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

As a security analyst we often get asked the question: “What threats and vulnerabilities do you expect us to see in the future?” This is a very interesting question but also an indication that the way we think about and discuss IT-security is fundamentally wrong. Do we really need to invest time and resources to focus on future threats when we are still vulnerable to attacks that have been discussed for over 20 years?
If you take a look at some of the major breaches we have seen in the past, the attackers did not use zero day vulnerabilities. Also if you look in the exploit kits, only very few are actually equipped with exploits taking advantage of zero day vulnerabilities. To analyze this in depth, Kaspersky researcher David Jacoby joined forces with Outpost24’s CSO Martin Jartelius, gaining access to unique statistics related to technical risk exposures from the vulnerability management vendor and performed several security audits which included both social engineering tests and penetration tests. However, everything was performed without exploiting any vulnerabilities. Hear David talk about how they were able to achieve the same powerful attacks at a targeted attack, but without any technical tools.

David Jacoby, Senior Security Researcher, Kaspersky Lab

09.40–10.05

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

Zacierająca się granica pomiędzy Network Operations Center (NOC) oraz Security Operations Center (SOC) wynika z potrzeby natychmiastowego dostępu do informacji o zagrożeniu obniżenia efektywności działania infrastruktury. Przyczyną zagrożenia może być przeciążone urządzenie sieciowe, czy też skompromitowana stacja końcowa kontrolowana przez botnet. Prezentacja przedstawia wizję Fortinet, jak poradzić sobie z wyzwaniem znalezienia źródła problemu i jego neutralizacji.

Robert Dąbrowski, SE Manager, Fortinet

10.05–10.25

The Real Costs of Building a Cyber Security Operations Center.

We have seen that in terms of security effectiveness, operational efficiency and staffing costs, the unified approach is clearly the most cost-effective way to build a SOC. It provides complete threat visibility across the operation, streamlines threat management and accelerates time to response. Deploying a unified SOC allows organizations to reduce the number of point tools being purchased, integrated and maintained. Together with lower staffing requirements, overall savings in total cost of ownership can reach up to 60% as compared to a traditional SOC approach. At the same time, a unified approach minimizes the risk of costly data breaches through better threat detection and response. Verint Threat Protection System™ is a pre-integrated, intelligence-driven platform that marks the onset of a new era in cyber security. Rather than reacting to the last attack, it lets SOC teams hone in on attacks as they happen. By orchestrating and automating intelligence across detection, forensics, investigation and response, Verint Threat Protection System™ brings the full attack storyline to analysts' fingertips, enabling better decisions and faster remediation.

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.

Jednym z najważniejszych, ale również najtrudniejszych zadań w odpowiedzi na zaawansowane ataki jest efektywne przeprowadzenie procesu naprawczego (remediation). Podczas prezentacji powiemy czym jest proces naprawczy, kiedy się zaczyna, a kiedy kończy oraz omówimy jego kolejne etapy. Opowiemy również o najczęściej popełnianych bledach, ich konsekwencjach oraz reakcji atakujących. Podzielimy się również dobrymi radami i doświadczeniami z prawdziwych incydentów.

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.

W chwili obecnej toczy się w Polsce dyskusja na temat kształtu i zawartości strategii cyberbezpieczeństwa RP. Za uzasadnione wydaje się potraktowanie tego dokumentu jako wzorca przy określaniu polityk bezpieczeństwa dla poszczególnych resortów, branży czy nawet pojedynczych jednostek organizacyjnych. W związku z tym należy dołożyć wszelkich starań żeby była to strategia oparta o rozwiązania zaczerpnięte z najlepszych światowych wzorców. Podczas prezentacji zostaną przedstawione i przeanalizowane niezbędne elementy strategii cyberbezpieczeństwa oraz zasoby, które musi posiadać organizator tej strategii. Podane przykłady będą przedstawiały modelowe rozwiązania możliwe do wykorzystania zarówno na szczeblu centralnym jak również w każdej jednostce organizacyjnej.

