KOMISJA
EUROPEJSKA

Bruksela, dnia 16.12.2020 r.
SWD(2020) 344 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

SPRAWOZDANIE ZE STRESZCZENIA OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Streszczenie oceny skutków

Ocena skutków dotycząca *przeglądu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej zwanej „dyrektywą w sprawie bezpieczeństwa sieci i informacji")*

A. Zasadność działań

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

Pomimo znaczących osiągnięć dyrektywy w sprawie bezpieczeństwa sieci i informacji, w tym przyczynienia się do istotnej zmiany nastawienia oraz instytucjonalnego i regulacyjnego podejścia do cyberbezpieczeństwa w wielu państwach członkowskich, okazało się, że ma ona pewne ograniczenia. Cyfrowa transformacja społeczeństwa (której skala znacznie wzrosła podczas kryzysu związanego z COVID-19) poszerzyła krajobraz zagrożeń i wiąże się z nowymi wyzwaniami, które wymagają adekwatnej i innowacyjnej reakcji. Liczba cyberataków dalej rośnie, a coraz bardziej wyrafinowane ataki pochodzą z wielu różnych źródeł w UE i poza jej granicami.

W ocenie skutków opartej na ocenie funkcjonowania dyrektywy w sprawie bezpieczeństwa sieci i informacji zidentyfikowano następującej problemy: niski poziom cyberodporności przedsiębiorstw działających w UE; różnice w poziomie odporności między państwami członkowskimi i sektorami oraz niski poziom wspólnej orientacji sytuacyjnej i brak wspólnego reagowania kryzysowego. Przykładowo na skutek niektórych z powyższych problemów i czynników doszło do sytuacji, w których główne szpitale w państwie członkowskim nie są objęte zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji; w związku z czym państwa te nie są zobowiązane do wdrażania środków bezpieczeństwa wynikających z dyrektywy, podczas gdy w innych państwach członkowskich niemal każdy szpital jest objęty wymogami w zakresie bezpieczeństwa sieci i informacji.

Jakie cele należy osiągnąć?

W przeglądzie dyrektywy w sprawie bezpieczeństwa sieci i informacji przewidziano trzy ogólne cele:

1. **zwiększyć poziom cyberodporności szerokiego grona przedsiębiorstw, prowadzących działalność na terenie Unii Europejskiej we wszystkich istotnych sektorach,** przez wprowadzenie przepisów, które zagwarantują, że wszelkie podmioty publiczne i prywatne na rynku wewnętrznym, odgrywające ważną rolę dla gospodarki i dla społeczeństwa jako takiego, będą zobowiązane do zastosowania adekwatnych środków w zakresie cyberbezpieczeństwa;
2. **ograniczyć różnice w poziomie odporności na rynku wewnętrznym w sektorach już objętych dyrektywą**, przez dalsze dostosowywanie (1) faktycznego zakresu, (2) wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, (3) przepisów regulujących krajowe środki nadzorcze i egzekucyjne oraz (4) kompetencji właściwych organów w państwach członkowskich;
3. **usprawnić wspólną orientację sytuacyjną oraz zbiorową zdolność do przygotowania się i reagowania na zagrożenia** przez zastosowanie środków służących zwiększeniu zaufania pomiędzy właściwymi organami, zwiększoną wymianę informacji oraz ustanawianie przepisów i procedur na wypadek wystąpienia incydentów na dużą skalę lub kryzysów.

Na czym polega wartość dodana działań na szczeblu UE (pomocniczość)?

Odporność pod względem cyberbezpieczeństwa w Unii nie będzie skuteczna, jeśli będzie ona traktowana różnie w ramach sztywnych struktur krajowych lub regionalnych. Dyrektywą w sprawie bezpieczeństwa

sieci i informacji wyeliminowano owo niedociągnięcie, przez ustanowienie ram bezpieczeństwa sieci i systemów informatycznych na szczeblu krajowym i unijnym. Tym niemniej transpozycja i wdrożenie dyrektywy również unaoczniły nieodłączne wady niektórych przepisów lub podejść, takie jak niejasno wytyczony zakres stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji. Co więcej, od początku kryzysu związanego z COVID-19 gospodarka europejska stała się bardziej niż kiedykolwiek wcześniej zależna od sieci i systemów informatycznych, a sektory i usługi są w coraz większym stopniu wzajemnie ze sobą powiązane. Pierwszy okresowy przegląd dyrektywy w sprawie bezpieczeństwa sieci i informacji stworzył szansę na dalsze działania na szczeblu UE. Interwencję UE wykraczającą poza środki obecnie stosowane w ramach dyrektywy w sprawie bezpieczeństwa sieci i informacji uzasadniają: (i) transgraniczny charakter problemów; (ii) potencjał działań unijnych do poprawy i ułatwienia skutecznych strategii krajowych; (iii) korzyści płynące z uzgodnionych i opartych na współpracy działań politycznych w zakresie bezpieczeństwa sieci i informacji dla skutecznej ochrony danych osobowych i prywatności.

B. Rozwiązania

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

W ramach oceny skutków analizowano cztery warianty strategiczne: (0) utrzymanie status quo; (1) środki o charakterze nieustawodawczym w celu dostosowania transpozycji; (2) wprowadzenie ograniczonych zmian w dyrektywie w sprawie bezpieczeństwa sieci i informacji w celu dalszej harmonizacji; (3) wprowadzenie zmian systemowych i strukturalnych w dyrektywie w sprawie bezpieczeństwa sieci i informacji. Wariant pierwszy odrzucono na wczesnym etapie, gdyż nie różni się on znacząco od wariantu utrzymania statusu quo. W ocenie skutków opowiedziano się za wariantem trzecim (tzn. **wprowadzeniem zmian systemowych i strukturalnych do ram dotyczących bezpieczeństwa sieci i informacji**) jako **wariantem preferowanym**, gdyż przewiduje on bardziej zasadnicze zmiany służące temu, by uwzględnić więcej sektorów gospodarek w Unii, ale równocześnie zapewnia nadzór ukierunkowany na proporcjonalnie większe, kluczowe przedsiębiorstwa i równocześnie, jasno określając zakres zastosowania. Wariant ten pozwala też uprościć i pełniej zharmonizować zobowiązania przedsiębiorstw związane z bezpieczeństwem, stworzyć bardziej efektywne ramy dla działań operacyjnych, określić jasne podstawy dla podziału obowiązków i rozliczalności właściwych podmiotów oraz zachęcić do wymiany informacji.

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

Większość właściwych organów i przedsiębiorstw wyraziła poparcie dla zmian w dyrektywie w sprawie bezpieczeństwa sieci i informacji. W trakcie różnych konsultacji zwracały one uwagę na fakt, że po proponowanym przeglądzie dyrektywa w sprawie bezpieczeństwa sieci i informacji powinna obejmować dodatkowe (pod)sektory, dostosować lub uprościć dalsze środki ochrony oraz obowiązki sprawozdawcze. Zainteresowane strony wyraziły również poparcie dla nowych koncepcji i środków w odniesieniu do polityki, które stanowią część preferowanego wariantu (np. polityka w zakresie bezpieczeństwa łańcucha dostaw, instytucjonalizacja operacyjnych ram zarządzania kryzysowego w UE).

C. Skutki wdrożenia preferowanego wariantu

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

Wdrożenie preferowanego wariantu przyniosłoby następujące znaczące korzyści. Szacunki dokonane na

podstawie modeli ekonomicznych opracowanych w ramach analizy uzupełniającej przegląd dyrektywy w sprawie bezpieczeństwa sieci i informacji wskazują, że preferowany wariant umożliwiłby zmniejszenie kosztów cyberincydentów o 11,3 mld EUR.

Zakres sektorowy byłby znacznie większy w ramach dyrektywy w sprawie bezpieczeństwa sieci i informacji, a oprócz wyżej wymienionych korzyści dyrektywa pozwoliłaby też na zrównoważenie obciążeń potencjalnie spowodowanych wymogami w zakresie bezpieczeństwa sieci i informacji, zwłaszcza w odniesieniu do nadzoru, dla podmiotów nowo objętych przepisami oraz dla właściwych organów. Dzieje się tak, gdyż nowe ramy dotyczące bezpieczeństwa sieci i informacji wiązałyby się z wybraniem podejścia dwupoziomowego, które kładzie szczególny nacisk na duże i najważniejsze podmioty oraz rozróżnia system nadzoru, który umożliwia wyłącznie działania nadzorcze *ex post* (czyli reagowanie na problem, wykluczające ogólny obowiązek systematycznego dokumentowania zgodności) dla wielu z tych podmiotów, przede wszystkim dla tych uważanych za „ważne" choć jeszcze nie „niezbędne".

