FORUM CYBERCRIME 2018

RZECZPOSPOLITA KONFERENCJE

20–21 MARCA
WARSZAWA

HOT TOPICS

Ransomware • Phishing
WannaCry • Petya/NotPetya • Kill Chain
Red team • Odzyskiwanie danych • Audyt IT
Automatyka przemysłowa • Systemy SCADA
RODO • NIS • Security Operations Center
Internet of Things • Reverse engineering
Data leak prevention • CERT
Współpraca z organami ścigania
Ataki socjotechniczne

INSPIRUJĄCE WYSTĄPIENIA

DOŚWIADCZONYCH MANAGERÓW Z RÓŻNYCH BRANŻ

CASE STUDIES

POŚWIĘCONE ZAPOBIEGANIU ROZMAITYM FORMOM CYBERATAKÓW

SESJE WSPÓLNE I RÓWNOLEGŁE

WYBIERZ WŁASNĄ ŚCIEŻKĘ UDZIAŁU!

GOŚĆ SPECJALNY

©Deborah Copaken Kogan

Julia Angwin
ekspertka ds. cyberbezpieczeństwa,
autorka książki
„Społeczeństwo nadzorowane”

WŚRÓD PRELEGENTÓW PRZEDSTAWICIELE M.IN.:

Currency One | Deloitte | EY | GAZ System | ING Tech Poland | ISACA
NASK | Open Life TU Życie | Orange | Polskie Sieci Elektroenergetyczne
Prokuratura Krajowa | PwC | SmartRecruiters | Urząd Dozoru Technicznego

RZECZPOSPOLITA KONFERENCJE | FORUM CYBERCRIME 2018

JUŻ DZIŚ ZAREJESTRUJ SIĘ NA FORUM CYBERCRIME 2018!

Spotkanie jest odpowiedzią na potrzeby praktyków – przyjdź i zdobądź obiektywną i merytoryczną wiedzę! Kompleksowa formuła wydarzenia pozwoli Ci w pełni dostosować program do Twoich potrzeb!

SESJE WSPÓLNE to szerokie spojrzenie na współczesne pole walki biznesu z cyberprzestępcami, przegląd najważniejszych ataków ostatnich miesięcy, omówienie krok po kroku postępowania przestępców planujących atak, ale też holistyczne spojrzenie na implementację polityki cyberbezpieczeństwa w strategię biznesu. To także temat RODO, który dotyczy każdej firmy, również w obszarze cyberbezpieczeństwa, oraz zagadnienia współpracy z organami ścigania!

SESJE RÓWNOLEGŁE pozwolą Ci wybrać te tematy, które są Tobie najbliższe zależnie od pełnionych funkcji. Każdy znajdzie wśród nich coś dla siebie! Każda prelekcja to potężna dawka wiedzy na konkretnych przykładach!

ANALIZA CASE STUDIES to najbardziej praktyczny sposób na prezentację zaawansowanych zagadnień z obszaru.

Bogactwo treści gwarantuje obecność prelegentów – doświadczonych ekspertów z różnych branż!

Spotkajmy się na
FORUM CYBERCRIME 2018!

Tomasz Jakubiak

T. Jakubiak

Project Manager „Rzeczpospolita”

PATRON ZAUFANA TRZECIA STRONA.PL

Cybercrime2018.rp.pl

PROGRAM

9:00 Rejestracja uczestników i poranna kawa

9:30

Nowe trendy, nowe ataki – co przyniósł 2017?

Adam Haertle – Redaktor Naczelny, Zaufana Trzecia Strona

- WannaCry i NotPetya – co się zmieniło i co nas czeka
- Zagrożenia ze strony łańcucha dostaw – jak wykrywać i przeciwdziałać
- Yahoo vs Equifax – nowa reakcja rynków na ataki

10:10

Podważenie status quo poprzez symulacje ataków

Marcin Ludwiszewski – Szef Zespołu Cyber i Red Team, Deloitte Polska

- Procedury, certyfikaty, duże budżety – dlaczego nie świadczą o dojrzałości zarządzania bezpieczeństwem
- Jak praktycznie zredukować cyber ryzyko, symulując ataki na organizację
- Istotne czynniki sukcesu dla podejmowania decyzji w strategii bezpieczeństwa

10:50 Przerwa networkingowa

11:20

Praktyczne aspekty współpracy z organami ścigania

prok. Tomasz Iwanowski, dział ds. Cyberprzestępczości Departamentu do Spraw Przestępczości Gospodarczej, Prokuratura Krajowa