Borys Iwaszko, Dyrektor Biura Bezpieczeństwa Cybernetycznego, Służba Kontrwywiadu Wojskowego

12.00–12.20

The Gamification of Targeted Attacks: Understanding Behaviour and Intent

Operation Sledgehammer is the name of a recent Distributed Denial of Service (DDoS) attack that targeted organizations with political affiliations that the attacker deems out of line with a particular country's government. Forcepoint Security Labs explore the behavior and intent of a set of hackers which gamified the process. Attackers are given rewards for every ten minutes they perform DDOS attempts at a select group of political websites. Join us as we reveal 2 twists in the story during a dive deep into the Tactics, Techniques and Procedures exhibited in this novel gamification method.

Carl Leonard, Principal Security Analyst, Security Labs Forcepoint

12.20–13.00

Ochrona cyberprzestrzeni RP w świetle kontroli Najwyższej Izby Kontroli.

W prezentacji zostaną przedstawione główne ustalenia kontroli Najwyższej Izby Kontroli pt.

- 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

W ciągu kilku ostatnich lat urządzenia mobilne stały się nieodłącznym elementem naszego życia - miejscem, w którym przechowujemy ogromną liczbę prywatnych i wrażliwych danych. W trakcie prezentacji zastanowimy się czy dane przechowywane na urządzeniach mobilnych są bezpieczne i czy twórcy złośliwego oprogramowania naprawdę mogli pominąć tak duży i dynamicznie rozwijający się rynek zbytu dla swoich aplikacji?
Na to pytanie (oraz wiele innych) odpowie moja prezentacja, w której przedstawię współczesne możliwości złośliwego oprogramowania na platformy mobilne. Zaprezentowane zostaną przykłady malware'u, a także ryzyko związane z jego występowaniem na urządzeniu mobilnym.

Zarządzanie bezpieczeństwem informacji

14.00–14.40

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

Modus operandi ataków client-side:

- 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,

Audyt IT

14.00–14.40

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

- Jakie instytucje i jakich danych mogą żądać od administratorow IT ich przedstawiciele?
- Jakie obowiązki spoczywają na administratorach IT w kontekście gromadzenia i przechowywania dowodów cyfrowych?
- Co może być zaliczane do dowodów, a co może być obalone jako dowód w postępowaniach sądowych?
- Jak wygląda proces pozyskiwania dowodów cyfrowych?
- Skąd można dane pobierać, jakich można użyć środków, jakich czynności należy unikać, aby zapewnić właściwą istotność i jakość.
- Czy dane pozyskane metodą "hackingu" mogą zostać użyte w postępowaniach?

Marcin Kaczmarek, CISA, ekspert bezpieczeństwa informacji, BZ WBK

Prezentacja zawiera również demonstracje działania w praktyce złośliwego oprogramowania dla każdej z następujących grup:

- 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

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

14.40–15.10

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

W roku 2016 zaobserwowaliśmy znaczny wzrost liczby malware'ów rozsyłanych drogą mailową. Wraz z rosnącą liczbą platform typu „ransomware as a service" nadchodzący rok wróży kolejną eksplozję ataków. Po wstępnej sytuacji w

14.40–15.10

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

Ogólne rozporządzenie EU o ochronie danych osobowych (RODO) wprowadza wiele zmian, nie tylko z perspektywy prawnej, ale przede wszystkim z perspektywy IT. Zmiany dotkną zarówno wewnętrznych działów IT, jak i dostawców oprogramowania,

14.40–15.10

„Lepiej zapobiegać, niż leczyć."

Ta zasada sprawdza się nie tylko w życiu, ale dotyczy też zdrowia i bezpieczeństwa naszych systemów IT. W dobie coraz większej liczby dostępnych rozwiązań i wzrostu świadomości zagrożeń pojawiają się ważne kwestie: czy audyt natywny wystarczy? czy używany przeze mnie SIEM odpowie na wszystkie istotne pytania? jak w odpowiednim czasie złapać za rękę intruza,

2016 roku przyjrzymy się ransomware, temu jak działa oraz mechanizmom oferującym skuteczną ochronę przed tego typu atakami.

