Projekt ustawy Federalnego Ministerstwa Spraw Wewnętrznych

Projekt aktu o wzmocnieniu cyberbezpieczeństwa[1]

Z dnia ...

Parlament Federalny Niemiec (Bundestag), za zgodą Rady Federalnej Niemiec (Bundesrat), przyjął następującą ustawę:

[…]

Artykuł 4

Zmiany do ustawy o ochronie danych i prywatności w telekomunikacji i usługach cyfrowych

Ustawa o ochronie danych i prywatności w telekomunikacji i usługach cyfrowych z dnia 23 czerwca 2021 r. (Federalny Dziennik Ustaw I s. 1982; 2022 I s. 1045), ostatnio zmieniona art. 3 ustawy z dnia 10 marca 2026 r. (Federalny Dziennik Ustaw 2026 I nr 64), zostaje zmieniona w następujący sposób:

1. po sekcji 19 ust. 4 dodaje się sekcje 5 i 6 w brzmieniu:

(1) „Jeżeli dostawca usług cyfrowych stwierdzi, że podczas korzystania z usługi przez użytkownika doszło do zakłócenia wynikającego z jednej z jego usług, musi niezwłocznie powiadomić o tym użytkownika, o ile jest znana jego tożsamość. W zakresie, w jakim jest to technicznie możliwe i uzasadnione ekonomicznie, dostawca musi, w zakresie swojej odpowiedzialności za usługi cyfrowe świadczone w celach zarobkowych, poinformować użytkownika o odpowiednich, skutecznych i dostępnych środkach technicznych, za pomocą których może on wykryć i usunąć zakłócenie. Jeśli dostawca został powiadomiony o zakłóceniu przez Federalny Urząd ds. Bezpieczeństwa Informacji (BSI), musi on przekazać użytkownikowi wszystkie informacje podane w powiadomieniu o zakłóceniu, które mogą być wykorzystane do wykrycia i usunięcia zakłócenia. Dostawca może przekierować część ruchu danych do i z wykorzystywanej usługi, w której występuje zakłócenie, o ile jest to konieczne do poinformowania użytkownika o zakłóceniu.

(2) Jeśli dostawca usług cyfrowych został powiadomiony przez Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) o szczególnych zagrożeniach dla bezpieczeństwa technologii informacyjnych wynikających z korzystania przez użytkownika z jednej z jego usług lub wpływających na to korzystanie, musi on niezwłocznie powiadomić o tym użytkownika, o ile jest znana jego tożsamość. Czyniąc to, dostawca musi w szczególności przekazać użytkownikowi wszystkie informacje zawarte w powiadomieniu Federalnego Urzędu ds. Bezpieczeństwa Informacji (BSI) zgodnie ze zdaniem 1, które umożliwiają identyfikację zagrożeń i zapobieganie im. Jeśli dostawca usług cyfrowych stwierdzi zagrożenie dla bezpieczeństwa technologii informacyjnych wynikające z korzystania przez użytkownika z jednej z jego usług lub wpływające na to korzystanie, może o tym poinformować użytkownika. W zakresie, w jakim jest to technicznie możliwe i uzasadnione ekonomicznie, dostawca może poinformować użytkownika o odpowiednich, skutecznych i dostępnych środkach technicznych, za pomocą których może on wykryć i usunąć te zagrożenia.”

---

[1] Art. 4 został notyfikowany zgodnie z dyrektywą (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

[…]

Uzasadnienie

B. Część specjalna

W odniesieniu do art. 4 (zmiany do ustawy o ochronie danych i prywatności w telekomunikacji i usługach cyfrowych)

W odniesieniu do pkt 1

Zgodnie z nowo wprowadzonymi ust. 5 i 6, dostawcy usług cyfrowych są zobowiązani do informowania swoich użytkowników o zakłóceniach (ust. 5) lub konkretnych zagrożeniach (ust. 6) wynikających z jednej z ich usług oraz do przekazywania użytkownikom informacji otrzymanych od Federalnego Urzędu ds. Bezpieczeństwa Informacji (BSI) dotyczących konkretnych zagrożeń mających wpływ na ich klientów, o ile informacje te są znane i możliwe jest ich przekazanie.

Obowiązki określone w ust. 5 i 6 zasadniczo odpowiadają już istniejącym obowiązkom dostawców usług telekomunikacyjnych określonym w sekcji 169 ust. 5 i 6 ustawy o telekomunikacji (TKG). Istniejące obowiązki dostawców usług telekomunikacyjnych określone w sekcji 169 ust. 5 i 6 ustawy o telekomunikacji (TKG) nie pozwalają w pełni przeciwdziałać tym zagrożeniom, ponieważ regularnie narażone są również systemy, których operatorzy nie podlegają przepisom TKG. Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) codziennie analizuje jednak liczne informacje dotyczące podatnych na ataki lub zainfekowanych systemów (dostawcy usług hostingowych, dostawcy usług w chmurze, dostawcy ośrodka przetwarzania danych, operatorzy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie bezpieczeństwa). Chociaż informacje te są obecnie przekazywane dostawcom usług, bardzo często sami dostawcy usług nie przekazują ich zainteresowanym użytkownikom z powodu braku takiego obowiązku prawnego. W związku z tym nie jest możliwe regularne i skuteczne przeciwdziałanie istniejącemu zagrożeniu.

Ust. 5 i 6 obejmują jedynie zakłócenia lub zagrożenia wynikające z usługi w kontekście korzystania z niej przez użytkownika. Chodzi tu o sytuacje, w których użytkownik korzysta na przykład z usług hostingowych w celu prowadzenia strony internetowej lub poczty elektronicznej, a strona internetowa lub poczta elektroniczna, za które jest odpowiedzialny, zostają zainfekowane i wykorzystywane do rozsyłania złośliwego oprogramowania lub wiadomości phishingowych. Dotyczy to zatem zakłóceń i zagrożeń, które mają wpływ na użytkownika podczas korzystania z usługi. Przykładami istotnych zakłóceń mogą być: zainfekowane konto e-mail wykorzystywane do wysyłania spamu, zainfekowany serwer wykorzystywany do ataków typu DDoS lub zainfekowana strona internetowa wykorzystywana do rozpowszechniania złośliwego oprogramowania.

Celem tego obowiązku jest zapobieganie szkodom powodowanym przez podatne na ataki lub już zainfekowane usługi. Tego rodzaju szkody mogą wystąpić zarówno u samego użytkownika, jak i u innych użytkowników internetu, jeżeli zostaną zaatakowani za pośrednictwem odnośnych usług (np. złośliwe oprogramowanie, phishing lub ataki typu DDoS). Ponadto na dostawcy usług cyfrowych spoczywa obowiązek powiadamiania tych użytkowników, których korzystanie z usług powoduje zakłócenia lub w przypadku których istnieje zagrożenie – o ile jest to znane – oraz przekazania tym użytkownikom wszelkich informacji przekazanych przez Federalny Urząd ds. Bezpieczeństwa Informacji (BSI).