NBP

Narodowy Bank Polski
Generalny Inspektorat
Nadzoru Bankowego

Rekomendacja D

z dnia 20 października 1997 r.

dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki

Warszawa, 1997 r.

NBP
N a r o d o w y B a n k P o l s k i
Generalny Inspektorat Nadzoru Bankowego

NB/ZPN/ 790 /97 Warszawa, 1997-10-20

PREZESI BANKÓW
wszystkich

Obserwowany w ostatnich latach szybki rozwój w dziedzinie systemów komputerowych i telekomunikacyjnych stawiają przed bankami nowe zadania w zakresie prac związanych z rozwojem własnych systemów przetwarzania danych, a szczególnie ich solidnością i niezawodnością.

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 systemu płatności przepływ środków pieniężnych odbywa się w skali całego świata a problemy dotyczące systemów informatycznych i telekomunikacyjnych mogą przyczynić się do niewypłacalności banku. Nie wywiązanie się z zobowiązań umownych, a także inne zakłócenia, czasem płynące też z banków o dobrym standingu finansowym, poprzez reakcję łańcuchową, mogą narazić każdy bank na straty, powodując paraliż i zagrożenie dla całego systemu finansowego.

Zapisy w księgach handlowych banku, tworzone w wyniku elektronicznego przetwarzania danych, informacje i dokumenty rutynowo transmitowane przez publiczne linie telekomunikacyjne (kablowe, radiowe i satelitarne), pomiędzy jednostkami organizacyjnymi banku, różnymi bankami, ich korespondentami i klientami narażone są na różnego typu ryzyko. Wielu użytkowników, włączając pracowników banku i klientów, ma bezpośredni dostęp do informacji. Wszystkie obszary działalności, a szczególnie usługi

udoskonalone, zindywidualizowane zgodnie z potrzebami klientów z nich korzystających i operacje zewnętrzne, charakteryzują się zwiększonym stopniem ryzyka naruszenia poufności, popełnienia błędu, oszustwa, czy też niewłaściwego wykorzystania informacji.

Rodzaje ryzyka występujące w systemach informatycznych są generalnie takie same, jak wchodzące w grę w ukształtowanych wcześniej strukturach. Jednak w porównaniu z systemami ręcznymi, w systemie elektronicznego przetwarzania danych szczególne niebezpieczeństwo bezprawnego ujawnienia poufnych informacji polega na możliwości przeniesienia większej ilości, materialnie istotniejszych informacji, w bardziej wygodny i metodologicznie dostępny sposób (np. kopie na taśmach lub dyskietkach) bez pozostawienia śladów nie autoryzowanego dostępu.

Obroty i stan środków na rachunkach klientów, wysokość linii kredytowych dla poszczególnych klientów, wielkość i rodzaj jednostkowych transakcji należą niewątpliwie do informacji poufnych. Trafienie ich w niepowołane ręce może zaszkodzić reputacji banku, jego profesjonalnym związkom z klientami, a także zaowocować zwiększoną ilością reklamacji. Do informacji, których poufność jest niezwykle ważna należą też plany strategiczne banku i korespondencja z klientami sporządzane i przechowywane w formie plików tekstowych.

Jest to wystarczający powód, aby bank przywiązywał należytą wagę do zagadnień adekwatności procedur zabezpieczających i kontrolnych. Poziom kontroli powinien być proporcjonalny do niebezpieczeństwa naruszenia poufności, integralności i dostępności zasobów, a także skutków potencjalnych strat materialnych oraz moralnych dla klienta i banku.

Szczególną uwagę należy skierować również na czynniki mogące spowodować uszkodzenia systemów i utratę danych lub oprogramowania co w konsekwencji stanowiłoby przeszkodę efektywnego funkcjonowania operacji bankowych dokonywanych w sieci.

W nowych systemach informatycznych dominuje tendencja dużej personalizacji i autonomiczności urządzeń, są one związane z pojedynczą osobą, często w pełni odpowiedzialną za rozwój, testowanie, wdrożenie i działania operacyjne na wybranej części programu. W tej sytuacji znacznie wzrasta rola stosowania odpowiednich procedur i obchodzenia się z danymi w sposób zgodny z obowiązującymi w jednostce standardami.

