NARODOWY BANK POLSKI

KOMISJA NADZORU BANKOWEGO

Generalny Inspektorat Nadzoru Bankowego

REKOMENDACJA D

dotycząca

zarządzania ryzykami
towarzyszącymi systemom informatycznym i telekomunikacyjnym
używanym przez banki

Tekst zaktualizowany

Warszawa, 2002 r.

I. DEFINICJE I PRZYDATNE SŁOWNICTWO[1]:

1. **aplikacja –** program komputerowy wykonujący złożone zadania określonego rodzaju – przetwarzanie danych (wprowadzanie, przechowywanie, aktualizacje lub wyszukiwanie danych);

2. **audyt bezpieczeństwa systemu** * **–** dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką bezpieczeństwa i z procedurami operacyjnymi oraz w celu wykrycia przełamań bezpieczeństwa i zalecenia wskazanych zmian w środkach nadzorowania, polityce bezpieczeństwa oraz w procedurach;

3. **audyt systemu informatycznego*** **-** sprawdzanie procedur stosowanych w systemie przetwarzania danych w celu oceny ich skuteczności i poprawności oraz w celu zalecenia ulepszeń;

4. **bankowość elektroniczna –** dostarczanie bankowych usług i produktów w dowolnym miejscu i czasie za pomocą elektronicznych kanałów dystrybucji przy użyciu powszechnie stosowanych urządzeń elektronicznych (takich jak: komputer, telefon, telewizor-platforma cyfrowa lub innych dostarczanych przez usługodawcę);

5. **dostępność*** **-** właściwość danych lub zasobów polegająca na tym, że mogą być one dostępne i wykorzystywane na żądanie uprawnionej jednostki;

6. **elektroniczne kanały dystrybucji –** Internet, sieci MAN, sieci WAN, sieci telefoniczne, sieci telewizyjne itp.;

7. **firewall –** zabezpieczenie fizyczne lub logiczne chroniące przed nieupoważnionym dostępem oraz kontrolujące przepływ informacji pomiędzy sieciami, w szczególności pomiędzy sieciami wewnętrznymi (banku, jednostki organizacyjnej banku), a zewnętrznymi (Internet);

8. **hacker –** osoba wykorzystująca słabości i luki zabezpieczeń oraz błędy w oprogramowaniu w celu uzyskania nieautoryzowanego dostępu do systemu informatycznego;

9. **integralność danych*** **-** właściwość polegająca na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób

10. **integralność systemu*** **-** właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej

11. **Internet-** ogólnoświatowa sieć operująca protokołem IP, łącząca rozsiane po świecie lokalne komputery agencji i instytucji edukacyjnych, badawczych rządowych, przemysłowych i prywatnych;

[1] Definicje słownictwa oznaczonego * zaczerpnięto z PN-ISO/IEC 2382-8 i PN-I-02000.

12. **karta smart –** karta „inteligentna”, którą można programować, najczęściej z mikroprocesorem (chipem) , wykorzystywana przeważnie do autoryzacji;

13. **władze banku -** Zarząd, Rada Banku;

14. **kryptografia*** **–** dyscyplina, która obejmuje zasady, środki i metody przekształcania danych w celu ukrycia ich zawartości semantycznej, zapobiegania ich nieuprawnionemu wykorzystaniu lub zapobiegania ich niewykrywalnej modyfikacji;

15. **nośnik danych –** dysk, dyskietka, taśma, CD, itp.;

16. **oprogramowanie (software) –** program lub zestaw programów pozwalający na wykonywanie przez komputer określonych zadań. Obejmuje programy, które na różnym poziomie sterują działaniem komputera (system operacyjny, programy użytkowe, aplikacje);

17. **plan awaryjny*** **-** określenie wszystkich działań, które powinny być podjęte przed, podczas i po awarii systemu łącznie z udokumentowanymi, przetestowanymi procedurami, których realizacja zapewni dostępność krytycznych systemów informatycznych i ułatwi utrzymanie ciągłości działania;

18. **poufność*** **–** właściwość danych, wskazująca obszar, w którym te dane nie powinny być dostępne lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom;

19. **sieć (net, network) –** układ komputerów i urządzeń końcowych (np. drukarki) połączony ze sobą łączami komunikacyjnymi umożliwiającymi wymianę komunikatów pomiędzy nimi;

20. **sniffer –** analizator sieciowy - program służący do przechwytywania i analizy pakietów danych przesyłanych w sieci;

21. **spoof - spoofing*** **–** zwodzenie, podjęcie działań zmierzających do oszukania użytkownika, obserwatora (takiego jak podsłuchujący) lub zasobu;

22. **system informatyczny –** program lub zbiór programów i funkcji, zarządzający zasobami oraz umożliwiający wykorzystanie tych zasobów przez użytkowników. Wyróżniamy systemy operacyjne, systemy baz danych, systemy użytkowe;

23. **system telekomunikacyjny –** zespół urządzeń telekomunikacyjnych współpracujących ze sobą w celu spełnienia określonego zadania.

24. **szyfrowanie*** **–** kryptograficzne przekształcenie danych.

II. WSTĘP

Poniższa rekomendacja zastąpiła „Rekomendację D z dnia 20 października 1997r. dotyczącą zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki".

Obserwowany w ostatnich latach szybki rozwój w dziedzinie systemów informatycznych i telekomunikacyjnych, a zwłaszcza szybki rozwój Internetu i rosnąca akceptacja do wykorzystywania tego medium jako kanału dystrybucji produktów i usług bankowych, stawiają przed bankami nowe wyzwania w zakresie prac związanych z rozwojem własnych systemów przetwarzania danych, a szczególnie ich solidnością i niezawodnością.

Ciągłe innowacje technologiczne i konkurencja pomiędzy istniejącymi i wchodzącymi na rynek organizacjami bankowymi, umożliwiły klientom detalicznym i hurtowym dostęp do znacznie szerszego zakres usług i produktów bankowych oraz ich dostarczanie poprzez elektroniczny kanał dystrybucji, nazywany powszechnie bankowością elektroniczną. Jednak szybki rozwój możliwości bankowości elektronicznej niesie ze sobą zarówno korzyści jak i ryzyka. Bankowość elektroniczna stała się częścią systemów informatycznych banków.

Banki zawsze narażone były na ryzyko błędów i oszustw, ale skala tego ryzyka i szybkość z jaką mogą te zjawiska obecnie wystąpić, zwiększyła się wydatnie wraz z rozwojem komputerowego przepływu środków pieniężnych, który odbywa się w skali całego świata.

Profil ryzyka każdego banku jest inny i wymaga dostosowania metody jego redukcji do skali zastosowań systemów informatycznych i operacji bankowości elektronicznej, istotności występujących ryzyk oraz woli i zdolności banków do zarządzania tymi ryzykami. Oznacza to, że metoda „jednego rozmiaru dla wszystkich" w zagadnieniach zarządzania ryzykiem w systemach informatycznych i bankowości elektronicznej może nie być odpowiednia.

Rodzaje ryzyka występujące w systemach informatycznych i w bankowości elektronicznej są generalnie takie same, jak wchodzące w grę w ukształtowanych wcześniej strukturach. Jednak w porównaniu z systemami ręcznymi, w systemie elektronicznego przetwarzania danych szczególne ryzyko rodzi możliwość bezprawnego ujawnienia, modyfikacji lub usunięcia większej ilości, materialnie istotniejszych informacji, w bardziej wygodny i metodologicznie dostępny sposób (np. kopie na nośnikach danych) bez pozostawienia śladów nie autoryzowanego dostępu. Szczególnej uwagi wymaga także zagadnienie zapewnienia właściwej dostępności tego typu systemów.

Zarządzanie ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym, w przedstawionej rekomendacji, zostało podzielone na cztery ogólne zagadnienia:1. Rola kierownictwa banku w zarządzaniu bezpieczeństwem systemów informatycznych , 2. Mechanizmy kontroli bezpieczeństwa, 3. Zarządzanie ryzykami, 4. Audyt informatyczny i nadzór.

Przedstawiona rekomendacja zawiera w swojej treści zalecenia Bazylejskiego Komitetu ds. Nadzoru Bankowego dotyczące zasad zarządzania ryzykiem w bankowości elektronicznej.

III. ROLA WŁADZ BANKU W ZARZĄDZANIU BEZPIECZEŃSTWEM SYSTEMÓW INFORMATYCZNYCH

A. NADZÓR

Władze banku w ramach wypełniania swoich funkcji są odpowiedzialne za opracowywanie strategii banku, w tym strategii w zakresie rozwoju i eksploatacji systemów informatycznych i sieci.

Technologia informatyczna jest podstawą funkcjonowania współczesnego banku. Systemy informatyczne i sieci są bazą dla systemu informacyjnego. Bank jest w stanie realizować swoją strategię i założone cele tylko wtedy, gdy strategia rozwoju informatyki jest spójna z ogólną strategią rozwoju banku. Prawidłowe i efektywne zarządzanie obszarem informatyki umożliwia niezawodne funkcjonowanie systemów informatycznych i telekomunikacyjnych oraz wzmacnia bezpieczeństwo banku i klientów.

Wraz z rozwojem banku rosną wymagania wobec systemów informatycznych i umiejętności pracowników. Dla efektywnego zarządzania niezbędne staje się uniezależnienie obsługi klienta od miejsca lokalizacji rachunku (tzw. odmiejscowienie rachunku).
Do władz banku należy decyzja o wyborze scentralizowanej lub rozproszonej architektury systemu informatycznego. Władze banku są odpowiedzialne za decyzję czy bank będzie świadczył usługi bankowości elektronicznej. W szczególności, władze banku powinny upewnić się, czy plany dotyczące bankowości elektronicznej są wyraźnie zintegrowane ze strategicznymi celami banku oraz czy jest prowadzona analiza ryzyka w zakresie elektronicznej działalności bankowej, czy ustanowione są odpowiednie procesy redukowania i monitorowania zidentyfikowanych ryzyk.

Ponadto, władze banku powinny upewniać się, czy prawidłowo są oceniane i uwzględniane aspekty ryzyka operacyjnego. Dostarczanie usług bankowych poprzez Internet może w istotny sposób zmodyfikować i/lub nawet zwiększyć tradycyjne ryzyka bankowe (np. ryzyko strategiczne, ryzyko reputacji, ryzyko operacyjne, kredytowe i płynności). Z tego względu należy podjąć działania służące zapewnieniu właściwej oceny i wprowadzeniu odpowiednich zmian do istniejących procedur zarządzania ryzykiem w banku, kontroli bezpieczeństwa, należytej staranności i kontroli w zakresie zlecania usług na zewnątrz w celu ich dostosowania do usług bankowości elektronicznej.

Władze banku powinny ustanowić efektywną kontrolę zarządczą ryzyk związanych z systemami informatycznymi, w tym ustanowić polityki i inne, bardziej szczegółowe regulacje służące zarządzaniu tymi ryzykami.

Bank nie powinien stosować nowych technologii informatycznych bez posiadania wiedzy umożliwiającej zarządzanie związanymi z nimi ryzykami.

Władze banku powinny zapewnić integrację procesów zarządzania ryzykiem w systemach informatycznych z procesami zarządzania ryzykiem w skali całego banku. Należy oceniać aktualną politykę i procesy zarządzania ryzykiem w celu upewnienia się, że są one wystarczająco sprawne, aby uwzględnić nowe ryzyka wynikające z prowadzonej lub planowanej działalności bankowości elektronicznej. Dodatkowe działania w zakresie zarządzania ryzykiem, które powinny być rozważone, obejmują:

- precyzyjne określenie akceptowanego przez bank poziomu ryzyka w zakresie systemów informatycznych,
- ustanowienie podstawowych upoważnień i mechanizmów podległości, w tym w odniesieniu do procedur zgłaszania przypadków wystąpienia incydentów wpływających na bezpieczeństwo, kondycję finansową lub reputację banku (np. przypadków penetracji sieci, złamania zasad bezpieczeństwa przez pracowników oraz wszelkich poważnych przypadków niewłaściwego użycia sprzętu komputerowego),
- uwzględnienie unikalnych czynników ryzyka związanych z zapewnieniem bezpieczeństwa, integralności i dostępności produktów i usług bankowości elektronicznej oraz wymaganie, aby strony trzecie, którym banki zleciły sprawy podstawowych systemów lub aplikacji, podejmowały te same kroki.

Wiążące się z bankowością elektroniczną zwiększone ryzyko reputacji powoduje konieczność czujnego monitorowania zdolności funkcjonowania systemu i poziomu zadowolenia klientów, jak również konieczność zgłaszania ewentualnych incydentów do władz banku.

