ORGANIZATORZY

EVENTION
CZAS ZAANGAŻOWANY

ISSA POLSKA

WSPÓŁPRACA MERYTORYCZNA

CSO COUNCIL

Wstępniak

Szanowni Państwo!

Kolejna konferencja „Advanced Threat Summit" już za nami. Konferencja w listopadzie 2016 r. przyciągnęła i zgromadziła rekordowo dużą liczbę uczestników, prelegentów i wystawców. Było to ze wszech miar udane przedsięwzięcie, czemu wyraz uczestnicy dali w ankietach, w których mogli ocenić organizację, wartość merytoryczną, poszczególne prezentacje, przygotowanie prelegentów. Bardzo wszystkim dziękujemy za udział w tym przedsięwzięciu – od samego początku chcieliśmy, by „Advanced Threat Summit" był wydarzeniem ważnym i potrzebnym dla środowiska menedżerów bezpieczeństwa informacji i cyberbezpieczeństwa z działających w Polsce firm i instytucji.

Program i zamysł konferencji jest profilowany właśnie pod ich potrzeby – osób na stanowiskach kierowniczych, które odpowiadają za bezpieczeństwo informacyjne swoich organizacji, z jednej strony podejmując różne wyzwania zarządcze, z drugiej zaś operując z trudną materią szybkozmiennej technologii i różnorodnych zagrożeń. Tego będziemy się też trzymać przy kolejnych edycjach konferencji i to oprócz różnorodnej formy i niezmiennie wysokiej jakości programu stanowić będzie jej wyróżnik.

Tymczasem zapraszamy do lektury raportu, w którym zebraliśmy ciekawe wypowiedzi, refleksje, materiał podsumowujący i ważne rozmowy. W raporcie znajdą Państwo również wiele zdjęć, pozwalających wrócić pamięcią do ostatniej konferencji „Advanced Threat Summit".

Ukłony,
Przemysław Gamdzyk
Evention

Spis treści

ADVANCED THREAT SUMMIT 2016

Nowe, proaktywne podejście do bezpieczeństwa

Technologie cyfrowe zmieniają nie tylko społeczeństwo i biznes, ale także tworzą nowe wyzwania w kontekście podejścia do bezpieczeństwa. Tradycyjne metody i systemy zaczynają stanowić raczej przeszkodę niż rozwiązanie. Potrzebna jest nowa strategia, która będzie daleko wykraczać poza działy bezpieczeństwa, a także nowe technologie, bo choć żadna sama w sobie nie stanowi panaceum, to jednak jest niezbędna w złożonym systemie obrony. To ważne, ponieważ tylko sprawny system obrony może zapewnić organizacji „cyfrową odporność" – twierdzili prelegenci konferencji „Advanced Threat Summit 2016".

Cyfrowa transformacja, która opanowała przedsiębiorstwa i instytucje na całym świecie, stanowi dzisiaj wyraźny trend. Biznes zmienia się, bo zmienili się klienci, którzy mają obecnie znacznie wyższe wymagania. Otwieranie firm na zewnątrz oznacza wzrost liczby zagrożeń i zwielokrotnienie ryzyka. Eksperci zgromadzeni na konferencji podkreślali jednak, że zamieszanie z tym związane ani też płynące ze zmian korzyści nie sprawiają, że kwestie bezpieczeństwa schodzą na dalszy

Jeśli chcemy osiągnąć rozsądny poziom cyberbezpieczeństwa w organizacji, to tak naprawdę mówimy o zmianie. Jak się za to zabrać? Zaczynamy od zebrania faktów. Następnie przedstawiamy projekt, wybieramy strategię i budujemy program. Rozpoczęcie dyskusji z zarządem na temat zmiany w podejściu do bezpieczeństwa jest już dzisiaj proste. A to dlatego, że zarząd jest zaniepokojony cyberzagrożeniami. To dobra wiadomość. Jest jednak również zła. Na pewno członkowie zarządu zapytają: co już zrobiłeś, żeby to zmienić?

DENIS VERDON,
BUPA

plan. Wszyscy zgadzali się jednak co do tego, że konieczne jest przebudowanie tradycyjnego podejścia do bezpieczeństwa. Potencjalne koszty włamań są ogromne. Podczas konferencji przywoływany był przykład amerykańskiej firmy Target, który pokazał, że kradzież danych kart kredytowych i debetowych może spowodować koszty przekraczające 1 mld zł.

Jak zatem zacząć wprowadzać zmiany? W wielu wystąpieniach prelegenci podkreślali znaczenie języka używanego w komunikacji z zarządem lub innymi działami, które powinny aktywnie uczestniczyć w budowaniu nowej strategii cyberbezpieczeństwa organizacji. Warto używać prostych do zrozumienia metafor – przekonywał Denis Verdon, odpowiedzialny za ryzyka związane z informacją w grupie Bupa, globalną korporacją usług medycznych, do której w Polsce należy sieć Lux-Medu.

Dlaczego? Ponieważ język używany przez „bezpieczników" jest często zupełnie niezrozumiały dla przedstawicieli innych departamentów. Wykazała to choćby analiza opisów poszczególnych wystąpień – akceptowanych przez środowisku, ale wymagających do pełnego zrozumienia wieloletniej edukacji. To niezwykle istotne, ponieważ kwestia odporności organizacji na cyberzagrożenia znacznie wykracza poza dział bezpieczeństwa. Obejmuje całe przedsiębiorstwo, w tym specjalistów od komunikacji, prawników i przedstawicieli biznesu.

Podczas spotkania dostępnych było jednak także wiele ciekawych wydarzeń dla ekspertów cybersecurity: prelekcje techniczne, warsztaty oraz sesje roundtables. „Advanced

Cyfrowa transformacja to już nie jest buzzword, ale bardzo wyraźny trend. Firmy muszą się zmienić, bo zmienili się ich klienci. To oni oczekują od firm czegoś innego niż dotychczas.

WIESŁAW KOTECKI,
DELOITTE DIGITAL CEE

Badania potwierdzają, że cyfrowa transformacja jest czymś, co się dzieje w wielu firmach. Jednak większość badanych mówi, że działy bezpieczeństwa są pomijane przy podejmowaniu kluczowych decyzji w tym obszarze. Firmy zajmujące się bezpieczeństwem mogą zrobić bardzo dużo, ale jeśli nie idą za tym zmiany w organizacjach, to nie spodziewajmy się zbyt wiele.

MICHAŁ OSTROWSKI,
FIREEYE

Z naszych prognoz wynika m.in., że w 2017 r. możemy spodziewać się dalszej konwergencji technologii oraz działań zmierzających do konsolidacji rynku dostawców rozwiązań bezpieczeństwa. Duże organizacje będą przejmować mniejsze firmy specjalizujące się w obszarze cyberbezpieczeństwa. Co to oznacza dla klientów? Małe firmy, które nie znajdą inwestorów albo nie zostaną przejęte przez większych graczy, będą znikać z rynku. Natomiast konsekwencją połączeń i przejęć będzie to, że rozwój niektórych produktów może zostać spowolniony albo w ogóle wstrzymany. Należy to brać pod uwagę, dokonując wyborów technologicznych.

CARL LEONARD,
FORCEPOINT SECURITY LABS

Threat Summit 2016" to jedna z najważniejszych i największych konferencji w tym obszarze organizowana w Polsce i adresowana do menedżerów z dużych organizacji – CSO, CISO, dyrektorów IT, ds. bezpieczeństwa, a także menedżerów i specjalistów bezpieczeństwa ICT.

Plan na wzrost

Wieczorem pierwszego dnia konferencji w centrum uwagi znalazł się rynek pracy dla ekspertów cybersecurity, jego potencjał, możliwości rozwoju oraz system kształcenia zawodowego. Przedstawiciele firmy Hayes Poland opowiadali o rynku pracy ekspertów bezpieczeństwa oraz ich zarobkach w Polsce. Dariusz Użycki z Pedersen & Partners poruszył temat planowania kariery profesjonalisty bezpieczeństwa informacji, znacznie wykraczający poza wiedzę i umiejętności techniczne oraz menedżerskie.

W trakcie debaty stanowiącej zwieńczenie tej sesji szczegółowe plany Ministerstwa Cyfryzacji dotyczące wzrostu liczby profesjonalistów cybersecurity w Polsce przedstawił Piotr Januszewicz, zastępca dyrektora Departmentu Cyberbezpieczeństwa. W ministerstwie wszyscy doskonale zdają sobie sprawę, że specjalistów w tym obszarze – ze względu m.in. na rozwój Internet of Things oraz inteligentnych technologii Smart City i Industry 4.0 – w przyszłości potrzeba będzie znacznie więcej. Konieczne jest zbudowanie mechanizmów kształcenia zorganizowanego oraz odpowiednie kształtowanie świadomości społecznej.

W planach znajduje się stworzenie nowych kierunków studiów kładących większy nacisk na zagadnienia

Na rynku ochrony zdrowia to nie konkurencja jest motorem napędzającym cyfryzację. Po prostu bez cyfryzacji dojdzie do zapaści opieki zdrowotnej. Potrzeby rosną, lekarzy mamy coraz mniej. Jeśli nie wykorzystamy technologii cyfrowych, to będzie katastrofa. Naturalną konsekwencją tego są wzmożone działania w obszarze bezpieczeństwa.

ANDRZEJ OSUCH,
LUX MED

W ekonomii „apek" firmy budujące doskonałe aplikacje będą wygrywać. Jednak wyzwania związane z bezpieczeństwem będą coraz większe. Zarządzanie łańcuchem dostaw odbywa się coraz szybciej i szybciej. W erze DevOps odbywa się z ogromną prędkością.

DANIEL SPICA,
SPICA SOLUTIONS

Jaki jest najlepszy sposób na zatrzymanie ataków ransomware? Istnieją trzy możliwości, ale tylko działanie na poziomie plików zapewnia 100-proc. skuteczność. Należy zablokować dostęp aplikacji do krytycznych plików. Kontrola aplikacji w połączeniu z usunięciem ze stacji roboczych kont uprzywilejowanych to najlepszy sposób walki z ransomwarem.

