



Centrum Prawa Bankowego i Informacji
www.cpb.pl

BANK
MIESIĘCZNIK FINANSOWY



ZWIĄZEK BANKÓW POLSKICH

10 maja 2018 r.
Novotel Warszawa Centrum



VII Forum Bezpieczeństwa Banków 2018

„Możesz wydać fortunę na zakup technologii i usług, a twoja infrastruktura sieciowa może nadal być podatna na staroświeckie manipulacje”.

Kevin Mitnick

BEZPIECZEŃSTWO ADEKWATNE DO WYZWAŃ

Słowa słynnego włamywacza komputerowego wskazują na potrzebę ciągłego analizowania statystyk oraz sposobów działania przestępców. Kevin Mitnick w swojej przestępczej działalności perfekcyjnie wykorzystywał inżynierię społeczną. Dlatego w VII edycji Forum Bezpieczeństwa Banków, do grona prelegentów zaprosiliśmy przede wszystkim doświadczonych praktyków. Nie będzie wśród nich Kevina Mitnicka, ale w prezentacjach oraz debatach nasi eksperci połączą dla Państwa teorię ze studiami konkretnych przypadków. Zaprezentują najnowsze osiągnięcia technologiczne w dziedzinie bezpieczeństwa, ale także proste i skuteczne metody, o których nie wolno nam zapominać.

www.aleBank.pl/FBB

[#ForumBB](https://twitter.com/ForumBB)

PROGRAM

09.15 – 09.30 Przywitanie uczestników i otwarcie VII FBB

- **Krzysztof Pietraszkiewicz** – Prezes, Związku Banków Polskich.
 - Prowadzący: **Andrzej Wolski** – Wiceprezes, Centrum Prawa Bankowego i Informacji Sp. z o.o.
-

09.30 – 11.00 Sesja I Bezpieczeństwo w erze open bankingu – GDPR/RODO i PSD2

Podczas sesji zaprezentujemy wiele aspektów aktualnie stanowiącego prawa. Na kilkanaście dni przed wejściem w życie nowych regulacji dotyczących ochrony danych osobowych (RODO/GDPR) podejmiemy w dynamicznym wielogłosie ekspertów następujące tematy:

- *RODO i co po RODO: konsekwencje, dalsze funkcjonowanie, możliwe scenariusze.*
 - *Jakie korzyści wnosi idea open bankingu i PSD2?*
 - *Jakich zagrożeń możemy oczekiwać wraz z pojawieniem się na rynku tzw. TPP (Third Party Provider)?*
 - *Co będzie dalej, czyli konsekwencje ustawy o krajowym systemie cyberbezpieczeństwa.*
 - *Na koniec sesji chcielibyśmy umieć odpowiedzieć na pytanie: Co jest już „twardym” prawem, a co jeszcze jest w świecie legislacyjnym i dopiero dojrzeje?*
-

Moderator: Włodzimierz Kiciński – Wiceprezes Zarządu ZBP.

- *Poważna i odpowiedzialna rozmowa pomiędzy ekspertami.* Głos zabiorą: radca prawny dr **Tadeusz Białek**, Dyrektor Zespołu Prawno-Legislacyjnego Związku Banków Polskich, dr **Maciej Kawecki**, Dyrektor Departamentu Zarządzania Danymi Ministerstwa Cyfryzacji oraz **Wojciech Pantkowski**, Dyrektor Zespołu Systemów Płatniczych i Bankowości Elektronicznej Związku Banków Polskich.
-

Pozostałe wystąpienia:

- *Postęp pełen paradoksów* – dr inż. **Krzysztof Serafin**, Naczelnik Wydziału Nadzoru i Rozwoju Systemów Ochrony Departamentu Bezpieczeństwa Narodowego Banku Polskiego.
Czy każdy postęp w zakresie technicznych zabezpieczeń ma sens? A jeżeli tak, to czy rozwój techniczny w połączeniu z nowymi regulacjami prawnymi nie tworzy większej liczby problemów niż rozwiązuje? Jeżeli znamy sposoby uniknięcia zagrożeń poprzez eliminowanie podatności, to wprowadzamy je, nie czekając na silną motywację wynikającą z poniesionych strat.
 - *Jak dyrektywy GDPR/RODO oraz PSD2 wpłyną na możliwości profilowania klientów?* – **Konrad Antonowicz**, Specjalista ds. bezpieczeństwa IT, Passus S.A.
Jeżeli nowe regulacje będą miały aż tak istotny wpływ na profilowanie waszych klientów, to nie możemy poprzestać tylko na opisie. Powiemy, jak sobie z tymi problemami radzić.
-