W zależności od zakresu i złożoności elektronicznej działalności bankowej, będą występowały różnice co do zakresu i struktury programów zarządzania ryzykiem w organizacjach bankowych. Zasoby wymagane do kontroli usług bankowości elektronicznej powinny odpowiadać poziomowi ryzyka z nimi związanymi.

W świetle unikalnych cech bankowości elektronicznej, nowe projekty w zakresie bankowości elektronicznej, które mogą wywrzeć istotny wpływ na profil ryzyka i strategię banku powinny być poddawane odpowiednim analizom strategicznym i analizom kosztów/korzyści. Bez dokonywania analizy strategicznej i ciągłych ocen wyników w relacji do planu, występuje ryzyko niedoszacowania kosztów i/lub przeszacowania zysków wynikających z podejmowanych przez banki inicjatyw w zakresie bankowości elektronicznej.

Z uwagi na rodzaj działalności banku jako instytucji publicznego zaufania, znaczną ilość informacji przetwarzanych w systemach informatycznych charakteryzować będzie wysoki stopień wrażliwości na utratę lub ujawnienie. Należy dokonać określenia stopnia poufności wszystkich rodzajów informacji przetwarzanych w systemach informatycznych, a w szczególności wskazać, które informacje i w jakim okresie powinny podlegać bez względu na formę absolutnemu zakazowi publikacji (czasowe embargo na niektóre informacje). Niezbędne jest również precyzyjne określenie zasad obowiązujących przy przekazywaniu danych.

Prawidłowy nadzór ze strony władz banku ma podstawowe znaczenie dla zapewnienia efektywnych wewnętrznych mechanizmów kontroli elektronicznej działalności bankowej. Oprócz

szczególnych cech internetowego kanału dystrybucji, znaczne wyzwanie dla tradycyjnych procesów zarządzania ryzykiem stanowią następujące aspekty bankowości elektronicznej:

- Główne elementy kanału dostarczania usług (kanały elektroniczne i związane z nim technologie – Internet, GSM, WAP) znajdują się poza zasięgiem bezpośredniej kontroli banku.
- Internet zapewnia dostarczanie usług do wielu krajowych jurysdykcji, włącznie z tymi, które nie są obecnie obsługiwane przez fizyczne placówki banku.
- Ze względu na złożoność zagadnień związanych z bankowością elektroniczną, jak również wysoce techniczny język i pojęcia, kwestie związane z tą działalnością pozostają w wielu przypadkach poza tradycyjnym doświadczeniem kierownictwa banku.

B. POLITYKA W ZAKRESIE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Kierownictwo banku odpowiada za stworzenie i realizację polityki bezpieczeństwa.

Odpowiedzialność za zabezpieczenie systemów informatycznych przed narażeniem na różnego typu ryzyko, związana jest instytucjonalnie z procesem zarządzania. Kierownictwo banku odpowiedzialne jest za bezpieczeństwo systemów informatycznych i sieci w każdej jednostce organizacyjnej banku.

Zapewnienie poufności, integralności i dostępności danych wymaga opracowania odpowiednich procedur i zasad kontroli ich realizacji.

Kierownictwo banku powinno nadzorować opracowanie, w formie pisemnej, procedur i zasad kontroli bezpieczeństwa zapewniających prawidłowe zabezpieczenie systemów informatycznych i danych (ze szczególnym uwzględnieniem bankowości elektronicznej) przed zagrożeniami wewnętrznymi i zewnętrznymi, pozwalających na zminimalizowanie prawdopodobieństwa wystąpienia negatywnych zdarzeń. Nadzór ten powinien obejmować nadawanie uprawnień, mechanizmy kontroli dostępu fizycznego i elektronicznego oraz adekwatną infrastrukturę zabezpieczającą, służącą zachowaniu odpowiednich ograniczeń dotyczących działań wewnętrznych i zewnętrznych użytkowników.

W celu zapewnienia odpowiednich systemów kontroli bezpieczeństwa, kierownictwo banku musi ustalić, czy bank posiada wszechstronny proces zabezpieczeń, w tym odpowiednią politykę i procedury, uwzględniające potencjalne wewnętrzne i zewnętrzne zagrożenia bezpieczeństwa. Dotyczy to zarówno zapobiegania incydentom, jak i odpowiedniego na nie reagowania.

Kierownictwo banku odpowiedzialne jest za stworzenie polityki bezpieczeństwa i zapewnienie stałego nadzoru nad jej realizacją.

Dla wypracowania i zatwierdzenia zasad polityki bezpieczeństwa zalecane jest wyłonienie spośród najwyższego szczebla kierownictwa banku stosownego komitetu. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek Zarządu banku.

Opracowana polityka powinna określać następujące, podstawowe elementy efektywnego procesu zabezpieczenia systemów informatycznych:

- obowiązki kierownictwa banku / pracowników w zakresie kontroli opracowywania i przestrzegania polityki bezpieczeństwa,

- odpowiednie zabezpieczenia fizyczne, zapobiegające dostępowi osób nieupoważnionych do sprzętu komputerowego, a szczególną uwagę należy zwrócić na właściwą lokalizację centrum komputerowego,
- odpowiednie zabezpieczenia elektroniczne oraz procesy monitorowania dostępu, zapobiegające wewnętrznemu i zewnętrznemu nieupoważnionemu dostępowi do systemów operacyjnych, aplikacji i baz danych,
- regularne analizowanie i testowanie środków i mechanizmów kontroli bezpieczeństwa, w tym ciągłe śledzenie nowych rozwiązań i trendów w zakresie zabezpieczeń oraz instalowanie odpowiednich nowych wersji oprogramowania, pakietów usług i innych wymaganych środków,
- zasady postępowania dotyczące zapewnienia zgodności systemów informatycznych z aktualnie obowiązującymi przepisami.

Ustalona i obowiązująca w banku polityka zabezpieczeń systemów informatycznych, określająca organizacyjne zasady planowania i eksploatacji zabezpieczeń, powinna mieć najwyższą rangę i być dostępna dla wszystkich pracowników odpowiedzialnych za bezpieczeństwo informacji.

Celem zabezpieczenia systemu informatycznego jest zapewnienie poufności, integralności i dostępności zasobów, pozwalające na przetwarzanie, przesyłanie i przechowywanie danych systemowych, zapewnienie ewidencji podejmowanych działań, autentyczności użytkowników oraz niezawodności systemu.

Dla zapewnienia bezpiecznego wykonywania przetwarzania informacji w banku niezbędne jest opracowanie właściwie udokumentowanych procedur i określenie zakresów odpowiedzialności. Procedury te, napisane w sposób jasny i zrozumiały, powinny obejmować swoim zakresem:

- wszystkie aplikacje funkcjonujące w banku,
- zasady tworzenia, testowania i wdrażania nowych aplikacji,
- zasady i sposób właściwego przechowywania zbiorów danych oraz ich archiwizowania, jak również udostępniania danych,
- postępowanie w przypadku wykrycia błędów,
- wykorzystanie systemów wspomagających w przypadku wystąpienia problemów technicznych,
- sposób postępowania w przypadku załamania się pracy systemu (proces odtworzenia).

Dla zapewnienia bezpiecznego dostępu do aplikacji i baz danych należy tworzyć i utrzymywać profile bezpieczeństwa. Dotyczy to także konkretnych przywilejów autoryzacji przyznawanych wszystkim użytkownikom systemów informatycznych i aplikacji bankowości elektronicznej, w tym wszystkim klientom, wewnętrznym użytkownikom bankowym oraz usługodawcom, którym zlecono usługi. W celu wsparcia właściwego podziału obowiązków należy opracować także mechanizmy kontroli dostępu elektronicznego. Bank może się zdecydować na ustanowienie scentralizowanego lub zdecentralizowanego systemu praw dostępu. Na przykład, może istnieć tylko jedna jednostka autoryzująca, odpowiedzialna za przyznawanie praw dostępu konkretnym osobom, grupom lub funkcjom w ramach banku. Może też istnieć szereg jednostek autoryzujących, realizujących różne potrzeby w ramach różnych pionów

organizacyjnych. Należy mieć na uwadze, że w przypadku istnienia wielu jednostek autoryzujących w banku, ich działania mogą nie być spójne.

Dane i systemy informatyczne powinny być klasyfikowane zgodnie z ich wrażliwością i znaczeniem oraz odpowiednio chronione. W celu ochrony wszystkich wrażliwych systemów i systemów wysokiego ryzyka, serwerów, baz danych i aplikacji należy stosować odpowiednie mechanizmy, takie jak szyfrowanie, kontrola dostępu i plany odzyskiwania danych (sposób tworzenia i przechowywania kopii zapasowych i archiwalnych). Należy również określić zasady realizacji krytycznych aplikacji w warunkach awaryjnych, katastrof lub klęsk żywiołowych (w tym plany działań awaryjnych i plany odtwarzania działalności).

Przechowywanie danych wrażliwych lub danych wysokiego ryzyka w systemach komputerów biurowych lub komputerów przenośnych organizacji powinno być ograniczone do minimum i właściwie chronione poprzez szyfrowanie, kontrolę dostępu i plany odzyskiwania danych.

W celu zapobieżenia dostępowi do głównych systemów, serwerów, baz danych i aplikacji bankowości elektronicznej bez upoważnienia należy wprowadzić odpowiednie mechanizmy kontroli fizycznego dostępu. Powinny obejmować mechanizmy kontrolne zabezpieczające przed nieupoważnionym dostępem do systemów stron zewnętrznych, takich jak goście, zleceniobiorcy i technicy. Strony te mogą mieć dostęp do pomieszczeń, chociaż mogą nie być bezpośrednio zaangażowane w usługi na rzecz systemów informatycznych.

Należy stosować odpowiednie techniki służące redukcji zewnętrznych zagrożeń dla systemów informatycznych i aplikacji bankowości elektronicznej, w tym korzystać z:

- oprogramowania wykrywającego wirusy we wszystkich najważniejszych punktach wejścia (np. w serwerach o zdalnym dostępnie, serwerach obsługujących pocztę elektroniczną) i w każdym systemie komputerów biurowych,
- oprogramowania wykrywającego próby włamań do systemu oraz z innych narzędzi oceny bezpieczeństwa służących okresowemu badaniu sieci, serwerów i stosowanych rozgraniczeń w celu wykrycia słabości i/lub przypadków naruszenia procedur bezpieczeństwa i mechanizmów kontrolnych,
- testowania pod kątem penetracji sieci wewnętrznych i zewnętrznych,
- raportowania wszelkich wykrytych lub podejrzewanych zjawisk, wskazujących na możliwość nadużyć,
- określenia trybu ich usuwania, zapobieganiu ponownemu wystąpieniu oraz określeniu zakresu działań analitycznych dla zidentyfikowania słabych ogniw zabezpieczenia systemu.

Należy stosować rygorystyczny proces analizy bezpieczeństwa wobec wszystkich pracowników i usługodawców zajmujących newralgiczne stanowiska.

Należy określić polityki i standardowe wymagania dotyczące zgodności i dostosowywania systemów informatycznych do obowiązujących przepisów prawa.

Należy utrzymywać niezbędny poziomu edukacji użytkowników wymaganej dla zapewnienia bezpieczeństwa informacji poprzez udział w seminariach, kursach i szkoleniach.

Z procedur obowiązujących w banku powinien jednoznacznie wynikać obowiązek oddzielenia funkcji operacyjnych od rozwojowych, a także funkcji administrowania systemem, zarządzania siecią, wprowadzania danych, technicznej obsługi komputerów, napraw systemu i

jego rozbudowy od administrowania bezpieczeństwem systemów komputerowych oraz audytu systemów informatycznych.

Oddzielenie i niezależna realizacja czynności testujących od operacyjnych zapobiega wprowadzaniu nieoczekiwanych i niepożądanych zmian do wersji użytkowej systemu oraz nadmiernemu dzieleniu się informacjami. Prace testujące powinny być oddalone od normalnej, operacyjnej pracy systemów informatycznych również w sensie fizycznym. Poszczególni użytkownicy aplikacji powinni mieć indywidualne, własne, często zmieniane hasła dostępu.

Modyfikacja systemu, wdrażania nowej wersji lub przejście na inny system jak również wymiana sprzętu powinna być prowadzona w taki sposób aby zabezpieczyć bank przed możliwością wystąpienia przestojów.

Pisemne zasady postępowania i zakresy odpowiedzialności powinny szczegółowo normować sposób postępowania w przypadkach incydentalnych: załamania się systemu, utraty danych, wystąpienia błędnych i/lub niekompletnych danych operacyjnych, naruszenia lub prób naruszenia poufności informacji. W każdym z takich przypadków powinno obowiązywać przeprowadzenie identyfikacji i analizy przyczyn oraz skutków sytuacji awaryjnych. W procedurach należy wskazać zasady analizy słabości systemów aktualnie funkcjonujących, planowania środków zaradczych, ich testowania i wdrażania.