Generalnie preferowany wariant strategiczny doprowadziłby do osiągnięcia efektywnych kompromisów i synergii, przy czym najlepszy z analizowanych potencjalnych wariantów strategicznych zapewniłby zwiększony i spójny poziom cyberodporności najważniejszych podmiotów w całej Unii, co w efekcie kiedyś doprowadziłoby do oszczędności zarówno dla biznesu, jak i dla społeczeństwa.

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

Wdrożenie preferowanego wariantu strategicznego zrodziłoby dla władz państw członkowskich pewne koszty przestrzegania i egzekwowania nowych przepisów (oszacowano, że zasoby wzrosłyby ogółem o 20–30 %). Nowe ramy wiązałyby się też ze znaczącymi korzyściami dzięki lepszemu oglądowi sytuacji kluczowych przedsiębiorstw oraz interakcji z tymi przedsiębiorstwami, dzięki transgranicznej współpracy operacyjnej i dzięki mechanizmom wzajemnej pomocy i wzajemnej oceny. To doprowadziłoby do ogólnej poprawy możliwości w zakresie cyberbezpieczeństwa we wszystkich państwach członkowskich.

Szacuje się, że w pierwszych latach po wdrożeniu nowych ram dotyczących bezpieczeństwa sieci i informacji przedsiębiorstwa objęte tymi ramami musiałyby zwiększyć swoje bieżące wydatki w zakresie bezpieczeństwa ICT o maksymalnie 22 % (w przypadku przedsiębiorstw objętych zakresem stosowania obecnej dyrektywy w sprawie bezpieczeństwa sieci i informacji wzrost ten wyniósłby 12 %). Tym niemniej średni wzrost wydatków w zakresie bezpieczeństwa ICT przyniósłby też proporcjonalne korzyści z takich inwestycji, zwłaszcza w wyniku znaczącego ograniczenia kosztów cyberincydentów (szacowanego na 11,3 mld EUR na przestrzeni dziesięciu lat).

Jakie są skutki dla MŚP i konkurencyjności?

W preferowanym wariancie małe i mikroprzedsiębiorstwa zostałyby wyłączone z zakresu ram dotyczących bezpieczeństwa sieci i informacji. Przewiduje się, że w pierwszych latach po wdrożeniu nowych ram dotyczących bezpieczeństwa sieci i informacji nastąpi wzrost wydatków na bezpieczeństwo ICT dla średnich przedsiębiorstw. Zaostrzenie wymogów bezpieczeństwa dla tych podmiotów również zachęciłoby je do poprawiania swoich zdolności w zakresie cyberbezpieczeństwa i pomogłoby usprawnić zarządzaniem ryzykiem ICT.

Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?

Przewiduje się następujący skutek dla budżetów i administracji krajowych: Szacuje się, że w krótkim bądź średnim okresie nastąpi wzrost zasobów o 20 do 30 %.

Czy wystąpią inne znaczące skutki?
Nie oczekuje się wystąpienia innych znaczących skutków negatywnych. Przewiduje się, że preferowany wariant strategiczny pozwoli na zwiększenie zdolności w zakresie cyberbezpieczeństwa i tym samym wpłynąłby bardziej znacząco na zmniejszenie liczby i stopnia ciężkości incydentów, w tym naruszeń ochrony danych. Również prawdopodobne jest, że dyrektywa pomoże zapewnić równe warunki działania we wszystkich państwach członkowskich dla wszystkich podmiotów objętych zakresem stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji, i że zmniejszy asymetrię informacyjną w zakresie cyberbezpieczeństwa.
Proporcjonalność?
Preferowany wariant nie wykracza poza to, co konieczne do zadowalającej realizacji konkretnych celów. Przewidziane dostosowanie i uproszczenie środków ochrony oraz obowiązków sprawozdawczych są odpowiedzią na apele państw członkowskich i sektora przedsiębiorstw o usprawnienie obecnych ram.
D. Działania następcze
Kiedy nastąpi przegląd przyjętej polityki?
Pierwszy przegląd polityki nastąpi po upływie 54 miesięcy od dnia wejścia instrumentu prawnego w życie. Komisja przekaże Parlamentowi Europejskiemu i Radzie sprawozdanie z takiego przeglądu. Przegląd zostanie przygotowany przy wsparciu ENISA oraz grupy współpracy.