Centrum Prawa Bankowego i Informacji

Związek Banków Polskich

BANK 25 lat MIESIĘCZNIK FINANSOWY

PROGRAM

9 maja 2017 r.
Warszawa, Hotel Novotel Centrum

BEZPIECZNY KLIENT = BEZPIECZNY BANK

W trakcie VI edycji konferencji kolejność wystąpień podporządkowano **przebiegowi procesu obsługi klienta banku**. Do grona prelegentów zaprosiliśmy przede wszystkim doświadczonych praktyków. W prezentacjach najnowszych osiągnięć technologicznych oraz debatach połączymy teorię ze studiami konkretnych przypadków. Często będziemy pytać o kryteria, które powinniśmy uwzględniać w trakcie wyboru poszczególnych technologii oraz rozwiązań. Czy potrafimy te kryteria obiektywnie sformułować? Konferencja przyniesie nam odpowiedź.

Sesje Q&A: Nie będą to typowe sesje pytań i odpowiedzi. Zbudowane wg metodologii *disruptive thinking* pozwolą na swoiste „wyjście z koleiny" stereotypowego podejścia. Zapewni to udział w tych sesjach wybitnych ekspertów, których pytania stanowić będą często swoiste uzupełnienia wystąpień prelegentów. W trakcie całego Forum zachęcamy wszystkich uczestników do debaty. Każdy może za pomocą swojego telefonu zadawać pytania oraz wyrażać opinie. Wystarczy wejść na stronę: **www.aleBank.pl/Pytania**.

PROGRAM

9.00 – 9.15 Przywitanie uczestników i otwarcie VI FBB

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

9.15 – 10.30 Sesja I Budujemy mocne fundamenty, czyli zanim przyjdzie do nas klient

Faza zjednywania potencjalnych klientów banku, budowanie u nich świadomości marki banku oraz jej pozytywnego wizerunku. Ale to także czas, w którym opracowujemy nowe rozwiązania organizacyjne i technologiczne, testujemy je oraz wprowadzamy do biznesowej praktyki banku.

Moderator sesji I: Paweł Widawski, Dyrektor Zespołu Systemów Płatniczych i Bankowości Elektronicznej, ZBP.

Wystąpienia:

- *W jaki sposób można zapewnić bezpieczeństwo aplikacji w chmurze obliczeniowej*, **Andrzej Kroczek**, System Engineer Manager for Eastern Europe, F5 Networks.

  Ataki DDoS stają się coraz częstsze i bardziej nieprzewidywalne. Ich celem jest niezmiennie spowodowanie awarii i przerwy w działaniu systemów, ale ataki i atakujący stają się coraz bardziej wyrafinowani. Spektrum zagrożeń staje się coraz szersze. W F5 zauważyliśmy, że ataki można podzielić na cztery typy: ilościowe, asymetryczne, obliczeniowe i wykorzystujące podatności. Co kryje się pod kryptonimem Mirai? Co wspólnego z atakami DDoS mają urządzenia IoT? Czy trzeba przekonywać klienta banku, że usługa bankowości internetowej musi być zawsze dostępna?

- *Bezpieczeństwo banków – 2016*, **Dariusz Polaczyk**, Dyrektor Departamentu Bezpieczeństwa Alior Bank S.A., Przewodniczący Rady Bezpieczeństwa Banków Związku Banków Polskich.

  Przedstawione zostaną wyniki badań przygotowanych przez Prezydium Rady Bezpieczeństwa Banków Związku Banków Polskich, przy organizacyjnym wsparciu Centrum Prawa Bankowego i Informacji.

  Podstawowym celem badania było przedstawienie i porównanie:

  - Rozwiązań organizacyjnych struktur bezpieczeństwa w sektorze bankowym.
  - Najczęstszych przestępstw, z jakimi miały do czynienia banki w Polsce w 2016 roku i ich poziomu.
  - Narzędzi informatycznych stosowanych w pracy komórek odpowiedzialnych za bezpieczeństwo w bankach.

- Skuteczne zabezpieczenie danych przed nieznanymi cyberzagrożeniami, **Aleksander Kroszkin**, Sales Engineer, Trend Micro.

  Nowoczesne instytucje finansowe coraz częściej wykorzystują moc chmury obliczeniowej – prywatnej, publicznej, hybrydowej – dzięki czemu sprawniej przetwarzają dane klientów i działają efektywniej. Czy mają Państwo pewność, że wszystkie serwery i aplikacje bankowe są dobrze zabezpieczone? W jaki sposób skutecznie chronić zasoby bez względu na ich lokalizację?

