1 dzień konferencji

08.00–08.50

Rejestracja uczestników. Poranny poczęstunek i networking.

08.50–09.00

Rozpoczęcie konferencji

09.00–09.30

Preparing for and Assessing GDPR Compliance and Cyber Resilience

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

Machine Learning in Cyber Security - beyond buzzword

Od ponad roku Machine Learning, czy Sztuczna Inteligencja to fraza odmieniana przez wszystkie przypadki. Chcielibyśmy przedstawić konkretne zastosowanie algorytmów uczenia maszynowego w rozwiązaniu Rapid Detection Service na różnych poziomach detekcji. Opowiemy, w jaki sposób dzięki uczeniu maszynowemu

jesteśmy w stanie zaalarmować użytkowników o incydencie zazwyczaj w ciągu mniej niż 10 minut. Podczas prelekcji oddzielimy prawdę od fikcji w zakresie tego, co uczenie maszynowe jest w stanie nam dać w rozwiązaniach cyber-security czy SOC, a co jest jedynie fantazją. Poruszymy też temat możliwych wektorów ataków na algorytmy AI oraz zupełnie nowych kategorii zagrożeń i mechanizmów obrony.

Leszek Tasiemski, Vice President Rapid Detection Center R&D Radar & RDS, F-Secure

10.20–10.40

How to future proof your security strategy

The threat landscape is constantly changing. Your security perimeters have to evolve faster than your attackers. In this presentation, we look at the trends in the region, explore different kinds of threats and zoom in on the attack methodology plus their exploits and impact. Are you ready for the next attack?

Gerhard Giese, Security Specialist, Akamai Technologies

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, CISO, Niebezpiecznik.pl

12.00–12.20

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

12.20–12.40

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

12.40–13.40

LUNCH

13.40–14.00

Nowe reguły detekcji anomalii w ruchu sieciowym wraz z centralizacją logów

Analizator ruchu

13.40–14.00

91% Cyberataków rozpoczyna się od e-maila

Czy w świetle RODO najważniejszy kanał komunikacyjny nadal musi być skazany na miano najsłabszego

13.40–14.00

8 miliardów urządzeń. Jak shakować Androida?

Mimo rosnących wydatków na zabezpieczenie danych Twój telefon jest nadal

13.40–14.00

WykrywanieMalwareDGA.net

Prezentacja pokaże jak przy pomocy DNS i metod uczenia maszynowego uderzyć w najwyższy punkt piramidy bólu,

sieciowego z Flowmona już wcześniej udowodnił swoją dużą wartość w obszarze bezpieczeństwa ruchu sieciowego. Pokażemy nowy moduł Flowmon Anomaly Detection System, który stanowi uzupełnienie aplikacji o możliwość samodzielnego tworzenia reguł. Operator nie czekając na aktualizacje producenta, może zbudować regułę alarmową, którą wypracował na bazie analizy własnego ruchu sieciowego. Zobaczymy również propozycję centralizacji takich alarmów w środowisku Energy Logserver pracującego na bazie ElasticSearch.

Artur Bicki, Dyrektor Wydziału Wdrożeń Technologii IT, EMCA

ogniwa w cyberbezpieczeństwie ?
Pomimo powszechnie dostępnych na rynku rozwiązań chroniących pocztę e-mail, ataki typu phishing czy ransomware nigdy nie były tak skuteczne jak na przestrzeni ostatnich 3 lat, a zwłaszcza w 2017 roku. Poczta elektroniczna nadal pozostaje główną drogą cyberataków, a rozwiązania Secure Email Gateway w zetknięciu z nimi zdają się być nieskuteczne. Podczas wystąpienia zostaną zaprezentowane najnowsze mechanizmy ataków na pocztę e-mail, a także luki w istniejących technologiach wraz z propozycjami metod poprawiających poziom ochrony skrzynki mailowej.

