REKOMENDACJA ARCHIWALNA

Komisja Nadzoru Finansowego

Rekomendacja D

dotycząca zarządzania obszarami technologii informacyjnej
i bezpieczeństwa środowiska teleinformatycznego w bankach

Warszawa, styczeń 2013 r.

Spis treści

I. Wstęp ... **4**

II. Słownik pojęć ... **6**

III. Lista rekomendacji ... **8**

IV. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego ... **12**

Rola zarządu i rady nadzorczej ... 12

System informacji zarządczej ... 13

Planowanie strategiczne ... 13

Zasady współpracy obszarów biznesowych i technicznych ... 14

Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego ... 16

Struktura organizacyjna ... 16

Podział obowiązków ... 16

Zasoby ludzkie ... 17

V. Rozwój środowiska teleinformatycznego ... **19**

Projekty w zakresie środowiska teleinformatycznego ... 19

Rozwój systemów informatycznych ... 20

VI. Utrzymanie i eksploatacja środowiska teleinformatycznego ... **25**

Zarządzanie danymi ... 25

Zarządzanie architekturą danych ... 25

Zarządzanie jakością danych ... 25

Zarządzanie infrastrukturą teleinformatyczną ... 28

Architektura infrastruktury teleinformatycznej ... 28

Komponenty infrastruktury teleinformatycznej ... 30

Aktualizacja oprogramowania komponentów infrastruktury teleinformatycznej ... 32

Zarządzanie pojemnością i wydajnością komponentów infrastruktury teleinformatycznej ... 33

Dokumentacja infrastruktury teleinformatycznej ... 35

Współpraca z zewnętrznymi dostawcami usług ... 35

Kontrola dostępu ... 39

Mechanizmy kontroli dostępu logicznego ... 39

Mechanizmy kontroli dostępu fizycznego ... 41

Ochrona przed szkodliwym oprogramowaniem ... 41

Wsparcie dla użytkowników ... 42

Edukacja pracowników ... 43

Ciągłość działania środowiska teleinformatycznego ... 43

Plany utrzymania ciągłości działania i plany awaryjne ... 43

Zasoby techniczne oraz warunki fizyczne i środowiskowe ... 44

Kopie awaryjne 47
Weryfikacja efektywności podejścia do zarządzania ciągłością działania 48
Zarządzanie elektronicznymi kanałami dostępu 48
Weryfikacja tożsamości klientów 48
Bezpieczeństwo danych i środków klientów 49
Edukacja klientów 50
Zarządzanie oprogramowaniem użytkownika końcowego 51
VII. Zarządzanie bezpieczeństwem środowiska teleinformatycznego 52
System zarządzania bezpieczeństwem środowiska teleinformatycznego 52
Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 52
Szacowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 53
Kontrola i przeciwdziałanie ryzyku w zakresie bezpieczeństwa środowiska teleinformatycznego 54
Monitorowanie i raportowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 55
Klasyfikacja informacji i systemów informatycznych 55
Klasyfikacja informacji 55
Klasyfikacja systemów informatycznych 57
Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego 57
Bezpieczeństwo formalno-prawne 59
Rola audytu wewnętrznego i zewnętrznego 60

I. Wstęp

Niniejsza Rekomendacja jest wydana na podstawie art. 137 pkt 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376 j.t. z późn. zm.). Zastępuje ona „Rekomendację D dotyczącą zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki" opracowaną i wydaną w 2002 r. Konieczność dokonania aktualizacji Rekomendacji wynika ze znacznego rozwoju technologicznego oraz systematycznego wzrostu znaczenia obszaru technologii informacyjnej dla działalności banków, jak również z pojawienia się nowych zagrożeń w tym zakresie. Aktualizacja ta uwzględnia także wnioski z działalności nadzorczej prowadzonej przez Urząd Komisji Nadzoru Finansowego.

Niniejsza Rekomendacja ma na celu wskazanie bankom oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami. Ryzyko to można określić jako niepewność związaną z prawidłowym, efektywnym i bezpiecznym wspieraniem działalności banku przez jego środowisko teleinformatyczne. Wiąże się ono przede wszystkim z ryzykiem operacyjnym (dlatego też niniejsza Rekomendacja powinna być traktowana jako uzupełnienie „Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach" w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego), ale również m.in. z ryzykiem utraty reputacji i ryzykiem strategicznym. Niniejszą Rekomendację stosuje się również odpowiednio wobec oddziałów instytucji kredytowych.

Dokument zawiera 22 rekomendacje, które podzielone zostały na następujące obszary:

- strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
- rozwój środowiska teleinformatycznego,
- utrzymanie i eksploatacja środowiska teleinformatycznego,
- zarządzanie bezpieczeństwem środowiska teleinformatycznego.

Wszystkie banki powinny stosować się do zawartych w niniejszym dokumencie rekomendacji. Biorąc jednak pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego oraz różnice w zakresie uwarunkowań, skali działalności oraz profili ryzyka banków, sposób realizacji tych rekomendacji i wskazanych w nich celów może być odmienny. W związku z tym, opisy i komentarze zawarte wraz z poszczególnymi rekomendacjami należy traktować jako zbiór dobrych praktyk, które jednak powinny być stosowane z zachowaniem zasady proporcjonalności. Oznacza to, że stosowanie tych praktyk powinno zależeć m.in. od tego, na ile przystają one do specyfiki i profilu ryzyka banku, szczególnych uwarunkowań prawnych, w jakich bank się znajduje oraz charakterystyki jego środowiska teleinformatycznego, jak również od stosunku kosztów ich wprowadzenia do wynikających z tego korzyści (także z perspektywy bezpieczeństwa klientów banku). Jednocześnie nadzór oczekuje, że decyzje dotyczące

zakresu i sposobu wprowadzenia wskazanych w Rekomendacji rozwiązań poprzedzone zostaną pogłębioną analizą i poparte będą stosowną argumentacją.

Ponadto, w przypadku banków spółdzielczych oczekiwaniem nadzoru jest, by banki zrzeszające wspierały proces wdrażania niniejszej Rekomendacji z uwzględnieniem skali i specyfiki działalności danego banku spółdzielczego, stosując zasadę proporcjonalności. Skala działalności i wykorzystywane technologie informatyczne powinny decydować o zakresie i stopniu przyjmowanych rozwiązań. Proces wdrażania tych rozwiązań w bankach spółdzielczych, pomimo aktywnej roli banku zrzeszającego, nie może jednak stać w sprzeczności ze zdefiniowanym w poszczególnych rekomendacjach zakresem obowiązków i odpowiedzialnością statutowych organów zrzeszonych banków spółdzielczych.

Komisja Nadzoru Finansowego oczekuje, że Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, stanowiąca załącznik do uchwały Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. (Dz. Urz. KNF z 2013 r. poz. 5), zostanie wprowadzona nie później niż do dnia 31 grudnia 2014 r.

II. Słownik pojęć

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (na podstawie ISO/IEC 27000:2009).

Cloud Computing („przetwarzanie w chmurze") – model świadczenia usług zapewniający niezależny od lokalizacji, dogodny dostęp sieciowy „na żądanie" do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług (na podstawie NIST Special Publication 800-145 „The NIST Definition of Cloud Computing", National Institute of Standards and Technology).

Dostępność danych – właściwość danych polegająca na tym, że są one dostępne i mogą być wykorzystywane na żądanie uprawnionej jednostki (na podstawie ISO/IEC 27000:2009).

Incydent naruszenia bezpieczeństwa środowiska teleinformatycznego – pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa środowiska teleinformatycznego (tj. wystąpienie stanu komponentu środowiska teleinformatycznego wskazującego na potencjalne naruszenie jego bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa) lub seria takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji (na podstawie ISO/IEC 27000:2009).

Infrastruktura teleinformatyczna – zespół urządzeń i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych banku.

Integralność danych – właściwość danych stanowiąca o ich dokładności i kompletności (na podstawie ISO/IEC 27000:2009).

Kierownictwo banku – zarząd banku oraz dyrektorzy, kierownicy komórek organizacyjnych i kierownicy ds. kluczowych procesów w banku.

Obszar bezpieczeństwa środowiska teleinformatycznego – obszar działalności banku mający na celu zapewnienie, że ryzyko dotyczące bezpieczeństwa środowiska teleinformatycznego banku jest odpowiednio zarządzane.

Obszar biznesowy – obszar działalności banku, którego funkcjonowanie jest wspierane przez środowisko teleinformatyczne, w tym np. działalność operacyjna, zarządzanie ryzykiem, rachunkowość, finanse itp.

Obszar technologii informacyjnej – obszar działalności banku mający na celu zapewnienie właściwego wsparcia funkcjonowania banku przez środowisko teleinformatyczne.

Podatność – słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie (na podstawie ISO/IEC 27000:2009).

Poufność danych – właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów (na podstawie ISO/IEC 27000:2009).

Profil ryzyka – skala i struktura ekspozycji na ryzyko.

Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

System informatyczny – aplikacja komputerowa lub zbiór powiązanych aplikacji komputerowych, którego celem jest przetwarzanie danych.

System zarządzania bezpieczeństwem środowiska teleinformatycznego – zbiór zasad i mechanizmów odnoszących się do procesów mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa środowiska teleinformatycznego.

Środowisko teleinformatyczne – infrastruktura teleinformatyczna banku wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w banku systemy informatyczne wspierające jego działalność, oparte na infrastrukturze teleinformatycznej zapewnianej przez podmioty zewnętrzne.

Zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji (na podstawie ISO/IEC 27000:2009).

III. Lista rekomendacji

Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

Rekomendacja 1

Rada nadzorcza banku powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd banku powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.

Rekomendacja 2

W banku powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.

Rekomendacja 3

Bank powinien opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania banku.

Rekomendacja 4

Bank powinien określić zasady współpracy oraz zakresy odpowiedzialności obszaru biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności banku.

Rekomendacja 5

Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach.

Rozwój środowiska teleinformatycznego

Rekomendacja 6

Bank powinien posiadać sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów.

Rekomendacja 7

Systemy informatyczne banku powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego.

Utrzymanie i eksploatacja środowiska teleinformatycznego

Rekomendacja 8

Bank powinien posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności banku.

Rekomendacja 9

Bank powinien posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych.

Rekomendacja 10

Bank powinien posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej banku.

Rekomendacja 11

Bank powinien posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infrastruktury teleinformatycznej.

Rekomendacja 12

Bank powinien zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem.

Rekomendacja 13

Bank powinien zapewniać wewnętrznym użytkownikom systemów informatycznych wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie.

Rekomendacja 14

Bank powinien podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.

Rekomendacja 15

System zarządzania ciągłością działania banku powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi.

Rekomendacja 16

Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.

Rekomendacja 17

Bank powinien posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego[1], skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.

[1] Oprogramowanie użytkownika końcowego (ang. *End-User Computing*, *EUC*) – narzędzia opracowane i funkcjonujące w oparciu o aplikacje instalowane na komputerach osobistych, takie jak MS Excel czy MS Access, dzięki którym użytkownicy niebędący programistami mogą tworzyć aplikacje biznesowe.

Zarządzanie bezpieczeństwem środowiska teleinformatycznego

Rekomendacja 18

W banku powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w banku.

Rekomendacja 19

Bank powinien klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa.

Rekomendacja 20

Bank powinien posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.

Rekomendacja 21

Bank powinien zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami.

Rekomendacja 22

Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być przedmiotem systematycznych, niezależnych audytów.

IV. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

Rola zarządu i rady nadzorczej

1. Rekomendacja 1

Rada nadzorcza banku powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd banku powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.

1.1. Szczególną uwagę rada nadzorcza i zarząd powinni poświęcić:

- zarządzaniu bezpieczeństwem środowiska teleinformatycznego[2] oraz ciągłością działania[3],
- procesowi tworzenia i aktualizacji strategii w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego[4],
- zarządzaniu elektronicznymi kanałami dostępu[5],
- współpracy z zewnętrznymi dostawcami usług w zakresie środowiska teleinformatycznego i jego bezpieczeństwa[6],
- zapewnieniu adekwatnej struktury organizacyjnej oraz zasobów kadrowych w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego[7],
- zarządzaniu jakością danych o kluczowym znaczeniu dla banku[8].

1.2. W celu zwiększenia skuteczności nadzoru i kontroli nad obszarem bezpieczeństwa środowiska teleinformatycznego, jak również zapewnienia efektywnej komunikacji w tym obszarze i zgodności jego działań z celami i potrzebami instytucji, bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[9] komitetu właściwego do spraw obszaru bezpieczeństwa środowiska teleinformatycznego. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu banku lub wyznaczony przez zarząd banku pełnomocnik.

---

[2] Patrz: sekcja „Zarządzanie bezpieczeństwem środowiska teleinformatycznego".
[3] Patrz: sekcja „Ciągłość działania środowiska teleinformatycznego".
[4] Patrz: sekcja „Planowanie strategiczne".
[5] Patrz: sekcja „Zarządzanie elektronicznymi kanałami dostępu".
[6] Patrz: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[7] Patrz: sekcja „Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego".
[8] Patrz: sekcja „Zarządzanie jakością danych".
[9] Nie jest wymagane, aby był to odrębny, dedykowany komitet – w szczególności dopuszczalne jest np. uwzględnienie zadań komitetu do spraw obszaru bezpieczeństwa środowiska teleinformatycznego w ramach komitetu do spraw ryzyka operacyjnego. Bank powinien jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

System informacji zarządczej

2. Rekomendacja 2

W banku powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.

2.1. Opracowując system informacji zarządczej w zakresie technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, bank powinien:

- zidentyfikować zagadnienia w obszarach technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, które powinny być objęte systemem informacji zarządczej, z uwzględnieniem związanego z nimi ryzyka i innych specyficznych uwarunkowań,
- określić sposób i zasady udostępniania i pozyskiwania informacji dotyczących ww. zagadnień (w tym również wskazać źródła, z których możliwe jest automatyczne pozyskiwanie tych informacji) oraz wskazać odpowiedzialności w tym zakresie,
- określić adekwatny zakres i częstotliwość raportowania,
- określić osoby lub funkcje, które powinny być odbiorcami informacji,
- zapewnić, aby informacje przekazywane każdemu z odbiorców były czytelne, rzetelne, dokładne, aktualne, miały odpowiedni zakres oraz były dostarczane terminowo i z właściwą częstotliwością.

Planowanie strategiczne

3. Rekomendacja 3

Bank powinien opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania banku.

3.1. Podstawową funkcją obszaru technologii informacyjnej w banku jest zapewnienie wsparcia dla działalności instytucji przez jej środowisko teleinformatyczne, zaś obszaru bezpieczeństwa środowiska teleinformatycznego – zapewnienie, że ryzyko związane z bezpieczeństwem tego środowiska jest odpowiednio zarządzane. W związku z tym, punktem wyjścia dla opracowania strategii[10] w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego powinna być strategia działania banku.

3.2. W celu zapewnienia, że strategia w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego jest realistyczna, a jednocześnie zgodna z aktualnymi i przyszłymi (przewidywanymi) uwarunkowaniami i oczekiwaniami biznesowymi, bank powinien dysponować niezbędną wiedzą o środowisku teleinformatycznym, pozwalającą na ujęcie wzajemnych zależności pomiędzy

[10] Liczba pojedyncza używana w sformułowaniu „strategia w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego" nie oznacza, że powinna ona zostać opracowana jako pojedynczy dokument. Bank powinien jednak zapewnić spójność strategii w obu tych obszarach.

poszczególnymi jego komponentami i przetwarzanymi w nim danymi oraz uwarunkowaniami, celami i potrzebami biznesowymi.

3.3. W zakresie realizacji powyższej strategii bank powinien w szczególności określić konkretne i mierzalne cele oraz programy / projekty o zdefiniowanych priorytetach i ramach czasowych (zgodnie z ustalonymi potrzebami). Powinny one obejmować:

– rozwój wykorzystywanego oprogramowania,
– zmiany w zakresie danych przetwarzanych w ramach działalności banku,
– rozwój infrastruktury teleinformatycznej,
– zmiany organizacyjne i procesowe w zakresie zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,

z uwzględnieniem wymagań dotyczących bezpieczeństwa środowiska teleinformatycznego, ryzyka związanego z realizacją tej strategii oraz środków finansowych koniecznych do jej realizacji.

3.4. Bank powinien zapewnić, aby realizacja powyższej strategii była w sposób efektywny nadzorowana, w szczególności poprzez monitorowanie realizacji określonych w niej celów oraz programów / projektów.