- Gdzie szukać pomocy w przypadku wystąpienia cyberataku – do kogo składać zawiadomienie?
- Jak sformułować zawiadomienie o popełnieniu przestępstwa
- Jak zabezpieczyć zaatakowaną infrastrukturę na potrzeby dochodzenia organów ścigania
- Krótki przegląd czynów, które możemy traktować jako cyberprzestępstwa i dlaczego
- Sposoby zabezpieczenia dowodów na potrzeby Policji i Prokuratury

12:00

Metody ataków, skutki, sposoby zabezpieczenia automatyki przemysłowej przed cyberatakami

Kamil Kowalczuk – Manager, Cyber Security Team, PwC

- Jakie systemy są najchętniej atakowane przez przestępców – jak określić słabe punkty w Twojej infrastrukturze
- Jak przestępcy atakują infrastrukturę przemysłową
- Jak zabezpieczyć systemy automatyki przemysłowej przed nieuprawnionym dostępem
- Ochrona systemów SCADA w obliczu nowych zagrożeń

12:50

Przerwa na lunch i wybór sesji

13:50

Red team jako nowa forma audytu cyberbezpieczeństwa

Marcin Fronczak – IT Audit Manager, OGP GAZ-System

Paweł Zięba – Security and Audit IT/ICS Expert, OGP GAZ-System

case study

- Rola audytora IT/OT w doskonaleniu cyberbezpieczeństwa
- Red team vs testy penetracyjne
- Strategia obrony – Red team jako continous security audit

Phishing i jego formy – jakie zagrożenie stanowi dla Twojego biznesu i jak się przed nim ustrzec?

Marek Frankiewicz – Information Security Officer, SmartRecruiters

case study

- Zaawansowane techniki działania hakerów – w jaki sposób działają przestępcy aby wyłudzić od Ciebie dane
- Techniki zabezpieczeń przed atakami phishingowymi
- Analiza ataków z ostatnich miesięcy

14:30

Przerwa na zmianę sal

14:40

Ataki ransomware – jak zabezpieczyć się przed atakiem szantażystów i nie stracić wartościowych danych

Przemysław Jaroszewski – Head of CERT Polska, NASK CERT Polska

- Jak ustrzec się przed atakami – czy jest to w ogóle możliwe?
- Płacić czy nie? Jak postępować w sytuacji zaszyfrowania dysków w organizacji przez przestępców
- Sposoby odzyskania danych po ataku – dostępne techniki i narzędzia

Data leak prevention – jak zabezpieczyć się przed niekontrolowanym wyciekiem danych

Grzegorz Fitta – Dyrektor Departamentu Bezpieczeństwa, Open Life TU Życie

case study

- Stosowane techniki w zakresie Data Leak Prevention
- Realizowane procesy i polityki ochrony
- Pokaz działania systemu na żywo

15:20

Przerwa na zmianę sal

15:30

Internet of Things – nowy cel ataków cyberprzestępców

Piotr Ciepiela – Associate Partner, OT/IoT Security & Critical Infrastructure Leader, EY

- Ewolucja Internetu Rzeczy (IoT) – jak zbudowano ekosystem pełen podatności
- Problematyka bezpieczeństwa IoT – powody i skutki dla infrastruktury krytycznej (...i prywatności)
- Przykłady cyberataków wykorzystujących infrastrukturę IoT
- Dobre praktyki rozwoju środowisk IoT

Twój klient a cyberzagrożenia – jak chronić się przed atakiem i minimalizować jego skutki

Tomasz Matuła – Dyrektor Infrastruktury ICT i Cyberbezpieczeństwa, Orange

case study

- Czy naprawdę jest czego się obawiać?
- Czy użytkownik ochroni się sam?
- Jak chronić się przed cyberzagrożeniami w praktyce?
- W jaki sposób informować o możliwych zagrożeniach i nowych atakach – najlepsze praktyki

---

16:20

Zakończenie pierwszego dnia Forum

9:00 Rejestracja uczestników i poranna kawa

9:30

Przypadki wykorzystania Internetu jako narzędzia do popełnienia przestępstwa case study

Artur Piechocki – radca prawny, założyciel kancelarii APlaw

- Sposób działania międzynarodowych grup przestępczych z wykorzystaniem Internetu
- Doprowadzenie, przy pomocy Internetu, do niekorzystnego rozporządzenia mieniem
- Ściganie przestępstw popełnionych z użyciem Internetu

10:15

Prywatność dobrem luksusowym XXI wieku. Najczęstsze sposoby naruszania prywatności przez podmioty gospodarcze. Wyłaniający się rynek „przywracania prywatności".