Marcin Romanowski, European Sales Manager, Vade Secure

wytrychem, za pomocą którego można dostać się do ważnych danych firmowych. Pokażemy na żywo, jak łatwo jest przejąć kontrolę nad urządzeniem mobilnym, jakie dziury wykorzystują najnowsze podatności i co zrobić, by się przed nimi chronić.

Grzegorz Jędrzejczyk, Wiceprezes, FancyFon

a więc wygenerować największe koszty po stronie atakującego. Korzystając z głębokich sieci neuronowych, serwer DNS jest w stanie wykryć transmisję danych w zapytaniach DNS bądź znaleźć domeny wygenerowane przez algorytmy DGA. Zablokowanie transportu danych przez protokół DNS bądź komunikacji C2 wymusza na atakującym całkowitą zmianę techniki, konieczność wymyślenia i stworzenia nowego oprogramowania, a tym samym generuje największe koszty. Podobnie zastosowanie grafu słów do analizy słownikowych algorytmów DGA sprawia, że nie wystarczy zamiana w malware słowników używanych do tworzenia domen, gdyż serwer DNS będzie w stanie automatycznie wyodrębnić te słowniki z samych zapytań DNS, bez potrzeby manualnej inżynierii wstecznej malware.

Piotr Głaska, Senior Systems Engineer, Infoblox

14.00–14.20

Interaktywna wyszukiwarka danych bezpieczeństwa – IT Security Search firmy Quest.

Mając miliardy zdarzeń gromadzonych z różnych źródeł trudno jest wyszukać właściwe dane i zrozumieć jaki mają one związek z incydentami bezpieczeństwa. Zautomatyzowana analiza i korelacja danych jest kluczowa do ich zinterpretowania oraz weryfikacji czy doszło do naruszenia polityki bezpieczeństwa i zewnętrznych regulacji. Szybka umiejętność zlokalizowania miejsca powstania incydentu jest sprawą priorytetową aby zapobiec stratom finansowym, utracie reputacji, ciągłości działania czy też konsekwencjom wynikającym z naruszenie regulacji zewnętrznych np. RODO. IT Security Search integruje

14.00–14.20

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 Wojciechowski, Lider zespołu Cyber Security, PwC

14.00–14.20

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

14.00–14.20

Wycieki danych z data center. Spektakularne jak katastrofy lotnicze i równie rzadkie.

„U siebie najbezpieczniej” - tak twierdzą zwolennicy posiadania serwerowni w firmie. Jeśli nie chcą skorzystać z usług zewnętrznego data center, to najczęściej posługują się argumentem o wyciekach danych z takich miejsc i przytaczają najgłośniejsze przykłady. Jednak firmy coraz częściej porównują co im się bardziej opłaca - czy własna serwerownia czy zewnętrzne data center ? Zdecydowanie rzadziej podejmują się analizy, które z tych dwóch wymienionych - bardziej im się nie opłaca. Porównania zakupu własnych serwerów do wynajęcia ich w data center, są na ogół dość spłaszczone i

wiele innych rozwiązań firmy Quest w obszarach zarządzania bezpieczeństwem i zgodnością oraz administrowania systemami IT. Wykorzystując prosty i naturalny język wyszukiwania, IT Security Search znacząco pomaga administratorom i zespołom ds. bezpieczeństwa w szybkim reagowaniu na incydenty bezpieczeństwa i w analizie sądowej.

Paweł Żuchowski, Wiceprezes i Dyrektor Techniczny, Quest Dystrybucja

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

nie uwzględniają wielu istotnych czynników. Liczy się głównie cena i... strach. Zapraszamy na prelekcję, podczas której pokażemy na co zwrócić uwagę, aby dokonać bezpiecznego wyboru zewnętrznej serwerowni. Powiemy czy lepiej wybrać centrum przetwarzania danych krajowe czy zagraniczne oraz jakimi zasadami powinni kierować się ludzie pracujący w takich miejscach. Pokażemy skąd nie należy czerpać wiedzy o data center i jak przygotować się do samodzielnej wizyty w takich obiektach oraz opowiemy o najbardziej interesującym zagadnieniu poruszanym przez każdego kto odwiedza taki obiekt, mianowicie o awariach, wyciekach danych i czy to jest w ogóle bezpieczne?