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

wykorzystuwanego do przetwarzania danych osobowych.

Podczas prezentacji zwrócimy uwagę na następujące aspekty:

- Nowe obowiązki i ograniczenia w fazach projektowania, wdrożenia i utrzymania systemów IT
- Privacy Impact Assessment, Privacy by Design, Privacy by Default inaczej niż myślisz
- Wdrażanie systemów IT - problem roku 2018 czy problem na dziś?

Anna Kobylańska, Adwokat, counsel, PwC
Łukasz Ślęzak, Menedżer, PwC

by uniemożliwić mu swobodne działanie? A gdyby tak koordynować na bieżąco informacje napływające ze wszystkich wykorzystywanych w firmie systemów zabezpieczeń i już w momencie zagrożenia automatycznie reagować usuwając wykryte luki? Pokażemy, że nie jest to tylko mrzonka, a dostępne na rynku rozwiązania można „zmusić" do wzajemnej współpracy.

Paweł Żuchowski, Wiceprezes i Dyrektor Techniczny, Quest Dystrybucja

15.10–15.50

Application security recipes for fast-paced environments

Ensuring the security of web applications in continuous delivery environments is an open challenge for many organizations. In fast-paced environments (e.g. startups, agile SDLC shops, etc.), traditional application security practices can slow continuous delivery or simply not address security at all. Instead, a new approach based on security automation and tactical security testing is required to make sure that important components are tested before going live. In this presentation,

15.10–15.50

Proces Vulnerability Management w globalnym koncernie

Proces zarządzania podatnościami staję się coraz częstszą praktyką szczególnie w większych firmach. Wiele z nich dopiero się z nim zaznajamia, niektórzy już go wdrażają, a inni... mają z nim już 9 lat doświadczenia. Będzie to historia o tym jak zbudowaliśmy taki system, skąd czerpiemy informacje do skanowania, jak korelujemy wyniki z innymi systemami, jakie stosujemy założenia (np. wektory ataku), jakie stosujemy reguły Compliancy, jak udało nam się go

15.10–15.50

Trzecia droga DevOps i bezpieczeństwo

Kontrola jakość w formie testów penetracyjnych na końcu projektu IT to nie koniecznie jest najskuteczniejszy pomysł, aby zapewnić bezpieczeństwo informacji. Identyfikacja i ukaranie winny to niekoniecznie jest najlepsza droga, aby motywować członków zespołów i użytkowników do troski o bezpieczeństwo.
To krótkie wystąpienie omawia zastosowania kultury małych kroków i narzędzi DevOps w spełnieniu postulatu „Security by Design" i „Security by

I will illustrate a few examples on how Silicon Valley-based startups approach security testing while seeking the perfect balance between compliance, security and business productivity.

Luca Carettoni, co-founder, Doyensec

zautomatyzować i wreszcie... czego się nauczyliśmy przez cały ten czas.

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

Default" w czasie projektowania, dostarczania i eksploatacji dużych systemów IT. Oparte na doświadczeniu własnym i innych.

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

Wszyscy dobrze znamy OWASP Top 10 – listę najczęściej występujących rodzajów podatności w aplikacjach webowych. Lista ta to projekt edukacyjny, który świetnie nadaje się do podnoszenia świadomości w zakresie bezpieczeństwa aplikacji, ale nie nadaje się do definiowania wymagań dla aplikacji. W tym celu powstała lista OWASP Top 10 Proactive Controls. Jest to lista technik bezpiecznego kodowania, które powinny być stosowane w każdym projekcie programistycznym. Opracowanie to może być podstawą do spisania wytycznych dotyczących tworzenia i zamawiania aplikacji w każdej instytucji, dla

16.10–16.50

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

Prezentacja będzie odpowiedzią na pytanie, czy bardziej należy dbać o świadomość pracowników w zakresie cyberzagrożeń, czy o wyeliminowanie podatności w systemach i infrastrukturze. W trakcie prezentacji omówione zostaną najciekawsze przypadki zaobserwowane podczas 15 letniej pracy prelegenta, jak również wyniki najnowszego Światowego Badania Bezpieczeństwa Informacji EY.

