KOMISJA
EUROPEJSKA

Bruksela, dnia 15.9.2022 r.
SWD(2022) 283 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW

odnoszącej się do aktu dotyczącego cyberodporności

Towarzyszący dokumentowi:

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady

w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Streszczenie oceny skutków (maks. 2 strony)

Ocena skutków odnosząca się do aktu dotyczącego cyberodporności

A. Zasadność działań

Na czym polega problem i dlaczego jest to problem na szczeblu UE?

Sprzęt i oprogramowanie często padają celem udanych cyberataków, które do 2021 r. doprowadziły do szacowanego globalnego rocznego kosztu cyberprzestępczości w wysokości 5,5 bln EUR. Z produktami tymi wiążą się dwa główne problemy zwiększające koszty dla użytkowników i społeczeństwa: 1) niski poziom cyberbezpieczeństwa, który przejawia się w powszechnych podatnościach oraz niewystarczającym i niespójnym dostarczaniu aktualizacji zabezpieczeń w celu wyeliminowania tych podatności, oraz 2) niedostateczne zrozumienie i dostęp do informacji przez użytkowników, co uniemożliwia im wybór produktów o odpowiednich właściwościach w zakresie cyberbezpieczeństwa lub korzystanie z nich w sposób bezpieczny.

Cyberbezpieczeństwo produktów z elementami cyfrowymi ma wyraźny wymiar transgraniczny, ponieważ produkty wytwarzane w jednym państwie są często wykorzystywane na całym rynku wewnętrznym. Ponadto incydenty początkowo dotyczące pojedynczego podmiotu lub jednego państwa członkowskiego często w ciągu kilku minut rozprzestrzeniają się na cały rynek wewnętrzny.

Chociaż obowiązujące przepisy dotyczące rynku wewnętrznego mają zastosowanie do niektórych produktów z elementami cyfrowymi, większość sprzętu i oprogramowania nie jest obecnie objęta żadnymi przepisami UE regulującymi ich cyberbezpieczeństwo. W szczególności obecne ramy prawne UE nie odnoszą się do cyberbezpieczeństwa oprogramowania niewbudowanego, nawet jeśli naruszenia bezpieczeństwa w wyniku cyberataku w coraz większym stopniu są wymierzone w podatności tych produktów, co powoduje znaczne koszty społeczne i gospodarcze. Do najnowszych przykładów należy oprogramowanie szpiegujące Pegasus, które wykorzystywało podatności w telefonach komórkowych, lub robak oprogramowania szantażującego WannaCry, który wykorzystywał podatność w systemie Windows, co miało wpływ na komputery na całym świecie.

Co należy osiągnąć?

Wskazano dwa główne cele służące zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego: 1) stworzenie warunków dla rozwoju bezpiecznych produktów z elementami cyfrowymi przez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z mniejszą liczbą podatności, a także aby producenci poważnie traktowali bezpieczeństwo w całym cyklu życia produktu, oraz 2) stworzenie warunków umożliwiających użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich. Określono cztery cele szczegółowe: (i) zapewnienie, aby producenci poprawiali bezpieczeństwo produktów z elementami cyfrowymi, począwszy od etapu projektowania i opracowywania oraz przez cały cykl życia; (ii) zapewnienie spójnych ram cyberbezpieczeństwa, ułatwiających producentom sprzętu i oprogramowania przestrzeganie przepisów; (iii) zwiększenie przejrzystości zabezpieczeń produktów z elementami cyfrowymi oraz (iv) umożliwienie przedsiębiorstwom i konsumentom bezpiecznego korzystania z produktów z elementami cyfrowymi.

Na czym polega wartość dodana podjęcia działań na poziomie UE (zasada pomocniczości)?

Wyraźnie transgraniczny charakter cyberbezpieczeństwa i coraz częstsze incydenty, których skutki uboczne są odczuwalne w innych krajach oraz dotykają inne sektory i produkty, oznaczają, że państwa członkowskie nie są w stanie skutecznie osiągnąć wspomnianych celów samodzielnie. Biorąc pod uwagę globalny charakter rynków produktów z elementami cyfrowymi, państwa członkowskie stoją w obliczu

tego samego ryzyka w przypadku tego samego produktu z elementami cyfrowymi na swoim terytorium. Pojawiające się niejednolite ramy potencjalnie rozbieżnych przepisów krajowych również mogą zakłócić otwarty i konkurencyjny jednolity rynek produktów z elementami cyfrowymi. Wspólne działanie na szczeblu UE jest zatem konieczne, aby wzbudzić większe zaufanie użytkowników i poprawić atrakcyjność produktów z elementami cyfrowymi wprowadzanych do obrotu w UE. Przyniosłoby to również korzyści rynkowi wewnętrznemu, gdyż zapewniłoby pewność prawa i równe warunki działania producentom produktów z elementami cyfrowymi.

