1 dzień konferencji - 15 marca 2018

08.50–09.00

Rozpoczęcie konferencji

09.00–09.30

Opening Speech

Matt Loeb, Chief Executive Officer, ISACA

09.30–10.00

Countering Security Threats with Trusted Intelligent Identities

Threats to Digital business in today’s highly connected world are on a rise and need to be addressed urgently. With proliferation of Digital Identities, Digital / Mobile Payments, Crypto Currency and increased use of mobile & cloud applications – new types of threats are emerging. Governments and standards bodies are working to secure personal information and data through initiatives like GDPR & PSD2. Transformation and Innovation in Authentication space are moving fast with Trusted Intelligent Identities in mobile and cloud, Behavioral Biometrics, Biometrics Authenticators (Iris, Face, Vein, Heartbeat etc.) and Use of Machine learning technology. We will discuss the current situation and how we can address & secure the digital business and apps using Trusted Intelligent Identities and the latest Innovative Technologies.

Rajan Barara, Global Senior Product Manager, Entrust Datacard

10.00–10.20

F-secure

10.20–10.40

Akamai

10.40–11.00

Dezinformacja i manipulacja w dobie internetu - analiza przypadków

Adam Haertle, Trener, wykładowca, redaktor naczelny, ZaufanaTrzeciaStrona.pl

11.00–11.30

Przerwa na kawę i herbatę. Networking.

11.30–12.00

Wpadki i potknięcia polskich banków

Piotr Konieczny, Założyciel, Niebezpiecznik.pl

12.00–12.20

Operationalise GDPR and Privacy by Design: What to Automate in Your Privacy Programme

To operationalise GDPR, companies will need to build the principles of privacy by design into all of their business processes. In this session, learn about the different parts of a privacy programme from PIA/DPIAs, data mapping, consent management, and cookie compliance to subject rights requests and vendor risk management. Discover how your organization can streamline privacy management through software automation, and where humans are absolutely essential.

Ian Evans, Managing Director, OneTrust EMEA

12.20–12.35

Innowacje w zarządzaniu bezpieczeństwem: szanse czy ryzyko?

Stosowanie sprawdzonych rozwiązań z zakresu bezpieczeństwa informatycznego podnosi bezpieczeństwo do pewnego momentu. Dokładanie kolejnych rozwiązań może już nie zwiększać bezpieczeństwa w sposób istotny. Czy rozwiązania innowacyjne mogą zmienić tę sytuację? Czy branża cyberbezpieczeństwa powinna inwestować w rozwiązania innowacyjne (domyślnie: niesprawdzone)? Czy raczej nie powinna ponosić ryzyka i konsekwentnie inwestować w rozwiązania sprawdzone, także przez hakerów? Wdrożenie jakiego typu innowacyjnych rozwiązań dla cyberbezpieczeństwa warto rozważyć?

- Modyfikowanie i ulepszanie procesów bezpieczeństwa czyli cykl Deminga dla funkcjonalności aplikacji
- Automatyzacja procesów związanych z bezpieczeństwem: skoro coraz więcej ataków jest automatycznych, to odpowiedź i remediacja też powinna być automatyczna.
- Tworzenie zintegrowanych systemów bezpieczeństwa

Jakub Jagielak, Security Business Development Manager, Atende

12.35–12.55

The True Value of Security Automation From Rule-Based to Artificial Intelligence

With the evolution of cyber-attacks into well-orchestrated operations and growing risk of breaches, Enterprises find themselves adding more and more layers of security, creating a complex environment to maintain and manage as well as an ever-growing flood of data that analysts need to go through to properly assess risk.
Overwhelmed security teams are ready to embrace automated solutions into their security operations, understanding that automated threat detection and investigation processes will not only deliver better security through actionable data, but also enable them to scale their team without the need to expand their workforce.
But what does security automation mean in reality? Which SOC activities are candidates for automation and which must involve human interaction? Are all automation methods the same? And what is the tangible ROI organizations can expect?
Join our presentation where we take a deeper look into and assess the value of different flavors of security automation, from rule-based alert validation and triaging to fully autonomous cyber investigations powered by artificial intelligence.

