



Zasady minimalizacji ryzyka naruszenia bezpieczeństwa informacji w bankach

CIS – Your Standard for Security



Andrzej Wojtas (2008)

Krótkie streszczenie wykładu



- W pierwszej części wykładu chciałbym Państwu najpierw przedstawić samo zagadnienie bezpieczeństwa informacji, potem główne rodzaje informacji chronionych.
- W drugiej części wykładu opiszę dwa podejścia do bezpieczeństwa informacji: spontaniczne i systemowe. Zaprezentuję przykładowe błędy i problemy związane z bezpieczeństwem informacji, które świadczą o stosowaniu spontanicznego podejścia do bezpieczeństwa informacji, po to, aby na koniec przedstawić zalety podejścia systemowego.

Bezpieczeństwo informacji



- Dla wszystkich oczywiste jest, że w bankach informacje są niezbędne do prowadzenia działalności.
- Pojęcie „bezpieczeństwo informacji” każdy rozumie jako zapewnienie ochrony informacjom.
- Jednak ludzie bardzo różnią się w ocenie, jakie informacje i w jaki sposób trzeba chronić.

CIS – Your Standard for Security

Definicja bezpieczeństwa informacji



- Bezpieczeństwo informacji to skuteczne zapewnienie informacjom posiadania następujących cech:
 1. Poufność informacji – zabezpieczenie udostępniania informacji tylko osobom upoważnionym (informacja nie jest ujawniana osobom nieupoważnionym)
 2. Integralność informacji - zabezpieczenie udostępniania informacji poprawnej i kompletnej (informacja nie jest zafałszowana lub niekompletna)

Definicja bezpieczeństwa informacji cd.



- Bezpieczeństwo informacji to skuteczne zapewnienie informacjom posiadania następujących cech:
3. Dostępność informacji – zapewnienie, że żądana przez uprawnioną osobę informacja jest dla tej osoby dostępna (informacja nie jest niedostępna lub trudno dostępna)

Główne rodzaje informacji chronionych w bankach



- Najważniejsze rodzaje informacji chronionych w banku to:
 1. tajemnica bankowa
 2. tajemnica danych osobowych
 3. tajemnica przedsiębiorstwa banku
 4. tajemnice przedsiębiorstwa kontrahentów banku

Bezpieczeństwo informacji w bankach



- Banki muszą chronić informacje w celu maksymalizacji swoich możliwości biznesowych (tajemnica przedsiębiorstwa banku), ale również w tym zakresie muszą wypełnić swój obowiązek wynikający z ustaw (tajemnica bankowa, ochrona danych osobowych) i obowiązek wynikający z umów (tajemnice przedsiębiorstwa kontrahentów banku).

CIS – Your Standard for Security

Podejście spontaniczne



- Można radzić sobie tak...
- Do zapewnienia bezpieczeństwa informacji podchodzimy intuicyjnie. Tworzymy ogólne polityki, kontrolujemy najważniejsze informacje, nadajemy uprawnienia w systemach informatycznych, szyfrujemy łącza i dane, robimy backupy, stosujemy ochronę antywirusową, zbieramy oświadczenia o zachowaniu poufności, podpisujemy umowy, poddajemy się kontrolom zewnętrznym i audytowi wewnętrznemu, reagujemy na incydenty, itp.
- Jakoś nam się dotychczas udawało i mamy nadzieję, że potrafimy sobie poradzić z problemami w przyszłości.

Podejście systemowe



- Można też radzić sobie lepiej...
- Według CIS - Certification & Information Security Services (www.cis-cert.pl) zapewnienie bezpieczeństwa informacji można osiągnąć znacznie wydajniej z wykorzystaniem systemów zarządzania opartych na normach ISO. Co więcej, tworząc i utrzymując w banku znormalizowany System Zarządzania Bezpieczeństwem Informacji, można uzyskać trwalszy efekt niż przy podejściu spontanicznym.

CIS – Your Standard for Security

Typowe błędy, problemy i dobre rady



- Na następnych kilku slajdach zostaną przedstawione typowe błędy i problemy związane z bezpieczeństwem informacji, które występują w bankach i świadczą o stosowaniu spontanicznego podejścia do bezpieczeństwa informacji.
- Do problemów zostaną podane dobre rady, których zastosowanie pomoże uniknąć tych problemów.

