FOLIA 250

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate et Educatione Civili 7 (2017)
ISSN 2082-0917
DOI 10.24917/20820917.7.8

Wojciech Cendrowski
Uniwersytet Pedagogiczny im. KEN w Krakowie

Cyberwojna: wybrane zagadnienia techniczne

Wprowadzenie

Zmiany technologiczne, jakie miały miejsce w ostatnich dziesięcioleciach bez wątpienia wpłynęły na każdą sferę ludzkiej aktywności, także na sposób prowadzenia wojen. Od kilku dziesięcioleci technologia informatyczna stała się jedną z najbardziej istotnych branż naukowych. Dla znacznej części mieszkańców naszej planety komputer jest niezbędnym elementem codziennego życia, dał możliwość kontaktu z resztą świata bez wychodzenia z domu, będąc też narzędziem gwarantującym sprawne funkcjonowanie gospodarki, administracji państw i wielu innych dziedzin życia. Zakończyła się era dominacji przemysłu i usług, istotna stała się informacja sama w sobie. To, co niesie za sobą zalety, szanse i nowe możliwości, przynosi jednak także zagrożenia, niebezpieczeństwa i nieznane dotąd problemy. Wojna, jaką znamy z przekazów medialnych, strzały, zniszczenia i uzbrojeni żołnierze, to dziś nie jedyne oblicze wojny, z jakim możemy mieć do czynienia[1]. Nowym jej teatrem stała się bowiem także cyberprzestrzeń.

Pojęcie cyberwojny nie zostało dotąd w jednoznaczny sposób zdefiniowane. Steve Winterfeld i Jason Andress wskazują, że definicja cyberwojny nie jest łatwa do ustalenia i to dlatego wciąż jest ona przedmiotem debaty naukowej[2]. Pojawiają się jednak mimo wielu trudności próby zbudowania jej naukowego opisu. James A. Green przez pojęcie cyberwojny rozumie rozszerzenie polityki poprzez działania podejmowane w cyberprzestrzeni przez podmioty państwowe lub przez podmioty niepaństwowe o znaczącym ukierunkowaniu lub wsparciu państwa, które stanowią poważne zagrożenie dla bezpieczeństwa innego państwa, lub działanie o takiej samej naturze podjęte w odpowiedzi na poważne zagrożenie dla bezpieczeństwa państwa (rzeczywiste lub postrzegane)[3].

---

[1] R. Klepka, *Wojna w mediach: wybrane zagadnienia dotyczące relacjonowania konfliktów zbrojnych*, „Wojny i konflikty. Przeszłość-Teraźniejszość-Przyszłość" 2016, nr 1(1), s. 6 i n.

[2] S. Winterfeld, J. Andress, *The Basics of Cyber Warfare*, Elsevier, Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013, s. 16.

[3] *Introduction*, [w:] *Cyber Warfare: A multidisciplinary analysis*, red. J. Green, Routledge Taylor & Francis Group, London, New York 2015, s. 2.

Przedmiotem niniejszego opracowania jest analiza i charakterystyka technicznych zagadnień dotyczących cyberwojny. Potrzeba takiej analizy wynika z faktu, iż w powszechnym odbiorze cyberwojna, choć dotyczy przestrzeni, z którą mamy na co dzień do czynienia, nie może dosięgnąć bezpośrednio nas. Tymczasem wiedza na temat uwarunkowań technicznych ataków w cyberprzestrzeni umożliwia zarówno zrozumienie natury istniejących zagrożeń, jak i prowadzi do świadomych działań mających na celu przeciwdziałanie im.

Sieć i jej działanie

Celem zrozumienia praktycznych działań, które wiążą się z cyberwojną oraz wykorzystywanymi w niej metodami ataków, konieczne jest zrozumienie bodaj przybliżonego i uproszczonego schematu działania Internetu jako głównej sfery cyberprzestrzeni, w której dzieją się cyberoperacje czy cyberataki. Schemat działania zostanie opisany na przykładzie praktycznym.

Typowy użytkownik internetu chce przy użyciu swojego komputera wejść na popularny portal internetowy www.onet.pl. Zakładamy że wspomniany użytkownik ma sprawny komputer, zawarł umowę z dostawcą usług internetowych (tzw. ISP – Internet Service Provider), który zapewnił mu podłączenie fizyczne i logiczne do sieci, np. za pomocą routera. Z perspektywy topologii logicznej, która *[…] definiuje standardy komunikacji, dzięki którym poszczególne komputery bezbłędnie porozumiewają się w sieci*[4], by rozpocząć proces połączenia się ze stroną, komputer musi ściągnąć zgodnie z tzw. IP (internet protocol – zbiór zasad wg których przesyłane są pakiety) na swoją pamięć dane w postaci pakietów, które w nagłówku mają zapisane dane nadawcy i odbiorcy (zgodnie z modelem protokołu TCP/IP, który z kolei jest zgodny z modelem ISO/OSI), dzięki czemu są w stanie dotrzeć do adresata bezpośrednio przez konkretne węzły sieci. Adresatem nie musi być pojedynczy komputer, numer IP może być także nadany sieciom lokalnym[5].

Tab. 1. Budowa pakietu opisana według modelu ISO/OSI i TCP/IP

<table>
<tr><th>Model ISO/OSI</th><th>Model TCP/IP</th><th colspan="2">Przykładowe protokoły</th></tr>
<tr><td>Warstwa aplikacji</td><td rowspan="3">Warstwa aplikacji</td><td rowspan="3">DNS, SNMP, syslog</td><td rowspan="3">Telnet, SSH, FTP, SMTP, http, POP, IMAP</td></tr>
<tr><td>Warstwa prezentacji</td></tr>
<tr><td>Warstwa sesji</td></tr>
<tr><td>Warstwa transportowa</td><td>Warstwa transportowa</td><td>UDP</td><td>TCMP</td></tr>
<tr><td>Warstwa sieciowa</td><td>Warstwa Internetu</td><td>IP</td><td>ICMP</td></tr>
<tr><td rowspan="2">Warstwa łącza danych</td><td rowspan="3">Warstwa dostępu do sieci</td><td rowspan="2">ARP, RARP</td><td>PPP SLIP</td></tr>
<tr><td>Etc.</td></tr>
<tr><td>Warstwa fizyczna</td><td colspan="2">IEEE 802.3</td></tr>
</table>

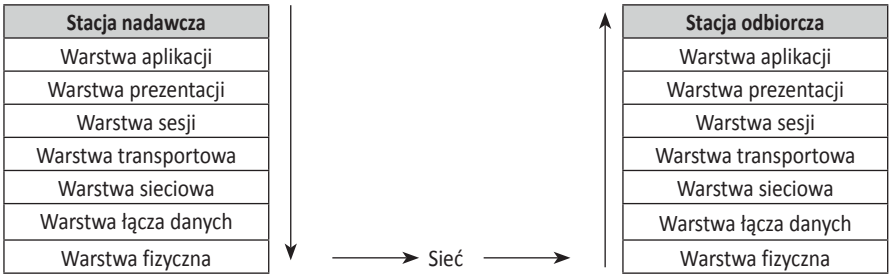
Źródło: opracowanie własne na podstawie K. Krysiak, *Sieci Komputerowe Kompendium*, wyd. Helion, Gliwice 2005, s. 30

[4] K. Krysiak, *Sieci komputerowe. Kompendium*, Gliwice 2005, s. 15.

[5] *Jak działa internet*, http://www.kopernik.org.pl/bazawiedzy/artykuly/technikabudowa-internetu-jak-dziala-internet [dostęp: 25.10.2017].

Tabela 1 przedstawia sposób, w jaki wygląda proces przesyłania danych. Drugim istotnym problemem jest drogą, dzięki której precyzyjnie za pomocą numeru IP przechodzi się konkretnie do wskazanego adresu, co prezentuje poniższy schemat.

Schemat 1. Opis transmisji danych między warstwami ISO/OSI



Źródło: R. Scrimger, P. LaSalle, C. Leitzke, M. Parihar, M. Gupta, *Biblia TCP/IP,* Gliwice 2002, s. 26

Z perspektywy połączenia topologii fizycznej, która opisuje sposoby fizycznego (np. elektrycznego) łączenia ze sobą komputerów[6], użytkownik w pierwszej kolejności łączy się z siecią lokalną tzw. LAN na przykład w budynku uniwersytetu. Przy założeniu, że będzie to laptop z wbudowaną kartą sieciową, odczytującą fale wifi oraz użytkownik będzie posiadał wymagane, ustalone przez administratora sieci hasło dostępu do sieci (o ile zostało takie ustanowione), połączy się z jednym z wielu routerów umieszczonym w zasięgu. Kontynuując, routerów jest kilkanaście w budynku, są one połączone kablem typu skrętka, na zasadzie topologii fizycznej typu gwiazda rozszerzona[7] z jednym urządzeniem (lub wieloma, zależy to od ilości routerów i innych czynników) zwanym switch.

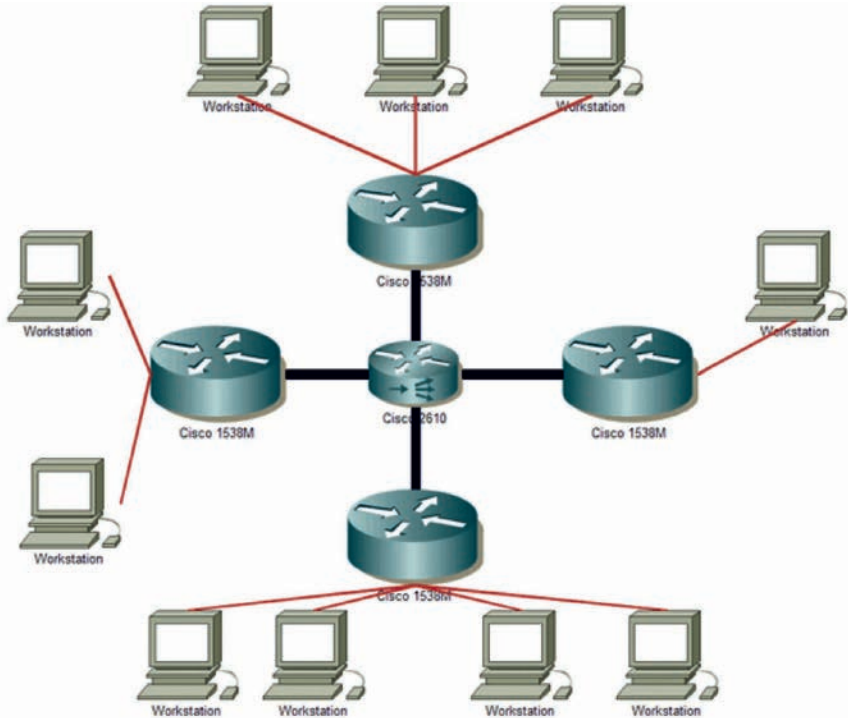
Switch jest bezpośrednio podłączony, w zależności od konkretnej technologii, określonym kablem z ISP. Te natomiast, dzięki posiadanej infrastrukturze komunikacyjnej, kontaktując się ze sobą tworzą ze punkty wymiany ruchu. Na nich oparte jest funkcjonowanie sieci MAN i WAN.

Internet, rozumiany potocznie, z którym łączymy się na co dzień, jest ostateczną formą wszelkiego wyniku działań, globalną „siecią sieci", która swoje funkcjonowanie opiera na istnieniu protokołu IP. Ten, natomiast składa się z tysięcy sieci WAN (Wide Area Network), czyli sieci obejmujących większy zakres powierzchniowy niż jedno miasto. Przykładem takiej sieci jest Pol-34, Polpak. Na sieci WAN składają się sieci MAN (Metropolitan Area Network), czyli sieć obejmująca całe miasto oraz LAN (Local Area Netwok) obejmująca zasięgiem jeden budynek, np. miejsce pracy, uniwersytet czy kawiarnię. Na końcu tego łańcucha jest odbiorca, który właśnie łączy się z infrastrukturą sieci LAN, nawet na drugim końcu świata. Zależności te ilustrują schematy 3 i 4.

[6] K. Krysiak, *Sieci komputerowe*..., s. 26.

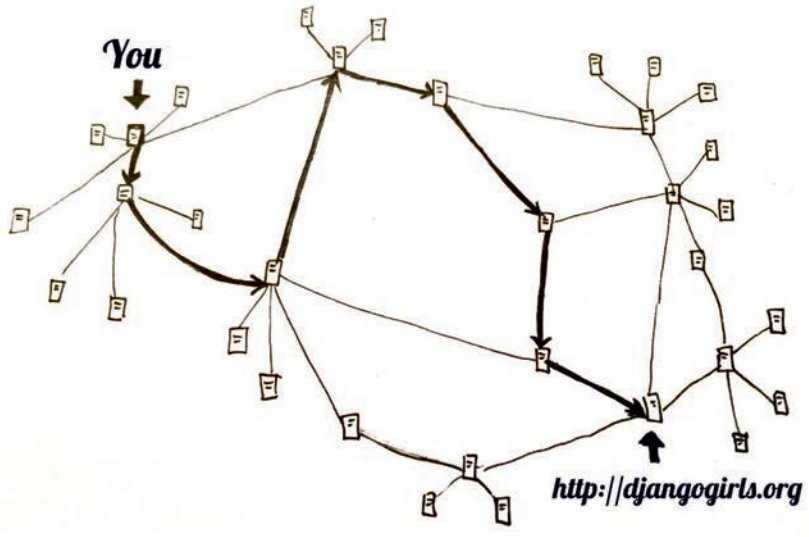
[7] Topologia fizyczna gwiazdy rozszerzonej jest jedną z wielu rodzajów takich topologii.

Schemat 2. Przykładowa struktura gwiazdy rozszerzonej



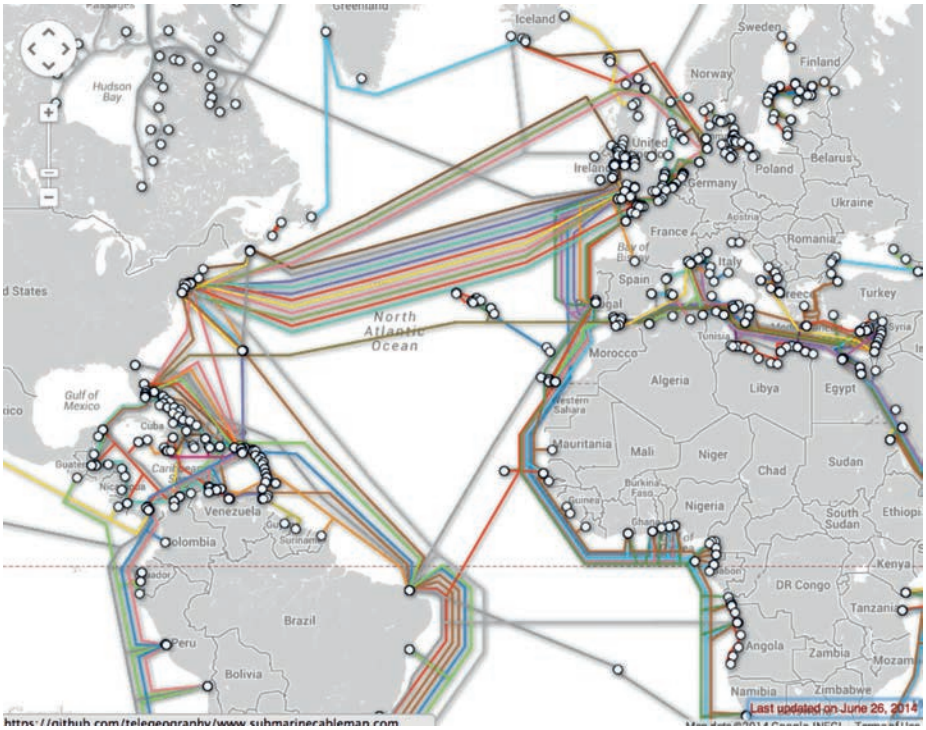
Źródło: Topologia sieci, http://kaliszmuzea.cba.pl/topologia-sieci.html [dostęp: 25.10.2017)

Schemat 3. Droga transmisji przez sieć fizyczną pomiędzy nadawcą (w tym wypadku stroną djangogirls.org) a odbiorcą



Źródło: http://tutorial.djangogirls.org/pl/how_the_internet_works [dostęp: 25.10.2017)

Schemat 4. Fragment mapy sieci światłowodów położonych na dnach mórz i oceanów, tworzących MAN



Źródło: Submarine Cable Map, http://submarinecablemap.com [dostęp: 25.10.2017)

Istnieją także sieci niepołączone z globalną siecią zwane intranetami. Najczęściej są budowane na potrzeby korporacji, przedsiębiorstw i nie są ograniczone czynnikami geograficznymi. Intranet działa podobnie do Internetu w sferze komunikacji, jednakże jest całkowicie oddzielony od globalnej sieci, Internetu.

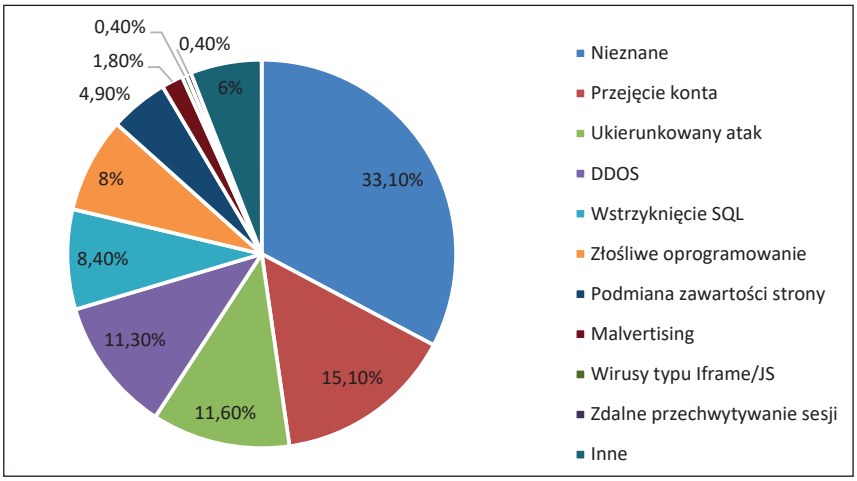
Metody ataków

By zapobiegać zagrożeniem oraz rozumieć ich istotę, ważna jest ich dogłębna znajomość. Zagrożenia związane z cyberprzestrzenią można kategoryzować pod kątem tego, czy powstały w związku z czynnikiem ludzkim, czy stricte z hardwarem lub softwarem. Jednak specjaliści od bezpieczeństwa nie podążają tym nurtem analizy, prawdopodobnie ze względu na jego nieprzydatność w odniesieniu do zagadnień związanych z zapobieganiem atakom. Bardzo często atak jest skierowany na wszystkie kategorie, które zostały wyżej wymienione, a znalezienie rozwiązania często wymaga improwizacji i niekonwencjonalnych działań.

Przyczyny i natura bardzo dużego odsetka ataków wciąż nie jest znana. Wiadomo, że system jest atakowany, lecz specjaliści nie potrafią go określić np. za pomocą jakiej metody. Problem ten ilustruje schemat 5.

Pracownicy polskiego CERT.GOV.PL (Computer Emergency Response Team), wyróżniają i kategoryzują zagrożenia w sposób, który precyzyjnie ilustruje tabela 2.

Schemat 5. Rozkład ataków w cyberprzestrzeni według ich typu w 2016 roku



Źródło: *2016 Cyber Attacks Statistics (Summary)*, http://www.hackmageddon.com/2017/01/19/2016-cyber--attacks-statistics/ [dostęp: 25.10.2017]

Organizacja CERT.GOV.PL jest rządową organizacją zajmująca się utrzymaniem bezpieczeństwa w kontekście cyberprzestrzeni w sektorze administracji publicznej i cywilnej, a jej głównym celami są między innymi

> [...] rozwijanie zdolności jednostek organizacyjnych administracji publicznej, Rzeczypospolitej Polskiej do ochrony przez zagrożeniami. Realizuje jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP. Stanowi poziom II-gi Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP[8].

Można więc uznać prezentowany przez nich spis zagrożeń za wiarygodny, a zaproponowaną nich ich kategoryzację za punkt wyjścia do analizy typologii zagrożeń.

Warto także zwrócić uwagę, żeCERT.GOV.PL nie jest jedyną organizacją zajmującą się bezpieczeństwem cyberprzestrzeni w Polsce. Od 1996 roku istnieje także CERT POLSKA, który funkcjonuje w ramach FIRST (Forum of Incidents Response and Security Teams)[9]. Z racji podobnych nazw i celów tych organizacji, często są one ze sobą mylone.

Nie można wszystkich wskazanych w powyższej tabeli zakwalifikować jako działania, które mogą implikować wybuch cyberwojny. Trudno też określić szczegółowo jak w praktyce wygląda działalność szpiegowska w kontekście cyberprzestrzeni ze względu na tajność tych informacji. Niewątpliwie warte szczególnej uwagi są najważniejsze, najbardziej znane i penetracyjne metody, które mogą być lub rzeczywiście były zastosowane podczas przeprowadzenia znanych cyberataków[10].

[8] *O nas CERT.GOV,* http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [dostęp: 25.10.2017].

[9] *CERT POLSKA*, http://www.first.org [dostęp: 25.10.2017] oraz http://www.first.org/members/teams/cert_polska [dostęp: 25.10.2017].

[10] Szerzej o przykładowych cyberatakach: W. Cendrowski, *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, [w:] *Walka informa-*

Tab. 2. Katalog zagrożeń stosowany przez CERT.GOV.PL

<table>
<tr><th></th><th>Zagrożenia</th><th colspan="5">Podatności</th></tr>
<tr><td rowspan="13">1. Działania celowe</td><td rowspan="2">1.1 – Oprogramowanie złośliwe</td><td>1.1.1 – Wirus</td><td colspan="2">1.1.3 – koń trojański</td><td colspan="2">1.1.4 – dialer</td></tr>
<tr><td colspan="3">1.1.2 – robak sieciowy</td><td colspan="2">1.1.5 – klient botnetu</td></tr>
<tr><td>1.2 – Przełamanie zabezpieczeń</td><td colspan="2">1.2.1 – nieuprawnione logowanie</td><td colspan="2">1.2.2 – włamanie na konta/ataki siłowe</td><td>1.2.3 – włamanie do aplikacji</td></tr>
<tr><td rowspan="2">1.3 – publikacje w sieci Internet</td><td>1.3.1 – treści obraźliwe</td><td colspan="2">1.3.2 – pomawianie (zniesławienie)</td><td colspan="2" rowspan="2">1.3.3 – naruszenie praw autorskich</td></tr>
<tr><td colspan="3">1.3.4 – dezinformacja</td></tr>
<tr><td rowspan="2">1.4 – gromadzenie informacji</td><td>1.4.2 – podsłuch</td><td colspan="2">1.4.3 – inżynieria społeczna</td><td colspan="2">1.4.4 – szpiegostwo</td></tr>
<tr><td colspan="3">1.4.1 – Skanowanie</td><td colspan="2">1.4.5 – SPAM</td></tr>
<tr><td rowspan="4">1.5 – sabotaż komputerowy</td><td colspan="3" rowspan="2">1.5.1 – nieuprawniona zmiana informacji</td><td colspan="2">1.5.5 – wykorzystanie podatności w urządzeniach</td></tr>
<tr><td colspan="2" rowspan="2">1.5.6 – wykorzystanie podatności aplikacji</td></tr>
<tr><td colspan="3">1.5.2 – nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji</td></tr>
<tr><td colspan="3">1.5.3 – atak dostępu (np. DDoS, DoS)</td></tr>
<tr><td>1.6 – czynnik ludzki</td><td colspan="5">1.5.4 – skasowanie danych</td></tr>
<tr><td>1.7 – cyberterroryzm</td><td colspan="3">1.6.1 – naruszenie procedur bezpieczeństwa</td><td colspan="2">1.6.2 – naruszenie obowiązujących przepisów prawnych</td></tr>
<tr><td rowspan="3">2. Działania niecelowe</td><td rowspan="2">2.1 – Wypadki i zdarzenia losowe</td><td colspan="5">1.7.1 – Przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni</td></tr>
<tr><td>2.1.1 – awarie sprzętowe</td><td colspan="2">2.1.2 – awarie łącza</td><td colspan="2">2.1.3 – awarie (błędy) programowania</td></tr>
<tr><td>2.2 – Czynnik ludzki</td><td>2.2.1 – naruszenie procedur</td><td colspan="2">2.2.3 – błędna konfiguracja urządzenia</td><td>2.2.4 – brak wiedzy</td><td>2.2.5 – naruszenie praw autorskich</td></tr>
<tr><td></td><td colspan="5">2.2.2 – zaniedbanie</td></tr>
</table>

Źródło: opracowanie własne na podstawie http://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731,Katalog-zagrozen-stosowany-przez-CERTGOVPL.html [dostęp: 25.10.2017)

Do tych z pewnością można zaliczyć pewne elementy z kategorii: oprogramowania złośliwego, sabotażu komputerowego, przełamywania zabezpieczeń, oraz gromadzenia informacji, w tym zwłaszcza inżynierii społecznej.

Zagrożenia związane ze złośliwym oprogramowaniem

Opis zagrożeń zawartych w tej części artykułu powstał przede wszystkim w oparciu o wcześniej zamieszczone opracowanie katalogu zagrożeń stosowanych przez CERT.GOV.PL oraz raport ENISA Threat Landscape 2015 – możliwie najaktualniejszy, wydany przez European Union Agency for Network and Information

cyjna. Uwarunkowania-incydenty-wyzwania, red. H. Batorowska, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Instytut Bezpieczeństwa i Edukacji Obywatelskiej, Katedra Kultury Informacyjnej i Zarządzania Informacją, Kraków 2017, s. 133 i n.

Security, jedną z ważniejszych instytucji odpowiedzialnych w UE za bezpieczeństwo w sieci. Ponadto warto zaznaczyć, że słowniczek NATO CCDCOE okazał się mało użyteczny. Dobór źródeł wynika w szczególności z oceny jego wartości. Dziwić może wysoka jakość źródeł UE i niekoniecznie jej dorównująca bazę wiedzy ze słowniczka NATO. UE stawia jednak bardzo mocny nacisk w swoich dwóch aktach prawnych na ochronę przeciw cyberprzestępczością i koncentruję się na ochronie cyberprzestrzeni na płaszczyźnie cyberprzestępstw. W przypadku bazy definicji NATO, która wciąż nie dysponuje jednolitym, mającym moc prawną dokumentem[11]. Sam słowniczek CCDCOE raczej koncentruje się na konkretnych zjawiskach oscylujących w tematyce cyberbezpieczeństwa w skali makro, co niekiedy obniża precyzję zawartych w nim definicji, niekiedy brakuje też opisu poszczególnych pojęć. Kryterium doboru zostało zastosowane w oparciu o uwarunkowania techniczne, czyli skalę możliwych negatywnych skutków oraz refleksji nad znanymi przypadkami incydentów cyberwojny.

1. Malicious code, malware – czyli wirusy, trojany, Robaki, Rootkity. Definicja tego zjawiska przede wszystkim sprowadza się do jego praktycznego działania – *[…] program infekujący pliki komputerowe poprzez umieszczenie kopii samego siebie w tych plikach[12]. Nazwa wzięła się od podobnego sposobu powielania jak wprzypadku wirusa biologicznego.*
2. SQL injection (z ang. 'wstrzyknięcie' kodu SQL), i jego odmiany np. Blind SQL injection oraz defacing – Jest to forma włamania się na stronę przy wykorzystaniu luk w kodzie i błędów popełnionych przez jej administratora. Właściwie pozwala na przejęcie kontroli nad stroną, uzyskaniu wszystkich informacji z serwera strony, na której się znajduje. Blind SQL injection jest losowym zgadywaniem haseł, komend, opierającym się na zasadach prostej logiki wynikającej z kodu strony. Defacment jest mniej wyrafinowany, jest to prosta zmiana treści, czy elementów graficznych, logicznych zawartych na stronie[13].
3. Odmowa Usługi (DoS – Denial of Service) – Jest to w chwili obecnej stara metoda ataku, ale wciąż skuteczna i jej stosowanie i skuteczność oraz popularność cały czas rośnie[14].Polega na zasypywaniu przez użytkowników serwera strony prośbami o dostęp. Ilość zgłoszeń musi przerosnąć umiejętności obliczeniowe serwera strony i dochodzi do zawieszenia systemu. Rodzajem ataku DoS jest DDoS – distributed denial of service, czyli atak z 'zewnątrz' (czyli zza granicy)[15].
4. Botnet – korelacja wielu maszyn uczestniczących w atakach DDoS czy DoS bez odpowiedniego oprogramowania jest niemożliwa. Dlatego w tym celu stworzono Botnety, czyli programy, które infekują tysiące komputerów i pozwalają

---

[11] Tallin Manual on the International Law Applicable to Cyber Warfare jest raczej opracowaniem prawnym i nie ma tam zawartych konkretnych definicji.

[12] Wirus [w:] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Akademia Obrony Narodowej, Warszawa 2008, s. 158.

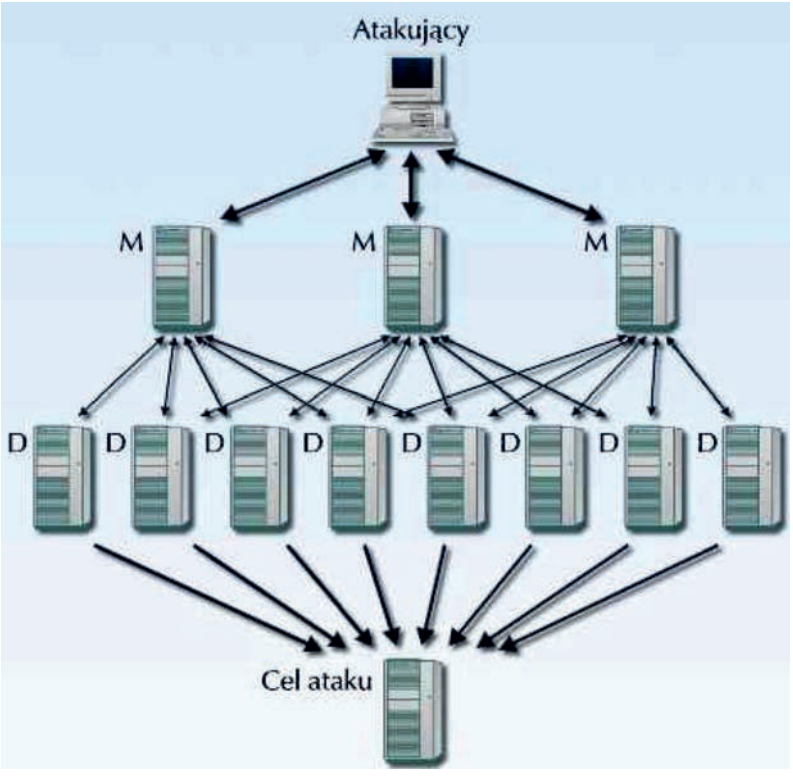
[13] SQL Injection – Podstawy, http://hack.pl/artykuly/dla-poczatkujacych/sql-injection-%E2%80%93-podstawy.html [dostęp: 25.10.2017].

[14] ENISA Threat Landscape 2015.

[15] G. Marczak, *8 mitów nt. ataków*,http://antyweb.pl/8-mitow-nt-atakow-ddos [dostęp: 25.10.2017].

przejąć nad nimi kontrolę lub tylko nad pewnymi jego działaniami[16]. Działanie botnetów w atakach DDoS czy Dos prezentuje schemat 6.

Schemat 6. Działania botneta w ataku DDos/DoS



Źródło: Ataki na systemy komputerowe, http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g7/#dos [dostęp: 25.10.2017)

5. Exploity – program jest najczęściej bardzo długim ciągiem kodu, wykonywanym w kompilatorze. Bardzo często przy jego pisaniu powstają błędy co jest dosyć normalne, ich ostatecznym wyeliminowaniem zajmują się pracownicy przeprowadzający testy penetracyjne w tym kodzie. Walka z błędami jest pewnego rodzaju standardem, ale też i niejednokrotnie jest ona skazana na porażkę. Doskonalenie konkretnych języków programowania, ciągłe przeszukiwanie kodu przez hakerów w celu znalezienia błędów, powodują, że mimo wydania np. konkretnego systemu operacyjnego, ciągle potrzebne jest wsparcie techniczne, które pracowały by nad tzw. patchami (z ang. łatkami). Tak też było np. w wypadku systemu Windows XP. Hakerzy, znajdując te luki, tworzą własne programy, które mogą 'dopisać', a właściwie 'doczepić' do luki coś, co może dać im dostęp do konkretnej lub szeregu jednostek operacyjnych[17].

[16] ENISA Threat Landscape 2015.

[17] *Exploity backdoory, rootkity*, https://www.pcformat.pl/Exploity-backdoory-rootkity,a,2577 [dostęp: 25.10.2017].

Zagrożenia związane z inżynierią społeczną

Powstanie cyberprzestrzeni pozwoliło na znaczny rozwój manipulacji i socjotechniki oraz szeroko pojętego wpływania na zachowania innych ludzi. Oczywiście, z historycznego punktu widzenia, nie jest to nowe zjawisko, jednakże rozwój technologiczny i zmiany społeczne doprowadziły do spopularyzowania tych zjawisk, wzrostu wartości szkód przy równoczesnej znikomej świadomości tego typu zagrożenia oraz braku rozwoju dziedziny obrony przed nimi. Warto przywołać tu przykład Kevina Mitnicka z USA, uważanego za największego orędownika socjotechniki samej w sobie. Dzięki bardzo dobrej znajomości systemów komputerowych, administracyjnych, telefonicznych, teleinformacyjnych i równoczesnym zastosowaniu metod socjotechnicznych, był w stanie w latach 80., w czasach nagłej informatyzacji społeczeństwa, bez problemu wykradać dane z największych ówczesnych korporacji oraz przez dwadzieścia lat uciekać przed amerykańskim wymiarem sprawiedliwości, zmieniając regularnie dane osobowe[18]. O ile jeszcze Mitnicka można uznać za cyberprzestępcę, to wiele wskazuje na to, że właśnie dzięki inżynierii społecznej udało się wprowadzić Stuxneta do komputerów obsługujących wirówki wzbogacające uran w Natanz[19].

W zakresie rozważań na temat socjotechniki (nazywanej niekiedy inżynierią społeczną) warto przytoczyć truizmy często przywoływane przez ekspertów: dany system bezpieczeństwa jest tak silny, jak jego najsłabsze ogniwo, zaś najczęściej tym najsłabszym ogniwem bywa człowiek[20]. To właśnie działanie człowieka niejednokrotnie otwiera drogę do ataku płynącego z cyberprzestrzeni. Przez taki rodzaj postępowania rozumieć należy podanie hasła nieodpowiedniej osobie, przyjęcie i zainstalowanie oprogramowania z nieodpowiedniego źródła czy choćby udzielenie informacji na temat typu zabezpieczeń przed złośliwym oprogramowaniem stosowanego w miejscu pracy.

Problematyka skutecznego narzucania swojej woli innym wydaje się zagadnieniem o ponadczasowym charakterze, jednak dopiero rozwój empirycznych metod badawczych w takich dyscyplinach naukowych jak psychologia czy socjologia, pozwoliły wyodrębnić i uzasadnić działanie określonych *metod i działań zmierzających do uzyskania pożądanego zachowania jednostek i grup ludzkich* [...][21], co stanowi istotę socjotechniki. Pozostaje jedynie kwestia świadomości ofiary – celem działania atakującego staje się osiągnięcie efektu w postaci podjęcia przez ofiarę świadomej decyzji, ale na zasadzie nieświadomego impulsu.

Wielu badaczy naprzemiennie stosuje słowa „manipulacja" i „socjotechnika", gdyż definicje obydwu tych pojęć są do siebie podobne. Analiza przykładów

[18] B. Gengler, *Super-hacker Kevin Mitnick takes a plea*, „Computer Fraud & Security" 1999, nr 5, s. 6 i n.

[19] P. Shakarian, J. Shakarian, A. Ruef, *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013, s. 224–234.

[20] *Człowiek najsłabszym ogniwem systemu bezpieczeństwa*, http://gazetasledcza.pl/2015/11/czlowiek-najslabszym-ogniwem-systemu-bezpieczenstwa [dostęp: 25.10.2017].

[21] T. Trejderowski, *Socjotechnika – podstawy manipulacji w praktyce,* Eneteia, Warszawa 2009, s. 15.

z praktyki wskazuje jednak, że socjotechnika jest bardziej uniwersalna pod względem możliwości jej stosowania, a stosujący ją bierze pod uwagę zdecydowanie mniej czynników w momencie, gdy chce wpłynąć na ofiarę[22]. Manipulacja z kolei, jak wskazują byli oficerowie CIA, Gregory Hartleya i Maryann Karinch w pracy pod tytułem *Podręcznik manipulacji*, wymaga pewnego schematu działania i zazwyczaj wymaga głębszej interakcji z celem[23]. To sprawia, że w operacjach w cyberprzestrzeni może mieć ona mniejsze zastosowanie, gdyż hakerzy chcą szybko osiągnąć swój cela zanim zostaną zdemaskowani. Atakujący bardzo często decydują się tylko na przelotny kontakt ze swoją ofiarą i nie mają czasu na zastosowanie bardziej skomplikowanych systemów manipulacji, także dlatego że przekraczanie kolejnych poziomów znajomości może doprowadzić do ujawnienia zamiarów atakującego. Priorytetem w socjotechnice jest zdobycie określonej informacji lub osiągnięcie konkretnego działania jednostki w jak najkrótszym czasie, najmniejszym wysiłkiem i bez wzbudzenia wątpliwości ofiary co do negatywnej oceny jej działania.

Niezaprzeczalnie techniki agentów CIA dotyczące skomplikowanej manipulacji prezentowane we wspomnianej książce są możliwe i przydatne w zdobywaniu potrzebnych informacji do prowadzenia cyberwojen czy cyberataków, jednakże na potrzeby niniejszego opracowania zaprezentowanych zostanie kilka podstawowych najczęściej stosowanych technik, powtarzających się socjotechnicznych reguł, które są fundamentem znacznej części ataków[24].

Pierwszą, podstawową regułą sięgającą swoją genezą niemalże początków kultury ludzkiej, jest reguła wzajemności. Często jest ona także określana w środowiskach socjologicznych i antropologicznych jako *Do ut des* (z łac. daję, abyś ty dawał). Chodzi tu o prostą zasadę rewanżu, chęć odwdzięczenia się drugiej osobie za wyświadczoną usługę. Tworzy to relację pomiędzy obydwiema stronami, która ma na celu ciągłą wymianę dóbr. Prowadzi to do wytworzenia się zaufania pomiędzy stronami, przekonania, że druga osoba w relacji będzie w stanie tak samo się poświęcić jak pierwsza[25]. Sama zasada nie zawsze jest zła, jednak staje się formą manipulacji, gdy zysk jest fikcyjny lub niższy niż spodziewany, a relacja wciąż trwa[26].

Drugim socjotechnicznym, a często też marketingowym dogmatem jest reguła sympatii. Chodzi w tym wypadku o wywołanie i utrwalenie możliwie najlepszych skojarzeń, pozytywnych emocji z danym obiektem. Dokonuje się tego poprzez zestawienie pozytywnych czynników z obiektem, których ten nie musi posiadać w rzeczywistości. |Potrzebne jest jedynie wytworzenie przekonania, że je posiada. Innym sposobem realizacji tej techniki jest, prezentacja przez atakującego takich samych lub podobnych cech, jakie posiada ofiara. Całokształt reguły odnosi się do sfery fizycznej, psychicznej i estetycznej[27].

---

[22] *Manipulacja, perswazja, socjotechnika – rozróżnienie pojęć*, http://liberum-cerebrum.blogspot.com/2013/09/manipulacja-perswazja-socjotechnika.html [dostęp: 25.10.2017].

[23] G. Hartley, M. Karinch, *Podręcznik Manipulacji*, Bellona, Warszawa 2011, s. 39–63.

[24] K. Mitnick, L.W. Simon, *Sztuka podstępu,* Helion, Gliwice 2010, s. 360.

[25] T. Trejderowski, *Socjotechnika – podstawy*…, s. 65.

[26] P. Sztompka, M. Kucia, *Socjologia. Lektury,* Znak, Kraków 2006, s. 102.

[27] T. Trejderowski, *Socjotechnika – podstawy*…, s. 102.

Trzecia reguła polega na ukazaniu konkretnego obiektu jako zasobu niedostępnego, rzadkiego, limitowanego, co sprawia, że jest ono postrzegane jako atrakcyjne. Zasada ta działa także w drugą stronę – wszystko co jest powszechnie dostępne dla jednostki ma dla niej niską wartość. Czwartą zasadą jest reguła dowodu społecznego, która polega na tym, że

> […] w swoich wyborach opieramy się na tym, co myślą i co robią inni, szczególnie w sytuacjach, w których nie wiemy jak się zachować. Świadomie lub nieświadomie kopiujemy wzorce zachowań innych. Robimy to zamiast wyrobić sobie własny pogląd i opierać się na nim. Ulegamy sugestii, że skoro wiele osób tak czyni, to nie może to być złe[28].

Piąta reguła, koncentruje się na wytworzeniu w obiekcie ataku sztucznego zaangażowania lub fałszywego przekonania, że został wdrożony w konkretny proces. Ma to implikować automatyczne wchodzenie na kolejne, głębsze poziomy procesu. W podobny sposób działa licencja oprogramowania w wersji trial. Użytkownik ściąga program który działa określoną ilość czasu, a po jego upływie jego opcje użytkowe wyłączają się. By je ponownie uaktywnić, trzeba wykupić pełną wersję. Chodzi o zmuszenie ofiary do podążania za konsekwencjami. Tak też się ta zasada nazywa – reguła konsekwencji[29].

Analizując socjotechnikę jako techniczne uwarunkowanie cyberataku, stwierdzić należy, że nie ma ściśle określonych technik walki z socjotechniką. Wydaje się, że najlepszą metodą jest zapobieganie poprzez praktyczną znajomość metod socjotechnik. To już daje umiejętność ich rozpoznawania i zareagowania z odpowiednią postawą asertywną. Inną metodą walki jest generowanie jak najmniej osobistych informacji na własny temat. Przed użyciem metod socjotechnicznych atakujący bardzo często dokonuje tzw. białego wywiadu na temat życia prywatnego swojego celu, by przeprowadzić atak możliwie najskuteczniej.

Podsumowanie

Internet sam w sobie jest przede wszystkim sferą komunikacji, w pewnej przenośni, dwutorową. Mamy kontakt z innymi poprzez przesyłane wiadomości, maile, obraz, etc. oraz poprzez nośnik tych treści – czyli komputer sam w sobie (hardware oraz software), pakiety przesyłane przez serwery etc. W związku z tym wskazać można dwie opcje na wykorzystanie Internetu w sposób zgodny z dążeniami konkretnego agresora, metody miękkie, uderzające bezpośrednio w wydobycie cennych informacji od osoby atakowanej, czyli socjotechnikę oraz drugą opcję, stricte techniczną, ingerująco bezpośrednio w systemy operacyjne użytkowników, czy serwerów. Cele samych ataków i zagrożeń cybernetycznych możemy podzielić na cele w skali mikro oraz makro. Celami mikro stają się przeciętni użytkownicy sieci, a celami makro pojedyncze miejsca o charakterze infrastruktury krytycznej, jak elektrownie, instytucje państwowe, lub media[30].

---

[28] Tamże, s. 164.

[29] Tamże, s. 186.

[30] *2013 Cyber Attacks Statistics,* http://www.hackmageddon.com/2014/01/19/2013-cyber-attacks-statistics-summary/ [dostęp: 25.10.2017].

W kontekście celów mikro, główna obrona bezpieczeństwa danych to firewalle lub antywirusy, które (jak sami ich twórcy przyznają) nie są w pełni przystosowane, mimo ciągłego wsparcia technicznego i aktualizacji, aby skutecznie ochraniać urządzenia[31]. Drugi problem tkwi w gwałtownym rozwoju informatyki, który implikuje znaczny problem z niezrównoważonym rozwojem w tym aspekcie. Tytułem egzemplifikacji w wielu państwach europejskich wciąż znaczna część bankomatów (które są de facto komputerami) funkcjonuje na przestarzałych systemach operacyjnych Windows XP[32], które z racji zakończonego wsparcia technicznego przez Microsoft na ten moment są niebezpieczne w użytkowaniu.

Podsumowując podkreśli należy, że szczególne znaczenie w zachowaniu względnego bezpieczeństwa w cyberprzestrzeni przypisać należy człowiekowi, jego ostrożności i przemyślanym zachowaniom. To zaś w możliwie największym stopniu osiągnąć można poszerzając wiedzę na temat tego, jak racjonalnie poruszać się na co dzień po cyberprzestrzeni.

Bibliografia

Opracowania

Cendrowski W., *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, [w:] *Walka informacyjna. Uwarunkowania-incydenty-wyzwania*, red. H. Batorowska, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Instytut Bezpieczeństwa i Edukacji Obywatelskiej, Katedra Kultury Informacyjnej i Zarządzania Informacją, Kraków 2017.

Cyber Warfare: A multidisciplinary analysis, red. J. Green, Routledge Taylor & Francis Group, London, New York 2015.

Gengler B., *Super-hacker Kevin Mitnick takes a plea*, „Computer Fraud & Security" 1999, nr 5.

Hartley G., Karinch M., *Podręcznik Manipulacji*, Bellona, Warszawa 2011.

Klepka R., *Wojna w mediach: wybrane zagadnienia dotyczące relacjonowania konfliktów zbrojnych*, „Wojny i konflikty. Przeszłość-Teraźniejszość-Przyszłość" 2016, nr 1(1).

Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005.

Mitnick K., Simon L.W., *Sztuka podstępu,* Helion, Gliwice 2010.

Shakarian P., Shakarian J., Ruef A., *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013.

Słownik terminów z zakresu bezpieczeństwa narodowego, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Akademia Obrony Narodowej, Warszawa 2008.

Sztompka P., Kucia M., *Socjologia. Lektury,* Znak, Kraków 2006.

Trejderowski T., *Socjotechnika – podstawy manipulacji w praktyce,* Eneteia, Warszawa 2009.

Winterfeld S., Andress J., *The Basics of Cyber Warfare*, Elsevier, Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013.

[31] *Katastroficzna wizja przyszłości Jewgienija Kasperskiego*, http://tech.wp.pl/kat,1009779,title,Katastroficzna-wizja-przyszlosci-Jewgienija-Kasperskiego,wid,14746527,wiadomosc.html?ticaid=11726d [dostęp: 25.10.2017].

[32] *Windows XP umiera – a co z bankomatami i urządzeniami informacyjnymi,* http://antyweb.pl/windows-xp-umiera-a-co-z-bankomatami-i-urzadzeniami-informacyjnymi/ [dostęp: 25.10.2017].

Źródła internetowe

O nas CERT.GOV. http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [dostęp: 25.10.2017].

SQL Injection – Podstawy, http://hack.pl/artykuly/dla-poczatkujacych/sql-injection-%E2%80%93-podstawy.html [dostęp: 25.10.2017].

Marczak G., *8 mitów nt. ataków*, http://antyweb.pl/8-mitow-nt-atakow-ddos [dostęp: 25.10.2017].

Exploity backdoory, rootkity, https://www.pcformat.pl/Exploity-backdoory-rootkity,a,2577 [dostęp: 25.10.2017].

Człowiek najsłabszym ogniwem systemu bezpieczeństwa, http://gazetasledcza.pl/2015/11/czlowiek-najslabszym-ogniwem-systemu-bezpieczenstwa [dostęp: 25.10.2017].

Manipulacja, perswazja, socjotechnika – rozróżnienie pojęć, http://liberum-cerebrum.blogspot.com/2013/09/manipulacja-perswazja-socjotechnika.html [dostęp: 25.10.2017].

2013 Cyber Attacks Statistics, http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ [dostęp: 25.10.2017].

Katastroficzna wizja przyszłości Jewgienija Kasperskiego, http://tech.wp.pl/kat,1009779,title,Katastroficzna-wizja-przyszlosci-Jewgienija-Kasperskiego,wid,14746527,wiadomosc.html?ticaid=11726d [dostęp: 25.10.2017].

Windows XP umiera – a co z bankomatami i urządzeniami informacyjnymi, http://antyweb.pl/windows-xp-umiera-a-co-z-bankomatami-i-urzadzeniami-informacyjnymi/ [dostęp: 25.10.2017].

http://www.first.org/members/teams/cert_polska [dostęp: 25.10.2017].

CERT POLSKA, http://www.first.org [dostęp: 25.10.2017].

Jak działa internet, http://www.kopernik.org.pl/bazawiedzy/artykuly/technikabudowa-internetu-jak-dziala-internet [dostęp: 25.10.2017].

Cyberwar: selected technical issues

Abstract

Cyberwar is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support)that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived). This article presents and analyzes selected technical issues of cyberwar: network behavior, attack methods, malware threats, and social engineering.

Słowa kluczowe: cyberwojna, socjotechnika, złośliwe oprogramowania, cyberprzestrzeń, cyberatak

Keywords: cyberwar, social engineering, malware, cyberspace, cyberattack

Wojciech Cendrowski
absolwent studiów na kierunku Bezpieczeństwo Narodowe na Uniwersytecie Pedagogicznym im. KEN w Krakowie, jego zainteresowania koncentrują się wokół problematyki cyberwojny i jej uwarunkowań, głównie prawnych i technicznych, autor artykułów poświęconych tej problematyce, uczestnik polskich i międzynarodowych konferencji naukowych.