V Forum Bezpieczeństwa Banków 2016

10 MAJA 2016 R., HOTEL Novotel Centrum w Warszawie

www.aleBank.pl/FBB

Mottem tegorocznego forum jest myśl francuskiego polityka, filozofa i pisarza, który wskazywał na cechy rządzące ludzkimi zachowaniami: hipokryzję, egoizm, słabość i próżność.

**„Bywają fałsze, które tak dobrze udają prawdę,
iż byłoby omyłką nie dać się im oszukać."**

François de La Rochefoucauld

Jak długa jest historia ludzkości, tak długa jest historia oszustwa. Oszuści zawsze poszukiwali luk umożliwiających osiągnięcie celu. Poszukiwania te dotyczyły technologii zabezpieczeń, procesów, a szczególnie ludzkiego funkcjonowania. Dlatego walka z takimi przestępstwami ma charakter wieloaspektowy: technologiczny, psychologiczny, kulturowy i społeczny.

Znajomość tych mechanizmów, poparta rzeczywistymi przykładami, pozwala na skuteczniejszą walkę z przestępczą patologią. Dlatego do grona prelegentów zaprosiliśmy osoby świata nauki zajmujące się technologiami zabezpieczeń, psychologią i socjologią. Zaprosiliśmy także doświadczonych praktyków. Zamierzamy połączyć teorię ze studiami przypadków.

PROGRAM

8.30 - 9.30 Rejestracja

9.30 - 09.45 Przywitanie uczestników i otwarcie Forum

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

9.45 - 10.15 Sesja I Inauguracyjna

- „Plany i zamierzenia Ministerstwa Cyfryzacji w zakresie prewencji i zwalczania przestępczości", **Generał Włodzimierz Nowak**, doradca w Ministerstwie Cyfryzacji.

  Uczestnicy poprzednich wydań FBB pamiętają dalekosiężne plany ministerstwa odpowiedzialnego za cyfryzację. Ukazywana uczestnikom perspektywa 2030 r. była nazbyt odległa, aby przekładała się na poczucie bezpieczeństwa w tym obszarze. Czy środowisko bankowe może liczyć na energiczne, ale też realne co do ich perspektywy czasowej, działania administracji, które wymierzone będą zarówno w istniejące, jak i te antycypowane zagrożenia? Przechodząc zaś do wymiaru biznesowej współpracy pomiędzy administracją a sektorem bankowym, oczekiwać będziemy na następujące pytania: Jakie nadzieje możemy pokładać w modelu federacyjnym e-tożsamości oraz w potencjalnym sukcesie wnioskowania o Program 500+ przez kanały bankowe?

10.15 - 10.50 Sesja II Największe zagrożenia: stan obecny, trendy, skuteczne przeciwdziałania

Podstawowa problematyka:

Jak technologia i rozwiązania proceduralno-organizacyjne mogą pomóc w walce z oszustwami? Przegląd zagrożeń, przede wszystkim tych największych i najkosztowniejszych pod względem strat, jakie powodują. Obserwowane zmiany i ich dynamika – próba projekcji na najbliższe lata. Prezentacja najnowszych na rynku rozwiązań, które mają im zapobiegać.

Wykład wprowadzający:

- „Zagrożenia: stan obecny i obserwowane trendy. Jak przygotować się do przyszłych zagrożeń?": **Dariusz Polaczyk**, Dyrektor Departamentu Bezpieczeństwa Alior Banku S.A., Przewodniczący Rady Bezpieczeństwa Banków ZBP.

10.50 - 12.10 Sesja II/A Zagrożenia zewnętrzne

Moderator Sesji II/A:

- **Mirosław Maj,** Prezes Fundacji Bezpieczna Cyberprzestrzeń.

Podstawowa problematyka:

Jak przeciwdziałać oszustwom i wyłudzeniom popełnianym przez osoby z zewnątrz banku?

To grupa najczęściej pojawiających się zagrożeń i zdawałoby się – najlepiej rozpoznana. Ale schemat „oblężonej twierdzy" i rutyna zmniejszają odporność na nowe sposoby działania przestępców. W sesji zaprezentujemy nie tylko komercyjne rozwiązania przeciwdziałające tym zagrożeniom, ale także zaskakujące wyniki badań.