Tomasz Stępski, Przewodniczący Zarządu, Polski Związek Ośrodków Przetwarzania Danych

14.20–14.50 | 14.20–14.50 | 14.20–14.50 | 14.20–14.50

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.

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

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

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

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 dostawcami.

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

kontekstach, tj. domeny bezpieczeństwa, procesy biznesowe, czy zagrożenia zewnętrzne. W trakcie przygotowywania tzw. cyberdashboardu należy znaleźć 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

14.50–15.20

Przerwa na kawę i herbatę. Networking.

15.20–15.50

IAM, IAG … good, bad and ugly: 10 rzeczy,

15.20–15.50

Znaczenie świadomości użytkowników i

15.20–15.50

Nowe wyzwania dla audytu wewnętrzneg

15.20–15.50

Public SaaS (nie)bezpieczny ?

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? 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!

Tomasz Onyszko, CTO, Predica

interesariusz y dla bezpieczeńst wa organizacji

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

o sektora publicznego, w aspekcie sprawnego przygotowani a 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

Jakie są główne ryzyka w Public SaaS? W czasie prelekcji poznamy je i jak możemy nimi zarządzać poprzez działania minimalizujące, ocenę wrażliwości danych. Postaramy się również znaleźć odpowiedź na pytanie kiedy Public SaaS może być bezpieczny a kiedy nie.

Jarosław Stawiany, Ekspert Zarządzania Organizacją Bezpieczeństwa Teleinformatyczne go, Orange Polska, ISACA Warsaw Chapter

15.50–16.20

Dylematy architekta bezpieczeństwa - jak chronić systemy krytyczne bez zakłócenia ciągłości działania?

Nowe prawo unijne, dyrektywa NIS nakłada na operatorów usług kluczowych (m.in.: z sektora energetycznego, transportowego, zdrowotnego i bankowości) oraz dostawców usług cyfrowych obowiązek ochrony świadczonych usług, zgłaszania incydentów i audytowania bezpieczeństwa. Wiele z tych usług realizowanych jest z użyciem systemów mission-critical - systemów, gdzie ciągłość działania jest najwyższym priorytetem bezpieczeństwa. Często systemy te przetwarzają dane osobowe i podlegają także wymaganiom RODO. Architekci bezpieczeństwa stają przed dużym wyzwaniem - jak

15.50–16.20

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 fizycznej, które mogą być wręcz rozbieżne z ryzykami organizacji.

Piotr Dzwonkowski, API, ISACA Warsaw Chapter, ISSA Polska

15.50–16.20

Cyfrowa demencja – jak sobie z nią radzić?

Nowe technologie to potoczne określenie całej gamy urządzeń i powiązanych z nimi usług. Z reguły mieszczą się do przeciętnej torebki kobiety i praktycznie towarzyszą przez cały dzień. Ich obecność zmienia nasze nawyki. Widzimy niewątpliwe zalety nowych technologii, ale czy dostrzegamy także wady? Okazuje się, że towarzyszy im nowe zjawisko, jakim jest „cyfrowa demencja”. Problem jest często nieuświadomiony, dostrzegalny w naszym społeczeństwie zaledwie od kilku lat, a jest przeszkodą w skutecznym wprowadzaniu zabezpieczeń w firmach. 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

