Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.130.2026
Warszawa, 17 listopada 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026-67a-10
dotycząca cyberbezpieczeństwa sektora bankowości i infrastruktury rynków finansowych

Podstawa i cel rekomendacji

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] i stanowi sektorowe uzupełnienie ogólnej rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026-67a-9 dotyczącej środków organizacyjnych i technicznych służących zwiększaniu poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa[2] (KSC).

Celem rekomendacji jest wskazanie środków organizacyjnych i technicznych służących zwiększeniu poziomu bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty sektora bankowości i infrastruktury rynków finansowych, z uwzględnieniem specyfiki tego sektora, w szczególności w zakresie zarządzania ryzykiem ICT, bezpieczeństwa łańcucha dostaw ICT, ochrony integralności danych finansowych, przeciwdziałania oszustwom oraz zapewniania odporności operacyjnej.

Rekomendacja nie zastępuje wymagań wynikających z przepisów prawa ani rekomendacji o charakterze ogólnym, lecz doprecyzowuje sposób ich stosowania z uwzględnieniem uwarunkowań sektora bankowości i infrastruktury rynków finansowych.

Streszczenie

Sektor bankowości i infrastruktury rynków finansowych wymaga środków bezpieczeństwa, które uwzględniają jednocześnie ochronę systemów ICT, integralność operacji finansowych, przeciwdziałanie oszustwom oraz utrzymanie dostępności usług. Incydent dotyczący jednego podmiotu lub wspólnego dostawcy może oddziaływać na innych uczestników rynku, klientów i infrastrukturę wykorzystywaną do rozliczeń.

Niniejszy dokument nie powtarza pełnego katalogu obowiązków wynikających z przepisów prawa, w szczególności ustawy o KSC i rozporządzenia DORA[3]. Wskazuje natomiast sposób przełożenia wymagań ogólnych na praktyczne obszary ochrony sektora.

Szczególne znaczenie ma zarządzanie ryzykiem ICT wynikającym z korzystania z dostawców i podwykonawców. Podmiot powinien znać cały łańcuch usług wspierających funkcje krytyczne lub istotne, rozumieć wspólne zależności i ryzyko koncentracji oraz zachować zdolność do nadzorowania usługi, reagowania na incydent i bezpiecznego

[1] Dz. U. z 2026 r. poz. 20, z późn. zm. (dalej jako: „ustawa o KSC").
[2] https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dot-srodkow-organizacyjnych-i-technicznych-zwiekszajacych-poziom-bezpieczenstwa-systemow-informacyjnych
[3] 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.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

zakończenia współpracy. Rejestr umów i dostawców powinien służyć bieżącemu zarządzaniu ryzykiem, a nie wyłącznie realizacji obowiązku ewidencyjnego.

Podmioty powinny stosować rekomendacje proporcjonalnie do charakteru, skali i złożoności działalności, znaczenia świadczonych usług oraz profilu ryzyka. W przypadku odstąpienia od środka adekwatnego do danego ryzyka podmiot powinien udokumentować przyczynę, zastosowane zabezpieczenia zastępcze i zaakceptowany poziom ryzyka rezydualnego.

1. Zakres podmiotowy i zasada proporcjonalności

Rekomendacja jest skierowana do podmiotów sektora bankowości i infrastruktury rynków finansowych w ramach KSC. Może być odpowiednio stosowana przez inne podmioty rynku finansowego, jeżeli charakter świadczonych usług, wykorzystywane rozwiązania ICT lub występujące zależności uzasadniają przyjęcie analogicznych środków.

Proporcjonalność nie oznacza możliwości pominięcia ryzyka bez przeprowadzenia oceny. Podmiot powinien najpierw ustalić znaczenie usługi, dane i aktywa objęte ochroną, prawdopodobne scenariusze incydentów oraz zależności od innych podmiotów. Dopiero na tej podstawie może dobrać zakres, poziom zaawansowania i harmonogram wdrożenia zabezpieczeń.

a) Podmiot powinien określić, które rekomendacje mają zastosowanie do jego działalności, i wskazać właścicieli odpowiedzialnych za ich wdrożenie oraz okresową ocenę skuteczności.

b) Decyzja o niewdrożeniu określonego środka powinna zawierać ocenę ryzyka, opis zabezpieczeń zastępczych, termin ponownego przeglądu i wskazanie osoby akceptującej ryzyko.

c) Mniejsze podmioty mogą stosować rozwiązania współdzielone lub usługi zarządzane, lecz powinny zachować zdolność do oceny dostawcy, otrzymywania informacji o incydentach i podejmowania decyzji dotyczących własnego ryzyka.

2. Profil zagrożeń sektora finansowego

W sektorze finansowym cyberatak może bezpośrednio prowadzić do nieautoryzowanej operacji, utraty środków, naruszenia tajemnicy prawnie chronionej albo zakłócenia dostępu do usług. Z tego względu ochrona poufności, integralności i dostępności systemów musi być powiązana z przeciwdziałaniem fraudowi, kontrolą procesów biznesowych i oceną wpływu incydentu na klientów oraz innych uczestników rynku.

Istotne są kampanie łączące kilka technik. Przejęte poświadczenia lub sesje mogą zostać użyte do fraudu, dostępu do SaaS, zmiany danych lub przygotowania ataku ransomware. DDoS może odciągać uwagę od włamania albo towarzyszyć działaniom reputacyjnym. Incydent dostawcy może jednocześnie dotknąć wiele instytucji korzystających z tej samej usługi, chmury lub mechanizmu uwierzytelniania.

Analiza ryzyka powinna zatem uwzględniać nie tylko pojedyncze techniki ataku, lecz także ich możliwe połączenia, wspólne zależności i skutek sektorowy. Szczególnej uwagi wymagają scenariusze dotyczące cyber-enabled fraud, kradzieży tożsamości i sesji, ransomware i data extortion, DDoS, łańcucha dostaw oraz wykorzystywania AI do automatyzacji działań ofensywnych.