Assaf Eyal, Senior Vice President, Verint Enterprise Cyber Global Business

12.55–13.25

Raport NIK

13.25–14.30

LUNCH

CYBER-1	MGM-1	AUDYT-1	CLOUD-1
14.30–14.50	14.30–14.50	14.30–14.50	14.30–14.50
EMCA	**ECTACOM**	**SNOW SOFTWARE**	**INFOBLOX**
14.50–15.10	14.50–15.10		14.50–15.10

T-MOBILE

15.10–15.40

Ryzyko kontra marketing – techniczna ocena popularnych podatności

W trakcie prezentacji zostaną przedstawione techniczne aspekty głośnych podatności, w szczególności zidentyfikowanych w ciągu ostatniego roku. Postaramy się odpowiedzieć na pytanie jakie realne ryzyko wynika z tych kwestii, w jaki sposób można było się przed nimi zabezpieczyć oraz dlaczego ciągle powtarzane są stare błędy. Na zakończenie spróbujemy ocenić, czy w dzisiejszych czasach faktycznie każda istotna podatność musi posiadać domenę, logo oraz chwytliwą nazwę i czy taki marketing może mieć pozytywny wpływ na nasze bezpieczeństwo.

Marcin Strzałek, Konsultant Cyber

Monitorowanie bezpieczeństwa - trendy i kierunki rozwoju

- Najczęstsze problemy z jakimi zmagają się organizacje przy budowie funkcji monitorowania (SOC)
- Globalne trendy związanych z rozwojem i funkcjonowaniem komórek SOC (aspekt technologiczny i organizacyjny)
- Obserwowane kierunki rozwoju komórek SOC i zwiększania ich dojrzałości w warstwie technologicznej i organizacyjnej
- Problematyka zasobów ludzkich

Tomasz Sawiak, Wicedyrektor w zespole Cyber Security, PwC

15.10–15.40

Czy jesteśmy bezpieczni, jak zobaczyć nasze cyberbezpieczeństwo, kilka słów o cyberdashboardzie

14.50–15.10

Zintegrowany system zarządzania bezpieczeństwem informacji i ciągłością działania – które elementy wykorzystać do wdrożenia RODO?

W ramach prezentacji omówione zostaną praktyczne aspekty wdrażania i certyfikacji zintegrowanego systemu zarządzania bezpieczeństwem informacji i ciągłością działania, z naciskiem na kluczowe czynniki sukcesu. W drugiej części przedstawiona będzie koncepcja wykorzystania elementów działającego systemu zarządzania do wdrożenia wymagań RODO.

Izabela Kos-Kleysa, Kierownik Zespołu Organizacji Systemów Zarządzania, ASSECO Poland S.A.
Bartłomiej Szlagowski,

SINERCIO

15.10–15.40

Organizacja procesu zarządzania ryzykiem od strony dostawców

W trakcie prelekcji uczestnicy dowiedzą się jak efektywnie zorganizować proces zarzadzania ryzykiem pochodzącym od naszych dostawców, m. in.:

- Wyzwania związane z naszymi dostawcami. Po co nam dostawcy? Co o dostawcach jako procesorach danych mówi RODO?
- Rekomendowane kroki związane z zapewnieniem zgodności i minimalizacji ryzyka (w kontekście weryfikacji zgodności oraz możliwości przeprowadzenia audytu).
- Przykład zarządzania dostawcami
- Krótki quiz dla uczestników związany z procesem zarządzania

Security, KPMG

15.50–16.20

Przerwa na kawę i herbatę. Networking.

16.20–16.50

IAM, IAG … good, bad and ugly: 10 rzeczy, których nie dowiesz się od dostawców rozwiązań

System zarządzania tożsamością to brzmi dumnie. Dostawcy tych rozwiązań obiecują rozwiązanie wszystkich problemów, i to bez większego wysiłku ze strony organizacji. A jak wygląda rzeczywistość? Dobrze wprowadzony program zarządzania tożsamością i dostępem może stanowić fundament bezpieczeństwa firmy i pozytywnie wpłynąć na pracę użytkowników. Dlaczego więc tak wiele z wdrożeń trwa lata, kosztuje miliony i kończy się porażką?

