Komisja Europejska

ORĘDZIE O STANIE UNII 2018

Budowanie silnego systemu cyberbezpieczeństwa w Europie

#SOTEU

12 września 2018 r.

„Ataki cybernetyczne nie znają granic, lecz nasza zdolność reagowania na nie bardzo się różni w poszczególnych krajach, powodując powstanie luk, które przyciągają kolejne ataki. UE potrzebuje silniejszych i skuteczniejszych struktur, aby zapewnić prawdziwą cyberodporność i reagować na cyberataki. Nie chcemy być najsłabszymi ogniwami w tym układzie globalnych zagrożeń."

Jean-Claude Juncker, Talliński Szczyt Cyfrowy, 29 września 2017 r.

Aby wyposażyć Europę w odpowiednie narzędzia umożliwiające jej sprostanie wciąż zmieniającym się cyberzagrożeniom, Komisja Europejska i Wysoki Przedstawiciel zaproponowali w 2017 r. szeroko zakrojony zestaw środków mających zapewnić solidne podstawy cyberbezpieczeństwa w UE. Uzupełnieniem tych wysiłków jest obecnie wniosek ustawodawczy, dzięki któremu UE może połączyć zasoby i wiedzę fachową w dziedzinie badań naukowych i innowacji oraz stać się liderem w dziedzinie technologii z zakresu cyberbezpieczeństwa i technologii cyfrowych nowej generacji.

Obecne cyberzagrożenia

Ponad 4 tys. ataków z użyciem oprogramowania typu ransomware dziennie w 2016 r.

80 proc. europejskich przedsiębiorstw doświadczyło w ubiegłym roku co najmniej jednego cyberincydentu

Liczba **incydentów związanych z bezpieczeństwem informacji** odnotowanych we wszystkich gałęziach przemysłu **wzrosła o 38 proc.** – to największy wzrost w ciągu ostatnich 12 lat

W niektórych państwach członkowskich cyberprzestępstwa stanowią nawet **50 proc. popełnianych przestępstw**.

Atak WannyCry w maju 2017 r. dotknął **ponad 150 państw i ponad 230 tys. systemów** w różnych sektorach i krajach i miał znaczny wpływ na podstawowe usługi świadczone za pośrednictwem internetu, m.in. na funkcjonowanie szpitali i pogotowia ratunkowego.

Wzmacnianie odporności na cyberataki

Komisja wspiera już wzmocnienie UE w zakresie odpierania cyberataków oraz odporności i reagowania na nie, między innymi poprzez:

wspieranie skutecznego wprowadzenia w życie pierwszych unijnych przepisów w dziedzinie cyberbezpieczeństwa (dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych), dzięki następującym środkom:

WIĘKSZE MOŻLIWOŚCI

Państwa członkowskie muszą poprawić swoje zdolności w zakresie cyberbezpieczeństwa

WSPÓŁPRACA

Ściślejsza współpraca na poziomie UE

ZAPOBIEGANIE ZAGROŻENIOM

Podmioty aktywne w kluczowych sektorach (takich jak energetyka, transport, służba zdrowia) muszą wprowadzić środki w zakresie zapobiegania zagrożeniom i postępowania w przypadku cyberataków

Elementy współpracy z państwami członkowskimi:

AGENCJA UE DS. CYBERBEZPIECZEŃSTWA

Wzmocnienie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w celu lepszego wsparcia państw członkowskich

UNIJNE RAMY CERTYFIKACJI

Ogólnounijne ramy certyfikacji zapewniające cyberbezpieczeństwo produktów i usług

SKOORDYNOWANA REAKCJA

Zapewnienie szybkiej i skoordynowanej reakcji na cyberataki o dużej skali

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) pomaga organom ds. cyberbezpieczeństwa w państwach członkowskich lepiej chronić UE przed cyberatakami.

Łączenie zasobów i wiedzy fachowej w dziedzinie technologii z zakresu cyberbezpieczeństwa

Oprócz już istniejących inicjatyw UE w zakresie cyberbezpieczeństwa Komisja proponuje dzisiaj uzupełnienie tych wysiłków utworzeniem sieci Centrów Kompetencji oraz Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, których zadaniem byłoby opracowywanie i udostępnianie narzędzi i technologii potrzebnych do stawiania czoła wciąż zmieniającym się zagrożeniom.

Europejskie Centrum będzie odpowiadać za możliwie jak najbardziej ukierunkowaną koordynację – wraz z państwami członkowskimi – funduszy przeznaczonych na potrzeby zapewnienia cyberbezpieczeństwa w ramach następnego wieloletniego budżetu UE. Pomoże to stworzyć nowe europejskie zdolności w zakresie cyberbezpieczeństwa.