3. Usługi i aktywa o szczególnym znaczeniu

Inwentaryzacja powinna łączyć perspektywę techniczną z biznesową. Sama lista urządzeń i aplikacji nie pozwala ustalić, które zależności decydują o dostępności usługi finansowej

ani jak naruszenie jednego elementu wpłynie na transakcje, klientów i pozostałych uczestników rynku.

Dla każdej funkcji krytycznej lub istotnej należy wskazać wspierające ją systemy, dane, dostawców, połączenia, poświadczenia techniczne i osoby odpowiedzialne. Mapa zależności powinna obejmować także elementy wspólne dla kilku usług, ponieważ ich awaria może unieruchomić jednocześnie proces podstawowy i rozwiązanie zastępcze.

a) Inwentaryzacja powinna obejmować systemy prowadzenia rachunków, księgi głównej, płatności, autoryzacji, rozliczeń i rozrachunku, a także systemy obrotu, depozytu i raportowania właściwe dla działalności podmiotu.

b) Podmiot powinien zidentyfikować kanały obsługi klientów, w tym bankowość internetową i mobilną, API, usługi kartowe, bankomaty oraz mechanizmy uwierzytelniania i autoryzacji operacji.

c) Mapa zależności powinna uwzględniać systemy antyfraudowe, systemy przeciwdziałania praniu pieniędzy, usługi DNS, pocztę, telekomunikację, usługi chmurowe, SaaS oraz zarządzane usługi bezpieczeństwa.

d) Dla usług krytycznych lub istotnych należy określić wymagany poziom dostępności, maksymalny czas przerwy, dopuszczalną utratę danych, kolejność odtwarzania oraz minimalny zakres działania w trybie awaryjnym.

e) Podmiot powinien wskazać zasoby kryptograficzne o wysokim znaczeniu, w szczególności klucze, certyfikaty, moduły HSM i mechanizmy podpisywania lub uwierzytelniania komunikacji.

4. Zarządzanie tożsamością sesjami i ryzykiem fraudu

Tożsamość cyfrowa jest wspólnym punktem dla bezpieczeństwa ICT i ryzyka fraudu. Przejęcie konta, tokenu, pliku cookie albo aktywnej sesji może umożliwić wykonanie operacji bez konieczności ponownego łamania uwierzytelnienia. Dlatego monitoring tożsamości powinien obejmować zdarzenia występujące po zalogowaniu, a nie tylko sam moment uwierzytelnienia.

Zespoły bezpieczeństwa i jednostki odpowiedzialne za przeciwdziałanie oszustwom powinny wymieniać informacje o anomaliach, przejętych poświadczeniach, podejrzanych urządzeniach i zmianach profilu zachowania. Pozwala to szybciej rozpoznać sytuacje, w których incydent techniczny prowadzi do nieautoryzowanej operacji finansowej.

a) Dla kont uprzywilejowanych, administracyjnych i zdalnego dostępu należy stosować uwierzytelnianie wieloskładnikowe odporne na phishing, jeżeli pozwala na to wykorzystywana technologia.

b) Podmiot powinien monitorować anomalie dotyczące sesji, tokenów, urządzeń i lokalizacji oraz zapewnić możliwość szybkiego unieważnienia aktywnych sesji i poświadczeń.

c) Zmiana rachunku docelowego, danych klienta, limitu, sposobu uwierzytelniania albo konfiguracji mechanizmu bezpieczeństwa powinna wymagać kontroli adekwatnej do ryzyka tej operacji.

d) Procesy o wysokim ryzyku powinny rozdzielać inicjowanie, zatwierdzanie i wykonanie operacji. Wyjątki od tej zasady wymagają udokumentowania i dodatkowego monitoringu.

e) Podmiot powinien posiadać procedurę weryfikacji dyspozycji przekazywanych kanałem głosowym lub wideo, w szczególności, gdy dotyczą płatności, zmiany danych lub udostępnienia informacji wrażliwych.

f) Dane z monitoringu bezpieczeństwa i systemów antyfraudowych powinny być korelowane w zakresie pozwalającym rozpoznać wspólny scenariusz ataku, z zachowaniem zasad ochrony danych i rozdziału odpowiedzialności.

5. Bezpieczeństwo DNS i domen internetowych

DNS jest elementem infrastruktury bezpieczeństwa, a nie wyłącznie usługą rozpoznawania nazw. Odpowiednio skonfigurowany protective DNS może blokować komunikację z domenami wykorzystywanymi do phishingu, dystrybucji złośliwego oprogramowania i komunikacji z infrastrukturą atakującego. Logi DNS dostarczają także danych istotnych dla wykrywania tunelowania, eksfiltracji i aktywności przejętych urządzeń.

W sektorze finansowym ochrona DNS powinna obejmować również integralność domen używanych w komunikacji z klientami. Przejęcie konta u rejestratora, niekontrolowana zmiana rekordu albo wygaśnięcie domeny może prowadzić do przekierowania klientów, utraty dostępności lub wykorzystania domeny w kampanii oszustw.

a) Podmiot powinien utrzymywać aktualny rejestr domen, subdomen, stref, serwerów autorytatywnych, rejestratorów oraz osób uprawnionych do dokonywania zmian.

b) Ruch DNS użytkowników i systemów powinien być kierowany przez centralnie zarządzane resolvery. Możliwość używania nieautoryzowanych usług DoH, DoT i DoQ należy ograniczyć lub objąć kontrolą adekwatną do ryzyka.

c) Należy wdrożyć filtrowanie ochronne DNS z wykorzystaniem wiarygodnych źródeł reputacyjnych, w tym list ostrzeżeń właściwych dla polskiej cyberprzestrzeni oraz zapewnić obsługę błędnych blokad.

d) Logi zapytań, odpowiedzi i blokad DNS powinny być przechowywane przez okres wynikający z analizy ryzyka i korelowane z danymi z DHCP, zapór sieciowych, systemów EDR i zarządzania tożsamością.

e) Serwery autorytatywne powinny być redundantne, odpowiednio odseparowane, monitorowane i chronione przed nieautoryzowanym transferem stref oraz zmianami konfiguracji.

f) DNSSEC należy stosować tam, gdzie analiza ryzyka wskazuje na potrzebę ochrony integralności danych DNS. Proces powinien obejmować bezpieczne zarządzanie kluczami, rotację oraz testowanie zmian.

g) Podmiot powinien monitorować rejestrację domen podobnych do własnych i posiadać proces ich oceny, zgłaszania oraz ograniczania skutków kampanii phishingowych.

