SEMAFOR 2015 - program

Pierwszy dzień konferencji - 26 marca 2015 (czwartek)

08.00–09.00	**Rejestracja Uczestników. Powitalny poczęstunek.**
09.00–09.10	**Rozpoczęcie konferencji.** *Piotr Filip Sawicki, ISACA Warszawa* *Jacek Skorupka, ISSA Polska, Citibank International* *Sebastian Watras, IDG Poland*
09.10–09.50	**The Windows Phone Freak Show – analiza luk w bezpieczeństwie aplikacji dla systemu Windows Phone razem z możliwością ich wykorzystania w praktyce.** *Luca De Fulgentis, Secure Network S.r.l*
09.50–10.10	**Ewolucja systemów zabezpieczeń wobec wyzwań w zwalczaniu ataków APT.** *Robert Dąbrowski, Fortinet Polska*
10.10–10.30	**Jak wykorzystać moc systemów Sandbox?** *Bartosz Chmielewski, McAfee. Part of Intel Security*
10.30–11.00	**Przerwa kawowa i networking.**
11.00–11.40	**CASE STUDY: Chińczycy od dawna atakują polskie firmy.** Prelekcja przedstawi historię ataku ukierunkowanego na jednego z klientów Niebezpiecznika, który w wyniku działań chińskich włamywaczy poniósł ponad milionowe straty. Ukazane zostaną techniki pracy chińskiego gangu oraz wyniki śledztwa, które ujawniło, że nasz klient nie był pierwszą ofiarą, a proceder wykradania pieniędzy jest regularny i masowy. *Piotr Konieczny, Niebezpiecznik.pl*
11.40–12.00	**The World's First Privileged Activity Monitoring Solution.** *Viktor Varga, Balabit*
12.00–12.30	**Defending against Advanced Persistent Threats with Identity Governance.** • Understand the current state of your existing role and privileged entitlements

compliance
- Establish centralized segregation of duties and risk profiling
- Continually monitor access rights and compliance and risk posture
- Create ID framework for adaptability & change

Yves LE ROUX, CA Technologies

12.30–13.00

Technologie mobilne w przedsiębiorstwie – aktualne trendy, zagrożenia i rozwiązania bezpieczeństwa.

Maciej Smyk, Samsung R&D Institute Poland

13.00–14.00

Lunch dla Uczestników konferencji w restauracji.

Ścieżka Cybersecurity

14.00–14.40

Wybrane problemy bezpieczeństwa aplikacji webowych.

Michał Sajdak, Sekurak

14.40–15.10

Poznaj swojego wroga: Metasploit czyli jedno z bardziej lubianych narzędzi hakerów/pentesterów w praktyce.

Paweł Maziarz, PwC Cyber Security

15.10–15.50

Złośliwe oprogramowanie w bankowości: „żaden problem...”

Przemysław Skowron

Ścieżka Zarządzania

14.00–14.40

Bezpieczeństwo w SDLC - dlaczego inne drogi prowadzą na manowce?

Michał Brandt, Raiffeisen Bank Polska

14.40–15.10

Kluczowe czynniki sukcesu programu IDM.

Jeremi Gryka, Bank BGŻ

15.10–15.50

CaaS (Crime-as-a-Service) – czy każdy może zostać cyberprzestępcą?

Jarosław Sordyl

Ścieżka Audytu

14.00–14.40

Obszar IT Governance i jego rola w procesie audytowym.

Łukasz Bydłosz, Bank BPH
Bartłomiej Dyrga, Bank BPH

14.40–15.10

Audytowanie ukierunkowane na ryzyko – przejście z mechanizmów kontrolnych w kierunku analizy i identyfikacji ryzyk.

- Definicji kontroli i ryzyka;
- Elementy zarządzania ryzykiem;
- Spojrzenia na funkcję audytu z punktu widzenia standardów międzynarodowych IIA; a także
- Model trzech linii obrony.

Lilianna Rother-Obrączka, ING Bank Śląski

15.10–15.50

(Nie)ład informatyczny w praktyce.

Jakub Syta, IMMUSEC

15.50–16.20

Przerwa kawowa i networking.

16.20–17.20

Sesja stolików tematycznych.

