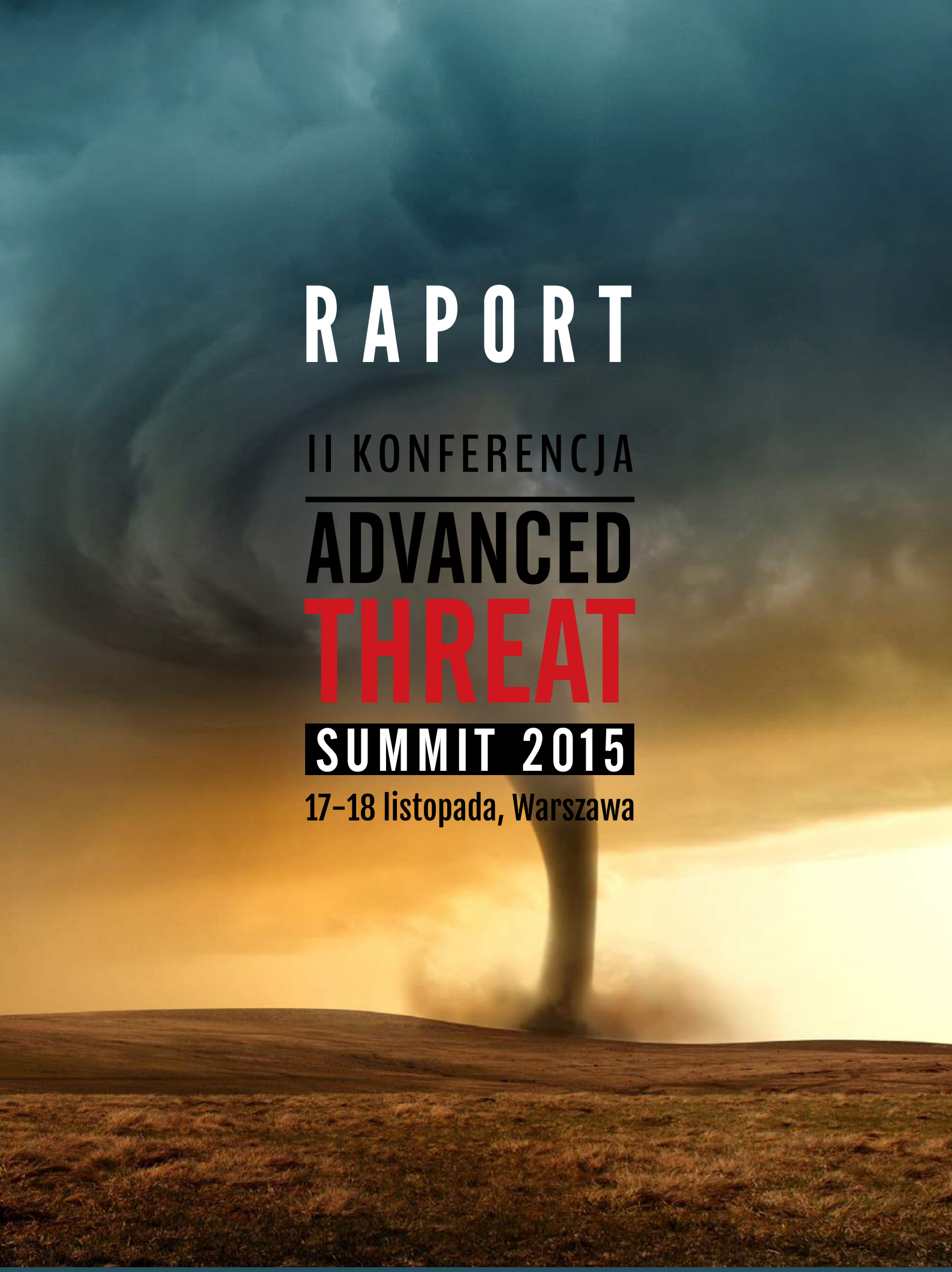


RAPORT

II KONFERENCJA

ADVANCED THREAT

SUMMIT 2015

17-18 listopada, Warszawa

www.atsummit.pl

Spis treści

Potrzeba współpracy całego środowiska

Polskie firmy wciąż mają problem z dzieleniem się informacjami o cyberzagrożeniach, jednak sytuacja ta stopniowo się zmienia. Współdziałanie na rzecz cyberbezpieczeństwa było jednym z głównych tematów konferencji „Advanced Threat Summit 2015" poświęconej najważniejszym i najbardziej zaawansowanym zagrożeniom w Internecie. Wydarzenie zostało zorganizowane po raz drugi w listopadzie 2015 roku w Warszawie przez ISSA Polska oraz Evention.

W Polsce występuje zauważalny problem z chęcią dzielenia się przez różne instytucje informacjami z zakresu cyberbezpieczeństwa – zauważa Piotr Kijewski z CERT Polska, zespołu do reagowania na zdarzenia naruszające bezpieczeństwo w Internecie. „W Europie ok. 20–30% respondentów byłoby skłonnych dzielić się z rządem informacjami o swoich problemach i dostrzeganych zagrożeniach. W Polsce ten wskaźnik wynosi blisko zero, co wygląda bardzo słabo" – mówi. „Mało jest podmiotów, które chcą się dzielić informacjami – my jesteśmy jednym z nielicznych" – dodaje.

Równocześnie Piotr Kijewski podkreśla, że istnieje duże zapotrzebowanie na tego typu informacje. „Można powiedzieć, że dane od nas płyną szerokim strumieniem. Dziennie mamy informacje z ok. pół miliona polskich adresów IP. Tą informacją bardzo chętnie się dzielimy ze wszystkimi zarówno w Polsce, jak i za granicą" – zauważa.

Piotrowi Kijewskiemu wtóruje Łukasz Guździoł z zespołu zajmującego się oceną ryzyka IT w Credit Suisse. „Z moich doświadczeń wynika, że w Polsce dzielenie się informacją ma dość ograniczony zakres" – mówi. Jego zdaniem, część firm i instytucji nie przesyła dalej informacji o zagrożeniach, gdyż nie potrafi dostrzec płynących z tego tytułu korzyści. „Wydaje mi się, że wiąże się to z niską dojrzałością tych firm" – ocenia.

Druga grupa to firmy, które rozumieją korzyści dzielenia się wiedzą o zagrożeniach, ale często nie wiedzą, jak z tej wiedzy skorzystać „Jest dużo informacji, ale nie mamy procesów, nie mamy ludzi, nie wiemy, jak zrobić z tego użytek

– w związku z tym może lepiej bądźmy cicho, nie dzielmy się tą wiedzą" – opisuje ich postepowanie Łukasz Guździoł. Często jest też to związane z tym, że wszelkiego rodzaju postępy w dziedzinie bezpieczeństwa w dużej mierze skoncentrowane były na konsumpcji wiedzy, a nie na dzieleniu się nią, więc ludzie nie są świadomi, jak wielki wpływ może to mieć na kształt tego sektora.

Jeszcze inna grupa to firmy, które widzą korzyści dzielenia się wiedzą, lecz równocześnie się tego obawiają – tylko ok. 30% firm to dostawcy wiedzy dotyczącej cyberbezpieczeństwa, zaś 70% to jej konsumenci. „Nie mamy de facto problemów z wymianą informacji o zagrożeniach od strony technicznej, bardziej od strony biznesowej" – podsumowuje Łukasz Guździoł.

Wnioski z dyskusji panelowej o wymianie informacji w zakresie cybersecurity

1. Są organizacje, które nie wiedzą, że można dzielić się informacją o cybersecurity, a jeśli już nawet mają taką świadomość, to nie wiedzą, co dalej z tą informacją zrobić.

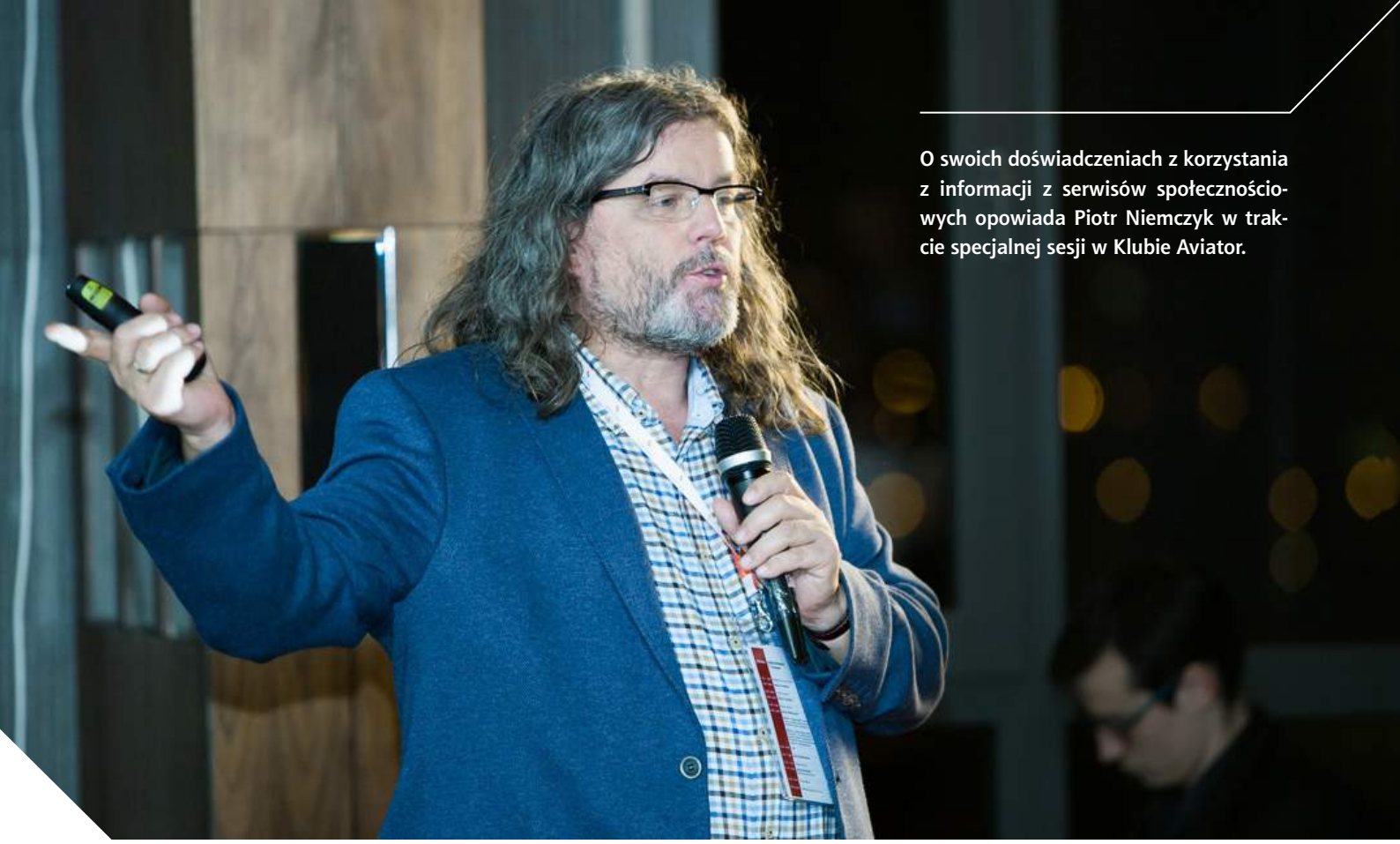
2. Trzeba rozbudzić i wzmocnić w środowisku profesjonalistów od cybersecurity potrzebę współpracy, tak żeby „biorcy" nie dominowali liczebnie nad „kontrybutorami". Ogólnie obowiązuje tutaj reguła: „Nie ten da, co ma, ale ten, co chce".

3. Działania powinny się koncentrować na poszczególnych elementach łańcucha wartości podziemia internetowego, tak żeby ten łańcuch przerwać. Nie wystarczy to, co robimy głównie teraz – koncentrując się na jego końcach (zagrożeniach albo efektach działań cyberprzestępców). To też determinuje zakres informacji, które warto ze sobą wymieniać.

4. Trzeba możliwie szybko pokazać korzyści z dzielenia się informacją, co pozwoli szybciej przełamać opór i rezerwę pozostałych, do tej pory niezaangażowanych.

5. Patrząc na wzorce ze świata, czerpmy z nich pełnymi garściami i róbmy mądrą selekcję, wybierając to, co może się sprawdzić w naszych warunkach.

6. Co jest ważniejsze: technologia czy organizacja w systemie wymiany informacji i współpracy? Trzeba znaleźć właściwe proporcje w odniesieniu do obu tych czynników. Potrzebne jest także właściwe miejsce dla dostawców, którzy agregują informacje na poziomie technicznym w skali globalnej (przede wszystkim chodzi o odczyty danych pochodzące urządzeń).



O swoich doświadczeniach z korzystania z informacji z serwisów społecznościowych opowiada Piotr Niemczyk w trakcie specjalnej sesji w Klubie Aviator.

Łukasz Hnatkowski, sekretarz Forum Bezpieczeństwa Transakcji Elektronicznych ZBP, podkreśla z kolei konieczność korzystania z różnych rozwiązań dotyczących cyberbezpieczeństwa. „Nie ma rozwiązania, które by zapewniało kompleksową ochronę przed wszystkim. Dlatego zapewnianie ochrony zarówno własnej, jak i całego sektora musi postępować wielotorowo, na kilku frontach równocześnie". Łukasz Hnatkowski podkreśla, że w przypadku bankowości dużym problemem bywa trudne do bezpośredniego kontrolowania nierozważne zachowanie klientów. „Bardzo ważną sprawą jest edukowanie użytkowników" – mówi. „Banki robią dużo, żeby zmaksymalizować sobie ochronę. Ważne jest również to, żeby uczulać klientów, że odpowiedzialność leży też po ich stronie".

Łukasz Hnatkowski ocenia, że w ostatnim czasie w sektorze bankowym zdecydowanie polepsza się współpraca w zakresie cyberbezpieczeństwa. „Ostatnio zauważamy trend, że banki naprawdę zaczynają rozumieć i czuć tę potrzebę; nie są w stanie przetrwać bezpiecznie na rynku same, w pojedynkę i nie dość, że przydatne, a wręcz niezbędne staje się to, żeby współpracować i wymieniać się tymi informacjami" – wskazuje.

Wtóruje mu Piotr Kalbarczyk z Departamentu Bezpieczeństwa banku PKO, który postuluje jeszcze większe rozszerzenie wymiany informacji dotyczących cyberbezpieczeństwa. „Ta informacja nie jest właściwa tylko i wyłącznie dla jednego sektora. Zagrożenia dotyczą w zasadzie całego państwa, całego świata. Wymiana informacji to nie jest tylko problem sektora – wymiana informacji powinna być międzysektorowa" – tłumaczy.

Konferencja ATS2016 zgromadziła 330 uczestników, zyskała bardzo wysokie oceny merytoryczne. Zapraszamy do udziału w kolejnym wydarzeniu w listopadzie 2016!