6. Odporność na ataki DDoS

Ataki DDoS pozostają istotnym zagrożeniem dla publicznych usług finansowych. Ochrona nie może ograniczać się do zakupu usługi mitygacyjnej. Skuteczność zależy również od architektury dostępu do Internetu, przepustowości, konfiguracji aplikacji, współpracy z operatorami i zdolności do podejmowania decyzji poza godzinami pracy.

DDoS może być połączony z próbą włamania, fraudem albo operacją reputacyjną. Zespół reagujący powinien utrzymać monitoring innych zdarzeń bezpieczeństwa i nie zakładać, że przeciążenie usługi jest jedynym celem atakującego.

a) Analiza ryzyka DDoS powinna obejmować ataki wolumetryczne, protokołowe i aplikacyjne oraz wskazywać usługi, których niedostępność może wpłynąć na klientów lub innych uczestników rynku.

b) Podmiot powinien zapewnić ochronę warstwową, obejmującą co najmniej łącza, infrastrukturę sieciową i warstwę aplikacyjną. Dobór rozwiązania należy potwierdzić testami dostosowanymi do architektury usługi.

c) Z operatorami telekomunikacyjnymi i dostawcami ochrony należy uzgodnić całodobową ścieżkę eskalacji, warunki uruchomienia mitygacji, zakres przekazywanych informacji i sposób działania podczas awarii kanału podstawowego.

d) Testy powinny obejmować bankowość elektroniczną, API, mechanizmy uwierzytelniania oraz pozostałe usługi publiczne, których utrata wpływa na realizację funkcji krytycznych lub istotnych.

e) W trakcie ataku należy utrzymywać monitoring bezpieczeństwa na poziomie pozwalającym wykrywać równoległe próby włamania, eksfiltracji lub fraudu.

f) Plan komunikacji powinien uwzględniać przekaz do klientów, partnerów i mediów oraz działania na wypadek rozpowszechniania fałszywych informacji o skutkach ataku.

7. Ransomware i wymuszenia oparte na kradzieży danych

Współczesne kampanie ransomware obejmują kradzież danych, niszczenie kopii zapasowych, presję na klientów i partnerów oraz publikację przejętych informacji. Organizacja powinna przygotować się także na wariant, w którym atakujący nie szyfruje systemów, lecz wykorzystuje samą groźbę ujawnienia danych lub zakłócenia działalności.

Skuteczne przygotowanie wymaga połączenia prewencji, detekcji, ograniczania skutków i odtwarzania. Kopia zapasowa jest wartościowa dopiero wtedy, gdy organizacja potrafi odtworzyć z niej usługę w akceptowalnym czasie, zweryfikować integralność danych i bezpiecznie włączyć system do środowiska produkcyjnego.

a) Kopie zapasowe usług krytycznych powinny być odseparowane od środowiska produkcyjnego, odporne na nieautoryzowaną modyfikację i chronione niezależnymi mechanizmami dostępu.

b) Testy odtwarzania powinny potwierdzać zdolność przywrócenia całej usługi wraz z konfiguracją, zależnościami, kluczami i danymi, a nie jedynie poprawność odczytu pojedynczego pliku.

c) Sieć, środowiska administracyjne i systemy kopii zapasowych powinny być segmentowane w sposób ograniczający przemieszczanie się atakującego oraz wykorzystanie jednego konta do przejęcia wielu warstw infrastruktury.

d) Dostęp uprzywilejowany powinien wykorzystywać odrębne konta i zarządzane stacje administracyjne. Należy monitorować tworzenie nowych kont, zmianę uprawnień i próby wyłączenia zabezpieczeń.

e) Plan reagowania powinien opisywać identyfikację, ograniczanie, zabezpieczenie dowodów, komunikację, obowiązki raportowe, odtwarzanie oraz działania po incydencie. Kopia planu i lista kontaktów powinny być dostępne również poza zagrożonym środowiskiem.

f) Podmiot powinien ćwiczyć scenariusz łączący szyfrowanie, kradzież danych, niedostępność podstawowych kanałów komunikacji i presję informacyjną kierowaną do klientów lub mediów.

8. Zarządzanie ryzykiem ICT i łańcuchem dostaw

Usługi finansowe zależą od rozbudowanego łańcucha dostaw ICT. Bezpośredni dostawca może korzystać z chmury, centrum danych, operatora telekomunikacyjnego, platformy

tożsamości, bibliotek oprogramowania oraz kolejnych podwykonawców. Podmiot finansowy może nie mieć z nimi umowy, ale awaria lub kompromitacja jednego z tych elementów może przerwać świadczenie usługi albo naruszyć bezpieczeństwo danych.

DORA wymaga zarządzania ryzykiem zewnętrznych dostawców ICT w całym cyklu życia umowy. Rekomendacje sektorowe powinny przełożyć te wymagania na zdolność operacyjną: aktualną wiedzę o zależnościach, ocenę ryzyka przed zawarciem umowy i po każdej istotnej zmianie, ciągłe monitorowanie usługi, skuteczne prawa audytowe oraz wykonalne plany wyjścia. Odpowiedzialność za ryzyko pozostaje po stronie podmiotu finansowego również wtedy, gdy realizację usługi powierzono dostawcy wewnątrz grupy lub podmiotowi zewnętrznemu.