Procedury powinny być ukierunkowane na zapobieganie, wykrywanie i powstrzymywanie skutków niepożądanych zdarzeń, zagrażających operacjom bankowym, niezgodnych z prawem, obowiązującymi procedurami, dokonanych z pominięciem zabezpieczeń kontrolnych. Powinny one również wskazywać możliwość użycia alternatywnych sieci komputerowych i systemów telekomunikacyjnych w przypadku awarii oraz być zgodne z procedurami wykrywania błędów i z planami poawaryjnego przywracania sprawności systemów, uszkodzonych w następstwie poważnych katastrof. Procedury działań ograniczających szkody powinny być ściśle związane z polityką zabezpieczenia systemów informatycznych przed stratami spowodowanymi nadużyciami pracowników, zniszczeniem programów i sprzętu komputerowego oraz z rachunkiem kosztów odzyskania danych.

Polityka korzystania z zewnętrznych urządzeń, warunkujących pracę systemu informatycznego oraz współpraca z firmami zewnętrznymi (dostawcami sprzętu, oprogramowania, ośrodkami przetwarzania danych na zlecenie) może potencjalnie zwiększać prawdopodobieństwo utraty danych. Niezbędna jest identyfikacja obszarów ryzyka, możliwości zapobiegania im i scenariusze postępowania w najmniej korzystnych sytuacjach, których wystąpienia nie można wykluczyć. Szczególnego rozważenia przez kierownictwo banku wymaga zasadność przetwarzania poza bankiem informacji o dużym stopniu poufności (czy sytuacja taka może mieć miejsce, jakie ryzyko jest z tym związane i jak można je zminimalizować poprzez systemy kodowania, szyfrowania itp.).

Zasady polityki bezpieczeństwa powinny uwzględniać wyżej wymienione uwarunkowania wewnętrzne i zewnętrzne, a także chronić przed wyborem nieprzyjaznego oprogramowania, zapobiegać niebezpieczeństwu zainstalowania technicznie złych programów, grożących umożliwieniem nieautoryzowanego dostępu i uszkodzeniem informacji (np. sieciowe wirusy, konie trojańskie, bomby logiczne). Należy też dołożyć należnej troski w stworzeniu właściwych, zgodnych ze wszelkimi wymogami warunków dla bezpiecznego funkcjonowania aktywów informatycznych.

Opracowanie zasad polityki powinno być poprzedzone sklasyfikowaniem poziomów bezpieczeństwa informacji i oznaczeniem ich dla określenia właściwych zabezpieczeń, w tym

również ustalenia zasad komunikowania się między poszczególnymi użytkownikami. Zasady polityki bezpieczeństwa należy cyklicznie analizować i aktualizować stosownie do zmieniających się warunków organizacyjnych.

C. PLANOWANIE SKALI SYSTEMÓW INFORMATYCZNYCH

Kierownictwo banku odpowiada za rozwój systemów informatycznych.

Planując opracowanie lub rozwój systemu informatycznego należy rozważyć czy projektowane wyposażenie informatyczne będzie mogło sprostać przyszłym potrzebom użytkowników. W celu wyeliminowania ograniczeń i zagrożeń związanych z niezdolnością funkcjonującego systemu informatycznego do rozwoju, zalecane jest prognozowanie przyszłego zapotrzebowania na sprzęt i usługi informatyczne oraz monitorowanie możliwości jego rozwoju i unowocześnienia.

Prognozy i plany powinny uwzględniać strategię marketingową banku (wprowadzanie nowych produktów), jego konkurencyjność na rynku finansowym także po wejściu Polski do Unii Europejskiej, analizę ryzyka, unowocześnianie sprawozdawczości zarządczej i zasad controllingu, realizację obowiązków sprawozdawczych wobec instytucji zewnętrznych (organów nadzorczych, statystyki państwowej). Szczególna uwaga powinna być skierowana na odpowiedni wybór i możliwości konfigurowania sprzętu oraz oprogramowania. Ważnymi cechami systemu jest jego dostosowanie do obowiązujących przepisów i norm, wydajność i mobilność, sposoby postępowania w przypadku wykrycia błędów i procedury poawaryjnego przywracania sprawności (szybkość naprawy). Planowane zmiany systemów wymagają oceny ich wpływu na: ewidencję księgową, udokumentowanie operacji, możliwość identyfikacji zmian i ich nadzorowania.

Prawodawstwo UE wymusza w zakresie współpracy z jej instytucjami spełnianie wymogów w zakresie ochrony informacji i bezpieczeństwa systemów teleinformatycznych. Zatem po wejściu do UE systemy teleinformatyczne powinny spełniać normy i standardy obowiązujące w UE czyli:

- Dyrektywy Parlamentu Europejskiego i Rady UE,
- Rezolucja Rady UE z 28.01.2002r w sprawie bezpieczeństwa informacji i sieci teleinformatycznych,
- Decyzje Komisji UE z 29.11.2001r w sprawie zasad i procedur bezpieczeństwa w ochronie informacji i sieci teleinformatycznych,
- Ramowa Propozycja Decyzji Komisji UE z 19.04.2002r w sprawie ataków na systemy informatyczne (wejście w życie 31.12.2003r)
- standard ISO-15408 określający wymogi bezpieczeństwa systemów informatycznych,
- standard ISO-17799 określający zasady zarządzania bezpieczeństwem.

Wybór nowych rozwiązań, tryb ich akceptacji i testowanie, przed podjęciem ostatecznej decyzji zakupu, powinny być zgodne z obowiązującymi w banku procedurami. Należy zwrócić uwagę, aby wprowadzenie nowych systemów nie zakłóciło pracy dotychczasowych, równolegle funkcjonujących w banku. Niezbędne jest zaplanowanie odpowiednich szkoleń dla użytkowników.

Planując skalę systemów informatycznych należy mieć na uwadze potrzebę zabezpieczenia na wypadek awarii sprzętu lub zdarzeń losowych (pożar, powódź itp.), a także konieczność archiwizowania danych. W związku z tym trzeba uwzględnić:

- potrzebę posiadania sprzętu zapasowego, na wypadek awarii (najlepszym rozwiązaniem jest posiadanie centrum zapasowego, a w przypadku baz scentralizowanych jest szczególnie zalecane)
- częstotliwość i zakres kopiowania informacji (backup) na nośnikach zewnętrznych, pozwalających na odtworzenie stanu systemu sprzed zdarzenia,
- prowadzenie księgi rejestrującej zdarzenia zachodzące w systemie (log),
- cykliczność i sposób archiwizowania informacji.

Nietrafny wybór mało elastycznych, niekompatybilnych z innymi, systemów może narazić bank, w przypadku wzrostu skali przetwarzanych informacji, na konieczność ich wymiany związaną z poważnymi kosztami.

Szczególnie niepożądane są wszelkie działania banku, prowadzące do zmiany obowiązujących przepisów prawnych wyłącznie z powodu przyjętych rozwiązań w systemie informatycznym banku.

IV. MECHANIZMY KONTROLI BEZPIECZEŃSTWA

A. MECHANIZMY KONTROLI DOTYCZĄCE WSZYSTKICH SYSTEMÓW INFORMATYCZNYCH

1. Analiza zagrożeń i metody zabezpieczeń

Bank powinien stosować zabezpieczenia systemów informatycznych za pośrednictwem narzędzi zawartych w systemach operacyjnych (dla sieci i/lub stanowisk komputerowych), wyspecjalizowanego oprogramowania, zastosowania rozwiązań sprzętowych, audytu, zarządzania konfiguracją, a także działań organizacyjnych, podejmowanych profilaktycznie na wypadek naruszenia zabezpieczeń oraz w stanach awaryjnych i katastrofalnych.

W procesie planowania zabezpieczeń powinny być określone wartości zasobów systemu informatycznego, ich klasyfikacja, zasady inwentaryzacji, osoby, którym zostały powierzone i ich zakresy odpowiedzialności oraz granice dopuszczalnych modyfikacji systemu zabezpieczeń. Wymienione czynniki mają wpływ na prawdopodobieństwo wystąpienia zagrożeń. Identyfikacja tych zagrożeń powinna poprzedzić określenie rodzaju ryzyka, analizę i zarządzanie ryzykiem poprzez wybór, testowanie i implementację nowych lub uzupełniających mechanizmów zabezpieczeń, minimalizujących ryzyko do poziomu, który może być przez bank akceptowany.

Wybór metod zapewnienia bezpieczeństwa systemów informatycznych powinien być adekwatny do ich rodzajów, typów ryzyka i wyników przeprowadzonej przez bank analizy opłacalności wybranych narzędzi, takich jak np.: tworzenie ścian zaporowych (firewalls), wykorzystanie kryptografii, kontrolowanie drogi przebiegu, uwierzytelnienie użytkownika (hasła jedno i wieloczłonowe, częstotliwość zmian), stosowanie wielopoziomowej kontroli dostępu, właściwe utrzymywanie zasobów informatycznych (np. w tzw. stanie gotowości neutralnej), podział czynności systemu wg klasyfikacji użytkowników, kwotowo określone uprawnienia do realizacji transakcji. Niezależnie od zabezpieczeń stosowanych w systemach informatycznych konieczne jest stosowanie zabezpieczeń fizycznych (ośrodki zapasowe, archiwa na niemodyfikowalnych dyskach optycznych) oraz organizacyjnych (proces tworzenia nowego oprogramowania powinien być podzielony na następujące, odrębne etapy: opracowanie strategii, analizę, projektowanie, budowę systemu wraz ze stworzeniem dokumentacji użytkowej, testowanie, wdrożenie i eksploatację).

Konieczne jest stosowanie kopii bezpieczeństwa (tzw. backup) i bieżącego dziennika zdarzeń (tzw. log), które w przypadku utraty danych w systemie informatycznym, powinny pozwolić na odtworzenie zasobów.

Kompletne zapisy kopii zapasowych (backup) powinny być przechowywane oddzielnie, w odpowiednim oddaleniu od systemu informatycznego, dobrze zabezpieczone fizycznie i środowiskowo. Minimalny zapas kopii powinien zapewnić odtworzenie systemu po awarii i

zależy od rodzaju stosowanych systemów. Niemniej jednak można przyjąć, że w zależności od częstotliwości zmian i wrażliwości danych powinien w zasadzie obejmować informacje wygenerowane w ciągu ostatnich 14 dni roboczych, nie mniej jednak niż z ostatnich 3 dni roboczych. Dane te należy regularnie sprawdzać w zakresie pozwalającym na ocenę ich stanu (możliwości użycia) w przypadku załamania pracy systemu.

Tworzone przez systemy księgi rejestrujące zdarzenia zachodzące w systemie (log) powinny zawierać wykazy wszystkich czynności, czasy przebiegu (od rozpoczęcia do zakończenia), wykryte błędy, działania naprawcze, potwierdzenie właściwego postępowania ze zbiorami danych i ewentualnie wydrukami.

Należy mieć na uwadze, iż za bezpieczeństwo systemów informatycznych odpowiada w każdym przypadku zarówno właściciel jak i użytkownik systemu. Określenie odpowiedzialności powinno być precyzyjne i mieć charakter personalny. Niezbędna jest alokacja odpowiedzialności za bezpieczeństwo systemów informatycznych, w formie wyznaczenia stanowisk i zakresów odpowiedzialności. Delegowanie uprawnień nie zdejmuje odpowiedzialności za bezpieczeństwo systemów informatycznych z właściciela.

2. Bezpieczeństwo dokumentacji systemowej

Bank powinien posiadać dokumentację systemową wszystkich systemów informatycznych używanych przez bank, dbać o jej aktualność i bezpieczeństwo.

W wypadku prowadzenia ksiąg rachunkowych przy użyciu komputera, z punktu widzenia przepisów o rachunkowości[2], dokumentacja powinna zawierać co najmniej:

1. wykaz zbiorów stanowiących księgi rachunkowe na nośnikach danych,
2. wykaz programów wraz z pisemnym stwierdzeniem dopuszczenia każdego nowego lub zmienionego programu do stosowania,
3. opis przeznaczenia każdego programu, sposobu jego działania (reguły obliczeń, ewidencji, kontroli i wydruku danych) oraz wykorzystywania podczas przetwarzania danych,
4. procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów,
5. programowych zasad ochrony danych, w tym w szczególności metod zabezpieczania dostępu do danych i systemu ich przetwarzania,
6. określenie wersji oprogramowania i daty rozpoczęcia jego eksploatacji,
7. opis systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów.