15.50–16.20

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. 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

zapewnić zgodność z nowym prawem cyberbezpieczeństwa i na odpowiednim poziomie chronić systemy mission-critical bez zakłócenia ich ciągłości działania? Zakłócenie działania tych systemów może bowiem doprowadzić do poważnych, niekiedy katastrofalnych konsekwencji jak zakłócenie bezpieczeństwa energetycznego kraju, katastrofa ekologiczna, utrata zdrowia i życia ludzi czy ogromne straty finansowe i wizerunkowe. W trakcie wykładu zostaną omówione następujące zagadnienia: - Zasady projektowania i rekomendacje cyberbezpieczeństwa dla różnych systemów mission-critical wydane przez uznawane instytucje, m.in. KNF, NIST, ISA. - Jak zbudować laboratorium bezpieczeństwa i używać go w projektach zabezpieczeń systemów DC/SDN i SCADA/OT. - Jakie możliwości dla systemów mission-critical oferują nowe technologie User and Entity Behavior

Wewnętrzny, Zespół Audytu Informatycznego, Bank Pekao, ISACA Warsaw Chapter

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 podatności trafiających do chmury
- Rekomendacje.

Paweł Rzepa, Starszy konsultant ds. bezpieczeństwa, Securing

Analytics (UEBA) i Security Orchestration, Automation and Response (SOAR)

dr inż. Mariusz Stawowski, Dyrektor Techniczny, CLICO

16.20–16.50

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 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.

16.20–16.50

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

16.20–16.50

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 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

16.20–16.50

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

Eoin Keary, Founder/CEO, edgescan.com

Błaszczak, Manager ICT, ISACA Warsaw Chapter

istniejących klientów 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,
Adwokat

20.00

Spotkanie integracyjne uczestników konferencji w restauracji BOHEMIA

Restauracja BOHEMIA Al. Jana Pawła II 23

2 dzień konferencji

08.30–09.00

Rejestracja uczestników. Poranny poczęstunek i networking.

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

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

09.50–10.10

Trudny „powrót do podstaw”, czyli bezpieczeństwo IT w czasach po konsumeryzacji

Bunt użytkowników firmowych systemów IT, zwany również konsumeryzacją, spowodował, że to co wygodne i łatwo dostępne wypiera to, co kiedyś było uważane za bezpieczne.
Wykorzystanie usług dostarczanych spoza firmowych Centrów Przetwarzania Danych, poprzez operatorów chmurowych powoduje, że wykorzystanie tradycyjnych metod zabezpieczeń, w celu zapewnienia podstawowego choćby poziomu ochrony, staje się niemożliwe. Krajobraz zagrożeń także zmienia się dynamicznie i wszystko wskazuje na to, że cyber-przestępcy szybciej dostosowują się do nowych trendów niż korporacyjne działy IT. W trakcie naszej prezentacji pokażemy Państwu jak poradzić sobie z „powrotem do podstaw” i pokonaniem nowych zagrożeń a także starych problemów dzięki technologiom Trend Micro.

Edmund Asare, Inżynier systemowy i inżynier wsparcia sprzedaży, Infradata
Andrzej Sawicki, Sales Engineer, Trend Micro

10.10–10.30

Testowanie bezpieczeństwa rozwiązań IoT – proces i narzędzia

W ramach prezentacji zostanie omówione przykładowe podejście do identyfikacji podatności w rozwiązaniach IoT, oraz narzędzia, które mogą wspomóc to zadanie.

Marcin Kopeć, Konsultant ds. Cyberbezpieczeństwa/Pentester, T-Mobile Polska S.A.

10.30–11.00

Stanowisko Najwyższej Izby Kontroli do projektu ustawy o krajowym systemie cyberbezpieczeństwa w świetle kontroli NIK

Marek Bieńkowski, Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego, Najwyższa Izba Kontroli

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

Graj w ofensywie – Threat Hunting i Threat Intelligence bez tajemnic

Cyberatak może mieć dalekosiężne skutki w całej organizacji, ataki często nie są wykrywane przez tygodnie lub miesiące. Nie wystarczy reagować, kiedy można zacząć działać - każda sekunda spędzona na identyfikowaniu i reagowaniu na naruszenie to kolejna sekunda, w której atakujący może uciec z wrażliwymi danymi. Skąd brać wiedzę i umiejętności, z jakich narzędzi korzystać? Czasem najlepsze efekty dają rozwiązania otwarte i zaprojektowane samemu. Zapraszam na krótką opowieść o tym, jak można przekuć wiedzę Threat Intelligence w konkretne akcje i jak szukać zagrożeń poprze Threat Hunting. Opowiem o tym, co można zrobić własnymi, domowymi środkami a do czego przydaje się zaufany partner.

