UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

KNF CSIRT

Departament Cyberbezpieczeństwa UKNF



Rekomendacje dla podmiotów rynku finansowego dotyczące przeglądu bezpieczeństwa usług SaaS i zarządzania ryzykiem dostawców ICT

Rekomendacje dla podmiotów rynku finansowego dotyczące przeglądu bezpieczeństwa usług SaaS i zarządzania ryzykiem dostawców ICT

Wstęp

W związku z obserwowanymi atakami na dostawców oprogramowania udostępnianego w modelu usługowym (Software as a Service, SaaS) oraz ujawnianymi incydentami naruszenia bezpieczeństwa przetwarzanych przez nich danych[1], Urząd Komisji Nadzoru Finansowego rekomenduje podmiotom rynku finansowego przeprowadzenie przeglądu wykorzystywanych usług SaaS oraz związanych z nimi mechanizmów zarządzania ryzykiem ICT.

Przegląd powinien służyć ustaleniu, czy zakres danych powierzanych dostawcom, przyznane uprawnienia oraz sposób integracji usług z systemami podmiotu są adekwatne do potrzeb biznesowych i aktualnego poziomu zagrożeń. Szczególną uwagę należy zwrócić na możliwość wykorzystania przejętej usługi, konta lub poświadczeń dostępowych do uzyskania dostępu do kolejnych zasobów, zmiany danych lub zakłócenia procesów biznesowych.

Korzystanie z usług SaaS wiąże bezpieczeństwo procesów podmiotu finansowego z zabezpieczeniami środowiska dostawcy oraz sposobem konfiguracji i użytkowania usługi. Zakłócenie lub naruszenie bezpieczeństwa takiego środowiska może oddziaływać jednocześnie na wielu odbiorców. Z tego względu przegląd powinien obejmować zarówno rozwiązania techniczne, jak i ustalenia umowne, podział odpowiedzialności oraz gotowość organizacji do samodzielnego ograniczenia skutków incydentu.

W przypadku podmiotów objętych rozporządzeniem DORA[2] działania te powinny stanowić element realizacji obowiązków dotyczących zarządzania ryzykiem związanym z ICT, w tym ryzykiem ze strony zewnętrznych dostawców usług ICT. Korzystanie z usług zewnętrznych nie zwalnia podmiotu finansowego z odpowiedzialności za realizację obowiązków wynikających z tego rozporządzenia. Należy przy tym podkreślić, że zgodnie z art. 8 ust. 2 zdanie pierwsze rozporządzenia DORA podmioty finansowe na bieżąco identyfikują wszystkie źródła ryzyka związanego z ICT, w szczególności ekspozycję na ryzyko w odniesieniu do innych podmiotów finansowych i pochodzące od tych podmiotów, oraz oceniają cyberzagrożenia i podatności w obszarze ICT mające znaczenie dla ich funkcji biznesowych wspieranych przez ICT, zasobów informacyjnych i zasobów ICT.

UKNF rekomenduje objęcie przeglądem następujących obszarów.

1. Identyfikacja usług i powierzanych danych

Należy zweryfikować kompletność informacji o wykorzystywanych usługach SaaS, w tym rozwiązaniach nabywanych bezpośrednio przez poszczególne jednostki biznesowe. Dla każdej usługi zaleca się określenie jej właściciela, wspieranych procesów, kategorii przetwarzanych danych oraz skutków naruszenia ich poufności, integralności lub dostępności. Ocena powinna obejmować również usługi pomocnicze, w szczególności rozwiązania księgowe, kadrowe, sprzedażowe i komunikacyjne.

