
RAPORT
ADVANCED
THREAT
SUMMIT 2014
19-20 listopada, Warszawa
www.atsummit.pl

ADVANCED THREAT SUMMIT 2014

Organizatorzy

EVENTION
CZAS ZAANGAŻOWANY

ISSA

Patroni Honorowi

BBN BIURO BEZPIECZEŃSTWA NARODOWEGO

Ministerstwo Administracji i Cyfryzacji

Partner strategiczny

FORTINET

Partnerzy

Akamai FASTER FORWARD

IBM

www.atsummit.pl

Warszawa, styczeń 2015 r.

Szanowni Państwo!

W imieniu organizatorów konferencji Advanced Threat Summit listopadzie 2014 r. – ISSA Polska oraz Evention – jeszcze raz bardzo dziękujemy wszystkim, którzy przyczynili się do jej powstania. W szczególności partnerom i patronom konferencji, członkom Rady Programowej oraz wszystkim prelegentom, uczestnikom debat panelowych i animatorom dyskusji roundtables. Oczywiście składamy również podziękowanie wszystkim uczestnikom, którzy tak licznie przybyli na tę niedawną konferencję.

Zapraszamy do lektury raportu powstałego po konferencji, w którym znajdziecie Państwo m.in. kilka inspirujących rozmów z naszymi prelegentami keynotes, podsumowanie dyskusji roundtables, fotoreportaż z konferencji. Mam nadzieję, że to będzie dla Państwa interesująca lektura.

Zapraszamy również do udziału w drugiej edycji konferencji Advanced Threat Summit na jesieni 2015 roku!

Ukłony,

Adam Danieluk
prezes zarządu ISSA Polska

Przemysław Gamdzyk
prezes zarządu Evention

ADVANCED THREAT SUMMIT 2014

Partnerzy merytoryczni

APIUS technologies

BT

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

Deloitte.

T · ·

hp

QUALYS® CONTINUOUS SECURITY

TREND MICRO™

Partnerzy warsztatów

COMPFORT MERIDIAN

prevenity SECURITY SOLUTIONS

Współpraca merytoryczna

IMMUSEC

SecuRing

Partnerzy wspierający

CHECKMARX

EM & CA

inveaTECH

Spis treści

Środowisko do zintegrowania

Rozmowa z Adamem Danielukiem, prezesem zarządu ISSA Polska oraz CSO w polskim oddzialem FirstData.

Jak duże jest polskie środowisko profesjonalistów zajmujących się bezpieczeństwem ICT? Jak można je oszacować liczbowo?

Nie jest to proste. Liczba certyfikowanych specjalistów oscyluje w granicach 500 osób, natomiast liczba profesjonalistów, którzy zajmują się bezpieczeństwem ICT, jest znacznie większa. Tym bardziej że część stanowisk w obszarze IT ma siłą rzeczy wpisaną odpowiedzialność za bezpieczeństwo w charakter swojej pracy. Myślę, że możemy mówić o kilku tysiącach osób, które są zaangażowane w bezpieczeństwo.

Czy widać tutaj także ludzi z instytucji sektora publicznego? Czy przedstawiciele tego sektora są adekwatnie do swego znaczenia reprezentowani w organizacji?

Obecność ludzi z instytucji sektora publicznego jest niestety słabo widoczna, co w porównaniu przede wszystkim do Stanów Zjednoczonych stanowi istotną różnicę. Tam sektor publiczny jest mocno reprezentowany w obszarze bezpieczeństwa. Na szczęście to się obecnie zmienia i sektor publiczny zaczyna być coraz bardziej widoczny również i u nas. Na listopadowej konferencji „Advanced Threat Summit" mieliśmy na przykład jedną z dyskusji w sesji roundtables poświęconą w całości kwestii bezpieczeństwa w sektorze publicznym.

No właśnie, skoro już o tym mowa, czy konferencja „Advanced Threat Summit", której ISSA Polska była współorganizatorem, spełniła Wasze oczekiwania?

Muszę przyznać, że tak. Zrobiliśmy naprawdę dobrą konferencję, co widać po ocenach uczestników i co miałem okazje słyszeć od obecnych. Nie co dzień udaje się zebrać w jednym miejscu

około 300 profesjonalistów zajmujących się bezpieczeństwem. Na pewno będzie warto ją powtórzyć za rok.

W jaki sposób ISSA Polska stara się animować i integrować środowisko wszystkich profesjonalistów bezpieczeństwa ICT? Co oferujecie swoim członkom – co w praktyce jest dla nich najważniejsze? Czy jesteście zadowoleni z dotychczasowych rezultatów?

Stowarzyszanie ISSA Polska stara się integrować i animować środowisko bezpieczeństwa ICT przede wszystkim poprzez organizowanie spotkań, zarówno bezpłatnych, jak i płatnych. Także poprzez wspieranie wybranych wydarzeń bezpieczeństwa w Polsce, zarówno poprzez patronaty, jak i bezpośredni udział członków stowarzyszenia. Staramy się także budować rozpoznawalność Polski poprzez promocję stowarzyszenia w ramach międzynarodowej ISSA International, m.in. byliśmy do tej pory dwukrotnie wybierani oddziałem roku przez ISSA International, dostaliśmy zaszczytny tytuł najlepszego oddziału w zakresie komunikacji ze środowiskiem bezpieczeństwa IT w Polsce. Jedna z firm działających w Polsce została wybrana najlepszą firma wspierającą bezpieczeństwo. To też bardzo dobra forma promocji, jeśli chcemy zaistnieć na rynku poza Polską. Zresztą, dopowiem, że po naszej nominacji firma ta została kupiona przez Cisco.

Nasz członek stowarzyszenia w związku z pracą na rzecz stowarzyszenia uzyskał tytuł Ochotnika Roku. ISSA International ufundowała mu pobyt na konferencji w USA, podczas której otrzymał nominację. Podejmujemy szereg działań, by budować i integrować środowisko bezpieczeństwa ICT.

Jak ważnym elementem tych działań są konferencje? Czy menedżerowie i eksperci bezpieczeństwa ICT chcą i potrzebują spotykać się w świecie realnym?

