Bankowość internetowa i mobilna

Cyberataki wymierzone w instytucje finansowe:

- **Ataki DDoS** – przeciążenie serwerów bankowych w celu ich unieruchomienia.
- **Ransomware** – zablokowanie dostępu do danych bankowych i żądanie okupu.
- **Ataki na systemy płatności** – przechwytywanie transakcji finansowych.
- **Ataki na terminale płatnicze (POS)** – przejęcie danych kart płatniczych.
- **Włamania do baz danych** – kradzież danych klientów banków

Cyberataki wymierzone w osoby prywatne:

- **Phishing** – fałszywe e-maile i strony internetowe podszywające się pod banki.
- **Smishing** – wyłudzanie danych poprzez SMS-y.
- **Vishing** – oszustwa telefoniczne podszywające się pod pracowników banku.
- **Malware** – złośliwe oprogramowanie wykradające dane logowania.
- **Kradzież tożsamości** – wykorzystanie cudzych danych osobowych do oszustw finansowych.
- **Keyloggery** – programy zapisujące każdy znak wpisywany na klawiaturze.

Najważniejszym zagrożeniem dla systemów informatycznych jest działalność ludzka.

Motywy działania sprawców:

– szpiegostwo, polegające na kradzieży cennych informacji i przekazaniu ich konkurencyjnemu bankowi,

– chęć osiągnięcia zysku,

– uzyskanie rozgłosu, poprzez ujawnienie faktu włamania.

Bezpieczeństwo w bankowości internetowej i mobilnej ze strony banku

- natychmiastowe potwierdzania tożsamości osób realizujących transakcję,
- stosowania skutecznego systemu szyfrowania transmisji informacji,
- odpowiednie zabezpieczenia serwera instytucji, będącej dostawcą internetowych usług finansowych,
- zabezpieczenia serwera przed celowymi atakami przeprowadzanymi zarówno z zewnątrz (Internet), jak i od środka (sieć lokalna).

Bezpieczeństwo w bankowości internetowej i mobilnej ze strony banku

Z reguły banki stosują również szereg innych, dodatkowych zabezpieczeń, takich jak np.

- zablokowanie konta klienta w przypadku kilkukrotnego podania błędnego hasła lub PIN-u,
- wylogowanie z systemu przy całkowitym braku aktywności ze strony klienta,
- potwierdzenie sms-em wykonanie operacji.

Bezpieczeństwo w bankowości internetowej i mobilnej ze strony klienta

- posiadane hasła powinny być starannie chronione,
- każdorazowe połączenie z bankiem wymaga sprawdzenia, czy przesyłane informacje są szyfrowane,
- należy unikać przesyłania siecią jakichkolwiek informacji, które mogłyby ułatwić dostęp do konta (np. adres, imię, nazwisko),
- konieczne jest wykorzystywanie sprawdzonych programów antywirusowych, które systematycznie należy aktualizować,
- odchodząc od komputera w czasie połączenia z bankiem, należy go odpowiednio zabezpieczyć bądź całkowicie wyłączyć.

Scenariusz 1

- **Scenariusz:**
  Otrzymujesz e-mail, który wygląda na wiadomość od Twojego banku. Proszą Cię o podanie danych logowania, aby zaktualizować Twoje konto lub rozwiązać problem z bezpieczeństwem.
- **Opcje:**
- Klikam w link w e-mailu i podaję swoje dane logowania.
- Sprawdzam oficjalną stronę banku lub aplikację, aby upewnić się, czy nie ma żadnych zaległych wiadomości od banku.
- Odpowiadam na e-mail i pytam, dlaczego proszą mnie o takie dane.

Scenariusz 2

- **Scenariusz:**
  Chcesz sprawdzić stan swojego konta w bankowości internetowej, ale jesteś w kawiarni i masz dostęp do darmowego Wi-Fi. Zastanawiasz się, czy jest to bezpieczne.
- **Opcje:**
- Korzystam z publicznego Wi-Fi, aby sprawdzić stan konta.
- Wyłączam publiczne Wi-Fi i korzystam z danych mobilnych, aby uzyskać dostęp do bankowości internetowej.
- Zgaduję, że Wi-Fi w kawiarni jest bezpieczne, i loguję się bez żadnych obaw.