3.5. Bank powinien zapewnić, aby powyższa strategia była systematycznie[11] przeglądana i dostosowywana do zmian zachodzących zarówno w samym banku, jak i w jego otoczeniu, takich jak zmiany w strategii działania banku, zmiany w jego profilu ryzyka, zmiany prawne i regulacyjne czy rozwój technologiczny.

3.6. Zakres i poziom szczegółowości dokumentacji powyższej strategii powinny być adekwatne do jej złożoności oraz skali i profilu działalności banku.

Zasady współpracy obszarów biznesowych i technicznych

4. Rekomendacja 4

Bank powinien określić zasady współpracy oraz zakresy odpowiedzialności obszaru biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności banku.

4.1. Zasady określające tryb współpracy obszarów biznesowych, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz sposób komunikacji tych obszarów powinny być określone i sformalizowane w sposób adekwatny do skali i profilu działalności banku.

[11] Tj. w sposób uporządkowany i metodyczny.

4.2. Powyższe zasady powinny zapewniać, że:

- tryb podejmowania decyzji oraz zakresy zadań i odpowiedzialności w zakresie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego są precyzyjnie określone i adekwatne do ustalonej w banku roli obszaru technologii informacyjnej,
- obszar biznesowy możliwie precyzyjnie określa swoje oczekiwania (w tym ich priorytety) wobec obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności poprzez współuczestnictwo w procesie tworzenia strategii w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego,
- obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego możliwie precyzyjnie informują obszar biznesowy o szacowanych środkach finansowych niezbędnych do spełnienia potrzeb tego obszaru,
- obszar bezpieczeństwa środowiska teleinformatycznego uczestniczy w procesie rozwoju systemów informatycznych oraz w procesie opracowywania i zatwierdzania standardów i mechanizmów kontrolnych, które mają wpływ na poziom bezpieczeństwa środowiska teleinformatycznego,
- obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego uczestniczą w opiniowaniu strategii działania banku, w szczególności w zakresie wskazania ograniczeń i zagrożeń związanych z tą strategią, zidentyfikowanych z perspektywy tych obszarów,
- obszar biznesowy jest regularnie informowany o stanie realizacji istotnych z jego punktu widzenia programów / projektów związanych ze środowiskiem teleinformatycznym.

4.3. W celu zwiększenia skuteczności nadzoru i kontroli nad obszarem technologii informacyjnej, jak również zapewnienia efektywnej komunikacji w tym obszarze i zgodności jego działań z celami i potrzebami instytucji, bank powinien przeanalizować zasadność (uwzględniając w szczególności skalę i specyfikę prowadzonej działalności, poziom złożoności środowiska teleinformatycznego oraz założenia strategiczne dotyczące rozwoju tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[12] komitetu właściwego do spraw współpracy pomiędzy obszarem biznesowym a obszarem technologii informacyjnej. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu banku lub wyznaczony przez zarząd banku pełnomocnik.

4.4. Jednocześnie, w celu zapewnienia możliwie ścisłej integracji zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z zarządzaniem całą instytucją, bank powinien zapewnić właściwą współpracę pomiędzy jednostkami odpowiedzialnymi za obszar technologii informacyjnej, strategię działania banku,

[12] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Bank powinien jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

bezpieczeństwo, ciągłość działania, zarządzanie ryzykiem operacyjnym, zarządzanie procesami, zarządzanie projektami oraz audyt wewnętrzny (z zachowaniem odpowiedniego stopnia niezależności każdej z nich).

Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

5. Rekomendacja 5

Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach.

Struktura organizacyjna

5.1. Bank powinien zapewnić, aby struktura organizacyjna w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalała na efektywną realizację celów banku w tych obszarach, odpowiednio do skali i profilu działalności banku oraz stopnia złożoności środowiska teleinformatycznego. Adekwatność tej struktury powinna być systematycznie weryfikowana i – w przypadku wystąpienia takiej potrzeby – dostosowywana do zmian w środowisku wewnętrznym banku i jego otoczeniu.

Podział obowiązków

5.2. Bank powinien precyzyjnie zdefiniować obowiązki i uprawnienia poszczególnych pracowników w zakresie technologii informacyjnej i bezpieczeństwa informacji. Określenie zakresów obowiązków i uprawnień powinno mieć formę pisemną, a podział obowiązków powinien minimalizować ryzyko błędów i nadużyć w procesach i systemach. W tym celu należy zwrócić uwagę na odpowiednią separację obowiązków pracowników, w szczególności oddzielenie:

- funkcji tworzenia lub modyfikowania systemów informatycznych od ich testowania (poza testami realizowanymi przez programistów w ramach wytwarzania oprogramowania), administracji i użytkowania,
- funkcji administrowania danym komponentem środowiska teleinformatycznego od projektowania związanych z nim mechanizmów kontrolnych w zakresie bezpieczeństwa,
- funkcji administrowania danym systemem informatycznym od monitorowania działań jego administratorów,
- funkcji audytu od pozostałych funkcji w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

5.3. Bank powinien wyznaczyć osoby lub funkcje odpowiedzialne za podejmowanie decyzji w zakresie poszczególnych systemów eksploatowanych w banku (często zwane właścicielami systemów), opartych zarówno na infrastrukturze teleinformatycznej banku, jak i infrastrukturze zapewnianej przez podmioty zewnętrzne. Do obowiązków tych osób lub funkcji powinno należeć w szczególności:

– zapewnienie prawidłowości działania i bezpieczeństwa systemu pod względem biznesowym (np. poprzez właściwe zdefiniowanie procedur korzystania z systemu, udział w procesie zarządzania ciągłością jego działania, udział w procesie zarządzania uprawnieniami),

– nadzór nad działaniami użytkowników systemu,

– udział w procesie podejmowania decyzji w zakresie rozwoju tych systemów.

W przypadku, gdy dla danego systemu informatycznego określony został więcej niż jeden właściciel, bank powinien poświęcić szczególną uwagę precyzyjnemu określeniu podziału ich kompetencji i obowiązków.

5.4. Zapewnienie bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym nie jest wyłącznie domeną komórek odpowiedzialnych za obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, ale w dużej mierze zależy od właściwego postępowania bezpośrednich użytkowników systemów informatycznych i danych. W związku z tym, każdy pracownik banku powinien być świadomy, że jego obowiązkiem jest dbanie o bezpieczeństwo informacji przetwarzanych w środowisku teleinformatycznym. W tym celu bank powinien podejmować działania mające na celu tworzenie tzw. kultury bezpieczeństwa informacji, edukować pracowników w zakresie bezpieczeństwa środowiska teleinformatycznego[13] oraz uzyskać pisemne zobowiązania do przestrzegania regulacji wewnętrznych dotyczących tego obszaru.

5.5. Jako uzupełnienie wobec powyższego, pracownicy obszaru bezpieczeństwa środowiska teleinformatycznego powinni w sposób niezależny aktywnie monitorować realizację czynności przypisanych w tym obszarze jednostkom biznesowym i odpowiedzialnym za obszar technologii informacyjnej (np. w zakresie okresowych przeglądów uprawnień do systemów, bieżącej kontroli w zakresie bezpieczeństwa środowiska teleinformatycznego prowadzonej w jednostkach organizacyjnych, testowania poprawności procesu odtwarzania komponentów środowiska teleinformatycznego na podstawie kopii awaryjnych itp.).

5.6. W odniesieniu do systemów transakcyjnych, zaleca się wprowadzenie mechanizmu potwierdzenia ręcznie wprowadzanych transakcji dotyczących znacznych kwot przez drugą osobę (tzw. „autoryzacja na drugą rękę”). Ustalenie wysokości znacznej kwoty powinno zostać dokonane przez bank na podstawie analizy charakteru realizowanych transakcji.

Zasoby ludzkie

5.7. Bank powinien zapewnić, aby zarówno liczebność, jak i poziom wiedzy i kwalifikacji pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalały na bezpieczną i poprawną eksploatację całości środowiska teleinformatycznego. W związku z tym, bank powinien:

– zapewnić, aby poziom obciążenia pracowników pozwalał na efektywną realizację powierzonych im obowiązków,

[13] Patrz też: sekcja „Edukacja pracowników”.

– zapewnić pracownikom regularne szkolenia (adekwatnie do specyfiki zajmowanego przez nich stanowiska)[14], promować zdobywanie wiedzy oraz umożliwiać im wymianę doświadczeń (np. poprzez dostęp do tzw. baz wiedzy, udział w konferencjach i forach branżowych).

5.8. Bank nie powinien wprowadzać do użytku nowych technologii informatycznych bez posiadania wiedzy i kompetencji umożliwiających właściwe zarządzanie związanym z nimi ryzykiem. W związku z tym, bank każdorazowo powinien oceniać adekwatność tych kompetencji, zaś w przypadku stwierdzenia, że są one niewystarczające – podjąć działania mające na celu ich uzupełnienie (np. szkolenia pracowników, zatrudnienie nowych pracowników, podjęcie współpracy z zewnętrznymi dostawcami usług itp.).

5.9. Bank powinien przyłożyć szczególną uwagę do doboru pracowników zatrudnianych na stanowiskach dających dostęp do informacji o wysokim stopniu poufności[15].

5.10. Bank powinien podejmować działania mające na celu minimalizację ryzyka związanego z ewentualnym odejściem z pracy kluczowych pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego. W szczególności bank powinien:

– identyfikować kluczowych pracowników, których odejście wiąże się ze znacznym ryzykiem dla działalności banku,
– zapewnić dostępność aktualnej i precyzyjnej dokumentacji środowiska teleinformatycznego[16],
– zapewnić, że czynności przypisane do kluczowych pracowników są okresowo realizowane przez inne osoby (np. w trakcie odpowiednio długich urlopów kluczowych pracowników),
– posiadać opracowane programy sukcesji kluczowych pracowników,
– promować dzielenie się wiedzą między pracownikami,
– objąć informacją zarządczą istotne zdarzenia w zakresie kluczowych pracowników (w szczególności informacje o ich odejściach z pracy lub długotrwałych nieobecnościach)[17].

[14] Patrz też: sekcja „Edukacja pracowników”.
[15] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[16] Patrz: sekcja „Dokumentacja infrastruktury teleinformatycznej”.
[17] Patrz też: sekcja „System informacji zarządczej”.

V. Rozwój środowiska teleinformatycznego

Projekty w zakresie środowiska teleinformatycznego

6. Rekomendacja 6

Bank powinien posiadać sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów.

6.1. Zasady prowadzenia projektów w zakresie środowiska teleinformatycznego powinny w szczególności:

- wprowadzać definicję projektu[18],
- obejmować wszystkie etapy projektu, od jego inicjacji i podjęcia decyzji o rozpoczęciu do formalnego zamknięcia,
- określać sposób wskazywania interesariuszy projektu,
- określać sposób doboru uczestników projektu i wskazywać ich role, uprawnienia i odpowiedzialności,
- uwzględniać sposób dokumentowania realizacji projektu,
- określać zasady współpracy i komunikacji stron biorących udział w realizacji projektu,
- określać zasady zarządzania harmonogramem, budżetem, zakresem i jakością w projekcie,
- określać zasady zarządzania ryzykiem w projekcie,
- określać zasady zarządzania zmianą w projekcie,
- określać zasady oraz role i odpowiedzialności w zakresie odbioru i wprowadzania do eksploatacji produktów prac projektu,
- określać zasady podejmowania decyzji o zaniechaniu realizacji projektu.

6.2. Projekty powinny być prowadzone z wykorzystaniem lub w odniesieniu do uznanych standardów i dobrych praktyk w obszarze zarządzania projektami, jak np. standardy dotyczące zarządzania projektami proponowane przez PMI (Project Management Institute) – w szczególności standard PMBoK (Project Management Body of Knowledge) – czy metodyka PRINCE2 (PRojects IN Controlled Environments).

6.3. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą uwzględnienia w zasadach prowadzenia projektów udziału przedstawicieli obszaru bezpieczeństwa środowiska teleinformatycznego w całym cyklu życia projektu.

[18] Definicja projektu może zostać określona np. w odniesieniu do wielkości szacowanego budżetu projektu lub liczby dni roboczych niezbędnych do jego realizacji.

Rozwój systemów informatycznych

7. Rekomendacja 7

Systemy informatyczne banku powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego.

7.1. Rozwój systemów informatycznych powinien być zgodny z założeniami planów wynikających ze strategii banku w zakresie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

7.2. Bank powinien określać szczegółowe wymagania w zakresie rozwoju systemów informatycznych z uwzględnieniem aktualnych i przewidywanych potrzeb oraz możliwości przyszłego rozwoju środowiska teleinformatycznego. Każde wymaganie powinno być formułowane w sposób umożliwiający jednoznaczną ocenę jego spełnienia. Analiza wymagań powinna w szczególności obejmować[19]:

- wymagania dotyczące funkcjonalności systemu,
- wymagania dotyczące zakresu, ilości oraz formy danych przetwarzanych w systemie, z uwzględnieniem oceny możliwości migracji danych z aktualnie użytkowanych systemów informatycznych,
- wymagania dotyczące możliwości komunikacji z innymi wykorzystywanymi przez bank systemami informatycznymi, w szczególności zasad i zakresu wymiany danych,
- wymagania dotyczące oczekiwanej wydajności i dostępności systemu, z uwzględnieniem sytuacji jego znacznego obciążenia,
- wymagania dotyczące odporności systemu na zdarzenia awaryjne, w tym wymagania dotyczące czasu odtworzenia po awarii oraz dopuszczalnej utraty danych,
- wymagania dotyczące środowiska działania systemu,
- wymagania dotyczące bezpieczeństwa systemu i przetwarzanych w nim danych, w tym w zakresie mechanizmów kryptograficznych, mechanizmów kontroli dostępu oraz rejestracji zdarzeń zachodzących w systemie,
- wymagania wynikające z przepisów prawa, regulacji wewnętrznych oraz obowiązujących w banku standardów[20].

7.3. W ramach projektowania systemu informatycznego bank powinien uwzględnić możliwość wprowadzania w przyszłości jego modyfikacji, wynikających w szczególności ze zmian w przepisach prawa, strategii działania banku lub obowiązujących w nim standardach. Oznacza to, że rozwijając systemy informatyczne bank powinien zidentyfikować możliwe do przewidzenia zmiany w uwarunkowaniach wewnętrznych i zewnętrznych i rozważyć zasadność zapewnienia elastyczności danego systemu w odpowiednim zakresie, umożliwiającej w przyszłości efektywne wprowadzanie niezbędnych zmian.

---

[19] W przypadku wprowadzania zmian do istniejących systemów informatycznych elementy brane pod uwagę podczas analizy wymagań powinny być adekwatne do zakresu tych zmian.

[20] Patrz też: sekcja „Bezpieczeństwo formalno-prawne".

7.4. Wprowadzenie nowego systemu informatycznego, jak również znacznej zmiany do już istniejącego systemu, powinno być poprzedzone przeprowadzeniem analizy ryzyka wynikającego z zastosowanych technologii informatycznych oraz dokonaniem oceny wpływu wprowadzanych zmian na środowisko teleinformatyczne i procesy biznesowe banku, ze szczególnym uwzględnieniem aspektów bezpieczeństwa[21].

7.5. W przypadku rozwoju oprogramowania realizowanego siłami własnymi, bank powinien posiadać zdefiniowane podejście w tym zakresie. Dobrą praktyką jest określenie:

– stosowanej metodyki rozwoju oprogramowania, określającej m.in. przebieg tego procesu,
– stosowanych standardów w zakresie rozwoju oprogramowania, w tym:
  - standardów architektonicznych, w tym wykorzystywanych platform, technologii, mechanizmów integracji itp.,
  - wykorzystywanych narzędzi programistycznych oraz repozytoriów kodów,
  - standardów w zakresie kodów źródłowych, w tym preferowanych języków programowania i zapytań, stosowanych notacji i sposobów komentowania,
  - zasad wykonywania bieżących testów i przeglądów kodu, zapewniających odpowiedni stopień niezależności tych przeglądów,
  - kryteriów jakości oprogramowania (np. w zakresie łatwości utrzymania, przenośności itp.),
  - standardów w zakresie tworzonej dokumentacji technicznej,
  - zasad wersjonowania oprogramowania.

