SEMAFOR 2016 - program

Pierwszy dzień konferencji - Czwartek 17 Marca 2016

08.00–09.00	**Rejestracja uczestników**
09.00–09.10	**Rozpoczęcie konferencji**
09.10–09.50	**How to talk about Information Security Governance with your boss in the elevator?** *Bruno Horta Soares, CISA®, CGEIT®, CRISC™, PMP®, Founder & Senior Advisor, GOVaaS - Governance Advisors, as-a-Service, Lda.*
09.50–10.10	**NERC CIP Compliance at E.ON - a Shell Control Box Case Study** *Zoltan Bakos, Balabit*
10.10–10.50	**Cybersecurity capability models** *Antonio Ramos, CISA, CISM, CRISC, CCSK, CDPP, ITIL Srv. Manager, Jonah*
10.50–11.20	**Przerwa kawowa i networking**
11.20–12.00	**Zapewnienie bezpieczeństwa teleinformatycznego w systemie ochrony infrastruktury krytycznej RP** *Maciej Pyznar, Szef Wydziału Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa*
12.00–12.30	**Weapons of mass intelligence to fight the bad bots** *Stefan Mardak, Senior Enterprise Security Architect, Akamai Technologies*
12.30–13.00	**Czy chmura i NGFW są na siebie gotowe?** *Robert Dąbrowski, Starszy inżynier systemowy, Fortinet*
13.00–13.15	**Rozstrzygnięcie konkursu Security Excellence 2016 i rozdanie nagród laureatom**
13.15–14.00	**Lunch dla uczestników konferencji**

Audyt IT

14.00–14.40

Warsztat - część I: Zastosowanie audytu w metodyce COBIT do prowadzenia kompleksowych audytów informatycznych.

Joanna Karczewska, ISACA Warsaw Chapter

14.40–15.20

Warsztat - część II: Zastosowanie audytu w metodyce COBIT do prowadzenia kompleksowych audytów informatycznych.

Joanna Karczewska, ISACA Warsaw Chapter

15.20–16.00

Warsztat - część III: Zastosowanie audytu w metodyce COBIT do prowadzenia kompleksowych audytów informatycznych.

Joanna Karczewska, ISACA Warsaw Chapter

16.00–16.30

Przerwa kawowa i networking

16.30–16.55

Warsztat - część IV: Zastosowanie audytu w metodyce COBIT do prowadzenia kompleksowych audytów informatycznych.

Joanna Karczewska, ISACA Warsaw Chapter

16.55–17.35

Warsztat - część V: Zastosowanie audytu w metodyce COBIT do prowadzenia kompleksowych audytów informatycznych.

Joanna Karczewska, ISACA Warsaw

Techniczne aspekty bezpieczeństwa informacji

14.00–14.40

Obcy kod w twojej przeglądarce

Prezentacja jest podsumowaniem badań prowadzonych w IDG, dotyczących bezpieczeństwa pracy firmowego środowiska IT z aplikacjami webowymi.

Marcin Marciniak, Dziennikarz, autor TechnoBloga, Computerworld

14.40–15.00

Jak zwiększyć bezpieczeństwo stacji roboczej i sieci komputerowej?

Prezentacja to pokaz praktycznej kontroli infrastruktury teleinformatycznej. Podczas prezentacji przedstawione zostaną kluczowe zagadnienia związane z bezpieczeństwem stacji roboczej i sieci komputerowej w obszarze monitorowania sieci, notyfikacji, inwentaryzacji oprogramowania i infrastruktury IT, zarządzania awariami oraz ochrony kluczowych danych.

Magdalena Wąsik, Inżynier Sprzedaży, Axence

15.00–15.25

Full packet capture w praktyce Weapons of mass intelligence to fight the bad bots

Robert Michalski, inżynier systemowy, Blue Coat Systems

15.25–16.00

Data Access Governance – czy wszystko mamy pod kontrolą?

Mariusz Przybyła, Konsultant IdM, Quest Dystrybucja

Zarządzanie bezpieczeństwem informacji

14.00–14.40

Błędy w zarządzaniu tożsamością i uprawnieniami (Jak zepsuć zarządzanie tożsamością).