Problem mierzalności bezpieczeństwa jest dosyć powszechny i rozumiany. Druga linia cyberobrony ma za zadanie stale mierzyć poziom bezpieczeństwa organizacji, poznawać obszary, które wymagają poprawy i oceniać implementowane mechanizmy kontrolne. Umiejętność określenia wskaźników, które w czasie rzeczywistym będą mierzalne i będą pokazywały czy poziom bezpieczeństwa jest satysfakcjonujący (czy ryzyko jest na akceptowalnym poziomie) nie jest trywialne. Wystąpienie przybliża problem zebrania informacji określenia wskaźników, które potem dadzą spójny obraz cyberbezpieczeństwa w różnych obszarach. Pokazuje cyberbezpieczeństwo w różnych kontekstach, tj. domeny bezpieczeństwa, procesy biznesowe, czy zagrożenia zewnętrzne. W trakcie przygotowywania tzw. cyberdashboardu należy znaleźć

Dyrektor Działu Wsparcia Procesów Przyjmowania i Udostępniania Danych, ASSECO Poland S.A.

15.10–15.40

Zasada „privacy by design” jako algorytm zapisany w polityce ochrony danych

Prezentacja ma na celu ukazanie, jak w praktyczny sposób zapewniać zgodności z zasadami przetwarzania danych poprzez zapisanie i zakomunikowanie działań niezbędnych do stworzenia lub zmiany zbioru danych.

Robert Żurakowski, ABI i programista, MIKROBIT

15.50–16.20

Przerwa na kawę i herbatę. Networking.

dostawcami.

Jan Anisimowicz, Director/Head of AdaptiveGRC, C&F, ISACA Warsaw Chapter

15.50–16.20

Przerwa na kawę i herbatę. Networking.

16.20–16.50

Public SaaS (nie)bezpieczny ?

16.50–17.20

Pułapki w usługach chmurowych na przykładzie AWS

Obecnie blisko 93% firm korzysta w większym, lub mniejszym stopniu z rozwiązań chmurowych. Powszechnym stało się używanie chmury do przechowywania danych, hostowania pojedynczych aplikacji czy nawet całej infrastruktury sieciowej firmy.

Jak rzeczywistość ma się do praktyki? Porozmawiajmy o praktycznych aspektach wdrożeń rozwiązań zarządzania tożsamością i dostępem i dlaczego wiele z tych projektów nie kończy się sukcesem! A mogłoby!

16.50–17.20

Mariusz Stawowski

17.20–17.50

Enterprise Vulnerability Management – Keeping the wolf from 1000 doors!

Eoin shall discuss how (from experience) to approach enterprise fullstack vulnerability management at scale and how to maintain a secure cybersecurity posture across 1000's of systems globally and web applications on an ongoing basis. How vulnerability discovery / scanning is a small part of an wspólny wymiar dla różnych obszarów (np. zarządzania podatnościami, czy bezpieczeństwo sieciowe). Osiąga się to poprzez sprowadzenie każdego mierzalnego elementu do wymiaru ryzyka. Taki cyberdashboard staje się istotnym elementem procesu zarządzania cyberryzykami w organizacji.

Ireneusz Tarnowski, Ekspert Bezpieczeństwa Informacji, BZ WBK, ISACA Warsaw Chapter

16.20–16.50

Znaczenie świadomości użytkowników i interesariuszy dla bezpieczeństwa organizacji

W trakcie wystąpienia zostaną omówione czynniki wpływające na świadomość pracowników oraz jak świadomość wymagań bezpieczeństwa wpływa na ogólne bezpieczeństwo

16.20–16.50

Nowe wyzwania dla audytu wewnętrznego sektora publicznego, w aspekcie sprawnego przygotowania jednostki do stosowania zasad RODO po dniu 25 maja 2018r.

W trakcie wystąpienia poruszone zostaną następujące zagadnienia: - Audytor wewnętrzny jako inicjator i koordynator wdrożenia zasad RODO w JSP - Budowanie relacji pomiędzy audytem wewnętrznym , zespołem IT a Inspektorem Ochrony Danych Osobowych - Nowe aspekty systemu kontroli zarządczej JSP w aspekcie stosowania RODO po dniu 25 maja 2018r.