MIRI HERSZFANG,
CYBERARK

związane z cyberbezpieczeństwem. Ma się pojawić nowy stopień naukowy: doktor inżynier lub magister inżynier cyberbezpieczeństwa. Tytuł będzie przyznawany absolwentom nowego kierunku studiów, w którego ramach będą obowiązywały takie specjalności, jak: zarządzanie cyberbezpieczeństwem, informatyka śledcza, informatyka analiz wsteczna kodu wysoko- i niskopoziomowego oraz układów elektronicznych, analiza działań przestępczych i terrorystycznych, a także zarządzanie centrum operacyjnym cyberbezpieczeństwa. Na innych kierunkach studiów mają być natomiast rozwijane specjalizacje interdyscyplinarne związane z tym obszarem. Wcześniej trzeba jednak na forum europejskim ustalić kwestie formalnoprawne dotyczące zawodu eksperta ds. cybersecurity. To zadanie trudne, ale wykonalne.

Ministerstwo Cyfryzacji ma także w planach zbudowanie platformy naukowej, która przyczyni się do zwiększenia liczby specjalistów pracujących w ośrodkach naukowych. Powstanie Naukowy Akademicki Klastra Cyberbezpieczeństwa, który umożliwi wykorzystanie potencjału polskich naukowców i polskiej myśli naukowo-technicznej. Na kilku wybranych uczelniach powstaną laboratoria, w których będą prowadzone programy badawcze poświęcone tworzeniu i wdrażaniu nowych metod ochrony. Pierwsze takie laboratorium ma powstać na Politechnice Warszawskiej. Ustalenia z innymi uczelniami są zaawansowane. Część pieniędzy na zatrudnienie naukowców ma dostarczyć Narodowe Centrum Badań i Rozwoju. Ministerstwo zakłada, że znaczną część prac uda się wykonać w ciągu najbliższych miesięcy. Konkretne efekty działań mają być widoczne już w przyszłym roku (więcej informacji pod adresem: www.cyberedu.gov.pl).

Wzrost zagrożeń związanych z postępującą cyfrową transformacją nie powinien zaskakiwać. To nie jest nowa sytuacja. Każda nowa technologia niesie ze sobą nowe rodzaje ryzyka. Dzisiaj jest ich tylko trochę więcej, może nie są do końca rozpoznane. Niemniej nie jest prawdą, że jesteśmy tak zafascynowani cyfrową transformacją, że tracimy z pola widzenia bezpieczeństwo. Takie spotkania jak AT Summit pokazują, że zdajemy sobie sprawę z zagrożeń. Konieczne jest jednak przebudowanie podejścia do bezpieczeństwa. Może też trzeba sobie uświadomić, że są miejsca, których chronić już nie warto.

GRZEGORZ STĘPNIAK,
PERN

Nowe rodzaje złożonych cyberataków wymagają równoczesnego zastosowania różnorodnych narzędzi obrony. Kluczowe jest, żeby zastosować odpowiednią technikę w odpowiednim czasie i miejscu. Właśnie współpraca różnych technologii to sposób na zwiększenie skuteczności ochrony. W takim wielowarstwowym systemie szczególne miejsce zajmuje sztuczna inteligencja. Nasze unikalne podejście wykorzystuje uczenie maszynowe – na etapie przed wykonaniem i w czasie wykonywania kodu.

MICHAŁ JARSKI,
TREND MICRO

Przedostanie się do sieci zajmuje przestępcom kilka minut. Od tego momentu średnio upływa 200 dni, zanim organizacja zorientuje się, że padła ofiarą włamania. Dalsze 80 dni upływa od wykrycia incydentu do uporania się z nim. Czego zatem brakuje w firmowej strategii cyberochrony stacji końcowych? Odpowiedź jest prosta: nie ma kompleksowej strategii działania po włamaniu.

DAN MICHELSON,
STEFEN SELLMER, MICROSOFT

Ważnym elementem rządowych planów jest partnerstwo publiczno-prywatne, dla którego podstawowym warunkiem jest otwarte podejście szkół i uczelni do współpracy z biznesem. Na razie przypadki takiej skutecznej współpracy w Polsce można policzyć na palcach jednej ręki. Szczególnym przykładem jest program podyplomowych studiów Cybersecurity Management na Uniwersytecie Ekonomicznym we Wrocławiu, którego kierownik, dr Maja Leszczyńska, opowiadała o samych studiach oraz współpracy z biznesem przy ich tworzeniu.

Szklana kula cybersecurity

Podczas konferencji sporo uwagi poświęcono także temu, co nas czeka w obszarze cybersecurity w roku przyszłym i latach kolejnych. Dobrym punktem wyjścia do dyskusji kuluarowych był zaprezentowany w czasie sesji otwierającej imprezę doroczny raport „Security Predictions" przygotowany przez firmę Forcepoint Security Labs, którego premiera odbyła się kilka dni przed „AT Summit 2016". Według firmy nadrzędnym trendem, który będzie wpływał na przyszłe wydarzenia i kształtował zjawiska, jest konwergencja świata cyfrowego i fizycznego, przenikanie zagrożeń; jego konsekwencją musi być integracja strategii i systemów obrony. Ta konwergencja będzie miała długofalowe konsekwencje w postaci powstania nowego cyfrowego ekosystemu stanowiącego poważne wyzwanie dla organizacji na całym świecie.

Trudno wskazać spośród 10 prognoz te najbardziej istotne albo prawdopodobne, dlatego każdy wybór będzie miał charakter arbitralny. Wydaje się, że najpoważniejsze

W obszarze cyberbezpieczeństwa kluczem do sukcesu jest informacja. Problemem natomiast to, że wiedza na temat zagrożeń jest rozproszona. Dlatego trzeba ją integrować.

MICHAŁ CEKLARZ,
CISCO

Z badań wynika, że zaledwie połowa używanych w firmach urządzeń jest skanowana pod kątem podatności. Tylko co dziesiąta skanuje całą swoją infrastrukturę. Organizacje powinny przestać koncentrować się na atakach „zero day", a zabrać się przede wszystkim za łatanie dziur dobrze znanych od tysiąca dni.

JASON CLARK,
TENABLE

Internet of Things posiada ogromny potencjał biznesowy, ale jednocześnie rodzi jeszcze większe wyzwania dla osób odpowiedzialnych za cyberbezpieczeństwo. Dowolne urządzenie podłączone do internetu, np. drukarka bezprzewodowa czy kamera, to dla hakerów potencjalny punkt wejścia. Tymczasem podłączamy kolejne „rzeczy", nie znając i nie rozumiejąc do końca wszystkich zagrożeń i ich konsekwencji dla bezpieczeństwa.

CHRISTOPHER J. HODSON,
ZSCALER

konsekwencje z punktu widzenia polskich organizacji i instytucji będzie miało rozporządzenie europejskie GDPR, wprowadzające nowe regulacje w zakresie ochrony danych osobowych, ale także wpływać będzie na obszar cybersecurity, w a w szczególności obowiązki informacyjne w przypadku wystąpienia incydentów. GDPR będzie skutkować także istotnym wzrostem wydatków. Należy pamiętać, że nie nie ma już zbyt dużo czasu na działania (rozporządzenie zacznie obowiązywać od maja 2018 r.). Trendem jest także eskalacja podatności związanych z tzw. abandonware, czyli „opuszczonym oprogramowaniem", starymi aplikacjami, systemami, które nadal są wykorzystywane, ale nie są aktualizowane – tego typu oprogramowanie to łatwy cel dla przestępców, dlatego można spodziewać się, że będzie źródłem wycieków danych.

Ciekawa była także prognoza dotycząca chmury obliczeniowej, a mianowicie, że będzie to coraz częstszy wektor ataków. Przestępcy zaczną specjalizować się w hakowaniu hyperwizorów, zaś dostawcy usług cloud będą coraz częstszymi ofiarami ataków typu DOS.

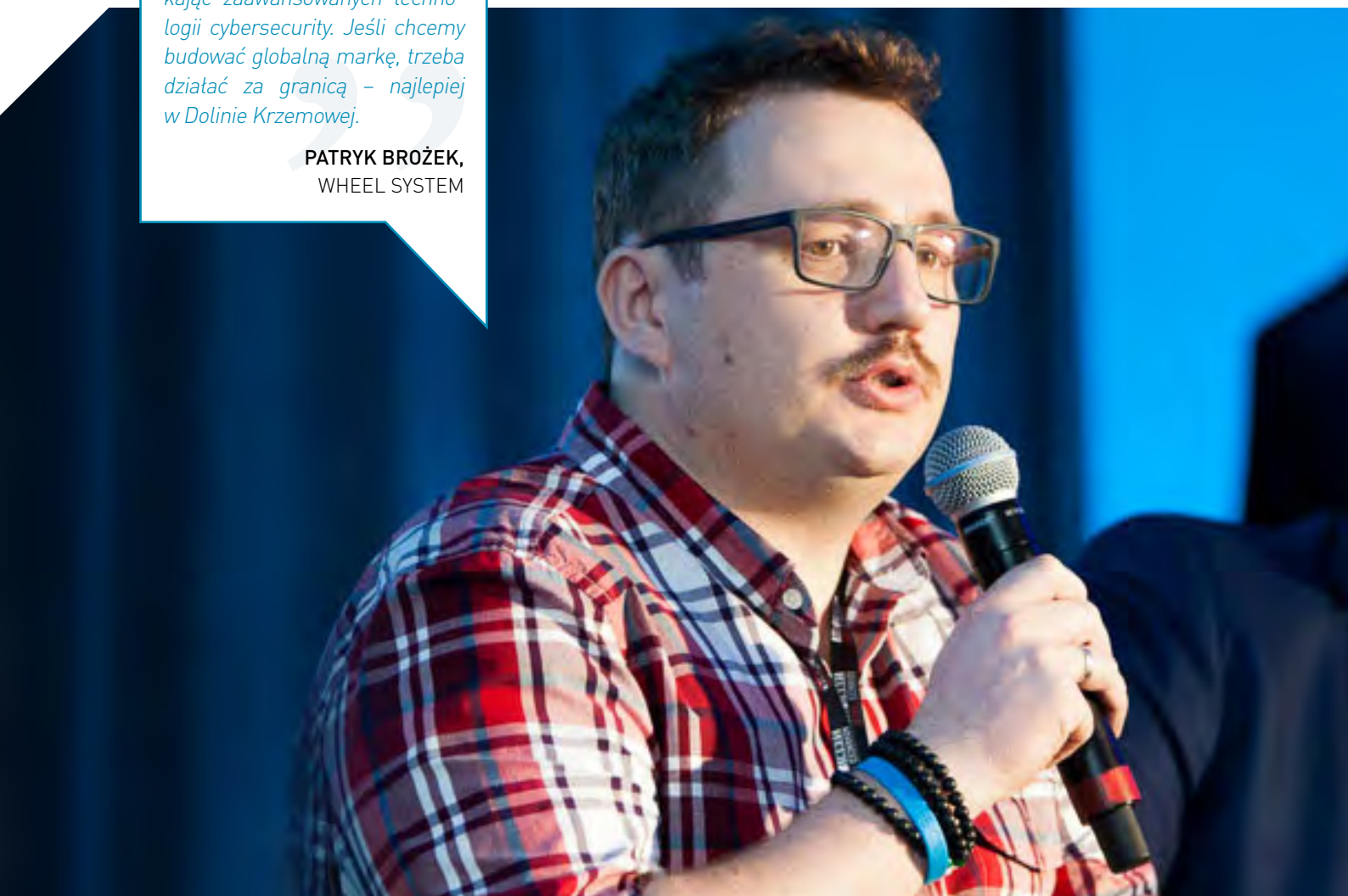
Tegoroczny „**Advanced Threat Summit**" zgromadził blisko 400 uczestników – w większości menedżerów bezpieczeństwa z różnych sektorów polskiej gospodarki oraz przedstawicieli firmy będącej dostawcami usług i rozwiązań cybersecurity. Kolejna konferencja planowana jest w listopadzie 2017 r.