Bank powinien posiadać udokumentowaną procedurę dostępu do informacji i systemów informatycznych. Każdy właściciel aplikacji powinien opracować precyzyjnie zdefiniowane procedury i zasady dostępu, które będą określały prawa dostępu poszczególnych użytkowników/grup użytkowników, sposoby autoryzacji i aktualizacji listy użytkowników oraz haseł.

[2] przepisy art.10 ust1 pkt 3 c) i pkt 4 oraz przepisy art. 71 ust. 2 Ustawy o rachunkowości.

Dokumentacja powinna być odpowiednio zabezpieczona, z zachowaniem zasady, że dokumentacja generowana przez system powinna być przechowywana oddzielnie od zbiorów danych. W każdym przypadku niezbędne jest ustalenie wymaganego poziomu zabezpieczeń i dostępu: sporządzenie listy osób upoważnionych do wglądu, wraz z listą zakresów dostępności (pełnej, ograniczonej) autoryzowaną przez właściciela aplikacji.

Jeśli dokumentacja udostępniana jest na zewnątrz w związku ze zleceniem przez bank usługi, niezbędny jest szczególnie staranny wybór zleceniobiorcy. Każda wymiana danych i oprogramowania powinna być poprzedzona zabezpieczeniem przed utratą, niepożądanymi modyfikacjami, złym wykorzystaniem, a także ściśle kontrolowana. Użytkowanie oprogramowania powinno wynikać z formalnych umów. Treść zawartych w nich warunków ostrożnościowych, ograniczających ryzyko prawne i organizacyjne: utraty danych, niepożądanych modyfikacji i złego wykorzystania powinna być proporcjonalna do wrażliwości (ważności) informacji bankowych. Powinna również zapewniać właściwą ochronę praw autorskich. Wymiana informacji z innymi użytkownikami (np. wzajemne przekazywanie przez banki informacji dla biur ryzyka itp.) może następować z zachowaniem warunków praw autorskich w zakresie dzielenia się informacją.

Na wypadek niebezpieczeństwa naruszenia poufności, integralności i dostępności informacji bank powinien mieć awaryjne scenariusze postępowania. Powinny one uwzględniać wartość transakcji i specyfikę operacji bankowych (rodzaj i formę np. elektroniczny transfer pieniędzy, transakcje walutowe, akredytywy potwierdzane elektronicznie itp.). Dokumentację tę należy przechowywać w odrębnych pomieszczeniach i bieżąco aktualizować, równolegle do zmian wprowadzanych w systemach informatycznych banku.

3. Zarządzanie sprzętem, wyposażeniem komputerowym oraz siecią

Kierownictwo banku odpowiedzialne jest za techniczne zabezpieczenie prawidłowego funkcjonowania systemów informatycznych i sieci.

Przetwarzanie danych w banku powinno odbywać się zgodnie zobowiązującymi procedurami i zakresami odpowiedzialności. Działania zabezpieczające przed przerwaniem pracy systemu i działania naprawcze, w każdym przypadku, powinny przebiegać według sformalizowanych procedur, a ich wykonanie powinno być poddane ścisłej kontroli. Działania naprawcze może podejmować jedynie ściśle określony personel. Każdorazowo powinna być sporządzona precyzyjna dokumentacja działań naprawczych, a ponadto w takich sytuacjach należy niezwłocznie przedstawiać raport kierownictwu banku.

Zarządzanie siecią ma na celu m.in. zapewnienie bezpieczeństwa informacji dostępnych w sieci. Mechanizmy kontroli, ustanowione dla ochrony poufności i integralności danych, powinny skutecznie zapobiegać przenikaniu informacji do publicznej wiadomości oraz ich nielegalnym zmianom. Czynności związane z zarządzaniem siecią i komputerami należy ściśle koordynować w celu optymalizacji usług oraz zapewnienia właściwego poziomu bezpieczeństwa w ramach infrastruktury informatycznej w banku.

Sposób postępowania z nośnikami danych wszelkiego rodzaju powinien zapobiegać uszkodzeniom sprzętu i zakłóceniom pracy systemu. Zarządzanie nośnikami danych powinno przebiegać zgodnie zobowiązującymi w banku procedurami zabezpieczeń a w szczególności powinno obejmować: oznakowanie nośników danych, przenoszenie na nie informacji, miejsce i sposób bezpiecznego ich przechowywania, sposób i forma autoryzacji zmian i usuwania danych, właściwa i trwała likwidacja niepotrzebnych danych. Oznakowanie wszystkich nośników danych, ustanowienie formalnego dziennika autoryzowanych użytkowników, zapewnienie kompletności danych wejściowych, stosowanie potwierdzania prawidłowości wszystkich transmitowanych danych, precyzyjne oznakowanie wszystkich kopii danych, przekazywanych autoryzowanym odbiorcom, systematyczne przeglądanie i autoryzowanie listy odbiorców danych i usług ma na celu ochronę informacji przed nieautoryzowanym dostępem, ujawnieniem i niewłaściwym wykorzystaniem.

Dla zapewnienia należytego bezpieczeństwa transakcji międzybankowych, zalecana jest współpraca z innymi bankami w tym z Narodowym Bankiem Polskim i Krajową Izbą Rozliczeniową, w zakresie wymiany doświadczeń i wniosków, wynikających z analizy wykrytych przypadków nadużyć. Wymiana informacji powinna być jednak limitowana tak aby nie została naruszona tajemnica służbowa i bankowa oraz zachowane bezpieczeństwo zgromadzonych w banku środków. Wskazane jest określenie zakresu przekazywanych informacji we wspólnych umowach.

Kierownictwo banku odpowiedzialne jest za przesyłane informacje: tj. ich zatwierdzenie, zabezpieczenie technicznych standardów dla transmisji i standardów identyfikacji kurierskich. Odpowiedzialność ta obejmuje nie tylko utratę danych, ale też narażenie banku na niebezpieczeństwo nieupoważnionego dostępu osób trzecich do informacji w czasie jej transmisji lub przekazywania do zewnętrznych ośrodków przetwarzania. Zapewnienie poufności danych może zabezpieczyć właściwa organizacja ich przekazu tj. wiarygodne transmisje lub kurierzy, stosowanie systemów kryptograficznych, fizyczna ochrona nośników danych, przekazywanie danych za pokwitowaniem itp. Informacje szczególnie wrażliwe na ryzyko utraty, ujawnienia i nieautoryzowany dostęp, które to zdarzenia mogłyby narazić bank na poważne straty materialne i moralne np. utratę dobrej reputacji, powinny być w miarę możliwości przesyłane kilkoma kanałami i w odpowiednich częściach tak, aby ich rozszyfrowanie i nieuprawnione wykorzystanie było maksymalnie utrudnione.

W celu minimalizacji ryzyka należy dokonać odpowiedniego wyboru rodzajów mediów telekomunikacyjnych. Poczta elektroniczna różni się od tradycyjnej szybkością przekazu i strukturą informacji. Przy korzystaniu z niej niezbędne jest jednak, aby bank wypracował jasną politykę jej statusu i wykorzystania oraz mechanizmów kontroli. Użytkownicy powinni zabezpieczyć się przed nieautoryzowaną zmianą komunikatów i ryzykiem błędu (np. niewłaściwego adresu). Należy liczyć się z tym, iż ograniczenia prawne, takie jak potencjalna konieczność udokumentowania pochodzenia informacji i źródła jej przesyłki, mogą nie chronić banku w dostateczny sposób przed ryzykiem nieuprawnionego wykorzystania. Wskazane jest rozważenie możliwości zastosowania podpisu elektronicznego.

Ujawnione, w trakcie okresowo przeprowadzanych kontroli, przypadki naruszenia obowiązujących w jednostce zasad dostępu powinny być raportowane kierownictwu banku.

4. Bezpieczeństwo systemów informatycznych a działania personelu i upoważnionych osób trzecich

Kierownictwo banku jest odpowiedzialne za stworzenie właściwej polityki bezpieczeństwa redukującej ryzyko błędu ludzkiego i niewłaściwego wykorzystania sprzętu i informacji.

Z uwagi na statystycznie wysoki odsetek użytkowników wewnętrznych, naruszających zasady bezpieczeństwa, zalecany jest bardzo staranny dobór, pod względem profesjonalnego przygotowania i cech osobowościowych, pracowników zatrudnianych na stanowiskach dających dostęp do szczególnie ważnych informacji. Odpowiednio przygotowane umowy o pracę lub odrębne oświadczenia powinny zawierać klauzule o ochronie tajemnicy służbowej oraz szczegółowy zakres obowiązków. Z treścią takiego dokumentu pracownicy powinni być zapoznani już na etapie rekrutacji. Należy przyjąć zasadę, iż przed przystąpieniem do pracy, osoby nowo zatrudnione potwierdzają podpisem na odpowiednim oświadczeniu fakt dokładnego zapoznania się ze swoimi uprawnieniami i obowiązkami w zakresie używania systemu komputerowego. Podpisują również oświadczenia znajomości zasad zachowania poufności informacji. Oznacza to objęcie tajemnicą służbową informacji na temat sprzętu i systemów informatycznych i telekomunikacyjnych oraz technologii przetwarzania stosowanych w banku również przez odpowiedni okres po zakończeniu pracy w banku.

Redukcja ryzyka błędu ludzkiego i niewłaściwego wykorzystania sprzętu i informacji wymaga szeregu działań ze strony kierownictwa jednostki. Do obowiązków kierującego zespołem pracowniczym należy przydzielenie zadań poszczególnym pracownikom, udzielenie wskazówek dotyczących ich wykonania, określenie granic uprawnień, odebranie odpowiednich oświadczeń na piśmie, przekazanie haseł lub innych środków kontroli dostępu, przechowywanie zdeponowanych haseł jakimi dysponują oraz raportów o wszystkich czynnościach wykonywanych przez wewnętrznych użytkowników. Ryzyko niedokładnego, niekompletnego bądź wielokrotnego wprowadzenia tych samych danych powinno być eliminowane przez odpowiednie procedury kontroli np. sprawdzanie i poprawianie prawidłowości danych, kontrola przy pomocy paczek danych, bilansowanie transakcji, rejestracja pozycji do wyjaśnienia i nadzór nad dalszym postępowaniem z nimi itp. W przypadku używania ruchomych nośników danych, po zakończeniu pracy powinny one być zdemontowane i zabezpieczone przed dostępem osób nieupoważnionych.

Ryzyko polegające na tym, że niepowołane osoby mogą uzyskać dostęp do funkcji przetwarzania w programach użytkowych, a następnie stosując procedury inicjowania, zatwierdzania i rejestrowania operacji gospodarczych dostęp do danych, powinno być zmniejszone poprzez kontrolę dostępu zapewniającą identyfikację użytkownika, sprawdzenie jego tożsamości, przyznawanie odpowiednich praw dostępu, zapewnienie poufności haseł. W czasie nieobecności stałego użytkownika komputera dostęp innych nieupoważnionych osób powinien być uniemożliwiony. Użytkownik danego terminala powinien być odpowiedzialny za

wszelkie czynności wykonane za jego pomocą. Przekazanie uprawnień powinno być dokonane na polecenie kierownictwa i dokumentowane.

Osoby odpowiedzialne za bezpieczeństwo systemów informatycznych nie powinny łączyć tych funkcji z pracami dotyczącymi obsługi systemów. Za dostępność odpowiada osoba, której powierzono odpowiedzialność za system. Odpowiedzialność za bezpieczeństwo dużych sieci, rozległych przestrzennie, może być powierzona zespołowi wyznaczonemu zgodnie z procedurami obowiązującymi w banku.

W przypadku przekazywania sprzętu do naprawy należy sprawdzić czy nie pozostały w nim informacje. Umowa zawarta pomiędzy bankiem a jednostką, której powierzono serwis, powinna określać procedury postępowania w przypadku wystąpienia możliwych do przewidzenia sytuacji, a przede wszystkim procedury zabezpieczenia ewentualnie skasowanych danych. Dodatkowo umowa powinna gwarantować bankowi uzyskanie wszelkich informacji o zmianach dokonanych w komputerach i ich funkcjach logicznych oraz zobowiązać jednostkę serwisującą do zachowania tajemnicy. Bank powinien prowadzić ewidencję napraw i konserwacji sprzętu, zawierającą dane personalne osób je wykonujących, daty wykonania i rodzaje uszkodzeń.

5. Współpraca z klientami

Kierownictwo banku jest odpowiedzialne za monitorowanie przestrzegania warunków umowy z klientami.