Krzysztof Radecki, ABI, audytor wewnętrzny CGAP®, ISACA Warsaw Chapter

16.50–17.20

Amazon Web Services reklamuje się jako dostawca wyjątkowo bezpiecznych rozwiązań. Pomimo tych zapewnień od początku istnienia usług w chmurze słyszymy o wielkich wyciekach poufnych informacji, takich jak np. dane 200 milionów uprawnionych do głosowania Amerykanów, czy dokumenty Pentagonu. Czy błąd leży po stronie dostarczanych usług, czy może winy należy doszukiwać się w braku wiedzy i doświadczenia administratorów? Jak cyberprzestępcy mogą zdobyć dostęp do naszej chmurowej infrastruktury? Czy podatności aplikacji w architekturze klasycznej niosą za sobą to samo ryzyko co tej samej aplikacji w chmurze? Na te i inne pytania znajdziesz odpowiedź podczas niniejszej prezentacji. Agenda:

- Czym jest AWS
- Omówienie modelu bezpieczeństwa usług w chmurze
- Wycieki danych w usłudze S3
- Wycieki kluczy dostępowych
- Nowe życie starych

overall enterprise vulnerability management function and how other activities and processes are also equally important in terms of orchestration and visibility of enterprise security robustness.

informacji oraz liczbę incydentów. Zostaną przedstawione doświadczenia zdobyte przez autora w Royal Bank of Scotland, a także rezultaty badań naukowych prowadzonych w tym zakresie.

Andrzej Sobczak, Oficer ds. Bezpieczeństwa i Ciągłości Działania, Royal Bank of Scotland

16.50–17.20

Podmiotowa i przedmiotowa analiza ryzyka i wpływu w ramach projektu RODO lub ISO/IEC27001

Zarządzanie ryzykiem w organizacji odbywa się często dwutorowo. Zarząd zarządza po swojemu swoimi ryzykami i IT zarządza po swojemu swoimi ryzykami. Prelekcja pokaże jak zarządzać ryzykiem w sposób zintegrowany. Podejście to jest szczególnie ważne w obszarze RODO, który wymusza zarządzanie ryzykami osoby

Środki organizacyjne w RODO, a cyfrowa demencja

W trakcie wykładu zostaną zaprezentowane środki organizacyjne wymagane przez RODO w oparciu o COBIT 5 - jak je wdrażać, testować i mierzyć. Zagadnienie nie jest trywialne, gdyż w Rozporządzeniu (RODO) brak jest konkretnych wytycznych w tym zakresie. Wprowadzane środki techniczne i organizacyjne mają służyć zapewnieniu odpowiedniego bezpieczeństwa danych osobowych. Jednak wdrażanie zabezpieczeń w firmach to proces wypracowania kompromisu pomiędzy możliwościami firmy, a wymaganiami wynikającymi z prawa i wewnętrznej polityki. Oprócz dotychczasowych ograniczeń, z jakimi borykają się organizacje przy prowadzaniu rozwiązań bezpieczeństwa pojawiło się nowe, jakim jest „cyfrowa

podatności trafiających do chmury
- Rekomendacje.

Paweł Rzepa, Starszy konsultant ds. bezpieczeństwa, Securing

17.20–17.50

Ryzyka dla ochrony danych osobowych związane z korzystaniem z międzynarodowego oprogramowania oraz rozwiązań typu cloud computing

Rozwiązania z zakresu marketingu i e-commerce sprzedawane są obecnie na całym świecie, często oparte są na rozproszonej architekturze IT i rozwiązaniach typu cloud computing. Przy użyciu tych narzędzi specjaliści ds. marketingu budują złożone bazy CRM oraz listy mailingowe liczące tysiące rekordów danych osobowych istniejących klientów

fizycznej, które mogą być wręcz rozbieżne z ryzykami organizacji.

Piotr Dzwonkowski, API, ISACA Warsaw Chapter, ISSA Polska

17.20–17.50

Trudy i znoje pracy ABI w placówkach oświatowych

Uczestnicy dowiedzą się o realiach pracy ABI i ASI w placówkach oświatowych na przykładzie zabrskich i gliwickich szkół i przedszkoli. O tym, jak czasami trudno przyłożyć korporacyjną miarę do realiów szkoły publicznej.

Przemysław Adam Śmiejek, Informatyk, ZSO5 w Zabrzu

demencja". Problem jest często nieuświadomiony, gdyż towarzyszy naszemu społeczeństwu od kilku lat. Co to jest, jak do niego podejść, jak sobie z nim poradzić – na te pytania postaram się odpowiedzieć w czasie wykładu.

Małgorzata Mazurkiewicz, Główny Audytor Wewnętrzny, Zespół Audytu Informatycznego, Bank Pekao, ISACA Warsaw Chapter

17.20–17.50

Ochrona Danych – z punktu widzenia Procesora

Pokazanie roli i odpowiedzialności Procesora (partnera, dostawcy, vednora, outsourcera) w procesach przetwarzania danych i ochronie danych - Na co zwrać uwagę - Czy można outsurcować odpowiedzialność - Co Procesorzy muszą, co powinni a czego nie zrobią - Co mówią normy i dobre oraz potencjalnych klientów. Ponadto tworzą kampanie reklamowe oparte na danych osobowych pozyskiwanych z mediów społecznościowych oraz wykorzystują profilowanie klientów. Niejednokrotnie wiąże się to z powiązaniem firmowych komputerów i urządzeń mobilnych z aplikacjami stworzonymi w krajach, w których nie ma kompleksowych regulacji dot. ochrony danych osobowych. Powyższa praktyka biznesowa powoduje, że działy e-commerce i marketingu mogą stanowić najsłabsze ogniwo firmy w rozumieniu RODO i narażać ją na odpowiedzialność dot. braku zapewnienia odpowiedniego poziomu ochrony danych osobowych. Podczas prezentacji zostaną przedstawione praktyczne przykłady sytuacji, w których zachodzi ryzyko naruszenia wymogów RODO w marketingu i e-commerce z punktu widzenia bezpieczeństwa IT firmy.

Joanna Mamczur,

praktyki, co mówi GDPR - Punkt widzenia Procesora, który dostarcza usługi przetwarzania danych do ponad 8.000 klientów w całej Europie i sam używa ponad 200 pod-procesorów.

Mirosław Błaszczak, Manager ICT, ISACA Warsaw Chapter

Adwokat

2 dzień konferencji - 16 marca 2018

09.00–09.30

What does Brexit mean for cybersecurity professionals

Following soon after GDPR, Brexit could be the Next Big Thing. Do you know how many people and organisations in your area may be affected by Brexit? How can IT professionals help organisations through Brexit? How can you benefit [and also help make IT good for society]? Come to this event to learn more...

Dalim Basu, Events Director, ISACA London Chapter

09.30–09.50

Wystąpienie Partnera

10.00–10.20

Firewalle następnej generacji - wiecej niż ochrona przedsiębiorstwa

W miarę ekspansji protokołu IP na obszary wykraczające poza sieci przedsiębiorstw pojawiła się potrzeba kontroli ruchu w strukturach przemysłowych oraz operatorów telekomunikacyjnych. Od dzisiejszych NGFW wymaga się nie tylko rozpoznawania i zabezpieczania aplikacji obecnych w internecie czy w sieciach określanych jako "enterprise", ale także aktywnej ochrony protokołów sterujących procesami produkcyjnymi oraz przepływem danych pomiędzy ISP. Prezentacja ma na celu przedstawienie zagadnień bezpieczeństwa

w sieciach przemysłowych ICS/SCADA oraz sieciach operatorskich wykorzystujących protokół GTP.

Robert Dąbrowski, SE Manager, Fortinet

10.20–10.40

Infradata

10.40–11.00

Exatel

11.00–11.30

Przerwa na kawę i herbatę. Networking.

11.30–12.00

Rola NASK i NC Cyber w świetle projektu ustawy o KSC

Podczas prezentacji pokazana zostanie rola i zadania jakie adresowane są Państwowemu Instytutowi Badawczemu NASK i działającemu w jego ramach Narodowemu Centrum Cyberbezpieczeństwa w świetle projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa. Podczas prezentacji wyjaśnione zostanie także znaczenie systemu Partnerstwa Publiczno-Prywatnego jako niezbędnego mechanizmu współpracy na rzecz podnoszenia bezpieczeństwa cybernetycznego usług firm i instytucji oraz obywateli jako użytkowników końcowych tych usług.

