DWUDZIESTE TRZECIE FORUM TELEINFORMATYKI®

Cyberbezpieczeństwo
czynnik determinujący zaufanie klientów do banku

Karolina Szostek, Tomasz Kaniecki

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CYBERBEZPIECZEŃSTWO (pojęcie nie jest terminem zdefiniowanym prawnie!)

> Zapewnienie ciągłości działania systemów teleinformatycznych oraz bezpieczeństwa ich funkcji i informacji w nich przetwarzanych, rozumiane jako ciągłość funkcjonowania, brak nieautoryzowanego dostępu, wykorzystania, zmiany czy uszkodzenia bez względu na przyczynę.

Zapewnienie najwyższego poziomu cyberbezpieczeństwa oferowanych rozwiązań bankowości jest obowiązkiem banków wynikającym z:

1. Aktów prawnych;
2. Norm i standardów technologicznych;
3. Rekomendacji KNF.

Bank ma za zadanie przewidywać zagrożenia, ostrzegać, tworzyć rozwiązania, by im przeciwdziałać. Głównym kryterium oceny działania banku jest **STARANNOŚĆ**.

AKTY PRAWNE

1. Ustawa z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz.U. 1997 nr 140 poz. 939) - cyberbezpieczeństwo wchodzi w ryzyko operacyjne banku;
2. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2011 nr 199 poz. 1175) dyrektywa PSD;
3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 833);
4. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. ;
5. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. 1997 nr 88 poz. 553);

W najbliższym czasie sektor bankowy czeka więcej obowiązków w zakresie bezpieczeństwa sieci i systemów informacyjnych:

- **Rozporządzenia RODO** (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE),
- **Dyrektywy PSD II** (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/W),
- **Dyrektywy NIS** (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).

NORMY I STANDARDY TECHNOLOGICZNE

Uznane standardy przez Polski Komitet Normalizacyjny (np. ISO/IEC 27032: 2012 – wytyczne dotyczące cyberbezpieczeństwa, ISO/IEC 27018:2014 – kodeks dobrych praktyk w zakresie ochrony danych osobowych w chmurach publicznych.

REKOMENDACJE KNF

1. Rekomendacja D;
2. Rekomendacja M;
3. Rekomendacja ws. bezpieczeństwa transakcji płatniczych wykonywanych w internecie;

Rekomendacja KNF ws. bezpieczeństwa transakcji płatniczych wykonywanych w internecie stanowi, iż banki powinny zapewniać klientom odpowiednie informacje w zakresie bezpieczeństwa transakcji płatniczych:

> Banki powinny zapewniać klientom niezbędną pomoc i wsparcie w zakresie bezpiecznego korzystania z usług płatności internetowych i stosować w tym zakresie przyjętą politykę edukacyjną.

CZY ASPEKTOM REGULACYJNYM MOŻNA PRZYPISAĆ WIĘKSZE ZNACZENIE?

W dobie rosnącego zagrożenia w sieci, informowanie o poziomie cyberbezpieczeństwa może stać się czynnikiem zwiększającym konkurencyjność banków oraz przyczynić się do zwiększania zaufania społeczeństwa do instytucji finansowych.

> **65 proc. konsumentów wskazuje bezpieczeństwo systemów mających chronić prywatność danych jako niezwykle ważny czynnik podczas wyboru docelowego banku.**
>
> Światowy Raport Bankowości Detalicznej (WRBR) 2016 opublikowany przez Capgemini

W praktyce obserwujemy różne podejście do zakresu informowania o cyberbezpieczeństwie na stronach internetowych największych banków.

Bank	Zakres informacji
PKO Bank Polski	Strona startowa (homepage) banku zawiera zakładkę dotyczącą bezpieczeństwa. PKO uważa się za lidera bankowości elektronicznej, a misją banku jest wyznaczanie najwyższych standardów w zakresie bezpieczeństwa sieci i systemów informacyjnych. W 2016 r. PKO BP jako pierwszy bank w Europie rozpoczął współpracę z firmą Microsoft w ramach programu Enterprise Customers Cyber Threat Intelligence Program. Bank nie wykorzystuje kwestii cyberbezpieczeństwa w celach stricte marketingowych. Strona banku zawiera szereg wskazówek dla klientów **(treść szczegółowa, informacja słabo widoczna).**
Bank Pekao	Na samym dole strony startowej (homepage) banku znajduje się zakładka dotycząca bezpieczeństwa. Bank całkowicie pomija kwestię bezpieczeństwa sieci i systemów informacyjnych w swojej ofercie. Pekao zwraca uwagę, iż bezpieczeństwo operacji zależy nie tyle od banku, ale od klientów. Bank stosuje szereg zabezpieczeń. Obok identyfikacji i autoryzacji, stosuje się się system szyfrowania transmisji, rejestracja aktywności, wygasanie sesji oraz limity transakcyjne. Bank przedstawia również zalecenia dla swoich klientów **(treść ogólna, informacja słabo widoczna).**
Bank Zachodni WBK	Strona startowa (homepage) banku zawiera zakładkę dotyczącą bezpieczeństwa. Bank wykorzystuje kwestię cyberbezpieczrństwa w celach marektingowych. WBK podkreśla, iż dysponuje nowoczesną i sprawdzoną infrastrukturą, doświadczeniem i wykwalifikowaną kadrą pracowników. Głównymi rozwiązaniami stosowanymi przez bank są szyfrowanie, cykliczne audyty oraz testy bezpieczeństwa. Bank zachęca do regularnego poszerzania wiedzy na temat zagrożeń w sieci **(treść szczegółowa, informacja dobrze widoczna).**
mBank	Strona startowa (homepage) banku zawiera zakładkę dotyczącą bezpieczeństwa. Bank wykorzystuje kwestię cyberbezpieczrństwa w celach marektingowych. Na stronie banku znajdują się informacje o stosowaniu najnowocześniejszych metod zabezpieczeń sprzętowych i programowych, tj. poufność przesyłanych informacji, bezpieczeństwo wymienianych z bankiem informacji, bezpieczne metody logowania do aplikacji i autoryzacji transakcji, możliwość decydowania przez klienta o sposobie dostępu do aplikacji i zakresie uprawnień swoich pracowników. Bank udostępnia również dekalog bezpieczeństwa w Internecie **(treść szczegółowa, informacja bardzo dobrze widoczna).**
BNP Paribas Fortis (Belgia)	Największy bank w Belgii utworzył specjalną stronę dotyczącą bezpieczeństwa w bankowości elektronicznej - Security First. Strona internetowa zawiera informacje na temat działań w zakresie bezpieczeństwa sieci i systemów informacyjnych oraz wskazówki dla klientów. Bank wykorzystuje kwestię cyberbezpieczrństwa w celach marektingowych. BNP sotosuje podstawowe narzędzia zabezpieczające (identyfikacja, zatwierdzanie określonych transakcji).
Swedbank (Estonia)	Największy bank w Estonii (państwa wysoce scyfryzowanego, o wysokim indeksie cyberbezpieczeństwa) nie używa kwestii bezpieczeństwa sieci i systemów informacyjnych w celach marektingowych. W ramach zabezpieczeń bank oferuje możliwosć wyboru narzędzi identyfikacyjnych (jako element oferty), przedstawia pakiet wskazówek dla klientów dotyczący postępowania w sieci. Bank przeprowadza także cykliczne reporty i testy bezpieczeństwa. Zawartość informacji przypomina Bank PKO BP.

Bank traktuje kwestię cyberbezpieczeństwa jako istotny element budowania zaufania klientów
Bank traktuje kwestię cyberbezpieczeństwa jako ważną, ale nie wykorzystuje jej w celach marketingowych
Bank nie traktuje kwestii cyberbezpieczeństwa jako elementu budowania zaufania klientów

Analiza stron internetowych czterech największych banków w Polsce oraz wybranego największego banku zagranicznego w Belgii i Estonii.