Biorąc pod uwagę wrogość środowiska cyfrowego – wielkość potencjalnej przestrzeń ataku, złożoność systemów chronionych przez niedostateczną liczbę specjalistów, a także poziom zaawansowania przeciwnika – Threat Intelligence to bardzo przydatny zbiór złożonych informacji o zagrożeniu. Wymagają one jednak interpretacji dokonywanej przez przygotowany, wyszkolony zespół specjalistów.

LECH LACHOWICZ,
SYMANTEC

Świat nie patrzy na Polskę, szukając zaawansowanych technologii cybersecurity. Jeśli chcemy budować globalną markę, trzeba działać za granicą – najlepiej w Dolinie Krzemowej.

PATRYK BROŻEK,
WHEEL SYSTEM



W Polsce trudno przebić się z innowacyjnymi produktami, zwłaszcza w obszarze IT i cybersecurity. Wynika to po części z narodowego przeświadczenia, że nie jesteśmy w stanie konkurować ze światowymi potęgami. Przełamanie bariery niewiary w siebie ma kluczowe znaczenie dla rozwoju naszego rynku i zwiększenie szans polskich produktów za granicą.

KRZYSZTOF SURGOWT,
CRYPTOMIND

PSE potrzebuje nowoczesnych, śmiałych pomysłów na narzędzia i aplikacje, a także na bezpieczeństwo naszych systemów informatycznych. Przy realizacji takiego zadania nie sprawdzają się brane z półki aplikacje dużych dostawców. Potrzebujemy rozwiązań szytych na miarę. To właśnie zadanie dla małych, ambitnych firm, których założyciele mają pasję i chcą pokonywać bariery. Jesteśmy otwarci na taką współpracę i staramy się ją stymulować.

ŁUKASZ KISTER,
PSE

Rozmowa z prof. Jerzym Surmą, kierownikiem studiów podyplomowych Zarządzanie Cyberbezpieczeństwem w Instytucie Informatyki i Gospodarki Cyfrowej w SGH

Proaktywna współpraca

CTI, czyli Cyber Threat Intelligence, to oparta na faktach wiedza o istniejących lub mających się wkrótce pojawić ryzykach, która pozwala podejmować lepsze decyzje potrzebne do obrony i neutralizowania zagrożeń. Tego typu informacje pozwalają na proaktywną ochronę mającą fundamentalne znaczenie we współczesnym, cyfrowym środowisku biznesowym – mówi prof. Jerzy Surma, kierownik studiów podyplomowych Zarządzanie Cyberbezpieczeństwem w Instytucie Informatyki i Gospodarki Cyfrowej w Szkole Głównej Handlowej, członek Rady Nadzorczej BZWBK.

W swoim wystąpieniu podczas konferencji „AT Summit 2016" mówił Pan, że w pełni zautomatyzowane CTI to kwestia przyszłości. Czy warto korzystać z tego typu rozwiązań? Co możemy dzięki nim osiągnąć?

Jest uzasadnione, aby stosować tego typu systemy i prowadzić działania określane jako Cyber Threat Intelligence w sytuacjach, kiedy organizacja jest narażona na systemowe ataki w cyberprzestrzeni. To niezwykle istotny element strategii, która nie polega wyłącznie na reagowaniu, ale również na antycypowaniu ataków.

Co można osiągnąć dzięki CTI? Ograniczamy fałszywe alarmy poprzez eliminację nieistotnych incydentów, nadajemy priorytety do instalacji aktualizacji, ustalamy przepływ właściwych danych do SIEM, co umożliwia skuteczną korelację danych, a także identyfikujemy zagrożenia i w tym kontekście zyskujemy możliwość zapobiegania atakom. Określamy również priorytety alertów dla zespołu SOC, co umożliwia koncentrację na rzeczywistych zagrożeniach. Informacje z systemu CTI pozwalają na dogłębne poznanie intencji i motywów działania grup przestępczych, umożliwiają decydentom zrozumienie aktualnych zagrożeń, a dzięki temu poprawną alokację budżetów oraz pracowników dla ochrony krytycznych zasobów. Wreszcie możemy

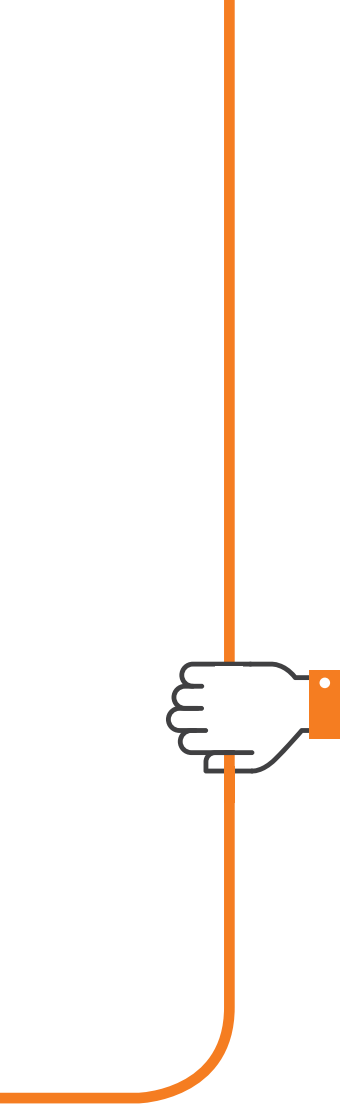
prof. Jerzy Surma,
kierownik studiów podyplomowych Zarządzanie Cyberbezpieczeństwem w Instytucie Informatyki i Gospodarki Cyfrowej w Szkole Głównej Handlowej, członek Rady Nadzorczej BZWBK

poprawnie zarządzać ryzykiem operacyjnym poprzez antycypację prawdopodobnych zagrożeń i komunikację ich do zarządu w celu podjęcia działań zapobiegawczych.

Na czym polega problem dostępnych na rynku systemów?

Na rynku amerykańskim istnieje szereg firm, które próbują penetrować dark internet. Starają dowiedzieć się, o czym dyskutują grupy przestępcze, jakie podatności są na ich celowniku, jakich narzędzi używają, jakie są potencjalne cele. Dzięki temu są w stanie przewidywać, co się może wkrótce wydarzyć. Mają na swoim koncie kilka spektakularnych sukcesów. Przykładowo firma Recorded Future, posiadająca platformę, która całościowo zbiera takie dane, analizując rosyjskie fora dyskusyjne, była w stanie przewidzieć wektory ataków, użyte narzędzia, a nawet wskazać potencjalne cele.

Problem polega na tym, że ludzie po drugiej stronie barykady, nasi przeciwnicy, wiedzą, jak działa inwigilacja w internecie. Trzecia liga podziemnego świata może nie mieć świadomości skali monitorowana. Jeśli jednak mówimy o pierwszej



lidze, to oni doskonale zdają sobie sprawę, że odbywa się takie automatyczne zbieranie informacji. Ci najlepsi są na to wyczuleni. Jeśli dostrzegą, że znaleźli się pod lupą, znikają albo konfabulują. Innymi słowy – i to jest problem fundamentalny – to sposób na niedzielnych hakerów. Jesteśmy w stanie zebrać dużo informacji o stosunkowo prostych zagrożeniach i niewiele o tych najbardziej poważnych.

Chciałbym przy tym zaznaczyć, że mówię o zbieraniu informacji w sposób automatyczny, o narzędziach wykorzystujących metody eksploracji danych (data mining). Jeśli zaczynamy mówić o ekspertach, white hackerach, którzy wchodzą incognito na takie fora, to sytuacja się zmienia. Tacy „szpiedzy" mogą naprawdę wiele, są skuteczni. To są jednak punktowe działania.

Czy uważa Pan, że obecne postępy w obszarze metod eksploracji danych, sztucznej inteligencji mogą coś zmienić?

Jestem sceptyczny. Zajmuję się tematyką sztucznej inteligencji od prawie 30 lat. Średnio co 10 lat obserwowałem już falę medialnych zachwytów nad postępami w tym obszarze. To, co się dzieje obecnie, to w moim odczuciu tylko następna fala, która wezbrała dzięki spektakularnym osiągnięciom metod maszynowego uczenia się w zakresie analizy dużych wolumenów danych behawioralnych, systemów rekomendacyjnych i analityki prowadzonej na klientach. Czy to jednak przełom, który pozwoli na penetrowanie w wyrafinowany sposób środowiska hakerskiego pod kątem potencjalnych ataków? Mam poważne wątpliwości.

Jakie są inne sposoby na proaktywność w obszarze cybersecurity? Co robić, żeby wyprzedzać działania cyberprzestępców?