1. Bank pilnuje sprzeciwów klientów wobec przetwarzania danych



- Typowe błędy... Wpłynął sprzeciw wobec przetwarzania marketingowego, a bank pomimo sprzeciwu wysłał klientowi reklamę.
- Problem polega na tym, że sprzeciwu w ogóle nie odnotowano (Nie wiedziałem...), odnotowano go nieprawidłowo (Zrobiłem notatkę w uwagach...) lub nie sprawdzono, że był sprzeciw (Robię coś, do czego nie stosuje się sprzeciw... / Nie wiedziałem, że trzeba sprawdzać jakieś sprzeciwy...).
- Dobre rady.... W jednej bazie przy danych klienta powinien być odnotowany sprzeciw w określonym polu za pomocą jednoznacznego symbolu. Wszyscy wiedzą, co robić ze sprzeciwami (wpisywać, sprawdzać przy przetwarzaniu). ABI edukuje pracowników nt. sprzeciwów i kwalifikacji przetwarzania względem sprzeciwów.

2. Bank prawidłowo zamyka rachunki, karty i kanały dostępu do rachunków



- Typowe błędy... Klient zamknął rachunki, a bank pomimo to nalicza opłaty, wysyła wyciągi, nowy regulamin, wzywa do podpisania aneksu, wznawia kartę lub zostawia kanał dostępu do zamkniętego rachunku .
- Problem polega na tym, że rachunek nie jest w ogóle zamykany (Nie wiedziałem...), przy wysyłaniu pism nie jest sprawdzane, że rachunek jest zamknięty (Nie wiedziałem...), nie odnotowano, że karty nie można wznawiać (Myślałem, że karty zamykają się wraz z rachunkiem...) lub nie zamknięto kanału dostępu (Nie wiedziałem, że trzeba zablokować dostęp przez Internet...).
- **Dobre rady.... Maksymalnie uprościć zamykanie rachunków wraz ze wszystkimi kartami i kanałami dostępu. Wszyscy wiedzą, co robić przy zamykaniu rachunków. Bank edukuje pracowników nt. zamykania rachunków, kart i kanałów dostępu.**

3. Bank prawidłowo otwiera rachunki, karty i kanały dostępu do rachunków



- Typowe błędy... Klient nie podpisał umowy, nie wystąpił z wnioskiem o kartę, a bank pomimo to otworzył rachunek, wydał kartę. Kanały dostępu do rachunków są otwierane w sposób, który umożliwia przejęcie kontroli nad rachunkiem przez osobę trzecią.
- Problem polega na tym, że rachunek jest otwierany zanim jest podpisana umowa (Klient się rozmyślił, nie podpisał umowy, a ja zapomniałem zamknąć rachunek...), aby wyprodukować nieaktywną kartę już trzeba otworzyć rachunek (Nasz system tak działa...), nowy kanał dostępu do istniejącego rachunku jest tworzony korespondencyjnie (Przypuszczaliśmy, że dostęp przez Internet dajemy klientowi...).
- **Dobre rady.... Otwierać rachunki po podpisaniu umowy. Jeśli się tak nie da, to pilnować zamknięcia rachunku w przypadku niepodpisania umowy. Karty produkować nieaktywne i podpinąć do rachunku po podpisaniu umowy. Kanały dostępu otwierać wymagając obecności klienta w banku. Bank edukuje pracowników nt. otwierania rachunków i kanałów dostępu oraz wydawania kart.**

4. Bank zbiera dane osobowe klientów spełniając obowiązek informacyjny



CIS – Your Standard for Security

- Typowe błędy... Zebrano dane osobowe, a bank nie spełnił prawidłowo obowiązku informacyjnego.
- Problem polega na tym, że klientowi w ogóle nie przekazano klauzuli informacyjnej (Nie wiedziałem, że trzeba...), lub przekazano nieaktualną klauzulę (Nie wiedziałem, że jest nowa...).
- **Dobre rady.... Opracować klauzulę informacyjną i ją aktualizować. Wszyscy wiedzą, co robić z klauzulą. ABI edukuje pracowników nt. aktualnej klauzuli i sposobu jej przekazywania klientowi.**

