

Pierwszy dzień konferencji

08.00-08.50

Rejestracja uczestników

08.50-09.00

Rozpoczęcie konferencji

09.00-09.40

KEYNOTE SPEECH: How to hack a Country

David Jacoby, Senior Security Researcher, Kaspersky Lab

09.40-10.05

Moja sieć jest bezpieczna i pracuje wydajnie - jak być pewnym?

Robert Dąbrowski, SE Manager, Fortinet

10.05-10.25

The Real Costs of Building a Cyber Security Operations Center.

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

10.25-10.55

Kick them out and keep them out. Proces naprawczy w odpowiedzi na zaawansowane ataki.

Adrian Pisarczyk, Konsultant, FireEye

10.55-11.20

Przerwa kawowa i networking

11.20-12.00

Obowiązkowe elementy strategii cyberbezpieczeństwa. Jakie zasoby musi posiadać organizator cyberstrategii.

Borys Iwaszko, Dyrektor Biura Bezpieczeństwa Cybernetycznego, Służba Kontrwywiadu Wojskowego

12.00-12.20

The Gamification of Targeted Attacks: Understanding Behaviour and Intent

Carl Leonard, Principal Security Analyst, Security Labs Forcepoint

12.20-13.00

Ochrona cyberprzestrzeni RP w świetle kontroli Najwyższej Izby Kontroli.

- Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP oraz
- Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych.

Zaprezentowane zostaną także informacje dot. realizacji wniosków pokontrolnych przez podmioty objęte ww. kontrolami i w tym kontekście zostanie przeanalizowany aktualny stan ich realizacji oraz planowane działania.

Tomasz Sordyl, Wicedyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego, NIK

13.00-13.10

Rozstrzygnięcie konkursu Security Excellence

13.10-14.00

Lunch dla uczestników konferencji

Techniczne aspekty bezpieczeństwa informacji

14.00-14.40

Aplikacje mobilne vs Malware

- SMS Premium
- Adware
- Aplikacje szpiegujące
- Botnet
- Ransomwar
- Złośliwe oprogramowanie dedykowane na aplikacje finansowe
- Złośliwe oprogramowania odblokowujące uprawnienia systemowe

Na koniec, zastanowimy się w jaki sposób użytkownicy oraz programiści aplikacji mobilnych mogą ograniczyć ryzyko związane ze złośliwym oprogramowaniem.

Łukasz Bobrek, Specjalista ds. bezpieczeństwa IT, SecuRing

Zarządzanie bezpieczeństwem informacji

14.00-14.40

Jak pływać w basenie pełnym rekinów - rzecz o cyberbezpieczeństwie z perspektywy użytkownika końcowego

- Socjotechniki
- Propagacja malware
- Przejęcie kontroli nad urządzeniem końcowym
- Skutki przejęcia - działania w fazie poeksploatacyjnej

Modus operandi ataków przejęcia tożsamości i password harvesting:

- Klonowanie stron WWW
- Przekierowania
- Socjotechniki
- JAK SIĘ NIE DAĆ?

Główna część to pokaz na żywo.

Michał Brandt, CSO, Ekspert ds. bezpieczeństwa informacji i systemów informatycznych, Raiffeisen Polbank
Janusz Nawrat, Dyrektor Departamentu Bezpieczeństwa Informacji i Systemów Informatycznych., Raiffeisen Polbank

Audyt IT

14.00-14.40

Jak pozyskiwać, przechowywać i przetwarzać dowody cyfrowe w informatyce śledczej?

Marcin Kaczmarek, CISA, ekspert bezpieczeństwa informacji, BZ WBK

14.40-15.10

Dlaczego ransomware'y są nadal wszechobecne, jeżeli sandboxing je zatrzymuje?

Krzysztof Karbowski, Konsultant Techniczny, Quest Dystrybucja
Marcin Romanowski, European Sales Manager, Vade Secure

14.40-15.10

RODO tyka... Jak rozporządzenie UE o ochronie danych osobowych wpłynie na obszar IT i bezpieczeństwa.

- Nowe obowiązki i ograniczenia w fazach projektowania, wdrożenia i utrzymania systemów IT
- Privacy Impact Assessment, Privacy by Design, Privacy by Default

14.40-15.10

„Lepiej zapobiegać, niż leczyć.”

Paweł Żuchowski, Wiceprezes i Dyrektor Techniczny, Quest Dystrybucja

inaczej niż myślisz

- Wdrażanie systemów IT
- problem roku 2018 czy
problem na dziś?