9. Zarządzanie

9.1. Rejestr informacji o dostawcach

Rejestr informacji wymagany przez DORA może być podstawowym źródłem danych o zależnościach ICT, jeżeli jest powiązany z mapą funkcji biznesowych, zarządzaniem ryzykiem, ciągłością działania i obsługą incydentów. Rejestr utrzymywany wyłącznie na potrzeby raportowania szybko traci aktualność i nie wspiera decyzji podczas incydentu.

a) Podmiot powinien utrzymywać jednoznaczne powiązanie pomiędzy funkcją biznesową, usługą ICT, umową, bezpośrednim dostawcą, istotnymi podwykonawcami, lokalizacją świadczenia usługi i przetwarzania danych oraz właścicielem biznesowym i technicznym.

b) Zakres rejestru powinien obejmować usługi nabywane centralnie, przez jednostki biznesowe, w ramach grupy oraz bezpośrednio w modelu SaaS. Proces zakupowy i finansowy powinien umożliwiać wykrywanie usług używanych poza uzgodnionym katalogiem.

c) Dane o łańcuchu usług ICT powinny być aktualizowane po zawarciu lub zmianie umowy, zmianie podwykonawcy, incydencie, zmianie lokalizacji danych albo istotnej zmianie architektury usługi.

d) Podmiot powinien prowadzić kontrole jakości danych obejmujące kompletność, spójność i aktualność rejestru. Właściciel usługi powinien okresowo potwierdzać zgodność wpisu ze stanem faktycznym.

e) Informacje z rejestru powinny być dostępne dla zespołów odpowiedzialnych za ryzyko ICT, bezpieczeństwo, ciągłość działania, zakupy, obsługę incydentów i audyt w zakresie niezbędnym do wykonywania ich zadań.

9.2. Ocena dostawcy przed zawarciem umowy

Ocena dostawcy powinna ustalić, czy posiada on zasoby i mechanizmy pozwalające świadczyć usługę w sposób bezpieczny i ciągły. Sam certyfikat nie daje takiej odpowiedzi, jeżeli nie obejmuje konkretnej usługi, lokalizacji i środowiska wykorzystywanego przez podmiot finansowy.

a) Przed zawarciem umowy podmiot powinien ocenić reputację, sytuację finansową, zasoby techniczne i kadrowe, model zarządzania ryzykiem, zabezpieczenia, zdolność reagowania na incydenty oraz ciągłość działania dostawcy.

b) Ocena powinna uwzględniać znaczenie wspieranej funkcji, rodzaj i zakres danych, poziom dostępu dostawcy, odwracalność integracji, lokalizację świadczenia usługi oraz ryzyka prawne i geopolityczne.

c) Certyfikaty, raporty z audytu i testów należy weryfikować pod kątem autentyczności, aktualności, zakresu, wyłączeń oraz stanu działań naprawczych. W przypadku funkcji krytycznej lub istotnej wskazane jest wykorzystanie więcej niż jednego źródła zapewnienia.

d) Podmiot powinien ocenić, czy posiada kompetencje i zasoby potrzebne do nadzorowania dostawcy. Brak własnej zdolności do interpretacji raportów, logów i informacji o incydentach stanowi odrębne ryzyko wymagające ograniczenia.

e) Istotna zmiana usługi, modelu świadczenia, własności dostawcy, podwykonawstwa, lokalizacji danych lub zakresu certyfikacji powinna uruchamiać ponowną ocenę ryzyka.

9.3. Podwykonawcy i pełny łańcuch usług ICT

Szczególnego nadzoru wymagają podwykonawcy, którzy faktycznie podtrzymują usługę wspierającą funkcję krytyczną lub istotną. Należą do nich podmioty, których zakłócenie może ograniczyć bezpieczeństwo lub ciągłość usługi, nawet jeżeli znajdują się dalej niż na pierwszym poziomie łańcucha.

a) Podmiot powinien identyfikować podwykonawców, którzy zapewniają istotną część usługi lub których awaria może naruszyć jej bezpieczeństwo albo ciągłość. Ocena nie powinna ograniczać się do pierwszego poziomu podwykonawstwa.

b) Umowa powinna określać, które elementy usługi mogą być podzlecane, wymagania wobec podwykonawców oraz odpowiedzialność bezpośredniego dostawcy za spełnienie wymagań w całym łańcuchu.

c) Dostawca powinien informować z odpowiednim wyprzedzeniem o planowanej istotnej zmianie podwykonawstwa. Podmiot finansowy powinien mieć czas i informacje potrzebne do oceny wpływu zmiany na ryzyko.

d) Jeżeli planowana zmiana przekracza tolerancję ryzyka, podmiot powinien móc zgłosić sprzeciw, zażądać modyfikacji albo skorzystać z prawa do zakończenia umowy na zasadach określonych w umowie i przepisach.

e) Prawa dostępu, audytu i inspekcji, wymagania dotyczące ciągłości, standardy bezpieczeństwa oraz obowiązki informacyjne powinny być przenoszone na podwykonawców w zakresie odpowiadającym znaczeniu świadczonej przez nich części usługi.

f) Ocena łańcucha powinna uwzględniać lokalizację podwykonawców i danych, zależność od podmiotów z państw trzecich oraz możliwe przeszkody w uzyskaniu informacji, przeprowadzeniu audytu lub odzyskaniu danych.

9.4. Ryzyko koncentracji i wspólnych zależności

Ryzyko koncentracji występuje również wtedy, gdy różne usługi mają odmiennych bezpośrednich dostawców, lecz korzystają z tej samej chmury, sieci dostarczania treści, platformy tożsamości, oprogramowania bazowego lub operatora telekomunikacyjnego. Analiza prowadzona oddzielnie dla każdej umowy może nie ujawnić takiej wspólnej zależności.

a) Podmiot powinien agregować zależności na poziomie organizacji i grupy, aby ustalić łączną ekspozycję na dostawcę, grupę kapitałową dostawcy, region, technologię oraz wspólnego podwykonawcę.

b) Analiza koncentracji powinna uwzględniać funkcje korzystające z danej usługi, skalę przetwarzanych danych, trudność migracji, dostępność alternatyw oraz czas potrzebny na ich uruchomienie.

c) Rozwiązanie określane jako zapasowe nie powinno być uznawane za niezależne, jeżeli korzysta z tego samego mechanizmu tożsamości, panelu zarządzania, łącza, regionu chmurowego lub innego wspólnego punktu awarii.

d) Dla koncentracji przekraczającej tolerancję ryzyka należy wdrożyć środki ograniczające, takie jak usunięcie wspólnego punktu awarii, niezależna kopia danych, możliwość pracy w trybie ograniczonym albo przygotowana usługa zastępcza.

e) Podmiot powinien monitorować zmiany własnościowe, kondycję finansową, istotne incydenty i zmiany modelu świadczenia usług przez dostawców, od których zależy wiele funkcji krytycznych lub istotnych.