Julia Angwin – ekspertka ds. cyberbezpieczeństwa, autorka książki „Społeczeństwo nadzorowane"

prelekcja w języku angielskim*

10:55 Przerwa networkingowa

11:10

Cyberbezpieczeństwo a RODO – razem czy osobno, czyli jak nowe rozporządzenie UE wpłynie na kwestie bezpieczeństwa przedsiębiorstw

Joanna Karczewska – Członek Zarządu, ISACA Warszawa

- Kluczowe wyzwania dla administratorów danych
- Co oznacza bezpieczeństwo „state of the art"?
- Czy organ nadzoru pomoże?

*organizator nie zapewnia tłumaczenia

11:50 Przerwa na kawę i wybór sesji równoległych

12:00

Jak wdrożenie Dyrektywy ds. Bezpieczeństwa Sieci i Informacji (NIS) wpłynie na funkcjonowanie zakładów przemysłowych

Michał Łoniewski – Specjalista, Departament Innowacji i Rozwoju, Urząd Dozoru Technicznego

- Dyrektywa NIS – główne założenia i kogo będzie dotyczyło wdrożenie?
- Jak wejście w życie przepisów Dyrektywy wpłynie na zarządzanie bezpieczeństwem w zakładach przemysłowych
- Przepisy amerykańskie i europejskie dotyczące cyberbezpieczeństwa przemysłowych systemów sterowania ICS
- Rodzaje systemów ICS, branże, narażone elementy systemów automatyki
- Audyt cyberbezpieczeństwa zakładu, analiza ryzyka i podatności przemysłowych systemów sterowania

Jak się przygotować, aby po ewentualnym incydencie sprawnie odzyskać dane i przywrócić działanie systemów?

Maciej Kołodziej – Specjalista Informatyki Śledczej, E-detektywi

- Jakich narzędzi i rozwiązań użyć do wykonywania kopii danych (backup vs archiwum)?
- Jak sprawnie przywrócić organizację do prawidłowego funkcjonowania po ataku na jej infrastrukturę teleinformatyczną?
- Jak, w świetle przepisów i dobrych praktyk, pogodzić retencję, dostępność danych, ciągłość działania, backupy i archiwa?

12:40 Przerwa na lunch i zmianę sal

13:25

Pracownik – najsłabsze ogniwo w Twoim systemie bezpieczeństwa organizacji

Maciej Pawlak – Chief Information Security Officer, Currency One

case study

- Budowanie świadomości zagrożeń, ich rodzaju i wpływu na funkcjonowanie biznesu
- Jak stworzyć odpowiedni system identyfikacji oraz wyceny zagrożeń i podatności
- Jak rozmawiać z managementem, aby pokazać skalę zagrożenia
- Dobre praktyki edukacji pracowników w zakresie cyberzagrożeń
- Jak komunikować incydenty bezpieczeństwa w organizacji

Działania CERTu w następstwie wzrostu cyberzagrożeń na przykładzie sektora energetycznego

Jarosław Sordyl – Zastępca Dyrektora ds. Cyberbezpieczeństwa, Szef CERT, PSE

case study

- Aktualne zagrożenia dla systemów w sektorze energetycznym
- Rola i działania CERTu
- Współpraca jako jeden z podstawowych elementów zapewnienia bezpieczeństwa IT
- Akredytacja i certyfikacja rozwiązań bezpieczeństwa IT/OT – konieczność czy dobre praktyki

14:05 Przerwa na zmianę sal

14:15

Jak zabezpieczyć się przed atakami nieznanego typu

Krzysztof Cudak – IT Security Chapter Lead, ING Tech Poland

case study

- Narzędzia i metody wykrywania ataków nieznanego typu
- Analiza dotychczasowych ataków a predykcja możliwych scenariuszy
- Jakie sensowne usługi IT Security zaktywizować w organizacji
- Reverse engineering i narzędzia open source vs realne potrzeby biznesowe

Dobre praktyki zarządzania bezpieczeństwem informatycznym w organizacji

Kamil Kiliński – Security Expert

case study

- Kryteria optymalizacji bezpieczeństwa a TCO (Total Cost of Ownership)
- Cykl bezpieczeństwa – czym jest i jak go wdrożyć w organizacji?
- Monitorowanie, audyty systemów – w jaki sposób je przeprowadzać

15:05 Zakończenie Forum i wręczenie certyfikatów potwierdzających udział

PRELEGENCI

©Deborah Copaken Kogan

Julia Angwin – ekspertka ds. cyberbezpieczeństwa, autorka książki „Społeczeństwo nadzorowane”

Amerykańska dziennikarka śledcza. Od ponad 10 lat specjalizuje się w tematyce cyberprzestrzeni – w szczególności bada zagadnienia związane z bezpieczeństwem, anonimowością i prywatnością w sieci, a także wpływ nowoczesnych technologii na tkankę społeczną. Laureatka Nagrody Pulitzera (2003). Przez wiele lat związana z dziennikiem „The Wall Street Journal". Obecnie pracuje dla portalu dziennikarstwa obywatelskiego ProPublica (www.propublica.org). Z wykształcenia matematyk. Mieszka w Nowym Jorku. Autorka książki „Społeczeństwo nadzorowane” (wyd. pol. Kurhaus).