Michał Kurek, Dyrektor w Dziale Zarządzania Ryzykiem Informatycznym, EY
Aleksander Ludynia, Starszy Menedżer w

16.10–16.50

Odpowiedzialność karna za cyberprzestępstwa

Przedmiotem wystąpienia będzie przedstawienie zjawiska cyberprzestępstw z perspektywy polskiego prawa karnego. Omówione zostaną przepisy kodeksu karnego, które regulują zasady odpowiedzialności karnej za cyberprzestępstwa wraz z przedstawieniem praktycznych aspektów postępowania karnego i konkretnych przykładów z praktyki. Celem prelekcji będzie zapoznanie audytorium z następującymi kwestiami:

- Jaka działalność z użyciem sprzętu elektronicznego podlega odpowiedzialności karnej?
- Jak definiowane są cyberprzestępstwa w polskim prawie karnym?

której problem bezpieczeństwa aplikacji jest kluczowy. Takie proaktywne podejście do bezpieczeństwa polega na wyznaczeniu i egzekwowaniu wymagań na początku projektu a nie tylko na wykrywaniu i usuwanie podatności na jego końcu. Lista OWASP Top 10 Proactive Controls może być przydatna zarówno dla zarządzających bezpieczeństwem, dla managerów IT zlecających stworzenie nowych aplikacji, jak i dla audytorów wewnętrznych. W takcie wykładu przedstawię pokrótce problem jakim jest właściwe definiowanie założeń niefunkcjonalnych dotyczących bezpieczeństwa oraz nową, zaktualizowaną listę OWASP Top 10 Proactive Controls.

Mateusz Olejarka, Starszy specjalista ds. bezpieczeństwa IT, SecuRing

Zespole Zaawansowanych Usług Bezpieczeństwa, EY

- 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

W trakcie prelekcji uczestnicy dowiedzą się m.in.

- Jakie są obecnie panujące "mity" na temat bezpieczeństwa SCADA/ICS,

16.50–17.30

Red teaming w Polsce.

W prezentacji zostaną ukazane prawdziwe przykłady z testów penetracyjnych typu RedTeam, w których każdy sposób na kradzież informacji jest dobry. Phishing, złośliwe oprogramowanie, fałszywe domeny, przełamywanie zabezpieczeń fizycznych - to tylko niektóre aspekty poruszane podczas prelekcji. Pokażemy nasze sukcesy oraz

16.50–17.30

Odpowiedzialność dostawcy usług IT za przypadki naruszenia cyberbezpieczeństwa

W sytuacji kiedy dojdzie do naruszenia cyberbezpieczeństwa, pokrzywdzony może upatrywać jego przyczyn w niewystarczających zabezpieczeniach stosowanych przez dostawcę IT w

- Jakie są możliwości audytowania bezpieczeństwa środowisk, gdzie aktywne metody testowania zabezpieczeń są niedopuszczalne,
- Jakie są rzeczywiste i (niestety) skuteczne techniki włamań do tych systemów,
- Jakie 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

porażki, metody ataków oraz dobre praktyki ograniczające możliwość skutecznego ataku wymierzonego w zasoby firmowe.

Borys Łącki, IT Seurity Consultant, Logicaltrust

dostarczanych rozwiązaniach. Jak ustalić zakres odpowiedzialności dostawcy za cyberatak na podstawie przepisów prawa? Kiedy możliwe i skuteczne jest wyłączenie jego odpowiedzialności już w zawieranej umowie? Czy cyberatak może zostać potraktowany jako siła wyższa, która zwalnia strony z odpowiedzialności? Wystąpienie koncentruje się na odpowiedzi na powyższe pytania, w szczególności poprzez przedstawienie podstaw prawnych odpowiedzialności za naruszenie cyberbezpieczeństwa i ich możliwych modyfikacji umownych.

