ADVANCED THREAT SUMMIT 2017

22–23 listopada 2017, Warszawa

ORGANIZATORZY

EVENTION
CZAS ZAANGAŻOWANY

ISSA POLSKA

WSPÓŁPRACA MERYTORYCZNA

CSO COUNCIL

Raport powstał przy współpracy merytorycznej z portalem Enterprise Software Review.

Enterprise Software Review to forum wymiany fachowej wiedzy i doświadczeń na temat wykorzystania informatyki w dużych organizacjach. Stawia sobie za cel problemowe podejście do prezentowanych zagadnień i dostarczanie treści, które pomagają w rozwiązywaniu konkretnych spraw związanych z zastosowaniem nowych technologii. To serwis skierowany do menedżerów i ekspertów IT. Porusza zagadnienia dotyczące praktycznych aspektów funkcjonowania informatyki w realiach biznesowej codzienności. Nie mówi o informatyce w ogóle – pokazuje jej użyteczność na przykładzie konkretnych wdrożeń, zastosowań i sytuacji.

ENTERPRISE SOFTWARE REVIEW

INFORMATYKA W DUŻYCH ORGANIZACJACH

www.e-s-r.pl

Wydawcą ESR jest Evention – firma specjalizująca się w podnoszeniu wartości spotkań biznesowych na rynku ICT. Organizator takich wydarzeń jak: Big Data Technology Warsaw Summit, InfraSec Forum, RIBA Forum, Chief Data Officer Forum, CyberGov czy Advanced Threat Summit. Współzałożyciel CSO Council – społeczności dyrektorów bezpieczeństwa informacji, którą rozwija wspólnie ze stowarzyszeniem ISSA Polska.

EVENTION

CZAS ZAANGAŻOWANY

Szanowni Państwo!

Polecam lekturę naszego raportu, który przygotowaliśmy zainspirowani ostatnią konferencją „Advanced Threat Summit 2017" – jednym z najważniejszych i największych wydarzeń w dziedzinie cybersecurity w Polsce. W raporcie znajdą Państwo wywiady z wybranymi prelegentami i omówienie tematów związanych z agendą ostatniego ATS.

Cyberbezpieczeństwo to dziedzina, która dynamicznie się rozwija i zmienia – szybciej niż samo IT. Wyrosła na kluczowy obszar wyzwań i zagadnień dla wszystkich firm. Im bardziej biznes jest cyfrowy, tym większe rodzi ryzyka po stronie cyberbezpieczeństwa. To temat, który przebił się już do mainstream'u, stał się też przedmiotem troski i zainteresowania zarządów firm.

Nie zawsze i nie wszędzie przekłada się to od razu na odpowiednią alokację środków oraz zasobów w firmowych budżetach. Kierunek zmian jest jednak jednoznaczny. To wyzwanie dla menedżerów, którzy swój rozwój zawodowy widzą właśnie w tej dziedzinie. Im dedykujemy nasz raport.

Przemysław Gamdzyk
Komitet Organizacyjny CSO Council

Spis treści

4 **Nowe wyzwania, nowe podejście, nowe umiejętności**
Masowa, cyfrowa transformacja, szeroka współpraca biznesowa na globalną skalę, dynamiczna ewolucja zagrożeń oraz nowe regulacje związane z zapewnieniem zgodności z określonymi wymaganiami wymuszają nowe podejście do bezpieczeństwa IT oraz cyberbezpieczeństwa. Tradycyjny model polegający na ochronie sieciowego perymetru już się nie sprawdza. Podział na to, co „zaufane" i „niezaufane" przeszedł do historii. Odpowiednio zmotywowany cyberprzestępca zawsze jest w stanie znaleźć słabe ogniwo, które umożliwi przeniknięcie do wnętrza systemu i rozpoczęcie kolejnych etapów ataku. Dlatego strategicznymi priorytetami stają się teraz: zabezpieczenie danych poprzez monitorowanie ruchu w sieci, wbudowanie bezpieczeństwa w aplikacje i urządzenia, kontrolowanie przywilejów użytkowników oraz zastosowanie mechanizmów dostępu opartych na rolach. To nowe podejście kształtują i wzbogacają innowacyjne technologie: analityka Big Data, sztuczna inteligencja oraz uczenie maszynowe.

12 **Ramię w ramię z biznesem**
Dział bezpieczeństwa musi wychodzić naprzeciw nowym zjawiskom i trendom. Tylko w ten sposób może skutecznie wspierać biznes – mówi Ewa Piłat, Chief Technology Security Officer w Vodafone UK.

16 **Świadomość i współpraca – fundamenty bezpiecznego programowania**
Eksperci są zgodni: wymagania bezpieczeństwa powinny być uwzględniane już na wczesnych etapach cyklu rozwoju oprogramowania. W przeciwnym razie pozostają jedynie działania „na ostatniej prostej", które oznaczają albo wysokie koszty, albo konieczność akceptowania dużego ryzyka.
W prezentacjach i rozmowach na temat związku bezpieczeństwa systemów z procesem ich tworzenia i cyklem rozwoju aplikacji przewijały się, poza prewencją, dwa inne hasła: automatyzacja systemów zabezpieczeń oraz współpraca pomiędzy działami programistycznymi, operacyjnymi, biznesowymi i bezpieczeństwa.

22 **Srebrne kule nie istnieją**
Niezbędna technologia jest dostępna. Potrzeba pojedynczej konsoli, która obejmie wszystkie elementy i źródła danych. Później należy skoncentrować się po prostu na nudnej robocie. Rozmowa ze Stuartem McKenzie, wiceprezesem Mandiant, FireEye.

28 **AT SUMMIT Roundtables**

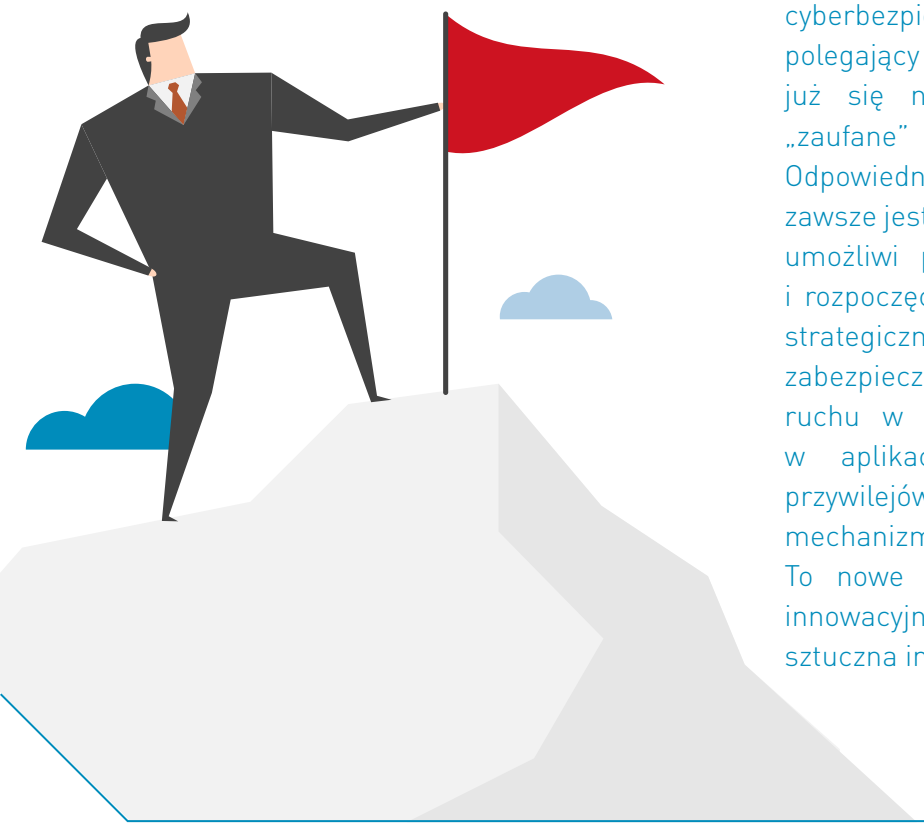
42 **Inteligentne wsparcie dla bezpieczeństwa**
Uczenie maszynowe, a w przyszłości sztuczna inteligencja mają do odegrania kluczową rolę w wykrywaniu nowych, nieznanych zagrożeń. Pomogą w ujawnieniu groźnych sytuacji, które nie były wcześniej zaobserwowane. Pierwsze rozwiązania wykorzystujące „samouczące się" technologie są już dostępne.

46 **RODO i cyberbezpieczeństwo: kompleksowo i długofalowo**
Rozmowa z Beatą Bielską, SAM & Cybersecurity Executive w APN Promise.

49 **Bezpieczeństwo i IT: razem czy osobno?**
Gdzie jest miejsce działu bezpieczeństwa w organizacji? Czy ma być częścią działu IT, czy samodzielną, wyodrębnioną komórką? Jak będzie wyglądało jego usytuowanie i rola w przyszłości? Komu powinien podlegać, aby skutecznie realizować swoje zadania? Podczas „Advanced Threat Summit 2017" dyskutowano o tym podczas panelu, który miał formę debaty oksfordzkiej.

ADVANCED THREAT SUMMIT 2017

Nowe wyzwania, nowe podejście, nowe umiejętności



Masowa, cyfrowa transformacja, szeroka współpraca biznesowa na globalną skalę, dynamiczna ewolucja zagrożeń oraz nowe regulacje związane z zapewnieniem zgodności z określonymi wymaganiami wymuszają nowe podejście do bezpieczeństwa IT oraz cyberbezpieczeństwa. Tradycyjny model polegający na ochronie sieciowego perymetru już się nie sprawdza. Podział na to, co „zaufane" i „niezaufane" przeszedł do historii. Odpowiednio zmotywowany cyberprzestępca zawsze jest w stanie znaleźć słabe ogniwo, które umożliwi przeniknięcie do wnętrza systemu i rozpoczęcie kolejnych etapów ataku. Dlatego strategicznymi priorytetami stają się teraz: zabezpieczenie danych poprzez monitorowanie ruchu w sieci, wbudowanie bezpieczeństwa w aplikacje i urządzenia, kontrolowanie przywilejów użytkowników oraz zastosowanie mechanizmów dostępu opartych na rolach. To nowe podejście kształtują i wzbogacają innowacyjne technologie: analityka Big Data, sztuczna inteligencja oraz uczenie maszynowe.

Bezpieczeństwo musi zostać wbudowane w ogólną strategię organizacji związaną z zarządzaniem danymi. Gdziekolwiek są dane, tam musi być bezpieczeństwo. To oznacza fundamentalną zmianę w sposobie myślenia o bezpieczeństwie.

RONEN SHPIRER,
SENIOR MANAGER, SOLUTIONS MARKETING W FORTINET

Obszar potencjalnych ataków powiększa się, zagrożenia są coraz bardziej złożone, a ich konsekwencje coraz bardziej poważne. Posiadamy zbyt wiele punktowych rozwiązań, z których każde ma własną konsolę zarządzającą. Poszczególne systemy nie współdzielą informacji, tworząc architekturę silosową.

„Bezpieczeństwo musi zostać wbudowane w ogólną strategię organizacji związaną z zarządzaniem danymi. Gdziekolwiek są dane, tam musi być bezpieczeństwo. To oznacza fundamentalną zmianę w sposobie myślenia o bezpieczeństwie" – mówił Ronen Shpirer, Senior Manager, Solutions Marketing w Fortinet, podczas sesji plenarnej otwierającej konferencję „Advanced Threat Summit 2017". Jego zdaniem, potrzebne są nowe, elastyczne rozwiązania, które będą adaptować się do konkretnej sytuacji i rozwiązań oraz do konkretnych miejsc, gdzie znajdują się dane. „Jednocześnie wszystkie elementy systemu będą 'świadome' istnienia pozostałych i będą wymieniać ze sobą informacje. Wreszcie działanie całości musi być zautomatyzowane – udział człowieka zwiększa ryzyko błędów" – dodał Ronen Shpirer.

Wszystkie zmiany powinny znaleźć wyraz w nowej strategii cyberbezpieczeństwa – spójnej ze strategią

Testować, testować i jeszcze raz testować. Nawet najlepsze i najbardziej szczegółowe plany będą całkowicie nieprzydatne, jeśli ludzie nie będą ich bardzo dobrze znali i nie będą regularnie ćwiczyć ich realizacji.

DARRON GIBBARD,
CHIEF TECHNICAL SECURITY OFFICER AND MANAGING DIRECTOR W QUALYS

biznesową organizacji, dopasowanej do celów przedsiębiorstwa, posiadanych zasobów, miejsca firmy na rynku oraz pozycji działu bezpieczeństwa w przedsiębiorstwie. Jak zbudować dobrą strategię, radziła Ewa Piłat, Chief Technology Security Officer w Vodafone UK. Z jej wiedzy i doświadczenia wynika, że dla osiągnięcia sukcesu wymagane jest zaangażowanie zarządu, zbudowanie odpowiednich kompetencji i wdrożenie narzędzi wspierających. Potrzebne jest przy tym regularne aktualizowanie strategii i uwzględnienie czynników zewnętrznych, m.in. trendów technologicznych i nowych regulacji prawnych. Jako najczęściej popełniane błędy można wskazać: oderwanie strategii cyberbezpieczeństwa od strategii firmy, inicjowanie projektu jej tworzenia bez zapewnienia udziału zarządu i wyższego kierownictwa oraz zaniechania w jej cyklicznej aktualizacji.

Technologia sztucznej inteligencji, chociaż bardzo przydatna, na razie nie jest w stanie w pełni zastąpić człowieka. To ostatecznie eksperci muszą zweryfikować wyselekcjonowane automatycznie przypadki i zatwierdzić przekazanie informacji o zdarzeniu klientowi.

Integralnym czynnikiem strategii powinno być także cykliczne testowanie poszczególnych jej elementów. „Testować, testować i jeszcze raz testować" – przekonywał Darron Gibbard, Chief Technical Security Officer and Managing Director w Qualys. Nawet najlepsze i najbardziej szczegółowe plany będą całkowicie nieprzydatne, jeśli ludzie nie będą ich bardzo dobrze znali i nie będą regularnie ćwiczyć ich realizacji w praktyce.

Próby zapewnienia bezpieczeństwa dopiero w końcowej fazie prac nad nowymi aplikacjami oznaczają zwykle duże koszty lub konieczność akceptowania ryzyka związanego z wprowadzeniem do produkcji kodu, który nie gwarantuje odpowiedniego poziomu bezpieczeństwa.

Nowy krajobraz

Zbliżający się ku końcowi rok 2017 pokazuje, jak ważną rolę w cyberbezpieczeństwie odgrywają: strategia, planowanie i testowanie. Europejczycy dopiero kilka miesięcy temu przekonali się, jakie spustoszenie mogą spowodować ataki prowadzone z wykorzystaniem narzędzi *ransomware* oraz *disruptive malware*. Specjaliści od bezpieczeństwa na Bliskim Wschodzie mieli taką świadomość już przynajmniej od kilku lat. Mówili

Coraz większą rolę w obszarze bezpieczeństwa IT i cyberbezpieczeństwa odgrywa sztuczna inteligencja albo, mówiąc bardziej precyzyjnie, uczenie maszynowe. Nowa technologia oznacza jednak i nowe wyzwania. Znane są już sposoby „oślepiania", oszukiwania i wprowadzania w błąd systemów uczenia maszynowego poprzez stopniowanie sygnałów. Oczywiście, pojawiają się także szanse na zastosowania sztucznej inteligencji w narzędziach używanych do obrony. Niektóre z nich pozwalają na wykrywanie ataków w czasie zbliżonym do rzeczywistego.

LESZEK TASIEMSKI,
VP, RAPID DETECTION CENTER, R&D RADAR & RDS W F-SECURE

Konieczna jest zmiana sposobu myślenia inżynierów. Ich obowiązkiem jest projektowanie rozwiązań technicznych z uwzględnieniem od początku wymagań bezpieczeństwa. Zaniechania w tym obszarze mogą dużo kosztować.

GEN. WŁODZIMIERZ NOWAK,
CZŁONEK ZARZĄDU,
DYREKTOR DS. PRAWNYCH,
BEZPIECZEŃSTWA
I ZARZĄDZANIA ZGODNOŚCIĄ
W T-MOBILE POLSKA

o tym Stuart McKenzie, Vice President, oraz Muks Hirani, Technical Director w Mandiant, firmie należącej do FireEye. Przekonywali, że w przyszłości należy spodziewać się nasilenia ataków tego typu. Co więcej, choć dotychczas stanowiły one domenę zorganizowanych grup sponsorowanych przez państwa, teraz można oczekiwać, że narzędzi pozwalających na ich realizację zaczną również używać zwykli przestępcy. Eksperci z Mandiant zwracali przy tym uwagę, że jeśli uda się wykryć próbę ataku na jednym z etapów przygotowawczych, można mu skutecznie zapobiec. W przeciwnym wypadku będzie to niemożliwe.

Z kolei Leszek Tasiemski, VP, Rapid Detection Center, R&D Radar & RDS w F-Secure, opowiadał o nowych paradygmatach ataków i obrony w świecie, w którym środowiska informatyczne stają się „hybrydą pomiędzy publiczną chmurą a tradycyjną twierdzą". Coraz większą rolę w obszarze bezpieczeństwa IT i cyberbezpieczeństwa odgrywa sztuczna inteligencja albo, mówiąc bardziej precyzyjnie, uczenie maszynowe. Nowa technologia oznacza jednak i nowe wyzwania. Znane są już sposoby „oślepiania", oszukiwania i wprowadzania w błąd systemów uczenia maszynowego poprzez stopniowanie sygnałów. Oczywiście,

pojawiają się także szanse na zastosowania w narzędziach używanych do obrony. Niektóre z nich pozwalają na wykrywanie ataków w czasie zbliżonym do rzeczywistego – z potwierdzeniem przekazywanym klientom w ciągu 30 minut.

Leszek Tasiemski zwracał jednak uwagę, że technologia ta, chociaż bardzo przydatna, to przynajmniej na razie nie jest w stanie w pełni zastąpić człowieka. To ostatecznie ludzie, eksperci muszą zweryfikować wyselekcjonowane automatycznie przypadki i zatwierdzić przekazanie informacji o zdarzeniu klientowi. Niemniej przyspieszenie, które można dzięki niej osiągnąć, jest spektakularne.

Bezpieczny development

Dużo uwagi podczas konferencji „Advanced Threat Summit 2017" poświęcono także problematyce jak najwcześniejszego włączania kwestii bezpieczeństwa w procesy produkcji oprogramowania. Zwracał na to uwagę m.in. gen. Włodzimierz Nowak, członek zarządu, dyrektor ds. prawnych, bezpieczeństwa i zarządzania zgodnością w T-Mobile

Polska. Mówił, że konieczna jest zmiana sposobu myślenia inżynierów. Ich obowiązkiem jest projektowanie rozwiązań technicznych z uwzględnieniem wymagań bezpieczeństwa. Zaniechania w tym obszarze, próby zapewnienia bezpieczeństwa dopiero w końcowej fazie prac nad nowymi aplikacjami oznaczają zwykle duże koszty lub konieczność akceptowania ryzyka związanego z wprowadzeniem do produkcji kodu, który nie gwarantuje odpowiedniej jakości pod względem bezpieczeństwa.

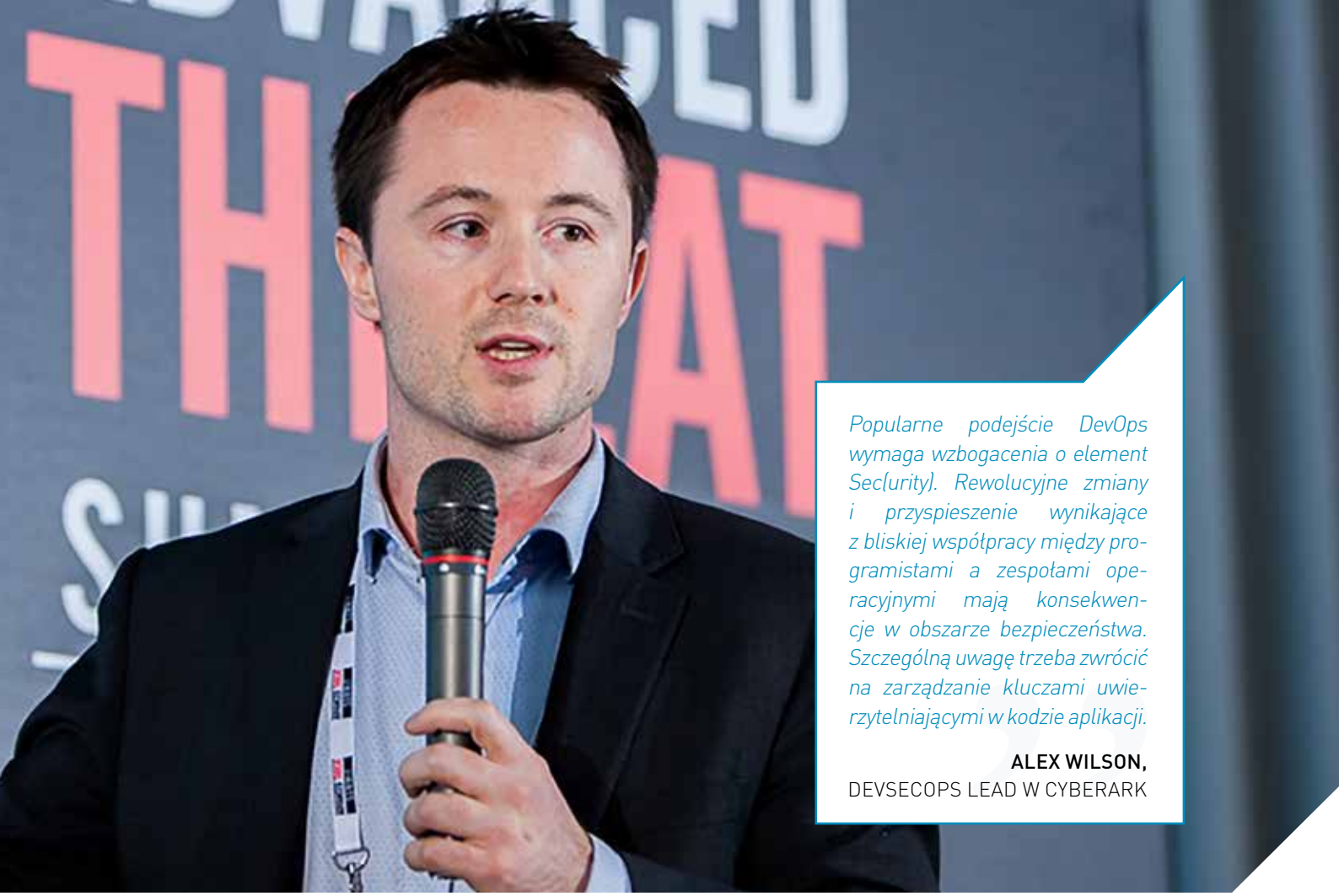
Konsekwencje wycieku danych przez „dziurawe" aplikacje mogą być poważne. Przykłady można mnożyć. Michał Kurek, partner KPMG (Cyber Security), lider OWASP Warszawa, powoływał się na najświeższy z nich – Equifax. Niezabezpieczona podatność w Apache Struts2 była źródłem wycieku 143 mln wrażliwych danych osobowych. Rozwiązaniem tego typu problemów jest kompleksowe podejście do wbudowania bezpieczeństwa w procesy produkcji oprogramowania. Michał Kurek rekomendował wykorzystanie narzędzia OWASP – SAMM (Software Assurance Maturity Model).

Zwłaszcza niezwykle popularne podejście DevOps wymaga wzbogacenia o element Sec(urity). Rewolucje zmiany i przyspieszenie wynikające z bliskiej współpracy między programistami a zespołami operacyjnymi mają konsekwencje w obszarze bezpieczeństwa. Mówił o tym m.in. Alex Wilson, DevSecOps Lead w CyberArk, zwracając szczególną uwagę na zarządzanie kluczami uwierzytelniającymi w kodzie aplikacji i prezentując zautomatyzowane rozwiązanie związanych z tym problemów – system Conjur.

Dla osiągnięcia sukcesu w budowaniu strategii cyberbezpieczeństwa wymagane są: zaangażowanie zarządu, zbudowanie odpowiednich kompetencji i wdrożenie narzędzi wspierających. Potrzebne jest też regularne aktualizowanie strategii i niepomijanie czynników zewnętrznych, m.in. trendów technologicznych i nowych regulacji prawnych.

Potrzebny Superbezpiecznik

Popularnym tematem pojawiającym się w wielu wystąpieniach było także RODO. Konsekwencjom rozporządzenia o ochronie danych osobowych poświęcona była dyskusji panelowa. Uczestnicy zwracali uwagę, że utrudni ono swobodny rozwój i prowadzenie biznesu, ograniczy innowacyjność. Mówili jednak też, że nie jest to sprawa nowa, że stanowi jedynie pewnego rodzaju uporządkowanie znanych, istniejących wcześniej zasad i dobrych praktyk.



Popularne podejście DevOps wymaga wzbogacenia o element Sec(urity). Rewolucyjne zmiany i przyspieszenie wynikające z bliskiej współpracy między programistami a zespołami operacyjnymi mają konsekwencje w obszarze bezpieczeństwa. Szczególną uwagę trzeba zwrócić na zarządzanie kluczami uwierzytelniającymi w kodzie aplikacji.

ALEX WILSON,
DEVSECOPS LEAD W CYBERARK

Podczas debaty zarysowały się także różnice w postrzeganiu RODO przez specjalistów ds. bezpieczeństwa i prawników. Jeden ze zdiagnozowanych problemów dotyczył wyzwań komunikacyjnych. Obie grupy posługują się różnymi, niespójnymi aparatami pojęciowymi. Tymczasem komunikacja stanowi fundament sukcesu dla projektów związanych z RODO. W tym kontekście rozmawiano o nowych wymaganiach wobec tradycyjnych „bezpieczników", a nawet tworzeniu nowego zawodu – menedżera ds. ochrony danych, który będzie łączył świat technologii i prawa, ponieważ skupienie się wyłącznie na jednym z tych obszarów to obecnie za mało.

Wszyscy zainteresowani rynkiem pracy w obszarze bezpieczeństwa IT mogli dowiedzieć się podczas konferencji o zapotrzebowaniu na usługi specjalistów w tym zakresie, wysokości wynagrodzeń oraz rotacji i metodach retencji ekspertów. Opowiadał o tym Paweł Biniarz z firmy Sedlak & Sedlak. Można też było posłuchać o pracy head hunterów i współpracy z nimi, a także o skutecznej komunikacji przedstawicieli działów bezpieczeństwa z innymi jednostkami w organizacjach. Ci, którzy wzięli sobie do serca konieczność poprawienia komunikacji z innymi menedżerami i zarządem w swojej firmie, mogli wziąć udział w warsztacie poświęconym sztuce przemówień publicznych prowadzonym przez Monikę Królak, założycielkę KMKM. Wysoka frekwencja sugerowała, że bezpiecznikom naprawdę zależy na podniesieniu swoich zdolności komunikacyjnych na wyższy poziom.

ADVANCED THREAT SUMMIT 2017

Ramię w ramię z biznesem

Dział bezpieczeństwa musi wychodzić naprzeciw nowym zjawiskom i trendom. Tylko w ten sposób może skutecznie wspierać biznes – mówi **Ewa Piłat**, Chief Technology Security Officer w Vodafone UK.

W wystąpieniu podczas „Advanced Threat Summit 2017", poświęconym budowaniu strategii cyberbezpieczeństwa, praktycznie nie mówiła Pani o technologii. Czy właśnie tak należy podejść do budowania strategii? Czy powinna być ona neutralna technologicznie?

Nie, to raczej ograniczenie wynikające z charakterystyki wystąpień konferencyjnych. Na pewnym etapie działań trzeba zejść do poziomu technologii. Staje się to konieczne w momencie, kiedy zaczynamy prowadzić analizę mającą na celu opisanie aktualnej sytuacji w organizacji. Ta analiza musi być bardzo szczegółowa, detaliczna, żeby precyzyjnie pokazać miejsce, w którym się znajdujemy. Jeśli poruszalibyśmy się wyłącznie na wysokim poziomie ogólności, to nie bylibyśmy w stanie określić, co trzeba zrobić, żeby przejść z obecnego miejsca do punktu docelowego. Nie wiedzielibyśmy, jak zrealizować postawione cele.

Czy z tego wynikają główne różnice między różnymi strategiami? Na ile strategia cyberbezpieczeństwa może być wspólna dla podobnych organizacji z tej samej branży?

Elementem wspólnym będą cele i zakres cyberbezpieczeństwa. Strategiczne cele będą zawsze takie same. Po pierwsze, mamy ochronę, po drugie, wykrywanie, po trzecie – reagowanie. Chronimy to, co posiadamy. Naruszenia wykrywamy dzięki wyspecjalizowanym systemom, korelującym informacje z różnych źródeł. Możemy wykrywać ataki, zanim faktycznie do nich dojdzie. Wiedząc, że może dojść do ataku, jesteśmy w stanie podjąć kroki, które temu zapobiegną. Niestety, czasem nie jesteśmy w stanie czegoś wykryć i zapobiec niechcianemu zdarzeniu. Dlatego musimy reagować – potrzebne są procesy, które w sposób efektywny złagodzą efekty ataków.

Ewa Piłat,
Chief Technology Security Officer w Vodafone UK

Realizację celów zawsze dopasowujemy do potrzeb konkretnej organizacji. Strategie będą się różnić pod względem tego, co należy chronić, a także tego, jakie wykorzystywane są obecnie technologie. O różnicach branżowych decyduje głównie zróżnicowanie pod względem poziomu cyfryzacji – inny będzie w farmacji czy sektorze finansowym, a inny w przemyśle budowlanym.

Podczas wystąpienia mówiła Pani również o tym, że budowa strategii cyberbezpieczeństwa trwa miesiącami. Czy ten proces można przyspieszyć, np. zatrudniając zewnętrzną firmę?

Oczywiście, firma zewnętrzna może wspierać budowę strategii. Można dzięki temu przyspieszyć jej opracowywanie. Organizacja musi jednak sama wykonać większą część pracy związanej z analizą. Ogólnie rzecz ujmując, zlecenie przygotowania strategii to dobry pomysł, ale należy być ostrożnym. Trzeba uważać, żeby firma zewnętrzna nie narzuciła trybu i celów, które sama ma do zrealizowania. I żeby to wsparcie było cały czas kontrolowane.

Decydując się na outsourcing, musimy już wiedzieć, co chcemy zrobić. Zewnętrzna firma może dostarczyć materiał, zweryfikować przy współpracy z IT to, co już mamy. Skracamy czas, ponieważ jesteśmy w stanie wykonać pewne kroki równolegle. Przy braku zasobów takie działania są po prostu niemożliwe.

Jak przekonać zarząd, że organizacja potrzebuje strategii cyberbezpieczeństwa?

Jedną ze skuteczniejszych metod przekonywania zarządu do zainicjowania wdrożenia strategii cyberbezpieczeństwa jest prośba o zaakceptowanie ryzyka.

Przyjęcie przez pion bezpieczeństwa funkcji budowania świadomości jest korzystne pod wieloma względami. Nie jest moją rolą zmuszanie zarządu do podjęcia decyzji. Ani walka, ani przekonywanie, że musimy coś zrobić. Ja podchodzę do tego z drugiej strony. Pokazuję, jakie ryzyka istnieją i na poparcie przedstawiam przykłady. Mówię: takie są ryzyka, takie są zagrożenia, takie są przykłady ataków na konkurencję czy firmy z innych branż. Jeśli nie zrealizujemy trzech podstawowych celów cyberbezpieczeństwa, to również nas może to spotkać. Czy zarząd akceptuje taki stan rzeczy?

Kiedy uda się zaangażować zarząd, kiedy strategia będzie stanowić inicjatywę zarządu, to wszyscy – wszystkie jednostki organizacyjne, które są istotne z punktu widzenia całościowego bezpieczeństwa – będą zobowiązani do jej wdrażania.

To czynniki wewnętrzne wpływające na strategię. Zwracała Pani również uwagę, żeby nie pomijać czynników zewnętrznych...

Trzeba wziąć pod uwagę przede wszystkim dwa czynniki zewnętrzne. Jeden z nich to nowe regulacje. GDPR to doskonały przykład. Wprawdzie ochrona danych osobowych zawsze była istotna, GDPR nie zmienia drastycznie całego podejścia do tego obszaru. Zmieniają się jednak konsekwencje – wysokość potencjalnych kar. To należy uwzględnić w strategii.

Drugi czynnik to technologia. Strategia cyberbezpieczeństwa ma zwykle w dojrzałych organizacjach charakter 3–5-letni. Jeśli budujemy środowisko cyberbezpieczeństwa i chcemy, żeby nasze systemy wspierały nas zgodnie z wszelkimi trendami, to nie może być tak, że na etapie planowania bierzemy pod uwagę wyłącznie istniejące, dostępne na rynku rozwiązania. Za pięć lat będą one przestarzałe, często nie będą nawet serwisowane przez producenta.

To chyba wyjątkowo trudne przewidzieć zmiany technologiczne w perspektywie kilkuletniej?

Oczywiście, że to nie jest proste, ale nie jest też niemożliwe. Potrzebne jest regularne aktualizowanie strategii w zależności od zmieniających się czynników zewnętrznych, w tym wypadku technologicznych. Podstawą jest uważne obserwowanie trendów rynkowych i technologicznych, a następnie właściwe reagowanie. Wprowadzenie zmian w obszarze technologicznym nie oznacza konieczności zmieniania całej strategii. Dostosowujemy ją jedynie do aktualnych albo do przyszłych warunków.

Przykładowo: mamy system wykrywania włamań. Kupując ten system, zakładaliśmy, że będziemy go używać przez trzy lata – taki jest średni cykl życia współczesnych technologii. Mając jednak 5-letnią strategię, już po drugim roku użytkowania, a czasem nawet już po pierwszym, powinniśmy się zastanowić, czy musimy kupić znowu taki sam system, czy też może potrzebujemy czegoś innego.

Jedną ze skuteczniejszych metod przekonywania zarządu do zainicjowania wdrożenia strategii cyberbezpieczeństwa jest prośba o zaakceptowanie ryzyka.

Obecnie większość usług wychodzi do chmury. To dobry moment, żeby zastanowić się, czy bezpieczeństwo także nie powinno postawić na rozwiązania chmurowe. Czy zamiast inwestować w niezwykle kosztowne urządzenia fizyczne, które ulokujemy we własnym centrum danych, nie lepiej skorzystać z modelu subskrypcyjnego? Dodatkową korzyścią będzie to, że zobaczymy trendy kształtujące się nie tylko wewnątrz naszej organizacji, opierające się na naszych scenariuszach zagrożeń. Będziemy mogli także wyrobić sobie opinię na podstawie zewnętrznych informacji, do których dostęp mają usługodawcy współpracujący z wieloma klientami na całym świecie.

Wspominała Pani o modelu subskrypcyjnym. Tradycyjne podejście do bezpieczeństwa i cloud computing nie idą raczej w parze. Czy to się właśnie zmienia?

Zdecydowanie tak. Dzisiaj chyba nikt nie ma wątpliwości, że chmura obliczeniowa to przyszłość. Przynajmniej w Wielkiej Brytanii. Tutaj większość dużych firm w swoje długookresowe, 3–5-letnie strategie ma wpisane wyjście z serwisami świadczonymi klientom do chmury. Co więcej, firmy często zastanawiają się – oczywiście decyduje o tym wyższa efektywność finansowa – nad połączeniem obszarów IT i sieci poprzez używanie nowych technologii takich jak SDN (Software Defined Networks) czy NFV (Network Function Virtualization). To technologie, które pozwalają wirtualnie albo programowo zarządzać siecią i systemami.

Jeśli będziemy się temu trendowi opierać, będziemy się cofać. Nie można zapominać, że rolą bezpieczeństwa jest wychodzenie nowym zjawiskom naprzeciw. Jeśli wiadomo, że firma będzie dostarczać usługi z chmury publicznej, np. Amazon czy Cisco, to naszą rolą jest zapewnienie, żeby nie tylko polegać na bezpieczeństwie oferowanym przez chmurę i jej dostawcę poprzez odpowiednie umowy. Musimy mieć także aktywny wpływ na to, jak bezpieczeństwo jest zorganizowane i zrealizowane. Mimo że jesteśmy klientami, powinniśmy kontrolować poziom bezpieczeństwa usług. Alarmy i weryfikowanie podatności, które będzie się odbywać się chmurze, będzie widoczne również w naszych systemach monitorujących.

Czy jest coś, co Panią zaskoczyło, kiedy zaczęła Pani pracę w cyberbezpieczeństwie w Wielkiej Brytanii?

Chyba największym zaskoczeniem był znacznie wyższy poziom cyfryzacji biznesu i całego społeczeństwa. Wyższa jest także dojrzałość, przynajmniej dużych organizacji, pod względem bezpieczeństwa. Jest jednak na to proste wyjaśnienie: Wielka Brytania jest w większym stopniu narażona na ataki. Decyduje o tym wielkość gospodarki oraz pozycja na arenie międzynarodowej. To sprawia, że skala zagrożeń jest inna, a także cele ataków odmienne niż w Polsce. Obserwowane przeze mnie próby ataku są zwykle sponsorowane przez duże organizacje albo przez rządy innych krajów. Mamy do czynienia głównie z atakami z Chin, Rosji, Zachodniej Afryki, Indii.

Pewnego rodzaju zaskoczeniem była niezależność działu bezpieczeństwa i jego mocna pozycja wewnątrz organizacji. W Polsce cyberbezpieczeństwo jest niedoinwestowane. Po części powodem jest wspomniana już inna skala zagrożeń. Brakuje także powszechnie znanych przykładów zdarzeń, które mogłyby zagrozić istnieniu przedsiębiorstwa.

Świadomość i współpraca – fundamenty bezpiecznego programowania

Eksperci są zgodni: wymagania bezpieczeństwa powinny być uwzględniane już na wczesnych etapach cyklu rozwoju oprogramowania. W przeciwnym razie pozostają jedynie działania „na ostatniej prostej", które oznaczają albo wysokie koszty, albo konieczność akceptowania dużego ryzyka. W prezentacjach i rozmowach na temat związku bezpieczeństwa systemów z procesem ich tworzenia i cyklem rozwoju aplikacji przewijały się, poza prewencją, dwa inne hasła: automatyzacja systemów zabezpieczeń oraz współpraca pomiędzy działami programistycznymi, operacyjnymi, biznesowymi i bezpieczeństwa.

Wycieki danych na skutek „dziur" w aplikacjach to poważne zagrożenie. Niedawny przypadek amerykańskiej firmy Equifax pokazał, jak niezałatana podatność w Apache Struts2 spowodowała ujawnienie 143 mln wrażliwych danych osobowych. Taki wyciek w kontekście wchodzącego wkrótce w życie rozporządzenia RODO wiązałby się ze znaczącymi konsekwencjami finansowymi. Straty bezpośrednie w wysokości 9 mln USD, które były efektem wycieku danych z RBS Worldpay przed blisko dekadą, dzisiaj z pewnością osiągnęłyby wyższy poziom.

„Statystyki są zatrważające. Doświadczenia ekspertów KPMG wskazują, że aż 83% testowanych aplikacji zawiera podatności o priorytecie wysokim lub krytycznym. Przykładowo, pozwalają one na uzyskanie pełnego dostępu do bazy danych, wykonywanie poleceń na serwerze albo przejęcie sesji użytkowników. Natomiast z raportu ‹High Tech Bridge App Security Trends Reports 2017› wynika, że fundamentalne luki w bezpieczeństwie zawiera aż 98% paneli administracyjnych IoT" – mówił Michał Kurek, partner KPMG Cyber Security, Lider OWASP (Open Web Application Security Project) Warszawa, występujący

Jeśli uda się przekonać deweloperów, że bezpieczeństwo musi pojawić się na wczesnych etapach procesu tworzenia oprogramowania, sukces będzie znacznie bliżej. Prewencja jest zawsze lepsza niż reagowanie.

WOJCIECH DWORAKOWSKI,
IT SECURITY EXPERT,
SECURING

z prezentacją: Jak włączać bezpieczeństwo w procesy wytwarzania aplikacji w kontekście RODO.

Przytoczone dane pokazują, że organizacje mają poważny problem z identyfikacją i eliminowaniem podatności. Potwierdzają to również inne badania. Niemal połowa aplikacji jest stale podatna na atak. Średni czas usunięcia podatności oznaczonych jako krytyczne wynosi 126 dni lub nawet 196 dni dla podatności o priorytecie wysokim. Takie dane podaje raport „2017 WhiteHat Security – Application Security Statistics".

„Właśnie dlatego kwestie bezpieczeństwa należy włączyć jak najwcześniej do prac nad oprogramowaniem, najlepiej na początkowym etapie cyklu SDLC – Software Development Lifecycle. Wykonanie testu penetracyjnego nie zapewni bezpieczeństwa, a przy tym działanie na końcowym etapie będzie bardzo kosztowne. Naprawa po wdrożeniu może wiązać się nawet ze stukrotnie większymi kosztami, niż gdyby udało się wprowadzić poprawki na początku cyklu" – ocenia Michał Kurek.

Dobre praktyki

Co można zatem zrobić? Jakie zastosować mechanizmy kontrolne? Po pierwsze, należy postawić na edukację. Świadomość cyberzagrożeń pozwala zwiększyć czujność. Nie sprawdzają się bowiem ani prośby, ani groźby. Znacznie lepszym rozwiązaniem są szkolenia – w pierwszej kolejności dla deweloperów. „Nie powinny one mieć technicznego charakteru, ale zamiast tego skupiać się na budowaniu świadomości. Jeśli uda się przekonać deweloperów, że bezpieczeństwo musi pojawić się na wczesnych etapach procesu tworzenia oprogramowania, sukces będzie znacznie bliżej. Prewencja jest zawsze lepsza niż reagowanie" – przekonywał

Niezależnie od tego, jak zabezpieczymy perymetr, jest prawdopodobne, że ktoś i tak będzie w stanie dokonać włamania. Przepisanie takiego systemu jest nierealne. Do tego system musi cały czas działać. Dlatego w większości przypadków najlepszym rozwiązaniem są działania polegające na stopniowym podnoszeniu bezpieczeństwa poprzez wykonywanie małych kroków.

PAWEŁ KRAWCZYK,
SPECJALISTA
BEZPIECZEŃSTWA INFORMACJI
W KRAWCZYK INDUSTRIES

podczas dyskusji w jednej z sesji Roundtables Wojciech Dworakowski, IT Security Expert, SecuRing.

Promowanie bezpieczeństwa i podnoszenie świadomości nie może przy tym ograniczać się wyłącznie do deweloperów. Pełne zrozumienie zagrożeń i konieczności uwzględnienia odpowiednich wymagań musi pojawić się także po stronie osób zlecających projekty. Funkcjonalność i czas nie mogą stanowić jedynych priorytetów podczas tworzenia oprogramowania.

Kolejnym środkiem zapobiegawczym jest modelowanie zagrożeń. „Mając przeanalizowane zagrożenia, można stworzyć specyfikację wymagań bezpieczeństwa, co pozwala najmniejszym kosztem zwiększyć bezpieczeństwo. Zamawiając rozwój systemu w firmie zewnętrznej, nie wolno zakładać, że bezpieczeństwo zostanie włączone w projekt. Niestety, tak nie jest. Wszystko trzeba wyspecyfikować. Nie wystarczy zapis, że aplikacja ma być bezpieczna. Najlepiej przygotować listę wymagań jako załącznik do umowy" – radził Michał Kurek.

Dobrą praktyką są testy automatyczne już na etapie tworzenia kodu. Istnieją gotowe narzędzia, które pozwalają je zrealizować. Na koniec należy przeprowadzić audyt bezpieczeństwa. Najbardziej efektywne kosztowo są testy penetracyjne. Jeśli natomiast oprogramowanie stanowi istotny z biznesowego punktu widzenia system, przydatne jest zlecenie inspekcji kodu. Pośród najlepszych praktyk w tym zakresie wskazywano na: OWASP SAMM (Software Assurance Maturity Model), SDL (Security Development Model

– Microsoft) oraz BSIMM (Builidng Security In Maturity Model).

Michał Kurek zwracał szczególną uwagę na OWASP SAMM v 1.5, który dzieli proces SDLC na 12 obszarów (4 funkcje i 3 poziomy dojrzałości). W jaki sposób SAMM może pomóc organizacji? Przede wszystkim umożliwia weryfikację bezpieczeństwa w obecnie realizowanym procesie wytwarzania oprogramowania. Budowa programu podniesienia bezpieczeństwa odbywa się w zdefiniowanych iteracjach. Można zaplanować dojście do idealnego stanu na dłuższy, kilkuletni okres. SAMM dostarcza także definicje i narzędzia do pomiaru skuteczności działań związanych z bezpieczeństwem aplikacji. W wersji 2.0 (planowanej na 2018/2019 rok) pojawi się też możliwość porównywania z innymi organizacjami. Zanonimizowane dane z różnych organizacji pozwolą każdemu na benchmarking.

Metoda małych kroków

Paweł Krawczyk, specjalista bezpieczeństwa informacji w Krawczyk Industries Ltd, podczas prezentacji „Wdrażanie strategii bezpieczeństwa oprogramowania" zwracał uwagę, że na bezpieczeństwo SDLC warto spojrzeć z różnych perspektyw. Wielu ekspertów ds. bezpieczeństwa dostrzega jedynie luki. Tymczasem warto przyjrzeć się kwestiom bezpieczeństwa także z perspektywy deweloperów.

„Większość realizowanych projektów to nie są nowe przedsięwzięcia. Mamy działające, krytyczne systemy biznesowe w produkcji. Są aplikacje, które powstały ponad 20 lat temu na potrzeby wewnętrzne, w bezpiecznej sieci, a dziś zaczyna im się stawiać zupełnie inne wymagania. Systemy napisane dla niewielkiej organizacji z czasem zaczynają obsługiwać ogromne przedsiębiorstwa" – mówił Paweł Krawczyk.

Czy takie systemy są bezpieczne? Czy do środka sieci można przeniknąć? Zdaniem Pawła Krawczyka, można. „Niezależnie od tego, jak zabezpieczymy perymetr, jest prawdopodobne, że ktoś i tak będzie w stanie dokonać włamania. Przepisanie takiego systemu jest nierealne. Do tego system musi cały czas działać. Dlatego w większości przypadków najlepszym rozwiązaniem są działania polegające na stopniowym podnoszeniu bezpieczeństwa poprzez wykonywanie małych kroków. Przykładowo, można wyizolować sieci wrażliwe, co pozwala takie starsze aplikacje ukryć" – uważa Paweł Krawczyk.

Co konkretnie można zrobić? Pierwszym krokiem może być odizolowanie sieci stacji roboczych od sieci serwerowych oraz ograniczenie dostępu do aplikacji wrażliwych poprzez uruchomienie firewalla na serwerze. Takie działania są łatwe do realizacji. Choć nie zapewnią od razu wysokiego poziomu bezpieczeństwa, to pozwolą na jego znaczące podniesienie – w prosty sposób, bez przerywania pracy aplikacji.

Można także izolować procesy. Starsze aplikacje czasem działają na przestarzałych, niebezpiecznych frameworkach. W takich przypadkach można użyć np. Dockera, który pozwala na izolowanie przy zachowaniu starego środowiska, starej aplikacji i bilioteki, ale przy użyciu współczesnego kernela, polityki bezpieczeństwa AppArmor czy SELinux. Inny przykład to Waratek oferujący AppArmor dla JAVA JRE, emulację starych wersji API, polityki bezpieczeństwa oraz RASP – Run Time Self Protection.

Warto także usuwać nieużywane komponenty oraz czyścić kod. Duże aplikacje kumulują stary kod. Chodzi więc

o blokowanie odwołań na poziomie web proxy, logowanie odwołań funkcji planowanych do usunięcia, a także usuwanie kodu źródłowego.

Bezpieczne DevOps

Na szczególną uwagę zasługuje coraz bardziej popularna metodyka DevOps. „Wykorzystywane na różnych etapach ‚linii produkcyjnych' DevOps klucze i hasła do uwierzytelniania wymagają odpowiedniego zabezpieczenia. Dlatego bezpieczeństwo w tym kontekście staje się coraz bardziej krytycznym zagadnieniem" – tłumaczył Alex Wilson, DevSecOps Lead w CyberArk.

DevOps realizuje się przez współpracę i zautomatyzowane zadania. Wymagana jest także odpowiednio przygotowana, działająca automatycznie infrastruktura. Przynosi to ogromne korzyści. Analitycy z Gartnera przekonują o 46-krotnym zwiększeniu częstotliwości wdrożeń, 96-krotnie szybszym odtwarzaniu po błędach, 440-krotnie szybszym czasie wprowadzania zmian, a przy tym 5-krotnie mniejszym wskaźniku awaryjności. Ze względu na te ogromne korzyści DevOps powoli staje się normą.

Organizacje stawiają na DevOps, żeby przyspieszać innowacje. Tradycyjne rozwiązania do zarządzania tożsamością i dostępem nie są jednak w stanie obsłużyć takich przepływów pracy. Dlatego potrzebne są nowe rozwiązania, które zapewnią bezpieczeństwo bez spowalniania tempa dostarczania oprogramowania.

Powszechne wykorzystywanie narzędzi pozwalających na automatyzowanie procesów DevOps oznacza, że realizowane do niedawna przez człowieka w formie interaktywnego procesu obecnie zaczynają być wykonywane przez automaty, boty. To właśnie dzięki narzędziom automatyzującym można osiągnąć wspomniane wcześniej korzyści. Te roboty stają się w praktyce uprzywilejowanymi użytkownikami – jeszcze kilka lat temu byli to ludzie.

W efekcie cały ten proces w zakresie tworzenia aplikacji i usług nie jest zabezpieczony na odpowiednim poziomie, m.in. pod względem podziału obowiązków czy jeśli chodzi o audyt obejmujący roboty. Jest to doskonale widoczne, gdy porównany istniejące w tym zakresie mechanizmy do środków zabezpieczających, jakie stosowane są w przypadku interaktywnych użytkowników będących ludźmi.

W stosunkowo krótkim czasie udało się zaobserwować pierwsze efekty tego stanu rzeczy. Można wskazać przynajmniej kilka znanych przykładów organizacji, które były niedostatecznie pod tym względem zabezpieczone i dające ogromne uprawnienia klucze uwierzytelniające zostały przez pomyłkę udostępnione publicznie. Istnieją także udokumentowane przypadki

Promowanie bezpieczeństwa nie może ograniczać się wyłącznie do deweloperów. Pełne zrozumienie zagrożeń i konieczności uwzględnienia odpowiednich wymagań musi pojawić się także po stronie osób zlecających projekty. Funkcjonalność i czas nie mogą stanowić jedynych priorytetów podczas tworzenia oprogramowania.

wycieków danych, które były efektem upublicznienia kluczy API dających szeroki dostęp do infrastruktury organizacji. Pomyłkowo przesłano je do publicznych repozytoriów kodu. W takim przypadku atakujący nie potrzebuje szczególnych umiejętności technicznych, żeby zyskać dostęp do środowiska i wszystkich znajdujących się w nim wrażliwych danych.

Narzędzia nowej generacji

„W świecie DevOps wykorzystuje się mnóstwo nowych narzędzi wymagających uwierzytelniania. Rzadko jednak stosuje się do nich takie same zasady jak do innych używanych w organizacji systemów. Przez to powstają 'wyspy bezpieczeństwa" – mówił Alex Wilson. I dodawał: „Linie DevOps są w pełni zautomatyzowane. W wielu miejscach trzeba umieścić tajne informacje służące do uwierzytelniania, żeby przepływ mógł być realizowany bez interwencji człowieka. To ogromne pole ataku".

CyberArk Conjur to zautomatyzowane rozwiązanie do zarządzania sekretnymi informacjami uwierzytelniającymi. Narzędzie dostosowane jest do wymagań chmury oraz środowisk DevOps. Pomaga zespołom IT oraz pionu bezpieczeństwa zarządzać kluczami i hasłami używanymi przez „maszyny" (aplikacje, mikrousługi, narzędzia, interfejsy API), a także użytkowników w skali całej linii DevOps.

Conjur jest w stanie obsłużyć środowiska skonteneryzowane, a przy tym może być uruchomiony lokalnie lub w dowolnej chmurze. Opiera się na mechanizmach RBAC (Role Based Access Control), dzięki czemu zróżnicowane przywileje mogą być przyznawane grupom użytkowników lub maszyn. Rozwiązanie integruje się z narzędziami Continuous Integration/Continuous Deployment (Ansible, Ched, Jenkins, Puppet) oraz platformami kontenerowymi, takimi jak Docker. Integruje się także z istniejącymi systemami i praktykami bezpieczeństwa.

> Powszechne wykorzystywanie narzędzi pozwalających na automatyzowanie procesów DevOps oznacza, że zadania realizowane do niedawna przez człowieka w formie interaktywnego procesu obecnie zaczynają być wykonywane przez automaty. Te roboty stają się w praktyce uprzywilejowanymi użytkownikami. To wymaga nowego podejścia do bezpieczeństwa.

„Włączenie bezpieczeństwa w procesy DevOps bez utraty korzyści płynących z tego modelu jest możliwe" – twierdzi Alex Wilson. Przede wszystkim należy zrozumieć, że celem DevOps jest zwiększenie szybkości procesów wytwarzania oprogramowania. Trzeba uważać, żeby stosowane zabezpieczenia nie wpłynęły na zatrzymanie procesów i nie zniwelowały zysków czasowych wynikających z ciągłej integracji oraz ciągłego dostarczania rozwiązań. Kluczowe znaczenie, zdaniem Alexa Wilsona, ma zatem to, żeby włączyć zespół bezpieczeństwa na takich samych zasadach, które pozwalają automatyzować i przyspieszać współpracę pomiędzy zespołami programistów i operacyjnymi. Należy dostarczyć usługi bezpieczeństwa, które nie spowolnią procesów i przepływów pracy.

ADVANCED THREAT SUMMIT 2017

Srebrne kule nie istnieją

Niezbędna technologia jest dostępna. Potrzeba pojedynczej konsoli, która obejmie wszystkie elementy i źródła danych. Później należy skoncentrować się po prostu na nudnej robocie. Rozmowa ze **Stuartem McKenzie**, wiceprezesem Mandiant, FireEye.

Czego w zakresie cyberbezpieczeństwa nauczył nas rok 2017?

W tym roku mogliśmy zaobserwować dalszą ewolucję w zakresie aktywnych podmiotów i źródeł zagrożeń. Mamy do czynienia z coraz większą liczbą działań z krajów, których nie uznaje się za światowe mocarstwa. Obserwujemy wzrost wyrafinowania Irańczyków, którzy działają na coraz większą skalę. Jesteśmy celem nieustannych ataków Korei Północnej. Przy tym Koreańczycy obierają sobie nietypowe cele. Byli powiązani z WannaCry oraz atakami na transfery międzybankowe. To sugeruje, że próbują w ten sposób pozyskiwać pieniądze. To przykład zacierania się granic pomiędzy różnymi grupami podmiotów prowadzących działania w cyberprzestrzeni – pod względem celów i motywacji.

Rok 2017 będzie prawdopodobnie znaczący ze względu na ataki przy wykorzystaniu destrukcyjnego, złośliwego oprogramowania na terenie Europy. Wcześniej występowało to na Bliskim Wschodzie. Działania tego typu obserwowaliśmy przez lata w Arabii Saudyjskiej. Pierwszy atak Shamoon został przeprowadzony w 2012 roku. Teraz doświadczyliśmy czegoś podobnego w Europie. Ransomware i destrukcyjny kod dotarły na Stary Kontynent. Sądzę, że ten trend będzie się nasilać.

Prawdopodobnie kolejny znaczący trend to nasilenie operacji propagandowych. Rosja w otwarty sposób uprawia propagandę na Twitterze, Facebooku i w innych mediach społecznościowych. Działania tego typu się wzmagają. Nie jest to nowość, propaganda istniała zawsze. Nowością jest nachalność tych działań

oraz, być może, towarzysząca im naiwność odbiorców. Wydaje się, że wszyscy bezrefleksyjnie akceptują wiadomości tego typu. Wiele mediów opisuje zdarzenia, które zostały nam podane przez roboty. Należy zastanowić się nad edukacją w tym obszarze.

Wspomniał Pan o ataku Shamoon w 2012 roku. Dlaczego wcześniej nie było podobnych ataków w Europie?

Jeśli spojrzymy na oryginalny atak Shamoon, to zobaczymy, że mieliśmy do czynienia z Irańczykami, którzy doszli do wniosku, że mogą nie kryć swoich działań. W owym czasie Chiny i Rosja nie decydowały się na taką otwartość. Kiedy badaliśmy przypadki rosyjskich ataków na terenie Unii Europejskiej czy w USA, mieliśmy do czynienia z „duchami". Wiedzieliśmy, że nastąpił atak, badaliśmy go, ale sprawcy już dawno zniknęli. Wykorzystywali oni bardzo zaawansowane technologie, głównie działające w pamięci, które zostawiają niewiele śladów.

W ciągu ostatniego roku mogliśmy zaobserwować, zwłaszcza u Rosjan, przekonanie, że ani Europa, ani Ameryka nie są dostatecznie silne, żeby nałożyć na nich sankcje. Postanowiły, że będą działać zdecydowanie i prawie całkiem otwarcie. Takie właśnie podejście od wielu lat mieli Irańczycy.

Rosjanie rozumieją, że Europa jest prawdopodobnie obecnie za bardzo skoncentrowana na GDPR i zmianach krajobrazu politycznego. To, co byłoby nie do zaakceptowania, powiedzmy, pięć lat temu, dzisiaj nie spotka się ze zdecydowaną reakcją. Możemy się spodziewać, że wkrótce także inne kraje zaczną napinać swoje muskuły i pokazywać, co potrafią. Podobnie cyberprzestępcy dostrzegli, jak niewiele rządy są w stanie zrobić, żeby ich powstrzymać. Egzekwowanie prawa pomiędzy różnymi jurysdykcjami jest bardzo trudne. Cyberprzestępcy oceniają, że stosunek ryzyka do potencjalnej nagrody jest obecnie dla nich bardzo korzystny.

Czy Rosja jest dziś głównym zagrożeniem w skali globalnej?

Nie dotarło to do szerokiej publiczności, ale znaczący był także atak przeprowadzony przez APT10. To chińska grupa, która naruszyła bezpieczeństwo globalnych łańcuchów dostaw. W ciągu kilku ostatnich lat niewiele słyszało się o Chinach w tym kontekście. Nie mieliśmy do czynienia z atakami na masową skalę, takimi, jakie można było obserwować w 2012 roku, przed dojściem Xi Jinpinga do władzy. Od 2006 do 2012 roku mieliśmy do czynienia z wieloma atakami i cyberszpiegostwem prowadzonym przez grupy z Chin. Wówczas FireEye raportował, że udało się nam powstrzymać wiele chińskich ataków, ale większość

Wiele organizacji przekazało w outsourcing monitoring bezpieczeństwa, myśląc, że dokonało zarazem outsourcingu ryzyka. To błędne przekonanie. Warto przemyśleć, co przekazuje się w outsourcing. Nie można przekazać swoich stacji roboczych i oczekiwać, że ktoś będzie nimi zarządzał.

Stuart McKenzie,
wiceprezes Mandiant,
FireEye

obserwatorów nie traktowała tego poważnie. Tymczasem była to prawda.

Teraz, przez ostatnie 18 miesięcy, chińska grupa APT10 infiltrowała globalne łańcuchy dostaw. Udało się jej uzyskać informacje kluczowe dla biznesu prowadzonego przez wiele organizacji. To niebezpieczny czas dla biznesu. Wiele organizacji przekazało w outsourcing monitoring bezpieczeństwa, myśląc, że dokonało zarazem outsourcingu ryzyka. To błędne przekonanie. Warto przemyśleć, co przekazuje się w outsourcing. Nie można przekazać swoich stacji roboczych i oczekiwać, że ktoś będzie nimi zarządzał.

Podczas „Advanced Threat Summit 2017" wielokrotnie mówiono, że należy zabezpieczać raczej dane, a nie zasoby fizyczne. Ludzie zaczynają to rozumieć. Po części to efekt GDPR i będzie dużym wyzwaniem dla wielu organizacji.

Nie wymienił Pan jeszcze żadnych technologii. Czy są jakieś nowości, które pojawiły się w ciągu ostatnich miesięcy, na które warto zwrócić uwagę?

Szczerze mówiąc, kluczem jest integracja informacji na jednym ekranie. Dzięki temu można połączyć wszystkie działania w obszarze bezpieczeństwa i naprawdę zrozumieć, co się dzieje w danej chwili. Dla nas oznacza to migrację w kierunku FireEye Helix, który integruje wszystkie nasze informacje, a także produkty bezpieczeństwa wszystkich pozostałych dostawców. Dzięki temu otrzymujemy jeden ekran, na którym można obserwować, co się dzieje. To kluczowa sprawa.

Organizacje nie muszą poszukiwać nowości. Większość problemów, o których mówimy, została już rozwiązana. Mamy przyzwoite technologie uczenia maszynowego i wykrywania anomalii. Są

wystarczające. Nie musimy wracać do pracy nad nimi. Na rynku dostępne są bardzo dobre produkty do ochrony końcówek. Jednym z nich jest HX. Dobrze pokryty jest obszar sieci.

Organizacje muszą natomiast skoncentrować się na łączeniu informacji zamiast analizowania logów z wielu źródeł. Prawdopodobnie najważniejszą rolę odegra w tym analityka zagrożeń. Spodziewam się, że posiadanie takiego „jednego ekranu" będzie priorytetem dla wielu organizacji. Dalej pozostaje już tylko skoncentrowanie się na nudnej robocie – instalowaniu łatek, zarządzaniu użytkownikami, upewnianiu się, że wycofujemy z użycia przestarzałe systemy operacyjne. Niezbędna technologia jest dostępna. Trzeba przestać szukać srebrnej kuli.

Dlaczego zabezpieczenie stacji końcowych jest tak ważne?

Jeśli nie jesteśmy w stanie kontrolować końcówek, wówczas nie ma nadziei na to, że będziemy w stanie zarządzać siecią. Zbyt wiele organizacji polega na ochronie antywirusowej. Tymczasem to zaledwie cyberhigiena. To podstawa i nic więcej. Ochrona antywirusowa zapewnia ochronę przed najbardziej oczywistymi, najbardziej widocznymi, prostymi atakami. Z pewnością jednak nie wystarcza. Porządna technologia ochrony końcówek jest w stanie zablokować zaawansowane zagrożenia, a następnie umożliwia prowadzenie dochodzenia.

Czego Europa może dziś nauczyć się od innych regionów świata w kontekście cybrebezpieczeństwa?

Możemy nauczyć się wiele od Amerykanów, zwłaszcza w obszarze raportowania naruszeń bezpieczeństwa. Informowanie opinii publicznej o naruszeniach w odpowiedzialny sposób jest szczególnie ważne. Trudno uwierzyć, patrząc na liczbę upublicznionych zdarzeń, że w Unii Europejskiej jest tak niewiele ataków. Wiemy z pewnością, że ataków jest więcej, ale nikt nie jest zobligowany, żeby o nich informować. Przez to prawdopodobnie organizacje nie koncentrują się dostatecznie na tym obszarze – bo nie jest to sprawa publiczna. Wyciągnięcie wniosków z doświadczeń amerykańskich w tym zakresie uważam za istotne.

Czego możemy spodziewać się w 2018 roku?

Wzrosną trudności związane z określaniem źródeł ataków. Sądzę, że będzie coraz trudniej odróżniać atakujących oraz określać, co jest ich ostatecznym celem. Właśnie dlatego niezwykle ważne będzie zrozumienie przez organizacje, że kluczem jest ochrona sieci, a nie przesadne zastanawianie się nad tym, „kto, co i dlaczego".

Firmy muszą skoncentrować się na łączeniu informacji zamiast analizowania logów z wielu źródeł. Prawdopodobnie najważniejszą rolę odegra w tym analityka zagrożeń. Posiadanie „jednego ekranu" będzie priorytetem dla wielu organizacji. Pozwoli on naprawdę zrozumieć, co się dzieje w danej chwili.

ADVANCED THREAT SUMMIT 2017

ADVANCED
THREAT

DARKTRACE

AT SUMMIT
ROUNDTABLES

ADVANCED
THREAT
SUMMIT 2017

Wydajność i wygoda użytkowników vs kontrola sprawowana przez działy IT – jak to ze sobą pogodzić

Moderator:
Bogdan Lontkowski, Regional Director PL, CZ, SL, Baltics, Ivanti

Zasadniczo możliwe jest zachowanie równowagi pomiędzy wolnością i wydajnością użytkowników a kontrolą, jaką działy IT muszą zapewnić, żeby organizacja była bezpieczna. W tym kontekście największą rolę odgrywa codzienna, cyfrowa „higiena". Przy tym postępowanie użytkowników musi być świadome. Do osiągnięcia takiego stanu konieczna jest edukacja. Wszyscy muszą doskonale zdawać sobie sprawę z istniejących zagrożeń. Tylko w ten sposób można wyeliminować najprostsze, a często najbardziej niebezpieczne błędy.

Oczywiście, nie można się do tego ograniczać. Działy IT powinny aktywnie wspierać użytkowników, żeby chronić ich przed zalewem potencjalnie niebezpiecznych treści, które mogą przynosić organizacji negatywne skutki. Jednocześnie muszą zapewnić przeciwdziałanie tym skutkom, kiedy się one pojawią.

Wreszcie zbudowanie świadomości wśród użytkowników oraz wyposażenie działu IT w odpowiednie narzędzia wymagają prowadzenia dialogu z zarządami organizacji i przekonywania, argumentowania, żeby zatwierdzone zostały wydatki, które pozwalają chronić biznes.

To trzy zasadnicze warunki, które pozwalają zapewnić równowagę pomiędzy wydajnością i wygodą a kontrolą.

Machine Learning jako cel ataku i jako metoda obrony

Moderator:
Leszek Tasiemski, VP, Rapid Detection Center, R&D Radar & RDS, F-Secure

Jesteśmy we wczesnej fazie adaptacji technologii uczenia maszynowego. To normalne na tym etapie rozwoju, że towarzyszy jej wiele niepewności. To faza eksperymentowania, faza sprawdzania pełnego spektrum możliwości nowej technologii. Niemniej już teraz ważne jest urealnienie oczekiwań. Powinniśmy zdać sobie sprawę, w czym uczenie maszynowe się sprawdza i w czym może nam pomóc. Z drugiej strony, powinniśmy uświadomić sobie, gdzie dajemy się ponieść fantazji i myślimy raczej o sztucznej inteligencji, a nie o uczeniu maszynowym. W przeciwnym wypadku może nas spotkać przykry zawód i rozczarowanie. Już wkrótce czeka nas przejście od obecnej fazy gadżetu, pobocznej funkcjonalności do fazy produktu, co sprawi, że wzrośnie atrakcyjność mechanizmów uczenia maszynowego jako celu ataku.

Podczas dyskusji poruszony został także temat trudności związanych z testowaniem algorytmów uczenia maszynowego. Mamy do czynienia z matematyczną czarną skrzynką. Niestety, nie wiemy, jak testować integralność takiej wewnętrznej bazy wiedzy. Możemy szukać analogii do tego, co się dzieje w świecie ludzkim, jak prowadzone są analizy. W przyszłości potrzebne będą jednak mechanizmy kontroli nad decyzjami systemu uczenia maszynowego. Być może uda się do tego wykorzystać kolejną warstwę uczenia maszynowego, która będzie kontrolować decyzje podejmowane przez warstwę niższą.

Epidemia ransomware – czy warto walczyć z ransomware, skoro być może jesteśmy nieodwołalnie skazani na porażkę?

Moderator:
Marcin Krzemieniewski, Business Line Manager – Security, Dimension Data Polska

Kluczową konkluzją dyskusji było stwierdzenie, że najważniejszym elementem ochrony infrastruktury, także przed zagrożeniami typu ransomware, jest edukacja użytkowników. Nikt nie miał co do tego wątpliwości. Wszyscy chętnie podzielili się swoimi doświadczeniami w tym zakresie. Okazało się, że powszechne jest nie tylko szkolenie użytkowników, ale także testowanie poszczególnych działów, kadry kierowniczej oraz szeregowych pracowników pod kątem tego, w jakim stopniu lekcje zostały zapamiętane. Tego typu działania doskonale się sprawdzają. Jeśli ktoś raz dał się złapać na prowokację, to najczęściej na drugi raz jest o wiele bardziej uważny. Co więcej, stara się propagować nabytą wiedzę wśród członków swojego zespołu.

Uczestnicy dyskusji doszli także do wniosku, że choć niewątpliwie narzędzia mogą stanowić doskonałe wsparcie, to nie zabezpieczają organizacji w 100%. Cyberprzestępca zawsze jest w stanie wymyślić scenariusz, na jaki my z pewnością nie wpadniemy, a także zastosować techniki, które wykorzystają luki w posiadanym przez nas zestawie narzędzi. Dlatego niezwykle ważne jest posiadanie planów działania odnoszących się do realnego ataku. Nie muszą być doskonałe, ale pomogą przetrwać i wydobyć się z problematycznej sytuacji.

Wpływ wirtualizacji na bezpieczeństwo sieci (wirtualizatory, maszyny wirtualne, kontenery, rekomendacje NIST, GDPR, ISO, usługi chmurowe, detekcja, blokowanie i usuwanie zagrożeń)

Moderatorzy:
Piotr Jabłoński, Senior Systems Engineer, Vmware,

Mikołaj Wiśniak, menedżer inżynierów systemowych, VMware

Zabezpieczenie i widoczność aplikacji w warstwie wirtualnej są obecnie szczątkowe. Zmiana tej sytuacji wymaga przede wszystkim zastosowania dobrego narzędzia monitoringu, które pozwoli zbudować świadomość, co dzieje się w danej chwili z aplikacjami. Wykorzystanie takiego

rozwiązania może wiązać się z koniecznością wyjścia poza silos danego departamentu, infrastruktury wirtualnej i sieci czy pionu bezpieczeństwa. Konieczne jest przyjęcie holistycznego podejścia, które będzie obejmować wiele obszarów. W tym kontekście dobrym pomysłem może okazać się cloud computing. Chmura publiczna, zwłaszcza z serwerami fizycznie ulokowanymi na terenie Polski, może zapewnić odpowiednią ochronę danych, a zarazem przekonać sceptyków. Należy przy tym zwrócić uwagę na konkretne zapisy w umowie. Ważne jest, żeby wynegocjować warunki, które zagwarantują maksymalną ochronę administratora danych osobowych.

Skuteczność ochrony w dobie zaawansowanych cyberzagrożeń

Moderator:
Wojciech Ciesielski, Major Account Manager, Fortinet

W trakcie wielowątkowej dyskusji udało się sformułować pewnego rodzaju rekomendację: ochrona informacji powinna rozpocząć się od klasyfikacji posiadanych informacji, a następnie należy stworzyć odpowiednią politykę i wdrożyć narzędzia, które pomogą te informacje w odpowiedni sposób zabezpieczyć. Wymagane jest jednocześnie, żeby firmowa infrastruktura, architektura bezpieczeństwa, znajdowała się na odpowiednimi poziomie dojrzałości. Tylko spełnienie tego warunku pozwala na wykrywanie zagrożeń, a także ocenianie skutków ataków, które dotknęły organizację.

W tym kontekście ciekawym zagadnieniem jest implementacja rozwiązań klasy SIEM. Jeśli rozpoczyna się taki projekt, to kluczowe jest dopasowanie narzędzi do konkretnych potrzeb. W przeciwnym wypadku osiągnięty efekt jest wręcz odwrotny do zamierzonego.

W dyskusji poruszony został również temat threat intelligence. Uczestnicy wskazywali, że konieczna jest wymiana informacji między różnymi podmiotami. Często jednak jest tak, że nie dzielimy się informacją, co ogranicza skuteczność wymiany i potencjalne korzyści.

Ochrona na poziomie DNS

Moderator:
Piotr Głaska, Senior Systems Engineer, Infoblox

Temat ochrony na poziomie DNS cieszy się coraz większym zainteresowaniem. Dyskusja potwierdziła jednak, że wciąż traktowany jest jako nowość. Niewiele firm posiada takie zabezpieczenia. Raczej na razie organizacje jedynie przyglądają się tego typu rozwiązaniom, ewentualnie zastanawiając się, w jakim miejscu umieścić je pośród priorytetów ogólnej strategii cyberbezpieczeństwa.

Jednym z dyskutowanych zagadnień była możliwość blokowania na bazie DNS i list reputacyjnych dostępu do określonych domen. Rozważano stosowanie „białych list" oraz „czarnych list". Uczestnicy dzielili się doświadczeniami płynącymi z różnych strategii. Okazało się, że w jednej z instytucji finansowych świetnie sprawdza się model, w którym ruch jest całkowicie zablokowany dla użytkowników. Muszą oni dodatkowo kliknąć przycisk na stronie, żeby dodać ją do białej listy. W innej, dużo większej instytucji finansowej taki model już się jednak nie sprawdził w praktyce. Z kolei uczestnik pracujący dla firmy z sektora zależnego od państwa stwierdził, że zastosowanie białych list nie wchodzi w grę. Okazuje się, że choć wszyscy mierzą się z tymi samymi problemami, niemożliwe jest zastosowanie jednego rozwiązania.

Na koniec poruszony został temat zabezpieczenia infrastruktury publicznego DNS. Wniosek, do jakiego doszli uczestnicy, jest taki, że nie warto wkładać „wszystkich jajek do jednego koszyka", czyli lepiej nie umieszczać serwerów DNS wyłącznie we własnym środowisku.

Strategia bezpieczeństwa IT – czy i jak dalece wspiera realizowanie zaleceń RODO

Moderatorzy:
Urszula Ptak-Małysiak, Senior Account Manager oraz Senior Partner Account Manager, Citrix,

Magdalena Ostrowicz, Senior Partner Account Manager, Citrix

Z punktu widzenia strategii IT problemy do rozwiązania za pomocą technologii i narzędzi związanych z RODO można podzielić na trzy grupy. Po pierwsze, centralizacja ochrony danych, kontrolowanie dostępu do danych, optymalizacja bezpiecznego dostępu z każdego urządzenia to wymagania zapisane wprost w wytycznych RODO. W tym zakresie potrzebne są systemy i rozwiązania, które umożliwiają realizację tego w najtańszy czy najmniej ingerujący w aplikacje i systemy sposób. Przy tym nie mogą zaburzać istniejących procesów i spełniających inne wymogi polityk bezpieczeństwa w danej organizacji. Po drugie, ochrona i zabezpieczenie danych przed niekontrolowanym wyciekiem, kradzieżą czy nieautoryzowanym dostępem. To kolejne zagadnienie, które wymaga zastosowania nie tylko polityk i zasad bezpieczeństwa, ale także wprowadzenia narzędzi IT, które zapobiegną tego typu sytuacjom. Wreszcie po trzecie, wymagania związane z realizacją prawa do bycia zapomnianym. Kluczowy problem to zapewnienie definitywnego usunięcia danych zgłoszonych do zapomnienia we wszystkich miejscach, w tym również w archiwach, zasobach skopiowanych na desktopy czy zapisanych w mailach lub załącznikach do nich. Podsumowując, wprowadzenie RODO wymaga strategicznego zaangażowania i współpracy z działami IT. Ważne, żeby nie zwlekać do chwili, w której pojawią się problemy, ale działać już na etapie audytu i przygotowania procedur oraz procesów.

Pozyskiwanie odpowiednio wykwalifikowanych ekspertów do zapewnienia bezpieczeństwa IT – różne modele w sytuacji deficytu na rynku pracy

Moderator:
Tomasz Sawiak, wicedyrektor w zespole Cyber Security, PwC

Sytuacja na rynku pracy jest wyjątkowo korzystna dla ekspertów odpowiedzialnych za zapewnienie bezpieczeństwa IT. To pracodawcy konkurują o pozyskanie pracowników. Brak równowagi w tym obszarze rynku pracy jest ewidentny.

Dlatego – na co zwracano uwagę w trakcie dyskusji – outsourcing części usług i procesów wspierających to godna rozważenia opcja. Dzięki temu osoby obecnie tworzące zespół będą mogły skoncentrować się na kluczowych z punktu widzenia podstawowego biznesu zadaniach, takich, które wygenerują największą wartość dodaną. Należy przy tym jednak pamiętać, że podobnie jak w przypadku każdego outsourcingu, taki wybór rodzi dodatkowe ryzyka. Outsourcing wymaga po stronie usługobiorcy podjęcia działań związanych z nadzorem oraz kontrolowaniem jakości dostarczanych usług. Ponadto konieczne są dodatkowe kwalifikacje.

W tej sytuacji warto rozważyć model cosourcingowy, w którym usługodawca oddelegowuje do klienta wyznaczonych pracowników. Takie podejście umożliwia pozyskanie wykwalifikowanej kadry i wspólną pracę z oddelegowanym zespołem w mieszanym środowisku. Ostatecznie sprzyja to transferowi wiedzy do wewnętrznych zespołów firmy i rozwojowi wewnętrznych kompetencji. W modelu cosourcingowym firmy rozwijają swoje procesy i know-how, przez co nie występuje problem uzależnienia od firm zewnętrznych.

Pełna wizualizacja stanu podatności i konfiguracji w czasie rzeczywistym – czy i kiedy potrzebujemy, czy jest cel do osiągnięcia oraz jak dużymi nakładami sił i środków

Moderator:
Marek Skalicky, dyrektor zarządzający, Qualys

Dyskusja skoncentrowała się wokół najbardziej efektywnych narzędzi pozwalających na zabezpieczenie przed naruszeniem firmowej infrastruktury i danych. Uczestnicy zgodzili się, że kluczowe znaczenie ma komplet przejrzyście podanych informacji na temat wszystkich zasobów i wszystkich komponentów infrastruktury. Zasadniczo jest bowiem tak, że jeśli czegoś nie widzimy, nie jesteśmy tego w stanie kontrolować ani zabezpieczyć.

Informacje na temat zasobów i stanu bezpieczeństwa są ważne nie tylko z punktu widzenia podstawowej infrastruktury, ale i całego środowiska organizacji. Każdy system jest przecież tak bezpieczny jak jego najsłabsze ogniwo. Dlatego nie można skoncentrować się wyłącznie na systemach produkcyjnych i jednocześnie ignorować systemy partnerów w łańcuchu dostaw podłączone do naszej infrastruktury. Nie można pominąć także systemów końcowych. Właśnie przez te elementy infrastruktury może zostać przeprowadzony skuteczny cyberatak.

Ważna jest także inwentaryzacja oraz klasyfikacja danych. Pozwala to odpowiednio ustawić priorytety. Nie wszystkie zasoby w ten sam sposób obsługują dane, dlatego inaczej należy określić dla nich priorytety. Pozostała infrastruktura musi działać zgodnie z podstawowymi zasadami bezpieczeństwa.

Syndrom Zero Day

Moderator:
Stuart McKenzie, Vice President Mandiant, FireEye

Dyskusja o podatnościach typu Zero Day rozpoczęła się od rozmowy o konkretnych przykładach rozwiązywania tego problemu oraz ich sposobach. Następnie skierowała się ku zagadnieniom szkoleń dla użytkowników i budowania wśród nich świadomości zagrożeń. Choć konieczność prowadzenia szeroko rozumianej edukacji nie budzi kontrowersji, to nadal dla wielu organizacji stanowi spore wyzwanie.

Kilku uczestników dyskusji mówiło również o tym, że ważna jest odpowiednia klasyfikacja alertów oraz odpowiednia klasyfikacja posiadanych zasobów. Należy wiedzieć, który alert jest istotny i niebezpieczny oraz jakie zasoby są najważniejsze – nie da się skupić na wszystkim.

Na koniec okazało się, że syndrom Zero Day nie jest tak bardzo poważnym zagrożeniem. Po pierwsze, tych podatności nie ma dużo. Po drugie, jest to jeden z droższych sposobów na włamanie się do sieci. Po trzecie, jeżeli ktoś chce jeszcze dodatkowo użyć kilku podatności Zero Day, żeby zaatakować przez kilka wektorów, to wówczas mówimy o atakach targetowanych APT – a takie ataki stanowią wyjątki. W związku z tym największe znaczenie ma cyberhigiena, czyli zwracanie uwagi na to, że bezpieczeństwo jest procesem. Nie polega wyłącznie na detekcji i prewencji; konieczna jest również analiza, odpowiednie reagowanie i bieżąca praca nad poprawą stanu bezpieczeństwa.

Rola ochrony endpoint w przełamaniu Kill Chain – techniki zapobiegania zagrożeniom na urządzeniu końcowym

Moderator:
Lech Lachowicz, kierownik Działu Inżynierów Systemowych, Symantec

Dzięki temu, że w dyskusji brali udział przedstawiciele różnych sektorów gospodarki, a przy tym zajmujący różne stanowiska w hierarchii organizacyjnej, jej charakter był żywiołowy i nieprzewidywalny. Ujawniło się kilka ciekawych wniosków. Pierwszy dotyczył stacji końcowych. To nadal istotny element całego systemu ochrony. Co więcej, można nawet powiedzieć, że odgrywa kluczową rolę w przełamywaniu ataków. Zazwyczaj jest bowiem źródłem, celem, a zawsze narzędziem, które jest wykorzystywane do przeprowadzenia skutecznych ataków. Dlatego właśnie ochrona stacji końcowej jest obecnie ważniejsza niż kiedykolwiek wcześniej.

Technik ochrony końcówek jest bardzo wiele. W tym kontekście dużo czasu poświęcono czystemu whitelistingowi. Okazuje się, że choć jest to temat trudny, to jednak skuteczny. Ostatnim wnioskiem jest stwierdzenie, że procedury reagowania na incydenty coraz częściej są skoncentrowane właśnie na stacjach końcowych. Wobec tego potrzebne są narzędzia i procedury, które w procesie odpowiedzi na atak uwzględniają końcówki.

Certyfikacja bezpieczeństwa produktów i usług ICT a jednolity rynek cyfrowy w Unii Europejskiej

Moderator:
dr inż. Elżbieta Andrukiewicz, ekspert, Polski Komitet Normalizacyjny

Główną siłą napędową wzrostu zainteresowania certyfikacją w obszarze bezpieczeństwa jest RODO, które zakłada mechanizmy certyfikacji jako mechanizmy wykazywania zgodności. Czy w obliczu tych nowych regulacji jakiś element certyfikacji będzie obowiązkowy? Bardzo możliwe, że tak będzie. Jeśli tak, to z pewnością wymóg ten będzie dotyczył infrastruktury krytycznej, operatorów usług kluczowych oraz zamówień publicznych.

Uczestników dyskusji interesowało, jakie najważniejsze cechy takiej certyfikacji powinny być brane pod uwagę. Po pierwsze, zastosowane rozwiązania powinny być uznawane w całej Europie, a najlepiej w całym świecie. Po drugie, powinny obejmować w szczególności weryfikację oprogramowania i certyfikację oprogramowania. Wreszcie powinna być zastosowana dojrzała metodyka.

Dyskusja skoncentrowała się na jedynej dojrzałej metodyce oceny, jaką są Common Criteria, czyli norma 15408. W tym aspekcie obejmuje ona jedynie częściowo to, co tak naprawdę jest potrzebne na rynku. Wynika to z faktu, że gdy się weźmie pod uwagę czas trwania oceny certyfikacji oraz jej elastyczność, a zatem również i koszty, to są one jeszcze stanowczo za wysokie.

Rok 2018 będzie kluczowy dla certyfikacji i należy się spodziewać odpowiednich regulacji w tym zakresie.

IT w obronie OT, czyli jak ochronić kolosa na glinianych nogach

Moderator:
Łukasz Staniak, Manager, Cyber Security, KPMG Advisory

Architektura OT nie została stworzona z myślą o gwarantowaniu bezpieczeństwa. Jej głównym zadaniem jest zapewnienie dostępności systemów. Odpowiedź na pytanie, czy ma szansę sama się obronić, jest oczywista. Właściwe pytanie brzmi: jakie stosować podejście do zabezpieczenia środowisk automatyki przemysłowej?

Głównym zabezpieczeniem powinna być segmentacja i ograniczenie dostępu do całej infrastruktury OT. Wszyscy uczestnicy dyskusji byli zgodni, że sieć zarówno OT, jak i IT powinna być monitorowana. Przy tym nie jest jednak dobrą praktyką stosowanie wykrywania nowych hostów czy otwartych portów na podstawie pasywnej weryfikacji ruchu sieciowego.

Wszyscy kładą również nacisk na zagadnienia związane z edukacją pracowników. Jako jedno z największych zagrożeń zostali wskazani pracownicy terenowi, którzy posiadają w zasadzie nieograniczony dostęp do systemów infrastruktury krytycznej. W tym zakresie jako niezwykle pomocne w ramach edukacji zostały

wskazane procedury, które powinny egzekwować konkretne zachowania i przyzwyczajenia pracowników.

Możliwości zabezpieczenie stacji końcowej użytkownika przed nieznanymi zagrożeniami

Moderatorzy:
Ewa Śniechowska, inżynier systemowy, Palo Alto Networks,

Radosław Wal, inżynier systemowy, Palo Alto Networks

Uczestnicy dyskusji dzielili się własnymi doświadczeniami w zakresie budowy infrastruktury, która mogłaby ograniczać albo przynajmniej minimalizować powodzenie ataków na stacje końcowe. Rozmawiano także o skutecznych sposobach zastosowania realnej prewencji. Rozważano scenariusze ataku, w tym często stosowane metody socjotechniczne, które pozwalają na dostarczenie złośliwych plików albo na wykorzystanie podatności w aplikacji na stacji klienckiej. Uczestnicy potwierdzili, że spotykali się z nimi w czasie swojej codziennej pracy. Zgodzili się, że bezpieczeństwo stacji końcowych przed nieznanymi zagrożeniami to zagadnienie, które dotyczy wszystkich.

Charakterystyka nowoczesnych ataków sprawia, że stacja końcowa stała się kluczowym elementem infrastruktury, który należy brać pod uwagę w momencie, kiedy myślimy o skutecznym bronieniu się przed takimi atakami. Sieć ma w związku ze swoją charakterystyką pewne ograniczenia, np. związane z deszyfracją ruchu. Część rozmówców zwróciła uwagę na ograniczenia wynikające z „narzutu korporacyjnego". Innymi słowy, nie zawsze pewne metody bezpieczeństwa jesteśmy w stanie zaimplementować w każdej sieci.

Uczestnicy dyskusji zwrócili uwagę na zagadnienie często pojawiające się też przy innych stolikach. Chodzi o wartość, jaką daje edukacja użytkowników w kwestiach bezpiecznego korzystania z infrastruktury sieciowej.

Jak podnieść efektywność cybersecurity i gdzie w pierwszej kolejności alokować zasoby

Moderator:
Krzysztof Kłaczek, konsultant/audytor, dyrektor zarządzający, IMNS Polska

Kanwą dla dyskusji był ranking organizacji Center for Internet Security (CIS) dotyczący najważniejszych obszarów z punktu widzenia bezpieczeństwa. CIS to amerykańska organizacja non profit, która realizuje swoje działania z dużymi przedsiębiorstwami.

Uczestnicy zostali podzieleni na dwie grupy i poproszeni o wybranie spośród 20 wskazanych obszarów 10 takich, które należy w pierwszej kolejności zabezpieczyć, aby uzyskać w krótkim czasie i przy małych zasobach najlepsze efekty. Wskazania w obu grupach nieznacznie się różniły. Jedna większy nacisk położyła na ochronę brzegu sieci, czyli budowę twierdzy, druga skoncentrowała się na użytkownikach mobilnych, którzy powinni mieć dobrze skonfigurowane przeglądarki oraz poprawnie przyznane uprawnienia.

Ostatecznie udało się dojść do wspólnego wniosku, że chociaż ranking zakłada określony poziom bezpieczeństwa, to każda z organizacji powinna przeprowadzać własną analizę ryzyka. Informacja o zasobach, informacja o oprogramowaniu,

o tym, czy mamy zainstalowane wszystkie łatki i poprawki jest istotna z tego punktu widzenia.

Płacić czy nie płacić? Czyli jak ransomware zagraża bezpieczeństwu Twojej firmy?

Moderator:
Michał Jaworski, dyrektor ds. strategii technologicznej, Microsoft

Dyskusja rozpoczęła się od próby udzielenia odpowiedzi na pytanie: płacić czy nie płacić. Pierwszy, podstawowy wniosek był taki, że odpowiedź jest uzależniona od tego, co chronimy. Najważniejsi są ludzie. Jeśli chronimy, to w pierwszej kolejności ludzi oraz zasoby firmy, potem procesy biznesowe, a dopiero na końcu reputację. Niestety, nie zawsze wszyscy o tym pamiętają. Moment, w którym ludzie są zagrożeni, jest tym momentem, w którym analiza ryzyka jest oczywista.

Dalej dyskusja skoncentrowała się na sprawach związanych z ransomware. Szybko okazało się, że nie ma uniwersalnego rozwiązania. Trzeba ludzi szkolić, ale doskonale wiemy, że w każdej organizacji znajdzie się pracownik, który będzie klikał we wszystko, co do niego przyjdzie. Dobrze byłoby, gdyby był tylko jeden, wówczas można go wyizolować. Niestety, najczęściej jest ich znacznie więcej. Oczywiście, mają znaczenie technologie i wsparcie technologiczne tego, co robimy, oraz support – zarówno na poziomie zapobiegania, czyli prewencyjny, jak i już później, kryzysowy. Ważne są także odpowiednie procedury, które mają zostać wdrożone.

Ważną rolę odgrywa także podstawowa higiena – od łatek, przez backup, przez

rejestr urządzeń, na prawach dostępu kończąc. Warto pamiętać, że RODO to dobry przyczynek, żeby uruchomić takie procesy.

Threat intelligence, czyli wartość informacji w cyberbezpieczeństwie

Moderator:
Bartłomiej Sobczyk, Territory Account Manager, FireEye

Nie było zaskoczenia, wszyscy uczestnicy zgodzili się, że informacje o cyberzagrożeniach są bardzo potrzebne, bez względu na to, czy mówimy o dużych, czy małych firmach oraz bez względu na sektor, w jakim te firmy działają. Z drugiej strony, żeby dobrze te zasoby informacyjne wykorzystać, potrzeba odpowiednich zasobów ludzkich. W tej kwestii także panowała zgoda: wszyscy przyznali, że co najwyżej 10% firm w Polsce jest w stanie efektywnie wykorzystać informacje tego typu w swoich procesach incident response. Warto zwrócić uwagę, że istotnym aspektem korzystania z threat intelligence jest automatyzacja, rozumiana jako skierowanie napływających informacji bezpośrednio do niektórych systemów, np. do firewalla czy serwera proxy.

Nie należy także zapominać o wartości, jaką niesie wymiana informacji. Skoro hakerzy ze sobą współpracują, to eksperci od bezpieczeństwa nie mogą być gorsi – firmy komercyjne oraz klienci powinni wymieniać informacje, żeby zwiększać efektywność

ochrony. Nie do końca wiadomo, jak taki mechanizm powinien wyglądać, być może na zasadzie opłat członkowskich za uczestnictwo w elitarnym klubie. Taka inicjatywa jest jednak potrzebna i mamy wszyscy nadzieję, że będzie rozwijana.

Maskowanie danych jako narzędzie ograniczania zakresu występowania danych wrażliwych, wymagających szczególnej ochrony

Moderatorzy:
Robert Dąbroś, ekspert,

Maciej Pęciak, ekspert, Apius Technologies

Dzięki temu, że w dyskusji uczestniczyli klienci końcowi oraz przedstawiciele dostawców, powstała doskonała okazja, żeby skonfrontować potrzeby i oczekiwania oraz możliwości obu stron. Po pierwsze, dane trzeba chronić. Security by design i by default to właściwie podstawowy wymóg. Dotyczy to nie tylko systemów produkcyjnych, ale wszystkich środowisk, w których dane występują, także środowisk testowych. Oczywiście, trzeba je chronić w sposób adekwatny. Przy tym stosowanie tradycyjnych mechanizmów zabezpieczeń może być kosztowne – maskowanie danych jest sensowną alternatywą.

Proces maskowania danych świetnie się wpisuje w takie scenariusze, w których chcemy przetwarzać dane wrażliwe, osobowe, chronione ustawowo i planujemy je przetwarzać do celów, do jakich nie zostały zebrane. Jeśli zostanie zastosowany proces maskowania, to można np. budować statystyki, używać danych do testowania systemów i aplikacji.

Musimy wiedzieć, co chcemy maskować i w jaki sposób. To z kolei musi być ściśle powiązane z procesami analizy ryzyka, rozumianymi jako cykliczny proces aktualizowania ocen w odniesieniu do nowych zagrożeń. To oznacza, że proces maskowania może się z czasem rozszerzać.

Rozwój aplikacji i bezpieczeństwo – kto wygrywa

Moderator:
Tomasz Bukowski, kierownik Zespołu Security Threat Intelligence, Bank Millennium

Wiadomo, że ocena jakościowa jest istotnym elementem pracy programistów i działu dewelopmentu. Bezpieczeństwo aplikacji powinno być elementem oceny jej jakości. Niestety, „dorabianie" bezpieczeństwa na końcu procesu programowania nigdy nie działa dobrze, powoduje duże konflikty, rozczarowania i generuje koszty. Przy tym o wiele łatwiej uzyskać pożądany efekt w przypadku rozwoju oprogramowania in-house, ze względu na bliską możliwość współpracy pomiędzy działami bezpieczeństwa i programistami. W przypadku współpracy z zewnętrznymi organizacjami konieczne jest dołączanie do wymagań biznesowych jasnych wymagań dotyczących spełnienia określonych standardów bezpieczeństwa. Potrzebne są też klarowne zapisy precyzujące, kto i w jaki sposób powinien reagować na problemy bezpieczeństwa w produkcie.

Jak skutecznie budować cybersecurity portfolio oraz nim potem zarządzać

Moderator:
Łukasz Guździoł, VP, Chief Information Security Officer, Credit Suisse Polska/TRISW/ISSA Polska

Ważne z punktu widzenia skuteczności działania jest lepsze poznanie i zrozumienie,

co chcemy chronić i które zasoby są dla biznesu krytyczne. W tym może pomóc analiza wpływu biznesowego. Konieczna jest dobra ocena ryzyka, która z kolei wymaga właściwego zrozumienia aktualnego krajobrazu zagrożeń, czyli określenia, jakie negatywne scenariusze mogą się wydarzyć oraz jakich ataków możemy stać się ofiarami. W tym celu należy wykorzystać dane z systemów wewnętrznych, czy to systemu zarządzania incydentami (ataki, które już wystąpiły), czy systemu wykrywania anomalii. Ostatecznym celem jest możliwość skupienia się na konkretnych atakach, na konkretnej kategorii zagrożeń i skoncentrowanie wysiłków zmierzających do ich wyeliminowania. Można to zrealizować poprzez inwestycje w mechanizmy zabezpieczeń w tych obszarach.

Oczywiście, jest to działanie czysto reaktywne, a potrzebne jest także działanie proaktywne. To można osiągnąć poprzez czerpanie informacji z systemów zewnętrznych, czy to wyspecjalizowanych dostawców szeroko pojętego threat intelligence, czy też instytucji typu CERT. W efekcie zyskuje się możliwość śledzenia zmian w krajobrazie zagrożeń, co pozwala w porę się do nich dostosować.

Poza tym istotna jest ciągła ocena mechanizmów kontrolnych, ciągła analiza ryzyka. Jeżeli dostrzegamy, że poziomy naszych zabezpieczeń nie są odpowiednie, może to oznaczać, że w niektórych obszarach konieczne są inwestycje. Do tego potrzebna jest elastyczność zarządzania portfolio inwestycyjnym. Dzięki niej stwierdzając, że zmienił się znacząco obraz zagrożeń, mamy możliwość zmiany priorytetów. Udaje się to osiągnąć np. poprzez rezerwę budżetową przeznaczoną na wszelkiego rodzaju sytuacje kryzysowe.

Zatrzymać bezpiecznika

Moderator:
Przemysław Dęba, dyrektor bezpieczeństwa systemów teleinformatycznych, Orange Polska

Najważniejszy wniosek z dyskusji: brak wykwalifikowanej kadry na pokładzie to największa z możliwych podatności. Jak zatem mądrze inwestować w ludzi w zespole bezpieczeństwa? Jakie zastosować metody motywacji? Co robić, żeby utrzymać specjalistów w zespole? Mimo szczerych chęci nie udało się nam znaleźć złotego środka na zatrzymanie bezpiecznika. Nie ma specyficznych metod rekrutacji czy motywacji ludzi związanych z bezpieczeństwem. Wydaje się, że akcenty mogą być tu różnie rozłożone.

W trakcie dyskusji praktycznie pominęliśmy tradycyjne metody rekrutacji. Są mało efektywne. Za to dużo czasu poświęcono wychowywaniu własnych bezpieczników

– poprzez dodawanie umiejętności innym istniejącym profilom technicznym, a także dzięki współpracy z uczelniami.

Jeżeli chodzi o motywację, to poza tradycyjnymi metodami finansowo-behawioralnymi, które powinny stać na najwyższym poziomie, ważna jest różnorodność zadań przydzielanych ludziom. Wydaje się dosyć istotne, żeby osoby pracujące w obszarze bezpieczeństwa widziały wpływ swojej pracy na organizację, co w tym zawodzie jest trudne. Szukanie dziury w całym jest samo w sobie frustrujące, a dodatkowe frustracje płyną z tego, że niewielu współpracowników wyraża entuzjazm dla działań podejmowanych przez bezpieczników.

Grupa wsparcia, czyli najpoważniejsze i najtrudniejsze obszary we wdrożeniu obszaru RODO

Moderator:
Michał Brandt, ekspert ds. bezpieczeństwa informacji, Alior Bank

RODO to temat kontrowersyjny, spędza sen z powiek wielu osobom. W dyskusji wzięli udział przedstawiciele firm zainteresowanych skutecznym wdrożeniem nowej regulacji, ale także dostawcy. Jeden z najważniejszych wniosków związany jest niepewnością dotyczącą organizacji projektu. Wiele firm wciąż zastanawia się nad zupełnie podstawowymi kwestiami, takimi jak „od czego zacząć" czy kto ma być odpowiedzialny – prawnicy, dział IT, a może pion bezpieczeństwa. Aktualny stan przygotowań jest zróżnicowany. Różnice wynikają m.in. z faktu, że niektóre firmy czy branże ze względu na inne regulacje są na wyższym poziomie gotowości. Tam pewne zagadnienia zostały rozwiązane już wcześniej i teraz jest o wiele łatwiej. Niestety, są także małe organizacje, które czasem nawet nie wiedzą, że w maju 2018 roku będą musiały spełnić pewne wymagania w zakresie ochrony danych osobowych.

Psychologiczny portret cyberprzestępcy

Moderator:
Mariola Dorota Wołoszyn, psycholog, członek zarządu, ACFE Poland Chapter

Czy poznanie psychologicznego portretu cyberprzestępcy ma znaczenie dla procesu tworzenia procedur bezpieczeństwa w organizacji? Istnieje konieczność badań społecznych i psychologicznych na temat uwarunkowań cyberprzestępczości oraz osobowości jej sprawców. Dyskutuje się wprowadzenie procedur weryfikujących dla nowo przyjmowanych pracowników i osób zatrudnionych pod kątem ich uczciwości, stałe sprawdzanie przestrzegania przez zatrudnionych procedur bezpieczeństwa względem ich odporności na cyberatak i wzmacnianie takich sposobów zarządzania zasobami ludzkimi, które minimalizują formatowanie i lustrowanie procedur.

Pewną cechą charakterystyczną dla cyberprzestępców jest minimalizowanie lub błędne interpretowanie konsekwencji swoich działań oraz przekonanie, że są to zachowania służące społeczeństwu. Takie osoby mają poczucie etycznej elastyczności. Do cech ich osobowości należą: wysoka inteligencja, ciekawość, abstrakcyjne myślenie, docenianie nowości. To zwykle indywidualiści, jednostki antykonformistyczne, posiadające zdolność do psychicznego wchłaniania, zatrzymywania i wykorzystywania dużej ilości szczegółów bez znaczenia. Interesuje ich każdy temat, który może pobudzać rozwój umysłu. Są maniakami kontroli. Zwykle są to osoby introwertywne, intuicyjne i myślące. Mają stosunkowo niewielką zdolność do emocjonalnego identyfikowania się z innymi ludźmi, gdyż zazwyczaj nie przypominają innych ludzi. Typowa jest dla nich skłonność do samopochłaniania, intelektualnej arogancji i niecierpliwości wobec ludzi oraz zadań postrzeganych jako marnowanie czasu.

Role Mining – wydatek (nie)zbędny

Moderator:
Paweł Kulpa, audytor, architekt bezpieczeństwa i wdrożeniowiec, ISC(2)

Jak zbudować role, czyli stworzyć z mnóstwa uprawnień, które ludzie posiadają, mniejsze zakresy, jakimi będzie łatwiej zarządzać? Pierwszym warunkiem automatyzacji jest działanie na danych dobrej jakości. Na początku należy zatem usunąć wszystkie „śmieci". Chodzi o wyeliminowanie sytuacji, w której z analizy wynika, że np. analitycy kredytowi muszą mieć prawa administratora w domenie. Przy tym trudno zanalizować całość, ponieważ otrzymamy bezwartościowe wyniki. Wartość pojawi się dopiero wówczas, gdy populacja uprawnień zostanie podzielona na drobne części. W ten sposób będzie można analizować wyniki, które otrzymaliśmy dzięki zastosowaniu narzędzia, oraz będzie można zrozumieć kontekst biznesowy.

Podstawowa konkluzja z dyskusji dotyczyła faktu, że analiza ról nie jest czynnością jednorazową. Nie można zrealizować projektu, wdrożyć ról i zapomnieć. Mamy do czynienia z procesem, w którego trakcie cały czas te role dopasowujemy, bo organizacja się zmienia, wszystko dookoła się zmienia i nasze uprawnienia też się zmieniają. W związku z tym modelowanie ról jest procesem ciągłym. Role mining daje dobry punkt wyjścia, ale nie stanowi rozwiązania ostatecznego.

Konteneryzacja jako rozwiązanie przyszłości

Moderator:
Grzegorz Cenkier, główny specjalista, Poczta Polska

Czy konteneryzacja to technologia przyszłości? Jak szybko się spopularyzuje? Na razie można stwierdzić, że technologia konteneryzacji jest mało znana. Niemniej jest prawdopodobnie ważna i będzie powszechnie stosowana w przyszłości. Dlatego należy zwrócić na nią uwagę. Bo choć jest mało znana, to coraz więcej organizacji w Polsce zaczyna dostrzegać korzyści wynikające z jej zastosowania. Przykładem jest portal Allegro, który używa kontenerów do szybkiej instalacji aplikacji na różnych platformach systemowych.

Problemy, na jakie należy zwrócić uwagę w tym kontekście, są takie same jak z każdym nowym produktem. Dodatkowo, podobnie jak w przypadku wirtualizacji, wyzwanie stanowią sposoby licencjonowana produktów komercyjnych wykorzystujących tę technologię.

Inteligentne wsparcie dla bezpieczeństwa

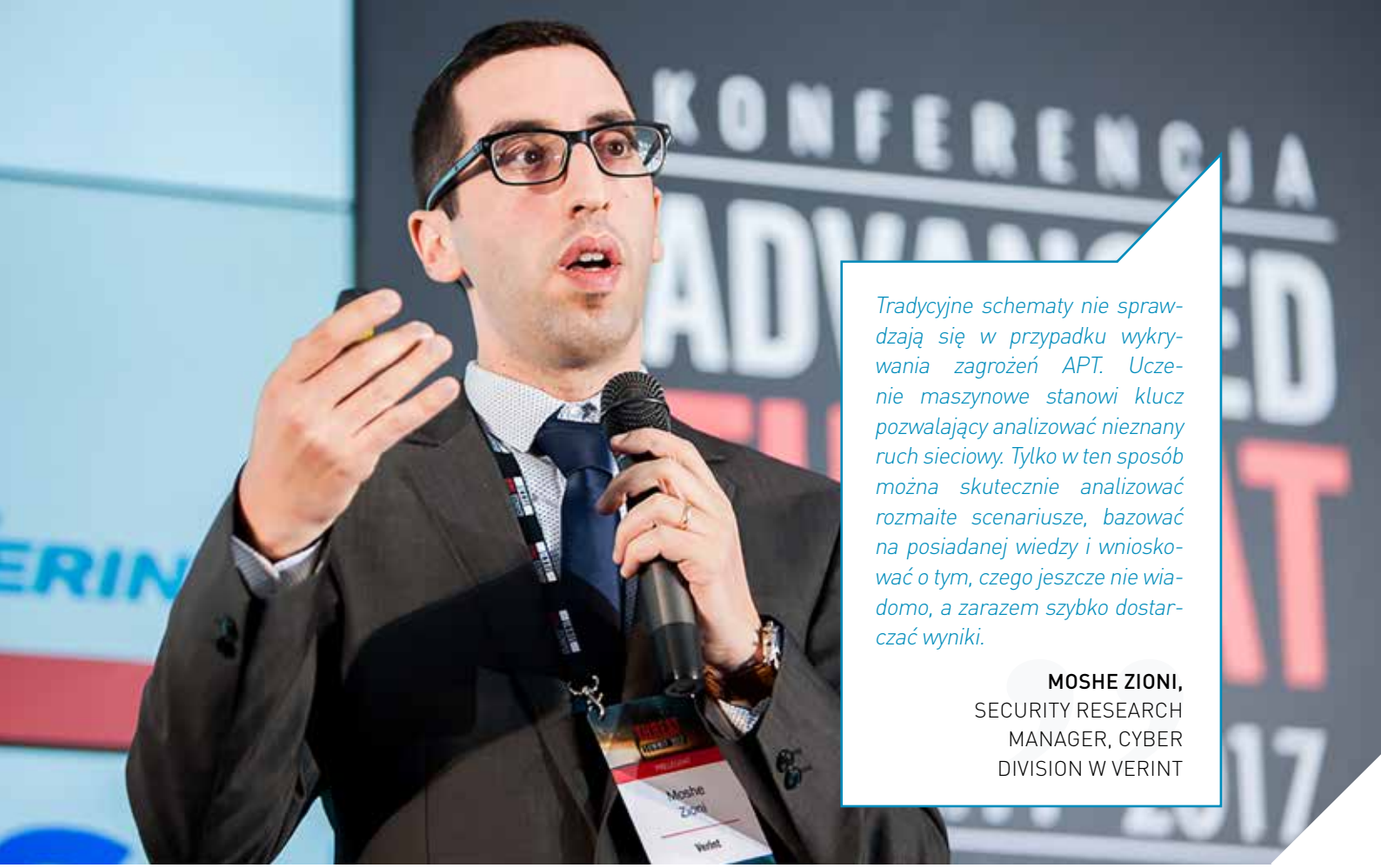
Uczenie maszynowe, a w przyszłości sztuczna inteligencja mają do odegrania kluczową rolę w wykrywaniu nowych, nieznanych zagrożeń. Pomogą w ujawnieniu groźnych sytuacji, które nie były wcześniej zaobserwowane. Pierwsze rozwiązania wykorzystujące „samouczące się" technologie są już dostępne.

Technologie uczenia maszynowego *(ML – machine learning)* uznawane są za kolejny etap rozwoju maszyn. Najpierw człowiek mógł przekazać maszynom zadania, do których potrzebna była siła mięśni. Następnie komputery przejęły relatywnie proste, powtarzalne zadania umysłowe. Teraz postęp w obszarze uczenia maszynowego sprawił, że są w stanie rozwiązać złożone problemy dzięki samodzielnemu uczeniu się. Korzysta na tym również bezpieczeństwo.

Trening na wzorcach

Firma Verint postawiła na uczenie maszynowe, poszukując alternatywnego podejścia do wykrywania zaawansowanych ataków w kanałach *command and control*. „Tradycyjne schematy nie sprawdzają się w przypadku wykrywania zagrożeń APT. Uczenie maszynowe stanowi klucz pozwalający analizować nieznany ruch sieciowy. Dlaczego? Dlatego że tylko w ten sposób można skutecznie analizować rozmaite scenariusze, bazować na posiadanej wiedzy i wnioskować o tym, czego jeszcze nie wiadomo, a zarazem szybko dostarczać wyniki" – mówił podczas „Advanced Threat Summit 2017" Moshe Zioni, Security Research Manager, Cyber Division w Verint.

Uczenie maszynowe wyewoluowało z badań nad rozpoznawaniem wzorów oraz ze studiów nad sztuczną inteligencją. To dziedzina nauki, która



Tradycyjne schematy nie sprawdzają się w przypadku wykrywania zagrożeń APT. Uczenie maszynowe stanowi klucz pozwalający analizować nieznany ruch sieciowy. Tylko w ten sposób można skutecznie analizować rozmaite scenariusze, bazować na posiadanej wiedzy i wnioskować o tym, czego jeszcze nie wiadomo, a zarazem szybko dostarczać wyniki.

MOSHE ZIONI,
SECURITY RESEARCH MANAGER, CYBER DIVISION W VERINT

koncentruje się na umożliwieniu komputerom „uczenia się" na przykładach oraz samodzielnego doskonalenia w wykrywaniu wzorów. Model uczy się, opierając się na znanych, sklasyfikowanych danych, a następnie dokonuje ekstrapolacji w celu osiągnięcia nietrywialnych z ludzkiego punktu widzenia rezultatów.

W obrębie samego uczenia maszynowego istnieje wiele metod. Każda z nich ma pewne zalety i wady. Firma Verint zdecydowała się wykorzystać *Supervised Learing*, typ uczenia maszynowego, które opiera się na oznaczonych danych treningowych. Ich wybór jest kluczowy dla optymalizacji modeli i ograniczenia błędów.

„Kluczem do sukcesu jest odpowiedni wybór danych. To najważniejszy element całej operacji. Jeśli na początku popełnione zostaną błędy, cały model będzie obarczony błędami" – tłumaczył Moshe Zioni. Stworzenie efektywnego modelu jest zależne od wyboru odpowiedniego zbioru danych oraz analizowanych cech. Próbka powinna składać się z różnorodnych, istotnych danych. „Przy zastosowaniu algorytmu Decision Tree Random Forest, Verint, udało się nam uzyskać niski False Positive Rate" – dodawał Moshe Zioni.

Bez wstępnych reguł

Z kolei rozwiązanie firmy Darktrace, prezentowane przez Mateusza Flaka pełniącego rolę Cyber Security Regional Manager CEE, opiera się na zaawansowanym uczeniu maszynowym nienadzorowanym (*Unsupervised*). Pozwala na wykrywanie zagrożeń w czasie rzeczywistym w sieciach biznesowych i przemysłowych. Technologia Darktrace jest w stanie po krótkim okresie nauki odróżniać to, co jest normalne w sieci, od tego, co nie jest. W ten sposób system może wykrywać cyberataki, które nie zostały nigdzie wcześniej zaobserwowane.

Nie ma żadnych sygnatur ani żadnych reguł, żadnej wiedzy a priori o tym co jest ‚złe', a co ‚dobre'. Urządzenie buduje cykle życia dla każdego obiektu w firmie. Uczy się, jak się zachowują poszczególne komputery i ich użytkownicy. Po wstępnym okresie nauki, około 7–10 dni, system jest już w stanie samodzielnie wykrywać anomalie. Nauka kontynuowana jest także później. System ewoluuje wraz ze środowiskiem.

MATEUSZ FLAK,
CYBER SECURITY REGIONAL MANAGER CEE W DARKTRACE

Oferta Darktrace to specjalne urządzenie, które lokalnie (bez przesyłania danych na zewnątrz organizacji), działając na kopii ruchu z przełącznika, przeprowadza głęboką inspekcję na pakietach sieciowych. Algorytmy mogą działać, mając do dyspozycji 360 wymiarów ruchu. Dla porównania, w przypadku rozwiązań klasy SIEM dokonywana jest analiza przepływów sieciowych oparta na kilkunastu zmiennych.

„Nie ma żadnych sygnatur ani żadnych reguł, żadnej wiedzy a priori o tym, co jest ‚złe', a co ‚dobre'. Urządzenie buduje cykle życia dla każdego obiektu w firmie. Uczy się, jak się zachowują poszczególne komputery i ich użytkownicy. Po wstępnym okresie nauki, około 7–10 dni, system jest już w stanie samodzielnie wykrywać anomalie. Oczywiście nauka kontynuowana jest także później, po tym wstępnym okresie. System na bieżąco ewoluuje wraz ze środowiskiem" – mówił Mateusz Flak.

Rezultaty uczenia maszynowego są trudne do zinterpretowania. W większości przypadków nie można udzielić odpowiedzi na pytanie, w jaki sposób maszyna zdecydowała, że analizowane zdarzenie ma charakter ataku.

Maszyna autonomicznie wykrywa anomalne obszary w obrębie dużych zbiorów danych i podejmuje na tej podstawie „inteligentne decyzje". Co ważne, choć system od pierwszego dnia może obserwować zagrożenia jako coś normalnego, to dzięki możliwości porównania z zachowaniami innych podobnych obiektów jest w stanie wykryć, że ma do czynienia z anomalią.

Trudności w interpretacji

Na otwierające się nowe możliwości, ale także słabe punkty uczenia maszynowego zwracał uwagę Leszek Tasiemski, VP, Rapid Detection Center, R&D Radar & RDS w F-Secure. „Uczenie maszynowe świetnie sprawdza się w wykrywaniu anomalii i grupowaniu poszczególnych zasobów sieci lub użytkowników pod kątem ich wzorców zachowań. Natomiast jeszcze nie jesteśmy na tym etapie, żeby uczenie maszynowe było nam w stanie odpowiedzieć na pytanie, dlaczego coś jest niebezpieczne. To jedna z dwóch największych słabości tej technologii" – mówił Leszek Tasiemski.

Na ten problem wskazywali także inni eksperci uczestniczący w konferencji. Rezultaty uczenia maszynowego są trudne do zinterpretowania. W większości przypadków nie można udzielić odpowiedzi na pytanie, w jaki sposób maszyna zdecydowała, że analizowane zdarzenie ma charakter ataku.

„Drugi problem to możliwość modyfikowania działania algorytmu przez atakującego poprzez oswajanie go ze wzorcem ataku. W ten sposób – dzięki takiemu poisoningowi, czyli podtruwaniu – w chwili ataku algorytm uznaje niebezpieczne działanie za coś normalnego" – dodawał Leszek Tasiemski.

Zdaniem Leszka Tasiemskiego, obecnie uczenie maszynowe sprawdza się przede wszystkim jako wsparcie dla człowieka, doświadczonego specjalisty z zakresu bezpieczeństwa systemów IT. Przykładem są usługi pozwalające na wykrywanie ataków w czasie zbliżonym do rzeczywistego. Początek pracy należy do maszyny. Dopiero w ostatnim etapie człowiek dokonuje ostatecznej selekcji oraz potwierdza, że mamy do czynienia z atakiem.

> Problemem jest możliwość modyfikowania działania algorytmu przez atakującego poprzez oswajanie go ze wzorcem ataku. W ten sposób w chwili ataku algorytm uznaje niebezpieczne działanie za coś normalnego.

Bazując na doświadczeniach F-Secure, można przedstawić, jak to wygląda w praktyce. Zakładając, że mamy do czynienia z organizacją, w której wykorzystywanych jest ok. 1300 stanowisk komputerowych, miesięcznie trzeba zmierzyć się z blisko 2 mld zdarzeń. Po wstępnej selekcji przy wykorzystaniu technologii uczenia maszynowego udaje się ograniczyć liczbę podejrzanych sytuacji do 900 tys., a następnie przy użyciu sita w postaci systemu eksperckiego zmniejszyć do 25. W tym momencie musi wkroczyć człowiek. Dysponując wiedzą i doświadczeniem oraz znając kontekst działań, jest w stanie potwierdzić, że kilka, kilkanaście zdarzeń to prawdziwe ataki, na które należy zareagować.

RODO i cyberbezpieczeństwo: kompleksowo i długofalowo

Rozmowa z **Beatą Bielską**, SAM & Cybersecurity Executive w APN Promise.

Za kilka miesięcy, w maju 2018 roku, wchodzi w życie RODO. Czasu pozostało zatem naprawdę niewiele. Czy organizacja, która nie zabrała się odpowiednio wcześnie za wdrożenie, ma jeszcze szansę, żeby nadrobić opóźnienia w przygotowaniach i zapewnić sobie zgodność z nową regulacją?

Niewątpliwie ta magiczna data oznacza rewolucję w niezmiernie ważnym dla każdej organizacji obszarze. Cały świat biznesu jest przejęty RODO, a dyskusje na ten temat są ożywione. Nadal natomiast brakuje np. przepisów wdrażających przygotowanych przez polski rząd. Z pewnością każda organizacja powinna przeanalizować wewnętrzne procesy oraz ocenić ryzyka, które następnie przy współpracy i wsparciu kompetentnej firmy można zmniejszyć. Tak naprawdę trzeba zacząć od określenia, czy i jakiego rodzaju dane osobowe są przetwarzane w organizacji, gdzie są zlokalizowane i w jaki sposób chronione przed naruszeniami.

To może wymagać wsparcia przez specjalistów z kilku dziedzin, posiadających odpowiednie kompetencje. Ta sytuacja może paraliżować firmy, ponieważ wyszukanie wewnątrz organizacji bądź na rynku takich ludzi

zwykle trochę trwa. Naszym klientom rekomenduję zacząć przygotowania po prostu od opracowania planu działania, którego realizacja pozwoli na koniec dnia powiedzieć: tak, spełniam wszystkie aspekty rozporządzenia RODO.

Czym wyróżnia się Państwa oferta?

Przede wszystkim ma kompleksowy charakter. Obejmuje wszystkie istotne aspekty związane z wprowadzanymi zmianami prawnymi. Proponowane działania realizowane są w czterech etapach. Rozpoczynamy od weryfikacji, następnie odbywa się dostosowanie, ustalenie procedur, a na koniec wykonywana jest kontrola i ustalany nadzór.

Do stworzenia kompleksowej oferty zainspirowało nas wieloletnie doświadczenie zdobyte w obszarze Software Asset Management (SAM – zarządzania infrastrukturą IT). Nasz zespół SAM to grupa ekspertów, która jest w stanie sprostać wielu wyzwaniom związanym zarówno z samym RODO, jak i szeroko pojętym zarządzaniem infrastrukturą IT.

Przeprowadzenie procesu w tym modelu umożliwia odpowiednie przygotowanie organizacji do wdrożenia w życie RODO, a następnie utrzymania poziomu przetwarzania danych zgodnie z warunkami wskazanymi przez rozporządzenie. Oczywiście, to pewien model teoretyczny. Każda organizacja ze względu na własną specyfikę może wymagać rozbudowania powyższego zakresu działań o dodatkowe punkty kontrolne.

Co jest kluczowe na pierwszym etapie – weryfikacji?

Rozpoczynająca projekt analiza działalności biznesowej pod kątem przetwarzania danych osobowych musi być bardzo szczegółowa. Jej wynikiem jest wskazanie poszczególnych procesów oraz form przetwarzania danych osobowych w organizacji. To od identyfikacji procesów przetwarzania oraz ich stanu zależeć będzie skala koniecznych do podjęcia prac.

Na tym etapie identyfikujemy aktywa informacyjne o charakterze osobowym, analizujemy procesy biznesowe pod kątem gromadzenia, podstawy oraz form przetwarzania danych osobowych, a także określamy przepływy danych. W tym momencie wskazywane są środki ochrony danych, w tym techniczne środki zabezpieczenia. Powstaje również wykaz formalnych i faktycznie stosowanych procedur organizacyjnych zarządzania bezpieczeństwem informacji. Wreszcie przygotowywane są mapy przepływu danych osobowych oraz opis procesów związanych z przetwarzaniem.

Beata Bielska, SAM & Cybersecurity Executive w APN Promise

W realizację zadań na tym jednym etapie z naszej strony angażujemy przeważnie przedstawicieli kancelarii prawnej, specjalistów od bezpieczeństwa i SAM, osoby techniczne odpowiedzialne za infrastrukturę czy też „białych hakerów".

Co następuje dalej, kiedy zakończona zostanie analiza?

Rozpoczyna się właściwe dostosowanie procesów przetwarzania do wymagań RODO. Prawidłowo przeprowadzone działania podniosą poziom zgodności działalności organizacji z przepisami o ochronie danych osobowych, jak również ich świadomość w firmie. Po zakończeniu tego etapu projektu firmy będą mogły mówić o dostosowaniu się do wymaganych zasad przetwarzania, praw osób, których dane są przetwarzane, oraz obowiązków administratora w zakresie bezpieczeństwa.

Wydaje się, że w tym miejscu projekt powinien się zakończyć...

Trzeba jeszcze ustalić zasady i procedury dostępu do danych oraz rozpocząć pracę nad podniesieniem świadomości ich ochrony. W efekcie powinniśmy określić precyzyjne zasady dostępu do danych dla pracowników firmy i podmiotów spoza organizacji. W szczególności pomocna okaże się w tym opracowana wcześniej mapa przepływu danych.

Ostatecznym celem jest opanowanie procesów przepływu danych oraz zagwarantowanie odpowiednich warunków udzielania dostępu do nich. Dzięki temu zwiększona zostanie świadomość organizacji, a każdy pracownik będzie wiedział, jak ma obchodzić się z powierzonymi informacjami.

Czy coś jeszcze pozostaje do wykonania?

Doprowadzenie do stanu zgodności z RODO to jedno. Drugim, ważnym czynnikiem jest stała kontrola oraz nadzór nad zachowaniem odpowiednich standardów i procedur na właściwym, wysokim poziomie. Należy jeszcze zbadać, czy organizacja podlega obowiązkowi posiadania Inspektora Ochrony Danych oraz – jeśli odpowiedź jest twierdząca – powołać go. Następnie trzeba ustalić procedury kontroli okresowych i stałego nadzoru, a także procedury postępowania w przypadku naruszenia ochrony danych, szczególnie w aspekcie obowiązku informowania organu nadzoru o konkretnej kategorii naruszeń.

Czy przygotowania do RODO przełożą się na podniesienie ogólnego poziomu cyberbezpieczeństwa w organizacjach?

Przystosowanie do RODO to z pewnością istotny impuls do działań w zakresie całego cyberbezpieczeństwa. Nie rozwiązuje jednak wszystkich problemów. Cyberbezpieczeństwo dotyczy całej organizacji, nie tylko danych osobowych. Wejście RODO wymusi niewątpliwie na firmach przemodelowanie szeroko pojętych, obowiązujących polityk i procedur bezpieczeństwa, przeprowadzenie analiz, weryfikację funkcjonujących ról oraz procesów. Wiem z doświadczenia, że jest to ogromna, czasochłonna praca, wymagająca zaangażowania znacznych zasobów. Niemniej organizacje muszą ją wykonać i jestem pewna, że przyniesie im ona znaczne korzyści.

Bezpieczeństwo i IT: razem czy osobno?

Gdzie jest miejsce działu bezpieczeństwa w organizacji? Czy ma być częścią działu IT, czy samodzielną, wyodrębnioną komórką? Komu powinien podlegać, aby skutecznie realizować swoje zadania?

W trakcie „Advanced Threat Summit 2017" dyskutowano o tym podczas panelu, który miał formę debaty oksfordzkiej. Pod dyskusję poddana została teza, że dział bezpieczeństwa powinien być niezależny i wydzielony w możliwie dużym stopniu ze struktur IT.

Bez konfliktu interesów

Jej obrońcy wskazywali na konflikt interesów, jaki potencjalnie istnieje między menedżerami odpowiedzialnymi za bezpieczeństwo w organizacji a kierującymi działem informatyki. CIO pracuje głównie pod presją terminów i wymagań klientów, musi dbać głównie o szybkość działania, elastyczność reagowania, zadowolenie użytkowników. Kwestie bezpieczeństwa są w takiej sytuacji drugorzędne.

Zwolennicy wydzielenia spraw cyberbezpieczeństwa ze struktur IT przyznawali, że obecnie CSO najczęściej raportują do CIO. Ich zdaniem, jest to jednak przeżytek i w przyszłości taki stan rzeczy będzie nie do utrzymania. Grozi bowiem przemilczaniem ważnych dla całości organizacji kwestii w imię utrzymania sprawności działania pionu IT. Skutki tego mogą być groźne dla całej firmy.

Należy dążyć do tego, aby docelowo CSO raportował bezpośrednio do CEO. Tylko wtedy będzie mógł należycie wykonywać swoje zadania. Jego rolą jest bowiem dbanie o bezpieczeństwo całej organizacji, a nie wspieranie działu IT. Musi więc mieć możliwość patrzenia na ręce również szefowi IT, a nie być zobligowanym do wykonywania jego poleceń. Standardy bezpieczeństwa muszą być spełnione przez wszystkich bez względu na to, jak utrudniają bieżącą pracę. Bezpieczeństwo IT nie jest sprawą IT, ale całej organizacji. Osoba zajmująca się bezpieczeństwem musi być więc poza strukturami IT. Dobrym rozwiązaniem może

być przekazanie kompetencji związanych z cyberbezpieczeństwem do działu zajmującego się bezpieczeństwem organizacji, w tym również fizycznym. Zdaniem niektórych uczestników dyskusji, działy bezpieczeństwa miały już dawno do czynienia z tym, co dzisiaj występuje w cyberbezpieczeństwie – kradzieżami, włamaniami, nieuprawnionym dostępem itp. Rozumieją, jak działają przestępcy, mają doświadczenie i wiedzą, jak sobie z nimi radzić. Potrzebują tylko wsparcia technologicznego.

Uczestnicy debaty przyznawali jednak, że dla osiągnięcia odpowiedniego poziomu bezpieczeństwa w organizacji potrzebna jest ścisła współpraca CSO i CIO. To podstawa cyberbezpieczeństwa. Dla sprawnego działania pionu bezpieczeństwa ważna jest też wiedza, którą specjaliści wynoszą z pracy w IT.

Wspólnie znaczy efektywnie

Przeciwnicy tezy o konieczności wydzielenia działu bezpieczeństwa ze struktur IT zwracali uwagę, że byłby to sztuczny rozdział, gdyż zarówno na IT, jak i na cyberbezpieczeństwo jest ten sam budżet. Wspólne są również technologie, które stanowią podstawę działania obu obszarów. W IT jest też wiele technologii i rozwiązań kluczowych z punktu widzenia cyber security. Jaki więc sens ma rozdzielanie czegoś, co jest i tak w praktyce jest z sobą powiązane?

Rozdzielenie prowadzi do dublowania struktur. Efektem tego jest utrudniona współpraca i komunikacja. Innym zagrożeniem jest pojawienie się wskutek tego niezdrowej rywalizacji między CSO i CIO. Występując przed tymi sami przełożonymi, będą konkurować o ten sam budżet i te same zasoby. W konsekwencji w trosce o utrzymanie operacyjnej sprawności działania na bezpieczeństwo może być mniej pieniędzy. poziomu bezpieczeństwa w firmie.

Zadaniem CSO jest zapewnić odpowiedni poziom bezpieczeństwa organizacji – bez względu na to, czy będzie działał w strukturach IT czy samodzielnie. Wszędzie ma tę samą rolę do odegrania. Jego działania muszą jednak przebiegać w stałym kontakcie z IT. Muszą być na bieżąco skoordynowane i skonsultowane z IT, chociażby w zakresie wymagań dla architektury bezpieczeństwa, modeli danych itp. W ramach jednej jednostki będzie to łatwiejsze i efektywniejsze. Procesy będą realizowane sprawniej i szybciej.

Oderwanie CSO od kontaktów z bieżącym działaniem firmy, od rozumienia potrzeb i wymagań klientów oraz użytkowników IT może okazać się również niebezpieczne dla całej organizacji. Może skutkować wymyślaniem nierealnych bądź wygórowanych wymagań, które zdezorganizują pracę firmy i będą miały negatywny wpływ na biznes. W konsekwencji usamodzielnienie się pionu CSO może doprowadzić do powstania stanowiska poza kontrolą.

Dodatkowym argumentem na rzecz pozostawienia bezpieczeństwa w ramach IT jest możliwość zapewnienia wysoko wykwalifikowanych kadr. CIO ma w tym względzie znaczącą przewagę nad CSO. Może zapewnić specjalistom zdecydowanie wyższe wynagrodzenie. Może też im zagwarantować lepsze warunki rozwoju zawodowego – kursy, szkolenia, certyfikaty. Ma na to środki, które trudno zdobyć szefowi bezpieczeństwa. Nie bez znaczenia jest też kwestia prestiżu. W pionie IT dzieją się też kluczowe dla rozwoju firmy i biznesu procesy i inicjatywy.

Tworzymy unikalne wydarzenia dla firm technologicznych.

Dajemy możliwość nawiązania kontaktów biznesowych z decydentami IT najważniejszych organizacji w Polsce.

EVENTION
CZAS ZAANGAŻOWANY

Zrealizowaliśmy
60 projektów konferencyjnych

Obsłużyliśmy
120 partnerów - firm technologicznych

Gościliśmy
3000 uczestników naszych wydarzeń

Kompleksowa obsługa

Zapewniamy kompleksowy program realizacji konferencji oraz spotkań biznesowych na zlecenie klienta.

Wartość merytoryczna

Wspieramy przy tworzeniu formuły i programu merytorycznego oraz towarzyszących publikacji.

Nasze kompetencje

Profesjonalny zespół ekspertów oraz znajomość rynku ICT podstawą naszych realizacji

---

W Evention wydarzenia biznesowe traktujemy jako integralny i trudny do zastąpienia element budowania relacji z potencjalnymi klientami. Szukamy innowacyjnych form realizacji spotkań, odpowiadających na potrzeby security menedżerów/menedżerów IT. Evention jest organizatorem uznanych na rynku konferencji o tematyce security, w tym m.in.:

• RIBA Forum • InfraSEC Forum • CyberGOV
• Technology Risk Management Forum • Advanced Threat Summit

WWW.EVENTION.PL

PARTNER GENERALNY

FireEye SECURITY REIMAGINED

PARTNER STRATEGICZNY

CYBERARK

FORTINET

advatech

PARTNERZY MERYTORYCZNI

CITRIX

Accellion

ARROW

Comp

DARKTRACE

Deloitte.

dimension data

EVERSYS

Extreme

F-Secure

IMNS Polska

Infoblox

integrity

ivanti

paloalto

proofpoint

pwc

QUALYS

Symantec

TREND MICRO

VERINT

PROMISE GRUPA APN PROMISE

Microsoft

vmware

MECENASI

APIUS technologies

COMARCH

ectacom

KPMG

IMMUSEC

Milloh-CS

Akamai PARTNER

securing

Vade Secure

PARTNER SPOŁECZNOŚCIOWY

ISACA Warsaw Chapter

WSPÓŁPRACA MERYTORYCZNA

CSO COUNCIL

PATRONI

Amrop

CSAFL

Cyberlaw.pl

(ISC)² CHAPTER POLAND

OWASP

POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

PTI

POMOCNIK RODO

sekurak.pl

TECHNOLOGY LAW & INFORMATION SECURITY

ZAUFANA TRZECIA STRONA.PL

SGH

ITWIZ TO CO ISTOTNE W IT

ISACA Katowice Chapter