Piotr Ciepiela – Associate Partner, OT/IoT Security & Critical Infrastructure Leader, EY

Jest współtwórcą praktyki OT (Operational Technology) oraz IoT w EY. Lider doradztwa z zakresu bezpieczeństwa infrastruktury krytycznej i systemów automatyki przemysłowej na region EMEIA (99 krajów). Prowadził liczne projekty na terenie Stanów Zjednoczonych, Europy oraz obszaru Bliskiego Wschodu. Uczestniczy w tworzeniu międzynarodowych standardów dotyczących Bezpieczeństwa systemów przemysłowych (m.in. ISA oraz NIST). Współautor książki dotyczącej Infrastruktury Krytycznej oraz licznych artykuł publikowanych m.in. w Harvard Business Review. Prelegent na licznych konferencjach w Polsce i na świecie. Ekspert Polskiego Radia ds. Infrastruktury Krytycznej i bezpieczeństwa Cyberprzestrzeni.

Krzysztof Cudak – IT Security Chapter Lead, ING Tech Poland

Jest odpowiedzialny za koordynowanie, wdrażanie oraz implementację systemów aktywnego monitoringu bezpieczeństwa IT dla krytycznych aplikacji bankowych. Posiada doświadczenie we współtworzeniu usług bezpieczeństwa IT tj: Vulnerability Scanning, Technical State Compliance Monitoring, IT Infrastructure Active Monitoring. Wieloletni konsultant IT w projektach prowadzonych w Polsce, USA, Holandii, Belgii, Indiach, Włoszech, Wielkiej Brytanii i Niemczech. Trener IT Security w amsterdamskiej ING IT Academy. Absolwent Informatyki Politechniki Poznańskiej, programu managerskiego ICAN Institute|Harvard Business Publishing oraz studiów MBA prowadzonych w warszawskim IPI PAN we współpracy z Utah Valley University. Stażysta w Granby Island Community Center w Plymouth (UK) oraz Information Risk Manager w ING USA. Prywatnie pasjonat raftingu oraz wspinaczki wysokogórskiej.

dr inż. Grzegorz Fitta– Dyrektor Departamentu Bezpieczeństwa, Open Life TU Życie

Absolwent AGH w Krakowie, zarządzający służbami informatycznymi w sektorze bankowym, energetycznym, edukacyjnym i ubezpieczeniowym, a także z doświadczeniem po stronie dostawców oprogramowania. W obszarze ochrony danych osobowych od 1997 r.

Marcin Fronczak – IT Audit Manager, OGP GAZ-System

Kieruje działem audytu teleinformatycznego w OGP GAZ-System S.A. Prezes Cloud Security Alliance Polska. Pierwszy w Polsce posiadacz certyfikatu i instruktor z zakresu bezpieczeństwa chmur Certified Cloud Security Knowledge (CCSK). Certyfikowany audytor systemów informatycznych oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem informacji – CISA, CIA, CRISC. Doświadczony doradca wyższej kadry zarządzającej. Przez wiele lat zarządzał bezpieczeństwem IT w sektorze finansowym. W latach 2000–2005 pracował w Deloitte, jednej z największych firm doradczych i audytorskich, gdzie w trakcie licznych projektów krajowych i międzynarodowych zdobył szeroką wiedzę i cenne doświadczenie w zakresie zarządzania ryzykiem informatycznym i operacyjnym oraz prowadzenia audytów informatycznych.

PRELEGENCI

Adam Haertle – Redaktor Naczelny, ZaufanaTrzeciaStrona.pl

Twórca i redaktor naczelny jednego z najpopularniejszych serwisów poświęconych bezpieczeństwu. Bezpiecznik z powołania i zamiłowania, zapalony prelegent i trener, bawiący i uczący słuchaczy w kraju i za granicą. Przez ostatnie kilkanaście lat odpowiadał za kwestie bezpieczeństwa informacji w UPC Polska. Dzisiaj skupia się na opisywaniu zagrożeń w świecie cyber i edukacji użytkowników.