Budować samemu czy korzystać z usług – jaka przyszłość bezpieczeństwa IT

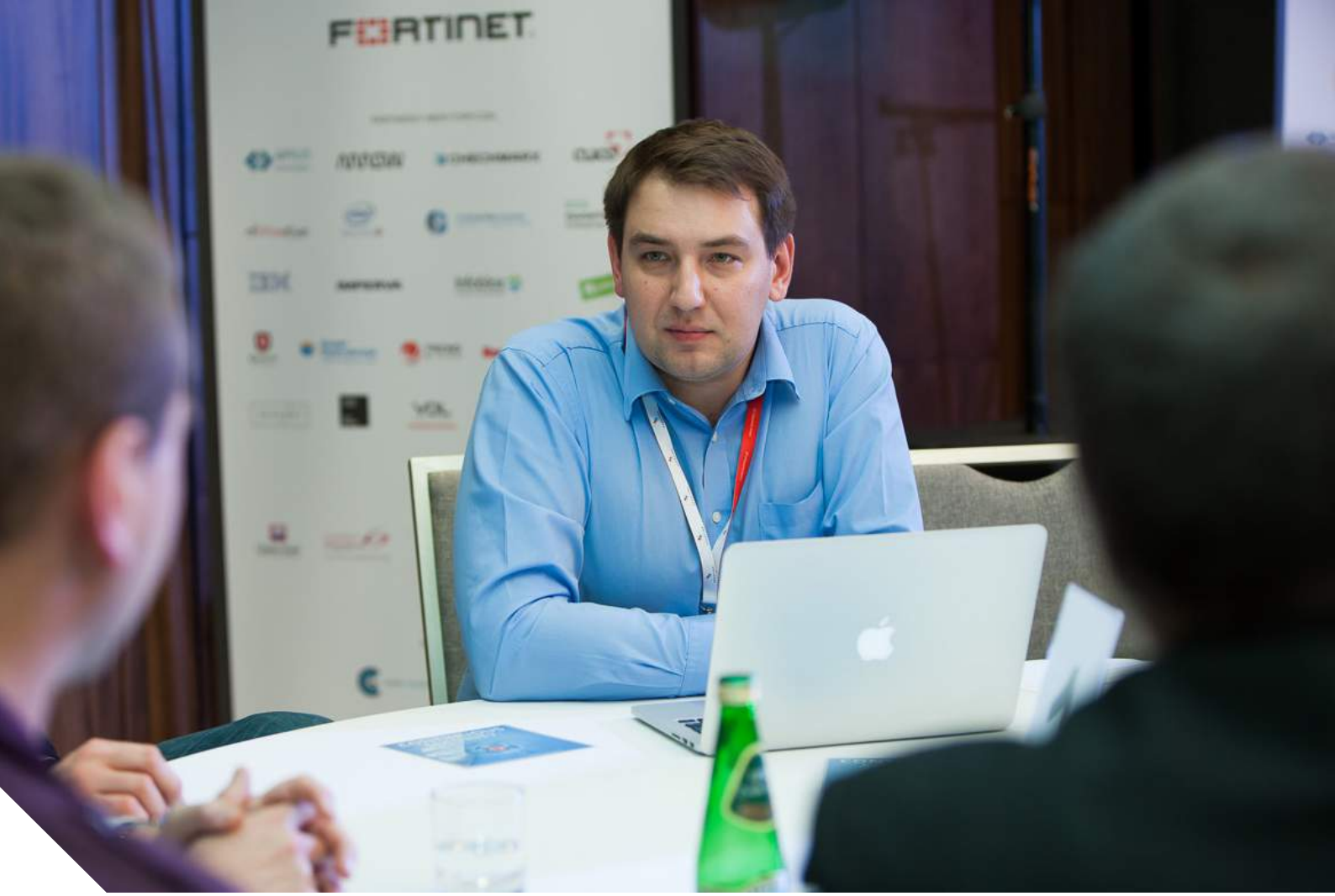
Jednym z punktów programu konferencji była debata o przyszłości bezpieczeństwa IT przeprowadzona na wzór debaty oksfordzkiej.

Zespół w składzie: Paweł Dobrychłop, ICT Security Manager w Dziale Bezpieczeństwa Teleinformatycznego w Polkomtelu i Cyfrowym Polsacie, Cezary Piekarski, dyrektor Departamentu Bezpieczeństwa i Ciągłości Biznesowej w Banku Millennium SA, oraz Krzysztof Szczepański, dyrektor Departamentu Bezpieczeństwa i Ryzyka w Krajowej Izbie Rozliczeniowej, bronił tezy, że przyszłość bezpieczeństwa to Security Managed Services, czyli specjalizacja kompetencji i outsourcing funkcji bezpieczeństwa do profesjonalnych zewnętrznych organizacji (w tym modelu wewnętrzne komórki bezpieczeństwa technologicznego zostaną zredukowane i ograniczone do obszaru kompetencji potrzebnych do zarządzania outsourcingiem w tym obszarze). Przeciwnikami tezy byli: Artur Ślubowski, kierownik Zespołu Bezpieczeństwa w PKP Informatyka, Piotr Kluczwajd, Regional Sales Manager w firmie Imperva, oraz Artur Barankiewicz, kierownik Wydziału Analiz i Strategii Bezpieczeństwa Systemów Teleinformatycznych w Orange Polska.

Oczywiście, zgodnie z konwencją był to podział umowny – chodziło o uwypuklenie argumentacji zwolenników i przeciwników tezy, a tak naprawdę o pobudzenie do myślenia o przyszłości cyberbezpieczeństwa i zainspirowanie uczestników. Kto wygrał, kto był bardziej przekonujący? Trudno powiedzieć, ale na pewno warto było posłuchać tej fascynującej dyskusji...

Sesje roundtables

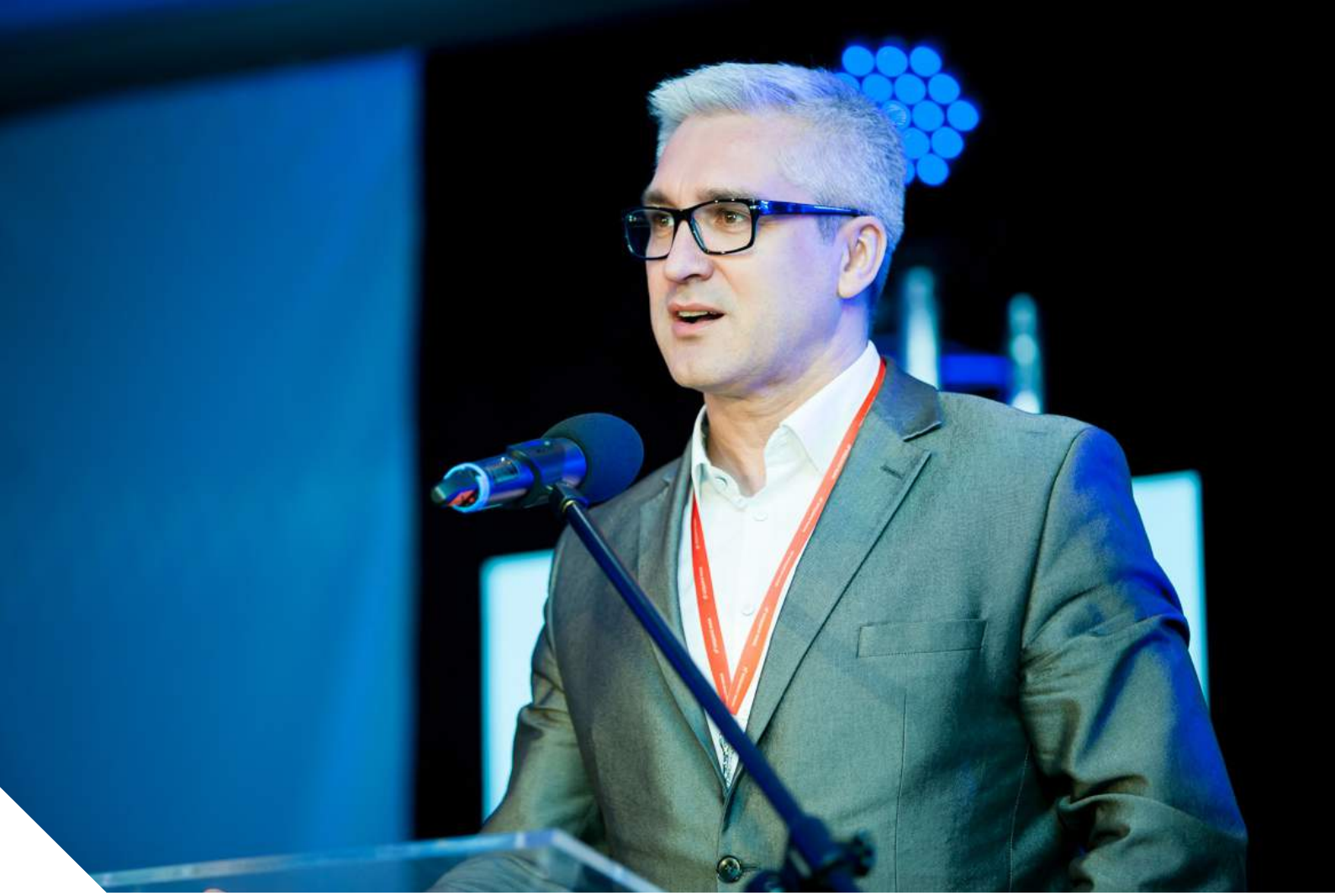
Równoległe dyskusje przy stolikach tematycznych to stały już element konferencji AT Summit, angażujący wszystkich uczestników. Spełniają one klika celów. Po pierwsze, umożliwiają bezpośrednią wymianę opinii i doświadczeń w ramach konkretnego zagadnienia, interesującego daną grupę uczestników. Po drugie dają możliwość spotkania i rozmowy z prowadzącym daną sesję – wybraliśmy bowiem do ich prowadzenia osoby o dużej wiedzy i doświadczeniu. Sesje roundtables przedstawiają bardzo szerokie spektrum tematów i cieszą się ogromnym zainteresowaniem uczestników konferencji.



Sesja: Zarządzanie bezpieczeństwem ICT w czasach Cloud Computing i Shadow IT

Prowadzenie: Andrzej Kleśnicki, Qualys

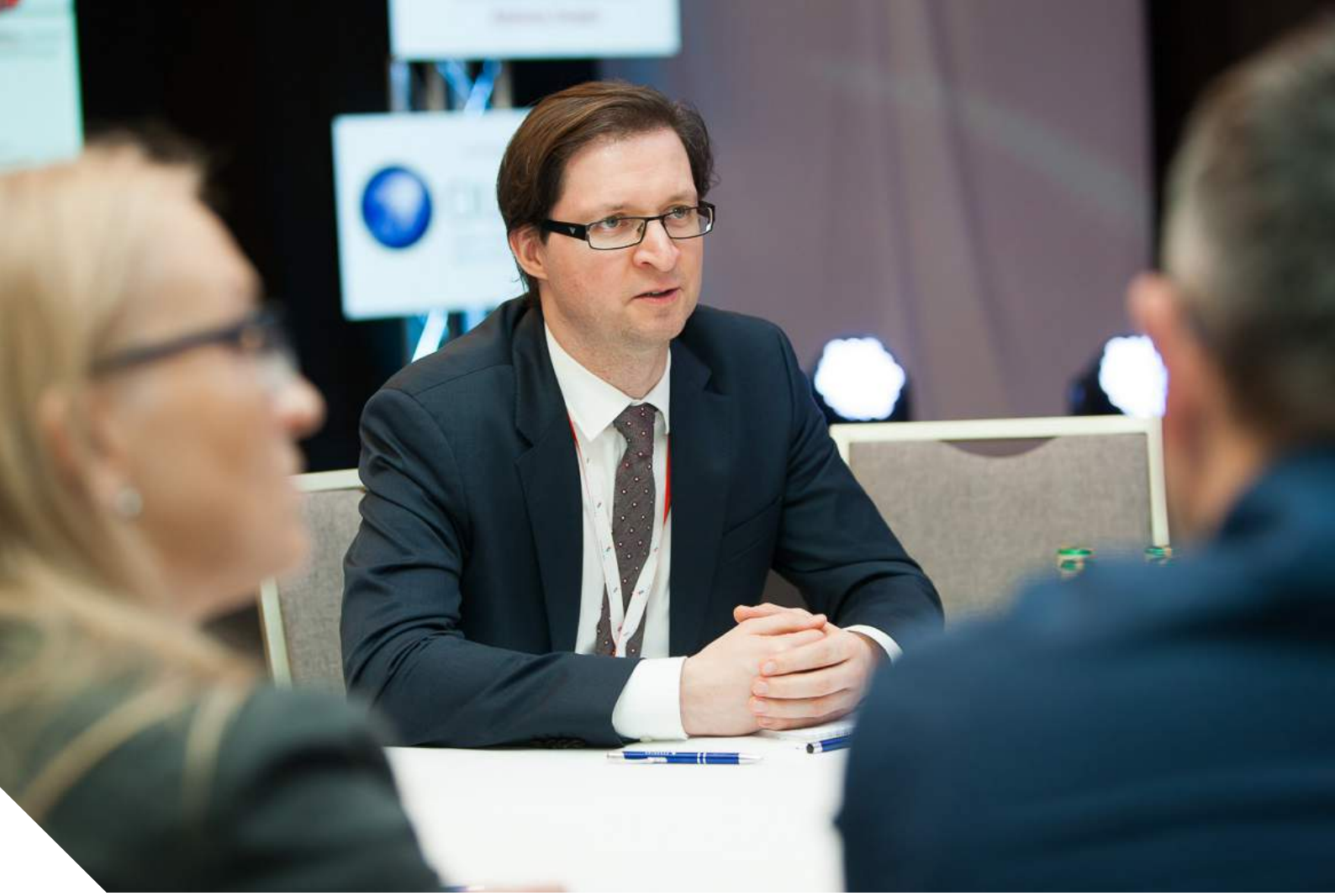
Czym jest *shadow IT*? To usługi i systemy informatyczne wykorzystywane przez użytkowników biznesowych poza wiedzą i oficjalną zgodą IT. Zjawisko jest ściśle związane z chmurą obliczeniową i mobilnością pracowników, ale nie jest nowe – występowało w postaci arkuszy kalkulacyjnych, w których przetwarzano ważne dane finansowe firmy. Obecnie wyrasta na jedno z poważniejszych zagrożeń bezpieczeństwa. Uczestnicy dyskusji zgodzili się, że blokowanie shadow IT nie jest rozwiązaniem, ponieważ oznacza to występowanie przeciw biznesowi. Informatyka powinna oferować usługi, które skutecznie konkurują z shadow IT. Remedium stanowi zintegrowany system bezpieczeństwa, edukacja pracowników i kompleksowe podejście do zasobów bez względu na to, gdzie one się znajdują – czy są lokalne czy w chmurze. Warto przy tym pamiętać, że choć chmura pozwala na minimalizowanie pewnych aspektów ryzyka, to ma ona – na co wskazywali uczestnicy dyskusji – słabe punkty w obszarach, takich jak: kontrola dostępu, zarządzanie kluczami i silna kryptografia.



Sesja: Kiedy już dojdzie do ataku, co robić?

Prowadzenie: Jacek Niedziałkowski, IBM Polska

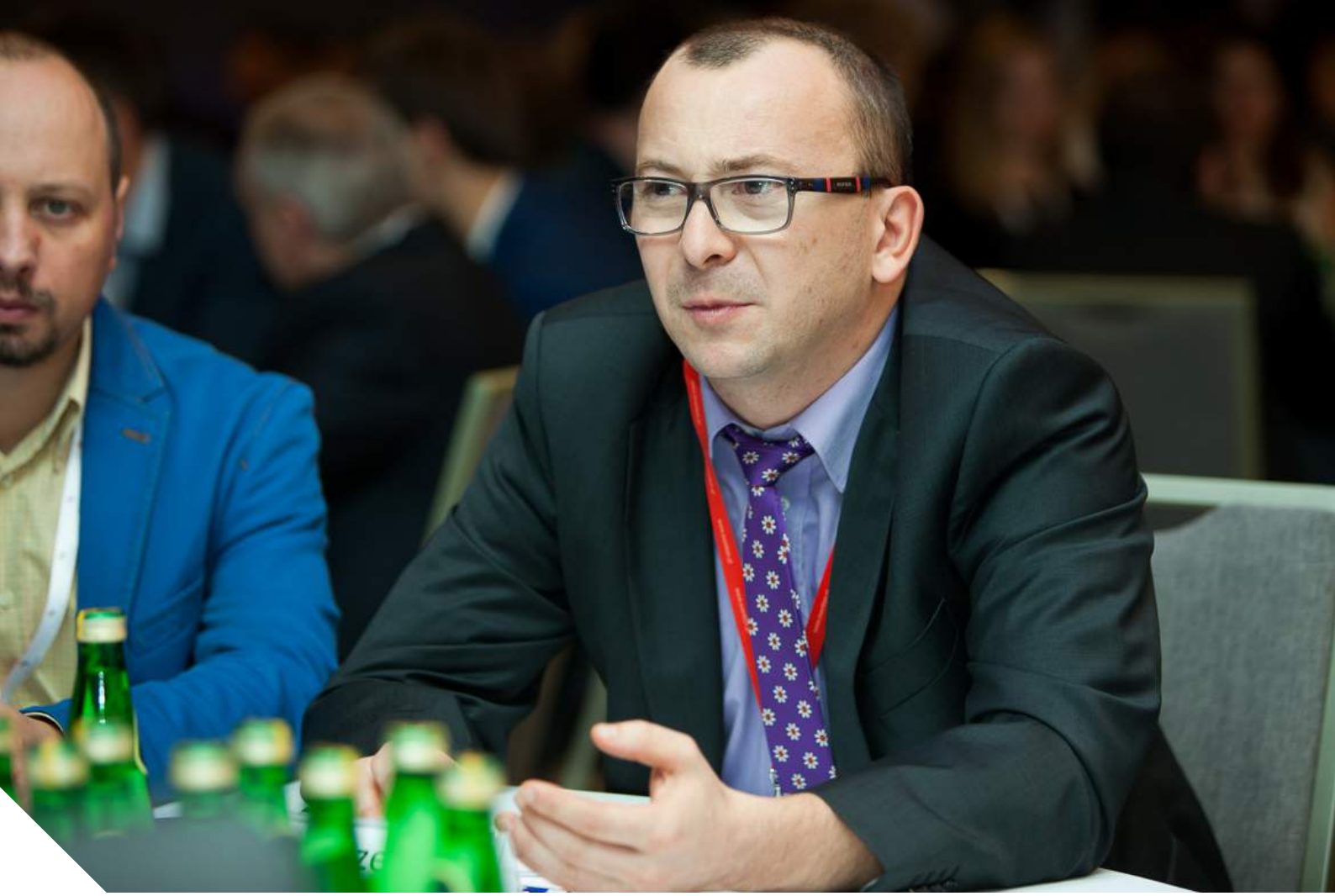
Jak należy zachowywać się w sytuacji naruszenia bezpieczeństwa? Jak się do tego przygotować? Dyskusja, podczas której omawiane były konkretne przypadki ataków, miała burzliwy charakter. Pierwszy i najważniejszy wniosek, na jaki zgodzili się uczestnicy, jest taki: w 2015 r. nie było organizacji, które mogła się czuć bezpiecznie. To oznacza, że wszyscy powinni się przygotować na atak. W związku z tym można rozważać, czy lepiej korzystać z zewnętrznego know-how, czy próbować tworzyć wewnętrzne zasoby eksperckie. Kluczowe jest jednak oparcie się na zdefiniowanej polityce bezpieczeństwa, która jest systematycznie aktualizowana. Konieczne jest stałe poszukiwanie nowych podatności w organizacji i dostosowywanie potencjalnych reakcji na atak. Przy tym niezwykle istotne jest, że jednostki odpowiedzialne za bezpieczeństwo muszą być odpowiednio umocowane w hierarchii organizacyjnej. Dzięki temu będą dysponować nie tylko kompetencjami, ale również odwagą i możliwościami podejmowania decyzji w sytuacji krytycznej.



Sesja: Czy w dobie zaawansowanych zagrożeń musimy budować własne zasoby do analityki złożonych incydentów bezpieczeństwa?

Prowadzenie: **Michał Bogucki, Wise Networks**

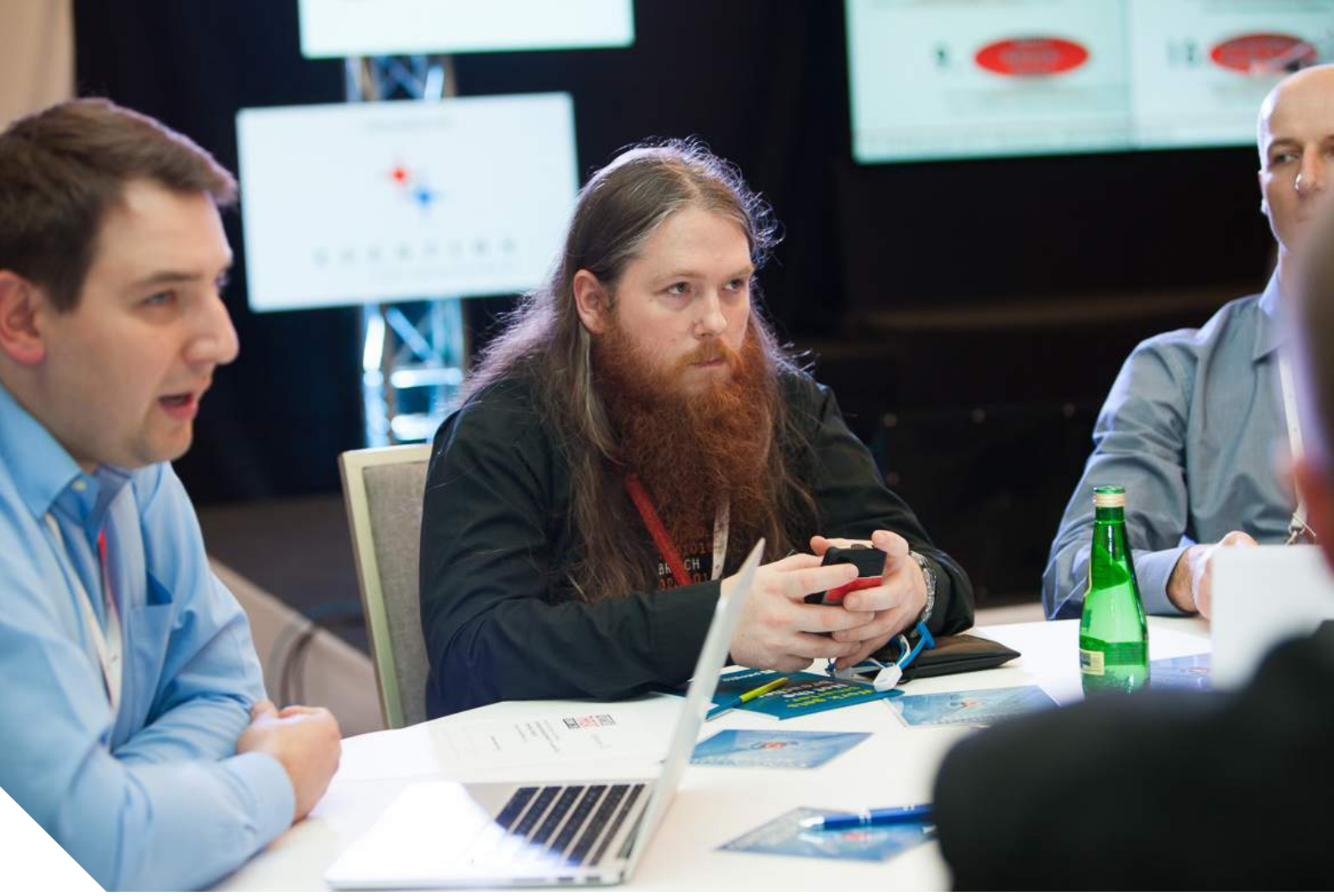
Czy warto wspierać analizę skomplikowanych incydentów bezpieczeństwa w organizacji przy wykorzystaniu zewnętrznych usług eksperckich? Czy może lepiej mieć własne zasoby i narzędzia? Dyskusja pokazała, że przez narzędzia analityczne rozumie się przede wszystkim systemy klasy SIEM. Wiele organizacji wdraża je. Uczestnicy wskazali jednak, że to nie wystarczy; organizacje powinny dzielić się wiedzą na temat zagrożeń i możliwych reakcji na nie, ponieważ to w istotny sposób przyczyniłoby się do opracowania i rozpowszechniania scenariuszy bezpieczeństwa do implementacji w systemach SIEM. Dzięki temu koszty opracowania takich scenariuszy rozłożyłyby się na większą grupę firm. Jednocześnie oznaczałoby to pożądany wzrost kosztów po stronie przestępców i mniejszą opłacalność ich działań – opracowywane przez nich wektory ataku musiałyby być bardziej skomplikowane. Gdyby taki scenariusz udało się zrealizować, wsparcie firm zewnętrznych byłoby wskazane tylko w przypadku najbardziej skomplikowanych incydentów bezpieczeństwa. To podstawowy obszar wykorzystania usług eksperckich – wyjątkowe sytuacje, w których należy wykorzystać bardziej zaawansowane narzędzia analityczne niż SIEM.



Sesja: DNS – ostatnie ogniwo niebezpieczeństwa

Prowadzenie: Rafał Szewczyk, CEE, Infoblox

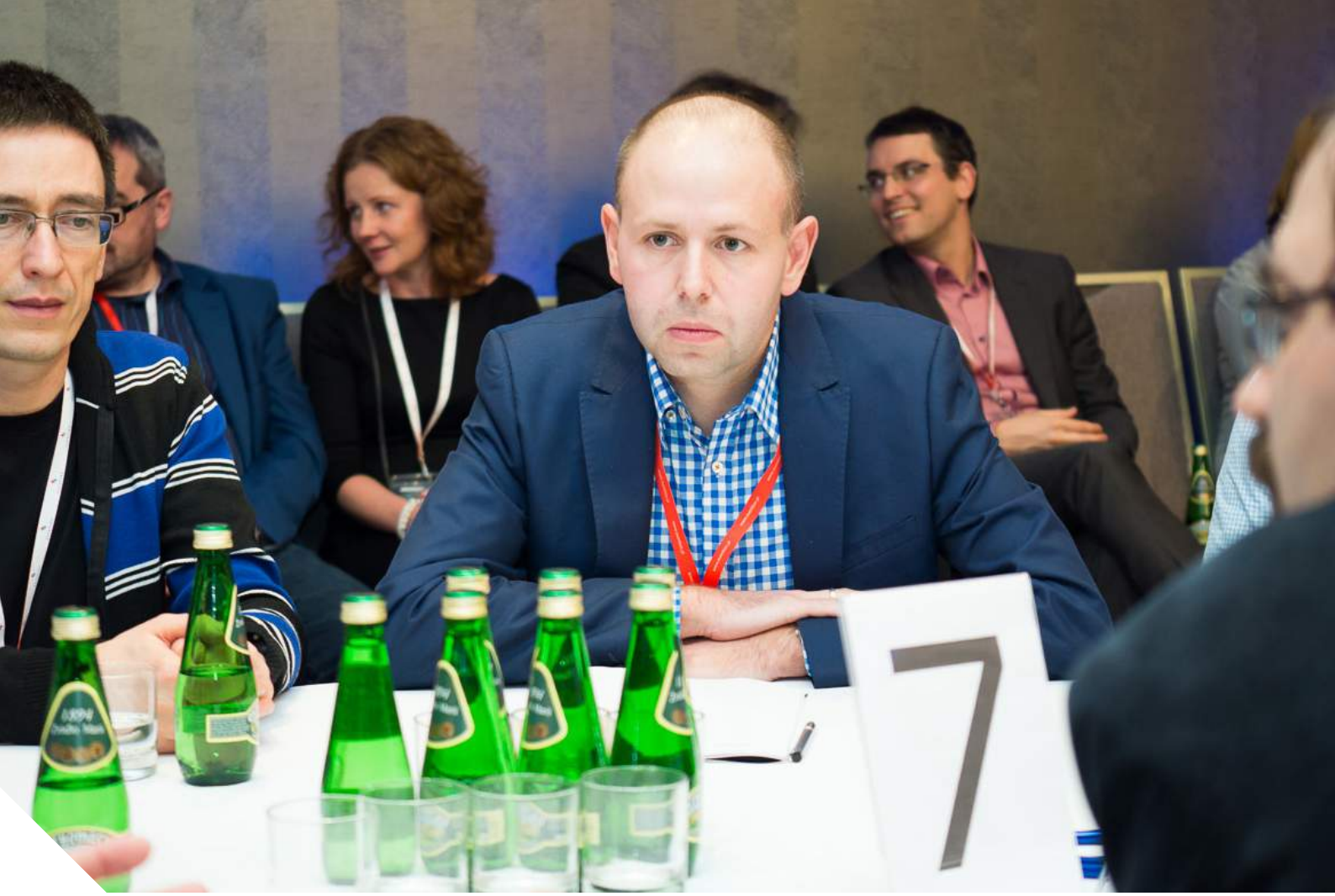
Czy organizacje zdają sobie sprawę, jakie ataki DNS-owe mogą je spotkać? Co się dzieje, kiedy DNS nie działa? Nie wszyscy wiedzą, że większość zarejestrowanych domen przez pierwsze 24 godziny nie służy do tego, żeby serwować wiadomości, ale stają się wektorem ataku. W trakcie dyskusji omówione zostały wszystkie zakresy DNS-ów – publiczny, wewnętrzny i wewnętrzny, który wychodzi do Internetu – oraz sposoby ich zabezpieczenia. Mówiono m.in. o zagrożeniu związanym z tunelowaniem w DNS, jego wpływem na organizację oraz możliwościami, jakie otwiera do wydobycia informacji o firmie, danych finansowych czy innych sekretów firmowych. Cześć dyskusji skoncentrowała się wokół protokołu DNSSEC, o którym – podobnie jak o yeti – większość słyszała, ale którego nikt nie widział. Rozmawialiśmy nie tylko o tym, czym jest DNSSEC, ale także dlaczego nie jest rozpowszechniony w Polsce w kontekście działań z zakresu bezpieczeństwa. Dla porównania wskazane zostały kraje, takie jak Szwecja i Holandia, a także Czechy, gdzie ten protokół jest bardzo rozpowszechniony, a instytucje rządowe są wręcz zobowiązane do jego wykorzystania.



Sesja: Ofensywne czy defensywne podejście do bezpieczeństwa systemów informatycznych

Prowadzenie: Andrzej Kleśnicki, Qualys

Ofensywne podejście do zagadnień bezpieczeństwa polega na wykorzystywaniu wiedzy i narzędzi do aktywnego wykrywania, naśladowania i izolowania intruzów. Warto przy tym zauważyć, że to, co jeszcze kilka lat temu uznawane było za podejście ofensywne, dzisiaj zalicza się do metod defensywnych – systemy typu antywirus, antymalware, IPS czy skanery podatności. W trakcie dyskusji uczestnicy zgodzili się, że narzędzia ofensywne istnieją przede wszystkim po to, żeby dostarczać informacji do obrony; to typowe podejście – budujemy naszą obronę na podstawie wiedzy z ataków. Jednocześnie uczestnicy uznali za godne podkreślenia, że działania w obszarze bezpieczeństwa należy odpowiednio priorytetyzować: nie ma sensu przygotowywać się na atak Zero Day, jeśli w naszym środowisku są dziury znane od miesięcy. Dlatego tak ogromne znaczenie ma podstawowa „higiena" – systemy muszą być zaktualizowane, żeby wyeliminować podatności, które mogą być wykorzystane. Dopiero to pozwala myśleć o podejmowaniu kolejnych kroków.



Sesja: Rola systemów klasy Sandbox w ochronie przed zaawansowanymi atakami

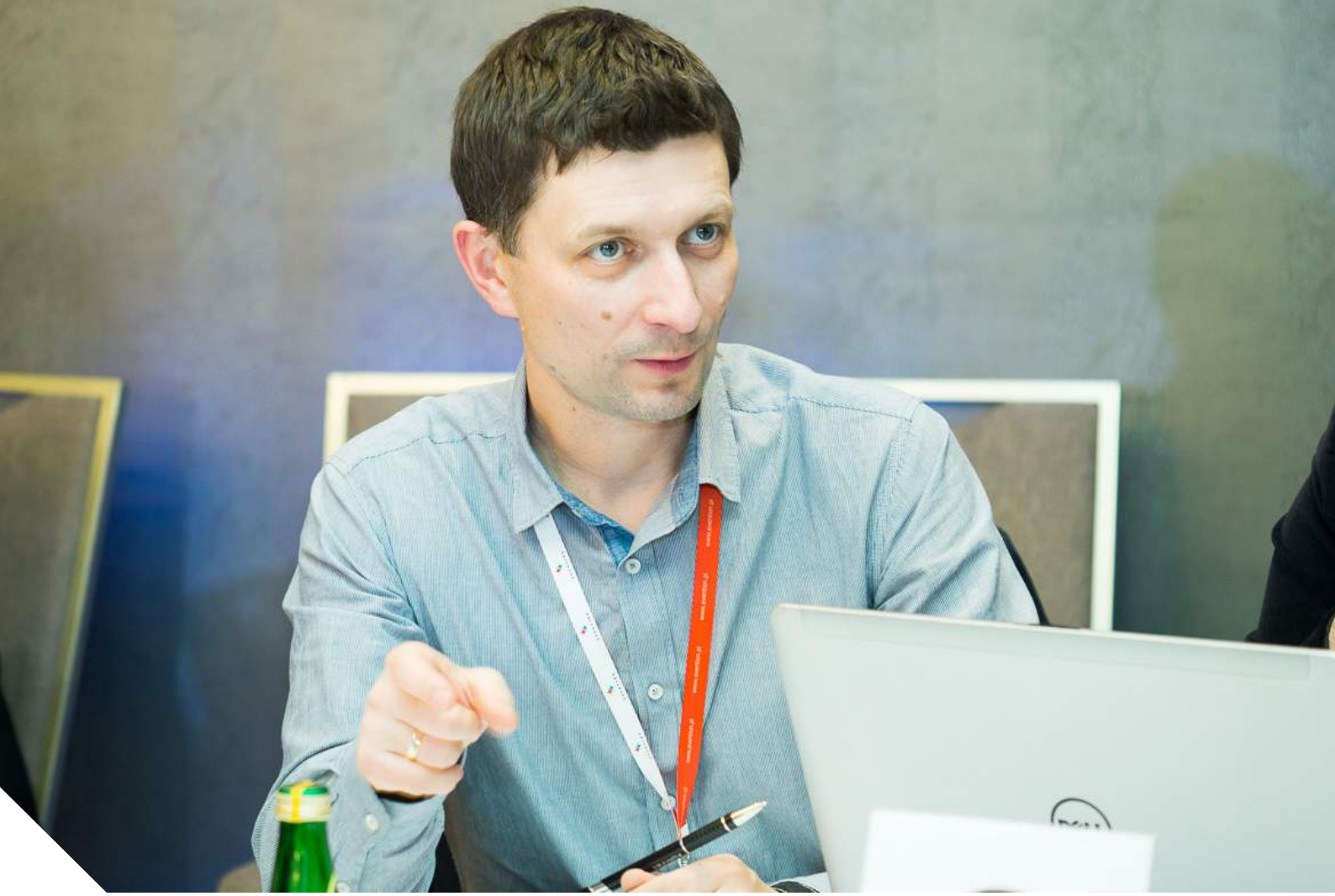
Prowadzenie: Bartosz Chmielewski, Intel Security

Choć nie są pozbawione wad, systemy Sandbox oferują wyższą skuteczność niż mechanizmy działające na bazie sygnatur. Dlatego stanowią dla nich dobre uzupełnienie. W związku z tym, że stają się coraz bardziej popularne na rynku, twórcy złośliwego kodu starają się uodpornić swoje działa na wykrycie. Czy system Sandbox może zastąpić ręczną analizę? Uczestnicy dyskusji zgodzili się, że nie. Nie daje tak dokładnych rezultatów, ale jednocześnie o wiele lepiej sprawdzi się w przypadku automatycznej oceny brzegu sieci. Jak zatem najlepiej wykorzystać wyniki systemów Sandbox poza analizowaniem generowanych przez nie raportów? Przede wszystkim tzw. IOC (*Indicators of Compromise*) mogą być wykorzystane przez systemy SIEM lub przez systemy typu EDR, które potrafią analizować symptomy na stacjach końcowych albo w warstwie infrastruktury. Jednocześnie uczestnicy zwrócili uwagę, że zagadnienie *false positives* i *false negatives* ma w przypadku systemów Sandbox większe znaczenie niż w przypadku systemów sygnaturowych, ponieważ rzutuje na zaufanie do narzędzia.

Sesja: Wilk w owczej skórze – jak zapobiec utracie danych i obniżeniu wiarygodności firmy?

Prowadzenie: Mariusz Przybyła, Quest Dystrybucja

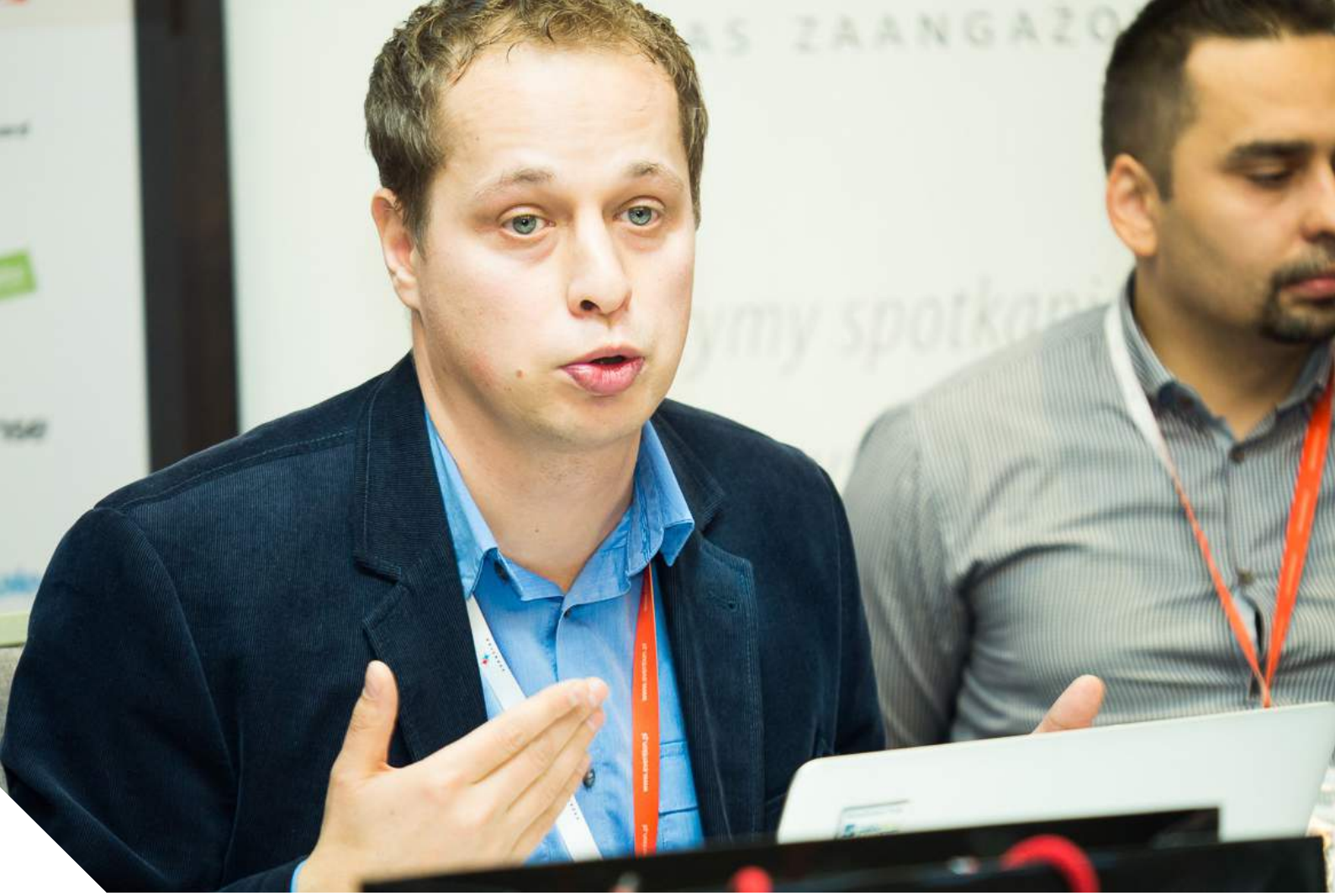
Czy monitorowanie sesji użytkowników uprzywilejowanych to dobry sposób na zwiększenie poziomu bezpieczeństwa w organizacji, w której dostęp do kont uprzywilejowanych musi być zawsze zachowany? Uczestnicy dyskusji zgodzili się, że można to traktować tylko jako element bardziej kompleksowych działań. Takie monitorowanie ma głównie wartość dowodową po wykryciu nadużycia czy nieautoryzowanego działania użytkownika w organizacji. Kompleksowe działania powinny być prowadzone przy użyciu narzędzi, które udostępniają informacje o zachowaniu użytkownika. Przy tym powinny one działać nie na zasadzie programowania konkretnych ścieżek, ale raczej wykrywania anomalii wskazujących na nieprawidłowe zachowania. Warto również pamiętać, że równie ważne jest połączenie mechanizmów zarzadzania kontami uprzywilejowanymi w całym cyklu funkcjonowania pracownika w organizacji.



Sesja: Jak efektywnie zaadresować bezpieczeństwo sieci w obliczu zaawanasowanych zagrożeń?

Prowadzenie: Robert Dąbrowski, Tomasz Jaglana, Fortinet

Intencje przestępców atakujących naszą firmę mogą być różne: od standardowych, czyli takich jak chęć zdobycia cennych danych czy wywarcie negatywnego wpływu na reputację firmy, przez żal pracownika, który czuje, że został niesłusznie zwolniony, aż po chęć wykorzystania elementu naszej infrastruktury do ataku na inne organizacji. Mając to na uwadze, zastanawialiśmy się wspólnie z uczestnikami dyskusji, czy elementy ich sieci znajdują się pod odpowiednią ochroną. Zgodziliśmy się, że odpowiedź na to pytanie wymaga zlokalizowania krytycznych elementów infrastruktury i przeprowadzenia dokładnej analizy wewnętrznej. Przy tym wszyscy podkreślali wartość audytów prowadzonych przez zewnętrznych specjalistów, ponieważ to jedyny sposób na obiektywne spojrzenie na organizację – ukazują to, czego nie widzą osoby z wewnątrz. Na koniec zgodziliśmy się również, że polityka bezpieczeństwa powinna stale ewoluować, podobnie jak powinny podlegać zmianom i aktualizacji środki oraz metody wykrywania nowych zagrożeń.



Sesja DEMO: Prześledź z nami cykl życia ataku hakerskiego

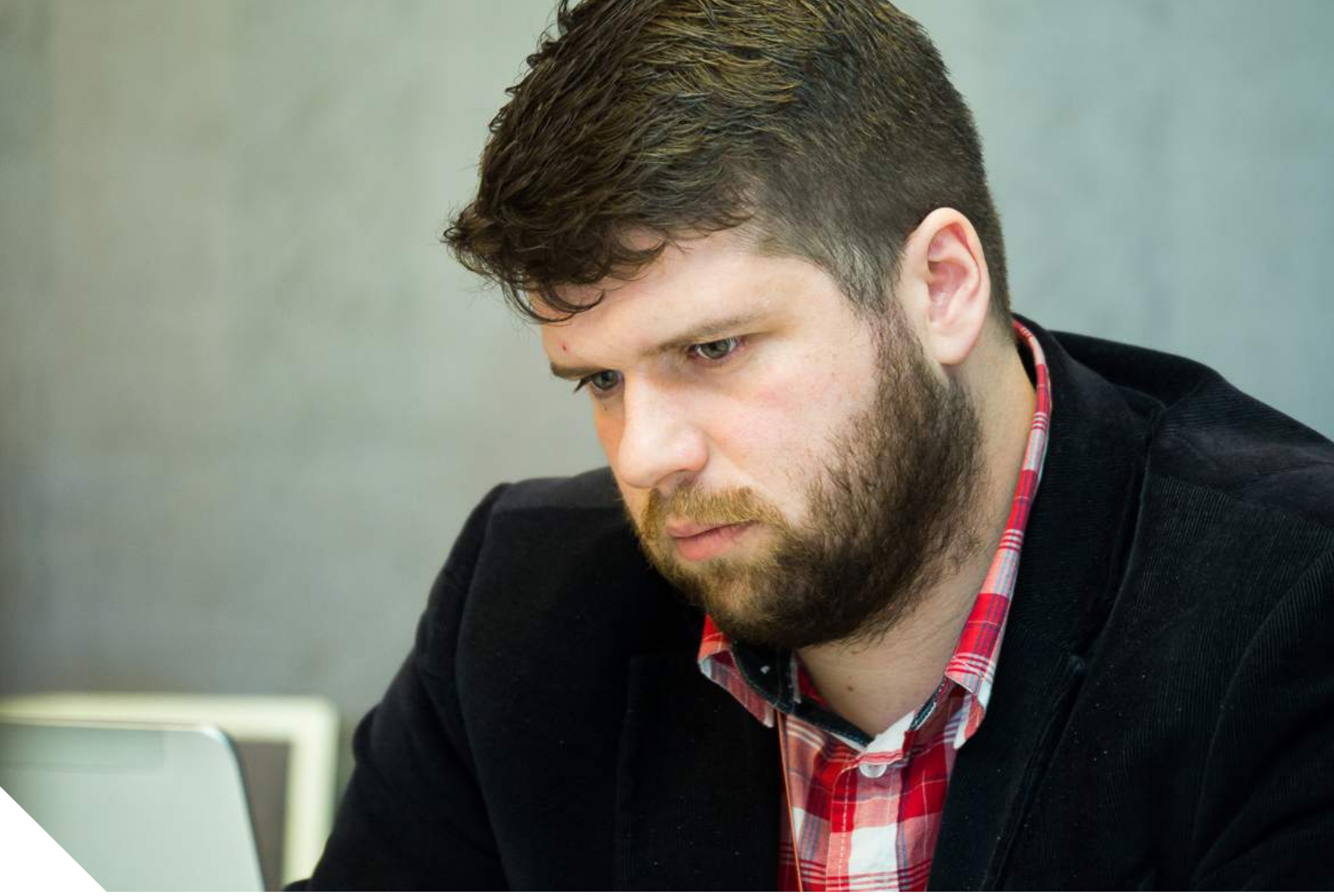
Prowadzenie: Seweryn Jodłowski, Ewa Śniechowska, Palo Alto Networks

Przeprowadzone demo pokazało, że niezwykle trudno jest w 100% zabezpieczyć się przed każdym rodzajem zagrożenia. Jeśli jednak mamy dobrze skonfigurowane rozwiązanie bezpieczeństwa, możemy być pewni, że minimalizujemy ryzyko ataku i wycieku danych. Najważniejsze wnioski, do jakich doszli uczestnicy dyskusji, dotyczyły uwarunkowań skutecznego reagowania na ataki: jeśli posiadamy dostęp do skonsolidowanych logów, a także jeśli podchodzimy do zabezpieczeń w sposób platformowy, to o wiele łatwiej jest nam zarządzać polityką bezpieczeństwa i mamy większe możliwości dynamicznego reagowania na to, co dzieje się w sieci.

Sesja DEMO: Zaawansowana ochrona stacji końcowych

Prowadzenie: Seweryn Jodłowski, Ewa Śniechowska, Palo Alto Networks

Jak skutecznie zabezpieczyć się przed bardziej zaawansowanymi atakami, z którymi tradycyjne rozwiązania, np. antywirusowe, sobie nie radzą? Jak przygotować się na zaawansowane zagrożenia, które trudno rozpoznać i wykryć nawet przy wykorzystaniu rozwiązań typu Sandbox? Dyskusja potwierdziła, że coraz więcej firm jest świadomych ograniczeń wykorzystywanych metod i narzędzi, a jednocześnie dostrzega potrzebę wychodzenia poza tradycyjne rozwiązania bezpieczeństwa. Dlatego na rynku pojawia się coraz silniejszy trend przesuwania ochrony przed zaawansowanymi atakami APT na stacje końcowe. Zwróciliśmy uwagę, że wymaga to zaimplementowania rozwiązań, które zabezpieczą przed technikami, jakich osoba atakująca może użyć, wykorzystując daną podatność.



Sesja: Rekomendacje i dobre praktyki w ochronie infrastruktury krytycznej

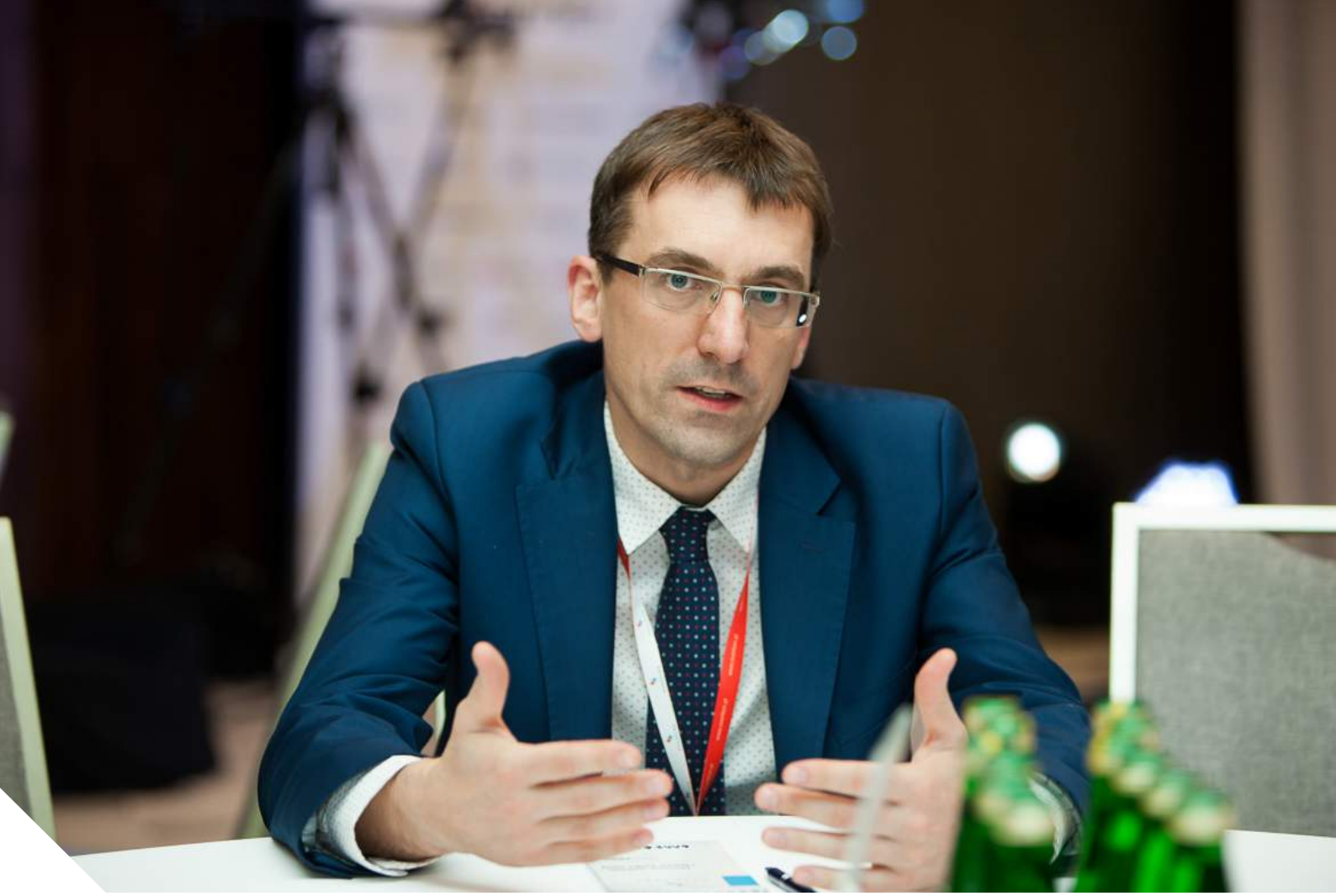
Prowadzenie: Kamil Kowalczuk, PGE

Dyskusja, zdominowana przez przedstawicieli firm energetycznych, koncentrowała się wokół kilku zagadnień, m.in.: zmiany podejścia do infrastruktury krytycznej, punktów szczególnie podatnych oraz fizycznego rozdzielenia systemów automatyki przemysłowej. Uczestnicy zgodzili się, że prezentowane w obowiązujących dokumentach tzw. podejście obiektowe powoli ewoluuje do funkcjonalnego. To dobra zmiana, ponieważ pozwoli np. na zmapowanie elementów systemów automatyki przemysłowej, które znajdują się poza zgłoszonym obiektem. Jeśli chodzi o punkty szczególnie podatne – zidentyfikowano je jako miejsca międzyoperatorskiej wymiany danych, dostępu do sieci publicznej i dostępu stron trzecich, a także punkty styku z systemami wewnętrznymi – to problem stanowi brak wytycznych i dokumentów formalnych. To się jednak zmieni, ponieważ powstaje zespół sektorowy, który wypracuje wytyczne. Ważnym tematem było także fizyczne rozdzielenie systemów sterowania, automatyki przemysłowej. Uczestnicy zastanawiali się, czy to dobra praktyka. Większość z nich zgodziła się, że osiągane dzięki temu bezpieczeństwo jest pozorne, a budowanie rozdzielenia fizycznego w dzisiejszych realiach jest kłopotliwe, a czasem nawet niemożliwe, bo nie pozwala na pełne monitorowanie obszaru automatyki przemysłowej.

Sesja: Jak sobie radzić z phishingiem przy ograniczonych zasobach?

Prowadzenie: Grzegorz Cenkier, Poczta Polska

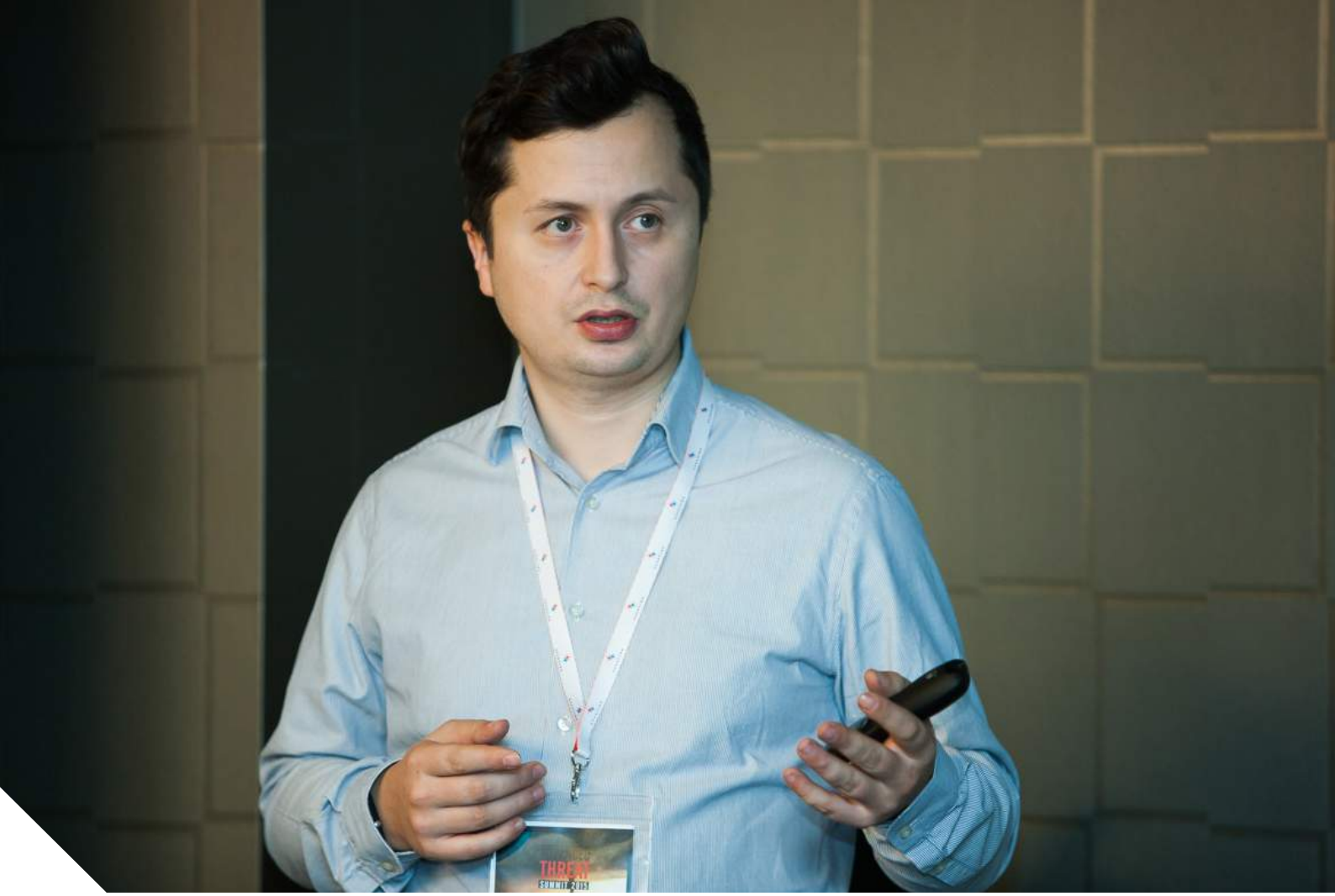
Niezwykle istotną kwestią w przypadku phishingu jest edukacja i informacja. W przypadku firm i instytucji można obserwować ruch na bramkach pocztowych i odpowiednio ostrzegać. Jeśli chodzi o klientów indywidualnych, to jest znacznie trudniej. Przykładowo, miliony osób otrzymują wiadomości, których nadawca podszywa się pod Pocztę Polską. Można o tym informować na stronie internetowej oraz w urzędach pocztowych. Jednak walka z phishingiem jest tak trudna przede wszystkim dlatego, że istnieją luki w systemie prawnym. Przez to działania ofensywne, które czasem są podejmowane, mogą być traktowane jako łamanie prawa. Zmiany w prawie to pierwszy krok na drodze do poprawienia sytuacji: osoba, która odpowiada za phishing, nie wysyła nam e-maila, bo chce nas o czymś poinformować, ale próbuje dokonać oszustwa.



Sesja: Outsourcing i leasing pracowników a bezpieczeństwo IT

Prowadzenie: Grzegorz Długajczyk, ING Bank Śląski

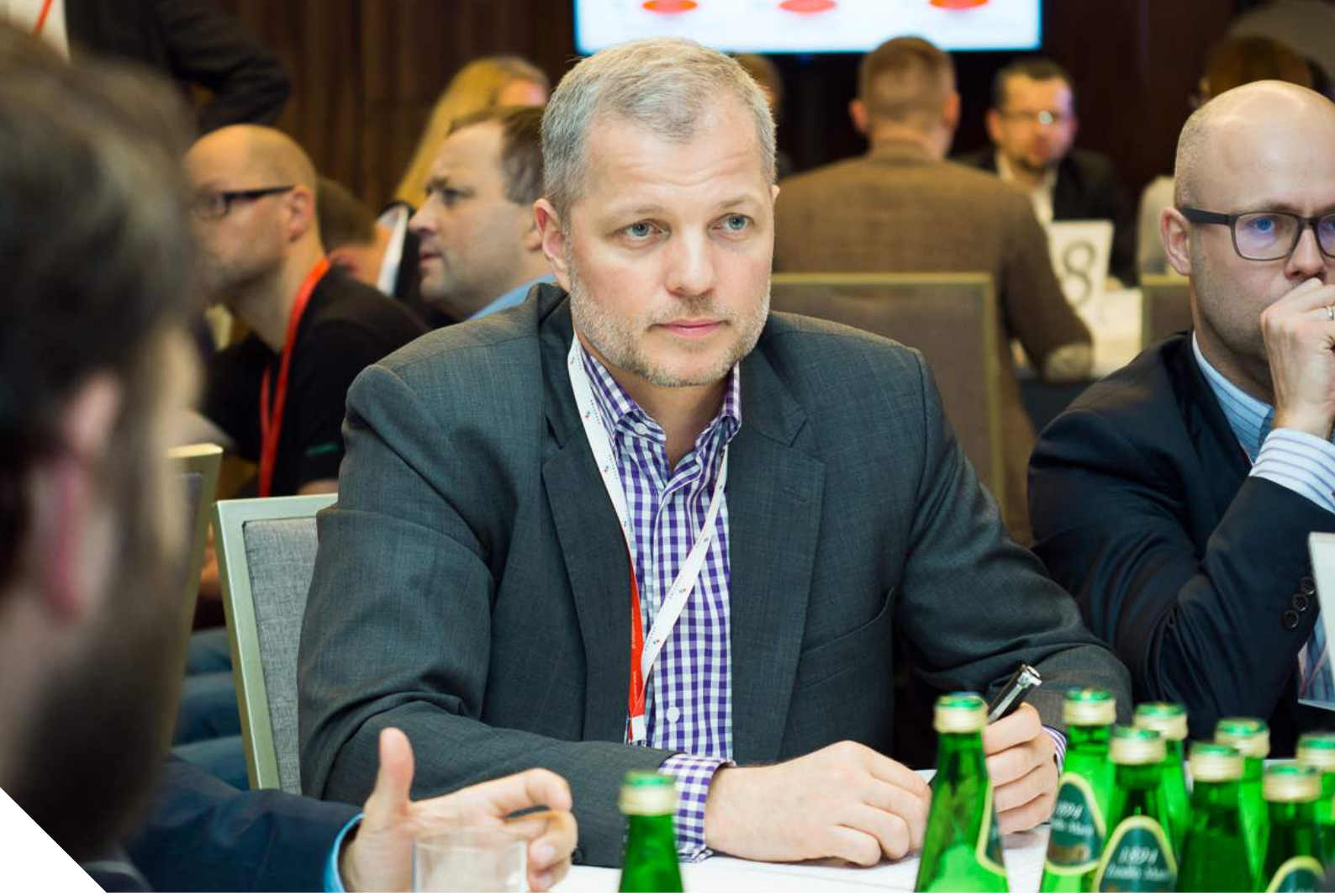
W trakcie dyskusji zastanawialiśmy się wspólnie, jak podejść do zagadnienia outsourcingu i bodyleasingu pracowników, żeby zapewnić bezpieczeństwo. Pierwszym krokiem jest wykonanie klasyfikacji danych dla usług i procesów, które chcemy outsourcować. Dzięki temu w kolejnym kroku można odpowiednio skonstruować klauzule umowne, określające, kto i do czego ma dostęp. Trzeba jednak odpowiedzieć sobie na pytanie, w jaki sposób chronić dane udostępniane zdalnie, a także zapewnić sobie prawo do audytu. W umowach powinna zostać zapisana możliwość kontrolowania wypełniania ustaleń. ING Bank Śląski zwraca także szczególną uwagę na rozwiązywanie umów i kontraktów outsourcingowych w kontekście bezpieczeństwa informacji, które zostały powierzone firmie w zakresie usług świadczonych dla klientów – jeśli nie są one już potrzebne, muszą zostać trwale usunięte.



Sesja: Reagowanie po incydentach – jak to komunikować

Prowadzenie: Marek Gieorgica, CCG

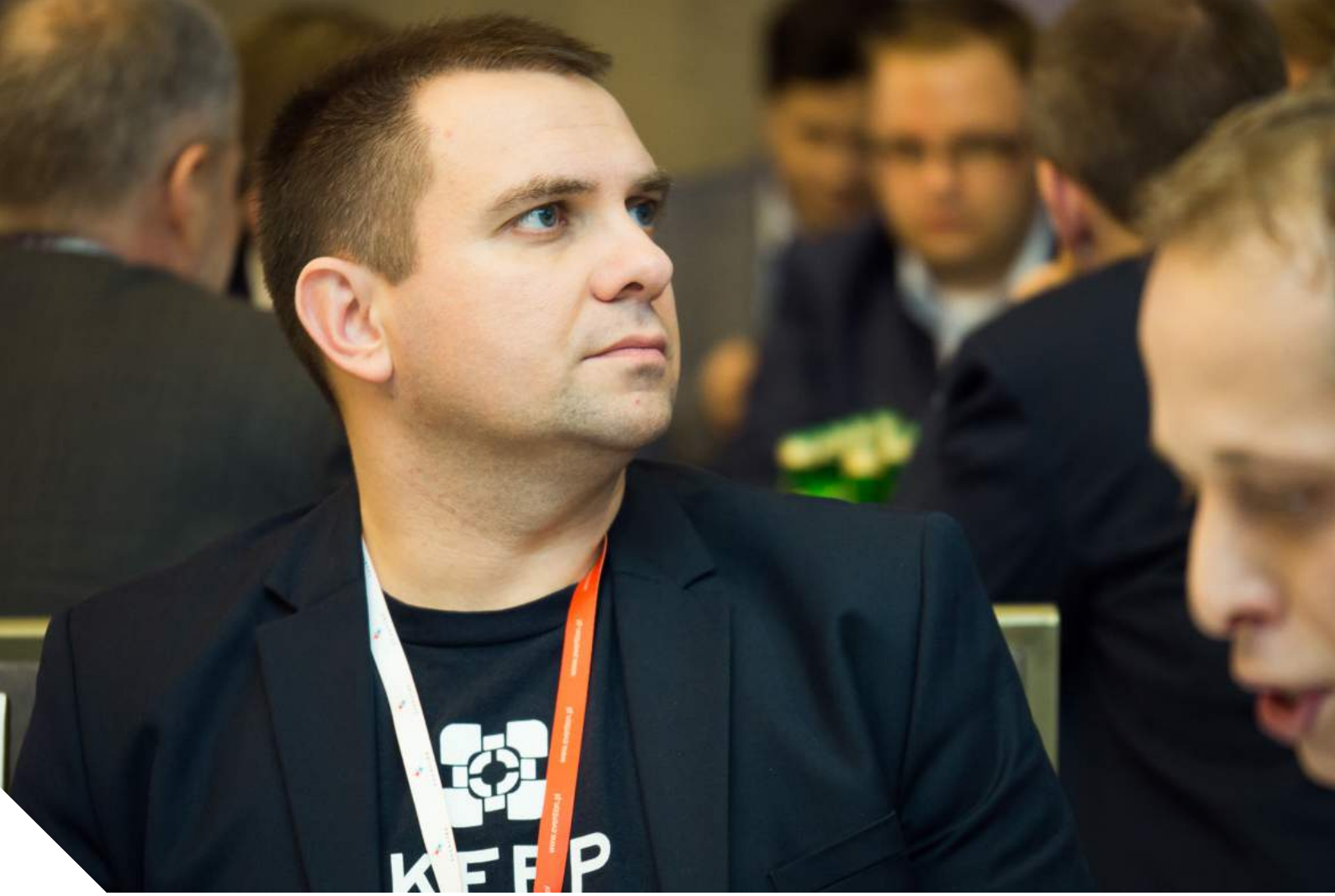
Chociaż wszyscy, jako specjaliści od bezpieczeństwa, jesteśmy świadomi ryzyka, zagrożeń i nieuchronności, jaka tym zagrożeniom towarzyszy, to przed nami jeszcze dużo pracy w zakresie edukacji pracowników i klientów. Te działania powinny objąć także dziennikarzy, którzy mają tendencję do nadawania pewnym incydentom w obszarze cyberbezpieczeństwa nazbyt sensacyjnego wydźwięku. To z jednej strony negatywnie wpływa na podejście zwykłych ludzi do technologii informatycznych, a z drugiej utrudnia pracę ekspertom mającym za zadanie ochronę przed zagrożeniami. Uczestnicy dyskusji zgodzili się, że kluczem do edukacji dziennikarzy jest używanie zrozumiałego dla nich języka; nie można wykorzystywać specjalistycznych terminów, bo oni tego nie rozumieją.



Sesja: Ochrona i audyt dostępu do kluczowych informacji oraz aplikacji w firmach i organizacjach

Prowadzenie: Piotr Kluczwajd, Imperva

W trakcie dyskusji zastanawialiśmy się, dlaczego w ogóle realizuje się projekty, które służą monitorowaniu dostępu do danych wrażliwych. Czy biznes rozumie taką potrzebę? Co powinniśmy zrobić, żeby z sukcesem takie projekty realizować? Doszliśmy do wniosku, że głównym powodem jest ochrona przed intruzami, dostawcami, osobami niepowołanymi, ale jednocześnie zabezpieczenie przed karami, jakie może nałożyć na organizację GIODO czy KNF za nieprzestrzeganie prawa. Projekty w tym obszarze dostarczają administratorom dowodu, że nie są odpowiedzialni za problemy; utwierdzają także organizacje w tym, że działają zgodnie z wytycznymi np. ustawy o ochronie danych osobowych.



Sesja: Techniki ochrony przed zaawansowanym malware

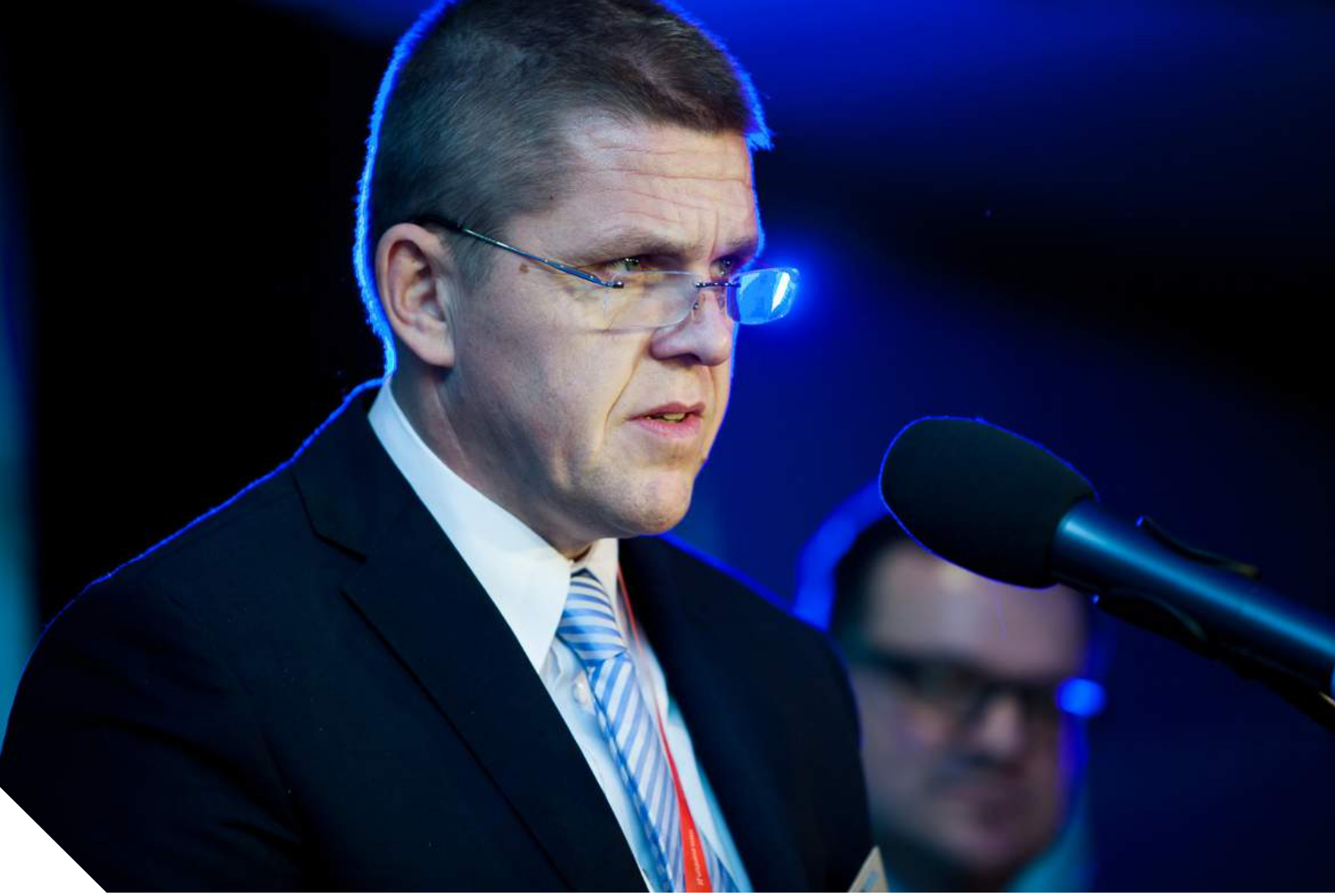
Prowadzenie: Mariusz Sawczuk, Sevenet

Poza „detonacją" w wirtualnych środowiskach, czyli *sandboxingiem* (niestety, bywa on obchodzony przez a*dvanced malware*), najlepsze efekty często dają metody podstawowe: blokowanie przesyłania plików czy kontrola plikowa. Z dyskusji wynikało, że część firm blokuje pobieranie plików wykonywalnych, ale część – nie. To oznacza, że ta druga grupa ma ograniczone możliwości zwalczania *advanced malware*. Ważnym elementem systemu ochrony jest także szyfrowanie ruchu. Jeśli tego nie robimy, możemy być pewni, że osoby atakujące zaszyfrują ruch do stacji ofiary. Warto pamiętać, że do zarażenia zawsze dochodzi na stacji końcowej. Jeśli organizacja nie dysponuje rozwiązaniem Endpoint Security nowej generacji, będzie jej trudno poradzić sobie z zaawansowanym złośliwym kodem.

Sesja: Systemy SIEM – czy warto je stosować i kiedy

Prowadzenie: Piotr Boetzel, Intel Security

Wdrożenie systemu SIEM jest trudne, a żeby było udane i system spełniał swoją rolę, muszą być spełnione dwa warunki: trzeba wybrać partnera, który ma doświadczenie i kompetencje oraz precyzyjnie zdefiniować potrzeby i oczekiwania. Jeśli wiemy, czego chcemy, jakie przygotowaliśmy scenariusze użycia, to wtedy mamy szansę je spełnić. W trakcie sesji zgodziliśmy się także, że system SIEM musi być modyfikowany wraz ze zmianami zachodzącymi w środowisku IT. Dyskutowaliśmy też o różnych modelach wdrożenia systemu SIEM: zespół i narzędzie należące do firmy, częściowy outsourcing – zewnętrzna firma obsługująca system klienta lub outsourcing pełny – narzędzie i zespół zewnętrznego partnera. Wybór rozwiązania zależy od sytuacji. Im większa organizacja, tym większe możliwości zbudowania kompetencji potrzebnych do samodzielnego utrzymania systemu. Gdy firma i zespół IT są małe, to preferowana jest zwykle współpraca z zewnętrznym partnerem.



Sesja: Czy można się przygotować do obrony swojej organizacji?

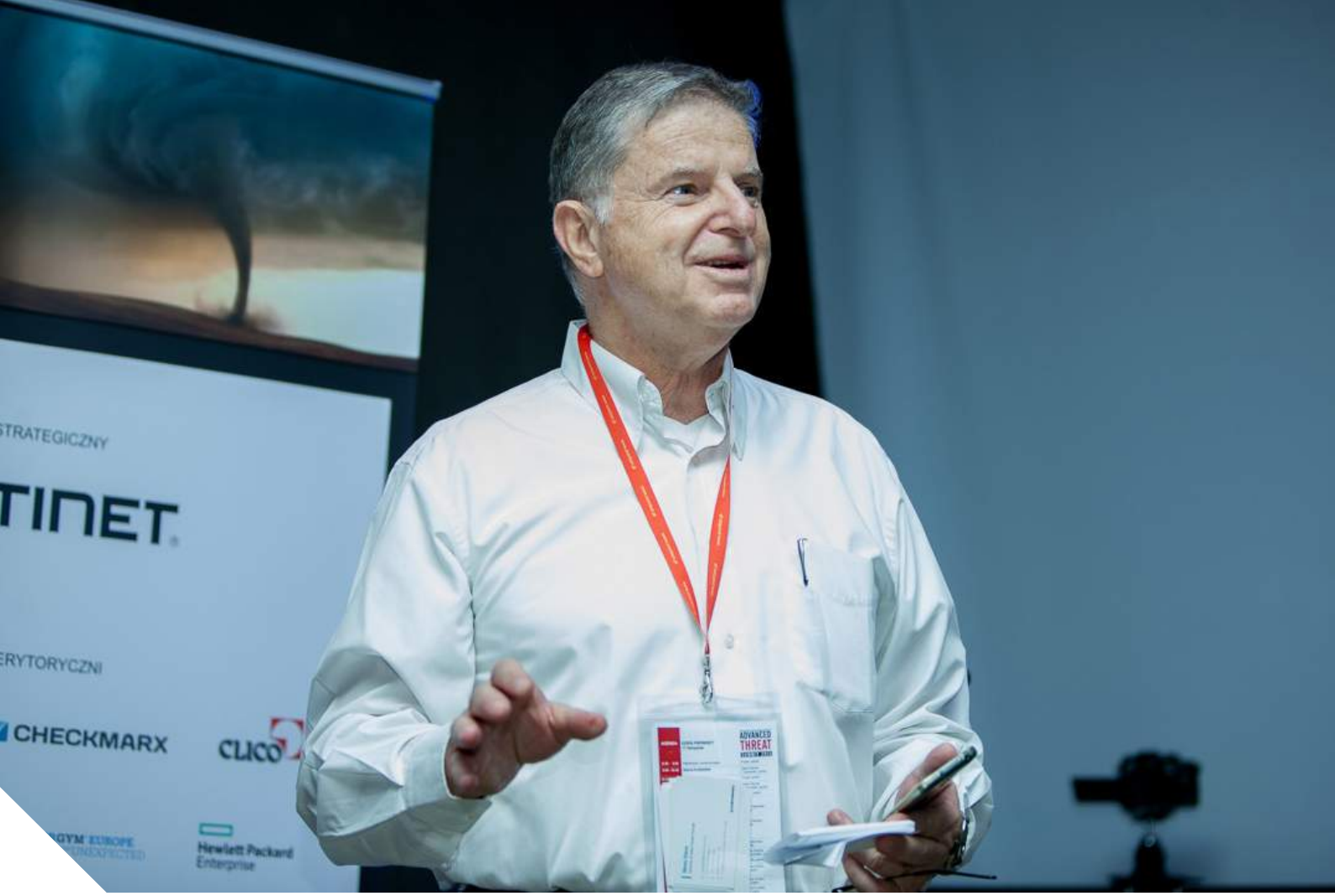
Prowadzenie: Martin Ingr, CyberGym Europe

Na kompletny łańcuch cyberochrony składają się narzędzia i sprzęt, drugi czynnik to ludzie, a trzeci i najważniejszy – wiedza specjalistów, którzy obsługują narzędzia. Czasem największym problemem może być jednak kadra zarządzająca, która nie chce podjąć decyzji o zakupie odpowiedniego rozwiązania dla zespołu bezpieczeństwa. W trakcie dyskusji zgodziliśmy się również, że niezwykle istotny jest realny trening. Jeśli chcesz być chroniony przed realnymi zagrożeniami, musisz przejść prawdziwe szkolenie i poznać rzeczywiste pole walki.

Sesja: Krajobraz po ataku APT. Jak minimalizować poniesione straty?

Prowadzenie: Klaudiusz Korus, FireEye

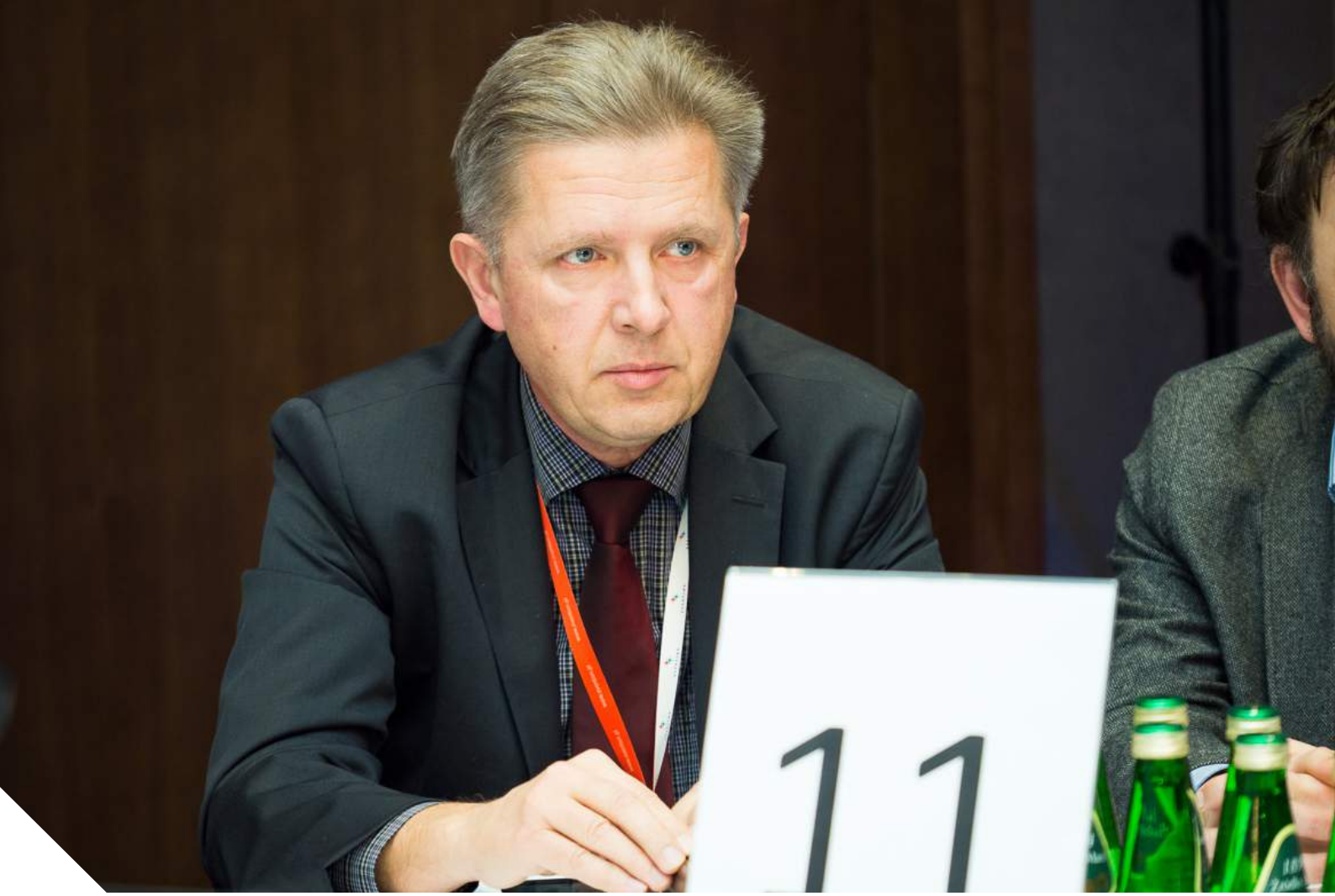
APT zdefiniowaliśmy jako ciągły, przeprowadzany aż do skutku i – biorąc pod uwagę narzędzia i wiedzę atakujących – zaawansowany atak, który ma precyzyjnie ustalony cel. Właśnie ta ostatnia cecha odróżnia go od innych, zwykłych ataków w Internecie, np. infekcji malware bankowym. Niestety, byliśmy zmuszeni zgodzić się, że nie ma skutecznej obrony przed takim działaniem. Co zatem możemy zrobić, jaki możemy stworzyć schemat działania? Przede wszystkim trzeba starać się zminimalizować czas, jaki upływa od chwili ataku do momentu jego wykrycia przez systemy lub ludzi. Przy tym ważne jest, żeby polegać nie tylko na specjalistach od bezpieczeństwa, ale także na zwykłych użytkownikach, którzy stanowią ostatnią linię obrony.



Sesja: **Bezpieczeństwo aplikacji – jak możemy o nie zadbać podczas przygotowania projektu**

Prowadzenie: **Moni Stern, Checkmarx**

Dlaczego statyczne testowanie bezpieczeństwa aplikacji jest tak istotne dla organizacji? Wyników osiąganych w przypadku standardowych testów nie da się nawet porównać ze statycznymi testami bezpieczeństwa aplikacji – ich efektywność jest znacznie większa. Druga istotna sprawa to edukacja deweloperów – dostarczanie im informacji zwrotnych, dzięki którym mogą uczyć się na błędach i nie popełniać ich ponownie. Rozwiązaniem jest uruchomienie bezpiecznego cyklu produkcji oprogramowania – programiści wykonują skan, otrzymują informacje zwrotne i poprawiają błędy; jednocześnie w ten sposób się uczą i nie popełniają podobnych pomyłek ponownie. Dzięki temu na produkcję nie trafi tysiąc takich samych błędów, bo są one eliminowane na początku.



Sesja: Bezpieczeństwo inteligentnej infrastruktury

Prowadzenie: Marek Wąsowski, Konsorcjum Smart Power Grids Polska

Inteligentna infrastruktura oznacza jednocześnie ogromną odpowiedzialność: informacje przetwarzane przez inteligentną infrastrukturę muszą być dobrze chronione. Wszyscy powinni mieć świadomość ryzyka, jakie dotyczy jej użytkowników. Inteligentna infrastruktura musi być zatem w pełni transparentna dla operatorów; w przeciwnym razie może stać się źródłem poważnych zagrożeń.

Gra zespołowa

Złożoność narzędzi, którymi posługują się cyberprzestępcy, powoduje, że jednym z podstawowych działań służb Biura Bezpieczeństwa Informatycznego w Departamencie Bezpieczeństwa w PKO Bank Polski *staje się współpraca, dzielenie się informacjami i wiedzą nie tylko z innymi pracownikami Banku, ale także zewnętrznymi organizacjami zajmującymi się problematyką cyberprzestępczości. Często firmy nawet nie wiedzą, że są atakowane; PKO BP jako duża organizacja ma większe możliwości przeciwdziałania cyberprzestępczości niż mniejsze firmy; możemy i chcemy zrobić więcej dla wspólnej ochrony przed cyberprzestępczością* – mówi Piotr Kalbarczyk, dyrektor Biura Bezpieczeństwa Informatycznego w Departamencie Bezpieczeństwa w PKO Bank Polski.

Czasem można usłyszeć, że nie mamy w ogóle szans na wygranie wojny z hakerami. Czy zgodzi się Pan z opinią, że skala zagrożeń i złożoność zagadnień związanych z bezpieczeństwem są tak duże, że nie jesteśmy w stanie tego opanować?

Piotr Kalbarczyk: Trudno generalizować właśnie ze względu na złożoność zagadnienia. W pewnych obszarach jest lepiej, w innych gorzej. Zacząłbym jednak od tego, że nie mamy do czynienia z wojną. Naszym przeciwnikiem nie jest organizacja, która chce coś zniszczyć. Celem działania jest zysk. Na końcu cyberprzestępczego łańcucha wartości znajdują się pieniądze. Podziemie internetowe jest doskonale zorganizowane. Paradoksalnie moglibyśmy powiedzieć, że w pewnych obszarach powinniśmy się uczyć od cyberprzestępców – chociażby tych związanych z wymianą informacji czy ich zabezpieczeniem – przeciętny człowiek nie ma takiej wiedzy; sięgają do niej co najwyżej specjalizujące się w tym służby.

Wachlarz stosowanych przez cyberprzestępców metod jest szeroki – od technologii po socjotechniki. Podobnie jak ludzi, którzy tworzą podziemie – wśród nich znajdują się specjaliści techniczni zajmujący się łamaniem systemów informatycznych i tworzeniem złośliwego oprogramowania oraz analitycy rozpracowujący procesy biznesowe.

Czy zatem mamy szansę, żeby pokonać cyberprzestępców, czy możemy jedynie próbować minimalizować straty?

P.K.: Przestępcy, jeśli tylko chcą, mogą być zwykłymi klientami banku – mają dostęp do naszych systemów bankowości elektronicznej, legalnie z nich korzystają i szukają w nich luk. Co więcej, jeśli ostrzegamy naszych klientów o potencjalnych zagrożeniach, to również cyberprzestępcy uzyskują informacje o tym, co robimy i co wiemy o ich działaniach. My postępujemy zgodnie z prawem, które zabrania nam działań ofensywnych, dlatego też rozpoznanie przestępczego biznesu jest dla nas o wiele trudniejsze.

Sukces w zwalczaniu cyberprzestępczości w dużej mierze zależy od posiadania pełnej informacji dostarczonej w odpowiednim czasie, niestety, często bardzo krótkim. W Polsce tego brakuje: nie wykorzystujemy możliwości, jakie stwarza szybka wymiana informacji pomiędzy legalnymi biznesami, instytucjami publicznymi, organami ścigania i wymiarem sprawiedliwości.

Czy podziemie internetowe to dobrze zorganizowane grupy, struktury mafijne, czy raczej indywidualności, które nawiązują współpracę, łączą siły na rzecz osiągnięcia pewnego wspólnego celu?

P.K.: W praktyce stykamy się zarówno z działalnością pojedynczych przestępców, jak i grup.

W podziemiu działa wielu specjalistów, którzy potrafią tworzyć złośliwy kod, wykorzystać socjotechnikę. Jeśli spojrzymy na TOR, jest to wolny rynek usług przestępczych oraz towarów. Mamy tam markety, w których można kupić praktycznie wszystko. Sprzedawcy są oceniani, tworzone są rankingi, istnieją nawet centra obsługi klienta. Nawet jeżeli trudno powiedzieć, czy jest to jedna czy wiele organizacji, czy tylko pojedyncze osoby, to z pewnością można stwierdzić, że świat przestępczy jest bardzo dobrze zorganizowany. Wiemy, że cyberprzestępcy dysponują

wsparciem prawnym, które pozwala im wynajdywać luki w przepisach i dzięki temu omijać różne regulacje. Mają także analityków biznesowych, którzy rozkładają działanie biznesu na części pierwsze. Dlatego trzeba mieć świadomość, że atakowane są nie systemy, a procesy biznesowe.

A czy zgodzi się Pan z opinią, że podziemie i zasoby przestępcze są najbardziej rozwinięte tam, gdzie państwa są nastawione na prowadzenie cyberwojny przeciw innym państwom? Rozwój podziemia może leżeć w interesie pewnych agend rządowych...

PK: Dofinansowywanie różnorodnych działań związanych przestępczością jest możliwe. Cele, na które można wykorzystać skradzione pieniądze, mogą być dowolne, mogą to być np. ataki na inne państwa czy terroryzm. Wiadomo, że doktryna wojny w cyberprzestrzeni jest w pewnych państwach rozwijana. Mapy wizualizujące działanie malware'u wyraźnie pokazują, że na wschód od naszej granicy aktywność jest wyraźnie mniejsza.

Podczas listopadowej konferencji „Advanced Threat Summit 2015" mówił Pan, że trzeba wiedzieć, w jaki sposób uderzyć w elementy przestępczego łańcucha wartości, tak aby wykazać inicjatywę strategiczną...

P.K.: Oczywiście, możemy zabezpieczać obszary odpowiadające samemu końcowi tego łańcucha, możemy nawet osiągnąć pewne sukcesy, ale i tak nie uda się nam zwalczyć „choroby". Efektywne działanie zależy od rozpoznania wszystkich elementów działalności przestępczej. Dopóki nie rozwiążemy tego problemu, będziemy koncentrować się na leczeniu objawów i prowadzić „kurację zachowawczą".

Obecnie poznajemy narzędzia i socjotechniki, które są wykorzystywane w końcowych etapach działań cyberprzestępców. Koncentrujemy się na tym i budujemy mechanizmy pozwalające temu przeciwdziałać. Co z tego, jeśli przestępcy na nasze zabezpieczenia prędzej czy później wymyślają nowe narzędzia i metody ataku.

Zatem musimy postawić na innowacyjność i ciągłe doskonalenie. Czy mamy przewagę nad internetowym podziemiem w tym obszarze?

P.K.: Odpowiadając na pierwszą część pytania: to rzeczywiście wymaga ciągłej pracy nad doskonaleniem metod i systemów ochrony. Wykorzystujemy wiele rozwiązań, nie tylko tych dostępnych

> Sukces w zwalczaniu cyberprzestępczości w dużej mierze zależy od posiadania pełnej informacji dostarczonej w odpowiednim czasie, niestety, często bardzo krótkim. W Polsce tego brakuje: nie wykorzystujemy możliwości, jakie stwarza szybka wymiana informacji pomiędzy legalnymi biznesami, instytucjami publicznymi, organami ścigania i wymiarem sprawiedliwości.

na rynku, ale również naszych, autorskich. Dbamy o ciągły rozwój naszych pracowników, promujemy inicjatywę i innowacyjność. Ponieważ systemy bazujące na sygnaturach tracą na znaczeniu ze względu na reaktywny charakter, budujemy rozwiązania wykorzystujące potężne narzędzia analityczne, dla których kluczowe jest zasilanie ich szerokim spektrum danych i informacji. Dlatego też tak ogromne znaczenie ma pełna informacja o funkcjonowaniu całego łańcucha przestępczego. Jeśli nie będziemy obejmować swoim działaniem wszystkich jego elementów, to zawsze będziemy o krok do tyłu. Oczywiście, sami nie jesteśmy w stanie wszystkiego zrobić. Wymiana wiedzy, informacji i współpraca pomiędzy biznesami, sektorami, organizacjami rządowymi, organami ścigania, wymiarem sprawiedliwości, regulatorami, a nawet państwami są kluczowe.

Co do przewagi, to należy stwierdzić, że obszar R&D po drugiej stronie jest świetnie rozwinięty. Wskazuje na to choćby ilość złośliwego kodu produkowana w ciągu roku – setki tysięcy odmian. Można chyba powiedzieć, że to oni mają nad nami w tym względzie przewagę. Złośliwe oprogramowanie ewoluuje, jego twórcy wyposażają go w funkcje umożliwiające mu ukrywanie się przed systemami zabezpieczającymi – przykładowo prowadząc swego rodzaju analizę behawioralną, malware sprawdza, czy dostał się do fizycznego komputera użytkownika, czy też jest na maszynie wirtualnej i środowisku testowym tzw. „sandbox".

Czy prowadzone są jakieś działania zmierzające do stworzenia systemowych rozwiązań ochrony?

P.K.: Nie mogę się wypowiadać za służby państwowe, ale na pewno tak. Niemniej przepływ informacji pomiędzy sferą prywatną i państwową jest wciąż niedostateczny. Raporty publikowane przez CERT co pół roku nie rozwiązują problemu. Mówimy o konkretnych wersjach malware'u, złośliwe oprogramowanie szybko mutuje, pojawiają się nowe wersje, dlatego tego typu informacje muszą być w sposób ciągły aktualizowane.

Najlepiej byłoby podjąć kompleksowe działania w skali globalnej, które całościowo obejmowałyby problem. Lokalnie także nie możemy się koncentrować wyłącznie na fragmentach, pojedynczych sektorach, czy też infrastrukturze krytycznej. Atak na sektor prywatny szybko może objąć swoim działaniem lub mieć wpływ na sferę publiczną. I odwrotnie.

Cyberprzestrzeń bezustannie ewoluuje, a wszelkie próby ujęcia jej w ramy przepisów są mało efektywne i niedostosowane do realiów. Weźmy na przykład ochronę danych osobowych. Paradoksalnie, w wielu przypadkach chronimy dawno skompromitowane dane. Użytkownicy Internetu bardzo często nie dbają o bezpieczeństwo swoich danych – publikują w Internecie swoje personalia, dane kart kredytowych. Natomiast nam restrykcje związane z ochroną danych osobowych uniemożliwiają często przeciwdziałanie przestępstwom.

Mówiąc o rozwiązaniach systemowych, nie można zapomnieć o inicjatywie Związku Banków Polskich i sektora bankowego mającej na celu utworzenie – najpierw dla sektora bankowego, potem w szerszej skali – platformy współpracy umożliwiającej przeciwdziałanie cyberprzestępczości. Inicjatywa

spotkała się z pozytywnym odzewem ze strony bankowców oraz Komisji Nadzoru Finansowego.

Czy system bankowy w Polsce dobrze radzi sobie z wykrywaniem nadużyć?

P.K.: Zacznijmy od tego, że czasem trudno powiedzieć, co jest przestępstwem. Często składa się ono z działań, które bez odpowiedniego kontekstu wyglądają na legalne. Dopiero drążąc w głąb, możemy odkryć, że u źródła znajduje się np. fraud. Przeciwdziałanie jest możliwe pod dwoma warunkami: po pierwsze musimy wiedzieć, że na początku doszło do przestępstwa, a po drugie musimy wiedzieć to szybko, bo czasu na przeciwdziałanie oszustwom jest niewiele. Polska stała się ofiarą szybkiego rozwoju technologii teleinformatycznej. Przebieg transakcji w systemie bankowym jest wyjątkowo sprawny. Jeśli nie wykryjemy fraudu za pomocą posiadanych narzędzi, a klient zorientuje się za późno, zabraknie czasu na reakcję.

Czy w Polsce istnieje wymiana informacji i współpraca pomiędzy instytucjami publicznymi a biznesem? Czy działania w tym obszarze są wystarczające?

P.K.: W mojej ocenie ta współpraca mogłaby być lepsza. Potrzebna jest platforma wymiany wiedzy i doświadczeń, ale także konkretne procedury operacyjne. Najważniejsze, żeby obie strony zaczęły traktować się po partnersku, bo tylko wtedy osiągniemy sukces.

A czy uważa Pan, że powinien powstać jeden centralny ośrodek bezpieczeństwa obejmujący sektor publiczny i państwowy?

P.K.: Jestem przekonany, że potrzebna jest organizacja, która będzie stanowiła platformę współpracy. Jej podstawowym celem powinno być rozwiązywanie problemów z cyberprzestępczością, zdobywanie wiedzy i dzielenie się nią oraz pomoc w komunikacji wszystkich zainteresowanych stron. Z pewnością powinna to być organizacja typu non profit, której jedynym celem działania będzie ochrona i rozwiązywanie problemów związanych z cyberprzestępczością. Trudno jednak powiedzieć, czy centralizacja to dobry pomysł. Mam obawy, czy nie pojawi się wówczas pokusa do odgórnego zarządzania wszystkim. Decydowanie np. o tym, jakich rozwiązań mamy używać, to nie najlepszy pomysł. Wystarczy zrobić krok za daleko w takich

> Cyberprzestrzeń bezustannie ewoluuje, a wszelkie próby ujęcia jej w ramy przepisów są mało efektywne i niedostosowane do realiów. Weźmy na przykład ochronę danych osobowych. Paradoksalnie, w wielu przypadkach chronimy dawno skompromitowane dane. Użytkownicy Internetu bardzo często nie dbają o bezpieczeństwo swoich danych – publikują w Internecie swoje personalia, dane kart kredytowych. Natomiast nam restrykcje związane z ochroną danych osobowych uniemożliwiają często przeciwdziałanie przestępstwom.

działaniach i pojawi się potężny problem; jednorodność spowoduje, że przełamanie zabezpieczeń w jednym miejscu będzie oznaczać pokonanie całego systemu ochrony. Różnorodność stosowanych rozwiązań jest naszą siłą.

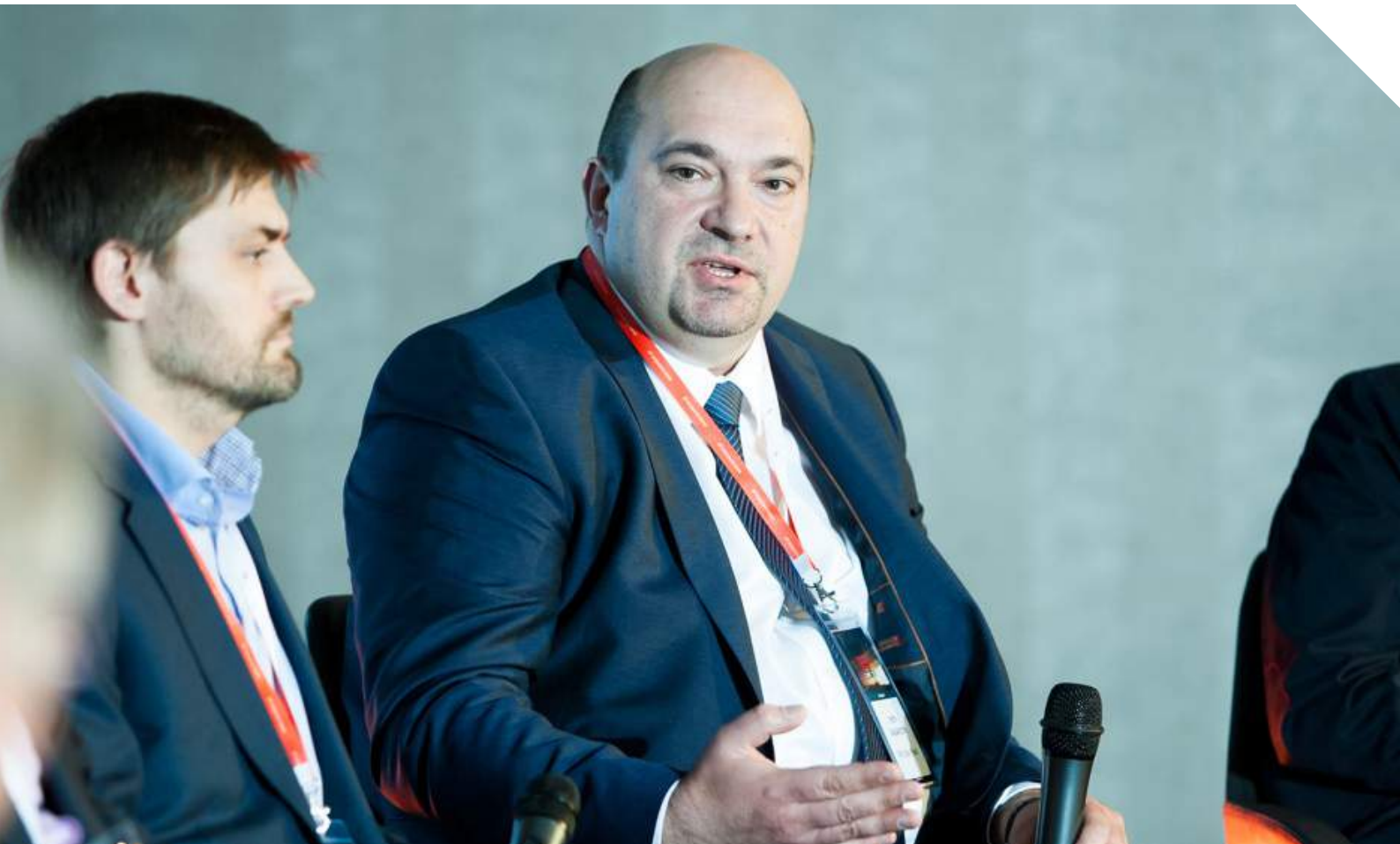
Co zatem proponuje Pan w zamian?

P.K.: Może nie w zamian, bo organizacja, jaką opisałem, jest potrzebna, jednak z mojego punktu widzenia kluczowe znaczenie ma szeroka współpraca – stworzenie sieci. Mamy ograniczony rynek, jeśli chodzi o specjalistów od bezpieczeństwa. Nie powinniśmy starać się wyrywać sobie tych ludzi za wszelką cenę. Lepiej współpracować i wykorzystywać ich wiedzę.

Bank ze względu na charakter swojej działalności zmuszony jest w sposób ciągły rozwijać systemy zabezpieczeń, mamy pewnie większe możliwości w tej dziedzinie niż mniejsze instytucje. Poza tym sektor bankowy jest jednym z ulubionych celów cyberprzestępców, dlatego też możemy być traktowani jako poligon, którego nic nie omija. W związku z powyższym zdobywamy doświadczenie i wiedzę, którą chcemy się dzielić. Może ona ułatwić działanie innym firmom, nie tylko z naszego sektora, a także organom ścigania i wymiarowi sprawiedliwości. Potrzeba jednak odpowiednich regulacji prawnych, które pozwoliłyby robić to szybciej i skuteczniej.

Czy współpraca sektorowa nie powinna mieć szczególnego znaczenia?

P.K.: I tak, i nie. Malware ukierunkowany na banki istnieje. Nie ma sensu jednak zamykać informacji w sektorze. Wymiana wiedzy bez takich ograniczeń



jest bardziej korzystna. Wykorzystajmy wzorce wypracowane w USA. Nie przystają one w 100% do naszych warunków, ale zacznijmy od tego, co się sprawdziło, i działajmy. Bo w USA dojście do obecnych rozwiązań zabrało kilkanaście lat.

Tam sprawdził się model sieciowy, w którym współpraca jest mocno rozwinięta. Banki należą do otwartych aliansów zwalczających cyberprzestępczość, których celem jest przyspieszenie wymiany informacji, dzielenie się wiedzą i rozwiązywanie konkretnych przypadków.

> Sektor bankowy jest jednym z ulubionych celów cyberprzestępców, dlatego też możemy być traktowani jako poligon, którego nic nie omija. W związku z powyższym zdobywamy doświadczenie i wiedzę, którą chcemy się dzielić. Może ona ułatwić działanie innym firmom, nie tylko z naszego sektora, a także organom ścigania i wymiarowi sprawiedliwości. Potrzeba jednak odpowiednich regulacji prawnych, które pozwoliłby robić to szybciej i skuteczniej.

Weźmy za przykład inicjatywę ZBP. Kierunek jest słuszny, ale nad szczegółami trzeba pracować. Organizacja powinna zrzeszać wszystkich chętnych do zwalczania cyberprzestępczości. W jej skład powinny wchodzić instytucje państwowe i służby, chociażby po to, żeby mieć informacje wynikające z profilowania świata przestępczego. Teraz informacje tego typu nie są udostępniane.

Mówi Pan o tym, że tego typu projekt wymaga czasu. My jednak tego czasu nie mamy...

P.K.: Inicjatywa podjęta przez ZBP realizowana jest dosyć szybko. Zaangażowanych jest wiele banków. Promujemy pewne podejście, choć nie wszyscy jeszcze je rozumieją i się z nim zgadzają.

Wiemy, co sprawdziło się w USA. Kładziemy nacisk na współpracę i zaufanie. Informacje, które chcemy wymieniać, są wrażliwe i niezwykle cenne dla drugiej strony. Trzeba tak zorganizować ich wymianę, żeby zabezpieczyć się przed wyciekiem.

Zmienia się podejście do wymiany informacji, UKNF wymusza na bankach bardziej szczegółowe raportowanie. Coraz więcej organizacji rozumie, że tylko wymieniając istotne informacje, jesteśmy w stanie przeciwdziałać skutkom cyberataków i cyberprzestępczości. Współpraca w dziedzinie cyberbezpieczeństwa zamiast konkurowania hasłami, które bardzo szybko weryfikuje życie – to na tym sektor powinien się skupić.

II KONFERENCJA

ADVANCED THREAT SUMMIT 2015

PARTNER STRATEGICZNY

FORTINET

PARTNERZY MERYTORYCZNI

APIUS technologies

ARROW

CHECKMARX

CLICO

CYBERGYM EUROPE
EXPECT THE UNEXPECTED

FireEye

Hewlett Packard Enterprise

IBM

IMPERVA

Infoblox
CONTROL YOUR NETWORK

intel Security

paloalto NETWORKS

QUALYS
CONTINUOUS SECURITY

Quest Dystrybucja
Dystrybutor Dell Software w Polsce

TREND MICRO

Raytheon | websense

SEVENET

cisco Gold Partner

VOL SOLUTIONS

WISENET

zscaler

II KONFERENCJA

ADVANCED THREAT SUMMIT 2015

MECENASI

WSPÓŁPRACA

ORGANIZATORZY

PATRONI

EVENTION

CZAS ZAANGAŻOWANY

Evention to spółka specjalizująca się w podnoszeniu wartości spotkań biznesowych na rynku ICT. W Evention **wydarzenia biznesowe traktujemy jako integralny i trudny do zastąpienia element budowania relacji i poprawy efektywności tych relacji pomiędzy firmami oraz tworzącymi je ludźmi**. Trzonem działalności spółki są spotkania realizowane w formule „custom event", w których kluczową rolę odgrywa zaangażowanie uczestników w całym procesie przygotowania wydarzenia. Szukamy innowacyjnych form realizacji spotkań, tak aby odpowiadało to obecnym aspiracjom, oczekiwaniom i potrzebom menedżerów z firm i instytucji publicznych.