ORGANIZATORZY

EVENTION
CZAS ZAANGAŻOWANY

ISSA
POLSKA

Konferencja „**Advanced Threat Summit**" to jedna z największych i najważniejszych w Polsce konferencji z dziedziny cybersecurity. W tym roku została zorganizowana już po raz piąty. To miejsce spotkania menedżerów cyberbezpieczeństwa i bezpieczeństwa informacji z dużych i średnich organizacji działających w naszym kraju. Daje okazję do poznania ekspertów z różnych branż i sektorów oraz wymienienia się spostrzeżeniami i podzielenia doświadczeniami.

W programie każdej edycji „AT Summit" uwzględniane są aktualne potrzeby i zainteresowania profesjonalistów, którzy odpowiadają za bezpieczeństwo cyfrowe i informacyjne swoich organizacji. Przed nimi stoją trudne wyzwania. Muszą być partnerami dla zarządów swoich firm i instytucji, chroniąc zasoby jednocześnie realizować cele biznesowe, odpowiadać za pozyskanie i właściwe spożytkowanie budżetów, nadzorować pracę swoich zespołów bezpieczeństwa. Technologia pełni dla nich rolę służebną – najważniejsze jest wpisanie cybersecurity i bezpieczeństwa informacji w praktykę funkcjonowania ich organizacji i działań użytkowników.

Idea konferencji zbudowana jest wokół tematyki najpoważniejszych i najbardziej zaawansowanych zagrożeń w środowisku cyfrowym. Każdego roku wybierane są aktualne zagadnienia i problemy, którymi żyje środowisko security. Takie podejście pozwala na bieżąco dostarczać wiedzy i informacji pomagających specjalistom od cyberbezpieczeństwa radzić sobie z najważniejszymi w danym momencie wyzwaniami, śledzić trendy i prognozować możliwe scenariusze rozwoju sytuacji.

Zachęcamy do zapoznania się z podsumowaniem dorobku programowego „Advanced Threat Summit 2018" i zapraszamy do udziału w kolejnej edycji. Informacje o wydarzeniu dostępne są na stronie atsummit.pl.

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

Spis treści

ADVANCED THREAT SUMMIT 2018

ADVANCED THREAT SUMMIT 2018

Cyberbezpieczeństwo: co słychać na froncie?

Nowe technologie, nowe metody i wektory ataku, nowi aktorzy na scenie teatru cybernetycznej wojny – dzisiaj praktycznie żadna organizacja nie jest w stanie uniknąć włamania. Powszechna zaczyna być także świadomość, że nie da się ochronić wszystkiego. Działania w obszarze cyberbezpieczeństwa są tym trudniejsze, że na rynku brakuje wykwalifikowanych specjalistów. Zwłaszcza mniejszym organizacjom bardzo trudno jest pozyskać wysokiej klasy ekspertów. Do tego dochodzą kolejne regulacje prawne, które dla wielu organizacji stanowią poważne wyzwanie – finansowe i organizacyjne. Dynamika zdarzeń w obszarze cyberochrony sprawia też, że zmienia się rola CSO i specjalistów ds. bezpieczeństwa. Pojawiają się nowe szanse i otwierają nowe możliwości, ale rośnie ryzyko, z którym trzeba sobie radzić, a potencjalne konsekwencje incydentów są coraz poważniejsze. Tematyka wystąpień podczas konferencji „Advanced Threat Summit 2018" stanowiła doskonałą tego ilustrację. W trakcie spotkania blisko pół tysiąca praktyków cyberbezpieczeństwa z różnych branż dyskutowało o najnowszych trendach, kluczowych wyzwaniach i przełomowych technologiach.

Nie można zapominać o sprawach fundamentalnych, o podstawowej higienie bezpieczeństwa. Warunkiem wysokiego poziomu bezpieczeństwa jest codzienne dokładanie starań w zakresie standardowych działań.

PIOTR KALBARCZYK,
DYREKTOR DEPARTAMENTU
CYBERBEZPIECZEŃSTWA
W PKO BANK POLSKI

CSO musi obecnie spodziewać się niespodziewanego. Któż mógłby pomyśleć, że sposobem włamania będzie aktualizacja prostego systemu księgowego? Kto by wpadł na to, że drogą mającego poważne konsekwencje ataku może być system wentylacyjny? Dlatego choć ochrona i prewencja nadal są ważne, coraz więcej organizacji koncentruje się na doskonaleniu wykrywania zagrożeń i reagowania na incydenty. Przy tym popularyzacja usług as-a-Service sprawia, że jednym z priorytetów staje się zabezpieczanie chmury i rozwiązań mobilnych.

W obliczu braków kadrowych i wzrostu skali oraz złożoności zagrożeń duże nadzieje wiązane są z technologiami takimi jak machine learning czy automatyzacja. Wkrótce – jeśli jeszcze nie są – staną się one standardowym komponentem rozwiązań bezpieczeństwa IT. Na razie sprawdzają się w wąskim zakresie zastosowań – maszyny przejmują dobrze zdefiniowane, czasochłonne, żmudne zadania, pełniąc rolę jedynie wspomagającą człowieka. Możliwe jednak, że wkrótce będą w stanie zrobić znacznie więcej. Obszary zastosowania narzędzi tego typu to m.in.: klasyfikacja danych, przewidywanie zagrożeń, reagowanie na incydenty, analizowanie złośliwego oprogramowania czy szeroko rozumiana analityka obszaru bezpieczeństwa. Postęp w tych dziedzinach wiąże się jednak równocześnie ze wzrostem zagrożeń – z nowości technologicznych będą mogli także skorzystać przestępcy.

Dlatego nie można zapominać o sprawach fundamentalnych i wszystkim dobrze znanych: o podstawowej higienie w obszarze bezpieczeństwa. Podczas „Advanced Threat Summit 2018" zwracał na to uwagę Piotr Kalbarczyk, dyrektor Departamentu Cyberbezpieczeństwa w PKO Bank Polski. Warunkiem osiągnięcia wysokiego poziomu bezpieczeństwa jest codzienne dokładanie starań w zakresie standardowych działań, takich jak: instalowanie łatek, aktualizacja systemów czy dbanie o poprawność konfiguracji.

Przestępcy mogą atakować samą sztuczną inteligencję. W napędzającym ją oprogramowaniu znajduje się ogromna liczba błędów, które nie są szybko poprawiane.

JANUSZ ŻMUDZIŃSKI,
WICEPREZES POLSKIEGO TOWARZYSTWA INFORMATYCZNEGO

Inteligentne maszyny na horyzoncie

Szef Google stwierdził niedawno, że sztuczna inteligencja będzie miała większy wpływ na nasz świat niż elektryczność czy ogień. Nikt nie ma wątpliwości, że odmieni ona także branżę cyberbezpieczeństwa. Jest przy tym bardzo prawdopodobne, że nastąpi to szybciej, niż się spodziewamy. Mimo to wydaje się, że większość przedstawicieli środowiska cybersecurity nie zdaje sobie sprawy z nadchodzących zagrożeń.

„Niewiele osób na świecie rozumie istotę i skalę problemów, z jakimi wkrótce przyjdzie się wszystkim mierzyć. Sztuczna inteligencja to domena uniwersytetów i instytucji naukowych. Tam ma swoją genezę większość nowości w tym obszarze. Biznes nie rozumie dobrze tych problemów. Dlatego warto postawić na wykorzystanie wiedzy akademickiej oraz bliską współpracę z badaczami i naukowcami" – przekonywał Menny Barzilay, CTO w Cyber Research Center działającym w ramach Tel-Aviv University.

Do tych technologii dostęp będą mieli także przestępcy. „Hakowanie przy wsparciu sztucznej inteligencji jest łatwiejsze niż obrona z jej pomocą. Nasze obecne systemy nie są na to gotowe, a jednocześnie brakuje środków na ich zastąpienie. Wkrótce będziemy mieć do czynienia z hakowaniem na masową skalę, w ramach którego maszyny będą szukały w internecie podatności do wykorzystania. Najlepszym rozwiązaniem tego problemu jest przyjęcie podejścia Security by Design" – mówił Menny Barzilay.

Podobno szachowy mistrz świata, Garri Kasparow, już w 1996 r., podczas pierwszego pojedynku z komputerem Deep Blue, wiedział, że kończy się pewna epoka w rozwoju ludzkich możliwości. Pomimo że ostatecznie zwyciężył, jego pierwsza przegrana partia dała mu do myślenia: jeśli komputer choć raz jest w stanie pokonać mistrza, to znaczy, że wkrótce będzie mógł wygrywać z człowiekiem za każdym razem. Jego przeczucie sprawdziło się rok później: Kasparow uległ, Deep Blue triumfował – komputer wygrał drugie starcie z mistrzem. A kiedy maszyna raz osiągnie dominującą pozycję, już nigdy jej nie odda.

Według Menny'ego Barzilaya, dzisiaj jesteśmy w podobnej sytuacji w dziedzinie cyberbezpieczeństwa. Chociaż komputery nie mogą jeszcze pokonać człowieka w hakerskich pojedynkach typu Capture the Flag, to już sam fakt, że są w ogóle są w stanie konkurować z najlepszymi ekspertami od cyberbezpieczeństwa na świecie, zwiastuje nadejście nowej ery. Jeszcze w nią nie weszliśmy – uczenie maszynowe, uczenie głębokie to jeszcze nie sztuczna inteligencja, niemniej ostatnie osiągnięcia, np. w obszarze widzenia komputerowego czy komunikacji w języku naturalnym, to prawdziwe kamienie milowe. „Połączenie tych nowych technologii otwiera ogromne możliwości. Ostatecznie spodziewam się, że sztuczna inteligencja przyniesie więcej dobrego niż złego, ale w krótkim czasie możemy oczekiwać

CSO musi obecnie spodziewać się niespodziewanego. Dlatego, choć ochrona i prewencja nadal są ważne, coraz więcej organizacji koncentruje się na doskonaleniu wykrywania zagrożeń i reagowania na incydenty.

Machine learning wymaga bardzo dużych próbek i długiego treningu. Z praktycznego punktu widzenia optymalne wydaje się zawężenie obszaru ochrony i skupienie się na krytycznych zasobach.

PAWEŁ ŁAKOMSKI,
TECHNOLOGY SOLUTION PROFESSIONAL, MICROSOFT

Bezpieczeństwo wbudowane w software

Zastosowanie podejścia Security by Design oznacza nie tylko ograniczenie ryzyka i zapewnienie wyższego poziomu bezpieczeństwa, ale także oszczędności, zgodność z regulacjami prawnymi oraz... mniej frustracji dla zespołu programistycznego – przekonywał Aleksander Ludynia, Security Director w AC Project, podczas wystąpienia w sesji „Wizje i realizacje".

Jego zdaniem, w praktyce często mamy do czynienia z „odkładaniem bezpieczeństwa na później", skupianiem się wyłącznie na testach penetracyjnych. Powszechny jest brak świadomości zagrożeń, dominuje założenie, że programiści „znają się na bezpieczeństwie". Tymczasem właśnie takie podejście jest źródłem wielu poważnych problemów.

Dlatego bezpieczeństwo musi zostać wbudowane w cały cykl rozwoju oprogramowania:

- od etapu **planowania** – wyznaczenie osoby bądź zespołu odpowiedzialnego za bezpieczeństwo, identyfikacja kluczowych regulacji i przepisów, wstępne określenie technologii oraz procesów;
- przez **analizę** i mapowanie wymagań bezpieczeństwa wynikających z regulacji, norm, oczekiwań klientów, najlepszych praktyk, rozwiązań konkurencyjnych i ryzyka;
- **projektowanie** – przełożenie wyników analizy na mechanizmy bezpieczeństwa w połączeniu z modelowaniem zagrożeń (wymaga to stałej współpracy pomiędzy programistami a bezpiecznikami);
- **implementację** – wytyczne, konsultacje, szkolenia dla programistów dotyczące zasad bezpiecznego kodowania, przegląd fragmentów kodu;
- **testowanie** dynamiczne i statyczne – testy penetracyjne, automatyzacja testów, weryfikacja komponentów zewnętrznych, ocena zaadresowania modelowanych zagrożeń;
- aż po **utrzymanie** – zarządzanie znanymi podatnościami, zarządzanie ryzykiem, monitoring, sprawna obsługa incydentów, okresowa weryfikacja.

Źródło: Aleksander Ludynia, prezentacja „Security by Design w praktyce. Tworzenie oprogramowania"

większej liczby zagrożeń niż korzyści" – mówił Menny Barzilay.

Internet nie został bowiem zaprojektowany z myślą o bezpieczeństwie. Nie to jest jednak najgorsze. Większym problemem jest fakt, że nie da się tego naprawić. Konieczna byłaby wymiana wszystkich urządzeń, a to nie jest możliwe. Co więcej, do tej niebezpiecznej infrastruktury podłączamy nowe urządzenia. Cały czas dokonujemy drobnych zmian, ale nie wpływają one zasadniczo na poprawę bezpieczeństwa sieci. Sztuczna inteligencja może spowodować radykalną zmianę, której potrzebujemy. Niemniej podstawowa zasada mówi: zmiana zawsze równa się nowym szansom, ale i nowym zagrożeniom.

Potrzeba nowego podejścia

O jakich zagrożeniach mówimy? Cyberprzestępcy będą mogli wykorzystywać sztuczną inteligencję na potrzeby realizowanych ataków. Można wyobrazić sobie nie tylko złośliwe, ale zarazem „rozumne" oprogramowanie. Tzw. bariera wejścia w technologię jest stosunkowo niska. Dostępne są liczne,

Blisko trzy na cztery ataki celowane zaczynają się od e-maila. Dlatego konieczne jest wykorzystanie zaawansowanych mechanizmów ochrony poczty nowej generacji.

TOMASZ ROT, COUNTRY SALES MANAGER, BARRACUDA

zaawansowane narzędzia w modelu open source, z których chętnie korzystają atakujący.

To jednak nie wszystko. „Przestępcy mogą atakować samą sztuczną inteligencję. W napędzającym ją oprogramowaniu znajduje się ogromna liczba błędów, które nie są szybko poprawiane. Można wyobrazić sobie także zatruwanie danych treningowych do uczenia maszynowego. Do tego dochodzą kwestie etyczne i zagrożenia dla prywatności" – podkreślał Janusz Żmudziński, wiceprezes Polskiego Towarzystwa Informatycznego. Jako przykład podawał realizowany przez Ministerstwo Obrony USA projekt broni autonomicznej Maven – współpracy przy jego rozwoju odmówili pracownicy Google. Wymieniał także chińskie projekty związane z systemem kredytu społecznego, okularów do rozpoznawania twarzy czy sieci monitoringu wizyjnego.

Do grona ekspertów, którzy mają obawy związane z wykorzystaniem przez hakerów sztucznej inteligencji, należy także Mikko Hypponena, Chief Research Officer w F-Secure. Uważa on, że wkrótce sytuacja może stać się poważna. „Na razie nie obserwujemy jeszcze ataków wykorzystujących technologię machine learning. Jeśli jednak sytuacja się zmieni i takie ataki się pojawią, będziemy mieli do czynienia ze znaczącym wyzwaniem. Wówczas będzie naprawdę źle" – mówił Mikko Hyponnen podczas wystąpienia „Gdzie jesteśmy i dokąd zmierzamy".

Zastanawiał się m.in., jak zabezpieczyć 10 mld nowych urządzeń, które w ciągu najbliższej dekady mają zostać podłączone do sieci. Dzisiaj praktycznie wszystkie urządzenia elektroniczne stają się komputerami. Jeśli jakiś sprzęt można określić jako „smart" – np. smart phone, smart TV czy smart watch – to oznacza, że jest on podatny na atak.

Dlatego potrzebne jest nowe podejście. Nie sprawdza się tradycyjny „model sejfu", który buduje się przy wykorzystaniu rozmaitych narzędzi, żeby trzymać w nim swoje najcenniejsze zasoby. Wszyscy wolimy myśleć, że nikt nie dostanie się do sejfu. Należy

Fakty i liczby: konsekwencje naruszenia bezpieczeństwa danych

(Raport Ponemon Institute, lipiec 2018 r.)

3,86 mln USD
średni koszt wycieku danych

148 USD
średni koszt w przeliczeniu na ukradziony rekord

27,9%
prawdopodobieństwo ponownego wycieku danych w ciągu dwóch następnych lat

6,4%
średni całkowity roczny wzrost kosztów

4,8%
roczny wzrost kosztów per capita

Dzięki nawiązaniu współpracy z zespołem Incident Response można osiągnąć średnie oszczędności kosztów na poziomie 14 USD w przeliczeniu na pojedynczy rekord.

Źródło: Daniel Donhefner, IBM Security Services CEE Leader w IBM, prezentacja „Trendy w cyberbezpieczeństwie – dziś i jutro"

Jakie wyzwania dla bezpieczeństwa tworzy model SaaS/IaaS?

Shadow IT
- nie wiadomo, ile usług SaaS jest wykorzystywanych w organizacji

Informacje i kontrola
- brakuje informacji, jakie dane i pliki są przechowywane w usługach SaaS/IaaS i komu są udostępniane
- kontrola nad konfiguracją zasobów IaaS jest ograniczona

Egzekwowanie polityk i zgodność
- nie ma możliwości kontrolowania dostępu czy dystrybucji danych w aplikacjach SaaS
- nie wiadomo, czy w przypadku SaaS utrzymane są standardy zgodności z regulacjami
- nie ma kontroli nad konsumpcją zasobów w IaaS

Zagrożenia z chmury
- nie wiadomo, czy informacje w chmurze są bezpieczne i nie stanowią zagrożenia dla użytkowników w wewnętrznej sieci

Wcześniejsze dane w chmurze
- firewall jest pomocny, ale nie wiadomo, co zostało zapisane w chmurze, zanim zaczęło to być monitorowane

Źródło: Roy Scotford, Consulting Systems Engineer w Fortinet, prezentacja „Monitoring bezpieczeństwa w chmurze – perspektywa klienta i użytkownika"

jednak założyć, że do tego dojdzie i przygotować się na włamanie. Nikt zazwyczaj nie spodziewa się, że zostanie zaatakowany przez niewinnego chatbota na stronie WWW – tymczasem tak to właśnie się odbywa.

„Stara mądrość o budowaniu bezpieczeństwa jako sejfu musi zostać zmieniona. Skoro nikt nie dostanie się do sejfu, to po co nam wykrywacz ruchu w sejfie? To błędne myślenie. Dlatego potrzebne są sensory. Pozwalają one wykrywać nietypowe działania. I choć czasem mogą generować fałszywe alarmy, to przynoszą o wiele więcej korzyści niż problemów. Taki fałszywy alarm pokazuje, że system działa, jest czujny" – mówił Mikko Hypponen.

Na nieadekwatność starych metod zwracali także uwagę Paweł Łakomski, Technology Solution Professional w Microsoft, oraz Przemysław Zębik, Doradca Technologiczny w Microsoft. Ich zdaniem, nowe wektory ataków i nowe ich metody związane z IoT czy łańcuchem dostaw wymagają nowego podejścia i zastosowania nowych rozwiązań. Na ciągu ostatnich kilku lat pojawiło się wiele technologii pozwalających zabezpieczyć się przed nowymi zagrożeniami. Wizja bezpieczeństwa

Ochrona danych przechowywanych w aplikacjach typu SaaS stanowi coraz większe wyzwanie. Zapewnienie bezpieczeństwa w tym obszarze jest jednym z największych problemów dla CISO.

ROY SCOTFORD, CONSULTING SYSTEMS ENGINEER, FORTINET

Chmura i mobilność napędzają cyfrową transformację, ale jednocześnie wymuszają zmiany w podejściu do bezpieczeństwa. Internet staje się nową siecią korporacyjną, którą trzeba kontrolować i zabezpieczać.

ALEX TETERIS,
PRINCIPAL TECHNOLOGY
EVANGELIST, ZSCALER

w dobie inteligentnych technologii proponowana przez Microsoft opiera się na analityce chmurowej, wykorzystaniu machine learning i zaawansowanej automatyzacji.

Przykładem zastosowania takich inteligentnych mechanizmów jest analizowanie danych o zdarzeniach i logów oraz prognozowanie na tej podstawie możliwych scenariuszy ataków i przygotowywanie potencjalnych odpowiedzi na incydenty. Paweł Łakomski zwracał jednak uwagę, że machine learning niesie ze sobą też wyzwania. Wymaga wykorzystania bardzo dużych próbek i zastosowania długiego treningu, w przeciwnym wypadku będziemy narażeni na dużą ilość fałszywych alertów. Dlatego z praktycznego punktu widzenia optymalnym podejściem wydaje się zawężenie obszaru ochrony i skupienie się wyłącznie na krytycznych zasobach.

Totalna automatyzacja

Wizję wykorzystania analityki, automatyzacji i machine learning podzielają także inne firmy, w tym wiele start--upów. O automatycznym wykrywaniu incydentów mówił podczas konferencji Alex Vaystikh, CTO i współzałożyciel firmy SecBI. Analiza ruchu sieciowego to doskonałe pole do działania dla zaawansowanych mechanizmów analitycznych. Dlaczego? Dlatego że bardzo trudno analizować tego typu dane – zbiory są ogromne, ciągle się zmieniają, a przy tym dotyczą rozmaitych urządzeń i środowisk. Analityka w połączeniu z machine learning pozwala na ich wykorzystanie

Analityka w połączeniu z machine learning pozwala na efektywne wykorzystanie ogromnych zbiorów danych o ruchu sieciowym i zdobycie niedostępnych w inny sposób informacji.

Sztuczna inteligencja przyniesie ostatecznie więcej dobrego niż złego. W najbliższym czasie możemy jednak oczekiwać większej liczby zagrożeń niż korzyści.

i zdobycie niedostępnych w inny sposób informacji. Dotyczy to zwłaszcza najtrudniejszego obszaru: detekcji, ale także dochodzenia oraz prowadzenia poszukiwań.

„Machine learning idealnie nadaje się do zastosowania w cyberbezpieczeństwie, ponieważ mamy do czynienia z coraz większą ilością danych. Na rynku brakuje odpowiednio wykształconych ludzi, a powierzchnia ataku ciągle się powiększa" – zwracał uwagę Alex Vaystikh.

Mechanizmy machine learning pomagają powstrzymywać phishing, chroniąc użytkowników poczty elektronicznej przed oddziaływaniem socjotechniki. „Blisko trzy na cztery ataki celowane zaczynają się od e-maila. Dlatego konieczne jest wykorzystanie zaawansowanych mechanizmów ochrony poczty nowej generacji. Przykładowo, technologia uczenia maszynowego bazująca na informacjach z 2,5 mln skrzynek pocztowych pomaga chronić przed atakami typu zero payload. Analizując 40 różnych składników, zapewnia stosunek false-positive bliski 1 do miliona" - mówił Tomasz Rot, Country Sales Manager w Barracuda.

Chmura możliwości i ryzyk

Upowszechnienie wykorzystania usług chmurowych w biznesie postępuje w ogromnym tempie. Każdego dnia w firmach wypróbowuje się nowe rozwiązania cloud computing. Przy tym o wiele łatwiej je wdrożyć,

Podejście Security by Design oznacza nie tylko ograniczenie ryzyka i zapewnienie wyższego poziomu bezpieczeństwa, ale także oszczędności, zgodność z regulacjami prawnymi oraz mniej frustracji dla programistów.

ALEKSANDER LUDYNIA,
SECURITY DIRECTOR, AC PROJECT

niż później wycofać z użycia. Najgorsze jest jednak to, że wchodzą one do organizacji bocznymi albo tylnymi drzwiami. Ich wykorzystania nie nadzoruje centralnie dział IT. Tworzy to poważne wyzwania w obszarze bezpieczeństwa. Pracownicy korzystają z ofert różnych dostawców, których usługi nie są zabezpieczone w taki sam sposób.

„Zwłaszcza ochrona danych przechowywanych w aplikacjach typu SaaS stanowi coraz większe wyzwanie. Zapewnienie bezpieczeństwa w tym obszarze jest jednym z największych problemów dla CISO, ponieważ odpowiedzialność za bezpieczeństwo w chmurze spoczywa na użytkowniku, a nie na dostawcy. To sprawia, że dynamicznie rośnie rynek systemów CASB" – podkreślał Roy Scotford, Consulting Systems Engineer w Fortinet.

CASB, czyli Cloud Access Security Broker, to nowa klasa rozwiązań, które pozwalają na identyfikowanie wrażliwych danych i plików, rozszerzania na nie polityki w zakresie dostępu i udostępniania, a także dostarczania raportów w zakresie ich wykorzystania. Zapewniają one także ochronę przed propagacją zagrożeń z chmury – wirusów i złośliwego oprogramowania. Chronią poza tym dystrybucję wrażliwych danych niezależnie od tego, czy jest celowa czy przypadkowa. System CASB dostarcza też narzędzia do audytowania usług SaaS i zapewnia ich zgodność z polityką bezpieczeństwa. W efekcie uzyskuje się pełen obraz aktualnej sytuacji oraz przejmuje kontrolę nad konsumpcją zasobów i ich konfiguracjami.

O bezpieczeństwie w świecie cloud first z nieco innej perspektywy mówił Alex Teteris, Principal Technology Evangelist w Zscaler. Chmura i mobilność napędzają cyfrową transformację, ale jednocześnie wymuszają zmiany w podejściu do bezpieczeństwa.

> Potrzebne są sensory pozwalające wykrywać nietypowe działania. Choć czasem mogą generować fałszywe alarmy, to przynoszą więcej korzyści niż problemów. Fałszywy alarm pokazuje, że system działa, jest czujny.

„Tradycyjna architektura sieci i bezpieczeństwa, określana jako hub-and-spoke, dostarcza niezawodnego i bezpiecznego dostępu do aplikacji w centrum danych. Jednak przeniesienie aplikacji na nowoczesne platformy chmurowe skutkuje niewygodą dla użytkowników, rosnącą złożonością dla IT oraz wysokimi kosztami dla organizacji. W efekcie użytkownicy pomijają mechanizmy bezpieczeństwa i wzrasta ryzyko dla firmy – zwracał uwagę Alex Teteris. Jego zdaniem, internet staje się nową siecią korporacyjną, którą trzeba kontrolować i zabezpieczać. Użytkownicy chcą szybkiego, wygodnego i bezpiecznego dostępu, a organizacje elastyczności i ograniczenia kosztów. To stawia przed ludźmi od bezpieczeństwa poważne wyzwania, z którymi będą musieli sobie coraz skuteczniej radzić.

ADVANCED THREAT SUMMIT 2018

Bezpieczeństwo z perspektywy akademickiej

O nowej, bezpiecznej, globalnej sieci komunikacyjnej, o sztucznej inteligencji, która zmieni branżę cyberbezpieczeństwa, jej naukowych źródłach oraz ciekawych start-upach w tym obszarze opowiada **Menny Barzilay**, dyrektor ds. technicznych ośrodka Cyber Research Center działającego w ramach Uniwersytetu w Tel Awiwie.

Podczas wystąpienia na konferencji „Advanced Threat Summit 2018" mówił Pan o fundamentalnych, nieusuwalnych problemach związanych z bezpieczeństwem w internecie. Czy jesteśmy skazani na ciągłe zagrożenie, czy też możemy coś z tym zrobić?

To ogromne wyzwanie, ale owszem – możemy. Głównym problemem internetu nie jest to, że nie został on zaprojektowany z myślą o bezpieczeństwie, ale fakt, że jego konstrukcja nie pozwala na odpowiednią aktualizację. Utknęliśmy w ślepym zaułku. Dla wyeliminowania wielu problemów bezpieczeństwa, z którymi się dzisiaj borykamy, trzeba by zmienić podstawowy sposób działania globalnej sieci. Dzisiaj nie ma takiej możliwości.

Nadzieje dają projekty takie jak Loon Google'a czy Internet.org Facebooka. Bezprzewodowe technologie komunikacyjne w ostatnich latach bardzo się rozwinęły. Wkrótce firmy komercyjne przy użyciu stosunkowo niewielkiej liczby urządzeń będą w stanie stworzyć globalne sieci pozwalające każdemu na dostęp do internetu z dowolnego miejsca na świecie o dowolnej porze.

Co, gdyby jedna z tych firm zdecydowała się nie zastosować tradycyjnego TCP/IP, ale jakiś nowy, bezpieczny protokół? To otwiera możliwość stworzenia nowego rodzaju internetu, działającego w inny sposób niż dotychczas, bo zbudowanego zgodnie z podejściem Security by Design. Nazywam tę koncepcję Alternative Global Network – AGN.

Czym się charakteryzuje to podejście?

AGN-y będą podobne do sieci definiowanych programowo. Można w nich zaimplementować rozwiązania z zakresu bezpieczeństwa, a także na bieżąco, w miarę potrzeb dokonywać aktualizacji. W takiej sieci wszystko udaje się bardzo szybko zmienić, a to oznacza znaczne obniżenie kosztów cyberbezpieczeństwa. To byłby koniec Dzikiego Zachodu, z jakim mamy do czynienia obecnie.

Czy sieci AGN miałyby stanowić rozszerzenie internetu, czy też go zastąpią?

Trudno w tej chwili to rozstrzygnąć. Moim zdaniem, potrzebne są dwie sieci. Posiadanie anonimowego internetu jest konieczne dla zapewnienia praw i swobód obywatelskich.

Jednocześnie potrzebna jest sieć, w której wymagana byłaby licencja czy paszport, żeby do niej wejść. Poza tym od chwili wejścia wszystko, co tam robisz, jest rejestrowane. Obecna sytuacja, kiedy w jednej sieci mamy usługi bankowe, usługi edukacyjne dla dzieci, a zarazem pornografię i pedofilię, nie jest optymalna.

Czy rozwiązaniem przynajmniej niektórych problemów cyberbezpieczeństwa może być zastosowanie sztucznej inteligencji?

Sztuczna inteligencja, oczywiście, stworzy nowe możliwości, ale jednocześnie przyniesie wiele nowych problemów. Kluczowe jest jednak to, że nie rozwiąże fundamentalnego problemu: nadal będziemy mieli do czynienia z wyścigiem polegającym na dokonywaniu kolejnych drobnych udoskonaleń, a nie z Security by Design.

W swojej prezentacji wspominał Pan o ogromnej liczbie start-upów powstających w obszarze sztucznej inteligencji. Na które z nich, Pańskim zdaniem, warto zwrócić szczególną uwagę?

Pojawiło się wiele ciekawych firm. Jedną z nich jest Cognito, która stworzyła agenta AI potrafiącego czytać dokumenty i rozumieć ich treść tak, że jest w stanie poklasyfikować dokumenty w sposób zgodny z wymaganiami GDPR. To bardzo przydaje się w przypadku wystąpienia incydentu wycieku danych, ponieważ łatwo można odkryć, kto miał do czynienia z tym danymi i kto je przesyłał. Dotychczas w podobnych sytuacjach konieczne było zatrudnienie kilkudziesięcioosobowego zespołu, który potrzebował sporo czasu na wykonanie zadania. Sztuczna inteligencja radzi sobie z tym błyskawicznie.

Inny przykład to obecna na konferencji „Advanced Threat Summit 2018" izraelska firma SecBI, która ma niesamowite osiągnięcia w obszarze automatycznej analizy informacji powiązanych z alertami bezpieczeństwa. To kolejny dowód na to, że sztuczna inteligencja może pomóc oszczędzać bardzo dużo czasu w dziedzinie cyberbezpieczeństwa, wykonując za ludzi żmudne, pracochłonne zadania.

Bardzo ciekawe firmy pojawiają się w obszarze automatycznych testów penetracyjnych. Przykładem jest XM Cyber, która w ciągu 24 godzin hakuje system, dostarczając informacji o potencjalnych problemach i koniecznych działaniach naprawczych.

Mówił Pan, że sztuczna inteligencja to problem naukowy. Czy to właśnie w ośrodkach akademickich rodzi się najwięcej innowacji w tym obszarze?

Cyberbezpieczeństwo to wyjątkowa dziedzina, zwłaszcza w Izraelu, gdzie można wskazać wiele przykładów, że badania rozpoczęte na uniwersytetach kontynuowane były w przemyśle. Niemniej sztuczna inteligencja to dziś tak naprawdę machine learning czy głębokie uczenie. Sztuczna inteligencja to po prostu modny termin. Branża IT lubi takie nośne marketingowo hasła i nie ma w tym nic złego. Warto jednak pamiętać, że na prawdziwą sztuczną inteligencję przyjdzie nam poczekać jeszcze 10, a może 50 lat.

Tak czy inaczej spodziewałbym się jej odkrycia właśnie w środowisku akademickim. Nie jest to chyba nic dziwnego, skoro i Google, i Microsoft współpracują z ośrodkami akademickimi w tym obszarze. To ważne, żeby stworzyć taki silny ekosystem innowacji obejmujący biznes oraz instytucje naukowe. W tym kontekście nie należy zapominać o armii. Izrael jest tu doskonałym przykładem.

Koncepcja Alternative Global Network (AGN) otwiera możliwość stworzenia nowego rodzaju internetu, działającego w bezpieczniejszy sposób niż dotychczas, bo zbudowanego zgodnie z podejściem Security by Design.

ADVANCED THREAT SUMMIT 2018

Bezpieczeństwo, czyli gotowość na najgorsze

Jesteśmy świadkami dynamicznych zmian w obszarze cyberbezpieczeństwa. W zasadzie każde urządzenie w sieci staje się komputerem. Inteligentne rozwiązania dają użytkownikom nowe, niespotykane dotąd możliwości, ale zarazem tworzą nowe pole działania dla cyberprzestępców. To rodzi nowe wyzwania w zakresie odpowiedzialności za stworzenie warunków do bezpiecznego korzystania z najnowszych technologii. Rozmowa z **Mikko Hypponenem**, pełniącym funkcję Chief Research Officer w F-Secure.

Podczas wystąpienia na „Advanced Threat Summit 2018" mówił Pan, że tradycyjny model bezpieczeństwa cyfrowego przestał się sprawdzać...

Przez lata nieustannie powtarzaliśmy firmom, żeby zabezpieczały swoje sieci w taki sposób, jakby budowały sejf, który pozwoli cały czas trzymać wszystkich z dala od kluczowych zasobów. To już nie działa. Dzisiaj trzeba budować systemy, które sprawiają wrażenie możliwości powstrzymania wszelkich ataków, ale jednocześnie pozwalają wykrywać próby ataków i umożliwiają skuteczne reagowanie w sytuacji, gdy dochodzi do włamania. Problem polega na tym, że nikt nie chce dopuścić do siebie takiej myśli. Nikt nie lubi myśleć o tym, że dojdzie do naruszenia bezpieczeństwa. Tymczasem właśnie nad tym powinniśmy się zastanowić: czy jestem gotowy na atak i co zrobię, kiedy do niego dojdzie, jak zareaguję?

Z czego wynika ta potrzeba? Jakie okoliczności powodują konieczność zmiany podejścia do kwestii bezpieczeństwa?

Największym wyzwaniem dla bezpieczeństwa w tej chwili jest fakt, że wszystkie urządzenia stają się komputerami. Pracowaliśmy jako branża intensywnie nad zabezpieczaniem komputerów przez 30 lat. Jesteśmy w tym dobrzy. Wiemy, jak to robić. Dzisiaj mamy jednak do czynienia z samochodami, które są komputerami. Kamery monitoringu wizyjnego tworzące systemy ochrony dla ludzi i mienia są komputerami. Nawet automaty do sprzedaży kawy są obecnie komputerami. I nie potrafimy ich dobrze zabezpieczyć w taki sam sposób, jaki sprawdzał się jeszcze kilkanaście lat temu w przypadku tradycyjnych komputerów. To kluczowe wyzwanie, z którym musimy się dziś zmierzyć. Nad tym musimy i będziemy pracować.

Jakie mogą być kierunki przeciwdziałania temu zagrożeniu? Kto i jakie działania powinien podjąć?

Odpowiedzialność za bezpieczeństwo podłączonych do sieci inteligentnych urządzeń IoT czy ICS jest rozproszona, za bardzo rozproszona. Oczywiście, częściowo odpowiedzialność spada na producentów, dostawców

tych urządzeń. Po części należałoby ją przypisać użytkownikom. Wiele problemów i luk w bezpieczeństwie systemów IoT wynika z tego, że użytkownicy nieprawidłowo je konfigurują. Część odpowiedzialności powinna także spadać na operatorów telekomunikacyjnych. Przecież to za pośrednictwem należących do nich sieci dokonywane są ataki. Możemy też mówić o odpowiedzialności regulatorów rynków i instytucji tworzących regulacje prawne. Jest bardzo prawdopodobne, że pewnego dnia będziemy mieli uregulowane kwestie nie tylko bezpieczeństwa fizycznego elektroniki domowej, ale także bezpieczeństwa cyfrowego tych urządzeń.

W jaki sposób można zabezpieczyć środowisko IoT?

Zabezpieczenie współczesnych urządzeń IoT wymaga zastosowania routera bezpieczeństwa. To jedyny sposób, w jaki można to zrobić, ponieważ nie jest możliwe zainstalowanie rozwiązania typu Endpoint Security Solution na samych urządzeniach. Konieczne staje się zatem wykorzystanie sieci. Na rynku są dostępne takie urządzenia. My też je oferujemy. Pozwalają uruchomić hotspot WiFi i podłączyć do niego wszystkie urządzenia w domu, na jakich nie można zainstalować żadnego oprogramowania, które by je chroniło. Oznacza to, że zabezpieczamy te urządzenia od strony sieci. To działa, ale nie wiadomo, jak długo będzie się sprawdzać. Cały czas pojawiają się nowe technologie. Wkrótce zacznie się popularyzować 5G. Ostatecznie WiFi przestanie być najważniejszym mechanizmem wykorzystywanym przez urządzenia IoT.

Czy w tym obszarze może coś zmienić wykorzystanie sztucznej inteligencji?

To gorący temat. Cały czas otrzymuję wiele pytań dotyczących uczenia maszynowego i sztucznej inteligencji: jakie znaczenie mają one dla bezpieczeństwa i co to znaczy w kontekście możliwych ataków. W tej chwili sytuacja jest zadowalająca. Widzimy, jak uczenie maszynowe jest wykorzystywane przez dobrych, a nie przez złych.

Firmy z branży cyberbezpieczeństwa używają uczenia maszynowego od lat. Przede wszystkim, żeby być w stanie obsługiwać ogromne ilości danych, z jakimi mamy na co dzień do czynienia. Prawdą jest jednak, że z uczenia maszynowego mogliby również skorzystać atakujący. Nie widzieliśmy jeszcze takiego zastosowania tej technologii w praktyce. Do tej pory mogliśmy obserwować tylko prace badawcze prowadzone na uniwersytetach. Naukowcy zastanawiali się, jak takie ataki mogłyby wyglądać. Na razie nie widzieliśmy, żeby przestępcy wykorzystali sztuczną inteligencję czy uczenie maszynowe w swojej działalności.

W jakiej perspektywie czasowej ta sytuacja może ulec zmianie?

Moim zdaniem, główny powód, dla którego uczenie maszynowe nie jest używane obecnie przez przestępców, jest taki, że na rynku istnieje ogromne zapotrzebowanie na talenty w obszarze uczenia maszynowego, analizy danych oraz programowanie do sztucznej inteligencji. Na rynku brakuje takich specjalistów. To oznacza, że jeśli masz jakieś umiejętności w tych dziedzinach, nie musisz schodzić na złą drogę. Wystarczy przejrzeć ogłoszenia i w dowolnym miejscu na świecie można znaleźć bardzo dobrze płatna pracę. Oczywiście, nie zawsze tak będzie. W końcu systemy uczenia maszynowego staną się tak dostępne, że praktycznie każdy średnio inteligentny przestępca będzie w stanie z nich skorzystać. Wówczas zaczniemy obserwować prawdziwe ataki prowadzone za pomocą sztucznej inteligencji.

Największym wyzwaniem dla bezpieczeństwa jest obecnie fakt, że wszystkie urządzenia stają się komputerami. Nie potrafimy ich dobrze zabezpieczyć w taki sposób, jaki sprawdzał się w przypadku tradycyjnych komputerów.

ADVANCED THREAT SUMMIT 2018

W stronę synergii działań

W walce z cyberzagrożeniami coraz większego znaczenia będzie nabierać wykorzystanie sztucznej inteligencji oraz automatyzacja działań związanych z cyberochroną. Nie oznacza to jednak zmniejszenia roli człowieka. Wręcz przeciwnie, skala wyzwań i zadań stojących przed menedżerami bezpieczeństwa w firmach może wzrosnąć w związku z potrzebą zapanowania nad coraz bardziej złożonym środowiskiem cyfrowym. Przyszłość cyberbezpieczeństwa będzie polegała na coraz większej synergii działań maszyn i ludzi. Już dzisiaj do funkcjonowania w takiej rzeczywistości trzeba się skutecznie przygotować – zwracali uwagę uczestnicy konferencji.

Automatyzacja potrzebna jest m.in. z powodu coraz szybszego działania programów atakujących. Do ochrony przed nimi stare narzędzia mogą okazać się już nieskuteczne. Nowych rozwiązań trzeba też szukać w związku z coraz większą ilością przetwarzanych w organizacjach danych oraz wykorzystywanych do tego celu aplikacji.

Lepsza widoczność

Jednym ze stosowanych w firmach sposobów zapewnienia bezpieczeństwa sieciowych zasobów jest wprowadzenie reguł uniemożliwiających wybranym aplikacjom komunikowanie się z określonymi hostami, lub też zabraniających komunikowania się z jakimkolwiek hostem. Żeby ten mechanizm sprawnie działał, trzeba stworzyć model listingowy, czyli wskazać odpowiednie aplikacje i hosty. Jak to jednak zrobić w sytuacji, gdy firmowe data center już działa? Nie można go zamknąć i zacząć wszystkiego od nowa.

„Wyjściem z sytuacji jest zapewnienie widoczności działających komponentów. Wówczas będzie następowała automatyczna segmentacja dozwolonych relacji pod kątem bezpieczeństwa" – tłumaczył podczas sesji „Technologie, narzędzia i użytkownicy" Mateusz Pastewski, Cyber Security Specialist w Cisco Systems Polska. Automatyzacja sprawdzi się również dlatego, że aplikacje ciągle się zmieniają. To oznacza, że trzeba wciąż aktualizować politykę dostępu, tworzyć od nowa reguły segmentacji.

Na tradycyjnie prowadzonych listach jest bardzo dużo wpisów. Człowiekowi trudno nad nimi zapanować. Często nawet nie wiadomo, które są jeszcze aktualne, a które już nie. Wykorzystanie narzędzi analitycznych pozwala na ominięcie tych utrudnień i zapanowanie nad całością polityki dostępności poszczególnych elementów firmowego środowiska informatycznego. „Platforma analityczna pozwala zrozumieć, jak działają aplikacje i na jakie zagrożenia są narażone. Uzyskana wiedza daje szansę stworzenia lepszej polityki bezpieczeństwa" – przekonywał Mateusz Pastewski.

Aplikacje są różne i działają w różnych środowiskach. Ważne, aby wiedzieć, które mogą komunikować się z jakimi komputerami. Na bazie tych informacji można

budować skuteczną politykę segmentacyjną. System sam tworzy mapę zależności aplikacji i w sposób automatyczny zarządza ich komunikacją z poszczególnymi hostami. Dzięki temu możliwa jest orkiestracja całego systemu.

Najważniejsze dane

Analityka przyda się też przy zasilaniu systemów SIEM (Security Information and Event Management) danymi. Zazwyczaj odbywa się to w czasie rzeczywistym. Dane pochodzą z wielu różnych źródeł (firewall, UTM, urządzenia końcowe, antywirusy, logi systemowe, systemy zarządzania incydentami, zarządzanie dostępem, monitoring sieci etc.). „Rośnie baza danych w systemie SIEM. W wyniku tego spada wydajność jego działania, ale jednocześnie rosną koszty funkcjonowania. Czy więc rzeczywiście wszystkie dane trzeba wprowadzać do systemu SIEM?" – pytał Piotr Kałuża, Presales Engineer z firmy Flowmon Networks.

Rozwiązaniem może być przetwarzanie metadanych zamiast danych. Chodzi o to, aby stworzyć mechanizmy automatycznego zasilania systemu SIEM tylko informacjami kluczowymi, optymalnymi z perspektywy bezpieczeństwa danego procesu. Czy zawsze bowiem trzeba zapisywać, że wszystkie komputery aktualizują w danej chwili oprogramowanie? „Ważne jest, aby były wykrywane anomalie, nie tylko statystyczne, ale też jakościowe, np. w sytuacji, gdy mamy do czynienia z małą liczbą danych, ale wysyłanych systematycznie. To bowiem też może świadczyć o przygotowywaniu ataku" – mówił Piotr Kałuża.

Dzięki temu udaje się osiągnąć większą automatyzację monitoringu sieci. W efekcie pojawią się też realne korzyści w postaci: mniejszej ilości danych potrzebnych do przetwarzania w systemie; przetwarzane dane będą lepszej jakości; zwiększy się wydajność systemu i poprawią się uzyskiwane wyniki; nastąpi lepsze wykorzystanie posiadanych danych.

Platforma analityczna pozwala zrozumieć, jak działają aplikacje i na jakie zagrożenia są narażone. Uzyskana wiedza daje szansę stworzenia lepszej polityki bezpieczeństwa.

MATEUSZ PASTEWSKI, CYBER SECURITY SPECIALIST, CISCO SYSTEMS POLSKA

Kultura bezpieczeństwa

Nawet najbardziej zaawansowane technologie i w najwyższym stopniu zautomatyzowane narzędzia nie zwolnią użytkowników systemów informatycznych od myślenia i stałego przestrzegania zasad

Chodzi o to, aby stworzyć mechanizmy automatycznego zasilania systemu SIEM tylko informacjami kluczowymi, optymalnymi z perspektywy bezpieczeństwa danego procesu.

PIOTR KAŁUŻA, PRESALES ENGINEER, FLOWMON NETWORKS

Sama wiedza o zagrożeniach na nic się nie zda, jeśli nie będzie włączona w proces zarządzania zagrożeniami. Threat Intelligence jest elementem całego systemu bezpieczeństwa, nośnikiem informacji o zagrożeniach.

IRENEUSZ TARNOWSKI, GŁÓWNY EKSPERT BEZPIECZEŃSTWA DS. ANALIZY ZAGROŻEŃ, SANTANDER BANK POLSKA

bezpieczeństwa. „Ważne, by systematycznie budować świadomość bezpieczeństwa w firmie" – podkreślał Jacek Wesołowski, Information Security Officer w Objectivity. Jego zdaniem główne grzechy popełniane przez ludzi odpowiedzialnych za firmowe szkolenia z zakresu cyberbezpieczeństwa to: program minimum, formalizm, niedopasowanie do odbiorcy i sztampowość szkoleń.

Menedżer bezpieczeństwa nie może być oddzielony od reszty pracowników. Nie da się zapewnić odpowiedniego poziomu bezpieczeństwa, jeśli nie będzie się z ludźmi. Trzeba wejść między ludzi i przybliżać im problematykę zagrożeń oraz środków ochrony przed nimi. Księgowej, kadrowej, handlowca nie interesuje bezpieczeństwo. Oni mają swoje zadania do zrealizowania. Rolą CSO jest uwrażliwienie ich na tę problematykę.

Nie sposób zaangażować wszystkich. Należy więc jak najaktywniej pozyskiwać tych, którzy wykazują choć odrobinę zainteresowania. „Trzeba pozyskiwać jak najwięcej ludzi jako ambasadorów bezpieczeństwa. To daje dużą skuteczność wprowadzenia zagadnień cyberbezpieczeństwa do organizacji, większą niejednokrotnie niż kursy i szkolenia" – zwracał uwagę Jacek Wesołowski.

Dobrą metodą na zaangażowanie pracowników w tematykę bezpieczeństwa jest posłużenie się grywalizacją. Można tutaj wykorzystać rozwiązania z zakresu rozszerzonej rzeczywistości czy wirtualnej rzeczywistości. Poprzez zabawę udaje się skutecznie zachęcać do zapoznania się z tematyką bezpieczeństwa. Ludzie lubią współzawodnictwo, rywalizację. Przy okazji mogą wdrażać się w tematykę cyberbezpieczeństwa.

Zdaniem Jacka Wesołowskiego nie ma jednak sensu mówić bezpośrednio o konkretnych technologiach. Co prawda ich wpływ na biznes rośnie, ale jednocześnie stają się one coraz bardziej skomplikowane. Zwykły użytkownik nie zauważy już dzisiaj sam obecności szkodliwego oprogramowania. Lepiej więc zwracać mu uwagę na zachowania przy korzystaniu z komputera i systemów informatycznych niż na konkretnie stosowane rozwiązania techniczne.

Klient odpowiada za to, co przetwarza w chmurze. Dane wędrują między różnymi systemami, użytkownikami. O ich bezpieczeństwo trzeba zadbać wszędzie, nie tylko na serwerze w chmurze, lecz w każdym miejscu organizacji.

ROBERT ŻELAZO, REGIONAL DIRECTOR, PALO ALTO NETWORKS

Holistyczne podejście

Właściwie ukształtowana i obecna na co dzień w organizacji kultura bezpieczeństwa

pozwoli m.in. na skuteczne wykorzystanie wiedzy o pojawiających się zagrożeniach. „Ataki ciągle się zdarzają, wciąż mamy do czynienia z nowymi, udanymi włamaniami i incydentami. Co robimy źle?" – pytał podczas sesji „Perspektywy zagrożeń" Ireneusz Tarnowski, główny ekspert bezpieczeństwa ds. analizy zagrożeń w Santander Bank Polska. Jego zdaniem zapominamy o sztuce wojennej, zapominamy o antycypacji wydarzeń. Działamy reaktywnie, a należy działać uprzedzająco. Trzeba cały czas rozpoznawać przeciwnika, dowiadywać się, jak działa, czego używa, na co możemy być z jego strony narażeni. Po to powstał Cyber Threat Intelligence – jako skuteczna analiza potencjalnych zagrożeń.

Sama wiedza o zagrożeniach nie wystarczy, nawet najpełniejsza i najbardziej wiarygodna. Na nic się nie zda, jeśli nie będzie włączona w proces zarządzania zagrożeniami. „Potrzebne jest podejście holistyczne. Threat Intelligence jest tylko elementem całego systemu bezpieczeństwa, nośnikiem informacji o zagrożeniach" – podkreślał Ireneusz Tarnowski.

Threat Intelligence umożliwia analizę ryzyka, ocenę tego, co może nas spotkać. Potem jednak wyniki tej analizy muszą być umiejętnie wykorzystane w całym łańcuchu zarządzania bezpieczeństwem organizacji. Dobrze przeprowadzony Threat Intelligence i umiejętnie wykorzystane jego wyniki pozwolą niejednokrotnie uniknąć ataków.

Wspólna odpowiedzialność

Szczególną uwagę należy zwrócić na zarządzanie bezpieczeństwem w przypadku korzystania z rozwiązań chmurowych. Mamy tutaj bowiem do czynienia ze wspólną odpowiedzialnością zarówno dostawcy usług chmurowych, jak i ich użytkownika. „To klient odpowiada za to, co przetwarza w chmurze. W jego gestii jest więc zabezpieczenie danych przekazywanych na serwer w chmurze" – zwracał uwagę Robert Żelazo, Regional Director w Palo Alto Networks. Chodzi m.in. o dopilnowanie, aby do przetwarzania nie zostały wysłane niewłaściwe informacje czy dokumenty, np. umieszczone przez pomyłkę dane osobowe. Zadaniem klienta jest też zapewnienie ochrony wykorzystywanym do przetwarzania danych aplikacjom.

„Odpowiedzialność za dostęp do aplikacji i za jakość danych jest po stronie klienta" – podkreślał Robert Żelazo. Bezpieczeństwo to jeden z najważniejszych aspektów korzystania z rozwiązań typu cloud computing. Dane są wszędzie, nie tylko w serwerowni usługodawcy, nie tylko na chmurowym dysku. Kopie plików są też na komputerach pracowników firmy korzystającej z usług w chmurze. Dane wędrują między różnymi systemami, użytkownikami, lokalizacjami. Dlatego też o bezpieczeństwo przetwarzanych zasobów trzeba zadbać wszędzie, nie tylko na serwerze w chmurze, ale też w każdym miejscu organizacji. Dostawca chmury nie zdejmie z klienta odpowiedzialności za korzystanie z aplikacji i danych.

Bezpieczeństwo zasobów powinno iść zawsze w parze z ochroną prywatności osób, których dane są przetwarzane. Projektując system bezpieczeństwa, warto od razu projektować reguły ochrony prywatności.

MONIKA ADAMCZYK,
GŁÓWNY SPECJALISTA W URZĘDZIE OCHRONY DANYCH OSOBOWYCH

W parze z prywatnością

Bezpieczeństwo zasobów i systemów organizacji powinno iść zawsze w parze z ochroną prywatności osób, których dane są przetwarzane – uczulała Monika Adamczyk, główny specjalista w Urzędzie Ochrony Danych Osobowych. Ważne, aby chronione z mocy prawa dane osobowe nie wyciekły na zewnątrz, aby zapewniony był do nich dostęp tylko przez uprawnionych użytkowników. Projektując system bezpieczeństwa, warto też więc od razu projektować reguły ochrony prywatności. To zapewnia firmie działanie zgodne z prawem. Daje też użytkownikom poczucie, że system jest bezpieczny, bo go chroni.

ADVANCED THREAT SUMMIT 2018

Bezpieczeństwo wymaga zaangażowania

Skuteczną ochroną przed cyberzagrożeniami jest zbudowanie kultury bezpieczeństwa w firmie. To daje gwarancję powszechnego stosowania zasad bezpieczeństwa w codziennej pracy – mówi **Jacek Wesołowski**, Information Security Officer w Objectivity.

Podczas konferencji przedstawił Pan zasady budowania programu świadomości bezpieczeństwa w organizacji. Na ile skuteczne może być jeszcze dzisiaj odwoływanie się do postaw ludzkich w sytuacji coraz większego skomplikowania technologicznego środowisk informatycznych, wprowadzania rozwiązań bazujących na sztucznej inteligencji, wykorzystywania algorytmów działających poza świadomością ich użytkowników?

Czynnik ludzki jest i będzie kluczowy dla systemu bezpieczeństwa w firmie. Gdy wchodzą do użycia nowe technologie, to rola człowieka w korzystaniu z nich nabiera jeszcze większego znaczenia. Sztuczna inteligencja, nawet zaawansowana, ciągle jest narzędziem. Systemy stają się coraz bardziej efektywne, więc mają coraz większy wpływ na biznes. W konsekwencji człowiek jest coraz bardziej potrzebny, żeby czuwał nad ich prawidłowym działaniem. Komputery będą powoli zastępować ludzi w wielu miejscach w pracy, ale do końca nigdy nie wyeliminują udziału człowieka.

Gdy systemy stają się coraz bardziej skomplikowane, konsekwencje ich oddziaływania na różne sfery życia też mogą być bardziej znaczące. Dlatego potrzebny będzie cały czas człowiek, który będzie potrafił zarządzać wykorzystaniem najnowszych technologii. Z drugiej strony jednak, dopóki człowiek będzie czynnikiem systemu bezpieczeństwa, dopóty będzie jego najsłabszym ogniwem. Będzie też jednocześnie i tym ostatnim ogniwem, które będzie w stanie wychwycić symptomy, że dzieje się coś złego. To stawia przed ludźmi odpowiedzialnymi za bezpieczeństwo w organizacjach szczególne wyzwania w zakresie kształtowania świadomości bezpieczeństwa.

Czego w takim razie uczyć użytkowników systemów informatycznych, żeby korzystanie z nich zapewniało firmie bezpieczeństwo? Że nie należy przylepiać karteczek z hasłami na monitorze? Że nie wolno otwierać podejrzanych e-maili od nieznanych nadawców? Że nie wolno wpuszczać obcych do

Ludzie mają tendencje do ułatwiania sobie życia, do chodzenia na skróty. A sfera bezpieczeństwa jest takim obszarem, gdzie pójść na skróty jest łatwiej i szybciej. Dlatego też nad wdrażaniem właściwych reguł postępowania trzeba pracować cały czas.

zakładu? Teraz to elementarz bezpiecznych zachowań, jak ktoś przychodzi do pracy, to takie rzeczy powinien już wiedzieć...

Gdyby tak faktycznie było, to nie miałbym zajęcia... Niestety, dzisiaj wciąż jeszcze cały czas trzeba wbijać te rzeczy ludziom do głowy. Podobnie jak z podstawowymi zasadami BHP, gdzie szkolenia też są organizowane non stop, chociaż każdy powinien wiedzieć, że się nie wkłada śrubokręta do gniazdka... Mówiąc ogólnie, ludzie mają tendencje do ułatwiania sobie życia, do chodzenia na skróty. A sfera bezpieczeństwa jest takim obszarem, gdzie pójść na skróty jest łatwiej i szybciej. Dlatego nad wdrażaniem właściwych reguł postępowania do codziennych zachowań trzeba cały czas pracować.

To jest praca nieustannie od podstaw, praca trudna, bo w zasadzie nigdy się niekończąca. To ciągłe kształtowanie świadomości użytkowników w obliczu zachodzących nieustannie zmian. Pojawiają się wciąż nowe rozwiązania, powstają nowe środowiska pracy; to, co wczoraj było istotne, dzisiaj już nie ma znaczenia. Przykładowo, kiedyś nikt nie przywiązywał wagi do kryptologerów, bo nie były rozpowszechnione. Mówiło się ludziom: jak masz wirusa, to komputer będzie ci wolniej chodził, zwracaj na to uwagę. Dzisiaj to niemożliwe, bo ransomware czeka ukryty w systemie, pracuje pod warstwą użytkownika i ujawnia się wtedy, gdy przychodzi czas. Mówienie więc teraz, że samemu trzeba wykryć wirusa, to absurd.

Na jakie kwestie technologiczne trzeba teraz szczególnie uczulać użytkowników, na jakie rozwiązania technologiczne zwracać ich uwagę w perspektywie polityki bezpieczeństwa? Jaką powinni mieć wiedzę z zakresu technologii, żeby mogli rozpoznać oznaki zagrożenia?

Nie ma sensu stawiać dzisiaj na samodzielne wykrywanie zagrożeń w programach. Systemy informatyczne są coraz bardziej skomplikowane, rośnie więc też i stopień skomplikowania narzędzi wykrywających. Wykrywanie zagrożeń może być elementem szkolenia, ale nie powinno być jego głównym tematem. Nacisk trzeba kłaść przede wszystkim na kształtowanie dobrych nawyków w pracy z komputerem. Warto uczyć, na jakie komunikaty systemu zwracać uwagę, jak je czytać i rozumieć oraz co w poszczególnych sytuacjach robić.

Na ile użyteczne mogą tu być rozwiązania bazujące na sztucznej inteligencji? W jakim zakresie sztuczna inteligencja może wesprzeć użytkowników w bezpiecznym korzystaniu z coraz bardziej skomplikowanych systemów?

W szkoleniu z cyberbezpieczeństwa nie ma sensu wchodzić głęboko w technologie. Trzeba raczej skupiać się na tym, jak obsługiwać programy, jak wchodzić w interakcję z systemem, jak rozumieć pochodzące z niego komunikaty i jak na nie reagować.

Perspektywy użycia są duże, konkretne zastosowania zależą jednak od wielu różnych czynników – społecznych, psychologicznych, prawnych. Jednym z możliwych zastosowań jest monitorowanie zachowań pracownika i dawanie mu podpowiedzi na podstawie analizy tego, co robi, np.: to, co teraz robisz, nie jest właściwe, to jest niebezpieczne, albo: zrobiłeś to dobrze, dalej tak postępuj. Tu oczywiście wchodzimy w sferę prywatności, bo system musiałby mieć dostęp do wszystkiego, co pracownik robi na komputerze, zbierać informacje o każdym otwartym oknie, każdej otwartej aplikacji, każdym wykonanym kliknięciu... Czy chcielibyśmy się zgodzić na taką ingerencję w nasze działania?

Wyjściem mogłyby być analizy statystyczne...

Tak, tu sprawdziłby się np. software skierowany na wykrywanie pracowników stanowiących potencjalne zagrożenie. Analizy byłyby robione w odniesieniu do określonych profili zachowań, system brałby m.in. pod uwagę nawyki pracowników – kiedy kto przychodzi do pracy, co najpierw uruchamia na komputerze, w jakim tempie wystukuje dane lub polecenia na klawiaturze. Chodziłoby o wykrywanie anomalii, to byłaby podstawa do sprawdzenia, dlaczego ktoś, kto zawsze przychodził do pracy o 8.00, nagle zaczął przychodzić o 7.30.

Sztuczna inteligencja może pomagać w walce z zagrożeniami, ale też może być użyta jako narzędzie ataków. Nowe rodzaje niebezpieczeństw mogą też wynikać z faktu zastosowania rozwiązań bazujących na sztucznej inteligencji w systemach biznesowych. Czy należy wobec tego uczyć pracowników podstaw sztucznej inteligencji, by lepiej przygotować ich do skutecznego stawienia czoła nowym zagrożeniom?

Nie ma sensu wchodzić głęboko w technologie. Trzeba raczej skupiać się na tym, jak obsługiwać programy, jak wchodzić w interakcję z systemem, niż uczyć o tym, jak od strony technicznej działają poszczególne narzędzia. Lepiej uczyć zachowań. To, co w środku systemu, to domena wąskiej grupy specjalistów. Użytkowników trzeba raczej uwrażliwiać na konieczność stosowania procedur, uczulać ich na zwracanie uwagi na komunikaty systemowe i anomalie w działaniu programów.

Na ile realne w świecie coraz bardziej zaawansowanych technologii, rozwiązań korzystających z coraz bardziej złożonych, działających niezależnie od człowieka algorytmów są zagrożenia oparte na najprostszych, fizycznych wręcz metodach działania? Powiedzmy, że ktoś wchodzi do serwerowni z dyskietką czy nawet z kartką papieru i długopisem w kieszeni i w ten sposób wyprowadza ważne dane z firmy. Czy jeszcze trzeba na takie rzeczy zwracać uwagę w programach kształtowania świadomości bezpieczeństwa w organizacji?

Posłużę się przykładem z wojska. Mamy coraz bardziej zaawansowane środki łączności. Nie wykryjemy jednak niczego, jeśli pododdział wyjdzie w pole i będzie się posługiwał do komunikacji chorągiewkami. Znika wtedy z pola widzenia, nie zostawia śladów elektromagnetycznych. Tak samo sam człowiek wchodzący do firmy może być poważnym zagrożeniem. A jak będzie bardzo chciał, to zawsze wejdzie, mimo kamer, mimo kart, mimo czujników. Są na to różne sposoby...

Socjotechnika wciąż górą?

Ona nigdy nie straci znaczenia. Bo zawsze człowieka można do czegoś zmusić, przekupić, zmanipulować, przekonać, zaszantażować czy ukierunkować. Mimo używania zaawansowanej techniki nigdy nie możemy powiedzieć, że mamy spokój i możemy czuć się w pełni bezpiecznie.

Jakie czynniki są kluczowe dla efektywnego kształtowania postaw bezpieczeństwa w firmie?

Potrzebna jest przede wszystkim zmiana sposobu myślenia o samym programie kształtowania świadomości bezpieczeństwa (security awareness). Powszechnie przeprowadza się szkolenia, odpytuje uczestników, potem jeszcze robi e-learning... Wszyscy są przekonani, że każdy przyswoił wiedzę i można się tym chwalić podczas audytu. Takie działania nie pozwalają jednak na zakorzenienie postaw bezpieczeństwa w świadomości pracowników.

Kluczowe jest, aby doprowadzić do wprowadzenia zagadnień bezpieczeństwa do środowiska pracy, do codziennych działań i zachowań pracowników. Nie werbalnie, ale innymi, bardziej angażującymi metodami. Można m.in. użyć do tego gier komputerowych, programów wykorzystujących wirtualną rzeczywistość – ludzie bawią się i rywalizują ze sobą, szukając, powiedzmy, punktów zagrożenia w firmie. Są wtedy bardziej zaangażowani w problematykę bezpieczeństwa, zanurzeni w nią, otoczeni nią.

W firmach jest jednak rotacja, pracownicy się zmieniają. Jak zapewnić stałą wewnętrzną integrację postaw bezpieczeństwa z codziennym działaniem organizacji w dłuższej perspektywie?

To nie jest problem. Zazwyczaj zmienia się jedynie około 10% stanu zespołu. Przy silnej, dobrze ukształtowanej kulturze organizacji pozostałe 90% może przekazać kolejnym przychodzącym obowiązujące zasady i reguły, wdrożyć ich w istniejące warunki i procedury. Ludzie pracujący w firmie nasiąkają jej kulturą. Jeśli będą w niej mocno osadzone kwestie bezpieczeństwa, to nimi też nasiąkną. Największym wyzwaniem jest zbudowanie takiej kultury – bo potrzebne są na to środki, bo przeszkadza codzienna walka o priorytety itd. Tu też jest duża rola menedżerów, bo to oni od pierwszych dni kształtują postawę pracownika. Jeśli od początku będą go uwrażliwiać na kwestie bezpieczeństwa, to nimi nasiąknie i będzie się z nimi identyfikował.

Socjotechnika nigdy nie straci znaczenia. Bo zawsze człowieka można do czegoś zmusić, przekupić, zmanipulować, przekonać, zaszantażować czy ukierunkować. Mimo używania zaawansowanej techniki nigdy nie możemy powiedzieć, że mamy spokój i możemy czuć się w pełni bezpiecznie.

ADVANCED THREAT SUMMIT 2018

Co dla maszyn, co dla ludzi?

Co będzie w przyszłości skuteczniejsze dla zapewnienia bezpieczeństwa w firmie: działania systemów sztucznej inteligencji czy aktywność człowieka? Odpowiedzi na to pytanie szukali uczestnicy panelu dyskusyjnego „Człowiek czy maszyna" przeprowadzonego w formie debaty oksfordzkiej.

Teza dyskusji brzmiała: Wszyscy podkreślają potrzebę inwestowania w budowanie „security awarness" – tak aby użytkownik był w pełni świadomy zagrożeń w cyberprzestrzeni i wiedział, jak powinien reagować i zachowywać się, by nie narażać firmy na niepotrzebne ryzyko. Może jednak nie ma to większego sensu, bo zawsze znajdzie się czarna owca, która się nie nauczy, a jeśli się nauczy, to nie będzie pamiętać, a nawet jeśli będzie pamiętać, to nie zrobi tego, co trzeba. Zamiast inwestowania w ludzi trzeba inwestować w narzędzia, które w automatyczny sposób zapobiegną niepożądanym sytuacjom. W czasach, gdy do świata cyberbezpieczeństwa wkracza AI i automatyzacja, stanie się to normą.

Przedstawiamy argumenty przytoczone przez uczestników odgrywających rolę zarówno zwolenników szerokiego zastosowania automatyzacji w cyberochronie, jak i broniących roli człowieka w tych działaniach.

W dyskusji panelowej „Człowiek czy maszyna?" udział wzięli: Tomasz Bujała, CISO, Grupa Ubezpieczeniowa Europa; Tomasz Dziurzyński, dyrektor Departamentu Bezpieczeństwa Systemów Informatycznych i Informacji, Citi Handlowy; Łukasz Guździoł, Head of Frameworks – Global Governance & Chief Information Security Officer PL & ISSA BoD Member, Credit Suisse/TRISW/ISSA Polska; Barbara Nerć-Szymańska, MBA, CISA, CISM, menedżer w Departamencie Bezpieczeństwa, mBank; Jacek Skorupka, dyrektor IT Security, Idea Bank SA; Krzysztof Słotwiński, CSO, BGŻ BNP Paribas. Prowadzenie: Robert Pławiak, prezes zarządu, Intelligent Logistic Solutions (IT SHARED SERVICES Grupy PELION).

Za maszyną

Szacuje się, że do 2030 r. na świecie będzie więcej robotów niż ludzi. Roboty zastąpią człowieka w wielu działaniach. Będą od niego efektywniejsze. Już dzisiaj system sztucznej inteligencji w samochodach autonomicznych jest w stanie przetworzyć 10 tys. razy więcej informacji niż człowiek i o 75% szybciej.

Ludzie, także ci zajmujący się cyberbezpieczeństwem, nie są w stanie poradzić sobie z olbrzymią ilością docierających do nich informacji. Sztuczna inteligencja reaguje szybciej, często reaguje od razu. Człowiek działa z opóźnieniem. Przy dużej ilości informacji sztuczna inteligencja będzie coraz bardziej potrzebna.

Użytkownicy sieci nabierają się cały czas na najprostsze metody phishingu. Maszyna rozpoznaje i blokuje malware. Wszystkich ludzi nie da się wyedukować. Nadal 20–30% kliknie w zainfekowany link. Maszyna może te ataki zablokować, by e-maile z niebezpieczną zawartością w ogóle do adresata nie doszły.

Na testy phishingowe potrzeba dużo czasu i zaangażowania ludzi do ich przygotowania. Są maszyny, które same robią testy. Automatycznie przygotowują środowisko testowe. Po co zatrudniać tyle ludzi do przeglądania logów, lepiej to zautomatyzować. Czas reakcji jest natychmiastowy. Ludzie reagują z opóźnieniem.

Wiele działań jest niemożliwych do wykonania przez człowieka bez wsparcia maszyny, bo informacji do przetworzenia jest coraz więcej. Ludzie nie sprawdzają się przy analizie dużych ilości danych. Lepiej wykorzystać maszynę, żeby chociażby ograniczyć zakres ważnych danych, na podstawie których można podjąć decyzję.

Mamy do czynienia z dużą szybkością zmian, również w dziedzinie cyberbezpieczeństwa. Pojawiają się wciąż nowe rodzaje zagrożeń i nowe metody ataków. Stare metody ochrony już się nie sprawdzają. Przestępcy też automatyzują swoją działalność. Żeby za nimi nadążać, trzeba się stale szkolić. Maszyna nadąża i dzięki temu jest w stanie zabezpieczać luki w systemie.

Człowiek nie radzi sobie ze skomplikowanymi modelami matematycznymi. Myśli liniowo, ma problemy z ogarnięciem funkcji wykładniczej. Wyobraźnia ludzka zawodzi, gdy stopień skomplikowania funkcji jest duży (np. Jak wysoka będzie kartka papieru złożona 45 razy? – Sięgnie aż do księżyca!). Maszyna lepiej sobie radzi, bo lepiej liczy.

Moc maszyn rośnie ekspotencjalnie. Rośnie też liczba kodu używanego do programowania różnych urządzeń, np. w samochodach. W rozrastających się kodach pojawia się coraz większa ilość błędów i pomyłek. To oznacza zagrożenie. Ludzie z ich znalezieniem i wyeliminowaniem sobie nie poradzą. Maszyna jest w stanie to zrobić.

Za człowiekiem

Ludzie będą potrzebni do podejmowania decyzji. W wielu przypadkach maszyna nie podejmie decyzji, człowiek będzie umiał zadecydować. Także w coraz trudniejszych i coraz bardziej skomplikowanych sprawach i sytuacjach. Warunek jest taki, że musi się cały czas uczyć.

Jeśli człowiek się myli, to trzeba go edukować. Trzeba podnosić świadomość ludzi odnośnie do możliwości korzystania z dobrodziejstw sztucznej inteligencji, jak również związanych z tym zagrożeń. Trzeba też koncentrować się na użytkownikach systemów informatycznych, aby radzili sobie z rozpoznawaniem ataków w coraz bardziej złożonym środowisku technicznym.

Tylko człowiek może być ekspertem od cyberbezpieczeństwa. Maszyna może dostarczyć wyniki analiz, ale i tak musi to być potem zweryfikowane przez człowieka. Na przykład wyniki generowane przez skanery podatności trzeba przeanalizować i skategoryzować. Należy im nadać odpowiednie wagi, określić, co jak będziemy traktować. Maszyna może monitorować sytuację, ale to człowiek decyduje ostatecznie, czy mamy do czynienia z faktycznym zagrożeniem, czy z fałszywym ostrzeżeniem.

Maszyna może wspomagać eksperta, nigdy go jednak nie zastąpi. To człowiek może udoskonalić działanie systemów, a nie odwrotnie. To człowiek musi wymyślić założenia, według których maszyna będzie działać. Bo człowiek rozumie kontekst wydarzeń. W tym jest zdecydowanie lepszy od algorytmów sztucznej inteligencji.

Przestępcy ciągle zmieniają metody ataków. Specjaliści od bezpieczeństwa muszą za nimi nadążać. Człowiek rozpoznaje zagrożenie, dopiero potem zatrudnia maszynę do monitorowania sieci. Gdy pojawia się nowy atak, to maszyna sobie nie radzi. Trzeba maszynie najpierw zadać zadanie, dopiero potem będzie działać automatycznie.

Żeby system automatyczny dobrze funkcjonował, potrzebuje odpowiednio przygotowanego środowiska – trzeba wyjść od dobrych danych, procedur, regulacji etc. Maszyny nie zlikwidują chaosu. Maszynie trzeba przygotować środowisko pracy. Może to zrobić tylko człowiek. Tylko on wiec decyduje, jak wszystko ma być zorganizowane, poukładane, żeby maszyna działała efektywnie.

ADVANCED THREAT SUMMIT 2018

Zaufanie walutą cybezpieczeństwa

Blockchain jest technologią, która może pomóc rozwiązać wiele problemów dotyczących bezpieczeństwa sieci komputerowych. O możliwościach jej zastosowania w obszarze cyberbezpieczeństwa mówił podczas „Advanced Threat Summit 2018" **Radosław Wojdowski**, Blockchain Transformation Practitioner z EY.

Internet projektowany był głównie z myślą o zapewnieniu komunikacji, brakuje mu mechanizmów bezpieczeństwa. Pojawił się jednak blockchain, który może tę sytuację odmienić. Technologia rejestrów rozproszonych nabiera szczególnego znaczenia dla bezpieczeństwa w sieci. Głównym argumentem za jej stosowaniem jest zaufanie. Gdy dojrzeje, będziemy mieli do czynienia z kolejnym etapem rozwoju internetu. Dla użytkownika nic się nie zmieni, „pod spodem" dojdzie tylko protokół, który doda bezpieczeństwo.

Blockchain staje się synonimem bezpieczeństwa. Zapewnia bezpieczeństwo transakcji, gwarantuje, że nawet hakerzy nie zmienią dokumentu, którego mamy klucz. Do tej pory jeszcze nikt blockchainu nie złamał. Oczywiście, zhakowano wiele giełd bitcoinów, które są elementami blockchainu. To nie było jednak zhakowanie protokołu, zdeprecjonowanie samej koncepcji.

Kto powinien podjąć się wdrażania rozwiązań opartych na blockchainie do sieciowych systemów bezpieczeństwa? Czy mają to robić instytucje publiczne, operatorzy telekomunikacyjni, czy banki lub inne środowiska biznesowe?

Zastosowań blockchainu jest wiele. Rozwiązania bazujące na tej technologii mogą być wprowadzane w różnych obszarach i przez różne podmioty. W wielu miejscach już działają.

Po ataku na Estonię władze państwowe szukały rozwiązania, które byłoby niedrogie, dostępne dla tak niedużego kraju, a jednocześnie pozwoliło na skuteczne zabezpieczenie ważnych zasobów – danych rządowych, bankowych etc. I wykorzystano do tego celu blockchain.

Na wprowadzenie blockchainu postawiły także rządy państw skandynawskich.

Blockchain, podobnie jak każda inna technologia, nie rozwiązuje wszystkich problemów cyberbezpieczeństwa, szczególnie gdy jest wdrażany wyspowo. W wielu sytuacjach może być jednak użyteczny.

> *Do tej pory jeszcze nikt blockchainu nie złamał. Zhakowano giełdy bitcoinów, które są elementami blockchainu. To nie było jednak zhakowanie protokołu, zdepreczjonowanie samej koncepcji rozwiązania.*
>
> **RADOSŁAW WOJDOWSKI**, BLOCKCHAIN TRANSFORMATION PRACTITIONER, EY

Chodzi o to, by w sytuacji zagrożenia od razu było wiadomo, że ktoś próbuje zmieniać dane. Można szybko sprawdzić, czy coś nie zostało zmienione.

W USA na wykorzystanie blockchaina zdecydowała się rządowa agencja wgrywająca oprogramowanie do dronów. To ma być zabezpieczenie na wypadek, gdyby ktoś nieuprawniony chciał przejąć drona.

Gdzie szukać liderów zmian w organizacjach? Czy wprowadzaniem blockchainu do firmowych struktur bezpieczeństwa powinny zajmować się działy IT, działy bezpieczeństwa, czy działy biznesowe?

Blockchain jest technologią nową, wiele się w jej obrębie dzieje, wiele jeszcze się zmienia. Sytuacja przypomina trochę tę z początków rozwoju oprogramowania w modelu open source, kiedy to firmy patrzyły na nie podejrzliwie. Dzisiaj już stosują je wszyscy.

W tej chwili na świecie jest wielu chętnych do finansowania prac nad rozwojem blockchainu. Postęp jest bardzo duży, chociaż technologia nie jest jeszcze pewna. Wielu potencjalnych użytkowników nie jest wciąż zadowolonych z jej stabilności, uważają, że nie udowodniła jeszcze swej dojrzałości. Z drugiej strony, jest już jednak wiele pionierskich wdrożeń i zastosowań. To nie są rozwiązania drogie, ale pionierskie. Decyduje się na nie także coraz więcej dużych organizacji.

Co powinien wiedzieć o blockchainie CSO lub CISO, żeby przekonać do jego stosowania środowiska biznesowe?

W kontekście cyberbezpieczeństwa wiele się dzisiaj mówi o sztucznej inteligencji, o uczeniu maszynowym. Warto spojrzeć również i na blockchain. Ta technologia, podobnie jak każda inna, nie rozwiązuje wszystkich problemów cyberbezpieczeństwa, szczególnie gdy jest wdrażana wyspowo. W wielu sytuacjach może być jednak użyteczna. Warto jej się przyjrzeć, sprawdzić, co to jest np. stały nośnik. To pierwszy etap w myśleniu o jej zastosowaniu. Potem już konkretne wdrożenia będą pokazywać i udowadniać jej przydatność.

ADVANCED THREAT SUMMIT 2018

ADVANCED THREAT SUMMIT 2018

Biometria behawioralna: nieważne, co robisz, ważne, w jaki sposób

Biometria behawioralna daje możliwość zapewnienia bezpieczeństwa dzięki analizie, jak użytkownik posługuje się komputerem i jak z niego korzysta, a nie tego, co robi. To sposób na zapewnienie ciągłej weryfikacji uprawnień użytkowników do korzystania z konkretnych zasobów czy usług – mówi **Mateusz Chrobok**, Chief Executive Officer oraz prezes zarządu w start-upie Digital Fingerprints.

Dużo już powiedziano o zastosowaniach rozwiązań biometrycznych w dziedzinie cyberbezpieczeństwa. Czym biometria behawioralna różni się od tradycyjnych metod biometrycznych, takich jak skanowanie siatkówki oka czy odczytywanie linii papilarnych?

Budowa siatkówki oka czy układ linii papilarnych nie są unikalne w skali globalnej, czyli dla wszystkich ludzi na świecie. W gruncie rzeczy możemy na ich podstawie, jak dla każdej biometrii, zidentyfikować człowieka jedynie z określonym prawdopodobieństwem. Mamy bowiem do czynienia z jednym elementem stanowiącym punkt odniesienia dla podjęcia decyzji.

Trochę inaczej wygląda sytuacja przy zastosowaniu biometrii behawioralnej. W obszarze interakcji użytkownika z komputerem (Human Computer Interaction – HCI) mamy do dyspozycji dużo danych pochodzących z wielu różnych źródeł. Dzięki temu można tworzyć profile zachowań dla każdego użytkownika komputera. Pozwalają one na ciągłą weryfikację użytkowników korzystających z określonego serwisu. Buduje się je z zastosowaniem technik sztucznej inteligencji i uczenia maszynowego, a także przetwarzania strumieniowego.

Testujemy obecnie takie rozwiązanie we współpracy z jednym z polskich banków. Daliśmy mu możliwość ciągłego uwierzytelniania użytkowników bankowości elektronicznej.

Jak duże prawdopodobieństwo identyfikacji konkretnego użytkownika można osiągnąć dzięki tej metodzie?

Każdy klient korzystający z tego rozwiązania będzie miał inne oczekiwania i potrzeby co do dokładności wyników. Każda predykcja zawsze obarczona jest jakimś błędem. Zależy to od wielu czynników, m.in. od danych, jakie są poddawane analizie. Ich zestaw jest ustalany w porozumieniu z partnerem biznesowym – bierzemy pod uwagę zarówno cechy jednostkowe, jak i właściwości o charakterze społecznym. Wspólnie też określane są granice błędu pomiaru dopuszczalne dla klienta, przykładowo, że system może się pomylić nie częściej niż raz na 100 tys. przypadków. Wtedy dopiero uznajemy, że model, który jest zbudowany dla konkretnego użytkownika, jest gotowy do uruchomienia.

Które zachowania przy komputerze są poddawane analizie dla zbudowania profilu użytkownika?

W grę mogą wchodzić różne źródła danych. Można badać szybkość pisania na klawiaturze, siłę nacisku na ekran dotykowy czy na touch pada lub trajektorię ruchów

myszki. Do wykorzystania są wszelkie rodzaje sensorów wbudowane lub możliwe do wbudowania w sprzęt komputerowy. Jakość danych zależy od liczby wykorzystanych źródeł, im więcej sensorów składa się na model, tym jest dokładniejszy.

W jaki sposób system uczy się rozpoznawania wzorców zachowań poszczególnych użytkowników? Jak długo trwa jego trenowanie, by można było zbudować model dla wybranej osoby?

Długość trenowania zależy od ilości danych, co jest pochodną liczby interakcji w czasie. Zależy to więc od intensywności korzystania z serwisu partnera. Gdy na przykład księgowa stale wprowadza dane, to możemy ją rozpoznawać już po jednej sesji. Na rozpoznanie osób, które rzadziej logują się do systemu, potrzeba więcej czasu. Ważna jest też ilość wprowadzanych danych. Im więcej interakcji z systemem, tym więcej danych o użytkowniku komputera, co w konsekwencji pozwala na stworzenie lepszego modelu. Tam gdzie ludzie mniej używają serwisu, potrzebnych jest więcej sesji do wytrenowania systemu. I odwrotnie.

Ile czasu potrzeba na przygotowanie systemu do pracy przy bardzo dużej liczbie użytkowników?

System można skalować. Działa on w tle, każdego użytkownika analizuje oddzielnie. To powoduje, że identyfikacja wzorców trwa bardzo krótko, a modele są gotowe dla każdego użytkownika tak szybko, jak dostarczy wystarczająco dużo danych dla spełnienia wymagań jakościowych.

A co w sytuacji, gdy z jednej maszyny korzysta więcej niż jeden użytkownik?

Przy współdzieleniu danych dostępowych do serwisu też można wykryć konkretnego użytkownika. System rozpozna, kiedy pracuje uprawniona osoba, a kiedy sesja zostaje przejęta przez kogoś innego. Gdy zmieni się osoba korzystające z serwisu, algorytm to rozpozna, bo będzie miał do czynienia z innym wzorcem zachowań. System działa cały czas, funkcjonuje w tle. W sposób ciągły sprawdza, czy z określonym prawdopodobieństwem jest to ta sama osoba czy nie. Prowadzone jest stałe badanie generowanego przez użytkownika strumienia danych.

A gdy użytkownik zmieni swój sposób korzystania z komputera, bo na przykład jest zmęczony i wolniej pisze na klawiaturze?

System szybko adaptuje się do zmian. Zachowanie użytkownika faktycznie może się zmieniać, gdy na przykład skaleczył palec i już inaczej pisze na klawiaturze, albo gdy ma inną klawiaturę i też inaczej wprowadzana niej dane, lub gdy w myszce bateria jest na wyczerpaniu itd. W takiej sytuacji system trzeba szybko przemodelować, nauczyć nowego wzorca zachowań. Adaptacja jest jedną z kluczowych cech, która umożliwia utrzymanie wysokiej jakości predykcji w naszym rozwiązaniu.

Co się dzieje, gdy zostanie zidentyfikowany nieuprawniony użytkownik? Jaka jest wtedy reakcja systemu?

O tym decyduje partner korzystający z systemu, na przykład bank. Może sobie zażyczyć zarówno tego, aby został powiadomiony wyznaczony pracownik, jak i tego, aby sesja została automatycznie przerwana, a dostęp zablokowany. Powiedzmy, że mamy do czynienia z sytuacją, gdy mąż wchodzi na konto bankowe żony. To partner, czyli na przykład bank, decyduje, co ma się wtedy stać – czy ma nastąpić odmowa dostępu czy obserwacja podejmowanych działań. Partner ustala sposób

W obszarze interakcji użytkownika z komputerem (Human Computer Interaction – HCI) mamy do dyspozycji dużo danych pochodzących z wielu różnych źródeł. To pozwala tworzyć profile zachowań dla każdego użytkownika komputera.

reakcji w konkretnej sytuacji. Nasz system przesyła do partnera informację o tym, jak bardzo konkretna sesja jest podobna do modelu użytkownika w naszym systemie. Decyzja, co z tą informacją zrobić, należy w pełni do partnera.

Kluczowego znaczenia nabiera pytanie o ochronę prywatności i zabezpieczenie danych charakteryzujących zachowania konkretnych osób. Informacje przetwarzane w ramach biometrii behawioralnej mogą zawierać masę cennych informacji o każdym użytkowniku. Jak rozwiązujecie problem ochrony danych osobowych?

Nasze rozwiązanie jest stworzone tak, by było zgodne z RODO. Respektujemy prawo do zapomnienia, umożliwiamy włączenie i wyłączenie systemu dla konkretnych użytkowników. My nie identyfikujemy użytkownika w sensie ustalenia, kim on jest. Może to zrobić jedynie partner, który korzysta z naszego rozwiązania i ma prawo przetwarzać dane osobowe użytkownika, na przykład bank obsługujący swojego klienta. Nasz system nie jest połączony z systemem bankowym w celu wymiany danych osobowych. Naszym zadaniem jest jedynie zweryfikować, czy aktualny użytkownik jest tym, który wcześniej korzystał z danego zasobu partnera.

Nie znamy użytkowników i nie chcemy wiedzieć, kim są, możemy tylko powiedzieć o nich, czy mają prawo korzystać z konkretnej usługi lub zasobów. System ma sprawdzać, czy aktualny użytkownik to rzeczywiście ten, który powinien akurat być. Nie identyfikujemy użytkownika, wychwytujemy jedynie modele zachowań i dostarczamy weryfikację. Nie chcemy wiedzieć, co użytkownik robi, przez co nazywamy nasze rozwiązanie bezkontekstowym.

Gdyby ktoś jednak chciał użyć Waszego systemu do identyfikacji użytkownika, na przykład służby specjalne albo firmy handlujące danymi osobowymi, to czy jest taka możliwość?

Przypisania modelu zachowań konkretnej osobie nie możemy zrobić. My dajemy narzędzie, które po zalogowaniu się użytkownika stwierdza tylko, że jego zachowanie jest zgodne z modelem określonym dla anonimowej osoby X lub nie jest zgodne. Użytkownik wysyła strumień danych związanych z obsługą komputera i tylko on jest poddawany analizie. Nasz system wykrywa, że z określonym prawdopodobieństwem jest to akurat klient X.

Nie ma punktów wymiany danych osobowych między naszym systemem a systemem partnera korzystającego z naszych usług. My przechowujemy w bazie tylko modele pozwalające na odwzorowanie zachowań użytkownika w trakcie jego korzystania z komputera. Zidentyfikować konkretnego użytkownika może jedynie partner korzystający z naszego rozwiązania.

Dodatkowo stworzyliśmy manifest, w którym mówimy wprost o tym, że celem przetwarzania danych jest wyłącznie dostarczenie rozwiązania bezpieczeństwa. Jest on dostępny na stronie: https://fingerprints.digital/manifesto.

Na czym polega przewaga rozwiązań z dziedziny biometrii behawioralnej nad tradycyjnymi metodami uwierzytelniania użytkowników systemów informatycznych?

Loginy lub hasła wcześniej czy później mogą wyciec, dostać się w niepowołane ręce bądź zostać złamane. W przypadku interakcji użytkownika z komputerem nie trzeba mieć żadnych dodatkowych rzeczy, o które trzeba specjalnie dbać. Uwierzytelnianie następuje po prostu w trakcie działań użytkownika. Nie jest ograniczone tylko do momentu logowania, lecz odbywa się podczas całej pracy z systemem partnera. Jest więc możliwość zareagowania, gdy sesja zostanie w trakcie przejęta przez kogoś obcego.

Oferujemy ochronę na pewnym poziomie prawdopodobieństwa jak każda biometr az tą różnicą, że nasze rozwiązanie jest zależne od ilości danych. System cały czas się uczy, mając do dyspozycji coraz więcej danych. Wraz ze wzrostem puli danych do analizy poprawia się jakość modeli.

Gdzie są granice optymalizacji modelu? Ile trzeba mieć danych, żeby uznać, że algorytmy gwarantują odpowiednią skuteczność wykrywania wzorców zachowań? Teoretycznie, można myśleć o nieograniczonej ilości danych...

System jest rozwijany tak, by sam identyfikował cechy najlepiej opisujące użytkownika. Nie ma sensu zbierać wszystkich danych dla wszystkich użytkowników. Przy dużej liczbie osób korzystających z komputerów byłoby to po prostu za drogie.

Czy Wasze rozwiązanie opiera się tylko na analizie strumienia danych generowanych przez użytkownika, czy też system ma również zaimplementowane informacje z dziedziny psychologii, socjologii, ekonomii, które porównuje z zachowaniami osoby pracującej na komputerze?

Oczywiście, dajemy systemowi jakieś cechy wyjściowe, na przykład trajektoria myszki, ale w naszym rozwiązaniu podstawową rolę odgrywa statystyka. Bazujemy na sile zbioru danych. Nie chcemy wiedzieć, co robią użytkownicy – z czego korzystają, jakie treści przesyłają, czy dopiero przyszli do pracy, czy też mają akurat przerwę śniadaniową. Informacje charakteryzujące postać użytkownika nie są nam potrzebne i użycie ich uważamy za nieetyczne. Nasze algorytmy opierają się tylko na analizie danych generowanych przez człowieka przy korzystaniu przez niego z komputera.

Idziemy w kierunku automatyzacji działań. Nie jesteśmy w stanie wszystkiego sami wymyślić, ustalić wcześniej, że na przykład trzeba zwracać uwagę na siłę i szybkość naciskania klawiszy, rytm i częstotliwość przerw robionych w pisaniu itd. Nie damy rady szczegółowo z góry określić, co może być ważne dla zachowań konkretnej osoby przy komputerze. Stawiamy na automatyzację, aby system sam znajdował cechy istotne dla określenia modelu działań użytkownika. Mogą to być czasami nawet wskaźniki zupełnie dla nas niezrozumiałe albo takie, o których sami byśmy nigdy nie pomyśleli. Jeśli jednak z analizy wyjdzie, że mogą mieć wpływ na wzorce zachowań, to algorytm automatycznie wykorzysta je do budowania modeli. Jest to nasz sposób na wykorzystanie tak zwanego uczenia głębokiego (deep learning).

W jakich branżach, poza wymienioną już bankowością, biometria behawioralna może znaleźć zastosowanie?

Może być wykorzystywana w najróżniejszych systemach, wszędzie tam, gdzie istnieje potrzeba stałego zabezpieczenia pracy w sieci. Poza bankowością może znaleźć zastosowanie w handlu czy w opiece zdrowotnej.

> W przypadku interakcji użytkownika z komputerem nie trzeba mieć żadnych dodatkowych rzeczy, o które trzeba specjalnie dbać. Uwierzytelnianie następuje po prostu w trakcie działań użytkownika. Nie jest ograniczone tylko do momentu logowania, lecz odbywa się podczas całej pracy z systemem partnera.

W bankowości wzrost zainteresowania tą metodą może nastąpić po wejściu w życie w przyszłym roku unijnej dyrektywy PSD2, która nałoży na instytucje finansowe obowiązek stosowania mocnych sposobów autoryzacji transakcji (Strong Customer Authentication). Do dalszego użytku nie będzie dopuszczona na przykład autentykacja przez SMS. To wymusi na sektorze finansowym poszukiwanie nowych, skuteczniejszych metod uwierzytelniania. Biometria behawioralna może być jedną z nich.

Może też być stosowana do walki z oszustwami. Pozwala bowiem na szybkie uwierzytelnianie i szybką reakcję. Odpowiedzi z systemu liczone są zazwyczaj w setkach milisekund. To pozwala między innymi na skuteczne zablokowanie podejrzanej transakcji. Przy dużej skali zagrożeń oszustwami ważne jest wiarygodne uwierzytelnienie i szybka reakcja. Tu sprawdzają się rozwiązania w pełni zautomatyzowane, bo one mogą zadziałać szybko. Człowiek spowalniałby taki system. Konkretne scenariusze zastosowań i wdrożeń będą jednak zależne od potrzeb oraz oczekiwań poszczególnych partnerów i ich użytkowników końcowych.

ADVANCED THREAT SUMMIT 2018

Ekspert i maszyna: praca w duecie poprawia wyniki

Analiza ruchu sieciowego zapewnia doskonałe wyniki w zakresie jak najlepszego pokrycia potencjalnej powierzchni ataku. Jej wykonanie stanowi jednak spore wyzwanie, ponieważ danych jest bardzo dużo, ciągle się zmieniają i dotyczą wielu różnych urządzeń. Rozwiązanie pozwalające analizować ruch w zautomatyzowany sposób skraca czas pracy eksperta od cyberbezpieczeństwa z tygodni do minut. Rozmowa z **Alexem Vaystikhem**, CTO i współzałożycielem firmy SecBI.

Czym zajmuje się SecBI?

Automatyzujemy jedno z największych wyzwań w Security Operations Center, czyli manualny proces dochodzeniowy realizowany przez ekspertów odpowiedzialnych za bezpieczeństwo. Muszą oni mierzyć się z ogromną ilością danych. Każdego dnia w organizacji może pojawiać się od 100 mln do nawet 1 mld nowych zdarzeń, a żeby wykryć atak, trzeba sprawdzić informacje dotyczące nie tylko jednego dnia, ale np. całego roku.

Opracowujemy algorytmy machine learning, które robią to całkowicie automatycznie. Dzięki temu analitycy mogą skupić się na podejmowaniu decyzji, a nie na rozwijaniu swoich umiejętności w obsłudze technologii Big Data czy uczenia maszynowego. W końcu zatrudniamy analityków ds. bezpieczeństwa właśnie po to, żeby analizowali zagadnienia związane z bezpieczeństwem, a nie zajmowali się innymi kwestiami.

W obszarze interakcji użytkownika z komputerem (Human Computer Interaction – HCI) mamy do dyspozycji dużo danych pochodzących z wielu różnych źródeł. To pozwala tworzyć profile zachowań dla każdego użytkownika komputera.

Jakie typy uczenia maszynowego wykorzystujecie?

Wykorzystujemy dwa typy uczenia maszynowego. Przede wszystkim uczenie nienadzorowane, które umożliwia wdrożenie w organizacji działającego, zapewniającego natychmiastowy efekt rozwiązania, bez konieczności jego wcześniejszego

Wykorzystujemy dwa typy uczenia maszynowego. Przede wszystkim uczenie nienadzorowane, które umożliwia wdrożenie w organizacji działającego, zapewniającego natychmiastowy efekt rozwiązania, bez konieczności jego wcześniejszego treningu.

treningu. Podobnie jak w przypadku autonomicznego samochodu: wsiadamy do niego i od razu jedziemy.

Tymczasem większość dostępnych obecnie na rynku rozwiązań z zakresu cyberbezpieczeństwa zanim zacznie działać, potrzebuje czasu na rozpoznanie sieci. Trzeba poczekać 30 dni, zanim będzie można z niego skorzystać. To złe podejście, bo jeśli intruz jest już w organizacji, niczego nowego się nie dowiemy. Jeśli włamywacz będzie powoli uczył system, przechytrzy maszynę. Dzisiaj nikt już nie chce czekać 30 dni, bo wtedy dowiaduje się rzeczy, o których wiedział już wcześniej.

Wykorzystując nienadzorowane uczenie maszynowe, kodujemy „fizykę" danych, czyli to, co w ogóle jest możliwe. Dzięki temu możemy natychmiast wykrywać rzeczy, które naruszają tę fizykę. W wyniku analizy na pierwszym, nienadzorowanym etapie powstają klastry, które składają poszczególne elementy układanki w całość. Otrzymujemy znacznie bardziej przejrzysty obraz, niż gdybyśmy patrzyli na pojedyncze logi. O wiele lepszy jest stosunek sygnału do szumu. To ważne, ponieważ w drugim etapie działania, wykorzystując uczenie nienadzorowane i częściowo nadzorowane, łącząc te dwa podejścia, jesteśmy w stanie z dużą dokładnością wykrywać zagrożenia.

Czy wymaga to zastosowania specjalnego sprzętu?

Nie, w związku z tym, że nasze rozwiązanie jest programowe, udaje się je uruchomić w chmurze. Właściwie może działać w stu procentach w chmurze.

W nazwie firmy pojawia się Business Intelligence. Czy celowo nie mówicie o AI, sztucznej inteligencji?

Używamy skrótu AI, ale mówimy raczej o Autonomous Investigation, a nie o Artificial Intelligence. Sztuczna inteligencja to bardzo szerokie pojęcie. Wybraliśmy BI, ponieważ historycznie systemy Business Intelligence, zostały przygotowane po to, żeby pomagać ludziom podejmować lepsze decyzje. To systemy eksperckie, których użycie pozwala podnosić skuteczność działania. Wiele firm odniosło dzięki nim istotne korzyści. Zwiększały swoją wydajność, poprawiały konkurencyjność w obszarze marketingu czy sprzedaży, ale

– przynajmniej dotychczas – nie w obszarze bezpieczeństwa. Wybraliśmy nazwę SecBI, ponieważ uważamy, że w bezpieczeństwie brakuje wykorzystania możliwości oferowanych przez BI.

Czy to oznacza, że uważacie, że AI jest nieprzydatna w obszarze bezpieczeństwa? A może dlatego, że sztuczna inteligencja nie jest jeszcze dostatecznie dojrzała?

Na pewnym poziomie zaawansowania można przyjąć, że uczenie maszynowe to forma sztucznej inteligencji. Zatem można powiedzieć, że stosujemy AI. Kluczowym założeniem naszej działalności jest to, że naśladujemy w tworzonych systemach działanie ludzkiego eksperta. To oznacza jednocześnie, że nasze rozwiązanie, łączące różne algorytmy, jest formą sztucznej inteligencji.

Jak skuteczny w tym naśladowaniu ludzkiego eksperta jest system SecBI?

Na pewno w przypadku niektórych zadań jest o wiele lepszy od człowieka. Trzeba jednak zaznaczyć, że naszym celem nie jest zastąpienie człowieka. Próbujemy automatyzować rzeczy, na które analityk bezpieczeństwa nie powinien marnować czasu. Tymczasem dzisiaj wielu z tych ekspertów poświęca bardzo dużo czasu na naukę nowego języka programowania, żeby móc analizować informacje zawarte w wielkich zbiorach danych. Sporo czasu zabiera im też samo oczekiwanie na wyniki. Nieraz po prostu toną w danych, a potrzebują tylko jednego elementu układanki, żeby podjąć decyzję.

My automatyzujemy proces pozyskiwania tych elementów układanki, który obecnie zajmuje 80–90% czasu pracy analityka. Proces realizowany jest z szybkością, z jaką działają komputery. Dzięki temu ekspert zamiast prowadzić jedno dochodzenie przez tydzień, może ich wykonać np. dziesięć dziennie.

Wybraliśmy nazwę SecBI, ponieważ uważamy, że w obszarze bezpieczeństwa brakuje wykorzystania możliwości oferowanych przez Business Intelligence.

Taka jest geneza powstania SecBI. Widzieliśmy, jak długo ten proces zajmuje. Zaczęliśmy zadawać sobie pytanie: czy możemy go zautomatyzować? Bo jeśli zrozumienie tego, co się stało, zajmuje nam kilka tygodni po tym, jak do tego doszło, to nie jesteśmy w stanie temu przeciwdziałać. Jeśli jednak zajętoby 5 minut czy 5 sekund, być może będziemy mogli odpowiednio zareagować i zapobiec zagrożeniu.

Czy w ten sam sposób rozumują również przestępcy? Czy oni także myślą o automatyzacji?

Tak, widzimy, że atakujący używają do realizacji rozmaitych celów coraz bardziej zaawansowanego uczenia maszynowego. Przykładem są zautomatyzowane, ukierunkowane ataki phishingowe, które dostosowują się do preferencji i charakterystyki atakowanych osób. Przykładowo, dane, które wyciekły po niedawnym ataku na Facebook, teraz mogą być wykorzystane do kolejnych, bardziej precyzyjnych ataków. To automatyzacja typu social engineering.

Inny kierunek to automatyzacja rozwoju technik ataku. Wyszukiwanie luk w zabezpieczeniach, które mogą być wykorzystane, jest bardzo czasochłonne. Coraz więcej zaawansowanych technologii, takich jak rozmyte sieci neuronowe, pozwala na automatyczne szukanie podatności, generowanie kodu i natychmiastowe uruchamianie wyrafinowanego ataku, który jest praktycznie nie do wykrycia. To następna fala tego, co było robione już od wielu lat w obszarze rozwoju złośliwego oprogramowania. W zasadzie jest to rozszerzenie polimorfizmu, który od lat pozwala omijać zabezpieczenia antywirusowe. Teraz dzięki automatyzacji możliwe stało się obchodzenie zaawansowanych systemów wykrywania włamań.

> Wykorzystujemy przede wszystkim uczenie nienadzorowane, które umożliwia wdrożenie w organizacji działającego, zapewniającego natychmiastowy efekt rozwiązania, bez konieczności jego wcześniejszego treningu. Nie trzeba czekać 30 dni na rozpoznanie sieci.

ADVANCED THREAT SUMMIT 2018

Cyberbezpieczeństwo w centrum zainteresowania prawa

Przyjęcie ustawy o krajowym systemie cyberbezpieczeństwa (KSC) to początek procesu podnoszenia poziomu cyberbezpieczeństwa w administracji i gospodarce naszego kraju. Dysponujemy systemem, który umożliwia sprawne działanie na rzecz wykrywania cyberataków, zapobiegania im i minimalizowania ich skutków. Ma on być konsekwentnie rozwijany. O tym, co wynika z ustawy i związanych z nią rozporządzeń, a także o tym, jak zmaksymalizować korzyści z tej regulacji dla cyberbezpieczeństwa, rozmawiano podczas spotkania CSO Council oraz podczas konferencji „Advanced Threat Summit 2018".

„Zgłaszanie incydentów to pierwszy krok. Uruchamiane są kolejne inicjatywy związane z funkcjonowaniem ustawy. Pracujemy nad przygotowaniem minimalnych standardów bezpieczeństwa, prowadzimy prace w obszarze badań i certyfikacji produktów, a także działamy na rzecz zbudowania europejskiego centrum kompetencyjnego w zakresie cyberbezpieczeństwa" – wyliczał Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji podczas spotkania CSO Council.

Ustawa o krajowym systemie cyberbezpieczeństwa weszła w życie w sierpniu br. To pierwsza kompleksowa regulacja poświęcona cyberbezpieczeństwu w Polsce, dotycząca obsługi incydentów zarówno w sektorze publicznym, jak i prywatnym. Celem stworzonego na jej podstawie systemu jest umożliwienie sprawnego działania na rzecz wykrywania cyberataków, zapobiegania im oraz minimalizowania ich skutków. Ma on przede wszystkim dawać ramy i możliwości dla współpracy, zwłaszcza międzysektorowej.

Bezpośrednim impulsem do uregulowania kwestii związanych z cyberbezpieczeństwem była dyrektywa NIS, ale pewne działania w tym obszarze były podejmowane już od chwili wstąpienia Polski do NATO. Dla organizacji, które wdrożyły ISO 27001, wymagania wynikające z ustawy o KSC nie są niczym nowym. Ustawa nie wprowadza

Pracujemy nad przygotowaniem minimalnych standardów bezpieczeństwa, prowadzimy prace w obszarze badań i certyfikacji produktów, działamy na rzecz zbudowania europejskiego centrum kompetencyjnego w zakresie cyberbezpieczeństwa.

ROBERT KOŚLA, DYREKTOR DEPARTAMENTU CYBERBEZPIECZEŃSTWA, MINISTERSTWO CYFRYZACJI

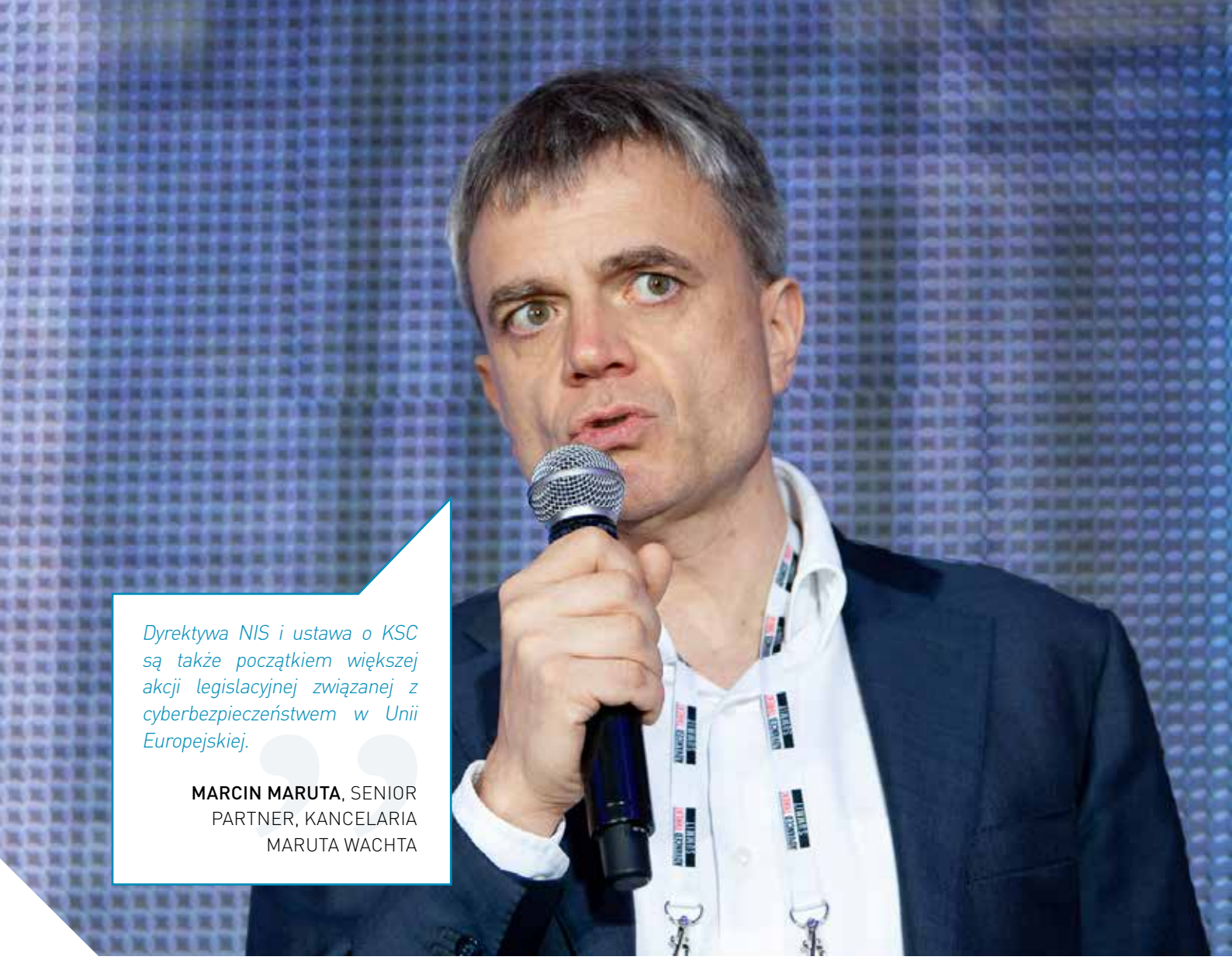
kolejnych wymagań, pozycjonuje tylko pewne standardy funkcjonujące w sektorze prywatnym. Wynikające z niej regulacje mogą być jednak nowością dla niektórych branż albo administracji publicznej.

„Po roku funkcjonowanie ustawy zostanie poddane ocenie. W związku z tym najprawdopodobniej przygotowana zostanie nowelizacja, ponieważ system ma być '*żywy*', odpowiadać zmieniającej się dynamicznie sytuacji" – zapowiedział Robert Kośla.

Operatorzy i CSIRT-y

Obecnie na liście operatorów usług kluczowych (OUK) znajduje się blisko 800 podmiotów. Kim jest OUK? Jest on identyfikowany na podstawie przynależności do jednego z sektorów, podsektorów i rodzajów podmiotów wymienionych w załączniku do ustawy. Jednocześnie świadczy usługę znajdującą się w wykazie usług kluczowych, której świadczenie zależy od systemów informacyjnych, a wystąpienie incydentu miałoby istotny skutek zakłócający świadczenie usługi kluczowej.

Określenie istotnego skutku zakłócającego powiązane jest: z liczbą użytkowników zależnych od świadczonej usługi, zależnością innych sektorów, z wpływem, jaki incydent może mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne. Dodatkowo



Dyrektywa NIS i ustawa o KSC są także początkiem większej akcji legislacyjnej związanej z cyberbezpieczeństwem w Unii Europejskiej.

MARCIN MARUTA, SENIOR PARTNER, KANCELARIA MARUTA WACHTA

brane są pod uwagę: udział podmiotu świadczącego usługę kluczową w rynku, zasięg geograficzny związany z obszarem, którego może dotyczyć incydent, oraz znaczenie podmiotu dla utrzymywania wystarczającego poziomu świadczenia usługi przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia.

„Będziemy jednak iść dalej. Planujemy mapowanie tego zagadnienia na wzajemne relacje pomiędzy operatorami, ponieważ atak na jednego z operatorów usług kluczowych może kaskadowo powodować skutki u innych operatorów" – mówił Robert Kośla.

Sam sposób wyznaczania operatora usługi kluczowej jest transparentny i uwzględnia procedurę odwoławczą. Organ właściwy bada rynek, szukając potencjalnych operatorów usług kluczowych. Następnie uruchamiane jest postępowanie administracyjne i zbierane są informacje o podmiocie. Sprawdza się, czy podmiot spełnia wymogi z rozporządzenia, a następnie wskazuje OUK decyzją administracyjną. Wybrany operator ma w kolejnych terminach – 3, 6 i 12 miesięcy – dostosować się do wymogów ustawy, a następnie realizować wynikające z niej obowiązki.

Jednym z ważniejszych wyzwań związanych z ustawą o KSC było

Firmy muszą zacząć postrzegać bezpieczeństwo jako część działalności gospodarczej. Potrzebna jest przy tym nie tylko zmiana sposobu myślenia, ale i działania zmierzające do edukacji kadr. Z tym jest problem.

PIOTR SKIBIŃSKI, DYREKTOR BIURA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO, POLKOMTEL

stworzenie CSIRT-u poziomu krajowego (Computer Security Incident Response Team). W wyniku długich dyskusji udało się uzyskać kompromis odnoszący się do kompetencji i właściwości poszczególnych podmiotów. W ten sposób powstały trzy zespoły tworzące CSIRT poziomu krajowego. Są to: odpowiedzialny za sferę wojskową CSIRT MON; CSIRT GOV, bazujący na strukturze CERT.gov, zbierający informacje o incydentach w administracji rządowej i sektorach kluczowych, jak również o zdarzeniach terrorystycznych w cyberprzestrzeni, oraz umieszczony w strukturze NASK CERT.pl, który zbiera informacje z pozostałych jednostek – samorządu terytorialnego, a także podmiotów, jakie nie zostały zakwalifikowane jako OUK.

Jest ustawa, ale to nie koniec

Co dalej? Dzisiaj problemem jest brak minimalnych, nadążających za rozwojem technologii standardów bezpieczeństwa dla administracji – takich, jakie obowiązują w innych państwach. W Polsce ich nie ma. Można natomiast wykorzystać standardy bezpieczeństwa fizycznego i informatycznego opracowane przez Rządowe Centrum

Bezpieczeństwa (RCB) we współpracy z Agencją Bezpieczeństwa Wewnętrznego (ABW) i Policją dla operatorów infrastruktury krytycznej.

W Ministerstwie Cyfryzacji prowadzone są prace nad metodologią zarządzania ryzykiem, która ułatwi interpretację wymagań technicznych zapisanych w rozporządzeniach. Pozyskano finansowanie na tego typu projekt i został on uruchomiony. Przygotowywane są także bazy wiedzy z wykładnią wszystkich odpowiednich organów. Dlatego – jak podkreślał Robert Kośla – wszystkie podmioty mające pytania dotyczące KSC proszone są o przesyłanie ich do Ministerstwa Cyfryzacji.

Poza tym trwają prace nad programami szkoleniowymi. Wspólnie z Naukową i Akademicką Siecią Komputerową (NASK) Ministerstwo Cyfryzacji przygotowuje szkolenia internetowe dla samorządu terytorialnego. NASK jest zaangażowany także w działania sektorowe. „Będziemy spotykać się z przedstawicielami sektorów i pracować nad regulacjami, które później przyjmą organy właściwe. Realizujemy to w ramach programu 'Partnerstwo dla cyberbezpieczeństwa" – mówił Juliusz Brzostek, dyrektor Narodowego Centrum Cyberbezpieczeństwa w NASK.

Warto pamiętać, że dyrektywa NIS i ustawa o KSC są także początkiem większej akcji legislacyjnej związanej z cyberbezpieczeństwem

Samo wypełnienie wymogów ustawowych nie wystarczy. Trzeba odpowiednio przygotować się do ogólnych wyzwań związanych z cyberbezpieczeństwem.

MICHAŁ OSTROWSKI,
REGIONAL DIRECTOR EASTERN EUROPE, FIREEYE

w Unii Europejskiej. Mówili o tym w swoim wystąpieniu mecenas Marcin Maruta i mecenas Marcin Serafin z Kancelarii Maruta Wachta. W pierwszej kolejności w 2019 r. ma pojawić się Cybersecurity Act, który będzie regulować schematy cyberbezpieczeństwa oraz europejskie i krajowe schematy certyfikacji. W kolejnych latach mają zostać zakończone prace nad regulacją dotyczącą European Competence Network, czyli siecią agencji krajowych finansowanych z budżetu europejskiego. Zajmie się ona uspójnianiem europejskiego systemu cyberbezpieczenstwa.

Dobry początek, trzeba działać dalej

Ustawa o KSC, choć niesie ze sobą spore wyzwania, spotkała się z dobrym przyjęciem w środowisku menedżerów i ekspertów odpowiedzialnych za cyberbezpieczeństwo. Wszyscy mają jednak świadomość, że to dopiero początek drogi i potrzebne są dalsze działania.

„Ustawa o KSC jest bardzo potrzebna. Uwzględnia to, że jako społeczeństwo jesteśmy narażeni na ataki. Niewiele jednak pomoże, jeśli nie będzie postępowała zmiana w postrzeganiu bezpieczeństwa przez zarządy firm. Organizacje muszą zacząć postrzegać bezpieczeństwo jako cześć działalności gospodarczej. Potrzebna jest przy tym zmiana nie tylko sposobu myślenia, ale i działania zmierzające do edukacji nowych kadr. Z tym jest ogromny problem. Sama ustawa, jeśli nie będzie poparta działaniami w obszarze edukacji, niewiele przyniesie" – mówił w trakcie dyskusji panelowej Piotr Skibiński, dyrektor Biura Bezpieczeństwa Teleinformatycznego w Polkomtelu.

Uczestnicy panelu zwracali też uwagę na inne aspekty systemowe. „Przykłady takie jak Wanna Cry czy Not Petya pokazują, że kluczowe znaczenie ma szybkość wymiany informacji. Samo informowanie nie rozwiązuje jednak problemu. Ważne, jak szybko będziemy w stanie zareagować. Dlatego informacja powinna być wymieniana w sieci, która jest w stanie sama reagować w przypadku wystąpienia incydentów. To pozwoli zminimalizować straty" – oceniał Piotr Kalbarczyk, dyrektor Departamentu Cyberbezpieczeństwa w PKO Bank Polski.

Wreszcie przedstawiciele branży cybersecurity mówili o konieczności odpowiedniego przygotowania się do ogólnych wyzwań związanych z cyberbezpieczeństwem. Samo wypełnienie wymogów ustawowych nie wystarczy. „Ustawa mówi o zgłoszeniu incydentu w ciągu 24 godzin. Jeśli jednak odkrywamy incydent dziś i zgłaszamy go w ciągu 24 godzin, ale tak naprawdę wystąpił on kilka miesięcy wcześniej, a firma nie dysponuje narzędziami, żeby to wyłapać, to nie ma tak naprawdę znaczenia, czy zgłoszenie zostanie dokonane w ciągu doby" – przestrzegał Michał Ostrowski, Regional Director Eastern Europe w FireEye. Firmy muszą więc myśleć o budowaniu struktur bezpieczeństwa w szerokim kontekście.

ADVANCED THREAT SUMMIT 2018

Trudna sztuka rozmowy

Osoba odpowiedzialna za bezpieczeństwo w firmie powinna nie tylko znać się na najnowszych technologiach. Musi również umieć pozyskiwać informacje od innych. Może się to przydać w razie konieczności ustalenia faktycznych przyczyn incydentu. Skutecznie przeprowadzona rozmowa pozwoli uzyskać odpowiedź na pytanie, na ile faktycznie zawinił system, a na ile zaistniałe wydarzenie było efektem błędu człowieka.

O sposobach docierania do informacji posiadanych przez inne osoby mówił podczas konferencji Wiesław Zyskowski, właściciel firmy „Zyskowski Szkolenia Doradztwo Consulting". W trakcie prowadzonego przez siebie warsztatu pt. „Trudne rozmowy z użytkownikami (i nie tylko), czyli jak uzyskać maksimum potrzebnych informacji drogą rozmowy i obserwacji – przesłuchania metodą FBI" przedstawił szereg rad dotyczących sposobów prowadzenia rozmów skutkujących pozyskaniem niezbędnych informacji.

Umiejętność zadawania pytań

Rozmowa to sztuka zdobywania informacji. Chodzi o to, aby poznać faktyczny stan rzeczy, a nie potwierdzić założoną wcześniej własną tezę. Ważna jest umiejętność słuchania oraz umiejętność zadawania pytań. Nie jest łatwo zadawać pytania. Dlatego trzeba się do tego dobrze przygotować. Warto m.in. przed rozmową pozyskać jak najwięcej informacji o rozmówcy.

Różnice w nastawieniu rozmówcy

Osoba szczera ma informację i chce się nią podzielić. To nie znaczy, że mówi prawdę (bo np. część faktów zapomniała, bo inaczej niż my rozumie pewne pojęcia). Osoba nieszczera ma informację, ale nie zamierza się nią podzielić, bo np. popełniła błąd, do którego nie chce się przyznać („nie naruszyłem bezpieczeństwa, to nie moja wina, to system ma złe algorytmy").

Wprowadzenie w temat

Podczas rozmowy poziom stresu jest wysoki. Mamy prawo nie pamiętać wszystkiego. Trzeba więc najpierw uaktywnić pamięć rozmówcy (przesłuchanie kognitywne). Należy zacząć od pytań o kontekst, a nie od razu pytać o szczegóły czy meritum sprawy.

Metoda na raka

Kłamcy kontrolują swoje wypowiedzi. Często jednak nieświadomie coś zdradzą, np. pomylą się w relacjonowaniu wydarzeń. Metoda na raka jest wtedy skuteczna, żeby sprawdzić, czy nie oszukują.

Trzeba poprosić, żeby opowiedzieli całą historię od końca. Zazwyczaj, jeśli ktoś kłamie, nie jest w stanie zachować chronologii wydarzeń w opowiadaniu od tyłu.

Mowa ciała

Kłamstwo widać też w zachowaniach rozmówcy. Trzeba tylko odpowiednio każdą osobę „skalibrować", określić dla każdego odpowiednią miarę zachowania. Nie warto tutaj ufać podręcznikom. Na przykład splecione ramiona nie zawsze muszą oznaczać zamknięcie się w sobie. Może się zdarzyć, że akurat komuś jest tak po prostu wygodnie siedzieć. Poza tym każdy mówi inną częścią ciała. I u każdego to samo, np. marszczenie brwi, może znaczyć całkiem co innego. Ten, kto prowadzi rozmowę, musi być pewien, że już odpowiednio „skalibrował" swojego rozmówcę. Dlatego trzeba dużo czasu poświęcić na rozmowę wprowadzającą.

Każdy reaguje inaczej

Człowiek jest jak system, pewne jego zachowania są do przewidzenia. Wiele można wyczytać z uścisku dłoni i sposobu witania się – to, co w głowie, to i w dłoni. Trzeba jednak pamiętać, że każdy z nas inaczej reaguje na różne sytuacje podczas rozmowy. Należy więc dla każdego ustalić indywidualne normy zachowania. Powinno się przy tym uwzględnić, że są pewne stałe normy, np. niektórzy wykonują ustalone, wyuczone gesty w celu oddziaływania na innych.

Metody obrony

Przesłuchiwani stosują podobne metody obrony. Najpierw jest zaprzeczenie, zdejmowanie winy z siebie („nie ukradłem, pożyczyłem sobie tylko"). Inny sposób to przekierowanie („przecież inni też wyłączali zabezpieczenia na swoich komputerach"). Zawsze łatwiej jest się przyznać w rozmowie z jedną osobą niż z kilkoma.

Rozmowa to sztuka zdobywania informacji. Chodzi o to, aby poznać faktyczny stan rzeczy, a nie potwierdzić założoną wcześniej własną tezę. Ważna jest umiejętność słuchania oraz umiejętność zadawania pytań.

WIESŁAW ZYSKOWSKI,
WŁAŚCICIEL FIRMY
„ZYSKOWSKI SZKOLENIA
DORADZTWO CONSULTING"

Decyduje punkt widzenia

Zazwyczaj jesteśmy skłonni oceniać innych. Chętnie wydajemy opinie, co należałoby zrobić, chociaż sami nigdy nie byliśmy w takiej sytuacji („najlepiej by go było od razu zwolnić"). Gdy się znajdziemy, to często też zmieniamy swoją opinię („pewnie się pomylił, trzeba mu dać drugą szansę").

Od ogółu do szczegółu

Umawiając się na rozmowę mającą za cel uzyskanie potrzebnych informacji, nie należy od razu wyłuszczać, o czym chcemy rozmawiać. Trzeba na początku raczej zakreślić temat rozmowy bardziej ogólnie („zdarzył się incydent, chcemy porozmawiać ze wszystkimi, którzy korzystali z tej aplikacji").

AT SUMMIT

PODSUMOWANIE SESJI ROUNDTABLES

ADVANCED THREAT SUMMIT 2018

RUNDA 1

Stolik nr 1

Pełna wizualizacja stanu podatności i konfiguracji w czasie rzeczywistym. Czy i kiedy tego potrzebujemy? Czy można to osiągnąć? Jeśli tak, to jakim nakładem?

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

Uczestnicy dyskusji byli zainteresowani w szczególności kwestią dostępności pełnej wizualizacji stanu bezpieczeństwa kluczowych zasobów i ich komponentów, oprogramowania oraz aplikacji w czasie rzeczywistym. W trakcie rozmowy wyjaśnione zostały główne zagadnienia związane ze sposobami pobierania i przetwarzania danych oraz przedstawione istotne korzyści z tego płynące. Dostępne są odpowiednie narzędzia, jednak to za mało. Konieczne jest ich włączenie w procesy. Trzeba dostarczyć do nich odpowiednio przygotowane dane, które następnie po przetworzeniu będzie można przekazać właściwym adresatom. Dzięki temu będziemy dysponować argumentami dla zarządu, a w efekcie możliwe stanie się minimalizowanie ryzyk, co czasem wymaga kosztów wyższych, niż początkowo zakładano.

Stolik nr 3

Systemy zarządzania podatnościami, czyli jak daleko nam do ideału i co z tym zrobić.

Prowadzący:
Sebastian Mazurczyk, Senior System Engineer, Veracomp

Dyskusja skoncentrowała się wokół tego, co jest ważne dla posiadaczy systemów do zarządzania podatnościami. W szczególności dotyczyła ich rozbudowy, automatyzacji oraz integracji z innymi systemami. Uczestnicy pytali w pierwszej kolejności o możliwość integracji z systemami ticketowania. Podstawowym warunkiem takich działań jest otwarte API. Zdaniem uczestników pożądane jest filtrowanie ticketów. Dzięki temu osoby odpowiedzialne za instalowanie łatek nie zostaną przytłoczone nawałem pracy. W przypadku systemów automatyki najlepszym rozwiązaniem są skanery pasywne. Dyskusja dotyczyła także kwestii łączenia systemów. Optymalne wydaje się łączenie z zachowaniem separacji w taki sposób, żeby użytkownicy mieli dostęp albo do jednych, albo do drugich danych. Istotna jest także integracja z systemami GRC oraz SIEM.

Stolik nr 4

Integracja różnych systemów bezpieczeństwa

Prowadzący:
Piotr Głaska, Senior Systems Engineer, Infoblox

Dyskusja rozpoczęła się od postawienia dodatkowego pytania: czy lepsze są systemy bezpieczeństwa homogeniczne czy heterogeniczne? Uczestnicy zgodzili się, że nie ma dziś możliwości obsłużenia wszystkich potrzeb w tym obszarze za pomocą jednego systemu. Dlatego jesteśmy skazani na integrację różnych systemów bezpieczeństwa, nie ma tutaj alternatywy. Znaczna część dyskusji poświęcona była powiązanemu zagadnieniu: automatyzacji. Nikt dziś nie wierzy, że uda się wszystko w pełni zautomatyzować w taki sposób, żeby system zastępował użytkownika. Wynika to przede wszystkim z braku zaufania. Integracja z automatyzacją ma jednak dostarczyć wsparcia dla „systemów białkowych". Kto powinien dokonywać integracji? Uczestnicy zgodzili się, że organizacja decyduje, co robimy, a integrator jest „narzędziem" wspierającym i wykonuje zlecone zadania.

Stolik nr 6

Jak zapewnić maksymalną wydajność użytkownikom przy jednoczesnym utrzymaniu pełnej kontroli przez działy IT?

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

Wolność z kontrolą można pogodzić. Jednym z warunków zachowania równowagi między maksymalną wydajnością użytkowników a utrzymaniem pełnej kontroli przez działy IT jest ciągła edukacja użytkowników mająca na celu zwiększanie świadomości zagrożeń. Szczególną grupą, grupą wysokiego ryzyka, którą należy wziąć pod uwagę w tym kontekście, jest top management. Dział IT potrzebuje pełnej kontroli nad dostępem do firmowych zasobów i jednocześnie musi zarządzać kontami uprzywilejowanymi. Do tego niezbędna jest dobrze zaplanowana i zrealizowana segmentacja infrastruktury. Przy tym konieczne jest świadome planowanie działania zespołu IT. Niektórzy uczestnicy dyskusji zwracali uwagę, że bez zachowania rozsądku może to jednak prowadzić do mającego negatywne skutki ograniczania swobody biznesu.

Stolik nr 7

Next generation threat management

Prowadzący:
Arkadii Kosoburov, Security MSS Threat Monitoring – Global manager, IBM

Jakie potrzeby ma biznes w kontekście zarządzania zagrożeniami? W pierwszej kolejności uczestnicy wskazywali na: domyślną zgodność, budowanie zaufania oraz zwinność. Ze względu na te wymagania kluczowymi wyzwaniami stojącymi przed obsługą IT oraz zarządzaniem zagrożeniami są problemy związane z pozyskaniem specjalistów oraz brak zarządzania ryzykiem w środowisku IT. Rozwiązania nowej generacji do zarządzania zagrożeniami powinny być przede wszystkim domyślnie zgodne z podstawowymi standardami w obszarze bezpieczeństwa. Wykorzystywane narzędzie najprawdopodobniej powinno być chmurowe, ze względu na to, że będzie w stanie zapewnić większą elastyczność działania. Kolejne wyzwanie to wysoki poziom automatyzacji potrzebny przy analizowaniu wielkich zbiorów danych oraz wykorzystanie sztucznej inteligencji, żeby ułatwiać i przyspieszać pracę, a także lepiej wypełniać wymagania biznesowe.

Stolik nr 9

Threat hunting – buzzword czy integralna część cyber security operations?

Prowadzący:
Dariusz Jurewicz, Cybersecurity Operations Manager, HSBC Service Delivery (Polska),

Przemysław Skowron, Threat Hunter, HSBC Service Delivery (Polska)

Threat hunting nie jest nowością: polowania były prowadzone już wcześniej, są prowadzone dzisiaj i nadal będą prowadzone. Czasem polowanie – ze względu na ostateczny cel – mylone jest z wykrywaniem. W obu przypadkach chodzi bowiem o to samo, czyli jak najwcześniejsze wykrycie zagrożeń. Choć threat hunting nie jest jeszcze mocno osadzony w realiach norm bezpieczeństwa ISO, to nie powód, żeby zaniechać tego typu działania. Zwłaszcza że polowanie nie musi być od razu procesem. Wystarczy zacząć od krótkich, kilkudniowych sprintów, żeby czerpać korzyści. Threat hunting może być też dobrą metodą poznawania organizacji przez nowych pracowników, także tych z małym doświadczeniem. Przeszukiwanie infrastruktury pod kątem wskaźników kompromitacji to

wykrywanie, a nie polowanie. Nie warto tracić na to energii łowców. Trzeba natomiast pamiętać, że efektywne polowania wymagają dostarczania łowcom szczegółowej wiedzy o tym, jak działają wrogowie. Threat hunting to oczywiście nie panaceum na wszystkie problemy, ale trudno uznać, że jest to argument przemawiający za zaprzestaniem polowań.

Stolik nr 10

Zarządzanie bezpieczeństwem danych w chmurze i ograniczenie znaczenia ataków pochodzących z wewnątrz organizacji

Prowadząca:

Jolanta Malak, regionalna dyrektor sprzedaży Polska, Białoruś i Ukraina, Fortinet

Nawet 30% wycieków danych z firmy jest związanych z pracownikami lub kontraktorami. Jakie wnioski z tego płyną? Najważniejszą sprawą jest to, żeby widzieć, co się dzieje w sieci. Jeśli widzimy kto, co, gdzie robi z danymi i jak z nimi pracuje w naszej organizacji. Wtedy możemy powiedzieć, że mamy system bezpieczeństwa. Powinien on w taki sam sposób działać zarówno w naszej sieci, centrum danych, jak i w chmurze. Nie można godzić się na kompromisy w tym względzie. Wszędzie powinna obowiązywać taka sama polityka bezpieczeństwa. Przy tym niezwykle ważna jest kwestia zaufania. Nawet jeśli ufamy dostawcy chmurowemu, nie wolno zapominać o jego kontrolowaniu, to jest konieczne. Klienci podpisują bowiem pewne zobowiązania wobec dostawców usług, natomiast dostawcy niekoniecznie już zapewniają zgodność z politykami bezpieczeństwa klientów. To na klientach spoczywa odpowiedzialność, żeby wchodzić ze swoimi politykami do infrastruktury dostawców, żeby kontrolować, co pracownicy i kontrahenci robią z danymi w chmurze.

RUNDA 2

Stolik nr 1

Konkretny produkt, rozbudowany system, a może zewnętrzna usługa? Czego tak naprawdę potrzebujemy?

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

Dyskusja koncertowała się wokół zagadnienia niewielkiego apetytu klientów na usługi typu managed security. Dlaczego niechętnie z nich korzystają? Wielu z nich nie decyduje się na to, nawet jeśli analiza ryzyka wypada pomyślnie. Są bowiem przekonani, że dadzą sobie radę samodzielnie. Uznają, że nie ma sensu przeznaczać środków finansowych na zewnętrzne usługi, jeśli za takie same kwoty można kupić własne narzędzia i utrzymać zespół. To dominujące wciąż podejście. Ostatecznie zwykle okazuje się jednak, że niemożliwością jest skompletowanie potrzebnego zespołu. Brakuje czasu i kompetencji, żeby wdrażać najnowsze rozwiązania. Dopiero gdy dochodzi do poważnego incydentu (można powiedzieć, że klient nauczył się na własnych błędach), wtedy zazwyczaj pojawia się decyzja o wykorzystaniu zewnętrznych usług. Dzisiaj wydaje się pewne, że cały rynek – zarówno globalny, jak i w Polsce – zmierza w tym kierunku: klienci są coraz częściej zainteresowani zewnętrzną pomocą.

Stolik nr 4

Jak się komunikować, aby skutecznie dotrzeć do nietechnicznych odbiorców i ich zaangażować?

Prowadzący:
Piotr Pobereźny, Regional Account & Channel Manager, North CEE, Qualys

Wszyscy doskonale wiemy, że to człowiek jest najsłabszym czynnikiem w całym systemie cyberbezpieczeństwa. Jak zatem dotrzeć do odbiorców, jak ich zaangażować i utrzymać ich uwagę? Każda grupa odbiorców wymaga innego, indywidualnego podejścia, każda ma bowiem inne motywacje. Cały czas trzeba poszukiwać tzw. sweet spot – podejścia, które będzie motywować daną osobę. Dla członków zarządu może być to premia, dla innych regulacja KNF. Poszukiwanie indywidualnego „punktu zaczepienia" jest kluczowe. Rozmowa na temat ryzyk cyberbezpieczeństwa, włączanie ich w proces zarządzania ryzykiem organizacji stanowi klucz do sukcesu.

Stolik nr 5

Jak przygotować się na wyzwania bezpieczeństwa w dobie inteligentnych technologii wykorzystujących mechanizmy IoT, Artificial Intelligence i Machine Learning?

Prowadzący:
Paweł Łakomski, Technology Solution Professional, Microsoft;

Przemysław Zębik, doradca technologiczny, Microsoft

Dyskusja rozpoczęła się od przyjrzenia się nowym wektorom i nowym metodom ataków, które wprawdzie istniały już od kilku lat, ale nie były oczywiste czy powszechne. Przykładem są ataki na IoT czy łańcuchy dostaw. Uczestnicy zastanawiali się, jak się przed nimi zabezpieczyć. Doszli do wniosku, że stare metody zaczynają się dezaktualizować. Istnieje duża potrzeba wykorzystania nowych rozwiązań. W trakcie rozmowy udało się nieco odczarować uczenie maszynowe. Ta technologia wymaga długiego trenowania i dużej liczby próbek. W przeciwnym wypadku trzeba się liczyć z ogromną ilością alertów fałszywie pozytywnych. Przy tym jeśli już decydujemy się trening, to trzeba podjąć decyzję, na jakiej próbie i na jakim obszarze. Czasem warto zawęzić obszar i chronić tylko krytyczne zasoby, a nie próbować objąć wszystkiego od razu. Nie należy jednak rezygnować z tradycyjnych metod: biorąc pod uwagę, że źródłem większości ataków jest phishing, to użytkownicy nadal są najsłabszym ogniwem i dlatego podnoszenie ich świadomości jest niezwykle ważne – przynosi to efekty w wielu organizacjach.

Stolik nr 6

Jak przygotować się na cyberatak?

Prowadzący:
Michał Kurek, partner KPMG, szef Zespołu Cyberbezpieczeństwa, lider OWASP Polska

Dzisiaj nikt nie jest w stanie obronić swojego przedsiębiorstwa przed cyberatakiem. Dlatego oprócz działań prewencyjnych konieczne jest inwestowanie w detekcję i reagowanie po ataku. W obszarze prewencji kluczowe znaczenie ma zarządzanie ryzykiem. Identyfikacja aktywów, informacji, które są najważniejsze z punktu widzenia organizacji, pozwala racjonalnie skoncentrować wysiłki i inwestycje. Jeśli chodzi

natomiast o monitorowanie bezpieczeństwa, o detekcję, to uczestnicy zgadzali się, że potrzebne jest bardziej aktywne podejście, threat hunting i związana z tym wymiana informacji, jak również przygotowanie organizacji na przyjęcie danych typu threat intelligence. Mając na uwadze reakcję, kluczowe jest posiadanie interdyscyplinarnego zespołu, gotowego na sytuacje stresowe i sprawnego operacyjnie, co można osiągnąć dzięki częstemu ćwiczeniu i prowadzeniu gier symulacyjnych.

Stolik nr 7

Cyber Security Forensic (analiza powłamaniowa), czyli jak uczyć się na błędach?

Prowadzący:
Bartłomiej Sobczyk, Territory Account Manager, FireEye;

Marcin Kacprzak, System Engineer, FireEye

Ze względu na problemy z doborem odpowiedniej kadry i utrzymaniem ludzi w zespołach, nie warto zaczynać od wydzielania specjalnego zespołu do samej analizy incydentów. Lepszym pomysłem, zwłaszcza jeśli zaczyna się od zera, jest powoływanie takiego zespołu per case. To zdecydowanie upraszcza sprawę, przynajmniej w początkowym okresie budowy SOC czy zespołu analizy incydentów. Drugim ważnym wnioskiem z dyskusji było to, żeby z wykrytego ataku wyciągać nauki nie tylko natury technicznej, dotyczące rekonfiguracji czy usprawnienia systemów ochrony, ale także natury proceduralnej, pozwalające udoskonalić procesy obowiązujące w firmie. Trzeba być także przygotowanym na najgorszy scenariusz. Dlatego w każdej procedurze dobrze jest mieć punkt mówiący o tym, że kiedy dochodzi do „wielkiego pożaru", mamy procedurę opisującą zaangażowanie firmy trzeciej. To z kolei wymaga wcześniejszego przygotowania umowy NDA z kilkoma potencjalnymi dostawcami. Potrzebne jest też przeprocesowanie kwestii prawnej z taką firmą, żeby w krytycznej sytuacji można było uruchomić współpracę w ciągu kilku godzin, a nie dni. Często bowiem to sprawy natury formalnej zajmują najwięcej cennego czasu.

Stolik nr 8

Digital forensics

Prowadzący:
Diogo Fernandes, Forensic and Cybersecurity Analyst, Booking.com

Digital forensics dotyczy w szczególności zbierania dowodów i prezentowania ich

w sądzie. Jest to niezwykle trudne zadanie, zwłaszcza jeśli skala organizacji jest ogromna. Do tego dochodzą nowe wyzwania: internet rzeczy, technologie mobilne i chmurowe. Przykładowo, telefony komórkowe często zabezpieczone są hasłem, a znajdujące się w pamięci dane są zaszyfrowane. Pozyskiwanie dowodów w takim wypadku wymaga zdobycia zaawansowanych narzędzi albo zatrudnienia wyspecjalizowanych organizacji, które mają porozumienia z producentami sprzętu i są w stanie przełamać istniejące zabezpieczenia. Decydując się na samodzielne działania, warto brać pod uwagę zarówno komercyjne narzędzia, jak i open source.

Stolik nr 9

Outsorcing cyberbezpieczeństwa – czy to ma sens?

Prowadzący:
Piotr Pietras, inżynier sprzedaży, F-Secure

Główne problemy outsourcingu cyberbezpieczeństwa zidentyfikowane w trakcie dyskusji to: brak kontroli nad dostawcami takich usług, brak zaufania do dostawców oraz brak chęci po stronie dostawców do podejmowania ryzyka w związku ze świadczonymi usługami, a także brak gotowości do zapewniania klientom kontroli nad usługą. Uczestnicy potwierdzili, że dostawcy zwykle w ciągu pierwszych miesięcy kontraktu zapewniają wysoki poziom usługi, w środkowym okresie jakość zdecydowanie spada, a pod koniec, kiedy dyskutuje się o przedłużeniu umowy, znowu się podnosi. Czasem problemem w wykorzystaniu outsourcingu jest bezzasadny opór kierownictwa organizacji, które chce zatrzymać jak najwięcej zasobów wewnątrz firmy. Co ważne, nie istnieją żadne większe problemy prawne, które wykluczałyby outsourcing cyberbezpieczeństwa. Główny wniosek z dyskusji jest taki, że jeżeli organizacja jest w stanie wykorzystać pracowników, których zatrudnia w pełnym wymiarze godzin, to powinna zająć się obszarem cyberbezpieczeństwa samodzielnie. Natomiast jeśli mówimy o pojedynczych przypadkach, to lepiej powierzyć ich obsługę zewnętrznym firmom, ponieważ poprzez outsourcing lepiej optymalizuje się koszty i zyskuje się dostęp do wiedzy ekspertów, którzy na co dzień zajmują się tematem.

Stolik nr 10

Droga do zgodności z NIS – wybrane wymogi wynikające z Ustawy o Krajowym Systemie Cyberbezpieczeństwa

Prowadzący:
Andrzej Malinowski, ekspert ds. bezpieczeństwa, IMMUSEC

Podczas dyskusji zastanawiano się, jak z wymogami ustawy o KSC poradzą

sobie w szczególności małe i średnie organizacje? Jak ludzie, którzy na co dzień nie zajmują się bezpieczeństwem IT, poradzą sobie z opracowaniem dokumentacji zgodnej z ISO 27001, wypełnią tabelkę oceny ryzyka lub uzgodnią ze swoim kierownikiem, dyrektorem albo prezesem, czy w ciągu 24 godzin podjąć decyzję o zgłoszeniu incydentu? Uczestnicy dyskusji zgodzili się, że właśnie dlatego potrzebne są maksymalnie skrótowe wytyczne w tym zakresie. Zmierzamy bowiem do systemu cyberbezpieczeństwa państwa i dobrze byłoby, żeby ten marsz był wspólny i jeden.

RUNDA 3

Stolik nr 1

Jak zarządzać kryzysem w organizacji, w której wystąpił poważny incydent bezpieczeństwa?

Prowadzący:
Grzegorz Długajczyk, Head of Technology Risk Team, ING Bank

Co robić w przypadku kryzysu, czegoś, co już się wydarzyło albo wiemy z pewnością, że wkrótce się wydarzy? Kryzys to nie tylko niedostępność usług, ale także szantaż, wyciek danych, kradzież własności intelektualnej. Przede wszystkim potrzebny jest plan zarządzania kryzysowego. Przy tym nie chodzi wyłącznie o papierowy dokument, ale o to, żeby faktycznie testować to, co jest w nim zapisane. Co powinien zawierać taki plan? Przede wszystkim obligatoryjną i fakultatywną listę osób, które uczestniczą w sztabie kryzysowym. Na liście obligatoryjnej kluczową rolę ma osoba podejmująca decyzje. Najlepiej, jeśli jest to członek zarządu. Najważniejszą zaś rolę na liście fakultatywnej ma do wypełnienia rzecznik prasowy, który komunikuje się z mediami. Plan powinien być aktualny, przez co należy rozumieć, że jest regularnie przeglądany, uzupełniany i zatwierdzany. Niezwykle ważne w tym kontekście jest dzielenie się wiedzą w skali sektorowej.

Stolik nr 2

Nie dajmy się zwariować, czyli o tym, jak zachować zdrowy rozsądek w gąszczu regulacji

Prowadzący:
dr Łukasz Kister, niezależny ekspert bezpieczeństwa i biegły sądowy

Punktem wyjścia do dyskusji była zdroworozsądkowa ocena regulacji, jakie pojawiły się w ciągu ostatnich miesięcy. Okazało się, że niektórzy uczestnicy uznali, że RODO i KSC to najlepsze, co mogło się nam przytrafić. Wreszcie bowiem w bezpieczeństwie zacznie być wykonywana analiza ryzyka. Należałoby jednak wobec tego zapytać retorycznie: czym w takim razie zarządzano wcześniej, jeśli nie analizowano ryzyka? Niepewnością? Kolejną ciekawą kwestią są zabezpieczenia techniczne. Regulacje ich nie wymuszają, a jedynie zobowiązują, żeby dobierać je odpowiednio do ryzyka. Każda organizacja samodzielnie decyduje, jaki poziom bezpieczeństwa chce osiągnąć. Zastosowane zabezpieczenia mają wynikać z celu, a celem jest zapewnienie ciągłości dostaw pewnych usług. I ponownie należy zapytać retorycznie: jeśli dotychczas tak organizacja nie działała, to jak zapewniała ciągłość usług i jak w ogóle funkcjonowała?

Stolik nr 3

Jak sprawić, by bezpieczeństwo znalazło się w strategii twojej organizacji, czyli by zarząd uznał je za ważną kwestię?

Prowadząca:
Agnieszka Ulanowska, dyrektor Działu Nadzoru Wewnętrznego i Bezpieczeństwa IT, Noble Funds TFI

W trakcie dyskusji wszyscy bez zastrzeżeń zgodzili się, że zarząd musi mieć świadomość nie samego bezpieczeństwa, ale przede wszystkim istniejącego ryzyka. Jak zatem osiągnąć ten stan? Uczestnicy sformułowali kilka porad, które mogą pomóc w budowaniu świadomości zarządu. Po pierwsze, ważna jest praca metodą „małych kroków" na różnych szczeblach organizacji. Edukacja powinna objąć całą organizację: od szeregowego pracownika po prezesa. Zarządowi trzeba pokazywać, że bezpieczeństwo to element całościowego systemu kontroli wewnętrznej. Ważne jest, żeby szukać sojuszników w innych działach. Pierwszorzędnym kandydatem na sojusznika jest departament ryzyka, ponieważ tam właśnie pracują ludzie, którzy mają ogromne doświadczenie w prezentowaniu ryzyka. Jednocześnie nie można zapominać mówić o zagrożeniach, np. o incydentach. Wreszcie, trzeba pamiętać o dokumentacji zarówno w odniesieniu do planu działania, jak i realizacji podjętych działań.

Stolik nr 4

Oczy nie śpią, czyli czy można monitorować sieć i zasoby użytkowników w zgodzie z prawem, a jeśli tak, to w jaki sposób?

Prowadzący:
Artur Piechocki, radca prawny, prezes, Kancelaria Prawna APLAW

Obowiązujące prawo nie przystaje do aktualnej sytuacji w obszarze monitoringu. Ciągle jest wiele wątpliwości i znaków zapytania. Tymczasem sam monitoring jest niezbędny, jeśli chcemy wykrywać anomalie, zapobiegać incydentom czy odtwarzać ich przebieg. Ważąc interesy pracownika w zakresie ochrony prywatności i tajemnicy korespondencji

wobec powodowanych przez niego, zwykle celowo, zagrożeń oraz bezpieczeństwo interesów gospodarczych pracodawcy, np. w zakresie tajemnicy przedsiębiorstwa, należałoby uznać wyższość tych ostatnich interesów nad pozostałymi. Oczywiście, przy uwzględnieniu spełnienia wobec pracownika obowiązku informacyjnego co do stosowanego wobec niego monitoringu, np. w regulaminie pracy czy regulacjach wewnętrznych zakładu.

Stolik nr 6

Polityka zarządzania hasłami i dostępami. Różne podejścia i ryzyka

Prowadzący:
Sebastian Pikur, architekt bezpieczeństwa, RyzykoIT.pl

Podobnie jak w innych przypadkach, także w odniesieniu do polityki haseł istnieje potrzeba szacowania ryzyka. Głównie chodzi o ryzyko w zakresie postępowania z informacjami. Optymalne jest wyjście od klasyfikacji informacji i dobrania polityki dostępu oraz haseł do istniejących ryzyk, które są związane z danymi informacjami. W trakcie dyskusji zastanawiano się, czy ktoś już zwalidował dotychczasowe wymagania odnośnie do polityki haseł i zmienił istniejące warunki. Dotychczas nie było sygnałów, żeby tak było. Jeśli chodzi o podejście do problemu skomplikowania czy trudności polityk bezpieczeństwa, to istotne jest, żeby z jednej strony brać pod uwagę pomyślne przechodzenie audytów, a z drugiej strony łatwość wdrażania.

Stolik nr 7

GDPR jako wektor ataku

Prowadzący:
Marcin Masłowski, konsultant ds. bezpieczeństwa informacji i CISO, Carrefour Polska

Uczestnicy dyskusji zgodzili się i potwierdzili, że GDPR jest wektorem ataku. Decyduje o tym, na razie wciąż deklaratywna, wielkość sankcji. To niewątpliwie stanowi zagrożenie. Jest kilka powodów wykorzystywania RODO jako narzędzia do ataku: wymuszenia świadczeń przez pracowników, rekonesanse, czyli zdobywanie i wyłudzanie informacji, które normalnie nie zostałyby podane, może to być także szantaż. Co można zrobić w tej sytuacji? Po pierwsze, należy zacząć od budowania świadomości pracowników. Po drugie, konieczne jest zapewnienie systemu obiegu informacji w organizacji w odniesieniu do zgłoszeń RODO – trafiają one praktycznie do wszystkich pracowników. Po trzecie, trzeba uzbroić się w cierpliwość i poczekać na orzecznictwo – nie mamy bowiem wpływu na to, w jakim kierunku będzie ono zmierzać.

Stolik nr 8

Security by Design i Privacy by Design – różnice i obszary tożsame

Prowadząca:
Monika Adamczyk, główny specjalista, Urząd Ochrony Danych Osobowych

Ciągle brakuje dobrego zrozumienia, czym jest prywatność i dlaczego powinniśmy chronić nasze dane. Dlatego konieczne jest inwestowanie w budowanie świadomości. Trzeba pamiętać, że informacje o nas są wartościowe. W pewnym sensie to waluta, którą możemy wykorzystać. Uczestnicy dyskusji zgodzili się, że obecna sytuacja nie jest dobra. Pozytywne natomiast jest to, że wprowadzone przepisy pozwalają efektywnie chronić informacje o nas. Niemniej sami musimy o to zadbać. Nikt inny nie zrobi tego za nas.

Jest wiele obszarów wspólnych między prywatnością a bezpieczeństwem. Nie ma jednak jeszcze wypracowanych narzędzi czy metod. Co nie znaczy, że nie można się oprzeć na bezpieczeństwie, żeby wdrożyć prywatność i zapewnić ochronę danych.

Stolik nr 9

Krok dalej niż SOC i CSIRT, czyli Cyber-Fusion. Jak zrównoważyć technologie i zasoby ludzkie, by jak najlepiej chronić organizację?

Prowadzący:
Francesco Chiarini, Senior Manager, Information Security Threat & Response, PepsiCo Global Information Security

Nadal niewiele osób zdaje sobie sprawę, czym jest CyberFusion. Dlatego dyskusja rozpoczęła się od zdefiniowania, jakie funkcje pełnią ośrodki Cyber-Fusion Center. Podstawowe to: cyber threat intelligence, threat hunting oraz wykrywanie zagrożeń, monitorowanie zdarzeń i reagowanie oraz analiza złośliwego oprogramowania. Wykorzystanie tego modelu ma oczywiście plusy i minusy. Wśród uczestników dyskusji nie było przedstawicieli organizacji, które zaimplementowały takie podejście, choć zdradzali oni ogromne zainteresowanie. Dlaczego jest to kusząca idea? Ponieważ pośród korzyści CyberFusion pojawia się lepsza organizacja działania, która skutkuje szybszym rozwiązywaniem problemów i reagowaniem. Dostaje się także lepsze wskaźniki, dzięki którym o wiele łatwiej uzasadniać inwestycje. Oczywiście istnieją i wyzwania. Kluczowe jest rekrutowanie wysokiej klasy specjalistów oraz koszty szkoleń pracowników – zwłaszcza kiedy projekt uruchamia się od podstaw.

Stolik nr 10

Czy stać mnie na własny SOC, czy lepiej kupić usługę? Porozmawiajmy o wadach i zaletach obu podejść

Prowadzący;
Adam Rafajeński, Chief Security Officer, Aegon

Dyskusja rozpoczęła się od rozważań nad samą koncepcja SOC. Uczestnicy zgodzili się, że uruchamianie takiego ośrodka w trybie 8/5 mija się z celem. Ważne jest przy tym ustalenie zakresu działania. Zwykle co innego przez SOC rozumie dział IT, o czym innym myśli zarząd, a zupełnie co innego proponuje potencjalny dostawca. Każda firma zainteresowana posiadaniem SOC musi zmierzyć się z trudnościami z pozyskaniem personelu. Bardzo wielu ekspertów nie chce pracować w trybie 24/7. Zarówno model własny, jak i outsourcingowy mają swoje zalety oraz wady. W pierwszym przypadku zaletą jest elastyczność i możliwości skupienia się na sytuacji, jaka się wytworzyła w firmie. Zawsze w organizacji istnieje bowiem dużo rozmaitych narzędzi, a zewnętrzny dostawca przychodzi ze swoimi. Dlatego outsourcing sprawdza się najlepiej, kiedy zaczynamy od zera. Własny SOC integruje różne technologie, podczas gdy dostawca koncentruje się na jednej. Jeśli w firmie działają trzy rodzaje systemów SIEM, to w przypadku outsourcingu na pewno pojawi się problem. Realizując SOC samodzielnie, łatwiej definiować use case'y. Dostawca zaoferuje raczej gotowy zestaw propozycji. Samodzielna realizacja to także znajomość infrastruktury oraz niższy koszt rozszerzenia SOC. Wadą natomiast jest niewątpliwie bardzo duża zależność od lokalnej polityki oraz podatność na rozmaite naciski.

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 menedżerów ICT. Evention jest organizatorem uznanych na rynku konferencji, m.in.:

Big Data Technology Warsaw Summit • CYBERGOV • CHIEF Data Officer Forum • IoT Summit • Advanced Threat Summit

WWW.EVENTION.PL

ORGANIZATORZY

EVENTION
CZAS ZAANGAŻOWANY

ISSA POLSKA

WSPÓŁPRACA MERYTORYCZNA

CSO COUNCIL

PARTNER GENERALNY

FireEye
SECURITY REIMAGINED

PARTNER STRATEGICZNY

F-Secure

PARTNERZY MERYTORYCZNI

Arrow
Barracuda
Cisco
comtegra
dimension data
EY
Flowmon
Driving Network Visibility
FORTINET
HSBC
IBM
Infoblox
IMMUSEC
IMNS
integrity partners
ivanti
KPMG
Microsoft
paloalto
PASSUS
pwc
Qualys.
RSA
SECB
AUTONOMOUS INVESTIGATION
Symantec
tenable
TREND MICRO
zscaler

MECENASI

Cynet
HOLISTIC SECURITY SIMPLIFIED
Bank Polski

PARTNER MERYTORYCZNY

ISACA
Warsaw Chapter

PATRONI

CSAPL
CyberDefence 24
ISACA
Katowice Chapter
(ISC)²
OFFICIAL CHAPTER
OWASP
PTI
sekurak.pl
WROCŁAW