Paweł Kulpa, Architekt rozwiązań bezpieczeństwa, Qumak

14.40–14.50

Czym jest Enteprise Digital Footprint i dlaczego zarządzanie cyfrowym śladem organizacji jest tak ważne w 2016 roku?

Daniel Spica, Spica Solutions
Colin Verrall, RiskIQ

14.50–15.05

O monitorowaniu cyberbezpieczeństwa systemów automatyki przemysłowej (OT) - praktycznie.

Dla świata IT najlepszą praktyką jest architektura "Defense In Depth". Czy tak samo dobrze sprawdza się dla systemów OT? Jak powinna wyglądać referencyjna architektura bezpieczeństwa? Jakie elementy są szczególnie istotne czy integracja z SOC funkcjonującym w obszarze IT jest możliwa?

Te i inne zagadnienia omówimy podczas tej prezentacji. Jednak jest ona adresowana nie tylko dla przedstawicieli firm posiadających systemy automatyki – zachęcamy do refleksji nad obecnymi paradygmatami w bezpieczeństwie IT i ich aktualności w kontekście bieżących zagrożeń.

Patryk Gęborys, Wicedyrektor w zespole cyberbezpieceństwa, PwC
Wojciech Kubiak, Starszy konsultant w

Chapter

16.00–16.30

Przerwa kawowa i networking

16.30–16.55

Jak zyskać przewagę w nierównej walce z atakami ukierunkowanymi - dobór skutecznych narzędzi przeciw atakom Advanced Persistent Threat

Janusz Mierzejewski, Presales Engineer, Symantec

16.55–17.35

Hacker vs reszta świata – wybrane przypadki

Michał Sajdak, Założyciel i redaktor serwisu, Sekurak

zespole cyberbezpieczeństwa, PwC

15.05–15.45

Usunięcie wszystkich plików nie zatrze wszystkich śladów - Jak namierzyliśmy agresora - Studium przypadku

Marcin Ulikowski, CSIRT Senior Security Engineer, Atos

15.45–16.15

Przerwa kawowa i networking

16.15–16.55

Ostateczni dowódcy. Autodestrukcyjny imperatyw bezpieczeństwa.

Błażej Boczula
Filip Nowak

16.55–17.35

Ochrona informacji poufnych w relacjach z pracownikami i współpracownikami.

Agnieszka Wachowska, Radca prawny, Traple Konarski Podrecki i Wspólnicy

17.35–17.45 **Zakończenie pierwszego dnia konferencji. Losowanie nagród**

20.00–23.59 **Spotkanie integracyjne uczestników konferencji- Klub Iguana**

Drugi dzień konferencji - Piątek 18 Marca 2016

08.30–09.20 **Rejestracja uczestników niezarejestrowanych pierwszego dnia**

09.20–10.00 **Evolving Cyber Security Profession**

Geoff Harris, Prezes ISSA w Wielkiej Brytanii, ISSA

10.00–10.20 **4D Security – jako przykład holistycznego podejścia do Bezpieczeństwa IT.**

Czy droga oparta na zwiększaniu budżetu oraz ilości zabezpieczeń może w dłuższej perspektywie prowadzić do oczekiwanych efektów? Jest to wątpliwe biorąc pod uwagę fakt, że systemy te stają się coraz bardziej skomplikowane, a zaczynamy również odczuwać brak specjalistów w zakresie Bezpieczeństwa IT potrzebnych do ich obsługi. W ramach

prezentacji chciałbym przyjrzeć się bardziej holistycznemu podejściu do tego zagadnienia na przykładzie koncepcji 4D Security firmy Forcepoint.

Alexander Raczyński, Sales Engineering, North East Europe, Forcepoint

10.20–11.00

OWASP Application Security Verification Standard (ASVS) wersja 3.0

Na etapie weryfikacji umożliwia on sprawdzenie czy są stosowane zasady dobrej praktyki i pozwala audytorowi na wypowiedzenie się o tym co jest poprawne, a nie tylko na koncentrowaniu się na błędach, jak to ma miejsce przy nieustandaryzowanych testach bezpieczeństwa. Ponadto stosowanie ASVS powoduje sprecyzowanie zakresu testów bezpieczeństwa, co jest istotne przy zlecaniu testów bezpieczeństwa na zewnątrz organizacji.