mgr inż. Joanna Karczewska – Członek Zarządu, ISACA Warsaw Chapter

Od 40 lat w informatyce. Przeszła całą drogę zawodową od operatora do dyrektora. Pracowała w instytucjach państwowych oraz firmach polskich i zagranicznych. Od 14 lat jako certyfikowany audytor – CISA – zajmuje się badaniem systemów informatycznych zgodnie z metodyką COBIT. Specjalizuje się w audytach w jednostkach sektora finansów publicznych. Od 12 lat prowadzi szkolenia z zakresu audytu informatycznego i metodyki COBIT według autorskich programów. Wykłada na Akademii Marynarki Wojennej i Politechnice Warszawskiej. Jest aktywnym członkiem międzynarodowego stowarzyszenia ISACA – obecnie bierze udział w pracach Grupy Roboczej d/s GDPR (RODO). Uczestniczy w konsultacjach polskich aktów prawnych dotyczących ochrony danych osobowych, bezpieczeństwa informacji i cyberbezpieczeństwa.

Maciej Kołodziej – Specjalista Informatyki Śledczej, E-detektywi

Wiceprezes Stowarzyszenia Administratorów Bezpieczeństwa Informacji. Wykładowca, doradca, specjalista informatyki śledczej FHU MatSoft i e-Detektywi.pl. ABI m.in. w Związku Pracodawców Branży Internetowej IAB Polska. Ekspert i konsultant ds. ochrony danych osobowych, bezpieczeństwa informacji, informatyki śledczej i systemów IT oraz audytor wiodący i wykładowca w zakresie norm ISO/EIC 27000. Uczestniczył w wielu branżowych projektach szkoleniowych dla instytucji rządowych, sektora publicznego, edukacji, bankowości, telekomunikacji oraz przedsiębiorstw branży e-commerce i nowych technologii. Autor publikacji związanych z ochroną danych osobowych. Wykładowca w Instytucie Nauk Prawnych PAN, Wyższej Szkole Bankowej w Poznaniu oraz Wyższej Szkole Ekonomii i Informatyki w Krakowie. Wykładowca stowarzyszony Wyższej Szkoły Policji w Szczytnie. Członek grup problemowych, działających przy Ministerstwie Administracji i Cyfryzacji oraz ZPBI IAB Polska i Polskiej Konfederacji Pracodawców Prywatnych Lewiatan, dotyczących regulacji prawnych i przyszłości Internetu, reklamy internetowej, e-commerce oraz rozwoju nowych technologii, ochrony danych osobowych oraz prywatności. Kierował Działem Technicznym w Grupie Solidex. W Grupie Onet.pl pełnił funkcje dyrektora Działu Bezpieczeństwa, CSO i ABI. Koordynował i nadzorował realizację Polityki Bezpieczeństwa Informacji w spółkach Grupy TVN. Był Administratorem Bezpieczeństwa Informacji w portalu NK.pl i Grupie Wydawniczej PWN. Uczestnik projektu wdrożenia polityki cyberbezpieczeństwa Ministerstwa Sprawiedliwości. Zajmuje się wdrożeniami regulacji dotyczących prawa ochrony danych, e-commerce oraz technologii i organizacji funkcjonowania usług społeczeństwa informacyjnego.

Kamil Kowalczuk – Manager, Cyber Security Team, PwC

Posiada ponad 10-letnie doświadczenie w obszarach architektury bezpieczeństwa IT/OT, zarządzania ryzykiem oraz ciągłością działania. Jako Ekspert ds. bezpieczeństwa OT wspiera Rządowe Centrum Bezpieczeństwa w obszarze automatyki przemysłowej. Opracowywał procesy bezpieczeństwa zarówno dla środowiska IT, jak i systemów kontroli przemysłowej (SCADA, DCS). Od lat związany z sektorem energetycznym, głównie w kontekście bezpieczeństwa systemów sterowania i nadzoru – SCADA, czy Infrastruktury Krytycznej. Zdobył doświadczenie pracując w Spółkach energetycznych (Gaz-System, PKP Energetyka, PGE). Ekspert ds. bezpieczeństwa automatyki przemysłowej, między innymi jako Dyrektor Projektu bezpieczeństwa Operation Technology w GK PGE prowadził przeglądy dojrzałości OT dla Spółek z Grupy. Projektował środowisko testowe oraz scenariusze ataku na potrzeby ćwiczeń Cyber-EXE 2012 w sektorze energetycznym – projekt realizowany pod auspicjami ENISA oraz Rządowego Centrum Bezpieczeństwa. Pełnił role wiodące w projektach wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z ISO 27001, Ciągłości działania w oparciu o ISO 22301 oraz brał udział w wielu projektacg technologicznych w Spółkach energetycznych i gazowych. Posiada certyfikaty: Certified Ethical Hacker (CEH), Certyfikat Network Defense Architect (CNDA), Audytor Wiodący ISO 27001, Generalny Inżynier Bezpieczeństwa ISecMan, ITIL Foundation Certificate, Prince2 Foundation Certyficate, Microsoft Certificate Profesional.