Oto lista tematów, które będą poruszane przy stolikach:

STRUMIEŃ AUDYTOWY

- Bezpieczeństwo IT- na czym powinien skupić się audytor IT
  Adam Rafajeński, Information Security and IT Quality Manager, Budimex SA
- Audyt bezpieczeństwa w chmurze – wyzwania, techniki, narzędzia
  Marcin Fronczak, Manager ds. Bezpieczeństwa IT i Ciągłości Działania
- Audyt organizacji zwinnych (agile)
  Michał Olczak, Team Leader, Bank Zachodni WBK
- Audytowanie ukierunkowane na ryzyko
  Lilianna Rother-Obrączka, Menedżer Audytu, ING Bank Śląski

STRUMIEŃ HARD SECURITY

- Wykrywanie i zapobieganie atakom APT
  Michał Kurek, Dyrektor w Dziale Zarządzania Ryzykiem Informatycznym, EY
- Weryfikacja bezpieczeństwa aplikacji - Czy można ją uporządkować, ustandaryzować lub zautomatyzować?
  Wojciech Dworakowski, IT Security Expert, Securing
- Pomiar bezpieczeństwa informacji
  Krzysztof Sierański, Security Consultant, Bupa
- Obiekty Infrastruktury Krytycznej w Polsce – wyzwania dla bezpieczeństwa, szczególnie teleinformatycznego.
  Piotr Roguski, Kierownik Działu Infrastruktury Krytycznej, Ochrony i Obronności, Polskie Górnictwo Naftowe i Gazownictwo
- Bankowość internetowa kontra malware - Jak leczyć przyczyny a nie skutki?
  Przemysław Skowron, Konsultant bezpieczeństwa IT
- Wyzwania współczesnej informatyki śledczej na przykładzie CLOUD FORENSICS - aspekty praktyczne i dobre praktyki.
  Krzysztof Bińkowski, Trener i konsultant SECURITY/FORENSCIC, Net Computer
- DDoS - Ataki odmowy obsługi - przyczyny, realizacja i skutki
  Marcin Marciniak, dziennikarz technologiczny, Computerworld

STRUMIEŃ SECURITY MANAGEMENT

- Rekomendacja D dla ubezpieczycieli (nowe wytyczne dla zakładów ubezpieczeń)
  Antoni Pajdo, Manager ds. bezpieczeństwa IT, ING Usługi Finansowe
- Cyber intelligence – jak odpowiedzieć na zagrożenie
  Łukasz Guździoł, AVP, Functional Risk Management Lead, Technology Risk Officer, Technology Risk & Information Security Wrocław
- Wyzwania związane z ochroną danych osobowych i prywatności w modelu Cloud Computing w globalnych organizacjach
  Aleksander Czarnowski; mec. Maciej Gawroński
- Praktyczne podejście do zarządzania ryzykiem
  Jarosław Stawiany, Kierownik Wydziału Zarządzania Procesami i Ryzykami Bezpieczeństwa Teleinformatycznego, Orange Polska
- Budowanie świadomości (awareness) w obszarze zarządzania bezpieczeństwem informacji
  Agata Osewska, Kierownik w Biurze Bezpieczeństwa, PZU SA
- Czy warto wdrażać ISO27001? Koszty i korzyści.
  Hubert Pilarski, Risk Manager, T-Mobile Polska

17.20–17.30

Zakończenie pierwszego dnia konferencji.

19.30–23.59

Spotkanie integracyjne Uczestników konferencji.

Drugi dzień konferencji - 27 marca 2015 (piątek)

09.30–10.10

Managing Your Business According to the Rules – How the Privacy and Security Regulation Patchwork affects Business.

Mark Williams, BlueCross BluShield of Tennessee

10.10–10.40

Bezpieczeństwo informacji - trzy perspektywy, wspólna odpowiedzialność.

Hubert Konopacki, PZU SA
Piotr Ratajczak, PZU
Artur Rudy, PZU

10.40–11.05

Five trends you should worry about. And the other 5 you probably shouldn't.

Michael Haas, WatchGuard

11.05–11.35

Czym ONI nas atakują? Analiza prawdziwych zagrożeń pochodzących z Internetu.

Marcin Marciniak, Computerworld

11.35–12.00

Przerwa kawowa i networking.

Ścieżka Cybersecurity

12.00–12.40

High Assurance Information Exchange Between Protected Domains.

- How can you share information between restircted- and open environments without comprimising security?
- How can the risk for information leaks in the transmission system be mitigated?
- Critical infrastructure, Healthcare and Public sector - how is the challenge adressed and what are typical use-cases?

Martin Nordqvist, Advenica AB

12.40–13.10

Ścieżka Zarządzania

12.00–12.40

Zarządzania ryzykiem w kontekście wieloaspektowej oceny wagi zagrożeń.

Łukasz Guździoł, Technology Risk & Information Security Wrocław

12.40–13.10

Administrator – pan i władca, czy zwykły pracownik?

Mariusz Przybyła, Quest Dystrybucja
Grzegorz Szafrański, Quest Dystrybucja

13.10–13.40

Websense Security Labs - the concept behind it.

Alexander Raczyński, Websense

Ścieżka Audytu

12.00–12.40

Nowe normy serii 27000.

Janusz Cendrowski, Asseco Poland

12.40–13.10

Wdrożenie i integracja SZCD ISO22301 z SZBI ISO/IEC 27001.

