Orędzie o stanie Unii: nowe unijne przepisy w zakresie cyberbezpieczeństwa zapewniają bezpieczniejszy sprzęt i oprogramowanie komputerowe

Bruksela, 15 września 2022 r.

Komisja przedstawiła dziś wniosek w sprawie nowego europejskiego aktu dotyczącego cyberodporności, aby chronić konsumentów i przedsiębiorstwa przed produktami o nieodpowiednich zabezpieczeniach. Pierwsze w historii ogólnounijne prawodawstwo tego rodzaju wprowadza obowiązkowe wymogi w zakresie cyberbezpieczeństwa dla produktów z elementami cyfrowymi na wszystkich etapach ich cyklu życia.

Akt ten, zapowiedziany przez przewodniczącą Ursulę **von der Leyen** we wrześniu 2021 r. w orędziu o stanie Unii, w oparciu o unijną strategię cyberbezpieczeństwa z 2020 r. i strategię UE w zakresie unii bezpieczeństwa z 2020 r., zapewni konsumentom w całej UE większe bezpieczeństwo produktów cyfrowych, takich jak bezprzewodowe i przewodowe produkty i oprogramowanie komputerowe. Oprócz zwiększenia odpowiedzialności producentów poprzez zobowiązanie ich do zapewnienia wsparcia w zakresie bezpieczeństwa i aktualizacji oprogramowania komputerowego w celu wyeliminowania zidentyfikowanych podatności na (cyber)ryzyko, umożliwi on konsumentom uzyskanie wystarczających informacji na temat cyberbezpieczeństwa produktów, które kupują i z których korzystają.

Margrethe **Vestager**, wiceprzewodnicząca wykonawcza do spraw Europy na miarę ery cyfrowej, powiedziała: *Zasługujemy na to, by czuć się bezpiecznie, gdy kupujemy produkty na jednolitym rynku. Podobnie jak można zaufać zabawce lub lodówce z oznakowaniem CE, dzięki europejskiemu aktowi dotyczącemu cyberodporności zapewnimy zgodność zakupionych przedmiotów podłączonych do internetu i oprogramowania z silnymi zabezpieczeniami w zakresie cyberbezpieczeństwa. Nałoży on odpowiedzialność na tych, którzy powinni ją zapewnić, czyli na podmioty wprowadzające produkty do obrotu.*

Margaritis **Schinas**, wiceprzewodniczący do spraw promowania naszego europejskiego stylu życia, stwierdził: *Europejski akt dotyczący cyberodporności jest naszą odpowiedzią na współczesne zagrożenia dla bezpieczeństwa, które są obecnie wszechobecne w naszym cyfrowym społeczeństwie. UE jest pionierem w tworzeniu ekosystemu cyberbezpieczeństwa poprzez przepisy dotyczące infrastruktury krytycznej, gotowości i reagowania w zakresie cyberbezpieczeństwa oraz certyfikacji produktów związanych z cyberbezpieczeństwem. Obecnie kończymy tworzenie tego ekosystemu za pomocą aktu, który zapewnia bezpieczeństwo w domach nas wszystkich, we wszystkich naszych przedsiębiorstwach i we wszystkich skomunikowanych wzajemnie produktach. Cyberbezpieczeństwo jest obecnie sprawą wagi społecznej, a nie tylko sektorowej.*

Thierry **Breton**, komisarz do spraw rynku wewnętrznego, dodał: *Jeśli chodzi o cyberbezpieczeństwo, Europa jest tak silna, jak jej najsłabsze ogniwo: niezależnie od tego, czy jest to państwo członkowskie podatne na zagrożenia, czy też produkt bez odpowiednich zabezpieczeń w całym łańcuchu dostaw. Komputery, telefony, urządzenia gospodarstwa domowego, urządzenia wirtualnego wspomagania, samochody, zabawki... każde z tych setek milionów podłączonych do internetu produktów stanowią potencjalny punkt dostępu dla cyberataku. Jednak obecnie większość sprzętów i oprogramowania komputerowego nie podlega żadnym obowiązkom w zakresie cyberbezpieczeństwa. Dzięki uwzględnieniu cyberbezpieczeństwa już na etapie projektowania europejski akt dotyczący cyberodporności pomoże chronić europejską gospodarkę i nasze bezpieczeństwo zbiorowe.*

Ataki z użyciem oprogramowania typu ransomware uderzają w organizacje na całym świecie co 11 sekund, a szacowany roczny koszt cyberprzestępczości w 2021 r. wyniósł 5,5 bln euro (cytat z magazynu Cybersecurity Ventures w sprawozdaniu Wspólnego Centrum Badawczego z 2020 r.: „Cybersecurity – Our Digital Anchor, a European perspective" [Cyberbezpieczeństwo, nasza kotwica w cyberprzestrzeni]). Zapewnienie wysokiego poziomu cyberbezpieczeństwa i zmniejszenie podatności produktów cyfrowych na zagrożenia – jednej z głównych przyczyn udanych ataków – jest ważniejsze niż kiedykolwiek wcześniej. Wraz z rozwojem inteligentnych i podłączonych do internetu przedmiotów cyberincydent w jednym produkcie może mieć wpływ na cały łańcuch dostaw, co może prowadzić do poważnych zakłóceń działalności gospodarczej i społecznej na rynku wewnętrznym, obniżyć poziom bezpieczeństwa lub nawet zagrażać życiu.

