Informator o ochronie teleinformatycznej

CIIPfocus

RCB Rządowe Centrum Bezpieczeństwa

www.rcb.gov.pl Styczeń 2015 nr 9

NOWY WEKTOR ATAKU WYKORZYSTUJĄCY SYSTEMY TYPU SCADA

W sieci pojawił się nowy typ cyberataku, który skierowany jest na pracowników firm, w których wykorzystywane są systemy typu SCADA. Tradycyjna metoda ataku polegająca na spear-phishingu zawiera element social engineeringu polegający na tym, że ofiara namawiana jest do ściągnięcia i instalacji pliku, który rzekomo ma być zaktualizowaną wersją systemu typu HMI (Human Machine Interface) dla systemów Siemens Simatic WinCC, GE Cimplicity i Advantech device drivers. W rzeczywistości oprogramowanie jest złośliwym kodem ukierunkowanym na ataki na bankowość elektroniczną. Dla uwiarygodnienia ataku w niektórych przypadkach ofiara przekierowywana jest na autoryzowane strony internetowe wspomnianych producentów.

http://securityaffairs.co/wordpress/32036/cyber-crime/financial-malware-icsscada.html

CYBERATAK NA NIEMIECKĄ HUTĘ

Niemieckie Federalne Biuro Bezpieczeństwa Informacji (BSI) opublikowało raport, w którym opisuje poważny atak jaki miał miejsce na jeden z niemieckich zakładów hutniczych. Atak spowodował fizyczne zniszczenia. Rozpoczął klasycznie od spear-phishingu (dedykowanego maila z załącznikiem zawierającym złośliwe oprogramowanie), dzięki któremu atakujący dostali się do sieci przedsiębiorstwa. Stamtąd łatwiej było już im przedostać się do sieci produkcyjnej huty i zaatakować urządzenia kontrolujące produkcje. Skutkiem było zaatakowanie systemu kontrolującego pracę wielkiego pieca, co jak się łatwo domyślić było powodem poważnych strat w hucie. Analiza przypadku trwa nadal, bo nie ma pewności, że odnotowane skutki były najważniejszym celem tego ataku. Raport wspomina również o innych atakach, np: związanych z Energetic Bear czy Dragonfly, w których jak wiadomo poszkodowane były również firmy polskie (patrz artykuł w nr 8 CIIPfocus).

http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Doktryna Cyberbezpieczeństwa RP

Gen. Stanisław Koziej: Cyberdoktryna pozwoli jednolicie pracować nad praktyką zarówno w zakresie cyberochrony i cyberobrony. Ma stanowić wspólny mianownik różnych gałęzi cyberbezpieczeństwa w sferze wykonawczej.

– wywiad s. 14

CYBER-EXE POLSKA 2014

Za nami kolejna edycja ćwiczeń z ochrony w cyberprzestrzeni. Po sektorze energetycznym i finansowym przyszedł czas na sektor telekomunikacyjny.

W opublikowanym raporcie znajdują się wnioski dotyczące działań wewnętrznych przedsiębiorców, całości sektora, działań administracji publicznej, komunikacji medialnej oraz organizacji ćwiczeń.

- czytaj s. 2

W numerze:

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Za nami kolejna edycja ćwiczeń z ochrony w cyberprzestrzeni. Po sektorze energetycznym i finansowym na warsztat wzięliśmy sektor telekomunikacyjny, którego przedstawiciele zresztą sami o to zabiegali, co było dla nas pozytywną motywacją do pracy z operatorami.

Co ciekawe - w trakcie prac i rozwoju projektu udało nam się doprowadzić do bardzo szerokiego udziału w ćwiczeniu administracji publicznej. Oprócz 7 operatorów do ćwiczenia przystąpiło pięć podmiotów administracji, które odgrywają istotną rolę w polskim systemie cyberbezpieczeństwa. Wszystkim uczestnikom ćwiczeń serdecznie dziękujemy i gratulujemy zaangażowania i odwagi, ponieważ ćwiczenia były nie tylko potwierdzaniem mocnych stron danej instytucji, ale także odkrywaniem słabości.

Ćwiczenia podsumowaliśmy w oficjalnym raporcie zawierającym wnioski i rekomendacje. (www.cybsecurity.org/cyberexepolska). Mamy nadzieję, że będą one bardzo przydatne w pracach nad poprawą sytuacji w organizacjach uczestników, ale nie tylko. Wiele z nich ma charakter uniwersalny i z powodzeniem może być wykorzystana przez tych operatorów, którzy nie wzięli udziału w ćwiczeniach, a nawet inne podmioty z innych sektorów. Dlatego warto się z nimi zapoznać. Część wniosków i rekomendacji jest skierowana do całego sektora telekomunikacyjnego, a część dotyczy szczególnej współpracy pomiędzy przedsiębiorcami telekomunikacyjnymi a administracją publiczną. Warto pamiętać, że operatorzy zarządzają częścią teleinformatycznej infrastruktury krytycznej i taka współpraca musi być bardzo dobrze zorganizowana. Ćwiczenia pokazują, że jest nad czym pracować. Właśnie te wnioski i rekomendacje dotyczące obszaru współpracy na styku operatorzy-państwo będą obiektem naszego szczególnego zainteresowania. Z roku na rok coraz bardziej skupiamy się na tym, żeby przedstawione po ćwiczeniach rekomendacje były wdrażane w życie.

Dlatego w 2015 roku, oprócz tego, że przygotowywać będziemy się do Cyber-EXE™ Polska 2015, to chcemy przeprowadzić wiele działań związanych z dokładnym omówieniem wniosków i rekomendacji z edycji roku 2014. Naszym celem jest znalezienie odpowiednich adresatów, którzy wdrożą proponowane przez nas rozwiązania. Z pewnością będzie jeszcze okazja na łamach CIIP focusa do informowania o tym procesie.

Mimo, że omawianie najważniejszych wniosków i rekomendacji z ćwiczeń Cyber-EXE™ Polska 2014 (CEP14) mogłoby z powodzeniem wypełnić większość numeru biuletynu, to tym razem chcielibyśmy przedstawić tylko te, które dotyczą warstwy organizacyjnej ćwiczenia. Zawsze podkreślamy, że organizacja ćwiczeń z ochrony w cyberprzestrzeni jest przedsięwzięciem, które z powodzeniem można przeprowadzać nie tylko na poziomie krajowym czy sektorowym, ale praktycznie na każdym innym - również na poziomie pojedynczej organizacji. Dlatego w naszych raportach umieszczamy wnioski dotyczące organizacji ćwiczeń, licząc na to, że będą one inspiracją i motywacją do przeprowadzenia własnych ćwiczeń.

Poniżej zamieszczamy zestawienie wybranych wniosków dotyczących organizacji ćwiczeń, do których dołączamy komentarze. Część z tego materiału ma charakter samokrytyki. Niech będzie to ukłonem wobec tych wszystkich uczestników ćwiczeń, którzy odważnie odsłaniają swoje słabe strony, aby nabrali przekonania, że podejście krytyczne stosujemy nie tylko i wyłącznie wobec nich, oszczędzając siebie jako organizatorów.

Wnioski dotyczące organizacji ćwiczeń Cyber-EXE™ Polska 2014 (wraz z komentarzami):

Odbyła się wystarczająca liczba spotkań zespołu planistycznego (100% opinii)

Ten wniosek, jak zresztą wiele innych, jest oparty o wyniki ankiety, którą przeprowadziliśmy wśród uczestników. Jak widać uznali oni, że spotkań zespołu planistycznego było wystarczająco dużo. Warto jednak przy tej okazji wskazać kilka aspektów, na które przy organizacji ćwiczeń powinno się zwrócić szczególną uwagę. Spotkania planistyczne to fragment fazy przygotowania ćwiczeń, która jest poprzedzona tzw. fazą identyfikacji. W fazie identyfikacji najważniejszym zadaniem jest ustalenie listy uczestników ćwiczenia. W przypadku Cyber-EXE™ Polska 2014 (CEP14) faza identyfikacji i pozyskiwania uczestników niebezpiecznie przemieszała się z fazą przygotowania. Dlatego uczestnicy dołączali do ćwiczenia stosunkowo późno i część z nich miała mocno skrócony czas na przygotowanie. Powodowało to również konieczność wprowadzania zmian w scenariuszu ćwiczeń, nad którym praca trwała niemal do końca przygotowań. Scenariusz jest kręgosłupem całego przedsięwzięcia i powinien być dopracowany jak najwcześniej. W ostatnim miesiącu przygotowań nie powinno się już wprowadzać żadnych zmian.

Skład zespołu planistycznego, w którym pracowali moderatorzy organizacyjni, był odpowiedni. Potwierdza to słuszność stosowanej zasady udziału tych samych osób w zespole planistycznym, które w czasie ćwiczenia pełnią zadania moderatora organizacyjnego. Również rozwiązanie, w którym osoba bezpośrednio zaangażowana w reakcję na zdarzenia przewidziane w scenariuszu również w ramach codziennych obowiązków pełni taką funkcję, wydaje się rozwiązaniem najlepszym.

Zgodnie z wnioskami - pełnienie przez osobę kluczową dla zarządzania cyberbezpieczeństwem w danej organizacji funkcji moderatora organizacyjnego, który jest pośrednikiem pomiędzy moderatorem głównym a jego organizacją, wydaje się być rozwiązaniem najlepszym. Nie oznacza to, że rozwiązaniem idealnym, gdyż w praktyce taka osoba, np.: szef wewnętrznego zespołu bezpieczeństwa, nie bierze udziału w ćwiczeniach jako ich uczestnik. Dzięki temu może wprawdzie sprawdzić jak radzi sobie jego zastępca, ale z drugiej strony zaburza to faktyczną sytuacje w organizacji, w której to zwykle szef bezpieczeństwa jest odpowiedzialny za działania przy pojawiających się zagrożeniach. Być może rozwiązaniem tego problemu byłoby zaangażowanie osoby, który bardziej pełni funkcje zarządcze a mniej operacyjne. Pamiętać tylko trzeba, że prace zespołu planistycznego, w których udział jest konieczny dla pełnienia funkcji moderatora organizacyjnego, jest bardzo czasochłonny, co może być problemem dla osób pełniących wyższe stanowiska zarządcze.

Zdaniem części uczestników (38%) instrukcja udziału w ćwiczeniu, choć w pełni zrozumiała (100%), powstała zbyt późno.

To z pewnością w naszym ćwiczeniu jest element, który wymaga szczególnej poprawy. Mimo tego, że dzięki udziałowi w pracach przygotowawczych, moderatorzy organizacyjni byli bardzo dobrze przygotowani do pełnienia swojej roli, to instrukcja w wersji 1.0 powinna znaleźć się w ich rękach zdecydowanie wcześniej. Instrukcja ma charakter porządkujący, może stanowić pewnego rodzaju listę kontrolną przygotowań, dlatego ważne jest, aby moderator organizacyjny otrzymał ją jak najszybciej. Najlepiej gdyby pojawiła się ona równocześnie z końcową wersją scenariusza, czyli nie później niż miesiąc przed rozpoczęciem ćwiczeń. Gotowa instrukcja wpływa pozytywnie na poczucie bezpiecznego przygotowywania się do ćwiczenia. Czasami jest potrzebna do przeprowadzenia wewnętrznego szkolenia dla uczestników (patrz punkt następny).

Przeprowadzenie szkolenia nie wymagało przeprowadzenia wewnętrznych szkoleń dla uczestników (62%)

Tego wniosku nie należy traktować zbyt arbitralnie. To, czy szkolenie przygotowujące do ćwiczeń jest potrzebne czy nie, w dużym stopniu zależy od przyjętego modelu. W fazie planowania CEP14 uczestnicy zdecydowali się na przeprowadzenie zespołowych ćwiczeń sztabowych – w trakcie których uczestnicy byli zorganizowani w zespół uprzednio powiadomiony o terminie, ogólnym zakresie oraz planowanym czasie trwania ćwiczeń. Uczestnicy byli w jednym pomieszczeniu a komunikacja między nimi miała charakter otwarty. Zgodnie z modelem częściowej symulacji otrzymali informację jedynie o zbliżającym się ćwiczeniu, swoim udziale, ale bez szczegółów na temat scenariusza, przedmiotu ćwiczeń czy oczekiwanej roli. Uczestnicy zajmowali swoje stanowiska pracy realizując również inne, codziennie obowiązki służbowe.

W trakcie realizacji modelu pełnej symulacji uczestnicy otrzymali informacje o ćwiczeniach już w trakcie samego wydarzenia (np. w formie wiadomości dołączonych do zdarzeń – „UWAGA TO TYLKO ĆWICZENIA"). Grupa uczestników nie była zdefiniowana i mogła się, w zależności od przebiegu, dynamicznie rozszerzać. Można wskazać na prostą korelacje, że szkolenie wewnętrzne jest tym bardziej potrzebne im bardziej nasz model będzie odbiegał od pełnej symulacji. Jeśli zdecydujemy się na zespołowe ćwiczenia sztabowe, konieczne jest aby dokładnie omówić zasady jego prowadzenia wewnątrz organizacji. Jak będą odgrywane role poszczególnych uczestników ćwiczenia, jakie będą zasady komunikacji, itd. Jeśli nasz model będzie modelem pełnej symulacji, to w praktyce nie ma za bardzo potrzeby szkolenia uczestników. Po prostu będą odgrywali swoją rolę w naturalnym środowisku pracy. Pozostaje poinformować ich o trzech rzeczach: dacie przeprowadzenia ćwiczenia, sposobie oznaczania informacji w trakcie ćwiczenia i sposobie "korzystania" z systemów teleinformatycznych, które w ćwiczeniach o charakterze organizacyjnym są w pewien sposób "podgrywane".

Uczestnicy pozytywnie ocenili wykorzystanie w ćwiczeniu narzędzia EXITO (4,8) (skala 1–6)

W roku 2014 po raz pierwszy, przy organizacji ćwiczeń, posłużyliśmy się narzędziem EXITO. Jest to narzędzie wytworzone przez Joint Reaserch Centre – komórkę badawczo-rozwojową Komisji Europejskiej (https://ec.europa.eu/jrc/en/scientific-tool/exito-exercise-event-injection-toolkit?search), dedykowane do koordynacji ćwiczeń. Jego główną funkcją jest możliwość zarządzania zdarzeniami (tzw. injectami). Bez żadnej wątpliwości narzędzie to okazało się bardzo przydatne. Przy tak wielu uczestnikach i dziesiątkach zdarzeń, możliwość zarządzania nimi odegrało kluczową rolę. Zauważyliśmy dużą jakościową poprawę w stosunku do sytuacji z lat ubiegłych, kiedy to zarządzanie zdarzeniami stanowiło nie lada wyzwanie i w dniu ćwiczeń było niezwykle obciążającym zadaniem dla moderatora głównego. Oczywiście EXITO nie jest narzędziem idealnym. Brakuje w nim na przykład możliwości komunikacji mailowej, ale nie zmienia to faktu, że warto je wziąć pod uwagę przy organizacji ćwiczeń.