9.5. Wymagania umowne monitoring i audyt

Umowa powinna umożliwiać podmiotowi wykonywanie obowiązków również w warunkach incydentu lub sporu z dostawcą. Ogólne postanowienie o zachowaniu bezpieczeństwa nie zastępuje określenia informacji, czasów reakcji, praw audytowych, zasad współpracy i odpowiedzialności za podwykonawców.

a) Umowa powinna jednoznacznie opisywać usługę, miejsca świadczenia i przetwarzania danych, poziomy usług, wymagania bezpieczeństwa, zasady ciągłości, zakres podwykonawstwa oraz podział odpowiedzialności.

b) Dostawca powinien przekazywać informacje o incydencie w czasie pozwalającym podmiotowi ocenić jego wpływ i wykonać obowiązki regulacyjne. Zakres powinien obejmować co najmniej dotknięte usługi i dane, chronologię, zastosowane mitygacje oraz dostępne wskaźniki kompromitacji.

c) Podmiot powinien posiadać prawo dostępu do informacji, logów, wyników testów i dokumentacji niezbędnych do oceny usługi oraz prawo audytu i inspekcji adekwatne do znaczenia wspieranej funkcji.

d) Ograniczenia audytu grupowego, certyfikacji lub raportów dostawcy powinny być oceniane pod kątem tego, czy zapewniają wystarczający poziom pewności. Stwierdzone luki wymagają dodatkowych dowodów albo środków ograniczających ryzyko.

e) Nieprawidłowości dostawcy powinny mieć właściciela, termin usunięcia i sposób potwierdzenia realizacji. Braki o wysokim ryzyku należy eskalować do poziomu uprawnionego do podjęcia decyzji o ograniczeniu lub zakończeniu usługi.

9.6. Ciągłość usługi i plany wyjścia

Plan wyjścia powinien opisywać możliwy do wykonania sposób utrzymania albo odtworzenia funkcji po zakończeniu współpracy. Powinien obejmować nie tylko planowane przejście do innego dostawcy, lecz także nagłą niedostępność, utratę zaufania do środowiska, upadłość dostawcy lub rozwiązanie umowy.

a) Dla każdej umowy wspierającej funkcję krytyczną lub istotną należy opracować plan wyjścia oparty na realistycznych scenariuszach, określający właścicieli, harmonogram, zasoby, zależności i kryteria uruchomienia.

b) Podmiot powinien zapewnić możliwość uzyskania danych, konfiguracji, logów i informacji niezbędnych do migracji w uzgodnionym formacie oraz zweryfikować czas potrzebny na ich pobranie i wykorzystanie.

c) Plan powinien uwzględniać unieważnienie poświadczeń, odłączenie integracji, zmianę DNS i certyfikatów, zachowanie dowodów, weryfikację integralności danych oraz usunięcie danych pozostających u dostawcy i podwykonawców.

d) Plany wyjścia powinny być okresowo przeglądane i testowane. Test może mieć formę technicznego odtworzenia danych, próby uruchomienia usługi zastępczej albo ćwiczenia decyzyjnego, ale powinien potwierdzać wykonalność kluczowych założeń.

e) Strategia wielodostawcowa powinna być oceniana pod kątem rzeczywistej niezależności rozwiązań. Samo zawarcie umowy z drugim dostawcą nie ogranicza ryzyka, jeżeli migracja nie została przygotowana albo oba rozwiązania mają wspólne zależności.

9.7. Bezpieczeństwo usług SaaS i integracji

W usługach SaaS część zabezpieczeń pozostaje po stronie klienta. Ryzyko może wynikać z nadmiernych uprawnień, trwałych tokenów, niekontrolowanych eksportów danych albo integracji pozwalającej przejętej usłudze wykonywać operacje w innych systemach. Ocena dostawcy musi więc być uzupełniona kontrolą własnej konfiguracji.

a) Podmiot powinien przeglądać konta techniczne, dostępy administracyjne, tokeny, klucze API, aplikacje połączone i uprawnienia nadane integracjom. Nieużywane dostępy i połączenia należy wyłączać.

b) Architektura powinna umożliwiać szybkie odcięcie zagrożonej integracji, unieważnienie poświadczeń i zatrzymanie masowego eksportu danych bez oczekiwania na działanie dostawcy, jeżeli jest to technicznie możliwe.

c) Zakres i czas przechowywania danych u dostawcy powinny odpowiadać celowi usługi i wymaganiom prawnym. Kontrola powinna obejmować kopie zapasowe, eksporty, środowiska testowe oraz dane przetwarzane przez podwykonawców.

d) Logi administracyjne i bezpieczeństwa powinny być dostępne w zakresie i przez okres umożliwiający wykrycie nadużycia, analizę skutków i zabezpieczenie dowodów niezależnie od dostępności konta administracyjnego u dostawcy.

e) Podmiot powinien ćwiczyć scenariusz przejęcia konta administracyjnego SaaS lub klucza integracji, obejmujący odcięcie dostępu, ustalenie wykonanych operacji, ocenę integralności danych i komunikację z dostawcą oraz CSIRT KNF.

10. Bezpieczeństwo aplikacji API i łańcucha dostaw oprogramowania

Aplikacje mobilne, interfejsy API i zautomatyzowane połączenia pomiędzy instytucjami są podstawowym elementem świadczenia usług finansowych. Błąd uwierzytelnienia, nadmierne uprawnienie albo przejęty sekret może umożliwić masowy odczyt danych lub wykonanie operacji w wielu systemach. Zabezpieczenia powinny obejmować cały cykl życia oprogramowania, od kodu i zależności po proces budowania i wdrażania.