Europa dysponuje już bogatą wiedzą fachową – w różnych miejscach w całej UE znajduje się ponad **660 centrów kompetencji w dziedzinie cyberbezpieczeństwa**. Aby skutecznie wykorzystać fachową wiedzę, którą posiadają te centra, Komisja proponuje mechanizm przewidujący:

łączenie, wymianę i zapewnianie dostępu do istniejącej wiedzy fachowej

pomoc we wdrażaniu unijnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa

zapewnienie długoterminowej strategicznej współpracy między przemysłem, środowiskami naukowymi i rządami

wspólne inwestowanie w kosztowną infrastrukturę i wspólne jej użytkowanie

Europejskie Centrum Kompetencji:

Będzie koordynować wykorzystanie funduszy przeznaczonych na potrzeby zapewnienia cyberbezpieczeństwa w ramach następnego wieloletniego budżetu UE na lata 2021–2027 w kontekście programów „Cyfrowa Europa" i „Horyzont Europa". Centrum to będzie wspierać Sieć i Środowisko z myślą o stymulowaniu badań naukowych i innowacji w zakresie **cyberbezpieczeństwa**. Będzie ono również organizować **wspólne inwestycje** UE, państw członkowskich i przemysłu. Przykładowo, w ramach programu „Cyfrowa Europa" kwota w wysokości **2 mld euro** zostanie zainwestowana w ochronę gospodarki cyfrowej, społeczeństwa i demokracji w UE poprzez zwiększanie potencjału unijnego sektora cyberbezpieczeństwa oraz finansowanie najnowocześniejszych urządzeń i infrastruktury w zakresie cyberbezpieczeństwa.

Sieć krajowych ośrodków koordynacji:

Każde państwo członkowskie wyznaczy jeden krajowy ośrodek koordynacji w ramach sieci, który będzie zaangażowany w rozwój nowych zdolności w zakresie cyberbezpieczeństwa i ogólne poszerzanie kompetencji. Sieć będzie pomagać we wskazywaniu i wspieraniu najważniejszych projektów w dziedzinie cyberbezpieczeństwa w państwach członkowskich.

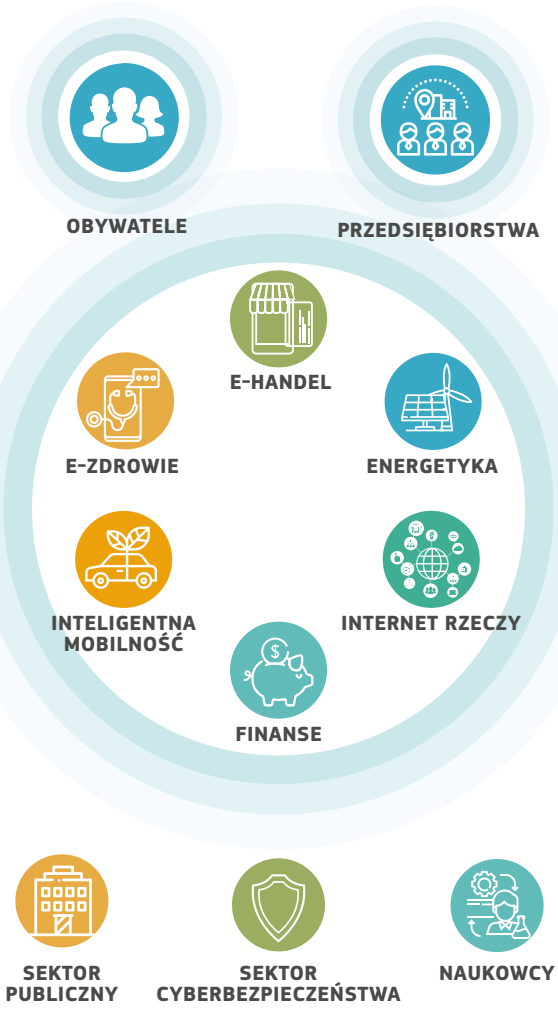
Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa:

Wielka, otwarta i zróżnicowana grupa, w której skład wchodzą podmioty zainteresowane kwestiami cyberbezpieczeństwa – od instytucji badawczych po jednostki sektora prywatnego i publicznego, obejmująca zarówno władze cywilne, jak i wojskowe.

Co ulegnie poprawie?

- lepsza koordynacja prac;
- dostęp do wiedzy fachowej;
- dostęp do zaplecza testowego i doświadczalnego;
- ocena cyberbezpieczeństwa produktów;
- dostęp do innowacyjnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa;
- wsparcie wprowadzania na rynek produktów i usług;
- lepsze wyeksponowanie wobec potencjalnych inwestorów i partnerów biznesowych;
- oszczędności kosztów dzięki wspólnym inwestycjom z innymi państwami członkowskimi;
- zdolność UE do samodzielnego zabezpieczenia swojej gospodarki i demokracji;
- wzrost znaczenia UE jako światowego lidera w dziedzinie cyberbezpieczeństwa.

Kto skorzysta?



Urząd Publikacji

Print ISBN 978-92-79-92483-5 doi:10.2775/9311 NA-04-18-693-PL-C
PDF ISBN 978-92-79-92464-4 doi:10.2775/08338 NA-04-18-693-PL-N