---

[1] Oficjalne komunikaty dostawców dotyczące incydentów bezpieczeństwa:

- MyDr, „Incydent MyDr": https://pro.mydr.pl/portal-info

- Qbusoft/Medyc, „Informacja dotycząca naruszenia bezpieczeństwa danych", aktualizacja 28.09.2026: https://medyc.pl/komunikaty/

- Fakturownia, komunikat dotyczący incydentu z 29.09.2026: https://fakturownia.pl/incydent

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (DORA), Dz.U. UE L 333 z 27.12.2022, s. 1, ze zm.; w szczególności art. 4, art. 6–13 oraz art. 28–30. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/pol

Dla każdej usługi należy ustalić podział odpowiedzialności pomiędzy podmiotem finansowym a dostawcą, w szczególności w zakresie konfiguracji zabezpieczeń, zarządzania tożsamością, rejestrowania zdarzeń i odtwarzania danych. Wskazane jest powiązanie inwentaryzacji usług z ewidencją umów i oceną znaczenia wspieranych funkcji. Pozwoli to identyfikować zależności, które mogą pozostać niewidoczne przy odrębnej ocenie poszczególnych aplikacji.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 8 ust. 1, 4 oraz 5, art. 28 ust. 1 i 3, art. 30 ust. 2 lit. a, b, e oraz f tego rozporządzenia.

2. Weryfikacja bezpieczeństwa dostawców

Zaleca się ponowną ocenę dostawców na podstawie aktualnych i możliwych do zweryfikowania informacji o stosowanych zabezpieczeniach. W przypadku wykorzystywania certyfikatów i raportów z audytów należy sprawdzić ich autentyczność, aktualność, zakres oraz to, czy obejmują konkretną usługę i środowisko, w którym przetwarzane są dane podmiotu.

Posiadanie certyfikatu nie powinno być traktowane jako wystarczające potwierdzenie bezpieczeństwa usługi. Ocena powinna uwzględniać również skuteczność zabezpieczeń, wyniki testów oraz sposób usuwania stwierdzonych nieprawidłowości.

Przegląd powinien prowadzić do ustalenia, czy deklarowane zabezpieczenia odpowiadają faktycznemu sposobowi świadczenia usługi. Stwierdzone braki należy omówić z dostawcą i określić sposób ich usunięcia lub zastosowania środków ograniczających ryzyko. Istotne zmiany usługi, incydenty bezpieczeństwa oraz zmiany zakresu certyfikacji powinny stanowić przesłankę ponownej oceny dostawcy.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 28 ust. 6 czy art. 30 ust. 3 lit. e tego rozporządzenia. W odniesieniu do usług wspierających krytyczne lub istotne funkcje podmioty objęte rozporządzeniem DORA powinny uwzględnić wymagania dotyczące wykorzystywania certyfikacji i raportów z audytów określone w rozporządzeniu delegowanym 2024/1773[3].

3. Weryfikacja integracji połączeń i uprawnień

Należy ustalić, z jakimi systemami wewnętrznymi i zewnętrznymi łączą się wykorzystywane usługi, jakie dane są przekazywane oraz jakie operacje mogą być wykonywane za pośrednictwem tych połączeń.

Zaleca się przegląd kont technicznych, dostępów administracyjnych, uprawnień aplikacji oraz tokenów i kluczy API. Uprawnienia powinny być ograniczone do zakresu niezbędnego do realizacji określonego celu, a nieużywane konta i integracje – wyłączone. Należy zapewnić możliwość szybkiego odcięcia poszczególnych połączeń bez konieczności oczekiwania na działania dostawcy, o ile pozwala na to architektura rozwiązania.

Szczególną uwagę należy zwrócić na integracje umożliwiające masowy odczyt lub eksport danych, zmianę uprawnień oraz wykonywanie operacji w wielu systemach. Zaleca się weryfikowanie uprawnień także po zmianie stanowiska pracownika, zakończeniu współpracy lub zmianie celu integracji. Przyznawanie dostępu powinno podlegać zatwierdzeniu przez właściwego właściciela zasobu i pozostawiać ślad umożliwiający późniejszą kontrolę.