Zdaniem Generalnego Inspektoratu Nadzoru Bankowego ryzyko związane z systemami informatycznymi może wzrastać w związku ze wskazanymi czynnikami.

Pragniemy też zwrócić Państwa uwagę na fakt, iż integracja naszego kraju ze strukturami europejskimi musi skutkować w niedalekiej przyszłości dążeniem do harmonizacji przepisów. I tak np. rozwiązania funkcjonujące w krajach Unii Europejskiej nakładają na banki np. w zakresie adekwatności kapitałowej (Dyrektywa Rady 93/6/EEC z dnia 15 marca 1993 r. w sprawie adekwatności kapitału firm inwestycyjnych i instytucji kredytowych) obowiązek podziału na księgę bankową i handlową i stosowne obciążanie kapitału. Są to techniczne wymagania w zakresie kalkulacji statystycznej pewnych ryzyk wymuszające wręcz stosowanie bardzo zaawansowanych systemów informatycznych.

Nasze Rekomendacje mają w pewnym stopniu zasygnalizować problem i zapewnić lepsze przygotowanie banków w zakresie zarządzania ryzykami towarzyszącymi systemom informatycznym w przyszłości.

W załączeniu przekazujemy Rekomendację, która ma na celu zasygnalizowanie jedynie głównych problemów, których świadomość powinni mieć kierujący wyżej wymienionymi obszarami i je nadzorujący. Generalny Inspektorat Nadzoru Bankowego pragnie zwrócić uwagę Zarządu banku, jako kierownictwa najwyższego szczebla, na istniejące zagrożenia i konieczność opracowania, wdrożenia i przestrzegania właściwych procedur ostrożnościowych.

Generalny Inspektor
Nadzoru Bankowego

/--/

Ewa Śleszyńska-Charewicz

Rekomendacja D

z dnia 20 października 1997 r.

dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki

Definicje i przydatne słownictwo

aktywa programowe (software) - oprogramowanie użytkowe (aplikacje), oprogramowanie systemowe, oprogramowanie narzędziowe,

aktywa fizyczne (hardware) - wyposażenie komputerowe, wyposażenie komunikacyjne, nośniki informacji (np. taśmy, dyski), inne wyposażanie techniczne (urządzania zasilające, klimatyzacja, meble),

aktywa informatyczne - wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne fizyczne, komunikacyjne lub ludzkie w systemie informatycznym lub działalności informatycznej,

analiza ryzyka - wszechstronna ocena różnego typu elementów ryzyka związanych z systemami informatycznymi -systematyczna metoda identyfikowania zagrożeń i podatności systemu na te zagrożenia - jakością informacji zarządczej dla kierownictwa i definiowaniem nadużyć (przestępstw, złego wykorzystywania komputerów - także mających wpływ na niewłaściwą jakość informacji zarządczych i związanych z tym skutków błędnych decyzji kierownictwa),

aplikacja - program komputerowy używany do wykonywania konkretnych zadań; termin używany zamiennie z terminem "program",

poufność - zabezpieczenie przed nieuprawnionym ujawnieniem danych; właściwość przypisana do danych określająca, do jakiego stopnia dane te nie mogą zostać udostępnione lub ujawnione nieuprawnionym osobom, podmiotom lub procesom,

integralność - zabezpieczenie przed nieuprawnioną zmianą danych i ich usuwaniem; pewność w każdych warunkach, że system będzie odznaczał się logiczną poprawnością i

niezawodnością, logiczną kompletnością sprzętu i oprogramowania, wdrażającego mechanizmy ochrony oraz procedury zapewniające spójność struktur i rzetelność przechowywanych danych,

integralność systemu - właściwość systemu informatycznego spełniającego swe cele eksploatacyjne, polegająca na zapobieganiu modyfikacji zasobów lub ich wykorzystywaniu przez użytkowników nieuprawnionych i/lub zapobieganiu niewłaściwej modyfikacji zasobów lub ich niewłaściwemu wykorzystywaniu przez użytkowników uprawnionych,

dostępność - zapewnienie dostępu do danych i usług na żądanie uprawnionego użytkownika,