7.6. W przypadku rozwoju oprogramowania realizowanego z udziałem podmiotów zewnętrznych, bank powinien korzystać z usług wiarygodnych dostawców o odpowiednim doświadczeniu (udokumentowanym w zrealizowanych projektach) oraz reputacji na rynku, zapewniających odpowiedni poziom jakości świadczonych usług. Bank powinien również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uwzględnienia w umowach zawieranych w zakresie rozwoju oprogramowania z dostawcami zewnętrznymi postanowień dotyczących stosowania przyjętych w banku standardów i metodyk rozwoju oprogramowania[22]. W szczególności bank powinien zapewnić, aby przed wdrożeniem testowym produktów prac w banku były one testowane wewnętrznie przez dostawcę, przy czym fakt przeprowadzenia takich testów nie powinien w żadnym stopniu ograniczać zakresu testów przeprowadzanych w banku.

7.7. Zarówno nowe oprogramowanie, jak i zmiany wprowadzane do już funkcjonujących rozwiązań informatycznych, powinny być testowane adekwatnie do swojej złożoności oraz wpływu na pozostałe elementy środowiska teleinformatycznego banku. Bank powinien

[21] Patrz: sekcja „Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego”.
[22] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług”.

posiadać metodologię testowania oprogramowania, uwzględniającą w szczególności następujące dobre praktyki:

- sposób organizacji testów powinien zapewniać możliwie wysoki stopień niezależności weryfikacji spełnienia przyjętych założeń,
- w testach powinni brać udział przedstawiciele możliwie szerokiego zakresu jednostek organizacyjnych banku wykorzystujących wdrażane rozwiązanie (lub – w przypadku wprowadzania zmian – jego modyfikowaną część), jak również obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
- scenariusze testowe oraz zakres i wolumen danych wykorzystywanych w testach powinny być możliwie zbliżone do procedur i danych przetwarzanych w ramach faktycznego korzystania z systemu, przy czym bank powinien zapewnić zachowanie odpowiedniego stopnia poufności rzeczywistych danych wykorzystywanych na potrzeby testów,
- sposób zgłaszania i dokonywania korekt błędów oprogramowania powinien być precyzyjnie określony i zapewniać rejestrację wszystkich zgłaszanych błędów,
- testy powinny być przeprowadzane w dedykowanym środowisku testowym,
- zakres przeprowadzanych testów powinien obejmować weryfikację spełnienia wszystkich wymagań, w szczególności następujące obszary[23]:
  - zgodność z ustalonymi wymaganiami funkcjonalnymi,
  - wydajność i dostępność systemu, z uwzględnieniem warunków znacznego obciążenia,
  - zgodność nowego rozwiązania z wymogami bezpieczeństwa, w tym w zakresie uprawnień,
  - poprawność funkcjonowania mechanizmów zapewniających wymaganą dostępność i odtwarzanie po awarii, w tym odtwarzania systemu z kopii awaryjnych,
  - zgodność z przyjętymi miarami jakości oprogramowania,
  - poprawność integracji (wymiany danych) danego systemu z innymi systemami,
  - poprawność funkcjonowania systemów zintegrowanych z danym systemem, jak również – w przypadku wprowadzania zmian – pozostałej (niemodyfikowanej) części funkcjonalności systemu.

7.8. Bank powinien zapewnić, aby procedury przenoszenia nowego systemu informatycznego lub zmiany już funkcjonującego systemu na środowisko produkcyjne minimalizowały ryzyko wystąpienia przestojów w działalności banku. W szczególności po przeniesieniu systemu na środowisko produkcyjne bank powinien zweryfikować poprawność

[23] W przypadku wprowadzania zmian do istniejących systemów informatycznych obszary uwzględniane podczas testów powinny być adekwatne do zakresu tych zmian.

jego działania i zgodność z wymaganiami, a następnie przez odpowiedni czas monitorować system pod tym kątem w celu identyfikacji ewentualnych problemów wymagających interwencji. W związku z tym, bank powinien przeanalizować zasadność (uwzględniając w szczególności możliwości techniczne oraz stosunek ryzyka do kosztów) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia mechanizmów umożliwiających powrót do stanu sprzed wdrożenia w przypadku wystąpienia sytuacji krytycznej (takich jak tworzenie kopii awaryjnych odpowiedniego obszaru środowiska teleinformatycznego).

7.9. Funkcjonujące w banku środowiska rozwojowe, testowe i produkcyjne powinny być odpowiednio odseparowane. Wybrana metoda separacji (np. separacja logiczna z zastosowaniem wirtualizacji, separacja fizyczna itp.) powinna odpowiadać poziomowi ryzyka i uwarunkowaniom technicznym związanym z danym środowiskiem i funkcjonującymi w nim systemami.

7.10. Bank powinien zapewnić, aby wraz z rozwojem systemów informatycznych tworzona lub aktualizowana była odpowiednia dokumentacja funkcjonalna, techniczna, eksploatacyjna[24] i użytkowa (z zapewnieniem jej wersjonowania), zaś użytkownikom rozwijanych systemów zapewniane były odpowiednie szkolenia[25].

7.11. W banku powinien funkcjonować sformalizowany proces zarządzania zmianą w systemach informatycznych, określający zasady i tryb postępowania w zakresie:

– zgłaszania propozycji zmian,
– akceptacji zmian,
– określania priorytetów zmian,
– realizacji zmian,
– monitorowania realizacji zmian,
– testowania realizacji zmian,
– zamykania zrealizowanych zmian,
– zarządzania zmianami pilnymi / awaryjnymi.

7.12. Podejmując decyzję w zakresie akceptacji zmiany bank powinien przeprowadzić analizę jej zgodności z wymaganiami uprzednio ustalonymi dla modyfikowanego systemu informatycznego, w szczególności związanych z jego bezpieczeństwem. W przypadku, gdy w powyższym zakresie występuje rozbieżność, decyzja o akceptacji zmiany powinna być podejmowana ze szczególną rozwagą.

7.13. Przebieg procesu wprowadzania zmian do systemów informatycznych powinien być odpowiednio udokumentowany, w szczególności bank powinien prowadzić rejestr zmian wprowadzanych do poszczególnych systemów oraz dokonywać okresowej weryfikacji zgodności zapisów tego rejestru ze stanem faktycznym.

[24] Patrz też: sekcja „Dokumentacja infrastruktury teleinformatycznej”.
[25] Patrz też: sekcja „Edukacja pracowników”.

7.14. Szczególnej uwagi banku wymagają zmiany w zakresie środowiska teleinformatycznego wynikające z fuzji lub przejęć. W takich przypadkach bank powinien zapewnić, aby zasoby dedykowane projektowaniu docelowego, połączonego środowiska, integracji i zastępowaniu systemów informatycznych, planowaniu i realizacji migracji danych oraz weryfikacji wyników tych prac były adekwatne do skali i specyfiki przeprowadzanych zmian.

7.15. Bank powinien posiadać sformalizowane regulacje w zakresie wycofywania z eksploatacji użytkowanych rozwiązań informatycznych. Regulacje te powinny w szczególności określać zasady:

- podejmowania decyzji w zakresie wycofywania systemów z eksploatacji, uwzględniające istotność systemu[26],
- informowania zainteresowanych stron (w tym użytkowników) o wycofaniu systemu,
- przeprowadzania migracji danych i kontroli jej poprawności,
- dokonywania archiwizacji wycofywanych rozwiązań, w szczególności z zapewnieniem wymaganego przepisami prawa i uwarunkowaniami banku dostępu do danych oraz ich prawidłowego zabezpieczenia,
- aktualizacji konfiguracji infrastruktury teleinformatycznej w związku z wycofaniem rozwiązania (np. w zakresie wyłączania kont systemowych, rekonfiguracji zapór sieciowych itp.),
- bezpiecznej eliminacji wycofywanych z użytku komponentów infrastruktury teleinformatycznej,
- aktualizacji dokumentacji środowiska teleinformatycznego banku.

[26] Patrz: sekcja „Klasyfikacja systemów informatycznych”.

VI. Utrzymanie i eksploatacja środowiska teleinformatycznego

Zarządzanie danymi

8. Rekomendacja 8

Bank powinien posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności banku[27].

Zarządzanie architekturą danych

8.1. Bank powinien dysponować wiedzą dotyczącą tego, jakie dane przetwarzane są w ramach prowadzonej przez niego działalności, jakie są ich źródła (w tym z określeniem, czy są to źródła wewnętrzne, czy zewnętrzne) oraz w jakich jednostkach, procesach i systemach realizowane jest to przetwarzanie. W tym celu bank powinien przeprowadzić inwentaryzację przetwarzanych danych oraz systematycznie przeglądać rezultaty tej inwentaryzacji pod kątem zgodności ze stanem faktycznym. Bank powinien również przeanalizować zasadność (uwzględniając w szczególności skalę i specyfikę prowadzonej działalności oraz poziom złożoności środowiska teleinformatycznego) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania elektronicznego repozytorium w celu przeprowadzenia ww. inwentaryzacji i gromadzenia jej rezultatów.

8.2. Zakres i poziom szczegółowości powyższej inwentaryzacji powinny być uzależnione od skali działalności banku oraz określonej przez bank istotności poszczególnych grup danych (tj. danych dotyczących pewnego, określonego przez bank obszaru jego działalności). W przypadku istotnych grup danych bank powinien opracować ich szczegółową dokumentację, zawierającą modele tych danych, opisujące m.in. zależności pomiędzy ich poszczególnymi elementami oraz przepływy pomiędzy systemami informatycznymi, jak również posiadać odpowiednie zasady (polityki, standardy, procedury itp.) przetwarzania tych danych.

8.3. Do każdej zinwentaryzowanej grupy danych (lub jej podzbioru) powinien zostać przypisany podmiot (jednostka organizacyjna, rola, osoba itp.), który jest ostatecznie odpowiedzialny za jakość tych danych i nadzór nad nimi, w szczególności w zakresie zarządzania związanymi z nimi uprawnieniami i udziału w rozwoju systemów informatycznych, w których są one przetwarzane.

Zarządzanie jakością danych

8.4. W banku powinny obowiązywać sformalizowane zasady zarządzania jakością danych, których zakres i poziom szczegółowości powinny być uzależnione od skali i specyfiki działalności banku oraz określonej przez bank istotności poszczególnych grup danych. Niezależnie od przyjętej przez bank metodologii i nomenklatury w tym zakresie, zasady te powinny obejmować:

– okresowe dokonywanie oceny jakości danych,

[27] Obszar zarządzania danymi – który można zdefiniować jako całość działań związanych z kontrolą, ochroną, dostarczaniem i poprawą danych i informacji – zawiera w sobie również inne elementy, takie jak zarządzanie rozwojem danych, zarządzanie bezpieczeństwem danych czy zarządzanie bazami danych. Elementy te omówione zostały w innych sekcjach niniejszego dokumentu.

– dokonywanie czyszczenia danych,

– identyfikację przyczyn błędów występujących w danych,

– bieżące monitorowanie jakości danych.

8.5. Dokonując okresowej oceny jakości danych, bank powinien w szczególności identyfikować błędy w danych oraz badać ich wpływ na swoją działalność. Bank powinien także upewniać się, że przetwarzane dane są odpowiednie z perspektywy zarządzania (w tym pomiaru) poszczególnymi rodzajami ryzyka, jak również zaspokajania potrzeb raportowych i analitycznych ich kluczowych odbiorców – to znaczy, czy i w jakim stopniu ewentualne podjęcie błędnych decyzji wynikać może z niskiej jakości danych stanowiących ich podstawę. W tym celu bank powinien w szczególności:

– określić atrybuty wykorzystywane do oceny jakości danych (np. dokładność, spójność, kompletność, aktualność itp.) oraz częstotliwość i sposoby dokonywania ich pomiaru (np. automatyczne porównanie danych dotyczących tych samych operacji przechowywanych w różnych źródłach, weryfikacja z dokumentacją źródłową na podstawie próby, badanie satysfakcji użytkowników danych); w stosunku do poszczególnych danych możliwe jest stosowanie różnych atrybutów lub sposobów ich pomiaru,

– określić wartości progowe dla powyższych atrybutów, które bank uznaje za akceptowalne w odniesieniu do poszczególnych danych,

– regularnie dokonywać pomiaru jakości danych, zgodnie z zasadami określonymi w ramach powyższych działań.

8.6. Dokonując czyszczenia danych (tj. zmiany danych ocenionych jako błędne w dane odpowiednie do potrzeb i celów ich użycia) – o ile działania te realizowane są w sposób zautomatyzowany – bank powinien przyłożyć szczególną uwagę do poprawnego skonstruowania algorytmów czyszczących. Niepoprawny algorytm poprawiając jedne dane może bowiem (poprzez efekty uboczne) spowodować pogorszenie jakości innych danych.

8.7. Dokonując identyfikacji przyczyn błędów występujących w danych, bank powinien uwzględniać m.in. przyczyny związane z niewłaściwymi procedurami przetwarzania danych oraz z niską skutecznością mechanizmów kontrolnych funkcjonujących w zakresie zapewniania jakości danych, a następnie wdrażać nowe i usprawniać już funkcjonujące mechanizmy (zarówno na etapie wprowadzania danych do systemów, jak i ich późniejszego przetwarzania), w szczególności poprzez:

– modyfikację procesów zbierania i przetwarzania danych (w tym również sposobów wymiany danych pomiędzy systemami informatycznymi),

– wprowadzanie lub modyfikację mechanizmów kontroli bieżącej (takich jak automatyczne reguły walidacyjne, monitorowanie interfejsów wymiany danych, umieszczenie w procesach biznesowych punktów pomiaru jakości danych, uzgadnianie danych pomiędzy systemami itp.),

– wprowadzanie lub modyfikację mechanizmów kontroli okresowej oraz innych elementów procesu zarządzania jakością danych,

– wdrażanie zautomatyzowanych rozwiązań wspierających proces zarządzania jakością danych.

Powyższe mechanizmy kontrolne powinny być również przeglądane i dostosowywane w przypadku wprowadzania istotnych zmian w przebiegu procesów biznesowych, strukturze organizacyjnej, systemach informatycznych itp.

8.8. Bieżące monitorowanie jakości danych powinno obejmować informacje pozyskane z wykorzystaniem wprowadzonych mechanizmów kontrolnych. Zagregowane informacje dotyczące wyników monitorowania, jak również wyniki okresowych ocen jakości danych, powinny być przekazywane odpowiednim szczeblom hierarchii organizacyjnej w ramach systemu informacji zarządczej[28].

8.9. Projektując podejście do zarządzania jakością danych – w szczególności w przypadku braku wyodrębnionej jednostki organizacyjnej odpowiedzialnej za ten obszar – bank powinien zapewnić, aby zakresy odpowiedzialności i podział zadań w tym zakresie były jednoznacznie i precyzyjnie określone. Bank powinien również zapewnić zachowanie odpowiedniego stopnia poufności danych wykorzystywanych w procesie zarządzania jakością danych.

8.10. Projektując i realizując proces zarządzania jakością danych bank powinien w szczególności uwzględniać typowe czynniki mogące prowadzić do niskiej jakości danych, do których zaliczyć można m.in.:

– ręczne wprowadzanie danych do systemów, które w przypadku braku dostatecznej walidacji danych wejściowych czyni je podatnymi na błędy ludzkie, zaś przy zbyt silnej kontroli – na wprowadzanie danych niezgodnych z rzeczywistością (np. wprowadzanie zer w wymaganych polach numerycznych, których faktyczna wartość nie jest znana),
– wymiana danych pomiędzy systemami, z którą wiążą się m.in.:
  - zagrożenia wynikające z braku aktualizacji reguł wymiany danych przy dokonywaniu modyfikacji systemu źródłowego lub docelowego,
  - zagrożenia wynikające z trudności w dokonywaniu korekt w danych zidentyfikowanych jako błędne w sytuacji, w której poprzez interfejsy wymiany danych zostały już one przekazane do innych systemów,
– migracje danych (w tym związane z konsolidacją systemów), w ramach których struktury danych w systemach źródłowych i docelowych są często odmienne, zaś sama jakość danych w systemach źródłowych niekiedy nie jest wystarczająca.

8.11. Bank powinien tworzyć kulturę organizacyjną, w której kładzie się nacisk na zapewnianie odpowiedniej jakości danych wprowadzanych przez pracowników do systemów informatycznych.

8.12. Podejście banku do zarządzania jakością danych powinno uwzględniać szczególne uwarunkowania związane z ograniczoną kontrolą banku nad jakością danych pochodzących

[28] Patrz też: sekcja „System informacji zarządczej”.

ze źródeł zewnętrznych (takich jak np. międzybankowe systemy wymiany informacji BIK, AMRON czy ZORO). Bank powinien podejmować działania mające na celu umożliwienie dokonania oceny jakości tych danych oraz jej poprawę, w szczególności poprzez wymaganie od dostawców danych zewnętrznych przedstawiania potwierdzenia odpowiedniej jakości danych (popartego wynikami niezależnego audytu zewnętrznego). Bank powinien również przykładać szczególną uwagę do jakości danych wprowadzanych przez niego do baz zewnętrznych.