[3] Rozporządzenie delegowane Komisji (UE) 2024/1773 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych doprecyzowujących szczegółową treść polityki w zakresie ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT, Dz.U. UE L, 2024/1773, 25.6.2024; w szczególności art. 6 oraz art. 8 ust. 2–3. https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/pol

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 8 ust. 1, 2, 4 i 5, art. 9 ust. 3 oraz ust. 4 lit. c tego rozporządzenia czy przepisach rozporządzenia delegowanego 2024/1774[4], jak w szczególności jego art. 21. Dodatkowo, stosownie do treści art. 12 ust. 1 i 2 wspomnianego rozporządzenia delegowanego podmioty finansowe przy wprowadzaniu zabezpieczeń przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem opracowują, dokumentują i wdrażają procedury, protokoły i narzędzia rejestrowania, które obejmują m.in. wymóg rejestrowania logicznej i fizycznej kontroli dostępu, o której mowa w art. 21, oraz zarządzania tożsamością, a także środki mające na celu ochronę systemów rejestrowania i informacji o rejestrach przed manipulacją, usuwaniem i nieuprawnionym dostępem, gdy są one przechowywane, przesyłane oraz, w stosownych przypadkach, wykorzystywane.

4. Ochrona poświadczeń i certyfikatów technicznych

Przegląd powinien obejmować sposób przechowywania, wykorzystywania, wymiany i unieważniania haseł, tokenów, kluczy oraz certyfikatów służących do uwierzytelniania i zabezpieczania komunikacji. Należy zweryfikować prawidłowość walidacji certyfikatów, ochronę kluczy prywatnych oraz rozdzielenie poświadczeń pomiędzy poszczególnymi integracjami i środowiskami.

Zaleca się stosowanie uwierzytelniania wieloskładnikowego, w szczególności dla kont administracyjnych, oraz sprawdzenie możliwości unieważnienia aktywnych sesji i poświadczeń w przypadku podejrzenia ich przejęcia.

Należy określić właścicieli poświadczeń technicznych oraz zapewnić kontrolę nad terminami ważności i procesem ich wymiany. Poświadczenia nie powinny być przechowywane w ogólnodostępnej dokumentacji, repozytoriach kodu ani logach. Procedury awaryjnej wymiany kluczy i certyfikatów powinny uwzględniać zależności między systemami, tak aby ograniczenie zagrożenia nie powodowało niekontrolowanej utraty dostępności usług.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 9 oraz art. 30 ust. 2 lit. c tego rozporządzenia. Zastosowanie w omawianym zakresie powinny znaleźć także przepisy rozporządzenia delegowanego 2024/1774, jak w szczególności jego art. 7, 20 czy też 21.

5. Ocena podwykonawców i przepływów danych

Należy zweryfikować, jakie podmioty uczestniczą w świadczeniu usługi, gdzie przetwarzane są dane oraz kto może uzyskać do nich dostęp. Ocena powinna uwzględniać istotne zależności od podwykonawców, zmiany w łańcuchu dostaw oraz ryzyko koncentracji.

Analiza koncentracji powinna obejmować również wspólne zależności pozornie niezależnych usług, na przykład od tego samego dostawcy chmury lub mechanizmu uwierzytelniania. Należy ocenić, czy awaria takiego elementu nie ograniczy jednocześnie działania kilku procesów oraz dostępu do rozwiązań przewidzianych jako zastępcze.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 28 ust. 3, art. 29 ust. 2 oraz art. 30 ust. 2 lit a oraz b tego rozporządzenia. W odniesieniu do podwykonawstwa usług ICT wspierających funkcje krytyczne lub istotne zastosowanie mają również wymagania rozporządzenia

[4] Rozporządzenie delegowane Komisji (UE) 2024/1774 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202401774

delegowanego Komisji (UE) 2025/532[5], jak również art. 9 rozporządzenia delegowanego 2024/1773.

6. Ograniczenie zakresu i czasu przechowywania danych

Zaleca się ocenę, czy zakres danych przekazywanych dostawcom jest niezbędny do realizacji usługi oraz czy okresy ich przechowywania pozostają uzasadnione. Przegląd powinien obejmować także dane archiwalne, eksporty, kopie zapasowe i środowiska testowe, z uwzględnieniem obowiązujących wymogów retencji.

Należy zweryfikować zasady zwrotu i usunięcia danych po zakończeniu współpracy oraz możliwość uzyskania potwierdzenia realizacji tych czynności.