Wojciech Dworakowski, IT Security Expert, SecuRing

11.00–11.30

Przerwa kawowa i networking

11.30–12.10

OpenSAMM: risk-driven software assurance

Bart De Win, Member of the OWASP Belgium Chapter board

12.10–12.50

OWASP Mobile TOP 10 na przykładzie aplikacji bankowych

Mateusz Kocielski, LogicalTrust

12.50–13.40

Lunch dla uczstników konfernecji

Techniczne aspekty bezpieczeństwa informacji

13.40–14.20

Praktyczne aspekty zapewnienia bezpieczeństwa aplikacji

W trakcie prezentacji zostaną przedstawione spostrzeżenia prelegenta w kwestii najlepszych praktyk tworzenia bezpiecznych aplikacji wynikające z doświadczenia opartego na kilkudziesięciu projektach audytu bezpieczeństwa aplikacji.

Poruszone zostaną tematy:

- budowania programu tworzenia bezpiecznych aplikacji przy uzyciu różnych aktywności,

Zarządzanie bezpieczeństwem informacji

13.40–14.20

"Czy jesteś dobrze przygotowany na przyszłość?" - innowacyjność w zarządzaniu ryzykiem technologicznym oraz bezpieczeństwem informacji w tych przełomowych czasach.

Niniejsza prezentacja umożliwi lepsze zrozumienie otaczających nas zmian technologicznych oraz rewolucji cyfrowej, która odciska swoje piętno na kolejnych sferach naszego życia. Zastanowimy się jak stać się częścią tych zmian, a jednocześnie być w stanie kontrolować związane z nimi

Audyt IT

13.40–14.20

Analiza wyników audytu bezpieczeństwa IT w Jednostkach Administracji Rządowej

Prezentacja wydaje mi się ciekawa, ponieważ Klienci przy prezentacji wyników audytu na zgodności z ISO 27001 zazwyczaj pytają „a jak nasza organizacja wypada na tle innych?" – liczę że ta prezentacja odpowie na to pytanie.

Kamil Pszczółkowski, Ekspert ds. bezpieczeństwa

14.20–15.00

Wykorzystanie standardów

takich jak: szkolenia wewnętrzne, definiowanie wymagań, programy bug bounty,
- współpracy z dostawcami zewnętrznymi pod kątem ich odpowiedzialności za podatności bezpieczeństwa,
- omówione zostaną główne wady i zalety podstawowych typów testów bezpieczeństwa, takich jak testy penetracyjne, testy narzędziami automatycznymi czy przeglądy kodu, wraz z dyskusją na temat specyfiki poszczególnych metod.

Uczestnicy wykładu uzyskają wiele praktycznych informacji m.in. na temat budowania programów zapewnienia bezpieczeństwa aplikacji w swoich organizacjach, zamawiania na rynku usług z dziedziny bezpieczeństwa aplikacji.

dr inż. Jakub Botwicz, Manager, Advanced Security Center, EY

14.20–15.00

Utrzymanie bezpieczeństwa aplikacji produkcyjnych na przykładach

W trakcie swojej prezentacji poruszę problematykę utrzymania bezpieczeństwa aplikacji po wdrożeniu produkcyjnym. Na przykładowych aplikacjach pokażę wyzwania z tym związane, w odniesieniu do konkretnej aplikacji oraz realiów, w jakich funkcjonuje. Wspólnie z uczestnikami przeanalizujemy możliwe mechanizmy mające na celu utrzymanie bezpieczeństwa aplikacji. Zastanowimy się nad optymalnym ich doborem oraz momentem, w którym warto z nich skorzystać, uwzględniając również koszt wykorzystania danego mechanizmu.

Przyjrzymy się mechanizmom takim jak:

ryzyko i nie dać się zaskoczyć.