To dobre pytanie. Na pewno eksperci i menedżerowie chcą się spotykać twarzą w twarz. Ograniczeniem jest czas, budżet, tematyka i spory wybór konferencji branżowych oraz okołobranżowych. Czasami w natłoku wydarzeń trudno wybrać coś sensownego. Można powiedzieć, że momentami cierpimy na klęskę urodzaju. Tym bardziej że każdy z dostawców próbuje na własną rękę i z różnym skutkiem organizować swoje spotkania. Właściwych uczestników w odpowiedniej liczbie ściągają dzisiaj już tylko nieliczne, najlepsze tego typu spotkania.

Pamiętając o AT Summit 2014

Ubiegłoroczna konferencja Advance Threat Summit za nami. Konferencja zgromadziła w sumie ponad 300 uczestników i przez to było to jedno z najważniejszych wydarzeń z obszaru cybersecurity w Polsce w 2014 r. Meliśmy kilkunastu partnerów i kilkunastu patronów, blisko 60 prelegentów.

Przez dwa dni jej uczestnicy się mogli wziąć udział w wykładach o aktualnych zagrożeniach w cyberprzestrzeni i skutecznej obronie przed nimi, prowadzonych przez znanych polskich i zagranicznych ekspertów. Wysłuchać debat koncentrujących się na największych wyzwaniach stojących przed osobami odpowiedzialnymi za bezpieczeństwo informacji w firmach i instytucjach. Także uczestniczyć w warsztatach i demonstracjach na żywo praktycznych umiejętności, niezbędnych w codziennej pracy.

Uczestnicy mogli również wziąć udział w równoległych sesjach roundtables, prowadzonych przez najlepszych fachowców w swoich dziedzinach i umożliwiających bezpośrednią wymianę opinii i doświadczeń – taka forma aktywnej partycypacji całego audytorium w konferencji dla wielu uczestników była istotną nowością. Sesje roundtable pomagały bowiem także na to, co w konferencjach najważniejsze – by nawiązać bezpośrednie relacje ze swoimi kolegami po fachu, bo efektywne bezpieczeństwo IT musi opierać się na dzieleniu się wiedzą i wspólnym działaniu.

Prezentujemy zbiór wrażeń i wypowiedzi z konferencji.

Aktualny obraz sytuacji.
Radosław Żuber, CERT Polska

W tym roku w dalszym ciągu można było zaobserwować w Polsce to, co zaczęło się w grudniu 2013. Przestępcy łączyli atak na routery domowe, podmianę DNS-ów i przepuszczanie ruchu przez proxy z wykorzystaniem serwerów ATS.

Przemija postać tego świata.
Guillaume Lovet, Fortinet

Wszyscy jesteśmy celem, a atak ma zawsze dwie fazy – uzyskanie dostępu do ofiary i monetyzację. Aby uzyskać dostęp zwykle na masową skalę jest rozsiewany malware, a następnie są wprowadzane w życie różne przestępcze modele biznesowe. Najprostszy z nich wykorzystuje przejęte bankowe dane uwierzytelniające...

FUD-y i mity narosłe wokół ataków ukierunkowanych i APT.

Udo Schneider, TrendMicro

W zwalczaniu ataków ukierunkowanych przyjęło się sądzić, że sandboxing jest Świętym Graalem, że wszystko załatwia. To dobra technika, ale tylko jedna z tych, które powinniśmy użyć, w dodatku bardzo zużywająca zasoby.

Praktyczna strona obsługi incydentu APT – case study.

Krzysztof Białek, Orange Polska

Spam to nie jest niby nic nowego i zaskakującego. Ale pierwszy raz przy zmasowanym ataku spamu, podszywającego się pod naszą markę, mieliśmy do czynienia z tak dużym wpływem na naszą firmę, naszych klientów, a także inne organizacje. Ten spam był bowiem powiązany z dystrybucją malware wymierzoną w bankowość elektroniczną dziewięciu polskich banków.

Autorski komentarz do sesji – w formie case study z ataku socjotechnicznego – czyli od jednego e-maila do kradzieży 9 milionów.

Piotr Konieczny, niebezpiecznik.pl

Wykradliśmy wszystkie informacje związane z wejściem firmy na giełdę. Wyciągi z firmowego konta, które były przesyłane mailowo. Stan konta. Dochody tej firmy z reklam. Negocjacje biznesowe. Dane osobowe... Koszt ataku 67 zł plus 21 dni, a wniosek taki, że każdego da się oszukać, zwłaszcza jak trafimy na jego słaby dzień. Dlatego firmy powinny starać się jak najbardziej minimalizować ryzyko takich zdarzeń.

Debata panelowa: Secure by design – ładne hasło czy przyszłość bezpieczeństwa IT.

Wśród argumentów padających w debacie najczęściej powracał mówiący ten, że budowanie bezpiecznych rozwiązań jest znacznie łatwiejsze niż późniejsze ich zabezpieczanie. Dlatego bezpieczeństwo powinno być wbudowane w proces tworzenia oprogramowania od samego początku. Problem w tym, że stosowane metodyki nie uwzględniają tego w należytym stopniu.

Rozprawa na wzór debaty oxfordzkiej.
Przyszłość aktywnego przeciwdziałania nieznanym atakom.

W debacie spierali się zwolennicy jak najdalej idącej automatyzacji bezpieczeństwa z obrońcami „interfejsu białkowego", czyli głosicielami tezy, że człowiek w zabezpieczaniu systemów informatycznych jest nie do zastąpienia. I choć obie strony przedstawiły przekonujące argumenty, to konkluzja mogła być tylko jedna – ludzie potrzebują automatów, a automaty nie poradzą sobie bez ludzi.

Wojna informacyjna w środowisku zaawansowanych technologii i ośrodków R&D – czy trzeba nam jeszcze więcej sygnałów alarmowych?

Dr. Hans-Joachim Popp, Deutsches Zentrum für Luft und Raumfahrt (DLR)

Trwa wojna informacyjna i sytuacja jest dramatyczna. Oprócz posiadania rozwiązań technologicznych, aby się bronić, musimy pilnie stworzyć prawne ramy funkcjonowania Internetu. Bez tego nie może być mowy o sukcesie w biznesie opartym na Sieci. Co ważne, aby ten cel osiągnąć, trzeba dążyć do współpracy lokalnych, europejskich firm i instytucji informatycznych.

Luki i podatności – całkiem nowy kierunek zagrożeń.

Martin McKeay, Senior Security Advocate w Akamai

Po niedawnym ujawnieniu od lat istniejących luk – takich jak Heartbleed, Shellshock i Poodle – przede wszystkim musimy mieć plan, co robić, gdy zdarzy się to znowu. Gdy będą dawać o sobie znać kolejne podatności. Stan wyjątkowy, jakiego będziemy doświadczać w perspektywie następnych 3-5 lat nie przypomina niczego, z czym mieliśmy dotąd do czynienia.

Potrzeba wspólnego działania. Komentarz do sesji.

Marcin Olender, Ministerstwo Administracji i Cyfryzacji

Sam rząd nigdy nie zapewni bezpieczeństwa w Internecie. Tylko we współpracy ze wszystkim innymi podmiotami, firmami, dostawcami Internetu możemy popychać to bezpieczeństwo w dobrym kierunku. Mamy w Polsce dużo bardzo dobrych fachowców i zespołów, ale wszyscy oni nie tworzą jeszcze spójnego systemu. To trzeba poprawić.

Debata: Bezpieczeństwo biznesu WWW czyli „Security i IT – wspólna sprawa".

Debata pokazała, że współpraca IT i Bezpieczeństwa nie zawsze układa się bezproblemowo. Między stronami nierzadko dochodzi do konfliktu interesów. Dział IT nie zawsze ma sprawy bezpieczeństwa w swoich priorytetach. Z kolei działowi bezpieczeństwa – gdy nie chce zaakceptować jakiegokolwiek ryzyka – zdarza się ograniczać administratorów przez narzucanie zbyt rygorystycznych warunków.

DDoS – gdzie jesteśmy i dokąd zmierzamy.

dr Martin Brown

Ponad połowa respondentów naszego globalnego badania uznała, że ataki DDoS za jedno z najpoważniejszych zagrożeń dla ich systemów informatycznych. Blisko 80 proc. z nich nie ma wystarczających zasobów, by im przeciwdziałać. Może im pomóc ISP, dysponujący technikami ograniczania skutków ataków DDoS i współdziałający w tym względzie z partnerami.

Ataki DDoS – jak się skutecznie obronić?

Hubert Gałka, GTS

Atak DDoS można w organizacji bez nazwy zamówić już za 100 dol. Może on trwać 24 godzin i mieć wolumen kilku Gb/s. Większość klientów biznesowych nie dysponuje łączem większym niż 1 Gb/s, więc taki atak oznacza automatyczne odcięcie od zasobów, takich jak CRM, od możliwości składania zamówień, wszelkiej komunikacji przez Internet.

Glib Paharenko, OWASP Ukraine

Ukraina była miejscem licznych ataków ze strony Rosji – w szczególności DDoS, robaków, atakó1) na sieci mobilne – począwszy od czasu Majdanu aż do dzisiaj.

Sesja Q&A, DDoS – czy istnieje optymalna droga obrony?

Wśród wniosków z tej sesji, wynikających z własnych doświadczeń jej uczestników, był taki, że ataki DDoS – jako najłatwiejsze do przeprowadzenia – są bardzo często przykrywką do przeprowadzania innych, ukierunkowanych ataków. A gdzie powinna znajdować się główna linia obrony przed DDoS – na miejscu czy u dostawcy usługi dostępowej? Na ten temat zdania były podzielone.

Marcin Kobyliński,
przewodniczący Rady Programowej konferencji i przedstawiciel ISSA Polska

Konferencja byłą miejscem networkingu i dyskusji bezpośrednich w formie roundtables. W trakcie konferencji miały także miejsce wydzielone warsztaty dla profesjonalistów.


ADVANCED
THREAT
Adam Gałach
GALACH CONSULTING


ISSA
Pasja, wiedza,
doświadczenie,
otwartość
FortiNet
FlowMon

APT to nie jest dobra nazwa

O ukierunkowanych atakach i obronie przed nimi mówi Udo Schneider, Security Evangelist w Trend Micro.

Czy rzeczywiście powinniśmy się aż tak bardzo obawiać ataków APT? Może to jednak bardziej straszak, używany przez dostawców zabezpieczeń, którzy lubią budzić pewien niepokój swoich klientów?

Osobiście nie lubię terminu APT. Pojęcie Advanced Persistent Threat po raz pierwszy pojawiło się w 2006 r. w kręgach związanych z obronnością w USA i dotyczyło militarnych zagrożeń. W związku z tym do APT w sensie informatycznym przylgnęło przekonanie, że odnosi się przede wszystkim do ataków na organizacje związane z instytucjami państwowymi. Dlatego firmy i korporacje zwykły sądzić, że jeżeli nie są związane z rządem, to nie raczej nie powinny być celem ataków.

Dlatego znacznie trafniejsze jest określanie tego rodzaju zagrożeń jako Targeted Attacks – ataków ukierunkowanych. Na konkretny cel. A takim celem może być każdy. Z punktu widzenia atakującego, jeśli firma ma jakieś zasoby, wrażliwe dane czy cokolwiek, co może zostać zamienione na pieniądze, to jest warta ataku. To nie znaczy, że zostanie zaatakowana, ale celem pozostaje.

Jak zatem powinniśmy się zabezpieczyć przed tego rodzaju atakami?

Powinniśmy być przygotowani na atak ukierunkowany, a obrona przed nim wiąże się zawsze z ograniczaniem ryzyka. Wymaga myślenia o tym, jak zareaguję, gdy stanę się celem takiego ataku. I tu nie chodzi tylko o środki techniczne, a nawet przede wszystkim nie o to.

Najgorszym scenariuszem jest panika. Gdy przyjrzymy się katastrofom, zauważymy, że do większości strat dochodzi tuż po zdarzeniu z powodu nieskoordynowanych, chaotycznych działań.

Dlatego oprócz rozwiązań technicznych musi być wdrożony kompletny proces reagowania na incydenty. Powinien on być stworzony, zanim dojdzie do incydentu. Oczywiście, dotyczy to też technicznych aspektów (działania sieci, operacji klient-serwer itp.), ale w zasadniczej mierze proces powinien polegać na zasobach ludzkich.

Jeśli dojdzie do ataku, musimy wiedzieć, kogo wezwać, kto jest członkiem zespołu reagowania na incydenty, jakie zadania zostały mu przydzielone. Gdy chodzi już o kwestie dochodzeniowe, musimy dysponować narzędziami, które gromadzą dane z najróżniejszych źródeł. Incydent naruszenia bezpieczeństwa możemy badać tylko na podstawie danych, jakie zdołaliśmy w związku z nim zebrać.

A jeśli przyjrzeć się technicznym zabezpieczeniom przed atakami ukierunkowanymi, to na co zwrócić uwagę?

W zwalczaniu ataków ukierunkowanych przyjęło się sądzić, że sandboxing jest Świętym Graalem, że wszystko załatwia. To dobra technika, ale tylko jedna z tych, których powinniśmy użyć, w dodatku bardzo zużywająca nasze zasoby. Jeśli musimy zbadać każdy plik i każdy dokument, który wędruje przez organizację, przepuszczając go przez sandbox, będzie to bardzo zasobożerne.

Moim zdaniem sandboxing powinien być traktowany wyłącznie jako ostatnia instancja. Zanim się na nią zdecydujemy, powinniśmy wykorzystać inne techniki detekcji zagrożeń, które bardzo szybko pomogą określić, czy coś powinno trafić do „piaskownicy", czy też nie. Ważne jest także to, że powinniśmy dostosować technikę sandboxingu do naszych warunków i wymagań. Na rynku są oferowane narzędzia określane jako „standardowy" lub „domyślny" sandbox. Moja dobra rada: nie należy ich używać. Jeśli byłbym atakującym, to dobrze odrobiłbym pracę domową i wiedziałbym, że ofiara wykorzystuje „standardowy" sandbox i odpowiednio się do tego przygotował.

Ponieważ nie ma jednego narzędzia do wszystkiego, trzeba stworzyć wielowarstwowe środowisko ochrony. Jak to zrobić?

Gdy budujemy wiele warstw ochrony, najłatwiej jest nam myśleć w kategoriach produktów. Stawiamy antywirus w tym miejscu, firewall w tamtym, sandbox jeszcze gdzie indziej, tutaj dajemy monitorowanie logów itd. Ale powinniśmy się z tym cofnąć o krok i sprawdzić, jak wygląda całe środowisko, jak współgra z procesami przebiegającymi w firmie, gdzie są dane, które mają być chronione. Bo może się okazać, że mamy dobry produkt umieszczony w złym miejscu. Dlatego trzeba wiedzieć, jakie narzędzie warto zastosować i gdzie ono powinno funkcjonować w strukturze organizacji.

Nie należy używać domyślnie skonfigurowanych snadboxów. Jeśli byłbym atakującym, to dobrze odrobiłbym pracę domową i wiedziałbym, że ofiara wykorzystuje „standardowy" sandbox i odpowiednio się do tego przygotował.

Czeka nas wiele pracy

O krytycznych lukach i podatnościach w internecie, które w najbliższych latach staną się normą, mówi Martin McKeay, Senior Security Advocate w Akamai.

Czy niedawno ujawnione, ale od lat istniejące luki – takie jak: Heartbleed, Shellshock i Poodle – to wierzchołek góry lodowej?

Rzeczywiście, w ostatnim czasie wychodzi na jaw wiele luk, choć pewnie nie uzyskują już takiego rozgłosu, jak te trzy wymienione. To jest w tym roku bardzo poważny problem i podobnie będzie w nadchodzących latach. Luki, takie jak: Heartbleed, Shellshock i Poodle, stanowią razem taki poziom podatności, jakiego dotąd nie doświadczaliśmy. Istniały przez lata i nawet nie wiemy, czy nikt ich nie wykorzystywał. Choć przez ostatnie dekady obserwowaliśmy, jak ujawniane były kolejne dziury w zabezpieczeniach, to dopiero teraz, gdy tak bardzo jesteśmy uzależnieni od internetu, podatności o dużym zasięgu mają siłę rażenia bez porównania większą niż 10 lat temu. Co gorsza, musimy się do tego przyzwyczaić, bo stanie się to normą w najbliższych latach. Co roku będziemy obserwować, jak tej klasy podatności wychodzą na światło dzienne. Internet od początku nie był tworzony z myślą o bezpieczeństwie, nie był też budowany zgodnie z tym, co dziś uważamy za dobre praktyki w programowaniu.

Co powinniśmy robić? Jak powinniśmy się do tego przygotować?

Powinniśmy zaangażować wszelkie środki i być przygotowanym na to, że skala ujawnianych luk nie będzie maleć. Mamy w internecie całą masę starego kodu. Mamy mnóstwo rzeczy, które od dawna są przełamane, ale nikt wcześniej do nich nie zaglądał. Ale teraz ludzie zaczęli się bardziej nimi interesować, bo znajdowanie tego typu luk stało się bardziej „sexy". I takie szukanie i znajdowanie będzie trwało przez wiele następnych lat.

Przez przynajmniej trzy lata do pięciu lat będziemy mieli do czynienia ze stanem wyjątkowym – systematycznie będą

ujawniane kolejne poważne luki, być może co kwartał, być może nawet częściej. Będziemy obserwować luki, które będą wymagać użycia wyjątkowych środków przez zespoły do spraw bezpieczeństwa, zespoły do spraw oprogramowania, przez całe przedsiębiorstwa.

Ale po pięciu latach wzmożonej walki z podatnościami nastanie szczęśliwy czas bez dziur w zabezpieczeniach?

Nigdy nie pozbędziemy się luk. Tego po prostu nie przewiduje ludzka natura. Ale sądzę, że większość luk – jakieś 70–80% tego, co istnieje obecnie – zostanie odkryta w ciągu następnych trzech do pięciu lat. Będziemy nadal zwiększać skuteczność praktyk zabezpieczania systemów i bezpiecznego programowania.

> Internet od początku nie był tworzony z myślą o bezpieczeństwie, nie był też budowany zgodnie z tym, co dziś uważamy za dobre praktyki w programowaniu.

W tym względzie będziemy obserwować znaczący postęp. Doprowadzi to do mniejszej liczby luk, ale nie możemy zakładać ich braku. Ale jeśli mamy plan postepowania związany z lukami i jesteśmy w stanie zareagować na te ujawniane teraz, lepiej będziemy sobie radzić z tymi, które wyjdą na jaw w przyszłości.

Czy kupowanie luk typu zero day jest w porządku?

To kontrowersyjna sprawa. Zależy od tego, kto sprzedaje i kto kupuje. Istnieje wiele programów typu Bug Bounty i firm nastawionych na handel podatnościami. Niektóre firmy sprzedają luki producentom oprogramowania, są też takie, które pomagają producentom w uruchomieniu własnych programów Bug Bounty. Niektóre firmy sprzedają ujawnione przez siebie luki instytucjom rządowym. Ale jest też ciemna strona procederu. Są ludzie, którzy sprzedają informacje o podatnościach przestępcom, którzy wykorzystają je do działań nielegalnych, niezgodnych z prawem.

Sprawa ma wiele aspektów i nie ma łatwej odpowiedzi na pytanie, czy taki handel powinien się odbywać. Osobiście wolałbym, żeby taki rynek nie istniał, ale jest na to zapotrzebowanie ze strony rządów, firm i, niestety, przestępców. Więc zamiast zastanawiać się, czy to źle, czy dobrze, powinniśmy wiedzieć, jak sobie z tym radzić.

Przemija postać tego świata

O nowych zagrożeniach i wyzwaniach w zakresie cyberbezpieczeństwa, jakie na nas czekają, mówi Guillaume Lovet, Cybercrime Analyst & Threat Response Manager w Laboratoriach FortiGuard firmy FORTINET.

W ostatnich latach świat wyraźnie przyspieszył. Jak w tym czasie ewoluowały zagrożenia?

Przed rokiem 2005 mieliśmy wirusy i malware, których autorzy nie traktowali jako narzędzia do zarabiania pieniędzy. Robili to dla zabawy, dla chwały, by „zniszczyć internet" i dla tego typu podobnych motywacji – przykładowo znane były robaki Slammer czy Love Letter. Potem pojawiły się malware, takie jak NetSky czy Bagle, które poprzez e-maile wysyłane na gigantyczną skalę zaczęły zarażać miliony komputerów. I widocznie ktoś doszedł do wniosku, że owszem, fajnie jest zainfekować taką masę komputerów, ale jeszcze fajniej byłoby mieć je wszystkie pod kontrolą. Więc pomyślał o umieszczeniu bota w robaku szerzącym się przez pocztę elektroniczną.

Punktem zwrotnym był rok 2005. Za sprawą robaka Mytob powstał wtedy pierwszy botnet złożony z komputerów Windows i od tej pory można mówić o atakach nastawionych ma monetyzowanie malware.

W jaki sposób przebiega monetyzacja ataku wykorzystującego złośliwe oprogramowanie?

Istnieje wiele różnych modeli biznesowych wykorzystywania malware. Najprostszy z nich wykorzystuje przejęte bankowe dane uwierzytelniające. Jest on stosunkowo nowy, bo przed nim monetyzowanie sieci zainfekowanych komputerów polegało głównie na użyciu ich do wysyłania spamu czy przeprowadzania ataków DDoS, wyświetlania reklam poprzez adware itp. To były dość skomplikowane modele, więc teraz monetyzacja stała się znacznie bardziej bezpośrednia – kradzież haseł dostępu do kont bankowych czy infekowanie złośliwym oprogramowaniem wymuszającym okup (ang. *ransomware*).

Coraz częściej celem ataku nie są same komputery PC, ale smartfony i inne urządzenia mobilne. Myślę, że z punktu widzenia cyberprzestępców system Android jest nowym MS Windows. Przede wszystkim z powodu popularności tej platformy – do Androida należy 80% rynku mobilnych systemów operacyjnych. Po drugie Android ma ten sam model instalowania oprogramowania jak Windows, więc te same podatności. Nie ma też jednego centralnego repozytorium aplikacji, jak App Store w przypadku iOS. W odróżnieniu jednak od komputerów PC z Windows, atak na urządzenia z Androidem jest znacznie łatwiej zmonetyzować, bo ze smartfonami jest zintegrowany sposób płatności – przez numery i SMS premium. Więc zarabianie jest jeszcze bardziej bezpośrednie.

Skuteczniejsza staje się też metoda wymuszania okupu przy użyciu ransomware blokującego smartfon, bo jest to urządzenie, bez którego użytkownik nie może się obejść, więc chętniej i szybciej płaci. Przy użyciu ataku na smartfon łatwiej jest wykorzystać i spieniężyć przechwycone hasła do kont bankowych. Uzyskuje się dostęp do urządzenia, za którego pomocą jednocześnie przeprowadza się transakcje i dokonywana jest dodatkowa metoda uwierzytelniania operacji bankowych.

Kogo dotyka cyberprzestępczość? Niektórzy twierdzą, że ich to nie dotyczy...

Cyberprzestępczość rozwinęła się na tyle, że każdy jest celem – osoba, firma albo państwo. Celem stali się polityczni i społeczni liderzy, celebryci także nie mogą się czuć bezpieczni. Wszyscy jesteśmy celem, a finansowo motywowany atak ma zawsze dwie fazy: uzyskanie dostępu do ofiary i monetyzację. Aby uzyskać dostęp, zwykle na masową skalę jest rozsiewany malware, a następnie są wprowadzane w życie różne przestępcze modele biznesowe.

Scena tego rodzaju przestępstw zrobiła się wielopoziomowa, a ci, którzy stoją na jej szczycie, osiągają olbrzymi zwrot z inwestycji – czasem nawet ponad 400-krotny!

Twórcy narzędzi ataku, ich użytkownicy oraz ci, którzy spieniężają efekty ataku, to wcale nie są te same osoby. Najczęściej nie pochodzą nawet z tych samych krajów. Może mieć to na celu ominięcie wprowadzanych przez zachodnie kraje ograniczeń sprzedaży i dostaw towarów do państw „podwyższonego ryzyka".

W światowym wymiarze dochody z całej przestępczości stanowią 3,6% GDP, co daje 300 bilionów dolarów, a straty z cyberprzestępczości osiągają wartość już 0,8% GDP, czyli 600 mld USD, i są już niemal równe dochodom z nielegalnego handlu narkotykami (0,9% GDP).

W światowym wymiarze rynek cyberprzestępczości osiąga wartość 0,8% globalnego GDP, czyli ok. 600 mld USD, co jest już niemal równe dochodom z nielegalnego handlu narkotykami (0,9% GDP).

Sprawozdanie z sesji równoległych dyskusji roundtable

– podsumowanie wniosków przygotowane przez animatorów dyskusji:

I runda

Stolik: W jaki sposób mierzyć, komunikować i transferować ryzyka bezpieczeństwa środowiska teleinformatycznego do biznesu?
Prowadzenie: Andrzej Kleśnicki, QUALYS

1. Bezpieczeństwo można i trzeba mierzyć. Należy używać KPI, KRI, dashboardów. Także tzw. map ryzyka, by móc skwantyfikować bezpieczeństwo i wiedzieć, w jakim stopniu jesteśmy bezpieczni.
2. Higiena bezpieczeństwa to podstawa – takie procesy, jak: patchowanie, vulnerability management, asset management, configuration management, muszą być częścią codziennej pracy z systemami IT.
3. Rolą bezpieczeństwa jest raportowanie do biznesu przekroczeń akceptowalnego poziomu ryzyka, czy inaczej przekroczenia progów KRI.
4. Akceptacja ryzyka musi być świadomą decyzją biznesową.

Stolik: Bezpieczeństwo usług w modelu cloud
Prowadzenie: Marcin Franczak, AXA Polska

1. Potrzebna jest zgodność z wymogami prawnymi (głównie GIODO).
2. Ważne jest również zaufanie i transparentność rozwiązań.
3. Kluczem jest szacowanie ryzyka.
4. W Polsce, niestety, brakuje dobrego benchmarkingu w tym zakresie.

Stolik: Infrastruktura krytyczna a bezpieczeństwo
Prowadzenie: Piotr Marczak, PSE

1. Trzeba pamiętać o ochronie fizycznej.
2. Państwo nie będzie w stanie objąć całej infrastruktury krytycznej.
3. Za strategią musi iść legislacja (ale nie na odwrót!).
4. Organizacje muszą zapewniać bezpieczeństwo całości swojej infrastruktury.
5. Ważny elementem tutaj jest integralność danych.

Stolik: Sprawa komunikacji pionowej – rozmowa z szefostwem firmy na temat bezpieczeństwa ICT
Prowadzenie: Dariusz Jurewicz, T-Mobile

1. Top Management w firmie to czasem prawdziwy „Advanced Threat"...
2. Do komunikacji potrzebne są: prosty język, zaufanie, właściwe case studies do zobrazowania sprawy.
3. CSO/CISO musi mieć odpowiedni autorytet, żeby w ogóle było o czym mówić.
4. Dobrze umieć wykazać ROI z bezpieczeństwa.
5. Pomóc może znajomość legislacji dotyczącej bezpieczeństwa.

Stolik: Budowanie pancernych organizacji – mrzonka, fanaberia czy konieczność
Prowadzenie: Radosław Kaczorek, ImmuSEC

1. Potrzebna jest właściwa definicja celów do osiągnięcia przy uwzględnieniu bezpieczeństwa.
2. Niezbędne jest zaangażowanie kierownictwa, sprawna komunikacja i budowanie świadomości wśród wszystkich pracowników.
3. Trzeba znaleźć balans między wygodą (sprawnością organizacji) a bezpieczeństwem.
4. Należy ograniczyć zależność od technologii na rzecz przesunięcia ciężaru na proces zarządzania.

Stolik: Bezpieczeństwo w całym cyklu rozwoju i życia aplikacji
Prowadzenie: Yaroslav Popov, HP

1. Warto pamiętać, że są dostępne zarówno, statyczne jak i dynamiczne metody badania aplikacji.

2. Wprowadzane rozwiązania bezpieczeństwa muszą być zintegrowane ze środowiskiem deweloperskim.
3. Trzeba włączyć system kontroli bezpieczeństwa aplikacji do ogólnego programu bezpieczeństwa firmy.
4. Potrzebna jest edukacja deweloperów w zakresie bezpieczeństwa.

Stolik: Nowa epoka bezpieczeństwa – wpływ ewolucji struktury demograficznej pracowników na charakterystykę obserwowanych zagrożeń

Prowadzenie: **Maria Kamińska, Lux-Med**

1. Utożsamianie się pracowników młodego pokolenia z firmą/organizacją jest już przeżytkiem. Świadomość i lojalność buduje się na poziomie zespołu.
2. Obserwujemy spadek zaufania do pracowników wiedzy. Działy IT muszą zabiegać o specjalistów oraz zwiększyć kontrolę sprawowaną przez administratorów (nagrywanie sesji).
3. Trzeba wziąć pod uwagę możliwość zapełnienia luki specjalistów, którzy z Polski emigrują, przez ekspertów zza wschodniej granicy lub innych krajów, dla których Polska byłaby atrakcyjnymi miejscem pracy.
4. Potrzebne jest monitorowanie portali społecznościowych i portali grup zawodowych, gdzie młodzi specjaliści szukają rozwiązań problemów technicznych zaistniałych w pracy – co grozi ujawnieniem informacji poufnych, np. przy budowanie kodu aplikacji.
5. Zmiana struktury demograficznej pracowników IT, w tym także tych zajmujących się bezpieczeństwem, wymaga podjęcia dodatkowych działań i wdrożenia nowych narzędzi, co sprawi, że cena bezpieczeństwa danych wpływać będzie na budżet organizacji.

Stolik: Kontraktowanie bezpiecznych aplikacji – jak to dobrze zrobić (aspekty prawne i techniczne)

Prowadzenie: **Beata Marek, Cyberlaw/ISSA Polska, oraz Wojciech Dworakowski, OWASP/Securing**

1. Potrzebna jest standaryzacja procesów sprzedażowych (w szczególności czego wymagać, w jaki sposób działać).
2. Kupowanie i zamawianie usług – problemem jest przygotowanie odpowiednich wzorników umów (jak się skutecznie zabezpieczyć) oraz właściwa współpraca działu IT i prawników.

3. Trzeba wcześniej wiedzieć, jakiego typu umowy potrzebujemy, czego powinniśmy wymagać, jakie zasady zastosować, jak ustawić cały proces, prowadzenie testów etc.
4. Powinno się wymóc zapis, że w przypadku negatywnych testów zmiany będą bezkosztowe.
5. Potrzebne jest zapewnienie prawa do dokonywania audytu przez firmy trzecie.