Ograniczenie ilości powierzanych danych powinno być uwzględniane już podczas wdrażania usługi i projektowania integracji. W miarę możliwości należy stosować dane testowe nieodwzorowujące rzeczywistych danych klientów oraz ograniczać tworzenie niekontrolowanych kopii i eksportów. Zasady retencji powinny obejmować także dane pozostające u podwykonawców.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 9 ust. 3 tego rozporządzenia, a także w art. 2 ust. 1 oraz 11 ust. 2 lit. g rozporządzenia 2024/1774.

7. Przygotowanie do incydentu i utrzymania ciągłości działania

Należy zweryfikować uzgodnienia dotyczące powiadamiania o incydentach, współpracy z dostawcą oraz udostępniania informacji i logów potrzebnych do oceny skutków zdarzenia. Procedury reagowania powinny uwzględniać odłączenie integracji, unieważnienie zagrożonych poświadczeń, weryfikację integralności danych oraz analizę operacji wykonanych z wykorzystaniem przejętych dostępów.

Zaleca się sprawdzenie możliwości odzyskania danych, uruchomienia rozwiązań zastępczych i zakończenia korzystania z usługi. Testy powinny uwzględniać zarówno niedostępność dostawcy, jak i sytuację, w której bezpieczeństwo jego środowiska zostało naruszone.

Weryfikacja powinna obejmować dostępność logów, ich zakres, okres przechowywania oraz możliwość zabezpieczenia dowodów niezależnie od dostawcy. Wskazane jest przeprowadzenie ćwiczenia obejmującego przejęcie konta administracyjnego lub naruszenie środowiska dostawcy. Wyniki ćwiczenia powinny potwierdzić zdolność do podjęcia decyzji, ograniczenia dostępu, odtworzenia usługi i skoordynowania komunikacji wewnętrznej oraz zewnętrznej.

W przypadku podmiotów objętych rozporządzeniem DORA działania te powinny stanowić realizację obowiązków, o których mowa m.in. w art. 11, art. 17, art. 24, art. 25, art. 28 ust. 8, art. 30 ust. 2 lit. f tego rozporządzenia, jak również w przepisach rozporządzenia delegowanego 2024/1774 (w szczególności rozdział IV tego rozporządzenia).

8. Współpraca z CSIRT KNF i wykorzystanie informacji o zagrożeniach

UKNF rekomenduje uwzględnianie informacji publikowanych przez CSIRT KNF w bieżącej ocenie bezpieczeństwa usług SaaS i ryzyka dostawców ICT. CSIRT KNF realizuje zadania zespołu sektorowego, wspierając podmioty finansowe w obsłudze poważnych incydentów związanych z ICT oraz analizując incydenty, trendy i zagrożenia w obszarze

[5] Rozporządzenie delegowane Komisji (UE) 2025/532 z dnia 24 marca 2025 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających elementy, które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo usług ICT wspierających krytyczne lub istotne funkcje, Dz.U. UE L, 2025/532, 2.7.2025. https://eur-lex.europa.eu/eli/reg_del/2025/532/oj/pol

cyberbezpieczeństwa[6]. Ostrzeżenia i materiały analityczne powinny być oceniane pod kątem ich znaczenia dla usług wykorzystywanych przez dany podmiot, powierzanych danych i istniejących integracji. Dodatkowo, do zadań KNF, zgodnie z art. 4 ust. 1 pkt 3b ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, należy również podejmowanie działań mających na celu przeciwdziałanie poważnym incydentom oraz zagrożeniom systemów teleinformatycznych w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, a także cyberzagrożeniom w rozumieniu art. 3 pkt 12 rozporządzenia 2022/2554 oraz incydentom związanym z ICT w rozumieniu art. 3 pkt 8 rozporządzenia 2022/2554 sieci i systemów informatycznych w rozumieniu art. 3 pkt 2 rozporządzenia 2022/2554 - wykorzystywanych przez podmioty podlegające nadzorowi KNF. Do działań takich należy zaś również publikowanie ostrzeżeń o nowych cyberzagrożeniach oraz powiązanych z nimi rekomendacji.