Sesja Q&A.

10.30 – 10.50 Przerwa kawowa i rozmowy kuluarowe

10.50 – 12.00 Sesja II Otwieramy rachunek dla naszego klienta

Faza intensywnego pozyskiwania danych od nowych klientów, szczególnie danych umożliwiających identyfikację i uwierzytelnienie tożsamości.

Moderator sesji II: Mateusz Górnisiewicz, Doradca Zarządu, ZBP

Wystąpienia:

- *Jakie korzyści w kontekście bezpieczeństwa daje nam monitoring transakcji w czasie rzeczywistym?* **Dariusz Wojtas**, Head of Product Management, IMPAQ.

  Podczas prezentacji eksperci opowiedzą o kluczowych regułach, które pomagają wychwycić wyłudzenia na transakcjach. Wskażą obszary, w jakich banki mogą się zabezpieczyć i co wymaga ciągłej poprawy, aby być zgodnym z obowiązującymi przepisami. Prezentacja będzie dużą dawką praktycznej wiedzy opartej o współpracę z wieloma bankami.

- *EDR jako rozproszone laboratorium.* **Daniel Goldberg**, Director Sales and Business Development EMEA, CYBERBIT.

  Kluczowe pytanie: Jeżeli pełna prewencja jest iluzją, to jak optymalizować nakłady na bezpieczeństwo?

Sesja Q&A.

12.00 – 13.10 Sesja III Bank doradcą swojego klienta w dziedzinie bezpieczeństwa

Zabiegając o rentowność, nie możemy ani na chwilę zapominać o wspólnym bezpieczeństwie. To faza rozszerzania współpracy z klientem banku oraz poszukiwania informacji o jego preferencjach, sytuacji finansowej i czynnikach ją stabilizujących. Jego dane są przetwarzane w wielu systemach. To faza, w której bank staje się doradcą swojego klienta także w dziedzinie bezpieczeństwa.

Moderator sesji III: Tomasz Chlebowski, Prezes Zarządu, ComCERT S.A.

Wystąpienia:

- *Jak ograniczyć zagrożenie związane ze zjawiskiem credential abuse? Perspektywa globalna i lokalna.* **Bartłomiej Jakubowski**, Solutions Engineer, Akamai Technologies.

  „Credential abuse", to jeden z najtrudniejszych i najaktualniejszych problemów do rozwiązania przez ekspertów. Prelegent przedstawi go z perspektywy globalnej oraz pokaże, jak firma Akamai Technologies – wspólnie z klientami z sektora bankowego – próbuje ograniczyć jego skutki oraz go rozwiązać.

- *IMSI Catcher – nowe narzędzie przestępców, ryzyko dla bankowości mobilnej.* **Bartosz Matysiak**, Zastępca Dyrektora Departamentu Bezpieczeństwa NBP, Członek Grupy Roboczej ds. Bezpieczeństwa Europejskiego Systemu Banków Centralnych przy Europejskim Banku Centralnym oraz przedstawiciel NBP w Central Bank Heads of Security Organisation.

  Ekspert opisze nowy rodzaj ataku skierowany na użytkowników wykorzystujących technologie GSM. Odnotowano pierwsze incydenty, ale ze względu na obniżające się ceny wykorzystywanych przez przestępców urządzeń należy założyć, że to dopiero początek. Czy ryzyko to może stanowić zagrożenie dla tak ważnego kanału komunikacji z klientem, jaką daje nam technologia GSM?

Sesja Q&A.

13.10 – 14.00 LUNCH i rozmowy kuluarowe

14.00 - 15.10 Sesja IV Wspólnie piszemy naszą historię

Faza współpracy z klientem, podczas której bank dysponuje dużą ilością danych o kliencie i z nim związanych, a także intensywnie je przetwarza i udostępnia podmiotom zewnętrznym.

Moderator sesji IV: Jerzy Cichowicz, Prezes Zarządu, Kalokagathia Sp. z o.o.

Wystąpienia:

- *Nowe technologie w systemach monitoringu wizyjnego*. **Maciej Pietrzak**, Sales Support Engineer, Dahua Technology Poland.