5. Podmioty działające w imieniu banku ujawniają klientowi skąd mają dane



- Typowe błędy... Podmioty kontaktują się z klientem nie informując go skąd mają jego dane, co w efekcie u klienta rodzi podejrzenie, że dane z banku wyciekły.
- Problem polega na tym, że klientowi w ogóle nie przekazano informacji, że podmiot działa na zlecenie banku (Nie uważaliśmy za wskazane, aby o tym klientowi wspominać...), lub klient zrozumiał, że podmiot stał się właścicielem danych (Nie chcieliśmy klientowi za dużo tłumaczyć...).
- **Dobre rady.... Opracować informacje dla klienta objaśniającej podstawę ujawnienia podmiotowi danych klienta i zobowiązać podmioty działające w imieniu banku do ich przekazywania. Bank edukuje współpracujące podmioty nt. informowania klientów.**

6. Bank sprawdza tożsamość osoby i jej uprawnienia do informacji



- Typowe błędy... Osoba nieuprawniona żąda dostępu do informacji chronionych, a bank nie sprawdza tożsamości i uprawnień tej osoby udzielając jej informacji, często choćby tylko potwierdzając to, o co osoba pytała.
- Problem polega na tym, że nie sprawdzono tożsamości (Myślałem, że to klient...), sprawdzono ją pobieżnie (Nie wiedziałem, że dane ojca i syna różnią się tylko PESEL-em...), nie sprawdzono uprawnień (Zawsze miał pełnomocnictwo...), potwierdzono informacje zawarte w pytaniu nie traktując tego jako ujawnienia tych informacji (Pytający wszystko sam wiedział...).
- Dobre rady.... Opracować skuteczne procedury sprawdzania tożsamości i uprawnień przy dostępie do informacji. Wszyscy pracownicy wiedzą, kiedy mogą udzielić informacji chronionych, a kiedy muszą odmówić. Bank edukuje pracowników nt. weryfikacji tożsamości i uprawnień osoby żądającej informacji chronionych.

7. Bank sprawnie odpowiada na pytania i żądania klienta



urity

- Typowe błędy... Klient w piśmie (np. skardze) skierowanym do banku prosi o informacje dotyczące przetwarzania jego danych osobowych. Bank nie odpowiada w terminie 30 dni i narusza ustawę o ochronie danych osobowych.
- Problem polega na tym, że pracownik, do którego trafiło pismo, nie wiedział, że takie pytanie klienta wymaga obowiązkowej i terminowej odpowiedzi (Nie wiedziałem...).
- **Dobre rady....** Wszyscy pracownicy odpowiadający na pisma klientów wiedzą, co zrobić z prośbą klienta o informacje dotyczące przetwarzania danych osobowych. ABI edukuje pracowników nt. praw klienta związanych z przetwarzaniem danych osobowych.

8. Bank sprawdza klienta w bazach zewnętrznych zgodnie z regulaminem



ity

- Typowe błędy... Pracownik banku niezgodnie z regulaminem korzystania z bazy zewnętrznej (np. BLK) sprawdza dane klienta, co zostawia wpis o zapytaniu widoczny dla innych banków i dostępny dla klienta.
- Problem polega na tym, że pracownik, korzystając z posiadanego dostępu do bazy sprawdza kogoś dla własnych celów (Chciałem tylko...), czasem jest proszony przez innego pracownika lub pośrednika o szybkie sprawdzenie (Sprawdź mi szybko.... , dokumenty prześlę później...).
- **Dobre rady....** Wszyscy pracownicy posiadający dostęp do baz zewnętrznych wiedzą, jak należy zgodnie z regulaminem korzystać z tych baz. Pracownicy współpracujący z pośrednikami pilnują bezpiecznej dla banku procedury. Bank edukuje pracowników nt. prawidłowego korzystania z zewnętrznych baz danych.

9. Bank uświadamia pracowników w zakresie bezpieczeństwa informacji



- Typowe błędy... Pracownik banku ujawnia w życiu prywatnym lub w życiu zawodowym poza bankiem, informacje o klientach, których dowiedział się przy okazji ich obsługi (np. przyjął dużą wpłatę od klienta) lub z własnej inicjatywy (np. odczytał z bazy danych).
- Problem polega na tym, że pracownik, wykonując czynności służbowe lub korzystając z posiadanego dostępu do bazy danych, posiada informacje, które wykorzystuje do własnych celów (Słuchaj, ile on ma na lokacie...), czasem dla konkurencji (W nowym banku przyda mi się baza klientów z mojego starego banku...).
- Dobre rady.... Wszyscy pracownicy znają odpowiedzialność za naruszenie tajemnicy. Dostęp do danych jest kontrolowany (np. zapisy w dzienniku zdarzeń wraz z kontrolą tych zapisów). ABI edukuje pracowników nt. obowiązku zachowania tajemnicy w trakcie i po ustaniu zatrudnienia.