W analizie ryzyka oraz przygotowaniu scenariuszy testów warto wykorzystywać również publikację CSIRT KNF „Krajobraz cyberzagrożeń w polskim sektorze finansowym 2026”[7]. Informacja o zagrożeniu dotyczącym dostawcy lub stosowanej technologii powinna uruchamiać weryfikację ekspozycji podmiotu, ocenę potrzeby wprowadzenia dodatkowych zabezpieczeń oraz ustalenie, czy konieczny jest kontakt z dostawcą. Należy wskazać osoby odpowiedzialne za analizę takich informacji i przekazywanie wniosków właścicielom usług.

Współpraca z CSIRT KNF powinna obejmować przekazywanie użytecznych informacji o obserwowanych zagrożeniach i incydentach, z zachowaniem wymogów ochrony informacji oraz właściwych zasad raportowania. Wczesna wymiana ustaleń technicznych może wspierać identyfikację zdarzeń oddziałujących na więcej niż jeden podmiot rynku finansowego. Współpracę operacyjną należy skoordynować z realizacją obowiązków zgłoszeniowych mających zastosowanie do danego podmiotu.

Zakończenie

Przedstawione rekomendacje mają na celu ograniczenie ryzyka, że naruszenie bezpieczeństwa usługi SaaS lub jej dostawcy doprowadzi do utraty danych, nieuprawnionych operacji albo zakłócenia działalności podmiotu finansowego. Skuteczność działań powinna być oceniana na podstawie sprawdzalnych rezultatów, w szczególności aktualności inwentaryzacji, zakresu przyznanych uprawnień, wyników testów i możliwości odtworzenia usług.

Wyniki przeglądu powinny zostać udokumentowane i wykorzystane do aktualizacji oceny ryzyka oraz opracowania planu działań naprawczych. Plan powinien wskazywać priorytety, właścicieli działań, terminy realizacji i sposób potwierdzenia usunięcia nieprawidłowości. W pierwszej kolejności należy ograniczać ryzyka związane z szerokim dostępem do danych i systemów, brakiem możliwości szybkiego odłączenia integracji oraz niewystarczającą zdolnością przywrócenia procesów biznesowych.

Istotne ustalenia przeglądu powinny zostać przedstawione organowi zarządzającemu, aby umożliwić podjęcie decyzji o zasobach, priorytetach oraz sposobie postępowania z ryzykiem. Należy zapewnić monitorowanie realizacji planu i okresową ocenę skuteczności wdrożonych rozwiązań. Przegląd powinien być ponawiany po istotnych zmianach usług, wystąpieniu incydentu lub uzyskaniu informacji wskazujących na zmianę poziomu zagrożenia.

---

[6] Urząd Komisji Nadzoru Finansowego, informacje o zadaniach CSIRT KNF jako zespołu sektorowego, w tym wsparciu obsługi incydentów oraz analizie trendów i zagrożeń w obszarze cyberbezpieczeństwa. https://www.knf.gov.pl/dla_rynku/CSIRT_KNF

[7] CSIRT KNF, „Krajobraz cyberzagrożeń w polskim sektorze finansowym 2026”, materiał wspierający analizę ryzyka, planowanie działań ochronnych i przygotowanie scenariuszy reagowania. https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Krajobraz_cyberzagrozen_w_polskim_sektorze_finansowym

Odniesienia do DORA i aktów uzupełniających należy stosować z uwzględnieniem ich zakresu podmiotowego, właściwych wyłączeń oraz zasady proporcjonalności. Wymagania szczególne dotyczące usług ICT wspierających funkcje krytyczne lub istotne należy uwzględniać zgodnie z kwalifikacją danej usługi.

UKNF rekomenduje traktowanie bezpieczeństwa usług SaaS jako stałego elementu zarządzania ryzykiem ICT i odpornością operacyjną. Odpowiedzialność za ten obszar powinna łączyć działania jednostek biznesowych, bezpieczeństwa, IT, zakupów i funkcji kontrolnych. Takie podejście sprzyja utrzymaniu kontroli nad powierzanymi danymi i zależnościami od dostawców oraz przygotowaniu organizacji do sprawnego działania w sytuacji kryzysowej.