gestor danych - statutowy organ, osoba czy też organizacja odpowiedzialne za szczególną kategorię informacji lub aktualne dane zawarte w informacji lub określone typy danych, do których należy sygnalizowanie użytkownikom i zarządzającym danymi potrzeby stosowania pewnych procedur obsługi danych związanych z zabezpieczeniem,

inspektor zabezpieczenia systemu - osoba odpowiedzialna za zabezpieczenie zautomatyzowanego systemu informatycznego, mająca uprawnienia do egzekwowania stosowania środków zabezpieczenia przez wszystkich innych, którzy mają dostęp do systemu,

zabezpieczenie systemu informatycznego - ochrona danych i zasobów przed przypadkowymi lub złośliwymi czynami, polegająca zwykle na podjęciu właściwych działań,

zabezpieczenie - zapewnienie poufności, integralności i dostępności informacji szczególnie wrażliwych, o doniosłym znaczeniu dla banku lub jego klienta, przed nieuprawnionymi użytkownikami,

kierownictwo banku - Zarząd, Rada Banku.

zasób - składnik systemu spełniający żądaną rolę prezentacji, pamiętania, transmisji lub przetwarzania,

zabezpieczenie administracyjne - ograniczenia wprowadzane przez kierownictwo tj. procedury operacyjne, administracyjne i rozliczeniowe, a także uzupełniające czynniki nadzorujące, ustanowione w celu zapewnienia dopuszczalnego poziomu ochrony danych,

zabezpieczenie danych - ochrona danych przed nieuprawnioną (przypadkową lub zamierzoną) modyfikacją, zniszczeniem lub ujawnieniem,

zabezpieczenie fizyczne - środki zastosowane w celu fizycznej ochrony zasobów przed umyślnymi lub przypadkowymi zagrożeniami,

zabezpieczenie informacji - system informatyczny wraz z zabezpieczeniem komunikacji składającym się z wytycznych i procedur administracyjnych, przeznaczony do identyfikacji, nadzoru i ochrony informacji przed nieuprawnionym ujawnieniem,

zabezpieczenia organizacyjne - administracyjne środki zapewnienia zabezpieczenia systemu informatycznego,

incydent zabezpieczenia systemu informatycznego - niekorzystne zdarzenie związane z systemem informatycznym, które według wewnętrznych reguł lub zaleceń dotyczących zabezpieczenia jest awarią i/lub powoduje domniemane lub faktyczne naruszenie ochrony informacji, albo powoduje naruszenie własności,

polityka zabezpieczenia - zestaw reguł określających wykorzystanie informacji, łącznie z jej przetwarzaniem, przechowywaniem, dystrybucją i prezentacją, niezależnie od wymagań dotyczących zabezpieczenia i celów zabezpieczenia,

polityka zabezpieczenia systemów organizacji - zbiór praw, reguł i wskazówek praktycznych, które ustalają sposób, w jaki aktywa informatyczne obejmujące informacje wrażliwe są zarządzane, chronione i rozpowszechniane wewnątrz organizacji, która je wykorzystuje,

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

Rekomendacje

1. Rola kierownictwa banku w zarządzaniu bezpieczeństwem systemów informatycznych

1.1. Nadzór kierownictwa

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

Zapewnienie poufności, integralności i dostępności danych wymaga opracowania odpowiednich procedur i zasad kontroli ich realizacji. Kierownictwo banku powinno ustanowić, w formie pisemnej, przejrzyste zasady polityki bezpieczeństwa i wykazać pełne poparcie dla jej realizacji w całym procesie zarządzania zabezpieczeniami. Do zadań Zarządu banku należy przede wszystkim ustanowienie adekwatnych procedur i wymagań dotyczących zabezpieczenia, pozwalających na zminimalizowanie prawdopodobieństwa wystąpienia negatywnych zdarzeń. Prewencyjne działania Zarządu banku powinny również znaleźć wyraz w szczególnie starannym zaprojektowaniu i lokalizacji centrum komputerowego.