Lech Lachowicz, Sales Engineering Manager, 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

14.00–14.30

Najważniejsze trendy i zjawiska w rozwoju cyberzagrożeń

Najważniejsze trendy i zjawiska w rozwoju cyberzagrożeń – z perspektywy policji i służb. Najbardziej spektakularne ataki. Profil współczesnego cyberprzestępcy. Na co należy się przygotować w perspektywie najbliższego roku? Czarne acz realistyczne scenariusze – czy jest czego się bać?

Beata Legowicz, Wykładowca, Polsko Japońska Akademii Technik Komputerowych

14.00–14.30

Doświadczenia z wykrywaniem danych osobowych na źródłach relacyjnych i plikowych

Ważnym elementem każdego wdrożenia RODO jest identyfikacji bądź potwierdzenia wiedzy o miejscach przetwarzania danych osobowych a także wytworzenie zdolności do realizacji praw podmiotów oraz dokumentowania zgód na przetwarzanie danych. W czasie krótkiej sesji przedstawię główne elementy organizacyjne i techniczne, jakie mogą być tu pomocne i podzielę się doświadczeniami w ich wdrażaniu.

Tomasz Kazimierski,

14.00–14.30

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

Podczas wystąpienia przedstawimy problem bezpieczeństwa informacji w małych, średnich i mikro przedsiębiorstwach ... Poruszone zostaną takie zagadnienia jak bezpieczeństwo prawne, ekonomiczne i organizacyjne, cyberbezpieczeństwo oraz wpływ RODO na zmianę w podejściu do bezpieczeństwa rozpatrywanego na różnych płaszczyznach.

Klaudiusz Kosidło, Ekspert Ochrony Danych Osobowych/ Audytor ISO 27001, ISACA Warsaw Chapter

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 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?

Robert Bienias,

Consulting Solution Director, Oracle Polska, ISACA Warsaw Chapter

Telecommunication Security Specialist, Polkomtel

14.30–15.00

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

Prezentacja na temat najczęstszych zagrożeń dla projektów wdrożenia scentralizowanych systemów zarządzania tożsamością i uprawnieniami. Wdrożenie zarządzania tożsamością to nie tylko projekt informatyczny ale głównie wielkie wyzwanie organizacyjne. Systemy klasy IDM, jak mało które, dotykają wszystkich aspektów życia organizacji od bezpieczeństwa i informatyki po biznes i procesy wspomagające (np. kadrowe). Tym samym projekt zarządzania tożsamością musi pogodzić nierzadko

14.30–15.00

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

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,

14.30–15.00

WARSZTAT - Zastosowanie metodologii PIA opracowanej 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

14.30–15.00

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

Paweł Olszar, Ekspert ds. bezpieczeństwa, ING Bank Śląski

sprzeczne cele interesariuszy. Podczas prezentacji zaprezentuję najczęstsze sytuacje mogące doprowadzić do porażki projektu i sposoby radzenia sobie z nimi, które zadziałały w rzeczywistych projektach.

Paweł Kulpa, Architekt bezpieczeństwa, audytor, Qumak SA, ISACA Warsaw Chapter

integralności i dostępności informacji. Jednocześnie wskazane zostaną zalety przedstawionego rozwiązania, jak również przeszkody w jego wdrożeniu oraz potencjalne kroki milowe w jego wdrożeniu.

Sebastian Burgemejster, Prezes, IIA Polska

fizycznych (art. 35 RODO).

Uczestnicy są proszeni o przyniesienie laptopów z dostępem do Internetu

Joanna Karczewska, ISACA Warsaw Chapter

15.00–15.30

Przerwa na kawę i herbatę. Networking.