Wszyscy uczestnicy ćwiczeń określili sposób podgrywania podmiotów nieuczestniczących w ćwiczeniu jako właściwy (6,00)

Podgrywanie tych, którzy realnie nie uczestniczą w ćwiczeniu, jest zadaniem szczególnie ważnym w sytuacji kiedy podgrywany podmiot w realnej sytuacji prawdopodobnie odegrałby istotną rolę w przebiegu ćwiczenia. Z taką sytuacją mieliśmy do czynienia w czasie CEP14. W ćwiczeniu nie mógł wziąć udział rządowy zespół reagowania na incydenty komputerowe - CERT.GOV.PL. Jak wiadomo pełni on ważną rolę w polskim systemie cyberbezpieczeństwa. W takiej sytuacji kluczowe jest przyjęcie jednoznacznej zasady dotyczącej podgrywania takiego podmiotu. W naszym przypadku zdecydowaliśmy się na to, żeby w żaden sposób nie odgrywać aktywnych działań. Takie działania, przy braku pewności ich realnego wystąpienia w przypadku uczestnictwa w ćwiczeniu zespołu CERT.GOV.PL, mogłyby wpłynąć znacząco na przebieg ćwiczenia i doprowadzić do wyciągnięcia mylnych wniosków. Zupełnie odwrotnie było w przypadku podgrywanego dostawcy sprzętu i oprogramowania. Nie wskazując konkretnego podmiotu pozwoliliśmy sobie na aktywne odgrywanie tego podmiotu, oczywiście w oparciu o własne doświadczenia.

Część uczestników (38%) wskazała na zbyt krótki czas ćwiczeń w kontekście zawartości scenariusza.

Nasze ćwiczenia trwało jeden dzień. W scenariuszu pojawiło się bardzo dużo zdarzeń. Powodowały one kryzysowe sytuacje, które jak wynika z doświadczeń uczestników, potrafią utrzymywać organizacje w stanie podwyższonej gotowości nawet przez kilka dni. Stąd zapewne niektórzy odczuwali pewien niedosyt jeśli chodzi o czas trwania ćwiczeń. Być może przeprowadzenie takich ćwiczeń w ciągu dwóch czy trzech dni oddawało by prawdziwą sytuację. Trzeba sobie jednak jasno powiedzieć, że tego typu obciążenie dla ćwiczących organizacji jest bardzo duże i jest mało prawdopodobne, żeby udało się przekonać tak wielu uczestników do dłuższych ćwiczeń. Przeprowadzenie dłuższych ćwiczeń dla pojedynczych organizacji jest jednak pomysłem jak najbardziej realnym, a nawet wskazanym. Tak wyglądają najciekawsze wnioski dotyczące organizacji ćwiczeń z ochrony w cyberprzestrzeni. Mamy nadzieję, że będą one przydatne w lepszym zrozumieniu idei ćwiczeń i będą dobrymi wskazówkami w przypadku decyzji o ich organizacji.

Zespół koordynujący ćwiczenia Cyber-EXE™ Polska 2014. Od lewej: Cezary Piekarski (Deloitte), Mirosław Maj (Fundacja Bezpieczna Cyberprzestrzeń), Maciej Pyznar (Rządowe Centrum Bezpieczeństwa), Michał Grzybowski (Rządowe Centrum Bezpieczeństwa)

Cyber-EXE™ Georgia 2014

- czyli ćwiczenia Cyber-EXE po gruzińsku

Fot. Piotr Szeptyński

Z wielu powodów Gruzję odwiedza coraz więcej turystów, w tym Polaków: niezapomniane krajobrazy, doskonałe wino i potrawy, przyjaźnie nastawieni ludzie oraz niepowtarzalna atmosfera przyciągają tak wielu przybyszów, że w sezonie uruchamiane są dodatkowe połączenia lotnicze (np. z Polski). Jednak Gruzja to nie tylko atrakcje turystyczne. Wielu odwiedzających tę byłą sowiecką republikę może zdziwić obecna na ulicach miast duża liczba przypominających nieco bankomaty e-kiosków. Są one interfejsem do systemów pozwalających nie tylko zapłacić rachunek czy doładować telefon, ale także załatwić wiele spraw urzędowych.

Piotr Szeptyński
Fundacja Bezpieczna Cyberprzestrzeń

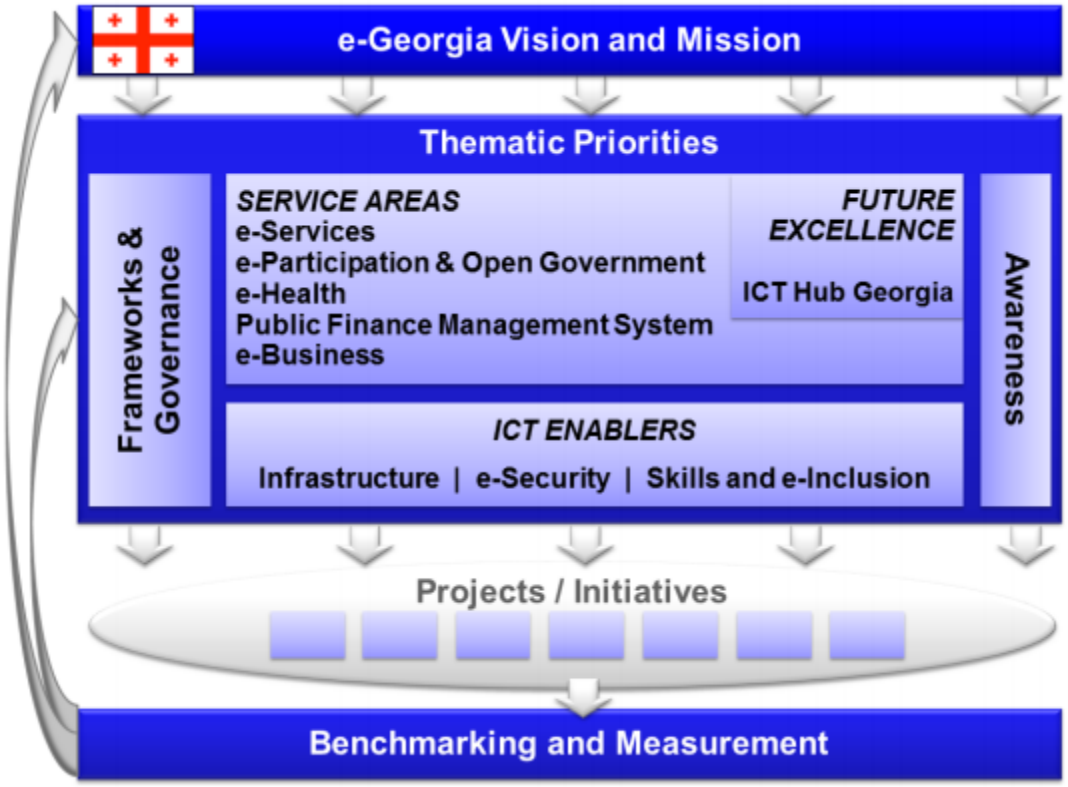
W kraju tym na bardzo wysokim poziomie stoją bowiem usługi G2C (ang. *Government-to-Citizen*) lub - innymi słowy - tzw. e-administracja. Strategia rozwoju "cyfrowej Gruzji"[1] stawia następujący cel: wzrost gospodarczy kraju poprzez współpracę i rozwój nowoczesnej technologii zapewniającej dostęp do zintegrowanych, bezpiecznych i wysokich jakościowo e-usług sektora publicznego (ang. *Georgia will become a more efficient and effective public sector offering integrated, secure, and high quality e-Services. Improved usage and participation enable ICT-driven sustainable economic growth*).

Poza oczywistymi korzyściami płynącymi z umożliwienia obywatelom bezpłatnego, łatwego i szeroko rozpowszechnionego dostępu do usług publicznych, autorzy strategii zdają sobie sprawę z zagrożeń z tym związanych, w tym ataków na infrastrukturę zapewniającą funkcjonowanie całego systemu. Słusznie podkreślają przy tym, że istotnym czynnikiem wzrostu gospodarczego i rozwoju społecznego jest zaufanie obywateli i podmiotów gospodarczych do bezpiecznej infrastruktury (ang. *When citizens and businesses trust the secure infrastructure, this becomes an important factor in economic growth and social development*). Świadomość tych zagrożeń dodatkowo wzmocniona jest doświadczeniami jakie Gruzini wynieśli z konfliktu z Federacją Rosyjską w 2008, kiedy to działaniom wojennym towarzyszyły działania w cyberprzestrzeni, związane głównie z atakami na gruzińskie serwery rządowe i na usługę dostępu do Internetu. To właśnie dlatego, na liście priorytetów w strategii znajduje się bezpieczeństwo świadczonych e-usług (ilustruje to Rysunek).

Praktycznym wyrazem troski o poziom bezpieczeństwa infrastruktury krytycznej kraju była inicjatywa działającej przy Ministerstwie Sprawiedliwości agencji DEA (ang. *Data Exchange Agency*), polegająca na przeprowadzeniu ogólnokrajowych ćwiczeń Cyber-EXE™ Georgia 2014 (CEG14). Celem tych ćwiczeń była ocena przygotowania organów państwa i jednostek sektora prywatnego (takich jak banki i firmy telekomunikacyjne), do obrony przed cyberatakami. Ćwiczenia przybrały formę praktycznej rozgrywki polegającej na obronie systemów teleinformatycznych przez zespoły (tzw. Blue Teams) reprezentujące uczestniczące podmioty. Zwycięzcą ćwiczeń zostawał zespół, który jednocześnie odparł największą liczbę ataków i zapewnił najwyższą dostępność usług świadczonych przez system będący celem ataku. Ćwiczenia Cyber-EXE™ Georgia 2014 zorganizowane zostały w ramach projektu EU-Georgia e-Governance Facility Project[2] i wspierane były przez dwa polskie podmioty – ComCERT SA i Fundację Bezpieczna Cyberprzestrzeń, która jest inicjatorem i wykonawcą ćwiczeń cyklu Cyber-EXE™.

[1] "e-Georgia strategy and action plan for 2014-2018", http://www.dea.gov.ge/uploads/eGeorgia%20Strategy.pdf, Dostęp: 18 grudnia 2014

[2] http://www.europeanprofiles.gr/index.php?option=com_content&view=article&id=1066%3Aeu-georgia-e-governance-facility&catid=65%3Aprojects&Itemid=120&lang=en

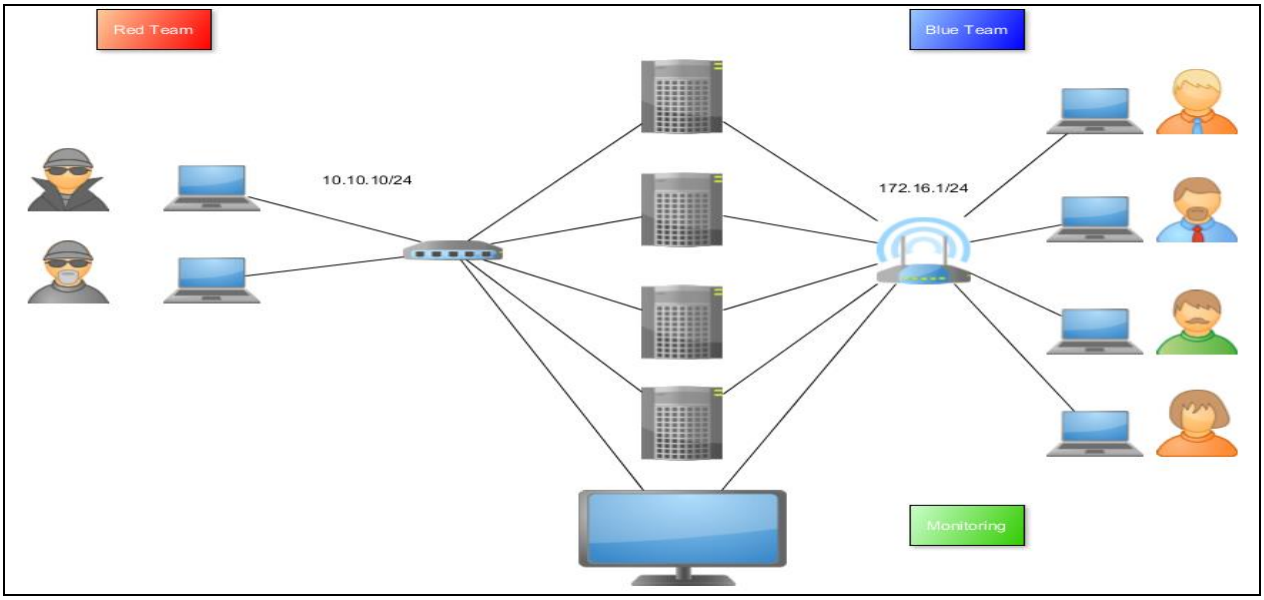


Elementy składowe strategii rozwoju cyfrowej Gruzji

Uczestnicy CEG14 do dyspozycji mieli zainstalowane w wirtualnym środowisku systemy Linux z uruchomionymi licznymi usługami sieciowymi podatnymi na znane zagrożenia (np. nieautoryzowany dostęp, ujawnienie informacji, eskalację uprawnień, odmowę usługi). Komputery połączone były w sieć (patrz: Rysunek 2), w której jednocześnie pracował zespół atakujący infrastrukturę (tzw. Red Team). Zanim jednak nastąpiły ataki, uczestnicy dostali czas na zapoznanie się z systemem i naprawienie zidentyfikowanych błędów oraz wyeliminowanie stwierdzonych usterek. Mogli to zrealizować na kilka sposobów: poprzez aktualizację oprogramowania, zmianę jego konfiguracji lub modyfikację ustawień systemu.

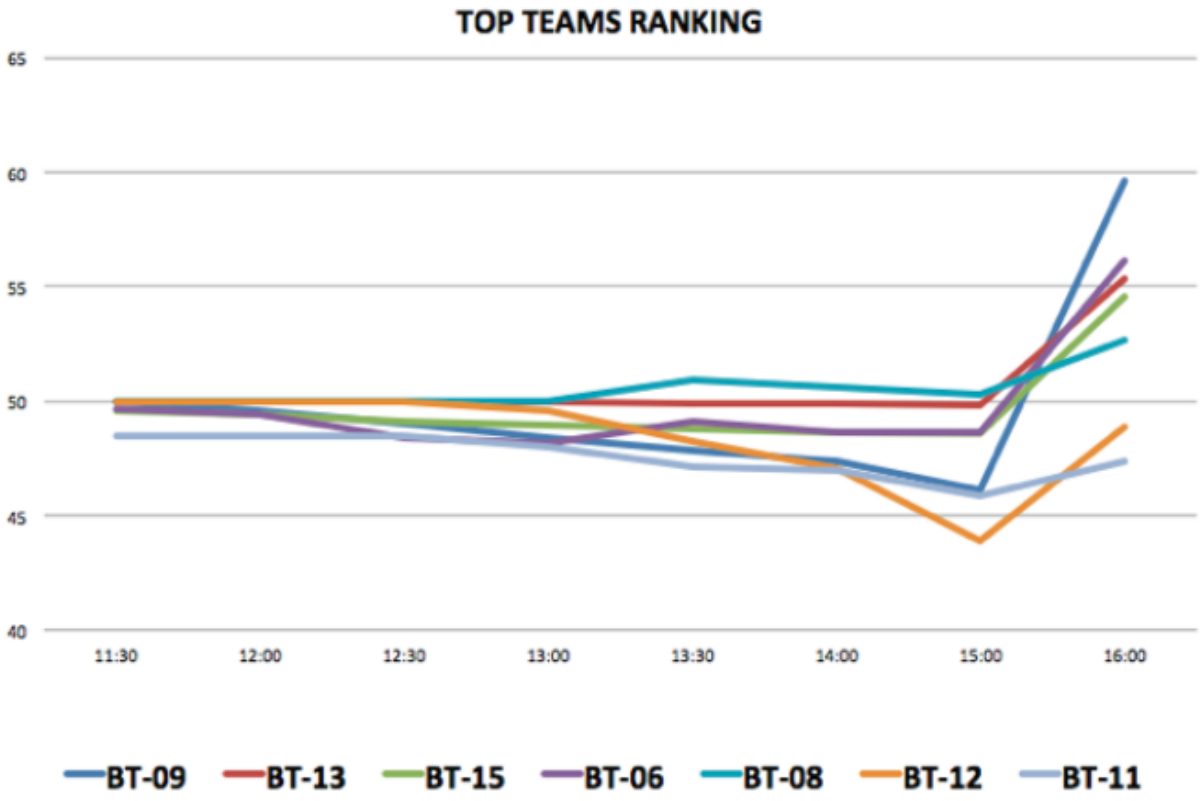
Uruchomione serwisy były typowymi usługami sieciowymi, które w większości spotkać można w rozbudowanych środowiskach IT różnych organizacji.

W czasie całego ćwiczenia mierzona była dostępność tych usług, przez co zespoły stanęły przed wyzwaniem polegającym na znalezieniu odpowiedzi na następujące pytanie: czy lepiej jest usługi zabezpieczyć, co jednak mogło wiązać się z czasową ich niedostępnością wynikającą np. z konieczności ponownego uruchomienia systemu, czy też lepiej jest zachować wysoką dostępność usług narażając je jednocześnie na udany atak?



Architektura systemu wspierającego realizację ćwiczeń

Statystyki pokazały, że zespoły podejmowały różne decyzje, zaś ostateczny wynik zależał zarówno od dostępności, jak i od poziomu bezpieczeństwa systemu po wdrożeniu poprawek przez uczestników. Poziom ten badany był przez Red Team przypuszczający ataki na usługi sieciowe. W tym celu wykorzystywano ogólnodostępne narzędzia oraz własne rozwiązania stworzone w czasie przygotowania ćwiczeń.



Zanonimizowane wyniki punktowe (oś Y) najwyżej ocenionych zespołów w czasie CEG14

Uczestnicy nie byli informowani o tym, że w danym momencie przeprowadzany jest atak na ich serwer - w rzeczywistości rzadko kiedy cyberprzestępcy informują swoje ofiary o przygotowywanych atakach. Zostały one przeprowadzone w dwóch falach w taki sposób, by dać szansę zespołom na wyciągnięcie wniosków i wdrożenie niezbędnych poprawek po pierwszej fali ataków. Organizatorzy ćwiczeń zadbali także o to, by w trakcie ćwiczeń na bieżąco prezentowane były zanonimizowane wyniki pokazujące dostępność usług poszczególnych uczestników, jak i ich skuteczność w odpieraniu ataków. Całość miała na celu motywowanie zespołów do działania i zwiększenie atrakcyjności oraz dynamiki wydarzenia.

ćwiczenia Cyber-EXE™ 2014 Georgia – sala Expo Georgia – miejsce rozgrywania ćwiczeń. (fot. Mirosław Maj)

Przez około 6 godzin trwania ćwiczeń ze strony uczestników pojawiło się kilka pytań i wątpliwości, które organizatorzy na bieżąco wyjaśniali. Nie obyło się także bez problemów natury technicznej (np. niedziałającej poprawnie sieci na dwóch identycznych modelach komputerach różnych uczestników, czy też niedającego się przewidzieć–i nietypowego zachowania niektórych elementów oprogramowania). Gdy wieczorem 24 września ćwiczenia skończyły się, zarówno uczestnicy, jak i organizatorzy wyrażali zadowolenie i chęć ponownego uczestnictwa w kolejnej edycji ćwiczeń. Choć wszystko odbyło się na niby, i żadna infrastruktura w praktyce nie ucierpiała, to z całego przedsięwzięcia każdy wyniósł cenne i całkiem realne wnioski. Udział w tego typu zabawie pozwala na praktyczną ocenę stopnia przygotowania organizacji do obrony przed cyberatakami bez konieczności narażania na niebezpieczeństwa ludzi, procesów i systemów. Takie inicjatywy bez wątpienia wpływają pozytywnie na poziom zaufania obywateli do państwa i prywatnych operatorów infrastruktury krytycznej.

Grupa APT28

nieproszeni goście w naszym domu

Za nami okres Świąt Bożego Narodzenia. Jak zwykle, zgodnie z tradycją, przy Wigilijnym stole nie zabrakło miejsca dla niespodziewanego gościa. Polacy słyną z tej tradycji od wielu lat. Ten artykuł dotyczy jednak zupełnie innych „gości" – takich, których z dużym trudem przyjęlibyśmy do stołu nawet w czasie Wigilii. „Gości" nieproszonych i niepożądanych. Co więcej „gości", którzy robią wszystko by się ukryć i podstępem wykradać nasze informacje. Mowa o tzw. cybergrupach, które wykonują zaawansowane ataki na sieci przedsiębiorstw i instytucji. Poniższy tekst przedstawia cechy działalności grupy określanej jako „APT28", na bazie wiedzy zebranej przez FireEye.

Jan Kowalski
Fundacja Bezpieczna Cyberprzestrzeń

Dlaczego grupa APT28 a nie na przykład APT1?

Od dłuższego czasu FireEye, a wcześniej Mandiant[3], gromadzi wiedzę na temat działalności cybergrup. Są to zarówno zorganizowane „prywatnie" grupy hackerów, jak również oddziały sponsorowane przez rządy państw. Przez grupę określa się osoby pracujące razem nad przeprowadzeniem ataku na te same cele. Te osoby wymieniają się zdobytymi informacjami, korzystają z tych samych narzędzi i technik, rozwijają je wspólnie. Pracują razem podczas ataku dla zdobycia dostępu do zaatakowanego celu i wydobycia interesujących danych. Różne grupy mogą jednak używać podobnych metod włamania i podobnych narzędzi, w szczególności, jeśli są to narzędzia dostępne w Internecie jak na przykład: pwdump, HTran czy Gh0st RAT. Zdarzają się sytuacje, kiedy różne grupy współpracują ze sobą dzieląc się nowym kodem exploita czy nawet personelem. Zdarza się, że różne grupy zatrudniają tych samych indywidualnych cyberprzestępców.

Co więc odróżnia cybergrupy i skąd wiadomo, że konkretny atak został przeprowadzony przez tą czy inną grupę?

Odróżnienie działalności jednej grupy od innych jest możliwe po zgromadzeniu wystarczająco dużej ilości szczegółowych danych o przebiegu ataku, porównań z wcześniej znanymi cechami działań danej grupy, czy w końcu na bazie aktywnego odkrywania narzędzi i osób związanych z działaniem grupy. Identyfikacja cybergrup jest bardzo podobna do prowadzenia śledztwa przez policję i prokuratora. Bardzo rzadko zdarza się[4], że przestępcy chcą być zidentyfikowani i pozostawiają swój podpis. W analizie cyberataku kluczowe jest zebranie jak największej ilości szczegółów – „okruszków chleba" – opisujących atak, a identyfikacja grupy, która go przeprowadziła jest szybsza, jeśli mamy już bazę wiedzy opisującą poprzednie działania tej grupy.

Wektor ataku, charakterystyczne frazy w spear phishing email, te same nazwy plików, sumy kontrolne, czasy kompilacji, samodzielnie opracowane funkcje i sposoby „zaciemniania" kodu, sposoby komunikacji z serwerami CnC to przykłady takich „okruszków chleba" identyfikujących grupę APT[5].

Aktualnie FireEye/Mandiant obserwuje działalność i gromadzi dane o około 300 różnych cybergrupach. Od czasu do czasu, firma publikuje artykuły i raporty opisujące ich działania – w ten sposób ostatnio przedstawialiśmy działania takich grup jak APT1, APT3, FIN4 a także APT28.

APT28 – charakterystyka celów ataków

APT28 wyróżnia się na tle innych grup, o których najczęściej słyszymy w kontekście ataków APT. Celem tej cybergrupy jest bowiem **szpiegostwo polityczne**, w odróżnieniu od znacznie częstszego szpiegostwa gospodarczego.

Skąd więc grupa posiada środki finansowe i zaplecze niezbędne do prowadzenia działalności? Działania grupy APT28 są monitorowane przez FireEye, a wcześniej przez Mandiant, od 2007 roku. Już sam fakt, że ta organizacja działa ponad 7 lat budzi przypuszczenia, że jej działalność jest w pewien sposób utrzymywana i zlecana.

Szpiegostwo polityczne grupy APT28 dotyczy zbierania informacji o działaniach rządów, organizacji militarnych (armie, dowództwa, sojusze) i instytucji zajmujących się bezpieczeństwem na świecie. Szczególnym obszarem zainteresowania tej cybergrupy, w ostatnim okresie, jest obszar Wschodniej Europy, Gruzji i ogólnie Kaukazu oraz instytucji, których działania mają wpływ na rozwój sytuacji w tym obszarze (np. NATO, OBWE, attaché wojskowi przy ambasadach).

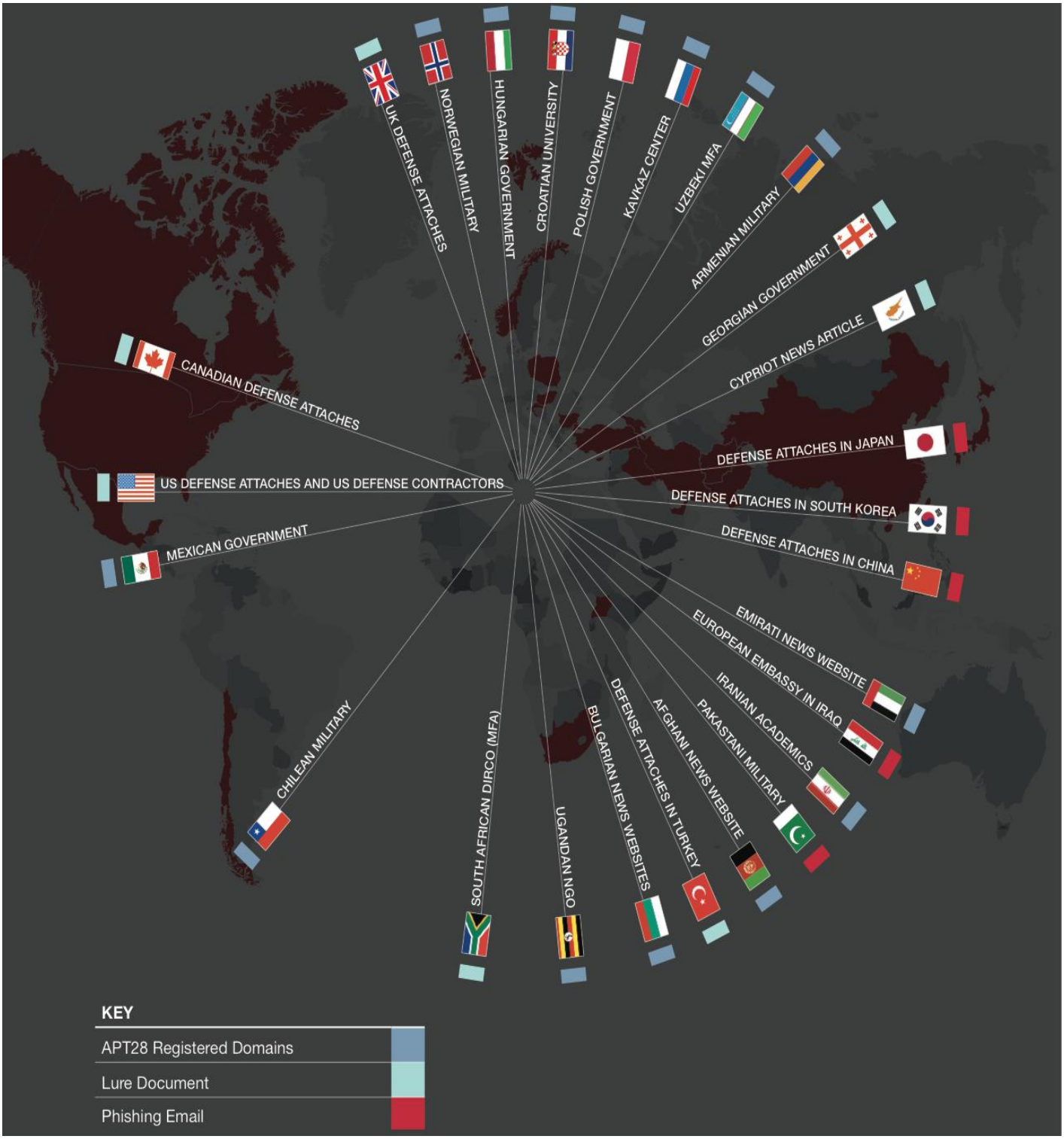
Byliśmy w stanie zidentyfikować ślady działań APT28 w odniesieniu do instytucji w Polsce, Gruzji, Czeczeni, Węgrzech, Mołdawii, Bułgarii, Armenii, a wcześniej Chile, Norwegii, Pakistanie, USA, Meksyku, Unii Europejskiej.

Wśród tych śladów są zarówno potwierdzenia wykrycia malware, jakim posługuje się APT28, w sieciach zaatakowanych instytucji, jak również uzyskane emaile przygotowane do ataku spearphishing na konkretne instytucje oraz domeny DNS rejestrowane przez grupę i zbliżone nazwami do domen instytucji i rządów tych państw.

[3] Firma Mandiant została przejęta przez FireEye na przełomie 2013 i 2014 roku

[4] Choć nie jest to zupełnie niespotykana sytuacja – przykładem są choćby działania grupy Anonymous (*http://www.forbes.pl/artykuly/sekcje/Wydarzenia/hakerzy-z-anonymous-zaatakowali-strony-sejmu,23441,1)*

[5] Więcej szczegółów na ten temat można znaleźć m.in. w artykule FireEye „Digital Bread Crumbs" (*http://www.fireeye.com/resources/pdfs/digital-bread-crumbs.pdf*)

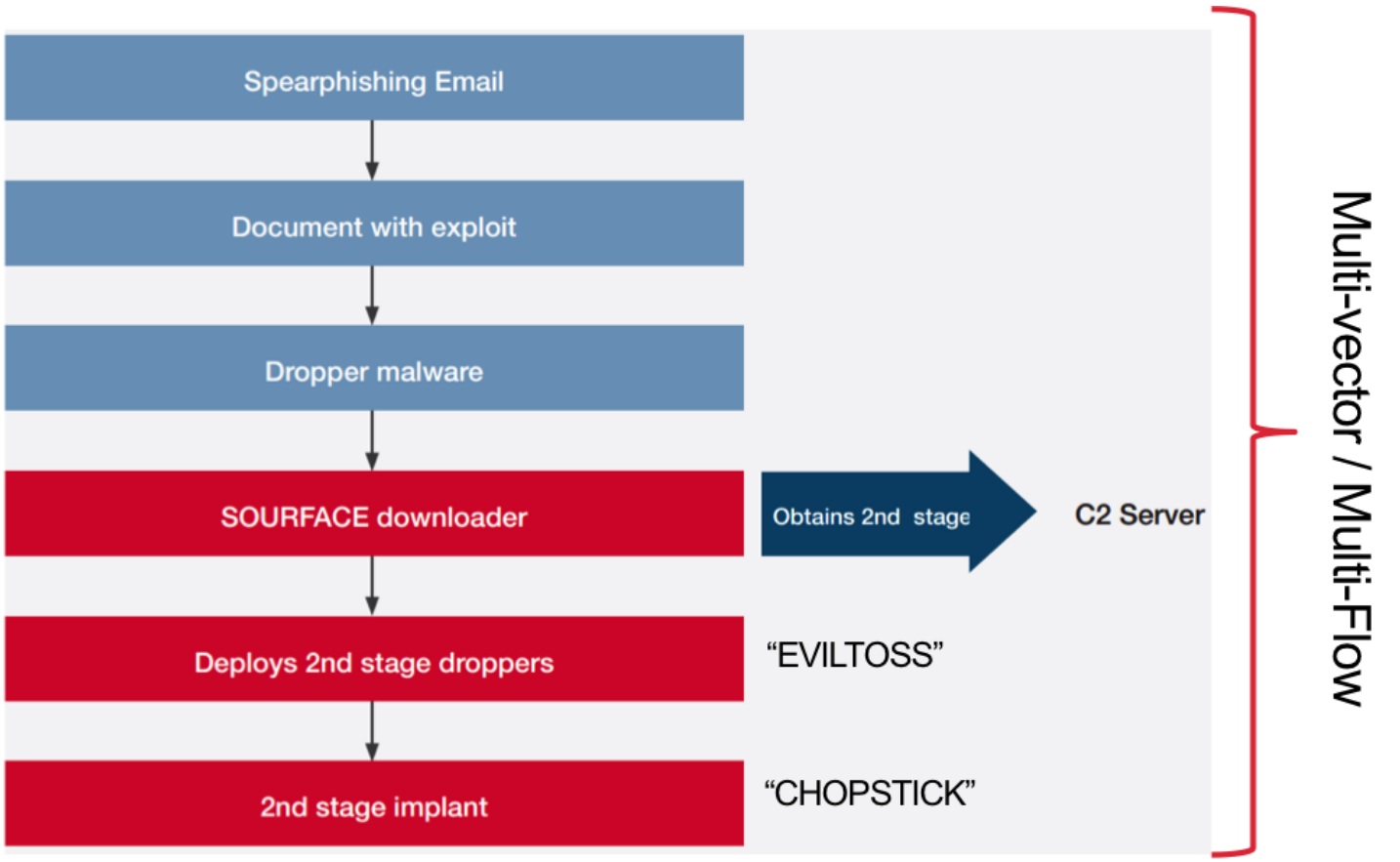


Państwa powiązane z działalnością grupy APT28 od 2007 roku
(źródło: raport FireEye „APT28: A Window Into Russia's Cyber Espionage Operations?")

APT28 – „okruszki chleba"

Jak już wspomniałem wcześniej, jednym z głównych wyróżników grupy APT28 są specyficzne cele ataków i zainteresowanie danymi o sytuacji w krajach i regionach, a nie cele gospodarcze lub finansowe. Również analiza stosowanych narzędzi, technik i metod (tzw. TTP[6]) ataków pozwala na znalezienie wspólnego mianownika działań APT28. Najczęściej stosowany przez APT28 cykl ataku został przedstawiony na poniższym schemacie.

[6] Tools, techniques, practices



Cykl ataków przeprowadzanych przez APT28
(źródło: raport FireEye „APT28: A Window Into Russia's Cyber Espionage Operations?")

Przedstawione na rysunku nazwy „Sourface" (aktualnie mamy też do czynienia z jego nowszą wersją zwaną „Coreshell"), „Eviltoss", „ChopStick" to nazwy własne poszczególnych składowych ataku na dane przez FireEye.

Większość znanych nam ataków APT28 rozpoczyna się od spearphishingu. Załącznikiem do wiadomości jest dokument zawierający kod exploit, który inicjuje kolejne fazy ataku pobierając kod droppera z zarejestrowanej lub skompromitowanej strony web. Pierwszy dropper nie kończy jednak fazy uzyskania pełnej funkcjonalności ataku. Dropper odpowiada za przygotowanie środowiska (ukrycie) kolejnych porcji malware. Są one pobierane w zaszyfrowanej postaci w następnych krokach, z innych miejsc w Internecie. Po ich uruchomieniu zainstalowany kod ataku uzyskuje pełną, zakładaną funkcjonalność dostosowaną do wybranego celu.

Mamy więc do czynienia z wielowektorowym atakiem (co najmniej email i web), realizowanego etapami i wymagającym złożenia razem wielu połączeń (*flows*) dla uzyskania całego kodu złośliwego zaangażowanego w atak.

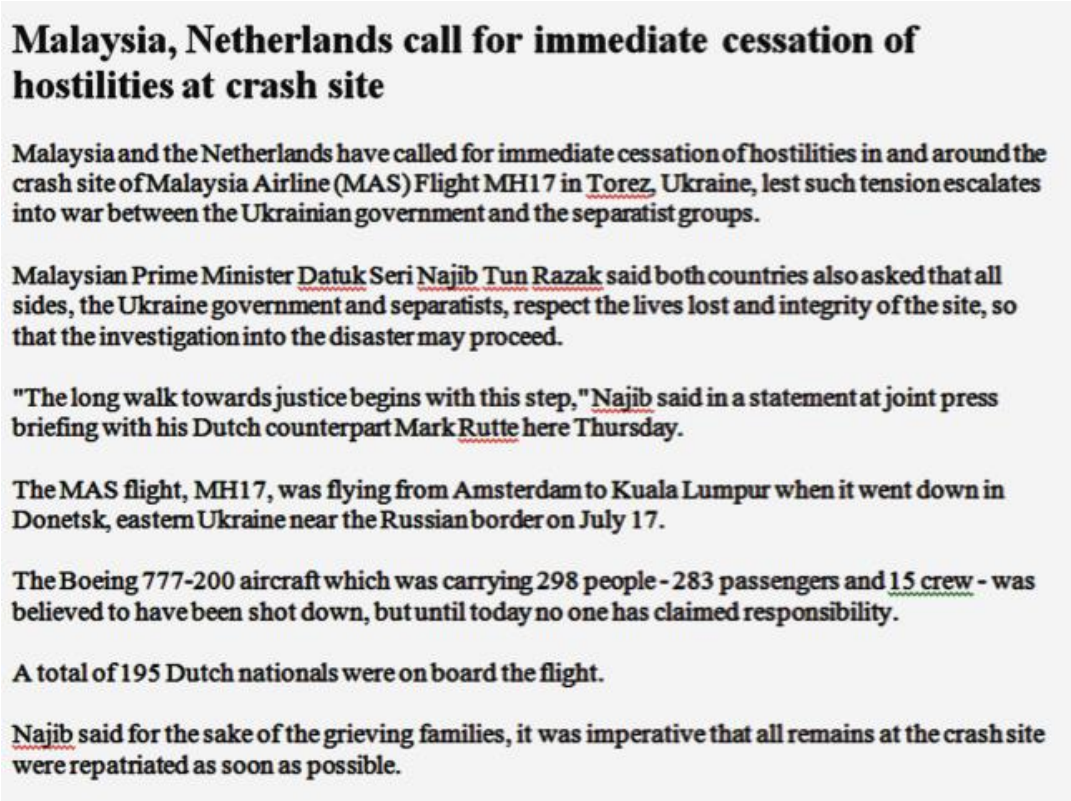
Cechą charakterystyczną grupy APT28 jest wysoki poziom skomplikowania kodu malware oraz drobiazgowe, wielotygodniowe przygotowanie do ataku. Przygotowania obejmują m.in. wybór celu ataku, dostosowanie kodu ataku do celu, rejestrację domen, które mają wprowadzić w błąd ofiarę, a także przygotowanie treści i załączników do wiadomości spearphishing.

O zaawansowaniu malware, który jest stopniowo rozwijany od 2007 roku, mogą świadczyć choćby takie cechy jak:
- utrudnianie analizy statycznej kodu przez zaciemnianie (*obfuscation*) stringów, które są „odciemniane" dopiero podczas uruchomienia kodu;
- opóźnianie analizy przez stosowanie nieużywanych, nieważnych z punktu widzenia działania kodu, instrukcji maszynowych;
- zaimplementowane funkcje wykrywania narzędzi automatycznej analizy kodu;
- szyfrowanie danych wykradanych przez atak (własnymi algorytmami szyfracji i mocnymi algorytmami opartymi na kluczu publicznym);
- modułowa budowa dropperów pozwalająca na włączanie określonych funkcji (np. keylogger, uruchamianie zdalne kodu, rekonesans, zdalny dostęp, wyszukiwanie i kradzież danych, itp.);
- moduł ChopStick umożliwia kradzież danych nawet z sieci izolowanych (*air-gap*) przez próby przeniesienia ich do innych segmentów sieci przez klucze USB nieświadomych tego użytkowników.

Poniższa tabela przedstawia przykłady domen zarejestrowanych i wykorzystywanych w atakach APT28, które są związane z polskimi instytucjami rządowymi oraz NATO i OBWE.

Domena używana w atakach APT28	Prawdziwa domena
q0v[.]pl, mail[.]q0v[.]pl	**gov.pl**, **mail.gov.pl** *Domena stosowana przez polskie instytucje rządowe*
poczta.mon[.]q0v[.]pl	**poczta.mon.gov.pl** *Domena pocztowa Ministerstwa Obrony Narodowej w Polsce*
nato.nshq[.]in	**nshq.nato.int** *Domena używana przez NATO Special Operations Headquarters*
natoexhibitionff14[.]com	**natoexhibition.org** *Domena używana podczas konferencji NATO: NATO Future Forces 2014 Exhibition & Conference*
login-osce[.]org	**osce.org** *Domena OBWE w Europie*

Mieliśmy także okazję przeanalizować przykłady email inicjujących atak. W każdym przypadku były to bardzo dobrze przygotowane wiadomości, z załącznikami, które odpowiadały treści email. Wiadomości odnosiły się do aktualnych wydarzeń interesujących dla celu ataku lub związanych z jego działalnością. Załącznik zawierał kod exploit dla MS Office lub PDF, który inicjował kolejne fazy ataku. Przykładem takiego załącznika do maila spearphishing użytego w czasie ataku na polską instytucję rządową w sierpniu 2014, jest notatka opisująca działania Malezji i Holandii w sprawie zestrzelenia samolotu linii malezyjskich nad Ukrainą.



Malaysia, Netherlands call for immediate cessation of hostilities at crash site

Malaysia and the Netherlands have called for immediate cessation of hostilities in and around the crash site of Malaysia Airline (MAS) Flight MH17 in Torez, Ukraine, lest such tension escalates into war between the Ukrainian government and the separatist groups.

Malaysian Prime Minister Datuk Seri Najib Tun Razak said both countries also asked that all sides, the Ukraine government and separatists, respect the lives lost and integrity of the site, so that the investigation into the disaster may proceed.

"The long walk towards justice begins with this step," Najib said in a statement at joint press briefing with his Dutch counterpart Mark Rutte here Thursday.

The MAS flight, MH17, was flying from Amsterdam to Kuala Lumpur when it went down in Donetsk, eastern Ukraine near the Russian border on July 17.

The Boeing 777-200 aircraft which was carrying 298 people - 283 passengers and 15 crew - was believed to have been shot down, but until today no one has claimed responsibility.

A total of 195 Dutch nationals were on board the flight.

Najib said for the sake of the grieving families, it was imperative that all remains at the crash site were repatriated as soon as possible.

Rys. 1 Zainfekowany załącznik do email użyty w ataku na polską instytucję rządową w sierpniu 2014 (źródło: raport FireEye „APT28: A Window Into Russia's Cyber Espionage Operations?")

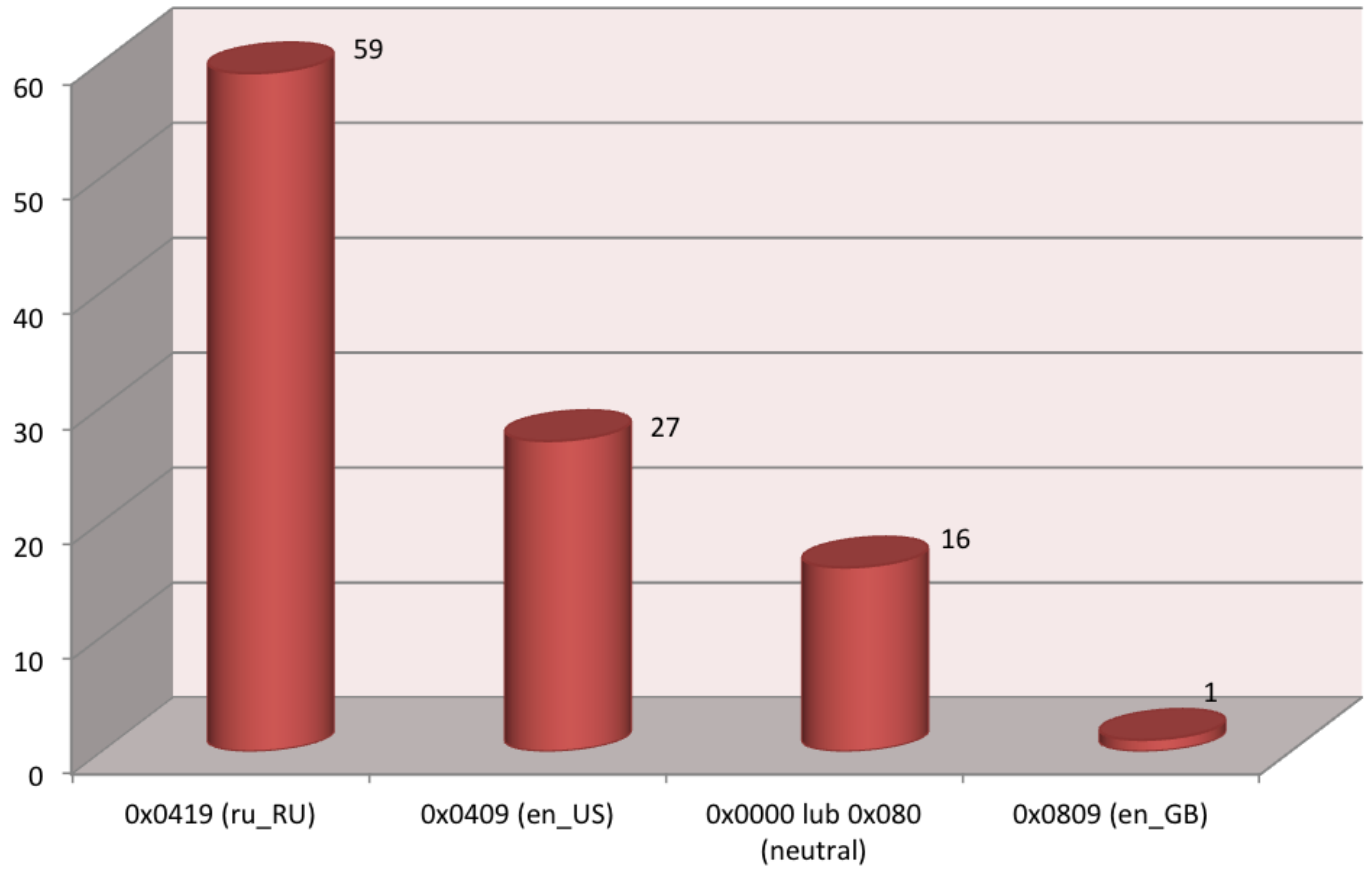
Ślady prowadzące do Rosji

Analiza ataków grupy APT28, a w szczególności analiza statyczna i *reverse engineering* kodu, jaki stosuje w swoich działaniach, wskazują na powiązania tej grupy z terytorium Rosji.

Wykorzystanie języka rosyjskiego

Na potrzeby raportu zostały przeanalizowane 103 próbki malware wykryte w atakach grupy APT28. Prawie połowa z nich miała rosyjskie ustawienia językowe. Pozostałe próbki używały neutralnych ustawień (zgodnych z ustawieniami lokalnego systemu), ustawień US i GB.

Poniższy wykres podsumowuje wyniki analizy ustawień językowych:



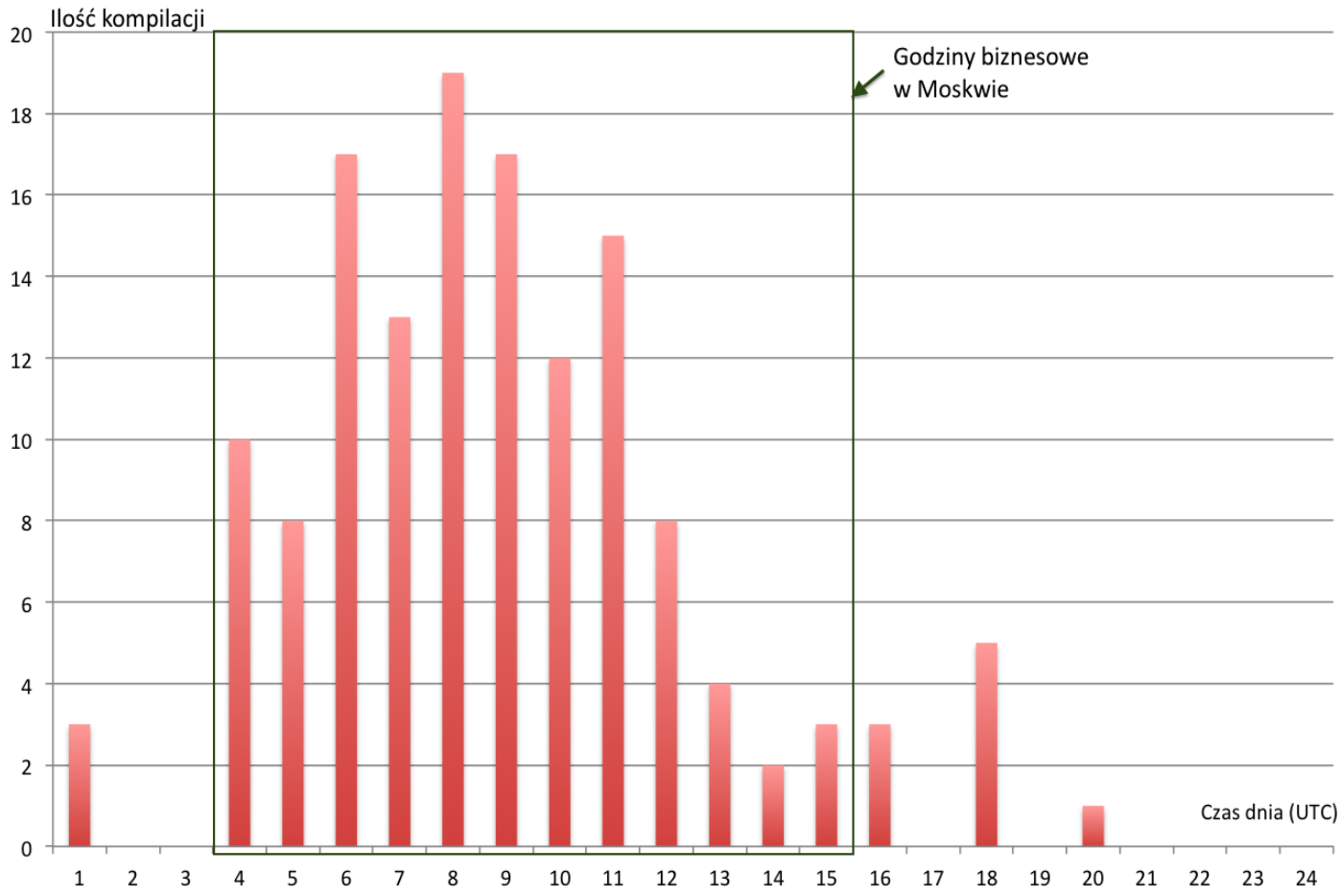
Rys. 2 Rodzaje ustawień językowych (locale ID) w odniesieniu do ilości analizowanych próbek malware APT28 (źródło: raport FireEye „APT28: A Window Into Russia's Cyber Espionage Operations?")

W analizowanym kodzie próbek były również wykryte stringi pisane cyrylicą. Zauważalne jest stopniowe wycofywanie takich wpisów i zastępowanie ich zwrotami angielskimi w nowszych wersjach kodu.

Czasy kompilacji kodu

Kolejnym śladem, na podstawie którego można wnioskować o związkach grupy APT z Rosją, są wyniki analizy czasów kompilacji kodu ataków APT28.

Ze 140 próbek kodu złośliwego, jakie powiązaliśmy z APT28, 89% było kompilowanych między 4:00 a 14:00 czasu UTC, co odpowiada 7:00 – 17:00 czasu moskiewskiego (aktualnie UTC+3, ale wcześniej także UTC+4 ze względu na zmiany w sposobie przechodzenia z czasu letniego na zimowy w Rosji w ostatnich latach). Ponad 96% tych próbek było skompilowanych między poniedziałkiem a piątkiem.



Rozkład godzin kompilacji próbek malware z ataków APT28
(źródło: raport FireEye „APT28: A Window Into Russia's Cyber Espionage Operations?")

Taki godzinowy i dzienny rozkład czasów kompilacji sugeruje, że były wykonywane przez „pracowników", w czasie kiedy przebywali w „biurze" i zajmowali się swoimi „codziennymi obowiązkami".

Podsumowanie

Polska i Europa Środkowo-Wschodnia są narażone na zaawansowane ataki APT prowadzone zarówno przez grupy zajmujące się szpiegostwem gospodarczym jak również politycznym. Opisany przykład działań grupy APT28 to tylko jeden z kilku przypadków APT w Polsce[7] nagłośnionych ostatnio w mediach.

Aktualna sytuacja polityczna w naszym regionie, udział Polski w międzynarodowych forach i instytucjach, powiązania handlowe naszych firm z firmami z EU i USA powodują, że jesteśmy celem ataków różnych grup. Musimy być tego świadomi i musimy odpowiedzialnie przygotowywać się do odpierania takich nieproszonych gości.

Przedstawione w artykule cechy grupy APT28 – jej cele, cechy charakterystyczne ataków, czy nawet godziny kompilacji kodu malware – mogą wskazywać na powiazania tej grupy z rządem Federacji Rosyjskiej. Informacje, których poszukuje grupa, odpowiadają aktualnym zainteresowaniom rządu Rosji. Sam fakt, że grupa APT28 istnieje i rozwija swoje narzędzia, zmienia cele ataków i dostosuje je do aktualnych wydarzeń na świecie od ponad 7 lat wskazuje, że jej działania są sponsorowane i koordynowane.

Oczywiście byłoby nieodpowiedzialne twierdzenie, że jesteśmy narażeni tylko na ataki sponsorowane z Rosji. Cybergrupy są utrzymywane przez wiele innych krajów. Ich działalność jest traktowana na równi z działaniami wywiadów (często są one jednostkami wywiadu) czy oddziałów specjalnych. I tylko od czasu do czasu ujawniane są przypadki i ślady ich działalności. Niemniej nawet te rzadkie sytuacje wyraźnie wskazują na rosnącą aktywność takich grup także w Polsce i w naszym regionie.

Cały tekst raportu na temat działalności grupy APT28 można znaleźć na stronach FireEye: *https://www.fireeye.com/resources/pdfs/apt28.pdf*

[7] Inne przykłady to: operacja Ke3Chang opisana przez FireEye, ataki SandWorm na instalacje SCADA według raportu iSight Partners, ataki grupy DragonFly na firmy energetyczne wg raportu Symantec

Z SZEFEM BIURA BEZPIECZEŃSTWA NARODOWEGO, GEN. STANISŁAWEM KOZIEJEM ROZMAWIA CIIP FOCUS:

CYBER DOKTRYNA RP

- Jakie są Pana zdaniem największe zagrożenia z cyberprzestrzeni, które mogą dotknąć RP oraz związane z nimi wyzwania i trudności dla Polski?

- Musimy pamiętać, że nie tylko instytucje państwa i podmioty prywatne, ale i społeczeństwo staje się coraz bardziej zależne od cyberprzestrzeni. Można postawić tezę, że w cyberprzestrzeni będą istniały takie same zagrożenia jak w świecie realnym. Zarówno zagrożenia dla państwa jako całości – rywalizacja miedzy państwami, presja polityczno-militarna, zastraszanie, aż do ataków destrukcyjnych, zakłócających funkcjonowanie – jak i zwykła przestępczość, np. kradzieże danych, pieniędzy. Jednym z wyzwań jest także przeniesienie się protestów społecznych do cyberprzestrzeni. Szczególnie narażone są też firmy prywatne. Możemy tu mówić np. o wykradaniu danych, kopiowaniu produktów, itp.

- Czyli z tymi zagrożeniami, które tak naprawdę nie są nowe, ma się zmierzyć Doktryna Cyberbezpieczeństwa RP. Czy może Pan przybliżyć jej projekt?

- Doktryna jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego. Określa ona cele w dziedzinie cyberbezpieczeństwa. Stanowi też podstawę ideową, wspólny mianownik dla podejmowanych przez instytucje państwa działań. Stworzenie w Polsce takiego jednolitego podejścia do spraw cyberbezpieczeństwa powinno umożliwić dobre przygotowanie konkretnych już dokumentów wdrażających. Jak np. Polityka Ochrony Cyberprzestrzeni RP, ale nie tylko. Uważam, że Polityka nie obejmuje całości spraw związanych z cyberbezpieczeństwem. Dotyczy przede wszystkim sfery cywilnej i publicznej. Wydaje się, że oprócz Polityki pojawi się potrzeba opracowania dokumentu dotyczącego np. cyberobrony. Ministerstwo Obrony Narodowej z pewnością taki plan będzie przygotowywało.

Co więc charakterystyczne dla Doktryny, to kompleksowe, zintegrowane podejście. Konieczne jest połączenie w jeden całościowy system wielu wymiarów: cyberochrony i cyberobrony; wymiarów – wojskowego i cywilnego. Kolejną kwestią jest połączenie sfery publicznej i prywatnej. Bezpieczeństwa prywatnych podmiotów, przedsiębiorstw, instytucji, nie można uregulować aktami urzędowymi, tak jak można to zrobić w stosunku do administracji. Tutaj Doktryna proponuje korzystanie z katalogu „dobrych praktyk", zachęcanie do współpracy sektorów prywatnego i publicznego. No i to wszystko jeszcze uzupełnione wymiarem obywatelskim, indywidualnym. Państwo musi oferować obywatelom pomoc, wsparcie, edukację, zachęty, czy też musi wykorzystywać inicjatywy obywatelskie.

- Wspomniał Pan o wymiarze obywatelskim i stwierdził, że tej sfery nie można uregulować tak jak administracji i trzeba szerzej spojrzeć na zaangażowane podmioty. Jednym z krajów, który ciężko doświadczył tych zagrożeń, zarówno w sferze ochrony i obrony, jest Estonia. Jednym z pomysłów , który tam się pojawił jest ochotnicza cyber armia, czyli Estońska Liga Obrony Cybernetycznej. Jak ta koncepcja się Panu podoba, czy jest ona do zrealizowania na polskim gruncie, czy doktryna wspomina o tego typu łączeniu sił zarówno administracji, jak i stowarzyszeń, fundacji, think-tanków.

- Pracując w BBN nad projektem Doktryny wykorzystaliśmy także doświadczenia innych państw, w tym m.in. Estonii. Staramy się zachęcać zarówno obywateli, jak i struktury państwa do współpracy, współdziałania, co łączy się ze wspomnianym wykorzystywaniem inicjatyw obywatelskich.

W Polsce jest podatny grunt na tego typu działania, co stało się szczególnie widoczne w kontekście kryzysu bezpieczeństwa w Europie i rosyjskiej agresji na Ukrainę. Widać, że obywatele w większym stopniu niż to było rok czy dwa lata temu, poczuwają się do osobistego angażowania w zapewnienie bezpieczeństwa Państwa, w tym także cyberprzestrzeni. Niedawno miałem możliwość obserwowania ćwiczeń organizacji proobronnych w Ostrowcu Świętokrzyskim, gdzie pojawił się także element działań w cyberprzestrzeni.

- Elementem, o którym Pan wspomina jest cyberobrona. Czy mógłby Pan zarysować, jak wyobraża Pan sobie rolę sił zbrojnych w ochronie cyberprzestrzeni. Jak powinna wyglądać współpraca ze sferą cywilną ochrony cyberprzestrzeni i jednocześnie z podmiotami gospodarczymi. Czy nie wydaje się Panu że w sytuacji krytycznej przedsiębiorcy powinni liczyć na pomoc armii?

- Rola sił zbrojnych w cyberbezpieczeństwie jest oczywiście bardzo duża, wręcz podstawowa w dziedzinie cyberobrony państwa. Siły zbrojne muszą zapewnić sobie bezpieczne funkcjonowanie, ale oczekuje się także od nich, aby stanowiły potencjał państwa, mogący zapobiec agresji w cyberprzestrzeni skierowanej wobec różnych elementów państwa, prywatnych firm i obywateli. Muszą mieć więc zdolności ofensywne, kontruderzeniowe.

Polska musi mieć zdolność odwetowej operacji w cyberprzestrzeni. I to, moim zdaniem, jest jedno z wyzwań, przed jakimi stoją dzisiaj wszystkie państwa. Mechanizm ten dobrze pokazały ostatnie wydarzenia, gdzie Korea Północna, która prawdopodobnie – co jest niezwykle trudne do udowodnienia – zastraszyła dużą firmę, spotkała się ze zdecydowaną odpowiedzią. Musimy pamiętać – co pokazuje historia wojen – że sama obrona jest niewystarczająca. Trzeba mieć zdolności zarówno obronne, jak i ofensywne. I dlatego w Doktrynie wskazujemy na konieczność budowania nie tylko potencjału obronnego, ale także zdolności kontruderzeniowych.

Oczywiście siły zbrojne nie mogą pełnić roli głównego koordynatora spraw cyberbezpieczeństwa w państwie. Tutaj dostrzegamy konieczność stworzenia systemu koordynacji podnadresortowej w zakresie cyberbezpieczeństwa. Zwracaliśmy na to uwagę już wcześniej m.in. w Strategicznym Przeglądzie Bezpieczeństwa Narodowego czy Białej Księdze. Widzimy konieczność utworzenia na szczeblu Rady Ministrów instytucji, która zajmowałaby się całościowym patrzeniem na wszystkie wymiary bezpieczeństwa, w tym na cyberbezpieczeństwo. Wskazujemy np. w Białej Księdze, że powinno to być swego rodzaju Rządowe Centrum Bezpieczeństwa Narodowego, z kompetencjami znacznie szerszymi niż tylko z zakresu zarządzania kryzysowego. Być może to jest kierunek, w którym powinniśmy iść. Bo jeśli chcemy całościowo, ponadresortowo regulować funkcjonowanie państwa w cyberprzestrzeni, to musi powstać instytucja państwa za to odpowiedzialna. Musimy także przygotować ludzi odpowiedzialnych za cyberbezpieczeństwo, uruchamiać nowe kierunki studiów. Jednym słowem tworzyć kompetencje narodowe w tej dziedzinie. Jedną z najważniejszych, bardzo specjalistycznych kompetencji, które musimy w kraju rozwijać jest kryptografia.

- Jak długo będzie trwało wdrożenie Doktryny cyberbezpieczeństwa RP?

- Jest to proces, który się nie kończy. Natomiast najważniejszy jest początek tego procesu, początek budowania zintegrowanego systemu, o którym mówimy. Na pewno Doktryna cyberbezpieczeństwa da pewien impuls. Wydaje się, że nadal będą budowane „wyspy" cyberbezpieczeństwa, o których teraz mówi się w teorii. Chciałbym, żeby już w przyszłym roku powstała instytucja, która mogłaby spinać w całość to, o czym mówimy, która zapewni ponadresortową zdolność realnego działania. Ze względu na wybory, 2015 r. jest trudny. Ale mam nadzieję, że jeżeli nie w 2015 to w 2016 r. takie instytucje powstaną – zarówno o charakterze politycznym, jak i o charakterze sztabowym. Bez tego trudno sobie wyobrazić realne nadążanie za szybko wzrastającymi potrzebami cyberbezpieczeństwa.

- Czy w związku z potrzebą tych wszystkich zmian widzi Pan konieczność skorzystania przez prezydenta z własnej inicjatywy ustawodawczej,

- Prezydent z pewną inicjatywą już wystąpił. Myślę tu o wprowadzeniu do ustawy o stanach nadzwyczajnych kategorii cyberprzestrzeni. Drugi krok prezydenta to właśnie Doktryna, która powinna dać impuls do działania. Natomiast praktyczne regulowanie życia państwa w cyberprzestrzeni jest jednak kompetencją rządu. Rząd może dużo tu zrobić nawet bez regulacji ustawowych. Mam na myśli tworzenie rozwiązań ponadresortowych. Ale jeżeli będą konieczne regulacje prawne, na przykład do zapewnienia systemowej współpracy sektora publicznego z sektorem prywatnym, to być może ze strony prezydenta taka inicjatywa się pojawi, ale pierwszy ruch należy do rządu.

- Dziękujemy bardzo.

Z gen. Stanisławem Koziejem rozmawiali: Anna Adamkiewicz (RCB) i Tomasz Szewczyk (RCB).

wyższa szkoła jazdy:

Security Operational Center

W poprzednim numerze CIIP focus, Tadeusz Włodarczyk pisał na temat rozwiązania SIEM. To bardzo ważne i pożyteczne rozwiązanie, które jest w stanie gromadzić i systematyzować informacje dotyczące zdarzeń związanych z cyberbezpieczeństwem organizacji. Oczywistym wnioskiem z rozważań nad coraz bardziej popularnym SIEM-em jest to, że sam w sobie nie jest on w stanie odpowiednio zwiększyć cyberbezpieczeństwa organizacji. Może jednak stać się punktem centralnym kluczowego rozwiązania, ale musi być odpowiednio wykorzystywany nie tylko technicznie, ale i organizacyjnie. Powinien być wpięty w większy system, w którym sama technologia jest tylko elementem.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Czymś co realizuje ten postulat jest SOC (Security Operational Center) czyli komórka organizacyjna, która przy wykorzystaniu odpowiedniej technologii, wspartej przez prawidłowo opracowane i wdrożone procesy i procedury, i co najważniejsze - zasilona wysokiej klasy specjalistami od bezpieczeństwa teleinformatycznego, jest w stanie stać się punktem centralnym systemu cyberbezpieczeństwa dowolnej organizacji. Spójrzmy na każdy z tych wymienionych kluczowych elementów i zastanówmy się co jest w nich najważniejsze.

Technologia

Wspomniałem już, że rozwiązanie typu SIEM może stać się kluczowym rozwiązaniem SOC-a - swoistym sercem systemu. Takich rozwiązań jest oczywiście wiele i trudno wskazać konkretnie, które jest najlepsze. Ich analiza jest prawdziwym wyzwaniem, a wybór najczęściej próbą połączenia nowatorskich funkcji produktów z realnym i skutecznym działaniem. Z pewnością kilka cech SIEM-a jest koniecznych do rozpatrzenia przy wyborze. Osobiście zwróciłbym uwagę na następujące:

- współpraca z wybranymi, być może już istniejącymi w organizacji, rozwiązaniami z zakresu bezpieczeństwa, takimi jak IDS/IPS, HIDS/HIPS, Antivirus, urządzenia sieciowe, kluczowe aplikacje, firewalle, systemy kontroli dostępu (w tym np.: SSO), system anty-DDoS (jeśli istnieje);
- wysoka jakość funkcji korelacji zdarzeń, która jest kluczowa dla wspierania prawidłowego reagowania na incydenty;
- przejrzystość i intuicyjność rozwiązania, dzięki której specjaliści będą mieli ułatwioną pracę;
- funkcje wspierające zadania związane z analizą śledczą komputerów i sieci i inne zadania związane z zaawansowanym zarządzaniem incydentami, które stanowią drugą linię wsparcia.

To nie wszystko – istnieje bardzo dużo funkcji, które być może nie są rzeczą oczywistą patrząc na „standard SIEM", a które mogą okazać się kluczowe dla konkretnej organizacji. Dobrym przykładem tego typu rozwiązania są produkty klasy MDM, służące do zarządzania urządzeniami przenośnymi, w tym do zarządzania bezpieczeństwem tych urządzeń. W dobie rozwiązań typu BYOD, dla niektórych może to być kluczowe rozwiązanie.

Następnym elementem niezwykle ważnym w funkcjonowaniu SOC-a jest dobrze działająca i zorganizowana wizualizacja zdarzeń. W centralnym punkcie, w którym „obrabia" się naraz setki, a czasami i tysiące zdarzeń, wsparcie w postaci wizualizacji jest niezwykle ważne – właściwie konieczne. Dzięki niemu możliwe jest wychwytywanie najważniejszych zjawisk, co z kolei wpływa na prawidłową priorytetyzację zadań w konkretnym momencie oraz na obserwowanie trendów w dłuższym okresie. Może to być bardzo istotne w podejmowaniu strategicznych decyzji dotyczących optymalizacji zadań i rozwoju SOC.

Procesy, procedury, serwisy

Drugim kluczowym elementem dla działania SOC-a są procesy, procedury i serwisy. Działanie SOC to olbrzymia liczba reakcji i decyzji każdego dnia. Przy ich podejmowaniu, w większości przypadków, nie powinno być żadnych wątpliwości i decyzje takie powinny być podejmowane wręcz automatycznie. Zresztą niektóre z nich da się w rzeczywistości zautomatyzować i to zaprogramowane maszyny mogą je podejmować – np.: decyzje związane odcinaniem zasobów sieciowych, które mogą stanowić poważne zagrożenie dla infrastruktury organizacji. Aby taka sprawności decyzyjna była możliwa, konieczne jest ujęcie większości sytuacji w ryzach procedur, w których dobrze są uwzględnione wszystkie czynności.

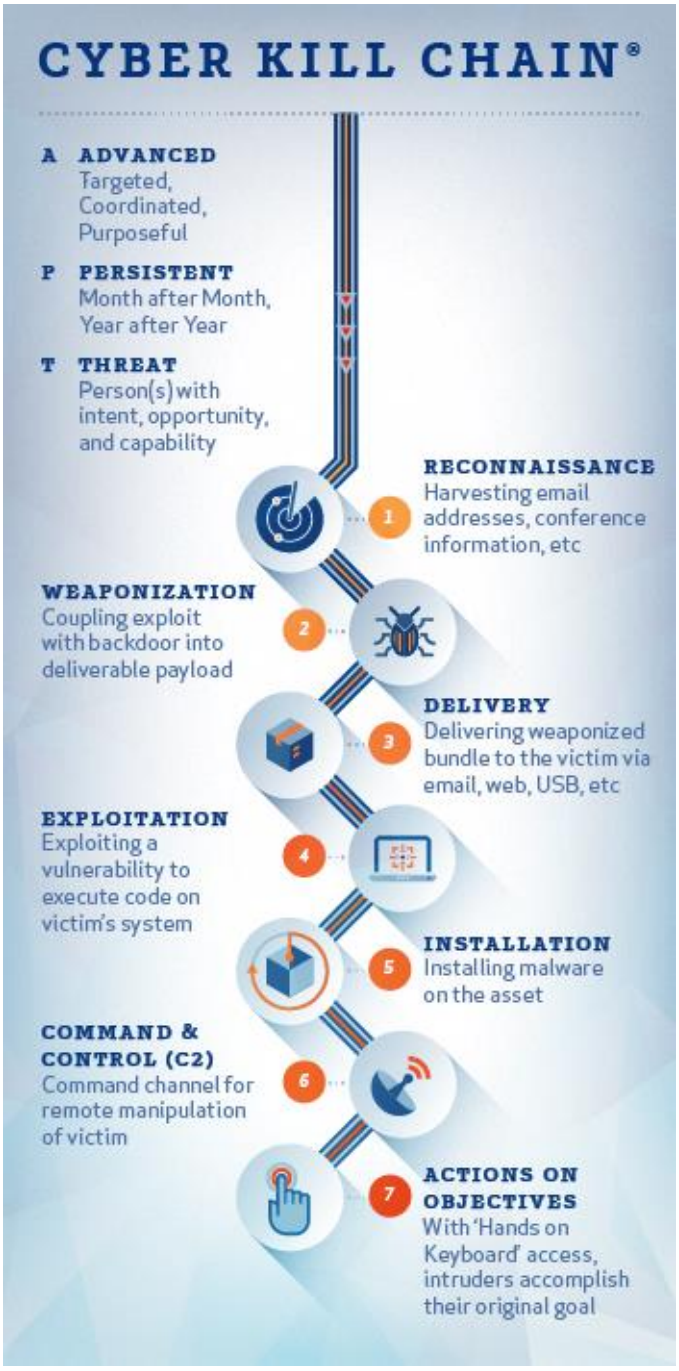
Jest kilka grup procedur, które z pewnością powinny się znaleźć w zestawie obowiązującym w SOC:
• procedury operacyjne – dotyczą one zasad funkcjonowania SOC-a, systemu zmian, dostępu do pomieszczeń, zapewnienia ciągłości działania, bezpieczeństwa fizycznego i technicznego, itp.;
• procedury zarządzania incydentami – kluczowe procedury dla funkcjonowania SOC-a opisujące zarówno sposób nadawania priorytetów dla incydentów, ich klasyfikowania jak i zasady zarządzania poszczególnymi incydentami;
• procedury raportowania – dotyczą zarówno tego jak będziemy raportowali zdarzenia obsługiwane przez SOC jak i to jak będziemy je przyjmowali. Trzeba pamiętać, że SOC oprócz naturalnego przyjmowania do „obróbki" incydentów, które są raportowane przez urządzenia do tego przewidziane, powinien być również przygotowany na „ręczne" zgłaszanie incydentów przez członków „constituency", czyli technologicznego obszaru działania za jaki jest odpowiedzialny SOC. SOC również podejmuje działania we współpracy z innymi ośrodkami bezpieczeństwa poza organizacja – to również powinno być objęte procedurami.

Oprócz tych trzech podstawowych grup można wydzielić jeszcze wiele innych. Od odpowiedzialnych za SOC zależy na ile chcemy dokonywać dalszego podziału grup procedur i na ile jesteśmy w stanie precyzyjnie określić te procedury. Bardzo prawdopodobnym, a być może również rozsądnym działaniem jest przygotowanie zestawu podstawowych, koniecznych procedur, które obowiązywać będą od samego początku funkcjonowania SOC-a i uzupełnienie tych procedur o nowe, które w trakcie pierwszej fazy funkcjonowania SOC-a okazały się niezbędne. Zresztą proces ciągłej poprawy istniejących procedur i uzupełniania (a być może i rezygnowania z niektórych procedur) powinien towarzyszyć całemu okresowi działania SOC-a.

Najlepszym rozwiązaniem, zarówno dla wszystkich procedur operacyjnych jak i tych, które mają dotyczyć monitoringu cyklu życia SOC-a, jest zastosowanie znanej, uniwersalnej strategii – OODA , czyli observe-orient-decide-act (obserwuj, rozpoznaj, zdecyduj i zadziałaj).

Procedury pozwolą nam na wypełnienie poszczególnych zadań, natomiast osiągnięcie celów postawionych SOC-owi, możliwe będzie dzięki przygotowaniu procesów. Dopiero wtedy do zaimplementowanych procedur będziemy mogli przypisać osoby i sprawić, że centrum zacznie funkcjonować. Będzie możliwe to, gdy na bazie całej informacji wejściowej, która trafia do SOC-a wypracujemy końcowe decyzje i działania, które z założenia powinny rozwiązać problemy, a jeśli rozwiązanie tych problemów wykracza poza możliwości SOC-a, bo na przykład konieczna jest decyzja na wyższym szczeblu, to będziemy wiedzieli jak dalej rozwiązywać problem. Warto też pamiętać o niezwykle ważnym elemencie dotyczącym procedur i procesów, jakim jest konieczność dostosowywania działania SOC do wymagań prawnych. Każda z organizacji wie najlepiej jakie spoczywają na niej obowiązki prawne, które dotyczą bezpieczeństwa teleinformatycznego.

W przygotowywaniu procedur i procesów dobrym pomysłem jest aby odnieść się do dość dobrze rozpoznanego w ostatnich latach procesu ataku teleinformatycznego, określonego jako kill chain. Nowoczesne strategie obronne nawiązują właśnie do tego procesu. Wyjaśnia on poszczególne fazy ataku. Uwzględnienie tych faz zarówno w działaniach wykrywających jak i przeciwdziałających atakom jest kluczowe w osiągnięciu sukcesu .



Fazy ataku teleinformatycznego określane jako "kill chain" (źródło: lockheedmartin.com)

Wszystkie procedury i procesy powinny odnosić się do serwisów jakie zdecydowaliśmy, że będzie świadczyć SOC. Wachlarz wyboru jest bardzo duży. SOC jest w stanie świadczyć całą gamę serwisów. Niektóre są oczywiste – na przykład obsługa incydentów, niektóre zaś wymagają świadomej decyzji, za którą powinny iść chociażby działania inwestycyjne w ludzi i sprzęt. Dobrym przykładem może być w tym przypadku wykonywanie testów penetracyjnych w powierzonym nam do ochrony środowisku. W zasadzie działanie SOC-a możemy ograniczyć do świadczenia dwóch serwisów – serwisu ciągłego monitoringu bezpieczeństwa zasobów w czasie rzeczywistym oraz serwisu reagowania na incydenty komputerowe. Jest to zestaw minimum. W praktyce może on być rozbudowywany o wielu serwisów z obszaru bezpieczeństwa teleinformatycznego. Ważne jest tylko, aby w tym rozszerzaniu usług nie naruszyć granicy pomiędzy SOC i NOC (Network Operation Center)[8]. Oprócz już wspomnianych - usługami, które bardzo często pojawiają się w zestawie świadczonych przez SOC serwisów są:

- informatyka śledcza (komputerowa i sieciowa);
- *threat intelligence* (sieciowe działania wywiadowcze), dzięki którym w sposób aktywny możemy wykorzystywać dane zewnętrzne, dotyczące naszych zasobów (np.: w postaci implementowania na urządzeniach wykrywających i filtrujących IoC (*indicators of compromise*), czyli wskaźników ataków komputerowych;
- testy penetracyjne – wykonywane na zlecenie, wg stałego schematu lub wyrywkowo wobec zasobów, które w naszej ocenie są szczególnie narażone w danym momencie;
- organizacja szkoleń, np.: technicznych szkoleń w formie ćwiczeń z ochrony w cyberprzestrzeni.

Ludzie

Truizmem jest stwierdzenie, że nawet najlepsza technologia obudowana przez procesy i procedury nie jest w stanie zapewnić świadczenia usług. Konieczna jest do tego wykwalifikowana kadra, która zapewni odpowiednie działanie wszystkich elementów SOC-a. Temat kadry SOC-a jest na tyle obszerny i ważny, że z pewnością wymaga szczegółowego przedstawienia, nawet jeśli decydujemy się omówić tylko podstawowe elementy prawidłowego działania SOC. W tym krótkim artykule jest miejsce tylko na zasygnalizowanie najważniejszych kwestii.

Przede wszystkim warto pamiętać, że pracownicy SOC to specjaliści od bezpieczeństwa teleinformatycznego, a nie inżynierowie sieciowi. Tym drugim pozostawmy możliwość pracy w NOC, o czym jest mowa w rekomendowanym artykule (patrzy przypis: 8). Wśród pracowników SOC podział kompetencyjny jest dość prosty. Wg znanej, amerykańskiej organizacji MITRE jest to de facto pięć grup specjalistów[9]:

- I-wsza linia wsparcia – pracownicy, którzy mają za zadanie reagować na wszystkie pojawiające się zdarzenia. W większości przypadków ich działania są standardowe i stanowią swoisty filtr, na wyjściu którego znajdują się tylko te przypadki, które zmuszają do działania specjalistów z II-giej linii wsparcia.
- II-ga linia wsparcia – zarządzają przypadkami, które wymagają zaawansowanej wiedzy dotyczącej reagowania na incydenty. W tej grupie pracują specjaliści z doświadczeniem.
- Grupa specjalistyczna – specjaliści z wąskich dziedzin takich jak informatyka śledcza, analiza złośliwego oprogramowania, sieciowe działania wywiadowcze, itp. Grupa ta często określana jest jako CTAC (Cyber Threat Analysis Center).
- Grupa administratorów SOC – specjaliści odpowiedzialni za utrzymanie całej infrastruktury teleinformatycznej SOC, co przy dużych organizacjach jest wyzwaniem samym w sobie.
- Grupa inżynierów SOC – grupa odpowiedzialna za ciągłą rozbudowę SOC. Jako, że bezpieczeństwo teleinformatyczne, chociażby ze względu na ciągłe pojawianie się nowych zagrożeń, jest jedną z najbardziej dynamicznych dziedzin rozwoju informatyki, to zadanie stałego dbania o aktualność i skuteczność stosowanych w SOC rozwiązań jest wyjątkowo ważna.

Personel pracujący w SOC, to w większości przypadków osoby, które stale dążą do poszerzania swojej wiedzy z dziedziny bezpieczeństwa teleinformatycznego. Jednocześnie, ze względu na charakter pracy, są stale narażeni na stres związany z koniecznością szybkiego reagowania w sytuacji kryzysowej. Biorąc pod uwagę te dwa czynniki, dostajemy obraz stanowisk pracy, na których łatwo o pewnego rodzaju zawodowe wypalenie lub znudzenie pracą powtarzalną w pierwszej linii wsparcia. Warto o tym pamiętać i zapobiegać problemom z tym związanym, na przykład poprzez rotację zadań, czy wypracowanie jasnych i atrakcyjnych ścieżek kariery wewnątrz organizacji.

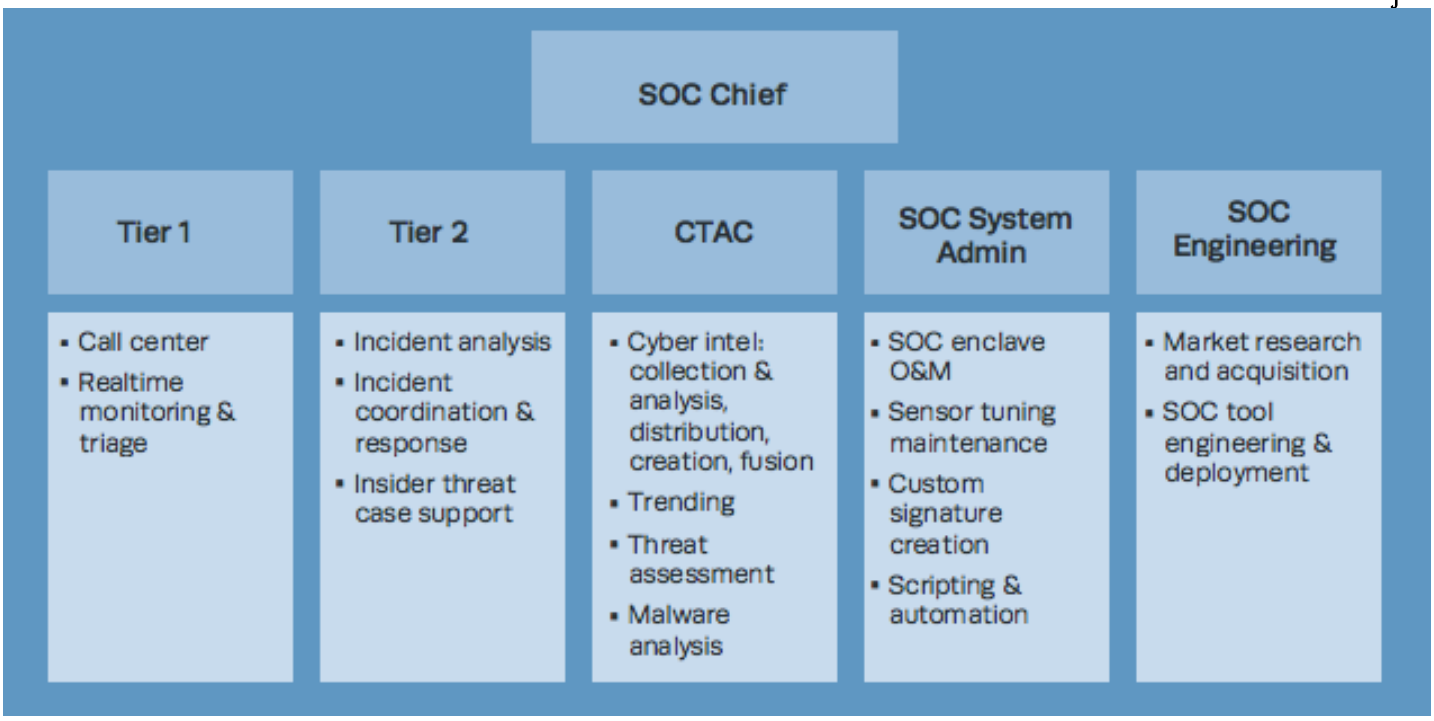
Podsumowanie

Ze względu na swoje ograniczenia objętościowe w artykule tylko zasygnalizowano najważniejsze aspekty funkcjonowania Security Operation Centers. Każdy z poruszanych tematów jest materiałem na dłuższe opracowania. Wiedza na temat podstaw funkcjonowania SOC-a zamyka się zazwyczaj na co najmniej kilkuset stronach tekstu.

Podsumowując, trzeba jasno powiedzieć, że budowanie i utrzymywanie SOC-a jest z pewnością jednym z najsilniejszych trendów w budowaniu zdolności dużych organizacji do odpierania cyberataków. Posiadając SOC, lub korzystając z zewnętrznych usług SOC-a, tworzymy scentralizowany ośrodek wiedzy na temat bezpieczeństwa swojej organizacji, który jednocześnie staje się również naszym „interfejsem" ze światem zewnętrznym w obszarze cyberbezpieczeństwa. Dla wielu ta organizacja przywołuje skojarzenia z tak często pojawiającym się na łamach CIIP focusa tematem funkcjonowania zespołów typu CERT. Nie przypadkowo – wiele zasad działania SOC-a i CERT-u jest bardzo podobnych – np.: działanie II linii wsparcia czy grupy specjalistycznej CTAC, ale to temat na inne opracowanie. W każdym razie, chcąc zbudować kompetentny ośrodek, który będzie szybko i skutecznie reagował na pojawiające się w organizacji cyberzagrożenia nie sposób nie rozważyć koncepcji SOC. Zachęcam do analizy takiego rozwiązania.

[8] w tej kwestii warto zapoznać się z artykułem: „SOC Mistake #10: You confuse your SOC with your NOC" - https://jimmyblake.wordpress.com/2012/05/18/soc-mistake-10-you-confuse-your-soc-with-your-noc/

[9] „Ten strategies of a World –Class Cybersecurity Operation Center": http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf



Struktura organizacji personelu SOC (źródło: mitre.org)

WARTO PRZECZYTAĆ:

METODYKA ATAKÓW NA SIECI ENERGETYCZNE

Na jednej z amerykańskich uczelni powstała praca magisterska dotycząca metodyki cyberataków na sieci energetyczne. Autor, wychodząc z założenia, że sieci energetyczne zawsze były obiektem ataków w czasie konfliktów militarnych i faktu, że sieci te stały się w bardzo dużym stopniu uzależnione od działań sieci teleinformatycznych i technologii informatycznych, przedstawia w jaki sposób może przebiegać atak na nie, właśnie w cyberprzestrzeni. W swojej pracy przedstawia znane przykłady ataków na sieci energetyczne (Irak, Bośnia, Jugosławia i Libia) wchodzących w skład obiektów militarnych. Pokazuje również jak mogłyby być prowadzone ataki na poszczególne elementy funkcjonowania takich sieci od strony technicznej.

https://vtechworks.lib.vt.edu/bitstream/handle/10919/49435/Saglam_M_T_2014.pdf?sequence=1

INICJATYWY CYBERBEZPIECZEŃSTWA W AMERYKAŃSKIEJ INFRASTRUKTURZE KRYTYCZNEJ

Stany Zjednoczone są znane z tego, że w sposób bardzo zaawansowany zajmują się sprawami cyberbezpieczeństwa infrastruktury krytycznej. Dlatego warto prześledzić tamtejsze inicjatywy z tej dziedziny. W notatce zamieszczonej w serwisie breakingenergy.com można przeczytać o programie wymiany informacji o zagrożeniach cyberprzestrzeni - Cybersecurity Risk Information Sharing Program, założeniach dokumentu "Energy Sector Cybersecurity Framework Implementation Guidance" i o kilku innych dokumentach i inicjatywach, które są wynikiem współpracy sektora prywatnego i publicznego. Praktycznie wszystkie przykłady są warte implementacji na poziomie poszczególnych organizacji. Są również pomysłami na budowę współpracy publiczno-prywatnej.

http://breakingenergy.com/2014/11/21/protecting-the-grid-from-all-hazards/

Relacja z konferencji w Amsterdamie

Black Hat Europe 2014

Paweł Krawczyk
Fundacja Bezpieczna Cyberprzestrzeń

Pierwsza konferencja BlackHat Briefings została zorganizowana przez Jeffa Mossa w USA w 1997 rok i od tej pory odbywają się one co roku w Stanach Zjednoczonych, Europie oraz Azji. Mając w tym roku możliwość uczestniczenia w europejskiej edycji w Amsterdamie, chciałbym podzielić się z czytelnikami CIIP focusa ciekawostkami, które były tam prezentowane.

BlackHat kładzie duży nacisk na praktyczny aspekt prezentowanych tematów: mało jest tam wystąpień z obszaru nauk teoretycznych, więcej praktycznych demonstracji konkretnych technik, nowych narzędzi i metod ataków na systemy teleinformatyczne. Poza prezentacjami, które odbywają się w trzech równoległych torach tematycznych, od kilku lat organizowana jest stała wystawa nazywana BlackHat Arsenal, na której można spotkać się z autorami programów oraz narzędzi sprzętowych.

W tym roku konferencję rozpoczął izraelski kryptolog Adi Shamir pokazując ukryty kanał kradzieży danych z budynków, do których atakujący może mieć jednorazowy dostęp np. w celu instalacji oprogramowania szpiegowskiego, ale ze względu na fizyczną izolację budynku nie ma kanału pozwalającego na cykliczne odzyskiwanie wyników jego działania. Atak, dość pomysłowy, wykorzystywał typowy skaner biurowy do dwukierunkowej komunikacji. Komunikacja „do budynku" odbywała się za pomocą lasera działającego na świetle widzialnym lub podczerwieni, która jest przez skanery „widziana". Komunikację „od budynku" zapewniał sam skaner, przekazując dane kodowane za pomocą mrugania lampą towarzyszącą głowicy skanującej. W obu przypadkach, co potwierdziły eksperymenty w terenie, zespół Shamira osiągał widoczność do około 1,5 km.

Adi Shamir w trakcie konferencji Black Hat Europe 2014 (fot. Bankinfosecurity.com)

W kolejnej prezentacji badacz z Hiszpanii pokazywał techniki ataku na protokół TLS, w szczególności na nagłówek Strict Transport Security wprowadzony kilka lat temu jako standard RFC 6797. Nagłówek ten instruuje przeglądarki, że z danym serwerem ma się ona komunikować wyłącznie szyfrowanym kanałem TLS i odrzucać wszelkie próby połączeń

nieszyfrowanych. Jest to dość skuteczna technika blokowania rozpowszechnionych w pewnym okresie rodziny ataków polegających na przechwytywaniu (man-in-the-middle) połączeń klienta do popularnych serwerów i oferowaniu mu połączenia nieszyfrowanego. Ponieważ zabezpieczenie oferowane przez STS jest ograniczone czasowo, atak opiera się głównie na zdolności atakującego do przestawienia zegara ofiary. I jak to często bywa w takim przypadku, próba obejścia STS doprowadziła autora do o wiele ciekawszych obserwacji: popularne systemy operacyjne są na taki atak podatne dzięki... automatycznej synchronizacji czasu za pomocą NTP. Głównie dlatego, że komunikaty NTP można fałszować, a ochrona autentyczności pakietów NTP pomimo, że dostępna w standardzie, nie jest w praktyce stosowana.

Interesującą metodę podsłuchu akustycznego zaprezentował zespół ze Stanford i Rafaela: wykorzystuje ona żyroskopy i akcelerometry instalowane masowo w telefonach komórkowych. Podczas eksperymentów udało się wykazać, że są one wystarczająco czułe by wychwytywać drgania fal dźwiękowych i zamieniać je na sygnał cyfrowy, czyli faktycznie spełniać rolę prymitywnego mikrofonu. W odróżnieniu od normalnych mikrofonów wbudowanych w telefony nie są one przy tym traktowane jako sensory „wrażliwe", więc aplikacje działające w tle mogą je odczytywać bez wiedzy użytkownika, co czyni z nich atrakcyjne narzędzia inwigilacji.

W dziedzinie, która najbardziej mnie interesuje, czyli bezpieczeństwie aplikacji webowych, najbardziej wartościowa była prezentacja nowego ataku Reflected File Download. Wykorzystuje on zapomnianą cechę adresów URL jaką jest znak średnika, interpretowany przez MS Internet Explorer jako sugestia nazwy pliku, który należy pobrać i wykonać. Atak, na które podatny były m.in. serwisy Google i LinkedIn, może ułatwiać instalowanie złośliwego oprogramowania.

Inny ciekawy zaprezentowany atak na aplikacje webowe to SOME (Same Origin Method Execution). Wykorzystuje on niedostatecznie filtrowane callbacki w wywołaniach JSONP w celu obchodzenia ograniczeń wynikających z polityki „identycznego pochodzenia" (same origin policy) narzucanej przez przeglądarki. Skutek: kradzież tokenów uwierzytelniających użytkownika, fałszowanie wiadomości w sieciach społecznościowych i tak dalej.

Paweł Krawczyk w czasie videoblogu relacjonuje konferencję Black Hat Europe 2014 (fot. Fundacja Bezpieczna Cyberprzestrzeń)

Podsumowując, BlackHat jest jedną z tych konferencji, na których regularnie pojawiają się przedstawiciele prywatnego i publicznego sektora bezpieczeństwa teleinformatycznego. Większość prezentowanych dziur jest wcześniej niepublikowana i o ile dziury w produktach komercyjnych są przeważnie udostępniane producentom i łatane przed „premierą" na konferencji, o tyle większość pozostałych ataków ma charakter uniwersalny i może być wykorzystywana przeciwko systemom tych instytucji, które o nich po prostu nie wiedziały.

Paweł Krawczyk przeprowadził cykl relacji video z konferencji Black Hat Europe 2014 w Amsterdamie. Zapis wideo dostępny jest na profilu YouTube Fundacji Bezpieczna Cyberprzestrzeń:
www.youtube.com/user/cybsecurity

WYZWANIA DLA POLITYKI ZAGRANICZNEJ

WSPÓŁCZESNYCH PAŃSTW PŁYNĄCE Z CYBERPRZESTRZENI

Cyberprzestrzeń zrewolucjonizowała funkcjonowanie państw w niemal wszystkich obszarach. Wpływa na bezpieczeństwo narodowe, rozwój gospodarki, jakość życia obywateli. Decydenci coraz częściej dostrzegają wagę świata cyfrowego i działań w nim realizowanych. Widoczny jest wzrastający trend kreowania polityk publicznych uwzględniających różnorodne „cyber problemy". Jednak to co odróżnia dojrzałych graczy, prowadzących zaawansowane działania w cyberprzestrzeni, od państw, które dopiero zaczynają poruszać się w tym obszarze, to zorientowanie się nie tylko na kwestie związane ze sprawami wewnątrz krajowymi, ale także uwzględnienie zagadnień związanych z cyberprzestrzenią w działaniach zewnętrznych. Problemy świata cyfrowego powinny na stałe wpisać się w agendę działań ministerstw spraw zagranicznych – to zadanie, przed którym stoi wiele państw. Stoi przed nim także Polska.

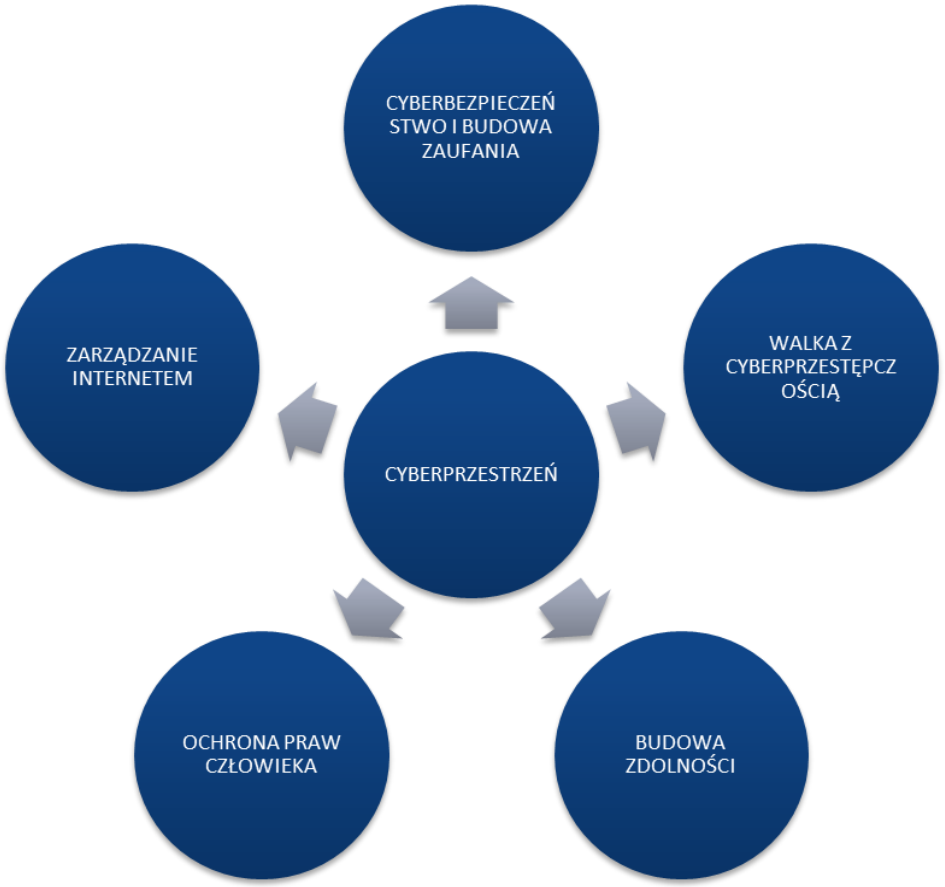
Joanna Świątkowska
Instytut Kościuszki

DIAGNOZA WYZWAŃ

Kluczową kwestią jest zrozumienie tego jak cyberprzestrzeń wpływa na relacje międzynarodowe. Konieczne jest zdiagnozowanie najważniejszych problemów, zmapowanie najistotniejszych aktorów i odszyfrowanie ról jakie oni odgrywają. Z uwagi na ogrom i różnorodność zagadnień, ich współzależności, a także relatywną nowość, przeformułowanie tradycyjnych mechanizmów prowadzenia polityki zagranicznej staje się jeszcze trudniejsze.

Do katalogu aktualnie najważniejszych wyzwań związanych z funkcjonowaniem państw w cyberprzestrzeni, w których podejmowanie zaangażowana powinna być dyplomacja należy[10]:

1. cyberbezpieczeństwo i budowanie zaufania w cyberprzestrzeni;
2. międzynarodowe wysiłki na rzecz walki z cyberprzestępczością;
3. budowanie zdolności związanych z cyberbezpieczeństwem;
4. ochrona praw człowieka w cyberprzestrzeni;
5. zarządzanie Internetem.



Najważniejsze zagadnienia związane z cyberprzestrzenią realizowane na arenie międzynarodowej; Opracowanie własne na podstawie H.Tirmaa-Klaar, Cyber Diplomacy: Agenda, Challenges and Mission [w:] Peacetime Regime For State Activities in Cyberspace, K. Ziolkowski (red), NATO CCD COE, Tallin 2013, ss. 509-531.

[10] H.Tirmaa-Klaar, *Cyber Diplomacy: Agenda, Challenges and Mission* [w:] *Peacetime Regime For State Activities in Cyberspace*, K. Ziolkowski (red), NATO CCD COE, Tallin 2013, ss. 509-531.

Działania podejmowane w odniesieniu do pierwszej kategorii wyzwań zorientowane są przede wszystkim na próby określenia i wdrażania norm zachowań państw w cyberprzestrzeni, szczególnie w kontekście potencjalnych konfliktów. Ważnym problemem jest ochrona infrastruktury krytycznej. Zaangażowanie dyplomatów jest niezbędne na przykład w negocjacjach dotyczących budowania mechanizmów zwiększających zrozumienie i poziom zaufania między państwami.

Drugie wyzwanie związane jest z koniecznością podejmowania wspólnych, międzynarodowych działań nakierowanych na zwalczanie problemu, który dotyka wszystkich. Cyberprzestępczość, która według danych Europolu przynosi dochody większe niż handel kokainą, marihuaną i heroiną łącznie, jest zagrożeniem globalnym[11]. Wiąże się z tym jeszcze poważniejsze i wzrastające zagrożenie atakami cyberterrorystycznymi. Są to problemy, wymagające współpracy nawet między podmiotami, które nie są naturalnymi sojusznikami.

Trzeci obszar odnosi się do podejmowania różnorodnych działań związanych ze wzmacnianiem zdolności państw do prowadzenia bezpiecznych działań w cyberprzestrzeni. Podstawowym założeniem jest tutaj fakt, że im więcej państw posiadać będzie skuteczne mechanizmy związane z cyberbezpieczeństwem, tym bardziej efektywne będą działania prowadzące do budowania stabilności całego środowiska cyberprzestrzeni.

Czwarta kategoria jest najbardziej zbliżona do tradycyjnych działań dyplomatycznych – ma na celu wzmacnianie ochrony praw człowieka i obywatela. Państwa demokratyczne powinny dbać aby te same prawa, które obowiązują w świecie realnym przestrzegane były także w cyberprzestrzeni. Szczególnie chodzi tutaj o prawo do wolności słowa, wymiany poglądów i prawo do prywatności.

Ostatni obszar, kluczowy z punktu widzenia działań międzynarodowych, to tocząca się dyskusja nad sposobem zarządzania Internetem i określeniem roli i odpowiedzialności poszczególnych graczy w tym kontekście. Wymaga on szczególnie dużego doświadczenia w prowadzeniu dialogu i negocjacji.

STRUKTURA I OKREŚLENIE PRIORYTETÓW

Wyżej opisane problemy to aktualnie jedne z najważniejszych kwestii jakie powinny znaleźć się na agendzie polityki zagranicznej współczesnych państw. Kluczowym zadaniem jest jednak określenie w odniesieniu do nich interesów narodowych, jakie powinni realizować funkcjonariusze służby zagranicznej. Muszą być one wyraźnie wskazane i wyartykułowane tak do wewnątrz jak i na zewnątrz. Dobrą praktyką w tym zakresie jest tworzenie strategii działań państwa na arenie międzynarodowej w kontekście problemów cyberprzestrzeni. Dokumenty tego typu zazwyczaj zawierają cele jakie dane państwo chce osiągać i narzędzia jakie będą wdrażane. W tym kontekście, ważne jest także, aby dyplomaci nauczyli się stosowania różnorodnych instrumentów polityki zagranicznej w odniesieniu do działań podejmowanych w cyberprzestrzeni. Tradycyjne sposoby działania stosowane dotychczas muszą być dostosowane do nowych potrzeb świata cyfrowego.

Realizacja interesów narodowych musi opierać się na dobrze zorganizowanej strukturze, gdzie zaangażowani aktorzy skutecznie się komunikują i współdziałają. „Cyber zagadnienia" muszą być wkomponowane w pracę ministerstw spraw zagranicznych, co często wymaga zmian organizacyjnych. Zazwyczaj różnorodne tematy takie jak ochrona praw człowieka, zagadnienia związane z prowadzeniem konfliktów, kwestie ekonomiczne prowadzone są przez różne departamenty. Jednak w przypadku cyberprzestrzeni problemy z nią związane łączy specyfika środowiska cyfrowego. Dlatego właśnie konieczne jest skoordynowanie „horyzontalnych" działań, oparte o skuteczną komunikację i ustalanie wspólnych celów[12].

W niektórych państwach, na przykład w USA czy RFN, powołano specjalne stanowiska dedykowane koordynacji działań związanych z cyberprzestrzenią[13]. Choć takie podejście ma wiele zalet, należy pamiętać, że skuteczną metodą jest elastyczne zarządzanie sieciowymi strukturami i unikanie sztywnej hierarchizacji działań, czy też skupienia kompetencji w jednej osobie. Dlatego tworzenie takich stanowisk nie powinno prowadzić do rezygnacji z podejścia horyzontalnego.

ZROZUMIENIE OTOCZENIA

W końcu, aby skutecznie poruszać się w międzynarodowym środowisku konieczne jest zrozumienie nie tylko problemów jakie niesie cyberprzestrzeń, ale także stanowisk i interesów poszczególnych państw oraz ról i zakresów działań zaangażowanych organizacji. Tworzenie koalicji z partnerami kierującymi się podobnymi celami jest konieczne do budowania bezpiecznej cyberprzestrzeni, opartej na wartościach i zasadach bliskich liberalnym demokracjom. Istnieją także takie zagadnienia (jak walka z cyberprzestępczością), które wymagają często pragmatycznego działania z krajami nie będącymi sojusznikami. Sprawne identyfikowanie stanowisk innych oraz zrozumienie na jakich forach można realizować poszczególne zadania jest kluczowe. Tylko wtedy można stosować właściwe narzędzia.

Poniższa tabela podsumowuje obszary i problemy jakimi zajmują się wybrane organizacje międzynarodowe w odniesieniu do cyberprzestrzeni (ze szczególnym uwzględnieniem problematyki cyberbezpieczeństwa). Pamiętać jednak należy, że w przypadku wielu z nich odpowiedzialności często nakładają się co wymaga skutecznego poruszania się w ramach wielu z nich jednocześnie.

[11] https://www.europol.europa.eu/ec/cybercrime-growing

[12] H.Tirmaa-Klaar, *Cyber Diplomacy: Agenda, Challenges and Mission* [w:] *Peacetime Regime For State Activities in Cyberspace*, K. Ziolkowski (red), NATO CCD COE, Tallin 2013, s.510.

[13] W amerykańskim Departamencie Stanu stworzone zostało stanowisko koordynatora ds. cyberprzestrzeni, w RFN funkcjonuje specjalna służba dedykowana temu zagadnieniu (International Cyber Policy Coordination Staff), powołany został także urząd Komisarza odpowiedzialnego za prowadzenie cybernetycznych tematów na arenie międzynarodowej (Commissioner for International Cyber Policy).

Z agadnienia cyberprzestrzeni poruszane na forach poszczególnych organizacji.

	ORGANIZACJA BEZPIECZEŃSTWA I WSPÓŁPRACY W EUROPIE	ONZ	ORGANIZACJA WSPÓŁPRACY GOSPODARCZEJ I ROZWOJU	RADA EUROPY	UE	G8	NATO
ZARZĄDZANIE INTERNETEM		X	X	X	X		
CYBERPRZESTĘPCZOŚĆ	X	X	X	X	X	X	
CYBERTERRORYZM	X	X				X	X
CYBERWOJNA		X					X

Źródło: Eneken Tikk, Global Cyber Security – Thinking About The Niche for NATO, "The SAIS Review of International Affairs", Fall 2010.

LEKCJA DLA POLSKI

Polska powinna stać się dużo bardziej aktywnym graczem na arenie międzynarodowej w obszarze działań dotyczących cyberprzestrzeni. Największy priorytet powinny mieć kwestie związane z cyberbezpieczeństwem, jednak i w kontekście innych zagadnień nasz głos musi być silny i słyszalny. Na wielu forach jesteśmy bowiem zbyt bierni lub całkiem nieobecni[14]. Ważnym krokiem, jaki należy wykonać, jest zwiększenie zrozumienia różnorodnych problemów związanych z cyberprzestrzenią wśród naszego korpusu dyplomatycznego. Odnosi się to zarówno do specyfiki poszczególnych zagadnień jak i do umiejętnego „czytania" innych graczy i samego środowiska.

To umożliwi realizację kolejnego etapu, czyli zidentyfikowania dostępnych narzędzi jakie można stosować. Wiedza i umiejętności wyżej wskazane będą najlepiej wdrażane w odpowiedniej strukturze opartej na systemie skutecznej komunikacji i koordynacji.

Jednak wszystko to przyniesie efekty wyłącznie gdy przyczyni się do realizacji interesów kraju. Należy jasno i wyraźnie określić do jakich celów dążymy prowadząc poszczególne działania związane z cyberprzestrzenią. Zrozumienie tego jest warunkiem podstawowym dla prowadzenia efektywnej polityki międzynarodowej. Wobec zwiększającej się roli cyberprzestrzeni są to działania niezbędne. Wszelkie zaniedbania w tym zakresie, skutkować będą obniżeniem potencjału Polski w świecie realnym.

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

Fotografie:
s. 1,14: Biuro Bezpieczeństwa Narodowego
s. 16,20, 24: www.publicdomainpictures.net

[14] Na przykład w ramach prac Group of Governmental Experts działającej przy ONZ.