Sesja Q&A

W trakcie trwania Sesji Q&A VII FBB, a szczególnie debaty końcowej Forum, wszyscy uczestnicy konferencji będą mogli za pomocą swoich telefonów komórkowych zadawać pytania oraz wyrażać opinie. Także uczestnicy otrzymywać będą specjalnie przygotowane przez ekspertów pytania, które zbudowane wg metodologii *disruptive thinking* pozwolą nam na swoiste „wyjście z koleiny” stereotypowego podejścia. Statystyczny rozkład odpowiedzi będzie prezentowany na ekranie, a zgromadzone wyniki zostaną wraz z rekomendacjami VII FBB rozesłane uczestnikom. Opisaną interaktywność zapewni specjalny system.

11.00 – 12.00 Sesja II Stare i nowe zagrożenia

Wstępem do sesji będzie wystąpienie Dyrektora Biura do Walki z Cyberprzestępczością Komendy Głównej Policji, podkom. **Dominika Rozdziałowskiego** oraz jego współpracowników. Ukazane zostaną autentyczne zagrożenia oraz sposoby przeciwdziałania.

Moderator: Piotr Balcerzak – Dyrektor Zespołu Bezpieczeństwa Banków, Związek Banków Polskich.

Wystąpienia:

- *Nasze dane na czarnym rynku. Jak monitorować potencjalne zagrożenia?* – **Piotr Narczyk**, Business Development Manager, Experian Polska Sp. z o.o.
O fakcie kradzieży swoich danych w sieci raczej się nie dowiesz... Ale możesz monitorować, czy Twoje dane nie są elementem sprzedaży bądź kupna. W sieci krąży ogromna ilość danych, jak adresy e-mail, numery kart kredytowych lub dokumentów tożsamości, które zostały wykradzione, a które można kupić i posługiwać się, podszywając pod właścicieli. Czy można zapobiec przypadkom kradzieży? Zapewne nie, ale za to możemy monitorować obrót takimi informacjami i zostać poinformowani, gdy dane takie pojawią się na rynku wtórnym w tzw. Dark Necie. Jak duża jest skala problemu oraz jak monitorować handel takimi danymi?
 - *Znane i nieznanne, ale zawsze piekielnie groźne* – **Robert Dąbrowski**, CISSP SE Manager, FORTINET.
Na podstawie wyników badań laboratorium bezpieczeństwa FortiGuard firmy FORTINET ukazany zostanie krajobraz
-

cyberzagrożeń dla sektora finansowego. Pokazane zostaną także sposoby ochrony przed znanymi i jeszcze nieznanymi zagrożeniami.

Sesja Q&A

12.00 – 12.30 Przerwa kawowa i rozmowy kulturalowe

12.30 – 13.30 Sesja III Kompetencje w zarządzaniu bezpieczeństwem

Chcielibyśmy, aby budowa świadomości wśród pracowników banków i użytkowników systemów bankowych następowała poprzez szeroko pojmowaną edukację, a wprowadzane do niej ćwiczenia, warsztaty i „gry wojenne” były stale doskonalone pod względem ich skuteczności. Polegać to powinno na cyklicznym sprawdzaniu efektów nauczania i śledzeniu zmian zachodzących w postawach i sposobach zachowania się szkolenych pracowników.

Aby to było możliwe, potrzebujemy większego udziału ekspertów praktyków w procesie opracowywania planów szkoleniowych oraz podczas ich realizacji. Potrzebne są także zajęcia w warunkach zbliżonych do autentycznych i pod wpływem stresu. Pozytywnym przykładem mogą być ćwiczenia Cyber-EXE.

Moderator: Tomasz Chlebowski – CEO w ComCERT S.A.