8.13. W związku z tym, że jakość danych przetwarzanych w środowisku teleinformatycznym w istotny sposób wpływa na jakość zarządzania bankiem, a jednocześnie często odbiorcy tych danych nie mają bezpośredniego wpływu na ich jakość (np. w przypadku danych wprowadzanych w ramach obszaru sprzedaży, a następnie wykorzystywanych przez obszar ryzyka), bank powinien przeanalizować zasadność (uwzględniając w szczególności specyfikę swojej struktury organizacyjnej oraz realizowanych procesów przetwarzania danych) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[29] komitetu właściwego do spraw zarządzania jakością danych.

Zarządzanie infrastrukturą teleinformatyczną

9. Rekomendacja 9

Bank powinien posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych.

Architektura infrastruktury teleinformatycznej

9.1. Rozległa sieć teleinformatyczna banku powinna zapewniać bezpieczeństwo przesyłanych danych. W szczególności sieć łącząca komponenty infrastruktury teleinformatycznej, których wyłączenie uniemożliwia prowadzenie działalności całego banku lub jego znaczącej części, powinna posiadać zapewnioną możliwość funkcjonowania w oparciu o łącza zapasowe.

9.2. Bank powinien przeanalizować zasadność (uwzględniając w szczególności stopień złożoności i rozproszenia środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań pozwalających na monitorowanie obciążenia sieci oraz na automatyczne uruchomienie łącza zapasowego.

9.3. Bank świadczący usługi za pośrednictwem elektronicznych kanałów dystrybucji powinien posiadać alternatywny dostęp do łączy telekomunikacyjnych wykorzystywanych na potrzeby tych usług na wypadek awarii u dostawcy podstawowego.

9.4. Styk sieci wewnętrznej banku z sieciami zewnętrznymi (w szczególności Internetem) powinien być zabezpieczony systemem zapór sieciowych[30].

---

[29] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Bank powinien jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

[30] Zapora sieciowa (ang. *firewall*) – zabezpieczenie fizyczne lub logiczne, kontrolujące przepływ danych do i z danego komponentu infrastruktury teleinformatycznej oraz pomiędzy podsieciami i sieciami (w tym pomiędzy sieciami wewnętrznymi a zewnętrznymi).

9.5. Bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą dokonania podziału sieci teleinformatycznej na podsieci (logiczne lub fizyczne), oddzielone zaporami sieciowymi zapewniającymi odpowiedni poziom kontroli dostępu i wykorzystujące inne mechanizmy (np. szyfrowanie ruchu sieciowego) uwzględniające wymagany poziom bezpieczeństwa przetwarzanych w nich danych, np. poprzez:

– oddzielenie podsieci dla wewnętrznych systemów bankowych od podsieci dla systemów wymieniających dane z otoczeniem zewnętrznym,
– oddzielenie podsieci obsługujących back-office od front-office,
– wydzielenie podsieci na potrzeby administracji infrastrukturą,
– wydzielenie podsieci na potrzeby rozwoju systemów informatycznych.

9.6. Reguły zarządzania ruchem sieciowym powinny zostać sformalizowane, podobnie jak reguły rejestrowania zdarzeń przez narzędzia monitorujące bezpieczeństwo infrastruktury teleinformatycznej i informowania o tych zdarzeniach. Zdarzenia te powinny podlegać systematycznej analizie. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań klasy IDS / IPS (ang. *Intrusion Detection System* / *Intrusion Prevention System*), zwiększających bezpieczeństwo infrastruktury teleinformatycznej poprzez wykrywanie (IDS) lub wykrywanie i blokowanie (IPS) ataków w czasie rzeczywistym.

9.7. Bank powinien posiadać sformalizowane zasady podłączania urządzeń końcowych (komputerów, urządzeń mobilnych) do infrastruktury teleinformatycznej. Opracowanie tych zasad powinno być poprzedzone przeprowadzeniem analizy ryzyka w tym zakresie. Ponadto w przypadku, gdy bank zezwala pracownikom na wykorzystywanie urządzeń prywatnych do celów służbowych, powinien on opracować sformalizowane zasady w tym zakresie, określające w szczególności:

– dopuszczalny zakres korzystania z takich urządzeń, wraz ze wskazaniem, jakiego rodzaju informacje mogą być na nich przetwarzane[31],
– dopuszczalne rodzaje urządzeń,
– dopuszczalne aplikacje, z których pracownicy mogą korzystać do celów służbowych,

jak również zapewnić wsparcie egzekwowania i kontroli tych zasad przez rozwiązania informatyczne oraz systematycznie edukować pracowników w zakresie bezpiecznego użytkowania urządzeń prywatnych do celów służbowych[32].

9.8. Korzystanie przez bank z sieci bezprzewodowych powinno wiązać się z analizą związanego z tym ryzyka. W szczególności bank powinien określić, jakie dane mogą być

[31] Patrz: sekcja „Klasyfikacja informacji".
[32] Patrz też: sekcja „Edukacja pracowników".

dostępne z wykorzystaniem tych sieci oraz jakie mechanizmy uwierzytelniania i szyfrowania będą wykorzystywane.

Komponenty infrastruktury teleinformatycznej

9.9. Rodzaj i konfiguracja każdego z komponentów infrastruktury teleinformatycznej powinny wynikać z analizy funkcji, jaką dany element pełni w środowisku teleinformatycznym oraz poziomu bezpieczeństwa wymaganego przez wykorzystujące dany komponent systemy informatyczne lub dane przesyłane za jego pośrednictwem[33]. W szczególności:

- rodzaj komponentu powinien być wybierany z uwzględnieniem wad i zalet danego rozwiązania z perspektywy punktu infrastruktury, w którym ma on zostać ulokowany (np. wybór pomiędzy sprzętowymi a programowymi zaporami sieciowymi),
- ustalając sposób konfiguracji komponentu, bank powinien kierować się zasadą minimalizacji udostępnianych przez dany komponent usług (w tym np. otwartych portów, obsługiwanych protokołów itp.), z jednoczesnym zapewnieniem planowanej funkcjonalności.

9.10. Bank powinien weryfikować predefiniowane ustawienia wprowadzone przez producenta urządzenia lub systemu – pozostawienie konfiguracji domyślnej (a zatem powszechnie znanej, np. w zakresie standardowych kont i haseł) w znacznym stopniu zwiększa poziom ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego.

9.11. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednie decyzje dotyczące:

- opracowania standardów konfiguracyjnych,
- utrzymywania rejestru komponentów infrastruktury informatycznej wraz z podstawowymi informacjami na temat ich rodzaju i konfiguracji,
- utrzymywania elektronicznego repozytorium kopii zastosowanej konfiguracji.

9.12. Bank powinien posiadać sformalizowane zasady dokonywania zmian w konfiguracji komponentów infrastruktury teleinformatycznej, uwzględniające istotność poszczególnych komponentów i zapewniające:

- realizację zmian w sposób zaplanowany i kontrolowany, z uwzględnieniem wpływu danej zmiany na inne komponenty,
- zabezpieczenie komponentów przed wprowadzaniem nieuprawnionych zmian,
- możliwość wycofania zmian, w tym dostępność kopii awaryjnych konfiguracji komponentów,
- możliwość identyfikacji osób wprowadzających oraz zatwierdzających poszczególne zmiany w konfiguracji.

[33] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

9.13. W przypadku przekazywania sprzętu do naprawy lub konserwacji do podmiotu zewnętrznego, bank powinien zapewnić, aby podmiot ten nie miał dostępu do zapisanych w tych urządzeniach danych o wysokim stopniu poufności[34], lub aby odpowiedzialność za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu współpracy uregulowana została w umowie z podmiotem zewnętrznym.

9.14. Bank powinien posiadać sformalizowane zasady wycofywania komponentów infrastruktury teleinformatycznej z eksploatacji, w szczególności zapewniające minimalizację ryzyka związanego z możliwością wycieku informacji przechowywanych na wycofywanych komponentach.

9.15. Konfiguracja systemu zapór sieciowych powinna zapewniać rejestrowanie niestandardowych aktywności w celu umożliwienia dokonywania ich analizy pod kątem wykrywania ataków zewnętrznych i wewnętrznych. System zapór sieciowych powinien także zapewniać kontrolę ruchu wychodzącego w celu blokowania prób nawiązania sesji z wewnątrz sieci przez szkodliwe oprogramowanie.

9.16. Bank wykorzystujący technologię wirtualizacji serwerów[35] powinien przeprowadzać analizę ryzyka związanego z tą technologią w odniesieniu do własnych uwarunkowań. Na podstawie wyników powyższej analizy, bank powinien zapewnić poprawne funkcjonowanie odpowiednich mechanizmów kontrolnych. Do dobrych praktyk w tym zakresie można zaliczyć m.in.:

– objęcie ścisłym nadzorem dostępności zasobów maszyny fizycznej (procesorów, pamięci operacyjnej, przestrzeni dyskowej itp.),
– lokowanie konsoli serwisowej i wszelkich narzędzi służących do zarządzania platformą wirtualizacji zasobów w podsieci dedykowanej administrowaniu tą platformą,
– ograniczenie możliwości nadużywania zasobów przez poszczególne maszyny wirtualne oraz współdzielenia schowka (ang. *clipboard*) pomiędzy maszyną fizyczną a wirtualną,
– szczególne zabezpieczenie maszyn fizycznych, na których ulokowane są maszyny wirtualne, przed nieuprawnionym dostępem do plików maszyn wirtualnych (ze względu na niewielka liczbę plików, które składają się na maszynę wirtualną, jest ona szczególnie podatna na wykradzenie) oraz innymi zagrożeniami, takimi jak ataki typu „*Denial-of-Service*”[36] (w przypadku wirtualizacji serwerów konsekwencje tego rodzaju ataków na maszynę fizyczną mogą być znacznie poważniejsze, dotykać bowiem będą wielu maszyn wirtualnych).

[34] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[35] Wirtualizacja serwerów – technika pozwalająca na jednoczesne funkcjonowanie wielu serwerów logicznych na danej platformie sprzętowej.
[36] Atak typu „*Denial-of-Service*” – atak polegający na podjęciu próby uniemożliwienia korzystania z danego komponentu środowiska teleinformatycznego przez inne komponenty tego środowiska lub przez autoryzowanych użytkowników.

9.17. Bank powinien monitorować sieci teleinformatyczne, komponenty infrastruktury teleinformatycznej, usługi sieciowe i systemy informatyczne pod kątem ich bezpieczeństwa i poprawności funkcjonowania adekwatnie do związanego z nimi poziomu ryzyka. Stopień automatyzacji ww. monitorowania powinien być adekwatny do złożoności środowiska teleinformatycznego banku.

9.18. Bank powinien przeanalizować zasadność (uwzględniając w szczególności stopień narażenia na ryzyko w zakresie bezpieczeństwa środowiska teleinformatycznego oraz liczbę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia dodatkowych zabezpieczeń w wykorzystywanym systemie poczty elektronicznej, ułatwiających sprawowanie kontroli nad informacjami o wysokim stopniu poufności[37] zawartymi w kierowanych na zewnątrz banku przesyłkach elektronicznych.

9.19. Eksploatowane w banku drukarki wykorzystywane do drukowania dokumentów zawierających informacje o wysokim stopniu poufności powinny być zabezpieczone przed możliwością wycieku informacji (w przypadku drukarek sieciowych – np. poprzez szyfrowanie przesyłanych do nich danych i przechowywanych przez nie zadań drukowania oraz odpowiednie mechanizmy weryfikacji tożsamości użytkowników). Bank powinien również zapewnić odpowiedni poziom ochrony wrażliwych formularzy papierowych przechowywanych w podajnikach drukarek.

9.20. Eksploatowane przez bank skanery sieciowe wykorzystywane do skanowania dokumentów zawierających dane osobowe lub takich, których nieuprawnione ujawnienie mogłoby narazić bank na znaczne straty, powinny być zabezpieczone przed możliwością wycieku informacji (np. poprzez przesyłanie danych w formie zaszyfrowanej). Rozwiązania banku w tym zakresie powinny również zapewniać, aby zeskanowane dokumenty były dostępne jedynie dla upoważnionych osób.

9.21. Konfiguracja komponentów infrastruktury teleinformatycznej powinna podlegać okresowej weryfikacji pod kątem pozostałych zmian zachodzących w tym środowisku, a także ujawnianych luk bezpieczeństwa. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia wsparcia tego procesu przez narzędzia automatyzujące czynności kontrolne. Jednym z narzędzi, które powinno być systematycznie stosowane przy ocenie skuteczności mechanizmów kontrolnych w obszarach infrastruktury teleinformatycznej o wysokiej istotności, są testy penetracyjne.

Aktualizacja oprogramowania komponentów infrastruktury teleinformatycznej

9.22. Bank powinien posiadać sformalizowane zasady dotyczące dokonywania aktualizacji oprogramowania – zarówno komputerów, jak i urządzeń mobilnych oraz pozostałych elementów środowiska teleinformatycznego (w tym aktualizacji systemów operacyjnych, systemów zarządzania bazami danych, oprogramowania użytkowego, oprogramowania urządzeń sieciowych itp.), uwzględniające istotność tego oprogramowania oraz poziom krytyczności poszczególnych aktualizacji.

[37] Patrz: sekcja „Klasyfikacja informacji”.

9.23. Zasady dotyczące aktualizacji oprogramowania komponentów infrastruktury teleinformatycznej powinny w szczególności wskazywać osoby odpowiedzialne za podejmowanie decyzji w zakresie zmian w środowisku produkcyjnym.

9.24. Przed dokonaniem aktualizacji oprogramowania komponentów środowiska produkcyjnego mających wpływ na systemy informatyczne o wysokiej istotności z perspektywy banku[38], bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą dokonania weryfikacji wpływu tej aktualizacji na środowisku testowym.

9.25. Terminowość i poprawność instalacji aktualizacji powinny być objęte okresową kontrolą. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania automatycznych mechanizmów instalacji aktualizacji oprogramowania komputerów osobistych i urządzeń mobilnych, jak również automatycznych narzędzi analizujących środowisko teleinformatyczne pod kątem aktualności oprogramowania.

9.26. Bank powinien dążyć do ograniczenia liczby komponentów środowiska teleinformatycznego pozbawionych odpowiedniego zakresu wsparcia producentów, w szczególności w zakresie elementów istotnych z perspektywy działalności banku. W tym zakresie bank powinien w szczególności:

– identyfikować i rejestrować przypadki występowania w środowisku teleinformatycznym komponentów pozbawionych wsparcia producentów oraz oceniać związane z tym ryzyko,
– przeprowadzać analizy dotyczące możliwości wymiany takich komponentów na komponenty objęte właściwym wsparciem lub podjęcia innych działań mających na celu kontrolę związanego z nimi ryzyka.

Powyższe działania powinny być dokonywane z odpowiednim wyprzedzeniem, tj. z uwzględnieniem okresu wymaganego do zrealizowania działań mających na celu zapewnienie kontroli ryzyka wynikającego z wykorzystywania komponentów nieobjętych wsparciem producentów.

Zarządzanie pojemnością i wydajnością komponentów infrastruktury teleinformatycznej

9.27. Infrastruktura teleinformatyczna banku powinna charakteryzować się:

– skalowalnością, rozumianą jako możliwość odpowiednio szybkiego podniesienia wydajności i pojemności,
– nadmiarowością, rozumianą jako możliwość bieżącej obsługi zwiększonej liczby transakcji w oparciu o aktualnie wykorzystywane zasoby (chwilowe zwiększenia obciążenia wynikać mogą m.in. z obsługi większej liczby transakcji w dniach zakończenia miesiąca księgowego, płatności rat, księgowania wynagrodzeń, obsługi

[38] Patrz: sekcja „Klasyfikacja systemów informatycznych”.

akcji promocyjnych, okresu przedświątecznego, niedostępności części komponentów infrastruktury teleinformatycznej itp.).