B. Rozwiązania

Jakie są różne warianty działań służących osiągnięciu celów? Czy wskazano preferowany wariant? Jeżeli nie, to dlaczego?

Przeanalizowano cztery warianty strategiczne i związane z nimi podwarianty wykraczające poza stan obecny: 1) podejście oparte na prawie miękkim i środki dobrowolne; 2) interwencja regulacyjna *ad hoc* w odniesieniu do konkretnego produktu dotycząca cyberbezpieczeństwa materialnych produktów z elementami cyfrowymi i odpowiedniego oprogramowania wbudowanego; 3) podejście mieszane, w tym horyzontalne przepisy bezwzględnie obowiązujące dotyczące cyberbezpieczeństwa materialnych produktów z elementami cyfrowymi i odpowiedniego oprogramowania wbudowanego, a także podejście stopniowe do oprogramowania niewbudowanego wraz z dwoma podwariantami odnoszącymi się do oceny zgodności oraz 4) horyzontalna interwencja regulacyjna wprowadzająca wymogi cyberbezpieczeństwa w odniesieniu do szerokiego zakresu produktów z elementami cyfrowymi, w tym oprogramowania niewbudowanego, wraz z podwariantami dotyczącymi zakresu i oceny zgodności.

W ramach oceny skutków stwierdzono, że **preferowanym wariantem** jest wariant 4 obejmujący wszystkie produkty z elementami cyfrowymi i przewidujący obowiązkową ocenę przez stronę trzecią produktów krytycznych na podstawie oceny skuteczności względem celów szczegółowych, efektywności kosztów w stosunku do korzyści oraz spójności.

Jakie są opinie poszczególnych zainteresowanych stron? Jak kształtuje się poparcie dla poszczególnych wariantów?

Zapytani o ocenę skuteczności interwencji politycznych respondenci biorący udział w konsultacjach publicznych zgodzili się, że wariant 4 byłby najskuteczniejszym środkiem (4,08 w skali od 1 do 5). Do respondentów tych należą organizacje konsumenckie (5,00), respondenci określający się jako użytkownicy (4,22), jednostki notyfikowane (4,17), organy nadzoru rynku (5,00) oraz producenci produktów z elementami cyfrowymi (3,85), w tym mali i średni producenci (4,05).

C. Skutki wdrożenia preferowanego wariantu

Jakie korzyści przyniesie wdrożenie preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Preferowany wariant może przynieść znaczące korzyści dla poszczególnych zainteresowanych stron. W przypadku przedsiębiorstw pozwoli on zapobiec rozbieżnym przepisom dotyczącym bezpieczeństwa produktów z elementami cyfrowymi oraz obniżyć koszty przestrzegania związanych z nimi przepisów dotyczących cyberbezpieczeństwa. Może się on przyczynić do zmniejszenia liczby cyberincydentów, obniżenia kosztów postępowania w przypadku incydentu oraz uniknięcia nadszarpnięcia reputacji. W przypadku całej UE szacuje się, że inicjatywa może doprowadzić do obniżenia kosztów związanych z incydentami dotyczącymi przedsiębiorstw o około 180–290 mld EUR rocznie. Ponadto inicjatywa może spowodować wzrost obrotu ze względu na coraz większe wykorzystanie produktów z elementami

cyfrowymi. Może również poprawić światową reputację przedsiębiorstw, co spowodowałoby wzrost popytu spoza UE. Jeżeli chodzi o użytkowników końcowych, preferowany wariant może zwiększyć przejrzystość zabezpieczeń i ułatwić korzystanie z produktów z elementami cyfrowymi. Konsumenci i obywatele odniosą także korzyść polegającą na lepszej ochronie ich praw podstawowych, takich jak prywatność i ochrona danych.