Należy zwrócić uwagę, iż szczególnym obszarem w działalności bankowej, narażonym na ryzyko naruszania bezpieczeństwa ochrony danych, jest współpraca z klientami banku realizowana za pomocą urządzeń komputerowych (np. system home banking, bankowość internetowa) i telekomunikacyjnych. Dostęp osób trzecich do urządzeń i sprzętu komputerowego powinien być ściśle kontrolowany i poprzedzony dogłębną analizą ryzyka. Umożliwienie dostępu należy poprzedzić zawarciem formalnej umowy szczegółowo określającej warunki dostępu. Niezbędne jest precyzyjne unormowanie w umowie zagadnień związanych z różnego typu rodzajami ryzyk, a w szczególności:

- ogólnych zasad ochrony i udostępniania informacji,
- dozwolonych metod kontroli dostępu (kody, hasła, identyfikatory, certyfikaty cyfrowe, itp.),
- ścieżek dostępu,
- list autoryzowanych osób (specyfikacji),
- ustalenia dat i czasu dostępu,
- zakresów odpowiedzialności stron,
- zakresu obowiązujących unormowań prawnych, w tym także związanych z legislacją ochrony danych,
- praw właściciela do monitorowania systemu dostępu osób trzecich,
- odpowiedzialności w zakresie instalacji oraz obsługi sprzętu i oprogramowania,
- prawa audytu odpowiedzialności umownych,
- restrykcji w zakresie kopiowania i ujawniania informacji,
- zabezpieczenia fizycznego informacji,

- raportowania i nadzorowania przypadków nadużyć.

Integralną częścią umowy pomiędzy klientem i bankiem są uprawnienia klienta do ochrony wkładów zdeponowanych w banku, zabezpieczenia tajemnicy rachunków bankowych, uzyskania usług świadczonych z należytą starannością, postanowieniami umowy i przepisami prawa oraz wzajemna odpowiedzialność odszkodowawcza stron.

Monitorowanie przestrzegania warunków umownych i szczegółowa analiza zachowań klientów, mających dostęp do systemów informatycznych, powinny być zinstytucjonalizowane procedurami obowiązującymi w tym zakresie.

6. Szkolenie użytkowników

Kierownictwo banku jest odpowiedzialne za szkolenie użytkowników.

Użytkownicy powinni być szkoleni w zakresie procedur bezpieczeństwa i właściwego korzystania ze sprzętu i systemów informatycznych. Zakres tematyczny szkoleń powinien pozwalać na dokładne zapoznanie z procedurami użytkowania sprzętu i oprogramowania oraz procedurami obowiązującymi w zakresie bezpieczeństwa systemu, zapewniającymi jego poufność, integralność i dostępność.

W trakcie szkoleń użytkownicy powinni być wyczuleni na obserwację i reagowanie na wszelkie przypadki, mogące mieć wpływ na bezpieczeństwo systemu i zapoznani z formalnoprawnymi procedurami postępowania w przypadkach faktycznego lub podejrzewanego zagrożenia bezpieczeństwa systemu oraz zasadami bezzwłocznego powiadamiania kierownictwa banku o nieprawidłowościach. Obowiązek raportowania dotyczy wszelkich przypadków działania systemów niezgodnie z ich przeznaczeniem.

Personel banku powinien być przeszkolony w zakresie ochrony systemów informatycznych przed wirusami, ze szczególnym zwróceniem uwagi na badanie nowych nośników danych włączanych do pracy w systemie i pilnego śledzenia wszelkich komunikatów i informacji pojawiających się na ekranach monitorów. W przypadku wykrycia wirusów, wewnętrzne procedury powinny nakładać obowiązek zaprzestania użytkowania systemu, odizolowanie środowisk niosących zagrożenie i natychmiastowe poinformowanie technicznych służb komputerowych i kierownictwa.

Dla zachowania bezpieczeństwa systemu, bank powinien opracować formalny proces dyscyplinarnego postępowania z osobami nie przestrzegającymi procedur i zapoznać z nim użytkowników systemu w trakcie szkoleń.

7. Bezpieczeństwo fizyczne i środowiskowe systemów informatycznych

Kierownictwo banku odpowiada za fizyczne i środowiskowe bezpieczeństwo systemów.

Stosowane przez każdą jednostkę zabezpieczenia fizyczne i środowiskowe powinny być adekwatne do skali i rodzajów systemów informatycznych oraz świadczonych usług. Duże organizacje gospodarcze, jakimi są banki wielooddziałowe o terytorialnie rozbudowanej sieci, posiadające własne ośrodki przetwarzania danych, mogą wymagać wyższego stopnia fizycznego i informatycznego zabezpieczenia.

Należy zdefiniować poziom zabezpieczenia fizycznego oraz procedury zabezpieczenia przeciwpożarowego proporcjonalnie do wartości sprzętu i wielkości potencjalnych strat, które mogą być wyrządzone w wyniku uszkodzenia zabezpieczeń.

Dla sprzętu komputerowego i nośników informacji, parametr bezpieczeństwa powinien określać, które obszary stanowią miejsca silnie strzeżone. Centrum przetwarzania danych powinno posiadać stosowne zabezpieczenia fizyczne, zarówno przed skutkami zdarzeń losowych (ogień, powódź, wybuchy itp.), jak i wszelkich ludzkich ingerencji. Zaleca się, aby ośrodki usług informatycznych i centralne jednostki systemów, zlokalizowane były w fizycznie wydzielonych strefach, zabezpieczonych przed możliwością przebywania w ich pobliżu osób do tego nieupoważnionych. Usytuowanie centrum informatycznego powinno uniemożliwiać publiczny dostęp osobom postronnym w postaci m.in.: osobnej nieruchomości, wyodrębnionej części budynku bez dostępu osób nieupoważnionych, osobnego, zamkniętego pokoju, fizycznej bariery uniemożliwiającej dostęp do sprzętu komputerowego itp.

Należy zwrócić uwagę na właściwy stopień zabezpieczenia pomieszczeń sąsiadujących. Zaleca się rezygnację z tablic identyfikacyjnych, szyldów, wywieszek informacyjnych itp., a także umieszczania numerów telefonów w spisach telefonicznych, pozwalających na łatwe zlokalizowanie zewnętrznych i wewnętrznych pomieszczeń, w których odbywa się przetwarzanie danych. Celowe jest ograniczenie rozprzestrzeniania informacji o miejscach przetwarzanie danych wśród pozostałego personelu banku, nie związanego z pracą systemów informatycznych.

Niezbędne jest wyposażenie centrum przetwarzania danych w systemy podtrzymujący pracę serwerów i innych urządzeń informatycznych na wypadek awarii zasilania.

Niezbędne jest odpowiednie wyposażenie pomieszczeń w czujniki ciepła i dymu, instalacje alarmowe, sprzęt przeciwpożarowy, wyjścia ewakuacyjne itp. Cyklicznie powinny być przeprowadzane przeglądy zabezpieczenia przeciwpożarowego. Procedury postępowania w nagłych wypadkach winny mieć formę pisemną i być okresowo sprawdzane w symulowanych warunkach zagrożenia, a pracownicy szkoleni w zakresie zasad bhp i p.poż. Niebezpieczne i łatwopalne materiały powinny znajdować się w bezpiecznej odległości od urządzeń i sprzętu komputerowego. Materiały łatwopalne należy przechowywać z zachowaniem zasad

bezpieczeństwa przeciwpożarowego. W okresach czasowej nieobecności pracowników w pomieszczeniu, okna i drzwi powinny być pozamykane, a systemy alarmowe włączone.

Kontrola fizycznego dostępu do obszaru centrum informatycznego powinna być uregulowana odpowiednimi procedurami i parametrami dostępu, wskazującymi sytuacje i osoby dopuszczone do przebywania w wydzielonych obszarach. Należy określić sposób ustalania, rejestracji i kontroli:

- praw dostępu i ich aktualizacji (np. pozbawiania dostępu pracowników odchodzących z pracy),
- identyfikacji personelu,
- czasu wejścia i wyjścia.

Bank powinien dysponować procedurami postępowania wobec osób, które nie posiadając do tego uprawnień, znalazły się w strefach wyłączonych z powszechnego dostępu.

Po opuszczeniu przez pracowników wydzielonych pomieszczeń, powinny one być zabezpieczone fizycznie (odpowiednie rodzaje zamknięć) i okresowo kontrolowane. Personel pomocniczy i osoby świadczące usługi naprawcze mogą mieć dostęp do wydzielonego centrum informatycznego tylko, jeśli jest to niezbędnie konieczne, po uzyskaniu stosownej autoryzacji ich dostępu i pod stałym nadzorem osób odpowiedzialnych. Procedury zachowań w centrum informatycznym powinny nie dopuszczać fotografowania, nagrywania taśm magnetofonowych, taśm video itp. jak również określać osoby upoważnione do ewentualnego wydawania zezwoleń na te czynności.

Analizując zabezpieczenie poufności i dostępności danych w centrum informatycznym, należy również mieć na uwadze usytuowanie urządzeń towarzyszących, takich jak: drukarki, fotokopiarki i faksy. Dla ochrony danych przed ich bezprawnym kopiowaniem, niezbędne jest stworzenie warunków kontroli użytkowania tych urządzeń.

B. SZCZEGÓLNE MECHANIZMY KONTROLI BEZPIECZEŃSTWA DOTYCZĄCE BANKOWOŚCI ELEKTRONICZNEJ

1. Współpraca z klientami

Banki powinny podjąć odpowiednie kroki w celu potwierdzenia tożsamości i upoważnień klientów, z którymi prowadzą interesy za pośrednictwem Internetu lub innych elektronicznych kanałów dystrybucji.

Podstawowe znaczenie w bankowości ma potwierdzenie, czy dana próba kontaktu, transakcji lub dostępu jest uprawniona. Zgodnie z powyższym, banki powinny stosować niezawodne metody weryfikowania tożsamości i upoważnień nowych klientów, jak również potwierdzenia tożsamości i uprawnień aktualnych klientów dążących do zainicjowania transakcji elektronicznych.

Weryfikacja klienta przy otwieraniu rachunku jest ważna, ponieważ zmniejsza ryzyko podszywania się pod inną osobę, oszukańczego wykorzystania rachunku i prania pieniędzy. Wynikiem braku adekwatnego potwierdzenia tożsamości klientów przez bank może być uzyskanie przez nieuprawnione osoby dostępu do rachunków bankowości elektronicznej i ostatecznie strata finansowa lub zaszkodzenie reputacji banku poprzez oszustwo, ujawnienie informacji poufnych lub mimowolne zaangażowanie w działalność kryminalną.

Stwierdzenie i potwierdzenie tożsamości i uprawnień osoby do dostępu do systemów bankowych w środowisku czysto elektronicznej otwartej sieci może być zadaniem trudnym. Uprawnienia użytkownika mogą być fałszywie przedstawione poprzez rozmaite techniki znane ogólnie jako "spoofing". Hakerzy sieciowi mogą także przejąć sesję uprawnionej, upoważnionej osoby poprzez zastosowanie techniki zwanej "sniffer" i prowadzić działania o charakterze szkodliwym lub kryminalnym. Procesy kontroli uwiarygodniania tożsamości mogą być także obchodzone poprzez zmianę baz danych dotyczących potwierdzania tożsamości.

Zgodnie z powyższym, podstawowe znaczenie ma posiadanie przez banki formalnej polityki i procedur określających odpowiednią metodologię zapewniającą właściwe potwierdzanie przez bank tożsamości i upoważnienia osoby, agenta lub systemu za pomocą środków, które są unikalne i, w praktycznym stopniu, wyłączają nieupoważnione osoby lub systemy. Banki mogą korzystać z różnych metod ustalania tożsamości, w tym osobistego numeru identyfikacyjnego PIN, haseł, podpisu elektronicznego, kart smart, danych biometrycznych i certyfikatów cyfrowych. Metody te mogą się opierać na jednym czynniku lub wielu czynnikach (np. stosowanie w celu potwierdzenia tożsamości zarówno hasła jak i technologii biometrycznej). Stosowanie wieloczynnikowego potwierdzenia tożsamości gwarantuje zazwyczaj większą wiarygodność.

W oparciu o dokonaną przez kierownictwo ocenę ryzyka powodowanego przez system bankowości elektronicznej jako całość lub jego różne części składowe, Bank musi ustalić metody potwierdzania tożsamości, które będzie stosował. Taka analiza ryzyka ocenia możliwości transakcyjne systemu bankowości elektronicznej (np. przelew środków, opłacanie rachunków, złożenie wniosku o pożyczkę, agregacja rachunku, etc.), wrażliwość i wartość przechowywanych danych bankowości elektronicznej oraz łatwość korzystania przez klienta z metody potwierdzenia tożsamości.