10. Bank posiada dokumentację wymaganą przepisami



CIS – Your Standard for Security

- Typowe błędy... Bank posiada jakieś dokumenty dotyczące bezpieczeństwa informacji - ogólną politykę, różne szczegółowe procedury.
- Problem polega na tym, że dokumentacja jest niewłaściwa – zbyt ogólna (Głównie deklaracje jak ma być...), napisana niezrozumiałym językiem (Terminologia specjalistyczna...), nieaktualna (Nikt jej nie potrzebuje...) lub niekompletna (Dokument opracowany przed laty jest nadal dobry...).
- **Dobre rady.... Dokumentacja jest dobrze opracowana i stosowana przez wszystkich pracowników i pośredników. Bank i ABI edukuje pracowników nt. zasad zawartych w dokumentacji.**

11. Bank posiada zabezpieczenia wymagane przepisami



- Typowe błędy... Bank posiada różne zabezpieczenia informacji – wdrażane w różnym czasie przez różne osoby.
- Problem polega na tym, że zabezpieczenia są niewłaściwe – nie tworzą systemu spójnego w banku (Mamy zaufanie do dostawcy...) lub u pośredników (Mamy zaufanie do pośrednika...), są przypadkowe (Administrator wie jak się zabezpieczyć...) lub za słabe (Nie przypuszczaliśmy, że ktoś tak może zrobić...).
- **Dobre rady.... Zabezpieczenia są zastosowane w wyniku decyzji następujących w wyniku postępowania z ryzykiem naruszenia bezpieczeństwa informacji. Bank i ABI analizuje ryzyko, podejmuje decyzje i wdraża zabezpieczenia.**

System Zarządzania Bezpieczeństwem Informacji (SZBI)



- W celu zastosowania systemowego podejścia do bezpieczeństwa informacji należy ustanowić, wdrożyć i eksploatować SZBI, który dla skutecznego długofalowego działania musi podlegać monitorowaniu i przeglądowi oraz utrzymaniu i doskonaleniu.
- Według CIS - Certification & Information Security Services (www.cis-cert.pl) najlepszym rozwiązaniem jest zastosowanie SZBI zdefiniowanego w normie PN-ISO/IEC 27001.

Opis SZBI wg norm ISO



CIS – Your Standard for Security

- Ustanowienie polityki SZBI, celów, procesów i procedur istotnych dla zarządzania ryzykiem naruszenia bezpieczeństwa informacji oraz doskonalenia bezpieczeństwa informacji, tak aby uzyskać wyniki zgodne z wymaganiami i oczekiwaniami dotyczącymi bezpieczeństwa informacji (polityki i cele organizacji).
- Wdrożenie i eksploatacja polityki SZBI, zabezpieczeń, procesów i procedur.
- Szacowanie i pomiar wydajności procesów w odniesieniu do polityki SZBI, celów i doświadczenia praktycznego oraz dostarczanie kierownictwu raportów do przeglądu.
- Podejmowanie działań korygujących i zapobiegawczych w oparciu o wyniki wewnętrznego audytu SZBI i przeglądu realizowanego przez kierownictwo lub innych istotnych informacji, w celu zapewnienia ciągłego doskonalenia SZBI.

SZBI - oferta CIS - Certification & Information Security Services



- Programy szkoleniowe „Manadżer Bezpieczeństwa Informacji“ (wdrożenie i eksploatacja SZBI)
- Programy szkoleniowe „Audytor (wewnętrzny) Bezpieczeństwa Informacji“ (audyt wewnętrzny SZBI i przygotowanie do audytu zewnętrznego SZBI)
- Stage reviews (audyty zewnętrzne SZBI przed certyfikacją SZBI)
 - Certyfikaty na zgodność ISO 27000 (certyfikacja SZBI)

Szczegóły znajdą Państwo na stronie
www.cis-cert.pl



CIS – Your Standard for Security

DZIĘKUJĘ ZA UWAGĘ

Andrzej Wojtas

ekspert jednostki CIS-Cert

e-mail: andrzej.wojtas@cis-cert.pl

tel. 608 148 242