Jest to trudna tematyka. Mamy oczywiście do dyspozycji całą klasę systemów określanych jako open source intelligence. Umożliwiają one prowadzenie wywiadu na podstawie publicznie dostępnych źródeł. Wykorzystywane są dosyć powszechnie przez państwowe służby, ale też wywiad gospodarczy.

Na popularyzację zasługują rozmaite formy współpracy, pozwalające na wymianę tego typu informacji

> Idealny system Computer Threat Intelligence powinien być dokładny, wyszukiwać istotne i wiarygodne informacje oraz zapewniać możliwość podejmowania na podstawie tych informacji (możliwość podemowania na podstawie tych informacji działania) działania. Praktyka jednak pokazuje, że dostępne narzędzia obarczone są pewnymi poważnymi problemami. Biorąc to pod uwagę, mam wątpliwości, czy działające w zautomatyzowany sposób narzędzia tego typu są w ogóle możliwe do stworzenia.
>
> **PROF. JERZY SURMA,**
> SGH

> Ludzie, którzy posiadają kompetencje w zakresie analizy złośliwego oprogramowania i inżynierii wstecznej, są poszukiwani przez pracodawców. Każdy chce ich zatrudnić. To dzisiaj ogromna luka na rynku.
>
> **PROF. JERZY SURMA,**
> SGH

wywiadowczych pomiędzy organizacjami. W tym wypadku mamy do czynienia nie tylko z informacją publicznie dostępną, ale także takimi, które zdobywają firmy specjalizujące się w cybersecurity, które prowadzą rozpoznanie grup przestępczych. Są na rynku organizacje, które budują bazy takich informacji. Istnieją możliwości integrowania tych danych, zbierania ich w postaci branżowych raportów, które w ramach danego sektora czy branży prezentują pewne tendencje i pozwalają wyłapywać zagrożenia.

Czy może Pan przybliżyć, na czym polega taka współpraca?

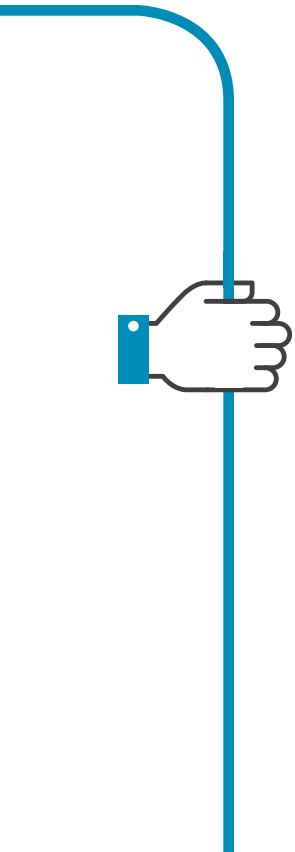
Przykładem może być współpraca sektora finansowego. Cyberbezpieczeństwo to jeden z obszarów, który można określić jako wspólny interes, w którego ramach którego można i należy współdzielić wiedzę, ostrzegać innych uczestników rynku. Z punktu widzenia pojedynczej organizacji zbudowanie zespołu specjalistów cyber therat intelligence jest bardzo trudne i kosztowne, ale zbudowanie takiego zespołu na poziomie sektora czy branży może być opłacalne.

Takie podejście pozwala zmniejszyć koszty pozyskania informacji, a zarazem zdobyć wiedzę, która umożliwia proaktywność – np. dostrzec wcześniej, że jakaś grupa hakerska poszukuje informacji na temat pewnej podatności, co jest groźne dla całego sektora. Na marginesie warto dodać, że hakerzy zwykle szukają najsłabszego ogniwa. Nie próbują wchodzić na Mount Everest. Jeśli da się coś zrobić szybciej i taniej, tym lepiej. To stricte biznesowe podejście, które polega na optymalizowaniu kosztów versus maksymalizacja przychodów.

Na jakim etapie znajduje się organizowanie takiej współpracy sektorowej w Polsce?

Sektor finansowy współpracuje w ramach ZBP. To najbardziej zaawansowana próba budowy takiej wspólnoty w Polsce – chodzi o współdzielenie wiedzy i partycypowanie w kosztach. Formalnie prace nad tą ideą są w realizacji. Jest przyzwolenie największych banków w Polsce, żeby je kontynuować. Działania prowadzone pod egidą ZBP powinny zaowocować już w 2017 r.

Są jednak inne sektory, w których taka współpraca jest niezbędna. Przede wszystkim odnosi się to do infrastruktury krytycznej. Sądzę, że jak tylko uporządkowane zostaną wszystkie kwestie związane z cyberbezpieczeństwem w naszym kraju, szybko dojdzie do takiej współpracy i powstaną sektorowe SOC.



AT SUMMIT
ROUNDTABLES

RUNDA 1

Stolik nr 1

Ludzie, czyli kluczowy i najtrudniejszy czynnik zarządzania bezpieczeństwem. Jak wciągnąć ich do gry?

Prowadzenie:
Jakub Roszewski, starszy specjalista, Immusec

W obszarze zarządzania bezpieczeństwem mamy poważny problem. Choć mamy dostęp do zaawansowanych systemów bezpieczeństwa, to nie jesteśmy w stanie objąć nimi ludzkich umysłów. Właśnie dlatego wektor ataków ukierunkowany jest w coraz większym stopniu właśnie na ludzi. Jak sobie z tym radzić? Przede wszystkim należy mieć tego świadomość i prowadzić w związku z tym ciągłą dyskusję z biznesem. Należy przy tym pamiętać, że nie rozmawiamy z ekspertami ds. cyberochrony, dlatego należy używać prostego języka i wykorzystywać łatwe do zrozumienia analogie.

Stolik nr 2

Czy hakerzy potrafią oszukać sandbox i czy sandbox można zabezpieczyć przed wykryciem?

Prowadzenie:
Marcin Krzemieniewski, ekspert, Dimension Data Polska

Sandbox to przydatne rozwiązanie, ale należy go traktować tylko jako jeden z elementów w ekosystemie bezpieczeństwa. Przestępcy, twórcy złośliwego oprogramowania, zdają sobie sprawę z istnienia takich technologii i robią wszystko, żeby je oszukać. Jeśli chcemy przeciwdziałać wykrywaniu środowiska sandboxowego, powinno ono dokładnie odzwierciedlać posiadane systemy i infrastrukturę. Dobrym rozwiązaniem jest także zasilanie środowiska informacjami o zagrożeniach i przesyłanie próbek. Informacje o potencjalnych zagrożeniach powinny być możliwe do przekazania do innych rozwiązań w sposób elastyczny.

Stolik nr 3

Jakie są główne przyczyny i rzeczywiste koszty cyberataków?

Prowadzenie:
Andrzej P. Kleśnicki, Technical Account Manager for Central Eastern Europe, Qualys

Na podstawie informacji pozyskiwanych z mediów można wyrobić sobie zdanie o rzeczywistych przyczynach i kosztach cyberataków. Należy jednak pamiętać, że media przedstawiają wydarzenia spektakularne, które „dobrze się sprzedadzą", ale które nie przynoszą realnych strat. Bardziej wiarygodnych informacji dostarczają nam raporty branżowe. Wynika z nich, że większość incydentów motywowana jest chęcią pozyskania pieniędzy. Ataki zwykle zaczynają się od umieszczenia złośliwego oprogramowania. Co istotne, większość udanych ataków wykorzystuje podatności znane od dawna, które łatwo wyeliminować poprzez instalację odpowiedniej łatki. Ciekawe jest także, że średni koszt ataku jest relatywnie niski.

Stolik nr 4

Retaining Security Talent

Prowadzenie:
Michael Sikorski, Director, FLARE Team, FireEye

Jak zatrzymać w organizacji najbardziej utalentowanych specjalistów od cyberbezpieczeństwa? Zacznijmy od tego, że nie jest to cel sam w sobie. To rezultat wielu działań, które możemy podejmować. Powinny być dostosowane do konkretnej sytuacji w organizacji, w zespole, do ludzi. Na co należy zwrócić uwagę? Trzeba zdobywać wiedzę o ludziach już w czasie rekrutacji i prowadzić okresowe dyskusje poświęcone ich rozwojowi osobistemu. Należy wyznaczyć zespołowi jasne cele – to przyciąga specjalistów. Istotną rolę w utrzymaniu talentów odgrywa menedżer zespołu, który powinien dbać o dobre relacje z pracownikami. Last, but not least: pieniądze nie są zwykle najważniejsze.

Stolik nr 6

Wyzwania związane z wykrywaniem i blokowaniem nowych zagrożeń ukrytych w ruchu szyfrowanym

Prowadzenie:
Aleksander Kijewski, Sales Engineer, Sonicwall

Wykrywanie zagrożeń w ruchu szyfrowanym jest możliwe, ale warunkiem jest jego analizowanie. Dlatego po pierwsze konieczna jest inspekcja ruchu szyfrowanego, a później sandboxing tego ruchu lub kodu, który jest wychwytywany w trakcie analizy. Jest to jednak wyzwanie z punktu widzenia technologicznego i finansowego – wymaga zastosowania mocnych firewalli i proxy, ponieważ ruchu jest coraz więcej. Z drugiej strony samo wdrożenie nie jest proste. Nie ogranicza się do wykonania jednej czynności. Ważne, aby zgodnie z najlepszymi praktykami zrobić wyjątki dla stron bankowych, medycznych oraz zakupowych.

Stolik nr 7

Zaawansowane zagrożenia: socjotechnika, malware, DDOS – analiza ryzyka i dobór reakcji

Prowadzenie:
Krzysztof Skibicki, dyrektor Działu Wsparcia Biznesu, Comp SA

Analizując uważnie ataki APT, musimy dojść do wniosku, że są to zagrożenia wypracowane przez służby specjalne, które następnie zostały przejęte przez organizacje przestępcze. Ich prowadzenie służy realizacji celów wywiadowczych i przestępczych. Dzisiaj nie jesteśmy w stanie skutecznie ochronić się przed atakami tego typu. Dlatego musimy skupić się na kluczowych zasobach i otoczyć je szczególną opieką. Szkolenia są nieefektywne, ponieważ pracownicy szybko wracają do niebezpiecznych zachowań. Należy skupić się przede wszystkim na tych pracownikach, którzy mają dostęp do zasobów krytycznych.

Stolik nr 8

Jak zmieni naszą codzienność dyrektywa GDPR (General Data Protection Regulation)?

