Listopad 2013 r.

e-terroryzm.pl

wydanie specjalne
DLA „INSPIRACJI GRUPY 3S”

Fot.: C. Roberts, © Crown Copyright 2013

str.

Terroryzm

Bezpieczeństwo

Redakcja

Biuletyn redagują:

Przemysław Bacik
Agnieszka Bylica
Hanna Ismahilova
Jacek Kowalski
dr Kazimierz Kraj
Tobiasz Małysa
Natalia Noga
Piotr Podlasek
Anna Rejman
dr Jan Swół
Bernadetta Stachura-Terlecka
Tomasz Tylak
Ewa Wolska
Anna Wójcik

Skład techniczny: Tobiasz Małysa
Administrator www: Bernadetta Stachura-Terlecka

INSTYTUT STUDIÓW NAD TERRORYZMEM
WYŻSZA SZKOŁA INFORMATYKI I ZARZĄDZANIA z siedzibą w Rzeszowie

Fotografia na okładce: C. Roberts, © Crown Copyright 2013. Ilustracja na licencji Open Government License.
Źródło: http://www.defenceimagery.mod.uk/fotoweb/Grid.fwx?archiveId=5042&search=45156101.jpg

Szanowni Czytelnicy!

W waszych rękach znajduje się specjalne wydanie miesięcznika *e-Terroryzm.pl*. Wybór artykułów młodych badaczy problematyki bezpieczeństwa i terroryzmu, dotyczy kilku zagadnień. Wśród nich cyberterroryzmu, informatycznej infrastruktury krytycznej i jej prawnej ochrony, przeciwdziałaniu wyciekowi informacji w sieciach WiFi, modelowi działania w zakresie bezpieczeństwa informatycznego, zastosowaniu analizy urządzeń mobilnych w kryminalistyce, operacji *Czerwony Październik* oraz szacowaniu, analizie i zarządzaniu ryzykiem w zakresie informacji. Numer zamyka kompetentna analiza globalnych trendów zamachów terrorystycznych w latach 2010 - 2013.

Młodzi badacze, skupieni wokół projektu o nazwie *e- Terroryzm.pl:* Natalia Noga, Bernadetta Terlecka, Tobiasz Małysa oraz Jacek Kowalski prezentują swoje możliwości intelektualne, fachowe oraz wiedzę, która nie ustępuje doświadczonym badaczom. Ich wartością dodaną jest brak rutyny oraz fakt, że projekt, wokół, którego są skupieni, jest ich własną inicjatywą, wspieraną jedynie przez starszych kolegów.

Przedstawione poniżej artykuły nie dają odpowiedzi na wszystkie pytania, nie zawierają kompletnej wiedzy, chociażby ze względu na ich objętość. Mają służyć Czytelnikowi, każdemu zainteresowanemu poruszaną problematyką, pomocą w pogłębianiu wiedzy na ten temat. Mogą stanowić inspirację dla innych, być źródłem wiedzy i pomagać w edukacji na rzecz szeroko pojmowanego bezpieczeństwa. W tym wypadku związanego z instalacjami telekomunikacyjnymi i teleinformatycznymi. Podkreślać wagę informacji we współczesnym świecie, w tym informacji mających charakter poufny (tajemnice handlowe, techniczne, ekonomiczne przedsiębiorstwa), informacji zawierających dane wrażliwe (np. akta kadrowe).

Numer specjalny miesięcznika został tak pomyślany, aby stanowić uzupełnienie dla przedstawionego podczas spotkania *Inspiracje Grupy 3S* wystąpienia: *Polityczny wymiar cyberterroryzmu*.

Zapraszamy do lektury naszego opracowania oraz przekazywania uwag, opinii, propozycji i wniosków, które będą stanowić inspirację dla młodych badaczy, tych, którzy zaprezentowali w tym numerze swoje umiejętności oraz pozostałych uczestników projektu oraz innych chętnych.

Za zespół
Kazimierz Kraj

Publikacja jest bezpłatna, a zespół redakcyjny oraz Autorzy nie odnoszą z niej korzyści materialnych. Publikowane teksty stanowią własność Autorów, a prezentowane poglądy nie są oficjalnymi stanowiskami Instytutu Studiów nad Terroryzmem oraz Wyższej Szkoły Informatyki i Zarządzania.

Artykuły poruszane w czasopiśmie służą celom edukacyjnym oraz badawczym. Redakcja nie ponosi odpowiedzialności za inne ich wykorzystanie.

Zespół redakcyjny tworzą pracownicy Katedry Bezpieczeństwa Wewnętrznego i Instytutu Studiów nad Terroryzmem Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie oraz skupieni wokół tych jednostek znawcy i entuzjaści problematyki.

Adresy i kontakt:

- Poczta redakcji biuletynu:
  redakcja@e-terroryzm.pl
- Strona internetowa biuletynu:
  www.e-terroryzm.pl
- Instytut Studiów nad Terroryzmem:
  www.terroryzm.rzeszow.pl
- Wyższa Szkoła Informatyki i Zarządzania:
  www.wsiz.rzeszow.pl

Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie,
ul. Sucharskiego 2, 32-225 Rzeszów

NATALIA NOGA

Cyberterroryzm - groźba realna

Terroryzm jest jednym z największych problemów współczesnego świata. Podczas ostatniej dekady problem ten ewoluował i przybrał nowe oblicze. Doszło do swoistej zmiany jakościowej tego zjawiska, gdzie działania o charakterze terrorystycznym zostały oparte na wykorzystaniu nowych środków i technik. Oczywisty jest fakt, iż w obecnych czasach funkcjonowanie społeczeństw w coraz większym stopniu staje się uzależnione od systemów informatycznych, a zwiększenie możliwości wykorzystania zaawansowanej technologii powoduje pojawienie się nowego obszaru do nielegalnej działalności.

Dostrzec można, że w związku z tym Internet może być doskonałym narzędziem wykorzystywanym również przez terrorystów. Dzięki rozwojowi technologii informacyjnej z terroryzmu klasycznego wyewoluował jego obecnie najgroźniejszy rodzaj – cyberterroryzm, a zapewnienie bezpieczeństwa w tej dziedzinie stanowi niezwykle ważną gałąź bezpieczeństwa narodowego i jest jednym z najważniejszych wyzwań XXI wieku. Głównym problemem podjętym w pracy jest wskazanie cyberterroryzmu jako jednego z najpoważniejszych i niedocenianych zagrożeń współczesnego świata. Ponadto, praca ma na celu ukazanie analizy tego zjawiska w dwóch aspektach – kiedy Internet jest obiektem ataków lub narzędziem w rękach terrorystów. W odpowiedzi na pytania badawcze autor przedstawi zalety stosowania tej metody walki widziane oczami terrorystów, sposoby, w jaki terroryści mogą wykorzystywać Internet w atakach oraz jakie skutki mogą przynieść takie ataki.

Cyberterroryzm – groźba realna

Internet łączy już dziesiątki milionów ludzi na całym świecie, a dynamiczny rozwój infrastruktury systemów komputerowych spowodował wzrost efektywności niemal każdej dziedziny ludzkiej działalności. Obecnie znaczna część gospodarki zależna jest od sprawnego funkcjonowania systemów komputerowych. Wraz z rozwojem tych systemów pojawiają się również problemy związane z jego niewłaściwym wykorzystaniem. Rozwój technologii informacyjnej niesie z sobą zatem nie tylko nowe możliwości, ale i nowe zagrożenia związane z cyberprzestrzenią. Jest ona bowiem nie tylko przestrzenią komunikacyjną, ale i *„polem walki, terenem, na którym podejmowane są skoordynowane akcje o zabarwieniu politycznym o mniej lub bardziej destrukcyjnym charakterze”*[1]. Już w latach 90. XX wieku zauważono związek pomiędzy zmianami zachodzącymi w światowym terroryzmie a gwałtownym rozwojem technik informatycznych. Coraz częściej mówiono o powstaniu zupełnie nowych form terroryzmu, który w dużej mierze nastawiony będzie na korzystanie z sieci komputerowych i informacyjnych[2]. Wykorzystanie takich technik sprzyjałoby przeprowadzaniu bardziej elastycznych i szybkich ataków. Nawet kilka lat temu Mohammed Omar Bakri, radykalny imam z Londynu, groził, że Al – Kaida wykorzysta sieć komputerową do zadania ciosu Zachodowi[3]. W niedługim czasie ekstremiści do perfekcji opanowali sztukę wykorzystywania Internetu do walki ideologicznej. Teraz szukają sposobów, by spowodować straty w gospodarce i zdezorganizować życie zachodnich społeczeństw. 11 września przekonaliśmy się, że groźba terroryzmu wzrasta, a terroryści są skłonni użyć wszelkich dostępnych środków do osiągnięcia celu. Rozpoczęta po atakach na World Trade Center wojna z terroryzmem przyczyniła się do szybkiego przejmowania taktyk walki cybernetycznej przez organizacje terrorystyczne. Miało to wpływ na powstanie nowej formy terroryzmu, a mianowicie cyberterroryzmu, który w najbliższym czasie może przyjąć formę szczególnego niebezpieczeństwa określanego nawet katastroficznym.

Omawiając zagadnienia związane z cyberterroryzmem i niebezpieczeństwem, jakie z sobą niesie, warto zacząć od przytoczenia definicji tego pojęcia. W literaturze takich definicji możemy znaleźć bardzo wiele. Zdaniem D. Denning, amerykańskiego eksperta do spraw cyberbezpieczeństwa, cyberterroryzm to *„(...) groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują poczucie strachu”*[4]. Analizując te słowa można wywnioskować, że zjawisko to polega na ingerencji w sieci informatyczne w celu objęcia całkowitej kontroli nad funkcjonowaniem systemu z zamiarem zniszczenia lub uniemożliwienia jego funkcjonowania czy też sprawowania nad nim kontroli. Jednak opierając się na tej definicji można stwierdzić, że do tej pory nie było przypadku aktu cyberterrorystycznego. Nieco inną definicję tego pojęcia stworzył NIPC (US National Infrastructure Protecion Centre - Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych), tj. *„(...) akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu”*[5]. Posługując się tą definicją można stwierdzić, że na świecie były już przypadki aktów cyberterroryzmu. Należą do nich między innymi przypadek „cybotażu” na australijską oczyszczalnię ścieków czy ataki cybernetyczne na obiekty infrastruktury krytycznej Estonii. Szczególnie użyteczną definicję pojęcia cyberterroryzmu przedstawia agent specjalny FBI, Mark Pollit. Łączy on dwa elementy – „terroryzm” i „cyberprzestrzeń” mówiąc, że *„cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany na informacje, systemy komputerowe, programy i bazy danych, który prowadzi do zniszczenia celów niewojskowych, przeprowadzony przez grupy obce narodowościowo lub przez tajnych agentów”*[6]. Jest to wybiegająca w przyszłość definicja cyberterroryzmu i terroryzmu w ogóle. Nie ogranicza ona cyberterroryzmu do zjawisk czysto informatycznych. Wywnioskować z niej można, że atak na informacje i systemy komputerowe może nastąpić przy użyciu środków zarówno fizycznych, jak i informatycznych. Na tej podstawie należy zrozumieć, czego możemy się spodziewać w najbliższym czasie i w jakim kierunku zmierza terroryzm. Wszystkie przedstawione definicje pojęcia cyberterroryzmu ukazują zatem, że jest to działanie, w którym posługiwanie się zdobyczami technologii informacyjnej ma na celu wyrządzenie szkody z pobudek ideologicznych lub politycznych, szczególnie w odniesieniu do infrastruktury o istotnym znaczeniu dla obronności lub gospodarki atakowanego kraju.

Trochę historii

Pierwsze wzmianki o niebezpieczeństwie zamachów terrorystycznych przy użyciu systemów komputerowych pojawiły się w 1979 r. w raporcie szwedzkiego ministerstwa obrony na temat zagrożeń społecznych związanych z komputeryzacją[7]. W wypowiedziach amerykańskich specjalistów w dziedzinie wywiadu wojskowego samo słowo *cyberterroryzm* zaczęło być używane już w latach 80. O tej nowej formie terroryzmu zaczęto mówić coraz częściej. Na przełomie lat 80/90 XX wieku medialną gwiazdą został Kevin Mitnick. Na liście poszukiwanych przez FBI oszustów komputerowych zajmował pierwsze miejsce. Został schwytany w 1995 r. i skazany wyrokiem sądu na wieloletnie pozbawienie polności uzasadnieniem: „uzbrojony w klawiaturę, jest groźny dla społeczeństwa”[8]. Był znakomitym hakerem, włamał się m.in. do komputerów Pentagonu, laborato-

rium Digital Equipment Corporation, banków i sieci telefonicznej Pacific Bell, z których wykradał tajne dane. Po odbyciu wyroku został konsultantem firmy zabezpieczającej komputery, a narzędzia, których używał w czasie włamań zostały wykorzystane w systemach zabezpieczeń wielu krajów. Zbieranie informacji oraz operacje psychologiczne i manipulowanie percepcją w wojnie informacyjnej stosowali również terroryści. Niektóre grupy w swoich działaniach wykorzystywali Internet do propagandy i zbierając informacje z różnych bezpośrednio przyłączonych źródeł. Clark Staten, dyrektor ENRI (Emergency Response & Research Institute - Instytut Badania Nagłych Sytuacji i Reagowania na nie) w lutym 1998r. zeznał przed podkomisją senatu amerykańskiego, że *„nawet małe grupy terrorystyczne korzystają teraz z Internetu do nadawania komunikatów i jednoczesnego wprowadzania w błąd ludności wielu krajów”*[9]. Przekazał on również kopie komunikatów z propagandą antyamerykańską i antyizraelską oraz groźbami, gdzie szeroko było rozpowszechniane hasło ekstremistów wzywające do „dżihad” przeciw Ameryce i Wielkiej Brytanii. W czerwcu tego samego roku w US News & World Report podano, że z 30 grup terrorystycznych (które umieszczone są na liście amerykańskiego Departamentu Stanu) 12 znajduje się w Internecie i nie można zmusić ich do opuszczenia sieci[10].

Obecnie nie ma dowodów na to, że któryś z krajów na świecie prowadzi cyberataki, jednak Internet już nie raz był wykorzystywany jako broń. W roku 1999, w czasie walk w Kosowie, obie strony konfliktu korzystały z Internetu. Wspierał on oficjalną propagandę zarówno natowską, jak i jugosłowiańską, służył do komunikowania się, demonizowania przeciwnika, atakowania za pomocą wirusów i włamywania się na strony internetowe. Serbowie wysyłali tysiące e-maili z apelem o zaprzestanie bombardowania do różnego rodzaju organizacji – prasy, radia, telewizji, rządów państw NATO. Niektóre z nich skupiały się na masakrach, które powodowały naloty dokonywane przez natowskie samoloty, inne miały charakter antyamerykański i antynatowski. Z kolei NATO, Brytyjczycy i Amerykanie Internetu używali do celów propagandowych[11]. NATO poniosło istotną porażkę prestiżową już tydzień po rozpoczęciu operacji. Atakujący hakerzy z Serbii i Czarnogóry zablokowali oficjalny serwer WWW Sojuszu wysyłając przez łącza poczty elektronicznej kilkadziesiąt tysięcy listów protestujących przeciw operacji NATO w Jugosławii. Informatycy musieli zmienić strukturę sieci i oficjalną stronę internetową, a także założyć odpowiednie filtry wzmacniające moc serwerów. Przykład ten jest znakomitym dowodem na to, że konfliktowi konwencjonalnemu mogą towarzyszyć również konflikty elektroniczne.

Falę ataków cyfrowych spowodował konflikt chińsko–tajwański. W roku 1999 r., kiedy prezydent Tajwanu Li Teng-Hui wezwał do traktowania Tajwanu i Chin jako równoprawnych państw mówiąc, że relacje z Chińską Republiką Ludową mają charakter „specjalnych stosunków międzypaństwowych”, spowodował wzrost napięcia w kontaktach z CHRL. Konflikt ten miał swoje odbicie w cyberprzestrzeni, gdyż na początku 1999 r. chińscy hakerzy uderzyli na kilka tajwańskich stron rządowych. Najpoważniejszym atakiem był ten z 11 sierpnia, kiedy zablokowano działanie i skasowano dane strony Kongresu. Na zaatakowanych stronach umieszczono napis „Istnieją tylko jedne Chiny, tylko jedne Chiny są potrzebne” oraz czerwoną flagę[12].

Najbardziej zaciętą wojną internetową był jednak konflikt arabsko – izraelski. Palestyńczycy nazywają tę formę walki elektronicznym *dżihadem*. Wszystko zaczęło się w październiku 2000 roku, gdy libański Hezbollah uprowadził do Libanu trzech izraelskich żołnierzy. Po raz pierwszy od wiosny 2000 roku, gdy siły zbrojne Izraela wycofały się z Libanu, ich pododdziały znowu się tam pojawiły. Zmaganiom towarzyszyły walki w sieci. Do akcji przystąpili hakerzy obu stron, bez słowa zachęty ze strony rządu. Pro-izraelscy hakerzy atakowali strony internetowe, przede wszystkim rządowe i finansowe. Włamali się również na stronę organizacji terrorystycznej umieszczając na niej gwiazdę Dawida, izraelski hymn i hebrajskie napisy. W odpowiedzi pro-

palestyńscy hakerzy zaatakowali strony Kancelarii Prezesa Rady Ministrów oraz Ministerstwa Obrony. Wśród nich działali terroryści z Hezbollahu, Hamasu, Al-Kaidy i innych organizacji.

Do komputerowych ataków dochodzi nie tylko na Bliskim Wschodzie. W kwietniu 2001 roku Chińczycy przejęli amerykański samolot zwiadowczy, który po zderzeniu z chińskim myśliwcem przymusowo lądował w Chinach. Pekin oskarżył Waszyngton o szpiegostwo, a do akcji ruszyli hakerzy, którzy próbowali usuwać słowa poparcia dla rządu wroga. Pomiędzy Chinami a USA wybuchła wojna elektroniczna. Amerykańscy hakerzy na stronach chińskich instytucji i firm umieścili pornograficzne obrazki i obraźliwe hasła, a ponadto dokonali kilkuset ataków m.in. na China Telecom, China Nuclear Information Center oraz strony rządowe. Chińczycy odpowiedzieli od razu. Na stworzonej przez nich stronie KillUSA.com wszyscy, którzy chcieli wziąć udział w antyamerykańskiej krucjacie, mogli znaleźć potrzebne do tego oprogramowanie. Zaatakowano też Biały Dom, Departamenty Pracy, Zdrowia, Energetyki, Spraw Wewnętrznych, Izbę Reprezentantów i Dowództwo Marynarki Wojennej. W wyniku obopólnych działań zdobyto ponad 300 chińskich i półtora tysiąca stron amerykańskich[13]. Elektroniczny konflikt między tymi dwoma państwami udowodnił, że ataki hakerów stają się coraz groźniejsze i że być może w przyszłości wojna taka spowoduje znacznie poważniejsze skutki.

Innym, nagłośnionym publicznie atakiem był przypadek „cybotażu" na oczyszczalnie ścieków w australijskim Sunshine Cost z 2000 roku. 49-letni konsultant projektu wodnego, którego nie przyjęto do pracy w firmie instalującej komputerowy system sterowania przepływem ścieków dla Maroochy Shire Council, włamał się do tego systemu i skierował miliony litrów zanieczyszczeń do parków, rzek i zakładów przemysłowych. W wyniku ataku zginęła olbrzymia liczba zwierząt wodnych, a woda w strumieniach stała się czarna. Jest to pierwsze znane umyślne cybernetyczne uderzenie na infrastrukturę krytyczną dokonane przy użyciu dostępnych w Internecie narzędzi. Istotny jest fakt, że powiodła się dopiero 45 próba ataku, a poprzednie 44 nieudane nie zostały nawet zauważone[14]. Możliwość przeprowadzenia ataku cyberterrorystycznego na infrastrukturę krytyczną państwa amerykańskie służby specjalne zauważyły też w roku 2002 roku. Znaleziono wtedy w Kabulu w komputerze członka Al-Kaidy dowody, że organizacja ta zainteresowana jest uderzeniem w cyfrowe systemy kontroli. Odkryto liczne narzędzia internetowe, mogące służyć do przeprowadzenia ataku, a także ukryte pliki przedstawiające model jednej z tam wodnych oraz oprogramowanie stymulujące katastrofę. Po raz kolejny widać, że przeprowadzenie ataku cyberterrorystycznego jest o wiele łatwiejsze, gdyż zniszczenie tamy w konwencjonalny sposób wymagałoby użycia wielu ton materiałów wybuchowych. Podobne zagrożenie istniało w roku 1997, kiedy to 12 letni haker przypadkowo włamał się do systemu sterującego tamą w Arizonie. Przez swoje działanie mógł spowodować ogromną katastrofę.

Stosowanie technologii informatycznych i zdobywanie doświadczenia w posługiwaniu się komputerami powinno być znakiem ostrzegawczym już po 11 września 2001 roku. Wtedy to Ramzi Yousef – mózg zamachu bombowego na World Trade Center – w swoim komputerze przechowywał plany zniszczenia amerykańskich samolotów[15]. Ataki na World Trade Center w Nowym Jorku i Pentagon w Waszyngtonie w sposób jednoznaczny udowodniły, że *„(...) dzisiejsze zagrożenia posiadają inną naturę i skalę niż dotychczas, a współczesna odpowiedź na te zagrożenia jest nieadekwatna. Broń projektowana w celu przeciwstawienia się zagrożeniom, w końcu ostatniego tysiąclecia, nie będzie w stanie sprostać im w pierwszych dekadach XXI wieku. Nowe, często o asymetrycznym charakterze zagrożenia dla bezpieczeństwa globalnego wymagają nowego myślenia"*[16]. Zamachy te pokazały, że pomiędzy cyberstrukturami i strukturami fizycznymi istnieją wzajemne powiązania, a zniszczenie jednej pociąga konsekwencje dla drugiej. Jest to tzw. efekt domina -

uszkodzenie sieci w jednym sektorze gospodarki może wywołać przerwanie działania wielu innych, a tym samym spowodować zagrożenie dla bezpieczeństwa narodowego. Po atakach stratami nie tylko ludzkimi, ale i właśnie zniszczeniami w gospodarce, stratami firm i rynków finansowych przechwalał się Osama bin Laden. W swoich wypowiedziach podkreślał często, że wydarzenia te kosztowały Amerykę biliony dolarów. Miał zatem rację Brenton Greene (zastępca menadżera National Communications System) mówiąc, że *„każde poważne cyberzdarzenie będzie miało swoje konsekwencje fizyczne i odwrotnie – każde poważne zdarzenie fizyczne będzie miało swoje konsekwencje w cyberprzestrzeni. W rezultacie oddzielenie zdarzeń obu typów nie będzie możliwy”*[17].

Ewolucja terroryzmu w kierunku korzystania z nowoczesnych technologii postępuje coraz szybciej od rozpoczęcia amerykańskiej wojny z terroryzmem. Zauważyć można coraz więcej dowodów wskazujących na zainteresowanie organizacji terrorystycznych wykorzystaniem nowoczesnych technologii, głównie Internetu, w swoich działaniach. W jednej z siedzib Al – Kaidy amerykańscy żołnierze znaleźli komputer z modelami zapory wodnej. Został on sporządzony za pomocą specjalistycznego oprogramowania inżynierskiego i architektonicznego, a służyć miał studiowaniu najlepszych sposobów atakowania zapór oraz symulowania katastrof spowodowanych ich uszkodzeniem[18]. Agenci Al – Kaidy, którzy rozproszeni są po całym świecie także przyznali, że byli szkoleni do przeprowadzania ataków na ważne części infrastruktury.

Rosnące zagrożenie cyberterrorystyczne zauważono także w roku 2002, kiedy CIA w liście przesłanym do przewodniczącego Senackiej Komisji specjalnej do spraw wywiadu – senatora Boba Grahama – stwierdza, że *„(...) Al - Kaida i różne sunnickie grupy ekstremistyczne popierające działania antyamerykańskie prawdopodobnie spróbują dokonać w przyszłości ataku cybernetycznego. Jest to zgodne zarówno z ich intencjami, jak i z żądzą rozwijania umiejętności hackerskich i informatycznych potrzeb do stworzenia efektywnego modus operandi, nieodzownego do dokonywania skutecznych cyberataków (...) Przeprowadzenie cyberataków na systemy staje się coraz bardziej możliwe dla terrorystów – w miarę zapoznawania się przez nich z celami ataków i technologiami potrzebnymi do ich przeprowadzenia. Różne grupy terrorystyczne, łącznie z Al – Kaidą i Hezbollahem, coraz skuteczniej posługują się technologiami internetowymi i komputerowymi – FBI odnotowuje rosnącą liczbę zagrożeń”*[19].

Cyberatak na Koreę Południową

W środę 20 marca nastąpił atak na serwery bankowe i sieci telewizyjnych w Korei Południowej. Do ataku doszło dzień po ogłoszeniu przelotów amerykańskich bombowców strategicznych B-52. O sprawstwo tegoż ataku Koreańczycy podejrzewali pierwotnie Koreę Północną. Jednak jak poinformował rzecznik Południowokoreańskiej Komisji ds. Komunikacji podczas konferencji prasowej adres IP z którego mogło dojść do ataków (połączył się on z poszkodowanymi organizacjami) należy do pul adresowych zarejestrowanych w Chinach. Na ekranach niektórych komputerów pojawiła się czaszka i ostrzeżenia grupy nazywającej się „Whois Team” oraz informujące o tym, że to dopiero początek.

W czasie ataku ucierpiały 3 stacje telewizyjne: KBS, MBC i YTN. Stacje te pomimo problemów nie przerwały nadawania programów. Kolejnymi celami ataków były 2 banki Shinhan Bank i NongHyup Bank. W przypadku banków problemy z serwerami uniemożliwiły ich pracę nie było możliwości wybierania pieniędzy z bankomatu czy płatności za pomocą kart, bankowość elektroniczna również przestała działać.

W kwietniu 2007 r. świat obiegła kolejna elektryzująca wiadomość. Tym razem doszło do zorganizowanego na dużą skalę ataku cybernetycznego na obiekty infrastruktury krytycznej Estonii. Za tym wydarzeniem przemawia kontekst sytuacyjny, gdyż przed inwazją doszło w Tallinie do krwawych zamieszek ulicznych między członkami rosyjskiej mniejszości narodowej a estońskimi nacjonalistami z powodu przeniesienia pomnika ku czci żołnierzy radzieckich. Rosyjscy hakerzy przechwycili kontrolę na ponad milionem prywatnych komputerów w 174 krajach i stworzyli cyberne-

tyczną broń, za pomocą której przez trzy tygodnie bombardowali serwery estońskiej infrastruktury krytycznej: banki, urząd prezydenta, ministerstwa, urzędy bezpieczeństwa państwa, środki masowej komunikacji itp[20]. Wszystkie te działania skutecznie paraliżowały pracę atakowanych obiektów. Premier Estonii przyznał, że *„testowano nowy model wojny cybernetycznej* i, że *to pierwszy przypadek takiego zaatakowania niepodległego państwa przez Internet"*[21]. Ten przypadek znów udowadnia skuteczność wojny cybernetycznej.

W 2008 roku również doszło do ataków cybernetycznych. Miały one miejsce w Gruzji, a odbyły się równolegle do konwencjonalnych działań wojennych. Doszło wtedy do zmasowanych ataków na gruzińskie strony internetowe, a zniekształcone zostały najważniejsze strony państwowe. Dziś o te ataki podejrzewa się głównie obywateli Rosji, a w szczególności organizację Russian Business Network. Wynika to z faktu, iż na rosyjskich serwisach internetowych podczas rozpoczęcia działań zbrojnych zaczęły się pojawiać narzędzia i ogólnodostępne instrukcje do przeprowadzania ataków wraz z listą celów[22].

Szokującą informacją dla świata była również wiadomość na temat ataku cybernetycznego z października 2010 roku, w skutek którego zainfekowane zostały irańskie systemy obsługujące niemal całą infrastrukturę państwa – od sieci elektrowni, przez rurociągi ropy naftowej, aż po systemy wojskowe. Przypuszcza się, że celem ataku było zniszczenie, uszkodzenie bądź zlikwidowanie reaktora jądrowego Iranu. Nie wyklucza się, że trojan którego użyto – *Stuxnet*[23], został wprowadzony do irańskiego systemu przez pracownika jednej z rosyjskich firm podwykonawczych zaangażowanych w budowę elektrowni. Trojan ten skutecznie sparaliżował irański system komputerowy, który nadzorował pracę podziemnego ośrodka wzbogacania uranu w Natanz, opóźniając uruchomienie elektrowni jądrowej w Buszerze o dwa miesiące[24]. O skali ataku świadczyć może fakt, że w Iranie zainfekowanych zostało blisko 30 tysięcy komputerów.

Przypisy

1 A. Adamski, Cyberterroryzm, [w:] Materiały z konferencji na temat terroryzmu 11.04.2002r., Wydział Prawa UMK Toruń, Toruń 2002, s.6.
2 W.J. Wójcik, Zagrożenia w cyberprzestrzeni a przestępstwa ekonomiczne, [w:] Cyberterroryzm – nowe wyzwania XXI wieku, [z:] http: // www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/Wojcik.pdf, s. 4, z dnia 15.06.2012
3 D. Verton., Black Ice. Niewidzialna groźba cyberterroryzmu, Helion, 2004, s.133.
4 D. Denning, Cyberterrorism, [z:] http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc, z dnia 24.08.2000
5 L. Garrison., M.Grand, Cyberterrorism: An evolving concept, NIPC Highlights, [z:] http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm
6 M. Pollit., Cyberterrorism: Fact or Fancy? Prceedungs of 20-th National Information Systems Security Conference, październik 1997, s. 285-289.
7 M. Łapczyński, Czy grozi nam cyberterroryzm? http://konflikty.wp.pl/kat,1020699,title,Czy-grozi-nam-cyberterroryzm,wid,11640989,wiadomosc.html?ticaid=1dcc6&_ticrsn=3, z dnia 29.10.2010.
8 L.M. Terrence, Cyberterrorism.
9 L. Staten Clark, zeznanie przed Subcommitte of Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, 24.02.1998.
10 D. Denning Wojna informacyjna i bezpieczeństwo informacji, Wydawnictwa Naukowo- Techniczne, Warszawa 2002, s.77.
11 M.F. Gawrycki, Cyberterroryzm, Fundacja Studiów Międzynarodowych, Warszawa 2003, s.166-167.
12 Tamże, s. 171.
13 L.M. Terrence, Cyberterrorism... dz. cyt.
14 D. Verton, Black ice..., dz. cyt., s.67.
15 B. Hołyst., Cyberterroryzm, [z:] http://www.zabezpieczenia.com.pl/ochrona-informacji/cyberterroryzm, z dnia15.06.2012.
16 R. Hall, C. Fox, Ponownie przemyśleć bezpieczeństwo, Przegląd NATO, Zima 2001/2002, s.8.
17 L.M. Terrence, Cyberterrorism, ETE TOO, productions for The History Channel, A&E Television Networks 2003.
18 D. Verton, Black Ice..., dz. cyt., s.68.
19 Tamże, s.164.
20 R. Białoskórski, Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku – zarys problematyki, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, s. 50.
23 Na Estonii testowano wojnę cybernetyczną, Wprost 24, 29.05.2007r. http://www.wprost.pl/ar/?O=107407, z dnia 15.06.2012.
24 I. Bunsch., J. Świątkowska, Cyberterroryzm – Nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku, [z:] http://ik.org.pl/pl/publikacja/nr/4298/ z dnia 15.06.2012, s. 9.
25 Pierwszy znany robak używany do przeprogramowywania instalacji przemysłowych i szpiegowania.
26 R. Białoskórski, Cyberzagrożenia..., dz. cyt,. s. 52.

NATALIA NOGA

Cyberterroryzm - nowe oblicze terroryzmu

Poruszyliśmy wcześniej problem definiowania cyberterroryzmu oraz jego historii, przywołując jego minione przykłady. Podobnych działań w sferze komputerów można oczywiście wymienić znacznie więcej. Wszystkie elektroniczne konflikty udowadniają jednak, że ataki hakerów stają się coraz groźniejsze. Na podstawie omówionych zdarzeń można stwierdzić, że z biegiem czasu ataki w sieci stawały się coraz częstsze, powszechniejsze a także bardziej niebezpieczne. Wiązało się to z rozwojem Internetu, coraz szerszym do niego dostępem oraz łatwością wykorzystania. Dlatego być może w przyszłości nie będziemy mieli do czynienia z konfliktami konwencjonalnymi, gdyż przeniosą się one do sieci. Wojna taka wiele razy okazała się skuteczna. Przeprowadzenie jej jest łatwe z uwagi na fakt, że nie wymaga wielu narzędzi – jedynie komputera, dostępu do Internetu oraz trochę umiejętności.

W Polsce zjawisko cyberterroryzmu zaczęto poważnie traktować również dopiero z początkiem XXI wieku. Obecnie nasz kraj znajduje się na piątym miejscu pod względem ataków internetowych pochodzących z urządzeń mobilnych. Dane na ten temat opracowała amerykańska firma Akamai, która jest jedną z największych firm na świecie zajmujących się zarządzaniem ruchu sieciowego.

Fakt, że Polska stoi tak wysoko w zestawieniu państw, w których najczęściej dochodzi do ataków pochodzących z sieci, wynika z kilku przyczyn. Jedną z najważniejszych jest to, że nasz kraj nie nadąża z rozwojem mechanizmów i procedur bezpieczeństwa w stosunku do tempa rozwoju technologii informacyjnych. Ponadto, Polacy nie zdają sobie sprawy z zagrożeń, jakie mogą wynikać z coraz powszechniejszego informatyzowania wielu dziedzin życia. Co więcej, do niedawna zagrożenia pochodzące z cyberprzestrzeni bagatelizowano. Dopiero na początku 2012 roku zauważono, że Polska również może być zagrożona cyberterroryzmem. Zaatakowane zostały wtedy strony rządowe, czego powodem był sprzeciw w sprawie podpisania porozumienia ACTA. Protesty związane z tymi wydarzeniami pokazały, że serwisy rządowe są niezwykle słabo zabezpieczone w Internecie. Ataki hakerów dobitnie udowodniły, że realne jest zagrożenie

Lp.	Kraj	Udział procentowy ataków pochodzących z sieci
1	Włochy	28 %
2	Wielka Brytania	11 %
3	Chile	9,1 %
4	Brazylia	7,4 %
5	**Polska**	**5,3 %**
6	Malezja	4,5 %
7	Chiny	3,4 %
8	Stany Zjednoczone	3,1 %
9	Rosja	2,6 %
10	Litwa	2,3 %
11	Inne	24 %

Tabela 1. Udział procentowy ataków pochodzących z sieci w poszczególnych państwach.
źródło: http://technologie.gazeta.pl/internet/1,104530,9036923,Mobilny_Internet_na_swiecie_Polacy_na_niechlubnym.html.

destabilizacji sytuacji państwa. Profesor Stanisław Koziej po tych wydarzeniach stwierdził, że „zagrożenie cyberterroryzmem jest realne i przestępczość internetowa to najbardziej dynamicznie rozwijająca się dziedzina, jeśli chodzi o bezpieczeństwo Polski”[1].

O niebezpieczeństwie ataków terrorystycznych z wykorzystaniem Internetu, a wymierzonych w życie i zdrowie ludzi, bezpieczeństwo publiczne oraz środowisko naturalne mówi się coraz więcej i powszechniej. Powodem jest rosnąca liczba przestępstw, wojen i aktów terroru w świecie wirtualnym. Co prawda nie zdarzył się do dziś przypadek zmasowanego ataku przy użyciu Internetu, ale dodać należy też, że przed 11 września 2001 r. nie zdarzył się przypadek użycia samolotu pasażerskiego jako bomby. Na jednym ze spotkań CIA, które szczegółowo w swojej książce „Black Ice. Niewidzialna groźba cyberterroryzmu” opisuje Dan Verton, uczestnicy zgodnie twierdzili, że choć nie było jak dotąd strategicznego ataku na obiekty infrastruktury krytycznej państwa, to wciąż przybywa informacji o rosnących możliwościach prowadzonych działań wojennych przez inne państwa. Agencja ostrzegała, że taki atak mógłby dotknąć prywatne i publiczne sektory gospodarki (w instytucjach cywilnych i wojskowych) podkreślając, że wiele krajów wciąż powiększa możliwość wykorzystania wyrafinowanych technologii informatycznych przeciw systemom komputerowym[2]. Już w roku 1998 George Tenet (dyrektor CIA) powiadomił Senacki komitet do spraw rządowych, że kraje sponsorujące terroryzm – Iran, Libia, Irak – intensywnie rozwijają możliwości wrogich działań informatycznych[3].

Ataki w cyberprzestrzeni ze strony organizacji terrorystycznych zależą w dużej mierze od woli kierownictwa i najbardziej zawziętych i radykalnych bojowników świętej wojny. Jednak nie tylko organizacje terrorystyczne dokonują ataków w sieci. Są to również tzw. hakerzy. Wielu autorów odróżnia „hakerów” od tzw. „crackerów”. Dariusz Doroziński w swojej książce „Hakerzy. Technoanarchiści cyberprzestrzeni” podaje definicję obu pojęć zastrzegając, że bardzo trudne jest zdefiniowanie tych zjawisk. Zdaniem autora „haker” to człowiek, który za sprawą zdolności informatycznych potrafi włamać się do innych komputerów. Nie kradnie jednak przy tym żadnych danych, nie niszczy informacji, sprawdza tylko swoje umiejętności. Z kolei „cracker” to wg autora człowiek zajmujący się nielegalnym udostępnianiem programów, bądź włamujący się do systemów w celu niszczenia lub kradzieży danych[4]. Władze przez długi czas nie zdawały sobie sprawy z zagrożenia, jakie wynika z działalności hakerów. Włamania do takich instytucji jak Pentagon, Departament Obrony, NASA czy wszelkich korporacji przemysłowych uznawane były jako nieszkodliwe zabawy młodych ludzi. Zjawisko hackerstwa uznano za niebezpieczne dopiero w momencie, gdy zaczęto się włamywać na konta bankowe i niszczyć komputery osobiste.

