Informator o ochronie teleinformatycznej

CIIP focus

RCB Rządowe Centrum Bezpieczeństwa

www.rcb.gov.pl Listopad 2014 nr 8

NIST SZYKUJE SIĘ DO BUDOWY ŚRODOWISKA TESTOWEGO DLA BADANIA SYSTEMU KLASY SCADA

Amerykański Narodowy Instytut Standardów i Technologii (NIST) chce podjąć jeszcze bardziej zorganizowane działania na rzecz poprawy bezpieczeństwa systemów SCADA. Instytut chce wybudować zaawansowane środowisko testowe, w którym będzie dokonywać badań poziomu zabezpieczeń systemów. Autorzy projektu doskonale zdają sobie sprawę, że systemy sterowania przemysłowego, nawet te w skali mikro czyli określane mianem Internetu Rzeczy (Internet of Things), są obecnie bardzo dynamicznym procesie rozwoju i konieczne jest wprowadzenie systemowego sposobu badania ich bezpieczeństwa i ograniczania ryzyka używania.
http://www.theregister.co.uk/2014/08/12/nist_wants_better_scada_security/

REKOMENDACJE FRANCUSKIEGO SEKTORA PUBLICZNO-PRYWATNEGO

Od 2013 roku przedstawiciele francuskiego sektora prywatnego i publicznego, w tym francuskiej agencji bezpieczeństwa systemów teleinformatycznych - ANSSI, pracowali, w ramach wspólnie powołanej grupy roboczej, nad zestawem rekomendacji dla ochrony infrastruktury krytycznej. W rezultacie tych prac powstały dwa dokumenty. Pierwszy z nich opisuje metody klasyfikacji systemów zarządzania infrastrukturą krytyczną i metody jej ochrony. Drugi zaś z większą dokładnością opisuje sposoby osiągania cyberbezpieczeństwa. Obydwa dokumenty zawierają wiele praktycznych wskazówek i są dostępne na stronie francuskiej agencji rządowej: http://www.ssi.gouv.fr/en/the-anssi/events/anssi-key-measures-to-improve-the-cybersecurity-of-industrial-control-systems.html

NIGERYJSKI BAROMETR BEZPIECZEŃSTWA

Raport, który ma być składową poprawy bezpieczeństwa teleinformatycznego w Nigerii, został wydany przez Wolf Pack, Digital Jews i wsparty przez Brytyjską Wysoką Komisję Nigerii. Raport opisuje międzynarodowe inicjatywy związane z cyberbezpieczeństwem, np: Konwencję Budapesztańską oraz sprawy bezpieczeństwa w kontekście wielu państw, a przede wszystkim tych stowarzyszonych z BRICKS oraz krajów afrykańskich. W opracowaniu można również znaleźć informacje na temat ważnych ataków sieciowych, które dotknęły państwa afrykańskie.
http://www.wolfpackrisk.com/2014_Nigerian_Cyber_Threat_Barometer_(Med_Res).pdf

EDUKACJA I WSPÓŁPRACA

Wywiad z Andrzejem Halickim, Ministrem Administracji i Cyfryzacji odpowiadającym za e-administrację i sprawy społeczeństwa cyfrowego – czytaj na s. 12

LOKALIZACJA URZĄDZEŃ W DOMENIE .EDU

W poprzednim numerze biuletynu CIIP focus opisywaliśmy funkcjonowanie projektu SHODAN. Dobrym uzupełnieniem tego materiału jest informacja dotycząca tego jak lokalizować systemy klasy ICS (Industrial Control System) i SCADA w sieciach domeny „.edu". Materiał opublikowany w serwisie tripwire.com jest dobrym dokumentem wspomagającym zespoły bezpieczeństwa pracujące w obszarze tej domeny. Mogą one posłużyć do opracowania całościowego materiału związanego z zabezpieczeniem urządzeń.
http://www.tripwire.com/state-of-security/government/locating-scada-and-ics-systems-on-edu-networks-with-shodan/

TECHNICZNA ANALIZA ATAKU LIGHTSOUT

Serwis zscaler.com opublikował wynik technicznej analizy ataku, który dotknął firmy sektora energetycznego na początku tego roku. Dzięki analizie możliwe jest zapoznanie się z modus operandi sprawców ataku. Autorzy opisują też szczegółowe działanie kluczowych modułów technicznych wykorzystanych w ataku oraz przytaczają fragmenty kodu związane z tymi atakami: http://research.zscaler.com/2014/03/lightsout-ek-targets-energy-sector.html

W numerze:

Zachęcamy do kontaktu z Redakcją, zgłaszania pomysłów artykułów, tematów, wywiadów: ***ciip-focus@rcb.gov.pl***

DRAGONFLY

Dragonfly to grupa hackerska, której działania wymierzone są w szereg firm, głównie z sektora energetycznego. Działania te obejmują następujące po sobie kampanie szpiegostwa komputerowego, które umożliwiają atakującym uzyskanie dostępu do wielu krytycznych segmentów sieci, odpowiedzialnych za sterowanie procesami przemysłowymi. Grupie Dragonfly udało się przełamać zabezpieczenia wielu ważnych firm i jeżeli grupa wykorzystałaby możliwości sabotażu (do których niewątpliwie uzyskała dostęp), mogłoby to spowodować awarie lub przerwy w dostawie energii w zaatakowanych krajach.

Marcin Siedlarz
Symantec

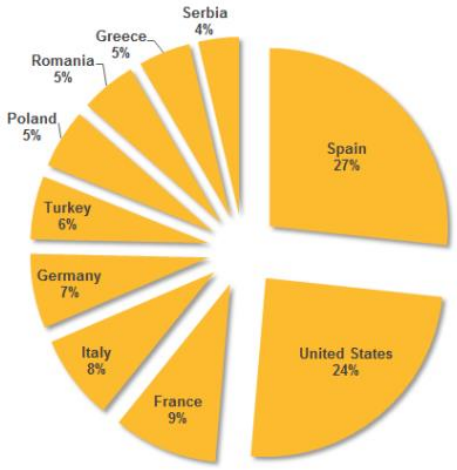
Celami grupy Dragonfly byli m.in. operatorzy sieci przesyłowych, elektrownie, operatorzy gazo i ropociągów producenci urządzeń SCADA/ICS. Do głównych krajów będących w zainteresowaniu grupy należą: Stany Zjednoczone, Hiszpania, Francja, Włochy, Niemcy, Turcja oraz Polska.

Dragonfly to dobrze zorganizowana grupa, która posługuje się specjalnie przygotowanym na swoje potrzeby złośliwym oprogramowaniem oraz jest zdolna do wykonywania ataków za pomocą różnych wektorów, z których najbardziej precyzyjny to umieszczenie malware'u w aktualizacjach oprogramowania wykorzystywanego do zdalnego dostępu do sieci przemysłowych oraz sterownikach urządzeń ICS/SCADA. W ten sposób firmy używające tego oprogramowania i urządzeń, podczas aktualizacji oprogramowania infekowały stacje robocze wykorzystywane przez własnych inżynierów do zdalnego dostępu do sieci ICS/SCADA. Dostęp do komputerów zarządzających sieciami przemysłowymi dał atakującym możliwość zmiany parametrów pracy urządzeń oraz ich wyłączenia. Innymi wektorami ataku były wiadomości email zawierające zainfekowane załączniki PDF oraz umieszczanie kodu złośliwego w źródłach stron internetowych o tematyce energetycznej. Grupa używa dwóch rodzajów backdoor'a, rozpoznawanego przez silniki antywirusowe jako Backdoor.Oldrea oraz Trojan.Karagany. Oldrea została najprawdopodobniej napisana przez członków grupy lub na ich zamówienie. W celu infekowania stron internetowych użyto exploit kita o dość podstawowych możliwościach (lecz również używanego jedynie przez grupę Dragonfly) – Lightsout Exploit Kit.

Kontekst

Grupa Dragonfly, znana również jako 'Energetic Bear' najprawdopodobniej rozpoczęła swoje działania w końcu roku 2011. W swoich początkowych kampaniach atakowała firmy związane z sektorem obronnym oraz lotniczym w Stanach Zjednoczonych oraz Kanadzie, aby w roku 2013 przenieść swoje zainteresowanie na branżę energetyczną zarówno w Ameryce Północnej jak i Europie. Rok 2013 przyniósł znaczny wzrost aktywności grupy wraz z uruchomieniem kampanii wysyłania złośliwych załączników PDF do pracowników firm z branży energetycznej. W późniejszych miesiącach Dragonfly uruchomiło kolejną kampanię infekowania stron internetowych exploit kitem Lightstout oraz jego drugiej wersji znanej również jako Hello Exploit Kit. Druga połowa roku 2013 oraz początek roku 2014 to nowe podejście do atakowania firm energetycznych. Być może w wyniku nieudanych operacji przy pomocy poczty elektronicznej oraz złośliwych stron internetowych, które miały prowadzić do uzyskania dostępu do określonych zasobów, atakujący przeprowadzili skuteczną kampanię podmiany plików aktualizacji oprogramowania i sterowników ICS/SCADA na stronach internetowych czterech producentów. Jest to jeden z przykładów ataku na łańcuch dostaw, gdy z różnych powodów nie jest możliwa skuteczna penetracja docelowej infrastruktury i w celu infekcji atakujący używa oprogramowania lub usług strony trzeciej, której produkty są używane w docelowej infrastrukturze (Jednym z najbardziej spektakularnych ataków na łańcuch dostaw, było przełamanie zabezpieczeń firmy Bit9 i wprowadzenie oprogramowania złośliwego na whitelistę produktu oferowanego przez Bit9 firmom z branży obronnej w USA).

Dragonfly nosi znamiona grupy sponsorowanej przez państwo, która posiada duże zdolności techniczne nie tylko do wykonywania ataków komputerowych, ale także do działań następujących po udanym włamaniu. Należy pamiętać, iż udana infekcja to tylko początek działań, a grupa Dragonfly ma w swoim wachlarzu oprogramowania złośliwego wiele modułów, które służą różnym celom: wykradaniu określonych plików, enumeracji środowiska sieciowego w poszukiwaniu serwerów OPC (OLE for process control – otwarty standard komunikacyjny stosowany w automatyce przemysłowej. Jest dostarczycielem danych z urządzeń sterujących i nadzorujących proces technologiczny). Na podstawie informacji o ilości wykradzionych danych z komputerów zainfekowanych przez Backdoor.Oldrea stworzono wykres najczęściej atakowanych państw:



Głównym motywem działania jest szpiegostwo komputerowe z potencjalną możliwością wykonywania ataków sabotażowych jako drugorzędnym celem działania grupy. Analiza czasów kompilacji próbek oprogramowania złośliwego wskazuje, iż grupa wykonuje swoje działania od poniedziałku do piątku, najczęściej w godzinach 9am-6pm w strefie czasowej UTC+4. Może to świadczyć o tym, że grupa pochodzi z jednego z krajów Europy Wschodniej.

Oprogramowanie złośliwe

Dragonfly używa dwóch rodzajów malware'u. Backdoor.Oldrea po udanej infekcji zbiera informacje o systemie operacyjnym, zainstalowanych programach, listą plików, dyskach twardych i sieciowych, ustawieniach BIOSu i wysyła za pomocą żądania HTTP do serwera C&C. Dodatkowo jeden z modułów Oldrea kopiuje informacje ze skrzynki adresowej Outlook'a oraz konfigurację jednego z klientów VPN używanego do zdalnej administracji urządzeniami PLC i zapisuje je w tymczasowym pliku, używając szyfrowania asymetrycznego. W kolejnych żądaniach HTTP zawartość tego pliku jest zapisywana na serwerze C&C. Oldrea może również pobierać dodatkowy malware z serwera C&C w postaci plików wykonywalnych lub binarnego szellkodu. Serwery C&C backdoor'a Oldrea są hostowane na przejętych przez grupę stronach internetowych. Większość z tych witryn pracuje w oparciu o CMS'y Wordpress i Joomla. Panel kontrolny backdoor'a Oldrea ma prosty interfejs i pozwala atakującym na pobranie wytransferowanych plików oraz umieszczenie dodatkowych modułów, które w późniejszym czasie będą uruchamiane na zainfekowanych komputerach.

Trojan.Karagany w przeciwieństwie do backdoor'a Oldrea był dostępny na czarnym rynku oprogramowania złośliwego. Kod źródłowy pierwszej wersji trojana Karagany wyciekł do sieci w roku 2010 i prawdopodobnie został zmodyfikowany przez Dragonfly do własnych celów. Do funkcjonalności trojana Karagany należy wykradanie plików oraz pobieranie i uruchamianie dodatkowego oprogramowania złośliwego. Karagany posiada również możliwość uruchamiania dodatkowych pluginów, które służą między innymi do wykradania haseł, wykonywania zrzutów ekranu oraz przeszukiwania dokumentów pod kątem zadanych parametrów.

Backdoor.Oldrea został użyty w większości udanych ataków przez grupę Dragonfly. Karagany stanowi jedynie 5% zarejestrowanych infekcji.

Wektory ataku

Grupa Dragonfly używa co najmniej trzech wektorów ataków. Pierwszy z nich, to przesyłanie zainfekowanych załączników poczty elektronicznej do inżynierów i menedżerów z firm energetycznych. Wiadomości używały niezbyt wyrafinowanych tematów takich jak „The Account" lub „Settlement of delivery problem". Wszystkie wiadomości były wysłane z jednego konta w domenie gmail.com. Kampania mailowa rozpoczęła się w lutym 2013 roku i trwała do czerwca. Liczba wiadomości wysłanych do poszczególnych firm wahała się od 1 do 84.

W maju 2013 roku rozpoczęła się kampania infekowania stron internetowych kodem exploit kita Lightsout. Atakujący celowo wybrali strony internetowe związane z branżą energetyczną, zwiększając tym samym szansę udanych infekcji w tej branży. W źródle każdej z przejętych stron internetowych umieszczono ramkę prowadzącą do zewnętrznej (również zhakowanej) strony, z której przy każdej wizycie pobierany i uruchamiany był kod mający na celu zainfekowanie użytkownika backdoor'em Oldrea bądź trojanem Karagany. Exploit kit Lightsout wykorzystuje w tym celu podatności w Internet Explorer oraz Java. We wrześniu 2013 roku, grupa Dragonfly uaktualniła wersję exploit kita, nazywanego również Hello exploit kit. Nowa wersja zawierała udoskonalone mechanizmy rozpoznawania typu systemu operacyjnego użytkownika odwiedzającego zainfekowaną stronę. Po zidentyfikowaniu pluginów w przeglądarce oraz enumeracji czcionek zainstalowanych w systemie, użytkownik był przekierowywany do kolejnej strony, na której umieszczony był dedykowany kod w zależności od rodzaju pluginów i systemu.

Brak jest informacji i dowodów, aby grupa Dragonfly używała eksploitów 0-day w trakcie wykonywanych ataków, jednak w roku 2012 po ujawnieniu jednej z podatności w Javie, Dragonfly w ciągu kilku dni umieścił kod wykorzystujący tę podatność w pierwszej wersji exploit kita Lightsout. Świadczyć to może o umiarkowanych zdolnościach atakujących do tworzenia eksploitów na podstawie ogólnie dostępnych informacji.

Najbardziej ciekawym i skutecznym wektorem ataku były jednak zatrojanowane uaktualnienia oprogramowania ICS/SCADA. Atakujący przejęli kontrolę nad witrynami co najmniej czterech firm oferujących oprogramowanie do kontroli sieci przemysłowych i umieścili backdoor Oldrea w dostępnych z Internetu plikach z aktualizacjami. Zidentyfikowano m.in. zawierające trojan oprogramowanie dwóch producentów używane do nawiązywania połączenia VPN z siecią przemysłową w celu konfiguracji urządzeń PLC, w tym przypadku grupa Dragonfly mogła uzyskać informacje konieczne do zdalnego dostępu do tych urządzeń i ich rekonfiguracji. Szacunkowe dane świadczą o tym, iż w przypadku pierwszej z firm, oprogramowanie mogło zostać pobrane około 250 razy pod koniec stycznia 2014 roku, natomiast w przypadku drugiej firmy plik był dostępny do pobrania przez około 10 dni w kwietniu 2014 roku, natomiast liczba pobrań nie jest znana.

Kolejnym zidentyfikowanym przypadkiem był zatrojanowany sterownik kamery 3D używanej w procesach pomiaru objętości lub systemach kontroli dostępu. Plik dostępny był na stronie internetowej producenta przez około 6 tygodni na przełomie czerwca i lipca 2013 roku. Był to też pierwszy z serii czterech ataków na łańcuch dostaw wykonany przez grupę Dragonfly.

Podsumowanie

Dragonfly jest grupą hackerską działającą najprawdopodobniej z terenu jednego z krajów Wschodniej Europy. W swoich działaniach ewoluowała przez szereg lat począwszy od roku 2011 dostosowując wektory ataku do swoich potrzeb oraz rozwijając narzędzia używane do kontroli zainfekowanych komputerów w sieciach firm energetycznych. Dragonfly koncentruje się na długoterminowym dostępie do zasobów atakowanych firm w celu wykradania informacji przemysłowych oraz potencjalnie w celu budowania możliwości wykonywania ataków sabotażowych. Z pewnością w szeregach grupy znajdują się specjaliści od systemów ICS/SCADA, których doradztwo jest niezbędne w procesie przygotowania oprogramowania złośliwego (można tu wymienić chociażby moduł backdoor'a Oldrea, którego zadaniem była enumeracja serwerów OPC w sieci LAN) oraz w czasie tzw. „post-exploitation", czyli działań wykonywanych po udanej infekcji tj. oceny wartości zasobów, do których uzyskano dostęp i ich odpowiedniej kontroli w dłuższej perspektywie.

Grupa posiada spore umiejętności w kontekście przełamywania zabezpieczeń stron internetowych. W okresie swojej działalności z powodzeniem umieszczała złośliwy kod na stronach należących do branży energetycznej, w tym dokonała co najmniej czterech podmian plików wykonywalnych, które stanowiły aktualizacje oprogramowania ICS/SCADA.

W ostatnim okresie aktywność grupy Dragonfly zmniejszyła się, co jest najprawdopodobniej efektem wielu publikacji na ten temat. Nie ulega jednak wątpliwości, że w przyszłości jeszcze usłyszymy na temat tej grupy, energetyka stanowi bowiem ważny element w kreowaniu światowej polityki, stąd też zapotrzebowanie na dedykowany zespół szpiegostwa komputerowego w tej branży.

Działania najróżniejszych haktywistów na stałe wpisały się w obraz cyberkonfliktów. Warto spojrzeć na realne działania w cyberprzestrzeni i ewentualne zagrożenia dla sektora, którego dotyczą - czyli w tym wypadku sektora teleinformatycznej infrastruktury krytycznej.

Operacja #OpPetrol

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Wygląda na to, że operacja #OpPetrol wpisała się na stałe w kalendarz działań haktywistów. 2014 rok był drugim z kolei, w czasie którego sieciowi aktywiści skierowali swoje działania przeciwko wszystkim, których oni sami uważają za odpowiedzialnych za stworzenie systemu światowego handlu ropą naftową, w ich opinii niesprawiedliwego dla świata arabskiego. Dlaczego organizują tę operację? Jak możemy przeczytać w ich manifeście: " (…) ponieważ walutą, którą się rozlicza handel ropą jest dolar i Arabia Saudyjska zdradziła muzułmanów" (http://pastebin.com/ucWDRAih). Zdaniem organizatorów operacji, ropa powinna być sprzedawana w walucie kraju, który ją eksportuje. Ogólnie rzecz biorąc, organizatorom nie podobało się, że zasoby Bliskiego Wschodu są kradzione przez państwa zachodnie. Manifest zawiera jeszcze wiele informacji o poglądach politycznych i światopoglądowych jej organizatorów, ale nie to jest tematem tego artykułu.

#OpPetrol 2014 była zaplanowana na czerwiec tego roku. Atakujący na celownik wzięli firmy i organizacje w bardzo wielu krajach. Z regionu Zatoki Perskiej były to: Kuwejt, Oman, Katar, Arabia Saudyjska (w tym wypadku skoncentrowali się na atakach na instytucje rządowe). Akcja dotyczyła również Stanów Zjednoczonych, ale również innych krajów, które są światowymi, ekonomicznymi potęgami: Chiny, Wielka Brytania, Izrael, Niemcy. Co ciekawe atak skierowano również na zasoby teleinformatyczne w krajach bloku BRIC (Brazylia, Rosja, Indie i Chiny), które przecież przez wielu są postrzegane jako konkurencja i przeciwwaga dla tradycyjnych potęg ekonomicznych.

Jeśli chodzi o listę konkretnych zaatakowanych zasobów, to można ja podzielić na dwie wyraźne grupy. Pierwsza z nich zawiera firmy z omawianego sektora, tj. przemysłu związanego z wydobyciem, przetwarzaniem i handlem ropą naftową, natomiast druga, to setki "bezimiennych" serwisów, które posłużyły jako dźwignia propagandowa, do rozpowszechniania treści manifestu operacji.

Oczywiście nie ma dokładnej informacji na temat tego, kto był sprawcą operacji. Autorzy cyberprzestrzępczych działań przedstawiali się jako członkowie najróżniejszych grup haktywistów, a najczęściej pojawiającymi się podpisami pod działaniami w sieci, na przykład podmianami stron www, były podpisy "#Anonymous" i "AnonGh0st". Na datę operacji wyznaczyli oni 20 czerwca 2014 roku, aczkolwiek plan zakładał wiele akcji przygotowawczych, które miały miejsce wcześniej. Akcje przygotowawcze polegały głównie namasowym przejmowaniu kontroli nad stronami internetowymi i umieszczenie na nich treści propagandowych. Przed rozpoczęciem zasadniczej operacji w ten sposób dokonano ataku na ponad 400 stron internetowych. Trzeba też przyznać, że właściwie ta metoda stała się podstawową techniką całej operacji. Mimo tego, że mówimy o akcji skierowanej na sektor infrastruktury krytycznej, to w jej trakcie nie doszło do żadnych poważnych incydentów wystawiających na krytyczne zagrożenie firmy i organizacje z tego sektora. Nie mieliśmy tu do czynienia z działaniami, które występowały przy okazji serii ataków na kraje arabskie, związanych na przykład z działaniem wirusa Shamoon, a już na pewno zagrożeń mających miejsce przy okazji działania wirusa Stuxnet, które przecież bardzo realnie zagroziły irańskiej elektrowni atomowej (o wspomnianych wirusach i innych cyberatakach skierowanych na państwa Bliskiego Wschodu pisaliśmy w poprzednich numerach Biuletynu "CIIP focus").

Haktywiści swój manifest umieścili w znanym portalu, będącym repozytorium działań sieciowych informatyków, również hakerów czy czyberprzestępców - w portalu pastebin.com. Natomiast o swojej działalności głównie informowali poprzez serwis twitter.com. Mimo, że podmiana stron internetowych, bazująca na słabości zainstalowanych na serwerach web-aplikacji, była najbardziej powszechnym sposobem cyberataku, to w czasie jego trwania używano innych metod atakowania. Ich lista zawiera co najmniej kilka pozycji, na której znajdują się i takie, które potencjalnie mogły być zarzewiem bardzo niebezpiecznego ataku:
- DDoS (Distributed Denial of Service), czyli atak prowadzący do blokady serwisu sieciowego,
- ataki spear-phishing, polegające na wysyłaniu dedykowanych maili phishingowych do pracowników atakowanych organizacji i w rezultacie próba przejęcia ich komputerów,
- bezpośrednie włamania do komputerów, głównie korzystając z tego, że nie były one odpowiednio „załatane".

Haktywiści, aby zwiększyć swoją „siłę rażenia" zdecydowali się również na udostępnienie kilku programów, które były używane przez zwolenników akcji. Cyberprzestępcy udostępnili trzy programy, które były skryptami napisanymi w programie Perl. Jeden z nich służył do przełamywania systemów autoryzacji poprzez ataki typu brute-force, dwa

inne służyły zaś do ataków na bardzo popularne programy do zarządzania serwisami - Joomlę i cPanel.

Tak jak wcześniej było wspomniane - mimo zaatakowania bardzo istotnego sektora jakim jest infrastruktura krytyczna - operacja haktywistów #OpPetrol miała głównie propagandowy charakter, związany z publikacją treści związanej z poglądami jej autorów. Co prawda w trakcie operacji doszło również do ataków, które skutecznie prowadziły do blokady serwisów internetowych oraz przedostawania się do wnętrza organizacji i zapewne wykradania zastrzeżonych informacji, to nieznane są żadne naprawdę ważne i niebezpieczne skutki tych ataków.

Paradoksalnie więc operacja #OpPetrol 2014, właśnie ze względu na brak krytycznych skutków, może zostać potraktowana jako bardzo korzystna z punktu widzenia osiągnięcia celów edukacyjnych. Wystarczy tylko uświadomić sobie fakt, że większość z działań haktywistów mogło być wykorzystane do osiągnięcia znacznie bardziej niebezpiecznych celów. Na przykład techniki takie jak spear-phishing są jedną z podstawowych technik, towarzyszących najpoważniejszym atakom typu APT (Advanced Persistant Threat), a skutki tych ataków potrafią być już bardzo poważne. Świadczą o tym chociażby przypadki z kilku ostatnich miesięcy takie jak atak na amerykańską firmę Target, który skończył się stratą w wysokości 1 biliona dolarów, atak na 300 firm z sektora energetycznego w Norwegii, firmę JPMorgan i kilka innych dużych firm finansowych w Stanach Zjednoczonych, czy historyczny już spektakularny atak sprzed kilku lat na największego dostawcę produktów bezpieczeństwa na świecie - firmę RSA Security, która po ataku rozpoczynającego się od kilku maili wysłanych do pracowników tej firmy, musiała wymienić na całym świecie 40 milionów tokenów do generowania haseł jednorazowych. Łatwo sobie wyobrazić, że koszty takiej operacji były olbrzymie.

Czego więc można nauczyć się analizując przebieg i konsekwencje operacji #OpPetrol. Poniższa lista przedstawia najważniejsze rekomendacje:
- Warto przejrzeć swój system monitoringu zdarzeń sieciowych i wykrywania zagrożeń. Chodzi głównie o systemy klasy IDS (Intrusion Detection System) i IPS (Intrusion Prevention System). Jak dużo generują one sygnałów? Czy nie jest tych sygnałów za dużo, co w praktyce usypia czujności operatorów systemu? Czy mają nowoczesne i aktualne sygnatury i mechanizmy wykrywania zagrożeń? Właściwie te same działania, które są związane z systemami IDS i IPS powinny dotyczyć systemów antywirusowych.
- Istotnym elementem strategii bezpieczeństwa teleinformatycznego jest warstwowe podejście do ochrony zasobów teleinformatycznych. Dostęp do nich powinien być limitowany zgodnie z zasadą "need to know", co ograniczy skutecznie zaatakowanie najpoważniejszych zasobów firmy, nawet po przełamaniu przez napastnika pierwszych linii obrony. Przy tej okazji warto również przejrzeć przydział praw administracyjnych na kluczowych urządzeniach i sprawdzić czy nie są nadużywane prawa administracyjne w tych systemach.
- Ciągłe monitorowanie stanu bezpieczeństwa serwisów wystawionych na zewnątrz organizacji, takich jak serwisy WWW czy poczta elektroniczna. Są one bowiem celem pierwszych ataków i przedmiotem wielu „badań" poszukiwaczy dziur w systemach, co powoduje dostępność skutecznych narzędzi ataku na te serwisy. Właściwie należy też uznać, że niezależny audyt techniczny takich serwisów jest koniecznością. Najlepiej, aby był to audyt cykliczny.
- Przygotowanie technicznej (np.: urządzenia anty-DDoS in-line i serwisy typu scrubbing center) i organizacyjnej (np.: zdolności kompetencyjne) strategii obrony przed atakami typu DDoS. Inwestycje w tę strategię powinny być wprost proporcjonalne do ryzyka jakie wiąże się z brakiem niedostępności bronionych serwisów. Pamiętając też, że cennym zasobem, który trzeba chronić jest reputacja serwisu i zaufanie do organizacji, która go utrzymuje.
- Przygotowanie swoich pracowników na tego typu ataki. Przygotowanie powinno się odbyć w dwóch grupach i omawiać dwie kategorie zagrożeń. Pierwsza grupa obejmująca większość pracowników organizacji, powinna być przeszkolona w kontekście powszechnych zagrożeń związanych z atakami na personel "nieinformatyczny". Mowa tu o działaniach przeciwdziałających przyszłym atakom typu spear-phishing czy drive-by download (przekierowywanie na infekujące serwisy). Warto w czasie takich szkoleń przedstawić techniczne zagrożenia jakie niesie ze sobą dystrybucja spamu i dokonać praktycznego przeglądu ataków socjotechnicznych. Takie szkolenie jeszcze bardziej jest efektywne jeśli towarzyszy mu audyt socjotechniczny. Druga grupa to pracownicy techniczni, odpowiedzialni za ochronę teleinformatyczną. Potrzebują oni zaawansowanej wiedzy i doświadczeń związanych z obroną przed atakami sieciowymi. Praktycznym, atrakcyjnym i efektywnym sposobem szkolenia jest przeprowadzenie ćwiczeń z ochrony w cyberprzestrzeni. Warto wspomnieć, że przeprowadzenie tak skonstruowanego programu szkoleniowego, to jedna z rekomendacji ćwiczeń Cyber-EXE™ Polska 2013, przeprowadzonych w sektorze bankowym.
- Przegląd stanu bezpieczeństwa - technicznego i operacyjnego - w kontaktach z podmiotami trzecimi realizującymi usługi dla organizacji. Może to mieć szczególne znaczenie w sektorze infrastruktury krytycznej, gdzie powszechne jest korzystanie z usług podmiotów trzecich w przypadku działań serwisowych. Pracownicy takich podmiotów bardzo często mają bezpośredni dostęp do serwisowanych urządzeń. Nie zawsze jest on bezpiecznie realizowany, co stwarza olbrzymie ryzyko naruszenia bezpieczeństwa systemu.

To tylko najważniejsze pozycje z zestawu działań ustanawiających lub poprawiających bezpieczeństwo teleinformatyczne w organizacji. Pełna lista jest znacznie dłuższa i powinna stać się wkładem do polityki bezpieczeństwa teleinformatycznego organizacji.

Wydaje się, że takich operacji jak #OpPetrol może być w przyszłości jeszcze więcej, a niektóre z nich mogą przybrać bardzo niebezpieczny charakter. W szczególności jeśli mamy do czynienia ze stałym napięciem politycznym w naszym regionie. Ryzyko takie potwierdzają tego typu zdarzenia towarzyszące innym konfliktom na świecie. Ostatnie krótkie ataki na stronę Prezydenta Rzeczpospolitej i Warszawską Giełdę Papierów Wartościowych są sygnałem, że instytucje państwa polskiego i inne podmioty działające w naszym kraju nie mogą się uważać za nienarażone na takie ataki. Podjęcie odpowiednich działań jest konieczne.

Źródła:
http://www.albawaba.com/business/hacktivists-middle-east-584207
http://www.forbes.com/sites/billconerly/2013/10/25/future-of-the-dollar-as-world-reserve-currency/
http://cdn2.hubspot.net/hub/130265/file-1039260999-pdf/48-Hour_Update_Cimation_Spot_Report_OpPetrol_June_18.pdf?submissionGuid=314a789b-24b7-4460-89c8-931970d3977a

#OpPetrol By AnonGhost Team

Again we back #OpPetrol" on the 20 June 2014 ,this Op is very special because we gonna hit many countries in the same time, especially:

*USA
*CANADA
*ENGLAND
*ISRAEL
*ARABIA SAUDIA (Only Gov)
*CHINA
*ITALY
*FRANCE
*RUSSIA
*GERMANY
*KUWAIT(Only Gov)
*QATAR (Only Gov)

Why this Op ?

Because Petrol is sold with the dollar ($) and Saudi Arabia has betrayed Muslims with their cooperation. So why isn't Petrol sold with the currency of the country which exports it?

Because the Zionists own us like this \!/

Historically, the Currency of Muslims was not the paper money that you know today, it was Gold and Silver.

The new world order installed their own rules so that they can control us like robots.

In the future, there will be no money paper and coins. The NWO are planning, by 2020, to make "Electronic Money" (like credit cards).

SIEM - od potrzeby do wdrożenia

Wdrożenie systemu SIEM jest zwieńczeniem prac nad bezpieczeństwem informatycznym organizacji, wisienką na torcie. Ta analogia pozwala uświadomić sobie skalę prac potrzebnych do wykonania w organizacji przed wdrożeniem SIEM oraz oceny pracochłonności i kosztów tego wdrożenia. By położyć wisienkę na torcie, trzeba najpierw zrobić tort.

Tadeusz Włodarczyk
PSE SA

System SIEM (ang. Security Information Event Management); system informatyczny realizujący funkcje: zbierania informacji o zdarzeniach bezpieczeństwa teleinformatycznego ze wszystkich podłączonych do niego monitorowanych systemów (najczęściej z systemowych dzienników logów lub dedykowanych systemów zarządzania i monitorowania), ich przekształcania do wspólnego formatu i archiwizacji, wyszukiwania w zbudowanej bazie danych informacji o zdarzeniach symptomów wystąpienia zagrożeń lub incydentów (np. poprzez wyszukiwanie zdefiniowanych sekwencji zdarzeń lub powtarzających się zdarzeń niebezpiecznych), a następnie alarmowania o wystąpieniu zdarzeń niebezpiecznych. System SIEM jest najskuteczniejszym narzędziem wspierającym wczesne wykrycie incydentu bezpieczeństwa teleinformatycznego.

Po co SIEM (wisienka)?

Właściwe pytanie, jakie należy zadać sobie przed rozpoczęciem planowania wdrożenia SIEM, brzmi: czy potrzebujemy w organizacji wiedzy o poziomie bezpieczeństwa przetwarzanych w niej informacji. Odpowiedź powinna być pozytywna, jeśli zachodzi którakolwiek z przykładowych przesłanek: funkcjonowanie organizacji jest uzależnione od poprawnego działania systemów przetwarzania informacji (np. prawidłowego działania systemów komputerowych sterujących procesami technologicznymi w produkcji lub systemów bankowych), występują w organizacji informacje, których nieuprawnione ujawnienie spowoduje konsekwencje prawne (np. wyciek baz danych osobowych klientów) lub finansowe (np. ujawnienie wyników prac badawczo-rozwojowych, dokumentacji produktów, powierzonych przez inne organizacje informacji, wobec których zobowiązaliśmy się umownie do zachowania ich w tajemnicy), a w ostateczności czy kradzież informacji lub sam fakt przełamania zabezpieczeń teleinformatycznych może wpłynąć negatywnie na starannie i przez wiele lat budowany wizerunek organizacji, od którego zależy jej wiarygodność na rynku. W szczególności w organizacjach działających w obszarze związanym z infrastrukturą krytyczną przesłanki powyższe występują powszechnie, a wpływ naruszenia bezpieczeństwa informacji wykracza daleko poza obszar organizacji, przenosząc się na społeczeństwo, środowisko i gospodarkę.

System bezpieczeństwa teleinformatycznego (nasz tort) powinien być złożeniem wielu zabezpieczeń, zarówno w sferze organizacyjnej, jak i technicznej. Przykłady tych zabezpieczeń znajdziemy w wielu standardach, normach, przepisach prawnych i opracowaniach z zakresu bezpieczeństwa teleinformatycznego. Począwszy od ustaw o ochronie informacji niejawnych lub danych osobowych, aż po normy ISO (katalog norm PN ISO/IEC 27000), mamy do czynienia z mniej lub bardziej uszczegółowionym wskazaniem wymaganych lub rekomendowanych zabezpieczeń, na które składają się: bezpieczeństwo osobowe, bezpieczeństwo fizyczne i środowiskowe sprzętu, zabezpieczenia sieciowe, kontrola dostępu, ochrona przed złośliwym oprogramowaniem, zapewnienie ciągłości działania i na końcu monitorowanie i zarządzanie incydentami bezpieczeństwa, nie przypadkowo wymienione, jako ostatnie. Przed podjęciem decyzji o rozpoczęciu wdrażania SIEM należy najpierw dokonać oceny, czy wszystkie wcześniej wymienione zabezpieczenia zostały już wdrożone w organizacji i czy objęły obszar, jaki będzie podlegał monitorowaniu w SIEM, a także czy proces monitorowania i zarządzania incydentami jest realizowany wystarczająco skutecznie.

Wzorowy system bezpieczeństwa (tort, jeszcze bez wisienki) to taki system, gdzie skutecznie wdrożone są w uzgodnionym obszarze wszystkie zabezpieczenia (oczywiście wg potrzeb), a administratorzy systemów informatycznych oraz operatorzy systemów monitorowania poświęcają na tyle dużo czasu na monitorowanie bezpieczeństwa, iż są w stanie na bieżąco wykryć każdy symptom lub wystąpienie incydentu. Taki system jednak nie istnieje. Praktyka jest bowiem taka, iż poza oczywistymi wyjątkami, jak komputery w kancelarii tajnej, bezpieczeństwo jest traktowane jako czynnik zwiększający koszty i czas inwestycji oraz generujący wyłącznie wzrost kosztów utrzymania, co przekłada się zarówno na ostateczny poziom uruchomienia zabezpieczeń systemowych, jak i na późniejszą eksploatację systemu bezpieczeństwa. Systemy informatyczne w organizacjach są połączone złożonymi relacjami, priorytetem jest szybki przepływ informacji pomiędzy nimi, a każda reguła blokująca te przepływy utrudnia funkcjonowanie całości. Dodatkowo dochodzi szybkie tempo wprowadzania zmian w infrastrukturze IT, przez co priorytetem eksploatacji są wdrożenia, na które poświęca się prawie 100% czasu. W takiej sytuacji nawet najbardziej świadomym zagrożeń administratorom systemów informatycznych wystarcza czasu jedynie na konfigurację zabezpieczeń w nadziei, iż nie wystąpi incydent, o którym dowiedzą się z portalu internetowego. Pokusa dołożenia do IT kolejnych etatów, dedykowanych monitorowaniu i zarządzaniu bezpieczeństwem systemów nawet się nie pojawia, gdyż na etaty jest ciągła blokada, a rozwiązanie to i tak nie byłoby skuteczne, ponieważ zorganizowanie wymiany informacji w zespole, w którym każdy jego członek monitoruje odrębnie pojedyncze składniki infrastruktury IT, jest niemożliwe. Tym samym skuteczność takiego monitorowania i tak byłaby znikoma.

Utrudnieniem w podejmowaniu decyzji o rozpoczęciu wdrażania jest fakt, iż świadomość Zarządów na temat bezpieczeństwa teleinformatycznego bywa różna, często kończy się ona na wydaniu zgody na kupno systemów ochrony antywirusowej, zasilania zapasowego, zapór sieciowych, wdrożenia systemu kontroli dostępu, konieczności zmiany haseł i blokowania ekranu (dla zgodności z wymaganiami ustawy o ochronie danych osobowych), co powinno się przekładać na zapewnienie pełnego bezpieczeństwa. Ważne jest edukowanie Zarządu na temat bezpieczeństwa, oczywiście na odpowiednim poziomie szczegółowości. Do listy zagadnień należy włączyć informacje o: skuteczności dedykowanych kampanii mailowych w dostarczaniu złośliwego oprogramowania, zasadach działania złośliwego oprogramowania (oparcie na sygnaturach), typowym przebiegu włamania (jego fazach, takich jak rekonesans i ukrycie), zagrożeniach dla sprzętu wynoszonego poza organizację. Pomocą w udowadnianiu potrzeby aktywnego monitorowania może być nawiązanie współpracy z zewnętrznym zespołem typu CERT (Computer Emergency Response Team). Dużo do myślenia może dać fakt, iż systemy monitorowania zespołów CERT ciągle coś wykrywają i nas o tym powiadamiają, a nasze zabezpieczenia niestety niczego nie widzą. Jeśli zadamy sobie trud i zliczymy, ile tak naprawdę w firmie jest istotnych logów do przejrzenia, łatwiej wytłumaczymy Zarządowi, dlaczego łatwo jest przeoczyć wśród nich istotny wpis. Na koniec, rolą IT w organizacji jest jeszcze udokumentowanie relacji pomiędzy incydentem bezpieczeństwa teleinformatycznego a jego konsekwencjami dla całości organizacji i jej władz (np. wynikających z ustawy o ochronie danych osobowych) i przedstawienie jej władzom organizacji. Zarządy Spółek są świadome ponoszonej przez nie odpowiedzialności i jeżeli uzyskają wiarygodną informację na temat istniejących zagrożeń, zaangażują się w proces podnoszenia bezpieczeństwa informacji.

Jeśli organizacja poczyniła już trud oceny swojej wiedzy o poziomie jej bezpieczeństwa i uczyniła to bez „malowania trawy na zielono", wtedy jest właściwy moment na rozpoczęcie prac nad wdrażaniem systemu monitorowania bezpieczeństwa teleinformatycznego. Pominę tutaj formalne metody przygotowania postępowania wyboru systemu i wykonawcy wdrożenia, skupię się jedynie na tych czynnikach, które powinny pozwolić na osiągnięcie końcowego sukcesu, jakim jest sprawnie funkcjonujący SIEM.

Większość zagadnień do zdefiniowania przed wdrożeniem SIEM dotyczy bowiem istniejącego systemu bezpieczeństwa, jest więc możliwa do opisania przez dział IT organizacji.
1. Czy zdefiniowany jest i uzgodniony w organizacji zakres wdrożenia, rozumiany jako wykaz krytycznych procesów biznesowych i informacji (dla których następnie IT musi utworzyć techniczną mapę infrastruktury teleinformatycznej wspierającej te procesy i przetwarzającej te informacje, biorąc pod uwagę interakcje pomiędzy tymi systemami)?
2. Jak IT ocenia poziom zabezpieczeń w obszarze infrastruktury objętej wdrożeniem SIEM?
3. Jakie systemy bezpieczeństwa są w organizacji wdrożone (ochrony przed złośliwym oprogramowaniem, firewalle, IPS/IDS etc.), czy pokrywają obszar objęty wdrożeniem i czy są wystarczająco poprawnie skonfigurowane?
4. Czy IT jest w stanie określić, jakie konkretnie incydenty bezpieczeństwa są dla niej najistotniejsze i które mają być wykrywane przez SIEM?
5. Czy organizacja jest w stanie określić, jaką liczbę zdarzeń generują jej systemy informatyczne?
Powyższe zagadnienia natychmiast wywołają wątpliwości każdego, kto będzie odpowiadał za wdrożenie SIEM w organizacji podlegającej ustawie o zamówieniach publicznych. Wydaje się bowiem, że precyzyjne opisanie systemu SIEM na potrzeby konkurencyjnego wdrożenia z sukcesem na końcu jest niemożliwe.

Nie jest tak strasznie, przecież SIEM miał być tylko wisienką na torcie. Z pomocą mogą bowiem przyjść normy i standardy (np. IEC 62351-8 pomoże zdefiniować zakres inspekcji, standard odnosi się do IT w energetyce, jednak zapisane tam zalecenia są natury ogólnej i można je śmiało stosować w innych sektorach). Wykaz systemów może być ich listą z kompletną informacją o wersjach systemów operacyjnych i zainstalowanych aplikacjach, pełnionych przez nie funkcjach w środowisku IT oraz ilości osób z nich korzystających (warto wziąć pod uwagę, iż opracowany wykaz może się stać nieaktualny w okresie pomiędzy jego opracowaniem a dniem, w których chcielibyśmy opublikować postępowanie, warto go sprawdzić na dzień przed publikacją lub zastosować bezpieczne przedziały podwyższające wymagania) – doświadczony wykonawca będzie już na tej podstawie mógł ocenić, jakiego rodzaju i ile logów wygenerują te systemy. Wsparcie dla IT przy konfiguracji systemów komputerowych i bezpieczeństwa organizacji może być elementem realizowanym przez dostawcę systemu SIEM (np. poprzez dostarczenie wzorców konfiguracyjnych). Definicja SIEM może być sporządzona poprzez określenie zakresu wykrywanych incydentów oraz wykazu systemów (zachęcam do takiego podejścia, w miejsce łatwiejszego w definiowaniu listowania ilości procesorów, pamięci, macierzy i obsługiwanych zdarzeń na sekundę – skutkuje ono bowiem koniecznością przeprowadzenia przez dostawców głębszej analizy treści zapytania ofertowego, dzięki czemu są oni potem lepiej przygotowaniu do realizacji wdrożenia). Wszelkie dodatkowe pytania i wątpliwości mogą być rozstrzygnięte w trakcie postępowania.

Na sam koniec należy sobie jeszcze odpowiedzieć na pytanie, czy oprócz funduszy na inwestycję w zakup systemu SIEM znajdą się również w organizacji środki na utrzymanie SIEM, w tym na dodatkowe etaty operatorów i administratorów SIEM (realizujących funkcje monitorowania i wprowadzania zmian). Stanowczo sugerowałbym nie łudzić się, że po wdrożeniu SIEM i automatyzacji procesu monitorowania zwolnią się jakieś zasoby w IT. Po pierwsze, monitorowanie zacznie się dopiero z wdrożeniem SIEM, a z chwilą gdy IT zacznie widzieć incydenty, uruchomione zostaną zadania związane z ich obsługą (SIEM automatycznie wyłącznie powiadomi o wystąpieniu incydentu). Dlatego bez zaplanowania i przyznania środków na późniejszą eksploatację SIEM będzie co najwyżej listkiem figowym, wskazującym niedoskonałości systemu bezpieczeństwa oraz przygnębiającym ilością informacji o incydentach, z którymi nic nie można zrobić. Dodatkowe koszty to również szkolenia dla operatorów i administratorów SIEM, których wiedza powinna obejmować wiele dyscyplin IT (systemy operacyjne, bazy danych, sieci i firewalle, systemy ochrony antywirusowej), by mogli oni właściwie interpretować prezentowane im przez system informacje i konfigurować nowe funkcje SIEM.

Warto wdrażać SIEM, nie ma bowiem nic lepszego, niż torcik z wisienką!

CYBER ARMIA OCHOTNIKÓW

Jeden z amerykańskich generałów stwierdził, że właściwie to w wielu przypadkach nie ma sensu na przykład bombardować lotniska nieprzyjaciela skoro można je po prostu wyłączyć. Oczywiście miał na myśli możliwość "elektronicznego" wyłączenia, cybernetycznego sparaliżowania infrastruktury, prowadzącego do jej wyeliminowania w trakcie konfliktu. To chyba najprostszy dowód na to jak działanie w obszarze cyberprzestrzeni może być istotnym elementem współczesnego konfliktu.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Dołączenie do arsenału współczesnych narzędzi bojowych narzędzi, które związane są z działaniem w cyberprzestrzeni, stało się faktem. Najpotężniejsze armie świata tworzą dedykowane oddziały bojowe, których zadaniem jest rozwijanie swoich zdolności defensywnych, ale i ofensywnych, jeśli chodzi o odpieranie i przeprowadzanie ataków w cyberprzestrzeni. James A. Lewis, który studiował zagadnienia cyberbezpieczeństwa w Centrum Studiów Strategicznych i Międzynarodowych w Waszyngtonie, twierdzi, że publicznie dostępne dokumenty sugerują, że dwanaście z największych mocarstw militarnych świata buduje aktywnie swoje programy cyberbezpieczeństwa.

Zdolność do prowadzenia działań w cyberprzestrzeni ma pewną istotną cechę, wyróżniającą ją od innych rodzajów zdolności obronnej lub ofensywnej państwa - jest ona nabywana relatywnie niskimi kosztami. Budowanie nawet zaawansowanych oddziałów ochrony cybernetycznej, w porównaniu na przykład do ponoszonych kosztów związanych z budowaniem arsenału pancernego czy floty powietrznej, jest stosunkowo tanie. Z drugiej strony relacja pomiędzy wydatkami poniesionymi na narzędzia informatyczne do tych, jakie powinny być poniesione na opłacenie specjalistów od bezpieczeństwa teleinformatycznego, jest niewielka. Inwestycja w cyberbezpieczeństwo to przede wszystkim inwestycja w kompetencje ludzkie.

Powyższe cechy sprawiają, że w niektórych warunkach społeczno-ekonomicznych całkiem atrakcyjne stają się projekty polegające na wsparciu regularnych sił państwowych ochotniczymi oddziałami specjalistów, którzy zdolni byliby do prowadzenia działań związanych z bezpieczeństwem w cyberprzestrzeni. Takie oddziały powstają w niektórych krajach. Przyjmują one różne modele. Modele te można podzielić na trzy grupy:

- model "state-sponsored"

W modelu tym, który można by określić jako „sponsorowany przez państwo", oddziały ochotnicze mają bardzo nieregularną, jeśli w ogóle, strukturę. Specjaliści spoza struktur państwowych angażowani są do działań zlecanych przez państwo. Typowymi przykładami takich sytuacji są cyberkonflikty jakie miały miejsce w Estonii w 2007 roku i w Gruzji w 2008 roku. W ich trakcie infrastruktura wspomnianych krajów była atakowana przez cyberprzestępców. Co prawda trudno ich było jednoznacznie zidentyfikować i oficjalnie oskarżyć, co stanowi jak wiadomo generalny problem przy atakach sieciowych, ale powszechnie wiadomo, że za tymi atakami stali cyberprzestępcy z Federacji Rosyjskiej, którzy jak się podejrzewa, na zlecenie „dowódców z Kremla" uczestniczyli w tych konfliktach. Część z nich robiła to nawet z pobudek patriotycznych, ale wiadomo też o „przymykaniu oczu" przez władze rosyjskie na przestępczą działalność swoich obywateli w Internecie, właśnie w zamian za usługi związane ze zleconymi atakami. Szczególnie jest tutaj znany przypadek struktur RBN (Russian Business Network). Jako przedstawicieli tego modelu możemy też podać Chińczyków, na przykład w związku z utrzymywaniem nieformalnych, ale efektywnych kontaktów rządu chińskiego z hakerami z „Honker Union".

- model formalnego wsparcia sił zbrojnych

Niektóre państwa zwiększają swoje siły w cyberprzestrzeni poprzez wsparcie regularnych oddziałów zajmujących się cyberbezpieczeństwem w strukturach sił zbrojnych, oddziałami specjalistów, którzy są na co dzień są cenionymi specjalistami w świecie cywilnym np.: pracownikami czołowych firm z tego obszaru. Właściwie taki model można tylko częściowo nazwać „ochotniczym". W praktyce mamy do czynienia z powoływaniem tych specjalistów w szeregi armii i wykorzystywaniem ich potencjału. Są oni nawet odpowiednio opłacani. Taki model znany jest na przykład w Stanach Zjednoczonych (USCYBERCOM), Wielkiej Brytanii (Teritorrial Army) czy Japonii, gdzie „Cybersecurity army" powstała w czerwcu 2013 roku.

- model ligi obrony cyberprzestrzeni

Ten model ma najwięcej wspólnego z czysto ochotniczym podjęciem się zadań związanych z cyberbezpieczeństwem własnego kraju. Wśród państw realizujących ten model mamy kilka interesujących przykładów. Przede wszystkim są to państwa nadbałtyckie - Estonia i Łotwa, ale co ciekawe można by do niego zaliczyć również dwa państwa z Bliskiego Wschodu - Iran i Syria. Zresztą ten ostatni przypadek - Syrii, jest chyba najbardziej znany, choć trzeba uczciwie przyznać, że nie do końca taki sam jak pozostałe. W Syrii działa coś co świat zna jako SEA - Syrian Electronic Army. Działalność tej organizacji mocno odbiła się mediach przy okazji konfliktu w Syrii w 2013 r. Zresztą to właśnie media padły największą ofiarą SEA. Chodzi o przypadek kiedy „żołnierze" SEA przejęli kontrolę nad kontem Twittera agencji Associated Press i opublikowali informację o ataku na Biały Dom, co na chwilę zachwiało nowojorską giełdą. Wspomniana różnica pomiędzy SEA, a innymi przykładami z tej grupy, to głównie to, że oficjalnie ich działania nie są powiązane ze strukturami państwowymi. Dlatego też można

ewentualnie rozważać, czy nie jest to przykład modelu „state sponsored". Przykład irański jest już bardzo oczywisty - władze w Tehernie zorganizowały ochotnicze cyberoddziały w ramach Basij militia i w ten sposób wykorzystują cywilny potencjał obywateli na swoje potrzeby. Najbardziej usystematyzowane i być może ze względu na bliskość kulturową, polityczną i geograficzną, najlepiej rozpoznane są przykłady lig obrony cyberprzestrzeni w Estonii i na Łotwie. Nazywają się one prawie tak samo - odpowiednio - Cyber Defense League and Cyber Defense Unit. Estońska inicjatywa powstała w 2011 roku i w dużej mierze wykorzystywała doświadczenia nabyte jeszcze w trakcie konfliktu z kwietnia i maja 2007 roku. Inicjatywa na Łotwie to bardzo świeży projekt. Ligę powołano tam w lutym tego roku.

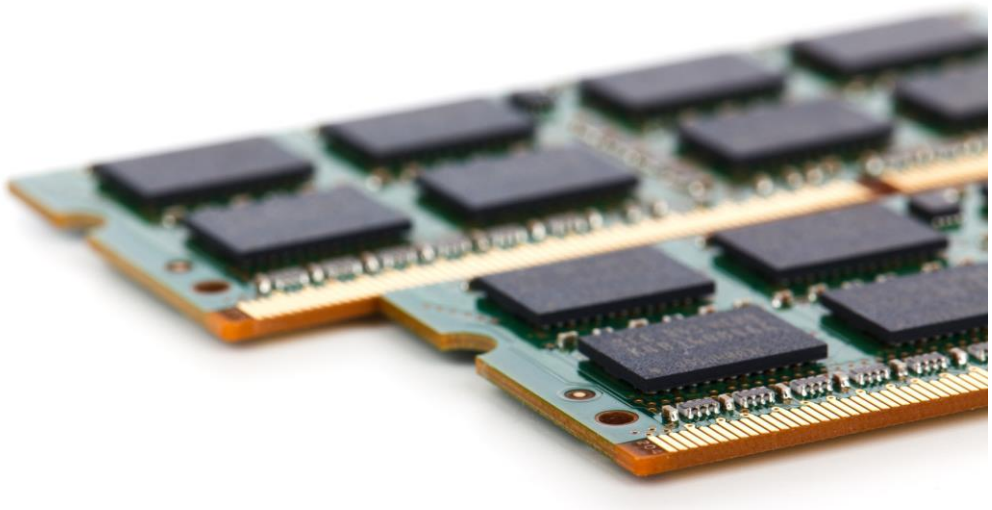
Te ostatnie przykłady - estoński i łotewski, są chyba kwintesencją absolutnie ochotniczego podejścia do kwestii zaangażowania się w cyberobronę swojego kraju, a jednocześnie inicjatywy te posiadają jasne reguły funkcjonowania. Biorąc pod uwagę ocenę możliwości realizacji projektu ochotniczej cyberarmi w Polsce, te przykłady i w ogóle model ligi obrony cyberprzestrzeni wydają się najbardziej odpowiednie.

Czym się zajmują się opisywane organizacje? W najprostszym opisie ich działalność polega na stałym podnoszeniu swoich zdolności do działań obronnych (choć również ofensywnych) w bliskiej współpracy z formalnymi strukturami powołanymi do tych działań. Realizowane to jest poprzez samokształcenie, ale i kształcenie w trakcie kursów czy szkoleń zewnętrznych. Zakłada się, że tak rozwijane zdolności będą mogły być wykorzystane w razie potrzeby, w ścisłej współpracy ze wcześniej wspomnianymi formalnymi strukturami. Członkowie oddziałów ochotniczych angażowani są również w działania uświadamiające związane z edukacją wybranych grup lub nawet całego społeczeństwa w obszarze bezpieczeństwa teleinformatycznego. Z tego roku znamy też przykłady uczestnictwa zespołów reprezentujących ochotnicze organizacje w międzynarodowych ćwiczeniach z ochrony w cyberprzestrzeni. Tak było na przykład w czasie tegorocznych ćwiczeń organizowanych przez agencję ENISA - Cyber Europe 2014, w których uczestniczył zespół reprezentujący łotewski Cyber Dyfense Unit.

Funkcjonowanie ochotniczej cyberarmii związane jest również z precyzyjnym ustalaniem reguł działania zarówno wewnątrz samej organizacji, na przykład poprzez określanie obszarów tematycznych jakim zajmuje się organizacja, jak i na zewnątrz - czyli szczegółowych zasad podejmowania działań w przypadku zaistnienia takiej potrzeby. Warto pamiętać, że nie należy kojarzyć „podejmowania działań" z sytuacją otwartego konfliktu w cyberprzestrzeni. Granica pomiędzy okresem spokoju i konfliktu jest w cyberprzestrzeni bardzo zatarta. Dlatego w praktyce właściwie cały czas występuje konieczność i możliwość podejmowania pożytecznych zadań. Funkcjonowaniu ochotniczych cyberoddziałów powinno towarzyszyć również istnienie kodeksu zasad etycznych, który wykluczy ryzyko współpracy z osobami, do których nie ma zaufania, bo na przykład nie przeszli pozytywnie weryfikacji ich przeszłości albo nie chcą się poddać obowiązującym w organizacji zasadom. Warto, aby przynależność do takiej organizacji miała również element elitarności i prestiżu.

Wydaje się, że w Polsce projekt powołania ochotniczej cyberarmii mógłby zakończyć się pełnym sukcesem. W naszym kraju nie brakuje specjalistów do spraw bezpieczeństwa teleinformatycznego, którzy z patriotycznych pobudek chętnie włączyliby się do działań na rzecz podniesienia poziomu cyberbezpieczeństwa Polski, a w sytuacji szczególnej potrzeby aktywnie współpracowali z wszystkimi, którzy formalnie otrzymali zadanie ochrony naszych cyber-granic. Charakter współczesnych konfliktów, przejawiających się na przykład wojną hybrydową, w której niezwykle istotne zadania powiązane są z prowadzeniem wojny informacyjnej, jak najbardziej sprzyja realizacji takich projektów. Formuła ochotniczej cyberarmii sprzyja także rozwojowi naszych zdolności obronnych, w szczególności w sytuacji kiedy bezpośrednie wykorzystanie największej klasy specjalistów byłoby projektem bardzo kosztownym, a być może nawet niemożliwym do zrealizowania, ze względu na to, że wielu z nich po prostu nie zgodziłoby się na funkcjonowanie w oficjalnych strukturach służb mundurowych czy służb specjalnych.

Jest jeszcze jeden bardzo istotny argument przemawiający za realizacją takiego projektu. Dotychczasowe konflikty w cyberprzestrzeni, niezależnie czy incydentalne, krótkotrwałe, czy stałe toczące się od lat pokazują, że praktycznie we wszystkich biorą udział osoby interesujące się bezpieczeństwem teleinformatycznym, które działają poza wszelką koordynacją i kontrolą. Takie działania paradoksalnie mogą być w sprzeczności ze strategią przyjętą przez podmioty oficjalne i w rezultacie szkodliwe. Warto zatem panować nad wektorem siły, która w takich sytuacjach zadziała.



Z Andrzejem Halickim, Ministrem Administracji i Cyfryzacji odpowiadającym za e-administrację i sprawy społeczeństwa cyfrowego rozmawia redakcja CIIP focus.

EDUKACJA I WSPÓŁPRACA

Jak Pan Minister ocenia dokument „Polityka Ochrony Cyberprzestrzeni RP"? W jaki sposób ministerstwo zamierza realizować jego zapisy?

Przede wszystkim niezwykle ważne jest, że udało się przyjąć tego typu dokument strategiczny, którego bardzo brakowało. Prace nad nim trwały już od 2007 r., ale z różnych przyczyn nie było doprowadzane do końca.

„Polityka" jest wobec tego pierwszym tego typu dokumentem przyjętym w Polsce i sądzę, że otwiera pewien nowy etap, w którym działalność Państwa w zakresie ochrony cyberprzestrzeni będzie bardziej spójna i lepiej koordynowana. Nie powinniśmy bowiem ulegać złudzeniu, że bez Polityki nic się nie działo – szereg instytucji, w tym także RCB, od wielu lat i z niemałymi sukcesami zajmuje się na różnych polach kwestią cyberbezpieczeństwa. Mamy jednak nadzieję, że uchwalenie „Polityki" i wyznaczenie centralnej roli MAiC w systemie pozwoli na stworzenie efektu synergii tych działań. Postępy w przenoszeniu różnych usług, zarówno publicznych jak i prywatnych, do Internetu oraz sytuacja międzynarodowa stanowią wyraźne sygnały, że tego typu intensyfikacja i konsolidacja działań są niezwykle potrzebne.

Ogólna diagnoza i kierunek działań wyznaczany przez „Politykę" uznaję za jak najbardziej słuszne. Wymienione w niej działania, takie jak szacowanie ryzyka jednostek administracji, stworzenie systemu współpracy i wymiany informacji, podnoszenie kompetencji pracowników administracji, kampanie społeczne czy współpraca z sektorem prywatnym to są wszystko działania niezwykle potrzebne i ministerstwo zamierza je w miarę możliwości realizować.

Z drugiej strony nie ukrywam, że „Polityka" jest także obarczona pewnymi niedoskonałościami. Niektóre wynikają naturalnie z pionierskiego w naszych warunkach charakteru przedsięwzięcia. Inne są skutkiem pewnych szczególnych cech naszego systemu prawno-instytucjonalnego. Wskazać tu należy przede wszystkim fakt, że „Polityka" obowiązuje tylko instytucje administracji rządowej – dla innych podmiotów (np. administracji samorządowej) może być jedynie dobrowolnie stosowaną rekomendacją. Nawet w obrębie administracji rządowej „Polityka" jest dokumentem nie nadającym ministrowi, który odpowiedzialny jest za jej implementację, żadnych uprawnień władczych czy kontrolnych. Możemy jedynie organizować współpracę i liczyć na pozytywny odzew pozostałych instytucji.

Ma więc „Polityka" pewne wady i z pewnością nie odpowiada na wszystkie wyzwania, które stoją przed Polską w zakresie cyberbezpieczeństwa. Prawdopodobnie rozwiązaniem tych problemów stanie się dopiero planowana ustawa o cyberbezpieczeństwie i kolejny dokument strategiczny, przyjęte jak sądzimy jako akty implementujące powstającą właśnie dyrektywę o bezpieczeństwie sieci i informacji (NIS). Niemniej jednak pozwala ona na znacznie lepszą niż do tej pory organizację działań państwa związanych z bezpieczeństwem sieci i informacji i na pewno realizacja jej postanowień pozwoli na osiągnięcie znacznej poprawy sytuacji. Jest to obecnie jeden z priorytetów ministerstwa.

Jeżeli chodzi o realizację konkretnych działań, to pierwszym z nich, w dużym stopniu warunkującym dalsze kroki, jest przeprowadzenie szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni. W ubiegłym roku Ministerstwo Finansów, na zlecenie KPRM, przeprowadziło audyt, którego tematem było „Zarządzanie bezpieczeństwem systemów teleinformatycznych w wybranych urzędach administracji rządowej". Objął on jawne systemy teleinformatyczne jednostek. Chodziło o to, by zebrać informacje nt. działań jednostek administracji rządowej w zakresie zapewnienia bezpieczeństwa wybranych systemów teleinformatycznych. Chciano zidentyfikować zagrożenia i słabe punktów w zarządzaniu bezpieczeństwem tych systemów. Teraz wyniki tego audytu zostały przedstawione do dyskusji na forum Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP i będą stanowiły materiał pomocniczy w dalszych pracach.

Na początku 2014 roku MAiC przystąpiło do przeprowadzenia właściwego szacowania ryzyka, zgodnie z przyjętą w tym celu metodyką. Do 31 marca jednostki organizacyjne administracji (głównie rządowej) przekazały do ministerstwa wypełnione sprawozdania, podsumowujące wyniki szacowania ryzyka własnych systemów teleinformatycznych za rok 2013. Otrzymaliśmy wyniki z około 200 ankiet i teraz poddajemy je analizie, a potem przygotujemy zbiorcze sprawozdanie z szacowania ryzyka. Chcemy na ich podstawie opracować docelową wersję metodyki sporządzania analizy ryzyka cybernetycznego tak, aby mogła ona stać się podstawą szacowania ryzyka za

bieżący rok. Dzięki temu będzie można w sposób ciągły szacować ryzyko każdego kolejnego roku, a na podstawie otrzymanych wyników planować dalsze działania w zakresie ochrony cyberprzestrzeni.

„Polityka" określa też obowiązki ciążące na poszczególnych podmiotach administracji, w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa. Przede wszystkim istnieje obowiązek opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI). Dotychczasowe badania, jak wspominany już audyt, pokazują, że w wielu jednostkach organizacyjnych wciąż nie funkcjonują odpowiednie rozwiązania w tym zakresie. Zgodnie z sugestią zawartą w „Polityce" minister AiC przy współpracy Zespołu zadaniowego, zamierza umieścić w „Planie działań" punkt dotyczący opracowania i zapewnienia wdrożenia wytycznych, dotyczących systemów zarządzania bezpieczeństwem informacji. Będziemy starali się zachęcać wszystkie podmioty do stosowania się do tych standardów, oferować pomoc i szkolenia w tym zakresie – na to pozwalają nam nasze kompetencje. Dotyczy to też obowiązku ustanowienia w każdej jednostce pełnomocnika ds. bezpieczeństwa cyberprzestrzeni. Osoba ta ma być odpowiedzialna za realizację obowiązków wynikających z przepisów aktów prawnych właściwych dla zapewnienia bezpieczeństwa cyberprzestrzeni, opracowanie i wdrożenie procedur reagowania na incydenty komputerowe, które będą obowiązywały w organizacji, identyfikowanie i prowadzenie cyklicznych analiz ryzyka, a także przygotowanie planów awaryjnych oraz ich testowanie. Krótko mówiąc za całość zagadnień związanych z cyberbezpieczeństwem w danej organizacji. Już ok. 100 jednostek organizacyjnych przekazało do MAiC informacje o wyznaczeniu pełnomocnika ds. ochrony cyberprzestrzeni i jesteśmy z nimi w stałym kontakcie.

„Polityka" kładzie także duży nacisk na działania edukacyjne. Jednym z zadań jest podnoszenie kwalifikacji wspomnianych pełnomocników ds. ochrony cyberprzestrzeni. Pierwsze takie szkolenie dedykowane dla pełnomocników, przygotowane przez MAiC, odbyło się we wrześniu. Poza przekazywaniem praktycznej wiedzy, szkolenia tego typu mają, w założeniu, służyć także nawiązywaniu bezpośrednich kontaktów pomiędzy pełnomocnikami oraz wymianie doświadczeń i dobrych praktyk. MAiC zleciło także przeprowadzenie szeregu kampanii w zakresie edukacji powszechnej, propagujących bezpieczne korzystanie z Internetu. Najważniejsza wydaje się realizacja zadania publicznego związanego z upowszechnianiem korzystania z Internetu i rozwoju kompetencji cyfrowych. MAiC zamierza, wykorzystując tu także powołany Zespół zadaniowy, zacieśnić współpracę z Ministerstwem Edukacji Narodowej. Chcemy przeprowadzić szeroką kampanię edukacyjną, skierowaną do dzieci i młodzieży, a także nauczycieli oraz rodziców. Uważamy także, że ta tematyka powinna być stale obecna w programach nauczania. Praktyka pokazuje, że często najsłabszym ogniwem systemu bezpieczeństwa jest człowiek i w tym zakresie możemy wiele osiągnąć.

Ponadto chcemy wprowadzić tematykę bezpieczeństwa teleinformatycznego jako stały element kształcenia na wyższych uczelniach – czyli inwestować w kształcenie przyszłych specjalistów w tej dziedzinie. W tej kwestii współpracujemy już z MNiSW. Podobnie, jak w przypadku programów badawczych dotyczących cyberbezpieczeństwa. Obecnie MAiC uczestniczy w projekcie badawczym „System ewaluacji zagrożeń bezpieczeństwa cyberprzestrzeni RP na potrzeby systemu zarządzania bezpieczeństwem narodowym RP (SEZBC)", finansowanym przez NCBiR, a realizowanym przez konsorcjum kierowane przez Wojskowy Instytut Łączności. Jego celem jest opracowanie systemu zbierania i analizy informacji o bieżących zagrożeniach cyberprzestrzeni RP. Mamy nadzieję, że

programów o tej tematyce będzie coraz więcej. Działania te wprowadzane są stopniowo, w miarę możliwości naszych i naszych partnerów. ponieważ na ich realizację nie przeznaczono dodatkowych środków – ma się odbywać w ramach w tych, posiadanych już przez jednostki.

Jak dyrektywa NIS wpłynie na obowiązujące w Polsce prawo w zakresie cyberbezpieczeństwa RP? Czy planowana jest nowa ustawa w tym obszarze?

Ponieważ Dyrektywa NIS określa wymogi dotyczące zarówno wewnętrznej organizacji systemów poświęconych bezpieczeństwu cyberprzestrzeni w Państwach Członkowskich UE, jak i współpracy międzynarodowej, w naszej ocenie przyjęcie Dyrektywy spowoduje konieczność przyjęcia aktu prawnego rangi ustawowej. Konieczne będzie wyznaczenie organu regulacyjno-kontrolnego w zakresie cyberbezpieczeństwa, do którego składane będą m. in. zawiadomienia o incydentach oraz nadanie mu konkretnych kompetencji – nie można tego zrobić inaczej, jak ustawą. Ponieważ akt UE odnosi się zarówno do sektora publicznego, jak i prywatnego, a „Polityka" dotyczy tylko administracji rządowej, powołany organ będzie musiał być wyposażony także w kompetencje władcze. To właśnie zwierzchnictwo nad sektorem prywatnym będzie zupełną nowością po podpisaniu NIS. Spowoduje także konieczność przyjęcia nowego dokumentu strategicznego, zgodnego w wymogami dyrektywy, który zastąpi obecną „Politykę". Nawiasem mówiąc nad takimi ustawami pracują chociażby Niemcy i Holendrzy. Będziemy uważnie przyglądać się ich doświadczeniom.

Dyrektywa NIS zawiera wiele zapisów, które jasno mówią co należy zrobić, jednak to czy zapisy te będą skuteczne, zależy od sposobu ich implementacji w Polsce. Jak powinien wyglądać proces ustalania konkretnych zapisów w Polskim prawie, odwołujących się do Dyrektywy?

W pracach na dyrektywą zdecydowana większość Państw Członkowskich, w tym my, obstaje za tym, aby pozostawiała ona duży margines swobody w implementacji do krajowych porządków prawnych. Państwa chcą przede wszystkim maksymalnie wykorzystać już istniejące instytucje i różnią się znacznie co do rozwiązań instytucjonalnych. Jest to podejście pragmatyczne i racjonalne, ale faktycznie nakłada na krajowego prawodawcę większą odpowiedzialność za końcowy efekt. Niewątpliwie wprowadzane przepisy będą

musiałby być bardzo dobrze przygotowane i dopracowane. Chcemy tu w maksymalnym stopniu otworzyć się na współpracę z szerokim gronem partnerów – zarówno instytucji publicznych, jak i przedsiębiorców, organizacji pozarządowych jak i środowisk akademickich. Sądzę, że taki otwarty model pracy nad regulacjami najlepiej się sprawdza w obecnym świecie. Do skutecznego funkcjonowania systemu cyberbezpieczeństwa konieczne jest wzajemne zaufanie jego uczestników. W szczególności podmioty prywatne powinny lepiej oceniać i akceptować instytucje w których powstaniu uczestniczyły i na których kształt miały realny wpływ. Odbyliśmy już szereg wstępnych spotkań z różnymi środowiskami, funkcjonuje już stały Zespół zadaniowy KRMC ds. ochrony cyberprzestrzeni RP, niebawem uruchomimy zespół konsultacyjny z sektorem prywatnym. Wszystkie rozwiązania będą także konsultowane społecznie w sposób całkowicie otwarty. Jest to też tematyka wrażliwa, więc transparentność tego procesu jest szczególnie istotna.

Jak powinna wyglądać współpraca publiczno-prywatna w ustalaniu, implementacji i egzekwowaniu zasad dotyczących cyberbezpieczeństwa?

Jest to jedno z trudniejszych zadań, przed którymi stajemy w obliczu wyznaczania ram ochrony cyberprzestrzeni RP. Jak już wspominałem, projekt Dyrektywy NIS dotyczy nie tylko sfery publicznej, ale także sektora prywatnego. Zgodnie z definicją, zawartą w obecnym projekcie dokumentu tzw. „operatorzy" to podmioty prywatne lub publiczne działające w sektorze energetyki, transportu, bankowości, finansów, zdrowia oraz odpowiedzialne za dostarczanie wody, które dostarczają „niezbędnych" usług. Jest to więc bardzo szeroka definicja. Prawdopodobnie, szczegółowe określenie którzy operatorzy zostaną objęci przepisami pozostawiona zostanie do decyzji państwa członkowskich, ale niewątpliwie będzie to dość szeroka i zróżnicowana grupa przedsiębiorców.

Do tej pory państwo polskie nie zajmowało się „od góry" cyberbezpieczeństwem sektora prywatnego. Wydaje się jednak, że ze strony przedsiębiorców istnieje dużo dobrej woli i zrozumienia dla konieczności współpracy z państwem w dziedzinie cyberbezpieczeństwa – jasno pokazują to prowadzone przez nas rozmowy. Konsultacje społeczne, prowadzone przez MAiC wykazały, że podmioty prywatne zdają sobie sprawę z konieczności współpracy. Istnieją oczywiście pewne kwestie newralgiczne, jak to jakie dane i kiedy wzajemnie sobie udostępniać. Chodzi o to, aby sektor prywatny nie odczuwał presji udostępniania tzw. danych wrażliwych, bo może to rodzić spory opór po stronie biznesu, zwłaszcza w przypadku organizacji transnarodowych. Konieczny jest więc dialog i dalsze konsultacje. Warto tu jednak zaznaczyć, że Europa nie jest pionierem w dziedzinie cyberbezpieczeństwa. USA od dawna prowadzi bardzo silną politykę w tym zakresie i pojawiają się liczne zarzuty ze strony firm, które skarżą się na konieczność udostępniania danych wrażliwych. Głośny jest przykład Microsoft, który wciąż walczy z amerykańskim ustawodawstwem. Europa ma w kręgach biznesu opinie bardziej pozytywną. Również przyjęta przez Komisję Europejską Strategia bezpieczeństwa cybernetycznego UE pt. „Otwarta, bezpieczna i chroniona cyberprzestrzeń" kładzie duży nacisk na to, by wszelkie działania podejmowane na rzecz ochrony cyberprzestrzeni brały pod uwagę ochronę praw podstawowych osób korzystających z Internetu.

Czy Pana zdaniem pojawiające się pomysły dotyczące powołania w Polsce ochotniczej cyberarmii są w stanie uzupełnić system cyberochrony RP?

Przede wszystkich chciałbym podkreślić, że bezpieczeństwo cyberprzestrzeni jest wspólną odpowiedzialnością wszystkich jej użytkowników. Administracja publiczna czy też służby mundurowe nigdy nie będą w stanie zapewnić pełnego bezpieczeństwa sieci i do takiej sytuacji nie chcemy nawet dążyć, bo musiałoby to oznaczać także pełna kontrolę nad siecią. Każdy wobec tego powinien w swoim zakresie przyczyniać się do poprawy bezpieczeństwa. W czasie pokoju wystarczy, aby użytkownicy przestrzegali zasad bezpieczeństwa. Sytuacja zmienia się jednak gwałtowanie w przypadku zaistnienia konfliktu na dużą skalę. Na co dzień w administracji publicznej, czy nawet w jednostkach wojskowych, nie jest potrzebna bardzo duża ilość specjalistów ds. cyberbezpieczeństwa, zwłaszcza takich, którzy posiadają zaawansowane umiejętności hakerskie i wiedzę techniczną. Nie bylibyśmy także w stanie ich zatrudnić na stałe i nie ma takiej potrzeby. Bardzo korzystna byłaby jednak możliwość wykorzystania umiejętności cywilnych informatyków - patriotów, którzy na co dzień pracują w prywatnych firmach, a w wolnym czasie podnoszą swoje kwalifikacje w dziedzinie cyberbezpieczeństwa. W momencie zagrożenia polskiej cyberprzestrzeni to właśnie oni mogliby stanąć do „walki", wspomagając służby państwowe, być może nawet pod wojskowym dowództwem. Podobne formacje istnieją już w Europie – na Łotwie i w Estonii. Estońska Liga Obrony Cyberprzestrzeni (The Estonian Defence League's Cyber Unit) została powołana, aby nie dopuścić do powtórzenia sytuacji z 2007 roku, kiedy to zaatakowano estońską e-administrację. Członkami estońskich „oddziałów" są cywilni specjaliści od bezpieczeństwa informacyjnego.

Obecnie zagrożenie cyberprzestrzeni jest jak najbardziej realne. Nie dalej jak na początku lipca tego roku ujawnione zostały informacje o tym, że hakerzy ze Wschodu przez ponad rok szpiegowali firmy energetyczne w USA i Europie, w tym także w Polsce. Celem ataków stali się operatorzy sieci elektrycznych, producenci energii i sprzętu oraz firmy zarządzające rurociągami. Co dwudziesty atak tej grupy był skierowany przeciwko przedsiębiorstwom w Polsce. Istnienie ochotniczej cyberarmii w bardzo wyraźny sposób przyczyniłoby się więc do uszczelnienia systemu cyberochrony Polski. Na podobnej koncepcji oparte są formacje typu Narodowych Sił Rezerwy czy Gwardii Narodowej w USA. Myślę, że przeniesienie tego typu koncepcji na grunt cyberprzestrzeni byłoby korzystne.

W kwietniu tego roku zapowiadał Pan powołanie, w ramach Komitetu Rady Ministrów do Spraw Cyfryzacji, zespołu zajmującego się problematyką cyberbezpieczeństwa Polski. Czy ten zespól powstał? Kto wchodzi (wejdzie) w jego skład i jakie są (będą) jego zadania?

Zespół Zadaniowy ds. bezpieczeństwa cyberprzestrzeni RP został powołany 13 czerwca br. przez ministra AiC, a jego pierwsze posiedzenie odbyło się 28 lipca br. w siedzibie MAiC pod przewodnictwem Ministra Trzaskowskiego. Ostateczne pojęliśmy po konsultacjach decyzję o umiejscowieniu Zespołu w ramach Komitetu Rady Ministrów ds. Cyfryzacji, aby nie tworzyć nowych instytucji, tylko wzmocnić istniejące. KRMC został wybrany, gdyż już dziś spotykają się w jego ramach przedstawiciele wszystkich resortów zaangażowanych w kwestie związane z informatyzacją. W skład Zespołu wchodzą ministrowie - członkowie KRMC oraz przedstawiciele szeregu ważnych z punktu widzenia cyberbezpieczeństwa instytucji państwowych, takich jak Agencja Bezpieczeństwa Wewnętrznego, Rządowe Centrum Bezpieczeństwa, UKE, URE czy KNF. Współprzewodniczącym Zespołu, obok ministra AiC jest minister spraw wewnętrznych.

Zespół, zgodnie z Polityką Ochrony Cyberprzestrzeni RP, zajmuje centralną rolę w procesie koordynacji jako stałe forum wymiany informacji, doświadczeń i dobrych praktyk

pomiędzy zaangażowanymi urzędami. Zespół jest odpowiedzialny za przygotowanie rekomendacji działań i rozwiązań dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni – obecnie opracowujemy, na podstawie przekazanych nam wkładów, pierwszy plan działań państwa w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP. Dyskutowane będą na nim także wszystkie projekty aktów prawnych związane z tą tematyką.

Na pierwszym posiedzeniu Zespołu omówiono formalne kwestie związane z jego funkcjonowaniem i przedstawiono także wyniki audytu zleconego przez Ministerstwo Finansów w 2013 i przyjęto harmonogram prac nad wspomnianym Planem działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP, przewidzianym w Polityce Ochrony Cyberprzestrzeni RP oraz w decyzji powołującej Zespół Zadaniowy.

Kto w Polsce powinien zadbać o koordynację spójności najważniejszych dokumentów dotyczących cyberbezpieczeństwa, takich jak doktryna, polityki, programy (np: NPOIK), ustawy?

Jeżeli chodzi o dokumenty rządowe lub opracowywane przez rząd, to niewątpliwie rolę tą powinien pełnić wspomniany powyżej Zespół zadaniowy. Nasza koncepcja jego działania opiera się właśnie na założeniu, że wszelkie dokumenty, programy i działania całej administracji w zakresie związanym z bezpieczeństwem cybernetycznym będą trafiały pod jego obrady. Być może będzie potrzeba wypracować tu stosowane mechanizmy, aby zapewnić, by wszystko trafiało pod obrady Zespołu, a to na pewno jest nasz cel. Chcemy także, aby wszystkie publiczne projekty informatyczne były obowiązkowo poddawane audytowi bezpieczeństwa a priori, a jego wyniki byłyby dyskutowane przez Zespół. Chcemy w ten sposób promować koncepcję security by design – każdy projekt już w fazie koncepcyjnej powinien zapewniać maksymalne bezpieczeństwo wychodząc z założenia, że na pewno będzie przedmiotem ataków. Obecnie często się o tym zapomina.

Czy minister administracji i cyfryzacji, jako minister odpowiedzialny za systemy IK, podejmuje działania zmierzające do przeprowadzenia oceny ryzyka w przypisanych systemach?

Obecnie trwa szacowanie ryzyka funkcjonowania cyberprzestrzeni w jednostkach administracji rządowej. Od jego wyników zależeć będą dalsze kierunki działań. Zgodnie z „Polityką" takie szacowanie prowadzone będzie corocznie i tego typu cykliczne szacownie ryzyka powinno stać się standardem dla wszystkich systemów IK.

Czy ministerstwo będzie dążyć do opracowania minimalnych wymagań bezpieczeństwa dla systemów teleinformatycznych wykorzystywanych przez operatorów IK?

Jak wspomniałem już obecnie kompetencje ministerstwa ograniczone są zasadniczo do administracji rządowej. W stosunku do niej tego rodzaju wymagania już istnieją – proszę zwrócić uwagę np. na rozporządzenie w sprawie Krajowych Ram Interoperacyjności, które w par. 20 nakazuje wprowadzenie systemu zarządzania bezpieczeństwem informacji w jednostkach i odwołuje się do stosownych norm ISO. Zgadzam się jednak, że są one dalece niewystarczające. Ministerstwo z pewnością w swoich działaniach będzie dążyło do opracowania różnego rodzaju rekomendacji i standardów do stosowania w różnych sektorach gospodarki.

Polityka Ochrony CRP przewiduje tego typu działania zarówno dla Zespołu, jak i dla samego ministra ds. informatyzacji, który w porozumieniu z szefem ABW i ministrem ON może opracować wytyczne dotyczące systemów zarządzania bezpieczeństwem informacji. Będziemy z pewnością chcieli tego typu wytyczne możliwie pilnie przygotować, a następnie promować ich stosowanie. Dobrym przykładem, który chcemy wykorzystać, jest opracowana przez Komisję Nadzoru Finansowego Rekomendacja D, dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Podkreślam jednak, że będą to działania „miękkie", o charakterze doradczym, gdyż minister nie ma w obecnym stanie prawnym żadnych uprawnień do ustanawiania bądź egzekwowania standardów bezpieczeństwa, bez względu na to, czy dotyczy to operatorów IK czy innych podmiotów. Stąd też liczymy na dobrowolną współpracę sektora prywatnego – rozwiązania dobrowolne potrafią być nawet bardziej skuteczne od systemu nakazów.

Ministerstwo Administracji i Cyfryzacji

ŚRODKI BUDOWY ZAUFANIA W CYBERPRZESTRZENI

Coraz bardziej intensywne zaangażowanie państw w prowadzenie działań w cyberprzestrzeni, zwiększa ryzyko wystąpienia międzynarodowego konfliktu. Skutki użycia narzędzi teleinformatycznych są trudne do określenia, jeszcze trudniej przewidzieć reakcję państw na potencjalne wrogie działania. Istnieje realna potrzeba podejmowania prewencyjnych działań, które zmniejszą ryzyko destabilizacji sytuacji międzynarodowej. Polska powinna brać w nich aktywny udział.

Joanna Świątkowska
Instytut Kościuszki

Jak wskazuje „The Cyber Index. International Security Trends and Realities”[1], przygotowany pod auspicjami ONZ, w szybkim tempie wzrasta liczba państw, które rozbudowują swój potencjał związany z prowadzeniem działań w cyberprzestrzeni (także ofensywnych). Sprawia to, że w najbliższym czasie prawdopodobnie obserwować będziemy coraz częstsze zdarzenia mogące przynieść poważne konsekwencje dla bezpieczeństwa państw.

Natura samej cyberprzestrzeni i działań w niej prowadzonych sprawia, że decyzja o podjęciu ofensywnych działań może mieć trudne do przewidzenia skutki, wywołać niespodziewane reakcje i prowadzić do eskalacji konfliktu. Po pierwsze współzależność i wzajemne połączenie systemów teleinformatycznych mogą prowadzić do zaistnienia efektu domina – czyli uszkodzeń na wielką skalę wywołanych jednym często mniejszym działaniem. Dodatkowo łatwo doprowadzić do wywołania „skutków ubocznych”, kiedy to w konsekwencji ataku ucierpią nie tylko bezpośrednie cele ataku, ale także podmioty postronne. Często takie efekty mają miejsce wbrew woli autora ataku.

Po drugie wobec braku precedensu związanego z poważnymi w skutkach działaniami w cyberprzestrzeni nie istnieją sprawdzone w praktyce mechanizmy zachowania i reakcji państw. W konsekwencji łatwo może dojść do sytuacji, w której w wyniku niezamierzonych działań, bądź złego odczytania intencji drugiego podmiotu, dojdzie do eskalacji konfliktu, który bardzo ciężko będzie opanować. Zagrożenie to jest jeszcze bardziej poważne wobec tego, że coraz więcej podmiotów państwowych deklaruje gotowość użycia także fizycznych środków odwetowych w sytuacji zaistnienia konfliktu w cyberprzestrzeni.

Społeczność międzynarodowa dostrzegła zagrożenia, jakie mogą być wynikiem takiego scenariusza. Jedną z metod przeciwdziałania destabilizacji międzynarodowej związanej z konfliktami prowadzonymi w cyberprzestrzeni stało się tworzenie i wdrażanie w życie środków budowy zaufania (ang. *confidence building measures* – CBM). Ogólnym celem stosowania CBM jest zapobieganie wybuchowi międzynarodowego konfliktu, który może być efektem błędnej oceny ryzyka, braku wzajemnego zrozumienia i zaufania. Najczęściej wiążą się one z większą transparentnością, ściślejszą współpracą i budową stabilności[2].

Geneza CBM związana jest z okresem Zimnej Wojny, kiedy państwa starały się znaleźć zabezpieczenia przed niekontrolowanym wybuchem konfliktu nuklearnego, który mógł być wynikiem między innymi złej interpretacji działań drugiej strony[3]. Tradycyjnie CBM miały bardzo zróżnicowaną formę od ustanawiania specjalnych kanałów komunikacyjnych, poprzez ujawnienie danych dotyczących zdolności bojowych, aż do tworzenia traktatów dotyczących kontroli zbrojeń.

Charakter samej cyberprzestrzeni i działań w niej prowadzonych utrudnia stosowanie konwencjonalnych działań, także odnoszących się do budowania stabilności. Na przykład mimo propozycji składanych przez niektóre państwa, nie łatwo (o ile w ogóle jest to możliwe) byłoby wprowadzić w życie decyzje o kontroli „cyber zbrojeń”. Dlatego CBM związane z działaniami w cyberprzestrzeni muszą być dostawane i specjalnie zaprojektowane. Pomimo utrudnień społeczność międzynarodowa zaczęła podejmować odpowiednie działania mając na uwadze konieczność zwiększania poziomu bezpieczeństwa.

Przykłady działań

Szczególnie intensywne prace w zakresie tworzenia CBM dedykowanych działaniom w cyberprzestrzeni są prowadzone na forum Organizacji Bezpieczeństwa i Współpracy w Europie. 2 grudnia 2013 wydana została Decyzja numer 1106 zawierająca początkowy zestaw środków budowy zaufania i bezpieczeństwa w cyberprzestrzeni. Należą do nich między innymi działania takie jak[4]:

- dobrowolna wymiana poglądów na temat różnorodnych aspektów związanych z krajowymi i międzynarodowymi

[1] Center for Strategic and International Studies, Institute for Peace Research and Security Policy, *The Cyber Index. International Security Trends and Realities*, UNIDIR, 2013, s. 3.

[2] Katharina Ziolkowski, *Confidence Builing Measures for Cyberspace - Legal Implications*, NATO Cooperative Cyber Defence Centre of Excellence, Tallin 2013, s. 12.

[3] http://www.un.org/disarmament/convarms/infoCBM/.

[4] OSCE, Decision No. 1106. Initial set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, 3 December 2013.

zagrożeniami wynikającymi z wykorzystania technologii informacyjno-komunikacyjnych;
- dobrowolna współpraca i wymiana informacji związanych z bezpieczeństwem;
- wyznaczanie punktów kontaktowych w celu ułatwienia komunikacji i dialogu;
- dobrowolne konsultacje w celu między innymi zwiększenia bezpieczeństwa krajowej i międzynarodowej infrastruktury krytycznej;
- dobrowolna wymiana informacji na temat strategii, organizacji, polityk i programów istotnych z punktu widzenia bezpieczeństwa oraz w zakresie korzystania z technologii informacyjno-komunikacyjnych.

Interesującym przykładem procesu, który sam w sobie może zostać uznany za mechanizm budowania zaufania i bezpieczeństwa w cyberprzestrzeni, jest chińsko – europejski dialog poświęcony cyberbezpieczeństwu (*Sino-European Cyber Dialogue* – SECD). Cel spotkań stanowi wymiana poglądów oraz dialog na tematy związane z bezpieczeństwem w cyberprzestrzeni. Pierwsza runda dialogu odbyła się na przełomie marca i kwietnia 2014 w Genewie. Wzięło w niej udział trzydziestu ośmiu uczestników z dwunastu krajów. Druga runda dialogu miała miejsce we wrześniu w Pekinie. Do udziału w procesie zaproszony został Instytut Kościuszki.

	TYP PROCESU	
	MULTILATERALNY	BILATERALNY
ZAANGAŻOWANE PODMIOTY/ORGANIZACJE	ONZ	USA-ROSJA
	OBWE	USA-CHINY
	ASEAN	
	G8	
	CHINY - EUROPA	

Wybrane fora na których rozwijane są CBM.

Najważniejsze wyzwania i rola Polski

Szczególnie istotnym problemem, jaki powinien stać się centralnym elementem wszystkich działań z obszaru CBM, jest ochrona infrastruktury krytycznej zarówno narodowej jak i rozumianej szerzej – w wymiarze międzynarodowym. Zrozumienie faktu, że jej niezakłócone funkcjonowanie warunkuje bezpieczeństwo nie tylko pojedynczych państw, ale w wyniku ścisłej współzależności wpływa także na stabilność międzynarodową, powinno prowadzić do zintensyfikowanych działań i inicjatyw służących zwiększeniu stopnia jej ochrony. Decydenci powinni uświadomić sobie, że wrogie działania nakierowane na infrastrukturę krytyczną mogą mieć tragiczne konsekwencje nawet dla samego atakującego. W konsekwencji powinni decydować się na rozwijanie odpowiednich CBM.

Polska powinna aktywnie włączać się we wszystkie procesy związane z CBM. Być może na poziomie regionalnym powinna stać się ich inicjatorem. Grupa Wyszehradzka czy Trójkąt Weimarski są doskonałymi przykładami platform gdzie można prowadzić tego typu inicjatywy.

Ponadto działania Polski w zakresie cyberbezpieczeństwa powinny spełniać standardy wyznaczone przez istniejące CBM. Aktualnie Biuro Bezpieczeństwa Narodowego pracuje nad przygotowaniem Doktryny Cyberbezpieczeństwa Polski. Opracowywany dokument ma m.in. wskazać cele strategiczne Polski w cyberprzestrzeni oraz określić zadania operacyjne w zakresie cyberbezpieczeństwa. Jego powstanie i upublicznienie (przynajmniej części) byłoby jednym z działań przyczyniających się do większej transparentności działań. To jednak wyłącznie przykłady inicjatyw, a Polska winna stać się aktywnym graczem w zakresie współtworzenia i wdrażania CBM.

BRYTYJSKI PROGRAM WZMOCNIENIA CYBERBEZPIECZEŃSTWA

Szczęśliwie jest tak, że tematyka cyberbezpieczeństwa, jako obszaru koniecznego do zagospodarowania również na poziomie państwowym, jest praktycznie zauważona już prawie wszędzie. Właściwie wszystkie państwa europejskie podejmują różne działania związane z osiągnięciem zdolności do lepszej obrony swojej cyberprzestrzeni. Oczywiście poziom, jakość i efektywność tych wysiłków jest bardzo różna. W niektórych krajach jest to poziom co najwyżej deklaratywny, w niektórych powstają strategie, polityki i programy dotyczące cyberbezpieczeństwa. One też mają różny poziom realnego wpływu na stan cyberbezpieczeństwa w poszczególnych krajach. Wreszcie w niektórych krajach powstają programy strategiczne zawierające zestawy konkretnych działań nakierowanych na poprawę cyberbezpieczeństwa. Ten poziom działania jest najbardziej dojrzały i powinien podlegać szczególnej analizie.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Właśnie taki program został ogłoszony w tym roku przez rząd brytyjski. Nazwano go UK Cyber Growth Partnership (CGP). Warto mu się przyjrzeć, ponieważ zawiera on wiele ciekawych pomysłów na to jak poprawiać bezpieczeństwo teleinformatyczne na poziomie całego państwa. Co więcej - wszystko wskazuje na to, że nie jest on czczym gadaniem, bo już teraz w Wielkiej Brytanii pojawiają się inicjatywy i działania, które niewątpliwie są elementami realizacji tego programu.

Zacznijmy przegląd tego programu od spojrzenia na cele strategiczne. Podejście twórców programu jest bardzo ciekawe. Założyli oni, że skoro jest tak, że właściwie nie ma innego wyjścia niż poważne zajęcie się sprawami cyberbezpieczeństwa państwa, ponieważ nie zrobienie tego stanowi dla państwa bardzo poważne ryzyko, to nie dość, że po prostu trzeba to zrobić to jeszcze warto to wykorzystać do innych strategicznych celów - na przykład poprawy stanu gospodarki. Brytyjscy decydenci najwyraźniej postanowili, że chcą uczynić z Wielkiej Brytanii światowe mocarstwo jeśli chodzi o tę tematykę i stworzyć bardzo silny sektor usług cyberbezpieczeństwa, który powinien skutecznie zdobywać rynki w innych państwach. W 2013 roku brytyjski eksport usług i produktów związanych z cyberbezpieczeństwem wyniósł 805 mln funtów brytyjskich. Brytyjczycy chcą sprawić, aby w 2016 roku wynosił on 2 mld funtów. Stanowi to wzrost o blisko 150%. To bardzo dużo. Zadanie jest ambitne, ale w przypadku jego realizacji - skutki powinny być niezwykle korzystne dla państwa brytyjskiego. Stało by się ono prawdziwą ekonomiczną potęgą w dziedzinie cyberbezpieczeństwa, tworząc przy okazji wiele nowych, wysokokwalifikowanych miejsc pracy, a jednocześnie osiągając to co w tym programie jest najważniejsze - czyli zdolności do działań cyberobronnych na najwyższym poziomie. Włączając w nie nie tylko bezpośrednie zdolności struktur administracji państwowej, ale liczne inicjatywy będące wynikiem partnerstwa publiczno-prywatnego. „Jest niezwykle ważne abyśmy posiadali ludzi i zdolności, które pozwolą Wielkiej Brytanii pozostanie forpocztą rewolucji informacyjnej" - powiedział Ed Vaizey - minister kultury i ekonomii cyfrowej, również zaangażowany w realizację projektu. To jasne postawienie celu.

Brytyjska administracja rządowa dla głoszonego programu GCP dają wsparcie na najwyższym poziomie. Ogłoszono go w czasie specjalnego spotkania towarzyszącego Cyber Security Summit w Londynie. Zrobił to Rhys Bowen pełniący funkcję zastępcy dyrektora do spraw cyberbezpieczeństwa w kancelarii premiera Wielkiej Brytanii. Zresztą program jest bardzo jasno komunikowany opinii publicznej i przedstawiciele administracji brytyjskiej wielokrotnie o nim wspominają przy okazji ważnych wydarzeń, np.: tematycznych konferencji poświęconych zagadnieniom cyberbezpieczeństwa. Program, zgodnie ze swoimi założeniami ma mocne wsparcie z sektora pozarządowego. Jednym z najbardziej znaczących sprzymierzeńców jest Brytyjskie Stowarzyszenie Handlu Technologiami (UKTech Trade Association), które podjęło się koordynacji współpracy z sektorem biznesowym i sektorem akademickim.

W ramach programu planuje się osiągnięcie co najmniej kilku poważnych celów. Pierwszym z nich jest stworzenie w Wielkiej Brytanii aż jedenastu centrów kompetencyjnych, w których rozwijane będą najróżniejsze projekty, odpowiadające bieżącym i długofalowym potrzebom. Oprócz tego planowane jest powołanie zbudowanie trzech instytutów badawczych, których badania będą dotyczyć tylko zagadnieniom cyberbezpieczeństwa. Jest też program szerokiego przepływu wiedzy. Co ciekawe, strona rządowa zamierza nie tylko pozyskiwać wiedzę z sektora prywatnego, ale sama zamierza aktywnie dzielić się swoimi osiągnięciami. Iain Lobban - dyrektor słynnej brytyjskiej agencji wywiadu - GCHQ, ogłosił plany dzielenia się nawet własnością intelektualną z brytyjskim biznesem. Administracja rządowa już skontaktowała się z setkami firm, w większości z sektora małych i średnich przedsiębiorstw, i zaangażowała się w sponsorowanie kilkudziesięciu przedsięwzięć, które mają charakter sprawdzenia słuszności powstających w tych firmach koncepcji, produktów i usług podnoszących poziom cyberbezpieczeństwa.

Bardzo ciekawie wygląda program wprowadzania tematyki cyberbezpieczeństwa do szkół i uniwersytetów. Cyberbezpieczeństwo ma się stać częścią każdego kierunku związanego z informatyką, co ma dać szanse młodym ludziom na poważne rozważenie tego kierunku rozwoju swojej kariery zawodowej. Działania w sektorze akademickim mają też swój dedykowany program. Nazywa się on MOOC (The Massive Open Online Course). W tym programie administracja rządowa - ramię w ramię z brytyjskim Open University ma dostarczyć materiały szkoleniowe przeznaczone dla każdego kto jest zainteresowany wiedzą ekspercką z dziedziny bezpieczeństwa teleinformatycznego. Co ważne kursy te mają być z założenia bezpłatne i dostępne w serwisie FutureLearn.com, który jest platformą edukacyjną oferującą

darmowe kursy dla brytyjskich i zagranicznych uniwersytetów. Zakres kursów obejmuje takie tematy jak: przegląd katalogu zagrożeń, kryptografia, analiza złośliwego oprogramowania czy zasady odpierania ataków teleinformatycznych.

Kolejnym strategicznym posunięciem proponowanym w programie GCP jest organizacja konkursów na stworzenie najróżniejszych rozwiązań z obszaru cyberbezpieczeństwa. Dobrym przykładem jest konkurs, który już ogłoszono. Jest to konkurs na wypracowanie narzędzia do automatycznego reagowania na incydenty naruszające bezpieczeństwo teleinformatyczne. Tematyka jak najbardziej ważna, bazująca na obserwacjach pokazujących, że w wyniku skutecznego włamania do sieci teleinformatycznej następuje bardzo szybka eskalacja problemów i dlatego potrzebne jest automatyczne zadziałanie, aby możliwie maksymalnie ograniczyć straty związane z takim włamaniem. Budżet jaki przeznaczono na ten konkurs wynosi 2 mln funtów brytyjskich, czyli około 10 mln złotych. Projekt jest planowany jako dwuetapowe przedsięwzięcie. W pierwszym etapie, który zorganizuje Centralne Laboratorium Nauki i Techniki na potrzeby ochrony przemysłu, mają spłynąć do oceny wszystkie propozycji koncepcji z tego zakresu. Wybrane koncepcje zostaną skierowane do realizacji w drugim etapie, gdzie każda z nich otrzyma indywidualne wsparcie finansowe.

Tych kilka przykładów pokazujących jak Brytyjczycy planują realizować program GCP wyraźnie wskazuje na to, że planują oni zbudować bardzo silne fundamenty swojej inicjatywy. Inwestycja w badania, wsparcie edukacji czy pobudzanie i wsparcie dla sektora prywatnego w rozwoju i świadczeniu usług i produktów bezpieczeństwa, to wszystko są działania tworzące spójny program budowania wyjątkowo silnej zdolności do skutecznych działań w cyberprzestrzeni. W kontekście ostatnich zmian jakie wprowadzono na szczycie NATO w Newport, gdzie zdecydowano, że sojusznicze wparcie opisane w art.5 Paktu Północno-Atlantyckiego, dotyczy również cyberataku, Wielka Brytania w krótkim czasie może stanowić jeden z najsilniejszych ośrodków kompetencyjnych i operacyjnych wśród państw członkowskich NATO i stać się szczególnie pożądanym sojusznikiem. Zdecydowanie warto przyglądać się dalszemu rozwojowi programu Cyber Growth Partnership, zarówno jako całościowej inicjatywie jaki i poszczególnym inicjatywom. Niewykluczone, że wiele z nich warto zaimplementować na gruncie polskim. Już przedstawione powyżej przykłady warto jeszcze dokładniej przeanalizować i zastanowić się, czy nie mogłyby być z sukcesem zaimplementowane w Polsce.

Źródła:
"Government behind UK cyber security economy" - http://www.computerweekly.com/news/2240223495/Government-behind-UK-cyber-economy
"Open University teams with UK government to offer free cyber security course" - http://www.itpro.co.uk/security/23032/open-university-teams-with-uk-government-to-offer-free-cyber-security-course
"MoD sponsors cyber defence automation competition" - http://www.computerweekly.com/news/2240226976/MoD-sponsors-cyber-defence-automation-competition?asrc=EM_MDN_32946640&utm_medium=EM&utm_source=MDN&utm_campaign=20140820_East%20Midlands%20gets%20cyber%20threat%20sharing%20node

Sukces polskich specjalistów z zakresu ochrony systemów IT

W dniach 20-23 maja bieżącego roku odbyły się międzynarodowe, wojskowe ćwiczenia Locked Shileds 2014. Ćwiczenia te mają formę współzawodnictwa zespołowego w zabezpieczaniu, dostarczonego przez organizatorów, środowiska teleinformatycznego (ponad 40 różnych systemów połączonych siecią IPv4 i IPv6) oraz późniejszym odpieraniu trwających dwa dni ataków cybernetycznych. Polska uczestniczyła już po raz drugi w tych ćwiczeniach. W tym roku polski zespół wywalczył I-sze miejsce, znacząco dystansując inne państwa oraz zespół reagowania na cyberataki Paktu Północnoatlantyckiego (NATO CIRC).

Artykuł przygotowali członkowie polskiego zespołu biorącego udział w Locked Shields 2014

Polski zespół został utworzony przez Ministerstwo Obrony Narodowej. W skład zwycięskiego zespołu wchodzili specjaliści zajmujący się bezpieczeństwem systemów informatycznych wybrani z następujących instytucji: Narodowego Centrum Kryptologii, MIL-CERT.PL, przedstawicieli rodzajów Sił Zbrojnych, Zespołu Informatycznego Reagowania Kryzysowego CERT Polska (Computer Emergency Response Team), CERT.GOV.PL, Służby Kontrwywiadu Wojskowego oraz Wojskowej Akademii Technicznej. Przedstawiciele Narodowego Centrum Kryptologii zapewnili koordynację prac zespołu na szczeblu planistyczno-organizacyjnym natomiast MIL-CERT.PL koordynował pracę na poziomie technicznym.

Ćwiczenie Locked Shileds 2014 zostało zorganizowane przez CCDCOE - Centrum Doskonalenia Cyberobrony NATO w Tallinie (NATO Cooperative CyberDefence Centre of Excellence) - międzynarodową organizację bezpieczeństwa cybernetycznego zlokalizowaną w Estonii. CCDCOE jest centrum treningowo – badawczym mającym za zadanie wzmocnić współpracę i poprawić wymianę informacji między NATO, krajami członkowskimi oraz innymi partnerami uczestniczącymi we wspólnej cyberobronie. Pełni również rolę ośrodka naukowo-technicznego, w którym prowadzone są szkolenia, konsultacje i konferencje. Ćwiczenie jest organizowane od trzech lat, wcześniej

organizowane było w mniejszym zakresie i pod inną nazwą. W tegorocznej edycji w ćwiczenie Locked Shields zaangażowanych było 300 osób z 17 krajów i to nie tylko członków NATO. Biorąc pod uwagę liczbę uczestniczących państw jest to więc prawdopodobnie największe tego rodzaju ćwiczenie na świecie.

Zespoły uczestniczące w ćwiczeniach mają przypisane role. Wyróżniane są:

- Zespoły niebieskie (Blue Team), które są odpowiedzialne są za obronę powierzonych im systemów teleinformatycznych.
- Zespół czerwony (Red Team). Zespół ten stara się na różne sposoby obniżyć wydajność systemów zespołów niebieskich. Zespół czerwony zna wcześniej szczegóły techniczne dotyczące początkowej konfiguracji systemów zespołów niebieskich Zespół czerwony posiada również możliwość skanowania systemów drużyn niebieskich w celu przygotowania ukierunkowanych ataków. Działania tego zespołu nie są oceniane.
- Zespół zielony (Green Team), który jest odpowiedzialny za przygotowanie infrastruktury technicznej.
- Zespół biały (White Team), który jest odpowiedzialny za ogólną organizację ćwiczeń. Członkowie tego zespołu określają cele szkoleniowe, tło sytuacyjne, scenariusze ataków (co konsultują z Red Team'em). W trakcie ćwiczeń zespół zajmuje się kontrolowaniem ich przebiegu.
- Zespół żółty (Yellow Team), który konfiguruje wymagane narzędzia do zbierania, analizy i wizualizacji informacji pochodzących z różnych źródeł. Przetworzone informacje stanowią informację zwrotną dla drużyn niebieskich nt. zdobytych punktów. Wyniki te podawane są uczestnikom, w miarę możliwości, na bieżąco.

W tym roku udział w ćwiczeniach wzięło 11 zespołów utworzonych z przedstawicieli 14 państw oraz zespół NATO CIRC. Zespoły jednonarodowościowe utworzyli Włosi, Estończycy, Polacy, Turcy, Węgrzy, Hiszpanie, Finowie, Francuzi, zaś Niemcy i Holendrzy, Litwini i Austriacy, Łotysze i Czesi połączyli siły w ramach wspólnych zespołów.

Przygotowania

W Polsce przygotowania do ćwiczeń rozpoczęły się w styczniu od skompletowania zespołu składającego się z ekspertów z różnych obszarów bezpieczeństwa teleinformatycznego, osoby, która miała odpowiadać w ćwiczeniach za kontakt innymi zespołami i (również symulowanymi) mediami oraz prawnika, który miał analizować zgodność podejmowanych działań z obowiązującymi przepisami. W ramach cyklicznych spotkań osób zaproszonych do zespołu reprezentującego Polskę wyznaczone zostały zespoły dziedzinowe, które miały się zajmować określonymi typami zagrożeń. Między innymi został wyodrębniony zespół chroniący aplikacje internetowe, stacje końcowe użytkowników, czy też zespół mający dbać o prawidłowe działanie sieci transmisyjnej. W tym ostatnim przypadku należało zadbać o odpowiednie skonfigurowanie tzw. hardering nie tylko routerów, ale również sieciowych urządzeń bezpieczeństwa takich jak zapory sieciowe. W każdym zespole była wyznaczona osoba koordynująca całokształt jego działań, co miało przeciwdziałać niespójności lub sprzeczności decyzji podejmowanych przez członków zespołu.

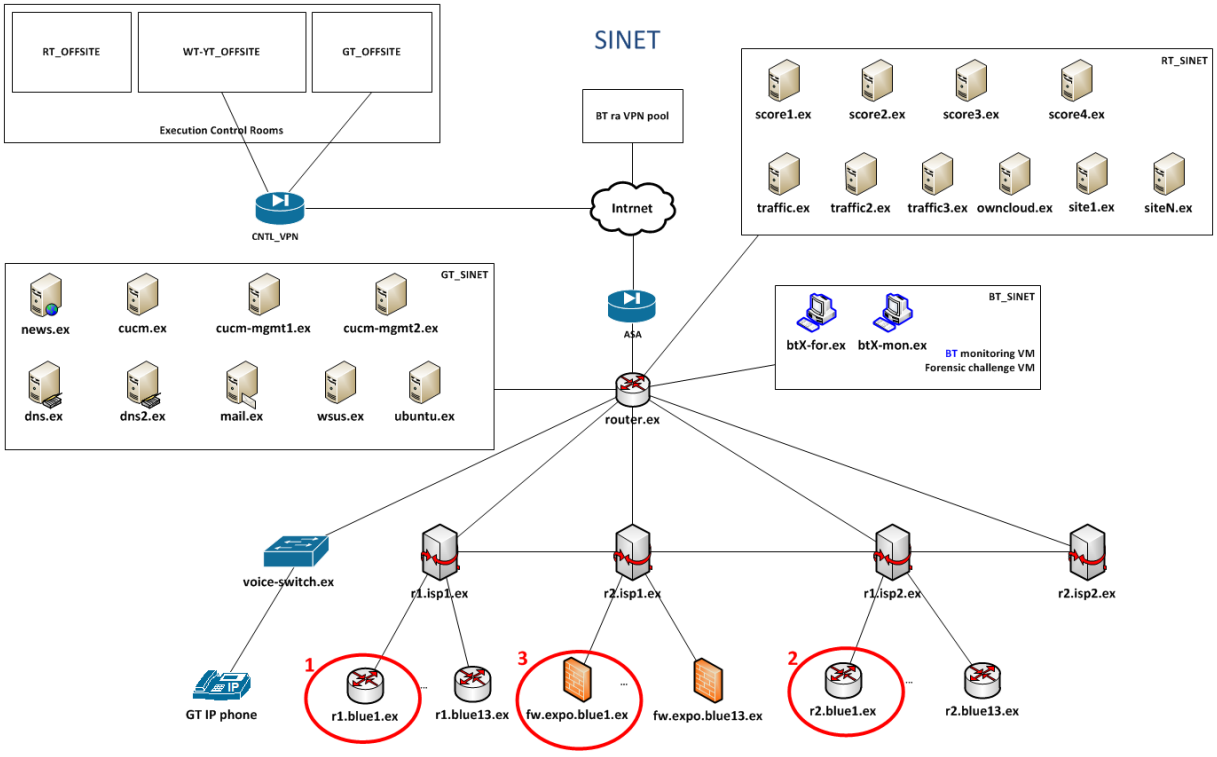
W tej fazie przygotowań należało również zdecydować jakie rozwiązania bezpieczeństwa będą zastosowane w sieci, nad którą zostanie powierzona opieka. Należy podkreślić, że na tym etapie nie znaliśmy jeszcze ani topologii tej sieci, ani też rodzajów i ilości systemów jakie trzeba będzie chronić. W takich warunkach nieokreśloności należało zdecydować co zostanie zainstalowane na dwóch wirtualnych maszynach, które każdy zespół mógł wprowadzić, do przygotowanego przez organizatorów środowiska. Maszyny te należało przekazać organizatorom jeszcze przed poznaniem topologii sieci. W tym roku powtórnie (między innymi biorąc pod uwagę doświadczenia zdobyte na poprzednich ćwiczeniach) zdecydowano się na wprowadzenie do chronionych sieci maszyn wirtualnych działających pod kontrolą systemu operacyjnego Linux Debian i wyposażonych w programowy system bezpieczeństwa IPS o nazwie Suricata, wspierany przez odpowiednio skonfigurowaną zaporę sieciową iptables. Należy zaznaczyć, że opracowane przez nas maszyny wirtualne były przygotowane do podłączenia do każdej z chronionych podsieci. Przygotowana konfiguracja umożliwiała zastosowanie dosyć nietypowego, autorskiego mechanizmu ochrony, w którym wspomniane maszyny wirtualne wykonywały atak arpspoofing względem ochranianych przez zespół sieci komputerowych. W praktyce umożliwiało to przechwycenie całego ruchu sieciowego (realizowanego m.in. pomiędzy poszczególnymi komputerami zlokalizowanymi w tych samych podsieciach) oraz filtrowanie go pod kątem niechcianych i niebezpiecznych transmisji za pomocą osadzonego na maszynach wirtualnych oprogramowania Suricata. Tak specyficzne (szczegółowe) sprawdzanie wszystkich transmisji było bardzo istotne, ponieważ w trakcie ćwiczeń kilkukrotnie okazywało się, że w naszych sieciach „niespodziewanie" zaczynały działać systemy, które nie były opisane w przekazanej nam dokumentacji. Warto dodać, że opisane rozwiązanie zostało przez nas rozbudowane o dodatkowe narzędzia programowe (przez nas zaimplementowane), które w przypadku wykrycia przez IPS złośliwego oprogramowania automatycznie dodawały odpowiednie reguły iptables blokujące wszelką transmisję spod adresu IP źródła ataku (także do innych chronionych komputerów) oraz uniemożliwiały rozprzestrzenianie się malware'u z zainfekowanego węzła.