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

Z uwagi na rodzaj działalności banku jako instytucji publicznego zaufania, dużą ilość informacji charakteryzować będzie wysoki stopień wrażliwości na utratę lub ujawnienie. Określając poufność należy wyraźnie wskazać, które informacje i w jakim okresie powinny podlegać bez względu na formę absolutnemu zakazowi publikacji (czasowe embargo na niektóre informacje). Niezbędne są również precyzyjne zasady dzielenia się informacją (przekazywanie danych).

Użytkowanie systemów informatycznych w banku może w określonych warunkach wymagać współpracy z zewnętrznymi specjalistami. Ustalenie form, metod i zakresu tej współpracy, należy do kompetencji kierownictwa banku, podobnie jak dopuszczenie zewnętrznych ekspertów do prac komitetu określającego politykę bezpieczeństwa systemów

informatycznych.

1.2. Polityka w zakresie zabezpieczenia systemów informatycznych

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. Oznacza to, że należy ustalić i realizować odpowiednią politykę zabezpieczenia, w tym politykę zabezpieczenia systemów organizacji, określającą organizacyjne zasady planowania i eksploatacji zabezpieczeń, powinna ona mieć najwyższą rangę i być dostępna dla wszystkich pracowników odpowiedzialnych za bezpieczeństwo informacji.

Polityka zabezpieczenia powinna zawierać co najmniej:

a/ zdefiniowanie systemu informatycznego, celów działania, wartości informacji przechowywanej w systemie,

b/ oświadczenie intencji i woli kierownictwa zachowania bezpieczeństwa informacji,

c/ definicje bezpieczeństwa informacji, w szczególności normujące kwestie udostępniania informacji, zdefiniowanie zagrożeń, określenie prawdopodobieństwa ich zaistnienia, rachunek kosztów zapewnienia skutecznej ochrony,

d/ określenie zasad polityki i standardowych wymagań dotyczących:
- zgodności postępowania z prawem i respektowania warunków umów dotyczących zabezpieczenia systemów,
- niezbędnego poziomu edukacji wymaganej dla zapewnienia bezpieczeństwa informacji,
- wykrywania i zapobiegania wirusom,
- zapewnienia ciągłości planowania i zatwierdzania zmian systemu, akceptowania i wdrażania nowych technologii informatycznych,
- tworzenia i utrzymania kopii zapasowych i archiwalnych

e/ definicje ogólnych i szczegółowych zakresów odpowiedzialności dla wszystkich obszarów zabezpieczenia informacji,

f/ określenie zasad raportowania wszelkich wykrytych lub podejrzewanych zjawisk, wskazujących na możliwość nadużyć, trybu ich usuwania, zapobiegania ponownemu wystąpieniu oraz zakres działań analitycznych dla zidentyfikowania słabych ogniw zabezpieczenia systemu; zasad realizacji krytycznych aplikacji w warunkach awaryjnych, katastrof lub klęsk żywiołowych (plany działań awaryjnych i plany odtwarzania działalności).

Dla zapewnienia bezpiecznego wykonywania przetwarzania informacji w banku niezbędne jest opracowanie właściwie udokumentowanych procedur i 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 problemów technicznych,
- sposób postępowania w przypadku załamania się pracy systemu (proces odtworzenia).

Z procedur obowiązujących w banku powinien jednoznacznie wynikać obowiązek oddzielenia funkcji operacyjnych od rozwojowych, a zwłaszcza: 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. Czynności testujące system i praca użytkowa powinny odbywać się na różnych komputerach, w różnych katalogach itp.. 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.

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 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 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.

1.3. Planowanie skali 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, 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.

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:

- 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 aktów prawnych wyłącznie z powodu przyjętych rozwiązań w systemie informatycznym.

Umowy zawierane z zewnętrznymi dostawcami sprzętu, oprogramowania i usług informatycznych powinny szczegółowo określać obowiązki i prawa stron oraz odpowiedzialność za wszelkie, w tym materialne skutki zdarzeń incydentalnych.

2. Infrastruktura zabezpieczeń i zarządzanie ochroną informacji

2.1. Analiza zagrożeń i metody zabezpieczeń

Realizacja zabezpieczeń następuje poprzez narzędzia zawarte w systemach operacyjnych (dla sieci i/lub stanowisk komputerowych), wyspecjalizowane oprogramowanie, zastosowanie rozwiązań sprzętowych, audyt, zarządzanie konfiguracją, a także działania organizacyjne, podejmowane profilaktycznie w przypadku 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 (podział procesu tworzenia oprogramowania na odrębne fazy: projektową, testową, modelową,

eksperymentalną wdrożeniową i eksploatacyjną).