9.28. Bank powinien posiadać udokumentowane zasady zarządzania wydajnością i pojemnością komponentów infrastruktury teleinformatycznej, uwzględniające istotność poszczególnych komponentów dla działalności banku oraz zależności pomiędzy tymi komponentami, obejmujące w szczególności:

- określenie parametrów wydajności (np. czas odpowiedzi systemu, czas przetwarzania) i pojemności (np. obciążenie sieci teleinformatycznej, stopień wykorzystania urządzeń pamięci masowych, stopień wykorzystania procesorów, liczba otwartych sesji połączeniowych), wraz ze wskazaniem wartości ostrzegawczych i granicznych w tym zakresie,
- monitorowanie powyższych parametrów,
- analizę trendów oraz prognozowanie zapotrzebowania na wydajność i pojemność, z uwzględnieniem celów strategicznych banku, w szczególności w zakresie planowanej liczby obsługiwanych klientów oraz zmian w profilu działalności i związanego z tym przewidywanego wolumenu przetwarzanych danych,
- podejmowanie działań w przypadku przekroczenia wartości ostrzegawczych i granicznych powyższych parametrów oraz w przypadku, gdy analizy w zakresie zapotrzebowania na wydajność i pojemność wykażą, że obecne zasoby nie są wystarczające do jego zaspokojenia,
- raportowanie w zakresie wydajności i pojemności komponentów infrastruktury teleinformatycznej, w szczególności do właścicieli systemów informatycznych.

9.29. W celu zwiększenia efektywności procesu zarządzania wydajnością i pojemnością, bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą:

- zastosowania narzędzi pozwalających na automatyzację monitorowania obciążenia zasobów,
- sformalizowania parametrów jakości usług świadczonych przez środowisko teleinformatyczne na rzecz użytkowników wewnętrznych i zewnętrznych oraz włączenie raportowania w tym zakresie do systemu informacji zarządczej[39].

9.30. Bank powinien dokonywać okresowej weryfikacji zdolności środowiska teleinformatycznego w ośrodku zapasowym do utrzymania wymaganych dla niego parametrów wydajności i pojemności.

[39] Patrz też: sekcja „System informacji zarządczej”.

Dokumentacja infrastruktury teleinformatycznej

9.31. Bank powinien zapewnić, że dokumentacja poszczególnych komponentów środowiska teleinformatycznego (w tym ich konfiguracji) oraz zależności między nimi:

- jest aktualna,
- jest szczegółowa adekwatnie do poziomu istotności każdego z tych elementów,
- umożliwia przeprowadzanie wiarygodnych analiz środowiska pod kątem jego bezpieczeństwa i optymalizacji,
- pozwala na lokalizację i usuwanie przyczyn awarii,
- umożliwia odtworzenie działalności w przypadku wystąpienia takiej konieczności,
- pozwala na efektywną realizację zadań w zakresie kontroli wewnętrznej.

9.32. Dokumentacja infrastruktury teleinformatycznej powinna podlegać ochronie adekwatnej do stopnia jej wrażliwości. Zakres dokumentacji (w szczególności dokumentów opisujących szczegóły konfiguracji i funkcjonowania systemów zabezpieczeń) dostępnej dla poszczególnych pracowników nie powinien wykraczać poza minimum wynikające z powierzonego im zakresu obowiązków.

9.33. Kolejne wersje dokumentacji powinny posiadać oznaczenie oraz metrykę zmian dokumentu (data wprowadzenia, osoby opracowujące i zatwierdzające).

9.34. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, częstotliwość wprowadzania zmian technicznych oraz liczbę administratorów i serwisantów) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wdrożenia elektronicznego repozytorium dokumentacji infrastruktury teleinformatycznej.

9.35. Bank powinien posiadać procedury eksploatacji i administracji poszczególnych elementów środowiska teleinformatycznego. Kompletność i aktualność tych procedur powinny podlegać okresowej weryfikacji, zwłaszcza w przypadku elementów środowiska teleinformatycznego, w których wprowadzane są częste zmiany.

Współpraca z zewnętrznymi dostawcami usług

10. Rekomendacja 10

Bank powinien posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej banku.

10.1. Uwzględniając specyfikę działalności sektora bankowego, spośród usług świadczonych przez podmioty zewnętrzne czynności realizowane w obszarze technologii informacyjnej mają szczególny charakter ze względu na ich bezpośredni wpływ na jakość i bezpieczeństwo usług świadczonych na rzecz klientów oraz reputację banku. Jednocześnie, w zależności od specyficznych uwarunkowań banku, wpływ jakości współpracy z podmiotami zewnętrznymi na jakość usług świadczonych przez bank na rzecz klientów wykazuje duże

zróżnicowanie. W związku z tym, proces zarządzania relacjami z usługodawcami zewnętrznymi powinien być dostosowany do tych uwarunkowań.

10.2. Bank nie powinien traktować zlecania jakichkolwiek usług podmiotowi zewnętrznemu jako zwolnienia z odpowiedzialności za jakość i bezpieczeństwo usług świadczonych na rzecz klientów oraz bezpieczeństwo ich danych.

10.3. Procedury doboru usługodawców zewnętrznych – zwłaszcza w przypadku usług o istotnym znaczeniu dla banku – powinny uwzględniać ryzyko związane z danymi usługami i obejmować w szczególności ocenę sytuacji ekonomiczno-finansowej usługodawcy, zapewnianego przez niego poziomu bezpieczeństwa oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów).

10.4. Bank powinien analizować ryzyko związane z upadłością usługodawcy zewnętrznego lub jego nagłym wycofaniem się ze współpracy oraz posiadać skuteczne plany awaryjne związane z wystąpieniem takich sytuacji. Bank powinien również w miarę możliwości ograniczać liczbę przypadków, w których usługodawca zewnętrzny posiada w stosunku do banku pozycję monopolistyczną.

10.5. Bank powinien monitorować jakość usług świadczonych przez dostawców zewnętrznych, zaś istotne spostrzeżenia wynikające z tego monitoringu powinny być okresowo prezentowane zarządowi banku w ramach systemu informacji zarządczej[40]. Zakres, częstotliwość i metody monitorowania i raportowania powinny uwzględniać specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania banku.

10.6. W przypadku, gdy usługi świadczone przez podmiot zewnętrzny obejmują przetwarzanie danych o wysokim stopniu poufności lub istotności dla banku[41] poza infrastrukturą teleinformatyczną banku (np. w modelu *Cloud Computing* lub innych formach modelu *Application Service Provision*, w zewnętrznych centrach przetwarzania danych itp.), bank powinien w szczególności:

– wprowadzić odpowiednie mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),

– zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,

– posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, oraz zapewnić zgodność świadczonych usług z przepisami prawa obowiązującymi w Polsce,

– zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług),

[40] Patrz też: sekcja „System informacji zarządczej”.
[41] Patrz: sekcja „Klasyfikacja informacji”.

– przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególnie w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego).

10.7. Bank powinien sprawować kontrolę nad działalnością usługodawcy w zakresie świadczonych przez niego usług. W zależności od charakteru i poziomu istotności tych usług z perspektywy banku oraz klasyfikacji informacji przetwarzanych przez usługodawcę[42] (w szczególności wynikającej z wymagań prawnych dotyczących przetwarzania danych osobowych klientów banku), kontrola taka może w szczególności polegać na:

– weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń usługodawcy, w których odbywa się świadczenie usług na rzecz banku,

– przeglądzie wyników weryfikacji mechanizmów kontrolnych realizowanych – np. z wykorzystaniem standardu SSAE 16 – przez audyt wewnętrzny usługodawcy lub niezależnych audytorów zewnętrznych.

Możliwość sprawowania kontroli nad działalnością zewnętrznych dostawców usług powinna być regulowana w zawieranych z nimi umowach.

10.8. Dodatkowo, umowy zawierane z zewnętrznymi dostawcami usług powinny w miarę możliwości określać:

– zakresy odpowiedzialności stron umowy,

– zakres informacji i dokumentacji przekazywanych przez usługodawcę w związku ze świadczeniem usług,

– zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska teleinformatycznego banku, uwzględniające w szczególności obowiązujące przepisy prawa oraz regulacje banku w tym zakresie; w przypadku usługodawców posiadających dostęp do informacji o wysokim stopniu poufności, uregulowana powinna zostać również kwestia odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy,

– zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, w szczególności dostępu do kodów źródłowych w przypadku zaprzestania świadczenia usług wsparcia i rozwoju oprogramowania przez jego dostawcę (np. z wykorzystaniem usług depozytu kodów źródłowych),

– parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania,

[42] Patrz: sekcja „Klasyfikacja informacji”.

– zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług,
– zasady i tryb dokonywania aktualizacji oprogramowania komponentów infrastruktury znajdujących się pod kontrolą dostawcy,
– zasady współpracy w przypadku wystąpienia incydentu naruszenia bezpieczeństwa środowiska teleinformatycznego,
– zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług,
– kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług.

10.9. Umowy zawierane przez bank z zewnętrznymi dostawcami usług powinny zapewniać, że świadczenie usług odbywać się będzie zgodnie z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi oraz przyjętymi w banku standardami[43].

10.10. Wzorce umów lub umowy zawierane przez bank z zewnętrznymi dostawcami usług powinny być weryfikowane w odpowiednim zakresie przez jednostki banku odpowiedzialne za obszar prawny oraz obszar bezpieczeństwa środowiska teleinformatycznego.

10.11. Bank powinien posiadać regulacje dotyczące współpracy z pracownikami zewnętrznych dostawców usług, uwzględniające w szczególności:
– warunki udzielania dostępu do informacji o wysokim stopniu poufności[44],
– zasady sprawowania nadzoru nad działaniami pracowników zewnętrznych,
– konieczność zapewnienia, że każdy pracownik zewnętrzny posiadający dostęp do informacji o wysokim stopniu poufności objęty jest co najmniej takimi restrykcjami w zakresie bezpieczeństwa, jak pracownicy banku posiadający dostęp do takich informacji.

10.12. Zasady współpracy pomiędzy bankiem a zewnętrznym dostawcą usług powinny uwzględniać reguły w zakresie komunikacji i koordynacji wykonywanych przez usługodawcę czynności (np. w zakresie przeprowadzania migracji danych, czynności konserwacyjnych, skanowania infrastruktury teleinformatycznej itp.), minimalizujące ich negatywny wpływ na jakość i bezpieczeństwo usług świadczonych na rzecz klientów banku.

10.13. Bank powinien poświęcić szczególną uwagę ryzyku związanemu z przyznawaniem usługodawcom zewnętrznym (w szczególności spoza grupy kapitałowej) kompetencji w zakresie administrowania prawami dostępu do bankowych systemów informatycznych.

[43] Patrz też: sekcja „Bezpieczeństwo formalno-prawne”.
[44] Patrz: sekcja „Klasyfikacja informacji”.

Kontrola dostępu

11. Rekomendacja 11

Bank powinien posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infrastruktury teleinformatycznej.

Mechanizmy kontroli dostępu logicznego

11.1. Systemy informatyczne eksploatowane przez bank powinny posiadać mechanizmy kontroli dostępu pozwalające na jednoznaczne określenie i uwierzytelnienie tożsamości oraz autoryzację użytkownika.

11.2. Parametry haseł dostępu (w tym długość i złożoność hasła, częstotliwość zmiany, możliwość powtórnego użycia historycznego hasła) oraz zasady blokowania kont użytkowników powinny zostać ustalone w regulacjach wewnętrznych, z uwzględnieniem klasyfikacji systemu[45] oraz innych uwarunkowań z nim związanych, w tym prawnych i związanych z przyjętymi w banku standardami[46]. Funkcjonalność wykorzystywanych systemów informatycznych powinna w miarę możliwości wymuszać stosowanie obowiązujących w banku reguł dotyczących haseł dostępu oraz reguł blokowania konta użytkownika w przypadku użycia błędnego hasła.

11.3. Proces zarządzania uprawnieniami powinien zostać sformalizowany w procedurach wewnętrznych, określających zasady wnioskowania, przydzielania, modyfikacji i odbierania dostępu do systemów lub ich funkcjonalności, jak również monitorowania dostępów. Zakres nadawanego dostępu nie powinien wykraczać poza merytoryczny zakres obowiązków i uprawnień użytkownika (w tym również użytkowników zewnętrznych, np. pracowników agencji bankowych) oraz podlegać okresowej kontroli.

11.4. Bank powinien przeprowadzać regularne przeglądy nadanych uprawnień, obejmujące zgodność uprawnień faktycznie nadanych w systemach informatycznych zarówno z uprawnieniami przypisanymi w rejestrach uprawnień, jak i z merytorycznym zakresem obowiązków i uprawnień poszczególnych użytkowników. Częstotliwość wykonywania tych przeglądów powinna wynikać z analizy poziomu ryzyka związanego z poszczególnymi pracownikami i systemami informatycznymi, przy czym nie powinna być ona niższa niż roczna. Przeglądy uprawnień powinny być dokonywane w odpowiednim zakresie również w przypadku zmian funkcjonalności systemów informatycznych oraz zmian zakresów obowiązków pracowników. Wykryte w ramach powyższych przeglądów istotne nieprawidłowości oraz podjęte w związku z nimi działania powinny być raportowane w ramach systemu informacji zarządczej[47].

11.5. W celu zwiększenia efektywności zarządzania i nadzoru nad uprawnieniami oraz ograniczenia ryzyka nadania nieadekwatnych praw dostępu, bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska

[45] Patrz: sekcja „Klasyfikacja systemów informatycznych".
[46] Patrz też: sekcja „Bezpieczeństwo formalno-prawne".
[47] Patrz też: sekcja „System informacji zarządczej".

teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz liczbę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą:

– opracowania standardowych profili dostępu dla określonych grup pracowników lub stanowisk pracy,

– zastosowania narzędzi automatyzujących proces zarządzania uprawnieniami użytkowników (w szczególności rejestrowania uprawnień historycznych).

11.6. Bank w miarę możliwości powinien ograniczać użytkownikom dostęp do funkcji pozwalających na samodzielne zwiększenie własnych uprawnień. W sytuacjach, gdy powyższa zasada nie może być przestrzegana (np. w przypadku administratorów systemów informatycznych) należy zapewnić inne mechanizmy kontrolne w tym zakresie.

11.7. W przypadku systemów, których nieuprawnione użycie może skutkować szczególnie wysokimi stratami, bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą połączenia haseł dostępu z innymi mechanizmami weryfikacji tożsamości użytkownika (np. tokeny, elektroniczne karty identyfikacyjne, metody biometryczne itp.).

11.8. Wszyscy użytkownicy systemów informatycznych banku powinni być informowani o odpowiedzialności za zapewnienie poufności haseł oraz za skutki działań wykonanych z wykorzystaniem ich kont.

11.9. Obowiązujące w banku zasady zarządzania uprawnieniami powinny w szczególności uwzględniać zagrożenia związane z nieprawidłowym wykorzystaniem uprawnień użytkowników uprzywilejowanych. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia mechanizmów zapewniających każdorazową rejestrację oraz możliwość monitorowania dostępu z poziomu uprawnień uprzywilejowanych do najbardziej wrażliwych komponentów środowiska teleinformatycznego.

11.10. Systemy informatyczne przetwarzające dane o wysokiej istotności dla banku[48] powinny posiadać mechanizmy pozwalające na automatyczną rejestrację zachodzących w nich zdarzeń w taki sposób, aby zapisy tych rejestrów mogły – w przypadku wystąpienia takiej konieczności – stanowić wiarygodne dowody niewłaściwego lub niezgodnego z zakresem zadań użytkowników korzystania z tych systemów. Mechanizmy rejestracji zdarzeń powinny również uniemożliwiać nieuprawnione usuwanie lub modyfikowanie zapisów.

11.11. Bank powinien posiadać sformalizowane zasady zarządzania kluczami kryptograficznymi, obejmujące w szczególności ich tworzenie, przechowywanie, dystrybucję, niszczenie oraz archiwizację, zapewniające ochronę kluczy przed nieuprawnioną modyfikacją i ujawnieniem.

[48] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

Mechanizmy kontroli dostępu fizycznego

11.12. Istotnym elementem bezpieczeństwa środowiska teleinformatycznego jest kontrola fizycznego dostępu do pomieszczeń, w których ulokowane są serwery i inne kluczowe elementy infrastruktury teleinformatycznej oraz urządzenia wspierające jej działanie (w tym zasilacze awaryjne, generatory prądotwórcze, klimatyzatory i rozdzielnie elektryczne). Mechanizmy kontroli dostępu fizycznego powinny zapewniać dostęp jedynie uprawnionych osób (tj. takich, w przypadku których konieczność posiadania dostępu wynika z zakresu obowiązków) oraz wszczęcie alarmu w przypadku prób dostępu podejmowanych przez osoby nieuprawnione. Mechanizmy te powinny również obejmować rejestrację ruchu osobowego. Stosowane rozwiązania powinny być adekwatne do poziomu ryzyka związanego z komponentami ulokowanymi w danym pomieszczeniu, specyficznych uwarunkowań (w tym lokalowych) banku oraz skali i charakteru prowadzonej działalności.