W miarę ciągłej ewolucji metod potwierdzania tożsamości zachęca się banki do monitorowania i przyjmowania rzetelnych praktyk stosowanych przez sektor w tym obszarze zapewniających, że:

- bazy danych dotyczących tożsamości, zapewniające dostęp do rachunków klientów bankowości elektronicznej lub systemów wrażliwych są chronione przed manipulacjami i korupcją. Każda próba manipulacji powinna być wykrywalna i powinny istnieć ścieżki audytu pozwalające na dokumentację takich prób,
- każdy przypadek dodania, usunięcia lub zmiany danych o osobie, agencie lub systemie w bazie danych dotyczących tożsamości jest należycie autoryzowany przez upoważnione źródło,

- stosowane są odpowiednie środki kontroli połączenia systemu bankowości elektronicznej, które uniemożliwiają nieznanym stronom trzecim podszywanie się pod znanych klientów, zatwierdzone sesje bankowości elektronicznej pozostają bezpieczne w ciągu całego okresu ich trwania, ewentualnie w przypadku upływu zabezpieczenia sesja powinna wymagać ponownego zatwierdzenia.

2. Zarządzanie transakcjami w bankowości elektronicznej

Banki powinny stosować takie metody potwierdzania transakcji, które uniemożliwiają negowanie dokonanych transakcji i wprowadzają odpowiedzialność za transakcje bankowości elektronicznej.

Uniemożliwienie negowania zrealizowanych transakcji obejmuje stworzenie dowodu dotyczącego pochodzenia lub miejsca przeznaczenia informacji elektronicznej w celu ochrony wysyłającego informacje przed fałszywym zanegowaniem otrzymania danych przez otrzymującego informację, lub ochrony otrzymującego informację przed fałszywym potwierdzeniem wysyłki informacji przez wysyłającego. Ryzyko negowania transakcji występuje już w konwencjonalnych transakcjach, takich jak karty kredytowe i transakcje papierami wartościowymi. Jednak, bankowość elektroniczna zwiększa to ryzyko z powodu trudności w pozytywnym potwierdzeniu tożsamości i uprawnień stron inicjujących transakcje, możliwości zmiany lub przejęcia transakcji elektronicznych i możliwości twierdzenia przez użytkowników bankowości elektronicznej, że transakcje zostały oszukańczo zmienione.

Rozwiązanie tych zwiększonych problemów wymaga podjęcia przez banki rozsądnych działań, odpowiadających poziomowi istotności i rodzajowi transakcji bankowości elektronicznej, które zapewnią, że:

- systemy bankowości elektronicznej są zaprojektowane w sposób zmniejszający prawdopodobieństwo zainicjowania przez upoważnionych użytkowników niezamierzonych transakcji oraz umożliwiający klientom pełne zrozumienie ryzyk związanych z każdą zainicjowaną przez nich transakcją,
- tożsamość wszystkich stron transakcji jest potwierdzana, a także zachowywana jest kontrola nad potwierdzonym kanałem,
- dane o transakcjach finansowych są chronione przez zmianą, a wszelkie dokonane zmiany są wykrywalne.

Banki mogą stosować różne techniki, które pomagają uniemożliwić negowanie dokonanych transakcji i zapewniają poufność i rzetelność transakcji bankowości elektronicznej, ze szczególnym uwzględnieniem podpisu elektronicznego.

Banki powinny upewniać się, że posiadają odpowiednie środki służące ochronie integralności transakcji, zapisów i informacji bankowości elektronicznej.

Integralność danych oznacza pewność, że informacje przesyłane i przechowywane nie są zmieniane bez autoryzacji. Niezachowanie integralności danych dotyczących transakcji, zapisów i

informacji może narażać banki na straty finansowe, jak również na znaczne ryzyko prawne i ryzyko reputacji.

Bezpośredni charakter procesów bankowości elektronicznej może sprawiać, że błędy w programie lub oszustwa mogą być trudniejsze do wykrycia na etapie wstępnym. Z tego względu jest ważne, aby banki wprowadzały bezpośrednie przetwarzanie danych w sposób zapewniający bezpieczeństwo i rzetelność oraz integralność danych.

Ponieważ transakcje bankowości elektronicznej są realizowane za pośrednictwem publicznych sieci, narażone są na dodatkowe zagrożenia w postaci (manipulowanie danymi, oszustwa itp.). W związku z powyższym, banki powinny upewniać się, że posiadają odpowiednie środki służące ustaleniu dokładności, kompletności i wiarygodności transakcji bankowości elektronicznej, zapisów oraz informacji przekazywanych za pośrednictwem elektronicznych kanałów dystrybucji, przechowywanych w wewnętrznych bazach danych banku lub przesyłanych/przechowywanych w imieniu banku przez usługodawców, będących stronami trzecimi.

Dla zachowania integralności danych w środowisku bankowości elektronicznej powinny być powszechnie stosowane następujące praktyki:

- zapewnienie realizacji transakcji bankowości elektronicznej w sposób, który czyni je w ciągu całego procesu wysoce odpornymi na manipulację,
- zapewnienie przechowywania, udostępniania i modyfikowania zapisów bankowości elektronicznej w sposób, który czyni je wysoce odpornymi na manipulację,
- zapewnienie realizowania transakcji bankowości elektronicznej i prowadzenia zapisów powinny być zaprojektowane w taki sposób, aby faktycznie uniemożliwić oszukanie systemu wykrywania nieautoryzowanych zmian,
- zapewnienie stosowania adekwatnych regulacji dotyczących kontrolowania zmian, w tym procedur monitorowania i testowania, w celu uchronienia się przed wszelkimi zmianami w systemie bankowości elektronicznej, które mogą wskutek błędu lub w sposób niezamierzony narazić mechanizmy kontrolne lub wiarygodność danych,
- zapewnienie wykrywania wszelkich przypadków manipulowania transakcjami lub danymi bankowości elektronicznej przez funkcje przetwarzania, monitorowania i rachunkowości transakcji.

3. Zarządzanie bezpieczeństwem w bankowości elektronicznej

Banki powinny upewniać się, że posiadają odpowiednie środki służące promowaniu adekwatnego podziału obowiązków w zakresie systemów, baz danych i aplikacji bankowości elektronicznej

Podział obowiązków jest podstawowym wewnętrznym mechanizmem kontrolnym służącym redukcji ryzyka oszustw w procesach i systemach operacyjnych i zapewnieniu właściwego systemu upoważnień do dysponowania aktywami spółki, oraz ewidencji i bezpieczeństwa aktywów. Podział obowiązków ma zasadnicze znaczenie dla dokładności i rzetelności danych i jest stosowany w celu zapobieżenia popełnianiu oszustw przez osobę fizyczną. Przy adekwatnym podziale obowiązków, oszustwo może być popełnione jedynie w wyniku zmowy.

Usługi bankowości elektronicznej mogą wymagać modyfikacji sposobów ustalania i przestrzegania podziału obowiązków, ponieważ transakcje są zawierane za pośrednictwem systemów elektronicznych, w których tożsamość może być łatwiej zamaskowana lub sfałszowana. Ponadto, funkcje operacyjne i transakcyjne stały się w wielu przypadkach bardziej sprężone i zintegrowane w aplikacjach bankowości elektronicznej. Z tego względu należy dokonać analizy mechanizmów kontrolnych wymaganych tradycyjnie dla zachowania podziału obowiązków, a także odpowiednio je dostosować w celu zachowania odpowiedniego poziomu kontroli. Ponieważ dostęp do słabo zabezpieczonych baz danych poprzez sieci wewnętrzne lub zewnętrzne jest łatwiejszy, należy podkreślać ścisłe procedury autoryzacji i identyfikacji, bezpieczną i solidną architekturę bezpośrednich procesów przetwarzania i adekwatne ścieżki audytu.

Praktyki stosowane powszechnie w celu ustalenia i stosowania podziału obowiązków dotyczących bankowości elektronicznej obejmują co następuje:

- procesy i systemy transakcyjne powinny być zaprojektowane w taki sposób, żeby uniemożliwiały każdemu pojedynczemu pracownikowi lub wynajętemu usługodawcy zainicjowanie, autoryzację i realizację transakcji,
- należy zachować podział na osoby inicjujące dane statyczne (w tym treść strony internetowej) i osoby odpowiedzialne za weryfikację rzetelności tych danych,
- należy testować systemy bankowości elektronicznej w celu upewnienia się, że nie można obejść podziału obowiązków,
- należy zachować podział na osoby opracowujące i osoby administrujące systemami bankowości elektronicznej.

Banki powinny upewniać się, że posiadają właściwe mechanizmy kontroli autoryzacji i uprawnień dostępu do systemów, baz danych i aplikacji bankowości elektronicznej.

W celu zachowania podziału obowiązków banki muszą w rygorystyczny sposób kontrolować zagadnienia autoryzacji i uprawnień dostępu. Brak adekwatnych mechanizmów kontroli autoryzacji może umożliwić osobom zmianę ich tożsamości, obejście podziału obowiązków i uzyskanie dostępu do systemów, baz danych lub aplikacji bankowości elektronicznej, do którego nie są uprawnione.

Zasady autoryzacji i praw dostępu w systemach bankowości elektronicznej mogą być określone w sposób scentralizowany lub zdecentralizowany w ramach banku. Stosowne dane są zazwyczaj przechowywane w bazach danych. Z tego względu ochrona tych baz danych przed manipulacją lub ujawnieniem ma podstawowe znaczenie dla efektywnej kontroli autoryzacji.

- Wszystkim osobom, agentom lub systemom, które prowadzą elektroniczną działalność bankową, należy przypisać konkretne przywileje autoryzacji i dostępu.

- Wszystkie systemy bankowości elektronicznej powinny być skonstruowane w taki sposób, aby zapewniały ich interakcję z ważną bazą danych dotyczących autoryzacji.

- Żaden indywidualny agent lub system nie powinien być uprawniony do zmiany swych własnych uprawnień lub przywilejów dostępu w bazie danych dotyczących autoryzacji dostępu do bankowości elektronicznej. Zasada ta może być niewykonalna w przypadku użytkowników będących administratorami systemu, w tym wypadku należy wprowadzić inne, surowe wewnętrzne mechanizmy kontrolne i podział obowiązków.

- W każdym przypadku nadanie nowej osobie, agentowi lub systemowi przywilejów dostępu lub ich zmiana w bazie danych dotyczących autoryzacji dostępu do bankowości elektronicznej powinno być we właściwy sposób autoryzowane przez uwiarygodnione źródło wyposażone w odpowiednie uprawnienia i podlegające odpowiedniej i bieżącej kontroli oraz ścieżkom audytu.

- Należy wprowadzić odpowiednie kroki służące uodpornieniu baz danych dotyczących autoryzacji dostępu do bankowości elektronicznej na manipulacje. Wszelkie przypadki manipulacji powinny być wykrywalne poprzez procesy ciągłego monitorowania. Konieczność dokumentowania takich prób manipulacji wymaga istnienia dostatecznych ścieżek audytu.

- Baza danych dotyczących autoryzacji dostępu do bankowości elektronicznej, która została poddana manipulacji, nie powinna być używana do czasu jej zastąpienia przez sprawdzoną bazę danych.

- Należy wprowadzić mechanizmy kontrolne zapobiegające zmianom poziomów autoryzacji podczas sesji transakcji bankowości elektronicznej, a wszelkie próby zmiany autoryzacji powinny być rejestrowane i poddawane uwadze kierownictwa.

Banki powinny podejmować odpowiednie kroki w celu zachowania poufności podstawowych informacji bankowości elektronicznej. Środki podejmowane w celu zachowania poufności powinny odpowiadać wrażliwości przekazywanych informacji i/lub informacji przechowywanych w bazach danych.

Poufność oznacza zapewnienie, że podstawowe informacje pozostaną prywatnymi informacjami banku oraz, że osoby nieupoważnione nie mają do nich wglądu, ani nie mogą z nich korzystać. Nadużywanie lub nieautoryzowane ujawnienie danych naraża bank na ryzyko prawne i ryzyko reputacji. Powstanie bankowości elektronicznej stwarza dodatkowe wyzwania dla banków, ponieważ zwiększa ryzyko, że informacje przekazywane za pośrednictwem publicznej sieci lub przechowywane w bazach danych staną się dostępne dla nieupoważnionych lub niewłaściwych stron, a także ryzyko ich wykorzystania w sposób niezgodny z intencją klienta udzielającego informacji. Ponadto, zwiększone korzystanie z usługodawców może umożliwiać dostęp innych stron do kluczowych danych banku.

W celu sprostania wyzwaniom w zakresie zachowania poufności kluczowych informacji bankowości elektronicznej, banki muszą upewnić się, czy:

- dostęp do wszystkich poufnych danych i zapisów banku posiadają wyłącznie odpowiednio upoważnione i potwierdzone osoby, agenci lub systemy,

- wszystkie poufne dane banku są przechowywane w bezpieczny sposób i chronione przed nieautoryzowanym wglądem lub modyfikacją podczas transmisji za pośrednictwem publicznych, prywatnych lub wewnętrznych sieci,
- w sytuacji, gdy strony trzecie mają dostęp do danych poprzez relacje związane ze zlecaniem usług na zewnątrz, należy przestrzegać stosowanych przez bank standardów i mechanizmów kontroli wykorzystania i ochrony danych,
- każdy dostęp do danych zastrzeżonych wymaga autoryzacji, a bank podejmuje odpowiednie działania w celu uniemożliwienia manipulacji identyfikatorami dostępu.