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.

Na poziomie kierownictwa banku wymagane są:
- autoryzacja użytkownika z punktu widzenia realizacji celów i zadań banku (cele i warunki użytkowania),
- zatwierdzenie techniczne (poprawność zainstalowania, praca w sieci, komunikacja między użytkownikami).

2.2. Bezpieczeństwo dokumentacji systemowej

Dokumentacja systemów informatycznych może zawierać np. opis procesów zastosowania, opisy aplikacji systemowych, procedur, struktur danych, procesów autoryzacji itp. Z punktu widzenia przepisów o rachunkowości[1] powinna zawierać co najmniej:

[1]Por. ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591)

- wykaz zbiorów stanowiących księgi rachunkowe na komputerowych nośnikach magnetycznych,
- wykaz programów wraz z pisemnym stwierdzeniem dopuszczenia każdego nowego lub zmienionego programu do stosowania,
- opis przeznaczenia każdego programu, sposobu jego działania (reguły obliczeń, ewidencji, kontroli i wydruku danych) oraz wykorzystywania podczas przetwarzania danych,
- zasady ochrony danych, w tym tworzenia kopii zapasowych,
- sposoby zapewnienia właściwego stosowania programów,
- zasady ewidencji przebiegu przetwarzania danych.

Bank powinien posiadać udokumentowaną strategię 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.

Dokumentacja powinna być zabezpieczona w sejfie 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.
Powinny być ustalone procedury tworzenia, przechowywania i udostępniania kopii aktualnych haseł dostępu.

2.3. Zarządzanie sprzętem, wyposażeniem komputerowym oraz siecią

Przetwarzanie danych w banku powinno odbywać się zgodnie z obowiązującymi 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 (dyskami, taśmami, dyskietkami, CD-ROM'ami itp.) powinien zapobiegać uszkodzeniom sprzętu i zakłóceniom pracy systemu. Zarządzanie jednostkami przenośnymi (dyskami, taśmami, dyskietkami, CD-ROM'ami itp.) a w szczególności: oznakowanie tych jednostek, przenoszenie na nie informacji, miejsce i sposób bezpiecznego ich przechowywania, sposób i forma autoryzacji zmian i usuwania danych, właściwa i trwała likwidacja niepotrzebnych danych, powinny przebiegać zgodnie z obowiązującymi w banku procedurami zabezpieczeń. Oznakowanie wszystkich nośników, 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 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 informatycznych (np. użycie wszelkiego rodzaju zamykanych pojemników), 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.

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

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

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. Niezbędne jest sprawdzenie kompletności dokumentów złożonych przez kandydata, dokładne sprawdzenie jego tożsamości na podstawie dowodu osobistego (paszportu), zapoznanie się z przebiegiem pracy zawodowej i zasięgnięcie opinii o niekaralności. 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 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 raportów o wszystkich czynnościach wykonywanych przez użytkowników systemu i hasłach jakimi dysponują. 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. Po zakończeniu pracy ruchome nośniki informacji powinny 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.

2.5. Współpraca 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) 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),
- ścieżek dostępu,
- list autoryzowanych osób (specyfikacji),
- 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.

Klienci banku - przed uzyskaniem dostępu do terminali (modemów itp.) - powinni złożyć oświadczenie o poufności informacji.

2.6. 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 formalno-prawnymi 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 zapobiegania wirusom w systemach informatycznych, ze szczególnym zwróceniem uwagi na badanie nowych nośników informacji 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.

2.7. Bezpieczeństwo fizyczne i środowiskowe systemów informatycznych

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 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),
- identyfikatorów 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.

3. Kontrola wewnętrzna i nadzór

3. 1.Kontrola wewnętrzna

Kierownictwo banku odpowiedzialne jest za powołanie, w ramach systemu kontroli wewnętrznej, komórki odpowiedzialnej za kontrolę bezpieczeństwa systemów informatycznych. Do zadań jej należy ocena ochrony danych; ocena jakości i efektywności stosowanego przez bank sprzętu i oprogramowania; monitorowanie i kontrola ryzyka, a w szczególności kontrola czy bank posiada:

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

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.