Juliusz Brzostek, Dyrektor Narodowego Centrum Cyberbezpieczeństwa, NASK

12.00–12.20

Innowacje w zarządzaniu bezpieczeństwem: szanse czy ryzyko?

Stosowanie sprawdzonych rozwiązań z zakresu bezpieczeństwa informatycznego podnosi bezpieczeństwo do pewnego momentu. Dokładanie kolejnych rozwiązań może już nie zwiększać bezpieczeństwa w sposób istotny. Czy rozwiązania innowacyjne mogą zmienić tę sytuację? Czy branża cyberbezpieczeństwa powinna inwestować w rozwiązania innowacyjne (domyślnie: niesprawdzone)? Czy raczej nie powinna ponosić ryzyka i konsekwentnie inwestować w rozwiązania sprawdzone, także przez hakerów?

Wdrożenie jakiego typu innowacyjnych rozwiązań dla cyberbezpieczeństwa warto rozważyć?

- Modyfikowanie i ulepszanie procesów bezpieczeństwa czyli cykl Deminga dla funkcjonalności aplikacji
- Automatyzacja procesów związanych z bezpieczeństwem: skoro coraz więcej ataków jest automatycznych, to odpowiedź i remediacja też powinna być automatyczna.
- Tworzenie zintegrowanych systemów bezpieczeństwa

Jakub Jagielak, Security Business Development Manager, Atende

12.20–12.40

Symantec

12.40–13.10

Bezpieczeństwo API REST - 20 przykładów z życia wziętych

Michał Sajdak, konsultant d/s bezpieczeństwa IT, Redaktor serwisu Sekurak, Securitum, Sekurak

13.10–14.00

LUNCH

FORENSIC

14.00–14.30

Beata Legowicz

14.30–15.00

Podróż przez pole minowe - jak wdrożyć w organizacji zarządzanie tożsamością i przeżyć.

MGM-2

14.00–14.30

Odzyskiwanie danych - fakty i mity

W trakcie wystąpienia omówione zostaną najczęściej spotykane fakty i mity dotyczące praktycznych aspektów informatyki śledczej. Prelegent podzieli się swoimi spostrzeżeniami z

AUDYT-2

14.00–14.30

Za mali na bezpieczeństwo? Rzecz o sektorze SMB ...

14.30–16.30

WARSZTAT - Zastosowanie metodologii PIA opracowanej

MOBILE THREATS

14.00–14.30

Zagrożenia w sieciach mobilnych - fakty i mity. Wpływ słabości SS7 na biznes

Opublikowanie przez niemieckich researcherów w 2015 roku podatności dotyczących sieci

15.00–15.30

Przerwa na kawę i herbatę. Networking.

15.30–16.30

Techniki Live Forensics and Triage na potrzeby zespołów monitorowania i reagowania na incydenty.

Warsztaty omówią teoretycznie i praktycznie problematykę dowodów elektronicznych zbieranych na potrzeby dochodzenia wewnętrznego i procesowego. Spojrzymy na techniki Live Forensics and Triage które mają sprostać współczesnym wyzwaniom stawianym zespołom reagowania na incydenty. Omówimy przykładowe narzędzia wraz praktycznymi demonstracjami oraz zwrócimy uwagę na wieloletniej praktyki zawodowej czołowego polskiego specjalisty informatyki śledczej. Umiejętność radzenia sobie nawet z najtrudniejszymi przypadkami sprawia, iż często pełni funkcję biegłego sądowego. W prezentacji zostaną uwzględnione doświadczenia ze współpracy z organami ścigania i sprawiedliwości oraz opinie wystawiane w oparciu o normę ISO 27037:2012 w zakresie ochrony dowodów cyfrowych.

Witold Sobolewski, Biegły sądowy z zakresu informatyki śledczej, Sąd Okręgowy w Gdańsku

14.30–15.00

Zintegrowane zapewnienie obszaru zarządzania bezpieczeństwem IT. Spojrzenie na SZBI z poziomu funkcji ryzyka, compliance i audytu wewnętrzneg

przez CNIL do dokonywania oceny skutków przetwarzania dla ochrony danych osobowych.