Jakie są koszty wdrożenia preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Preferowany wariant może zwiększyć koszty przestrzegania i egzekwowania przepisów ponoszone przez przedsiębiorstwa, jednostki notyfikowane i organy publiczne, w tym organy notyfikujące, organy ds. akredytacji i organy nadzoru rynku. W przypadku twórców oprogramowania i producentów sprzętu zwiększy to bezpośrednie koszty przestrzegania przepisów w związku z nowymi wymogami cyberbezpieczeństwa, oceną zgodności, obowiązkami w zakresie dokumentacji i zgłaszania incydentów, co spowoduje, że zagregowane koszty przestrzegania przepisów wyniosą około 29 mld EUR przy szacowanej wartości rynkowej produktów z elementami cyfrowymi sięgającej 1 485 mld EUR w przeliczeniu na obroty. Użytkownicy końcowi, w tym biznesowi użytkownicy końcowi, konsumenci i obywatele mogą doświadczyć wyższych cen produktów z elementami cyfrowymi. Należy je jednak postrzegać w kontekście znaczących korzyści opisanych powyżej. W przypadku jednostek notyfikowanych przewiduje się, że dodatkowe koszty zostaną zrekompensowane przez wzrost obrotów.

Jakie są skutki dla MŚP i konkurencyjności?

Nowe wymogi będą miały wpływ na MŚP zarówno jako producentów, jak i użytkowników końcowych. Pod względem kosztów przestrzegania przepisów MŚP mogą odczuć co do zasady większy wpływ niż duże przedsiębiorstwa, które zazwyczaj mają lepsze korzyści skali i większą świadomość w dziedzinie cyberbezpieczeństwa. MŚP odniosą jednak duże korzyści z inicjatywy, ponieważ cyberbezpieczeństwo uwzględnione w produktach z elementami cyfrowymi oznacza znaczne zmniejszenie kosztów dla MŚP jako użytkowników. Jako producenci MŚP mogą czerpać korzyści w postaci większego zaufania użytkowników końcowych i nowych klientów. Niezakłócony dostęp do rynku wewnętrznego i ograniczenie fragmentacji rynku może być jeszcze bardziej korzystne dla MŚP, które są gorzej przygotowane do radzenia sobie z różnymi wymogami regulacyjnymi. Podkreślając konieczność zastosowania proporcjonalnego podejścia i środków wspierających, MŚP ogólnie poparły równe warunki działania dla wszystkich przedsiębiorstw i stwierdziły, że w przypadku realizacji scenariusza obowiązkowych wymogów horyzontalnych nie znajdą się w niekorzystnej sytuacji w porównaniu z większymi przedsiębiorstwami .

Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?

Przedmiotowa inicjatywa będzie miała wpływ na organy krajowe, takie jak krajowe organy notyfikujące, organy ds. akredytacji i organy nadzoru rynku jako odpowiedzialne za monitorowanie i egzekwowanie proponowanych środków. Organy te poniosą dodatkowe koszty dostosowania (np. szkolenia i zasoby ludzkie) i egzekwowania z uwagi na uwzględnienie nowych wymogów. Środki wydatkowane przez jednostki akredytujące są jednak równoważone i ponoszone w dużej mierze przez jednostki oceniające zgodność w drodze zakupu usług akredytacyjnych.

Czy wystąpią inne znaczące skutki?

Nie przewiduje się innych znaczących negatywnych skutków. Preferowany wariant strategiczny pomoże zmniejszyć liczbę i dotkliwość incydentów, w tym naruszeń ochrony danych osobowych, oraz przyniesie pozytywne skutki społeczne, takie jak ograniczenie cyberprzestępczości. Zapotrzebowanie na specjalistów

w dziedzinie bezpieczeństwa prawdopodobnie wzrośnie, a asymetria informacji w zakresie cyberbezpieczeństwa zostanie ograniczona.
Proporcjonalność?
Preferowany wariant nie wykracza poza to, co konieczne do zadowalającej realizacji celów szczegółowych. Przedmiotowa interwencja może zapewnić zabezpieczenie produktów z elementami cyfrowymi w całym cyklu ich życia i w sposób proporcjonalny do występującego ryzyka.
D. Działania następcze
Kiedy nastąpi przegląd przyjętej polityki?
W terminie [36 miesięcy] od daty rozpoczęcia stosowania niniejszej inicjatywy, a następnie co cztery lata Komisja powinna przedkładać Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszej inicjatywy.