Łańcuch dostaw oprogramowania obejmuje również biblioteki open source, narzędzia budowania, repozytoria pakietów, mechanizmy aktualizacji i komponenty dostarczane wraz z usługą. Podmiot powinien być w stanie ustalić, gdzie używany jest podatny albo skompromitowany komponent, oraz zablokować wdrożenie artefaktu o niepotwierdzonym pochodzeniu.

a) Publiczne i partnerskie API powinny być objęte inwentaryzacją, klasyfikacją krytyczności, testami bezpieczeństwa i monitoringiem nadużyć. Dokumentacja powinna wskazywać właściciela, odbiorców danych i operacje dostępne przez interfejs.

b) API powinny stosować silne uwierzytelnianie usług, walidację danych wejściowych, ograniczenia szybkości zapytań oraz kontrolę zakresu uprawnień. Mechanizmy te należy testować także dla błędnych i nietypowych sekwencji operacji.

c) Podmiot powinien utrzymywać informacje o komponentach i zależnościach oprogramowania istotnych dla usług krytycznych. Informacje te powinny pozwalać szybko ustalić ekspozycję po ujawnieniu podatności.

d) Repozytoria kodu, systemy CI/CD, klucze podpisujące, konta dostawców i artefakty wdrożeniowe powinny być chronione przed nieautoryzowaną zmianą. Wdrożenie powinno umożliwiać weryfikację pochodzenia i integralności artefaktu.

e) Proces zarządzania podatnościami powinien uwzględniać ekspozycję usługi, możliwość wykorzystania podatności, dostępność środków ograniczających i wpływ aktualizacji na ciągłość działania.

f) Bezpieczeństwo aplikacji mobilnych powinno uwzględniać przejęte urządzenia, złośliwe nakładki, nadużycie usług dostępności, manipulację aplikacją, kradzież sesji oraz scenariusze wykorzystujące komunikację NFC.

g) Dla oprogramowania wspierającego funkcje krytyczne lub istotne należy uzgodnić z dostawcą zasady informowania o podatnościach, incydentach w procesie wytwarzania, zakończeniu wsparcia oraz komponentach wymagających pilnej aktualizacji.

h) Podmiot powinien ograniczać korzystanie z niezaufanych repozytoriów i pakietów oraz stosować mechanizmy weryfikacji podpisu, sum kontrolnych i pochodzenia komponentów przed dopuszczeniem ich do procesu budowania.

i) Informacja o składzie oprogramowania, jeżeli jest dostępna lub wymagana w procesie zakupowym, powinna być utrzymywana w formie pozwalającej powiązać komponent z konkretną wersją usługi i szybko ocenić wpływ nowej podatności.

j) Incydent dotyczący dostawcy kodu, narzędzia CI/CD, repozytorium pakietów lub mechanizmu aktualizacji powinien uruchamiać ocenę integralności wcześniej pobranych i wdrożonych artefaktów.

11. Kryptografia i integralność danych finansowych

Integralność danych finansowych ma znaczenie niezależne od dostępności systemu. Po incydencie podmiot musi być w stanie ustalić czy zmieniono dane klienta, parametry transakcji, salda, konfigurację rozliczeń albo historię operacji. Ochrona kryptograficzna powinna obejmować zarówno dane i komunikację, jak i proces zarządzania kluczami.

a) Podmiot powinien prowadzić rejestr kluczy, certyfikatów, algorytmów i systemów korzystających z kryptografii, ze wskazaniem właściciela, przeznaczenia, terminu ważności oraz sposobu przechowywania.

b) Generowanie, aktywowanie, używanie, rotacja i niszczenie kluczy powinny podlegać rozdzieleniu obowiązków i rejestrowaniu. Dla kluczy wysokiego ryzyka należy stosować rozwiązania sprzętowe lub równoważne środki ochrony wynikające z analizy ryzyka.

c) Podmiot powinien monitorować nieautoryzowane zmiany danych transakcyjnych, parametrów rozliczeń, konfiguracji systemów i uprawnień umożliwiających modyfikację tych danych.

d) Procedury odtwarzania powinny zawierać sposób potwierdzenia spójności i integralności danych przed wznowieniem realizacji operacji finansowych.

e) Należy prowadzić analizę wpływu zmian w standardach kryptograficznych i przygotować plan wymiany algorytmów oraz komponentów, których bezpieczeństwo lub wsparcie może przestać być wystarczające.

12. Wpływ modeli Frontier AI na zagrożenia

Rozwój zaawansowanych modeli AI nie zmienia podstawowych celów atakujących, ale może zwiększać skalę i tempo ich działań. Dotyczy to przygotowywania treści socjotechnicznych, rekonesansu, analizy kodu, wyszukiwania podatności oraz dostosowywania prób ataku do konkretnej organizacji. Może również skrócić czas pomiędzy ujawnieniem podatności a pojawieniem się prób jej wykorzystania.

Przygotowanie sektora powinno koncentrować się na zdolności do szybkiego ustalania ekspozycji, podejmowania kontrolowanych działań naprawczych i weryfikowania informacji otrzymywanych kanałami podatnymi na manipulację. Odrębnym zagadnieniem jest bezpieczne używanie narzędzi generatywnych przez pracowników i dostawców.

a) Scenariusze ryzyka i testy odporności powinny uwzględniać wykorzystanie AI do phishingu, vishingu, deepfake, automatyzacji rekonesansu i przyspieszenia prób wykorzystania podatności.

b) Podmiot powinien posiadać aktualne dane pozwalające ustalić, czy nowo ujawniona podatność dotyczy jego aktywów, usług zewnętrznych lub komponentów oprogramowania, oraz określić osoby uprawnione do podjęcia decyzji o mitygacji.

c) Procedury obsługi pilnych podatności powinny umożliwiać zastosowanie środków tymczasowych, kontrolowane wdrożenie poprawki, test działania usługi i zwiększony monitoring po zmianie.

d) Pracownicy powinni znać zasady korzystania z narzędzi generatywnej AI. Do usług niezatwierdzonych nie należy przekazywać danych klientów, tajemnic prawnie chronionych, kodu, poświadczeń ani szczegółów architektury bezpieczeństwa.

e) Wynik modelu AI nie powinien stanowić jedynej podstawy krytycznej decyzji dotyczącej bezpieczeństwa, fraudu, blokady klienta lub realizacji transakcji. Organizacja powinna określić wymagany udział człowieka i zasady weryfikacji wyniku.