Pewną klasyfikację osób dokonujących ataków w cyberprzestrzeni (ze względu na motywacje polityczne) podaje Dorothy E. Denning. Wyróżnia ona (oprócz hakerów) także „aktywistów”, „haktywistów” i „cyberterrorystów”. Aktywistami nazwani są ludzie prowadzący niedestrukcyjną działalność, w ramach której Internet służy wsparciu prowadzonej kampanii. Mogą oni używać Internetu w celu zbierania informacji, publikowania własnych tekstów, tworzenia stron WWW, porozumiewania się, koordynowania pewnych akcji czy lobbowania na rzecz pewnych rozwiązań[5]. Haktywistami nazwane są osoby wykorzystujące metody hackerskie przeciw stronom internetowym, serwerom, oprogramowaniu w celu zakłócenia normalnego funkcjonowania Internetu, nie powodując przy tym poważnych strat. Ważne w tej działalności jest zwrócenie uwagi na dany problem, a nie zniszczenie zasobów przeciwnika[6]. Zjawisko haktywizmu jest obecnie szeroko rozpowszechnione. Stanowi realne zagrożenie dla firm i instytucji, państw, korporacji międzynarodowych i różnego rodzaju organizacji. Cyberterrorysta od haktywisty różni się tym, że jego celem jest

wyrządzenie możliwie jak największych strat przeciwnikowi. Włączyć w to można również ofiary ludzkie, np. poprzez włamanie do systemu kontroli lotów i doprowadzenia do zderzenia samolotów. Z uwagi na coraz większą popularność Internetu, a także rosnącą liczbę przestępstw w świecie wirtualnym można stwierdzić, że cyberprzestrzeń przestała być bezpieczna. Zauważyć można, że w Internecie istnieje wiele postaci, które deklarują chęć zaangażowania się w tzw. świętą wojnę elektroniczną lub cyberdżihad przeciw Zachodowi. Należy zdać sobie sprawę, że metody stosowane przez hakerów, aktywistów czy haktywistów mogą zostać użyte również przez terrorystów. Ponadto już dziś wiadomo, że grupy terrorystyczne monitorują odpowiedzi (m.in. amerykańskie) na ataki hackerskie, traktując to jako materiał instruktażowy do opracowania własnych, bardziej wyrafinowanych metod ataku. Może oznaczać to, że w przyszłości większym zagrożeniem od konfliktu konwencjonalnego będzie cyberwojna.

Dotychczasowa liczba ataków cybernetycznych w porównaniu do konwencjonalnych aktów terroru jest stosunkowo niewielka. Po części ma to związek z dominacją w organizacjach terrorystycznych osób starszych, które pełnią funkcje kierownicze. Jednak coraz częściej podejrzewa się organizacje terrorystyczne o szkolenie swoich członków z zakresu telekomunikacji i informatyki, co świadczy o tym, że ta dziedzina walki wzrasta w oczach terrorystów[7]. Coraz częściej wzrasta liczba podmiotów doceniających wagę informacji oraz znaczenie cybernetyki. Wykrycie autorów wrogich ataków i wyciągnięcie wobec nich konsekwencji jest niezwykle trudne z uwagi na łatwość ukrycia tożsamości w Internecie i dużą anonimowość.

Generał Franciszek Gągor, szef Sztabu Generalnego WP, na łamach dziennika „Rzeczpospolita" wypowiedział się, że „cyberprzestrzeń – po lądzie, morzu, powietrzu i przestrzeni kosmicznej – stała się faktycznie piątym polem, na którym prowadzone są działania wojenne"[8]. Andrzej Pająk w swoim artykule „Punkt zapalny: Elektroniczna wojna w Internecie" również zwraca uwagę, że walka informacyjna stosowana przez organizacje terrorystyczne to problem jak najbardziej realny. Wspomina, że FBI zamierza umieścić zagrożenie atakiem cyberterrorystycznym na trzecim miejscu (po ataku nuklearnym i broni masowego rażenia) listy największych zagrożeń bezpieczeństwa Stanów Zjednoczonych[9]. Ataki w cyberprzestrzeni stają się coraz popularniejsze głównie dlatego, że funkcjonowanie każdego wysoko lub średnio rozwiniętego państwa jest uzależnione od prawidłowego działania w cyberprzestrzeni. W nowoczesnej walce informacyjnej narzędzia informatyczne i urządzenia, dzięki którym można oddziaływać na wojskowe i cywilne systemy komputerowe przeciwnika stały się głównymi środkami rażenia. Mogą zakłócić lub całkowicie uniemożliwić ich użytkowanie. Rosnące możliwości techniczne rodzą niebezpieczeństwo ataków cyberterrorystycznych, gdyż ich wykorzystanie umożliwia rozszerzenie działań terrorystów o zasięg ogólnoświatowy.

Rosnące zagrożenie atakiem w cyberprzestrzeni było powodem zorganizowania w 1997 roku przez Pentagon ćwiczeń, których celem było sprawdzenie, w jakim stopniu amerykańska infrastruktura podatna jest na ataki komputerowe. Ćwiczenia objęte zostały klauzulą tajności, a nadano im nazwę „Eligible Receiver". Grupa specjalistów z National Security Agency o kryptonimie „Red Team" otrzymała zadanie dokonania uderzenia cyberterrorystycznego. Jeden ze scenariuszy przygotowywanych ćwiczeń zakładał zniszczenie amerykańskiego dowództwa na Pacyfiku, które jest odpowiedzialne za działania armii na Dalekim Zachodzie. Okazało się, że grupa hakerów z Pentagonu była w stanie pozbawić prądu mieszkańców Los Angeles, Nowego Jorku, Waszyngtonu i Chicago, wstrzymać pracę rafinerii ropy naftowej, sparaliżować działania amerykańskiej armii na Pacyfiku a także przejąć kontrolę nad systemem lotów. W kolejnej fazie ćwiczeń, fazie którą przeprowadzono, hakerzy wła-

mali się do ponad 4 tysięcy serwerów i wojskowych komputerów Pentagonu. Wstrzymano wtedy wszelkie działania Red Team[10]. Żadne z działań nie zostało zauważone przez administratorów sieci oraz komórki odpowiedzialne za bezpieczeństwo informacji. Hakerzy nie zostali zlokalizowani ani zidentyfikowani. Istotny jest również fakt, że narzędzia do dokonania ataku hakerzy zdobyli ze stron internetowych poświęconych hackerstwu. Ćwiczenia te pokazały, że podatność na ataki w cyberprzestrzeni jest wysoka. Ponadto zauważono, że w przypadku cyberataku amerykańskie władze mogłyby nawet nie wiedziałyby nawet o przeprowadzonym ataku terrorystycznym.

W lutym 1998 roku to, co było tematem *Eligible Receiver*, stało się rzeczywistością - dokonano kilkuset ataków na serwery Departamentu Obrony. Zastępca sekretarza obrony John Hamre określił to jako „najlepiej zorganizowany atak w historii"[11] i przyznał, że jeszcze nigdy nie był atakowany w tak systematyczny sposób. Początkowo sądzono, że atak ten był sponsorowany przez Irak, a celem było uniemożliwienie wysłanie sprzętu i posiłków na Zatokę Perską. Okazało się jednak, że atakującymi byli 18-latek z Izraela i dwaj 16-latkowie z Kalifornii. Hakerzy, po dostaniu się do komputerów, zainstalowali program do przeszukiwania danych, dzięki czemu mogli zdobyć hasła do komputerów wojskowych i rządowych. Mieli też dostęp do serwerów z kontami osobistymi. Strony rządowe, tak jak i prywatne, są bardzo podatne na tego typu ataki. Wskutek działań hakerów bardzo szybko można narobić sporego zamieszania. Ważne jest aby pamiętać, iż jeśli nie zadbamy o bezpieczeństwo, ataki w przyszłości będą się stawały coraz groźniejsze.

W roku 2002 amerykańska Marynarka Wojenna zorganizowała grę wojenną o nazwie „Cyfrowe Pearl Harbor". Próbowano wtedy sprawdzić, czy zjawisko, jakim jest cyberterroryzm, naprawdę istnieje. W campusie University Of Wales w Newport zebrano 100 właścicieli przedsiębiorstw i dyrektorów firm, którzy przez trzy dni zastanawiali się, w jaki sposób mogą zostać zaatakowane systemy finansowe, telekomunikacja i sam Internet. Przed internetowym Pearl Harbor nie wiedziano, czy jeśli zostaną zaatakowane wyłącznie systemy bankowe, to można jednocześnie spodziewać się ataku na sieć telekomunikacyjną, sieć przesyłu prądu czy Internet. Plan „Cyfrowego Pearl Harbor" zakładał ataki internetowe połączone z konwencjonalnymi, a jednym ze scenariuszy był atak na nowojorską giełdę. We wnioskach z gry wojennej stwierdzono, że atak cyberterrorystów mógłby spowodować ogromne straty, zwrócono też uwagę na brak systemu wczesnego ostrzegania przed tego typu atakiem. Zdaniem autorów symulacji atak taki wymagałby znacznych środków finansowych, ponadto co najmniej kilku lat przygotowań i organizacji na poziomie średniej wielkości państwa[12]. Jednak organizacje terrorystyczne o brak środków finansowych nie muszą się martwić, co więcej, organizacja ich poczynań jest na wysokim poziomie. Ponadto, nie należy wykluczać, że terroryści przygotowują się do tego typu ataków. Skutkami działania w cyberprzestrzeni może być dotknięta ogromna liczba ludzi, co wynika z globalnego charakteru informatyzacji. Zgodnie z tym medialność ataku jest ogromna, czyli jeden z celów terrorystów jest osiągnięty.

W tym samym roku w raporcie dla Departamentu Obrony FBI informowało, że według potwierdzonych informacji „(...) internauci z Arabii Saudyjskiej, Indonezji i Pakistanu wielokrotnie sprawdzali systemu amerykańskich zabezpieczeń sieci telefonicznych, systemu alarmowego 911, sieci energetycznej, wodociągów, gazociągów i elektrowni atomowej"[13]. Ponadto, eksperci ostrzegali także o możliwości łamania przez cyberterrorystów (...) „zabezpieczeń cyfrowych rozdzielających systemów kontroli oraz systemów kontroli i poboru danych SCADA"[14]. Systemy te odpowiedzialne są za sprawne działanie zwrotnic kolejowych, przepływ wody, ropy czy gazu. Niektóre z nich są bardziej skomplikowane i sterują obiektami telekomunikacyjnymi czy energetycznymi. Włamanie się do któregoś z tych sys-

temów mogłoby przynieść katastrofalne skutki w każdej dziedzinie życia.

Istnieje wiele powodów, które mogą skłonić terrorystów do ataków w cyberprzestrzeni, dlatego coraz powszechniej mówi się o tym, iż w przyszłości wojna będzie toczyła się właśnie w świecie wirtualnym. Powodem może być po pierwsze to, że koszty przeprowadzenia cyberataku są nieporównywalnie niższe niż w przypadku klasycznych działań terrorystycznych. Przygotowanie ataku, nawet w trudnym do oszacowania rozmiarze i zasięgu, nie wymaga dużych nakładów finansowych ani specjalistycznej wiedzy. Do ataku cyberterrorystycznego wystarczy zwykły komputer, dostęp do Internetu i trochę umiejętności. Nie ma potrzeby kupowania broni i materiałów wybuchowych. Wykorzystywane są natomiast wirusy, robaki i konie trojańskie, które przesyłane są do celu ataku. Niskie koszty materialne mogą być zatem doskonałym powodem przeprowadzania ataków w sieci. Bardzo niebezpieczne jest to, że w przypadku cyberataku zakłócone zostaje postrzeganie zagrożenia. Nie wiadomo, czy zagrożenie jest realne, czy wirtualne. Niezwykle trudne jest również wykrycie ataku - nie znamy intencji atakującego, jego zdolności, umiejętności. Nie wiemy też, jaki jest cel ataku, ani w jaki sposób zostanie on dokonany. Ważnym powodem wykorzystania Internetu przez terrorystów jest również relatywna anonimowość w sieci. Terroryści mogą używać pseudonimów bądź wykorzystywać opcję anonimowego użytkownika. Sprawi to, iż zidentyfikowanie nazwisk będzie niemożliwe. Skutkiem może być zatem możliwość manipulowania informacją, utrudnianie państwom odparcie ataku i budowanie koalicji. Ciężko jest ustalić, kto rzeczywiście inspirował konkretny akt cyberterroryzmu, więc cyberterroryści mogą prowadzić działania z pewnością, że ich lokalizacja ani zamiary nie zostaną wykryte. Bardzo ważne jest też środowisko działania i jego cechy. Z uwagi na fakt, iż Internet umożliwia nieograniczoną komunikację, umożliwia on także planowanie i koordynowanie akcji cyberterrorystycznych z różnych miejsc świata, bez ograniczeń miejscowych ani czasowych. Także dostępność narzędzi potrzebnych do przeprowadzenia ataku nie stanowi żadnego problemu, gdyż komputer podłączony do sieci jest przedmiotem dostępnym dla każdego. Cyberterroryzm może być stosowany również dlatego, że wszelkie działania odbywają się ponad granicami państw. Nie wiadomo, skąd pochodzi atak ani kto atakuje. Ogólnoświatowa sieć połączeń sprawia, że ataki można przeprowadzić z niemal każdego miejsca na świecie. Oznacza to, że uderzyć można również w każdy obiekt na całym globie.

	Tamilskie Tygrysy (LITE - The Liberation Tiggers of Tamil Eelam)
Sprawca	Grupa ludzi / osoba
Lokalizacja	Sri Lanka / cały świat
Metody	Groźby / przemoc / rekrutacja / szkolenie / strategie
Narzędzia	Porwania / nękanie / prześladowanie / propagowanie / szkolenie
Cele	Przedstawiciele władz / rekruci
Afiliacja	Faktyczna / deklarowana
Motywy działania	Społeczne / polityczne zmiany

Tabela 3: Atrybuty terroryzmu na przykładzie organizacji Tamilskie Tygrysy wzmocnione o metody techniki komputerowej
Źródło: S. Gordon Cyberterrorism?, Symantec, 2003, s.5, [z:] http://www.security.iia.net.au/downloads/cyberterrorism/pdf

	Tamilskie Tygrysy (LITE - The Liberation Tiggers of Tamil Eelam)
Sprawca	Grupa ludzi
Lokalizacja	Sri Lanka
Metody	Groźby / przemoc
Narzędzia	Porwania / nękania / prześladowanie
Cele	Przedstawiciele władz / rekruci
Afiliacja	Faktyczna / deklarowana
Motywy działania	Społeczne / polityczne zmiany

Tabela 2: Atrybuty terroryzmu na przykładzie organizacji Tamilskie Tygrysy
Źródło: S. Gordon Cyberterrorism?, Symantec, 2003, s.5, [z:] http://www.security.iia.net.au/downloads/cyberterrorism/pdf.

Dowód na to, iż terroryści coraz częściej zauważają Internet i technologie informacyjną jako cenny element do wykorzystania w działaniach przedstawia Dorota Opalach–Nusbaum. Wykorzystując elementy składowe terroryzmu (sprawców, lokalizację, metody/model działania, narzędzia, cele, afiliację i motywy) porównuje atrybuty terroryzmu klasycznego z atrybutami terroryzmu wzmocnionego o metody techniki komputerowej na przykładzie organizacji Tamilskie Tygrysy.

Zestawienie to ukazuje, że wzmocnienie terroryzmu o nowe technologie przyniosło zmiany w większości z jego elementów składowych. Połączone komputery oraz powiązania informatyczne sprawiły, że dostęp do informacji stał się powszechny. Komputer może stać się zarówno celem, jak i narzędziem, a akcje przeprowadzane w świecie wirtualnym mogą przynieść konsekwencje w świecie rzeczywistym.

Coraz częściej atak za pośrednictwem sieci umożliwia eskalację konfliktów i ich ekspansję poza tradycyjne pola walki. Przeniesione są na teren wroga, a ponadto są znacznie tańsze od tradycyjnych narzędzi militarnych. Ataki cyberterrorystyczne mogą stać się zatem powszechnym sposobem rozwiązywania konfliktów.

Cyberterroryści mogą również dostosować swoje działania tak, aby zmaksymalizować pozytywny dla siebie wynik. Ponadto, cyberterroryzm nie wymaga treningu fizycznego ani dużego zabezpieczenia logistycznego. Nie wymaga ponadto podróżowania. Ataki w cyberprzestrzeni nie stwarzają ryzyka poniesienia śmierci lub obrażeń fizycznych, ograniczają więc konieczność narażania życia – zamachy w sieci nie wymagają bowiem ataków samobójczych[15]. Aby przeprowadzić taki atak, nie potrzeba posiadać praktycznie żadnych umiejętności – można wynająć crackerów, którzy łamiąc zabezpieczenia (często nie zdając sobie sprawy ze skutków swojego działania) za pieniądze przeprowadzą atak terrorystyczny. Terroryści zdają sobie również sprawę, iż walka z cyberterroryzmem wymaga o wiele większej koordynacji działań niż w przypadku klasycznego ataku. Państwa ponadto dysponują bardzo małymi możliwościami zastosowania sankcji – nie wiadomo, w jaki sposób odpowiedzieć na taki atak. W konsekwencji można stwierdzić, że cyberterrorystą może zostać każdy, dlatego kwestia cyberterroryzmu może stanowić kluczowy problem bezpieczeństwa międzynarodowego w XXI wieku. Ryzyko cyberterroryzmu będzie wzrastać w społeczeństwie wraz ze wzrostem znaczenia Internetu w naszym życiu. Cyberwojnę już dziś można prowadzić niezależnie od konfliktu na lądzie i morzu, w dodatku mniejszym nakładem kosztów. Systemy informacji w podstawowych dziedzinach gospodarki – bankowości, finansach, telekomunikacji, handlu – już dziś stały się nadrzędne, dlatego dostęp do nich lub ich blokada mogłyby skutecznie sparaliżować działanie instytucji i państwa. Wiele racji miał zatem sekretarz generalny NATO Jaap de Hoop Scheffer mówiąc, że „cyberataki nie wymagają użycia ani jednego żołnierza, czy naruszenia granic – mogą jednak sparaliżować działanie państwa”[16].

Przypisy

1 http://technologie.gazeta.pl/internet/1,104530,9036923,Mobilny_Internet_na_swiecie___Polacy_na_niechlubnym.html, z dnia 15.06.2012.
2 Tamże.
3 L.M. Terrence, Cyberterrorism... dz. cyt.
4 D. Doroziński, Hakerzy. Techno anarchiści cyberprzestrzeni, Helion 2001.
5 M. F. Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Fundacja Studiów Międzynarodowych, Warszawa 2003, s 60.
6 Tamże.
7 A. Chorobiński, Walka informacyjna, jako fundamentalny składnik działalności terrorystycznej w przyszłości,[z:] http://www.e-debiuty.byd.pl/file/rznnonhy6wpijz7/PDF/chorobinski.pdf, z dnia 15.06.2012, s. 2.
8 E. Żemła, Żołnierze na cyberwojnę, [z:] http://www.rp.pl/artykul/339842.html, z dnia 25.07.2009.
9 A. Pająk, Punkt zapalny: elektroniczna wojna w Internecie, [z:] http://chip.pl/artykuly/trendy/2009/11/punkt-zapalny-elektoniczna-wojna-w-internecie, z dnia 13.11.2009.
10 L.M. Terrence, Cyberterrorism... dz. cyt.
11 Tamże.
12 M.F. Gawrycki, Cyberterroryzm..., dz. cyt., s. 86.
13 Tamże, s. 137.
14 Tamże.
15 I. Bunsch, J. Świątkowska, Cyberterroryzm..., dz. cyt., s. 2.
16 Nowe NATO rodzi się w Krakowie, Gazeta Wyborcza, [z:] http://wyborcza.pl/1,76842,6297288,Nowe_NATO_rodzi_sie_w_Krakowie.html, z dnia 19.02.2009.

NATALIA NOGA

Podmioty i motywy działań w cyberprzestrzeni

Bez wątpienia, dla lepszego zrozumienia wielu złożonych zagadnień pomocne okazać mogą się podsumowania, zestawienia oraz klasyfikacje. Jedną z klasyfikacji osób, które są podmiotami działań w cyberprzestrzeni, zastosował Przemysław Maj. Twierdzi on, iż „(...) wśród podmiotów działań wyróżnić można grupy zorganizowane i cyberterrorystów indywidualnych”[1]. Do grup zorganizowanych zaliczyć można zarówno klasyczne organizacje terrorystyczne, jak i organizacje cyberterrorystyczne. Klasyczne organizacje terrorystyczne, takie jak Hezbollah, Al-Kaida czy Tamilskie Tygrysy - oprócz środków konwencjonalnych – w swych działaniach wykorzystują również cyberprzestrzeń, natomiast organizacje cyberterrorystyczne działają wyłącznie w cyberprzestrzeni, a składają się z hackerów komputerowych. W przypadku cyberterrorystów indywidualnych mówimy już o profesjonalnych hackerach, którzy posiadają wysokie kwalifikacje i doskonale znają się na dziedzinie, w której pracują.

Obecnie istnieje około 1000 osób na świecie, które można określić mianem profesjonalnych hackerów. Osoby te za odpowiednią opłatą mogą zrobić wszystko, co jest zlecone przez organizacje terrorystyczne (również wykonywać zadania o charakterze politycznym). Znaczna część z nich rekrutowana jest w kręgach studenckich[2]. W swojej książce „Black Ice. Niewidzialna groźba cyberterroryzmu” Dan Verton przytoczył słowa Richarda Clarke, który również wspomina o aktorach sceny cyberterrorystycznej. Twierdzi on, że „na świecie jest wielu różnych ludzi, którzy mogą prowadzić własne cyberwojny (...). W niektórych krajach są tworzone specjalne cyberwojenne jednostki. Także niektóre organizacje kryminalne nie stronią od cyberzbrodni. Cyberbroni poszukują także niektóre, znane nam grupy terrorystyczne. Ale nie muszę długo rozmyślać, aby przewidzieć, kto zamierza zostać następnym atakującym”[3].

Fot. Jarrod Drake, commons.wikimedia.org

Aktorów sceny cyberterrorystycznej znakomicie obrazuje schemat przedstawiony przez Thomasa R. Mockatis’a (T. R. Mockatis, The New Terrorism: Myths and Realists, Stanford University Press 2008). Autor wśród aktorów sceny cyberterrorystycznej wymienia kryminalne organizacje, które pełnią rolę ubezpieczającą działania cyberterrorystyczne oraz państwa posługujące się terrorem i go wspomagające, wśród których ogromną rolę pełnią cyberterrorystyczne grupy. Większość ludzi w ogóle nie zdaje sobie sprawy z faktu, że wszechobecna sieć stwarza dogodne pole na cyberataki. Perspektywa ta, w ostatnim czasie, jest coraz bardziej atrakcyjna nie tylko dla hakerów i zorganizowanych grup przestępczych, ale i dla terrorystów. Zaczęli oni bowiem wchodzić w nową erę szerzenia strachu wśród użytkowników Internetu.

Osoby, które mogą dokonać aktów cyberterrorystycznych stanowią grupę działaczy różnych organizacji typową dla XXI wieku. W opinii specjalistów spośród nich można wyróżnić fanatyków religijnych, ortodoksyjnych działaczy New Age, separatystów i rewolucjonistów etniczno–narodowościowych oraz

innego rodzaju ekstremistów[4]. Mając na uwadze fanatyków religijnych (szczególnie islamskich) w wielu przypadkach zauważa się, iż metody cyberterrorystyczne nie są przez nich stosowane. Przywódcy często nie znają się lub nie rozumieją nowoczesnych technologii, a ponadto brak im przygotowanej technologicznie i zaangażowanej ideowo kadry. Inaczej jest w przypadku ortodoksyjnych działaczy New Age, wśród których można wyróżnić organizacje działające na rzecz praw zwierząt lub antyglobalistów. Posiadają oni w swych szeregach członków organizacji bardzo dobrze przygotowanych do roli cyberterrorystów, jednak ze względu na poglądy nie stosują cyberterroryzmu przeciw życiu ludzkiemu i wręcz wykluczają ofiary w ludziach. Bardzo groźną grupą (o różnym przygotowaniu specjalistycznym) są separatyści i rewolucjoniści etniczno–narodowościowi, którzy nie posiadają żadnych obiekcji w stosunku do obiektów ataku. W miarę postępu cywilizacyjnego na świecie mogą pojawić się również innego typu ekstremiści. Grupa, spośród wcześniej wymienionych, może być najgroźniejsza. Aż do dnia, kiedy zaatakuje, stanowić może nieokreślone zagrożenie, gdyż wśród swoich członków posiada ludzi obytych z techniką komputerową. Nową, bardzo niebezpieczną zmianę w cyberterroryzmie (która przyspieszyć może nadejście tego groźnego zjawiska) wyznacza pojawienie się tzw. „najemników". Jest to ostatnio coraz częściej pojawiająca się tendencja wykorzystywania znawców zaawansowanych technologii w przestępczych działaniach komputerowych. Na ten temat mówiono na konferencji zastosowań kryptograficznych ENIGMA 2005 gdzie przedstawiono, że badania aktywności cyberprzestępców coraz częściej wskazują na pojawianie się w sieci hakerów do wynajęcia[5].

Organizacje terrorystyczne, które posługują się nowymi technikami można (zdaniem A. Rathmella) podzielić na trzy kategorie:

– kategoria I, która obejmuje nowe techniki używane przez terrorystów do prowadzenia tradycyjnej działalności. Internet wykorzystuje się tutaj do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacyjnych.
– kategoria II, w której wykorzystywane są stare techniki do nowej działalności. Używana jest tutaj siła fizyczna, która ma na celu zniszczenie systemu informacyjnego.
– kategoria III, w której używa się nowe techniki do nowych działań – jest to atak w cyberprzestrzeni na system informacyjny[6].

Należy również pamiętać, że nie da się z działalności w sieci wykluczyć wszystkich agresorów. Richard Clarke w wywiadzie dla autora Dana Vertona twierdzi również, iż „załóżmy dla przykładu, że następny atak jest planowany przez Al–Kaidę. Nawet gdyby udało się dobrać im do skóry i wyeliminować całkowicie albo zmniejszyć do pozbawionej znaczenia grupki, nie wyeliminuje to całkowicie zagrożenia w cyberprzestrzeni. Ktoś inny wyszuka słabe punkty naszych systemów i wykorzysta je do ataków. Nie ma co zgadywać, kto będzie następnym atakującym, nawet gdyby w końcu udało się go wyśledzić i zrobić z nim, co należy. Trzeba zająć się słabościami, które umożliwiają ataki. Dopóki sobie z nimi nie poradzimy, dopóty będziemy narażeni na ryzyko ataków"[7].

Działalność cyberterrorystów w sieci jest bardzo poważnym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, zarówno pod względem finansowym, jak i bezpieczeństwa, jest trudna do oszacowania. Amerykański wywiad ocenia, że obecnie techniczne możliwości ataku na infrastruktury informatyczne mają Rosja i Chiny. Ponadto, zamiar zastosowania cyberataków przeciw Stanom Zjednoczonym wyraziły organizacje terrorystyczne takie jak Al-Kaida, Hamas i Hezbollah[8]. Do grupy wymienionych państw, tworząc oficjalnie specjalną jednostkę wojskową ds. wojny

cybernetycznej złożonej z ok.100 hakerów dołączyła także Korea Północna. Większość z nich ma na celu sparaliżowanie ważnych służb publicznych, kradzież wrażliwych informacji, usunięcie bądź zniekształcenie stron internetowych lub wprowadzenie wirusów.

Wszystkie organizacje terrorystyczne, które korzystają z sieci, charakteryzują się pewnymi cechami. Są to przede wszystkim:

- budowanie i zmienianie komunikacji i koordynacji stosownie do zadań
- nieformalne powiązania o różnym stopniu intensywności (zależnie od potrzeb)
- brak biurokratycznego zarządzania, lecz więzy wewnętrzne i zewnętrzne umożliwiające podzielanie wspólnych norm i wartości oraz wzajemne zaufanie
- uzupełnianie wewnętrznych sieci przez łączność z osobami nie związanymi z organizacją (możliwość wychodzenia poza granice państw)[9].

Problem przeanalizował NCS (National Communications System), stwierdzając w 2000 r., iż „globalna zależność od połączonych ze sobą komputerów i słabości tego systemu sprzyja wzrostowi zagrożenia cyberterroryzmem. Ponadto kierunek ewolucji grup terrorystycznych czyni je szczególnie dostosowanymi do wykorzystania Internetu w realizacji swych celów. Wiele grup terrorystycznych przeszło ewolucję od struktur silnie hierarchicznych z określonymi przywódcami na czele do stowarzyszeń o dość luźnych powiązanych między częściowo niezależnymi komórkami, bez wyraźnej hierarchii – jak Hamas i organizacja bin Ladena. Dzięki połączeniom internetowym luźno powiązane grupy bez wyraźnie określonych przywódców mogą pozostawać w stałym kontakcie i wymieniać informacje”[10].

Zauważyć można również, że coraz częściej organizacje ekstremistyczne (głównie islamskie) w celu wsparcia swych działań i przeprowadzania ofensywnych ataków budują sieci hackerskie - chcą w ten sposób między innymi atakować najważniejsze komputery rządowe. Już w 1998 roku ustalono, że członek jednej z indyjskich grup separatystycznych usiłował od grupy hackerskiej kupić oprogramowanie wojskowe. Grupa hackerska – Harkat–ul- Ansar, będąca na liście kilkudziesięciu organizacji terrorystycznych stworzonej przez Departament Obrony USA - twierdziła wtedy, że oprogramowanie to ukradła z sieci Departamentu Obrony[11]. Również przedstawiciele FBI w 2000 roku potwierdzili, że cyberataki dokonywane przez pro palestyńskie grupy hackerskie zmieniają swój charakter i ich działania stają się bardziej wyrafinowane. Niektórzy hakerzy zaczęli się informować o słabych punkach poszczególnych systemów, a nawet wyrazili chęć atakowania witryn, których niszczenie mogłoby przyczynić się do jak najszerszego upowszechniania informacji o ich celach – są to przede wszystkim serwisy internetowe handlu elektronicznego na terenie Stanów Zjednoczonych i Izraela[12].

Obecnie można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem. Pierwszym z nich jest tzw. simple–unstructured. Polega na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych poprzez wykorzystanie narzędzi internetowych skonstruowanych przez inną osobę. Zgodnie z tym organizacje terrorystyczne nie mają zdolności analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli czy uczenia się nowych metod atakowania w cyberprzestrzeni. Drugim poziomem zagrożenia jest tzw. advanced–structured. W poziomie tym cyberterroryści dokonują bardziej skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Posiadają możliwość tworzenia lub modyfikacji własnych narzędzi, które służą do atakowania w cyberprzestrzeni, mają zdolność analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania. Ostatnim, najpoważniejszym poziomem zagrożenia jest tzw. complex–coordinated. Cyberterroryści dokonują tu skoordynowanych ataków mających na celu totalną destrukcję zintegrowanego systemu

obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni a także analizę celów będących przedmiotem ataku. Mogą dowodzić, kontrolować a także samodoskonalić się[13].

Dzięki aktywnemu wykorzystywaniu komputerowych technologii szyfrowych i kawiarni internetowych grupy terrorystyczne coraz częściej potrafią utrzymać wysokie tempo operacji. Zauważyć można tendencję przechodzenia od tradycyjnej formy terroryzmu sponsorowanego przez rządy do modelu, w którym Internet i inne nowoczesne technologie są wykorzystywane m.in. do propagandy, zbierania funduszy i rekrutacji nowych członków. Te i inne sposoby wykorzystywania Internetu przez terrorystów zostaną opisane w dalszych częściach cyklu.

Motywy działań w cyberprzestrzeni

Internet, z uwagi na globalny zasięg, umożliwia dotarcie informacji do szerokich rzesz odbiorców na całym świecie. Stwarza możliwość rozpowszechniania informacji zarówno tych prawdziwych, jak i fałszywych (lub w określony sposób spreparowanych). Za jego pomocą można również promować własne ideologie na skalę globalną. Z tego powodu organizacje terrorystyczne w dużej mierze przywiązują wagę do prowadzenia za pomocą Internetu kampanii propagandowych. Może być wykorzystywany do wzniecania niepokojów, szerzenia nienawiści, jak i do prowadzenia wojny psychologicznej. Motywy przewodnie propagandy terrorystów to deprecjonowanie przeciwnika i dyskredytacja jego sił oraz gloryfikacja wysiłku własnego. Ważne jest też budowanie wśród islamistów przeświadczenia o tym, iż ich państwo jest miejscem wojny między chrześcijaństwem a islamem oraz nakłanianie rządów do wycofania się wojsk z Bliskiego Wschodu. Działania prowadzone są przez Al–Kaidę, afgańskich i tamilskich Talibów, separatystów kaszmirskich i terrorystyczne ugrupowania palestyńskie[14].

Propagandowe możliwości Internetu zauważono już w 2004 roku, kiedy to Al–Kaida opublikowała w sieci odezwę wzywającą naród iracki do walki z okupantem. Internet dostarczał informacji o przebiegu wojny i przeprowadzanych atakach terrorystycznych, jednocześnie krzewiąc ideę „świętej wojny". Ponadto, tym samym sposobem dostarczano instruktaży konstruowania bomb i dokonywania zamachów z ich użyciem, a także rekrutowano członków grup terrorystycznych[15]. Przez Al–Kaidę wykorzystywane są w działalności propagandowej głównie strony internetowe i nagrania audio i wideo publikowane w arabskich telewizjach satelitarnych. Coraz częściej można też zauważyć wzrost liczby tłumaczonych na wiele języków komunikatów audiowizualnych autorstwa tej organizacji terrorystycznej. Poświęcone są one różnej tematyce i dystrybuowane według skomplikowanej struktury. Działalność propagandowa tej organizacji stale się zwiększa. Od 2004 roku organizacja ta rozpoczęła nawet wydawanie magazynu internetowego pt. „Obóz treningowy Al Battara", którego nazwa pochodzi od przezwiska byłego osobistego ochroniarza bin Ladena – szejka Yousefa al–Ayyiri. Miał on na celu przygotowanie (pod względem ideologicznym i mentalnym) przyszłych bojowników „Świętej Wojny"[16].

Działalność propagandowa w Internecie prowadzona jest za pośrednictwem stron internetowych umiejscowionych na całym świecie. Al-Kaida i Talibowie na bieżąco wykorzystują strony takie jak Al Neda, Islamie Studies and Research (ISR) oraz Jihad Online. Wzmożone korzystanie z serwerów pakistańskich Jehad oraz Alemarh zauważono natomiast w okresie poprzedzającym wkroczenie wojsk koalicji do Republiki Afganistanu w ramach operacji „Enduring Freedom". Umieszczano wówczas na stronach informacje o bieżących działaniach Al–Kaidy i poglądach Osamy bin Ladena, przedstawiano osiągnięcia innych radykalnych ruchów islamskich i wyrazy poparcia dla reżimu Talibów w Afganistanie. Ponadto, wychwalano

zamachy samobójcze ich członków. Miały być one aktami godnymi naśladowania. Wszystko to miało na celu stworzenie u odbiorców wrażenia istnienia proislamskiego ruchu, który walczy przeciw ekspansji Zachodu w państwach muzułmańskich[17].

Kolejna z organizacji terrorystycznych, Hezbollah, ma kilka głównych stron informacyjnych. Jedna służy jako oficjalna strona organizacji, inna jest źródłem wszelkiego rodzaju informacji, kolejna opisuje ataki na izraelskie cele. Niektóre, tworzone w języku angielskim, adresowane są do społeczeństw z całego świata, inne tworzone wyłącznie w języku arabskim, adresowane do członków znających ten język. Celem tworzenia tych stron jest umożliwienie komunikowania się między sympatykami i członkami danej grupy[18].

Niektóre organizacje palestyńskie, a także Al–Kaida, prowadzą również kampanie propagandowe mające na celu dezinformowanie społeczeństw przeciwników. Najbardziej spektakularną akcją było umieszczenie na serwisie kavkaz.org przez Czeczenów informacji o zatonięciu rosyjskiego strategicznego okrętu podwodnego. Sugerowano wtedy udział jednego z członków załogi – muzułmanina, który rzekomo współpracował z Czeczenami i przemycił ładunek wybuchowy na pokład okrętu celem zatopienia go. Innym przykładem kampanii dezinformacyjnej było zamieszczenie w roku 2002 na wspierającym bin Ladena serwerze Al Neda informacji o pożarach lasów w Stanach Zjednoczonych. Spłonęło wtedy ok. 1,84 mln akrów lasów na terytorium 19 stanów, a sugerowano, że był to wynik zamachu terrorystycznego[19].

Oprócz wyżej wymienionych działań propagandowych, doskonale są znane również groźby terrorystów, a także pokazywane przez nich akty egzekucji. Hezbollah posiada nawet własnych kamerzystów. Filmują oni izraelskie ofiary, by w końcu wysłać je do izraelskiej telewizji.

Internet, oprócz propagandy, wykorzystywany jest przez terrorystów również do celów komunikacyjnych. W przypadkach takich wykorzystywane są dosyć często takie innowacje jak telekonferencje czy czaty internetowe. Są one znakomitym środkiem komunikacji – pozwalają na wymianę informacji bez względu na odległość. Jak twierdzi Brunon Hołyst, posługiwanie się Internetem „przyspiesza mobilizację członków grup terrorystycznych, umożliwia dialog między nimi i zwiększa elastyczność organizacji przez możliwość zmiany taktyki w razie potrzeby. Członkowie grup terrorystycznych mogą dzielić się na podgrupy, ustalać miejsca spotkania, przeprowadzać operacje terrorystyczne, po czym szybko przerywać swoje powiązania i rozpraszać się”[20]. Terroryści w komunikacji posługują się również metodami ukrywania tajnych danych w plikach graficznych lub innych informacjach.

W roku 1990, w wyniku operacji antyterrorystycznych wymierzonych w bazy GIA[21], odkryto komputery i dyskietki, które zawierały szczegółowe instrukcje konstruowania bomb. Dziś już wiadomo, że organizacja ta stosuje komputery do przechowywania i procesowania rozkazów, a także do przesyłania informacji do członków organizacji z wielu państw europejskich[22].