Łukasz Guździoł, AVP, Functional Risk Management Lead, Technology Risk Officer, Technology Risk & Information Security Wrocław

14.20–15.00

Reakcja na incydent - studium przypadków

Grzegorz Idzikowski, Manager, EY
Tomasz Wilczyński, Manager, Advanced Security Center, EY

15.00–15.30

Przerwa kawowa i networking

15.30–16.10

Błędy typu "information-in-transit", czyli jak nie należy ustalać procesu wymiany danych

Jakub Syta

16.10–16.50

Bezpieczeństwo informacji - edukacja pracowników - dlaczego robimy to źle?

Efektywne zwiększanie świadomości personelu to proces skomplikowany i trudny, wychodzący daleko poza ramy standardowych kursów, do których przyzwyczajeni są pracownicy. Autor przedstawi nowe podejście do edukacji 'najsłabszego ogniwa' każdego systemu bezpieczeństwa, poparte testami i własnym doświadczeniem.

Borys Łącki, IT Seurity Consultant, Logicaltrust

branżowych przy audycie bezpieczeństwa konfiguracji systemów IT

Adam Gałach, Międzynarodowy ekspert bezpieczeństwa systemów teleinformatycznych

15.00–15.30

Przerwa kawowa i networking

15.30–16.10

Wyzwania audytu w dobie nowych zagrożeń bezpieczeństwa

W trakcie wystąpienia zostaną poruszone kwestie:

- oceny opublikowanych przez Ministerstwo Cyfryzacji w styczniu br. wytycznych do audytowania systemów informatycznych
- analizy ryzka jako podstawowego „narzędzia" audytora
- nowych wyzwań w zakresie bezpieczeństwa (np. „shadow IT", „łańcuchy podwykonawców" outsourcingu IT oraz modelu Cloud Computing, ocena skuteczności szkoleń dot. phishingu) na jakie muszą być przygotowani audytorzy

Adam Mizerski, Prezes ISACA Katowice, ISACA Katowice Chapter

16.10–16.50

Audyt bezpieczeństwa w rozmiarze XXL

Prezentacja to opis doświadczeń zebranych podczas 10 miesięcy audytu bezpieczeństwa (technicznego i proceduralnego) systemu informatycznego dla jednego z największych klientów na świecie. Zawiera zarówno informacje techniczne jak i doświadczenia i obserwacje związane z audytem

- testy penetracyjne
- konsultacje/szkolenia
- definiowanie wymagań dotyczących bezpieczeństwa aplikacji
- obsługa incydentów
- narzędzia automatyczne
- monitorowanie podatności w wykorzystywanych komponentach

Postaramy się również wypracować odpowiedzi na poniższe pytania:

- Co można zrobić wewnętrznie?
- Jakie prace zlecić?
- Jakich kompetencji poszukać?
- Jak dobrać szkolenia?
- Jakiego typu narzędzi poszukać?
- Co uwzględnić w rozmowach z dostawcą aplikacji?

Chciałbym dać uczestnikom proste recepty na to, jak zadbać o utrzymanie bezpieczeństwa aplikacji, z którymi pracują.

Mateusz Olejarka, Starszy specjalista ds. bezpieczeństwa IT, SecuRing

15.00–15.30

Przerwa kawowa i networking

15.30–16.10

Piękno systemów biometrycznych

- zostaną usystematyzowane pojęcia podstawowe z przedmiotowego obszaru
- przedstawione zostaną systemy biometryczne (w laboratorium oraz życiu codziennym)
- przedstawiony zostanie problem bezpieczeństwa systemów biometrycznych
- zostanie przeprowadzona na żywo analiza podatności systemu biometrycznego
- zostanie przeprowadzona 5 minutowa sesja Q&A dotycząca systemów biometrycznych (służę

informatycznym środowiska klasy enterprise.

Krzysztof Olejniczak, Service Delivery Manager, Sysnet Global Solutions

wiedzą zdobywaną w tym zakresie na przestrzeni ostatnich 18 lat)

Adrian Kapczyński, Adiunkt, Politechnika Śląska, Instytut Matematyki

16.10–16.50

Dynamiczna analiza złośliwych makr VBA w dokumentach Microsoft Office

Kacper Szurek, Detection Engineer, ESET

16.50–17.00 **Podsumowanie i zakończenie konferencji.**

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