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

17.30–17.35

Zakończenie pierwszego dnia konferencji. Losowanie nagród

20.00–23.59

Spotkanie integracyjne uczestników konferencji w Restauracji Bohemia

Restauracja BOHEMIA
Al. Jana Pawła II 23

Drugi dzień konferencji

08.30–09.00

Rejestracja uczestników niezarejestrowanych pierwszego dnia

09.00–09.30

Zabezpiecz swoją karierę

Obserwujemy duże zainteresowanie tematem świadomego rozwoju kariery, jego planowania i wcielania w życie. Jednak jest to pojęcie różnie rozumiane i wdrażane w organizacjach.
Prezentacja na przykładzie historii pracownika działu bezpieczeństwa IT pokaże jakie mechanizmy stosuje się podczas rozwoju kariery i jak się w nich odnaleźć.

Omówione zostaną :

- 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?

Wiele z urządzeń bezpieczeństwa, które znajdują się w naszych sieciach bazuje na możliwości „zobaczenia” przychodzącego ruchu. Inwestycje, które zostały poczynione w poprzednich latach miały na celu ochronę tych sieci przed atakami. Teraz prognozuje się, że 70% ruchu z Internetu jest ruchem szyfrowanym a jego ilość dalej będzie rosła. I co teraz, gdy „zobaczenie” ruchu jest niemożliwe/trudne?

Maciej Iwanicki, Inżynier systemowy, F5 Networks

09.50–10.30

Как взломать выборы - Jak zhakować wybory? Podrecznik pisany cyrylicą

Czy można zhakować wybory w największym światowym mocarstwie? Jak dużych umiejętności technicznych może wymagać takie zadanie? Czy da się je wykonać nie pozostawiając za sobą śladów? Czy możemy spodziewać się kolejnych, podobnych kampanii? Na te i inne pytania spróbujemy odpowiedzieć śledząc historię tego, jak podejście do bezpieczeństwa informacji mogło zmienić losy świata.

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

10.30–10.45

Śmierć firewalla - narodziny bezpieczeństwa kompleksowego

Wiele organizacji wdrażając firewall na styku z Internetem czuje się zabezpieczona przed zagrożeniami danych wewnętrznych płynącymi ze świata. Podczas prezentacji chciałbym zwrócić uwagę, jak złudne poczucie bezpieczeństwa oferuje klasyczny firewall oraz pokazać różne wektory ataków mogące skutkować przejęciem danych w hipotetycznych przedsiębiorstwach.

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

W trakcie prezentacji zaprezentowane zostaną wybrane podatności zlokalizowane w ostatnim roku w świecie IoT.
W szczególności, pokazane zostanie jak za pomocą jednego, odpowiednio spreparowanego adresu URL można
przejąć bez uwierzytelnienia kamerę jednego ze znanych producentów. Atak na kamerę CCTV zrealizowany będzie na żywo.

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

11.50–12.10

Automatyzacja Security Baseline

Podczas prelekcji omówione zostaną podstawowe zagadnienia dotyczące standardów bazowej polityki bezpieczeństwa („security baseline"), w szczególności wytyczne CIS (Center for Internet Security). W dalszej części przedstawione zostaną problemy związane z implementacją wytycznych „security baseline" oraz systemy zarządzania konfiguracją, które umożliwiają automatyzację tych procesów w rozmaitych scenariuszach i w kontekście różnych platform sprzętowych. Zaprezentujemy środowisko testowe, na którym omawiane rozwiązania zostały zaimplementowane w praktyce.

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?