PRELEGENCI

Marcin Ludwiszewski – Szef Zespołu Cyberbezpieczeństwa i Red Team, Deloitte Polska

Cieszy się pracą i rozwojem w Deloitte testując bezpieczeństwo klientów, a także pomagając im budować strategie obronne, jak również zdolności ofensywne. Przed dołączeniem do Deloitte, pracował ze świetnymi specjalistami w zespołach cyber Royal Bank of Scotland oraz UPC. Jest byłym oficerem ABW, gdzie m.in. jako Z-ca Dyrektora Departamentu Bezpieczeństwa Teleinformatycznego wspierał działania dochodzeniowo-śledcze oraz operacyjno-rozpoznawcze w obszarze cyber – w tym, w ramach CERT.GOV.PL, NATO SC4 oraz tzw. Klubu Berneńskiego.

Michał Łoniewski – Specjalista w Wydziale Rozwoju Usług Technicznych i Metod Badawczych, Departament Innowacji i Rozwoju Urzędu Dozoru Technicznego

W 2005 roku ukończył kierunek Mechanika i Budowa Maszyn na Politechnice Warszawskiej. W latach 2006-2009 pracował w Przemysłowym Instytucie Automatyki i Pomiarów (PIAP) oraz w firmie ABB gdzie zajmował się robotyką przemysłową. Od 2010 r. pracownik UDT, gdzie obszarem jego działalności jest automatyka zabezpieczająca procesy przemysłowe (poziomy nienaruszalności bezpieczeństwa SIL, analizy zagrożeń pochodzące od systemów sterowania ICS – analizy C-HAZOP), cyberbezpieczeństwo przemysłowych systemów sterowania ICS, a także zastępowanie klasycznych badań wizualnych w inspekcji, oceną wizualną zdalną z wykorzystaniem bezzałogowych statków powietrznych – dronów.

Tomasz Matuła – Dyrektor Infrastruktury ICT i Cyberbezpieczeństwa, Orange Polska

W Orange Polska od 2004 r. (do 2013 r. Grupa Telekomunikacja Polska). Rozwinął kluczowe obszary kompetencyjne m.in.: cyberbezpieczeństwo, data center, cyfrowe środowisko pracy, cloud computing, usługi ICT. Ukończył Politechnikę Śląską, kierunek Telekomunikacja. W 2002 r. uzyskał Międzynarodowy Dyplom Managementu IFG (MBA) Francuskiego Instytutu Zarządzania, w 2009 ukończył Advanced Management Program IESE Uniwersytetu Nawarra. Zdobył tytuł Lidera Green IT 2009 dla Grupy TP, zajął I miejsce w konkursie CIO Roku 2010. W 2016 r. wyróżniony tytułem Digital Leader of the Year CIONET POLSKA. Finalista European CIO of the Year 2017.

Maciej Pawlak – Chief Information Security Officer, Currency One

Jest odpowiedzialny za rozwój, wdrażanie i zarządzanie, strategią i programem bezpieczeństwa informacji. Swoje kompetencje zdobywał jako risk manager oraz koordynator planów ciągłości dla systemów IT w jednej z największych światowych firm branży farmaceutycznej. Doświadczony specjalista z dziedziny analiz cyber nadużyć finansowych oraz przeciwdziałania praniu pieniędzy. Currency One SA to czołowa spółka na rynku wymiany walut online w Polsce. Powstała w wyniku połączenia pierwszej społecznościowej platformy wymiany walut Walutomat.pl oraz pierwszego e-kantoru Internetowykantor.pl, które umożliwiają szybką i bezpieczną wymianę walut. Currency One SA to ponad 450 tys. klientów, którzy miesięcznie wymieniają dziesiątki milionów euro, dolarów, funtów, franków i wielu innych walut.

Artur Piechocki – radca prawny, założyciel kancelarii APlaw

Radca prawny wpisany na listę Okręgowej Izby Radców Prawnych w Warszawie. Absolwent Wydziału Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz studiów podyplomowych w zakresie Prawa Własności Intelektualnej na Uniwersytecie Jagiellońskim. Specjalizuje się w prawie technologii informacyjnych oraz komunikacyjnych (ICT), fintech, ochronie danych i prywatności oraz cyberbezpieczeństwie. Posiada blisko 20-letnie doświadczenie w doradztwie prawnym na rzecz spółek polskich i międzynarodowych, głównie z sektora bankowości, finansów, IT, energetyki, telekomunikacji i mediów. Jest ekspertem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency (ENISA) w zakresie doradztwa regulacyjnego, ochrony prywatności i danych osobowych. Jest członkiem Grupy Operatorów Telekomunikacyjnych oraz Komitetu Mediów Elektronicznych przy Polskiej Izbie Informatyki i Telekomunikacji (PIIT). Przez wiele lat pracował jako Doradca ds. prawnych i polityki domenowej rejestru PL w Naukowej i Akademickiej Sieci Komputerowej (NASK). Prawnik rekomendowany przez Media Law International 2017 w dziedzinie prawa mediów, telekomunikacji i Internetu.