Innym, ciekawym rozwiązaniem, które wykorzystał nasz zespół był system agentów OSSEC, które zostały zainstalowane podczas ćwiczenia na ochranianych stacjach z systemem Linux i umożliwiały kontrolowanie (ewentualnie blokowanie) operacji wykonywanych przez ich użytkowników. Zastosowane oprogramowanie było centralnie zarządzane z tych samych maszyn wirtualnych, na których była zainstalowana Suricata oraz zapora sieciowa iptables. Zastosowana konfiguracja umożliwiała monitorowanie działań m.in. każdego intruza, któremu udałoby się przełamać inne zabezpieczenia i uzyskać dostęp do ochranianych systemów.

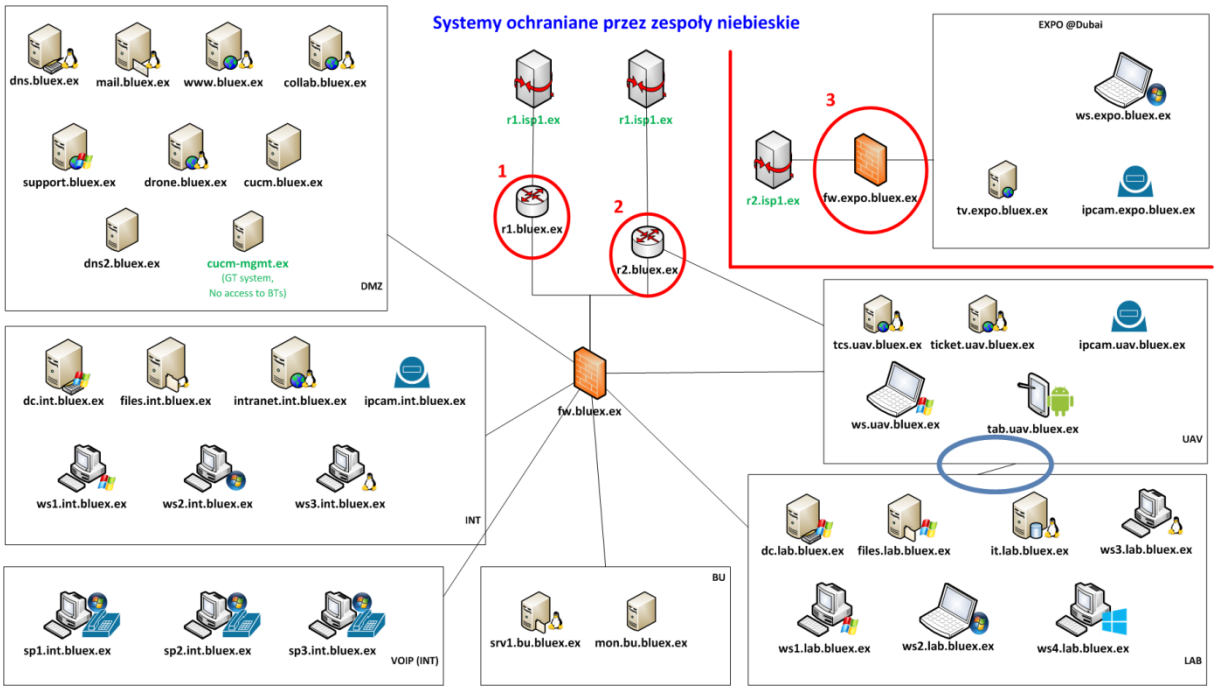
Opisana, wielopoziomowa ochrona obejmująca: monitorowanie transmisji sieciowych pomiędzy wszystkimi węzłami sieci komputerowej, filtrowanie złośliwego oprogramowania oraz kontrolowanie działań użytkowników stanowiła istotny atut naszej koncepcji obrony.

Tegoroczny scenariusz zakładał umieszczenie zespołów w fikcyjnym kraju Berylia, którego przemysł załamał się pod wpływem rosnącej fali ataków na sieci informatyczne. Poza stroną techniczną obrony, ćwiczenie obejmowało również szereg dodatkowych aspektów związanych z zagadnieniami prawnymi i kryminalistyką, co mocno upodobniło symulowane działania do świata rzeczywistego.

Ostatnim etapem przygotowania do ćwiczeń było dwudniowe rozpoznanie środowiska (13-14 maja), w którym mieliśmy działać za tydzień. Dopiero wtedy został przekazany niebieskim zespołom schemat sieci komputerowej (rys. 1 i 2) oraz informacje o obecnych w niej systemach.



Rys.1. Infrastruktura sieciowa Berylii – szkielet



Rys.2. Infrastruktura sieciowa Berylii – sieć ochraniana przez zespoły niebieskie (7 stref bezpieczeństwa, ponad 40 systemów)

Był to czas na sprawdzenie poprawności działania wcześniej przygotowanych i dostarczonych organizatorom wirtualnych maszyn oraz na wykrywanie jak największej ilości podatności, a także sprawdzenie skuteczności sposobów ich usuwania. Kluczowym przy opracowywaniu strategii obrony było poznanie funkcji jakie mają pełnić powierzone opiece systemy, a to dlatego, że monitorowanie dostępności oferowanych usług było jednym z ważniejszych kryteriów oceny skuteczności ich ochrony. Dysponując tym poziomem wiedzy można było przystąpić do opracowania bardziej szczegółowych reguł obrony, w szczególności zasad filtrowania ruchu na poszczególnych urządzeniach, które mogły to zadanie realizować. Należy podkreślić, że zadanie to było bardzo istotne, gdyż analiza połączeń między poszczególnymi systemami wskazywała na ich (celowo) błędną konfigurację (przykład tego typu niebezpiecznego połączenia został na rysunku 2 oznaczony niebieską elipsą). Podstawowymi punktami filtrowania ruchu były przygotowane systemy z oprogramowaniem Suricata. Dodatkowo uruchomiono mechanizmy filtrowania na routerach brzegowych (r1 i r2) i zaporach sieciowych (fw), gdzie był zainstalowany pfSense. O złożoności dostarczonego środowiska może świadczyć ilość wpisów w listach filtrujących ruch – na routerach brzegowych pojawiło się ponad 400 wpisów ACL, na zaporach Suricata było ich jeszcze więcej.

Przed przejściem do opisu przebiegu ćwiczeń wartym wyjaśnienia jest sposób oceny współzawodniczących ze sobą zespołów. Przy ocenie działania zespołów niebieskich brano pod uwagę:

- powodzenie ataków,

- dostępność chronionych usług,
- współpracę z innymi zespołami,
- zgłaszanie faktu wykrycia ataku,
- odtwarzanie systemów w pierwotnej konfiguracji (tzw. powrót do „snapshot'u", np. po utracie kontroli nad komputerem,
- specjalne zdarzenia, np. brak możliwości połączenia się z daną stacją przez członków drużyny białych.

Przebieg ćwiczeń

Właściwe ćwiczenia rozpoczęły się 20 maja, dodatkowo organizatorzy przeznaczyli jeszcze jeden dzień na rozpoznanie środowiska (tzw. Gamenetu). Być może było to podyktowane tym, iż tydzień wcześniej znaczna liczba systemów, które były opisane w dokumentacji do ćwiczeń była dla rozpoznających niedostępna. O 16.00 wszystkie maszyny przywrócono do stanu pierwotnego, czyli takiego jak je przygotowali organizatorzy, a nam zablokowano dostęp do Gamenetu. Następnego dnia o 8.30 przywrócono dla ćwiczących dostęp do Gamenetu i mieliśmy 30 minut na wprowadzenie najpilniejszych zmian w konfiguracji zarządzanych systemów, np. modyfikację haseł dostępowych. O 9.00 zaczęto przeprowadzać, ze zmienną intensywnością, różnego typu ataki.

Jednym z aspektów obrony teleinformatycznej w ramach ćwiczeń LS 2014 była ochrona aktywnych urządzeń sieciowych – dwóch routerów oraz dwóch zapór sieciowych. Routery, stanowiące punkt dostępu do sieci chronionej przez Blue Team, były umiejscowione w topologii w taki sposób, że umożliwiały działanie w trybie redundantnym tzn. w przypadku awarii lub niedostępności jednego z urządzeń, jego funkcję przejmowało drugie urządzenie. Mechanizm zapewniający nadmiarowość w sieci był uzyskany poprzez użycie protokołu HSRP. W celu poprawnego działania należało wskazać router aktywny, przez który fizycznie przesyłane były pakiety (Master) oraz router pasywny (Standby) poprzez ustawienie priorytetu (ważności) routera w topologii. Ze względu na to, że routery były podłączone do dwóch niezależnych dostawców sieci Internet (ISP) wymagane było dodatkowo włączenie śledzenia stanu interfejsu routera aktywnego od strony ISP. Polski zespół jako jedyny poprawnie skonfigurował tę funkcję – w momencie zasymulowania awarii routera ISP przez zespół organizatorów, router pasywny poprawnie przejął funkcję routera aktywnego i łączność z siecią Internet nie została przerwana. Ze względu na charakter ćwiczenia (wzajemna pomoc innym niebieskim zespołom) osoba odpowiedzialna za urządzenia sieciowe udzieliła wsparcia pozostałym zespołom – po niecałych 10 minutach wszystkie zespoły były w stanie komunikować się z siecią Internet.

Kolejną próbą zakłócenia poprawnej pracy routerów brzegowych były próby odgadnięcia hasła dostępowego. Wykonane próby zakończyły się niepowodzeniem, w dużej mierze z powodu zastosowania mechanizmu zaostrzającego znacznie rygory logowania w zakresie nieudanych prób, co skutecznie przeciwdziałało atakom słownikowym lub siłowym. Dodatkowo administrator routera informowany był o takich próbach, co pozwalało na odpowiednie raportowanie tych ataków premiowane dodatkowymi punktami za ich wykrycie.

Inną, tym razem udaną, próbą ataku (przeprowadzoną pod koniec 2 dnia ćwiczeń) na routery brzegowe był atak na protokół BGP, poprzez który wymieniane były informacje o trasach w sieci Internet z routerami ISP. Zespół czerwony przygotował atak typu „BGP route poisoning" sztucznie wydłużając poprawną trasę do globalnie dostępnych serwerów sieci Internet (sieć GT_SINET, w której znajdował się m.in.: główny serwer DNS, serwer poczty elektronicznej, centrala telefoniczna itd.). Dodatkowo została wstrzyknięta trasa do wymienionej podsieci poprzez nieistniejący router. Po zidentyfikowaniu niedostępności zasobów z sieci GT_SINET i wykryciu przeprowadzonego ataku, zastosowano mechanizm, który przywrócił poprawną komunikację. Mianowicie wykorzystano do tego celu mechanizm mapy routingu, w której wskazano w sposób manualny poprawną trasę do sieci docelowej.

Oprócz wymienionych ataków oraz przedstawionych mechanizmów ochrony stosowano inne popularne mechanizmy utwardzające konfigurację routerów brzegowych (np. silne hasła, zmiana nazwy użytkownika, listy kontroli dostępu dla sesji zarządzającej itp.). Routery realizowały filtrowanie pakietów poprzez zastosowanie stanowej zapory sieciowej – Zone Based Firewall. Należy podkreślić, że przy tej liczbie wpisów w listach ACL i dynamicznie zmieniających się potrzebach utrzymanie poprawności filtrowania pakietów w trakcie całego ćwiczenia nie było rzeczą łatwą.

Warto również wspomnieć o innym, ciekawym ataku, który miał miejsce ostatniego dnia ćwiczeń. Mianowicie, atakujący przejęli kontrolę nad centralną zaporą sieciową fw.bluex.ex (widoczną na rysunku 1), zmienili hasło administratora i wprowadzili do niej złośliwe oprogramowanie, które przechwytywało wszystkie znaki wpisane przez użytkowników podczas próby zalogowania się. Atak miał na celu pozyskanie haseł ustawionych przez zespoły niebieskie w urządzeniach sieciowych i innych, ochranianych przez nie zasobach. Uwzględniając liczbę chronionych komputerów logicznym było, że ze względów organizacyjnych uczestnicy będą wykorzystywali te same hasła dostępu do wielu systemów. Jednakże czujność naszego zespołu umożliwiła wczesne wykrycie opisanego nadużycia i zmianę skompromitowanych już haseł. Niestety podjęte działania nie umożliwiły odzyskania kontroli nad zaporą sieciową fw.bluex.ex. Zespół rozwiązał ten problem poprzez całkowite zablokowanie możliwości zalogowania się do tego systemu zarówno z sieci wewnętrznych, jak i zewnętrznych poprzez wprowadzenie odpowiedniej konfiguracji na routerach brzegowych oraz maszynach wirtualnych z zainstalowanym oprogramowaniem Suricata. Takie podejście zabezpieczyło fw.bluex.ex przed dalszymi nieautoryzowanymi modyfikacjami i pozwoliło dotrwać do końca ćwiczeń z konfiguracją wprowadzoną jeszcze przed atakiem, a tym samym uchroniło nas przed koniecznością utraty punktów na skutek przywrócenia stanu pierwotnego tej maszyny.

Różnorodność ataków była tak duża, że w zasadzie każdy uczestnik ćwiczeń cały czas był zajęty reagowaniem na dynamicznie zmieniające się zagrożenia dla systemów, za które był odpowiedzialny. Bardzo intensywnie musiały również pracować osoby, które w polskim zespole były odpowiedzialne za zgłaszanie organizatorom wykrytych incydentów, tworzenie raportów sytuacyjnych oraz współpracę z innymi zespołami. Ćwiczenia pokazały jak ważna dla skuteczności obrony jest współpraca wszystkich osób w zespole, wzajemna pomoc i szybka wymiana informacji, co przesądzało o spójności i komplementarności działań.

Podsumowanie

Po dwóch wyczerpujących dniach zmagań w cyberprzestrzeni zespół polski prowadził w generalnej punktacji, jednak oficjalne wyniki miały być ogłoszone dnia następnego, po uwzględnieniu ewentualnych reklamacji. Tak więc 23 maja spotkaliśmy się jeszcze raz, aby usłyszeć ostateczny werdykt, który potwierdził zdobycie przez polski zespół I-szego miejsca w tegorocznej edycji ćwiczeń. Nagrodą był puchar i duża satysfakcja z wygranej w tak prestiżowych zawodach.