Stolik: Ludzie, którzy dla nas pracują czyli kwestia zaufania
Prowadzenie: Adam Rafajeński, ISACA Warsaw Chapter oraz Budimex

1. Sprawa dotyczy zarówno pracowników stałych, tymczasowych, jak i podwykonawców i ich pracowników. Zalecamy korzystanie z analizy ryzyka obszaru, do którego będzie miała dostęp określona osoba lub system przez nią tworzony/nadzorowany.
2. Weryfikowanie personelu jest kulturowo w Polsce postrzegane jeszcze negatywnie, natomiast już samo właściwie zakomunikowane przed rozpoczęciem procesu rekrutacji jest coraz częściej dobrze odbierane i akceptowane, eliminuje w dużym stopniu przystępowanie do niej przez osoby mające coś do ukrycia.

3. Mechanizmy weryfikacji:
   - losowa weryfikacja kandydatów przez HR lub specjalistyczną agencję HH;
   - serwisy społecznościowe, przede wszystkim LinkedIN, Golden Line, Facebook, Google;
   - lista referencyjna podana przez kandydata.

   Zauważyliśmy, że rozmów sprawdzających nie można przeprowadzać bez odpowiedniego przygotowania po jednej i drugiej stronie. Telefony z zaskoczenia mogą być kłopotliwe dla obu stron.

4. Zabezpieczanie się przed skutkami błędów/sabotażu
   - niezależna weryfikacja pracy;
   - polisa odpowiedzialności zawodowej;
   - polisa OC firmy;
   - kary przewidziane w umowie.

5. Rotacja: dostrzegamy problem w przypadku korzystania z niededykowanych zasobów – koszt przygotowania osoby do pracy to czasem kilka tygodni; potem okazuje się, że osoba może zostać wymieniona. Należy wprowadzać do umów zapisy o minimalnym okresie utrzymywania osób na określonych stanowiskach.

Stolik: Ludzie, którzy dla nas pracują czyli kwestia zaufania
Prowadzenie: Filip Demianiuk, Checkpoint

1. Sandboxing w chmurze stanowi poważny problem ze względu na ochronę danych. W szczególności w instytucjach finansowych wykorzystanie chmury pojawiało się w projektach biznesowych, ale nie było w stanie skutecznie bronić się przed wewnętrznymi, jak i zewnętrznymi regulacjami w zakresie ochrony informacji.

2. W dużych instytucjach okazuje się, że po zastawieniu kosztów wykorzystania środowisk tak zwanej chmury zewnętrznej oraz tej wewnętrznej (w końcu chodzi o wykorzystanie wirtualizacji), koszty usługi były bardzo podobne, a kontrola nad wrażliwymi danymi o wiele większa w przypadku wykorzystania własnej infrastruktury.

3. Przedstawiciele mniejszych organizacji zwracali uwagę na ograniczone zasoby IT w swoich firmach i chętniej spoglądali w stronę emulacji zagrożeń „w chmurze" wyrażając też duże zainteresowanie modelem hybrydowym, czyli emulacją lokalną dokumentów i „offloadowaniem" do chmury plików wykonywalnych i takich które nie mogą potencjalnie zawierać danych poufnych.

II runda

Stolik: APT – Ewolucja zagrożeń, kierunki zmian
Prowadzenie: Andrzej Wojtkowiak, IBM Polska

1. W przypadku zagrożeń spod znaku APT technologia nie wystarczy, niezbędna jest edukacja użytkownika końcowego.
2. Prowadzenie testów to także element uświadamiania użytkowników.
3. Można się spodziewać, że ataków APT będzie coraz więcej.
4. Problemów nie rodzi samo przeciwdziałanie (bo prawdę mówiąc, nie da się skutecznie przeciwdziałać). Clou to skuteczne wykrywanie ataków APT.

Stolik: Dziurawe aplikacje webowe – kogo winić i jak je naprawić?
Prowadzenie: Andrzej Kleśnicki, Qualys

1. Deweloperzy mają zazwyczaj priorytety rozbieżne z bezpieczeństwem.
2. Edukacja deweloperów jest kluczowa, bo deweloperzy (jak chcą) potrafią tworzyć bezpieczny kod.
3. Odbiorcy oczekują, że za bezpieczeństwo nie należy dodatkowo płacić – powinno być wliczone w koszty usługi. Tak jednak być nie może. To odbiorcy powinni wymagać bezpiecznych aplikacji poprzez właściwe określenia polityk, metodyki oraz wymagań bezpieczeństwa.
4. Brakuje instytucji zaufania publicznego, która by oceniała bezpieczeństwo aplikacji, a niewidzialna ręka rynku, jak widać, nie działa.
5. Narzędzia automatyczne do ochrony i detekcji problemów z aplikacjami są ostatnią (często też jedyną) deską ratunku, nie zastąpią jednak dojrzałego i zorientowanego na bezpieczeństwo procesu wytwarzania oprogramowania.

Stolik: Testy Business Continuity – teoria a praktyka
Prowadzenie: Krzysztof Miareczko, PP Porty Lotnicze

1. Praktykuje się testy częściowe – głównie ze względu na skomplikowanie i koszty testów całościowych.
2. Testy powinny być przeprowadzane przy wolumenie transakcji czy wielkości ruchu tożsamym z produkcyjnym, bo tylko wtedy testy mają sens.

3. Testy częściowe można stosować tylko wtedy, gdy są częścią całościowej układanki – odbywa się to w ramach zaplanowanego całościowego procesu, który obejmuje wszystkie elementy składowe.

4. Tylko testy całościowe mogą pokazać pewne zależności, w wyniku czego widać braki w obszarach, których pierwotnie nawet nie bralibyśmy pod uwagę.

Stolik: Jak w milionie zdarzeń zidentyfikować prawdziwe zagrożenie, czyli doświadczenia z wykorzystania SIEM

Prowadzenie: Andrzej Wojtkowiak, IBM Polska

1. Potrzebny jest odpowieni dobór plików typu log.
2. Trzeba mieć wiedzę ekspercką.
3. Należy dążyć do eliminacji false-positive.
4. Trzeba wcześniej przygotować przypadki użycia (use case).