13. Ciągłość działania i odporność sektorowa

Plany ciągłości powinny odpowiadać rzeczywistym zależnościom usług. Test ograniczony do awarii pojedynczego systemu może nie ujawnić, że rozwiązanie zastępcze korzysta z tego samego dostawcy tożsamości, sieci, chmury lub centrum operacyjnego co środowisko podstawowe.

W sektorze finansowym należy uwzględnić także efekt równoczesnego zakłócenia kilku podmiotów lub usług wspólnych. Test powinien sprawdzać zdolność do ustalenia priorytetów, wymiany informacji, ograniczenia ryzyka dla klientów i bezpiecznego wznowienia operacji.

a) Testy powinny obejmować niedostępność operatora telekomunikacyjnego, dostawcy chmury lub SaaS, usług DNS, systemu tożsamości oraz podstawowego kanału komunikacji.

b) Podmiot powinien określić minimalny zakres usług utrzymywanych lub odtwarzanych w pierwszej kolejności oraz warunki bezpiecznego działania w trybie ograniczonym.

c) Ćwiczenia powinny angażować kierownictwo, zespoły techniczne, bezpieczeństwo, jednostki odpowiedzialne za fraud i zgodność, obsługę klientów, komunikację oraz właścicieli usług biznesowych.

d) Scenariusze powinny obejmować jednoczesną utratę dostępności, wątpliwości co do integralności danych i presję informacyjną. Test powinien sprawdzić sposób podejmowania decyzji przy niepełnych informacjach.

e) Wnioski z testów i rzeczywistych incydentów powinny prowadzić do zmian w architekturze, procedurach, umowach lub monitoringu. Działania naprawcze należy rejestrować, przypisywać właścicielom i weryfikować po wdrożeniu.

14. Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług bankowych

Podczas działań bieżących oraz w odniesieniu do działań planowanych, w szczególności w obszarze usług wykorzystujących elektroniczne kanały dostępu, dostawcy usług bankowych powinni konsekwentnie stosować paradygmat określany jako „security first", determinujący prowadzenie pogłębionych analiz ryzyka, uwzględniających nie tylko kwestie bezpieczeństwa środowiska teleinformatycznego dostawcy bezpośredniego czy dostawców outsourcingowych, ale również ryzyk związanych z korzystaniem z usług finansowych przez klientów. Dlatego też uwzględniając stosowanie zasady „security first", zasadnym są wdrożenia w systemie transakcyjnym funkcjonalności dającej klientowi możliwość ustawienia potwierdzenia silnym uwierzytelnieniem każdej płatności.

Dostawcy usług bankowych powinni mieć świadomość, że podejmowane przez nich indywidualne inicjatywy, które w ich ocenie nie wpływają negatywnie na poziom ryzyka w obszarze prowadzonej działalności biznesowej, w tym także na bezpieczeństwo środków finansowych klientów, w kontekście całego rynku finansowego i w konsekwencji wszystkich klientów tego rynku, mogą już takie ryzyko generować i stanowić czynnik ryzyka systemowego w obszarze cyberbezpieczeństwa.

15. Współpraca z CSIRT KNF i wymiana informacji

Szybka wymiana informacji ogranicza czas potrzebny na rozpoznanie wspólnego zagrożenia i pozwala ostrzec inne podmioty korzystające z tej samej technologii lub usługi. Informacja przekazywana do sektorowego zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT KNF powinna umożliwiać ocenę techniczną zdarzenia oraz jego potencjalnego wpływu na sektor.

a) Podmiot powinien utrzymywać całodobową zdolność do odbierania ostrzeżeń CSIRT KNF oraz przekazywania ich do jednostek odpowiedzialnych za ocenę i wdrożenie działań ochronnych.

b) Kontakty operacyjne i decyzyjne powinny być aktualizowane po zmianach organizacyjnych i okresowo testowane. Należy zapewnić kanał zastępczy na wypadek niedostępności podstawowej poczty lub systemu zgłoszeniowego.

c) Podmiot powinien mieć proces oceny wskaźników kompromitacji i zaleceń otrzymanych z zewnątrz, ich bezpiecznego wdrażania oraz weryfikowania skuteczności zastosowanych reguł.

d) Informacja o incydencie powinna, w zakresie możliwym i zgodnym z obowiązującymi zasadami, zawierać chronologię, dotknięte usługi, zależności od dostawców, wskaźniki kompromitacji, zastosowane mitygacje i ocenę wpływu na klientów oraz inne podmioty.

e) Wymiana informacji powinna uwzględniać właściwą klasyfikację, ograniczenie dystrybucji oraz ochronę danych prawnie chronionych. Zasady te nie powinny jednak prowadzić do nieuzasadnionego opóźnienia ostrzeżenia o zagrożeniu sektorowym.

16. Weryfikacja wdrożenia

Ocena wdrożenia powinna opierać się na dokumentacji i wynikach działania zabezpieczeń. Samo istnienie polityki lub procedury nie potwierdza, że podmiot potrafi zareagować na incydent, odtworzyć usługę albo ograniczyć zagrożenie wynikające z przejętej integracji.

Obszar	Przykładowe dowody wdrożenia
Usługi i zależności	Mapa usług krytycznych i istotnych, przypisani właściciele, dostawcy, dane, połączenia oraz parametry odtwarzania
Tożsamość i fraud	Wyniki przeglądu kont uprzywilejowanych, konfiguracja MFA, rejestry sesji, test procedur unieważniania dostępów i zasady korelacji zdarzeń
DNS i domeny	Rejestr domen i stref, konfiguracja resolverów, źródła filtrowania, wyniki monitoringu oraz test ciągłości DNS
DDoS	Analiza ryzyka, architektura ochrony, uzgodnienia z operatorami, wyniki testów i wnioski z ćwiczeń
Ransomware	Wyniki odtwarzania usług, konfiguracja ochrony kopii, plan reagowania i wyniki ćwiczenia scenariuszowego
Ryzyko dostawców ICT	Rejestr informacji powiązany z funkcjami, oceny dostawców, właściciele ryzyka, wyniki monitoringu oraz potwierdzenie realizacji działań naprawczych
Łańcuch podwykonawców	Lista podwykonawców podtrzymujących usługi krytyczne lub istotne, warunki podwykonawstwa, lokalizacje, wyniki ocen zmian oraz prawa audytowe
Koncentracja i wyjście	Analiza wspólnych zależności, scenariusze utraty dostawcy, niezależność rozwiązań zastępczych oraz wyniki testów migracji i odzyskania danych
SaaS i integracje	Mapa kont technicznych, tokenów i połączeń, konfiguracja logowania, test odcięcia integracji oraz wyniki ćwiczenia przejęcia konta administracyjnego
Podatności i oprogramowanie	Informacje o komponentach, terminy obsługi podatności, wyniki testów aplikacji, pochodzenie artefaktów i zabezpieczenia procesu wdrażania
Ciągłość działania	Scenariusze testów, protokoły z ćwiczeń, decyzje podjęte podczas testu i potwierdzone działania naprawcze

17. Priorytety wdrożeniowe

Podmiot powinien rozpocząć od działań, które ograniczają ryzyko utraty środków, integralności danych i dostępności usług krytycznych. Kolejność powinna wynikać z analizy ryzyka. W pierwszej grupie działań powinny znaleźć się kompletna mapa łańcucha usług ICT, ocena koncentracji i wykonalności planów wyjścia, zabezpieczenie dostępu uprzywilejowanego oraz potwierdzona zdolność odtworzenia usług.

a) Uzupełnić rejestr usług, danych, dostawców, podwykonawców, domen, API i zależności technologicznych oraz powiązać go z funkcjami krytycznymi lub istotnymi.

b) Zidentyfikować wspólne zależności i koncentracje, których nie widać przy odrębnej analizie pojedynczych umów, oraz ocenić niezależność rozwiązań zastępczych.

c) Zweryfikować umowy wspierające funkcje krytyczne lub istotne pod kątem informacji o podwykonawcach, terminów powiadamiania o incydentach, praw audytowych, dostępu do danych i możliwości zakończenia współpracy.

d) Przetestować plan wyjścia dla co najmniej jednej usługi o wysokiej krytyczności, w tym pobranie danych, odcięcie integracji, zmianę poświadczeń i uruchomienie trybu zastępczego.

e) Usunąć braki umożliwiające przejęcie dostępu uprzywilejowanego, trwałych tokenów, kluczy API lub systemów kopii zapasowych.

f) Potwierdzić w praktyce zdolność odtworzenia usług i działania w przypadku niedostępności podstawowego dostawcy, kanału komunikacji lub mechanizmu tożsamości.

g) Przetestować ochronę usług publicznych przed DDoS oraz odporność DNS i procesów zarządzania domenami.

h) Przeprowadzić ćwiczenie obejmujące incydent u dostawcy, kradzież poświadczeń, ryzyko fraudu i konieczność skoordynowanej komunikacji z CSIRT KNF.

i) Przyjąć plan usunięcia pozostałych braków wraz z terminami, właścicielami, sposobem weryfikacji i zasadami raportowania do kierownictwa.

Dokumenty stanowiące punkt odniesienia

Rekomendacje sektorowe wykorzystują wnioski z materiałów opublikowanych wcześniej przez CSIRT KNF. Dokumenty te zachowują własny zakres i powinny być stosowane łącznie z niniejszą rekomendacją tam, gdzie odpowiadają profilowi działalności i ryzyka podmiotu.

Publikacja	Znaczenie dla rekomendacji sektorowej
Rekomendacja ogólna nr 2026-67a-9	Minimalny katalog środków organizacyjnych i technicznych dla podmiotów KSC
Bezpieczne wdrożenie systemu DNS w organizacji	Protective DNS, integralność domen, logowanie i odporność infrastruktury DNS
Dobre praktyki w zakresie przeciwdziałania atakom DDoS	Dobór architektury, usług mitygacji i procedur reagowania na DDoS

Publikacja	Znaczenie dla rekomendacji sektorowej
Dobre praktyki w zakresie zapobiegania i reagowania na ataki typu ransomware	Przygotowanie, ograniczanie skutków, odtwarzanie i działania po incydencie
Rekomendacje dotyczące bezpieczeństwa usług SaaS i ryzyka dostawców ICT	Inwentaryzacja usług, integracje, poświadczenia, podwykonawcy i ciągłość działania
Rekomendacje dotyczące wpływu modeli Frontier AI na cyberbezpieczeństwo	Zmiana intensywności zagrożeń, zarządzanie podatnościami i odporność operacyjna
Krajobraz cyberzagrożeń w polskim sektorze finansowym 2026	Scenariusze ryzyka dotyczące fraudu, tożsamości, łańcucha dostaw, DDoS i AI
Rozporządzenie DORA	Zarządzanie ryzykiem ICT, incydenty, testowanie odporności oraz ryzyko zewnętrznych dostawców ICT
Standard DORA dotyczący polityki umów ICT	Cykl życia umowy, należyta staranność, monitoring, audyt oraz plany wyjścia
Standard DORA dotyczący podwykonawstwa ICT	Ocena podwykonawców wspierających funkcje krytyczne lub istotne oraz kontrola zmian w łańcuchu
Standard DORA dotyczący rejestru informacji	Struktura danych o umowach, dostawcach, funkcjach i łańcuchach usług ICT

Rekomendacja powstała w ramach współpracy Ministerstwa Cyfryzacji i Urzędu Komisji Nadzoru Finansowego, w tym CSIRT KNF.

Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa