ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Jacek GRUBER, Ireneusz J. JÓŹWIAK, Adam RETKIEWICZ
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

MIĘDZYNARODOWE ĆWICZENIA Z ZAKRESU OCHRONY CYBERPRZESTRZENI

Streszczenie. W artykule omówiono podstawowe zagadnienia dotyczące zagrożeń płynących z cyberprzestrzeni. Opisano rzeczywiste incydenty zaistniałe w Polsce oraz ataki na instytucje finansowe na całym świecie. Następnie zaprezentowano ideę wykonywania ćwiczeń z zakresu ochrony cyberprzestrzeni i zaprezentowano historię organizacji ćwiczeń. Opisano kolejne ich edycje, jak m.in. międzynarodowe manewry *Baltic Cyber Shield, Cyber Coalition, Locked Shield*. Przedstawiono także polski wkład w tym zakresie: wygrana Polskiej ekipy na „Locked Shield 2014" oraz propozycja polskiego testu „Cyber-Exe".

Słowa kluczowe: bezpieczeństwo, cyberprzestrzeń, sieć.

INTERNATIONAL EXERCISES TO PROTECT CYBERSPACE

Summary. Article seeks to illustrate the reader about the dangers flowing from cyberspace. The article begins with a description of actual events in the country and against financial institutions around the world. Followed by an explanation of the idea and a brief history of the organization of training goes into descriptions of subsequent editing. Described are international maneuvers such as "Baltic Cyber Shield", "Cyber Coalition", "Locked Shield". There will be Polish accent, is mentioned about winning Polish team for "Locked Shield 2014" and you will find information about Polish test: "Cyber-Exe".

Keywords: security, cyberspace, network.

1. Wprowadzenie

Bezpieczeństwo jest procesem ciągłym, a nie jest stanem lub produktem końcowym. W wyniku globalizacji i szybkiego rozwoju technologii informacyjnych pojęcie bezpieczeństwa teleinformatycznego nie powinno być lekceważone. Powoli jest zatracana

granica pomiędzy światem rzeczywistym a wirtualnym. Pojęcie bezpieczeństwa jest ważne w przypadku małych firm, dużych korporacji międzynarodowych, państw, a także koalicji międzynarodowych. Polski rząd, chcąc wyjść naprzeciw temu zadaniu, przez Ministerstwo Administracji i Cyfryzacji utworzył dokument *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016* [1, 2, 7]. Dokument w ogólny sposób opisuje strategiczne cele programu, dając w ten sposób spore pole manewru przy jego realizacji. Jest on skierowany do wszystkich osób korzystających z sieci teleinformatycznych, do zwykłych użytkowników Internetu oraz do administracji rządowej. Proponowane są działania legislacyjne, czyli stworzenie odpowiedniej infrastruktury prawnej, działania proceduralno-organizacyjne, działania edukacyjne, poprzez wszystkie szczeble edukacji, a także dla pracowników, z główną myślą o uzmysłowieniu wagi problemu. Ważnym aspektem są także działania techniczne, które dają największą swobodę. Dokument opisuje w sposób ramowy przekazywanie informacji, współpracę, koordynację i obowiązki różnych instytucji. Występuje rozróżnienie pomiędzy incydentami w sieci, cyberprzestępczością a cyberterroryzmem związanym z infrastrukturą publiczną i militarną. Polityka Ochrony Cyberprzestrzeni uwzględnia rozwój technologiczny, dlatego jest bardzo ogólnikowa i jest aktualizowana przynajmniej raz na rok.

Dokument określa zalecenia, do których powinny dostosować się wszystkie podmioty administracji rządowej, pozostałe jednostki i urzędy państwowe mogą je stosować na zasadzie rekomendacji. Adresatami Polityki pośrednio są wszyscy użytkownicy cyberprzestrzeni, zarówno osoby fizyczne, jak i przedsiębiorcy korzystający z Internetu. Współtwórcą powyższego dokumentu jest *CERT-Polska* (Computer Emergency Response Team), organizacja będąca pierwszą linią obrony w zagrożeniach teleinformatycznych [2-4]. W Polsce zespół działa od 2009 roku, w corocznym raporcie *CERT* znajdują się szczegółowe informacje o zaistniałych zagrożeniach w sieci na terenie Rzeczypospolitej Polskiej, głównie w stosunku do jednostek administracji publicznej. Znajdziemy tam podział ilościowy i jakościowy zaistniałych incydentów, znalezione podatności na wybranych stronach WWW oraz lokalizacje, skąd były przeprowadzane ataki. Podobną działalność, ale w skali globalnej, prowadzi *IBM X-Force*, wspierający obronę teleinformatyczną dla ponad 100 milionów użytkowników z ponad 350 instytucji finansowych na całym świecie. Od 2010 roku *X-Force* wydaje raporty, w których opisuje aktualne zagrożenia. Według ich raportu najwięcej ataków, bo aż 28%, jest prowadzonych przeciwko firmom związanych z IT. Drugie miejsce, 15% wszystkich ataków, zajmują ataki na agencje rządowe. Trzecim najbardziej zagrożonym sektorem, zawierającym 12% ataków, są instytucje finansowe. Najpopularniejszymi typami ataków są kolejno: DDoS (20%, *distributed denial of service*, rozproszone ataki blokujące serwis), *SQL injection* (13%), *malware* (10%, złośliwe oprogramowanie), *XSS* (1%, *cross site scripting*, wstrzykiwanie kodu). W Polskim raporcie jest dokładniejszy wykaz zaistniałych incydentów, ataki DDoS/DoS nie były najpopularniejszym zagrożeniem, natomiast przy wykrytych podatnościach witryn WWW pierwsze miejsce zajęły XSS, a drugie Blind SQL/

SQL injection. Analizując oba raporty, można znaleźć pewne podobieństwa oraz rozbieżności w zagrożeniach lokalnych i globalnych.

Powyższe raporty opisują głównie statystyki zagrożeń. Rzeczywisty poziom zabezpieczeń w danej firmie można przetestować za pomocą audytów bezpieczeństwa. Sprawdzają one aktualny stan formalny i rzeczywisty danego przedsiębiorstwa. Tańszą alternatywą są testy penetracyjne, które często mają przebieg nieformalny. Sposobami podniesienia kwalifikacji pracowników są różnego rodzaje szkolenia, jednak niektórych doświadczeń nie można wynieść ze szkoleń. Dobrą formą przetestowania kompetencji jest realizacja ćwiczeń, w których można przetestować swoje aktualne umiejętności i porównać je do innych specjalistów w tej dziedzinie.

W sytuacjach kryzysowych nie tylko umiejętności pracowników odpowiedzialnych za bezpieczeństwo są istotne. Ważną kwestią są procedury, jakie powinni realizować, oraz aspekty prawne. Może się zdarzyć, że w sytuacji kryzysowej pracownik musi szybko ocenić, czy działać w interesie firmy, czy postępować według procedur albo według aktualnego prawa krajowego lub międzynarodowego. Z tą myślą powstały międzynarodowe ćwiczenia dotyczące ochrony cyberprzestrzeni. W ćwiczeniach biorą udział ludzie reprezentujący różne instytucje prywatne oraz rządowe. Starają się oni przetestować fikcyjne scenariusze, które są oparte albo na realnych zdarzeniach, albo na realnych zagrożeniach. Zdarzenia są fikcyjne, ale używane metody ataków i obrony oraz profilaktyki są jak najbardziej rzeczywiste i aktualne. W przeciwieństwie do codziennej polityki w ćwiczeniach czasami używa się nie najbardziej aktualnych wersji oprogramowania, które mają luki, m.in. ze względu na to, by testy były bardziej dynamiczne.

2. Międzynarodowe ćwiczenia z zakresu ochrony cyberprzestrzeni

W listopadzie 2002 roku na szczycie NATO w Pradze podjęto decyzję o utworzeniu Programu Obrony Cybernetycznej *The Cyber Defense Program* i Zdolności Reagowania na Incydenty Komputerowe *The Computer Incident Response Capability.* Spektakularny cyberatak na Estonię w 2007 roku spowodował przyjęcie w 2008 roku Strategii Obrony Cybernetycznej *The Policy on Cyber Defence,* a w maju 2008 roku zostało podpisane memorandum o utworzeniu w Tallinnie w Estonii Centrum Kompetencyjnego ds. Obrony Teleinformatycznej *The Concept for Cooperative Cyber Defense Centre of Excellence* (CCD COE). W październiku 2008 przyznano pełną akredytacje dla Centrum jako *The NATO Centre of Excellence* oraz status „The International Military Organization" – IMO. Centrum w Tallinie nie jest jednostką operacyjną i nie podlega strukturom dowodzenia NATO. W listopadzie 2011 roku do CCDCOE przystąpiły Polska i USA [5, 6, 8-15].

Odpowiedzią na cyberatak na Estonię z 2007 roku było zorganizowane pierwszego tego typu ćwiczenia, które odbyło się 6 grudnia 2008 roku. Przeprowadzono je pomiędzy szwedzkimi i estońskimi uniwersytetami. Gospodarzem była wyższa uczelnia techniczna w Tallinie. Na ćwiczeniach były prezentowane cyberataki na ważne strony internetowe, konta e-mail oraz serwery DNS. Tallinn było gospodarzem dla wielu późniejszych ćwiczeń międzynarodowych.

CCDCoE wraz ze Szwedzką Akademią Obrony Narodowej (*Swedish National Defence College*, *SNDC*) postanowili powtórzyć eksperyment w maju 2010 roku, ale tym razem na większą skalę, zorganizowali pierwsze międzynarodowe ćwiczenia *Baltic Cyber Shield*. Kolejnymi współorganizatorami byli: Szwedzka Agencja Badań Obrony (*Swedish Defence Research Agencyę*, *FOI*), Estońska Liga Cyber Obrony (*Estonian Cyber Defence League*, *ECDL*), *NATO Communication and Information Systems Services Agency Computer Incident Response Capability – Technical Centre* (*NCSA NCIRC – TC*). Scenariusz opisywał niestabilne środowisko geopolityczne, gdzie został zatrudniony nowy zespół ekspertów do spraw bezpieczeństwa w cyberprzestrzeni. W rolę specjalistów wcieliło się sześć konkurujących ze sobą niebieskich drużyn. Ich celem była obrona systemów informatycznych przedsiębiorstwa energetycznego przed coraz bardziej wyrafinowanymi atakami hakerów, którzy byli reprezentowani przez drużynę czerwoną. Ogromną zaletą *Baltic Cyber Shield* było to, że na jego podstawie powstały kolejne edycje ćwiczeń, takie jak: *Cyber Coalition*, *Locked Shield* czy Polskie *Cyber-Exe* [11, 15].

Następnym ważnym, dużym ćwiczeniem, które warto by odnotować, było *Cyber Europe.* Odbyło się ono 4 listopada 2010 roku [5]. Trwało tylko 7 godzin, od godz. 10 do 17. Organizowane było przez członków UE oraz ENISA (ang. *European Union Agency for Network and Information Security*) oraz wspomagane przez JRC (ang. *Joint Research Centre*). Głównym ośrodkiem ćwiczących były Ateny. Członkowie pochodzili z 22 krajów, z czego 50 osób było bezpośrednio w głównym ośrodku, a reszta brała udział zdalnie ze swoich miejsc pracy. Główną ideą ćwiczenia było sprawdzenie reakcji ćwiczących na krytyczne zdarzenia w trakcie realizacji swoich normalnych prac. Zadanie polegało na odzwierciedleniu połączeń międzyoperatorskich pomiędzy krajami (IIS) i stopniowym usuwaniu niektórych połączeń w wyniku ataków. Uczestnicy widzieli tylko swoje lokalne połączenia i nie mogli określić stanu innych połączeń na kontynencie. Globalny widok miał tylko główny moderator ćwiczenia. Zadaniami ekspertów były wspólne usiłowania przeciwdziałania symulowanym próbom mającym na celu sparaliżowanie Internetu.

W 2011 roku odbył się pierwszy *Cyber Coalition* [13, 14]. Była to dobra okazja do przetestowania współpracy krajów należących do NATO, mającej na celu przeciwdziałanie atakom na dużą skalę w wirtualnej infrastrukturze NATO oraz przeciwko indywidualnym krajom. Brało tutaj udział ponad 100 specjalistów z 23 krajów NATO oraz z 6 innych partnerskich państw. Celem ćwiczenia było sprawdzenie zdolności reagowania na incydenty komputerowe, współpracy między instytucjami oraz podejmowania ważnych strategicznych

decyzji dla krajów członkowskich. Scenariusz opierał się na wielu atakach przeprowadzonych jednocześnie przeciwko NATO i jego państwom członkowskim.

Kolejna edycja *Cyber Coalition* odbyła się 13-16 listopada 2012 roku. Ćwiczenie przeprowadzono razem z *Crisis Management Exercise* (CMX). Udział brali członkowie NATO oraz Węgry i Estonia. Testowane scenariusze obejmowały narastające zagrożenia atakami: chemicznym, biologicznym i radiologicznym. Element *Cyber Coalition* obejmował scenariusz wielu cyberataków na dużą skalę realizowanych przez agresora opisanego jako „afrykański kraj zaangażowany w konflikt z NATO". Hakerzy z „afrykańskiego kraju", realizując atak za pomocą wirusów komputerowych, doprowadzają do katastrofy wojskowej awionetki i cywilnych samolotów transportowych NATO, uśmiercając w ten sposób wojskowych i cywili. Terroryści atakują także ważniejsze obiekty infrastruktury Estonii. Zadaniem ćwiczących było zidentyfikowanie napastnika i przeprowadzenie odwetu. W scenariuszu agresorem był „kraj afrykański". Rzeczywistymi krajami, których obawiało się NATO, były Rosja, Chiny i Iran. Według raportu z działalności ABW na rok 2013 *Cyber Coalition 2012* było pierwszym ćwiczeniem międzynarodowym, w którym brali udział Polacy. Od 2012 roku *Cyber Coalition* zmieniło nazwę na *Locked Shield* (LS). Jednak pierwsze ćwiczenie LS nastąpiło 26-28 marca 2012 roku, ponad pół roku przed listopadowym ćwiczeniem.

Manewry *Locked Shield 2012* odbyły się w Tallinie, brało w nich udział ponad 250 osób z wielu organizacji. Organizowane były w ramach kooperacji m.in. pomiędzy Szwajcarskimi Siłami Zbrojnymi (SAF), Fińskimi Siłami Obronnymi (FDF), Centrum Kompetencyjnym ds. Obrony Teleinformatycznej (*Cooperative Cyber Defence Centre of Excellence*, NATO CCD COE), Estońską Ligą Obrony Cybernetycznej (*Estonian Cyber Defence League*, ECDL) oraz pomiędzy innymi instytucjami rządowymi i firmami prywatnymi. Organizacja ćwiczenia uwzględniała podział na kilka kategorii grup: Blue, Red, Green, White, Legal, Yellow, MNE7 SA. Głównymi zadaniami zdarzenia były: przeszkolenie i sprawdzenie umiejętności członków drużyn Blue i Legal w kampanii międzynarodowej, sprawdzenie podatności technologicznych i świadomości uczestników oraz wzajemna nauka pomiędzy niebieskimi i czerwonymi drużynami. Drugim głównym celem była dobra okazja do przeszkolenia drużyny prawnej na sposoby ataku i obrony systemów IT. W przypadku prostych scenariuszy prawnicy przez większość czasu byli tylko obserwatorami. W testowanym scenariuszu niebieskie drużyny reprezentowały małe firmy telekomunikacyjne, każda z nich miała podobną sieć składającą się z 25 wirtualnych maszyn. Ich systemy były celowo źle skonfigurowane oraz miały wiele podatności. Niebieskie grupy konkurowały ze sobą i były oceniane przez grupę białą. Rolę atakujących przypisano drużynom czerwonym, w których skład wchodzili specjaliści i ochotnicy głównie z Finlandii i Estonii. Agresorzy nie konkurowali ze sobą, mieli ustalone cele i wolną rękę do ich realizacji. Biała drużyna była odpowiedzialna za określenie celów dla grup czerwonych, za punktację grup niebieskich oraz brała udział w tworzeniu ogólnego scenariusza. Drużyna zielona miała najtrudniejsze zadanie:

była odpowiedzialna za utworzenie całej technicznej infrastruktury w laboratorium oraz za wirtualizacje testowanej sieci. Udzielała ona wszelkich pomocy technicznych. Członkowie grup żółtych wyszukiwali i starannie wybierali rozwiązania i metody, które były później testowane na ćwiczeniach. Drużyna prawnicza, podobnie jak i niebieska, była najbardziej obserwowaną grupą. Ich zadaniami były: opracowanie przepisów dla fikcyjnego zdarzenia, obserwowanie i analiza wszystkich zdarzeń pod względem prawnym, doradzanie drużynom niebieskim w kwestiach prawnych oraz spojrzenie na ataki w cyberprzestrzeni od strony technicznej.

Testowane scenariusze dotyczyły współpracy małych firm teleinformatycznych atakowanych przez różne grupy hackerskie. Symulowane były połączenia DSL z Internetem, współdzielony web hosting, e-mail hosting czy dostarczenie wirtualnych prywatnych serwerów. Testowane sytuacje były oparte na prawdziwych wydarzeniach. Przykładem jest grupa hakerów aresztowana przez Interpol; byli oskarżeni o prowadzenie hostingu w celu kradzieży tożsamości, wyłudzeń finansowych oraz spamowania DDOS. Kolejnym pierwowzorem był zhakowany system chłodzenia serwerowni firmy CoolAirz czy oskarżenia ISP (ang. *Internet Service Provider*) o działania szpiegowskie na dużej populacji studentów.

Kolejna edycja programu *Locked Shield* odbyła się 23-26 kwietnia 2013 roku. Wzięło w niej udział 18 organizacji z 15 państw, w tym m.in. NATO. Podobnie jak we wcześniejszej edycji programu uczestnicy byli podzieleni na grupy: Blue, Red, Green, White, Legal, Yellow. Głównymi różnicami w stosunku do LS2012 były użycie większej liczby nowoczesnych urządzeń oraz większe nastawienie na współpracę między niebieskimi drużynami. Przygotowany scenariusz opisywał konflikt w fikcyjnym państwie *Boolea*. Kraj znajdował się na wyspie w okolicach północnej Afryki. Państwo było pogrążone w wojnie domowej pomiędzy plemionami północnymi a południowymi. W międzyczasie wybuchła epidemia cholery na północy. Oprócz tradycyjnych działań wojennych od kwietnia 2013 roku zaczęły się pojawiać cyberataki przeciwko systemom IT oraz przeciwko sieciom organizacji humanitarnych. Lokalne władze były zmuszone poprosić o pomoc organizacje międzynarodowe. Niebieskie drużyny wcieliły się w rolę przedstawicieli ONZ, których celem była ochrona niesklasyfikowanych sieci militarnych oraz sieci organizacji charytatywnych. Czerwone drużyny wcieliły się w dwie role: w lokalnych ekstremistów z niskimi bądź średnimi umiejętnościami oraz w międzynarodowych terrorystów ze średnimi bądź z wysokimi umiejętnościami. Celem czerwonych było utrudnienie pracy organizacjom humanitarnym i rozszerzenie chaosu w kraju. Głównymi celami ćwiczenia, oprócz sprawdzenia i podwyższenia umiejętności niebieskich drużyn, były: rozpoznanie niezidentyfikowanych sieci, administracja, prewencja, monitorowanie oraz detekcja i odpowiedź na ataki. Ważna także była kooperacja międzynarodowa i pomiędzy drużynami, umiejętność ogólnego spojrzenia na sprawę oraz komunikacja w krytycznych momentach. Główne wyzwania dla niebieskich drużyn były skupione na obronie web aplikacji, detekcji złośliwego kodu, łagodzeniu efektów tzw. porwań BGP (IP hijacking) oraz na inicjonowaniu

efektywnej informacji między zespołami. Członkowie niebieskich byli znacznie lepiej przygotowani niż wcześniej, dlatego radzili sobie efektywniej aniżeli w poprzedniej edycji programu.

W dniach 22-23 maja 2014 roku odbyła się kolejna edycja *Locked Shield*; zaangażowanych było ponad 300 osób pochodzących z 17 krajów. Tegoroczny scenariusz opisywał ochronę fikcyjnego kraju *Berylia* przed zmasowanymi cyberatakami. Program przewidywał podział uczestników na różne drużyny, podobnie jak w poprzednich edycjach programu. Pierwszy dzień ćwiczeń rozpoczął się od małej aktywności hakerów, z zbiegiem czasu działania się nasilały. Celami czerwonych drużyn poza tradycyjnymi cyberatakami były także sabotaże oraz działania szpiegowskie przeciw *Berylii*. W działaniach uczestniczyło 11 niebieskich drużyn, najskuteczniejszą niebieską grupą okazała się reprezentacja Polski. Nasza reprezentacja składała się ze specjalistów z wybranych instytucji. Wystawione były po 2 osoby z następujących organizacji: Ministerstwo Obrony Narodowej, Zespół Informatycznego Reagowania Kryzysowego CERT Polska, Służby Kontrwywiadu Wojska oraz z Wojskowej Akademii Technicznej. Grupie dowodził Tomasz Strycharek, szef MIL CERT-PL [16].

3. Polskie ćwiczenia z zakresu ochrony cyberprzestrzeni

Mikołaj Rej napisał „Iż Polacy nie gęsi, iż swój język mają". Na podstawie *Baltic Cyber Shield* zostało zorganizowane polskie ćwiczenie dotyczące ataków w cyberprzestrzeni: *Cyber Exe-Polska* [2-4]. Pierwsza edycja odbyła się 19 września 2012 we wrocławskiej Hali Ludowej. Zaangażowanych było 13 instytucji i około 80 osób. Harmonogram ćwiczeń obejmował nie tylko samo przeprowadzenie ćwiczenia, lecz całą organizację przez identyfikację zagrożeń i tematyki zajęć, przez planowanie, przeprowadzenie ćwiczenia oraz końcowej oceny wszystkich przedsięwzięć. W odróżnieniu od *Locked Shield* scenariusz był starannie zaplanowany, nie przypominał niezaplanowanego pola walki jak w międzynarodowych manewrach, był podobny do starannie opracowanego ataku cyber terrorystycznego. Atak był przeprowadzony na infrastrukturę teleinformatyczną w środowisku testowym, która była wzorowana na rzeczywistych odpowiednikach. Polskie manewry w 2012 roku przewidywały 2 dokładnie zaplanowane ćwiczenia: scenariusz dla sektora gazowego oraz scenariusz dla sektora elektroenergetycznego. W pierwszym przypadku ataki początkowo miały na celu odcięcie informacji pomiarowych z jednego z punktów dystrybucyjnych. Kolejnym krokiem był atak na APN (ang. *Access Point Name*). Docelowo hakerzy mieli przejąć kontrolę nad systemem sterującym. W drugim ćwiczeniu agresorzy zaczęli od ataków APT (ang. *Advanced Persistant Threat*) na pracowników, następnie infekowali komputery na stacjach elektroenergetycznych. Głównym celem było uszkodzenie autotransformatorów stacyjnych. Raport dokładnie opisuje używane metody ataków.

Cyber-Exe Polska 2013 odbyło się 29 października 2013 roku. Ćwiczenie dotyczyło ataków na instytucje finansowe. Organizatorem ćwiczenia była Fundacja Bezpieczna Cyberprzestrzeń. Partnerami organizacyjnymi było Rządowe Centrum Bezpieczeństwa oraz firma doradcza Deloitte. W scenariuszu było przewidzianych 6 konkurujących ze sobą grup broniących się, każda drużyna była reprezentowana przez inny bank. Testowane były dwa przypadki ataków: ścieżka ataku DDoS i ścieżka ataku APT. W pierwszym przypadku atak był podzielony na 4 fazy: kontakt szantażysty z biurem obsługi klienta, wstępny testowy atak DDoS, następnie główny atak DDoS, w trakcie którego zostały zebrane dane klientów banku. Ostatnia faza to atak phishingowy, czyli wykorzystanie danych klientów do działań przestępczych. Drugi scenariusz opisywał atak APT. Szantażysta udostępnił publicznie szczątkowe poufne informacje banku i zażądał okupu za nieudostępnianie reszty informacji. Ćwiczący mieli za zadanie przeanalizować atak i współpracować z zewnętrznymi instytucjami typu policja czy CERT.

4. Podsumowanie

Krajowe i międzynarodowe ćwiczenia ochrony cyberprzestrzeni są tworzone w podobnym celu: sprawdzenie kompetencji, zwiększenie umiejętności uczestniczących oraz spojrzenie na aspekty prawne podczas sytuacji kryzysowej. *Cyber-Exe*, *Locked Shield*, *Cyber Coalition* wywodzą się od wspólnego przodka: *Baltic Cyber Shield.* Polskie wydarzenie kontynuuje tradycję i przy dobrej organizacji jest wykonywane w ciągu jednego dnia. Ćwiczenia międzynarodowe mają znacznie więcej uczestników i zostały rozszerzone na dwa dni. Obecnie *Locked Shield* jest największym przedsięwzięciem tego typu na świecie. Oba wydarzenia uwzględniają zwykle jeden dodatkowy dzień, tzw. dry day, najczęściej odbywa się on tuż przed właściwym ćwiczeniem. Polega on na zapoznaniu się ze środowiskiem, przetestowaniu go i na przeprowadzeniu próbnych ataków.

Porównując raporty z ćwiczeń lokalnych i międzynarodowych, można zauważyć drobną różnicę. Raporty z dużych ćwiczeń skupiają się na opisie przeprowadzanego scenariusza, „dry day" i samym przeprowadzonym ćwiczeniu. Dobrze opisane są metody ataków, obrony, kolejne fazy scenariuszy oraz sposoby punktowania. Można także znaleźć statystyki konkretnych udanych i nieudanych ataków. Raport polskiego ćwiczenia *Cyber-Exe* opisuje zdarzenie w szerszym zakresie. Zawiera informacje o procesie planowania zdarzenia, identyfikacji zagrożeń, realizacji samego ćwiczenia oraz opisuje wnioski i proponuje rekomendacje na przyszłość.

Rozbieżności w charakterze napisanego raportu mogą wynikać z tego, że oba ćwiczenia są przeprowadzane w nieco innej formie. Testy międzynarodowe przypominają pole bitwy z różnymi grupami agresorów i broniących się. Po przeprowadzonej bitwie dobrze jest

spojrzeć na statystyki, kto jakich metod używał. Polskie ćwiczenie przypomina dobrze zaplanowany atak terrorystyczny, podane są konkretne rodzaje używanych metod w kolejnych fazach. W tym przypadku statystyki nie odgrywają kluczowej roli, wystarczy wynik w formie opisowej.

Ważnym elementem każdego ćwiczenia jest dobrze zaplanowany scenariusz. Powinien być w miarę możliwości realistyczny, oparty na realnych zagrożeniach, dzięki czemu można by przetestować metody, które można by później powtórzyć w prawdziwym życiu. Duże ćwiczenia starają się testować sytuacje, w których wymagana jest kooperacja organizacji międzynarodowych. Nasze lokalne ćwiczenia nie muszą być prowadzone na taką skalę, ale organizatorzy starają się także zorganizować ćwiczenia wymagające kooperacji instytucji prywatnych i rządowych.

Oba rodzaje ćwiczeń różnią się od siebie i często wymagają innego podejścia do sprawy. Dzięki różnicom uczestnicy mogą zdobyć nowe, cenne doświadczenia. Ważne jest, by tego typu ćwiczenia odbywały się systematycznie i regularnie.

Wiedza uzyskana na tego typu zdarzeniach jest wykorzystywana także w tworzeniu dokumentu „Polityka Ochrona Cyberprzestrzeni Rzeczypospolitej Polskiej".

„Cyber-Exe Polska 2013 dowiodło, że procedury i wyposażenie są warunkiem koniecznym, ale niewystarczającym, by nawet duża organizacja mogła sprostać zaawansowanemu atakowi teleinformatycznemu. Podczas reakcji na cyberatak istotną rolę odgrywa także doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie oraz zdolność do koordynacji działań w sytuacjach kryzysowych" [4].

Bibliografia

1. Agencja Bezpieczeństwa Wewnętrznego: Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2013 r. Warszawa 2014.
2. CERT.GOV.PL: CERT.GOV.PL Raport o stanie bezpieczeństwa RP w 2013 roku. Warszawa 2014.
3. Cyber-EXE Polska: CYBER-EXE Polska 2012. Ćwiczenia z ochrony w cyberprzestrzeni, przygotowanie, przebieg, analiza, wnioski i rekomendacje. RAPORT. Warszawa 2012.
4. Cyber-EXE Polska: CYBER-EXE Polska 2013. Ćwiczenia w zakresie ochrony przed zagrożeniami z cyberprzestrzeni dla polskiego sektora bankowego. Przygotowanie, przebieg, analiza, wnioski i rekomendacje. RAPORT. Warszawa 2013.
5. European Union Agency for Network and Information Security (ENISA): Cyber Europe 2010 - Evaluation Report. Heraklion - Crete, Greece 2011.
6. IBM: IBM X-Force Threat Intelligence Quarterly, 1Q 2014. United States of America.

7. Ministerstwo Administracji i Cyfryzacji: Polityka Ochrony Cybeprzestrzeni Rzeczypospolitej Polskiej. Warszawa 2013.
8. NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE): Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report. Tallinn, Estionia 2010.
9. NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE): Cyber Defence Exercise Locked Shields 2012, After Action Report. Estonia, Tallinn 2012.
10. NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE): Cyber Defence Exercise Locked Shields 2013, After Action Report. Estonia, Tallinn 2013.
11. CCDCOE. Estonian-Swedish Cyber Defence exercise was won by students of the Tallinn Technology University [online] (December 9, 2008), available on the web: http://www.ccdcoe.org/91.html
12. Security and Defence Agenda. Nato Cyber-Defence Exercise [online] (19.12.2011), available on the web: http://www.securitydefenceagenda.org/ Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId /3025/categoryId/62/NATO-cyberdefence-exercise.aspx
13. North Atlantic Treaty Organization. Cyber Coalition 2011 exercise tests NATO procedures for cyber defence [online] (13.12.2011), available on the web: http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease
14. General Knowledge Today. Cyber Coalition 2013: NATOS's largest-ever cyber-security exercise held in Estionia [online] (1.12.2013), available on the web: http://currentaffairs.gktoday.in/cyber-coalition-2013-natos-largest-ever-cyber-security-exercise-1220139987.html
15. CCDCOE. Poland Was Crowned the Winner of Locked Shields 2014 [online] (23.05.2014), available on the web: http://www.ccdcoe.org/526.html
16. Polacy z ABW, SKW, MON-u, WAT-u oraz CERT.PL zwyciężyli w ćwiczeniach NATO symulujących ataki internetowe. Available on the web: http://niebezpiecznik.pl/post/polacy-z-abw-skw-mon-u-oraz-cert-pl-zwyciezyli-w-cwiczeniach-nato-dot-atakow-internetowych/ (23.05.2014).

Abstract

During crisis situations, not only skills of workers responsible for cyberspace security are important – safety procedures are also fundamental thing.
Due to this, international training related to cyberspace security came into being. During this training participants are solving problems of fictional cyberspace attacks. Those scenarios are based on real events and dangers. In the paper the events that happened in Poland and all over the world has been described and analysed.