Prowadzenie:
Piotr Kluczwajd, Area VP-Eastern Europe, Russia, CIS, Turkey, Imperva

Witold Wojakowski, konsultant w obszarze bezpieczeństwa informatycznego oraz ochrony danych osobowych, Imperva

Rozporządzenie wejdzie w życie w maju 2018 r. Związane z nią wyzwania są poważne. Zasadniczo zarządy firm mają tego świadomość, dlatego prowadzone są przygotowania, identyfikowane obszary i opracowywane plany. Jednak szczegółowość i stopień tych działań są różne. Ważne jest spojrzenie na to zagadnienie z perspektywy audytów, wycieków danych oraz 72-godzinnego informowania o naruszeniach. Polski rząd ma świadomość konieczności wprowadzenia zmian i przygotowuje się do wejścia w życie ustawy. GIODO otrzyma narzędzia potrzebne do egzekwowania prawa, zatem pojawi się realne zagrożenie karą – wysoką karą.

Stolik nr 10

Monitorowanie użytkownika końcowego – DLP i narzędzia analizy

Prowadzenie:
Alexander Raczyński, inżynier systemowy, Forcepoint

W kontekście monitorowania użytkownika końcowego niezwykle przydatne są narzędzia. W najbliższych latach ich wykorzystanie będzie coraz bardziej popularne. Istnieje jednak wiele wątpliwości co do ich użycia. Jak traktuje ich stosowanie polskie prawo. Sytuacja nie jest jasna i trzeba będzie poczekać, aż się wyklaruje. Dzisiaj jedni mówią, żeby się wstrzymać ze względu na istniejące interpretacje, a inni są zdania, żeby działać, bo wymagania w związku z GDPR są coraz większe. Oczywiście prawo powinno nadążać za dynamicznym rozwojem technologicznym, ale to trudne. Tak czy inaczej dane generowane w wyniku coraz bardziej dokładnego analizowania danych o użytkownikach należy otoczyć wzmocnioną ochroną.

RUNDA 2

Stolik nr 1

Optymalny poziom kompetencji kadry i liczebność zespołu bezpieczeństwa w firmie

Prowadzenie:
Krzysztof Miareczko, kierownik programu Wspólna Infrastruktura Państwa, Ministerstwo Cyfryzacji

Trudno powiedzieć, czy jesteśmy skazani na to, że pracownicy prędzej czy później odejdą. Niemniej panuje powszechna zgoda, że najlepiej w przypadku zespołów bezpieczeństwa sprawdza się model hybrydowy: część funkcji realizowana jest przez zespół wewnętrzny, a część – tych bardziej specjalistycznych – kupowana jest na zewnątrz. W małych firmach wewnętrzny zespół może ograniczać się choćby do jednej osoby, ale ważne jest, że ktoś był w środku firmy. To istotne ze względu na wrażliwe dane, których nie chcemy przetwarzać poza firmą, regulacje rządowe, szybką i trafną ocenę wpływu incydentów na procesy biznesowe oraz reagowanie, a także – biorąc pod uwagę reputację firmy – fakt, że niektóre incydenty nie powinny wychodzić poza organizację.

Stolik nr 2

Jak wygrać z ransomware, skoro sygnatury nie działają?

Prowadzenie:
Łukasz Bogucki, kierownik Zespołu Bezpieczeństwa, Dimension Data Polska

Każdy słyszał o ransomware, niektórzy wiedzą o nim bardzo dużo, a niektórzy mieli nawet styczność z takim oprogramowaniem (badania pokazują, że blisko 40% organizacji doświadczyło podobnych problemów). Analiza wektorów ataku pokazuje, gdzie najczęściej możemy się na nie natknąć: dwa najbardziej popularne kanały to poczta elektroniczna i strony internetowe. Użytkownicy klikają w zawartość, np. e-maila, i dochodzi

do infekcji. Sygnatury nie sprawdzają się w ochronie przed ransomwarem. Podobnie pełnej ochrony nie zapewniają sandboxy. Ransomware działa w zróżnicowany sposób, zwykle przebiegle. Jedynym sposobem obrony jest lista bezpiecznych aplikacji, odpowiednio patchowanych, słownikowych oraz ochrona urządzeń końcowych użytkowników.

Stolik nr 3

Bezpieczeństwo ICT w czasach cloud computing i shadow IT

Prowadzenie:
Andrzej P. Kleśnicki, Technical Account Manager for Central Eastern Europe, Qualys

Czym jest shadow IT? Dla wielu osób często jest to nie tyle shadow, ile dark IT. Oczywiście, nie jest to nowe zagadnienie dla bezpieczeństwa w organizacjach. Każdy zapewne spotkał się z użytkowaniem arkuszy kalkulacyjnych, które są na dyskach sieciowych znajdujących się poza organizacją. W takich przypadkach, kiedy pracownik odchodzi z firmy, proces biznesowy może się zatrzymać. Jak sobie z tym radzić? Pomysły są różne, m.in. edukacja pracowników, stosowanie technologii wymuszających dostęp do usług i zapewniających bezpieczeństwo, ale każda organizacja musi stworzyć własną strategię.

(Stolik n 4)

Budowanie własnych kompetencji lub outsourcing – dyskusja o sposobach efektywnego zarządzania obsługą incydentów

Prowadzenie:
Tomasz Pietrzyk, Manager Systems Engineering, FireEye

Organizacje nie mają problemu z przekazywaniem obsługi incydentów na zewnątrz. Nie mają także problemu z przekazywaniem danych, chyba że kłóci się to z regulacjami obowiązującymi firmę. Oczywiście, w tym przypadku lepiej współpracować z dostawcami z Europy lub takimi, którzy mają na terenie Unii swoje centra przetwarzania danych. Obsługa incydentów traktowana jest jako dodatkowy zasób, po który chętnie się sięga w sytuacji krytycznej. Wykorzystanie firmy zewnętrznej ma tę dodatkową zaletę, że obsługa odbywa się w trybie 24/7. Na razie polski rynek nie jest jeszcze nasycony tego typu ofertami. Niestety, głównym kryterium wyboru pozostaje cena.

Stolik nr 5

Post Breach Detection with Windows Defender Advanced Threat Protection

Prowadzenie:
Dan Michelson, Program Manager, Enterprise & Security Team, Microsoft

Stefan Sellmer, Security Researcher, Microsoft

Windows Defender Advanced Threat Protection to nowa usługa Microsoftu, która umożliwia wykrywanie, dochodzenie i reagowanie w odpowiedzi na zaawansowane, celowane ataki. Analizując dane z kilku miesięcy, można dojść do następujących wniosków: bardzo trudno wskazać konkretną maszynę, która jest atakowana, nawet jeśli wiemy, że taki atak występuje, a po naprawieniu szkody trudno powiedzieć, czy klient albo firma stosują się do przedstawionych im rekomendacji. Warto dodać, że dochodzenia trwają kilka dni, a nie sekundy czy godziny, a ich koszty należy zestawić z kosztami poszczególnych systemów.

Stolik nr 6

Cyberbezpieczeństwo i jego strategia – jak zmienić postrzeganie wagi problemu w oczach zarządu

Prowadzenie:
Marcin Lisiecki, Manager, Cyber Security, Deloitte

Zmienia się rola CISO w organizacji. Teraz to osoba, która jest aktywnym propagatorem zmian. To właśnie na barkach CISO spoczywa obowiązek informowania o zagrożeniach i dyskutowania o tym z zarządem. Oczywiście, dopasowanie bezpieczeństwa do celów biznesowych to wyzwanie. Dlatego trzeba zrozumieć sposób pracy zarządu i cele, które chce osiągnąć. Podejmowane działania powinna determinować solidna analiza ryzyka, a nie intuicja. Ważne, by zachować zdrowy rozsądek i mieć na uwadze zasady prowadzenia biznesu.

Stolik nr 7

Tworzenie zespołów SOC (Security Operation Center) – czy? jak? dlaczego?

Prowadzenie:
Michał Kurek,Executive Director, EY

Czy warto wdrażać SOC? A jeśli tak, to jak to robić i dlaczego? Odpowiedź na ostatnie pytanie jest najłatwiejsza. Dzisiejszy sposób prowadzenia i sama złożoność cyberataków sprawiają, że bardzo trudno się przed nimi bronić. Co więcej, należy założyć, że takie ataki już nastąpiły. Dlatego warto zainwestować środki pozwalające na ich szybkie wykrywanie. Czy i jak wdrażać SOC – to już zagadnienia na dłuższą dyskusję. Najważniejszy aspekt to integracja z biznesem. Ważne, żeby przy budowie SOC wyjść od celów biznesowych – przeanalizować

profil, przeprowadzić gruntowną analizę ryzyka. Dopiero na tej podstawie można udzielić sensownej odpowiedzi.

Stolik nr 8

Dziesięć kwestii, jakie powinien zawierać twój Disaster Recovery Plan

Prowadzenie:
Tomasz Bujała, kierownik Biura Bezpieczeństwa Teleinformatycznego, TU Europa SA oraz TU na Życie Europa SA

Jakie punkty powinny znaleźć się w firmowych planie odtwarzania po awarii? Jednym z najważniejszych zagadnień jest dopasowanie planu do faktycznych potrzeb. Wybrane podejście do DRP powinno być precyzyjnie dopasowane do wymagań stawianych przez branżę, w której działa organizacja. Kolejne istotne zagadnienie to zapewnienie wersjonowania oraz posiadania szczegółowej historii aktualizacji. W dobrze przygotowanym DRP powinna zostać dokładnie opisana komunikacja realizowana w przypadku wystąpienia katastrofy, należy opracować możliwe scenariusze działań, wreszcie plan musi zawierać listę kluczowych aplikacji, opisywać także niezbędne do sprawnej jego realizacji szkolenia i konieczne do przeprowadzenia testy.

Stolik nr 9

Zarządzanie uprawnieniami użytkowników i aplikacji na stacjach roboczych

Prowadzenie:
Michał Ciemięga, Regional Sales Manager, CyberArk

Zarządzanie uprawnieniami na stacjach roboczych to skuteczny sposób na ochronę najszerszego dostępnego punktu wejścia do organizacji. Nie są do tego potrzebne zaawansowane systemy ochrony przed złośliwym oprogramowaniem. Największym problemem są bowiem konta z uprawnieniami administracyjnymi na stacjach końcowych. Najlepszym rozwiązaniem tego problemu jest usunięcie tych kont. Niektórzy mogą powiedzieć, że to niemożliwe, że są one potrzebne. Okazuje się jednak, że wystarczą jedynie podwyższone uprawnienia zwykłych użytkowników. Selektywne zarządzanie uprawnieniami to jednocześnie mniej zgłoszeń do help desku.

