowiązuje od 2019 r., zapewnił Europie ramy certyfikacji cyberbezpieczeństwa produktów, usług i procesów oraz wzmocnił mandat Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

Jeżeli chodzi o cyberbezpieczeństwo sieci 5G, państwa członkowskie, przy wsparciu Komisji i ENISA, ustanowiły – z wykorzystaniem zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G przyjętego w styczniu 2020 r. – kompleksowe i obiektywne podejście oparte na analizie ryzyka. W przeglądzie zalecenia Komisji z marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G stwierdzono, że większość państw członkowskich poczyniła postępy we wdrażaniu zestawu narzędzi.

Począwszy od strategii Unii Europejskiej w zakresie cyberbezpieczeństwa z 2013 r., UE opracowała spójną i całościową międzynarodową cyberpolitykę. Współpracując ze swoimi partnerami na szczeblu dwustronnym, regionalnym i międzynarodowym, UE promuje globalną, otwartą, stabilną i bezpieczną cyberprzestrzeń, której przyświecają podstawowe wartości UE, oraz opartą na praworządności. UE wspiera państwa trzecie w zwiększaniu ich cyberodporności i zdolności do walki z

cyberprzestępczością, a także wykorzystuje zestaw narzędzi dla dyplomacji cyfrowej z 2017 r., aby w jeszcze większym stopniu przyczyniać się do bezpieczeństwa międzynarodowego i stabilności w cyberprzestrzeni, m.in. poprzez zastosowanie w 2019 r. po raz pierwszy, wobec 8 osób oraz 4 podmiotów i organów, systemu sankcji w związku z cyberatakami. UE poczyniła znaczne postępy również jeśli chodzi o współpracę w sferze cyberobrony, w tym w odniesieniu do zdolności w zakresie cyberobrony, zwłaszcza na gruncie ram polityki UE w zakresie cyberobrony (CDPF, ang. *Cyber Defence Policy Framework*), a także w kontekście stałej współpracy strukturalnej (PESCO, ang. *Permanent Structured Cooperation*) i prac Europejskiej Agencji Obrony.

Cyberbezpieczeństwo jest priorytetem również w kolejnym długoterminowym budżecie UE (2021-2027). W ramach programu „Cyfrowa Europa" UE będzie wspierać badania naukowe, innowacje i infrastrukturę w dziedzinie cyberbezpieczeństwa, cyberobronę oraz unijny sektor cyberbezpieczeństwa. Ponadto w odpowiedzi na kryzys związany z koronawirusem, kiedy to doszło do nasilenia cyberataków podczas zamknięcia, w ramach planu odbudowy dla Europy, zapewniono dodatkowe inwestycje w cyberbezpieczeństwo.

UE od dawna uznaje potrzebę zapewnienia odporności infrastruktury krytycznej służącej do świadczenia usług, które mają zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego oraz życia i źródeł utrzymania obywateli europejskich. Z tego powodu w 2006 r. UE ustanowiła europejski program ochrony infrastruktury krytycznej i przyjęła w 2008 r. dyrektywę w sprawie europejskiej infrastruktury krytycznej, która ma zastosowanie do sektorów energii i transportu. W późniejszych latach środki te zostały uzupełnione różnymi środkami sektorowymi i międzysektorowymi dotyczącymi konkretnych aspektów, takich jak uodparnianie na zmianę klimatu, ochrona ludności czy bezpośrednie inwestycje zagraniczne.

Więcej informacji:

Notatka prasowa na temat nowej strategii UE w zakresie cyberbezpieczeństwa

Notatka prasowa na temat wniosku dotyczącego dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji)

Notatka prasowa na temat cyberbezpieczeństwa: działania zewnętrzne UE

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

Wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji albo „dyrektywa NIS 2")

Wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych (zob. załącznik 1 do wniosku, a także ocenę skutków oraz jej streszczenie)

Europejska unia bezpieczeństwa

Ocena skutków zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji („dyrektywa NIS 2")

Więcej na temat cyberbezpieczeństwa

Więcej na temat dyrektywy NIS

IP/20/2391

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