Internetu do przekazywania komunikatów operacyjnych i informacji używa również wojownicza organizacja islamska Hamas. Aktywiści tej grupy w USA używają pokojów czatowych do planowania operacji i działań, a za pomocą poczty elektronicznej w Gazie, na Zachodnim Brzegu Jordanu i w Libanie koordynują swe zadania[23]. Organizacje antyterrorystyczne nie są w stanie kontrolować całego przepływu danych w Internecie, dlatego członkowie Hamasu doskonale wiedzą, że Internet służyć może do stosunkowo bezpiecznego przesyłania informacji.

Internet daje ogromne możliwości w komunikowaniu się i koordynowaniu akcji. Znosi wszelkie ograniczenia, jakie wiążą się z tradycyjnymi środkami przekazu, dlatego daje nieograniczone możliwości terrorystom w propagowaniu swoich idei. Ponadto, służyć może ugrupowaniom terrorystycznym do werbowania i szkolenia nowych członków. Mogą świad-

czyć o tym raporty holenderskiego wywiadu, z których wynika, że część członków skazanej w 2006 roku grupy Hofstad zwerbowano właśnie w sieci. Oczywiście utrudnia to pracę służbom specjalnym, gdyż „(...) wirtualni dżihadyści nie chodzą do radykalnych meczetów, nie spotykają się ze znanymi fanatykami i nie jeżdżą na szkolenia do Pakistanu i Afganistanu”[24]. Nowoczesne technologie do wsparcia swych działań terrorystycznych – również w ramach szkoleń i rekrutacji – stosuje Al-Kaida. Procesy te przeprowadza się szczególnie starannie, podobnie do naboru pracowników wywiadu oraz członków jednostek do zadań specjalnych. Istotne znaczenia mają sprawność intelektualna oraz często kondycja fizyczna.

Niektóre z organizacji terrorystycznych wykorzystują Internet do lepszej organizacji i koordynacji rozproszonych działań, co spowodowane jest chęcią poprawy skuteczności i elastyczności działań. Terroryści, wprzęgając siłę informacji technicznej do tworzenia nowych doktryn operacyjnych i form organizacyjnych, odchodzą od hierarchicznej biurokracji, stają się zdecentralizowane i często zmieniają sieć ugrupowań złączonych wspólnymi celami[25]. Powstanie takich sieciowych układów jest częścią szerszego ruchu - poza sponsorowanymi przez państwo, formalnymi grupami, mogą iść w kierunku prywatnie finansowanych i luźnych sieci osób, które cieszą się strategiczną niezależnością, jednocześnie posiadając strategiczne kierownictwo[26]. W przekazywaniu operacyjnych informacji Internetem posługuje się również bojowa grupa islamska Hamas. Zdaje sobie ona sprawę, że wywiad kontr terrorystyczny nie jest w stanie dokładnie monitorować wszystkich treści przepływających przez Internet, dlatego często używa tego środka komunikacji do przekazywania informacji. Podczas planowania i realizacji operacji wykorzystuje ona kanały dyskusyjne, tzw. chatrooms. Posługuje się także pocztą elektroniczną w koordynowaniu akcji w Libanie, Gazie, na Zachodnim Brzegu Jordanu[27]. Posługiwanie się Internetem może także przyspieszyć mobilizację członków grup terrorystycznych – za jego pomocą można ustalać miejsca spotkań, przeprowadzać akcje terrorystyczne, dzielić się na podgrupy aby w końcu rozpraszać się i przerwać swoje działania.

Nie można pominąć również wykorzystywania Internetu przez organizacje terrorystyczne do zdobywania środków finansowych - tą drogą mogą oni pozyskiwać ogromne sumy pieniędzy. Według informacji FBI już w latach 90-tych za pośrednictwem komputerów dokonano kradzieży na sumę około 3 – 7.5 mld dolarów. Znany jest przypadek podjęcia dużych kwot z kont wahabitów w Arabii Saudyjskiej. Terroryści na ich bazie zamierzali utworzyć własny bank. Organizacje te mogą również czerpać olbrzymie środki ze sfingowanych przelewów elektronicznych, wymuszeń w bankach czy skradzionych kart kredytowych[28]. Bardzo ważne jest tu znaczenie zagadnienia finansowania terroryzmu, a w szczególności zdobywania środków w ramach cyberterroryzmu. Jest to podstawowy warunek działalności organizacji terrorystycznych, który sprzyja realizacji planów terrorystów.

Al–Kaida ma doświadczenie w ukrywaniu swych źródeł finansowania za pomocą fikcyjnych firm fasadowych. Kiedyś firmy te korzystały z prostych technologii, ale od 2002 r. służby celne USA zauważyły rozwój firm fasadowych wysokich technologii na terenie kraju. Firmy te miały na celu infiltrację wrażliwych na ataki obiektów wojskowych, nuklearnych, a także instytucji finansowych, które służyć mogły do finansowania operacji terrorystycznych lub prania brudnych pieniędzy[29].

Wysiłki Al–Kaidy i jej komputerowy program badawczy początkowo rozwijał się powoli. Skupiał się głównie na zagadnieniach sterowania, wydawania poleceń oraz narzędziach komunikacyjnych służących do ukrywania planów operacji. Ostatnio jednak wysiłki organizacji zaczęły się skupiać na używaniu zaawansowanych technologii informatycznych do poznawania słabych punktów celów – np. inżynierskich niedociągnięć w konstrukcji mostów, elektrowni, różnego ro-

dzaju budynków[30]. Widać zatem, iż kolejnym powodem stosowania Internetu przez terrorystów jest możliwość gromadzenia za jego pomocą potrzebnych informacji. Niezwykły rozwój i ewolucja technologii informatycznych może wskazywać, że w przyszłości możemy mieć do czynienia z bardziej bezpośrednim wykorzystaniem Internetu jako broni ofensywnej. Komórki Al–Kaidy coraz częściej używają w swoich działaniach olbrzymią ilość baz danych. Zawierają one masę dokładnych i szczegółowych informacji na temat potencjalnych celów w USA. Internet służyć może do gromadzenia danych wywiadowczych o przyszłych celach (zwłaszcza tych krytycznych dla gospodarki), natomiast nowoczesne oprogramowanie umożliwia analizowanie materiału i poszukiwanie słabych punktów konstrukcji. Przewidywane mogą być również reakcje atakowanych systemów. Na ten temat wypowiedział się również Richard Clarke – były przewodniczący Prezydenckiej Rady ds. Ochrony Infrastruktury Krytycznej, który twierdzi, iż „Al-Kaida posługuje się Internetem przynajmniej do wstępnego rozpoznania elementów amerykańskiej infrastruktury. Jeżeli razem złożycie wszystkie jawne informacje, możecie czasem otrzymać coś, co powinno być tajne”[31].

Poprzez włamanie się na strony internetowe oraz dojście do strzeżonych danych, organizacje terrorystyczne mogłyby również uzyskać informacje na temat danych dotyczących broni nuklearnej i chemicznej lub danych o lokalizacji wojsk. Bezpieczeństwo informacyjne jest zatem nierozerwalnie związane z bezpieczeństwem fizycznym i materialnym państwa.

Terroryści coraz częściej używają technologii informacyjno–komunikacyjnych również w nowoczesnych technologiach, między innymi do detonowania miniaturowych ładunków wybuchowych. Przykładem może być próba zamachu Al–Kaidy na księcia saudyjskiego Mohammeda bin Nayefa w 2009 roku. Eksplodowała wtedy mini–bomba ukryta w odbycie terrorysty Abdullaha Hassana al Asiriego. Uruchomił ją sam książę, kiedy połączył się z podanym przez terrorystę numerem telefonu innego „skruszonego terrorysty”. Komórka podłączona była do specjalnego urządzenia, które wywołało eksplozję w ciele zamachowca. Zdarzenie to zdaniem ekspertów potwierdza otwarcie nowego rozdziału miniaturyzacji we współczesnym terroryzmie z wykorzystaniem bomb –czopków, trudnych do wykrycia w praktyce[32].

Przypisy

1 P. Maj, Cyberterroryzm w stosunkach międzynarodowych, [z:] http://www.politologia.pl/fck_pliki/File/consensus/consensus_1.pdf z dnia 15.06.2012.
2 Tamże.
3 D. Verton, Black ice..., dz. cyt., s. 220.
4 L. Wolaniuk, Cyberterroryzm jako element cywilizacji informacyjnej, [w:] M. Żuber, Katastrofy naturalne i cywilizacje. Zagrożenia i reagowanie kryzysowe, Wrocław 2006, s. 160-161.
5 Tamże.
6 R. Białoskórski, Cyberzagrożenia ... dz. cyt., s. 59.
7 D. Verton, Black ice..., dz. cyt., s. 220.
8 Biuro Bezpieczeństwa Narodowego, Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji, Warszawa, 2009, [z:] http://www.bbn.gov.pl/portal/pl/501/1779/Terroryzm_cybernetyczny__zagrozenia_dla_bezpieczenstwa_narodowego_i_dzialania_am.html, z dnia 15.06.2012, s. 11.
9 B. Hołyst, Cyberterroryzm... dz. cyt., s. 2.
10 D. Verton, Black ice..., dz. cyt., s. 194.
11 Tamże, s. 67.
12 Tamże, s. 159.
13 R. Białoskórski, Cyberzagrożenia..., dz. cyt., s.61.
14 A. Chorobiński, Walka informacyjna..., dz. cyt., s. 6.
15 M. Czyżak, Wybrane aspekty zjawiska cyberterroryzmu, [z:] www.smerf.fero.pl/f/download.php?id=1163&sid, s. 48
16 A. Chorobiński, Walka informacyjna..., dz. cyt., s. 6.
17 Tamże.
18 M. F. Gawrycki, Cyberterroryzm... dz. cyt., s. 112.
19 A. Chorobiński, Walka informacyjna..., dz. cyt., s. 7.
20 B. Hołyst, Cyberterroryzm... dz. cyt., s. 3.
21 Groupe Islamique Arme – Islamska Grupa Zbrojna.
22 D. Verton, Black ice..., dz. cyt., s. 161.
23 Tamże, s. 162.
24 J. W. Wójcik, Zagrożenia w cyberprzestrzeni..., dz. cyt., s. 7.
25 B. Hołyst, Cyberterroryzm...,dz. cyt., s. 1.
26 Tamże.
26 Tamże, dz. cyt., s. 3.
28 Tamże, dz. cyt., s. 11.
29 D. Verton, Black ice..., dz. cyt., s. 165.
30 Tamże, s. 136.
31 Tamże, s. 139.
32 http://www.rp.pl/artykul/374456.html.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 7/2013 (19)]

NATALIA NOGA

Internet jako cel ataków terrorystów

Uświadomienie sobie powagi zagrożenia, jakim jest cyberterroryzm, przyczynia się do zdefiniowania potencjalnych celów, które mogłyby być obiektami ataków. Z powodu coraz częstszego zainteresowania nowymi technologiami przez organizacje terrorystyczne zauważa się szkolenie przez nich specjalistów w zakresie informatyki i telekomunikacji.

Wynikać może z tego, że cyberterroryzm będzie przybierał na znaczeniu i być może stanie się ważnym elementem podejmowanych aktów terrorystycznych. Z uwagi na kryterium celu działania, cyberterroryzm podzielić można na skierowany przeciwko:

- Systemom komputerowym i danym w nich przechowywanym (cele wirtualne)
- Obiektom świata rzeczywistego (cele rzeczywiste)[1].

W pierwszym przypadku celem ataków są elementy świata wirtualnego. Mogą być to, zatem systemy i programy komputerowe, a także dane w nich zgromadzone. Mimo, iż ataki wymierzone są w obiekty wirtualne, mają wpływ na świat realny. W drugim przypadku – choć co prawda jak dotąd nie było strategicznego cyberataku na obiekty świata rzeczywistego, a przede wszystkim na obiekty infrastruktury krytycznej, wciąż przybywa informacji o rosnących możliwościach prowadzenia przez różne państwa informatycznych działań wojennych. Atak taki mógłby dotknąć wszystkie sektory gospodarki (publiczne i prywatne) w instytucjach cywilnych i wojskowych, a spowodować mógłby przerwanie kluczowych linii telekomunikacyjnych pełniących znaczącą rolę wobec innych gałęzi gospodarki (takich jak finanse), kierowanie ruchem lotniczym czy zasilanie energetyczne. Dla funkcjonowania gospodarki rezultaty takich zdarzeń mogą mieć strategiczne znaczenie, gdyż spowodować mogą utratę zaufania społeczeństwa do niezawodności działania pewnych ważnych dla życia infrastruktur. Organizacje terrorystyczne są coraz bardziej świadome, że infrastruktura krytyczna może być doskonałym celem ataków. Sprawę z tego zdaje sobie również NCS (National Communications System), który w 2000 roku tę sytuację zanalizował: *„(...) wiele grup terrorystycznych dopiero zaczyna zdawać sobie sprawę z korzyści, które niesie technologia internetowa. W miarę, jak członkowie tych grup zaczynają coraz sprawniej posługiwać się technologią internetową, rośnie wśród nich świadomość jej potencjalnych możliwości niszczących. Ponadto rozgłos jest jednym z najważniejszych elementów powodzenia ataków terrorystycznych. Wiele wysiłku włożono w jak najszersze poznanie niedomagań amerykańskiej infrastruktury informatycznej i możliwości jej uszkodzenia za pomocą ataku cyberterrorystycznego. To może prowadzić terrorystów do przekonania, że wymierzony w Stany Zjednoczone atak cyberterrorystyczny da im znaczny rozgłos. Mogą się również spodziewać, że będzie on olbrzymi nawet wówczas, gdy atak nie będzie udany. Jest możliwe, że rozgłos związany z potencjalnym cyberterroryzmem może stać się samospełniającym się proroctwem. To wszystko będzie wymagać bezprzykładnej współpracy gospodarki i rządu”*[2].

Warto zauważyć, że ataki Al – Kaidy z 11 września pokazały światu, że strategia terroryzmu osiągnęła nowy poziom. Dokonano wtedy ataków ekonomicznych, które ponadto przyniosły śmierć tysiącom ludzi. Słowa wypowiedziane przez Osamę bin Ladena kilka miesięcy później udowadniają tę strategiczną zmianę. Głosił on wtedy, iż *„najważniejsze jest ugodzenie gospodarki Stanów Zjednoczonych, bo gospodarka jest podstawą ich militarnej potęgi. Niczym się tak nie przejmą jak ciosem wymierzonym w gospodarkę”*[3].

Zgrupowania wyznające ideologię dżihadu nie wykluczają rozpoczęcia świętej wojny z Internetem. Dowodem na to może być artykuł opublikowany w piśmie „an-Ansar" kilka miesięcy od ataków z 11 września przez doradcę Osamy bin Ladena – Abu Ubeid al -Qurashi, który napisał, że „święta wojna z Internetem" będzie jednym z koszmarów, które wkrótce spadną na Amerykę[4]. Wypowiedzi te powinny obudzić świadomość, że terroryści doskonale zdają sobie sprawę z słabości i rosnącego braku odporności na ciosy zadawane w cyberprzestrzeni. Terroryści będą bowiem uderzać w gospodarkę i styl życia wszelkimi możliwymi środkami. Al - Kaida i wiele innych organizacji terrorystycznych dało jasno do zrozumienia, że docenia znaczenie wysokich technologii dla prowadzonych działań w przyszłości.

Bardzo prawdopodobne jest – w oparciu o analizę dotychczasowej strategii działań terrorystycznych – prawdopodobieństwo zaatakowania systemów informatycznych wykorzystywanych w sferze wojskowej.[5] Znane są przypadki włamań do systemów sterowania satelitów i złamania ich zabezpieczeń. W roku 2000 nieokreślona liczba hakerów włamała się do komputera Marynarki Wojennej USA. Ściągnięto wtedy kody źródłowe, które służą do sterowania systemami satelitów komercyjnych, ale również wojskowych. Złamanie tych systemów zabezpieczeń uczyniło podatną na działanie złego oprogramowania całą sieć satelitów[6]. Znany jest też przypadek włamania do wojskowego systemu komputerowego amerykańskiej bazy lotniczej. Sprawcami byli 16-latek z Wielkiej Brytanii i 22-letni Izraelczyk, którzy wykorzystując połączenia przez Kolumbię i Chile, włamali się do sieci w Nowym Jorku, Seattle i Waszyngtonie. Złamali zabezpieczenie prawie 150 komputerów, w tym jedenastu amerykańskich wojskowych baz lotniczych i marynarki wojennej oraz siedziby głównej NATO. Atak ten kosztował rząd ok. 500 tysięcy dolarów[7].

Oprócz potencjalnych celów cyberterrorystów, jakimi są systemy informatyczne stosowane w sferze militarnej, zaatakowane mogą zostać również systemy cywilne. W znacznym stopniu dostęp do nich ułatwiony jest przez brak odseparowania fizycznego od innych sieci komercyjnych i publicznych. Wywołanie zakłóceń w obiektach, którymi zainteresują się grupy terrorystyczne, mogą spowodować duże straty ekonomiczne oraz negatywne zjawiska społeczne[8].

Systemy informatyczne, które mogą być zaatakowane, to między innymi:

- systemy, które wspomagają zarządzanie transportem (szczególnie kolejowym) oraz ruchem powietrznym
- systemy, które wykorzystywane są w instytucjach państwowych, a których działanie opiera się na sprawnym funkcjonowaniu baz danych
- systemy powiadamiania służb ratowniczych i reagowania antykryzysowego
- systemy, które pracują w różnych sektorach – np. bankowości – oraz stosowane przy produkcji i dystrybucji dóbr o strategicznym znaczeniu (energia elektryczna, woda, gaz, ropa).

W Polsce, gdy protesty w sprawie ACTA pokazały, że zagrożenie cyberatakami jest jak najbardziej realne, rozpoczęło się wiele spekulacji na temat bezpieczeństwa w sieci podczas mistrzostw EURO 2012. Gdyby cyberterroryści przeprowadzili ataki na serwisy WWW lotnisk lub komunikacji miejskiej, mogliby doprowadzić nawet do śmierci wielu ludzi.

Nieco inny schemat potencjalnych celów i obiektów cyberataków przedstawia Krzysztof Liedel. Wspomina on, że jednym z kluczowych celów ataków cyberterrorystycznych mogą być ataki na infrastrukturę krytyczną. Ataki te mogłyby zniszczyć lub przerwać działanie infrastruktury krytycznej państwa poprzez wykorzystanie słabości komputerowych. Do głównych elementów tej infrastruktury zalicza się:

- telekomunikację: linie telefoniczne, satelity, sieci komputerowe – komercyjne, wojskowe, akademickie

- system energetyczny: produkcja, przemysł i dystrybucja energii oraz transport i magazynowanie surowców niezbędnych do jej produkcji
- produkcję, magazynowanie i transport gazu ziemnego i ropy naftowej: cały proces wydobycia ropy naftowej i gazu ziemnego, przetwarzania, magazynowania i transportu za pomocą statków, rurociągów, transportem kolejowym i kołowym
- system bankowy i finansowy: system przepływu kapitałów
- transport: lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz system wsparcia logistycznego
- system zaopatrzenia w wodę: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania jej dla rolnictwa, przemysłu, straży pożarnych i indywidualnych odbiorców
- służby ratownicze: komunikacja z służbą zdrowia, strażą pożarną i policją
- ciągłość funkcjonowania władzy i służb publicznych[9].

Wśród obiektów infrastruktury krytycznej należy wymienić również tzw. krytyczną infrastrukturę teleinformatyczną, na której działaniu opiera się większość systemów odpowiedzialnych za prawidłowe funkcjonowanie większości instytucji i przedsiębiorstw w państwie. Działanie tej infrastruktury oparte jest na prawidłowym działaniu wielu systemów na nią złożonych. W związku z tym atak na jeden z systemów mógłby spowodować katastrofalne skutki, gdyż infrastruktura teleinformatyczna odpowiedzialna jest za poprawne funkcjonowanie instytucji państwowych oraz poprawny przebieg procesów gospodarczych. Schemat, który znakomicie obrazuje, jakie systemy infrastruktury teleinformatycznej są najbardziej narażone na ataki, przedstawia Grzegorz Krasnodębski. Autor wśród najbardziej zagrożonych systemów tej infrastruktury wymienia systemy ewidencyjne, systemy finansowe, systemy bankowe, systemy logistyczne, systemy medyczne, systemy transportowe, systemy administracji państwowej, systemy bezpieczeństwa i systemy zarządzania kryzysowego. Należy pamiętać, że jednym z elementów infrastruktury teleinformatycznej są zwykłe domowe komputery podłączone do Internetu i, że to właśnie ich działanie może przyczynić się nawet do destabilizacji kraju.

Współcześnie praktycznie cała infrastruktura drogowa, kolejowa i lotnicza wykorzystuje w pracy rozwiązania teleinformatyczne. Jest to dobry powód dla terrorystów, aby wykorzystując sieć móc spowodować katastrofę komunikacyjną. Hakerzy, poprzez uzyskanie dostępu do zasobów głównych linii lotniczych mogliby spenetrować systemy zaplecza czy rezerwacji. Mogliby dostać się do list pasażerów czy nawet wprowadzić bagaż z nielegalną zawartością. Za pomocą sieci komputerowej lub Internetu terroryści mogliby zaatakować system kontroli powietrznej i doprowadzić do zderzenia dwóch samolotów pasażerskich. Już w 1997 roku nastoletni haker odciął połączenia telefoniczne portu lotniczego w Worchester w Massachusetts unieruchamiając główny komputer firmy telefonicznej. W wyniku tych działań wieża kontrolna lotniska pozbawiona była ważnych usług. Ponadto, samoloty przyjmowane być mogły jedynie za pomocą komunikatów radiowych i instrukcji lądowania przesyłanych przez inne lotniska[10]. Co prawda nie był to klasyczny akt cyberterroryzmu (choć w myśl obowiązującego obecnie prawa w Stanach Zjednoczonych i Wielkiej Brytanii nie jest to tak oczywiste), jednak działanie to stanowiło istotne zagrożenie bezpieczeństwa narodowego i międzynarodowego. Skoro dostęp do strzeżonych danych mógł uzyskać haker, mógł to zrobić również terrorysta.

Uszkodzenie – często nieodwracalne – baz danych, zasobów danych finansowych czy tajnych dokumentów mogłyby doprowadzić nawet do śmierci ludzi lub zniszczenia mienia. Przykładem takiego działania mogłoby być zablokowanie działania serwera szpitalnego. W momencie, gdy służy on do przechowywania,

gromadzenia i udostępniania danych, włamanie się do systemu może być traktowane jako akt cyberprzestępczy. Gdyby działanie osób w sieci doprowadziło jednak do śmierci wielu pacjentów – np. poprzez zmodyfikowanie systemu podawania leków i dostarczaniu ich nieodpowiednim osobom – uznać to można jako cyberterroryzm[11].

Jeden ze scenariuszy, dotyczący możliwości manipulacji przez terrorystów w systemie komputerowym pogotowia ratunkowego w dużym mieście, powstał w Centrum Studiów Strategicznych i Międzynarodowych w Waszyngtonie. Okazało się, że terroryści są w stanie wysłać wszystkie karetki pogotowia w jedno miejsce. W miejscu tym mogliby również zorganizować zasadzkę. Podobny scenariusz ustalono w związku z działaniem straży pożarnej. Gdyby terroryści faktycznie wyłączyli odpowiednie służby z możliwości interwencji, w przeciągu niedługiego czasu mogliby sparaliżować funkcjonowanie miasta[12].

Internet i przemysł telekomunikacyjny ułatwiają życie terrorystom, infrastruktura ta jest bowiem celem łatwiejszym do uszkodzenia i trafienia. Dowodzi tego również drugi roczny raport Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction z 15 grudnia 2000 roku, w którym przeczytać można, że *„możliwe jest dokonanie przez terrorystów ataku cyberterrorystycznego na instalacje energetyczne lub wodne albo na zakłady przemysłowe – na przykład fabryki chemiczne produkujące substancje silnie toksyczne – aby liczba ofiar sięgała setek tysięcy”*[13].

Obecnie większość rzeczy na świecie zależnych jest od różnych form energii – elektryczności, gazu ziemnego czy ropy naftowej. Jeżeli więc w sektorze energetycznym nastąpi awaria, ucierpieć może wszystko, co zależne jest od dostaw energii. Duża jest również zależność dostaw poszczególnych źródeł energii. Potwierdzają to słowa Dana Verton’a, który słusznie twierdzi, że *„przemysł zaopatrzenia w energię jest pierwszą kostką domina, która może spowodować przewrócenie wielu następnych i ogólne załamanie infrastruktury w różnych działach gospodarki”*[14]. Coraz większe znaczenie – z punktu widzenia potencjalnych celów cyberataków – ma rosnąca liczba instalacji dostarczających wodę, która sterowana jest cyfrowo przez systemy SCADA. Systemy te nadzorują pracę pomp i urządzeń obróbki wody. Hakerzy za pomocą swego działania mogliby wyszukać wrażliwe punkty tego systemu i doprowadzić do problemów z dostarczaniem wody. Istotny jest też fakt, że dostęp do lokalnych instalacji wodnych coraz częściej umożliwiony jest za pomocą Internetu i lokalnych sieci komputerowych. Z tego powodu system ten narażony jest w dużej mierze na działanie wirusów i złośliwych programów. Ponadto, systemy wodne stają się podatne na ataki odmowy dostępu, w rezultacie czego może dojść do przerwania działania urządzeń. System dostarczania gazu często również zależy od systemu SCADA. Łącza te, z uwagi na podłączenie do Internetu, podatne są na wiele cybernetycznych zakłóceń. W przypadku zmiany zasadniczego ciśnienia w gazociągach mogłoby dojść nawet do rozerwania rur i eksplozji. Mimo, że wiele instalacji - zarówno wodociągowych jak i gazowych - wyposażonych jest w zawory zabezpieczające przed takim działaniem, znaczna część z nich jest zabezpieczeń pozbawiona. Mogą być one zatem uszkadzane za pomocą tego rodzaju ataków przeprowadzonych z Internetu. Spore zniszczenia mógłby spowodować także atak na oczyszczalnię ścieków, kanalizację lub urządzenia chlorujące wodę. Atak taki mógłby mieć istotne znaczenie dla zdrowia, co zauważono podczas ataku na oczyszczalnię ścieków w Sunshine Cost w 2000 roku poruszanego w poprzednich częściach.

Ogromnym zagrożeniem ze strony cyberterroryzmu jest werbowanie specjalistów z dziedziny informatyki, którzy w agencjach rządowych lub korporacjach prywatnych zaangażowani byli przy tworzeniu oprogramowania. Przykład taki zaobserwowano w Japonii w 2000 roku, kiedy to członkowie grupy Aum Shinryko opracowali oprogramowanie umożliwiające śledzenie pojaz-

dów policyjnych (również tych nieoznakowanych). Wiele japońskich firm i agencji rządowych, jak się później okazało, zatrudniało członków tej sekty[15]. Grupy terrorystyczne coraz częściej są w posiadaniu wiedzy, by dokonywać takich ataków. Jednak, aby zniszczyć sieć informatyczną, a tym samym sparaliżować życie w państwach wysoko rozwiniętych, nie trzeba znać się na informatyce. Bardzo niebezpieczne jest działanie tradycyjnych terrorystów wiedzących jedynie, gdzie uderzyć, używających tradycyjnych środków – na przykład materiałów wybuchowych.

Z uwagi na fakt, iż coraz więcej państw zwiększa stopień zinformatyzowania kraju, coraz większa liczba ataków może być skierowania właśnie w infrastrukturę teleinformatyczną. Najlepszym przykładem jest Estonia, w której ponad 90% transakcji bankowych dokonywanych jest on-line, a nawet deklaracje podatkowe mogą być składane przez Internet. Ponadto, obywatele za pomocą Internetu mogą głosować, a wszelkie rządowe dokumenty dostępne są w sieci[16]. Po atakach z 2007 roku sieć teleinformatyczna w Estonii doprowadzona została do stanu krytycznego. Te wszystkie czynniki udowodniły, że infrastruktura teleinformatyczna jest znakomitym celem cyberataków. Wszelkie instytucje finansowe – banki, towarzystwa kredytowe, domy brokerskie – śpieszą się do zastosowania technologii informacyjnych i sieci bezprzewodowych. Wynika to z nieustannego dążenia do obcinania kosztów i ulepszania obsługi klientów. Korzystanie z technologii bezprzewodowych ma istotne znaczenie, a z związku z tym zauważa się rosnącą liczbę ataków hakerów. W roku 2001 ponad 50% wszystkich hackerskich ataków było wymierzonych właśnie w banki i instytucje finansowe[17].

Cyberataki wymierzone mogą być również w system bankowy, którego zakłócenie może mieć wpływ na funkcjonowanie całego państwa. Celem destrukcyjnego ataku zdaniem Jakuba Syty mogłoby być *„zafałszowanie danych światowych giełd papierów wartościowych, machinacja na potężną skalę kursami walut czy modyfikowanie na potężną skalę zapisów dotyczących stanu środków na rachunkach czy poziomu zadłużenia (...)”*[18]. Zdaniem autora tych słów, szturmowanie banków oraz przecena wartości papierów wartościowych zdecydowanie spowodowałyby chaos gospodarczy. Ponadto, pogłębiłby się spadek zaufania do banków, a nawet zamykane zostałyby przedsiębiorstwa, zwalniani pracownicy oraz aktywa gromadzone na rachunkach byłyby zamrażane[19].

Najlepszym przykładem ataku cyberterrorystycznego, który przerwał działanie ważnych instalacji i urządzeń telekomunikacyjnych, był atak z 11 września. Sieć bezprzewodowa została zablokowana nadmiarem połączeń, a na większość wezwań nie można było odpowiedzieć. Zablokowane zostały połączenia między poszczególnymi agencjami Pentagonu i nie można było porozumieć się przy prowadzeniu działań ratunkowych. Trwał szturm na magazyny i zaopatrywanie pracowników służb ratunkowych w radiotelefony. Dla cywilów sieć telefoniczna i komórkowa przez większość dnia była niedostępna.

Cyberterroryzm, podobnie jak inne formy terroryzmu, są atakami niosącymi masowe ofiary i przerażenie. W każdej z form głównym celem i narzędziem jest strach. W przypadku cyberterroryzmu ataki cyfrowe na wodociągi czy infrastruktury finansowe budzą atmosferę niepewności i utraty zaufania. Liczba potencjalnych scenariuszy, jakie mogą mieć miejsce, jest nieskończona. Atak na infrastrukturę krytyczną znacząco mógłby wpłynąć na gospodarkę zaatakowanego państwa. Ponadto, mógłby spowodować straty wśród ludności cywilnej. Włamanie się chińskich i rosyjskich hakerów do amerykańskiej sieci energetycznej z kwietnia 2009 roku potwierdzają realność takiego zagrożenia. Hakerzy zostawili wtedy w systemie oprogramowanie, które w chwili kryzysu miało zakłócić pracę całego systemu a ponadto zainteresowani byli także pozostałą częścią infrastruktury krytycznej[20].

Bardzo niebezpieczny jest fakt, że informacje o potencjalnych celach, które mogą być obiektem ataków, są często ogólnodostępnymi informacjami. Przy-

kładem może być działanie Irlandzkiej Armii Republikańskiej, której członkowie w 1996 roku przygotowywali się do wysadzenia w powietrze ważnych podstacji elektrycznych, rurociągów i zaworów gazowych w Londynie. Członkowie tej organizacji chcieli pozbawić miasto zasilania, a dane o całej sieci elektrycznej zaczerpnęli z ogólnie dostępnych źródeł informacji - biblioteki i Internetu[21].

Należy pamiętać, że nie tylko obiekty infrastruktury krytycznej mogą stać się obiektem ataków, a informacje dla terrorystów planujących atak zawarte w Internecie o tych obiektach nie są jedynym problemem. Celem ataku mogą stać się również firmy publikujące informacje zawierające komunikaty popierające globalizację. Al – Kaida jest przeciwna publikowaniu takich informacji w witrynach i na stronach internetowych. W USA w jednej z firm wykryto pliki zawierające zamrożone konta bankowe, które należały do osób i instytucji wspierających Al – Kaidę. Gdyby członkowie tej organizacji znaleźli taką informację, mogłoby to wzbudzić agresję i stać się przyczyną ataku na firmę[22].

Technologia informacyjna może być zarówno celem, jak i narzędziem w rękach terrorystów. Zaatakowane mogą być sieci i systemy teleinformatyczne oraz instytucje państwowe, które znacząco wpływają na bezpieczeństwo państwa. Ataki mogą przyczynić się do zmniejszenia poczucia bezpieczeństwa obywateli, spowolnienia lub zaniechania procesów gospodarczych, a nawet mogą wpłynąć na zdrowie i życie ludzi. Infrastruktura ta ma kluczowe znaczenie dla bezpieczeństwa narodowego, a jej uszkodzenie może spowodować istotne zagrożenie zarówno dla zdrowia, życia ludzi, jak i interesów obronności oraz bezpieczeństwa państwa.

Obecnie Internet jest źródłem mnóstwa informacji dla terrorystów. Stał się zatem jednym z głównych narzędzi służących pozyskaniu niezbędnych danych o obiektach, które mogą być celem ataku. Ataki cyberterrorystyczne mogą zostać skierowane i zagrozić funkcjonowaniu niemal każdego z elementów infrastruktury krytycznej państwa, ponieważ obecnie wszystko, co spełnia w życiu oczywistą rolę - telekomunikacja, systemy energetyczne, produkcja, system bankowy i finansowy, transport, system zaopatrzenia w wodę, służby ratownictwa oraz ciągłość w funkcjonowaniu służb publicznych – może działać jedynie dzięki komputerom. Jest to opis nie tego, co się zdarzy w przyszłości, a tego, co może się zdarzyć, jeśli nie podejmiemy odpowiednich działań. Na tym właśnie polega najważniejsza i największa groźba, jaką niesie rozprzestrzenianie się cyberterroryzmu.

Przypisy

1 D. Opalach – Nusbaum, Cyberterroryzm – Nowe oblicze terroryzmu [w:] Malendowski W. Świat współczesny. Wyzwania, zagrożenia i współzależności w procesie budowy nowego porządku międzynarodowego, Poznań 2008, s.304.
2 D. Verton, Black ice..., dz. cyt., s. 195.
3 Tamże, s. 132.
4 Tamże, s. 302
5 T. Jemioło, Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku [w:] Cyberterroryzm– nowe wyzwania XXI wieku,[z:] http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/Jemiolo.pdf, s.9, z dnia 15.06.2012.
6 D. Verton, Black ice..., dz. cyt., s. 118.
7 M.F. Gawrycki, Cyberterroryzm... dz. cyt., s. 80-81.
8 T. Jemioło, Wyzwania i zagrożenia... dz. cyt., s.9.
9 K. Liedel, Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Toruń 2006, s. 39.
10 D. Verton, Black ice..., dz. cyt., s. 68.
11 L. Wolaniuk, Cyberterroryzm... dz. cyt., s.160.
12 J.K. Wójcik, Zagrożenia w cyberprzestrzeni ... dz. cyt., s.4.
13 Drugi roczny raport Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, 15 grudnia 2000.
14 D. Verton, Black ice..., dz. cyt., s. 80.
15 T. Szubrycht, Cyberterroryzm jako nowa forma zagrożenia terrorystycznego, [z:] http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Szubrycht_T.pdf, z dnia 15.06.2012, s.184.
16 J.G. Rattray, Wojna strategiczna w cyberprzestrzeni, Warszawa 2004, s. 29.
17 D. Verton, Black ice..., dz. cyt., s. 120 -121.
18 J. Syta, Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego, [z:] http://www.immusec.com/sites/default/files/publikacje/sektor_bankowy_jako_potencjalny_cel_ataku_cyberterrorystycznego.pdf, z dnia 15.06.2012, s. 2.
19 Tamże.
20 Biuro Bezpieczeństwa Narodowego, Terroryzm cybernetyczny... dz. cyt., s.6.
21 D. Verton, Black ice..., dz. cyt., s. 68.
22 Tamże, s. 175 – 176.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 8/2013 (20)]

NATALIA NOGA

Klasyfikacja ataków w cyberprzestrzeni

Obawy związane z aktywnością terrorystyczną w sieci w ostatnich latach przybierają na sile. W przypadku takich działań skutki destrukcyjne mogą mieć ogromny zasięg, tym bardziej, że uzależnienie społeczeństw od technologii informatycznych wciąż postępuje. Wielu specjalistów coraz częściej zdaje sobie sprawę z rosnącego zagrożenia zjawiskiem cyberterroryzmu.

Dyrektor FBI - Louis Freeh twierdził, że FBI „uważa, że cyberterroryzm, czyli stosowanie cybernarzędzi do wyłączania, uszkadzania i powodowania zaniechania świadczenia usług przez infrastruktury krytyczne – takie jak energia, transport, łączność i służby rządowe – służy do wpływania siłą na działania rządu oraz do zastraszania władz i ludności. Jest to nowa groźba, która zmusza nas do stworzenia specjalnego systemu obrony, odstraszania i odpowiadania na ataki”[1]. Wraz z rosnącym postępem technologicznym i rosnącymi możliwościami jego niewłaściwego wykorzystania, należałoby sklasyfikować, z jakimi atakami ze strony organizacji terrorystycznych w sieci możemy mieć do czynienia. Zgodnie z definicją zjawiska „cyberterroryzmu” M. Pollita, wyróżnić można dwa rodzaje akcji cyberterrorystycznych, które mogą się wzajemnie uzupełniać i być samodzielną akcją lub częścią większej kampanii. Należą do nich: ataki mające miejsce w cyberprzestrzeni i ataki fizyczne na systemy informacyjne. Każdy z nich może zachwiać stabilność gospodarki.