Wystąpienia:

- *Wnioski i rekomendacje z ćwiczeń Cyber-EXE Polska* – **Mirosław Maj**, Prezes Zarządu Fundacji Bezpieczna Cyberprzestrzeń.
Zaprezentowane zostaną wnioski i rekomendacje z ćwiczeń Cyber-EXE Polska, a przede wszystkim doświadczenia ich uczestników. Pokażemy, jak wykorzystują oni przebieg ćwiczeń do doskonalenia własnych procesów zarządzania incydentami i przygotowania organizacji do kolejnych wyzwań w obszarze cyberbezpieczeństwa. Przykładem takiego wyzwania są nowe zasady ochrony danych osobowych.
- *Bezpieczeństwo skoncentrowane na ludziach* – **Alexander Raczyński**, Sales Engineering North East Europe, Forcepoint.
Co możemy osiągnąć poprzez studiowanie i profilowanie zachowania upoważnionych użytkowników, którzy posiadają rutynowy dostęp do danych?
- *Nowa meteorologia? Czyli zarządzanie ryzykiem danych w chmurze* – **Krzysztof Grabczak**, Sales Director Enterprise Security, Identity Governance w ORACLE.
Transformacja cyfrowa, która odbywa się na naszych oczach, powoduje szybki wzrost wykorzystania chmury obliczeniowej, gdzie stajemy w obliczu bardzo trudnej konfrontacji ze światem nowych, licznych i wyspecjalizowanych zagrożeń. Aby podołać takim wyzwaniom musimy zmienić zasady podejścia i wykorzystać nowe możliwości jakie daje wsparcie Machine Learning czy Big Data. Nasz ekspert opowie w jaki sposób można kontrolować usług oferowane w chmurze.

Sesja Q&A

13.30 – 15.00 Sesja IV DEBATA: Inspiracja, twórczy ferment czy nowe zagrożenie?

Moderator sesji i debaty: Dariusz Polaczyk – Dyrektor Biura Przeciwdziałania Przemysłom w Departamencie Bezpieczeństwa Getin Noble Bank S.A. oraz Przewodniczący Rady Bezpieczeństwa Banków ZBP.

Wstępem do debaty będzie krótka prezentacja jednej z firm oferującej na polskim rynku zaawansowane rozwiązanie FinTech. Produkty oferowane przez firmy tego nowego sektora wzbudzają zarówno zainteresowanie co i obawy o ich bezpieczeństwo. Prezentacja wyrafinowanych technologii, które są wykorzystywane do ochrony nowych produktów i usług finansowych ma za zadanie ukierunkować debatę na próbę odpowiedzi na pytanie: Jak weryfikować bezpieczeństwo nowych produktów i usług oraz w jaki sposób pozyskiwać dla nich wiarygodne referencje?

Wystąpienia:

- *Najlepszy towarzysz w podróży* – **Karol Sadaj**, Country Manager Poland, Revolut.
Poznamy nowe funkcjonalności karty i usługi, które pozwalają na szybkie i pewne zarządzanie jej bezpieczeństwem.
- *Jak chronić komunikację aplikacji?* – **Andrzej Kroczyk**, Manager Systems Engineering Eastern Europe, F5 Networks.
Dowiemy się, w jaki sposób efektywnie chronić komunikację aplikacji odbywającej się poprzez interfejs API (ang. Application Programming Interface).
- *Mamy system SIEM... I co dalej?* – **Marcin Spychała**, Cyber Security Consultant Poland & Baltics, IBM.
Wykrywanie zagrożeń i podatności jest bardzo ważne, ale to dopiero początek. Co dalej powinniśmy robić po ich wykryciu, dowiemy się od naszego eksperta.

W debacie swój udział zapowiedzieli następujący eksperci:

- **Piotr Balcerzak** – Dyrektor Zespołu Bezpieczeństwa Banków, Związek Banków Polskich
- mł. insp. dr hab. inż. **Jerzy Kosiński** – Wyższa Szkoła Policji w Szczytnie

- kom. **Dominik Rozdziałowski** – Dyrektora Biura do Walki z Cyberprzestępczością Komendy Głównej Policji
- dr **Krzysztof Serafin** – Narodowy Bank Polski

15.00 – 15.05 **PODSUMOWANIE VII FBB – Włodzimierz Kiciński, Wiceprezes Zarządu ZBP**

15.05 – 15.20 **Losowanie atrakcyjnych upominków ufundowanych przez sponsorów VII FBB**

15.20 – 17.00 **LUNCH i rozmowy kulturalowe**

Organizatorzy



ZWIĄZEK BANKÓW POLSKICH

Patron honorowy



Ministerstwo
Cyfryzacji

Partnerzy generalni



Partnerzy



Patroni medialni