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

3.2. Wymagania nadzorcze

Z nadzorczego punktu widzenia, mającego na celu zapewnienie bezpieczeństwa środków pieniężnych, zgromadzonych na rachunkach bankowych oraz tajemnicy bankowej niezbędna jest ocena czy system informatyczny banku ma atrybuty systemu bezpiecznego, który cechuje poufność, wiarygodność i dostępność. Czy bank posiada i jak realizowane są zasady polityki bezpieczeństwa, procedury identyfikacji użytkowników, jednoznacznego potwierdzania i rejestracji korzystania z zasobów systemu, czy i jak funkcjonują pozostałe metody zabezpieczeń oraz czy procedury postępowania zapewniają odpowiednie monitorowanie ryzyka i zarządzanie nimi. Istotna jest także ocena efektywności działania komórki odpowiedzialnej za kontrolę wewnętrzną bezpieczeństwa systemów informatycznych. Okresowo dokonywane badania powinny obejmować również trafność doboru programów elektronicznego przetwarzania danych dla prawidłowej realizacji statutowych zadań banku oraz wpływ rozwiązań organizacyjnych, przyjęty podział kompetencji, upoważnienia dostępu udzielone użytkownikom itp. na poziom bezpieczeństwa systemu.

W każdym wyspecjalizowanym obszarze szczególnie pomocne w realizowaniu funkcji nadzorczych jest korzystanie z ekspertyz opracowanych przez audytorów

zewnętrznych. Można przyjąć, iż prosty kwestionariusz lub raport, są w zasadzie wystarczające dla uzyskania wstępnej oceny, nie zastąpią jednak specjalistycznego audytu lub szczegółowego przeglądu.

Inspektorzy nadzoru bankowego i audytorzy, wykonujący badania w banku, wykorzystują swoją wiedzę fachową, wytyczne i podręczniki inspekcji przygotowane przez władze nadzorcze oraz wyspecjalizowane instytucje, a także informacje pracowników banku na temat budowy systemu, programów operacyjnych i kontrolnych. Na prośbę osób przeprowadzających kontrolę powinny one uzyskać wyczerpujące wyjaśnienia na temat procedur, budowy systemu, zabezpieczeń, a także doboru parametrów w aplikacjach bankowych (np. limity dla poszczególnych kredytobiorców, limity ryzyka i metody wyceny dla transakcji pochodnych itp.) od kompetentnych pracowników banku.

Do protokółu inspekcyjnego mogą być włączone notatki, obserwacje i protokóły kontroli wewnętrznej, ilustrujące poziom dbałości banku o właściwe zabezpieczenie poufności, integralności i dostępności użytkowanych systemów informatycznych.

Spis treści

	Definicje i przydatne słownictwo	1
	Rekomendacje	4
1	Rola kierownictwa banku w zarządzaniu bezpieczeństwem systemów informatycznych	4
1.1.	Nadzór kierownictwa	4
1.2.	Polityka w zakresie zabezpieczenia systemów komputerowych	5
1.3.	Planowanie skali systemów informatycznych.....	8
2	Infrastruktura zabezpieczeń i zarządzanie bezpieczeństwem informacji	9
2.1.	Analiza zagrożeń i metody zabezpieczeń	9
2.2.	Bezpieczeństwo dokumentacji systemowej	10
2.3.	Zarządzanie sprzętem, wyposażeniem komputerowym oraz siecią	12
2.4.	Bezpieczeństwo systemów informatycznych a działania personelu i upoważnionych osób trzecich	14
2.5.	Współpraca z klientami	15
2.6.	Szkolenie użytkowników	16
2.7.	Bezpieczeństwo fizyczne i środowiskowe systemów informatycznych	17
3	Kontrola wewnętrzna i nadzór	19
3.1.	Kontrola wewnętrzna	19
3.2.	Wymagania nadzorcze	20

Opracowano w Zespole Polityki Nadzorczej GINB

Aprobowała:

Ewa Śleszyńska-Charewicz

Generalny Inspektor Nadzoru Bankowego