III runda

Stolik: Zagrożenia dla aplikacji mobilnych

Prowadzenie: Piotr Skibiński, Pokomtel

1. Poufność i prywatność danych użytkowników musi być różnie traktowana w przypadkach użytkowników będących osobami fizycznymi i osobami prawnymi. Kłopotliwe jest połączenie tych dwóch aspektów w jednym urządzeniu, z którego jednocześnie korzysta osoba fizyczna prywatnie i jako pracownik firmy, szczególnie w przypadku, kiedy korzysta ze służbowego urządzenia do celów prywatnych (np. korzysta z aplikacji bankowych lub ochrony zdrowia i pracodawca nie ma prawa do danych zgromadzonych w tych aplikacjach). Odpowiednie rozwiązania bezpieczeństwa dopiero raczkują i nie spełniają oczekiwań rynku.

2. Trudne jest połączenie bezpieczeństwa z odpowiednio wysokim poziomem zadowolenia użytkownika aplikacji mobilnych. Użytkownik chce szybko, prosto i łatwo – bez konieczności odblokowywania urządzenia i temu podobnych czynności. Jednocześnie chce, aby dane były bezpieczne w przypadku utraty urządzenia. Tymczasem odpowiednia zaawansowana biometria jest jeszcze dopiero przed nami.

3. Rozwiązania klasy MDM (Mobile Device Management) dotyczą tylko problemów związanych z bezpieczeństwem urządzeń, aplikacji i danych firmowych. Nie mają dobrego zastosowania do ochrony danych prywatnych ani w sytuacji, gdy

urządzenie jest używane zarówno do celów prywatnych, jak służbowych. Warto też odnotować, że nie ma zbyt dobrego rynku zbytu w Polsce na tego typu usługi, bo niewiele podmiotów jest skłonnych płacić dodatkowo za tego typu usługi.

4. Operator nie może wiele zrobić, aby pomóc rozwiązać opisane wyżej problemy. Obecnie sprowadza się to do oferty na rozwiązania MDM czy typu personal security suite. Operator nie ma możliwości wzięcia na siebie odpowiedzialności za bezpieczeństwo aplikacji mobilnych i klientów. W Polsce dane przetwarzane przez operatorów pochodzą z sieci i mają dobrą ochronę prawną wynikającą zarówno z Ustawy o ochronie danych osobowych, jak i z Prawa telekomunikacyjnego. Znacznie większym problemem są aplikacje mobilne sprzedawane w ramach ekosystemów Android/iOS/Windows, ponieważ ich umowy licencyjne są niezrozumiałe, rzadko kiedy bazują na gruncie prawa polskiego i nie ma żadnej kontroli nad tym, jak dane pozyskane przez te aplikacje są wykorzystywane.

Stolik: Procesy obsługi incydentów (SIH)
Prowadzenie: Janusz Nawrat, Raiffeisen Bank

1. Potrzebna jest skuteczna komunikacja i wymiana informacji na temat IH wewnątrz samej organizacji, jak również pomiędzy instytucjami na rynku.
2. Niezbędna jest edukacja kadry zarządzającej.
3. To nie może się udać bez pracy nad zbudowaniem właściwego języka komunikacji.
4. Trzeba dążyć do centralizacji IH w organizacji – to droga do doskonalenia tego procesu.
5. Trzeba udrożnić komunikację z operatorami telekomunikacyjnymi (na przeszkodzie mogą stać ograniczenia prawne).
6. Doświadczenie uczy, że lepiej budować lokalne kompetencje w zakresie IH, niż zdawać się na pełen outsourcing w tym zakresie.

Stolik: Czarny rynek usług – czyli czy można kupić DDoS, APT
Prowadzenie: Marcin Kobyliński, ISSA Polska

1. Problemem jest brak wystarczającego zaufania i współpracy pomiędzy firmami, także w obszarze wymiany wiedzy.
2. W Polsce brakuje dobrego huba informacyjnego, choć tę rolę mógłby/powinien pełnić CERT.
3. Nie ma dobrego feedbacku ze strony CERT-u dla zgłaszających ataki.
4. Czy można i czy powinno się stosować strategię typu „bite back", czyli kontrataktować?
5. US Services/Verisign/DDoS: Revert to verstion, EU Level.

Stolik: Cyberatak w jednostce administracji publicznej – i co dalej?

Prowadzenie: Maciej Gajewski, Podkarpacki Urząd Wojewódzki, Marcin Olender, Ministerstwo Administracji i Cyfryzacji

1. Każdy (walczy) sam, brak wsparcia z CERT.GOV – wnioskowanie o pomoc nic nie daje. Brak koordynacji i systemowych rozwiązań, które są potrzebne.
2. Konieczne są zmiany na poziomie ustawowym, aby je wymusić nie tylko na administracji rządowej, ale i samorządowej. Także w zakresie infrastruktury krytycznej.
3. MAIC powinno przyjąć rolę przewodnią, wziąć odpowiedzialność i skonsolidować różne, rozbieżne rozwiązania.
4. Potrzebne są czytelne wytyczne i standardy dostosowane do danego odbiorcy, w zależności od rodzaju administracji.
5. Popularyzować należy standardy międzynarodowe (konieczne tłumaczenia).

Stolik: Bezpieczeństwo sieci APT w dobie zagrożeń APT

Prowadzenie: Wojciech Dworakowski, OWASP/Securing

1. Obecnie nie jesteśmy w stanie skutecznie chronić stacji roboczych (bo użytkownicy przeglądają internet, korzystają z portów USB, wpinają komputery do obcych sieci).
2. Idealnie „czysta stacja robocza" to mrzonka.
3. Powinniśmy skupić się na ochronie systemów kluczowych.
4. Nie należy chronić systemów tylko dane!
5. Monitorowanie i wykrywanie anomalii – to sprawdza się w małej w sieci, w dużej przetwarzanie real time ogromnych ilości informacji to problem i duże koszty.
6. Segmentacja sieci jest kosztowna, ale można wykorzystać różne inne projekty do tego, by podpiąć do nich pewne elementy bezpieczeństwa (oczywiście tam, gdzie to ma uzasadnienie).
7. By myśleć o skutecznych działaniach przeciw APT, najpierw trzeba sklasyfikować zasoby informacyjne w firmie.

EVENTION

CZAS ZAANGAŻOWANY

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