

CYBERBEZPIECZEŃSTWO: REKOMENDACJE UKNF DOTYCZĄCE USŁUG SAAS



UKNF opublikował rekomendacje, które znajdują zastosowanie do wszystkich podmiotów rynku finansowego, w tym podmiotów objętych rozporządzeniem DORA, które dotyczą przeglądu bezpieczeństwa usług SaaS i zarządzania ryzykiem dostawców ICT. Co warto wiedzieć?

1

INWENTARYZACJA USŁUG SAAS

UKNF rekomenduje identyfikację wszystkich wykorzystywanych usług SaaS. Należy ustalić zakres przetwarzanych danych, procesy wspierane przez usługę oraz podział odpowiedzialności z dostawcą za zdarzenia związane z cyberbezpieczeństwem.

2

WERYFIKACJA BEZPIECZEŃSTWA DOSTAWCÓW

Zalecana jest ponowna ocena dostawców pod kątem stosowanych przez nich zabezpieczeń, na podstawie aktualnych informacji, audytów i testów. Sam certyfikat nie powinien być uznawany za wystarczające potwierdzenie bezpieczeństwa usługi.

3

KONTROLA DOSTĘPÓW I INTEGRACJI

Przegląd powinien objąć m.in. połączenia usługi z innymi systemami, konta administracyjne, tokeny i klucze API. UKNF zaleca ograniczenie uprawnień do niezbędnego zakresu oraz możliwość szybkiego odłączenia integracji.

4

DANE I PODWYKONAWCY

Należy zweryfikować, jacy podwykonawcy uczestniczą w świadczeniu usług, a także lokalizację i okres przechowywania przez nich danych związanych z usługą.

5

GOTOWOŚĆ NA INCYDENT

UKNF zaleca również sprawdzenie procedur reagowania, dostępności logów, możliwości odzyskania danych i uruchomienia rozwiązań zastępczych na wypadek incydentów związanych z bezpieczeństwem świadczenia usługi.

FinTech desk



Gabriela Kocurek

radca prawny, ekspert ds. FinTech

gabriela.kocurek@kwkr.pl

+48 690 302 211



Łukasz Wieczorek

radca prawny, partner

lukasz.wieczorek@kwkr.pl

+48 517 851 868