Tradycyjne podejście organizacji - zapewnić pracownikom wstępne szkolenia z zakresu polityk bezpieczeństwa, a następnie polegać na ich pamięci oraz zbiorowej dobrej woli - okazuje się być nieskuteczne w zakresie utrzymania norm zgodności oraz podwyższenia poziomu bezpieczeństwa informacji. Zabezpieczenie przed naruszeniami oraz utrzymanie bezpieczeństwa na wysokim poziomie to ogromne wyzwanie, zwłaszcza w obliczu czynnika ludzkiego. Niezależnie od tego czy jest to świadomy błąd, zaniedbanie, czy brak świadomości - pracownicy wewnętrzni, użytkownicy uprzywilejowani oraz pracownicy kontraktowi mają skłonność do łamania polityk firmy, wystawiając tym samym organizację na ryzyko.

Jak skutecznie zapobiegać zagrożeniom wewnętrznym przy użyciu minimum środków i czasu?
Podczas prelekcji zostaną poruszone kwestie:

- 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 odsłonie

Podczas prezentacji omówimy wyzwania stojące przed departamentami SOC. Poruszymy zagadnienia związane ze zmiennym charakterem anomalii sieciowych oraz pracą w rosnącej skali wolumenu danych. Prelegenci postarają się zestawić zamierzone cele SOC z ekonomiką implementacji zachowując konieczność silnej analizy danych, korelacji oraz predykcji. Zaprezentowane rozwiązanie stanowić będzie połączenie silnych cech produktów takich jak Flowmon ADS, ElasticSearch oraz Splunk.

Artur Bicki, Dyrektor Wydziału Wdrożeń Technologii IT, EMCA
Klaudyna Busza - Kujawska, Specjalista, Flowmon Networks

12.50–13.40

Lunch dla uczstników konfernecji

Techniczne aspekty bezpieczeństwa informacji

13.40–14.20

Sekrety blockchain – śledzenie kryptowalut

Waluta hakerów, całkowita anonimowość, pranie pieniędzy – jeśli z tym kojarzy Ci się kryptowaluta (w tym najpopularniejszy Bitcoin) to zapraszamy na naszą prelekcję. Obalamy mity i stereotypy związane z krypowalutami. Omówimy mechanizmy i algorytmy na których opierają się kryptowaluty, a na przykładzie Bitcoin przedstawimy jak śledzić transakcje i (przy odrobinie szczęścia) identyfikować osoby lub podmioty które zarządzają

Zarządzanie bezpieczeństwem informacji

13.40–14.20

Defragmentacja wiedzy CISO w obszarze incydentów bezpieczeństwa informacji

W trakcie wystąpienia zostaną przedstawione wyniki przeprowadzonej konsolidacji informacji na temat incydentów bezpieczeństwa, które wystąpiły w 2016 roku w polskich organizacjach. Zakres przedmiotowy wystąpienia obejmuje wszystkie udokumentowane incydenty, do których opisu udało się dotrzeć autorowi prezentacji.
Kalendarium incydentów

Audyt IT

13.40–14.20

Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO.

Nadciąga tsunami RODO, czyli unijne rozporządzenie o ochronie danych osobowych. Jest coraz bliżej a czasu na przygotowania jest coraz mniej. W trakcie warsztatów uczestnicy dowiedzą się m.in.:

- 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.

portfelami.

Mariusz Litwin, Analityk, EY

bezpieczeństwa zostanie zamknięte całorocznym TOP 10 w zakresie podatności, zagrożeń i zabezpieczeń stosowanych w systemach zarządzania bezpieczeństwem informacji.

Adrian Kapczyński, Członek Zarządu, Polskie Towarzystwo Informatyczne

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.

Joanna Karczewska, ISACA Warsaw Chapter

14.20–15.00

Techniczne szczegóły ataku „przez KNF"

Prezentacja będzie zawierać opis tego, co miało miejsce oraz techniczna analiza każdego etapu:

- Kiedy i jak wyzwalany był exploit
- Co się działo dalej na komputaerze ofirary

W trakcie prezentacji będzie poruszone także:

- Opis typów IoC i co oznazają
- Jak przyłożyć te IoC do własnej infrastruktury (konsumować)
- Jakie narzędzia (darmowe) mogą wspomagać konsumpcje

Tomasz Bukowski, Kierownik Zespołu Security Threat Intelligence, Bank Millennium SA

14.20–15.00

Bug bounty w mojej firmie.