W przypadku ataku fizycznego terroryści w cyberprzestrzeni dokonują działań ułatwiających bądź pozorujących uderzenie w realnym świecie. Nie trzeba w tym przypadku znać się nawet na informatyce, można użyć tradycyjnych środków (np. materiałów wybuchowych) i jedynie wiedzieć, gdzie uderzyć. Już w 1985 roku japońska grupa terrorystyczna Frakcja Środka uszkodziła kable telefoniczne i kable energetyczne systemu sterowania komputerowego ruchem pociągów, czym spowodowała chaos w komunikacji, w czasie największego ruchu. Atak miał być demonstracją solidarności ze strajkującymi kolejarzami, którzy protestowali przeciw prywatyzacji japońskich kolei. Wskutek działań około 6, 5 miliona osób nie dojechało do pracy[2]. Ataki mogą być zatem prowadzone starymi metodami, jednak zmienione zostały cele tych akcji – organizacje terrorystyczne zdają sobie bowiem doskonale sprawę z tego, że atak na infrastrukturę informacyjną może odnieść większe skutki niż atak konwencjonalny. Również w latach 70. organizacje terrorystyczne podejmowały próby niszczenia powstających sieci informatycznych. Firmy elektroniczne i komputerowe we Włoszech zostały 27 razy zaatakowane przez Czerwone Brygady, których członkowie głosili, że niszcząc systemy i instalacje komputerowe „atakują samo serce państwa”[3]. Fizyczne niszczenie elementów sieci komputerowych i infrastruktury informatycznej jest łatwe do przeprowadzenia, ale pozwala terrorystom jedynie na osiągnięcie efektu wyłącznie w skali lokalnej. Znaczenie tego ataku rośnie jednak, gdy stanowi element wspierający główną operację terrorystyczną.

Klasyczny atak mający miejsce w cyberprzestrzeni ma na celu ingerencję w sieci informatyczne, z zamiarem zniszczenia bądź uniemożliwienia ich funkcjonowania lub sprawowania nad nimi kontroli. Ataki te mogą obejmować oprogramowanie przeciwnika (software) lub systemy informacyjne i sprzęt komputerowy (hardware). Ze względu na różnorodność form ataku oraz różnorodność kryteriów opisu tego zjawiska nie ma jednoznacznej klasyfikacji. W swojej książce „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie” A. Bógdał – Brzezińska i M.F. Gawrycki przedstawiają w wyczerpujący sposób ten problem.

Klasyfikacja ataków

Pierwszą, zaprezentowaną metodą klasyfikacji jest lista siedmiu kategorii działań w cyberprzestrzeni, opracowana przez S. Bellovina i W. Cheswicka:

1. Stealing passwords (tłum. z ang. kradzież haseł) – metoda polegająca na uzyskaniu haseł dostępu do sieci;
2. Social engineering (tłum. z ang. inżynieria społeczna) – wykorzystanie niekompetencji osób mających dostęp do systemu;
3. Bugs and backdoors (tłum. z ang. błędy i tylne drzwi) – używanie oprogramowania z nielegalnych źródeł lub korzystanie z systemu bez specjalnych zezwoleń;
4. Authentication failures (tłum. z ang. błędy uwierzytelniania) – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji;
5. Protocol failures (tłum. z ang. błędy protokołu) – wykorzystywanie luk w zbiorze reguł, które sterują wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami bądź procesami;
6. Information leakage (tłum. z ang. wyciek informacji) – uzyskanie informacji dostępnych tylko administratorowi, które niezbędne są do poprawnego funkcjonowania sieci;
7. Denial of services (tłum. z ang. odmowa usługi) – uniemożliwienie użytkownikom korzystania z systemu[4].

Mając na uwadze powyższą listę kategorii, F. Cohen stworzył własną kategoryzację. Sformułowana jest ona na zasadzie opisania rezultatu ataku w cyberprzestrzeni:

1. Corruption (tłum. z ang. zepsucie, rozkład) – nieuprawniona zmiana informacji;
2. Leakage (tłum. z ang. wyciek) – informacja znalazła się w niewłaściwym miejscu;
3. Denial (tłum. z ang. odmowa) – kiedy sieć lub komputer nie nadają się do użytkowania[5].

Atakujący dokonują uderzenia w niecodziennych sytuacjach. Wynika stąd, że działań w sferze cyberprzestrzeni nie da się zakwalifikować wyłącznie do jednej kategorii. Dłuższą listę, opartą na danych empirycznych, stworzyli zatem P. Neumann i D. Parker. Lista ta daje możliwość klasyfikacji różnego rodzaju ataków:

1. External Information Theft (tłum. z ang. zewnętrzna kradzież informacji) – kradzież lub przeglądanie informacji przez osobę spoza systemu;
2. External Abuse of Resources (tłum. z ang. zewnętrzne nadużywanie zasobów) – niszczenie twardego dysku;
3. Masquerading (tłum. z ang. podszycie, maskarada) – podawanie się za kogoś innego;
4. Pest Programs (tłum. z ang. szkodliwe programy) – instalacja złośliwego programu;
5. Bypassins Authentication or Authority (tłum. z ang. omijanie autentyczności lub autoryzacji) – łamanie haseł;
6. Authority Abuse (tłum. z ang. nadużywanie autoryzacji) – fałszowanie danych;
7. Abuse Through Inaction (tłum. z ang. nadużywanie bezczynności) – celowe prowadzenie złego zarządzania;
8. Indirect Abuse (tłum. z ang. pośrednie nadużycie) – używanie innych systemów do tworzenia złośliwych programów[6].

Kategoryzacja ta wydaje się najpełniejsza spośród wcześniej omawianych. Innym rozwiązaniem, stworzonym przez C. Landwehra i A.R. Buli, są tzw. matryce pojęciowe. Opierają się one na następujących aspektach:

1. Genesis (tłum. z ang. geneza) – wykorzystaniu luk w zabezpieczeniach;
2. Time of Introduction (tłum. z ang. moment wprowadzania) – czasie „życia" oprogramowania i sprzętu komputerowego;
3. Location (tłum. z ang. lokalizacja) – lokalizacji

„dziur" w oprogramowaniu i sprzęcie komputerowym[7].

Matryca ta bardzo dokładnie opisuje różne rodzaje ataków w cyberprzestrzeni. Jednak przydaje się do klasyfikacji indywidualnych uderzeń (takich, które można przypisać do jednej kategorii). Nie jest to łatwe w przypadku ataków złożonych.

Inną, ostatnią już klasyfikacją opartą na działaniu jest zdefiniowanie czterech rodzajów ataków przez W. Stallingsa. Ma jednak ona ograniczoną możliwość zastosowania, gdyż dotyczy jedynie ataków traktowanych jako seria działań. Są to:

1. Interruption (tłum. z ang. przerwanie) – nie można zastosować zabezpieczenia systemu lub zostało ono zniszczone;
2. Interception (tłum. z ang. przechwytywanie) – dostęp do istniejących zabezpieczeń zdobyła nieuprawniona osoba;
3. Modification (tłum. z ang. modyfikacja) – nieuprawniona osoba zdobyła dostęp a także manipulowała zabezpieczeniem;
4. Fabrication (tłum. z ang. produkcja) – przez nieuprawnioną osobę do systemu wprowadzony został sfałszowany obiekt[8].

Przedstawiona różnorodność klasyfikacji aktów cyberterrorystycznych jest dowodem na wieloaspektowość tego zagadnienia, jak również dynamikę zjawisk zachodzących w cyberprzestrzeni. Stworzenie słownika pojęć związanych z cyberterroryzmem daje zatem możliwość scharakteryzowania różnego rodzaju ataków w cyberprzestrzeni.

Metody ataków

Bardzo przydatne w ustaleniu potencjalnych metod, jakimi mogą posługiwać się cyberterroryści, są informacje uzyskane od pana mgr. Waldemara Mielniczek – dostawcy Internetu w firmie Neconet. Osoba ta jest specjalistą w zakresie bezpieczeństwa sieci i wielokrotnie w swojej pracy miała do czynienia z przestępcami komputerowymi. Co prawda, nie można było ich zaliczyć do grona cyberterrorystów, ale nie należy zapominać, że cyberterroryści mogą się również posługiwać tradycyjnymi i prostymi metodami, a cyberprzestępczość coraz częściej przyjmuje wymiar cyberterroryzmu. W rozmowie, mgr W. Mielniczek wspomina, że najczęstszą metodą działań osób niepożądanych w sieci jest zdobywanie informacji, które są niezbędne do poprawnego działania sieci dostępnych wyłącznie dla administratora, a ponadto uniemożliwienie użytkownikom korzystania z ich systemów. Twierdzi również, że jedną z bardziej popularnych metod cyberataku, może być uzyskanie dostępu do sieci za pomocą hasła poprzez wykorzystanie niekompetencji osób mających dostęp do systemu. Ponadto, cyberagresorzy, aby mieć dostęp do sieci, mogą zniszczyć mechanizm używany do autoryzacji, wykorzystać luki w zbiorze reguł sterujące wymianą informacji pomiędzy dwoma (lub wieloma) niezależnymi urządzeniami lub procesami a także korzystać z systemu bez specjalnych zezwoleń lub używać oprogramowania z nielegalnych źródeł. Rozmówca oprócz udzielenia informacji na temat potencjalnych metod ataku cyberterrorystów wyraził opinię nt. możliwości przeprowadzenia takiego cyberataku. Jest zdania, że w dobie społeczeństwa informacyjnego i niezwykle dynamicznego rozwoju systemów komputerowych a także nieograniczonego dostępu do Internetu w oczywisty sposób jesteśmy narażeni na ataki, a przestępczość będzie coraz częściej przybierać taką formę. Twierdzi, że jest to łatwe do przeprowadzenia, a narzędzia do przeprowadzenia takiego ataku są dostępne nawet w Internecie.

Podobnie twierdzi Grzegorz Krasnodębski, który wymienia zagrożenia wynikające z ataków w cyberprzestrzeni. Widać, że jest ich bardzo wiele. Nie-

które z nich wskazują na aktywność niszczącą, inne na zakłócającą. Ponadto, niektóre wskazują, że środkami do prowadzenia ataków mogą być zasoby komputerowe, inne, że systemy informacyjne są celami tych ataków. Zdaniem tego autora zauważyć można, iż wśród najczęstszych zagrożeń wynikających z ataków w cyberprzestrzeni są:

1. Uszkodzenie i nieuprawnione modyfikacje łączy telekomunikacyjnych;
2. Brak wiedzy oraz świadomości wśród personelu i kadry zarządzającej w zakresie bezpieczeństwa teleinformatycznego;
3. Niewłaściwa ochrona elementów sieci;
4. Niepożądane działania administratorów i użytkowników, a nawet celowe wprowadzanie szkodliwego oprogramowania do systemów lub jego uszkodzenie[9].

Nieco inny podział metod ataku opisuje w swoim artykule R. Kośla. Jego zdaniem, ogólne metody ataku cyberterrorystycznego to: metoda fizyczna, ataki elektroniczne i ataki sieciowe[10]. W metodzie fizycznej użyte są środki konwencjonalne, które skierowane zostają przeciw instalacjom komputerowym lub liniom transmisyjnym. Dominują tu działania związane z np. niszczeniem infrastruktury teleinformatycznej za pomocą materiałów wybuchowych lub przerywaniem linii przesyłowych. Ataki elektroniczne realizowane mogą być poprzez szereg sposobów wykorzystujących zjawiska fizyczne – począwszy od impulsu elektromagnetycznego (wyzwalanego np. w czasie wybuchu jądrowego) poprzez stosowanie silnych pól magnetycznych, skończywszy na zastosowaniu urządzeń elektronicznych do generowania silnego pola elektromagnetycznego o określonej charakterystyce[11]. Niektórzy specjaliści twierdzą, że nawet oddziaływanie telefonu komórkowego ma negatywne skutki, gdyż za jego pomocą można otworzyć zatrzask zamka elektronicznego lub uszkodzić płytę główną komputera PC. Mówiąc o atakach sieciowych, należy wziąć pod uwagę przede wszystkim nieupoważnione wejście do systemu czy manipulowanie informacją, jak również wszelkie ataki na usługi dostępne w sieci. Posługujący się tą metodą cyberterroryści (jak niemal wszyscy przestępcy komputerowi) działają wg pewnego schematu. Zawiera on następujące kroki:

1. Rekonesans. W etapie tym cyberterrorysta poszukuje danych, które mogą być użyteczne w późniejszym nielegalnym dostępie do sieci – wirusy, metody socjotechniczne.
2. Skanowanie. Etap ten polega na sprawdzeniu przez atakującego, na ile wiarygodne i użyteczne są zdobyte informacje. Tworzone jest oprogramowanie wykorzystane później do ataku, jednak jeszcze nie odbywa się ingerencja w system.
3. Uzyskanie dostępu. Krok ten polega na przejęciu kontroli nad systemem – cyberterrorysta może np. nadać sobie uprawnienia administratora.
4. Zacieranie śladów. Ostatni etap obejmuje zniszczenie wszelkich śladów w systemie, które mogły zarejestrować działanie cyberterrorysty (pod warunkiem, że celem ataku było utrzymanie tego w tajemnicy, a nie działanie spektakularne)[12].

Metody cyberataków identyfikuje w swym raporcie też M.A.Vatis[13]. Uwzględnia on podział na:

a. Modyfikowanie stron WWW, szerzenie informacji i propagandę;
b. Sabotaż komputerowy, którym jest naruszenie lub paraliżowanie systemów komputerowych za pomocą wirusów i robaków komputerowych lub poprzez przeprowadzenie ataków na DoS (Denial of Service Attacks);

c. Zamachy mogące powodować zakłócenia w funkcjonowaniu infrastruktury krytycznej i zniszczenie danych dla niej kluczowych.

Strony WWW – jak powszechnie wiadomo - mogą być wykorzystywane na wiele sposobów, głównie przez firmy. Jednym z nich jest reklama, która pozwala ukazać najnowsze osiągnięcia, gadżety czy podać szczegółowe informacje o ważnych działaniach. Wszystkie te działania – mimo, że pozytywne dla przemysłu technologicznego, mogą stanowić zagrożenie bezpieczeństwa narodowego. Ponadto, internetowe strony WWW są znakomitym miejscem dla terrorystów poszukujących informacji o infrastrukturze krytycznej, która może być zarazem potencjalnym celem ataku. Gdy terrorysta zbierze potrzebne mu informacje z różnych stron i połączy je w całość, może otrzymać informację, która powinna być zakwalifikowana jako tajna. Najlepszym przykładem będzie znalezienie w jaskiniach Afganistanu laptopa należącego do jednego z członków Al - Kaidy. W komputerze tym znajdowały się ważne informacje na temat amerykańskiej infrastruktury.

Ataki na strony WWW prowadziła również propalestyńska grupa hackerska USG (Unix Security Guards). Miała ona na celu przeciwstawienie się amerykańskiej wojnie z terroryzmem i działaniom określanym jako agresja Indii przeciw muzułmanom w Kaszmirze Grupa zniekształcała strony WWW, które wyglądały jak montaże multimedialne. Często złożone były z muzyki arabskiej i zdjęć zniszczeń. Grupę tą uznano za odpowiedzialną za zniszczenie prawie 2 tysięcy stron WWW i umieszczenie na nich informacji antyizraelskich i antyamerykańskich. Kolejną powstałą grupą pro palestyńską było WFD, która identyfikuje się ideologicznie z organizacją terrorystyczną, jaką jest Hezbollah. Przeprowadzała ona dobrze zorganizowane operacje, których skutkiem było m.in. zablokowanie oficjalnej strony wyborczej izraelskiego premiera Ariela Sharona oraz spenetrowanie indyjskiego Ministerstwa Informacji i Technologii[14]. Działania te pokazały, że grupy hackerskie mogą spowodować bardzo poważne uszkodzenia i zniszczenia – a w przypadku tej grupy nawet kryzys w Izraelu. Wydawać się może, że uszkadzanie stron WWW nie są poważnym problemem, ale jednak mogą być one doskonale zorganizowane, a cele ataku są zwykle przemyślane. Innym przykładem, w 2001 roku, grupa będąca muzułmańskim sojuszem Al - Kaidy zwana AIC (Anti -India Crew) przeprowadziła ataki na serwery należące do Generalnego Biura Rozrachunkowego GAO (odpowiednik polskiej Najwyższej Izby Kontroli). Do grupy tej należą osoby z profesjonalnym wykształceniem, a także posiadacze certyfikatów z różnych dziedzin wiedzy technicznej. Oprócz zniszczenia witryny GAO wyłączono internetowy system automatycznego rozsyłania raportu oraz zmodyfikowano stronę tak, by wyświetlała komunikat głoszący: „Będziemy atakować serwery rządowe (amerykańskie, indyjskie i izraelskie), aż wokół nas zapanuje pokój![15].

Grupy terrorystyczne mogą również prowadzić akcje sabotażowe. Kampanię taką zauważono już w 1997r. Na przedmieściach Algierii muzułmańscy fundamentaliści fizycznie zaatakowali systemy telekomunikacyjne i sparaliżowali algierski system telefoniczny. Ataki przyczyniły się do uniemożliwienia korzystania z telefonów na przedmieściach Algieru oraz zakłócenia dostaw gazu i elektryczności w stolicy. Gospodarka krajowa w wyniku tych aktów straciła ponad 2 miliardy dolarów[16].

Jedną z metod, którą coraz częściej zaczynają stosować w atakach cyberterroryści, jest wykorzystanie sieci bezprzewodowych. Obecnie coraz większa liczba firm z różnych sektorów gospodarki spieszy się z zastosowaniem sieci bezprzewodowych

i technologii internetowych, nie zwracając uwagi na zagrożenia temu towarzyszące. Wraz z nadejściem ery technologii bezprzewodowej zmienia się nieodwracalnie koncepcja Internetu. Dostęp do danych finansowych za pomocą urządzeń bezprzewodowych jest coraz częściej uzyskiwany przez klientów, jednakże dostęp do nich w instytucjach finansowych, bankach i innych firmach świadczących usługi komunikacyjne i pośredniczące w dokonywaniu transakcji oznacza wzrost liczby punktów ułatwiających ataki. Jeden ze scenariuszy wykorzystania technologii bezprzewodowych przez terrorystów opisuje Dan Verton. Mówi on, że „zaszyfrowane dane docierają z sieci bezprzewodowej do bramki, przez którą są przekazywane do Internetu, a stamtąd do firmy świadczącej usługi finansowe. Jednakże sieci bezprzewodowe i kablowe używają do przesyłania zaszyfrowanych danych innych protokołów komunikacyjnych. W rezultacie w bramce dane są na kilka sekund odszyfrowywane i następnie szyfrowane ponownie. W ciągu tych kilku sekund mogą być przechwycone przez hakerów i już przyczyniło się to do utraty setek milionów dolarów".

Oprócz omówionych metod ataku w cyberprzestrzeni należy szczególną uwagę zwrócić na tzw. „swarming attack" (jednoczesne wykonywanie wielu ataków konwencjonalnych oraz cyberataków wymierzonych w liczne infrastruktury). Jest to najgroźniejsza metoda, jaką mogą posługiwać się terroryści, a polega ona na spiętrzeniu i nałożeniu na siebie ataków przeciwko infrastrukturze krytycznej państwa prowadzonych w cyberprzestrzeni oraz fizycznie, przeciwko jej materialnym nośnikom[18]. Jest to o tyle istotne, że w przypadku ataku w cyberprzestrzeni zakłóceniu ulec może działanie materialnych elementów infrastruktury krytycznej. Howard Schmidt – były przewodniczący Prezydenckiej Rady ds. Ochrony Infrastruktury Krytycznej mówi, że „cyberprzestrzeń, z Internetem jako ważnym elementem, stworzyła zależności, które teraz w nieprzewidywalny i groźny sposób zmieniają swą naturę (...). To właśnie swarming attack jest tym, czego powinniśmy się najbardziej obawiać przy każdym ataku fizycznym, a także przy każdym akcie kryminalnym i kataklizmie naturalnym. Takiemu zdarzeniu zwykle towarzyszy uszkodzenie lub degradacja linii i usług telekomunikacyjnych. To są właśnie te wzajemne zależności, których obawiamy się najbardziej"[19]. Należy wspomnieć, że infrastruktura teleinformatyczna i systemy telekomunikacyjne mają wiele słabych punktów. Umożliwiają one przeprowadzenie cyberataku, który w istotny sposób może obniżyć ich wartość i sprawność.

Przypisy

1 Oświadczenie byłego dyrektora FBI Louisa Freeh'a przed United States Senate Committees on Appropriations, Armed Services oraz przed Select Committee on Intelligence, 10 maja 2001.
2 D. Denning., Wojna informacyjna..., dz. cyt., s. 230.
3 M.F. Gawrycki, Cyberterroryzm... dz. cyt., s. 140.
4 Tamże, s. 142.
5 Tamże.
6 Tamże, s. 142-143.
7 Tamże, s. 143.
8 Tamże, s. 143-144.
9 G. Krasnodębski, Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego, [z:] http://www.uwm.edu.pl/.../42_ , z dnia 15.06.2012 , s. 5.
10 L. Wolaniuk, Cyberterroryzm... dz. cyt., s.161.
11 Tamże.
12 Tamże, s.162.
13 D. Opalach – Nusbaum, Cyberterroryzm... dz. cyt., s.304.
14 D. Verton, Black ice..., dz. cyt., s. 156 - 158.
15 Tamże, s. 160.
16 D. Denning, Wojna informacyjna..., dz. cyt., s. 229.
17 D. Verton, Black ice..., dz. cyt., s. 121.
18 K. Liedel, Bezpieczeństwo informacyjne..., dz. cyt., s. 41.
19 D. Verton, Black ice..., dz. cyt., s. 300.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 9/2013 (21)]

NATALIA NOGA

Narzędzia stosowane przez cyberterrorystów

Na działalność cyberterrorystyczną składa się wiele technik. Niektóre z nich wymagają dużych umiejętności praktycznych oraz przygotowania teoretycznego, inne mogą być stosowane przez praktycznie każdego członka organizacji. Jedną z takich technik, najpopularniejszą, jest wykorzystanie komputerowych „bakterii", „robaków" i „wirusów".

Narzędzia te należą do tzw. oprogramowania złośliwego i są one bardzo popularnym oraz niezwykle skutecznym sposobem atakowania przeciwnika. Bakterią nazywamy program, którego głównym celem jest rozmnażanie. Po reprodukcji zajmuje on ogromną ilość miejsca w pamięci procesora, co powoduje trudności w użytkowaniu komputera. Robak jest programem, który wykorzystując słabe punkty w poczcie elektronicznej bądź stronach internetowych rozprzestrzenia się w sieci komputerowej. Wirus natomiast jest kodem, który zmienia sposób działania sprzętu uszkadzając programy bądź dane. Poprzez swoje działanie zarażać on może duże obszary w komputerze[1]. Obecnie w Internecie można znaleźć instrukcje pomagające w napisaniu własnego programu.

Co więcej, dla cyberterrorystów nie istnieje problem znalezienia i zatrudnienia hakera, który mógłby stworzyć wirus, bakterię lub robaka trudnego do wykrycia, a mogącego spowodować znaczne straty. Jak dotąd, mieliśmy już kilka razy, do czynienia z atakami z użyciem tych narzędzi. Bardzo poważnym zagrożeniem był atak robaków *Code Red* z 2001 roku oraz *Sapphire* z 2003roku. Code Red przeprowadził m.in. nieudany atak na strony Białego Domu, zniszczył anglojęzyczne strony internetowe, zainfekował kilka milionów hostów na całym świecie oraz spowodował opóźnienia produkcyjne i straty w wysokości ok. 2 milionów dolarów. Program Sapphire zarażał komputery podłączone do sieci, a liczba jego kopii podwajała się co 8.5 sekundy. Robak ten wyrządził szkody szacowane na ponad miliard dolarów. Zaatakowane zostały m.in. Bank of America i American Express, których klienci nie mogli przez długi czas korzystać z wkładów finansowych. Ponadto, opóźnione zostały loty Continental Airlines[2].

Fot. Brian Klug, http://www.flickr.com/photos/brianklug/6870002408/

Narzędzia takie, jak wirusy i robaki wykorzystane przez terrorystów mogą zatem stanowić poważne zagrożenie dla funkcjonowania państwa i społeczeństwa. Mogą przyczynić się także do spowodowania strat w gospodarce. Przykładem kolejnego wirusa może być program *I love you,* który wywołał powszechną panikę niszcząc zawartość komputerów. Po otwarciu przez użytkownika maila zatytułowanego „I love you" oraz jego załącznika, szkodliwy program wysyłał swoje kopie do wszystkich osób z książki adresowej i się pod nie podszywał. Rozpoczął działanie 4 maja 2000 r. i w ciągu dnia rozprzestrzenił się na cały świat. Zaraził 10 procent wszystkich komputerów, które miały dostęp do Internetu. Straty oszacowano na ok. 5.5 miliarda dolarów. Aby pozbyć się wirusa, instytucje takie jak

Pentagon, CIA i Parlament Brytyjski oraz wielkie korporacje musiały wyłączyć serwery e-mail[3].

Kryzys spowodowany działaniem niszczycielskiego robaka NIMDA przesłanego Internetem świat poznał 18 września 2001r. Eksperci twierdzili, że robak ten ma związek z wydarzeniami 11 września i miał za zadanie pogłębić straty w amerykańskiej gospodarce. W ciągu 30 minut od jego pojawienia stał się problemem globalnym. Działanie robaka polegało na niszczeniu danych. Ponadto, posiadał on zdolność przechodzenia przez słabe punkty Internetu od komputera do komputera. W skutek jego działań wiele firm zostało zmuszonych do zaprzestania wykonywania operacji, a koszty zniszczeń sięgnęły kilku miliardów dolarów.

Cybernetycznym centrum hakerów i twórców wirusów sympatyzujących z Al-Kaidą jest Malezja, która jest źródłem największych ataków internetowych na świecie. Bardzo aktywna grupa w regionie - MHA (Malaysian Hacker Association) - przejawia proirackie, proalkaidowe i pro islamskie sympatie. Jeden z twórców wirusów tej grupy był autorem m.in. VBS.OsamaLaden@mm i Nedal (Laden czytany na wspak), które pozostawiały komunikaty dotyczące ataków terrorystycznych z 11 września i kasowały pliki z folderu systemowego Windows. Twórca tych wirusów groził, że kolejnego wirusa planuje wypuścić na wolność, jeśli Stany Zjednoczone zaatakują Irak. 12 września 2002 włamał się na strony rządowe USA i umieścił napis „Niech Allah błogosławi Saddama Husseina i wszystkich muzułmanów”[4]. Działania te ukazują, że grupy terrorystyczne chcąc odnieść oczekiwany efekt (często bardziej spektakularny), mogą zacząć dokonywać bardziej przemyślanych ataków i zacząć rozpowszechniać bardziej złośliwe robaki i wirusy.

Kolejnym, równie groźnym narzędziem służącym do ataków w sieci są ataki typu „Denial of Services” - DOS (odmowa usługi) oraz „Disturbed Denial of Service” - DDoS (atak rozproszony odmowy usługi). Są to działania, których rezultatem jest zawieszenie komputera bądź zablokowanie serwisu sieciowego. Ataki tą metodą polegają na blokowaniu serwerów przez zalewanie sieci ogromną ilością danych. Za pomocą tej metody w lutym 2000 roku zostały zaatakowane internetowe giganty – Yahoo, Amazon, CNN, eBay. Wskutek tych ataków na jakiś czas te serwisy zostały zablokowane. Amerykańscy eksperci stwierdzili wtedy, że ataki te były testem skuteczności przeprowadzonym przez członków organizacji Hezbollah, a opinia publiczna zdała sobie sprawę, że ataki w cyberprzestrzeni stały się faktem[5]. W takich przypadkach niebezpieczne są głównie ataki osób z wewnątrz, które mając ułatwiony dostęp do celu ataku (np. poprzez pracę w danej firmie, instytucji), mogą z łatwością przeprowadzić uderzenie bądź ułatwić dostęp cyberterrorystom, a także ukryć ich działanie. Tą technikę wykorzystano także podczas ataku cybernetycznego w Estonii. Zmasowane ataki cyfrowe uderzyły w systemy informacyjne centralnych organów państwa, a także największych banków i mediów, co spowodowało ich niewydolność. Dowiedziono tym atakiem skuteczności wojny cybernetycznej, gdyż uderzono w starannie wybrane cele. Ataki typu DDoS zauważono również podczas ataków na polskie strony rządowe przeciw podpisaniu umowy dotyczącej porozumienia ACTA. Hakerom wystarczyły proste narzędzia, by zdobyć dostęp do informacji o pracy administracji publicznej, co dziś stanowi przecież informację krytyczną.

Kolejną z technik jest tzw. „web sit-in”. Polega ona na okupowaniu sieci w tym samym czasie przez dużą liczbę użytkowników, co powoduje brak możliwości lub utrudnienie wywołania strony. Zdarzenie takie miało miejsce chociażby w roku 2000, w czasie powstania palestyńskiego. Witrynę IDF, którą zwykle odwiedzało ok. 7 tysięcy Internautów tygodniowo, po wybuchu zamieszek zaczęło okupować blisko 130 tysięcy osób[6].

Następne narzędzie, tzw. „e-mail bombing", polega na wysyłaniu ogromnych ilości wiadomości pocztą elektroniczną, co powoduje przepełnienie skrzynek i uniemożliwienie otrzymywania innych, ważnych listów. Przykładem wykorzystania tej techniki może być atak separatystów tamilskich na serwery ambasad Sri Lanki w 1998r. Atak ten polegał na wysłaniu ok. 1 tysiąca e-maili dziennie przez okres dwóch tygodni i spowodował sparaliżowanie systemów informatycznych kilku ambasad państwa oraz systemu łączności Ministerstwa Spraw Zagranicznych Sri Lanki. Wiadomość zawierała oświadczenie w kwestii roszczeń niepodległościowych, a kończyła się informacją o celowości działań. Jej treść brzmiała: „Jesteśmy Internetowymi Czarnymi Tygrysami i zamierzamy uszkodzić wasz system łączności"[7]. Był to pierwszy znany atak terrorystyczny na rządowy system komunikacyjny. Choć w porównaniu z innymi działaniami terrorystycznymi efekt zalewania przeciwnika nadmiarem e-maili może się wydać znikomy, intencje atakujących mogą pozwolić na zrozumienie natury cyberterroryzmu.

Dość znanym narzędziem do walki w sieci są „bomby logiczne". Są to programy, które pozostają uśpione, aż do momentu uaktywnienia. Można powiedzieć również, że jest to pewien rodzaj wirusa, który po zainfekowaniu komputera przez długi czas może pozostać nieaktywny, do powstania jakiegoś niezwykłego zdarzenia. Uaktywnienie polega na zajściu pewnego zdarzenia lub obecności określonych danych albo ich braku. Zdarzeniem, które uruchamia ten program może być prawie wszystko - obecność odpowiednich plików, wybrany dzień tygodnia lub określona data. W momencie uaktywnienia „bomba logiczna" dostarcza swój ładunek, którym może być dowolne oprogramowanie destrukcyjne (np. kasowanie plików). Zniszczenie może być również bardzo rozległe, a biorąc pod uwagę, że współcześnie komputery kontrolują wiele systemów fizycznych, atak bombą logiczną może w efekcie mieć charakter ataku fizycznego[8]. Przykładem użycia bomby logicznej może być CIH (Czarnobyl) stworzony w Tajwanie w 1998 r., którego nazwa pochodzi od przypadkowej zbieżności daty aktywacji tej bomby logicznej z datą katastrofy atomowej w Czarnobylu, a który znalazł się na liście 20 największych zagrożeń komputerowych firmy Panda Security. Każdego roku od 1999 r., 26 kwietnia wirus zamazywał zawartość pamięci komputera uszkadzając BIOS. Już w pierwszym roku działalności w samej Azji doszło do uszkodzenia ok. 500 tysięcy komputerów. Na świecie ta liczba osiągnęła ponad 2 miliony. Dość niebezpieczny może być przypadek, kiedy bomby takie podkładane są przez informatyków mających legalny dostęp do systemu. Skutki takiego działania zauważono w firmie Omega wykonującej zamówienia rządu USA w postaci wyspecjalizowanych urządzeń elektronicznych dla marynarki wojennej. Bombę logiczną w komputerach firmy podłożył zwolniony informatyk pracujący w firmie, czym spowodował wielomilionowe straty - w postaci straconych zamówień, ale i kosztach odbudowy informacji w bazach danych (których usunięto 80 %)[9]. Bomby logiczne często wykorzystywane są wraz z wirusami. Wirus ma wtedy za zadanie rozpowszechnić bombę czekającą w systemie, aż do momentu nadejścia zaprogramowanego wcześniej uwolnienia jej zawartości. Wiele razy okazało się, że użycie takich bomb bywa skuteczne i może nieść destrukcyjne skutki również w instytucjach rządowych. W 1991 roku pracownik firmy będącej podwykonawcą Departamentu Obrony USA, który prowadził prace nad bazą danych części i dostawców dla systemu bojowego opracowanego dla rządu USA, umieścił bombę logiczną w bazach danych. Nie miała ona właściwie tworzonych kopii zapasowych, co pracownik chciał wykorzystać. Po jego odejściu z firmy bomba miała się uaktywnić, a powrócić miał on jako dobrze opła-

cany konsultant. W porę jednak – zupełnie przypadkowo – inny technik odkrył bombę, którą następnie „rozbroił”[10].

Kolejnym narzędziem, jakim mogą posługiwać się terroryści, są tzw. „konie trojańskie”. Trojanem jest program, który może wykonywać - nieprzewidziane przez użytkownika programu – niepożądane działania. Może on usuwać pliki, formatować dysk czy bez zgody lub wiedzy użytkownika przesyłać dane do innych miejsc. Można go umieścić niemal w każdym programie, a rozpowszechnia się go umieszczając w Internecie lub za pomocą poczty elektronicznej. Dzięki temu programowi hackerzy mogą nawet przechwytywać hasła[11]. Trojan jest doskonałym narzędziem dla organizacji terrorystycznych, gdyż jego główną zaletą jest to, że nie zwracając na siebie uwagi można penetrować zasoby informacyjne atakowanego obiektu.

„Tylne drzwi” są narzędziem dającym cyberterrorystom szerokie możliwości wykorzystania do realizacji swoich własnych celów. Jest to luka w zabezpieczeniach systemu komputerowego, która jest utworzona umyślnie w celu późniejszego wykorzystania[12]. Backdoor może być utworzony przez twórcę danego programu bądź poprzez uruchomienie przez użytkownika tzw. „Trojana”. Zazwyczaj pozostawiony jest w systemie przez intruza, który włamał się w inną lukę w oprogramowaniu.

Oprócz wcześniej omówionych, dość prostych narzędzi wykorzystywanych do ataków w cyberprzestrzeni, cyberterroryści dysponują bardziej wyrafinowanymi, wymagającymi specjalnej wiedzy i przygotowania technikami. Jedną z nich jest „spoofing”, który jest dość skomplikowany i może być stosowany wyłącznie przez specjalistów bądź doświadczonych włamywaczy. Mimo to jest niezwykle skuteczny. Polega na podszyciu się atakującego pod jednego użytkownika systemu, który posiada własny numer IP (numer identyfikujący użytkownika). Technika ta ma na celu omijanie wszelkich zabezpieczeń, jakie zastosował administrator w sieci wewnętrznej. Za pomocą tej techniki można udawać dowolnego użytkownika, czyli również wysyłać sfałszowane informacje. W 1995 r. na wielu stronach internetowych znaleźć można było informacje, że rząd meksykański zbombardował pewne miasto: „korytarze szpitala w Comitan były pełne trupów, a żołnierze gwałcili kobiety i mordowali dzieci”[13]. Dopiero jakiś czas później okazało się, że doniesienia były fałszywe. Inną, również trudną w użyciu techniką, jest „hijacking”. Atak ten polega na przechwyceniu transmisji odbywającej się między systemami, dzięki czemu możliwe jest uzyskanie dostępu do szczególnie chronionych programów lub informacji[14].

Metoda polegająca na śledzeniu ruchu w sieci to „sniffing”. Cyberterroryści za pomocą tej techniki mogą uzyskiwać dane osobowe, hasła dostępowe oraz wiele innych cennych informacji. W technice tej specjalne programy wychwytują wiadomości, które przemieszczają się w sieci, a wybrane z nich kopiują na dysk. Tropiciel umieszczony w dowolnym komputerze przyłączonym do sieci dzięki nowoczesnym technologiom może czytać niemal wszystkie przepływające przez sieć wiadomości[15]. Jednym ze scenariuszy zastosowania tej techniki mogłoby być (poprzez zainstalowanie na laptopie programu do przeszukiwania danych zwanego „snifferem”) zdobycie informacji o pasażerach samolotu. Informacje te w dalszym etapie posłużyć by mogły do uzyskania dostępu do systemu nadzorującego działanie sieci komputerowej linii lotniczych, co w efekcie przyczynić by się mogło nawet do załadowania bagażu, którego właściciela nie ma na pokładzie samolotu. Ta metoda umożliwia zatem terrorystom dostęp do szerokiego zasobu informacji, którymi w zależności od celu i motywu można by dowolnie manipulować.

Technika tzw. „phishing” polega na wyłudzaniu poufnych informacji osobistych (np. szczegółów

karty kredytowej bądź haseł) poprzez podszywanie się pod poważaną instytucję lub godną zaufania osobę. Popularnym celem ataku są banki czy aukcje internetowe. Amerykanie przyznali, że hakerzy zdołali się włamać do najbardziej zaawansowanego i najkosztowniejszego programu zbrojeniowego realizowanego przez Pentagon, czyli programu budowy myśliwców F-35. Intruzi zdołali skopiować i wyprowadzić dane m.in. na temat ułatwiających obronę przed potencjalnym atakiem z użyciem tego myśliwca systemów elektronicznych. W tym czasie doszło również do ataków na system kontroli lotów sił powietrznych USA. Obcy szpiedzy mogą infiltrować zatem komputery używane do kontroli infrastruktury, a w tym dystrybucji energii[16].

Social engineering (inżynieria społeczna) polega na wykorzystaniu niekompetencji osób mających dostęp do danych, które są potrzebne do dokonania ataków poprzez podszywanie się pod kogoś i tym sposobem zebraniu informacji. W swojej książce „Haker i samuraj" Jeff Goodel opisuje historię Kevina Mitnicka, który w swoich działaniach (oprócz oczywistych umiejętności informatycznych) wykorzystywał właśnie znajomość ludzkiej psychologii. Udowadnia tym samym, że często hakerzy nie marnują czasu na zgadywanie hasła otwierającego system komputerowy jakiejś korporacji, ale np. poprzez zatelefonowanie do administratorów i podając się za szefów o to hasło proszą[17]. Za pomocą tej techniki częściowo uzyskano dane do ataków podczas wcześniej omawianych ćwiczeń w Pentagonie.

