

# Wiadomości

2019-03-13

## Przepisy o cyberbezpieczeństwie w odpowiedzi na zagrożenia ze strony Chin



- Unijny system certyfikacji bezpieczeństwa cybernetycznego produktów, procesów i usług informatycznych
- Lepsza ochrona konsumentów i łatwiejsze procedury dla przedsiębiorstw
- Więcej uprawnień dla unijnej agencji ds. bezpieczeństwa cybernetycznego

Wdrażając technologię 5G trzeba uwzględnić zagrożenie informatyczne ze strony Chin

### **Parlament przyjął unijny system certyfikacji bezpieczeństwa cybernetycznego dla produktów, procesów i usług w odpowiedzi na zagrożenia technologiczne ze strony Chin.**

We wtorek Parlament Europejski przyjął unijny „akt ws. cyberbezpieczeństwa”. Projekt poparło 586 posłów, 44 było przeciw a 36 wstrzymało się od głosu. Przepisy wprowadzają pierwszy obowiązujący w całej Unii system certyfikacji bezpieczeństwa cybernetycznego. Celem jest zapewnienie, że certyfikowane produkty, procesy i usługi sprzedawane w krajach UE spełniają standardy bezpieczeństwa cybernetycznego.

Parlament przyjął również rezolucję wzywającą do podjęcia działań na szczeblu UE w sprawie zagrożeń dla bezpieczeństwa związanych z rosnącą obecnością technologiczną Chin w UE.

Posłowie wyrażają głębokie zaniepokojenie pojawiającymi się ostatnio opiniami, wedle których sprzęt funkcjonujący w sieci 5G może mieć wbudowane moduły umożliwiające chińskim producentom i władzom nieuprawniony dostęp do danych osobowych Europejczyków i systemów telekomunikacyjnych w UE.

## **Chińskie prawo ochrony państwa zagrożeniem dla bezpieczeństwa cybernetycznego UE**

Parlament wskazuje też na zagrożenie dla unijnego bezpieczeństwa wynikające z przepisów obowiązujących w niektórych krajach spoza UE. Chodzi o przepisy, które nakładają na wszystkie zarejestrowane w tych krajach przedsiębiorstwa, w tym producentów i sprzedawców sprzętu informatycznego, obowiązek współpracy z organami państwowymi w zakresie ochrony bezpieczeństwa narodowego. „Bezpieczeństwo narodowe” zwykle zdefiniowane jest tam bardzo szeroko i obejmuje również zagraniczną działalność krajowych firm. Chińskie prawo bezpieczeństwa państwa wywołało reakcje w różnych krajach, takie jak wzmocniona kontrola zabezpieczeń a nawet bezwarunkowy zakaz stosowania technologii 5G przez daną firmę.

Posłowie chcą, żeby Komisja Europejska i państwa członkowskie opracowały wskazówki dla nabywców jak radzić sobie z zagrożeniami cybernetycznymi i podatnością na ataki cybernetyczne przy zakupie sprzętu 5G, na przykład poprzez dywersyfikację sprzętu od różnych dostawców, wprowadzenie wieloetapowych procesów zamówień publicznych oraz ustanowienie strategii mającej na celu zmniejszenie uzależnienia Unii Europejskiej od zagranicznych technologii bezpieczeństwa cybernetycznego.

Wzywają również Komisję, by upoważniła unijną Agencję Bezpieczeństwa Cyberprzestrzeni (ENISA) do pracy nad systemem certyfikacji gwarantującym, że 5G w UE spełnia najwyższe standardy bezpieczeństwa.

### **„Akt ws. cyberbezpieczeństwa” umożliwi certyfikację urządzeń sieciowych**

Unijny „akt ws. cyberbezpieczeństwa” został już wstępnie uzgodniony z państwami członkowskimi. Kładzie on nacisk na znaczenie certyfikacji infrastruktury krytycznej, w tym sieci energetycznych, wodociągowych, dostaw energii i systemów bankowych, a także innych produktów, procesów i usług. Certyfikacja będzie na razie dobrowolna. Do 2023 roku Komisja oceni, czy któryś z nowych systemów powinien stać się obowiązkowy.

Przepisy o bezpieczeństwie cybernetycznym przewidują również stały mandat i większe zasoby ludzkie i finansowe dla unijnej Agencji Bezpieczeństwa Cyberprzestrzeni, ENISA.

### **Cytat**

Po głosowaniu nad ustawą o bezpieczeństwie cybernetycznym, sprawozdawczyni [Angelika Niebler](#) (EPL, Niemcy) powiedziała: "To znaczący sukces, pozwoli on UE sprostać wyzwaniu wzrastającego poziomu ryzyka w świecie cyfrowym w nadchodzących latach. Te przepisy są kamieniem węgielnym, dzięki któremu UE może stać się globalnym graczem w dziedzinie bezpieczeństwa cybernetycznego. Konsumenci, jak również przemysł, muszą być w stanie zaufać rozwiązaniom informatycznym".

## **Dalsze kroki**

„Akt ws. cyberbezpieczeństwa” musi teraz formalnie zatwierdzić Rada. Rozporządzenie wejdzie w życie 20 dni po jego opublikowaniu w Dzienniku urzędowym UE.

Rezolucja w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE zostanie przesłana do Komisji i państw członkowskich

Źródło: PE

Źródło:

<http://paliwa.pl/strona-startowa/archiwum/przepisy-o-cyberbezpieczenstwie-w-odpowiedzi-na-zagrozenia-ze-strony-chin>