PRELEGENCI

Jarosław Sordyl – Zastępca Dyrektora ds. Cyberbezpieczeństwa w Departamencie Bezpieczeństwa PSE S.A., Szef CERT PSE, PSE

Wieloletni konsultant w zakresie bezpieczeństwa systemów teleinformatycznych, ekspert Informatyki Śledczej oraz eDiscovery, Lead Auditor Systemów Zarzadzania Bezpieczeństwem Informacji – ISO/IEC 27001 a także Certified Lead Penetration Tester. Wykładowca współpracujący na co dzień z instytucjami szkoleniowymi, akademickimi oraz jednostkami naukowymi w zakresie tematów związanych z bezpieczeństwem IT. Do 2014 roku członek Zarządu Europolu, przedstawiciel Polski na forum Szefów Krajowych Jednostek Europolu, członek grup roboczych Zarządu Europolu ds. IT i korporacyjnych. Produkt Menadżer oraz trener systemów informacyjnych Europolu. Były Szef Krajowej Jednostki Europolu w Biurze Międzynarodowej Współpracy Komendy Głównej Policji. Od ponad 18 lat zajmuje się problematyką bezpieczeństwa IT i cyberprzestępczości m.in. w ramach międzynarodowej współpracy organów ścigania. Posiada wiele certyfikatów związanych z bezpieczeństwem teleinformatycznym m.in.: CISSO, CDFE, CPTE, CDRE, ISO 27001 – Lead Auditor, ISO 27002 – Lead Implementer, CLPT - Certified Lead Penetration Tester, ISO 37001 Lead Implementer. Równocześnie posiadacz certyfikacji – MCP: Microsoft Certified Profession. Członek stowarzyszeń specjalistów organów ścigania „Computer Forensics – IACIS" oraz członek HTCIA – High Technology Crime Investigation Association. Ukończył Akademię Interpolu – IP Crime Investigators.

Paweł Zięba – Security and Audit IT/ICS Expert, OGP GAZ-System

Pracuje jako ekspert dziedzinowy w dziale audytu teleinformatycznego w OGP GAZ-System S.A. Certyfikowany audytor bezpieczeństwa informacji oraz ciągłości działania. W ramach wcześniejszego doświadczenia pracował przy wielu projektach w kraju i zagranicą w globalnym centrum kompetencyjnym EY Global IT\OT Advisory Service Center – jednej z największych firm doradczych i audytorskich EY(dawniej Ernst& Young). W ramach EY zdobywał doświadczenie i wiedzę w tworzeniu: standardów bezpieczeństwa OT\IT, strategii bezpieczeństwa OT\IT, przeglądów bezpieczeństwa architektury OT\IT oraz testów bezpieczeństwa OT\IT dla firm sektora infrastruktury krytycznej oraz organizacji rządowych w regionie EMEIA. Ponadto posiada ponad 10-letnie doświadczenie w ramach projektowania, implementacji i wdrażania aplikacji typu SCADA oraz systemów IT.

FORUM CYBERCRIME 2018

TERMIN I MIEJSCE WYDARZENIA: 20–21 marca 2018 r., Warszawa

- ❑ *Wyrażam zgodę na przesyłanie przez Gremi Media S.A. z siedzibą w Warszawie, ul. Prosta 51, na udostępniony przeze mnie adres poczty elektronicznej i numer telefonu informacji handlowych w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz. 1204 ze zm.). W każdym momencie przysługuje mi prawo do odwołania powyższej zgody.*
- ❑ *Wyrażam zgodę na przekazanie moich danych osobowych, w tym adresu poczty elektronicznej i telefonu spółkom powiązanym z Gremi Media S.A. z siedzibą w Warszawie, ul. Prosta 51, oraz partnerom wydarzeń na przetwarzanie ich przez w/w podmioty w celu marketingu bezpośredniego ich produktów lub usług oraz w celu przesyłania informacji handlowych w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz. 1204 ze zm.). W każdym momencie przysługuje mi prawo do odwołania powyższej zgody.*
- ❑ *Przyjmuję do wiadomości, że moje dane osobowe umieszczone zostają w bazie danych administratora danych tj. Gremi Media S.A. z siedzibą w Warszawie, ul. Prosta 51, i zgodnie z treścią art. 23 ust. 1 pkt. 3 i 5 ustawy o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z 1997 r. ze zm.) i mogą być przetwarzane w celu wykonania zawartej ze mną umowy oraz w celu marketingu bezpośredniego własnych produktów lub usług administratora danych. Jednocześnie przyjmuję do wiadomości, że podanie przeze mnie danych jest dobrowolne i przysługuje mi prawo wglądu do swoich danych, ich poprawiania oraz usunięcia z bazy.*