Do bardzo nowoczesnych metod ataków w cyberprzestrzeni, których użyciem zainteresowani są terroryści, są „receptory van Eycka". Ta podsłuchowa technika polega na zdalnym przechwytywaniu i podglądaniu na oddzielnym monitorze repliki obrazów, które wyświetlane są na ekranie atakowanego komputera. Wykorzystywany jest do tego specjalistyczny sprzęt[18]. Niepokój specjalistów zajmujących się bezpieczeństwem informacji budzi również rozwój narzędzia, jakim jest „broń elektromagnetyczna". Broń tego typu emituje silny impuls elektromagnetyczny i zakłóca pracę urządzeń elektronicznych. Do broni tego typu zalicza się:

- EMP – broń elektromagnetyczna
- HMP - broń mikrofalowa
- HERF - broń radiowa

EMP – broń elektromagnetyczna (Elektro- Magnetic Pulses), tzw. „bomba E" jest to urządzenie, którego niszczące działanie polega na wysłaniu w krótkim czasie bardzo silnego impulsu elektromagnetycznego o wielkiej mocy. Może powodować zniszczenie lub poważne uszkodzenie systemów elektronicznych. Technologia odkryta została w roku 1870 i zdaniem ekspertów może być użyta przez terrorystów posiadających podstawowe wykształcenie techniczne lub inżynieryjne. Urządzenia te są łatwe do przenoszenia i można nimi zdalnie sterować. Ponadto, ataki te mogą być zaplanowane niezwykle precyzyjnie i z wyprzedzeniem, co daje terrorystom poczucie bezpieczeństwa i anonimowości[19]. Ataki za pomocą bomby E mogłyby sparaliżować działanie urządzeń komputerowych, komunikacyjnych, sieci energetycznych, systemów transportowych, ale również handlu – ponieważ nowoczesny sposób życia w głównej mierze zależy od sprawnego funkcjonowania urządzeń elektronicznych. Często broń ta jest nazywana kolejnym rodzajem broni masowego rażenia, a jej użycie jest jak najbardziej realnym zagrożeniem ze strony terrorystów. Z ich punktu widzenia EMP jest nawet łatwiejsza do zdobycia, ukrycia i transportu niż broń jądrowa, a również może okazać się skuteczna by spowodować straty gospodarcze które Osama Bin Laden określił jako cel działań wojennych[20].

Broń mikrofalowa HPM (High - Power Microwave) jest na razie w fazie testów, ale istnieje obawa, że jest już w posiadaniu terrorystów. HMP ge-

neruje impuls elektromagnetyczny mogący zniszczyć systemy elektroniczne, wyrzutnie rakietowe, systemy łączności. Może również unieruchomić pojazdy, nie czyniąc jednocześnie szkody ludziom ani budynkom. Co więcej, jej wielkość daje możliwość umieszczenia na pokładzie bezzałogowego samolotu czy w głowicy rakiety[21]. Użycie tej broni mogłoby być niezwykle skuteczne i spowodować oczekiwane rezultaty, gdyż nad wielkością i zasięgiem wybuchu można mieć kontrolę.

Do broni radiowej HERF (High Energy Radio Frequency) zaliczyć można urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego. Ataki polegają na użyciu energii elektromagnetycznej o dużej mocy w celu zakłócenia pracy urządzeń elektronicznych (których działanie opiera się na wykorzystaniu mikroelektroniki) lub uszkodzenia bądź zniszczenia tych urządzeń. Amerykańscy eksperci twierdzą, że terroryści mogli wejść w posiadanie tej broni, która wyprodukowana była w państwach byłego Związku Radzieckiego, z uwagi na niedoskonałości rosyjskiego systemu zabezpieczeń. Urządzenia tego typu były już stosowane np. przez Czeczenów do niszczenia rosyjskiego systemu komunikacji elektronicznej[23]. Ponadto, zarówno broń HERF jak i EMP została użyta podczas otwartych konfliktów w Kosowie oraz podczas wojny w Iraku.

Należy pamiętać, że nawet gdyby udało się „dobrać do skóry" jednej z organizacji terrorystycznych i wyeliminować całkowicie albo zmniejszyć zagrożenie płynące z ich strony, nie wyeliminuje to całkowicie zagrożenia w cyberprzestrzeni. Ktoś inny może bowiem wyszukać słabe punkty systemów i wykorzystać je do ataków. Bardzo ważne jest zatem zwalczenie słabości, które umożliwiają włamanie do systemu, ponieważ dopóki sobie z nimi nie poradzimy, dopóty będziemy narażeni na ryzyko ataków.

Uwagi końcowe

Współczesny terroryzm ma różne oblicza, a zagrożenia z nim związane nasilają się wraz z postępem technologicznym. Postęp ten sprawił, że ugrupowania terrorystyczne zaczęły stosować niekonwencjonalne metody walki. Jedną z nich jest stosowanie obecnie najgroźniejszej z nich – cyberterroryzmu. Zjawisko to przybiera wiele form, co sprawia, że stanowi problem trudny do zdefiniowania, jak i zwalczania. Cyberterroryzm jest zatem problemem, który stanowi jedno z najważniejszych wyzwań XXI wieku. Ataki w cyberprzestrzeni będą się stawały coraz częstsze, ponieważ funkcjonowanie każdego wysoko lub średnio rozwiniętego państwa jest uzależnione od prawidłowego działania w cyberprzestrzeni. Znaczenie Internetu i teleinformatycznej infrastruktury krytycznej jest tak ogromne we współczesnym świecie, że stały się one najbardziej wrażliwym i kluczowym elementem odpowiedzialnym za sprawne funkcjonowanie całego państwa. Świadczy o tym nasilająca się liczba ataków dokonanych na komputery administracji i wojska. Zamachy z 11 września 2001 roku udowodniły, że nawet mała, lecz dobrze zorganizowana grupa osób przy odpowiedniej motywacji, dysponująca odpowiednim zapleczem technologicznym i finansowym jest w stanie wpłynąć na praktycznie całą infrastrukturę państwa. Atakiem cyberterrorystycznym może być zagrożone każde państwo, a szkody będą tym większe, im bardziej skomputeryzowana jest jego gospodarka.

Należy pamiętać, że już dziś ataki cyberterrorystyczne są jak najbardziej realne, a niedługo mogą stać się powszechnym sposobem rozwiązywania konfliktów. W przyszłości nowoczesne armie będą mogły wykorzystywać cyberprzestrzeń nawet do prowadzenia działań mających na celu unieszkodliwienie infrastruktury krytycznej państw. W porównaniu do klasycznych metod terrorystycznych, koszty prze-

prowadzenia ataku w cyberprzestrzeni są nieporównywalnie niższe. Zakłócone jest postrzeganie zagrożenia, nie wiadomo czy jest realne, czy wirtualne. Co więcej, trudne jest wykrycie ataku, który można przeprowadzić z każdego miejsca na świecie. Zaatakowany może być więc również każdy obiekt na całym globie. Ze szczegółowej analizy istoty cyberterroryzmu wynika, że o zjawisku tym możemy mówić, gdy Internet jest celem bądź narzędziem w rękach terrorystów. Oznacza to, że terroryści wykorzystując technologie informatyczne coraz częściej posiadają wiedzę na temat celów, mogą przeprowadzać kampanie propagandowe, zdobywać fundusze, rekrutować nowych członków, a za pomocą Internetu mogą dokonywać ataków na wszelkie obiekty infrastruktury krytycznej.

Oprócz tego, że Internet może być celem i narzędziem w rękach terrorystów, jest także miejscem, gdzie tworzy się obronę przeciw atakom. Z przykrością należy jednak stwierdzić, że aktywność Polski w zapewnieniu bezpieczeństwa cyberprzestrzeni i zwalczaniu cyberprzestępczości jest niewielka. Dotyczy to zarówno dostarczania wiedzy i doświadczeń na ten temat, jak i wykorzystania wiedzy. Najpoważniejszym problemem jest fakt, że zjawiska cyberterroryzmu nie można zwalczyć fizycznymi metodami. Ponieważ celami ataków mogą stać się zarówno urządzenia podlegające władzom, jak i będące częścią gospodarki prywatnej, eliminacja ich potencjalnych słabości wymaga ścisłej koordynacji wysiłków każdego z tych sektorów. Państwo powinno większy nacisk nałożyć na zapewnienie bezpieczeństwa w sieci. Receptą na zmianę takiego stanu rzeczy jest rygorystyczne i konsekwentne prowadzenie polityki bezpieczeństwa teleinformatycznego oraz zatrudnienie specjalistów znających techniki hackerskie, którymi zwykle posługują się cyberterroryści. Specjaliści ci powinni być jednak już na początku rzetelnie zweryfikowani celem sprawdzenia ich wiarygodności i lojalności w wykonywanej pracy.

Pomimo, iż funkcjonowanie społeczeństw coraz częściej uzależnione jest od sprawnego funkcjonowania systemów teleinformatycznych, należy pamiętać, że obecnie nie istnieje bezpieczny system tego rodzaju. Zjawisko ataków w sieci, w tym cyberterroryzm, będzie się stawało coraz powszechniejsze i częstsze. Dynamiczny rozwój systemów informatycznych sprawia, że sieć jest świetnym miejscem, w którym mogą działać terroryści. Może zatem być niezwykle szkodliwym zjawiskiem zarówno dla społeczeństwa i prawidłowego rozwoju działalności gospodarczej, jak i infrastruktury krytycznej państwa, a bezpieczeństwo w cyberprzestrzeni jest jednym z najważniejszych obecnych wyzwań.

Przypisy

1 M.F. Gawrycki, Cyberterroryzm..., dz. cyt., s. 145.
2 Tamże, s. 146-147.
3 Biuro Bezpieczeństwa Narodowego, Terroryzm cybernetyczny..., dz. cyt., s. 3.
4 D. Verton, Black ice..., dz. cyt., s. 154.
5 http://www.sgh.waw.pl/instytuty/ism/materialy/CYBERTERRORYZM%202007.pdf, z dnia 15.06.2012.
6 A. Chorobiński, Walka informacyjna... dz. cyt., s. 3.
7 D. Verton, Black ice..., dz. cyt., s. 67.
8 D.L. Pipkin, Bezpieczeństwo informacji, Wydawnictwo Naukowo – Techniczne, Warszawa 2002, s. 53.
9 J.K. Wójcik, Zagrożenia w cyberprzestrzeni..., dz. cyt., s. 4.
10 D.L. Pipkin, Bezpieczeństwo informacji, s. 54.
11 M.F. Gawrycki, Cyberterroryzm..., dz. cyt., s. 149.
12 Słownik terminów dotyczących bezpieczeństwa komputerowego, [z:] http://www.tp.pl/prt/pl/tpcert/bezpieczenstwo/zagrozenia/zlosliwe_programy/zlosliwe_programy_inne?_a=670081, z dnia 15.06.2002.
13 A. Pietrzak, Światowy terroryzm, Magazyn globalizacji i integracji europejskiej nr 6/ listopad 2002r. – Glob@lizator.
14 M.F. Gawrycki, Cyberterroryzm..., dz. cyt., s. 151.
15 D. Denning, Wojna informacyjna..., dz. cyt., s. 210.
16 http://www.wprost.pl/ar/159323/Wlamanie-do-najdrozszego-programu-Pentagonu/.
17 J. Goodell, Hacker i samuraj, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1996, s. 29.
18 R. Białoskórski, Cyberzagrożenia..., dz. cyt., s. 85.
19 D. Verton, Black ice..., dz. cyt., s. 151-153.
20 Tamże, s. 153.
21 http://kopalniawiedzy.pl/bomba-mikrofalowa-HPM-wirkator-generator-mikrofale-impuls-elektromagnetyczny,7303.
22 D. Denning, Wojna informacyjna..., dz. cyt., s.289.
23 M.F. Gawrycki, Cyberterroryzm..., dz. cyt., s.157.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 6/2012 (6)]

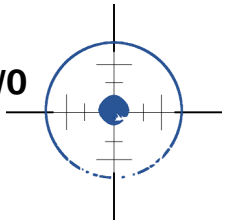
TOBIASZ MAŁYSA

Informatyczna infrastruktura krytyczna i jej ochrona prawna

Rozwój oznacza postęp, czyli najczęściej technologie i ich upowszechnianie się. Związane są z tym nowe wyzwania, które stają oko w oko z dotychczasowym stanem i pojmowaniem bezpieczeństwa państw oraz społeczeństw. Jednym z takich wyzwań jest zwrócenie uwagi na bezpieczeństwo tzw. infrastruktury krytycznej. Wyodrębniamy ją bowiem coraz częściej spośród pozostałych krajowych obiektów. Infrastruktura ta i związane z nią obiekty nie pozostają w izolacji od zmieniającego się świata i również czerpią szerokimi garściami z postępu technologicznego. Co za tym idzie, w wyniku poszerzającej się informatyzacji tych obiektów i włączaniu ich do ogólnoświatowej sieci informacyjnej – Internetu – pojawia się kolejne wyzwanie. To sprawa zapewnienia bezpieczeństwa tym obiektom od strony informatycznej.

Powszechna informatyzacja to nie zaledwie sam rozwój dostępu do Internetu. To jeszcze większa obecność komputerów połączonych siecią, w wielu instytucjach państwowych, pozarządowych oraz przedsiębiorstwach. Dziś ich informacje są składowane nie tylko w formie papierowej, zajmując miejsce w przepastnych archiwach; ilości danych niemożliwe do oszacowania są już przechowywane w postaci cyfrowej na podobnie niezliczonych serwerach. Sieć internetowa pozwala na szybką i łatwą ich wymianę pomiędzy uprawnionymi instytucjami. Również obywatele coraz chętniej poprzez komputer załatwiają wiele swoich urzędowo-administracyjnych spraw, które wcześniej wymagały złożenia bezpośredniej wizyty w odpowiedniej placówce. A przeniesienie działalności urzędów administracji i ich kontaktu z petentami do Internetu, jest tylko jednym z wielu w praktyce już funkcjonujących przykładów informatyzacji działania państwa. Z tym wszystkim wiąże się i wzrost umiejętności informatycznych ogółu społeczeństwa, gdzie jeszcze więcej osób posiada i poznaje wiedzę na temat rzeczywistych prawideł funkcjonowania różnych systemów, dowiadując się tak o ich mocnych i pożytecznych aspektach, jak i tych słabych i możliwych do wykorzystania tylko we własnym interesie. W XXI wieku przy niewielkim wysiłku przecież niemal każdy może stać się zarówno sprawnie poruszającym się w cyberprzestrzeni człowiekiem, jak i groźnym dla innych cyberprzestępcą-hackerem. W jaki sposób to wszystko przekłada się więc na bezpieczne funkcjonowanie całego państwa? Czym są elementy informatycznej infrastruktury krytycznej, jakie istnieją dla niej zagrożenia? Jak zapobiegać i przeciwdziałać zagrożeniom?

Artykuł, podzielony na trzy kolejno następujące po sobie części, poświęcony jest próbie odpowiedzi, co należy rozumieć poprzez bezpieczeństwo informatycznej infrastruktury krytycznej. Jest to chęć wyjaśnienia jakie awarie, ataki czy inne zdarzenia mogą zakłócić jej funkcjonowanie, i jaka jest organizacja jej ochrony wraz z niektórymi regulacjami prawnymi. W części pierwszej podjęty został cel opisania czym jest infrastruktura krytyczna oraz jej informatyczna część, co się na nią może składać, jaka jest jej charakterystyka i jakie są podstawy prawne jej ochrony. Część druga wyjaśni z jakimi zagrożeniami może spotkać się informatyczna infrastruktura krytyczna. W części trzeciej i ostatniej, opisane zostaną praktyczne sposoby i proces ochrony tej infrastruktury, zaczynając od form instytucjonalno-organizacyjnych, po fazy obrony oraz praktyczne środki zaradcze. Ważnym aspektem podczas pisania było zwrócenie uwagi na zagadnienie cyberterroryzmu, i rozpatrywania go jako jednego z niebezpieczeństw grożących informatycznej infrastrukturze krytycznej, stąd wyróżnienie tej kwestii w tytule artykułu. Przedstawione zostaną zarówno poglądy zaczerpnięte z literatury, opinie ekspertów na ten temat, jak też własne uwagi oraz komentarze autora.



Informatyczna infrastruktura krytyczna państwa i jej ochrona prawna.

Czym jest infrastruktura krytyczna? Polska *Ustawa o zarządzaniu kryzysowym* rozumie przez to pojęcie „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[1].

Według ustawy, infrastruktura krytyczna obejmuje systemy:

- Zaopatrzenia w energię i paliwa;
- Łączności i sieci teleinformatycznych;
- Finansowe;
- Zaopatrzenia w żywność i wodę;
- Ochrony zdrowia;
- Transportowe i komunikacyjne;
- Ratownicze;
- Zapewniające ciągłość działania administracji publicznej;
- Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochronę infrastruktury krytycznej, wedle ustawy rozumieć należy jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”[2].

W Ustawie o ochronie osób i mienia wymienia się obszary i obiekty podlegające obowiązkowej ochronie. Również *Rozporządzenie RM z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony* wylicza szereg takich obiektów. Wśród przykładów wskazuje się na strategicznie ważne zakłady produkcyjne i magazyny, zapory wodne, obiekty telekomunikacyjne, porty morskie i lotnicze oraz inną infrastrukturę transportowo-logistyczną, a także większe banki, i obiekty elektro-energetyczne.

Wszystko, czego uszkodzenie bądź zniszczenie może drastycznie zagrozić funkcjonowaniu państwa na jakimś jego obszarze, jest więc obiektem infrastruktury krytycznej. Przeciwieństwem są tzw. obiekty miękkie, jak centra handlowe, miejsca rozrywki, czy edukacji oraz miejsca pracy, których uszkodzenie lub zniszczenie także wywierałoby negatywne skutki, ale, nie ograniczało w istotnym stopniu działania i bezpieczeństwa państwa.

Można podzielić infrastrukturę krytyczną ze względu na formę własności albo miejsce zlokalizowania, wyróżniając:

- Cywilną lub wojskową;
- Prywatną albo państwową;
- Rządową lub pozarządową;
- Krajową albo zagraniczną;

Lub też, mówić o ogólnej infrastrukturze krytycznej, albo szczególnej, takiej jak:

- Logistyczna (transport, przesył, zaopatrzenie);
- Energetyczna (dostawy energii);
- Zasoby (surowce);
- Administracyjna (zarządzanie i kierowanie);
- Informatyczna (informatyka, telekomunikacja).

Takich kryteriów może być więcej, zależnie od potrzeb. Informatyczna infrastruktura krytyczna jest jednym z jej elementów.

Informatyczna infrastruktura krytyczna i jej rodzaje

Obecna *Ustawa o zarządzaniu kryzysowym* „nie definiuje pojęcia krytycznej infrastruktury teleinformatycznej państwa i w żaden sposób nie rozpatruje jej specyfiki"[3].

W listopadzie 2004 r. zespół ds. Krytycznej Infrastruktury Teleinformatycznej powołany przez premiera stwierdził, że „systemy i sieci teleinformatyczne, których nieprawidłowe funkcjonowanie lub uszkodzenie - niezależne od przyczyn i zakresu - może spowodować istotne zagrożenie dla życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę"[4] to infrastruktura krytyczna.

E. Lichocki, w opracowaniu *Cyberterrorystyczne Zagrożenie Dla Bezpieczeństwa Teleinformatycznego Państwa Polskiego* wymienia następujące szczególnie narażone na cyberataki teleinformatyczne i teleinformacyjne systemy:[5]

- Kontrola ruchu lotniczego (lotniska cywilne);
- Nadzór ruchu statków (VTS Gdynia, VTS Gdańsk i VTS Szczecin - Świnoujście);
- Łączność cywilna oraz łączność wojskowa (teleinformatyczna, teleinformacyjna i satelitarna);
- Teleinformatyka wykorzystująca komercyjne linie transmisyjne (zwłaszcza bazy danych osobowych);
- Powiadamianie służb ratowniczych i reagowania kryzysowego;
- Teleinformatyka stosowana w sektorze bankowości i finansów.

Uderzenie w takie systemy może być w skutkach katastrofalne dla funkcjonowania państwa. Nie będą to jedyne możliwe rodzaje infrastruktury informatycznej, których zniszczenie lub uszkodzenie takie może mieć takie skutki. W zasadzie, niemal każdy obiekt infrastruktury krytycznej posiada jakieś systemy informatyczne. Jeśli za obiekt taki uznajemy na przykład gazociąg, to atak na komputery nim sterujące może doprowadzić do zmian ciśnienia i w konsekwencji wybuchów oraz poważnych zniszczeń[6]. Podobnie, każdy inny obiekt infrastruktury krytycznej posiada wrażliwe informatycznie elementy, a ich ilość oraz zasięg zależne są od jego funkcji.

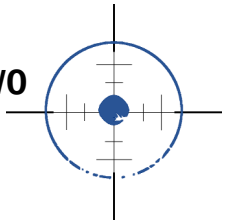
Według K. Baniaka, „Krytyczną infrastrukturą telekomunikacyjną (KIT) nazywamy zespół sieci oraz struktur komunikacyjnych, które uszkodzone lub zniszczone, w sposób istotny wpłynęłyby na funkcjonowanie państwa (społeczeństwa)"[7].

Wśród przykładowych systemów wchodzących w skład krytycznej infrastruktury teleinformatycznej, inny autor, Grzegorz Krasnodębski w opracowaniu *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego* wymienia takie rzeczy jak:[8]

- Systemy ewidencyjne;
- Systemy finansowe;
- Systemy bankowe;
- Systemy logistyczne;
- Systemy medyczne;
- Systemy transportowe;
- Systemy administracji państwowej;
- Systemy bezpieczeństwa;
- Systemy zarządzania kryzysowego.

Omawiany wcześniej Ernest Lichocki, w innym swoim opracowaniu *Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa* podaje[9] taki podział tej infrastruktury, z umiejscowieniem w niej i teleinformatyki:[10]

1. Energia;
2. Woda;
3. Transport;



4. Systemy i technologia teleinformacyjna, łączność, ICT (Technologia informacyjno- komunikacyjna):
   - sieci teleinformatyczne, oprogramowanie, procesy i ludzie dbające o prawidłowe działanie i bezpieczeństwo. Instalacje służące pierwotnemu przechowywaniu i składaniu danych;
   - Systemy automatyki (SCADA, itd.);
   - Internet;
   - Stacjonarne systemy telekomunikacyjne. Centrale telefoniczne;
   - Mobilne systemy telekomunikacyjne (telefonia komórkowa);
   - Łączność i nawigacja radiowa;
   - Łączność i nawigacja satelitarna;
   - Systemy powiadamiania (Broadcasting);
5. Zdrowie;
6. Żywność;
7. Bankowość i finanse;
8. Administracja państwowa;
9. Narodowe pomniki i pamiątki;
10. Istotny przemysł gospodarki;
11. Wymiar sprawiedliwości;
12. Przestrzeń kosmiczna, eksploracja kosmosu;
13. Kluczowe zasoby.

Ten sam autor, z punktu widzenia natomiast Sił Zbrojnych RP, problematykę opisuje w pracy *Bezpieczeństwo danych w krytycznej infrastrukturze teleinformatycznej* wskazując, że „krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polski (KITI SZ RP) obejmuje systemy teleinformatyczne i teleinformacyjne niezbędne dla prowadzenia podstawowych działań i prawidłowego funkcjonowania Sił Zbrojnych RP”[11]. Wśród szeregu innych czynników istotnych dla ogólnej infrastruktury krytycznej Sił Zbrojnych (takich jak woda, energia, transport, żywność, administracja, przemysł) wymienia też rzeczy takie jak „systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność”, oraz, technologię komunikacyjno-informacyjną, i wchodzące właśnie w skład KITI[12].

Zapoznając się z tym opracowaniem, możemy w składzie wojskowej krytycznej infrastruktury teleinformatycznej wyliczyć:[13]

- Satelitarne i radiowe systemy nawigacyjne;
- Systemy Dowodzenia i Kierowania Obronnością Sił Zbrojnych (Państwa);
- Systemy Kierowania Systemami Walki;
- Systemy kontroli i naprowadzania lotnictwa;
- Systemy łączności cyfrowej;
- Systemy łączności radiowej;
- Systemy łączności satelitarnej;
- Systemy opto-elektroniczne techniki bojowej;
- Systemy powiadamiania (Broadcasting);
- Systemy rozpoznania;
- Systemy teleinformatyczne, bazy danych, oprogramowanie;
- Stacjonarne i mobilne systemy telekomunikacyjne (sieci wymiany informacji);
- Zautomatyzowane Systemy Dowodzenia.

Charakterystyka informatycznej infrastruktury krytycznej

Pojęcia „informatyczna”, „teleinformatyczna” oraz „telekomunikacyjna” odnoszące się do wyszczególnienia infrastruktury krytycznej można używać zamiennie na potrzeby niniejszego artykułu, jako synonimy. Z drugiej strony, ustawowe uściślenie i ujednolicenie pojęć oraz klasyfikacji tego co wchodzi w skład infrastruktury krytycznej i na co się ona dzieli, byłoby pożądane, na co zwraca uwagę wielu autorów. W końcu technicznie można byłoby podzielić informatyczną infrastrukturę krytyczną na telekomunikacyjną, bazo-danową, obliczeniową, użytkową, itd. To przecież zarówno informatyka, jak i tele-komunikacja oparta na informatyce oraz inne wykorzystanie elektroniki i komputerów. Mogą to

być też warstwy sprzętu czy oprogramowania oraz urządzeń pomocniczych, które wciąż można odpowiednio dzielić. Stąd, konieczne w pracach nad programami jej ochrony jest przemyślane i jasne sklasyfikowanie wszystkich składowych.

Z wcześniejszych rozważań można wysunąć chyba wniosek, że samo ogólne pojęcie informatycznej infrastruktury krytycznej może być rozpatrywane dwojako. Albo, będzie to infrastruktura sama w sobie ogromnie zinformatyzowana, taka jak telefonia komórkowa (której całkowita awaria wywołałaby poważne skutki), lub stanowić będzie tylko element tej infrastruktury nie najważniejszy dla jej funkcjonowania (np. komputerowe systemy przesyłowe w gazociągu), lecz nadal ogromnie istotny dla jego bezpieczeństwa i działania. Informatyczna infrastruktura krytyczna jest więc albo sektorem wśród wielu innych infrastruktur (obok energii, transportu, administracji, itp.), albo tylko elementem każdego z tych sektorów, bo trudno wyobrazić sobie funkcjonowanie niemal ich wszystkich, bez systemów informatycznych. Zależności ciekawie przedstawiają autorzy projektu *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016*, uznając, że informatyczna infrastruktura krytyczna pozostając elementem infrastruktury krytycznej jest także „częścią cyberprzestrzeni o krytycznym znaczeniu dla jej (infrastruktury krytycznej) funkcjonowania”[14].

Ostatecznie, to i sam Internet będzie w tym rozumieniu infrastrukturą krytyczną. Poważny atak na działanie sieci mógłby być paraliżujący w efektach dla nowoczesnego społeczeństwa i gospodarki oraz bardzo wielu obiektów infrastruktury krytycznej.

Czym różni się zapewnianie bezpieczeństwa infrastrukturze krytycznej państwa, od zabezpieczania podobnie działających systemów informatycznych, ale nie będących już infrastrukturą krytyczną? Wydaje się, że w sprawach technicznych zajdzie przede wszystkim rozszerzenie skali użycia i skomplikowania stosowanej informatyki. Wszystkie instytucje eksploatujące postęp informatyczny, będą przecież korzystały z elektroniki i komputerów, serwerów, stacji roboczych, przewodów i metod przesyłu danych oraz używały oprogramowania i nośników informacji.

W przypadku infrastruktury krytycznej, często rozbudowanej, zmienią się co najwyżej rodzaje oprogramowania na bardziej specjalistyczne, ilość oraz moc obliczeniowa, albo rozmiary baz danych w których składowane są informacje. Zwiększa się zatem stopień rozbudowania całego systemu informatycznego, oraz komplikuje sprawa odpowiedniego jego zabezpieczenia. Większe są i wymagania prawne co do zakresu ochrony. Jednak co do spraw czysto technicznych, związanych z zagrożeniami oraz sposobami przeciwdziałania i zapobiegania, można bardzo często – choć nie zawsze – mówić o tym samym.

To co więc dobrze zabezpiecza mało ważny system informatyczny, może być dobre i do zabezpieczania znacznie poważniejszego systemu, ale samo może okazać się niedostateczne. Żeby zabezpieczyć zwykłe komputery, najczęściej wystarczy dobre oprogramowanie antywirusowe, zapora sieciowa, i przestrzeganie odpowiednich reguł. Te same wskazówki należałoby dać administratorom komputerów i systemów wchodzących w skład infrastruktury krytycznej, lecz zastosować oprogramowanie bardziej profesjonalne, a procedury bezpieczeństwa rozszerzyć i to istotnie. I nadal nie będzie to wszystko co trzeba zrobić, aby dobrze zabezpieczyć system infrastruktury krytycznej, prawie zawsze o wiele bardziej skomplikowany od tych systemów, które infrastrukturą krytyczną nie są. Czy zatem to co stanowi optimum zabezpieczeń dla zwykłej infrastruktury informatycznej, nie jest absolutnym minimum dla tych systemów, które są niezbędne lub ogromnie ważne dla funkcjonowania

państwa? Zmienia się jeszcze i skala zagrożenia, oraz możliwe ich źródła. Układem sterowania światłami na skrzyżowaniu któregoś z powiatowych miast, zainteresuje się w najlepszym razie cybernetyczny wandal, albo któryś z przestępców, dopatrzywszy się w tym być może metody na łatwiejszą ucieczkę w chaosie po rabunku. Czy w miejsce takie natomiast, chętnie uderzą cyberterroryści? Co innego, komputerowe systemy zarządzające przesyłem energii elektrycznej, w odróżnieniu od poprzedniego przykładu wchodzące już w skład informatycznej infrastruktury krytycznej. Atak na takie ważne węzły mógłby nawet na kilka dni niemal całkowicie pozbawić energii elektrycznej znaczną część kraju, wywołując bardzo złowieszcze skutki. Należy zauważyć przy tym, że z reguły, wraz ze skalą zagrożenia, rośnie stopień zabezpieczenia danego systemu, ograniczając znacznie szanse i źródła potencjalnego skutecznego uderzenia. Ataku na infrastrukturę krytyczną raczej nie dokona amator, a jeśli, świadczyć to będzie o tragicznie niskim poziomie zabezpieczenia jej.

Podsumowując, dla zapewniania bezpieczeństwa informatycznej infrastrukturze krytycznej czerpanie z doświadczeń ochrony zwykłych systemów informatycznych będzie słuszne, jednak należy wziąć solidną poprawkę uwzględniając znaczenie tego, co się zabezpiecza.

Ochrona prawna

W jaki sposób informatyczne systemy niezbędne dla funkcjonowania państwa, lub których uszkodzenie mogłoby wywołać fatalne dla niego skutki, są chronione w prawie?

Po pierwsze, należałoby zwrócić uwagę, że z reguły prawo odnoszące się do ochrony ogólnej infrastruktury krytycznej oraz ochrony przed terroryzmem, a także cyberprzestępczością, będzie miało wpływ na bezpieczeństwo informatycznej infrastruktury krytycznej. Dlatego właśnie prawne kwestie zarządzania kryzysowego, zwalczania przestępczości zorganizowanej oraz terroryzmu, są tym co może nas interesować. Wybór pod tym względem okazuje się bardzo szeroki, więc trzeba ograniczyć się do wyliczenia najistotniejszych kwestii, związanych z tematem – czyli ochroną informatycznej infrastruktury krytycznej.

Z konwencji międzynarodowych mających znaczenie dla bezpieczeństwa teleinformatycznego, a których stroną jest Polska, warto wymienić następujące dokumenty:[15]

- Konwencja o zwalczaniu cyberprzestępczości RE z dnia 23 listopada 2001 r. (ETS No. 185);
- Decyzja Rady Ministerialnej OBWE nr 3/04 z dnia 7 grudnia 2004 r., nr 7/06 z 5 grudnia 2006 r. w sprawie działań związanych ze zwalczeniem wykorzystywania Internetu do celów terrorystycznych.

Unia Europejska przyjęła własne prawa i dokumenty, mające organizować ochronę infrastruktury krytycznej, w tym, zwrócenie uwagi na informatyczną ich część. Z inicjatyw UE należy wymienić tu tzw. zieloną księgę w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (2005), komunikat KE w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (2006), i w 2008 roku dyrektywę w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz potrzeb w zakresie poprawy jej ochrony.

Oto z kolei polskie ustawy oraz rozporządzenia, najistotniejsze[16] dla tematu rozważań:

- Ustawa z dnia z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926 ze zm.);

- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. nr 128, poz. 1402);
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz.1800, z późn. zm.);
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm.);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego Dz.U.2011.159.948
- Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29 lipca 2008 roku w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Rządowy Program Ochrony Cyberprzestrzeni RP

Jeżeli chodzi o praktyczne rozwiązania prawne w Polsce, najbardziej interesujące wydają się *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009 – 2011* (RPOC) oraz projekt tego dokumentu, na lata 2011 - 2016 (obecnie w wersji 1.1).

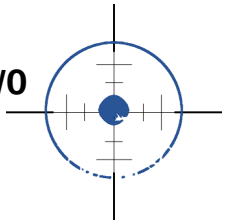
Jak czytamy w projekcie programu, jego przedmiotem „są propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Program nie obejmuje swoim obszarem zadaniowym niejawnych sieci i systemów teleinformatycznych. Należy podkreślić, że obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych w wydzielonych systemach i sieciach teleinformatycznych. Podstawowym dokumentem prawnym jest ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz.1631 z późn. zm.)."[17]

Adresatami tego projektu, oprócz organów władzy publicznej w postaci administracji rządowej i samorządowej oraz państwowej, są i „operatorzy infrastruktury krytycznej, których działalność jest zależna i nie zależna od prawidłowego funkcjonowania cyberprzestrzeni"[18].

Na temat operatora infrastruktury krytycznej w projekcie napisano, że jest to „właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, wyodrębnionych w systemie łączności i sieci teleinformatycznych i ujawnionych w wykazie infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym"[19]. Krytyczna infrastruktura teleinformatyczna natomiast, rozumiana jest jako „wyodrębniona w systemie łączności i sieciach teleinformatycznych i ujawniona w wykazie Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym". Za realizację celów programu, odpowiadają również, odpowiednio co do swoich kompetencji i „przedsiębiorcy – właściciele zasobów stanowiących krytyczną infrastrukturę teleinformatyczną państwa"[20]. Program można moim zdaniem uważać za konkretny krok do przodu w dziedzinie zabezpieczania infrastruktury krytycznej w Polsce. To zwrócenie uwagi na jej informatyczną jej stronę oraz źródło zagrożeń i konieczność ochrony.

Zostańmy na koniec tej części, przy polskim prawie karnym. Mimo wszystkich podstaw prawnych wyżej wymienionych, brakuje w nim jasnej definicji cyberterroryzmu[21]. Można jedynie wymieniać ogół przestępstw komputerowych albo o charakterze terrorystycznym. Według RPOC, w kodeksie karnym ściganie przestępstw komputerowych dotyczy:[22]

- Przestępstw przeciwko Rzeczypospolitej Pol-



skiej (Rozdział XVII),
- Przestępstw przeciwko bezpieczeństwu powszechnemu (Rozdział XX),
- Przestępstw przeciwko ochronie informacji (Rozdział XXXIII),
- Przestępstw przeciwko wiarygodności dokumentów (Rozdział XXXIV),
- Przestępstw przeciwko mieniu (Rozdział XXXV).

Wszystkie z tych czynów „mogą być potraktowane jako akty terroru, jeżeli ich charakter odpowiadać będzie ustawowej definicji przestępstwa mającego charakter terrorystyczny ustalonej w art. 115 § 20 kk”[23].

Ochrona infrastruktury krytycznej przed uszkodzeniem (także w wyniku działań cyberterroryzmu) podlega również Ustawie o zarządzaniu kryzysowym, która nakłada na administrację publiczną obowiązki takie jak[24] zapobieganie sytuacjom kryzysowym i przygotowanie do przejmowania nad nimi kontroli, reagowanie w przypadku ich wystąpienia, usuwania skutków takich sytuacji oraz odtwarzania infrastruktury krytycznej.

Przypisy

1 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).
2 Tamże.
3 Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, s. 10. Warszawa, marzec 2009. Źródło online: [http://www.cert.gov.pl/download.php?s=3&id=40], dostęp: 2011-12-27.
4 zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego”, Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [„http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznejinfrastruktury krytycznejwdobierozwojuspoleczenstwainformacyjnego.doc”], dostęp: 2011-12-30.
5 Por. E. Lichocki, „Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego", Centrum Symulacji i Komputerowych Gier Wojennych Akademii Obrony Narodowej, Źródło online: [http://www.csikgw.aon.edu.pl/index.php/pl/pobieranie/Publikacje/Cyberterrorystyczne-zagrożenie- dla-bezpieczeństwa-teleinformatycznego-państwa-polskiego-PAN-Warszawa-2008./] Dostęp: 2011-12-26.
6 Tamże.
7 K. Baniak, „Analiza zagrożeń telekomunikacyjnych sektora publicznego”. Źródło online: [http://www.bbn.gov.pl/download.php?s=1&id=1000], dostęp: 2011-12-26.
8 Zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego”, Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznej infrastrukturykrytycznejwdobierozwojuspoleczenstwainformacyjnego.doc], dostęp: 2011-12-30.
9 E. Lichocki, „Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa”, s. 156-158 [w:] „Ochrona infrastruktury krytycznej”, red. Tyburska Agata. Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010.
10 Opracowane przez E. Lichockiego na podstawie: Trusted Information Sharing Network for Critical Infrastructure Protection in Australia, Australia 25 March 2003 r., Zielona księga w sprawie europejskiego programy ochrony infrastruktury krytycznej, COM/2005/576 końcowy, Bruksela, 17 listopada 2005 r. oraz K. Liedel, P. Piasecka, „Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej”, Warszawa 2007.
11 E. Lichocki, „Bezpieczeństwo danych w krytycznej infrastrukturze teleinformatycznej”, s. 3.
12 Tamże, s. 1-2.
13 Tamże, s. 2-3
14 Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016, projekt, wersja 1.1, s. 12. Warszawa, czerwiec 2010. Źródło online: [http://bip.msw.gov.pl/download.php?s=4&id=7445], dostęp: 2011-12-27.
15 Za: Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Wersja 1.1, s. 10. Źródło online: [http://bip.msw.gov.pl/download.php?s=4&id=7445], dostęp: 2011-12-26.
16 Tamże.
17 RPOC na lata 2011-2016..., s. 5.
18 Tamże, s. 8.
19 Tamże, s. 6.
20 Tamże, s. 9.
21 Zob. A. Baworowski, „Cyberterroryzm w prawie karnym materialnym - przyczynek do dyskusji na gruncie analizy dogmatycznej”. Źródło online: [http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/ Cyberrteroryzm/baworowski.pdf], dostęp: 2011-12-26.
22 Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, s. 9. Warszawa, marzec 2009. Źródło online: [http://www.cert.gov.pl/download.php?s=3&id=40], dostęp: 2011-12-27.
23 Tamże, s. 9.
24 J. Świątkowska, I. Bunsch. „Cyberterroryzm - nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku”, s. 4-5. Brief Programowy Instytutu Kościuszki. Źródło online: [http://ik.org.pl/pl/publikacja/nr/4298/], dostęp: 2011-12-26.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 7/2012 (7)]

TOBIASZ MAŁYSA

Zagrożenia dla informatycznej infrastruktury krytycznej

Kto zagraża informatycznej infrastrukturze krytycznej, i w jakich formach zagrożenie to może się manifestować? Najprościej podzielić zagrożenia tak jak każde inne, wymieniając[1] wśród nich naturalne (żywioły) oraz techniczne (usterki). Zagrożenia mogą pochodzić też z działalności ludzkiej, świadomej i nieświadomej, w wyniku popełnianych błędów czy zaniedbań. W tym artykule to działalność ludzi będzie przedmiotem największego naszego zainteresowania. Ludzie mogą być członkami większej grupy albo działać samotnie. Będą mieć mocodawców lub inspiratorów, a niekiedy sami dla siebie okażą się sterem i okrętem. Staną się członkami grup o charakterze terrorystycznym lub o profilu przestępczo–zarobkowym. Być może, jako indywidualni komputerowi geniusze działać będą na własne konto, uznając włamanie się do ściśle chronionego systemu infrastruktury krytycznej za wyzwanie godne siebie i swoich umiejętności.

Cyberwojna

Nie możemy zapominać o atakach innych państw na systemy informatyczne ważne dla funkcjonowania kraju. Atak nie musi wcale nadejść od strony organizacji terrorystycznej. Agresorem może okazać się sąsiad, pozostający w przeciwnym bloku militarnym, a poprzez swoje działania (często ukryte) będzie chciał zademonstrować swoją siłę lub osłabić gospodarkę i system obronny przeciwnika. Skutki takiego ataku mogą być podobne do tego przeprowadzonego przez terrorystów. Ważne zaznaczenia jest, że państwa podejmujące cyberataki z reguły posiadają lepsze od terrorystów środki i ataki mogą być groźniejsze, z większymi następstwami. Z drugiej strony, ewentualne międzynarodowe i dyplomatyczne konsekwencje takiego ataku mogą prowadzić do konieczności zacierania śladów, co może ograniczać jego zasięg. Bowiem, w przeciwieństwie do grup terrorystycznych, państwa podejmujące cyberataki zazwyczaj nie będą chciały nagłaśniać ich medialnie i oficjalnie się pod nimi podpisywać.

Do jednego z pierwszych cyberataków w dziejach doszło w 2007 roku w Estonii[2]. W ciągu kilku tygodni ataki zakrojone na szeroką skalę uderzyły na strony internetowe i serwery parlamentu, ministerstw, policji oraz inne obiekty, paraliżując ich działanie w sieci. Celem agresji stały się również prywatne firmy, w tym dwa największe banki które zostały zmuszone do zawieszenia swoich usług.

Jak podsumował J. Jaloen, „życie zwykłego obywatela zostało więc zakłócone jedynie nieznacznie. Ale lęk przed tym, co mogłoby się stać, gdyby cyberataki były silniejsze i szerzej zakrojone, pozostał. Estonia jest bowiem krajem wysoce zinformatyzowanym, a banki, usługi, administracja i nawet system głosowania są ze sobą powiązane. Łatwo sobie wyobrazić, jakie skutki mógłby mieć skoncentrowany atak, wspierany przez pełne zasoby jakiegoś kraju”[3]. Stroną atakującą byli najprawdopodobniej rosyjscy cyberwandale. Nie udało się ustalić ich związków z rosyjskim rządem.

Podobne zdarzenia nastąpiły rok później, podczas rosyjskiej wojny z Gruzją. Wiele informatycznych systemów tego zakaukaskiego kraju zostało wtedy sparaliżowanych[4]. Być może, do oznak cyberwojny można zakwalifikować również uderzenie wirusa Stuxnet na irańskie instalacje programu atomowego[5]. Zdarzenie to może wydać się bardzo interesujące, w kontekście omawiania zagrożeń cyberterrorystycznych dla infrastruktury krytycznej. W końcu, czy irańskie instalacje atomowe nie są infrastrukturą krytyczną tego kraju?

Cyberprzestępcy

Jak wspominano wcześniej, istotnym zagrożeniem dla infrastruktury krytycznej mogą być również cyberprzestępcy. Ich ataki jak dotąd obejmują głównie podszywanie się pod internetowe strony bankowe. Wyłudzanie od ich klientów haseł umożliwia dostęp do kont oraz pieniędzy.

Na czym jeszcze mogą skoncentrować się oni, atakując sektor bankowy? Według autora opracowania „Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego”[6], ich celami mogą być bank centralny, komercyjne banki, centra rozliczeniowe w tym dla kart kredytowych, sieci bankomatowe i terminale POS oraz giełdy i systemy płatnicze. Dalej zdaniem autora, ataki skutkować mogą: „zakłóceniem swobodnego przepływu środków pieniężnych, zafałszowaniem danych dotyczących bieżącej sytuacji gospodarczej i finansowej, manipulowaniem notowaniami kursowymi bądź giełdowymi, odebraniem firmom i osobom prywatnym bieżącego dostępu do zgromadzonych środków, zafałszowaniem informacji dotyczących poziomu zadłużenia, oraz kradzieżą i legalizacją znacznych sum”. J. Syta podsumowuje, że „wszystkie z powyższych ataków mogłyby zachwiać stabilnością gospodarki. W niesprzyjających okolicznościach mogłyby stać się pretekstem do histerii i związanych z nią gwałtownych ruchów jak na przykład przecena akcji czy masowe wypłacanie środków z rachunków bankowych”. Jest to zatem zagrożenie bardzo poważne.

Cyberterroryści

Jeden z ostatnich ataków, który można uznać za cyberterrorystyczny nastąpił 21 listopada 2011 roku w USA. Grupa hakerów dokonała tego dnia zdalnego włamania do stacji uzdatniania wody w stanie Illinois, wyłączając pompę odpowiedzialną za jej uzdatnianie[7]. Choć zagrożenia tego nie można jeszcze uznać za przynależące do grup o najwyższym stopniu niebezpieczeństwa, uświadamia to możliwości specjalistów w zakresie ataku na obiekty niezbędne dla funkcjonowania kraju, a więc te które są jego infrastrukturą krytyczną. Zamiast podkładać ładunek wybuchowy pod istotny cel, żeby poważnie zakłócić albo uniemożliwić jego działanie, wystarczy włamać się do jego systemów komputerowych nawet z drugiego końca świata.

Natomiast, co do możliwych scenariuszy cyberterrorystycznych ataków, ciekawe opracowanie autorstwa Joanny Jedel dotyczy zagrożenia dla morskich centrów logistycznych. Przykładem stało się Pomorskie Centrum Logistyczne. W pracy, autorka zwraca uwagę na istotę takich centrów dla współczesnej logistyki oraz gospodarki, a także stopień ich zależności od systemów informatycznych mogących być celem ataku. Skutki paraliżującego uderzenia mogłyby być bardzo kosztowne. Jak napisała autorka, „ewentualny atak terrorystyczny w cyberprzestrzeni na Pomorskie Centrum Logistyczne może stworzyć ogromne zagrożenie i straty w wymiarze ekonomicznym, finansowym i społecznym. Udany cyberatak terrorystyczny na centrum logistyczne może spowodować odejście inwestorów, nadawców i odbiorców towarów z regionu i przeniesienie ich w inne miejsca, a tym samym straty finansowe. Skuteczny cyberatak na port morski, który pełni funkcję centrum dystrybucji, spowoduje brak wiarygodności Polski jako partnera zabezpieczającego wymianę handlową na arenie międzynarodowej”[8]. Nadmieńmy, że jest to tylko jedno z możliwych miejsc, gdzie mogą zaatakować cyberterroryści.

Czym jest informatyczny atak terrorystyczny? Według dr inż. Tomasza Bąka polegać może on na włamaniach, paraliżowaniu dróg przepływu informacji bądź manipulacji nimi, albo zniszczeniu tych informacji lub elektronicznej destrukcji systemu informacyjnego[9]. Dodaje on, że „ataki na systemy informacyjne mogą

być połączone z innymi rodzajami ataków terrorystycznych”[10], a nawet, że mogą być one wstępem do zasadniczych ataków. Dodajmy, że równie dobrze cyber–atakiem wymierzonym w infrastrukturę krytyczną może być też kradzież niejawnych informacji, ważnych dla bezpieczeństwa kraju, a przechowywanych w systemach bazo–danowych odpowiednich służb czy agencji. Zagrożenia uderzające w bezpieczeństwo informatycznej infrastruktury krytycznej to więc nie tylko niszczenie, zaburzanie bądź utrudnianie jej funkcjonowania, ale także, wykorzystywanie zdobyczy ataku z niesieniem szkody dla bezpieczeństwa państwa.

W swojej książce „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie” Bógdał–Brzezińska i Gawrycki przyjmują za to następującą definicję cyberterroryzmu: „politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów”.

Inne definicje przytacza T. Szubrycht, w opracowaniu „Cyberterroryzm jako nowa forma zagrożenia terrorystycznego”. Wśród wymienianych przez niego definicji kilku różnych autorów najciekawszą moim zdaniem jest, że cyberterroryzm to: „wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań (wg James Lewis)”[11].

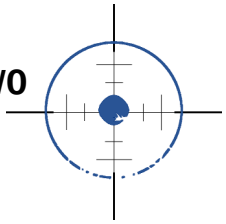
Hakerzy i cyberwandale

Z reguły, hakerzy koncentrują się na mniej destruktywnych celach niż opisane powyżej, a ich działań nie można zaliczyć do terrorystycznych. Ataki najczęściej dotyczą podmian wyglądu stron internetowych, albo usuwania danych i ich kradzieży. Są to więc działania zbliżone do wandalizmu, podpadające raczej pod wykroczenia i kodeks karny, a zatem bezpieczeństwo publiczne, aniżeli państwowe.

Przy omawianiu hakerów jako zagrożenia dla infrastruktury krytycznej, nie można jednak subiektywnie uznawać wszystkich z góry jako cyberwandali. Wielu zdolnych geniuszy komputerowych włamuje się głównie po to, aby pokazać własne umiejętności, ukazując zarazem administratorom serwerów błędy popełniane przez nich w zabezpieczeniach. Pod pewnymi względami może to być działalność społecznie pozytywna, bo wydobywa niedostatki zawodowców. Jednocześnie, dodatkowe zagrożenie w postaci hakerów może mobilizować administratorów do lepszego zabezpieczania serwerów, którymi się opiekują. Z drugiej strony, nawet niedestruktywna bezpośrednio działalność hakerska, będąc nieodpowiedzialną, naraża zaatakowane systemy na dalsze niebezpieczeństwo wskazując ich słabości, możliwe do wykorzystania już przez naprawdę groźne grupy i jednostki. Rzadko zdarza się, aby strona danej instytucji po ataku była nadal funkcjonalna dla osób chcących z niej skorzystać. Pomimo czasem nie do końca złych chęci, hakerzy łamiąc zabezpieczenia, łamią obowiązujące prawo.

Charakterystyka zagrożeń

Różnica pomiędzy grupami jest nieznaczna, jeśli chodzi o metody. Gdy wszystkie strony będą wykorzystywały w działaniach luki w zabezpieczeniach, inne okażą się cele. Cyberprzestępcy chcą się wzbogacić, cyberterroryści raczej wykorzystają posiadane fundusze do przeprowadzenia ataku o możliwie najbardziej katastrofalnych skutkach. Podczas kiedy cyberprzestępców zaciekawią głównie te dziedziny w których będą mogli osiągnąć zysk, pośrednio lub bezpośrednio, cybeterroryści nie będą „wybrzydzać”. Każdy sektor



infrastruktury krytycznej potencjalnie leżący w zasięgu ręki, może ich zainteresować. Nie można mimo wszystko wykluczyć i ataku zarobkowego ze strony ugrupowań terrorystycznych. Dotyczyłoby to np. systemów bankowych. Inne mogą być też rozmiary cyberataku. Osobną grupę stanowią hakerzy – zazwyczaj indywidualne osoby, nie współpracujące z żadną organizacją. W swoich działaniach kierują się głównie medialnością skutków, albo znaczeniem ich osiągnięcia dla środowisku w którym funkcjonują. Skutki są trudne do przewidzenia. Może być to działalność przestępcza, ale równie dobrze czysto popisowa. Celem ataku komputerowego geniusza może być zarówno niezmiernie ważny dla funkcjonowania kraju system, jak i ten niewiele istotny. Może on być w następstwach destrukcyjny, a równie stanowić jedynie osobisty podpis bez efektów wandalizmu, swoiste zatknięcie chorągiewki na systemie uważanym za trudnym do zdobycia, czyli kolejne osiągnięcie. Ponadto hakerzy to atrakcyjni specjaliści do wykorzystania przez cyberprzestępców i cyberterrorystów, mogą być więc przez nich werbowani i wykorzystywani.

Klasyfikacja ataków

Autorzy amerykańskiego raportu „Cyberterror: prospects and implications" (z Centre for the Study of Terrorism and Irregular Warfare w Monterrey), wymieniają trzy poziomy zagrożenia cyberterrorystycznego, które przytaczam za opracowaniem „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie"[12]:

Przy pierwszym stopniu zagrożenia, nazywanym *simple–unstructured* cyberterroryści dokonują włamań o małym stopniu trudności, do indywidualnych systemów informacyjnych, stosując narzędzia internetowe stworzone przez innych (np. hackerów, cyberprzestępców).

Drugi poziom, to *advanced structured* – ataki wycelowane są w bardziej złożone systemy, a narzędzia których używają, są tworzone lub modyfikowane przez nich.

Ostatni, najwyższy stopień, nazywany jest *complex–coordinated*. W tym przypadku, uderzenie jest skoordynowane, i ma na celu zupełną destrukcję zintegrowanego systemu obronnego, przy pomocy narzędzi tworzonych samodzielnie.

Raport, powstały w roku 1999, przewidywał, że terroryści mieli osiągnąć zdolność poziomu II do roku 2003, a uderzenia o najwyższym poziomie zagrożenia, być w stanie wykonywać już od lat 2005–2009[13].

Inna klasyfikacja amerykańskich specjalistów z Monterey, dotyczyła grup mogących dokonać cyberataku. Wymienia się w niej[14] grupy: rewolucyjne, religijne, new–age, separatystów etno-nacjonalistycznych i ekstremistów prawicowych. Charakter tych działań może być wieloraki, od form po prostu bezprawnych, po hakerstwo, szpiegostwo, cyberterroryzm, kończąc na cyberagresji[15]. Z kolei kategorie działań w cyberprzestrzeni, mogą według P. Neumanna i D. Parkera dotyczyć[16]:

- przeglądania i kradzieży informacji,
- fałszowania danych,
- zniszczenia informacji,
- podszywania się pod kogoś innego,
- zainstalowania złośliwego programu,
- złamania haseł,
- celowego złego zarządzania systemem,
- używania innych systemów do stworzenia „złośliwych" programów.

Oba cytowane opracowania, tj. A. Bógdał–Brzezińskiej i M. Gawryckiego oraz T. Szubrychta, uznają powyższą klasyfikację za najbardziej pełną, bo zezwalającą na klasyfikację wielu różnych ataków, choć nie jest to według nich lista idealna.

Incydenty możliwe w cyberprzestrzeni opisuje J. Siwek, w opracowaniu „Cele sił zbrojnych – zdolność reagowania na incydenty komputerowe", wyliczając:[17]

- ataki kodów złośliwych,
- wtargnięcie do systemu,
- nieautoryzowane wykorzystanie usług,
- odmowa lub przerwanie wykonania usługi,
- nadużycie,
- szpiegostwo,
- złośliwe dowcipy, fałszywe informacje.

Na podstawie witryny internetworldstats.com, G. Krasnodębski sporządził natomiast następującą listę zagrożeń dla krytycznej infrastruktury teleinformatycznej[18]:

- starzenie się technologii, czas życia programów,
- niewłaściwa ochrona,
- nieświadomość zagrożeń,
- błędy i luki,
- nielojalni pracownicy,
- programy szkodliwe,
- modyfikacja,
- uszkodzenie.

Z kolei E. Lichocki w artykule „Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa" wymienia następujące rodzaje zagrożeń[19]:

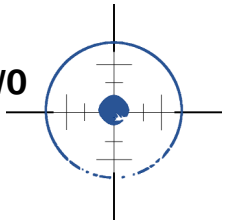
- fizyczne ataki na obiekty, które są składnikami tej infrastruktury,
- cyberataki z cyberprzestrzeni ukierunkowane na informację, systemy teleinformatyczne oraz systemy zarządzania infrastrukturą krytyczną,
- zagrożenia związane z bezpieczeństwem infrastruktury,
- zagrożenia związane z przyjętymi rozwiązaniami projektowymi infrastruktury i architekturą,
- zagrożenia związane z eksploatacją infrastruktury,
- zagrożenia związane z ilością i rodzajem transportowanego medium.

Jeszcze inaczej niebezpieczeństwa wymienia A. Adamski, opisując trzy formy ataków[20]:

- propagandowo–dezinformacyjne, czyli modyfikacja stron www, i/lub powielanie na wielką skalę treści ideologicznych,
- komputerowy sabotaż, paraliż systemów oraz inne metody destrukcji funkcji oprogramowania,
- fizyczne zamachy na informatyczną infrastrukturę krytyczną w celu jej zniszczenia.

Metody i technika ataków

Jakie są praktyczne metody i sposoby wykorzystywane podczas omawianych wcześniej ataków na systemy informatyczne? W publikacji „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie" autorzy wymieniają szereg możliwych do zastosowania agresywnych technik. Przykładowo, atakujący może podszyć się pod wybrany komputer bądź stronę internetową czy aplikację, przechwytując dzięki temu istotne dla siebie dane, które same w sobie mogą być celem albo posłużą żeby dokonać ataku głębiej. Zamiast podszywania się, można po prostu podsłuchiwać strumień informacji przesyłanych w sieci, jeśli w odpowiednim miejscu ustawi się urządzenie zwane snifferem lub zainstaluje tego typu oprogramowanie na komputerze w podsłuchiwanej sieci. Równie dobrze, na komputerze wybranym jako cel ataku można zamieścić oprogramowanie wirusowe, szpiegujące czy umożliwiające przejęcie zdalnej kontroli nad jego systemem. Jakie skutki może taka udana próba wywrzeć na całokształcie bezpieczeństwa obiektu infrastruktury krytycznej, jeśli jeden z komputerów jej pracowników stanie się w ten sposób dostępny dla atakującego?



Istnieją metody wykorzystujące błędy w oprogramowaniu systemów operacyjnych i użytkowanych aplikacji. Niemal w każdym oprogramowaniu są luki, które odkryte, mogą stać się źródłem włamania i instalacji szkodliwych programów, które dadzą dalszy dostęp agresorowi. Czasami to błędy niezamierzone, innym razem tego typu tylnie drzwi były celowo zostawione na etapie pisania programu dla pożytecznych celów, a następnie o nich zapomniano. Metody ataku mogą wynikać także z ograniczeń technicznych stosowanego oprogramowania, gdy przez atakującego zaczyna być ono używane w sposób, w jaki nie przewidział jego twórca i odpowiednio do takich rzadkich wypadków nie zabezpieczył.

Niekiedy wystarcza tylko odpowiednia inżynieria społeczna. Jest to takie wykorzystanie pracowników instytucji, aby przekonani o słuszności swoich działań dostarczyli atakującemu tego, czego potrzeba mu do ataku. Można to osiągnąć poprzez podszywanie się pod innych pracowników, rozbudzając zaufanie.

Niszczyć można też fizycznie. Aby wyłączyć z działania komputer nie trzeba wysadzać go w powietrze, wystarczy użycie bomb z impulsem elektromagnetycznym. Tego typu ataki mogą być szczególnie groźne, ponieważ trwale niszczą sprzęt, a ochrona przed nimi jest dość kosztowna.

Zagrożenia w Polsce

Kwartalne i roczne raporty[21] publikowane przez CERT.GOV.PL – Rządowy Zespół Reagowania na Incydenty Komputerowe, działający przy Agencji Bezpieczeństwa Wewnętrznego dobrze uświadamiają skalę cybernetycznego zagrożenia dla Polski. W roku 2010 zespół odnotował 621 zgłoszeń pochodzących od obiektów państwowych, a 155 z nich zakwalifikowano jako rzeczywiste incydenty[22]. Większość z nich, stanowiło skanowanie systemów oraz działania administratorów. Występowała kradzież tożsamości z podszywaniem się, nieuprawnione zmiany informacji oraz ataki wirusami. Agresja wydająca się najbardziej groźna, czyli paraliżujące ataki typu DoS/DDoS, włamania na konta uprzywilejowane oraz nieuprawniony dostęp do informacji były w mniejszości. Odnotowano też trzy przypadki oprogramowania szpiegowskiego.

Niemal 40% ataków pochodziło z Chin, a jedna czwarta z USA. Ataki z Rosji stanowiły 7% wszystkich, a pochodzące z Polski klasyfikowały się na piątym miejscu z udziałem 5%. Ponad co dziesiąty atak nie mógł zostać namierzony[23].

Wśród instytucji które najsłabiej zabezpieczały swoje strony internetowe, wymieniono m. in. Rządowe Centrum Legislacji, Polską Agencję Rozwoju Przedsiębiorczości i Centralny Ośrodek Geodezji i Kartografii. W testach oraz ocenach obok lokalnych izb skarbowych i jednej prokuratury najlepiej wypadło Centrum Obsługi Kancelarii Prezesa RM[24].

Raport stwierdza, iż w porównaniu do lat wcześniejszych „zaobserwowano również znaczne przesunięcie obszaru działań nielegalnych w cyberprzestrzeni (z aktów czysto kryminalnych, na ataki o charakterze szpiegowskim lub noszące znamiona cyberwojny). Oznacza to przesunięcie problematyki bezpieczeństwa teleinformatycznego z obszaru ochrony bezpieczeństwa i porządku publicznego (za którego ochronę, zgodnie z art. 29 ust. 1 pkt 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej odpowiada MSWiA oraz podległe mu służby), do obszaru ochrony bezpieczeństwa państwa”[25]. Wśród głównych zagrożeń we wnioskach wymieniono „ataki ukierunkowane na użytkowników sieci administracji publicznej, mające charakter szpiegostwa komputerowego – wykonywane za pomocą niebezpiecznych załączników poczty elektronicznej i nacechowane elementami inżynierii społecznej”[26]. Ogólny poziom bezpieczeństwa polskiej cyberprzestrzeni uznano za niewystarczający.

Jakie więc awarie, ataki, i inne zdarzenia, mogą zakłócić funkcjonowanie informatycznej infrastruktury krytycznej? Scenariusz możliwych wypadków jest bardzo szeroki. Obiekty takie bądź ich informatyczne urządzenia mogą zostać:

- sparaliżowane zupełnie w swoim funkcjonowaniu w cyberprzestrzeni,
- sparaliżowane na pewnym tylko wycinku swoich działań w cyberprzestrzeni,
- ograniczone w swoim ogólnym funkcjonowaniu bez paraliżu,
- zagrożone paraliżem i/lub ograniczeniem bez widocznych i negatywnych dla działania skutków.

Aby osiągnąć któryś z tych stanów, strona atakująca może dokonać:

- kradzieży danych/informacji lub manipulacji nimi albo zniszczenia ich,
- technicznego ograniczenia funkcjonalności systemów informatycznych lub funkcjonalności ich oprogramowania,
- zapoczątkowania procesów szkodliwych dla działania infrastruktury albo nawet dla niej destrukcyjnych,
- fizycznego zniszczenia systemów informatycznych i elektronicznych lub ważnych dla nich elementów.

W celu realizacji tych przedsięwzięć, możliwy do zastosowania wachlarz sposobów, metod i technik jest bardzo szeroki. Te które zostały wcześniej wymienione mogą wcale nie wyczerpywać wszystkich istniejących możliwości.

Należy pamiętać, że uczestnictwo zewnętrznego agresora wcale nie musi być niezbędnym czynnikiem, do zaistnienia zagrożenia. Awarie i nieprawidłowe funkcjonowanie mogą wynikać z błędu ludzkiego, bądź z niezawinionych przyczyn technicznych. Źle zaprojektowane lub zainstalowane urządzenie albo oprogramowanie może popsuć się i pociągnąć za sobą fatalne dla całego systemu skutki. Także błąd ludzki może przynieść szkody, poprzez bezmyślne lub nieumiejętne użytkowanie tego typu systemów. Teleinformatyczna infrastruktura krytyczna może znaleźć się w paraliżu lub ograniczeniu swojego koniecznego działania również w sytuacji, gdy nastąpią takie zmiany warunków oraz środowiska w którym ona funkcjonuje, do jakich jej nie przygotowano.

Przypisy

1 Por. K. Liedel, Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa, s. 10–11, Warszawa 2010.
2 Zob. J. Jaloen, „Dni, które wstrząsnęły Estonią", eesti.pl. Źródło online: [http://www.eesti.pl/index.php?dzial=panstwo&strona=cyberataki], Dostęp: 2011–12–29.
3 Tamże.
4 Zob. Cyberataki na Gruzję. Działania CERT Polska. Cert.pl. Źródło online: [http://www.cert.pl/news/866] Dostęp: 2011–12–29.
5 W. Lorenz, „Cyberatak nowej generacji na Iran", rp.pl. Źródło online: [http://www.rp.pl/artykul/541272.html] Dostęp: 2011–12–29.
6 Zob. J. Syta, Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego, [w:] Cyberterroryzm – nowe wyzwania XXI wieku, Praca zbiorowa Jemioła T., Kisielnicki J. i Rajchel K. [red.], Warszawa 2009, str. 696–703.
7 Za: „Hakerzy grają z wodą. Jaki będzie kolejny cel?", interia.pl. Źródło online: [http://nt.interia.pl/internet/wiadomosci/news/hakerzy–igraja–z–woda–jaki–bedzie–kolejny–cel,1724354,62] Dostęp: 2011–12–20.
8 J. Jedel, „Cyberprzestrzeń nową płaszczyzną zagrożeń terrorystycznych dla morskich centrów logistycznych". Zeszyty Naukowe Akademii Marynarki Wojennej. Rok XLIX Nr 2 (173) 2008.
9 T. Bąk, „Terroryzm zagrożeniem bezpieczeństwa świata i Polski", s. 14. [w:] Oblicza terroryzmu / pod red. Tomasza Bąka. – Kraków: Konsorcjum Akademickie – Wydawnictwo WSE w Krakowie, WSIiZ w Rzeszowie i WSZiA w Zamościu, 2011.
10 Tamże.
11 Zob. T. Szubrycht, „Cyberterroryzm jako nowa forma zagrożenia terrorystycznego", s. 175, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1 (160) 2005. Źródło online: [http://www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Szubrycht_T.pdf].
12 Za: A. Bógdał–Brzezińska, M. Gawrycki – „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie", s. 87. Warszawa 2003.
13 Tamże, s. 87.
14 Tamże.
15 Zob. T. Szubrycht, „Cyberterroryzm jako nowa forma..." op. cit., s. 177.
16 Tamże, s. 181.
17 J. Siwek, "Cele sił zbrojnych – zdolność reagowania na incydenty komputerowe", s. 3–4. Źródło online: [http://www.cert.pl/PDF/secure2003/siwek.pdf] Dostęp: 2011–12–29.
18 Zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego", Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznej infrastrukturykrytycznejwdobie-rozwojuspoleczenstwainformacyjnego.doc] Dostęp: 2011–12–30.
19 E. Lichocki, „Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa", s. 159 [w:] „Ochrona infrastruktury krytycznej", red. Tyburska Agata. Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010.
20 A. Adamski, „Cyberterroryzm". Wydział Prawa i Administracji UMK w Toruniu, Katedra Prawa Karnego i Polityki Kryminalnej. [za:] Syta J., „Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego". [w:] „Cyberterroryzm – nowe wyzwania XXI wieku", Praca zbiorowa Jemioła T., Kisielnicki J. i Rajchel K. [red.], Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009, str. 696–703.
21 Zob. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Źródło online: [http://cert.gov.pl/download.php?s=3&id=121] Dostęp: 2012–01–01.
22 Tamże, s. 7.
23 Tamże, s. 11.
24 Tamże, s. 20.
25 Tamże, s. 50.
26 Tamże.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 8/2012 (8)]

TOBIASZ MAŁYSA

Zapobieganie i przeciwdziałanie zagrożeniom informatycznej infrastruktury krytycznej

Proces zapobiegania zagrożeniom bezpieczeństwa systemów informatycznych jest złożony. Zagrożenia można oddalać, albo minimalizować ich skutki, gdy już wystąpią. Istotne okaże się zarówno podnoszenie odporności systemów informatycznych na ataki jak i przeciwdziałanie potencjalnym źródłom zagrożenia. Dosyć trudne z samej natury musi być zapobieganie atakom cyberprzestępców, i cyberterrorystów, co wynika z uwarunkowań działania oraz formowania się takich grup. Są to organizacje zamknięte oraz ukryte. Przenikanie do nich agentów–funkcjonariuszy służb jest bardzo utrudnione o ile w ogóle możliwe. Ciężko wykorzystać ich informatyczne talenty na własny użytek. Niemniej, działania na etapie rozpracowywania i unieszkodliwiania tych grup są konieczne.

Wydaje się, że najprościej zapobiegać atakom typowo hakerskim, choć jednocześnie najmniej groźnym. Można osiągnąć to na etapie szkolno-edukacyjnym. Wyławiając talenty informatyczne i oferując im dalszy zawodowy rozwój mogłoby zniechęcić ich do łamania prawa. Czy nie można ich użyć jako cywilnych specjalistów od zabezpieczeń? Tym, którzy poszukują kolejnych systemów do łamania, w celu osiągania pozycji w hakerskim środowisku, można zaproponować coś innego. Będzie to prestiżowa praca w zespołach chroniących kraj przed cyberatakami. Potrzebne są na to pieniądze i dobrze działający program. Należy wziąć pod uwagę, że rodzimi hakerzy mogą zostać użyci przeciwko własnemu krajowi przez organizacje przestępcze lub terrorystyczne. Mogą podjąć płatną współpracę w pełni świadomi jej charakteru, mogą też być wykorzystani, nie do końca znając prawdziwe przeznaczenie swojej pracy. Tym bardziej zwrócenie uwagi na to, co dzieje się na „własnym podwórku", może być dla bezpieczeństwa niezwykle istotne. Osłabianie terrorystycznego i przestępczego przeciwnika w jego wnętrzu to za mało. Potrzebne jest umacnianie własnych sił obronnych. Inną sprawą jest zapobieganie i przeciwdziałanie naturalnym zagrożeniom, technicznym i tym wynikającym z ludzkiego błędu. Dobre przygotowanie może wiele pomóc, a uwzględnianie wszystkich możliwych scenariuszy, z mierzeniem dostępnych sił i zasobów na zamiary, jest konieczne.

Zorganizowane formy ochrony

Wśród zorganizowanych form zapobiegania zagrożeniom informatycznej infrastruktury krytycznej, można wymienić kilka interesujących przykładów. Jednym z nich jest IMPACT – Międzynarodowe Wzajemne Partnerstwo Przeciwko Cyber-Terroryzmowi (International Multilateral Partnership Against Cyber-Terrorism). To organizacja non-profit, oparta na partnerstwie publiczno-prywatnym. Działalność koncentruje się na organizowaniu szkoleń z zakresu bezpieczeństwa informatycznego, wydawaniu certyfikatów, oraz wspierania badań w tym zakresie. Przy IMPACT działa również Globalne Centrum Odpowiedzi[1], na sytuacje kryzysowe z dziedziny zagrożeń cybernetycznych, mające oferować pomoc rządom, które znajdą się w niebezpieczeństwie.

Podobnych, czysto cywilnych zagranicznych instytucji można opisać wiele. ITU (International Telecommuniactions Union), prowadzona przez ONZ. To wyspecjalizowana agencja ds. cyberbezpieczeństwa[2]. W jej ramach powołano plan GCA, czyli Global Cybersecurity Agenda, mający między innymi działać na rzecz standaryzowania i wprowadzania skutecznych rozwiązań dla cyberbezpieczeństwa, czy współpracy międzynarodowej z innymi instytucjami.

Również organizacje militarne działają na tym polu. NATO posiada własne Centrum Cyberobrony w Tallinie, do którego niedawno przystąpiła Polska. W jego ramach sojusz może wysyłać grupy szybkiego reagowania złożone ze specjalistów tam, gdzie zajdzie taka potrzeba ze względu na zagrożenie. NATO chce także wdrożyć system NCIRC (NATO Computer Incident Response Capability) mający podnieść bezpieczeństwo sojuszu.

Polska zobowiązała się w ramach NATO i UE przyłączyć do obrony cyberprzestrzeni, rozbudować własne odpowiedniki zagranicznych instytucji mogące z nimi współpracować. Z naszych struktur wojskowych mających wpływ na ochronę informatycznej infrastruktury krytycznej można wymienić System Reagowania na Incydenty Komputerowe resortu obrony narodowej (SRnIK)[3]. W jego skład wchodzą Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki w Warszawie oraz Centrum Zarządzania Systemami Teleinformatycznymi. Jednym z zadań jest współpraca z NCIRC Sojuszu.

CERT to Zespół Reagowania na Incydenty Komputerowe. Jego zadania to całodobowe monitorowanie cyberprzestrzeni oraz podejmowanie akcji w razie niebezpieczeństw. Wiadomości na temat ich wystąpienia mogą pochodzić z własnych systemów wykrywania, albo ze zgłoszeń napływających od zaatakowanych instytucji. Zespoły publikują raporty ze swojej działalności i rekomendacje na rzecz bezpieczeństwa, pełnią więc również rolę edukacyjno-szkoleniową.

W Polsce, oprócz CERT-u w ramach SRnIK działa Rządowy Zespół Reagowania na Incydenty Komputerowe[4], a także CERT Polska[5] w ramach NASK (Naczelny Administrator Sieci Komputerowych) i CERT Telekomunikacji Polskiej[6].

Jakich narzędzi, inicjatyw oraz programów ochronnych używać mogą wymieniane instytucje? W projekcie „Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2016" wymienia się pięć takich programów-inicjatyw. Pierwszy to ABUSE-FORUM, stanowiący nieformalną grupę ekspertów skupiającą przedstawicieli jednostek CERT oraz specjalistów wchodzących w skład zespołów zapewniających bezpieczeństwo przedsiębiorcom telekomunikacyjnym.

Drugi system to ARAKIS. Pod jego nazwą kryje się Agregacja, Analiza i Klasyfikacja Incydentów Sieciowych. ARAKIS stanowi system wczesnego ostrzegania przed zagrożeniami w sieci, wykrywając anomalie a więc odchylenia od statystycznej normy. Jest to polski projekt, zespołu CERT Polska z NASK. Dla współpracy z ABW uruchomiono rządową implementację nazywaną ARAKIS-GOV.

Ciekawymi projektami są HSN (HoneySpider Network) oraz Wombat, budujące i wykorzystujące tzw. HoneyPoty. W dosłownym tłumaczeniu, są to garnki z miodem, czyli pułapki mające na celu zwabienie oraz wykrycie potencjalnego agresora. Włamywacz sądzi, że dokonuje włamania na interesujący go obszar, a w rzeczywistości działa w sposób izolowany i kontrolowany, umożliwiając swoje wykrycie, a co najmniej ma utrudnione możliwości wyrządzenia prawdziwych szkód.

Z kolei, projekt Virustotal prowadzony przez firmę Hispasec ma na celu gromadzenie największej na świecie bazy wszelkiego złośliwego oprogramowania, w celu prowadzenia na nich badań i analiz. Dla potrzeb współpracy europejskiej, planuje się za to opracować system EISAS, który stanie się ogólnoeuropejskim forum informacyjnym, umożliwiając ostrzeganie przed zagrożeniami i wymianę informacji dotyczących bezpieczeństwa.

Z innych ciekawych inicjatyw, warto wspomnieć projekt National Cyber Range[7]. Jest to budowana kosztem 130 mld $ przez Stany Zjednoczone symulacja środowiska światowego Internetu, do zastosowań symulacji cyberwojny. Używając takiej symulacji, dzięki cyber-poligonowi można przetestować różne scenariusze ataków cyberterrorystycznych na sieć, dzięki czemu łatwiej dopracuje się odpowiednie systemy i strategie obrony przed nimi.

Stany Zjednoczone współpracują także z Europą w obronie cyberprzestrzeni. W listopadzie ub. r., Departament Bezpieczeństwa Wewnętrznego USA wraz z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA) rozpoczął pierwsze europejsko-amerykańskie ćwiczenia w cyberbezpieczeństwie[8], nazwane Cyber Atlantic 2011[9]. W ćwiczeniach tych sprawdzano dwa scenariusze. Pierwszy z nich dotyczył usiłowania kradzieży i publikacji poufnych informacji z instytucji oraz agencji zapewniających bezpieczeństwo w Europie. Drugi scenariusz sprawdzał odporność systemów używanych przez energetykę. Poszukiwano także możliwości wzajemnej pomocy obu kontynentów, w razie prawdziwego cyberataku.

Na koniec opisywanych instytucji oraz inicjatyw można wymienić i rodzimy GIODO – Generalny Inspektor Ochrony Danych Osobowych. Jest to państwowy organ działający na mocy Ustawy o ochronie danych osobowych, a którego zadaniem jest kontrola zgodności przetwarzania oraz ochrony i bezpieczeństwa tych informacji również w systemach informatycznych.

Dlaczego współpraca tak wielu instytucji oraz użycie tylu inicjatyw mogą być ważne dla bezpieczeństwa infrastruktury krytycznej, gdy wiele z nich zajmuje się ogólnie pojmowanymi cyber-zagrożeniami? Przykłady nasuwają się łatwo do wyobraźni. Hakerski atak na portal społecznościowy jest w stanie wydobyć dane o pracownikach obiektów wchodzących w skład infrastruktury krytycznej. Może posłużyć to do podszycia się pod nich czy zainstalowania im w przesyłce budzącej zaufanie oprogramowania wirusowego. Umożliwi to atakującym kontrolę nad ich komputerami, skrzynkami pocztowymi i zaoferuje przejmowanie już poufnych danych oraz ułatwi dalszy dostęp w głąb systemu. Dobre zabezpieczenie wszystkich komputerów, serwerów i stron internetowych może więc ostatecznie okazać się bardzo ważne. Najsłabsi w zabezpieczeniach w końcu mogą okazać się ludzie, poprzez swoją beztroskę albo naiwność czy niewiedzę.

Fazy i narzędzia obrony przed atakiem cybernetycznym

W swojej pracy „Cyberterroryzm - nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku" J. Świątkowska oraz I. Bunsch za opracowaniem „Cyberspace as a medium for terrorists"[10] (S. E. Goodman, J. C. Kirk, M. H. Kirk) wymieniają[11] trzy fazy obrony przed atakiem cybernetycznym:

I. Zarządzanie prewencyjne
II. Zarządzanie atakiem
III. Zarządzanie konsekwencjami

Na etapie prewencji, zaleca się wprowadzenie elementów zabezpieczających o szerokim zasięgu, już podczas projektowania danego systemu teleinformatycznego. Postuluje się, aby bezpieczeństwo było jednym z najważniejszych komponentów ich projektowania. Zwraca się uwagę na udział czynnika ludzkiego. Roztacza się ochronę nad istotnymi elementami systemu przed osobami, które mogłyby stanowić dla nich zagrożenie, mogąc być teraz lub w przyszłości zwerbowani przez terrorystów. Należy również prowadzić odpowiednią politykę odstraszania, polegającą na tworzeniu odpowiedniego i jasnego prawa. Trzeba koordynować i harmonizować wszystkie międzynarodowe działania i rozwiązania prawne. Odstraszanie to także prezentacja swoich możliwości technologicznych w tym do przeprowadzenia kontrataku i namierzania sprawców. Odpowiednio prowadzone odstraszanie mogłoby od razu zniechęcać potencjalnych agresorów.

Na zarządzanie atakiem składa się podnoszenie efektywności i zdolności do alarmowania, w tym rozbudowa systemów wczesnego ostrzegania. Należy wzmacniać fizyczną i techniczną obronę systemów wrażliwych na ataki. Zagrożenie można zmniejszać poprzez tworzenie kopii zapasowych czy rezerwowych systemów, które będą mogły szybko przejąć zadania uszkodzonych części infrastruktury, w razie przeprowadzonego skutecznie ataku. Zwraca się uwagę na ko-

nieczność ciągłego prowadzenia polityki cyberobrony, przez każdy pojedynczy podmiot, aby każda zaangażowana osoba znała swoje miejsce oraz funkcję i procedury, podczas zwalczania zagrożenia.

Ostatnią fazą jest zarządzanie konsekwencjami ataku. Należy regenerować uszkodzone systemy, i zastosować odpowiedź, która może być zarówno schwytaniem i prawnym ukaraniem sprawcy, jak i wykonaniem własnego cybernetycznego uderzenia na sprawców, jeśli ich schwytanie nie jest możliwe.

W procesie ochrony przydadzą się narzędzia takie jak programy antywirusowe i zapory sieciowe, programy szyfrujące dane oraz połączenia, w tym zaawansowane profesjonalne narzędzia. Można zabezpieczać się w dodatkowe źródła zasilania, kopie zapasowe bieżących danych, zapasowe systemy elektroniczne i serwery, gotowe do podpięcia i użycia w razie uszkodzenia głównych. Czy przygotowane wcześniej elementy nie przydadzą się w razie udanego ataku, gdy zaistnieje konieczność odbudowy systemu przywracając go do funkcjonowania? Nie zapominajmy o odpowiednich procedurach bezpieczeństwa i postępowania, które wdrożyć powinni kierownicy oraz informatycy, stosując się do nich wraz z użytkownikami.

Elementy procesu ochrony teleinformatycznej infrastruktury krytycznej, wymienia także G. Krasnodębski:

- ocena systemów i sieci, czyli monitoring;
- procedury awaryjne;
- koordynacja reagowania;
- ewidencja incydentów;
- prace badawcze;
- tworzenie narzędzi;
- szkolenia;
- testowanie[12].

Proces ten tworzy zamknięty krąg, polegający na ciągłej i nieustannej analizie stanu faktycznego, i dostosowywania do niego własnych możliwości, w zakresie zapewniania ochrony zagrożonym obiektom.

Uwagi końcowe

Zwalczanie efektów cyberterroryzmu, jako zagrożenia dla infrastruktury krytycznej państwa, różni się w swojej naturze od przeciwdziałania skutkom zamachów tradycyjnych. Gdy dochodzi do wybuchu bomby w samolocie, centrum handlowym, czy wzięci zostają zakładnicy, poza następstwami psychospołecznymi nie ma trwałych skutków dla danego państwa. Nawet zamachy na tak wielką skalę jak te w Nowym Jorku, Madrycie albo Londynie, nie wyrządziły same w sobie większej szkody państwom które padły jego ofiarami. Czy bowiem, za ich przyczyną funkcjonowanie państwa stało się niemożliwe? Zabrakło energii, paliw, administracja rządowa stała się niesprawna? Nie.

Były to jednak zamachy o skali przede wszystkim wysoko medialnej, uderzającej w psychikę i mentalność społeczeństwa oraz polityków. Nie naruszały podstawowych funkcji państwa. Teoretycznie, oprócz uprzątania materialnych szkód, niesienia pomocy ofiarom oraz rodzinom, jedynym poważnym problemem i wyzwaniem mogło być zmniejszanie skutków psychospołecznych, które wystąpiły po udanym zamachu. Należało po prostu zmniejszyć ich chorobliwy i paraliżujący stan na mniej szkodliwy, przywracając społeczne i polityczne życie państwa do normy. Inną sprawą były następstwa polityczne, ale wykraczają one poza to opracowanie.

Ale w przypadku ataku terrorystycznego na infrastrukturę krytyczną sytuacja zmienia się diametralnie. Już nie wystarczy tylko akcja ratownicza i zmniejszanie rozmiarów paniki. Uszkodzone centralne informatyczne systemy bankowe albo giełdowe na wiele dni lub tygodni mogą uniemożliwić sprawne funkcjonowanie rynków. Gdy zwykły zamach staje się dla państwa tylko bolesnym zranieniem, w najgorszym razie trudno się gojącym, atak terrorystyczny na infrastrukturę krytyczną będzie

już podcięciem nóg. Wszystko może stracić swoją równowagę.

Zapobieganie wystąpieniu takich zdarzeń to jedno. Leży ono na barkach polityków uchwalających ustawy oraz budżety, powołujących odpowiednie zespoły lub centra. Nieszczęście może się w końcu wydarzyć, pomimo starań i wkładanych środków. Wtedy, przeciwdziałanie negatywnym skutkom informatycznego zamachu terrorystycznego wymaga zastosowania planów alternatywnych, wdrożenia systemów odtwarzania uszkodzonej infrastruktury krytycznej i jej naprawy.

Zakładając hipotetyczny scenariusz - oto w wyniku uderzenia cyberterrorystów bankomaty oraz karty płatnicze nie działają. Ludzie pozbawieni gotówki przez wiele dni nie mogą zrobić żadnych, nawet podstawowych zakupów. Na wypadek takiego przebiegu zdarzeń, być może, lokalne urzędy administracji powinny rozpatrywać jakąś alternatywę na krótki czas sytuacji kryzysowej. Mieć przygotowane do użycia systemy kartkowe na podstawowe artykuły. Banki mogłyby zaś posiadać odpowiednie zapasy gotówki do wypłat poza bankomatami i to na bardzo dużą skalę, zakładając, że możliwe będą przynajmniej operacje i przelewy na ich kontach. A jeśli przygotowania nie będzie? Czy do momentu usunięcia awarii społeczeństwo czeka bezgotówkowy paraliż?

Zagrożenie może nadejść z każdej strony, na dowolny element. Zdarzyć się może w najmniej oczekiwanej chwili. Nawet przy 99% skuteczności służb przeciwdziałania, na sto ataków ten jeden może być udany. Pozostaje zadać sobie pytanie, czy w ogóle możemy osiągnąć tak wysoką skuteczność? Jak wysoka jest ona dzisiaj? Czy jesteśmy gotowi? To chyba pytania bez jednoznacznej odpowiedzi.

Najlepsze co można, to swoją gotowość zwiększać. Zarówno do odpierania prób cyberataków, jak i usuwania szkód, które wyrządzą. Nie da się tego realizować, a jest to proces ciągły, bez posiadania odpowiedniej wiedzy, sprzętu oraz wyszkolonych specjalistów.

Niezbędne w tym celu są jednak finansowe nakłady i odgórne wsparcie tych procesów, przez politykę władz państwowych. Chcąc się rozwijać, musimy nieustannie i wielopłaszczyznowo zwiększać swoje bezpieczeństwo. Jest to obowiązkiem całego społeczeństwa i nas samych.

Przypisy

1 Zob. Oficjalna strona internetowa IMPACT – [http://www.impact-alliance.org/services/grc-introduction.html], dostęp: 2012-08-15.
2 J. Świątkowska, I. Bunsch. „Cyberterroryzm - nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku", s. 8. Brief Programowy Instytutu Kościuszki. Źródło online: [http://ik.org.pl/pl/publikacja/nr/4298/], dostęp: 2012-07-26.
3 Zob. Decyzja nr 357/MON z dnia 29 lipca 2008 r., w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.
4 Strona www: [http://cert.gov.pl/], dostęp: 2012-07-29.
5 Strona www: [http://www.cert.pl/], dostęp: 2012-07-29.
6 Strona www: [http://www.tp.pl/prt/pl/tpcert/obsluga/zglaszanie/incydent/], dostęp: 2012-07-29.
7 Za: „US builds net for cyber war games", bbc.co.uk. Źródło online: [http://www.bbc.co.uk/news/technology- 13807815], dostęp: 2012-07-26.
8 Por. „Pierwsze wspólne cyberćwiczenia", kopalniawiedzy.pl. Źródło online: [http://kopalniawiedzy.pl/Cyber- Atlantic-2011-cwiczenia-Unia-Europejska-USA,14228], dostęp: 2012-07-26.
9 Zob. „First joint EU-US cyber security exercise conducted today", enisa.europa.eu. Źródło online: [http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011], dostęp: 2012-07-16.
10 S. E. Goodman, J. C. Kirk, M. H. Kirk, „Cyberspace as a medium for terrorists", [w:] „Technological Forecasting &Social Change" 74 (2007), s. 201.
11 J. Świątkowska, I. Bunsch. „Cyberterroryzm...", op. cit.
12 Zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego", Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznejinfrastrukturykrytycznejwdobierozwojuspoleczenstwainformacyjnego.doc], dostęp: 2012-07-30.

TOBIASZ MAŁYSA

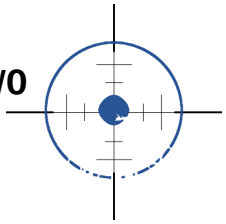
Podstawowe aspekty bezpieczeństwa informacji

W ujęciu informatycznym (informatyka – „nauka o tworzeniu i wykorzystywaniu systemów komputerowych”[1], ale też „gałąź nauki i techniki zajmująca się teorią i technologią przetwarzania informacji”)[2], informacja to zbiór danych w dowolnej formie, służący do dalszego przetwarzania tych danych i przekształcenia ich w wyniki, które stają się kolejnymi danymi[3]. Informacją mogą być zatem np. zebrane podczas czynności operacyjnych dane związane z terenem działania i obiektach zainteresowania, przekształcone w odpowiednie raporty (to znów dane), które posłużyć mogą do otrzymania statystyk (następnych danych) lub wysunięcia wniosków (to także dane), nadal mogących ulegać dalszemu przetwarzaniu i uzyskiwania kolejnych danych. Cały proces narażony jest na zagrożenia.

Niezależnie od sposobu ich przechowywania można wymienić takie niebezpieczeństwa dla informacji jak nieuprawnione ujawnienie (np. przechwycenie, wykradzenie, upublicznienie), modyfikacja (np. sabotażu, dostanie się błędów), zniszczenia czy uniemożliwienia korzystania z informacji poprzez blokowanie do niej dostępu (sabotaż, wandalizm, awaria)[4]. Zagrożone mogą być nie tylko informacje, ale system i jego elementy, środowisko w którym są one przetwarzane[5]. Dlatego możemy mówić o takich cechach bezpieczeństwa informacji jak poufność (tajność, to dostęp do informacji tylko odbiorcom mających do tego upoważnienie, zależnie od przyznanych uprawnień i wagi poufności informacji), integralność (spójność, to pewność czy informacje nie były manipulowane, przez nieuprawnione osoby i niedozwolone sposoby) oraz dostępność (dosięgalność, dostęp do informacji zapewniony jest zawsze w okolicznościach i warunkach, które na to zezwalają[6]). Szersze spojrzenie na klasyfikację zagrożeń (tzw. klasyfikacja STRIDE[7]) pozwala wyszczególnić podszywanie się (dostęp w drodze udawania uprawnionego użytkownika, włamania na sieciowe konta, inżynieria społeczna), manipulację danymi (przyznanie nieuprawnionego dostępu do operacji na danych), negowanie (zaprzeczanie, że atak się odbył, lub utrudnianie identyfikacji źródła ataku), ujawnienie danych (przypadkowe błędne nadanie uprawnień lub niecelowe ujawnienie informacji, podsłuch, włamanie), zakłócenie funkcji systemu (blokada usług, dostępu do danych, niszczenie informacji lub sprzętu, wykorzystywanie słabych punktów do paraliżowania go, sabotowanie złośliwym oprogramowaniem) oraz podniesienie przywilejów (nieuprawnione pozyskanie uprawnień).

Bezpieczeństwo informacji w świetle przedstawionych zagrożeń wymaga podjęcia szeregu kroków na różnych płaszczyznach. Skoro chroniona informacja ma być poufna (niemożliwa do wykorzystania przez nieupoważnione osoby czy procesy), dostępna (zawsze i tylko upoważnionym osobom i procesom w dopuszczonych warunkach) oraz spójna (wszelkie modyfikacje na operacji dają się ustalić, a możliwe są tylko dozwolone działania), to stosownie do rodzaju zagrożenia (których ogólne rodzaje wstępnie wytypowaliśmy), należy zastosować odpowiednie metody, które możemy nazwać „usługami ochrony informacji”[8].

Kontrola dostępu daje ochronę informacji przed nieuprawnionym do niej dostępem (ujawnieniem informacji) lub zakłóceniem funkcji systemu (odmowa usługi, np. uniemożliwienie uprawnionego dostępu do informacji, jej przetwarzania, przechowania, itp. paraliżowanie działań). Bezpieczeństwo może być tu zapewnione poprzez np. nadawanie informacjom określonego stopnia poufności oraz weryfikowanie uprawnień przy próbach dostępu (dostęp limitowany)[9]. Systemy powinny być też odporne na akty złośliwości i sabotażu oraz awarie i usterki techniczne, gwarantując ciągłość pracy i niezawodność, co można osiągnąć przez np. układy zapasowe oraz eliminowanie luk i słabych punktów.



Integralność danych, a więc zapewnienie im spójności, to ochrona przed ich zmianą. Źródło takiego zagrożenia leżeć może nie tylko po przypadkowej lub zamierzonej stronie działalności ludzkiej, ale i w używanym sprzęcie, oprogramowaniu[10]. Zastosowanie np. podpisów cyfrowych czy kodów uwierzytelniających da pewność, czy informacje nie były w nieuprawniony sposób zmanipulowane. W zapewnieniu bezpieczeństwa pomocne mogą być poprawne procedury przesyłu informacji, zgodnie z ustalonymi protokołami. Taki protokół, dla informacji jawnych, lecz zagrożonych utratą integralności (nieuprawnioną zmianą treści) omawialiśmy w listopadowym numerze biuletynu w ub. roku[11]. Wtedy rozpatrywana była wiadomość radiowa, wielokrotnie przekazywana przez kolejne radiostacje w łańcuchu przekazu, aż do pożądanego odbiorcy. Aby uniknąć efektu „głuchego telefonu" i zniekształcenia wiadomości po drodze, przedstawiono sposób składający się z preambuły (krótkiej bądź pełnej), właściwego komunikatu i danych kontrolnych (np. liczby znaków, wyrazów w wiadomości). Pozwalał on na zachowanie stałej treści komunikatu, ale nie cechował się odpornością na złośliwość czy przypadkowe błędy.

Uwierzytelnienie (autoryzacja) informacji i nadawców zapewnia ochronę przed podszywaniem się, nadawaniem fałszywych informacji[12]. Źródło nadanej informacji musi być weryfikowalne. Można to realizować stosowaniem certyfikatów, kodów uwierzytelniających, kluczy jednorazowych (tokenów - generatorów), podpisów cyfrowych, itp. Metody te jednak mogą być podatne na ich przechwycenie przez potencjalnego intruza.

Niezaprzeczalność dotyczy niemożliwości wyparcia się faktu podejmowania swoich działań, np. wewnątrz systemu[13]. Wszystkie przeprowadzane operacje (dostęp, modyfikacja, kopiowanie, przesył, odbiór) są zapisywane. Możliwa jest identyfikacja osób (procesów) biorących w nich udział. System musi być zawsze zdolny do udowodnienia tych działań, w każdej sytuacji. Jest to możliwe w drodze używania dzienników zdarzeń (w tym automatycznych, komputerowych) lub innych sposobów ich rejestrowania (monitorowania).

Poufność danych to ostatnia z omawianych usług (metod). O ile kontrola dostępu (wedle przyznanych uprawnień, klasyfikacji) oferowała ochronę przed nieuprawnionym dostępem[14], poufność danych w tym rozumieniu chroni je przed np. podsłuchem czy przechwyceniem informacji przez intruza. Realizacja, oprócz stosowania metod kontroli dostępu odbywa się przede wszystkim poprzez szyfrowanie informacji i używanie bezpiecznych kanałów jej przechowywania i przesyłu.

Uwagi końcowe

Okazuje się, że zapewnienie informacjom poufności (realizowanej np. kryptografią) to jedynie niewielka część bezpieczeństwa informacji. Cóż po informacji poufnej, ale zagrożonej niedostępnością, nieuprawnioną modyfikacją? Co więcej, przedstawione metody zapewniania bezpieczeństwa informacji chociaż wywodzą się ze spojrzenia typowo informatycznego, mogą być potraktowane uniwersalnie, nie tylko dla informacji przechowywanych w systemach czy sieciach komputerowych.

Przypisy

1 Za: Informatyka, hasło sjp.pwn.pl. Źródło online: [http://sjp.pwn.pl/slownik/2561527/informatyka], dostęp: 2013-02-12.
2 Za: Informatyka, hasło sjp.pl. Źródło online: [http://www.sjp.pl/informatyka], dostęp: 2013-02-12.
3 Por. Wprowadzenie do informatyki, J. Kluczewski. Źródło online: [http://www.staff.amu.edu.pl/~psi/informatyka/kluczew/I1_Introduction.htm], dostęp: 2013-02-12.
4 K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa 2008, s. 12.
5 Tamże, s. 12.
6 Tamże, s. 12-13.
7 Metoda używana przez firmę Microsoft w procesie wytwarzania oprogramowania. Zob. Application Security Best Practices at Microsoft. The Microsoft IT group shares its experiences. White Paper. January 2003, s. 27-28. Źródło online: [http://download.microsoft.com/download/0/d/3/0d30736a-a537-480c-bfce-5c884a2fff6c/AppSecurityWhitePaper.doc], dostęp: 2013-02-12.]
8 Por. K. Szczypiorski, P. Kijewski. Podstawy ochrony informacji - handel elektroniczny, s. 1-2. Źródło online: [http://krzysiek.tele.pw.edu.pl/pdf/wroc99.pdf], dostęp: 2013-02-12.
9 Por. K. Liderman, Analiza... dz.. cyt.., s. 98.
10 Application Security Best Practices at Microsoft... op. cit., s. 27
11 T. Małysa, Radioamatorska komunikacja kryzysowa, e-Terroryzm.pl nr 11/2012, s. 20-21.
12 Por. Z. Świerczyński, Wybrane metody uwierzytelnienia użytkownika sieci komputerowej. Źródło online: [http://www.ita.wat.edu.pl/~z.swierczynski/SBS/Lab_8_AAA/Uwierzytelnianie.pdf], dostęp: 2013-02-26, s. 1-3.
13 Por. D. Srokowski, Bezpieczeństwo systemów ISDN. Źródło online: [http://zstux.ita.pwr.wroc.pl/archiwum/isdn_ref_2002/15.pdf], dostęp: 2013-02-26, s. 4-6.
14 Por. K. Liderman, Analiza ryzyka... dz.cyt., s. 32-33.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 6/2013 (18)]

TOBIASZ MAŁYSA

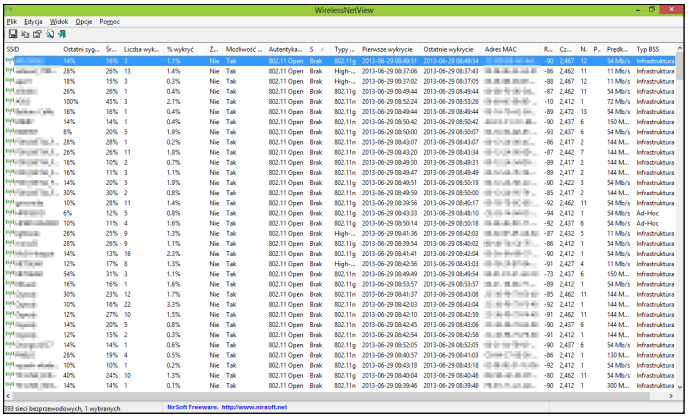
Przeciwdziałanie wyciekowi informacji w sieciach WiFi

Człowiek chętnie podąża ku wygodzie, upraszczając swoją pracę. Wykonując wiele razy te same czynności mamy ponadto skłonność do popadania w rutynę. Możliwe są wtedy błędy wynikające z lenistwa bądź nieuwagi, nadmiernej pewności siebie albo beztroski. To co przemieniło się w rutynę traktowane jest też jako bardziej znane, wręcz „od podszewki". Tym samym, na nowości oraz zmiany środowiska i nowe zagrożenia reagujemy być może z mniejszą czujnością. Postawa taka podczas przetwarzania informacji mających pozostać poufnymi niesie wyjątkowe ryzyko. Dotyczy to m. in. tak powszechnej dziś komunikacji przez Internet, zwłaszcza bezprzewodowy, narażony na podsłuch.

Bezprzewodowe łączenie się z siecią Internet za pomocą WiFi i punktów dostępowych, to jedna z najbardziej popularnych metod, cechująca się dużą wygodą. Tymczasem, z technicznego punktu widzenia jest ona bardziej narażona na wyciek przesyłanych informacji niż połączenie poprzez „klasyczny" kabel.

Punkty dostępowe z siecią WiFi są powszechne. Znajdziemy je we własnym domu, w jego pobliżu (urządzenia naszych sąsiadów), na terenie osiedli oraz blokowisk, wewnątrz obiektów handlowych, instytucji, w przestrzeni miejskiej (gdy mowa o silniejszych nadajnikach), a nawet w środkach komunikacji publicznej. Można zgrupować je ze względu na sieci prywatne i publiczne, a także szyfrowane i nieszyfrowane, oraz autoryzowane i nieautoryzowane. Sieć publiczna nie zawsze jest niezaszyfrowana i odwrotnie - wiele z sieci prywatnych jest nieszyfrowanych, a dostęp do nich może uzyskać każdy.

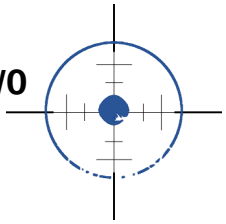
Decydując się na korzystanie z danej sieci bezprzewodowej do przesyłania informacji narażonych na ujawnienie (np. służbowych, handlowych), należy wziąć pod uwagę stopień jej zabezpieczenia. O ile na stopień bezpieczeństwa własnej sieci mamy pewien wpływ (np. poprzez odpowiednią jej konfigurację), to łącząc się z obcą siecią niewiele możemy w tym zakresie uczynić. Poza oczywiście, zadbaniem o zabezpieczenie własnego komputera lub innego mobilnego urządzenia.



W typowym miejskim środowisku, w gęsto zabudowanym terenie funkcjonować może od kilkuset to nawet tysięcy sieci WiFi na obszarze 1-2 km². Wiele z nich nie posiada żadnych zabezpieczeń, co czyni korzystanie z nich, dla ich użytkowników, nie do końca bezpiecznym. Sieci te narażone są zdecydowanie na wyciek informacji.
Na obrazku, screen z przykładowego oprogramowania pozwalającego na skanowanie pasma używanego przez sieci bezprzewodowe, uzyskując szczegółowe informacje na ich temat (np. nazwa sieci, siła sygnału, rodzaj uwierzytelnienia, rodzaj szyfrowania, adres MAC, itp.).

WiFi - sieć bezprzewodowa

Czym właściwie jest sieć bezprzewodowa? Najczęściej mamy w jej przypadku doczynienia z punktem dostępowym, zwanym routerem. Jego rola to coś w rodzaju pośrednika, pomiędzy urządzeniem chcącym uzyskać dostęp do Internetu, a Internetem. Posługujemy się uproszczeniem, gdyż cały Internet jest w zasadzie siecią, złożoną z serwerów przechowujących informacje lub oferującymi usługi oraz dróg dostępu do nich, bram i pośredników. Niemniej router wykonuje tu zadania bramy dostępowej. Musi być on zatem sam wpięty do sieci np. poprzez kabel telefo-



niczny, antenę radiową czy innego rodzaju złącze, "oferujące" Internet od dostawcy (np. Neostrada, Netia, lokalne firmy, popularne „radiówki"). Do takiego routera drogą kablową lub - w przypadku naszych rozważań - bezprzewodową (tzw. sieć WiFi) podłączane są urządzenia końcowe użytkownika. To np. komputery stacjonarne i przenośne (laptopy), tablety czy telefony komórkowe. Wszystko to odbywa się dzięki falom elektromagnetycznym, poprzez komunikację cyfrową przy pomocy odpowiednich układów elektronicznych i protokołów.

Żeby komunikacja była możliwa, obydwa urządzenia (np. router - punkt dostępowy i nasz laptop, za pomocą bezprzewodowej karty sieciowej) muszą "widzieć się" we wzajemnym zasięgu. W zależności od mocy nadajników i rodzaju terenu (otwarty, budynek, przeszkody) odległość taka waha się od 5-10 metrów do kilkudziesięciu. Jeśli karta sieciowa urządzenia jest zgodna z protokołem stosowanym przez router (stare urządzenia nie zawsze współdziałają z nowymi), istnieje możliwość nawiązania połączenia. Warunkiem jest, aby router rozgłaszał w okolicy swoją nazwę (tzw. SSID, może być to dowolny zestaw znaków, wyrazów, często to nazwa własna punktu dostępowego). Inna metodą jest wpisanie nazwy niewidocznego punktu dostępowego w urządzeniu, podczas wykrywania go. Oznacza to, że istnieje możliwość ukrycia swojego routera, jakkolwiek nie można traktować tego jako skuteczną ochronę. Istnieje oprogramowanie zdolne poprzez nasłuch WiFi uzyskać ukrytą nazwę SSID. Poza tym, taki tryb pracy może być trochę mniej efektywny dla szybkości czy przepustowości połączenia internetowego, a więc osłabiać jego jakość.

Uwierzytelnianie

Jeśli poprzednio wymienione warunki są spełnione, rozpoczyna się proces nawiązywania połączenia z siecią. W tym momencie możliwe są dwa scenariusze - router czyli punkt dostępowy nie wymaga uwierzytelniania (autoryzacji) nowych urządzeń, lub tak. Jest to tzw. tryb WPS. Z reguły bazuje on na identyfikowaniu urządzeń (np. telefon, laptop) po ich adresie MAC. Adres ten jest unikalny dla każdej karty sieciowej urządzenia, i przyjmuje on postać 48 bitów (np. 00:0A:E6:3E:FD:E1). Liczba możliwych kombinacji adresów sięga 2 do potęgi 48. Autoryzacja polega na ręcznym wprowadzeniu adresu MAC do puli akceptowanej przez router, lub o wiele częściej, na wciśnięciu w nim odpowiedniego przycisku, zezwalającego w ciągu kolejnych 2 minut na podłączenie nowych urządzeń, które automatycznie są rozpoznawane jako dopuszczone. Teoretycznie metoda ta daje pewność „odfiltrowania" i nie dopuszczenia niepożądanych urządzeń do sieci, jeśli osoba niepowołana nie ma fizycznego dostępu do routera. Z drugiej strony, nie jest problemem uzyskanie akceptowanych przez router adresów MAC poprzez nasłuch WiFi odpowiednim oprogramowaniem. Zmiana na jeden z nich adresu własnej karty sieciowej może pozwolić na wpuszczenie „intruza".

Dane niezaszyfrowane

Pozytywne przejście przez proces uwierzytelnienia oznacza uzyskanie dostępu do sieci, jeśli nie jest ona dodatkowo szyfrowana i nie wymaga podania klucza. Gdyby przyjrzeć się bliżej wymianie pomiędzy naszym urządzeniem a routerem, zobaczylibyśmy, że ta komunikacja dzieli się na pakiety. Wysyłając niniejszy artykuł tradycyjną nieszyfrowaną pocztą (ok. 16 000 znaków) zostanie on podzielony na kilkanaście paczek, rozpoczynających się od określonego nagłówka (nadawca, adresat, data, suma kontrolna, itp.) i zawierających następnie właściwą treść. Taka forma ułatwia kontrolę nad pakietami, gdy któraś z nich ulegnie zagubieniu albo zakłóceniu. Pozwala to uniknąć błędów, gdyż urządzenia będą wysyłały utracone pakiety ponownie do skutku.

Słowniczek

Karta sieciowa – jedna z kart rozszerzeń komputera, która przekształca pakiety danych w sygnały w celu przesyłania ich siecią internetową. Każda z nich posiada swój adres (tzw. MAC), który jest niepowtarzalny. Spotyka się karty sieciowe wbudowane w płytę główną lub w nią wpinane, albo dołączane do jednego z portów USB.

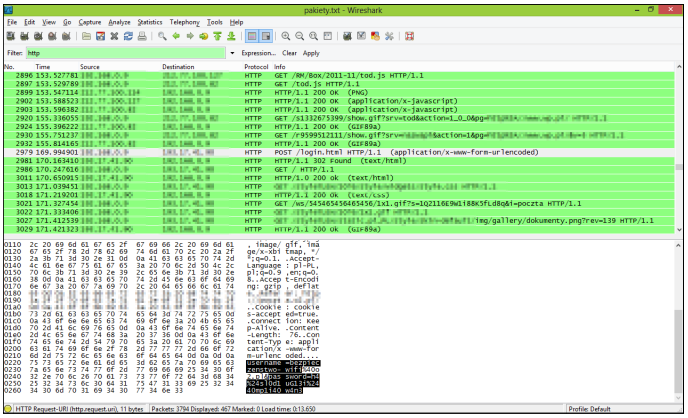
Protokół – zbiór procedur składających się ze ściśle określonych reguł oraz kroków. Służą one do porozumiewania się ze sobą urządzeń oraz oprogramowania poprzez Internet. W ustandaryzowany sposób regulują one np. przepływ informacji podzielonej na pakiety.

Suma kontrolna – liczba dołączana do pakietu danych w celu możliwości wykonania przez komputer operacji sprawdzającej poprawność nadanych informacji. Liczbę tą uzyskuje się poprzez operacje matematyczne na danych za pomocą odpowiedniego algorytmu, działającego w obie strony. Jeśli w dane w którymś miejscu w trakcie transmisji wkradną się błędy, lub ich część zostanie utracona, wtedy suma kontrolna nie będzie się zgadzać. Protokoły umożliwiają wtedy nadanie takiego pakietu ponownie, aż do skutku.

HTTPS – jest to protokół sieci WWW, przez który „wczytują się" strony internetowe w przeglądarkach. W odróżnieniu od protokołu HTTP, ten w całości szyfruje komunikację.

WEP/WPA/WPA2 – są to kolejne wersje standardów szyfrowania w sieciach WiFi. Kryptografia odbywa się za pomocą jednego klucza symetrycznego, służącego zarówno do kodowania jak i dekodowania danych.

Jawna postać pakietów jest możliwa do odczytania w ich źródłowej postaci. To, co odczytywane jest przez naszą kartę sieciową w sieci WiFi, można "podglądnąć" odpowiednią aplikacją komputerową. W standardowym trybie działania karta sieciowa odrzuca wszystkie pakiety, które nie są do niej zaadresowane. Specjalne aplikacje zwane snifferami (m. in. to legalne programy do monitoringu sieci) pozwalają na przestawienie karty w tryb przechwytujący wszystko, co do niej napływa. Większość takich pakietów, a zaadresowanych do innych użytkowników sieci to fragmenty np. pobieranych plików czy stron internetowych. Przeczesanie ich po zapisaniu (dostępne są np. filtry) może pokazać również bardziej interesujące potencjalnego intruza fragmenty. Będą to choćby dane wysyłane przez formularze na stronach internetowych (w tym, do logowania się) zawierające loginy oraz hasła, jeśli połączenie z taką stroną nie jest zaszyfrowane dodatkowymi metodami (np. protokołem HTTPS zamiast HTTP).



Nawet długie i skomplikowane hasło nie jest mocną ochroną w przypadku jego wycieku przez np. niezabezpieczoną sieć WiFi. Na obrazku, program do diagnostyki sieci bezprzewodowej pozwalający na podgląd przesyłanych przez nią pakietów. Logowanie się do banku czy poczty przez nieszyfrowane protokoły zezwala potencjalnemu intruzowi na bezpośredni podgląd przesyłanego siecią loginu oraz hasła. Odnalezienie interesujących danych w gąszczu tysięcy przesyłanych pakietów nie jest wcale trudne. Po przeformatowaniu ich na ciąg znaków klawiatury (np. znak "$" w haśle to "%24" w pakiecie) zalogowanie-włamanie na skrzynkę pocztową jest już możliwe.

Szyfrowanie połączenia bezprzewodowego

Komunikacja pomiędzy naszym urządzeniem (komórką, laptopem), a routerem - punktem dostępu sieci bezprzewodowej może być szyfrowana. Służą do tego odpowiednie metody, kodujące w locie całość wymienianych informacji. Sieć zaszyfrowana w momencie podłączania pod nią autoryzowanego urządzenia prosi o podanie klucza, bez którego niemożliwy jest dostęp do WiFi. Kodowanie danych czyni ewentualnie przechwycone przez intruza pakiety nieczytelnymi. Trzeba jednak zwrócić uwagę na to, że łamanie haseł i algorytmów szyfrujących jest możliwe. Rodzaj zastosowanej metody wydłuża tylko potrzebny do tego czas, wymagając też większych środków, bardziej specjalistycznej wiedzy. Niemniej, wybór np. metody WPA2 (o wiele lepszej, niż podatna na złamanie metoda WEP i nieco silniejsza WPA) daje stosunkowo większą pewność, chociaż nadal nie absolutną.

Bezpieczny punkt dostępowy

Router pracujący w trybie WPS i szyfrujący pakiety za pomocą WPA2 wydaje się być pewnym minimum, jeśli chodzi o bezpieczeństwo. Można je zwiększać poprzez zastosowanie jeszcze bardziej wymagających algorytmów szyfrowania (np. z certyfikatami i kluczami osobistymi), ale komplikuje to funkcjonowanie takiej sieci. Również ukrycie nazwy SSID routera (co nie zawsze jest zalecane), a przynajmniej uczynienie jej niewiele mówiącą dla potencjalnego intruza może oddalić prawdopodobieństwo włamania (np. dokładna znajomość modelu routera bywa pomocna).

Rzeczą często pomijaną w sieciach bezprzewodowych, zwłaszcza domowych, są natomiast login, hasło oraz adres dostępu do panelu administracyjnego routera. Z reguły login (*admin*) oraz hasło to nie są zmieniane po jego instalacji (np. *admin, password*), co więcej pozostawiany jest domyślny adres IP z którego łączymy się poprzez przeglądarkę z panelem (np. *192.168.1.1*, *192.168.0.1*). Zmiana loginu oraz hasła na dłuższe i bardziej skomplikowane są w stanie uniemożliwić nieautoryzowany dostęp do tego urządzenia, podobnie jak ustawienie innego adresu IP. Zaniedbanie tej kwestii grozi choćby wandalizmem, czyli najczęściej resetem ustawień do stanu fabrycznego. Oznacza to ni mniej, ni więcej jak odcięcie nas od internetu, aż do naprawy tego stanu rzeczy przez nas samych lub technika.