15.30–16.00

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

Warsztaty omówią teoretycznie i praktycznie problematykę dowodów elektronicznych zbieranych na potrzeby

15.30–16.00

Inżynieria Ochrony Danych Osobowych – metoda działań Inspektora ODO

Nowe prawo dotyczące ochrony danych osobowych wskazuje strategie jaką organizacje muszą realizować w procesach związanych z ochroną danych osobowych. W odróżnieniu od

15.30–16.00

II część WARSZTAT - Zastosowanie metodologii PIA opracowanej przez CNIL do dokonywania oceny skutków przetwarzania dla ochrony danych osobowych.

15.30–16.00

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

Prezentacja opowie jak w prosty sposób poprawić bezpieczeństwo pracowników terenowych jednocześnie zapewniając zgodność z obecnymi wymogami

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

Osoby, które pragną aktywnie uczestniczyć w warsztatach powinny przygotować własny laptop z systemem Windows 7/8/10 oraz dostępem do Internetu.

Krzysztof Bińkowski, Ekspert informatyki śledczej, ISSA Polska

aktualnie obowiązujących aktów prawnych nie wskazuje ono konkretnych działań operacyjnych w zakresie ochrony danych osobowych, które powinny być podejmowane przez organizacje. Takie podejście stawia wiele niewiadomych przed Inspektorami Ochrony Danych Osobowych, którzy będą pełnić kluczową rolę w procesach związanych z przetwarzaniem danych osobowych. Biorąc pod uwagę złożoność i interdyscyplinarność procesów związanych z ochroną danych osobowych oraz fakt, że przeważająca część danych jest przetwarzana z wykorzystaniem technologii i narzędzi informatycznych w trakcie prelekcji przedstawiona zostanie koncepcja wykorzystania wiedzy i doświadczeń inżynierskich w procesie ochrony danych osobowych (Inżynieria Ochrony Danych Osobowych) jako jednej z metod działań Inspektora ODO.

Tomasz Mikołajczyk, Inżynier

prawnymi.

Kamil Pakalski, ROW IT Security Specialist/ABI, Optima

oprogramowania, konsultant ISO 27001.

16.00–16.30

II część WARSZTAT: Techniki Live Forensics and Triage na potrzeby zespołów monitorowania i reagowania na incydenty.

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

16.00–16.30

III część WARSZTAT - Zastosowanie metodologii PIA opracowanej przez CNIL do dokonywania oceny skutków przetwarzania dla ochrony danych osobowych.

16.00–16.30

Bezpieczeństwo komunikatorów mobilnych wyzwaniem dzisiejszego świata technologicznego

Analiza potrzeb i rozwiązań w zakresie bezpieczeństwa szyfrowanych komunikatorów mobilnych. W dzisiejszym świecie, komunikatory mobilne zainstalowane są na większości używanych na smartfonów. Większość z rozwiązań posiada zaimplementowane mechanizmy szyfrowania prowadzonej komunikacji, zarówno głosowej, jak i tekstowej. Poczucie bezpieczeństwa, które daje przykrycie kryptograficzne komunikacji powoduje, iż są one coraz częściej wykorzystywane nie tylko przez użytkowników

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

indywidualnych, biznes, ale także przez organizacje przestępcze i terrorystyczne. Czy istnieje zatem sposób na złamanie tak prowadzonej komunikacji i przejęcie jej treści? Czy użytkownicy mogą zdać się jedynie na szyfrowanie? Czy wymagane są dodatkowe środki ostrożności?

Kamil Kaczyński, Asystent naukowo-dydaktycznego, Instytut Matematyki i Kryptologii Wydział Cybernetyki Wojskowa Akademia Techniczna

danych osobowych oraz dojrzałością procesów zarządzania u administratora.

dr inż. Janusz Cendrowski, Kierownik Produktu, Asseco Data Systems, ISACA Warsaw Chapter

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