  Nowe zdobycze techniki i nowe technologie pozwalają znacznie zwiększyć skuteczność systemów monitoringu. Firma Dahua Technology opracowała standardy, które umożliwiają wykorzystanie istniejącej infrastruktury na obiektach i płynną migrację do nowego rozwiązania. W pełni otwarty system pozwala na integrację z istniejącymi elementami różnych systemów, a przy tym oferuje prostotę i przejrzystość.

- *Ocena ryzyka w oparciu o dane z wielu kanałów płatności, czyli jak matematyka, algorytmika i sztuczna inteligencja pomagają zapobiec oszustwom finansowym*. **Konrad Antonowicz**, Specjalista ds. Bezpieczeństwa IT, Passus S.A.

  Wykorzystanie wiedzy naukowej do analizy danych z kanałów płatności elektronicznej w celu zautomatyzowania wykrywania nadużyć i anomalii w zachowaniu klientów. Przykłady zastosowania m.in. w bankowości online oraz transakcji kartami płatniczymi. Przedstawimy metody tworzenia elastycznych reguł, budowania profili łączących dane z wielu źródeł transakcji elektronicznych, jak i możliwości automatyzacji procesów decyzyjnych w oparciu o najnowsze odkrycia z zakresu sztucznej inteligencji.

Sesja Q&A.

15.10 - 16.00 Sesja V Szczególna staranność rozstania

Faza współpracy z klientem, gdzie bank archiwizuje, przenosi lub kasuje dane klienta. Ze względu na podatności oraz reputację banku przetwarzanie danych klienta w tej fazie wymaga zachowania szczególnej staranności.

Moderator sesji V: Krzysztof Kowalski, Doradca Ochrony Danych.

Wystąpienie:

- *Rozwiązania typu DLP (Data Loss Prevention) w kontekście wymagań rozporządzenia GDPR*. **Alexander Raczyński**, Sales Engineering, North East Europe, Forcepoint.

  GDPR narzuca podmiotom pracującym na danych osobowych nowe wymagania. Jednym z nich, które wydaje się kłopotliwe z praktycznego punktu widzenia, jest *„prawo do bycia zapomnianym"*. Jak środki techniczne, a konkretnie technologie klasy DLP mogą nam pomóc w realizacji niektórych aspektów GDPR?

Sesja Q&A.

16.00 – 16.45 Sesja VI DEBATA: Na jakie wsparcie możemy liczyć?

Moderator debaty: Dariusz Polaczyk, Dyrektor Departament Bezpieczeństwa Alior Bank i Przewodniczący Rady Bezpieczeństwa Banków ZBP.

- *Wstęp do debaty,* podkom. **Dominik Rozdziałowski**, Dyrektor Biura do Walki z Cyberprzestępczością Komendy Głównej Policji.

  Utworzenie w strukturze Komendy Głównej Policji specjalnego Biura do Walki z Cyberprzestępczością jest wydarzeniem historycznym, na które długo czekaliśmy. Determinacja, z jaką zostało stworzone, jak również dobór sił i środków budzi nadzieję na współpracę międzyresortową. Debata pozwoli nam na poznanie jej warunków, zakresu, a co za tym idzie – weryfikację oczekiwań.

Podstawowa problematyka:

- Możliwości współpracy oraz zastosowania rozwiązań międzysektorowych (bankowość, energetyka, zdrowie, telekomunikacja, administracja) do np. zwalczania przestępczości podatkowej.
- Współpraca bankowa w obszarze cyberbezpieczeństwa – szczególnie w świetle ostatnich ataków i koncepcji Bankowego Centrum Cyberbezpieczeństwa.

Swój udział w debacie zapowiedział już mł. insp. dr hab. inż. **Jerzy Kosiński**, profesor nadzwyczajny Zakładu Studiów nad Przestępczością Zorganizowaną i Terroryzmem Instytutu Badań nad Przestępczością Kryminalną i Terroryzmem Wydziału Bezpieczeństwa Wewnętrznego Wyższej Szkoły Policji w Szczytnie.

16.45 – 17.00 PODSUMOWANIE VI FBB 2017 – dr Mieczysław Groszek, Związek Banków Polskich

ORGANIZATORZY

PATRONI HONOROWI

PARTNERZY GENERALNI

PARTNERZY

PATRONI MEDIALNI

WWW.ALEBANK.PL/FBB

TWITTER: @MIESIECZNIKBANK / #FORUMBB

FACEBOOK: FACEBOOK.COM/MIESIECZNIKFINANSOWYBANK / #FORUMBB