Pokazanie zastosowania aplikacji PIA opracowanej przez CNIL i przetłumaczonej na j.polski do oceny skutków dla ochrony danych, czyli Privacy Impact Assessment - wymaganej w przypadku przetwarzania – w szczególności z użyciem nowych technologii – które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 RODO).

moblinych wywołało spore poruszenie i zwrócenie uwagi na niebezpieczeństwa, przed którymi użytkownik nie może się sam uchronić. Wokół tematu zagrożeń narosły mity zarówno możliwości atakujących jak i samych ataków. A jak jest w rzeczywistości? Czy i w jaki sposób możemy zostać zaatakowani z sieci mobilnej? Czy i jak nasz operator może nas przed tym ochronić?

14.30–15.00

Bezpieczeństwo komunikatorów mobilnych wyzwaniem dzisiejszego świata technologiczn ego

15.00–15.30

Przerwa na kawę i herbatę. Networking.

15.30–16.00

kontrowersje towarzyszące tym technikom. W części praktycznej przećwiczymy omawiane narzędzia.

o.

W ramach prezentacji zostanie przedstawiony zintegrowany model GRC (Governance – Risk – Compliance) w obszarze zarządzania bezpieczeństwem informacji. Autor wskaże, w jaki sposób różne mechanizmy zapewnienia funkcjonujące w ramach drugiej i trzeciej linii obrony organizacji wg modelu COSO wpływają na skuteczność i efektywność SZBI, a tym samym ograniczają ryzyko dla poufności, integralności i dostępności informacji. Jednocześnie wskazane zostaną zalety przedstawionego rozwiązania, jak również przeszkody w jego wdrożeniu oraz potencjalne kroki milowe w jego wdrożeniu.

15.00–15.30

Przerwa na kawę i herbatę. Networking.

Jak nie stracić 20 milionów - właściwe zabezpieczenie urządzeń mobilnych pracowników terenowych

16.00–16.30

Socjotechniki, czyli złośliwe oprogramowanie to nie wszystko?!

- CxO fraud - czyli „na prezesa”
- Fałszywa faktura
- Facebook i „moi znajomi”
- Nowe „bankowe” usługi
- „na wnuka”, „na policjanta”, „na...” - Nigeryjski przekręt

15.30–16.00

Mikołajczyk

16.00–16.30

Metodyki szacowania ryzyka przydatne w implementacji RODO

Rozporządzenie RODO w wielu miejscach wymaga, aby administratorzy oraz podmioty przetwarzające identyfikowali i szacowali ryzyka naruszenia praw lub wolności osób, których dane są przetwarzane. Szczególnie dotyczy to przypadków, kiedy należy przeprowadzić „ocenę skutków dla ochrony danych” (art 35 i 36). RODO nie wskazuje jednak żadnej konkretnej metodyki. Natomiast wytyczne „Grupy Roboczej art. 29” wskazują w tym zakresie Normy Międzynarodowe ISO 31000:2009 oraz ISO/IEC 29134:2017. Interesująca jest zwłaszcza ta ostatnia, opublikowana w

czerwcu 2017 r. i aktualnie tłumaczona na język polski w Komitecie Technicznym nr 182 PKN. Norma ta zawiera opis metodyki (podejście top-down) i kilkanaście przykładów typowych ryzyk. Prezentacja podejmie temat, przydatności metodyka przedstawionej w ISO/IEC 29135, jak również przydatności w obszarze danych osobowych Polskiej Normy PN-ISO/IEC 27005:2014, która zawiera zalecenia w zakresie zarządzania ryzykiem w bezpieczeństwie informacji. Prezentacja zawiera tezę, że z wdrożeniem RODO wiążą się jeszcze inne istotne ryzyka, które nie podejmuje żadna z ww. norm a mianowicie ryzyka związane z niewykonaniem przez Administratora praw podmiotowych o których stanowi art. 11 – do art. 22 RODO, oraz obowiązków określonych art. 33 i art. 34 (raportowanie incydentów). Prezentacja będzie zawierać propozycję metodyki obliczania tego ryzyka na podstawie kilku

parametrów związanych m.in. z ilością i kategorią danych osobowych oraz dojrzałością procesów zarządzania u administratora.

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