10.50 - 11.10
- „Najlepszą obroną jest... unikanie zagrożenia": **Krzysztof Nierodka**, Major Account Manager, CHECK POINT.

  Podczas prezentacji przedstawione zostanie rozwiązanie firmy Check Point Software Technologies pozwalające na minimalizację ryzyka wystąpienia strat spowodowanych przez znane i nieznane ataki sieciowe. Zademonstrowana zostanie również unikalna koncepcja redukcji prawdopodobieństwa wystąpienia ataku na system informatyczny.

11.10 - 11.30
- „Bezpieczeństwo logiczne w praktyce, czyli co oferuje audytorowi przemyślana segmentacja sieci?": **Paweł Wachelka**, IP Product Manager, Enterprise Networking Solutions, HUAWEI POLSKA.

  Podczas prezentacji zostanie omówiona problematyka segmentacji sieci, która jest niezbędna do zwiększenia bezpieczeństwa infrastruktury sieciowej oraz przeprowadzenia audytu po incydencie.

11.30 - 11.50
- „Groźne następstwa udanej ewakuacji?", Grzegorz Cieślak, Ekspert Centrum Badań nad Terroryzmem, Collegium Civitas.

  Prelegent w swoim wystąpieniu odpowie przede wszystkim na pytanie: Jakie wnioski dla banków płyną z analiz zamachów terrorystycznych?

11.50 - 12.10
- „Dostęp uprzywilejowany – klucze do królestwa, którego nikt nie pilnuje", **Bartosz Kryński**,Regional Sales Engineer Poland, Hungary and Baltics, Cyberark.

  Dlaczego ochrona kont uprzywilejowanych jest tak istotna? Konta uprzywilejowane stanowią jeden z największych czynników ryzyka bezpieczeństwa banków. Przejęcie przez atakującego danych użytkownika uprzywilejowanego pozwala mu poruszać się w sposób niezauważony wewnątrz organizacji i z każdym krokiem podwyższać swoje uprawnienia. Podczas prezentacji przedstawione zostaną zagrożenia towarzyszące kontom uprzywilejowanym, wskazane zostaną miejsca, gdzie najczęściej można znaleźć niepilnowane hasła, a także przybliżone zostaną przykłady ataków wykorzystujących konta uprzywilejowane. Omówione zostaną również metody skutecznej ochrony.

12.10 - 12.40 Przerwa kawowa

12.40 - 14.00 Sesja II/B Groźna współpraca

Moderator Sesji II/B:

- **Jerzy Cichowicz**, Prezes Kalokagathia Sp. z o.o.

Podstawowa problematyka:

Jak przeciwdziałać oszustwom i wyłudzeniom popełnianym przez współpracujące ze sobą osoby z zewnątrz banku i pracowników banków? To grupa najgroźniejszych zagrożeń. W sesji zaprezentowane zostaną rozwiązania przeciwdziałające tym zagrożeniom, a także praktyczne doświadczenia policyjnych ekspertów oraz firmy ubezpieczeniowej.

12.40 - 13.00
- „Duńska szklarnia", przedstawiciele Komendy Wojewódzkiej Policji w Lublinie: nadkom. **Jarosław Cholewiński**, Zastępca Naczelnika Wydziału do walki z Przestępczością Gospodarczą, podinsp. **Andrzej Solarz**, Ekspert Wydziału do walki z Cyberprzestępczością.

13.00 - 13.20
- „Jak skutecznie budować i wdrażać zabezpieczenia do walki z wyłudzeniami?", Dariusz Wojtas, Head of Product Management, IMPAQ oraz Tomasz Imbiorowski, Dyrektor Departamentu Bezpieczeństwa w Banku Pocztowym S.A.

  Studium przypadku. Autor w swoim wystąpieniu przedstawi sposób budowy, a następnie rozbudowy systemu, który uwzględnia aktualnie występujące oszustwa, monitorowanie zainstalowanego systemu oraz antycypację przyszłych zagrożeń. Punktem wyjścia dla rozważań autora będzie wdrożenie systemu do przeciwdziałania oszustwom kredytowym dla Banku Pocztowego S.A.