Anna Kobyłańska, Adwokat, counsel,
PwC

Łukasz Ślęzak, Menedżer, PwC

15.10-15.50

Application security recipes for fast-paced environments

Luca Carettoni, co-founder, Doyensec

15.10-15.50

Proces Vulnerability Management w globalnym koncernie

Łukasz Stachowicz, IT Infrastructure
Security Service Manager, BSH Sprzęt
Gospodarstwa Domowego

15.10-15.50

Trzecia droga DevOps i bezpieczeństwo

Tomasz Kazimierski, Consulting Solution
Director, Oracle Polska

15.50-16.10

Przerwa kawowa i networking

16.10-16.50

10 przykazań bezpiecznego programowania - OWASP Top10 Proactive Controls

Mateusz Olejarka, Starszy specjalista ds.
bezpieczeństwa IT, SecuRing

16.10-16.50

Dziurawe aplikacje, czy nieświadomi pracownicy? Czyli co hakerzy lubią najbardziej...

Michał Kurek, Dyrektor w Dziale
Zarządzania Ryzykiem Informatycznym,
EY
Aleksander Ludynia, Starszy Menedżer w
Zespole Zaawansowanych Usług
Bezpieczeństwa, EY

16.10-16.50

Odpowiedzialność karna za cyberprzestępstwa

- Jaka działalność z użyciem
sprzętu elektronicznego
podlega odpowiedzialności
karnej?
- Jak definiowane są
cyberprzestępstwa w
polskim prawie karnym?
- Jakie kary grożą za
cyberprzestępstwa?
- Jakie są praktyczne
aspekty dochodzenia
roszczeń związanych z
cyberprzestępstwem?

dr Izabela Szczygielska, Adwokat,
Wierciński Kwieciński Baehr

16.50-17.30

Bezpieczeństwo systemów sterowania automatyki przemysłowej w odniesieniu do zagrożeń natury informatycznej

- Jakie są obecnie panujące
"mity" na temat
bezpieczeństwa
SCADA/ICS,
- Jakie są możliwości
audytowania
bezpieczeństwa
środowisk, gdzie aktywne

16.50-17.30

Red teaming w Polsce.

Borys Łącki, IT Security Consultant,
Logicaltrust

16.50-17.30

Odpowiedzialność dostawcy usług IT za przypadki naruszenia cyberbezpieczeństwa

Xawery Konarski, Adwokat, Traple
Konarski Podrecki i Wspólnicy
Agnieszka Wachowska, Radca prawny,
Traple Konarski Podrecki i Wspólnicy

- metody testowania zabezpieczeń są niedopuszczalne,
- Jakże są rzeczywiste i (niestety) skuteczne techniki włamań do tych systemów,
 - Jakże są standardy i wytyczne wydane przez uznawane światowe organizacje, które można wykorzystać do wzmocnienia bezpieczeństwa systemów SCADA/ICS.

dr inż. Mariusz Stawowski, Dyrektor
Techniczny, CLICO

17.30-17.35

Zakończenie pierwszego dnia konferencji. Losowanie nagród

20.00-23.59

Spotkanie integracyjne uczestników konferencji w Restauracji Bohemia

Drugi dzień konferencji

08.30-09.00

Rejestracja uczestników niezarejestrowanych pierwszego dnia

09.00-09.30

Zabezpiecz swoją karierę

- czynniki motywujące i demotywujące pracowników i dlaczego pieniądze nie są głównym z nich,
- istotne czynniki sprawiające, że pracownicy zostają w swoich organizacjach i rosną wraz z nimi.

Pokazane zostanie:

- jak firmy poszukują kandydatów o określonych kompetencjach,
- jak kandydaci mogą się w tym procesie najlepiej odnaleźć i gdzie szukać pomocy,
- jak omawiane sytuacje zawodowe wyglądają z perspektywy pracodawcy i pracownika.

Uczestnicy będą mogli wyciągnąć praktyczne wnioski dla swojej sytuacji.
Prezentacja jest podsumowaniem doświadczeń zawodowych rekrutera i menedżera IT.

Jakub Anderwald, Delivery Director, KMD Poland
Paulina Czarkowska, IT Recruitment Expert/Lead, KMD Poland

09.30-09.50

Czy jesteś w stanie zobaczyć dzisiejsze ataki?

Maciej Iwanicki, Inżynier systemowy, F5 Networks

09.50-10.30

Как взломать выборы - Jak zhakować wybory? Podrecznik pisany cyrylicą

Adam Haertle, Kierownik ds. bezpieczeństwa informatycznego, UPC Polska, ISACA Warsaw Chapter

10.30-10.45

Śmierć firewalla - narodziny bezpieczeństwa kompleksowego

Robert Ślaski, Chief Network Consultant, Atende

10.45-11.10

Przerwa kawowa i networking

11.10-11.50

Hackowanie kamery CCTV i inne kluczowe zagadnienia w bezpieczeństwie IoT

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

11.50-12.10

Automatyzacja Security Baseline

Antoni Grzymała, Specjalista, Exatel S.A.

Tomasz Wodziński, Kierownik Security Operations Center (SOC), Exatel S.A.