1. Wymagania normy ISO/IEC 27001 w zakresie ciągłości działania ISO22301
2. Omówienie procesu zarządzania ciągłością działania wg ISO 22301 i jego praktyczna implementacja
3. Integracja SZCD i SZBI w jeden zintegrowany system zarządzania

VPN dla dużych chłopców. Co fizycy zrobili z protokołem IPSec?

Piotr Nowotarski, *Barracuda Networks*

13.10–13.40

Trojany finansowe w 2014 roku.

Maciej Iwanicki, *Symantec Poland*
Paweł Wojciechowski, *Symantec Poland*

Marek Abramczyk, *Exatel SA*
Piotr Stępniewicz, *Exatel SA*

13.10–13.40

Ocena bezpieczeństwa dostawców.

Łukasz Komorzycki, *The Royal Bank of Scotland*

13.40–14.40 **Lunch dla Uczestników konferencji w restauracji.**

14.40–15.20

Typowe podatności mobilnego dostępu do Internetu.

Karol Więsek

15.20–16.00

Warsztat: Testowanie bezpieczeństwa aplikacji mobilnych na przykładach platformy Android. Część 1

- dekompilacja i analiza kodu aplikacji
- pliki zapisywane przez aplikację na urządzeniu
- weryfikacja logów systemowych
- badanie możliwości ataku na wystawione przez aplikację IPC
- poprawność konfiguracji połączenia SSL
- przechwytywanie ruchu sieciowego pomiędzy aplikacją mobilną a serwerem
- atakowanie interfejsu API po stronie serwera

Uczestnicy otrzymają maszynę wirtualną zawierającą komplet narzędzi wspomagających ocenę bezpieczeństwa aplikacji mobilnych oraz przykładowe aplikacje zawierające podatności, możliwe do uruchomienia w załączonym emulatorze Android. Dla każdej podatności omówione zostanie ryzyko z nią związane, a

14.40–15.20

Nowe trendy i wymagania budowy sieci bezprzewodowych z uwzględnieniem analityki aplikacji, zarządzania tożsamością użytkowników i korelacji informacji bezpieczeństwa - WiFi 2.0.

Dawid Królica, *Extreme Networks*
Marcin Laskowski, *Extreme Networks*

15.20–16.00

Wdrożenie PCI DSS w organizacji.

Bartosz Kwiatkowski, *AXA Assistance Solutions*

16.00–16.40

Darmowe narzędzia wspomagające procesy zabezpieczania infrastruktury firmowej.

Borys Łącki, *Logicaltrust*

14.40–15.20

Czy Twoje firewalle chronią Cię wystarczająco?

- Co to jest i do czego służy firewall dzisiaj, w tym np. typy zapór sieciowych;

- Dlaczego potrzebujemy firewalli, najczęstsze zastosowania oraz wymagania regulacyjne;

- Weryfikacja aspektów technicznych takich jak architektura, konfiguracja, ochrona dostępu do firewall, hardening, logowanie, klastrowanie;

- Sprawdzenie aspektów procesowych jak np. zarządzanie konfiguracją, analiza ryzyka związana z modyfikacją reguł firewall, rejestr wyjątków, wpływ na Secure SDLC i zarzadzanie projektami;

- Przykłady, gdzie można się spodziewać najsłabszych punktów

Prezentacja celuje w omówienie najważniejszych i najciekawszych elementów takiego audytu. Nie jest celem prezentacji dostarczenie kompletnego zestawienia testów audytowych czy też podręcznikowej wiedzy dot. audytowania systemów informatycznych.Temat zainteresuje zapewne audytorów IT, osoby zarządzające IT i bezpieczeństwem IT, architektów infrastruktury oraz

także sposoby jej usunięcia.

Sławomir Jasek, Securing

16.00–16.40

Warsztat: Testowanie bezpieczeństwa aplikacji mobilnych na przykładach platformy Android. Część 2

Sławomir Jasek, Securing

administratorów sieci.

Rafał Gucwa, UBS

15.20–16.00

Warsztat: Zastosowanie nowego programu audytu w metodyce COBIT 5 do prowadzenia kompleksowych audytów IT. Część 1

Joanna Karczewska, ISACA Warsaw Chapter

16.00–16.40

Warsztat: Zastosowanie nowego programu audytu w metodyce COBIT 5 do prowadzenia kompleksowych audytów IT. Część 2

Joanna Karczewska, ISACA Warsaw Chapter

16.40–17.00 **Podsumowanie i zakończenie drugiego dnia konferencji.**

Organizatorzy dołożą wszelkich starań, aby konferencja odbyła się zgodnie z prezentowanym programem, jednak zastrzega się możliwość częściowych zmian.