Uwagi końcowe

Nawet w przypadku korzystania z nieszyfrowanej sieci istnieją metody zabezpieczenia się po stronie własnego komputera przed podsłuchem fali radiowej. Oprócz korzystania z bezpiecznych protokołów (np. w przeglądarce internetowej - strony z przedrostkiem HTTPS zamiast nieszyfrowanego HTTP, a także szyfrowane połączenia w programach pocztowych) komunikację z Internetem można uczynić bardzo trudną do przechwycenia poprzez używanie z programów anonimizujących. Programy te łączą się z serwerem pośrednikiem (zwanym VPN), który nie tylko ukrywa nasze własne IP ale dodatkowo, co w temacie naszych rozważań istotne, szyfrują absolutnie całość ruchu. Czyni to ewentualnie przechwycone dane w niezabezpieczonej sieci nieprzydatnymi. Szczegóły dotyczące tych aplikacji wykraczają poza ramy tego opracowania.

Możliwości przechwycenia komunikacji w Internecie, jak to zostało zarysowane, istnieje wiele, co ryzyko podsłuchu czyni wysokim. Każe to zwrócić szczególną uwagę na kwestię zabezpieczenia połączenia z siecią, zwłaszcza podczas korzystania z bezprzewodowych punktów dostępowych. Uwzględnienie wymienionych zagrożeń jest niezwykle istotne we wszelkiej pracy związanej np. z przetwarzaniem informacji niejawnych (z punktu widzenia ustawowego, to też tajemnica np. adwokacka, lekarska), ale także wrażliwych informacji biznesowych (ochrona przed nieuczciwą konkurencją) oraz prywatnych, które chcemy szczególnie chronić.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 8/2013 (20)]

TOBIASZ MAŁYSA

Model działań bezpieczeństwa teleinformatycznego
z punktu widzenia Ustawy o ochronie informacji niejawnych

W polskim systemie prawnym bezpieczeństwo informacji niejawnych jest regulowane przede wszystkim przez Ustawę o ochronie informacji niejawnych (Dz. U. 2010 nr 182 poz. 1228), zwaną dalej UOIN. Poprzez taką informację niejawną należy rozumieć taką, której ujawnienie spowodowałoby szkodliwe skutki dla funkcjonowania państwa.

Informacje tego typu są odpowiednio klasyfikowane, według czterech kategorii klauzul: ściśle tajne (najwyższa), tajne, poufne, zastrzeżone (najniższa). Klauzula ściśle tajne może dotyczyć informacji, które ujawnione mogłyby doprowadzić do np. identyfikacji funkcjonariuszy tajnych służb, zagrozić świadkom koronnym lub ich rodzinom. Informacje tajne to takie które ujawnione mogą m. in. pogorszyć stosunki z innymi krajami, zakłócić przygotowania obronne, utrudnić czynności operacyjno-rozpoznawcze i śledcze. Informacje poufne grożą natomiast w przypadku ujawnienia np. zakłóceniem porządku publicznego, utrudnieniem prowadzenia bieżącej polityki zagranicznej, utrudnić wykonywanie zadań służbom ochrony państwa. Najniższa klauzula, zastrzeżone, dotyczy ogólnie ujętego szkodliwego wpływu na działanie organów władzy publicznej, realizacji polityki wewnętrznej i zagranicznej, itd. Klauzule odpowiednio do wrażliwości danej informacji nadaje osoba odpowiadająca za podpisanie dokumentu zawierającego tę informację.

Ogólnie, to od tego momentu (a nawet już od rozpoczęcia tworzenia informacji) zaczyna się jej ścisła ochrona. Ustawa przewiduje kontrolę dostępu do niej na podstawie przydzielania odpowiednich zezwoleń przez ABW/SKW (tzw. poświadczenia bezpieczeństwa uzyskiwane po wnikliwym sprawdzeniu osoby). W miejscu jej przechowywania wymagane stają się zabezpieczenie fizyczne informacji (m. in. kancelarie tajne) oraz szkolenia w zakresie ochrony informacji oraz kontrolę stanu ich zabezpieczenia przez odpowiedzialne za nie jednostki. Ustawa zajmuje się również problematyką bezpieczeństwa teleinformatycznego.

Z systemami teleinformatycznymi spotykamy się codziennie. Są to zarówno komputery osobiste jak i serwery, urządzenia przesyłowe (np. służące sieci Internet, czy telefonii komórkowej) i towarzyszące im dodatkowe wyposażenie elektroniczne. Razem stanowią one określony system, który wykorzystywany jest do pewnych działań. Ponieważ systemy wykonując swoje funkcje nie pozostają wolne od zagrożeń, niezbędne staje się zapewnienie im bezpieczeństwa.

Bezpieczeństwo nazywane jest niekiedy stanem i procesem. Niektórzy autorzy określają bezpieczeństwo jako „obiektywną pewność gwarancji nienaruszalnego przetrwania i swobód rozwojowych”[1]. Stanisław Koziej dodaje, że w bezpieczeństwie rozumianym jako dynamiczne zjawisko, działalność podmiotu którego ono dotyczy „zmierza do zapewniania możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”[2]. Naruszenie bezpieczeństwa systemów teleinformatycznych godzi więc w gwarancję swobód przetrwania i rozwoju podmiotu, w którym urządzenia funkcjonują lub dla którego mają one istotne znaczenie. W przypadku przechowywania informacji niejawnych w systemie komputerowym może oznaczać to sprowadzenie zagrożenia zarówno dla jednostki organizacyjnej (np. starostwo, przedsiębiorstwo) jak i na podmioty trzecie, bądź nawet całe państwo, w zależności od rodzaju przechowywanych informacji. Informacje niejawne mogą trafić do niepowołanych rąk,

być publicznie ujawnione, zmodyfikowane bez uprawnień lub zniszczone albo niedostępne[3]. Zagrożenie może przyjść ze strony celowej działalności ludzkiej (służby wywiadowcze innych państw, przestępczość), błędów ludzkich (w oprogramowaniu, użytkowaniu), błędów techniki czy nawet zagrożeń naturalnych (szczególnie dla paraliżu całych systemów poprzez działania żywiołów). Zwiększanie bezpieczeństwa można tu osiągnąć poprzez stosowanie odpowiednich środków w celu wykorzystania szans (np. technologicznych), przeciwdziałanie i zapobieganie (np. szkolenia personelu) i redukcję ryzyka (np. ochrona fizyczna, kontrola dostępu).

Prawne środki bezpieczeństwa teleinformatycznego

Ochrona prawna systemów teleinformatycznych organizowana jest w Polsce przez szereg powiązanych ze sobą ustaw i rozporządzeń. Wśród najważniejszych ustaw, oprócz Ustawy o ochronie informacji niejawnych, należy wymienić także: Ustawę prawo telekomunikacyjne (z dnia 16 lipca 2004 roku), Ustawę o ochronie baz danych (z dnia 27 lipca 2001 roku), czy Ustawę o podpisie elektronicznym (z dnia 18 września 2001 roku). Rozporządzeń związanych z bezpieczeństwem teleinformatycznych jest kilkadziesiąt[4]. Dochodzą do nich także zarządzenia i wytyczne, w tym np. „Wytyczne służby kontrwywiadu wojskowego w sprawie powoływania i odwoływania kancelarii kryptograficznych (z 22 maja 2012 roku)". Nie można pominąć też norm obronnych, wyznaczających standardy ochrony. Jednak na potrzeby tematu tego opracowania oprócz UOIN najistotniejszym dokumentem jest Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku, Dz.U.2011.159.948). Wraz z Ustawą o ochronie informacji niejawnych oba dokumenty tworzą pewien model działań które zapewniają bezpieczeństwo teleinformatyczne w kontekście ochrony niejawnych informacji. W artykule zostanie podjęta próba opisania zarysu modelu, na podstawie analizy wymienionych i innych dokumentów.

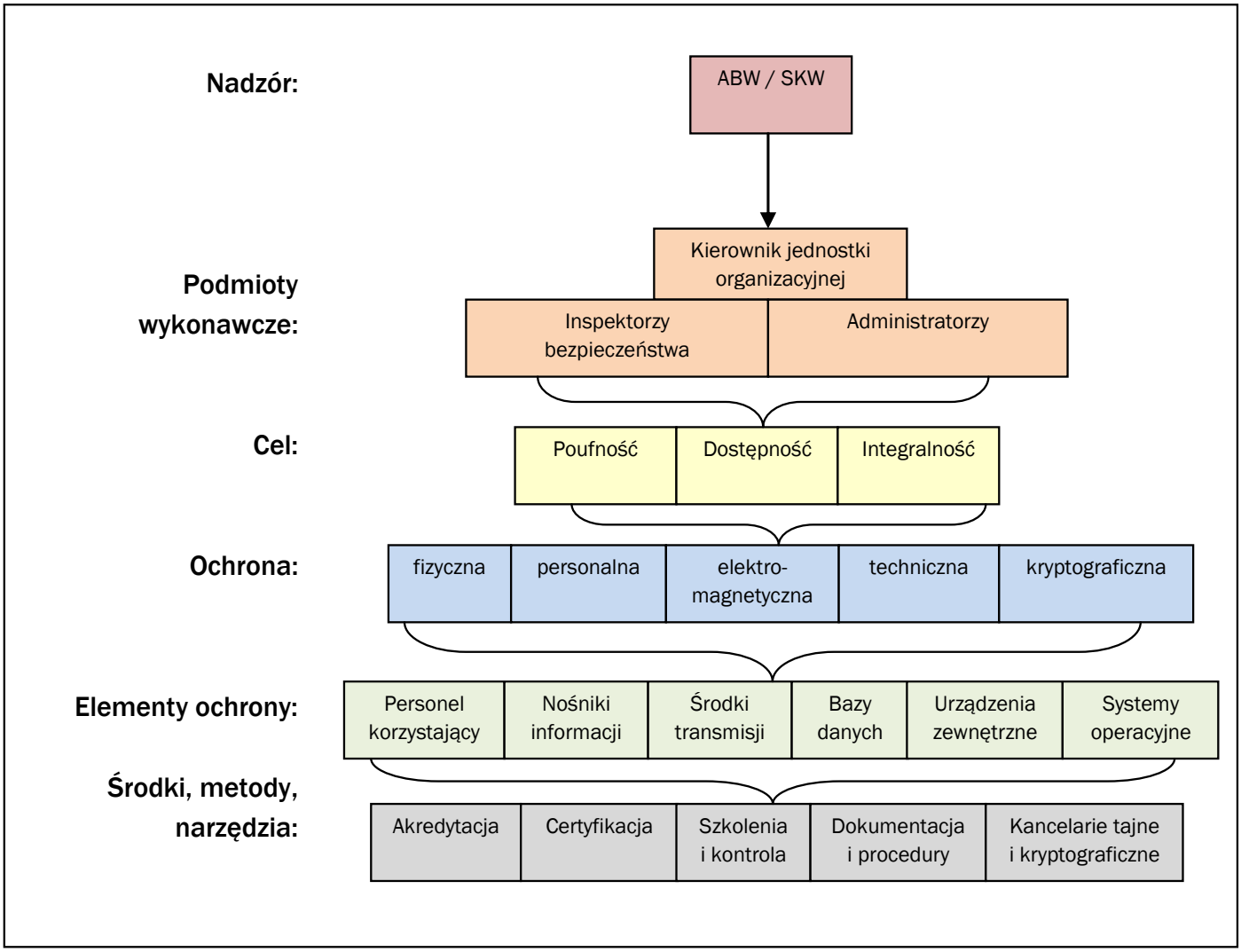
Model działań zapewniających bezpieczeństwo teleinformatyczne

Za ochronę systemów teleinformatycznych przetwarzających informacje niejawne w jednostce organizacyjnej odpowiedzialni są inspektor bezpieczeństwa telekomunikacyjnego oraz administrator. Pewne role pełnią też kierownik jednostki organizacyjnej i nadzorujące całość Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego[5]. Zadaniem osób w jednostce organizacyjnej (kierownika i powołanych przez niego inspektora i administratora) jest dbanie o bezpieczeństwo informacji niejawnych w systemie teleinformatycznym, poprzez zapewnienie temu systemowi poufności, dostępności oraz integralności[6]. Bezpieczeństwo powinno zostać zapewnione w sferze fizycznej, personalnej, elektromagnetycznej, kryptograficznej oraz technicznej[7]. Zagłębiając się w funkcjonowanie systemu teleinformatycznego można jeszcze wyróżnić poszczególne elementy ochrony, składające się na całość systemu informatycznego.

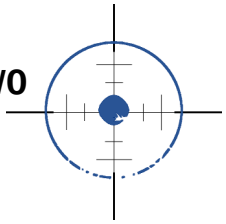
Proces bezpieczeństwa teleinformatycznego i jego etapy

Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku) wymienia pięć etapów zapewnienia bezpieczeństwa teleinformatycznego. Są to kolejno[8] planowanie, projektowanie, wdrażanie, eksploatacja i wycofywanie. Etap planowania służy określeniu przeznaczenia tego systemu, maksymalnej klauzuli do jakiej ma być dopuszczony, trybu bezpieczeństwa jego pracy, szacunkowej liczby jego użytkowników oraz lokalizację, gdzie ma

być umieszczony[9]. Na etapie projektowania szacuje się ryzyko, dokonuje odpowiedniego wyboru zabezpieczeń, uzgadnia się z podmiotem akredytującym (ABW/SKW lub kierownik jednostki organizacyjnej) plan dopuszczenia tego systemu do danej klauzuli, rodzaj i ilość odpowiednich urządzeń kryptograficznych oraz opracowuje się dokument szczególnych wymagań bezpieczeństwa[10]. Etap wdrażania dotyczy pozyskania i uruchomienia potrzebnych urządzeń i elementów wchodzących w skład systemu, przeprowadzanie testów bezpieczeństwa, dalsze szacowanie ryzyka, tworzy się dokument procedur bezpiecznej eksploatacji i uzupełnia dokument szczególnych wymagań bezpieczeństwa[11]. Następnie system poddaje się akredytacji. Etap eksploatacji to utrzymanie systemu w zgodności z jego dokumentacją, dalsze szacowanie ryzyka, okresowe przeprowadzanie testów bezpieczeństwa, wprowadzanie koniecznych zmian do systemu i dokumentacji - za zgodą ABW/SKW jeśli są to modyfikacje istotne dla bezpieczeństwa[12]. Ostatnim etapem jest wycofywanie systemu – zaprzestaje się jego



Schemat modelu działań zapewniających bezpieczeństwo teleinformatyczne w świetle Ustawy o ochronie informacji niejawnych (z dnia 5 sierpnia 2010) i Rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku).
Opracowanie własne.



eksploatacji, powiadamia ABW/SKW, oddaje im wydane przez nich świadectwo akredytacji, i usuwa informacje niejawne przechowywane w wycofywanym systemie[13].

Akredytacja bezpieczeństwa teleinformatycznego

Podstawą dopuszczenia systemu teleinformatycznego do przetwarzania informacji niejawnych jest udzielenie mu akredytacji bezpieczeństwa. Jeśli system ten ma współdziałać tylko z informacjami o klauzuli „zastrzeżone", to akredytację taką przyznaje sam kierownik jednostki organizacyjnej, któremu dany system podlega[14]. Wymogiem jest analiza oraz akceptacja dokumentacji bezpieczeństwa przez kierownika i następnie przekazanie dokumentacji do ABW/SKW. Służby mogą przedstawić, co do dokumentacji, własne zalecenia dotyczące wprowadzenia zmian polepszających bezpieczeństwo[15]. Jeśli kierownik nie dostosuje się do tych zaleceń w wystarczającym stopniu, służby mogą nakazać wstrzymanie przetwarzania informacji niejawnych w systemach[16] pomimo udzielenia im akredytacji przez kierownika. Pozwala to zapobiec sytuacji, kiedy dopuszczony do informacji „zastrzeżonych" zostanie system niespełniający minimalnych wymogów bezpieczeństwa. Natomiast, aby system informatyczny mógł przetwarzać informacje niejawne o wspominanych klauzulach „poufne" i wyższe, niezbędne jest wydanie akredytacji przez ABW/SKW. Odbywa się to po spełnieniu dwu wymogów.

Pierwszym wymogiem udzielenia akredytacji przez ABW/SKW jest pozytywna ocena dokumentacji, a drugim warunkiem jest pozytywny wynik przeprowadzonego w jednostce audytu. Akredytacja przyznawana jest na czas 5 lat. Powodem takiego okresu jest m. in. fakt, że elektronika oraz oprogramowanie wchodzące w skład systemów teleinformatycznych z roku na rok pozostają powoli w tyle za nowszymi ich wersjami, okres ten wystarcza, aby system stał się przestarzały, co negatywnie odbiłoby się na jego bezpieczeństwie. Ustawodawca zatem z góry przewidział konieczność przeprowadzania ponownej procedury udzielania akredytacji po 5 latach od jej przyznania[17].

Zadania kierownika, inspektora oraz administratora

Za ochronę informacji niejawnych w jednostce organizacyjnej odpowiada jej kierownik. Jego podstawowym zadaniem jeśli chodzi o bezpieczeństwo teleinformatyczne jest określenie, czy w podległych mu systemach teleinformatycznych lub sieciach są przetwarzane informacje niejawne, albo będą takie w przyszłości. Otrzymuje od ABW/SKW niezbędną pomoc do realizacji swoich zadań, w postaci zaleceń w zakresie bezpieczeństwa teleinformatycznego. Powiadamia te służby o incydentach zagrożenia bezpieczeństwa. Kierownik zapewnia również szkolenie osób przeznaczonych do pracy z systemem teleinformatycznym przed ich dopuszczeniem do pracy. Udziela akredytacji bezpieczeństwa systemom przeznaczonym do klauzul „zastrzeżone" - po spełnieniu wcześniej omawianych warunków. Odpowiada za przekazanie ABW/SKW dokumentacji bezpieczeństwa teleinformatycznego, akceptuje wyniki procesu szacowania ryzyka (o samym procesie analizy ryzyka będzie mowa dalej). Kierownik wyznacza pracowników pionu ochrony, którzy będą pełnić odpowiednio: funkcję inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu. Przy czym, te osoby nie mogą piastować obu funkcji jednocześnie.

Inspektor bezpieczeństwa teleinformatycznego jest odpowiedzialny za „weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej

eksploatacji”[18]. Inspektor bierze też udział w procesie szacowania ryzyka, weryfikując poprawność realizacji zadań administratora, „właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom”[19], „znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych”[20] oraz weryfikuje „stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego”[21].

Zadaniem z kolei administratora jest odpowiedzialność za „funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego”[22]. Administrator bierze też udział w tworzeniu dokumentacji bezpieczeństwa oraz w procesie zarządzania ryzykiem[23]. Realizuje szkolenia użytkowników systemu, utrzymuje zgodność systemu z jego dokumentacją i wdraża zabezpieczenia systemowe.

Uprawnienia dostępu do informacji niejawnych w systemie teleinformatycznym

Z systemu teleinformatycznego będą korzystać użytkownicy, przetwarzając za jego pomocą informacje niejawne. Z tego powodu, systemy powinny działać w różnych trybach swojej pracy, charakteryzujących się różnym poziomem bezpieczeństwa. Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku) wymienia trzy takie tryby, i są to kolejno tryb dedykowany, systemowy, i wielopoziomowy[24].

Tryb dedykowany oznacza, że wszyscy użytkownicy „posiadają uprawnienie do dostępu do informacji niejawnych o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie teleinformatycznym”[25], przy jednocześnie posiadanej ku temu uzasadnionej potrzebie. Uprawnienie to poświadczenie bezpieczeństwa.

Tryb systemowy to spełnienie pierwszego powyższego warunku, ale zakłada się, że nie wszyscy z tych użytkowników posiadają taką uzasadnioną konieczność[26].

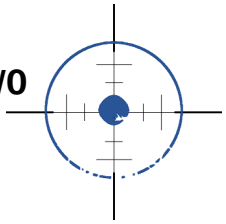
Tryb wielopoziomowy całkiem odwraca sytuację. Użytkownicy mają różne poziomy uprawnień, i różnią się w uzasadnieniu swoich potrzeb[27]. Jeśli więc system przetwarza informacje zastrzeżone, poufne i tajne, w tej konfiguracji niektórzy użytkownicy mogą mieć dostęp tylko do informacji zastrzeżonych i to w niewielkim zakresie potrzeb. System musi więc być tak skonstruowany, aby nadal zapewniał poufność, integralność i dostępność.

Ochrona fizyczna i elektromagnetyczna

Ochrona fizyczna i elektromagnetyczna dotyczy bezpieczeństwa systemu pod kątem fizycznego dostępu (nieuprawnionego, kradzieży, zniszczenia) oraz jego podsłuchu lub zakłócania za pomocą różnych środków technicznych. Bezpieczeństwo fizyczne opisywane jest w dokumencie szczególnych wymagań bezpieczeństwa, który przedstawia m. in. granice i lokalizacje stref kontrolnych i inne środki ochrony[28]. Dokument precyzuje sposoby ochrony elektromagnetycznej. Środki stosowane w tym celu dobiera się na podstawie przeprowadzonej analizy ryzyka, po uwzględnieniu zaleceń[29]. Środki takie podlegają również certyfikacji i badaniom bezpieczeństwa[30] prowadzonym przez ABW/SKW. Certyfikaty takie wydawane są na okres nie krótszy niż 3 lata, a od odmowy wydania takiego certyfikatu nie służy odwołanie.

Analiza, ocena i szacowanie ryzyka

Ryzykiem nazywa się kombinację skutków oraz ich prawdopodobieństwa. Jeśli skutki zdarzenia są wysokie, lecz prawdopodobieństwo nikłe, ryzyko przyjmuje postać niską. Lecz już średnie prawdopo-



dobieństwo przy średniej wagi skutkach daje średnie ryzyko - jednocześnie, skutki pomijalnej wagi przy wysokim prawdopodobieństwie nie czynią ryzyka wysokim. Ryzyko to bierze się z możliwych zagrożeń dla systemu informatycznego. Proces analizy, oceny i szacowania ryzyka zajmuje ważne miejsce w zadaniu zapewnienia bezpieczeństwa tym systemom.

Wyniki procesu szacowania tego ryzyka powinny znajdować się w dokumencie szczególnych wymagań bezpieczeństwa teleinformatycznego[31]. Szczególną uwagę zwraca się na możliwości wykrycia, przechwycenia lub zakłócenia transmisji danych w tym systemie. Identyfikuje się posiadane zasoby, możliwe zagrożenia, stopnie podatności, potrzebne zabezpieczenia oraz skutki wystąpienia danych zagrożeń[32]. Ryzyko należy kontrolować poprzez wdrażanie nowych zabezpieczeń i obniżanie zidentyfikowanego ryzyka, pozostawianie go bez zmian, jeśli jest to ryzyko akceptowalne, unikanie go w drodze nie podejmowania działań będących jego źródłem, bądź też w drodze przenoszenia odpowiedzialności i ryzyka na inny podmiot[33].

Uwagi końcowe

Zaprezentowany w artykule model działań zapewniający bezpieczeństwo teleinformatyczne to zaledwie wycinek całości zagadnienia. Zagłębiając się w nie, wiele miejsca poświęcić można praktycznie każdemu z jego elementów, z których nie wszystkie zostały, nawet ogólnie nakreślone. W artykule skupiono się poza tym na procesie zabezpieczenia informacji na podstawie Ustawy o ochronie informacji niejawnych oraz rozporządzeń wydanych do niej. Warto odnotować, iż nie jest to jedyny dokument dotyczący tych kwestii. Przykładem jest norma ISO/IEC 27001 regulująca tworzenie SZBI (Systemu zarządzania bezpieczeństwem informacji), mająca szerokie zastosowanie w przedsiębiorstwach zainteresowanych ochroną swoich wrażliwych informacji, choć nie będących niejawnymi z punktu widzenia omawianej Ustawy.

Przypisy

1 R. Jakubczak, J. Flis, Bezpieczeństwo narodowe Polski w XXI w. Warszawa 2006, s. 16.
2 S. Koziej, Między piekłem a rajem: szare bezpieczeństwo na progu XXI w., Toruń 2006, s. 7.
3 K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, s. 13. Warszawa 2008.
4 Zob. Systemy teleinformatyczne - przepisy, strona www. Źródło online: [http://www.iniejawna.pl/przyciski/tele_info.html], dostęp: 2013-08-04. Autorzy strony wymieniają ponad 50 ustaw i rozporządzeń jako związanych z bezpieczeństwem teleinformatycznym.
5 Agencja Bezpieczeństwa Wewnętrznego odpowiada za jednostki cywilne, a Służba Kontrwywiadu Wojskowego za jednostki wojskowe. Dzieje się tak, ponieważ ABW można uznać za kontrwywiad cywilny, a ABW - za kontrwywiad wojskowy. Pod ABW podlegają więc w ochronie informacji niejawnych takie podmioty jak starostwa, gminy, urzędy miejskie, ale także Policja. Pod SKW podlegają jednostki wojskowe, ale też Żandarmeria Wojskowa.
6 Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. § 5. 1. (Dz.U.2011.159.948)
7 Zob. K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych..., wyd. cyt.., s. 14. Autor wymienia sferę fizyczno-techniczną, sprzętowo-programową, i organizacyjno-kadrową.
8 Rozporządzenie... § 18. 1.
9 Tamże, § 18. 2.
10 Tamże, § 18. 3.
11 Tamże, § 18. 4.
12 Tamże, § 18. 5.
13 Tamże, § 18. 6.
14 Ustawa o ochronie informacji niejawnych, art. 48, ust. 9 (Dz.U. 2010 nr 182 poz. 1228)
15 Tamże, art. 48, ust. 11-12.
16 Tamże, art. 48, ust. 12.
17 Tamże, art. 48, ust. 2.
18 UOIN, art. 52. ust. 1, p. 1.
19 Rozporządzenie... § 14. p. 1.
20 Tamże, § 14. p. 2.
21 Tamże, § 14. p. 3.
22 UOIN, art. 52. ust. 1, p. 2.
23 Rozporządzenie... § 13.
24 Tamże, § 3.
25 Tamże, § 3, ust. 1.
26 Tamże, § 3, ust. 2.
27 Tamże, § 3, ust. 3.
28 Rozporządzenie... § 25, ust. 3, p. 5.
29 tamże, § 8, ust. 1.
30 UOIN, art. 50. Ust. 1. Tutaj jak z rozporządzeniem
31 Tamże, art. 49, ust. 1.
32 Rozporządzenie... § 20. ust. 1.
33 Rozporządzenie... § 21. ust 1.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 5/2013 (17)]

BERNADETTA TERLECKA

Zastosowanie analizy urządzeń mobilnych w kryminalistyce

Analiza śledcza urządzeń mobilnych jest dziedziną cyfrowej analizy śledczej ukierunkowanej na odzyskiwanie cyfrowych dowodów z urządzeń mobilnych. Mówiąc lub myśląc urządzenia mobilne zwykle przed oczyma stają nam telefony komórkowe. Ten zwrot oznacza jakiekolwiek urządzenie cyfrowe, które posiada pamięć wewnętrzną i może służyć do komunikacji, włączając w to urządzenia typu PDA, GPS czy tablety.

Fakt wykorzystywania telefonów podczas planowania lub wykonywania przestępstw jest niezaprzeczalny i od dawna o tym wiadomo. Jednak analiza urządzeń mobilnych jest bardzo młodą dziedziną (powstałą pod koniec lat 90). Rozwój urządzeń przenośnych na rynku konsumenckim (smartfony, tablety) wymusił konieczność opracowania nowych technik analizy urządzeń mobilnych, gdyż istniejące, nie pozwalały na uzyskanie pełnych danych z urządzenia[1].

Telefony komórkowe mogą być używane do zapisywania różnego rodzaju informacji, takich jak: kontakty, zdjęcia, nagrania wideo, kalendarze, notatki, SMS'y czy MMS'y. Smartfony dodatkowo mogą zawierać dane o przeglądanych stronach internetowych, lokalizacji (GPS) czy komunikaty z portali społecznościowych lub wiadomości poczty elektronicznej.

Istnieje wiele wyzwań na polu dowodowym i technicznym, a analiza śledcza urządzeń mobilnych dostarcza nam problemów na wielu płaszczyznach[2]. Jednym z największych jest lokalizacja telefonu komórkowego na podstawie jego użytkowania. Metody wykorzystywane do tego celu nie są metodami naukowymi. W konsekwencji możliwa jest tylko przybliżona lokalizacja urządzenia na podstawie określenia strefy komórkowej, z której połączenie zostało wykonane lub gdzie zostało odebrane.

Przenośny write-blocker połączony z twardym dyskiem.
Fot. ErrantX, commons.wikimedia.org

Na tej podstawie nie można określić dokładnej lokalizacji telefonu podczas odbierania lub wykonywania rozmowy jednak można zawęzić teren poszukiwania lub przypuszczać, że dana osoba mogła być na miejscu zdarzenia.

Producenci sprzętu, by pozostać konkurencyjni, zaczęli wprowadzać nowe struktury i systemy plików, usługi przechowywania danych, urządzenia peryferyjne, złącza czy kable, w rezultacie eksperci śledczy muszą używać całkiem innych metod i narzędzi niż śledczy pracujący nad sprzętem komputerowym.

Ponadto, pojemność urządzeń rośnie, dzięki zapotrzebowaniu na coraz mocniejsze urządzenia typu „mini komputer"[3]. Ewoluują też nie tylko typy danych, ale także sposób, w jaki urządzenia mobilne są wykorzystywane.

W wyniku tych wyzwań powstało wiele narzędzi pozwalających na wyodrębnienie dowodów z urządzeń mobilnych, nie ma jednej metody skutecznej wobec każdego urządzenia. W związku z czym bardzo ważne jest przeprowadzanie intensywnych szkoleń dla ludzi mających zostać eksper-

tami sądowymi w dziedzinie pozyskiwania danych cyfrowych. Szkolenia te mają na celu zapoznanie z narzędziami i sposobem ich obsługi oraz pozyskiwania dowodów, utrzymywania standardów i spełniania wymogów prawnych.

Historia

Dziedzina analizy urządzeń mobilnych jak wspomniałam pochodzi z późnych lat 90 ubiegłego wieku i początków obecnego. Rola telefonów komórkowych w zbrodni już dawno została uznana przez organy ścigania za bardzo ważną. Wraz ze wzrostem dostępności tego typu urządzeń na rynku konsumenckim oraz szeroką gamą platform komunikacyjnych obsługiwanych przez nie, np. poczta elektroniczna czy strony WWW, oprogramowanie VoIP, wzrosło też zapotrzebowanie analizy tych urządzeń[4].

Wczesne formy analizy urządzeń mobilnych były zbliżone do metod analizy pierwszych komputerów, czyli analiza polegała na sprawdzeniu zawartości telefonu przy użyciu klawiatury i wyświetlacza, fotografując jednocześnie ważne dla śledztwa treści[5], takie czynności okazały się jednak bardzo czasochłonne, szczególnie gdy liczba urządzeń poddawanych analizie zaczynała wzrastać. Śledczy domagali się skuteczniejszych metod pozyskiwania dowodów. Niekiedy korzystali telefonów komórkowych lub urządzeń w stylu PDA synchronizując oprogramowanie i dane lub po prostu sprawdzali komputer podejrzanego pod kątem istnienia właśnie danych z urządzenia mobilnego. Jednak to oprogramowanie może tylko odczytywać i zapisywać dane z telefonu, nie może jednak odzyskać skasowanych danych.[6]

Niektórzy eksperci sądowi twierdzili, że są w stanie odzyskać nawet usunięte dane za pomocą urządzeń opracowanych przez producentów, nazywanych „flasher" lub „twister". Urządzenia te służyły do testowania i aktualizacji pamięci telefonów, jednak są to urządzenia inwazyjne, mogące naruszać dane oraz skomplikowane w obsłudze, gdyż zostały zaprojektowane do zupełnie innych celów niż narzędzia śledcze[7]. Dla fizycznej analizy konieczne było stworzenie lepszej alternatywy.

Informatyka śledcza nie jest ograniczona tylko do komputerowych mediów i nośników danych. Fot. agr, commons.wikimedia.org

By sprostać tym wymaganiom powstały komercyjne narzędzia, które pozwoliły śledczym odzyskiwać dane z pamięci telefonu przy minimalnych stratach i analizować je poza urządzeniem bazowym[8]. Z biegiem czasu i rozwojem technik analitycznych, odzyskiwanie danych stało się możliwe dzięki specjalistycznym narzędziom, które dodatkowo automatyzowały wiele procesów ekstrakcji danych, czyniąc odzyskiwanie procesem stosunkowo łatwym.

Rodzaje dowodów

Wraz z rozwojem technologii urządzeń mobilnych coraz więcej typów danych zaczęło się pojawiać w pamięciach tychże urządzeń. Ilość potencjalnych danych odzyskanych z telefonu komórkowego drastycznie wzrosła i mogła pochodzić z pamięci telefonu, kart SIM czy rozszerzeń pamięci telefonu w postaci kart pamięci SD/MMC.

Tradycyjne techniki analizy telefonów komórkowych powstały w oparciu o pozyskiwanie wiadomości SMS czy MMS oraz listy połączeń, kontaktów i numerów IMEI/ESN telefonu. Nowsze generacje telefonów - smartfony - zawierają również inne potencjalnie ważne dane:

- historię przeglądanych stron,
- ustawienia sieci bezprzewodowych,
- informacje geolokacyjne (włączając w to geotagi dodawane do zdjęć wykonanych aparatem),
- wiadomości poczty elektronicznej,
- wiadomości i kontakty portali społecznościowych
- inne dane przekazywane za pomocą sieci czy „zapamiętane" w aplikacjach.

Pamięć wewnętrzna

Obecnie najczęstszymi technologiami wykonania pamięci flash dla telefonów komórkowych są technologie NAND lub NOR. Dokładny ogląd na analizy pamięci NAND sporządził Salvatore Fiorillo w roku 2009[9].

Pamięć zewnętrzna

Zewnętrznymi nośnikami pamięci są karty SIM, karty SD/MMC/CF (spotykane tak w urządzeniach nawigacji satelitarnej GPS jak i w telefonach) czy pamięciach USB.

Logi usługodawcy

Jednym z elementów analizy śledczej urządzeń mobilnych są informacje dotyczące połączeń czy wiadomości tekstowych uzyskane od operatora. Dane te mogą służyć jako swoista „kopia zapasowa" rejestru połączeń i wiadomości, jeśli te zostaną usunięte z pamięci telefonu, lub, gdy usługi oparte na lokalizacji są wyłączone. Rekordy dotyczące połączeń oraz użytych nadajników mogą posłużyć do ustalenia przybliżonej lokalizacji telefonu w danym czasie oraz tego, czy się przemieszczał[10]. Nośnik danych oraz dane zebrane razem, mogą być wykorzystane do potwierdzenia informacji z innych źródeł, przykładowo z nagrań monitoringu, lub do uzyskania przybliżonej lokalizacji wykonania zdjęć bez geotagów.

Unia Europejska wymaga od krajów członkowskich przechowywania przez pewien czas danych telekomunikacyjnych stosowanych w dochodzeniach. Dane te zawierają informacje na temat odbieranych i nawiązywanych połączeń telefonicznych. Na ich podstawie możliwa jest przybliżona lokalizacja telefonu komórkowego. W Stanach Zjednoczonych Ameryki Północnej nie ma takich wymogów. Prawo nie reguluje tam jak długo usługodawcy powinni zachować dane ani co one mają zawierać. Przykładowo: wiadomości tekstowe mogą być przechowywane dzień czy dwa, natomiast dzienniki połączeń mogą być przechowywane przez kilka tygodni lub miesięcy. Funkcjonariusze chcący zmniejszyć ryzyko, że dane zostaną utracone, muszą przedstawić oficjalnie swoje zamiary usługodawcy, aby ten sporządził kopię danych, która zostanie przekazana policji po uzyskaniu przez nią nakazu[11].

Proces analizy

Proces analizy urządzeń mobilnych graniczy i pokrywa się z wieloma dziedzinami informatyki śledczej, niektóre metody nie są stosowane nigdzie indziej. Generalnie proces można podzielić na trzy etapy:

- przejęcie;
- pozyskanie;
- badania i analizy.

Inne aspekty komputerowej analizy sądowej, takie jak sporządzenie dokumentacji, walidacja, czy archiwizacja nadal obowiązują[12].

Przejęcie

Przejęcie urządzeń mobilnych objęte jest takimi samymi przepisami jak innych nośników cyfrowych.

Telefony komórkowe często przejmowane są w stanie włączonym, ich transport do analizy powinien być przeprowadzony w tym samym stanie co przejęcie, by nie doprowadzić do zamykania aplikacji, które mogą zmienić część plików, a tym samym pozbawić śledczych dowodów[13].

Jednakże pozostawienie włączonego telefonu niesie ryzyko, że połączenia będą nadal przychodzić i dane dowodowe mogą zostać zastąpione nowymi. W celi nie dopuszczenia do tego typu incydentów, urządzenia mobilne powinny być transportowane i badane wewnątrz klatki Faradaya. Takie rozwiązanie ma jednak dwie wady:

1. pomimo tego, że urządzenie nadaje się do użytku, jego ekran dotykowy lub klawiatura, nie mogą być stosowane;
2. urządzenie szukając połączenia do sieci przełączy się na maksymalną moc nadawczą, co spowoduje szybsze wyczerpanie baterii.

Urządzenia i ich baterie można ładować ponownie, lecz istnieje ryzyko włączenia blokady telefonu. Dlatego, zaleca się izolowanie urządzenia przez wejście w tryb samolotowy i klonowanie karty SIM[14].

Pozyskanie

Drugim etapem procesu jest pozyskanie materiałów z urządzenia – porównując do informatyki śledczej, wykonanie kopii bitowej urządzenia[15].

Ze względu na charakterystykę telefonów komórkowych, często nie jest możliwe pozyskanie jakichkolwiek danych z wyłączonego urządzenia. Większość danych pozyskuje się „na żywo". W pracy z bardziej zaawansowanymi smartfonami wykorzystującymi zaawansowane zarządzanie zasobami, podłączenie ich do ładowarki i włożenie do klatki Faradaya nie jest najlepszym pomysłem. