Informator o ochronie teleinformatycznej

CIP focus

RCB Rządowe Centrum Bezpieczeństwa

www.rcb.gov.pl Sierpień 2016 nr 10

DUŻA AWARIA ENERGETYCZNA W TURCJI

Ponad połowa tureckich prowincji, w których mieszka 40 mln ludzi (włączając to Ankarę i Istambuł) była odcięta od prądu przez połowę doby 31 marca tego roku. Spekulacje dotyczące przyczyny tak poważnej awarii mówią o celowym cyberataku ze strony Iranu. Iran jest znany z tego, że niezwykle intensywnie rozbudowuje swoje zdolności defensywne i ofensywne w dziedzinie cyberbezpieczeństwa. Stało się tak po doświadczeniach z 2010 roku związanych ze słynnym Stuxnetem - wirusem, który zaatakował irański program atomowy poprzez atak na jedną z ważnych instalacji elektrowni atomowej.

http://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/

NOWA STRATEGIA CYBERBEZPIECZEŃSTWA USA

Nową strategię cyberbezpieczeństwa ogłosił w kwietniu na uniwersytecie w Stanford Sekretarz Obrony USA. Wg komentatorów jest to pierwszy tego typu dokument, który w sposób otwarty mówi o możliwości użycia przez USA sił cybernetycznych w potencjalnych konfliktach. Jest to zasadnicza różnica wobec pierwszej wersji dokumentu z 2011 roku, który koncentrował się na opisie zadań obronnych. Nowa strategia określa trzy ważne zasady działania: (1) DoD musi bronić swoich własnych sieci, systemów i informacji, (2) DoD musi być przygotowany do obrony Stanów Zjednoczonych i ich interesów przed cyberatakami o znaczących konsekwencjach, (3) Jeśli zdecyduje o tym Szef Sekretariatu Obrony, DoD musi być gotowy do przeprowadzenia działań o charakterze cybernetycznym, wspierających operacje militarne i plany ciągłości działania.

http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Powstaje Polska Obywatelska Cyberarmia. O jej koncepcji czytaj na s. 8

NOWY RAPORT ICS-CERT

Amerykański CERT sektorowy dla infrastruktury krytycznej opublikował nowy raport, podsumowujący 2014 rok (de facto rok fiskalny tj. X'2013 - IX'2014). W tym okresie odnotowano 245 ataków skierowanych na urządzenia klasy ICS (Industrial Control Systems). Najczęściej atakowanymi sektorami była energetyka i kluczowa produkcja (Critical Manufacturing). Zdaniem autorów raportu, jedną z przyczyn łatwej identyfikacji urządzeń ICS w sieci jest popularność wyszukiwarek internetowych i umiejętność zadawania odpowiednich zapytań, np: w wyszukiwarce Google, a tym bardziej w wyszukiwarce Shodan. Raport oprócz danych na temat bezpieczeństwa sektora, bardzo dobrze pokazuje zakres działania CERT-u sektorowego.

http://darkmatters.norsecorp.com/2015/03/13/industrial-control-systems-attacked–245-times-in–2014/

ATAK NA REAKTOR ATOMOWY NA PŁW. KOREAŃSKIM

Korea Południowa oskarżyła sąsiada z północy o atak na operatora reaktora atomowego w grudniu 2014 roku. Jak łatwo się domyślić Pjongjang odrzuca oskarżenia. Z infrastruktury operatora wyciekły istotne dokumenty, w tym wyniki przeprowadzanych testów. Ustalenie sprawcy oparte było między innymi o analizę technik i kodów użytych w ataku, które zdaniem Koreańczyków z południa używane były już wcześniej przez cyberprzestępców z Korei Północnej. Dane z włamania publikowane były między innymi na Twiterze. Kolejne napięcie związane z konfliktem w cyberprzestrzeni skłania Seul coraz bardziej do stworzenia specjalnego zespołu, który miałby zajmować się tego typu sprawami. Zapewne chodzi o tematykę infrastruktury krytycznej, gdyż jak wiadomo w Korei Południowej działa już duża struktura reagowania na incydenty - KrCERT/CC (http://eng.krcert.or.kr/main/main.jsp)

http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317

W numerze:

ROZMOWA Z **DARIUSZEM ŁYDZIŃSKIM** – SPECJALISTĄ DS. BEZPIECZEŃSTWA, PRACUJĄCYM NAD TWORZENIEM ZESPOŁU DS. REAGOWANIA NA PRZYPADKI NARUSZENIA BEZPIECZEŃSTWA W GRUPIE ENERGA.

Eksperckie podejście do bezpieczeństwa

Dlaczego obszary ICT i OT w sektorze energetycznym należy traktować jako strategiczne dla Państwa?

Informacja i umiejętność jej pozyskiwania to kluczowe elementy warunkujące sukces w prowadzeniu biznesu i utrzymania konkurencyjności na rynku.

Dzisiejszy obraz cyberprzestrzeni wskazuje na konieczność traktowania obszaru ICT i OT w sektorze energetycznym jako jednego ze strategicznych z punktu widzenia obronności kraju. Wskazują na to dwie podstawowe przesłanki. Pierwsza to fakt, że technologia ICT jest kluczowym komponentem infrastruktury krytycznej państwa, np. jest wykorzystywana do zarządzania sieciami energetycznymi, zaś cyberatak na infrastrukturę krytyczną może automatycznie wprowadzić w stan poważnego zagrożenia bezpieczeństwo funkcjonowania państwa. Drugą przesłanką jest znaczenie, jakie zyskują technologie ICT w każdej sytuacji konfliktowej.

Czyli jest to obszar szczególny?

Sektor energetyczny jest specyficznym obszarem gospodarki, który charakteryzuje się koniecznością zapewnienia niezawodności w wytwarzaniu i przesyłaniu energii. W energetyce stosowane są dwa rodzaje systemów: informatyczne (ICT – ang. *Information and Communication Technologies*) oraz sterowania przemysłowego (OT – ang. **Operational Technology**). Ta część infrastruktury, która dotyczy usług dla obywateli, korzysta przede wszystkim z rozwiązań ICT. Pojęcie ICT w energetyce jest szerokie i obejmuje różnego rodzaju aplikacje, od zarządzania biznesem energetycznym (IT) do aplikacji związanych z techniczną kontrolą operacji sieciowych. Natomiast wszystkie procesy technologiczne wykorzystują systemy sterowania przemysłowego.

A jak wygląda to z punktu bezpieczeństwa tych systemów?

Operatorzy na całym świecie pilnują/dbają, aby komputery odpowiedzialne za sterowanie pracą elektrowni (OT) nie były połączone ani z internetem, ani z siecią biurową (ICT). Powodem takiego działania są obawy związane z integracją tych systemów, np. eskalacja ataku na systemy SCADA *(*ang. **Supervisory Control And Data Acquisition***)* poprzez np. luki w zabezpieczeniach stron internetowych lub bezpośrednio w systemach operacyjnych i aplikacjach udostępnianych do obsługi klientów. Strony te, systemy i aplikacje powszechnie uważane są za podatne na coraz częstsze ataki hakerów.

Systemy SCADA zaprojektowane do wieloletniego działania, nie uwzględniały w swoim schemacie bezpieczeństwa sieciowego. Z drugiej strony, informacje o pracy urządzeń siłowni muszą być okresowo przenoszone na inne komputery (biurowe), wtedy połączenie jest konieczne, ale musi być bardzo dobrze szyfrowane i kontrolowane.

Dodatkowo pomiędzy systemami SCADA a korporacyjnymi systemami informatycznymi często istnieje połączenie, powstałe w wyniku wprowadzenia zmian w zarządzaniu informacjami. Wynika ono z potrzeby zdalnego dostępu do systemu – umożliwienie administratorom systemu SCADA jego nadzorowanie i sterowanie nim z punktów dostępu znajdujących się w sieci korporacyjnej. Często również tworzono łącza pomiędzy systemami korporacyjnymi a systemami SCADA w celu umożliwienia kierownictwu natychmiastowego dostępu do danych związanych ze stanem systemów eksploatacyjnych.

Wynika z tego, że nie jesteśmy w stanie całkowicie wyizolować systemów SCADA?

Systemy SCADA są włączane do infrastruktury, której przez wzgląd na oczekiwania biznesowe nie da się w pełni odizolować od środowisk publicznych. Stają się częścią infrastruktur działających w oparciu o protokół IP. Taka ewolucja usprawnia działanie oraz zarządzanie systemami przemysłowymi, a jednocześnie eksponuje je na zagrożenia, ponieważ z uwagi na dotychczas zakładany, wyizolowany charakter systemów przemysłowych, kwestia ich bezpieczeństwa nie była uznawana dotychczas za priorytetową. Dlatego też, nie stosowano zbyt często w nich łatek systemowych ani aktualizacji, które mogłyby zakłócić ich pracę, a co z pewnością wpływało na poziom bezpieczeństwa systemów. Wraz z utratą autonomiczności, jaką gwarantowało odseparowanie ich od sieci, systemy te stały się w takim samym stopniu narażone na ataki cyberprzestępców, jak systemy korporacyjne.

Jaki kierunek należy przyjąć, aby zwiększyć bezpieczeństwo systemów OT?

Organizacje korzystające z systemów SCADA powinny uznać je za ogólną część swojej struktury IT oraz stosować te same środki i techniki bezpieczeństwa, jakie stosowane są w odniesieniu do wewnętrznej infrastruktury IT. Systemy SCADA wymagają zabezpieczenia przed programami typu malware i atakami w taki sam sposób, jak pozostałe elementy infrastruktury IT, stosując różnego rodzaju rozwiązania, np.: *Intrusion Detection Systems* (IDS) czy antimalware, które odnoszą się nie tylko do SCADA.
Bezwzględnie zalecane jest używanie wewnętrznych zapór ogniowych i systemów wykrywania włamań, w połączeniu z regułami wymuszającymi stosowanie silnych haseł.

Systemy SCADA przetwarzają duże ilości danych – czy ich izolacja wpływa na możliwości wykorzystania tego potencjału?

Izolowanie technologii informatycznych od systemów automatyki przemysłowej nie daje możliwości wykorzystania potencjału, jaki płynie z rosnącej liczby zbieranych danych w tych systemach. Brak integracji prowadzi również do ograniczenia możliwości wymiany informacjami wewnątrz samej organizacji oraz wykorzystania aplikacji służących do optymalizacji działań operacyjnych. Integracja olbrzymiej liczby danych pochodzących z systemów technologicznych z informacjami o sieci i kliencie, stanowi ogromny potencjał do rozwoju systemów analitycznych w energetyce, w tym systemów zarządzania zdarzeniami. Konwergencja technologii informatycznych i operacyjnych oznacza integrację takich technologii, jak zarządzanie dystrybucją energii czy zarządzanie w czasie rzeczywistym na poziomie sieci przesyłowej i podstacji z systemami IT wspierającymi działanie liczników, procesy biznesowe związane z obsługą klientów, analitykę oraz systemy bilingowe.

Integracja pozwala na osiągnięcie celów związanych z opracowaniem i stworzeniem spójnego, pojedynczego widoku systemów zarządzania informacją w organizacji, który dostarczy danych w odpowiednim formacie do właściwych osób i we właściwym czasie, co usprawni podejmowanie decyzji. Ponadto poprzez integrację możliwe jest przejście do automatyzacji i optymalizacji procesów biznesowych w czasie rzeczywistym, co wymaga dostępu na bieżąco do wszystkich informacji związanych z danym procesem. Niedopuszczalne stają się przestoje wynikające z braku dostępności do danych o problemach.

Integracja systemów umożliwia osiągnięcie także takich korzyści jak: podejmowanie lepszych decyzji, powiązanie obszarów operacyjnych z celami biznesowymi, sprawniejsze raportowanie i spełnianie wymogów prawnych, a także optymalizację procesów operacyjnych, zarządzanie zasobami.

Czy integracja wpływa również na jakość monitorowania tych systemów?

Mając świadomość negatywnych skutków oddziaływania zagrożeń pochodzących ze środowiska zewnętrznego na infrastrukturę krytyczną, należy bezwzględnie ją chronić. Przez ochronę infrastruktury krytycznej należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Dlatego też, bardzo ważną kwestią jest umiejętność monitorowania, w tym przewidywanie zagrożeń i potencjalnych ataków. Analiza czynników, które sprzyjają cyberatakom na systemy technologiczne, pomoże zaplanować strategię ochrony przed tego typu zagrożeniami. Tym bardziej, że stają się one powszechne. Istotne jest, aby istniała możliwość zrozumienia poziomu bezpieczeństwa całej sieci oraz jednoczesnej kontroli użytkownika. Poprzez monitorowanie i analizę tego co dzieje się w sieci, mamy możliwość właściwego zareagowania na zdarzenia sieciowe i podjęcia odpowiednich czynności.

Ataki stają się coraz bardziej wyrafinowane, dlatego też integracja bezpieczeństwa środowisk systemów jest kluczowa dla ich funkcjonowania w sposób, w jaki zostały zaprojektowane. Przewidywanie przyszłego poziomu zagrożeń dla infrastruktury krytycznej jest niezwykle trudne, ponieważ jej elementy są funkcjonalnie zależne, a możliwe scenariusze zagrożeń są praktycznie niepoliczalne. Zespoły bezpieczeństwa organizacji w celu unikania potencjalnych zagrożeń, powinny posiadać możliwość kontroli sieci oraz użytkowników i aplikacji.

Pełne wykorzystanie potencjału systemów SCADA na poziomie zarządzania całą organizacją wymaga zintegrowania infrastruktury przemysłowej z rozwiązaniami wspierającymi procesy biznesowe. Integracja systemów, pomimo iż może być kłopotliwa, zapewnia odpowiednią strategię bezpieczeństwa w sieci oraz obronę przed zagrożeniami.

Stopień skomplikowania infrastruktur teleinformatycznych i sieciowych oraz wyzwania związane z ich organizacją mogą utrudniać właściwe zarządzanie bezpieczeństwem sieci. W jaki sposób można sobie z tym poradzić?

Zdolności do zapewnienia cyberbezpieczeństwa obejmują dysponowanie przygotowanym personelem, procedurami, organizacją, narzędziami i strategią. Kiedy mają miejsce incydenty z zakresu bezpieczeństwa teleinformatycznego, należy reagować szybko i efektywnie. Im szybciej nastąpi rozpoznanie i reakcja na incydent, tym skuteczniej można ograniczać zakres szkód i kosztów przywrócenia normalnej działalności. Dobrym rozwiązaniem będzie utworzenie zespołu CERT, w celu zapewnienia sobie możliwości szybkiego reagowania, a także zapobiegania incydentom w przyszłości.

Stąd pomysł na stworzenie zespołu CERT ENERGA?

GK ENERGA przykłada dużą wagę do bezpieczeństwa teleinformatycznego. Już teraz nasi specjaliści monitorują poziom bezpieczeństwa urządzeń użytkowników naszej sieci, przyjmując zgłoszenia, reagując na zidentyfikowane incydenty bezpieczeństwa i podejmując działania zmierzające do minimalizacji zagrożeń. Ataki na systemy informatyczne, telekomunikacyjne i produkcyjne nie są już przedmiotem zainteresowania wyłącznie specjalistów ds. bezpieczeństwa informacji i IT. Ich konsekwencje są odczuwalne dla zarządów organizacji i innych interesariuszy, w tym także dla klientów. Media bardzo często podają informacje związane z złamaniem zabezpieczeń w organizacjach. W połowie 2014 roku głośno było o akcji grupy hakerskiej wymierzonej w sektor energetyczny. Cyberprzestępcy, na swoje ofiary obrali sobie amerykańskie i europejskie firmy energetyczne z sektora zbrojeniowego, z sektora IT oraz agencje rządowe z co najmniej 23 krajów europejskich (w tym Polski) oraz z Chin i Japonii. Skala prowadzonej operacji obejmowała co najmniej kilka tysięcy potwierdzonych infekcji na całym świecie, w tym również komputerów należących do polskiej cyberprzestrzeni.

W tym momencie zrodził się pomysł utworzenia komórki, która zajmowałaby się koordynacją przeciwdziałań tego typu zagrożeniom. Utworzenie zespołu CERT to znakomity sposób zapewnienia sobie możliwości szybkiego reagowania, a także zapobiegania incydentom w przyszłości. Skala obecnych zagrożeń oraz ich potencjalny wpływ na działalność biznesową wymagają zmiany dotychczasowego spojrzenia na to, co stanowić powinno bezpieczną infrastrukturę IT. Domena teleinformatycznej infrastruktury krytycznej wymaga dobrze zorganizowanego procesu reagowania na incydenty. Praktyka wykazała, że nadzorowanie i sterowanie urządzeniami odpowiedzialnymi za utrzymanie tej infrastruktury narażone są na niemalże wszystkie bezpośrednio przychodzące z sieci internet zagrożenia. Seria poważnych naruszeń bezpieczeństwa w systemach SCADA na całym świecie udowodniła, że problem jest realny, a jego lekceważenie może być wyjątkowo niebezpieczne. Z raportu zespołu CERT.GOV.PL, działającego w Agencji Bezpieczeństwa Wewnętrznego za

2014 r. wynika, że polskie instytucje zostały zaatakowane ponad 5 tysięcy. Zapobieganie tego typu zagrożeniom stanowi obecnie bardzo wysoki dla nas priorytet. Podstawowym celem CERT-ów jest gromadzenie informacji o zagrożeniach, wczesne reagowanie na incydenty w cyberprzestrzeni oraz opracowywanie rozwiązań mających na celu zapobieganie atakom w przyszłości.

Częsty też jest trend, w którym bezpieczeństwo informacji jest traktowane jako problem w zasadzie techniczny i możliwy do rozwiązania poprzez zakup właściwego oprogramowania lub kolejnego urządzenia. Bezpieczeństwo informacji dotyczy tymczasem współpracy ludzi, usług i technologii. Dlatego też, w codziennej pracy nawiązujemy współpracę na szczeblu operacyjnym z krajowymi i międzynarodowymi organizacjami zajmującymi się problematyką bezpieczeństwa IT. W ten sposób powstała idea utworzenia CERT ENERGA. Temat powołania wewnętrznego CERT-u jest kwestią rozważaną przez każdą świadomą bezpieczeństwa teleinformatycznego organizację. Tworzenie tego typu zespołów jest odpowiedzią na pojawianie lub nasilanie się zagrożeń teleinformatycznych, które stanowią dla organizacji realne zagrożenie dla funkcjonowania i spełniania celów biznesowych lub statutowych.

Czy zespoły typu CERT są potrzebne?

Istnienie zespołów takich jak CERT jest koniecznością, gdyż kwestia zagrożeń dla bezpieczeństwa teleinformatycznego staje się coraz poważniejsza. Każda organizacja powinna nie tylko zabezpieczać się przed wystąpieniem zagrożeń z sieci. Powinna również być przygotowana do radzenia sobie w sytuacji, gdy takie zagrożenie mimo wszystko następuje. Internet, który kojarzy nam się z ułatwieniami, jest także środowiskiem aktywnej działalności grup przestępczych. Mamy do czynienia z doskonale zorganizowanymi środowiskami, które stwarzają poważne zagrożenie dla firm i organizacji. W ich skład wchodzą osoby dobrze wykształcone, z dużym doświadczeniem, mające świadomość szkód jakie może przynieść ich działanie i niejednokrotnie czerpiące duże korzyści finansowe z dostępu do cennych danych, zarówno korporacji jak i zwykłych użytkowników. Cyberprzestępczość charakteryzuje się profesjonalizmem i innowacyjnością, a jej sieć ma ogólnoświatowy zasięg. Oddziaływania przez cyberataki mogą być skierowane przeciwko obiektom gospodarczym i użyteczności publicznej za pomocą zainfekowanych systemów sterowania komputerami. Dlatego też, wraz z postępującą cyfryzacją administracja państwowa, podlegające jej instytucje, elementy infrastruktury krytycznej stały się wrażliwe na działania przeprowadzone za pośrednictwem sieci. Cyberprzestrzeń może być skutecznie wykorzystana zarówno do pozyskania pilnie strzeżonych informacji, jak i do zakłócenia prawidłowego działania funkcjonowania organizacji. Zapobieganie tego typu zagrożeniom stanowi obecnie bardzo wysoki priorytet.
Ochrona cyberprzestrzeni stanowi obecnie jeden z podstawowych celów strategicznych w obszarze bezpieczeństwa każdej organizacji. Bardzo ważna jest umiejętność monitorowania, a w tym, przewidywanie zagrożeń i potencjalnych ataków. Należy się zastanowić nad jej bezpieczeństwem, ponieważ z jednej strony zmiany technologiczne ułatwiają i przyśpieszają pracę, z drugiej wywołują dodatkowe ryzyko i możliwości ataku cybernetycznego. Zarówno skala, jak i charakter ataków świadczą o tym, że atakujący, świadomie i z rozmysłem, wykorzystują fakt olbrzymiej współzależności między organizacjami oraz dostępność nowych technologii, a także brak skutecznej kontroli nad ich wykorzystaniem. Ofensywne działania w cyberprzestrzeni stały się skuteczną bronią, tak w rękach przestępców, jak i rządów poszczególnych państw. To, kto lub co jest celem, wyznaczane jest przez interes polityczny oraz finansowy lub ideologię. Tylko działanie proaktywne i zauważalne nakłady finansowe na bezpieczeństwo cyberprzestrzeni pozwolą na skuteczną reakcję w obliczu ataku na infrastrukturę o kluczowym znaczeniu dla bezpieczeństwa państwa. Ważne przy tym jest, aby cyberbezpieczeństwo było rozumiane szeroko, co pozwoli stosować kompleksowe rozwiązania sprowadzające się nie tylko do umacniania rozwiązań IT. Równie ważne jak wprowadzanie najlepszych rozwiązań technicznych jest całościowe spojrzenie na problem i umacnianie wszystkich jego elementów, w tym czynnika ludzkiego. Cyberataki wykorzystują bowiem tak słabości technologiczne jak i błędy ludzkie. Narodowy Program Ochrony Infrastruktury Krytycznej zakłada, że do osiągnięcia celu – jakim jest ciągłe bezpieczeństwo RP w cyberprzestrzeni – niezbędne jest utworzenie ram o charakterze organizacyjno-prawnym, technologicznym i edukacyjnym, które obejmą swoim zakresem administrację publiczną, przedsiębiorców i użytkowników sieci.

Wymiana informacji na temat zagrożeń stała się silną bronią przeciwko potencjalnym atakom. Taką możliwość daje właśnie tworzenie zespołów CERT-owych, zrzeszonych w międzynarodowych organizacjach. Obecność zespołu CERT zorientowanego na wyjaśnianie incydentów pozwala na unikanie kryzysów i wyciąganie wniosków z występujących problemów. Świadomość sytuacyjna dostarczana poprzez wiedzę z istniejących systemów bezpieczeństwa pozwala łatwo określić stan normalności, a każde odchylenie od tego stanu, wywołane nawet przez całkowicie nieznane zagrożenie będzie zauważalne.

Dariusz Łydziński – Od ponad 15 lat zajmuje się zawodowo szeroką problematyką systemów bezpieczeństwa i jakości oraz praktyką utrzymania ciągłości działania, w tym zarządzania ryzykiem. Specjalizuje się w szczególności w rozwiązaniach e-security. Realizował złożone projekty zabezpieczania danych wagi państwowej, obsługując procesy funkcjonowania systemów łączności, a także bezpieczeństwa informacji w kontekście ochrony funkcjonalności wysoce zaawansowanych sieci oraz systemów teleinformatycznych i telekomunikacyjnych. Równolegle z pracą zawodową z zaangażowaniem realizuje projekty z zakresu bezpieczeństwa na rzecz biznesu, jak również na zlecenia administracji publicznej.

ATAK APT

JAKO GENERYCZNY MODEL ATAKU SIECIOWEGO I STRATEGIA OBRONY PRZED NIM

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

W marcu 2011 roku słynna amerykańska firma RSA Security ogłosiła, że była celem ataku cyberprzestępców, którzy skradli jeden z najbardziej cennych zasobów tej firmy związanych z funkcjonowaniem tokenów do generowania jednokrotnych haseł. Zmusiło to firmę do ogłoszenia programu wymiany tokenów na całym świecie. W liście do klientów firmy prezes RSA Security[1] – Art Coviello napisał:

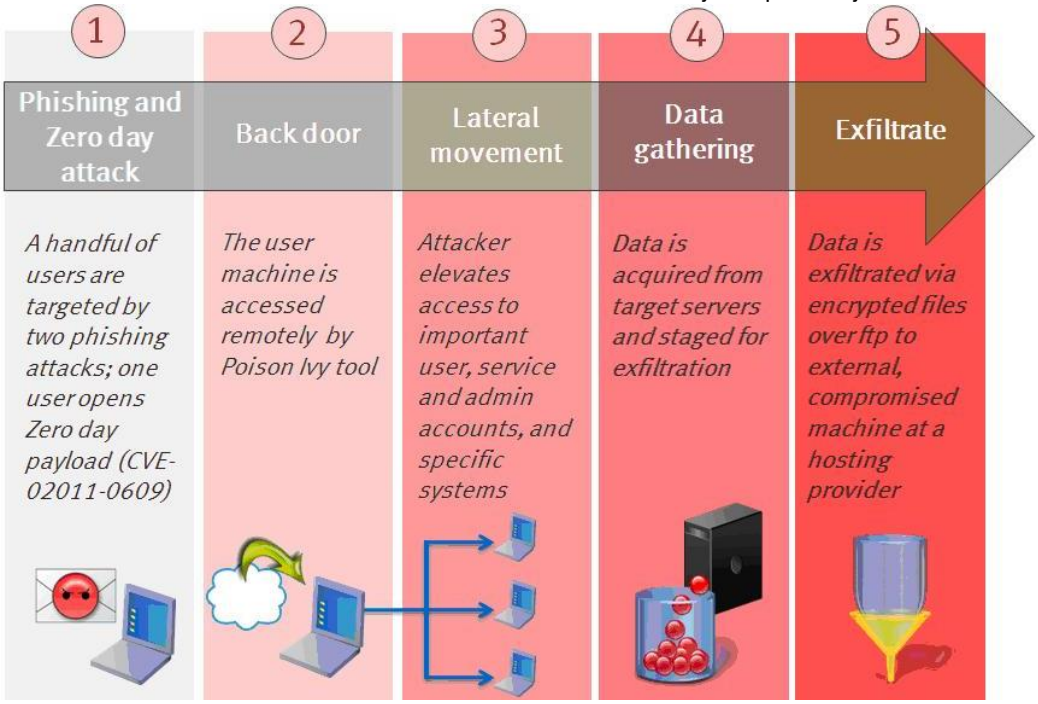
„Nasze śledztwo doprowadziło nas do przekonania, że atak jest z kategorii ataków określanych jako Advanced Persistant Threat (APT)".

Tym samym w świat dyskusji o bezpieczeństwie na dobre został wprowadzony termin APT, a RSA Security śladem wielu dotkniętych porażką przyjęło strategię obrócenia tej porażki w sukces i już po niedługim czasie zaczęło się przedstawić jako dostawca usług i produktów bezpieczeństwa, który jest tym znającym się najlepiej na tego typu atakach.

Napisałem, że termin został wprowadzony do dyskusji, a nie, że powstał nowy rodzaj ataku, ponieważ tak naprawdę model ten przedstawia w całościowym ujęciu właściwie każdy typ ataku.

Oczywiście poszczególne fazy ataku APT "realizowane" są z różną intensywnością, ale nie zmienia to faktu, że występują.

Wróćmy do podstaw. Przyjęło się stosować angielską nazwę dla opisywania ataku APT, choć de facto najczęściej stosuje się po prostu skrót nazwy. To dość uzasadnione, dlatego że nie ma w tym przypadku dobrego tłumaczenia. Najczęściej spotykane to: „zaawansowane uporczywe zagrożenie", ewentualnie „uporczywe" może być zastąpione słowem „uciążliwe" albo „trwałe". Nie zmienia to faktu, że nazwa w wydaniu oryginalnym jest na tyle ugruntowana, że nie ma potrzeby zabiegania o stosowanie polskiego tłumaczenia. To zresztą typowe dla świata bezpieczeństwa teleinformatycznego. Adoptowanie nazw angielskich tworzy „wspólny język", w którym nikt nie musi dociekać czym są przetłumaczone nazwy dla DDoS-a, spamu czy phishingu. Podsumowując w APT mamy do czynienia z atakiem zaawansowanym, który potrafi trwać długo, co określa determinację atakującego i stanowi realne zagrożenie dla atakowanej organizacji. To są oczywiście cechy jakościowe, nadające APT szczególnego znaczenia. Natomiast same fazy mogą równie dobrze być przedstawione w odniesieniu do innych ataków. Przypomnijmy te fazy. W znanych modelach jest ich zazwyczaj od pięciu, tak jak w publikacji RSA Security opisującej wspomniany na początku atak[2], do siedmiu, tak jak w publikacji Lockheed Martin[3], która również

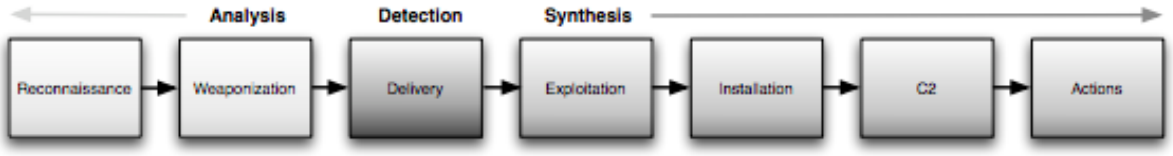


Rysunek 1 - Schemat ataku na RSA Security pokazujący jednocześnie fazy ataku APT (źródło: https://blogs.rsa.com/anatomy-of-an-attack/)

[1] http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex991.htm

[2] https://blogs.rsa.com/anatomy-of-an-attack/

[3] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf



Rysunek 2 - Model ataku APT wg Lockheed Martin, przy okazji pokazujący wczesną fazę wykrycia ataku (źródło: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf)

Niezależnie od tego ile wyodrębnimy faz ataku APT, bardziej ciekawe jest to w jaki sposób poznanie tego modelu może wpłynąć na naszą zdolność do obrony przed nim. Ciekawe pod tym względem staje się wspomniane opracowanie Lockheed Martin, które informuje nie tylko o proponowanych fazach ataku, ale również proponuje schematy zachowań broniącego się, które mają spowodować zerwanie łańcucha ataku (ang. kill the chain). Ma to powstrzymać atak zanim osiągnie on najbardziej destrukcyjny wymiar.

W modelu APT wyróżnione zostały następujące fazy:

- rozpoznanie
- uzbrojenie
- dostarczenie
- włamanie
- instalacja
- kontrola
- akcja

Każda z tych faz może zostać przeanalizowana i broniący się może ustalić jakie podejmie działania. Mogą one przybrać różny charakter. Przede wszystkim może nastąpić **wykrycie ataku**. I nie chodzi tu o to, że odbędzie się to bardzo wcześnie z punktu widzenia faz modelu, chodzi o to, że takie wykrycie może nastąpić w każdej fazie ataku począwszy od prowadzonych przez atakującego działań rozpoznawczych, kończąc na realizacji tego, co przetłumaczyliśmy jako „akcja", a co w praktyce oznacza realizację przez atakującego docelowego zadania, tego najbardziej destrukcyjnego dla zaatakowanej organizacji. Inną metodą powstrzymania ataku może być **odmowa**, kiedy konfiguracja naszego układu teleinformatycznego nie pozwoli na wykonanie przez atakującego zaplanowanego przez niego działania. Następną klasą zachowania obronnego może być **ograniczenie**, czyli sytuacja w której działanie atakującego zostanie wykonane, ale tylko w ograniczonym zakresie. Oprócz tego możemy atakującego **oszukać**, co sprawi, że realizował będzie on swój scenariusz ataku, a my pozostaniemy bezpieczni. Klasycznym przykładem takiej techniki obronnej są honeypoty[4]. Na koniec pozostaje nam również w arsenale obronnym najbardziej agresywna technika, która de facto jest działaniem ofensywnym, czyli **zniszczenie** zasobów atakującego, którymi posługuje się w czasie ataku.

Aby zrozumieć możliwe scenariusze obronne prześledźmy możliwe działania w poszczególnych fazach.

Przykładowo w fazie I-wszej modelu APT (rozpoznanie) możliwe jest rozważenie następujących działań:

Wykrycie działań rozpoznawczych:

- Wykrycie działań rozpoznawczych możliwe jest przez szczegółowe badanie aktywności intruza wobec atakowanych zasobów, np: analiza logów serwera www;
- Wykrycie możliwe jest poprzez współpracę z podmiotami zewnętrznymi częściowo utrzymującymi indywidualne zasoby pracowników atakowanego podmiotu lub zasobów należących bezpośrednio do takiego podmiotu (np: w ramach świadczenia usług outsourcingu serwisów teleinformatycznych, a w szczególności outsourcingu usług bezpieczeństwa);
- Wykrycie możliwe jest poprzez analizowanie zasobów zewnętrznych, w których atakujący potencjalnie może przechowywać wyniki swoich działań rozpoznawczych (np.: serwisy typu pastebin).

Odmowa, utrudnienie i ograniczenie działań rozpoznawczych są zadaniami o podobnym charakterze. W ich realizacji powinny być uwzględniane następujące czynniki:

- Ustalenie priorytetu szybkich działań reakcyjnych wobec działań kontr-rozpoznawczych, prowadzących do identyfikacji intruza. Kwestią decydującą może tu być poziom zagrożenia związany z działaniami rozpoznawczymi wobec atakowanego podmiotu oraz poziom zaawansowania i skuteczności systemu identyfikacji działań rozpoznawczych;
- Możliwość praktycznego zastosowania działań odmownych, utrudniających lub ograniczających, w kontekście ich wpływu na poziom świadczonych usług (np.: nie można blokować całości ruchu http do serwera www, w sytuacji konieczności stałego świadczenia usługi).

Oszukanie działań rozpoznawczych:

- Stałe lub incydentalne (tj. po wykryciu działań rozpoznawczych) prezentowanie fałszywych informacji intruzowi, poprzez: prezentację poszczególnych informacji niezgodnych z rzeczywistością i prowadzących do osłabienia lub eliminacji potencjalnego ataku (dobrym, aczkolwiek zupełnie podstawowym i niezaawansowanym przykładem, jest stosowanie zmian w strukturze adresu email prezentowanego w publicznych serwisach, tak aby nie mógł być on wykorzystany w atakach spamerskich), wystawianie nieprawdziwych usług w oparciu o techniki typu honeypot, co prowadzi do pozyskania błędnej informacji w czasie działań rozpoznawczych, a dodatkowo pozwala na potencjalną identyfikację źródła ataku i stosowanego przez atakującego modus operandi.

Zniszczenie (destrukcja) działań rozpoznawczych:

W tym przypadku bardzo ważne jest aby była pełna świadomość konieczności rozwoju technik i funkcjonalności,

[4] https://pl.wikipedia.org/wiki/Honeypot

które są zgodne z obowiązującym prawem. Zadania związane w ramach tych czynności mogą być następujące:
- Ofensywna eliminacja źródła działań rozpoznawczych poprzez atak dedykowany na te źródła (w tym również atak typu DDoS);
- Prowadzenie działań instytucjonalnie ograniczających lub eliminujących działania rozpoznawcze, np.: poprzez współpracę z operatorem telekomunikacyjnym.

	WYKRYCIE	ODMOWA	UTRUDNIENIE	OGRANICZENIE	OSZUKANIE	ZNISZCZENIE
REKONESANS		ACL FW			HONEYPOT	
UZBROJENIE	NIDS	NIPS				
DOSTAWA			AV SANDBOX			
WŁAMANIE	HIDS	HIPS		SEGREGACJA SIECIOWA		
INSTALACJA		KOTROLA REJESTRÓW				
KONTROLA		LISTY REPUTACYJNE			SINKHOLING	
AKCJA	DLP	DLP				KONTRATAK SIECIOWY

Rysunek 3 - przykładowe techniki obronne w poszczególnych fazach APT i odpowiednich klasach zachowań obronnych

Jeśli spojrzymy w zaproponowany sposób na atak sieciowy, to okaże się, że jest cały wachlarz działań obronnych, które możemy podjąć. Ujmując rzecz ilościowo – do momentu przeprowadzenia przez atakującego ostatecznej, najbardziej destrukcyjnej akcji, mamy aż 42 różne sposoby na działania obronne. Oczywiście w poszczególnych fazach APT możliwość ich użycia jest czasami ograniczona, np.: trudno wyobrazić sobie działania kontrofensywne w pierwszej fazie ataku, tj. w rozpoznaniu. Nie zmienia to faktu, że w konfrontacji z atakującym nie stoimy na straconej pozycji. Trzeba jednak swoje działania poprzedzić dobrą analizą tego co i w jaki sposób warto robić, aby efektywnie wykorzystać zasoby przeznaczone na obronę.

Powstaje Polska Obywatelska Cyberarmia

Kolejny krok w kierunku realizacji inicjatywy wykonany

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Koncepcja wykorzystania wiedzy i doświadczenia specjalistów z zakresu cyberbezpieczeństwa w narodowym systemie obronnym pojawiała się już wcześniej na łamach CIIP focusa. W numerze 8-mym, z listopada 2014 roku, opisywałem jak ten pomysł realizowany jest w kilku krajach. Jakie są jego zalety i jak wyglądają różne modele. W artykule również pojawiło się następujące zdanie: "Wydaje się, że w Polsce projekt powołania ochotniczej cyberarmii mógłby zakończyć się pełnym sukcesem."

W ostatnim czasie zrobiliśmy pierwszy krok i trzeba przyznać, że jak na razie weryfikacja tego twierdzenia idzie w pozytywnym kierunku.

Fundacja Bezpieczna Cyberprzestrzeń zorganizowała w czasie ostatniej konferencji CONFidence cały blok tematyczny poświęcony pomysłowi powołania do życia Polskiej Cyberarmii Ochotników. Pierwszego dnia wystąpił nasz gość z Łotwy, który opowiedział jak pomysł jest realizowany w ich kraju. Prezentację przedstawiającą powstanie i działalność Cyber Defence Unit, działającego w ramach National Guard of Latvia, wygłosił dowodzący tą formacją - Gatis GRAUDIŅŠ. Była to jednak tylko przygrywka do zasadniczego punktu programu, który miał miejsce drugiego dnia konferencji. Ponad dwugodzinny blok tematyczny poświęcony polskiej inicjatywie składał się z dwóch pozycji - przedstawieniu samej koncepcji przez Tomasza Chlebowskiego i Mirosława Maja z Fundacji Bezpieczna Cyberprzestrzeń, a później do dyskusji w roli panelistów dołączyli wspomniany już Gatis GRAUDIŅŠ z Łotwy i Wojciech Dworakowski z polskiego oddziału OWASP. W debacie bardzo ważną rolę odegrali również uczestnicy sesji. Większość czasu to właśnie oni dzielili się swoimi przemyśleniami, pomysłami i opiniami. Również krytycznymi i sceptycznymi. Przeważały jednak głosy, opowiadające się za powołaniem cyberarmii i wykonaniu kilku oczywistych kroków, które staną się kołem zamachowym dla całej inicjatywy.

Główne założenia koncepcji

Zanim przedstawiliśmy pierwszą propozycję funkcjonowania Polskiej Cyberarmii Ochotników przejrzeliśmy szczegółowo doświadczenia wiodących w tego typu przedsięwzięciach krajów. Przeanalizowaliśmy koncepcje ze Stanów Zjednoczonych, Wielkiej Brytanii, Estonii i Łotwy. Założenia, które umieszczone są w tym artykule zawierają również spostrzeżenia i postulaty, które pojawiły się w czasie wspomnianej dyskusji na CONFidence.

Naszym celem jest powołanie stowarzyszenia, które dzięki wiedzy i doświadczeniom swoich członków stworzy potencjał do wykorzystania przez polskie struktury odpowiedzialne za bezpieczeństwo teleinformatyczne. Członkowie stowarzyszenia zadeklarują swoje wsparcie dla Państwa Polskiego w sytuacji zagrożenia.

Jest kilka obszarów, które już teraz - na początku inicjatywy - muszą być ustalone. Jednym z nich są **zasady rekrutacji**. Planujemy rekrutację ekspertów w zakresie cyberbezpieczeństwa spośród najbardziej kompetentnych środowisk w Polsce i zagranicą (oczywiście dotyczy to tylko obywateli polskich przebywających zagranicą). Zakładamy, że aby przystąpić do cyberarmii należy mieć polskie obywatelstwo, być osobą pełnoletnią, niekaralną. Niewykluczone, że konieczne będzie przejście podstawowych testów osobowościowych. Bardzo ważna przy wstąpieniu będzie deklaracja wkładu pracy. Na przykład na Łotwie można zadeklarować, że w ciągu roku poświęci się minimum 4 godziny na przeprowadzenie szkoleń, z których mogą korzystać inni wolontariusze. Chcemy podobne zadania postawić przed uczestnikami polskiej inicjatywy. Zakładamy również że członkostwo w cyberarmii jest na warunkach opt-in - opt-out. Tzn. w każdym momencie można do cyberarmii przystąpić, rzecz jasna po spełnieniu warunków, i w każdym momencie z niego wystąpić.

Cyberarmia, oprócz zagospodarowania specjalistów z najwyższej półki, będzie również szansą dla młodych fascynatów cyberbezpieczeństwa, którzy będą chcieli podnosić swoje kwalifikacje. Nie wykluczamy jednak zastosowania chociażby podstawowego testu kompetencyjnego. W wyniku dyskusji doszliśmy również do wniosku, że nie powinniśmy tylko i wyłącznie postawić na czyste kompetencje techniczne. Dlatego zakładamy możliwość przystąpienia do inicjatywy specjalistów z innych obszarów - np.: prawników czy specjalistów od socjotechniki.

Nie trudno odgadnąć, że przynajmniej dla realizacji części zadań konieczne będzie posiadanie dopuszczenia do przetwarzania informacji niejawnych. Dlatego jeśli kandydat nie posiada uprawnień, będzie musiał zadeklarować gotowość do przejścia postępowania sprawdzającego.

Kolejnym zagadnieniem jest **kwestia podległości i struktury organizacyjnej**. Powołaliśmy Stowarzyszenie–POC, czyli "Polska Obywatelska Cyberarmia". W tej chwili, zgodnie z art. 45 Prawa o Stowarzyszeniach, zakres działalności Stowarzyszenia uzgadniany jest z Ministrem Obrony Narodowej, gdyż planowana działalność POC bezpośrednio związana jest z obronnością państwa.

Oczywiście jednym z głównych zadań jest współpraca z instytucjami rządowymi. Naturalnymi partnerami są: MON,

ABW, MAiC i RCB. Te instytucje wykonują dziś zadania w polskim systemie cyberbezpieczeństwa i liczymy na to, że uda się wypracować najlepszy model wykorzystania potencjału cyberarmii. Oczywiście szczególne istotne będzie omówienie zadań związanych z udziałem członków cyberarmii w sytuacjach realnych zdarzeń naruszających cyberbezpieczeństwo RP. W takiej sytuacji nie może być miejsca na jakiekolwiek nieskoordynowane działanie. To zresztą jest jednym z głównych celów inicjatywy - skoordynowane wsparcie dla komórek rządowych w sytuacji kryzysu w cyberprzestrzeni.

Liczebność organizacji będzie dostosowana po potrzeb i zadań. Zapewne najważniejsze jest to jakie **praktyczne zadania** będą postawione przed Cyberarmią. Tak jak wspomnieliśmy wcześniej - część z nich będzie ustalona z innymi podmiotami, niemniej jednak kilka jest dość oczywistych. Zakładamy, że powstaną grupy tematyczne, które będą zdolne do rozwijania kompetencji w ważnych obszarach cyberbezpieczeństwa, takich jak: bezpieczeństwo sieciowe, analiza złośliwego oprogramowania, czy analizy typu forensic. POC powinna prowadzić działania edukacyjne jak również korzystać ze szkoleń zewnętrznych. Z pewnością jednym z ważnych punktów jej działalności powinno być uczestnictwo w różnych ćwiczeniach, np: takich jak Cyber Europe czy Locked Shield, organizowanych przez agencję ENISA i NATO. Zadania powinny być tak sformułowane, aby dawały szansę na stały rozwój kompetencji, a uczestnictwo w nich prowadziło do możliwości utrzymania swojego statusu członka cyberarmii.

Oczywiście przy realizacji jakiegokolwiek przedsięwzięcia powinno powstać założenie dotyczące jego **budżetu**. Nie chcemy tworzyć iluzji, że coś może skutecznie działać za darmo, aczkolwiek zgodnie z zasadą wolontariatu, bardzo dużo będziemy mogli osiągnąć właśnie dzięki wkładowi pracy na zasadach ochotniczych. Zakładamy, że członkowie cyberarmii nie będą pobierali stałego wynagrodzenia. Zakładamy, że będzie możliwe wsparcie budżetem pozwalającym na realizację zadań związanych z prowadzeniem wybranych, ustalonych z ośrodkiem rządowym projektów. Chcemy również aby członkowie mogli korzystać z budżetu przeznaczonego na edukację, na przykład poprzez udział w wybranych konferencjach i szkoleniach. Również działania administracyjne i reprezentacja inicjatywy będzie wymagać pewnych środków, np: na Łotwie w Cyber Defence Unit zatrudnionych są cztery osoby odpowiedzialne za jego funkcjonowanie.

Następne kroki

Wiele zasad funkcjonowania cyberarmii jest już ustalonych. Niemniej jednak czeka nas jeszcze dużo pracy związanej z dopracowaniem koncepcji. Bardzo pomocnym materiałem w realizacji tego zadania będą wnioski z dyskusji, która miała miejsce w czasie konferencji CONFidence.

W tej chwili zgłaszają się do nas kolejni zainteresowani wsparciem inicjatywy, którzy wstępnie deklarują przystąpienie do niej. Mamy już kilkunastoosobową grupę gotową do dalszych działań. Formalna inauguracja działalności cyberarmii nastąpi 16 września tego roku w czasie Konferencji Security Case Study 2015, organizowanej przez Fundację Bezpieczna Cyberprzestrzeń. Inauguracji towarzyszyć będzie dyskusja z przedstawicielami sektora rządowego i prywatnego, która ma nas przybliżyć do uruchomienia jak najbardziej efektywnych, konkretnych działań. Serdecznie zapraszamy do udziału w tej inauguracji, jak również do samego zgłaszania się do inicjatywy. Można to robić przesyłając deklarację zainteresowania na adres kontakt@cybsecurity.org. Ten adres może posłużyć również do przekazania nam swoich uwag, również tych krytycznych, i propozycji dotyczących funkcjonowania inicjatywy. Serdecznie zapraszamy do dzielenia się z nami swoimi opiniami, a przede wszystkim do włączenia się w samą inicjatywę Polskiej Obywatelskiej Cyberarmii.

Bezpieczeństwo w polskiej sieci Internet
na podstawie raportu
CERT Orange Polska

Michał Rosiak

Jest źle. A będzie jeszcze gorzej. Cyberprzestępcy nie odpuszczą i będą wpadać na coraz to nowe pomysły na okradanie nas z pieniędzy i wrażliwych danych, a firm – ze wszystkiego co ma jakąkolwiek wartość dla nich lub dla ich konkurencji. Takie wnioski można wysnuć z lektury Raportu CERT Orange Polska za 2014 rok. Na pewno nie oznacza to jednak, że pozostało nam tylko powyłączać komputery, opróżnić serwerownie i przenieść się do pustelni w Bieszczadach!

Miliardy zdarzeń miesięcznie, regularne kampanie phishingowe, exploitowane coraz to nowe podatności, ponad sto tysięcy alertów DDoS w ciągu roku – te liczby pokazują, że w dzisiejszych czasach dostawca usług internetowych, nawet niewielki, bez dedykowanego zespołu bezpieczeństwa nie ma racji bytu. Takie wnioski można wysnuć z lektury Raportu CERT Orange Polska za 2014 rok. Wyjątkowo dokładnie (to gratka dla osób z wiedzą techniczną, zainteresowanych tematyką złośliwego oprogramowania) zanalizowane w załącznikach raportu przypadki malware'u dowodzą, że znaczna część tego typu ataków skupia się na usługach e-bankowości. W każdym przypadku cyberprzestępcy wykorzystywali do ataków socjotechnikę, coraz częściej przygotowując maile pod kątem polskich użytkowników. Liczba ataków z załącznikami udającymi faktury za rzekomo wykonane usługi lawinowo rośnie i ta sytuacja długo nie ulegnie zmianie. Między innymi jeden z przypadków tego typu ataków, bardziej szczegółowo opisany w Raporcie CERT Orange Polska był głównym impulsem do zmiany formy faktur wysyłanych do naszych Klientów i wzmocnienia zabezpieczeń domeny wysyłkowej.

DDoS za kieszonkowe

Chciałbyś przeszkodzić w prowadzeniu biznesu firmie, która Ci ostatnio podpadła? Dostałeś już kieszonkowe i masz chwilę wolnego po lekcjach, a chcesz wygrać rozgrywkę on-line ze swoim kolegą? Nic prostszego! Parę chwil szukania, kilkanaście dolarów i w efekcie nawet rozgarnięty gimnazjalista może postawić przed specjalistami IT swojej ofiary twardy orzech do zgryzienia lub zablokować możliwość korzystania z sieci Internet dowolnemu użytkownikowi. 900 Mbps – średnia wartość ataku DDoS zaobserwowanego w 2014 roku przez CERT Orange Polska – wystarczy bez problemu do zablokowania znacznej części średniej wielkości serwisów, zaś z największym (ponad 90 Gpbs) nie poradziłyby sobie nawet duże serwisy. Co więcej – ataki są coraz krótsze, co paradoksalnie powoduje, że stają się groźniejsze. Powodem jest fakt, że w znacznej część platform, służących ochronie przed DDoS od stwierdzenia wystąpienia ataku do faktycznego uruchomienia jego mitygacji może minąć kilka minut. W tym czasie napastnik zdąży już zakończyć atak, by po jakimś czasie uderzyć – znów na krótko – po raz kolejny. Orange Polska dysponuje możliwością rozproszenia dużych ataków wolumetrycznych, dzięki rozbudowanej infrastrukturze oraz możliwości odfiltrowania klas adresowych potwierdzonych jako źródła ataku. Statystyki i trendy wskazują, że liczba i siła ataków DDoS będą regularnie rosnąć, tym bardziej, iż cyberprzestępcy coraz częściej wykorzystują błędy w konfiguracji serwerów (np. synchronizacji czasu), pozwalające na skierowanie w stronę ofiary ataku większego nawet o kilkaset razy od inicjującego go pakietu!

Życie przerasta Hollywood

Malware ukierunkowany na ataki APT (Advanced Persistent Threat) – z tym wektorem ataku w opinii FireEye, jednego z partnerów Raportu CERT Orange Polska, będziemy spotykać się coraz częściej. Celami tego typu ataków bardzo często jest administracja rządowa, tak jak w przypadku opisywanych APT Kaba (obecnych w sieci już od 2007 roku!), które okazały się być ukierunkowane na gromadzenie danych związanych z polityką i obronnością z krajów Europy Zachodniej, ale również Kaukazu i Gruzji. Obserwując aktywność przestępców sponsorowanych przez państwa, niebawem można spodziewać się wzrostu ataków APT bazujących na złośliwym oprogramowaniu, które do niedawna mogłoby kojarzyć się raczej z hollywoodzkimi produkcjami. Po wykonaniu zadania będą potrafiły same się zniszczyć, a nawet... tak się zamaskować, by zrzucić odpowiedzialność za wyciek danych np. na bogu ducha winnych pracowników ofiary.

Po pierwsze – przejrzystość

Luty 2014 nie będzie miło wspominanym miesiącem przez zespoły ds. bezpieczeństwa IT dostawców internetu. Wtedy bowiem doszło do jednego z największych ataków na polskich internautów. Dotyczył wszystkich operatorów telekomunikacyjnych, a w samej sieci Orange Polska wykorzystywał podatność w popularnym oprogramowaniu ok. 100 tysięcy routerów klienckich do obsługi szerokopasmowego internetu. Pozwalał cyberprzestępcom na zalogowanie się na domowym urządzeniu i w efekcie na dostęp do całego ruchu wychodzącego z domowej sieci. Taka sytuacja stwarzała im olbrzymie pole do popisu, jednak w tym przypadku chodziło o kradzież danych dostępowych do systemów bankowości elektronicznej za pośrednictwem podstawionych serwerów DNS, wpisanych do przejętych routerów. Akcja przygotowana była pod kątem internautów z naszego kraju, bowiem fałszywe DNS prowadziły do podstawionych, łudząco przypominających prawdziwe, witryn polskich banków. Przeciwdziałanie Orange Polska opisane jako studium przypadku w raporcie dowiodło, że w podobnych sytuacjach najlepszą kontrakcją jest pełna przejrzystość działań. Po publikacji informacji dotyczących ataku za pośrednictwem mediów dotarła ona do wielu internautów, motywując ich do sprawdzenia stanu bezpieczeństwa własnych urządzeń, co być może uratowało ich przed stratą oszczędności całego życia.

Internet otwartych drzwi

Jesteśmy atakowani, bo sami się o to prosimy – to niestety kolejna konkluzja, dotycząca stanu polskiego, a zapewne i światowego, internetu. Nawet gdy pamiętamy o zasadach tak podstawowych jak choćby używanie bezpiecznych haseł, cóż nam z najlepszego zamka, gdy drzwi okazują się być wykonane z dykty... Cyberprzestępcy nie mają czasu i zasobów na atakowanie każdego indywidualnie. Najpierw pracujące za nich automaty szukają otwartych, nieużywanych, podatnych na ataki usług i portów. Tych samych, które bardzo często nieświadomie zostawiamy otwarte. Dzięki tym podatnościom osoby ze złymi zamiarami mogą dostać się do naszego komputera udając oprogramowanie do zdalnej administracji, czy też „zajrzeć" do bazy danych przez niezabezpieczony port dla serwera MS SQL. Najpopularniejsza podatność, stwierdzona przez CERT Orange Polska (21 procent całości) to Directory Listing, która pozwala na zajrzenie do dowolnego katalogu na serwerze docelowym, np. /etc/passwd/, zawierającego hasła dostępu poszczególnych użytkowników. Dalszy krok to już drobny problem – statystyki publikowane regularnie po większych wyciekach danych na świecie wskazują, że ponad połowę (niekiedy nawet do 80 procent) haseł da się złamać w ciągu kilku minut! A jeśli cyberprzestępca chce wykraść strategiczne dane z firmowej sieci, nie musi włamywać się do komputerów menedżerów, często wystarczy jeden niefrasobliwy zwykły użytkownik.

Nikt nie jest bezpieczny

Jeszcze całkiem niedawno można było usłyszeć opinie fachowców: „Chcesz mieć bezpieczny komputer? Zainstaluj Linuxa, albo jakikolwiek z systemów unixowych". Ta sytuacja od ubiegłego roku zmieniła się niemal o 180 stopni, a eksperci CERT Orange Polska bardzo dokładnie przeanalizowali i opisali w raporcie przyczyny tej zmiany, którymi są podatności Heartbleed, Shellshock i Poodle. Mocno niepokojący jest fakt, że dwie z nich dotyczą szyfrowania transmisji za pośrednictwem protokołu SSL, dzięki czemu osoba niepowołana może odszyfrować przesyłane dane lub nawet włączyć się w ich przesyłanie (atak Man-in-The-Middle), podstawiając własną treść. To z jednej strony dowód na to, że nie można spoczywać na laurach, traktując a priori jako bezpieczne systemy i rozwiązania które przez lata takie się wydawały, z drugiej zaś – zapowiedź wzrostu zainteresowania atakami na systemy serwerowe, bez konieczności wykorzystania zwykłych użytkowników do „otwarcia drzwi". Nie obejdzie się bez regularnych aktualizacji oprogramowania i instalowania łat. W przypadku dużych organizacji warto pamiętać o wielopłaszczyznowym podejściu do kwestii bezpieczeństwa, a także niekorzystaniu ze zbędnych usług i programów, co ograniczy powierzchnię ataku.

Wybuchające bojlery i wściekłe tostery?

Kilka lat temu oglądałem z dziećmi film „Załoga G". Jego bohaterami były świnki morskie, broniące świata przed buntem sterowanych centralnie przez sieć urządzeń (pamiętam wściekłe ekspresy do kawy). Bajka? Niekoniecznie… 10 lat temu wearables też były traktowane jak science fiction, a teraz do internetu podłączmy lodówkę, samochód, liczniki prądu, czujniki obsługujące inteligentny dom i wiele innych rzeczy. Po co się włamywać do tego typu systemów? Dla fraudu, dla dziwnie rozumianej zabawy, czy nawet – a może przede wszystkim – dla szantażu, grożąc np. wybuchem rozgrzanego do białości sterowanego przez sieć bojlera. To nie jest science fiction – takie urządzenia funkcjonują, są niestety dostępne z internetu (co obserwuje również CERT Orange Polska) i bardzo często podatne na cyberataki. I tak jak pozostałe ryzyka – nie zanosi się na to, by to akurat miało w przyszłości maleć.

EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

CYBERSEC

NOWA PLATFORMA STRATEGICZNYCH ROZMÓW O CYBERBEZPIECZEŃSTWIE

Prace nad Dyrektywą NIS, "cyber pierwiastek" konfliktu na Ukrainie, szczyt NATO w Warszawie, podczas którego jednym z priorytetów będzie problematyka cyberbezpieczeństwa, kolejne strategiczne inicjatywy na krajowym i międzynarodowym poziomie - wszystko to pokazuje jak ważnym zagadnieniem z punktu widzenia współczesnych państw i innych podmiotów staje się bezpieczne funkcjonowanie w cyberprzestrzeni. Polska musi stać w pierwszym szeregu państw aktywnych w tym obszarze.

Joanna Świątkowska
Instytut Kościuszki

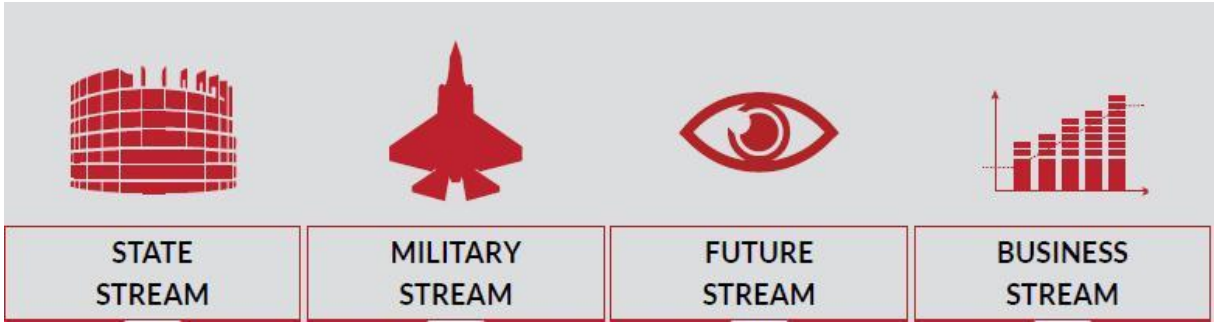
Zapewnienie cyberbezpieczeństwa wiąże się nie tylko z umiejętnościami i wiedzą techniczną. Aktualnie równie istotne i konieczne staje się intensywne prowadzenie odpowiednich działań politycznych na najwyższym szczeblu. Cyberprzestrzeń i kwestie z nią związane na stałe zostały ujęte w planie relacji międzynarodowych i stały się jednym z priorytetów współczesnych państw. Państwa muszą być aktywne w tej sferze, w przeciwnym razie zrezygnują z możliwości zabierania głosu w coraz bardziej kluczowych dyskusjach kształtujących ład międzynarodowy i wpływających na ich wewnętrzne bezpieczeństwo.

Przestrzeń cyfrowa coraz częściej staje się także miejscem prowadzenia konfliktów, które wpisują się w definicję popularnej koncepcji wojny hybrydowej. W okolicznościach gdy bezpieczeństwo państw, ich gospodarek, ale także codzienne funkcjonowanie podmiotów prywatnych i obywateli uzależnione jest od bezpieczeństwa cyberprzestrzeni, nie sposób nie dostrzegać wagi tego problemu.

Polska oraz cały region Europy Środkowej, musi aktywnie brać udział w procesach zmierzających do poprawy bezpieczeństwa cyberprzestrzeni . Nasz region powinien korzystać z doświadczeń i unikać błędów, które popełnili na różnych etapach swojego cyfrowego rozwoju inni światowi gracze. Wiąże się to z koniecznością tworzenia platform umożliwiających współpracę oraz wymianę doświadczeń,

gdzie najważniejsi przedstawiciele sektorów prywatnych i publicznych będą mieli możliwość wspólnego wypracowania rozwiązań na rzecz cyberbezpieczeństwa. Istnieje potrzeba odważnych działań oraz silnej współpracy zarówno na poziomie poszczególnych państw, regionu, Europy ale także w przestrzeni transatlantyckiej. Warunkami koniecznymi dla realizacji tych postulatów są prowadzenie dialogu oraz wzajemne zrozumienie i zaufanie.

Europejskie Forum Cyberbezpieczeństwa (CYBERSEC) to konferencja poświęcona najważniejszym wyzwaniom związanym z funkcjonowaniem w cyberprzestrzeni. Jej pierwsza edycja odbędzie się we wrześniu tego roku w Krakowie, kolejne powtarzane będą cyklicznie co rok. Cztery ścieżki tematyczne: państwo, wojsko, przyszłość i biznes, wypełnione merytorycznymi dyskusjami w różnych formatach, gwarantują kompleksowe potraktowanie kluczowego tematu cyberprzestrzeni. W trakcie dwóch dni obrad i w ramach prac poprzedzających konferencję, najważniejsi interesariusze nie tylko zidentyfikują problemy jakie stoją przed współczesnymi państwami, ale także zaproponują rekomendacje zmierzające do podniesienia poziomu cyberbezpieczeństwa. Wypracowane rozwiązania, szeroko promowane wśród starannie wyselekcjonowanych grup docelowych (takich jak kluczowi decydenci polityczni, eksperci zajmujący się kwestiami bezpieczeństwa, właściciele i operatorzy infrastruktury krytycznej, wojskowi), stanowić będą drogowskaz dla najważniejszych decyzji. Polityczny impuls płynący z obrad ma na celu inspirowanie najlepszych rozwiązań podnoszących bezpieczeństwo całej Europy i ma służyć budowaniu trwałego zaufania i zrozumienia z innymi partnerami.



Rysunek 4. Cztery ścieżki tematyczne Europejskiego Forum Cyberbezpieczeństwa.

W CYBERSEC wezmą udział goście ze Stanów Zjednoczonych oraz Europy – m.in. z Ukrainy - państwa, które znajduje się w środku konfliktu mającego także swoje odzwierciedlenie w cyberprzestrzeni.

Wydarzenie będzie skierowane także do przedstawicieli biznesu – zarówno tego z obszaru IT – oferującego najwyższej klasy rozwiązania, ale także do podmiotów prywatnych głównie z tych sektora obejmującego infrastrukturę krytyczną. CYBERSEC pozwoli im nie tylko zaprezentować podejście do spraw związanych z cyberbezpieczeństwem, ale także uczestniczyć w przekazywaniu najlepszych praktyk i doświadczeń.

Jednym z kluczowych celów będzie także połączenie punktu widzenia podmiotów prywatnych i publicznych w kontekście wdrażanych lub przyszłych rozwiązań regulacyjnych, a także podjęcie dyskusji dotyczącej warunków współpracy prywatno – publicznej.

Konferencja zyskała wsparcie najważniejszych podmiotów odpowiedzialnych za zapewnienie cyberbezpieczeństwa w naszym kraju. Pełna lista patronów znajduje się na stronie internetowej: www.cybersecforum.eu.

Elementem towarzyszącym organizacji Forum będzie wydanie eksperckiego czasopisma poświęconego strategicznym problemom związanym z cyberprzestrzenią. Na jego łamach eksperci prezentować będą rekomendacje i kierunki działań.

Rysunek 5 Etapy prac

Bezpieczeństwo zarówno Polski jak i Europy wymaga budowania stabilnych relacji i trwałej współpracy. CYBERSEC ma za zadanie stworzyć ku temu sprzyjające warunki. Zapraszamy do współpracy wszystkich, którzy zechcieliby zaangażować się w ten proces.

EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA odbędzie się 28-29 września 2015 r. w Krakowie. Więcej informacji o wydarzeniu: www.cybersecforum.eu, Twitter: @CYBERSECEU.

FP7 CAMINO roadmap

W niniejszym artykule przedstawiono rezultaty europejskiego projektu CAMINO, którego celem jest dostarczenie wytycznych oraz szczegółowej „mapy drogowej" działań badawczo-rozwojowych (tzw. *research agenda*) w dziedzinie przeciwdziałania cyberprzestępczości oraz cyberterroryzmowi. W artykule przedstawiono najważniejsze aspekty ujęte we wstępnej mapie drogowej projektu CAMINO, będące wynikiem analizy obecnych zagrożeń, wyzwań oraz potrzeb związanych z walką z cyberprzestępczością.

Damian Puchalski, Michał Choraś
ITTI Sp. z o.o.

Projekt FP7 CAMINO

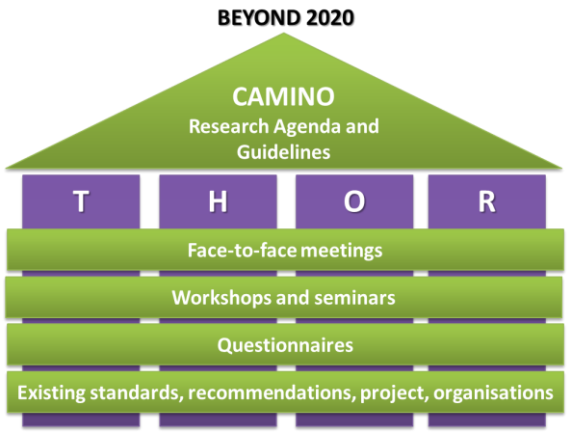
Szybki rozwój technologii komputerowych oraz coraz bardziej dostrzegalny trend stałego połączenia użytkowników z Internetem, włączając w to dostęp do sieci za pomocą różnych urządzeń mobilnych, to znak obecnych czasów. Media społecznościowe, bankowe usługi *on-line*, powszechne wykorzystanie usług typu *cloud* to codzienność. Z jednej strony przynoszą one społeczne i gospodarcze korzyści, z drugiej mogą być jednak źródłem różnego rodzaju zagrożeń ze strony osób i organizacji przestępczych.

Informacje zamieszczane w sieci przez użytkowników i instytucje są łatwe do pozyskania przez osoby o złych intencjach, a następnie wykorzystane w celach przestępczych. Szeroko pojęty dostęp do zasobów sieci jest ułatwieniem nie tylko dla zwykłych użytkowników (społeczeństwa), ale może być także narzędziem cyberprzestępców oraz kanałem propagandowym organizacji terrorystycznych.

Projekt CAMINO – "Comprehensive Approach to cyber roadMap coordINation and development", współfinansowany w ramach Siódmego programu ramowego Unii Europejskiej w zakresie badań i rozwoju technologicznego (7PR) jest odpowiedzią na tego rodzaju zagrożenia. Ma on na celu stworzenie całościowej agendy badawczej w zakresie walki z cyberprzestępczością i cyberterroryzmem oraz zainicjowanie długoterminowych działań w celu zrzeszenia ekspertów i instytucji działających na polu cyberbezpieczeństwa.

Projekt rozpoczął się w kwietniu 2014 r. i będzie trwał do końca marca 2016 r. Konsorcjum projektowe składa się z 10 partnerów (ITTI Sp. z o.o., CBRNE Ltd., CNR, DFRC AG, Espion Ltd., Everis, Uniwersytet w Montpellier, Wyższa Szkoła Policji w Szczytnie, S21sec Lab oraz Sec-Control Finland) pochodzących z 8 krajów (Polska, Irlandia, Wielka Brytania, Finlandia, Hiszpania, Francja, Szwajcaria, Włochy) oraz dodatkowo około 20 członków wspierających, z różnych europejskich państw. Liderem projektu jest firma ITTI Sp. z o.o. z Poznania. W skład konsorcjum wchodzi jeszcze jedna jednostka z Polski, tj. Wyższa Szkoła Policji w Szczytnie.

Główny celem projektu jest stworzenie szczegółowej „mapy drogowej" działań badawczo-rozwojowych (tzw. *research agenda*) w dziedzinie przeciwdziałania cyberprzestępczości oraz cyberterroryzmowi. Mapa drogowa CAMINO określa główne obszary europejskiej działalności badawczo-rozwojowej, w których należy podjąć pewne działania zmierzające do zwiększenia bezpieczeństwa cybernetycznego w kontekście rosnących zagrożeń związanych z cyberprzestępczością i cyberterroryzmem. Opracowanie mapy drogowej poprzedzone zostało kompleksową analizą istniejących wytycznych, map drogowych i strategii z zakresu cyberbezpieczeństwa, a także wyników zakończonych oraz trwających projektów badawczo-naukowych. W ramach projektu analizowane były aspekty techniczne, ludzkie, organizacyjne i prawne w kontekście walki z cyberprzestępczością i cyberterroryzmem, zgodnie z przyjętą przez Konsorcjum CAMINO koncepcją THOR (Technological, Human, Organisational, Regulatory - rysunek poniżej).



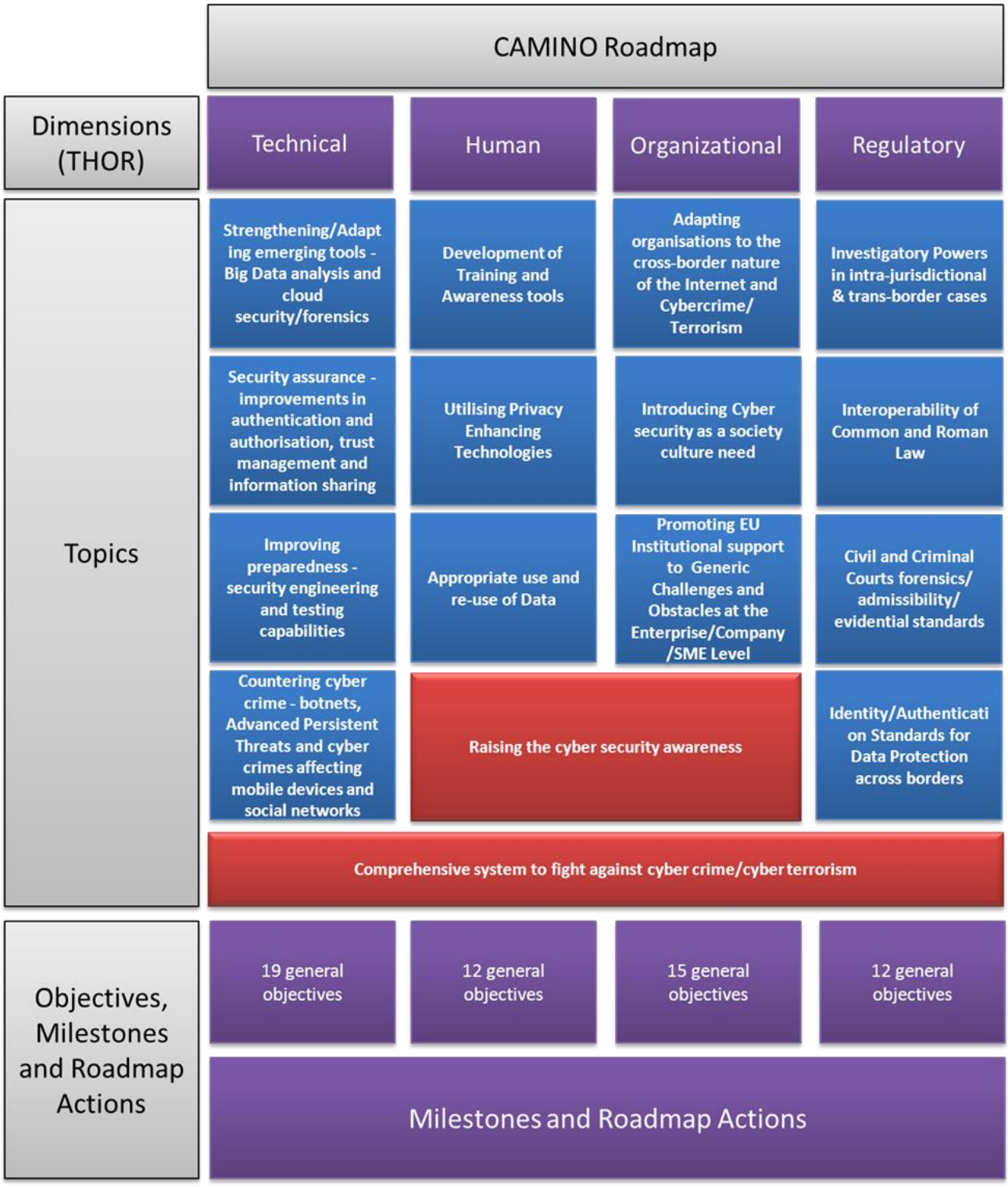
Rysunek 6: Koncepcja THOR projektu CAMINO

„Mapa drogowa" projektu CAMINO

Wstępna wersja "Mapy drogowej" CAMINO jest wynikiem pierwszego roku działań projektu. Dokument ten stworzony

został w oparciu o podejście THOR, w związku z tym jego struktura odpowiada podziałowi na 4 główne obszary badawcze walki z cyberprzestępczością (skupiające się na aspektach technicznych, ludzkich, organizacyjnych oraz prawnych).

Każdy z 4 wymiarów zdefiniowanych w podejściu THOR opisany został w mapie drogowej za pomocą tej samej struktury. W toku wcześniejszych prac i analiz, w projekcie zidentyfikowanych zostało 14 głównych obszarów (*Roadmap topics*). Obszary te, w kontekście struktury mapy drogowej oraz podziału na wymiary THOR, pokazane zostały na kolejnym rysunku.



Rysunek 7: Mapa drogowa CAMINO

Obszary z **wymiaru technicznego** skupiają się na technicznych aspektach związanych z dochodzeniem i informatyką śledczą w sprawach dotyczących cyberprzestępczości, a także na poprawie mechanizmów autoryzacji
i uwierzytelniania, kwestiach inżynierii bezpieczeństwa cybernetycznego oraz testów. Poruszone zostały też kwestie związane z najbardziej istotnymi wyzwaniami walki z cyberprzestępczością, jak np. analiza i przetwarzanie dużych ilości danych (Big data), walka z sieciami botów oraz złośliwym oprogramowaniem, przeciwdziałanie atakom ukierunkowanym (APT). W wymiarze technicznym roadmapy, opracowane zostały także wytyczne dotyczące bezpieczeństwa urządzeń mobilnych oraz sieci społecznościowych.

Wymiar ludzki roadmapy skupia się na potrzebach uregulowania aspektów prywatności danych (np. wykorzystywania danych personalnych), a także na elementach treningu i szkoleń służących podnoszeniu świadomości i wiedzy z zakresu cyberbezpieczeństwa.

Wymiar organizacyjny dokumentu dotyczy głównie kwestii społecznych i kulturowych związanych z zapewnianiem bezpieczeństwa cybernetycznego oraz procesów adaptacyjnych organizacji w świetle internacjonalizacji cyberprzestępczości i cyberterroryzmu. W wymiarze organizacyjnym nie można pominąć także wyzwań związanych z kooperacją pomiędzy organizacjami (np. współpraca organizacji działających w danym sektorze, narażonych na podobne zagrożenia oraz zmagających się z podobnymi wyzwaniami), jak i współpracy na linii sektor prywatny – sektor publiczny, np. wsparcie instytucji rządowych dla przedsiębiorstw.

Aspekty prawne, związane z sądownictwem, interoperacyjnością prawa, informatyką śledczą, a także regulacjami związanymi z ochroną danych w kontekście ich transgranicznej wymiany, są przedmiotem **wymiaru prawnego** mapy drogowej CAMINO.

Dalsze prace w projekcie

W drugim roku działań projektowych, konsorcjum CAMINO postawiło sobie za cel skonkretyzowanie oraz uzupełnienie wstępnej wersji mapy drogowej, a także wspieranie działań związanych z szeroką akceptacją mapy drogowej CAMINO.

Jedną z metod walidacji mapy drogowej CAMINO jest seria zaplanowanych przez konsorcjum warsztatów przeznaczonych dla ekspertów z obszaru cyberbezpieczeństwa oraz służących wymianie informacji i opinii na temat produktów projektu.

Jak dotąd odbyły się 3 warsztaty projektowe: w Bernie (Szwajcaria, wrzesień 2014), w Barcelonie (Hiszpania, marzec 2015) oraz w Montpellier (Francja, kwiecień 2015). Na pozostałą część projektu zaplanowano jeszcze co najmniej 2 warsztaty: w Londynie, 15-16 czerwca 2015 oraz finalne warsztaty w Madrycie (2016 r.).

Innym celem konsorcjum, przewidzianym na najbliższe miesiące są działania zorientowane na budowanie społeczności wokół projektu CAMINO. Projekt od samego początku wspierany był i wywodził się z grupy IMG-S (ang. *Integrated Mission Group for Security*), Thematic Area 7: Cybersecurity (http://img-s.eu). Grupa IMG-S zrzesza przedstawicieli europejskiego przemysłu, małych i średnich przedsiębiorstw, organizacji rządowych, badawczych oraz uniwersytetów i ma na celu ustalanie celów badawczych dla Europy w zakresie bezpieczeństwa oraz wspieranie działań dążących do ich realizacji.

W celu zbudowania społeczności ekspertów powołany zostanie CAMINO think tank, zrzeszający ekspertów z zakresu cyberbezpieczeństwa, działający na zasadzie platformy ułatwiającej wymianę wiedzy i doświadczeń dotyczących cyberbezpieczeństwa, a w szczególności dotyczących zagrożeń związanych z cyberprzestępczością i cyberterroryzmem.

Więcej informacji na temat projektu FP7 CAMINO dostępnych jest pod adresem: http://www.fp7-camino.eu/home