11.13. W pomieszczeniach, w których ulokowane są kluczowe elementy infrastruktury teleinformatycznej, poza sytuacjami wyjątkowymi nie powinno się zezwalać przebywającym tam osobom na fotografowanie, nagrywanie audio/video itp. Zezwolenia przewidujące wyjątki w tym zakresie powinny być udzielane przez odpowiednio upoważnione osoby oraz rejestrowane.

Ochrona przed szkodliwym oprogramowaniem

12. Rekomendacja 12

Bank powinien zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem.

12.1. Bank powinien zapewnić automatyczną ochronę przed szkodliwym oprogramowaniem (takim jak wirusy, konie trojańskie, robaki, oprogramowanie *rootkit*[49] itp.), zarówno w przypadku wymagających takiej ochrony centralnych elementów infrastruktury teleinformatycznej (serwerów, kontrolerów domeny itp.), jak i komputerów osobistych i urządzeń mobilnych. Ochrona ta powinna być realizowana w sposób ciągły, zaś użytkownicy nie powinni mieć możliwości jej wyłączenia. Zakres ochrony powinien wynikać ze stopnia narażenia każdego komponentu infrastruktury na wystąpienie zagrożenia, jak również potencjalnej dotkliwości skutków jego wystąpienia dla banku.

12.2. Aplikacje chroniące przed szkodliwym oprogramowaniem oraz sygnatury szkodliwego oprogramowania powinny być systematycznie aktualizowane. O ile to możliwe, bank powinien zapewnić, aby powyższa aktualność weryfikowana była każdorazowo przy próbie podłączenia urządzenia do sieci wewnętrznej banku.

[49] Oprogramowanie *rootkit* – narzędzie, które modyfikuje pliki systemowe w taki sposób, aby ukryć swoją obecność na komputerze przed użytkownikiem, oprogramowaniem antywirusowym itp., oraz umożliwia wykonywanie akcji określonych przez twórcę (takich jak np. przechwytywanie haseł użytkownika czy uniemożliwienie dokonania aktualizacji oprogramowania antywirusowego) bez wiedzy użytkownika.

12.3. Bank powinien posiadać sformalizowane zasady w zakresie ochrony przed szkodliwym oprogramowaniem, obejmujące w szczególności:

– sposób postępowania z poszczególnymi rodzajami wykrytego szkodliwego oprogramowania,
– tryb podejmowania decyzji o zaprzestaniu użytkowania zagrożonych komponentów środowiska teleinformatycznego lub ich izolowaniu od pozostałej części tego środowiska,
– tryb informowania odpowiednich jednostek banku o zagrożeniu[50].

12.4. Niezależnie od poziomu stosowanej automatycznej ochrony przed szkodliwym oprogramowaniem, kluczowa z tej perspektywy jest również świadomość użytkowników końcowych w zakresie zasad bezpieczeństwa. W związku z tym, bank powinien zapewnić odpowiedni poziom edukacji użytkowników w tym zakresie[51].

Wsparcie dla użytkowników

13. Rekomendacja 13

Bank powinien zapewniać wewnętrznym użytkownikom systemów informatycznych wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie.

13.1. Sposób działania obszaru zapewniania wsparcia dla wewnętrznych użytkowników systemów informatycznych powinien być dostosowany do skali prowadzonej działalności, złożoności środowiska teleinformatycznego i liczby jego użytkowników wewnętrznych oraz uwzględniać ewentualną zależność od zewnętrznych dostawców usług.

13.2. Funkcjonowanie procesu wsparcia wewnętrznych użytkowników systemów informatycznych powinno być sformalizowane adekwatnie do złożoności środowiska teleinformatycznego banku oraz liczby wewnętrznych użytkowników systemów informatycznych. Zgłoszenia powinny być rejestrowane oraz analizowane w celu umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów. Osoby odpowiedzialne za zapewnienie wsparcia dla użytkowników powinny również być przeszkolone w zakresie identyfikacji i eskalacji incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego[52].

13.3. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz liczbę i charakterystykę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia wsparcia obsługi zgłoszeń użytkowników przez system informatyczny, pozwalający w szczególności na gromadzenie i raportowanie danych o występujących problemach oraz monitorowanie jakości zapewnianego wsparcia.

---

[50] Patrz też: sekcja „Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego”.
[51] Patrz: sekcja „Edukacja pracowników”.
[52] Patrz: sekcja „Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego”.

Edukacja pracowników

14. Rekomendacja 14

Bank powinien podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.

14.1. Bank powinien utrzymywać kwalifikacje wszystkich pracowników na poziomie odpowiednim dla zapewnienia bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym i umożliwienia właściwego korzystania ze sprzętu i systemów informatycznych. Poziom ten powinien być zróżnicowany w zależności m.in. od ryzyka związanego z poziomem uprawnień i kompetencji poszczególnych pracowników oraz pełnionej przez nich roli w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego.

14.2. W celu zapewnienia odpowiedniego poziomu kwalifikacji pracowników w powyższym zakresie, bank powinien stosować adekwatne formy szkoleń, zapewniać właściwe materiały, jak również prowadzić różnorodne akcje edukacyjne mające na celu podniesienie kultury bezpieczeństwa informacji (np. z wykorzystaniem plakatów czy wygaszaczy ekranu). Bank powinien również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą premiowania zachowań wspierających tworzenie kultury bezpieczeństwa informacji.

14.3. W ramach prowadzenia edukacji pracowników bank powinien uwzględniać m.in. zagrożenia związane z korzystaniem z urządzeń mobilnych, korzystaniem z własnego sprzętu informatycznego w celach zawodowych oraz korzystaniem ze sprzętu służbowego w celach prywatnych, publikowaniem przez pracowników informacji dotyczących banku w Internecie (w szczególności na portalach społecznościowych) oraz z atakami socjotechnicznymi, jak również informować pracowników o procesie postępowania dyscyplinarnego wobec osób nieprzestrzegających procedur bezpieczeństwa.

Ciągłość działania środowiska teleinformatycznego

15. Rekomendacja 15

System zarządzania ciągłością działania banku powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi.

Plany utrzymania ciągłości działania i plany awaryjne

15.1. Plany utrzymania ciągłości działania oraz plany awaryjne banku powinny spełniać warunki określone w „Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach”.

15.2. Bank powinien przeanalizować zasadność (uwzględniając w szczególności stopień narażenia na ryzyko w zakresie bezpieczeństwa środowiska teleinformatycznego oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą

wyznaczenia lub wskazania[53] stałego komitetu właściwego do spraw ciągłości działania, którego zadaniem powinien być w szczególności nadzór nad zapewnieniem dostępności niezbędnych zasobów pozwalających na kontynuowanie lub odtworzenie działalności.

15.3. Ponieważ odtworzenie działania środowiska teleinformatycznego jest zwykle niezbędne dla wznowienia funkcjonowania procesów biznesowych, bank powinien poświęcić szczególną uwagę zarządzaniu ciągłością działania w zakresie jednostek odpowiedzialnych za funkcjonowanie tego środowiska.

15.4. Dokumentacja systemu zarządzania ciągłością działania banku w zakresie środowiska teleinformatycznego (w szczególności procedur replikacji danych, tworzenia kopii zapasowych i procedur odtworzeniowych) powinna uwzględniać klasyfikację systemów informatycznych oraz przetwarzanych w nich informacji[54], jak również zależności pomiędzy tymi systemami. Aktualność tej dokumentacji powinna być regularnie weryfikowana.

15.5. Bank powinien posiadać efektywny system dystrybucji dokumentacji systemu zarządzania ciągłością działania w zakresie środowiska teleinformatycznego, zapewniający zarówno jej poufność, jak i dostępność dla odpowiednich osób.

15.6. W ramach podejścia do zarządzania ciągłością działania bank powinien uwzględniać zależności od zewnętrznych dostawców usług, których znaczenie jest kluczowe z perspektywy ciągłości działania banku. W szczególności bank powinien:

– określić tryb komunikacji i współpracy z usługodawcą w przypadku wystąpienia sytuacji awaryjnej,
– uwzględnić udział usługodawców zewnętrznych w procesie testowania systemu zarządzania ciągłością działania[55],
– opracować zasady związane z wystąpieniem konieczności zmiany usługodawcy w trakcie sytuacji awaryjnej.

Zasoby techniczne oraz warunki fizyczne i środowiskowe

15.7. Bank powinien posiadać adekwatne do skali i specyfiki prowadzonej działalności zasoby techniczne, pozwalające na bieżące funkcjonowanie kluczowych procesów oraz ich odtworzenie w przypadku wystąpienia sytuacji awaryjnej, w szczególności z uwzględnieniem zdefiniowanych dla tych procesów:

– parametrów określających maksymalny czas trwania odtwarzania funkcjonowania tych procesów[56],
– parametrów określających, jak wiele (tj. za jaki okres) maksymalnie danych przechowywanych w systemach informatycznych może zostać utraconych[57].

[53] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Bank powinien jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.
[54] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".
[55] Patrz: sekcja „Weryfikacja efektywności podejścia do zarządzania ciągłością działania".
[56] RTO – ang. *Recovery Time Objective*.
[57] RPO – ang. *Recovery Point Objective*.

15.8. W przypadku wystąpienia sytuacji rozległej awarii lub niedostępności podstawowego ośrodka przetwarzania danych, bank powinien posiadać możliwość odtworzenia środowiska teleinformatycznego (adekwatnego do założeń planów awaryjnych) w lokalizacji zapasowej. Lokalizacja ta powinna być odpowiednio odległa od ośrodka podstawowego, w celu minimalizacji ryzyka związanego z niedostępnością obu ośrodków w wyniku zajścia pojedynczej przyczyny (np. powodzi). Proces odtwarzania środowiska powinien zostać sformalizowany w szczegółowych regulacjach wewnętrznych, określających zakresy kompetencji, niezbędne zasoby oraz kolejność i sposób odtwarzania komponentów środowiska teleinformatycznego.

15.9. Charakter funkcjonowania ośrodka zapasowego powinien być dostosowany do skali i specyfiki prowadzonej działalności operacyjnej oraz uwzględniać maksymalny akceptowany przez bank czas niedostępności usług.

15.10. Warunkiem nieprzerwanego i bezpiecznego funkcjonowania środowiska teleinformatycznego jest zapewnienie bezpieczeństwa fizycznego i środowiskowego w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, w szczególności w zakresie warunków związanych z ciągłością zasilania elektrycznego oraz stabilnością jego parametrów, temperaturą, wilgotnością i poziomem zapylenia, jak również kluczowe elementy instalacji zabezpieczających przed zalaniem, pożarem, włamaniem i kradzieżą lub celowym uszkodzeniem. W związku z tym, bank powinien identyfikować zagrożenia w powyższym zakresie oraz analizować ich potencjalny wpływ na bezpieczeństwo środowiska teleinformatycznego i ciągłość działania (w szczególności w przypadku, gdy zasoby ośrodka zapasowego nie pozwalają na szybkie wznowienie działalności). Analiza ta powinna umożliwić określenie, czy lokalizacja pomieszczeń, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej jest odpowiednia oraz czy są one adekwatnie zabezpieczone.

15.11. Przeprowadzając powyższą analizę bank powinien w szczególności uwzględnić zagrożenia związane z:

- lokalizacją i sąsiedztwem budynku (w tym znajdującymi się w jego okolicy lotniskami, obiektami wojskowymi itp.),
- lokalizacją i sąsiedztwem pomieszczeń, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej (w szczególności zagrożenia związane z ulokowaniem tych pomieszczeń w piwnicach lub na poddaszach),
- uwarunkowaniami konstrukcyjnymi (np. wytrzymałością stropów, szczelnością pomieszczeń, jakością instalacji odgromowej).

15.12. W celu zapewnienia właściwych warunków fizycznych i środowiskowych w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, bank powinien w szczególności przestrzegać następujących zasad:

- Drzwi, okna, ściany i stropy w pomieszczeniach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, powinny zapewniać właściwą odporność mechaniczną, przeciwpożarową i przeciwwłamaniową.

– W pomieszczeniach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, nie powinno się umieszczać materiałów łatwopalnych lub – w przypadku takiej konieczności – odpowiednio je zabezpieczać (np. w szafach gwarantujących ochronę przeciwpożarową).

– Stosowane czynniki gaszące powinny minimalizować ryzyko uszkodzenia urządzeń elektronicznych i zapisanych w nich danych.

– Systemy zabezpieczeń antywłamaniowych i przeciwpożarowych powinny zapewniać niezwłoczne powiadomienie osób odpowiedzialnych za ochronę oraz wszczęcie akcji gaśniczej i ratunkowej. Bank powinien również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uzupełnienia systemu ochrony przeciwpożarowej o urządzenia automatycznego gaszenia.

– W pomieszczeniach, w których ulokowane są komponenty infrastruktury teleinformatycznej, należy zapewnić utrzymywanie parametrów środowiskowych (np. temperatury, wilgotności, zapylenia itp.) na poziomie określonym przez producentów tych komponentów. Stosowane przez bank urządzenia kontrolujące te parametry powinny charakteryzować się właściwą wydajnością oraz redundancją (na wypadek awarii). Bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań zapewniających automatyczne monitorowanie i regulację parametrów środowiskowych.

– Dobór mechanizmów zapewniających ciągłość zasilania elektrycznego powinien uwzględniać oraz skalę i specyfikę działalności banku. Zasilanie awaryjne w oparciu jedynie o zasilacze bateryjne (UPS) pozwala na podtrzymywanie pracy zasobów przez ograniczony czas i z reguły w ograniczonym zakresie, dlatego bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia niezależnego zasilania elektrycznego w oparciu o generator prądotwórczy, w miarę możliwości uruchamiany automatycznie w przypadku zaniku zasilania podstawowego, jak również stosowanie zwielokrotnionych linii elektrycznych.

15.13. W przypadku czasowego przeniesienia sprzętu teleinformatycznego do innego pomieszczenia (np. w związku z remontem) bank powinien zapewnić w tym pomieszczeniu odpowiednie warunki fizyczne i środowiskowe oraz właściwy poziom kontroli dostępu[58].

15.14. Skuteczność funkcjonowania mechanizmów mających na celu zapewnienie właściwych warunków fizycznych i środowiskowych w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, powinna podlegać okresowej weryfikacji.

[58] Patrz: sekcja „Mechanizmy kontroli dostępu fizycznego”.

Kopie awaryjne

15.15. Jednym ze środków mających na celu zapewnienie ciągłości działania w przypadku awarii lub katastrofy są awaryjne kopie danych, instancji systemów informatycznych oraz konfiguracji kluczowych komponentów infrastruktury teleinformatycznej. Bank powinien posiadać sformalizowane zasady zarządzania nośnikami danych przechowującymi kopie awaryjne. Zasady te powinny w szczególności obejmować:

– zakres, sposób i częstotliwość kopiowania danych,

– sposoby identyfikacji nośników,

– miejsce, okres i sposób bezpiecznego przechowywania nośników,

– sposób i formę autoryzacji zmian na nośnikach i usuwania danych,

– role i odpowiedzialności w zakresie zarządzania nośnikami,

– sposoby właściwej i trwałej likwidacji niepotrzebnych danych (w zakresie zarówno likwidacji danych zapisanych na nadal eksploatowanych nośnikach, jak i likwidacji nośników wycofywanych z eksploatacji).

15.16. Poprawność wykonywania kopii awaryjnych oraz możliwość odtworzenia z nich danych powinny podlegać okresowej kontroli. Kontrola taka może być wykonywana automatycznie, przy czym w takim przypadku należy zapewnić, aby odpowiednie osoby były informowane o jej wynikach.

15.17. Bank powinien posiadać szczegółowe regulacje i instrukcje odtwarzania komponentów środowiska teleinformatycznego na podstawie kopii awaryjnych. Dokumenty te powinny być napisane w taki sposób, aby możliwe było przeprowadzenie tego procesu przez posiadające odpowiednie kwalifikacje i uprawnienia osoby trzecie (tj. takie, które na bieżąco nie zajmują się administracją danym komponentem środowiska). Proces odtwarzania komponentów środowiska teleinformatycznego powinien być systematycznie testowany.

15.18. Bank powinien zapewnić integralność kopii awaryjnych od momentu ich utworzenia aż do likwidacji. Oznacza to, że przez cały ten okres powinny one odzwierciedlać faktyczny stan zasobów na moment utworzenia kopii, co wyklucza możliwość usuwania z nich jakichkolwiek danych. Regulacje i instrukcje w zakresie odtwarzania danych z kopii awaryjnych powinny uwzględniać zasady dotyczące wprowadzania w odtworzonych danych zmian powstałych pomiędzy utworzeniem danej kopii awaryjnej (lub ich sekwencji) a użyciem jej do odtworzenia stanu środowiska teleinformatycznego sprzed awarii.