12.10-12.30

Abracadabra! Jak zmienić największe zagrożenie bezpieczeństwa - użytkowników wewnątrz organizacji - w skuteczną linię obrony przed naruszeniami oraz jak utorować drogę dla GDPR/RODO?

- dwukierunkowej komunikacji w czasie rzeczywistym pomiędzy pracownikami a działem bezpieczeństwa
- możliwości uzyskania informacji zwrotnej od pracowników w celu minimalizacji naruszeń polityk bezpieczeństwa
- obniżenia kosztów związanych z wykrywaniem, zapobieganiem i śledzeniem incydentów bezpieczeństwa
- wdrożenia wewnętrznych procesów i narzędzi, gwarantujących zgodność z normami GDPR/RODO

Piotr Kawa, Kierownik Działu Monitorowania Sieci, BAKOTECH

Mark Kreymer, Regional Sales Director for Central & Eastern Europe, ObserveIT

12.30-12.50

Nowoczesny SOC - Flowmon ADS, ElasticSearch i Splunk w jednej odświeżce

Artur Bicki, Dyrektor Wydziału Wdrożeń Technologii IT, EMCA

Klaudyna Busza - Kujawska, Specjalista, Flowmon Networks

12.50-13.40

Lunch dla uczestników konferencji

Techniczne aspekty
bezpieczeństwa informacji

13.40-14.20

Zarządzanie
bezpieczeństwem
informacji

13.40-14.20

Audyt IT

13.40-14.20

Jak metodyka COBIT może

Sekrety blockchain - śledzenie kryptowalut <i>Mariusz Litwin, Analityk, EY</i>	Defragmentacja wiedzy CISO w obszarze incydentów bezpieczeństwa informacji <i>Adrian Kapczyński, Członek Zarządu, Polskie Towarzystwo Informatyczne</i>	pomóc przygotować się do wdrożenia RODO. • od czego zacząć przygotowania, • jak wyznaczyć ścieżkę dojścia oraz plan i harmonogram działań do 24 maja 2018r., • które procesy informatyczne są kluczowe, • jak wykazać się należytą starannością o dane osobowe na co dzień i w razie kontroli organu nadzorczego. Prowadząca pokaże, jak przydatne w przygotowaniach do stosowania RODO okażą się dobre praktyki i inne podpowiedzi zawarte w metodyce COBIT 5. Podczas warsztatu uczestnicy będą potrzebowali swoich laptopów do pracy. <i>Joanna Karczevska, ISACA Warsaw Chapter</i>
14.20-15.00 Techniczne szczegóły ataku „przez KNF” • Kiedy i jak wyzwalany był exploit • Co się działo dalej na komputaerze ofirary W trakcie prezentacji będzie poruszone także: • Opis typów IoC i co oznaczają • Jak przyłożyć te IoC do własnej infrastruktury (konsumować) • Jakie narzędzia (darmowe) mogą wspomagać konsumpcje <i>Tomasz Bukowski, Kierownik Zespołu Security Threat Intelligence, Bank Millennium SA</i>	14.20-15.00 Bug bounty w mojej firmie. <i>Kacper Szurek, Detection Engineer, ESET</i>	14.20-15.00 Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO. <i>Joanna Karczevska, ISACA Warsaw Chapter</i>
15.00-15.30 Przerwa kawowa i networking		
15.30-16.10	15.30-16.10	15.30-16.10

Wzbogacanie danych w procesach SOC i CERT. • Jakiek są główne problemy związane z zarządzaniem podatnościami bezpieczeństwa w dużych organizacjach. • Jak powiązać realne ryzyko biznesowe z informacjami dot. zagrożeń w systemach IT. • Jak skrócić czas od wykrycia podatności, przez identyfikację odpowiedzialności za nią, do jej usunięcia. <i>Andrzej Dalasiński, Group Leader, Vulnerability Management & Compliance Checks, Bosch Cyber Defense Center</i>	Bezpieczeństwo to żyć bezpiecznie i mieć wszystko pod kontrolą? Teza prawdziwa dla bezpieczeństwa IT, a jak to jest kiedy zostaje się CISO, CIO? <i>Robert Pławiak, Dyrektor Departamentu Informatyki, Europejski Fundusz Leasingowy</i>	Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO. <i>Joanna Karczevska, ISACA Warsaw Chapter</i>
16.10-16.50 Odpieranie ataku sieciowego i analiza powłamaniowa w praktyce. <i>dr Marek Robak, Head of IT Operations, Gemius</i>	16.10-16.50 Kiedy zaczniemy kupować antywirusy do lodówek? <i>Marcin Biernatowski, Poland Channel Services Head, Citi Handlowy</i>	16.10-16.50 Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO. <i>Joanna Karczevska, ISACA Warsaw Chapter</i>
16.50-17.00 Podsumowanie i zakończenie konferencji.		

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