V. ZARZĄDZANIE RYZYKAMI

Komitet Bazylejski zauważył, że bezprecedensowa szybkość zmian w zakresie innowacji technologicznych i obsługi klienta, wszechobecny, globalny charakter otwartych sieci elektronicznych, integracja aplikacji bankowości elektronicznej z pozostałymi systemami informatycznymi oraz rosnące uzależnienie banków od stron trzecich dostarczających niezbędnej technologii informatycznej nie tworząc całkowicie nowych ryzyk zwiększyły i zmodyfikowały niektóre tradycyjne ryzyka związane z działalnością bankową, w szczególności ryzyko operacyjne, prawne i reputacji, wywierając przez to wpływ na ogólny profil ryzyka bankowości. Banki powinny zatem identyfikować, analizować i w sposób ostrożnościowy zarządzać ryzykami występującymi w systemach informatycznych.

Ryzyko operacyjne[3], które należy rozumieć jako ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów lub zdarzeń zewnętrznych, powinno być za pomocą narzędzi do kontroli i zarządzania ryzykiem, analizowane a następnie minimalizowane.

Zarządzanie ryzykiem operacyjnym obejmuje adekwatną kontrolę ze strony kierownictwa banku, zapewniającą m.in. właściwe mechanizmy systemu kontroli wewnętrznej, procedury przeciwdziałające oszustwom, rzetelne plany utrzymania ciągłości pracy, politykę bezpieczeństwa oraz procedury obejmujące poważne modyfikacje systemów wewnętrznych.

Bank jest zobowiązany do zapewnienia swoim klientom ochrony danych osobowych i dostępności usług na poziomie zbliżonym do zapewnianego w przypadku transakcji realizowanych za pośrednictwem tradycyjnych bankowych kanałów dystrybucji.

Banki powinny podejmować odpowiednie kroki w celu zapewnienia przestrzegania wymagań w zakresie ochrony danych o klientach obowiązujących w jurysdykcjach, w których bank oferuje produkty lub świadczy usługi.

Zachowanie poufnego charakteru danych o kliencie jest podstawowym obowiązkiem banku. Niewłaściwe użycie lub ujawnienie poufnych danych o kliencie bez upoważnienia naraża bank zarówno na ryzyko prawne jak i ryzyko reputacji. W celu sprostania wyzwaniom w zakresie zachowania poufnego charakteru informacji o kliencie, banki powinny podejmować wszelkie wysiłki w celu zapewnienia, że:

- stosowana przez bank polityka i standardy poufności danych o klientach są zgodne ze wszystkimi ustawami i regulacjami obowiązującymi w jurysdykcjach, w których bank oferuje produkty lub świadczy usługi,
- klienci posiadają znajomość regulacji banku dotyczących ochrony danych oraz związanych z nimi zagadnień poufności w zakresie produktów i usług bankowości elektronicznej,

[3] Definicja przyjęta za Bazylejskim Komitetem ds. Nadzoru Bankowego

- klienci mają możliwość nie wyrażenia zgody na przekazywanie przez bank osobom trzecim dla celów wzajemnego marketingu wszelkich informacji dotyczących ich potrzeb osobistych, interesów, pozycji finansowej i korzystania z usług bankowych,
- dane o klientach nie są wykorzystywane dla celów niezgodnych z przeznaczeniem lub dla celów nie wynikających z upoważnień udzielonych przez klientów,
- strony trzecie posiadające dostęp do danych o klientach w wyniku realizacji umów o zlecanie usług są zobowiązane do przestrzegania standardów banku w zakresie tych danych.

Dobrą praktyką jest przestrzeganie następujących zasad:
- Bank powinien używać odpowiednich technik kryptograficznych, szczególnych protokołów lub innych mechanizmów kontroli bezpieczeństwa, zapewniających poufność danych o klientach.

- Bank powinien opracować odpowiednie procedury i mechanizmy kontrolne w celu okresowej oceny swej infrastruktury i protokołów w zakresie bezpieczeństwa klientów.

- Bank powinien upewniać się, że realizowana przez współpracujących z nim dostawców usług będących stronami trzecimi polityka w zakresie poufności i prywatności informacji jest spójna z polityką banków.

- Bank powinien podejmować odpowiednie kroki w celu poinformowania klientów o zasadach poufności i prywatności stosowanych wobec informacji na ich temat. Kroki te mogą obejmować:
  - instruowanie klientów na temat potrzeby ochrony ich haseł, osobistych numerów identyfikacyjnych (PIN) oraz innych danych bankowych i/lub osobowych.
  - informowanie klientów na temat polityki banku w sprawie poufności danych; podstawowe znaczenie dla zapewnienia pełnego zrozumienia polityki poufności przez klienta ma stosowanie jasnego i zwięzłego języka; jest prawdopodobne, że większość klientów nie przeczyta długich, choć precyzyjnych, opisów prawnych; dla klientów bankowości elektronicznej dopuszczalne jest umiejscawiania ww. informacji na stronie internetowej banku.
  - klientom bankowości elektronicznej należy dostarczać informacji dotyczących ogólnego bezpieczeństwa ich komputera osobistego, w tym korzyści płynących ze stosowania oprogramowania antywirusowego, mechanizmów kontroli fizycznego dostępu i osobistych rozgraniczeń od statycznych połączeń internetowych.

Bank powinien posiadać zdolność efektywnego świadczenia usług, zapewniać ciągłość działalności oraz posiadać procesy planowania awaryjnego w celu zapewnienia dostępności systemów i usług.

W związku z koniecznością zabezpieczenia banków przed ryzykiem gospodarczym, prawnym i ryzykiem reputacji, usługi muszą być świadczone w sposób i w czasie zgodnym z oczekiwaniami klientów. Osiągnięcie tego celu wymaga zdolności banku do dostarczania usług użytkownikom końcowym ze źródeł podstawowych (np. wewnętrzne systemy lub aplikacje banku) lub wtórnych.(np. systemy lub aplikacje usługodawców). Utrzymanie adekwatnego

poziomu dostępności usług zależy także od zdolności awaryjnych systemów podtrzymywania do redukcji zagrożeń wynikających z ataków wiążących się z blokowaniem usług, bądź z innych zdarzeń, które mogą spowodować zakłócenia prowadzonej działalności.

Wyzwania dla zachowania ciągłej dostępności systemów i aplikacji mogą być poważne biorąc pod uwagę możliwość wystąpienia dużego popytu na transakcje, szczególnie w godzinach szczytu. Ponadto, znaczenie dużej zdolności świadczenia usług, ciągłości działalności i planowania awaryjnego zwiększają duże oczekiwania klientów dotyczące krótkiego cyklu przetwarzania transakcji ich stałej dostępności (24 godziny x 7 dni). W celu zapewnienia klientom zgodnej z ich oczekiwaniami dostępności usług bankowości, banki muszą zapewnić, że:

- bieżąca pojemność systemów i ich przyszłe możliwości zostały zanalizowana w świetle ogólnej dynamiki rynku elektronicznej działalności handlowej (transakcje bezgotówkowe i bankowość elektroniczna) i przewidywanego poziomu akceptacji produktów i usług elektronicznej działalności handlowej przez klientów,
- dokonuje się oszacowań, testowania awaryjnego i okresowych analiz zdolności przetwarzania transakcji bankowości elektronicznej,
- istnieją odpowiednie plany dotyczące ciągłości działalności podstawowych systemów przetwarzania i dostarczania usług elektronicznej działalności handlowej oraz plany awaryjne, które są poddawane okresowym testom.

Dobrą praktyka jest stosowanie następujących zasad:

- Wszystkie usługi i aplikacje elektronicznej działalności handlowej, w tym dostarczane przez usługodawców będących stronami trzecimi, należy identyfikować i oceniać pod względem ich znaczenia.

- Należy dokonywać oceny ryzyka w odniesieniu do każdej podstawowej usługi i aplikacji, w tym oceny potencjalnego wpływu wszelkich zakłóceń działalności na ryzyko kredytowe banku oraz jego ryzyko rynkowe, płynności, prawne, operacyjne i ryzyko reputacji.

- Należy ustanowić kryteria funkcjonowania dla każdej podstawowej usługi i aplikacji. Poziom usług powinien być monitorowany pod kątem takich kryteriów. Należy podejmować odpowiednie środki w celu zapewnienia, że systemy mogą obsłużyć dużą i małą liczbę transakcji oraz, że funkcjonowanie i pojemność systemów są zgodne z oczekiwaniami banku w zakresie przyszłego rozwoju elektronicznej działalności handlowej.

- Należy rozważyć opracowanie alternatywnych rozwiązań przetwarzania danych, aby sprostać popytowi, gdy systemy bankowości elektronicznej osiągną określone pułapy zdolności przetwarzania.

- Należy sformułować plany ciągłości bankowości elektronicznej uwzględniające wszelkie uzależnienia od dostawców usług będących stronami trzecimi oraz wszelkie inne zewnętrzne uzależnienia wymagane dla przywrócenia działalności.

- Plany awaryjne dotyczące bankowości elektronicznej powinny określić proces przywracania lub zastępowania zdolności przetwarzania bankowości elektronicznej, rekonstrukcji informacji wspierających transakcje i obejmować, podejmowane w przypadku zakłócenia

działalności, środki służące wznowieniu dostępności podstawowych systemów i aplikacji bankowości elektronicznej.

Bank powinien opracować odpowiednie plany reagowania na incydenty służące zarządzaniu, przeciwdziałaniu i minimalizacji problemów wynikających z nieoczekiwanych zdarzeń, w tym ataków wewnętrznych i zewnętrznych, które mogą szkodzić funkcjonowaniu systemów i świadczeniu usług bankowości elektronicznej.

Efektywne mechanizmy reagowania na incydenty mają podstawowe znaczenie dla minimalizowania ryzyka operacyjnego, prawnego, i ryzyka reputacji, które są skutkiem nieoczekiwanych zdarzeń, takich jak ataki wewnętrzne i zewnętrzne, i mogą wpływać na funkcjonowanie systemów i świadczenie usług bankowości elektronicznej. Bank powinien opracowywać odpowiednie plany reagowania na incydenty, w tym strategie komunikowania się, które zapewniają ciągłość prowadzonej działalności, kontrolę ryzyka reputacji i ograniczają zobowiązania związane z zakłóceniami świadczonych przez banki usług bankowości elektronicznej, w tym z zakłóceniami funkcjonowania systemów i usług zleconych na zewnątrz.

W celu zapewnienia efektywnego reagowania na nieprzewidziane incydenty, Bank powinien opracować:

- Plany reagowania na incydenty uwzględniające przywracanie systemów i usług w różnych scenariuszach, różnej działalności i lokalizacjach geograficznych. Analizy scenariuszy powinny uwzględniać kwestię prawdopodobieństwa wystąpienia ryzyka oraz jego wpływ na bank. Systemy bankowości elektronicznej zlecone usługodawcom będącym stronami trzecimi powinny stanowić integralną część tych planów.
- Mechanizmy służące niezwłocznemu wykrywaniu incydentu lub sytuacji kryzysowej, oceny ich istotności oraz kontrolowaniu ryzyka reputacji związanego z zakłóceniami usług.
- Strategię komunikacji w adekwatny sposób uwzględniającą kwestie kontaktu z rynkiem zewnętrznym i mediami w przypadku naruszenia bezpieczeństwa, ataków sieciowych i/lub awarii systemów bankowości elektronicznej.
- Jasno określony proces alarmowania właściwych władz nadzorczych w przypadkach wystąpienia istotnego naruszenia bezpieczeństwa lub zakłóceń działalności.
- Powołać zespoły ds. reagowania na incydenty dysponujące uprawnieniami umożliwiającymi podejmowanie działań w nagłych okolicznościach, przeszkolone w zakresie analizy wykrywania incydentów/systemów reagowania oraz interpretowania znaczenia ich skutków.
- Jasno określony system podległości obejmujący zarówno operacje wewnętrzne jak i zlecone, zapewniający podejmowanie natychmiastowych działań odpowiadających powadze incydentu. Ponadto, należy opracować procedury dotyczące powiadamiania i komunikacji wewnętrznej, które, jeśli właściwe, powinny obejmować informowanie kierownictwa banku.
- Proces zapewniający właściwy tryb i czas informowania odpowiednich stron zewnętrznych, w tym klientów banku, kontrahentów i media, o rozwoju wydarzeń w zakresie istotnych przypadków zakłóceń bankowości elektronicznej oraz o wznawianiu tej działalności.
- Proces gromadzenia i zabezpieczania dowodów sądowych, umożliwiających odpowiednie późniejsze analizy wszelkich incydentów dotyczących bankowości elektronicznej, jak również pomagających w ściganiu osób odpowiedzialnych za ataki.

Bank powinien udostępniać odpowiednie informacje na swych stronach internetowych, które umożliwią ich potencjalnym klientom wyciągnięcie dobrze ugruntowanych wniosków na temat tożsamości banku oraz jego statusu prawnego przed rozpoczęciem realizacji transakcji bankowości elektronicznej.

Przykłady informacji, które bank może udostępnić na swej stronie internetowej obejmują:

- nazwę banku oraz miejsce lokalizacji jego siedziby i placówek lokalnych,
- sposób kontaktowania się z centrum obsługi klientów banku w sprawach dotyczących problemów w zakresie usług, skarg, podejrzewanych przypadków nadużycia rachunków, etc.,
- informacje na temat instytucji nadzoru bankowego (lub zamieszczenie przejścia na stronę internetową, które zawierają takie informacje).

Kierownictwo banku jest odpowiedzialne za zapewnienie jasności co do najważniejszych ryzyk w organizacji i wyjaśnienie bankowych polityk podejmowania lub unikania ryzyka. Polityki powinny być jasno sformułowane, udokumentowane i zakomunikowane wszystkim właściwym szczeblom pracowniczym.

Kierownictwo banku winno być świadome, że ostateczna odpowiedzialność za zarządzanie ryzykiem należy do niego i w sytuacji delegowania zadań na szczeble kierownicze, należy zapewnić, że cechy delegowania są odpowiednio przedstawione i precyzyjnie rozumiane. Polityki kontrolowania ryzyka są przenoszone na widoczne procedury organizacyjne i administracyjne oraz zintegrowane z systemami informatycznymi i codziennymi czynnościami właściwego personelu. Powinien być prowadzony systematyczny monitoring zgodności z regulacjami.

Kierownictwo banku powinno być świadome, że istniejący system kontroli wewnętrznej do zarządzania ryzykiem ma także możliwości generowania efektywności kosztowej.

Kierownictwo banku powinno być świadome, że przejrzyste i aktywne podejście do zarządzania ryzykiem może kreować przewagę konkurencyjną.

Kierownictwo banku powinno dołożyć starań, aby system zarządzania ryzykiem był wbudowany w działające procedury, odpowiadał szybko na zmieniające się ryzyka i raportował niezwłocznie do odpowiednich poziomów zarządzania.

VI. AUDYT INFORMATYCZNY I NADZÓR

Zadaniem audytu informatycznego jest m. in. zbadanie czy proces zarządzania ryzykiem jest adekwatny do potencjalnych zagrożeń i zapewnia wystarczającą ochronę aktywów/zasobów i informacji, oraz czy kontrola w obszarze całej infrastruktury informatycznej jest realizowana w sposób efektywny i skuteczny, zgodnie z przyjętymi standardami i kryteriami.
Do zadań audytu informatycznego należy również zbadanie bezpieczeństwa systemów informatycznych.

Audyt informatyczny powinien być przeprowadzany regularnie, a dodatkowo każdorazowo po wprowadzeniu istotnych zmian w systemach informatycznych.
Aby wyniki audytu informatycznego były wiarygodne musi on być niezależny i odnosić się do uznanych standardów międzynarodowych, dotyczących badania i oceny bezpieczeństwa informacji w systemach informatycznych. Do takich standardów należą na przykład:

- standardy audytowania systemów informatycznych ISACA (Information Systems Audit and Control Asociation),
- COBIT (Control Objectives for Information and related Technology) opracowany przez IT Governance Institute,
- standardy Institute of Internal Auditors Inc.
- standard COSO (Committee of Sponsoring Organisations of the Trade Commission).

A. KONTROLA WEWNĘTRZNA

Władze banku są odpowiedzialne za powołanie, w ramach kontroli instytucjonalnej, komórki odpowiedzialnej za audyt systemów informatycznych.

W celu osiągnięcia wysokiej jakości wewnętrznego audytu informatycznego władze banku powinny zapewnić niezależność audytu i regularnie badać zgodność raportów audytu wewnętrznego z zakresem zadań ujętych w planie rocznym oraz skuteczność usuwania nieprawidłowości i słabości wskazywanych w raporcie.

Do zadań kontroli wewnętrznej należy kontrola czy bank posiada:

- pisemne zasady polityki i procedury zabezpieczeń i zarządzania bezpieczeństwem systemów informatycznych z uwzględnieniem bankowości elektronicznej[5] oraz czy są one prawidłowo realizowane,
- wykaz zbiorów stanowiących księgi rachunkowe na nośnikach danych,
- dokumentację systemu elektronicznego przetwarzania danych, zgodną z obowiązującymi przepisami,

[4] Gdy bank prowadzi działalność bankowości elektronicznej.
[5] Gdy bank prowadzi działalność bankowości elektronicznej.

a także czy zapewnione są:

- merytoryczna, formalna i prawna prawidłowość wyceny aktywów i pasywów,
- kompletność i niezawodność działania programów kontroli bieżącej,
- szybki dostęp do terminowych, pełnych i rzetelnych informacji dla celów operacyjnych,
- prawidłowe informacje zarządcze dla kierownictwa banku,
- poprawna i terminowa sprawozdawczość dla instytucji zewnętrznych,
- archiwizowanie i ochrona danych zgodna z obowiązującymi przepisami.

Inspektorzy, audytorzy lub specjaliści powinni systematycznie przeprowadzać niezależne testy bezpieczeństwa systemu i kontrolę procedur. Częstotliwość i głębokość badań testowych związanych z danym obszarem działalności powinna być odpowiednio dostosowana do poziomu ryzyka, poziomu zabezpieczenia i niezawodności bieżących procedur kontrolnych.

Większość aplikacji bankowych zawiera narzędzia kontrolne, a także tworzy raporty służące zabezpieczaniu i ochronie informacji. Instrumenty kontroli wewnętrznej powinny zapewniać możliwość identyfikowania słabych punktów zabezpieczenia systemów użytkowanych przez bank i przypadków odstąpienia od wymaganej kontroli wstępnej, zwłaszcza operacji o podwyższonym stopniu ryzyka. Krytyczne zbiory i programy muszą być szczególnie chronione przed nie autoryzowanymi zmianami. Należy zwrócić uwagę, aby osoby zatrudniane w obszarach decydujących o bezpieczeństwie całego systemu, miały predyspozycje psychiczne i moralne, były odpowiednio przeszkolone a wyznaczone im zakresy obowiązków powinny być tak określone, aby czynności nie były zmonopolizowane w stopniu utrudniającym bieżącą kontrolę ich legalności.

Kierownictwo banku odpowiada za określenie ścieżek audytu w zakresie transakcji bankowości elektronicznej.

Świadczenie usług finansowych za pośrednictwem elektronicznych kanałów dystrybucji może utrudniać stosowanie i egzekwowanie wewnętrznych mechanizmów kontrolnych i utrzymywanie jasno określonych ścieżek audytu, jeśli bank nie przyjmie odpowiednich środków w odniesieniu do środowiska bankowości elektronicznej. Wyzwaniem dla banku jest nie tylko zapewnienie efektywnej kontroli wewnętrznej w wysoko zautomatyzowanych środowiskach, lecz także zapewnienie niezależnego audytu mechanizmów kontrolnych, szczególnie jeśli dotyczą one najważniejszych zdarzeń i aplikacji bankowości elektronicznej.
Jeśli bank nie jest w stanie zachować jasno określonych ścieżek audytu w odniesieniu do prowadzonej przez siebie elektronicznej działalności bankowej, może wystąpić osłabienie wewnętrznej kontroli. Dzieje się tak ponieważ większość (a czasami wszystkie) posiadane dane i dowody mają postać elektroniczną. Dokonując ustaleń, w jakich obszarach należy zachować jasno określone ścieżki audytu, należy rozważyć następujące rodzaje transakcji bankowości elektronicznej:

- otwieranie, modyfikację lub zamykanie rachunku klienta,
- wszelkie transakcje mające konsekwencje finansowe,
- wszelkie udzielone klientowi upoważnienia do przekroczenia limitu,
- wszelkie przypadki udzielenia, modyfikacji lub cofnięcia praw lub przywilejów dostępu do systemów.

Dobrą praktyka jest aby:

- wszystkie transakcje bankowości elektronicznej były w odpowiedni sposób rejestrowane w celu ustanowienia jasno określonej ścieżki audytu oraz pomocy w rozwiązywaniu sporów.
- systemy bankowości elektronicznej były zaprojektowane i zainstalowane w taki sposób aby umożliwiały wychwycenie i zabezpieczenie dowodów sądowych (tzn. adekwatną kontrolę dowodów, a także zapobieganie manipulacjom oraz gromadzeniu fałszywych dowodów).
- w przypadkach, gdy za systemy przetwarzania danych i związane z nimi ścieżki audytu odpowiada usługodawca będący stroną trzecią:
  - bank upewnił się, że posiada dostęp do odpowiednich ścieżek audytu utrzymywanych przez usługodawcę,
  - oraz, że ścieżki audytu utrzymywane przez usługodawcę spełniają standardy banku.

B. KONTROLA ZEWNĘTRZNA

Zarząd banku może również zlecić audytorom zewnętrznym, w trakcie przeprowadzanego przez nich badania sprawozdań finansowych, lub w formie odrębnej ekspertyzy, ocenę słabych stron i niedoskonałości systemów informatycznych. Planowanie, przygotowanie i przeprowadzenie kontroli przez komórkę kontroli wewnętrznej oraz zlecanie kontroli niezależnym specjalistom wyższego szczebla zarządzania i profesjonalnym organizacjom zewnętrznym, specjalizującym się w badaniu prawidłowego funkcjonowania standardów w zakresie ochrony danych jest czynnikiem wzmacniającym bezpieczeństwo funkcjonowania systemów informatycznych.

Niezależny audyt zewnętrzny powinien zweryfikować prawidłowość wyników uzyskanych przez audyt wewnętrzny oraz uzupełnić go o specjalistyczne badania.

Audyt zewnętrzny może być przeprowadzany dla całego banku, lub dla wybranego obszaru działalności.

C. ZALECENIA NADZORCZE

Nadzór bankowy będzie dokonywał oceny zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym, w tym czy systemy informatyczne i telekomunikacyjne spełniają obowiązujące przepisy i normy.

Z nadzorczego punktu widzenia, mającego na celu zapewnienie bezpieczeństwa środków pieniężnych, zgromadzonych na rachunkach bankowych oraz tajemnicy bankowej, nadzór bankowy podczas inspekcji na miejscu będzie oceniał czy sposób zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym zapobiega powstawaniu zagrożeń i gwarantuje szybkie ujawnienie i naprawienie popełnionych błędów i nieprawidłowości oraz eliminuje powstanie ich w przyszłości, a w szczególności , że bank

- posiada i realizuje procedury zarządzania technologią informatyczną;
- posiada i realizuje zasady polityki bezpieczeństwa, w tym: procedury identyfikacji użytkowników, jednoznacznego potwierdzania i rejestracji korzystania z zasobów systemu;
- posiada opracowane i wdrożone procedury awaryjne;
- posiada opracowane i wdrożone plany rozwoju systemów informatycznych i sieci;
- posiada określone i funkcjonujące metody dotyczące zabezpieczeń zasobów informatycznych, w tym zabezpieczeń fizycznych;
- posiada procedury postępowania zapewniające odpowiednie monitorowanie i zarządzanie ryzykami;
- posiada opracowane i przyjęte w banku procedury audytu wewnętrznego;
- posiada efektywnie działającą komórkę odpowiedzialną za kontrolę wewnętrzną bezpieczeństwa systemów informatycznych;
- posiada opracowaną i wdrożoną politykę szkoleń użytkowników końcowych.

Okresowo dokonywane badania mogą obejmować również wpływ rozwiązań organizacyjnych, przyjęty podział kompetencji, upoważnienia dostępu udzielone użytkownikom itp. na poziom bezpieczeństwa systemu.

Inspektorzy nadzoru bankowego i audytorzy przeprowadzający kontrolę powinni uzyskać wyczerpujące wyjaśnienia na temat procedur, budowy systemu i zabezpieczeń od kompetentnych pracowników banku.

SPIS TREŚCI

Opracowano:

w Wydziale Informatyki
Biura Polityki Nadzorczej GINB

Aprobował:

Wojciech Kwaśniak
Generalny Inspektor Nadzoru Bankowego