CENA:

2750 zł/os + 23% VAT

Cena obejmuje: udział w dwudniowym forum, materiały, lunch, przerwy kawowe.

UWAGI .....

WARUNKI ZGŁOSZENIA:

1. Warunkiem zgłoszenia udziału w usłudze edukacyjnej jest przesłanie wypełnionego formularza rejestracyjnego na stronie www.konferencje.rp.pl, e-mailem pod adres **wojciech.winiarski@rp.pl** (dalej „Zgłoszenie") oraz otrzymanie e-mailowego potwierdzenia o uczestnictwie w usłudze edukacyjnej.
2. Przesłane Uczestnikowi przez Organizatora potwierdzenie Zgłoszenia równoznaczne jest z zawarciem umowy o świadczenie usługi edukacyjnej, stanowi warunek dopuszczenia do usługi edukacyjnej oraz podstawę do obciążenia Uczestnika opłatą za usługę.
3. Wpłaty należy dokonać w terminie 14 (czternastu) dni od daty otrzymania wezwania do dokonania płatności za udział w usłudze edukacyjnej, nie później jednak niż 2 (dwa) dni przed jej rozpoczęciem. Wpłaty należy dokonać na rachunek:
   Gremi Media S.A. ul. Prosta 51, 00-838 Warszawa
   Ing Bank Śląski S.A. 14 1050 1025 1000 0090 3096 4259
   Niedokonanie wpłaty we wskazanym terminie nie jest jednoznaczne z rezygnacją Uczestnika z udziału w usłudze edukacyjnej.
4. Uczestnik jest uprawniony do rezygnacji z usługi edukacyjnej na następujących zasadach:
   a. rezygnacja winna zostać złożona na piśmie i przesłana Organizatorowi w trybie wskazanym w ust. 1;
   b. w przypadku doręczenia rezygnacji w terminie co najmniej 21 (dwudziestu jeden) dni przed jej rozpoczęciem Organizator obciąża Uczestnika opłatą administracyjną w wysokości 400 zł +23% VAT;
   c. w przypadku doręczenia rezygnacji w terminie krótszym niż 21 (dwadzieścia jeden) dni przed jej rozpoczęciem, Uczestnik zobowiązany jest do zapłaty pełnych kosztów uczestnictwa w usłudze edukacyjnej (100% ceny) wynikających z zawartej umowy.
5. W przypadku nieodwołania zgłoszenia uczestnictwa oraz niewzięcia udziału w wydarzeniu, zgłaszający Uczestnik zobowiązany jest do zapłaty pełnych kosztów uczestnictwa w usłudze edukacyjnej (100% ceny) wynikających z zawartej umowy.
6. W przypadku gdyby usługa edukacyjna nie odbyła się z powodów niezależnych od Organizatora, Uczestnikowi zostanie zaproponowany, według uznania Organizatora, udział w usłudze edukacyjnej w innym terminie lub w ciągu 14 dni roboczych zostanie zwrócona pełna kwota wpłaty.
7. Dokonanie Zgłoszenia jest równoznaczne z akceptacją niniejszych warunków oraz akceptacją warunków Regulaminu i upoważnieniem Organizatora do wystawienia faktury VAT bez składania podpisu przez Uczestnika albo osobę upoważnioną ze strony zgłaszającego Uczestnika.
8. Organizator zastrzega sobie prawo do wprowadzania zmian dot. programu, prelegentów oraz do odwołania wydarzenia.

Nazwa Firmy/Osoba fizyczna:

.....

NIP: .....

ulica, nr domu, nr lokalu:

.....

Miejscowość/kod pocztowy:

.....

Telefon: .....

Faks: .....

e-mail: .....

DANE UCZESTNIKA/UCZESTNIKÓW:

Imię i nazwisko: .....

Stanowisko: .....

e-mail: .....

Telefon: .....

Imię i nazwisko: .....

Stanowisko: .....

e-mail: .....

Telefon: .....

miejscowość, data i podpis
pieczątka firmy