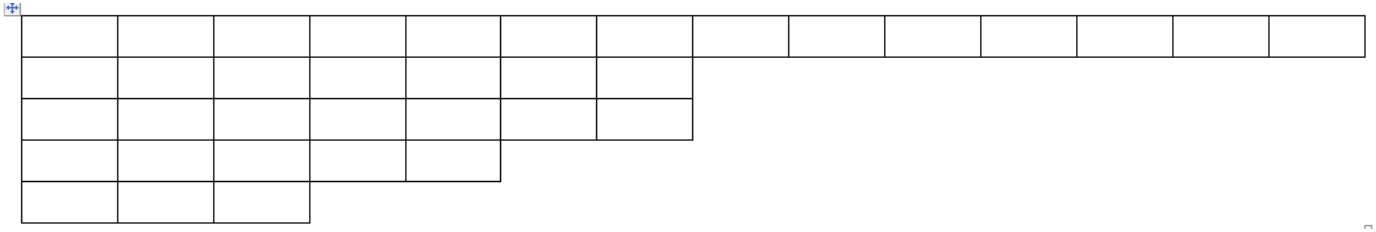
Scenariusz 3

- **Scenariusz:**
  Otrzymujesz SMS-a z linkiem, który prowadzi do „ważnej aktualizacji” aplikacji bankowej. Wiadomość wygląda na autentyczną.
- **Opcje:**
- Klikam w link i wykonuję instrukcje w SMS-ie.
- Ignoruję wiadomość i sprawdzam oficjalną aplikację bankową w sklepie z aplikacjami.
- Odpowiadam na SMS, pytając, skąd pochodzi ta wiadomość.

Scenariusz 4

- **Scenariusz:**
  Na Twoim komputerze pojawia się komunikat, że masz wirusa i musisz zapłacić, aby go usunąć.
- **Opcje:**
- Klikam w komunikat i dokonuję płatności, aby usunąć wirusa.
- Ignoruję komunikat, uruchamiam program antywirusowy i skanuję komputer.
- Dzwonię do firmy zajmującej się bezpieczeństwem IT, aby dowiedzieć się, jak rozwiązać problem.

Krzyżówka



- 1)Sposób uwierzytelniania wymagający dwóch różnych metod
- 2)Oszustwo internetowe polegające na podszywaniu się pod inną osobę
- 3)Rodzaj oprogramowania używanego do kradzieży danych
- 4)Szyfrowane połączenie stosowane w bezpiecznych stronach internetowych
- 5)Metoda szyfrowania danych przesyłanych przez Internet

Przeanalizuj następujący mail

- **Temat:** "Pilne! Twoje konto zostanie zablokowane!"
  - Nadawca: "Bank Centralny" (ale adres e-mail to np. bank@secure-service.com)
  - Treść: "Wykryliśmy podejrzane logowanie. Kliknij tutaj, aby zweryfikować swoje konto."

Przeanalizuj następujący mail

- **Temat:** "Zwrot podatku czeka na Ciebie!"
  - Nadawca urząd skarbowy, prosząc o podanie danych konta.
  - Załączony plik zawiera szczegóły zwrotu.

Przeanalizuj następujący mail

- **Temat:** "Twoja paczka nie mogła zostać dostarczona"
  - Nadawca firma kurierska.
  - Link do strony, gdzie użytkownik ma podać dane bankowe do rzekomej opłaty.

Przeanalizuj następujący mail

- **Temat:** „Faktura do opłacenia"
  - Nadawca firma APKA.
  - Link do wiadomości zawiera fakturę.

Podsumowanie

- Jakie jest najbezpieczniejsze rozwiązanie przy tworzeniu hasła?
  - a) 123456 b) Data urodzenia c) Długi ciąg losowych znaków d) Imię pupila
- Co to jest phishing?
  - a) Rodzaj wirusa komputerowego b) Technika wyłudzania danych c) System szyfrowania d) Program do ochrony bankowości
- Które połączenie jest bezpieczne do logowania się do banku?
  - a) Publiczne Wi-Fi b) HTTPS c) Otwarte sieci w kawiarniach d) Dowolne, jeśli używasz tego samego hasła

Zadanie dodatkowe:

Przygotuj krótki poradnik na temat "Jak chronić się przed cyberatakami w bankowości online?".