Stolik nr 10

DDoSy i masowe zagrożenia dla dzisiejszych sieci Enterprise – jak bronić własne firmy w obliczu wszechobecnej łączności wszystkich ze wszystkimi

Prowadzenie:
Łukasz Bromirski, dyrektor techniczny, Cisco Systems Poland

Przed IT stoją liczne, nowe poważne wyzwania: trzeba objąć ochroną urządzenia osobistech (BYOD), elektroniczne gadżety (wearables) oraz wszelkiego typu urządzenia podłączane do sieci i tworzące Internet Rzeczy (IOT), a także zapanować nad ich wykorzystaniem w firmowych sieciach. W tym kontekście najważniejsze jest zajęcie się zagadnieniami związanymi z separacją ruchu pomiędzy urządzeniami a strefami chronionymi w sieci. Istnieją systemy, dzięki którym można to przeprowadzić w sposób zautomatyzowany. Warto takie systemy testować i wdrażać. Separacja zapewnia bowiem wyższy poziom bezpieczeństwa. Ważna jest także edukacja użytkowników i poszukiwanie nowych pomysłów na pokazywanie zagrożeń.

RUNDA 3

Stolik nr 1

White Hat czy Black Hat – dylemat niezadowolonego pracownika IT

Prowadzenie:
Tobiasz Koprowski, członek zarządu, ISSA Polska

Niezadowoleni pracownicy stają się atrakcyjnym celem ataków. Być może sami mogą być ich źródłem. Problem dotyczy w takim samym stopniu wszystkich branż. Nie jest także obcy administracji publicznej. Sytuację pogarszają zmiany na rynku pracy. Mamy do czynienia z rynkiem pracownika, w którym może on urządzać castingi na pracodawcę. Jakie mogą być przyczyny niezadowolenia? Różne. Częstym zjawiskiem jest po prostu wypalenie zawodowe. Atak na takiego pracownika to typowy atak socjotechniczny. Wystarczy zaangażować odpowiednią ilość czasu, a sukces jest bardzo prawdopodobny. Dlatego istotne są szkolenia pracowników i rozmowy z nimi, które pozwalają rozpoznać potencjalne zagrożenia.

Stolik nr 2

Wewnętrzne procedury, zalecenia i najlepsze praktyki w zakresie zapewnienia bezpieczeństwa informacji

Prowadzenie:
Anna Adamska, Security & Governance Manager, CBS DanIS Nordics & Central Europe (DANONE)

Jak uzupełnić wiedzę pracowników w zakresie bezpieczeństwa i wiedzę o cyberzagrożeniach? Możliwe są trzy

wektory działań. Przede wszystkim istotne jest wprowadzenie procedur, prowadzenie szkoleń, a przy tym ścisła współpraca z zarządem. Procedury są istotne, ponieważ pozwalają usystematyzować informacje. Dostarczają jednocześnie dokumentacji dla audytorów. Szkolenia – zewnętrzne i wewnętrzne – pozwalają weryfikować zdobywaną wiedzę. Ważne, żeby maksymalnie upraszczać przekazywane wiadomości. Jeśli chodzi o współpracę z zarządem, warto wziąć pod uwagę fakt, że na wszystkie inwestycje i działania potrzeba pieniędzy.

Stolik nr 3

Sytuacja kryzysowa – dobre praktyki postępowania w biznesie

Prowadzenie:
dr inż. Andrzej Bartosiewicz, dyrektor ds. bezpieczeństwa korporacyjnego, Xademi SECURITY

W tym roku ujawniono 99 mln rekordów zawierających dane osobowe. To aż 2,5 razy tyle co w roku ubiegłym. Rok 2017 z tej perspektywy zapowiada się bardzo ciekawie. Co można zrobić w tej sytuacji? Po stronie administracji rządowej mamy do czynienia z chaosem, jeśli chodzi o zarządzanie incydentami – jest za dużo instytucji. Przez to w przypadku wykrycia naruszenia przedsiębiorstwa nie wiedzą, gdzie zgłaszać powiadomienie i jakie informacje powinny zostać przekazane. Dlatego niezwykle istotna jest współpraca branżowa. Należy brać sprawy we własne ręce i organizować wspólne centra SOC. To jednak nie wszystko. Potrzebne są jeszcze procedury. Cała firma powinna być przygotowana na zarządzanie kryzysowe.

Stolik nr 4

Zarządzanie incydentami w przedsiębiorstwie w kontekście zagrożeń APT

Prowadzenie:
Francesco Chiarini, Manager, Information Security Threat & Response, PepsiCo International – Information Security Group (ISG)

Ataki APT to zaledwie podzbiór wszystkich incydentów. Udzielenie odpowiedzi na pytanie, czy jesteśmy przygotowani do zarządzania zagrożeniami APT, jest możliwe dopiero po sformułowaniu odpowiedzi na pytanie, czy w ogóle jesteśmy przygotowani na zarządzanie incydentami bezpieczeństwa. Niemniej w kontekście APT trzeba zwrócić uwagę na następujące czynniki: pieniądze – trudno uzasadnić przejście od prostego reagowania na incydenty do zaawansowanego; pentesty – są w stanie dobitnie pokazać, że możemy stać się ofiarą ataku hakerskiego; wreszcie, standaryzacja procesów – to niezwykle istotny czynnik przygotowań.

Stolik nr 5

Skuteczne planowanie ryzyka i zarządzanie nim w obszarze outsourcingu i usług hybrydowych

Prowadzenie:
Grzegorz Długajczyk, Manager – Departament Zarządzania Ryzykiem Operacyjnym, ING Bank

Pomimo różnic pomiędzy sektorami gospodarki i branżami, jeśli chodzi o outsourcing, mamy wspólny mianownik. Chodzi o zbiór podstawowych zasad dla organizacji, która korzysta z outsourcingu. Ważne jest zwłaszcza zarządzanie ryzykiem. W tym

kontekście kluczowa jest ocena ryzyka związanego z powierzanymi informacjami. Na tej podstawie należy przygotować plan wymagań bezpieczeństwa. Kolejny istotny punkt to umowa i klauzule. Najważniejsze jest prawo do przeprowadzenia audytu. Na bieżąco trzeba monitorować kontrakt, żeby mieć pewność, że deklaracje zgadzają się z rzeczywistością.

Stolik nr 6

Strategia cyberbezpieczeństwa w firmie

Prowadzenie:
Przemysław Dyk, CISO, Bank Zachodni WBK

Stworzenie skutecznej strategii cyberbezpieczeństwa w firmie i późniejsza praca nad nią, żeby nie stała się wyłącznie dokumentem w szufladzie, to niełatwe zadanie. Przede wszystkim strategia powinna zawierać realne cele i korzyści. Dzięki temu łatwiej budować listę zadań. Strategia powinna być także na bieżąco monitorowana pod kątem tego, czy zadania z listy są po kolei realizowane i czy zbliżamy się do określonego w niej celu. Raz do roku powinien odbywać się przegląd strategii, w którego ramach stwierdza się, czy zmiany w świecie, w bliskim otoczeniu, a także wewnątrz organizacji nie sprawiają, że konieczne jest wprowadzenie poprawek i uzupełnień w dokumencie.

Stolik nr 7

Phishing, inżynieria społeczna i kradzież tożsamości – skuteczne narzędzia w rękach cyberprzestępców

Prowadzenie:
Krzysztof Słotwiński, CSO, BGŻ BNP Paribas

Według raportu Kaspersky Lab w 2016 roku zarejestrowano ogromny wzrost liczby ataków phishingowych. W trzecim kwartale doszło do ponad 73 mln incydentów (dla porównania w pierwszym kwartale zarejestrowano tylko 41 mln). Zdaniem CERT Polska, najważniejszy i najbardziej niepokojący trend to phishing ukierunkowany na użytkowników bankowości internetowej. Niestety, ochrona użytkowników przed takimi

atakami jest bardzo trudna. Dlatego ważne jest, żeby budować świadomość, żeby wytworzyć gotowość. Ciekawym pomysłem jest nano-learning polegający na tworzeniu materiałów w postaci bardzo krótkich filmów lub wiadomości.

Stolik nr 8

Bezpieczeństwo w całym cyklu życia systemu IT – jak je zawsze zapewnić

Prowadzenie:
Dariusz Jurewicz, Head of Central Risk Services, UBS Business Solutions Poland

Opieranie bezpieczeństwa tylko na dobrej współpracy pomiędzy IT a bezpieczeństwem nie wystarczy. Nie zapewni także bezpieczeństwa SDLC, jeśli jego istnienie będzie ograniczało się do „martwego" papierowego dokumentu. Konieczne jest dokładne opisanie SDLC i zdefiniowanie etapów, zasad itd. Przede wszystkim trzeba je jednak wdrożyć i użytkować – tylko wtedy można mówić o bezpieczeństwie. Pośród kryteriów sukcesu należy wymienić: zapewnienie wsparcia wszystkich zaangażowanych stron, zapewnienie wsparcia kierownictwa firmy oraz zwiększenie świadomości ryzyka wśród właścicieli.

Stolik nr 9

Skuteczne zarządzanie ryzykiem technologicznym w organizacji – doświadczenia praktyczne

Prowadzenie:
Łukasz Guździoł, zarządzanie ryzykiem IT, Credit Suisse/TRISW/ISSA Polska

Jak skutecznie zarządzać ryzykiem technologicznym? Co robić, żeby można było dzięki temu podejmować lepsze decyzje biznesowe? Podstawowy warunek to komunikacja pomiędzy IT a biznesem przy użyciu jednego, wspólnego języka. Szacowanie ryzyka przez biznes pozwala na definiowanie celów i konsekwencji. Umożliwia również realne oszacowanie prawdopodobieństwa włamania. Na pewno potrzebna jest w organizacji osoba, która będzie odpowiedzialna za ryzyko. Powinna ona dysponować budżetem, który pozwoli jej na rozwiązanie problemu, kiedy ryzyko się zmaterializuje. Przy tym analiza ryzyka powinna być proaktywna, a nie reaktywna. Należy ją prowadzić już na etapie wyboru dostawcy, tworzenia projektu, a nie po fakcie.

Stolik nr 10

Prawne oblicze cyberbezpieczeństwa, czyli jak skutecznie zamawiać bezpieczne systemy IT

Prowadzenie:
Dariusz Czuchaj, Senior Associate / Legal Counsel at TMT/IP Department, Kancelaria Prawna Dentons

Najważniejszym i najbardziej interesującym tematem cyberbezpieczeństwa w aspekcie prawnym jest kwestia odpowiedzialności. Środek ciężkości w umowach z dostawcami przechodzi w kierunku bezpieczeństwa. Jest to związane z tym, że weszły nowe regulacje prawne, a wkrótce – w 2018 r. – wejdzie w życie Rozporządzenia o ochronie danych osobowych. To siła napędowa, która wpływa na wzrost liczby i intensywności dyskusji o bezpieczeństwie. Zwłaszcza że dotychczasowe umowy nie odpowiadają na nowe wyzwania. Powoduje to konieczność ich renegocjowania – te procesy już trwają albo właśnie się zaczynają.

Rozmowa z Michael'em Sikorskim, dyrektorem i założycielem FLARE Team

Złośliwe oprogramowanie. Cała wstecz!

Kiedy prowadzi się dochodzenie, odpowiedzi trzeba znaleźć najszybciej, jak to jest możliwe. Zaangażowani są prezesi, dyrektorzy generalni firm. Koszty są wysokie, a wynagrodzenie liczone jest od godziny. Klienci oczekują efektów w ciągu kilku godzin. Nie chcą czekać kilka dni, a czasem tyle czasu właśnie potrzeba. To jednak rzadkie przypadki. Zwykle udaje nam się rozwiązać problem w czasie liczonym w godzinach – mówi Michael Sikorski, dyrektor i założyciel FLARE Team, działającego w firmie FireEye zespołu specjalistów zajmujących analizą złośliwego oprogramowania i inżynierią wsteczną, uczestniczącego w dochodzeniach dotyczących najbardziej groźnych incydentów naruszenia bezpieczeństwa na świecie.

Czym zajmuje się FLARE Team?

FireEye Labs Advanced Reverse Engineering, czyli FLARE, to zespół zajmujący się analizą złośliwego oprogramowania i inżynierią wsteczną obsługujący FireEye w zakresie najtrudniejszych problemów. Kiedy inne zespoły nie mogą sobie z czymś poradzić, przychodzą do nas. Bierzemy także udział w dochodzeniach związanych z incydentami, które dotyczą największych klientów. To największe tego typu przypadki na świecie. Jeśli w wyniku dochodzenia wykrywane jest złośliwe oprogramowanie, przesyłane jest do FLARE Team.

Ile osób pracuje w zespole?

Mamy 30 analityków zajmujących się złośliwym oprogramowaniem i specjalistów od inżynierii wstecznej. Mamy także kilku badaczy zajmujących się podatnościami, którzy szukają luk bezpieczeństwa w oprogramowaniu albo analizują ataki dnia zerowego.

Michael Sikorski,
dyrektor i założyciel FLARE Team

Mamy również niewielki zespół programistów, który pomaga tworzyć narzędzia wspomagające naszą pracę. Dzięki tym dodatkowym narzędziom zwiększamy efektywność, możemy coraz szybciej analizować coraz więcej przypadków. Mamy także narzędzia, które pomagają ludziom w terenie. Przykładowo, jeśli ktoś odkryje złośliwe oprogramowanie w czasie dochodzenia albo jeśli natrafi na coś, czego nie potrafi rozpoznać, to mamy system, do którego możemy przesłać podejrzany plik i uzyskać dodatkowe informacje. Automatycznie wykonywane są takie działania jak klasyfikacja złośliwego oprogramowania. W ten sposób można szybko uzyskać informacje, nie zawracając głowy wyspecjalizowanym analitykom.

Czy udostępniają Państwo te narzędzia?

Tworzymy także narzędzia wspierające analizę złośliwego oprogramowania, które udostępniamy społeczności. W tym roku udostępniliśmy bezpłatnie dwa takie narzędzia. Jedno z nich to FakeNet-NG, które pozwala oszukać złośliwe oprogramowanie tak, żeby uznało, że jest podłączone do internetu. Drugie z nich to Floss, przeznaczone do deobfuskacji, czyli ujawniania pewnych ciągów ukrytych w złośliwym oprogramowaniu. Ich twórcy chcą często schować coś przed nami, a dzięki Floss łatwiej nam to odkryć.

Wracając do zespołu, jest całkiem duży, zwłaszcza jeśli weźmie się pod uwagę brak specjalistów z tej dziedziny na rynku.

Z mojej wiedzy wynika, że to jeden z największych zespołów tego typu na świecie. Większe można spotkać tylko w agendach rządowych. Niektóre duże firmy być może zatrudniają tylu specjalistów od inżynierii wstecznej, ale są oni rozproszeni po całej organizacji, nie

tworzą jednolitego zespołu, nie współpracują na bieżąco, nie opracowują własnych narzędzi i nie osiągają sukcesów jako zespół w rzeczywistych sytuacjach reagowania na incydenty.

Czy wobec tego rynek, na którym działa FLARE Team, jest konkurencyjny?

Konkurencja odbywa się raczej w obszarze reagowania na incydenty i prowadzenia dochodzeń. Klienci, którzy padli ofiarą ataku, często zatrudniają równocześnie kilka zespołów. Mówią: znajdźcie wszystko, co się da. W efekcie te konkurujące zespoły depczą sobie po piętach, ale to prawdziwa konkurencja. Liczy się to, kto pierwszy znajdzie przestępcę. Jesteśmy częścią tego procesu. Nasz zespół, który coś znajdzie, przesyła nam swoje odkrycia.

A czy jest coś, czego Pan się obawia? Czy są jakieś niepokojące trendy?

Kiedy hakerzy kogoś atakują, zwykle najpierw używają najprostszych narzędzi. Nie chcą od razu używać swojej najlepszej broni, ponieważ raz wypuszczona do sieci może zostać rozpracowana. Zamiast tego używają najpierw prostych rozwiązań. I w większości przypadków odnoszą sukces.

Monitorujemy tych napastników i wiemy, co jest ich prostą bronią, a co najbardziej zaawansowaną. Potrafimy także rozpoznać działania poszczególnych hakerów czy grup. Co więcej, prowadziliśmy dochodzenia, w których spotykaliśmy się z prostymi narzędziami pewnej grupy hakerskiej w jednej firmie i bardziej zaawansowanymi w innej organizacji. Kiedy widzimy, że stosowane są proste narzędzia, to wiemy, że klient ma kłopoty, bo nic nie wie o bezpieczeństwie.

Niepokojący jest fakt, że przestępcy będą w końcu musieli zrezygnować z tych prostych narzędzi i zacząć używać częściej najlepszych rozwiązań. To spowoduje, że trzeba będzie coraz więcej czasu poświęcać na analizę. Ostatecznie jednak nie boimy się niczego. Nigdy nie spotkaliśmy się jeszcze ze złośliwym kodem, którego nie bylibyśmy w stanie zanalizować, mając odpowiednią ilość czasu. Są pewne techniki, które mogą nas spowolnić, ale nie są w stanie nas zatrzymać.

Na koniec pytanie o Pańską książkę. „Practical Malware Analysis" to jedna z niewielu pozycji na rynku poświęconych tej tematyce. Dlaczego zdecydował się Pan na jej napisanie, kto ją powinien przeczytać i dlaczego?

Napisałem tę książkę wspólnie z Andrew Honigiem, moim kolegą z college'u, który pracuje w Google, z kilku powodów. Największe znaczenie miał fakt, że zajmowałem się nauczaniem analizy złośliwego oprogramowania i inżynierii wstecznej przez wiele lat. W tym czasie opracowałem na potrzeby kursów

dużą ilość materiałów dydaktycznych, które ułatwiały wyjaśnienie i naukę pewnych rzeczy studentom. Napisanie tego rodzaju książki to sposób, żeby za jednym razem przekazać wiedzę o wiele większej grupie ludzi. Normalnie wchodzę do sali i uczę 20 studentów. W przypadku książki mogę dotrzeć do tysięcy ludzi.

Poza tym mam do czynienia z brakiem takich umiejętności na rynku. Ludzie, którzy posiadają kompetencje w zakresie analizy złośliwego oprogramowania i inżynierii wstecznej, są poszukiwani przez pracodawców. Każdy chce ich zatrudnić. To ogromna luka na rynku. Książka to szansa na poprawę sytuacji szeroko rozumianej branży bezpieczeństwa.

Efektem ubocznym, którego nie przewidywaliśmy, jest fakt, że obecnie publikacja wykorzystywana jest na 50 uniwersytetach na świecie. Początkowo używano jej w ramach ogólnych programów poświęconych wiedzy o komputerach czy inżynierii komputerowej, ale powstały programy dotyczące bezpieczeństwa. Ta książka jest bardzo chętnie wybierana jako podręcznik na zajęciach z analizy złośliwego oprogramowania czy inżynierii wstecznej. To spełnienie naszych marzeń. Nie planowaliśmy tego, po prostu tak wyszło.

Kto Pańskim zdaniem powinien ją przeczytać?

Książka jest przeznaczona dla wszystkich, którzy chcą nauczyć się analizowania złośliwego oprogramowania. Zaczynamy od podstaw, więc każdy, kto zajmuje się zawodowo bezpieczeństwem IT, powinien zrozumieć treści zawarte w pierwszych trzech rozdziałach. Oczywiście potrzebne są pewne fundamenty. Do zrozumienia książki potrzeba wiedzy o programowaniu.

Natomiast kolejne rozdziały są przeznaczone dla osób, które chcą wejść naprawdę głęboko w tę materię. Pomysł na książkę nie ograniczał się tylko do treści do przeczytania. Napisaliśmy 51 przykładów złośliwego kodu, który udostępniliśmy za darmo wraz z książką. Dzięki temu po przeczytaniu rozdziału można „wziąć udział" w laboratoriach, które pozwalają samodzielnie, praktycznie zmierzyć się z problemem. Na końcu książki jest dodatek, który zawiera rozwiązania prowadzące Czytelnika krok po kroku, mówiąc, co zrobić w przypadku poszczególnych laboratoriów. To bardzo dobry materiał szkoleniowy, bo to jakby lekcja w książce. Podaje wszystko, czego potrzeba, łącznie z podpowiedziami na końcu książki, jak rozwiązać problemy.

Dla tych, którzy chcą uczynić z tego swój zawód, to książka typu how-to. Jeśli zatem ktoś chce się tego naprawdę nauczyć, to książka dla niego. Jeśli ktoś jest już ekspertem, być może przyda się jako materiał referencyjny na biurku.

> Kiedy hakerzy kogoś atakują, zwykle najpierw używają najprostszych narzędzi. Nie chcą od razu używać swojej najlepszej broni, ponieważ raz wypuszczona do sieci może zostać rozpracowana. Zamiast tego używają najpierw prostych rozwiązań. I w większości przypadków odnoszą sukces.

EVENTION
CZAS ZAANGAŻOWANY

HARMONOGRAM KONFERENCJI EVENTION Z OBSZARU CYBERBEZPIECZEŃSTWA I BEZPIECZEŃSTWA INFORMACJI NA ROK 2017

InfraSEC Forum Bezpieczeństwo twardej infrastruktury — 24 stycznia 2017 r., Warszawa

- Pierwsza w Polsce konferencja o konkretnych aspektach bezpieczeństwa twardej infrastruktury – od Internetu Rzeczy, poprzez Operational Technology aż do Infrastruktury Krytycznej
- Planowana liczba uczestników: 100 osób
- Konferencja zgromadzi menedżerów i ekspertów zajmujących się cyberbezpieczeństwem fizycznej infrastruktury z wybranych firm i przedsiębiorstw, których usługi i funkcjonowanie silnie zależą od posiadanej infrastruktury, w szczególności szeroko rozumianej branży utilities

Więcej na: www.infrasecforum.pl

RIBA Forum RODO-Innowacje-Bezpieczeństwo-Audyt — 6-7 kwietnia 2017 r., Warszawa

Wyzwania ochrony danych w czasach nowych regulacji

- Pierwsza edycja konferencji poświęcona bezpieczeństwu informacji z perspektywy ochrony danych osobowych
- Planowana liczba uczestników: 120—150 osób
- Konferencja zgromadzi osoby odpowiedzialne za ochronę danych osobowych w tym ABI, prawnicy, compliance menagerowie, przedstawiciele działów biznesowych zainteresowanych tematyką ochrony danych osobowych z firm dużych i średniej wielkości oraz instytucji publicznych

Więcej na: www.ribaforum.pl

CyberGOV 2017 Bezpieczeństwo ICT w sektorze publicznym — 18 maja 2017 r., Warszawa

- Trzecia z cyklu konferencja o bezpieczeństwie IT i audycie technologicznym dedykowana specyfice sektora publicznego
- Planowana liczba uczestników: 250 - 300 osób
- Konferencja zgromadzi przedstawicieli sektora publicznego - od urzędów gmin, poprzez miasta, urzędy powiatowe, marszałkowskie, wojewódzkie, aż do urzędów centralnych, agend rządowych i ministerstw - w szczególności osoby odpowiedzialne za bezpieczeństwo IT i bezpieczeństwo informacji w tych instytucjach oraz audyt związany z tymi obszarami
- Konferencja we współorganizacji z MC, ISACA Warsaw Chapter, ISSA Polska

Więcej na: www.cybergov.pl

Technology Risk Management Forum — **czerwiec 2017 r., Wrocław**

Zarządzanie Ryzykiem Technologicznym

- II konferencja o zarządzaniu ryzykiem technologicznym, bezpieczeństwie i ciągłości działania w kontekście rozwoju technologicznego firm
- Planowana liczba uczestników: 150 osób
- Konferencja przeznaczona jest dla wyższej kadry menedżerskiej w szczególności do CIO, CSO, IT Risk Managerów, audytorów
- Konferencja we współorganizacji z Technology Risk & Information Security Wrocław oraz ISSA Polska

Więcej na: www.techrisk.pl

Advanced Threat Summit 2017 — listopad 2017 r., Warszawa

- Czwarta zbudowana wokół tematyki najpoważniejszych i najbardziej zaawansowanych zagrożeń w Internecie
- Planowana liczba uczestników: 250-300 osób
- Konferencja zgromadzi CIO, CISO i Security menedżerów, osoby odpowiedzialne za bezpieczeństwo teleinformatyczne
- Konferencja we współorganizacji z ISSA Polska

Więcej na: www.atsummit.pl

Czym jest ISSA Polska?

- Jest to elitarne, ogólnoświatowe Stowarzyszenie osób zajmujących się zawodowo bezpieczeństwem informacji oraz bezpieczeństwem systemów informatycznych.
- Polski oddział ISSA jest 100 oddziałem (w skali światowej, i należy do jednych z najszybciej rozwijających się oddziałów w Europie.

Dla kogo jest ISSA Polska?

- Dla profesjonalistów zawodowo związanych z bezpieczeństwem systemów informacyjnych.
- Dla osób, które interesują się bezpieczeństwem systemów informacyjnych, planują w przyszłości rozwój kariery zawodowej w tym obszarze.
- Dla studentów pragnących w przyszłości zawodowo związać się z tematyką bezpieczeństwa systemów informacyjnych.

Co zapewnia ISSA Polska?

- **Integrację środowiska** – ułatwienia w postaci np. dedykowanych zamkniętych grup w serwisach typu LinkedIn, GoldenLine, Facebook.
- **Kontakt** – stanowi platformę kontaktu dla profesjonalistów (spotkania, zamknięte grupy projektowe, oraz dyskusyjne).
- **Platformę wymiany wiedzy fachowej** (spotkania merytoryczne, konferencje, biuletyny, ISSA Journal, e-seminaria, webcasty, itd.).

Korzyści z członkostwa w ISSA Polska

- **Rozwój zawodowy** - zwiększenie możliwości wszechstronnego rozwoju zawodowego.
- **Wiedza** - wymiana informacji i dostęp do najnowszej wiedzy fachowej:
  - ➔ Ze źródeł: ISSA International oraz ISSA Polska.
  - ➔ Dostęp do repozytorium z m.in. z prezentacjami merytorycznymi.
- **Wsparcie** - wzajemne wsparcie, doradztwo i pomoc członków Stowarzyszenia.
- **Prestiż** - elitarność członkostwa w ISSA podnosi prestiż zarówno firmy, jak i samego pracownika.
- **Punkty edukacyjne** - zdobywanie punktów edukacyjnych CPE, potrzebnych np. posiadaczom certyfikatów CISSP, SSCP, CISA, CISM, CRISC oraz innych.
- **Zniżki** - liczne zniżki/darmowe wejściówki na konferencje krajowe i międzynarodowe, szkolenia, seminaria, materiały edukacyjne.
- **Materiały edukacyjne** - dostęp do licznych projektów, materiałów i opracowań zrealizowanych w ramach stowarzyszenia ISSA Polska dotyczących m.in. ochrony prywatności,

bezpieczeństwa IT, rekomendacji dla sektora MSP, zastosowaniach IoT w bezpieczeństwie, czy praktycznych porad związanych z bezpieczeństwem teleinformatycznym w różnych aspektach codziennego życia, w tym bezpieczeństwem dzieci z punktu widzenia rodziców.

- **Dodatkowe benefity** - możliwość uzyskania cennych produktów od członków wspierających Stowarzyszenie (oprogramowanie, odzież z logo, branżową prasę, gadżety na każdą okazję itp.).

Jak dołączyć do ISSA Polska ?

- Wystarczy odwiedzić stronę **https://issa.org.pl** wypełnić dokumenty i wysłać na membership@issa.org.pl:
- Deklarację członkowską w ISSA Polska.
- Link do profilu zawodowego na Linkedin lub CV.
- Potwierdzenie wniesienia opłaty za członkostwo.
- Potwierdzenie członkostwa w ISSA International (tylko dla osób które chcą być członkami ISSA International, osoby nie posiadające takiego członkostwa mogą je uzyskać pod adresem **http://issa.org**).

Rodzaje członkostwa w ISSA Polska:

- **Aktywny** - członek ISSA International – link: **https://www.issa.org/general/register_member_type.asp?**
- **Stowarzyszony** - posiada jeden z profesjonalnych certyfikatów uznawanych przez branżę bezpieczeństwa informacji (np. CISSP, CSSLP, CAP, SSCP, CISM, CISA, CRISC, CGEiT, CompTIA Security+, CEH, QSA), nie jest członkiem ISSA International;
- **Zwykły** - posiada przynajmniej trzyletnie doświadczenie zawodowe w zakresie ochrony informacji, zabezpieczania systemów informatycznych, przeprowadzania audytów bezpieczeństwa systemów i aplikacji, przeprowadzania testów penetracyjnych lub w zakresie innych zagadnień związanych z bezpieczeństwem w środowisku IT, nie jest członkiem ISSA International:
- **Student** - jest studentem uczelni wyższej, nie jest członkiem ISSA International.

Opłaty za członkostwo w ISSA Polska:

Opłata członkowska wynosi 100 PLN
Członkostwo na zasadach członka: Stowarzyszonego, Zwykłego, Studenta.
Płatność poprzez przelew na konto bankowe wg następujących zasad (warunek nie dotyczy kandydatów ubiegających się o członkostwo Aktywne):
Odbiorca: ISSA Polska
Numer konta: 73 2130 0004 2001 0379 4211 0001
Tytułem: Opłata członkowska ISSA Polska – Imię i nazwisko
Składka 100zł płatna jest rocznie (na 1 rok).
W przypadku członkostwa w ISSA International - opłaty wynoszą jak poniżej:
95USD - General Membership - /1rok,
995USD - CISO Executive Membership,
90USD - Government Organizational Membership,
30USD - Student Membership

Nie zwlekaj
– zapisz się do ISSA Polska!
I rozwijaj swoją karierę zawodową razem z nami

PARTNER GENERALNY

PARTNER STRATEGICZNY

PARTNERZY MERYTORYCZNI

MECENASI

WSPÓŁPRACA

PATRONI

www.atsummit.pl