13.20 - 13.40
- „Inteligentny detektyw – skuteczny sposób zapobiegania największym zagrożeniom bezpieczeństwa informacji", **Robert Głowacki**, Quest Dystrybucja.

  Jak sprostać zagrożeniom pochodzącym jednocześnie z wnętrza i z zewnątrz organizacji? Banki często nie doceniają elementów infrastruktury i ryzyka z tym związanego dla zachowania bezpieczeństwa i ciągłości działania. Będziemy mówić o koncepcji, która integruje zarządzanie bezpieczeństwem w kontekście efektywności, automatyzacji oraz współdziałania ludzi i systemów będących częścią procesów biznesowych.

13.40 - 14.00
- „Nowy rodzaj terapii – pigułki poprawiające świadomość bezpieczeństwa", **Agata Osewska**, Kierownik Zespołu Kształcenia Świadomości Bezpieczeństwa PZU S.A./PZU Życie S.A.

14.00 - 15.20 Sesja II/C Luki i dziury

Moderator Sesji II/C:

- **Dariusz Kozłowski,** Wiceprezes Zarządu Centrum Prawa Bankowego i Informacji.

Podstawowa problematyka:

Jak przeciwdziałać oszustwom i wyłudzeniom popełnianym przez przestępców wykorzystujących luki prawne, proceduralne i systemowe? To grupa najciekawsza, ale czy rzeczywiście taka groźna? W praktyce okazuje się, że najbardziej niepokojąca poprzez swoją nieprzewidywalność. Zazwyczaj o lukach, czy tzw. dziurach w systemach dowiadujemy się po dokonanym przestępstwie lub podjętej próbie jego popełnienia. Czy można im skutecznie przeciwdziałać? Zaprezentowane zostaną komercyjne rozwiązania przeciwdziałające tym zagrożeniom, ale także niezwykle użyteczne wyniki badań naukowych.

14.00 - 14.20
- „(Nie)legalna rutyna - ewolucja przejmowania wartości", **dr Wojciech Kurowski**, Instytut Zarządzania Wartością, SGH.

  Rutyna dotyczy w tym samym stopniu biznesu jak i sposobów popełniania oszustw. Przestępcy wykorzystują ją w biznesie, ale również sami muszą uważać w organizowaniu przestępstwa. W gospodarce cyfrowej na nowo ożywa pojęcie rutyny poprzez takie słowa, jak automatyzacja i sztuczna inteligencja, algorytmy oraz powielanie pomysłów, procesów i innowacji. Wydaje się zatem, że rutyna jest ewolucyjnym konstruktorem mechanizmów, które mimo setek lat ciągle spajają kreowanie wartości w biznesie legalnym, jak i przestępczym. Jest ona wykorzystywana do tworzenia pułapki przechwytywania wartości oraz w systemach bezpieczeństwa. Dlaczego od wieków chciwość każe nam popełniać tak naiwne błędy? Dlaczego udostępniając tak wiele danych o nas, z taką naiwnością podchodzimy do informacji? Czy znamy na to lekarstwo, jakąś terapię, tabletkę lub plasterek?

14.20 - 14.40

- „Pokonać Ransomware”, **Grzegorz Ciołek**, Fortinet.

  Ransomware z dnia na dzień stwarza coraz większe zagrożenia dla przedsiębiorstw. Raz po raz pojawiają się nowe i często zaskakujące jego odmiany. Zostanie przedstawiona historia tych szkodników – od małych, irytujących programów, do obecnych, bardzo wyrafinowanych odmian szyfrujących. Następnie zanurzymy się głębiej i zobaczymy, w jaki sposób złośliwe oprogramowanie jest dostarczane do ofiary. Prześledzimy poszczególne fazy ataku. Przedstawimy sposoby jak sobie radzić z tym procederem.

14.40 - 15.00

- „Anonimizacja danych – metody ukrywania danych przed niepowołanym personelem”: **Cezary Prokopowicz**, Menedżer Sprzedaży na Europę Wschodnią Enterprise Security Products, HEWLETT-PACKARD ENTERPRISE.

  Webowe i mobilne aplikacje stanowią główny cel ataków hackerskich. Jak zminimalizować to ryzyko? Metoda eliminacji potencjalnych zagrożeń oraz zapewnienia bezpieczeństwa aplikacji poprzez analizę kodu źródłowego, zabezpieczenie kolumn baz danych oraz szyfrowanie poczty do klientów banku.

15.00 - 15.20

- „The Real Cost of Card Not Present Fraud to Your Business”, **Bradi Van Noy Hays**, Entrust Datacard.

  An overview of CNP fraud statistics impacting financial institutions globally and how Entrust Datacard authentication solution is combatting the rising cost and impact.

15.20 - 16.10 LUNCH

16.10 - 17.30 Sesja III DEBATA: Bezpieczeństwo - wyzwania przyszłości

Moderator Sesji III (Debaty):

- **dr Mieczysław Groszek**, Wiceprezes Związku Banków Polskich.

16.10 - 16.40 **Wystąpienie wprowadzające do debaty**:

- „Banki w obliczu aktów terroru – od procesów analitycznych do polityki bezpieczeństwa w ujęciu praktycznym”, **dr Grzegorz Cieślak**, Ekspert Centrum Badań nad Terroryzmem Collegium Civitas.

  Celem wykładu jest wprowadzenie do debaty poprzez postawienie odpowiedź na następujące pytanie: Jakich przyszłych zagrożeń oczekujemy i dlaczego nas zaskoczą? W wykładzie dowiemy się, z jakimi zagrożeniami aktami terroru powinniśmy się liczyć (prognoza dla sektora bankowego na 2016 rok), gdzie mamy do czynienia z deficytami analiz ryzyka i jaką rolę pełni polityka bezpieczeństwa w funkcjonowaniu banku (założenia, a jej rzeczywiste skutki).

16.40 - 17.30 Debata

1. Kultura konkurencyjnego biznesu, a ekspozycja na działania oszustów.
2. Czy procedury i standardy mogą przeciwdziałać wykorzystywaniu przez oszustów tzw. ludzkich słabości?
3. Rola biegłych i „nowej” kryminologii i kryminalistyki w tworzeniu procedur uodparniających organizacje na działania przestępcze.

Uczestnicy:

- **dr Grzegorz Cieślak**, Centrum Badań nad Terroryzmem Collegium Civitas.
- **Sławomir Kosieliński**, Prezes Instytutu Mikromakro.
- **Mł. insp. dr hab. Jerzy Kosiński**, Ekspert Wyższej Szkoły Policji w Szczytnie.
- **Artur Piechocki**, APLaw – Ekspert ENISA.
- **Dariusz Polaczyk**, Dyrektor Departamentu Bezpieczeństwa Alior Banku S.A., Przewodniczący Rady Bezpieczeństwa Banków ZBP.
- **Paweł Weżgowiec**, Ekspert Fundacji Bezpieczna Cyberprzestrzeń, Specjalista ds. standardów ICT Security.

W trakcie Forum, a szczególnie podczas debaty, wszyscy uczestnicy konferencji będą mogli za pomocą swoich telefonów komórkowych zadawać pytania oraz wyrażać opinie. Organizatorzy umożliwią taką interaktywność dzięki specjalnemu systemowi.

17.30 - 17.45 PODSUMOWANIE FORUM – dr Mieczysław Groszek, Wiceprezes Zarządu ZBP

17.45 Losowanie atrakcyjnych upominków ufundowanych przez Sponsorów FORUM

ORGANIZATORZY

Centrum Prawa Bankowego i Informacji

25 lat 1991-2016 Związek Banków Polskich

BANK Miesięcznik Finansowy

PATRONI HONOROWI

BBN Biuro Bezpieczeństwa Narodowego

Ministerstwo Cyfryzacji

NBP Narodowy Bank Polski

PARTNERZY GENERALNI

Check Point Software Technologies Ltd

CYBERARK

Entrust Datacard Trusted Identities | Secure Transactions

FORTINET

Hewlett Packard Enterprise

HUAWEI

IMPAQ

Quest Dystrybucja Dystrybutor Dell Software w Polsce

SOLIDEX®

PARTNERZY

BIK Biuro Informacji Kredytowej

EQUINIX

FORCEPOINT

NCR

WATRA

PATRONI MEDIALNI

aleBank.pl

NBS Nowoczesny Bank Spółdzielczy

www.aleBank.pl/FBB