Co to jest bug bounty, jakie może przynieść korzyści oraz ile kosztuje. Te i inne odpowiedzi z perspektywy osoby, biorącej udział w tego rodzaju programach.

Kacper Szurek, Detection Engineer, ESET

14.20–15.00

Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO.

Kontynuacja warsztatu cz.2

Joanna Karczewska, ISACA Warsaw Chapter

15.00–15.30

Przerwa kawowa i networking

15.30–16.10

Wzbogacanie danych w procesach SOC i CERT.

Prelekcja będzie dotyczyć łączenia danych z różnych systemów w procesach Security Operations Center i Computer Emergency and Response Team.
Uczestnicy prelekcji będą mogli dowiedzieć się m.in.:

- Jakie 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.

Andrzej Dalasiński, Group Leader, Vulnerability Management & Compliance Checks, Bosch Cyber Defense Center

15.30–16.10

Bezpieczeństwo to żyć bezpiecznie i mieć wszystko pod kontrolą? Teza prawdziwa dla bezpieczeństwa IT, a jak to jest kiedy zostaje się CISO, CIO?

Prelekcja będzie dotyczyć nowych aspektów jakie pojawią się w świecie bezpieczeństwa i zarządzania informacją, w świecie cyberbezpieczeństwa i jak nad tym wszystkim zapanować i jeszcze zrobić karierę, zbudować autorytet. W trakcie spotkania będą poruszone najważniejsze elementy z życia, doświadczenia które okazały się przełomowe dla osiągnięcia sukcesu ale także porażek, które są nieodłączne przy zarządzaniu i przewodzeniu ludźmi.

Robert Pławiak, Dyrektor Departamentu Informatyki, Europejski Fundusz Leasingowy

15.30–16.10

Jak metodyka COBIT może pomóc przygotować się do wdrożenia RODO.

Kontynuacja warsztatu cz.3

Joanna Karczewska, ISACA Warsaw Chapter

16.10–16.50

Odpieranie ataku sieciowego i analiza powłamaniowa w

16.10–16.50

Kiedy zaczniemy kupować antywirusy do

16.10–16.50

Jak metodyka COBIT może pomóc przygotować się do

praktyce.

Podsumuję praktyczne doświadczenia z ataku na infrastrukturę firmy Gemius latem 2016 roku, skupiając się na sposobach odpierania ataku i analizie powłamaniowej, w wyniku której firma złożyła wniosek do prokuratury zawierający dziesiątki gigabajtów materiału dowodowego. Powiem o wyzwaniach, które pojawiały się w trakcie ataku, niepewności czy atak się zakończył, presji biznesu, znaczeniu pomysłowości pracowników w tropieniu śladów, podejmowaniu szybkich decyzji, znaczeniu biblioteczki i o tym, jak przygotowania do certyfikacji ISO 27001 przygotowały pracowników do tego typu sytuacji.

dr Marek Robak, Head of IT Operations, Gemius

lodówek?

Jako społeczeństwo czerpiemy korzyści z innowacji, nowych technologii i cyfrowych ułatwień. Cyfrowy świat wdziera się w nasz świat, nasze życie, nasze domy. Czy tego chcemy czy nie internet rzeczy jest faktem, wirtualna rzeczywistość przestała być domeną filmów S-F a inżynierowie i innowatorzy myślą w jakich dziedzinach życia można zastosować sztuczną inteligencję.
Podczas swojego wystąpienia chciałbym zwrócić uwagę na społeczny wymiar zmian technologicznych, co powinien wiedzieć współczesny człowiek aby lodówka nie wyczyściła konta bankowego a autonomiczny samochód bezpiecznie dowiózł do celu.

Marcin Biernatowski, Poland Channel Services Head, Citi Handlowy

wdrożenia RODO.

Kontynuacja warsztatu cz.4

Joanna Karczewska, ISACA Warsaw Chapter

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.