15.19. Kopie, zwłaszcza transportowane lub transmitowane poza bank, powinny podlegać zabezpieczeniu (np. kryptograficznemu) przed nieuprawnionym dostępem, na poziomie adekwatnym do klasyfikacji przechowywanych na nich danych[59]. Nośniki zawierające kopie powinny być przechowywane w sposób minimalizujący ryzyko ich uszkodzenia (np. w wyniku pożaru, zalania, wpływu pola magnetycznego) lub nieuprawnionej modyfikacji. Powinny być one również składowane oddzielnie od komponentów środowiska, których dotyczą.

[59] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

15.20. Nośniki uszkodzone lub wycofane z użycia powinny podlegać zniszczeniu w sposób uniemożliwiający odtworzenie danych.

Weryfikacja efektywności podejścia do zarządzania ciągłością działania

15.21. Bank powinien regularnie weryfikować efektywność przyjętego podejścia do zarządzania ciągłością działania w zakresie środowiska teleinformatycznego, w tym w zakresie zdolności do odtworzenia działalności w oparciu o środowisko zapasowe. Częstotliwość, zakres oraz sposób przeprowadzania testów (taki jak np. symulacje, całościowe testy operacyjne itp.) powinny uwzględniać skalę i specyfikę działalności banku oraz zagrożenia związane z poszczególnymi komponentami środowiska teleinformatycznego. Plany testów, zwłaszcza w przypadku, kiedy mogą mieć one wpływ na bieżącą działalność banku, powinny być konsultowane w organizacji i zatwierdzane przez zarząd banku. Wyniki testów oraz plany działań naprawczych, które należy podjąć w celu usunięcia zidentyfikowanych nieprawidłowości, powinny być dokumentowane. Rada nadzorcza i kierownictwo banku powinno być informowane o wynikach testów oraz terminowości i skuteczności podejmowanych działań naprawczych.

Zarządzanie elektronicznymi kanałami dostępu

16. Rekomendacja 16

Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.

Weryfikacja tożsamości klientów

16.1. Kluczowe znaczenie w usługach bankowości świadczonych za pośrednictwem elektronicznych kanałów dostępu ma potwierdzenie, czy dana próba kontaktu, dostępu lub transakcji jest uprawniona. W związku z tym, bank powinien określić i stosować możliwie niezawodne metody i środki:

– weryfikacji tożsamości klienta przy otwieraniu rachunku, również w przypadku zawierania takich umów na odległość (bez fizycznej obecności klienta w placówce banku), z uwzględnieniem wymagań prawnych w tym zakresie[60],

– potwierdzania tożsamości i uprawnień klientów korzystających z elektronicznych kanałów dostępu, minimalizujące ryzyko udzielenia dostępu nieupoważnionym osobom.

16.2. Wybór stosowanych przez bank metod potwierdzania tożsamości klientów korzystających z elektronicznych kanałów dostępu powinien być dokonywany w oparciu o analizę ryzyka związanego z tymi kanałami. Analiza ta powinna być przeprowadzana systematycznie i uwzględniać możliwości transakcyjne oferowane przez dany kanał dostępu, przetwarzane w nim dane, rozpoznane techniki ataków, a jednocześnie łatwość korzystania przez klienta z poszczególnych metod potwierdzania tożsamości. Typowe środki

[60] Patrz też: sekcja „Bezpieczeństwo formalno-prawne".

wykorzystywane w zakresie potwierdzania tożsamości w elektronicznych kanałach dostępu obejmują m.in. osobisty numer identyfikacyjny, hasła, podpis elektroniczny, karty smart, kody jednorazowe, tokeny, dane biometryczne czy certyfikaty cyfrowe, przy czym metody weryfikacji tożsamości mogą opierać się na jednym lub wielu czynnikach (np. stosowanie zarówno hasła, jak i kodów jednorazowych). Bank powinien także przeanalizować, czy i w jakim stopniu zastosowanie wieloczynnikowej weryfikacji tożsamości przyczyni się do zwiększenia poziomu bezpieczeństwa klientów.

16.3. Bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania innych mechanizmów zabezpieczających, takich jak np. weryfikacja miejsca i czasu logowania do elektronicznego kanału dostępu w przypadku usług bankowości elektronicznej świadczonych dla przedsiębiorstw.

Bezpieczeństwo danych i środków klientów

16.4. Poza powyższymi środkami, w celu uniemożliwienia uzyskania nieupoważnionego dostępu do rachunku klienta z wykorzystaniem elektronicznych kanałów dostępu, jak również uniemożliwienia negowania przez klientów zrealizowanych transakcji, systemy informatyczne wykorzystywane w obszarze tych kanałów powinny być zaprojektowane i skonfigurowane w sposób zapewniający odpowiednio wysoki poziom integralności, poufności i dostępności danych dotyczących transakcji (jak również innych danych przetwarzanych z wykorzystaniem tych kanałów) w całym procesie ich przetwarzania (zarówno w ramach banku, jak i przez zewnętrznych dostawców usług). Dodatkowo, bank powinien zapewnić, że:

- posiada zasady nadawania uprawnień do elektronicznych kanałów dostępu oraz system wykrywania przypadków manipulowania transakcjami lub danymi bankowości elektronicznej minimalizujące ryzyko wystąpienia przypadków oszustw wewnętrznych,
- sesje połączeniowe bankowości elektronicznej są szyfrowane oraz wprowadzone są dodatkowe mechanizmy, które w możliwie największym stopniu uodparniają te sesje na manipulacje (np. poprzez zamykanie sesji w przypadku braku aktywności użytkownika przez określony czas lub po zamknięciu aplikacji klienckiej bez wylogowania),
- systemy informatyczne wykorzystywane w zakresie elektronicznych kanałów dostępu umożliwiają zidentyfikowanie i zabezpieczenie dowodów, które mogą zostać wykorzystane w ewentualnym postępowaniu sądowym (w szczególności zminimalizowane jest ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),
- systemy informatyczne wykorzystywane w zakresie elektronicznych kanałów dostępu są zaprojektowane w sposób minimalizujący prawdopodobieństwo przypadkowego zainicjowania transakcji przez upoważnionych użytkowników,
- rozwiązania wykorzystywane w zakresie elektronicznych kanałów dostępu zapewniają bankowi dostęp do ścieżek audytu, w szczególności obejmujących:
  - transakcje,

- otwieranie i zamykanie rachunku klienta,
- zmianę danych klienta,
- wszelkie udzielone klientowi limity i upoważnienia do ich przekroczenia,
- udane i nieudane próby zalogowania do systemów,
- wszelkie przypadki udzielenia, modyfikacji lub cofnięcia uprawnień dostępu do systemów.

16.5. W przypadku, gdy w procesie świadczenia usług za pośrednictwem elektronicznych kanałów dostępu uczestniczą usługodawcy zewnętrzni, bank powinien upewnić się, że posiadają oni właściwe programy zarządzania bezpieczeństwem informacji przetwarzanych na rzecz banku, zgodne z przyjętymi w banku standardami[61].

16.6. O ile obowiązujące przepisy prawa nie dopuszczają w danym przypadku braku zawarcia umowy z klientem elektronicznych kanałów dostępu, umowa taka powinna określać zasady ochrony informacji i szczegółowe warunki dostępu (zwłaszcza metody weryfikacji tożsamości).

16.7. Bank powinien udostępniać klientom kanał komunikacji (np. skrzynkę e-mail, numer telefonu) umożliwiający informowanie banku o zidentyfikowanych przez klientów zdarzeniach dotyczących bezpieczeństwa elektronicznych kanałów dostępu (np. o atakach opartych o technikę *phishing*).

Edukacja klientów

16.8. W związku z tym, że znaczna część kanału świadczenia usług znajduje się poza bezpośrednią kontrolą banku, bank powinien dążyć do zapewnienia klientom korzystającym z elektronicznych kanałów dostępu odpowiedniego poziomu wiedzy pozwalającej na zrozumienie zagrożeń związanych z wykorzystaniem tych kanałów i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Może być to realizowane np. w formie wyraźnie widocznych informacji zamieszczonych na stronach bankowości elektronicznej, poprzez ulotki informacyjne, przesyłane do klientów wiadomości e-mail itp.

16.9. Bank powinien informować klientów o zagrożeniach związanych w szczególności z:

– nieodpowiednim zabezpieczeniem danych wykorzystywanych do logowania do elektronicznych kanałów dostępu,
– nieodpowiednim zabezpieczeniem urządzeń wykorzystywanych do realizacji usług świadczonych za pośrednictwem elektronicznych kanałów dostępu (telefonów komórkowych, komputerów), w tym o istotności stosowania oprogramowania antywirusowego i zapór sieciowych, kontroli fizycznego dostępu, regularnej aktualizacji oprogramowania itp.,
– innymi technikami mającymi na celu przechwycenie informacji umożliwiających dostęp do rachunku (np. poprzez ataki oparte o technikę *phishing*), wraz ze wskazaniem sposobów zabezpieczania się przed takimi technikami.

[61] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".

Zarządzanie oprogramowaniem użytkownika końcowego[62]

17. Rekomendacja 17

Bank powinien posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego, skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.

17.1. Ze względu na zagrożenia związane z wykorzystywaniem oprogramowania użytkownika końcowego (takie jak wysoka podatność na błędy programistyczne, prawdopodobieństwo utraty danych zwykle wyższe niż w przypadku typowych systemów informatycznych, wysoka podatność na ingerencję w zawarte w tych narzędziach algorytmy przetwarzania danych itp.), w zakresie zarządzania tego typu oprogramowaniem bank powinien w szczególności:

- identyfikować istotne oprogramowanie użytkownika końcowego, tj. takie, w którym przetwarzane są dane o wysokiej istotności dla banku lub które ma istotne znaczenie z perspektywy realizowanych w banku procesów,
- dokumentować istotne oprogramowanie użytkownika końcowego, w tym jego role w procesach biznesowych, zakresy przetwarzanych danych, algorytmy przetwarzania danych itp.,
- prowadzić rejestr funkcjonującego w obrębie banku istotnego oprogramowania użytkownika końcowego,
- zapewnić odpowiedni poziom bezpieczeństwa istotnego oprogramowania użytkownika końcowego (np. poprzez ochronę folderów, w których jest ono zapisane, czy też zablokowanie możliwości edycji formularzy) w celu zapobieżenia nieautoryzowanym zmianom, zarówno w samym narzędziu, jak i w przechowywanych w nim danych,
- posiadać sformalizowane zasady tworzenia, testowania i dokonywania zmian w istotnym oprogramowaniu użytkownika końcowego,
- analizować zagrożenia i problemy związane z wykorzystywaniem oprogramowania użytkownika końcowego w poszczególnych obszarach działalności i – w przypadku stwierdzenia istotnych zagrożeń lub problemów w tym zakresie – przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastępowania go przez funkcjonalności istniejących lub nowych systemów informatycznych.

[62] Oprogramowanie użytkownika końcowego (ang. *End-User Computing*, *EUC*) – narzędzia opracowane i funkcjonujące w oparciu o aplikacje instalowane na komputerach osobistych, takie jak MS Excel czy MS Access, dzięki którym użytkownicy niebędący programistami mogą tworzyć aplikacje biznesowe.

VII. Zarządzanie bezpieczeństwem środowiska teleinformatycznego

System zarządzania bezpieczeństwem środowiska teleinformatycznego

18. Rekomendacja 18

W banku powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w banku.

18.1. System zarządzania bezpieczeństwem środowiska teleinformatycznego powinien wynikać ze strategii banku w obszarze bezpieczeństwa środowiska teleinformatycznego i być oparty o sformalizowane regulacje wewnętrzne. Podstawowym dokumentem w tym zakresie powinna być polityka bezpieczeństwa informacji.

18.2. System zarządzania bezpieczeństwem środowiska teleinformatycznego powinien być przedmiotem systematycznych przeglądów, mających na celu wprowadzenie ewentualnych usprawnień oraz uwzględnienie w nim zmian zachodzących zarówno w otoczeniu banku, jak i w jego środowisku wewnętrznym.

18.3. Bank powinien przeanalizować korzyści wynikające ze stosowania międzynarodowych standardów (lub ich polskich odpowiedników) w zakresie bezpieczeństwa informacji (takich jak np. normy z serii ISO/IEC 27000) oraz podjąć decyzję w zakresie ewentualnego dostosowania funkcjonującego w banku systemu zarządzania bezpieczeństwem środowiska teleinformatycznego do ich wymagań.

18.4. Bank powinien zapewnić możliwie ścisłą integrację systemu zarządzania bezpieczeństwem środowiska teleinformatycznego z systemem zarządzania ryzykiem operacyjnym. W tym celu bank powinien m.in. wykorzystywać w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego stosowane narzędzia zarządzania ryzykiem operacyjnym, takie jak narzędzia oparte o czynniki otoczenia gospodarczego i kontroli wewnętrznej[63], samoocena ryzyka operacyjnego, analizy scenariuszowe czy mapy ryzyka.

Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.5. Celem identyfikacji ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego jest określenie związanych z nim zagrożeń mogących spowodować stratę (w tym finansową) w danej instytucji oraz określenie gdzie, w jaki sposób i dlaczego te zagrożenia mogą się zmaterializować.

18.6. Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być dokonywana systematycznie i opierać się na:

[63] Np. liczba incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego w danym okresie sprawozdawczym, liczba istotnych zaleceń z zakresu bezpieczeństwa tego środowiska wydanych przez komórkę audytu wewnętrznego, liczba niezabezpieczonych podatności w istotnych komponentach środowiska teleinformatycznego.

– identyfikacji ryzyka związanego z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń,

– identyfikacji ryzyka związanego z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń.

18.7. Identyfikując ryzyko związane z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń, szczególną uwagę bank powinien poświęcić identyfikacji istniejących podatności środowiska teleinformatycznego (w tym komponentów infrastruktury teleinformatycznej) oraz zagrożeń, które mogą je wykorzystać. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania automatycznych narzędzi pozwalających na identyfikację istniejących podatności. Niezależnie od okresowej oceny, identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być przeprowadzana każdorazowo w przypadku planowania istotnych zmian, zarówno w samych systemach informatycznych[64], jak i w ich wykorzystaniu, a także w przypadku planów wdrożenia nowych technologii (np. płatności wykorzystujących komunikację bliskiego zasięgu[65], bankowości mobilnej, technologii wykorzystujących portale społecznościowe do komunikacji z klientami itp.).

18.8. Identyfikując ryzyko związane z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń, bank powinien gromadzić informacje o zaistniałych w prowadzonej działalności zdarzeniach mających wpływ na bezpieczeństwo przetwarzanych w banku informacji oraz – w przypadku zgodności z przyjętą w banku definicją zdarzenia operacyjnego – uwzględniać je w bazie zdarzeń operacyjnych.

18.9. Zaleca się nawiązanie stałej współpracy z innymi bankami (w szczególności z wykorzystaniem międzybankowych systemów wymiany informacji) w zakresie wymiany informacji o zidentyfikowanych zagrożeniach oraz wniosków i doświadczeń wynikających z analizy zidentyfikowanych przypadków naruszeń bezpieczeństwa środowiska teleinformatycznego. Sposób oraz zakres wymienianych informacji powinny zapewniać ich poufność, w szczególności dochowanie tajemnicy bankowej.

Szacowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.10. Szacowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego ma na celu określenie prawdopodobieństwa i potencjalnego wpływu zmaterializowania się zagrożeń związanych z tym ryzykiem na instytucję oraz – na tej podstawie – dokonanie oceny tego ryzyka.

18.11. Działania w zakresie szacowania ryzyka powinny być realizowane z uwzględnieniem klasyfikacji informacji i systemów informatycznych[66]. Badanie wpływu zidentyfikowanych zagrożeń powinno obejmować również elementy powiązane z komponentem, dla którego zidentyfikowano dane zagrożenie. W wyniku przeprowadzenia szacowania ryzyka bank

[64] Patrz też: sekcja „Rozwój systemów informatycznych”.
[65] NFC – ang. *Near Field Communication*.
[66] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

powinien uzyskać wiedzę na temat występujących w jego działalności zagrożeń związanych z bezpieczeństwem środowiska teleinformatycznego, prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń oraz możliwych skutków zmaterializowania się tych zagrożeń, z uwzględnieniem potencjalnej utraty reputacji, która może prowadzić do spadku zaufania klientów i zakończenia przez nich współpracy z bankiem, co w szczególności może mieć wpływ na sytuację płynnościową banku. Wiedza ta powinna pozwolić na podjęcie właściwych decyzji w zakresie kontroli i przeciwdziałania ryzyku.

Kontrola i przeciwdziałanie ryzyku w zakresie bezpieczeństwa środowiska teleinformatycznego

18.12. Uwzględniając wyniki dokonanego oszacowania ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego, bank powinien podejmować stosowne decyzje dotyczące podejścia do poszczególnych zagrożeń, polegające na:

- ograniczaniu ryzyka, tj. wprowadzaniu i modyfikacji istniejących organizacyjnych i technicznych mechanizmów kontrolnych w zakresie bezpieczeństwa środowiska teleinformatycznego,
- transferze ryzyka, tj. przeniesieniu części lub całości ryzyka związanego z danym zagrożeniem na podmiot zewnętrzny[67], w szczególności poprzez zlecanie wykonywania czynności zewnętrznym dostawcom usług[68] lub stosowanie ubezpieczeń,
- unikaniu ryzyka, tj. niepodejmowaniu działań, z którymi wiąże się dane zagrożenie,
- akceptacji ryzyka, tj. świadomym niepodejmowaniu działań mających na celu ograniczenie prawdopodobieństwa lub skutków zmaterializowania się danego zagrożenia, wraz z ewentualnym zapewnieniem środków na pokrycie potencjalnie związanych z nim strat.

18.13. Stosowane mechanizmy kontrolne powinny być adekwatne w szczególności do:

- zidentyfikowanych zagrożeń, oszacowanego ryzyka wynikającego z tych zagrożeń oraz istotności związanych z nimi komponentów środowiska teleinformatycznego, w szczególności systemów informatycznych[69],
- skali i specyfiki działalności banku,
- złożoności środowiska teleinformatycznego banku.

18.14. Bank powinien zapewnić, aby wszystkie wyjątki od obowiązujących w banku regulacji oraz stosowanych mechanizmów kontrolnych były ewidencjonowane i kontrolowane zgodnie ze sformalizowaną procedurą, określającą m.in. sytuacje, w jakich dopuszcza się udzielenie zgody na odstępstwo, zasady składania i akceptacji wniosku o udzielenie takiej zgody (z zapewnieniem, że wniosek zawiera uzasadnienie potrzeby zastosowania wyjątku), osoby upoważnione do udzielenia zgody, akceptowalny czas obowiązywania odstępstw oraz zasady

[67] Bank nie może jednak traktować transferu ryzyka jako alternatywy dla właściwego zarządzania ryzykiem.
[68] Patrz: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[69] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".

raportowania w tym zakresie. Bank powinien również systematycznie analizować ryzyko związane z ww. odstępstwami.

18.15. Bank powinien regularnie weryfikować, czy przyjęte mechanizmy kontrolne są adekwatne do jego profilu ryzyka, a sposób ich funkcjonowania jest prawidłowy. W przypadku zaistnienia takiej konieczności (np. w przypadku stwierdzenia, że zasoby wewnętrzne banku nie są wystarczające w danym zakresie), bank powinien wykorzystać w tym celu zewnętrznych specjalistów, mając jednak na uwadze konieczność zachowania przez nich poufności informacji pozyskanych w związku z wykonywaną kontrolą.

18.16. Kontrola ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być sprawowana adekwatnie do poziomu tego ryzyka niezależnie od tego, czy związane jest ono z przetwarzaniem danych klientów banku (lub prowadzeniem innych operacji w ramach działalności bankowej lub handlowej), czy też z przetwarzaniem danych dla zewnętrznych podmiotów (np. w przypadku, gdy bank pełni rolę depozytariusza TFI).

Monitorowanie i raportowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.17. Wyniki identyfikacji i szacowania ryzyka w zakresie środowiska teleinformatycznego oraz rezultaty badania efektywności wprowadzonych mechanizmów kontrolnych powinny być monitorowane (w tym pod kątem występujących trendów), jak również prezentowane kierownictwu banku i radzie nadzorczej w ramach funkcjonującego w banku systemu informacji zarządczej[70]. Informacje te powinny być przekazywane regularnie, zaś ich częstotliwość i zakres powinny uwzględniać profil ryzyka banku oraz dawać możliwość podjęcia odpowiedniej reakcji.

Klasyfikacja informacji i systemów informatycznych

19. Rekomendacja 19

Bank powinien klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa.

Klasyfikacja informacji

19.1. Bank powinien opracować zasady klasyfikacji informacji zapewniające, że każda informacja przetwarzana w środowisku teleinformatycznym banku zostanie objęta odpowiednim dla niej poziomem ochrony. W tym celu niezbędne jest ustanowienie takiego systemu klasyfikacji informacji, który będzie obejmował wszystkie dane przetwarzane w systemach informatycznych banku, jak również zapewnienie, że klasyfikacja każdej informacji jest adekwatna do aktualnych uwarunkowań wewnętrznych i zewnętrznych banku.

19.2. Informacje powinny być klasyfikowane pod kątem wymaganego poziomu bezpieczeństwa z uwzględnieniem w szczególności:

– znaczenia tych informacji dla banku i realizowanych w nim procesów,

[70] Patrz też: sekcja „System informacji zarządczej”.

– znaczenia tych informacji z perspektywy zarządzania rodzajami ryzyka, które zostały zidentyfikowane jako istotne w prowadzonej przez bank działalności,
– skutków utraty lub nieuprawnionej zmiany danej informacji,
– skutków nieuprawnionego ujawnienia danej informacji,
– szczególnych wymagań regulacyjnych i prawnych dotyczących danego rodzaju informacji[71].

19.3. Klasyfikacja każdej informacji powinna być uwzględniana w ramach określania mechanizmów zabezpieczających te informacje w całym cyklu ich przetwarzania – od pozyskania, poprzez wykorzystanie, ewentualne przekazywanie poza bank, aż do momentu archiwizacji oraz usunięcia.

19.4. Dostęp do informacji o wysokim stopniu poufności powinien być udzielany jedynie osobom, w stosunku do których bank stwierdzi w świetle obowiązujących przepisów prawa dopuszczalność udzielenia dostępu do takich informacji. Ponadto, każda osoba, której bank udziela dostępu do informacji o wysokim stopniu poufności, powinna zostać zobligowana do podpisania zobowiązania w zakresie zachowania ich poufności (również przez odpowiedni czas po ustaniu tego dostępu), przy czym zasada ta nie znajduje zastosowania w przypadkach, gdy powszechnie obowiązujące przepisy prawa nakładają obowiązek udzielenia takiego dostępu.

19.5. Przechowywanie informacji o istotnym znaczeniu dla banku na komputerach stacjonarnych, komputerach przenośnych lub urządzeniach mobilnych powinno być ograniczone do niezbędnego minimum i chronione adekwatnie do klasyfikacji tych informacji (np. poprzez szyfrowanie, mechanizmy kontroli dostępu, mechanizmy zapewniające możliwość odzyskiwania danych).

19.6. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania rozwiązań automatyzujących działania w zakresie kontroli ryzyka związanego z bezpieczeństwem informacji przetwarzanych w środowisku teleinformatycznym, takich jak np. rozwiązania ograniczające użytkownikom systemów informatycznych możliwość zapisu informacji na przenośnych nośnikach danych, umożliwiające sprawowanie kontroli nad informacjami przesyłanymi za pośrednictwem poczty elektronicznej oraz ograniczające dostęp do innych niż przyjęte w banku systemów poczty elektronicznej. Należy jednak pamiętać, że wykorzystanie tego rodzaju automatycznych rozwiązań nie zwalnia banku z konieczności sprawowania przez pracowników nadzoru nad tym obszarem.

[71] Patrz też: sekcja „Bezpieczeństwo formalno-prawne”.

Klasyfikacja systemów informatycznych

19.7. Bank powinien opracować zasady klasyfikacji systemów informatycznych, uwzględniające w szczególności:

– klasyfikację informacji przetwarzanych w obrębie danego systemu,

– znaczenie danego systemu dla działalności banku,

– istotność innych systemów informatycznych, których funkcjonowanie zależy od danego systemu.

Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego

20. Rekomendacja 20

Bank powinien posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.

20.1. Bank powinien posiadać regulacje wewnętrzne opisujące zasady postępowania w przypadkach wystąpień incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, czyli m.in. awarii i przeciążeń systemów informatycznych, utraty urządzeń lub danych, błędów ludzkich skutkujących zagrożeniem dla bezpieczeństwa środowiska teleinformatycznego, naruszeń lub prób naruszeń zabezpieczeń, niekontrolowanych zmian w systemach itp. Zakres i poziom szczegółowości powyższych regulacji powinny być adekwatne do skali i specyfiki działalności banku oraz poziomu złożoności jego środowiska teleinformatycznego.

20.2. Zasady postępowania z incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego powinny w szczególności określać:

– metody i zakres zbierania informacji o incydentach,

– zakresy odpowiedzialności w obszarze zarządzania incydentami,

– sposób przeprowadzania analiz wpływu incydentów na środowisko teleinformatyczne, w tym jego bezpieczeństwo,

– zasady kategoryzacji i priorytetyzacji incydentów, uwzględniające klasyfikację informacji i systemów informatycznych związanych z danym incydentem[72],

– zasady wykrywania zależności pomiędzy incydentami (przykładem tego rodzaju zależności jest atak typu „*Denial-of-Service*" uniemożliwiający szybką identyfikację innego incydentu lub usunięcie jego przyczyn),

– zasady komunikacji, obejmujące zarówno pracowników banku, jak i zewnętrznych dostawców usług oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich (klientów, kontrahentów itp.), zapewniające

[72] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".

odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu,

– zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych (w szczególności minimalizujące ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),

– zasady dotyczące podejmowania działań naprawczych i zapobiegawczych, obejmujące w szczególności przypisanie osób odpowiedzialnych za realizację tych działań oraz monitorowanie stanu ich realizacji.

20.3. W celu m.in. umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów, bank powinien prowadzić rejestr incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, w którym przechowywane powinny być w szczególności informacje dotyczące:

– daty wystąpienia i identyfikacji incydentu,

– przyczyn zajścia incydentu,

– przebiegu incydentu,

– skutków incydentu,

– podjętych działań naprawczych.

20.4. Bank powinien zapewnić, aby wszyscy pracownicy oraz inne osoby świadczące usługi na rzecz banku, które mają dostęp do jego środowiska teleinformatycznego, były poinformowane o zasadach dotyczących zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego w zakresie odpowiednim do wykonywanych czynności i posiadanych uprawnień. W szczególności osoby te powinny być zobowiązane do zgłaszania incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego (w tym podejrzeń wystąpienia takich incydentów) możliwie najszybciej. W tym celu bank powinien ustanowić odpowiedni punkt kontaktowy (np. w ramach jednostek odpowiedzialnych za wsparcie użytkowników systemów informatycznych) dedykowany obsłudze zgłoszeń w powyższym zakresie, który będzie powszechnie znany w organizacji, stale dostępny oraz pozwoli na zapewnienie odpowiedniego czasu reakcji. Osoby odpowiedzialne za obsługę zgłoszeń powinny posiadać kwalifikacje i wiedzę zapewniające właściwą klasyfikację każdego zgłoszenia i podjęcie odpowiednich działań związanych z ich obsługą lub eskalacją, tj. przekazaniem do obsługi przez osoby o wyższym poziomie kompetencji w danym zakresie (w szczególności na podstawie klasyfikacji informacji lub systemów informatycznych, z którymi związany jest dany incydent[73]).

20.5. Zaleca się, aby w stosunku do incydentów mających istotny wpływ na bezpieczeństwo przetwarzanych danych, w tym w szczególności na bezpieczeństwo środków klientów (również w przypadkach incydentów, o których bank jest informowany przez zewnętrznego

[73] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

dostawcę usług[74]), bank posiadał szybką ścieżkę raportowania ich wystąpienia (wraz z określeniem prawdopodobnych przyczyn oraz skutków) wysokiemu szczeblowi kierownictwa banku. Szybki przepływ informacji w zakresie zaistniałego istotnego naruszenia bezpieczeństwa powinien pozwalać na odpowiednie zaangażowanie kierownictwa banku w proces podejmowania działań naprawczych. Kierownictwo banku powinno być również systematycznie informowane o stanie realizacji tych działań.

20.6. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą określenia składu osobowego zespołów, które odpowiedzialne będą za podjęcie odpowiedniej reakcji w przypadkach wystąpienia incydentów mających istotny wpływ na bezpieczeństwo przetwarzanych danych (w szczególności na bezpieczeństwo środków klientów), posiadających odpowiednie kwalifikacje i wiedzę w tym zakresie oraz dysponujących uprawnieniami umożliwiającymi podejmowanie skutecznych działań w nagłych okolicznościach.

20.7. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania rozwiązań klasy SIEM (ang. *Security Information and Event Management*), ułatwiających zarządzanie incydentami naruszenia bezpieczeństwa m.in. poprzez centralizację zbierania, analizowania i przechowywania dzienników zdarzeń generowanych przez systemy informatyczne i inne komponenty środowiska teleinformatycznego.

Bezpieczeństwo formalno-prawne

21. Rekomendacja 21

Bank powinien zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami.

21.1. Bank powinien systematycznie identyfikować i dokumentować oraz monitorować zgodność z wymaganiami dotyczącymi obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego (również w zakresie działalności zleconej zewnętrznym dostawcom usług[75]) wynikającymi z obowiązujących przepisów prawa, regulacji wewnętrznych i zewnętrznych, zawartych umów i przyjętych w banku standardów, w tym m.in.:

– ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376 j.t. z późn. zm.),

– ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2009 r. Nr 152, poz. 1223 j.t. z późn. zm.),

[74] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[75] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".

- ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. Nr 46, poz. 276 j.t. z późn. zm.),
- ustawy z dnia 14 grudnia 1994 r. o Bankowym Funduszu Gwarancyjnym (Dz. U. z 2009 r. Nr 84, poz. 711 j.t. z późn. zm.),
- ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 j.t. z późn. zm.),
- ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228 z późn. zm.),
- ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 j.t. z późn. zm.) oraz umów i licencji w zakresie eksploatowanego oprogramowania,
- ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z 2012 r. poz. 1232 j.t. z późn. zm.),
- aktów wykonawczych w zakresie powyższych ustaw,
- regulacji nadzorczych.

21.2. Spełnienie powyższych wymagań powinno być przedmiotem raportowania w ramach systemu informacji zarządczej[76].

Rola audytu wewnętrznego i zewnętrznego

22. Rekomendacja 22

Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być przedmiotem systematycznych, niezależnych audytów.

22.1. Bank powinien przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą powołania w ramach audytu wewnętrznego jednostki odpowiedzialnej za audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego. W przypadku banków spółdzielczych dopuszczalne jest, aby funkcje w tym zakresie pełnione były przez audytorów z banku zrzeszającego.

22.2. Osoby odpowiedzialne za przeprowadzanie audytów obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny posiadać odpowiednie kwalifikacje. Audyty powinny być przeprowadzane z wykorzystaniem uznanych standardów międzynarodowych i dobrych praktyk w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, jak np.:

- standardy dotyczące audytowania systemów informatycznych ISACA (Information Systems Audit and Control Association),
- COBIT (Control Objectives for Information and related Technology),

[76] Patrz też: sekcja „System informacji zarządczej”.

– GTAG (Global Technology Audit Guide) oraz GAIT (Guide to the Assessment for IT Risk),

– normy ISO (International Organization for Standardization).

22.3. Audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinien być przeprowadzany regularnie oraz każdorazowo po wprowadzeniu zmian mogących znacząco wpłynąć na poziom bezpieczeństwa środowiska teleinformatycznego. Częstotliwość i zakres audytów powinny wynikać z poziomu ryzyka związanego z poszczególnymi obszarami audytowymi oraz wyników ich wcześniejszych przeglądów.

22.4. Zlecanie dodatkowych audytów profesjonalnym instytucjom zewnętrznym specjalizującym się w badaniu obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego jest czynnikiem, który może wzmocnić w istotny sposób kontrolę nad ryzykiem związanym z tym obszarem. W związku z tym, bank powinien przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uzupełnienia działań audytu wewnętrznego przez audyty zewnętrzne przeprowadzane przez tego rodzaju podmioty, w szczególności w zakresie obszarów o wysokim poziomie ryzyka.

Opracowano w:

Departamencie Inspekcji Bankowych, Instytucji Płatniczych
i Spółdzielczych Kas Oszczędnościowo-Kredytowych UKNF