Proponowane dziś środki opierają się na nowych ramach prawnych w zakresie unijnego prawodawstwa dotyczącego produktów i będą określać:

(a) przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia ich cyberbezpieczeństwa;

(b) zasadnicze wymagania dotyczące projektowania, opracowywania i wytwarzania produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów;

(c) zasadnicze wymagania dotyczące procedur postępowania z podatnością wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów zawierających elementy cyfrowe przez cały cykl ich życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur. Producenci będą również musieli aktywnie zgłaszać podatności, które zostały wykorzystane do ataków, oraz incydenty;

d) przepisy dotyczące nadzoru rynku i ich egzekwowania.

Nowe przepisy zrównoważą odpowiedzialność producentów, którzy muszą zapewnić zgodność produktów z elementami cyfrowymi udostępnianymi na rynku UE z wymogami bezpieczeństwa. W rezultacie przyniosą one korzyści konsumentom i mieszkańcom UE, a także przedsiębiorstwom korzystającym z produktów cyfrowych, zwiększając przejrzystość zabezpieczeń i promując zaufanie do produktów zawierających elementy cyfrowe, a także zapewniając lepszą ochronę praw podstawowych ich użytkowników, takich jak prywatność i ochrona danych.

Podczas gdy inne jurysdykcje na całym świecie analizują te kwestie, europejski akt dotyczący cyberodporności prawdopodobnie stanie się międzynarodowym punktem odniesienia, wykraczając poza rynek wewnętrzny UE. Unijne normy oparte na europejskim akcie dotyczącym cyberodporności ułatwią jego wdrożenie i będą stanowić atut dla unijnego sektora cyberbezpieczeństwa na rynkach światowych.

Proponowane przepisy będą miały zastosowanie do wszystkich produktów, które są bezpośrednio lub pośrednio połączone z innym urządzeniem lub siecią. Istnieją pewne wyjątki w zakresie produktów, w odniesieniu do których wymogi cyberbezpieczeństwa są już określone w obowiązujących przepisach UE, jak w przypadku wyrobów medycznych, lotnictwa lub samochodów.

Dalsze działania

Przeanalizowanie projektu europejskiego aktu dotyczącego cyberodporności należy teraz do Parlamentu Europejskiego i Rady. Po przyjęciu nowych przepisów podmioty gospodarcze i państwa członkowskie będą miały dwa lata na dostosowanie się do nowych wymogów. Wyjątkiem od tej zasady jest obowiązek aktywnego zgłaszania przez producentów przypadków wykorzystywania podatności i incydentów, który miałby zastosowanie już rok od daty wejścia w życie, ponieważ wymaga on mniejszej liczby dostosowań organizacyjnych niż inne nowe obowiązki. Komisja będzie regularnie dokonywać przeglądu europejskiego aktu dotyczącego cyberodporności i składać sprawozdania na temat jego funkcjonowania.

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. Szacuje się, że roczne koszty naruszeń ochrony danych wynoszą co najmniej 10 mld euro, a roczne koszty szkodliwych prób zakłócenia ruchu w internecie szacuje się na co najmniej 65 mld euro (sprawozdanie z oceny skutków towarzyszące rozporządzeniu delegowanemu Komisji uzupełniającemu rozporządzenie delegowane odnoszące się do dyrektywy w sprawie urządzeń radiowych).

W strategii Unii Europejskiej w zakresie cyberbezpieczeństwa, przedstawionej w grudniu 2020 r.,

zaproponowano włączenie cyberbezpieczeństwa do wszystkich elementów łańcucha dostaw oraz dalsze połączenie działań i zasobów UE w ramach czterech płaszczyzn związanych z cyberbezpieczeństwem – rynku wewnętrznego, egzekwowania prawa, dyplomacji i obronności. Strategia ta czerpie z unijnej strategii Kształtowania cyfrowej przyszłości Europy i strategii UE w zakresie unii bezpieczeństwa oraz opiera się na szeregu aktów ustawodawczych, działań i inicjatyw wdrożonych przez UE w celu wzmocnienia zdolności w zakresie cyberbezpieczeństwa i zapewnienia większej cyberodporności Europy.

Nowy europejski akt dotyczący cyberodporności uzupełni unijne ramy cyberbezpieczeństwa: dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS), dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS 2), która została niedawno uzgodniona przez Parlament Europejski i Radę, oraz unijny akt o cyberbezpieczeństwie.

Informacje dodatkowe

Pytania i odpowiedzi: europejski akt dotyczący cyberodporności

Zestawienie informacji na temat europejskiego aktu dotyczącego cyberodporności

Wniosek w sprawie europejskiego aktu dotyczącego cyberodporności

Zestawienie informacji na temat nowej strategii UE w zakresie cyberbezpieczeństwa

Zestawienie informacji na temat wniosku dotyczącego dyrektywy w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji – NIS2)

Zestawienie informacji 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 wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS 2)

Wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych

IP/22/5374

Kontakty z mediami:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

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

Related media

Cybersecurity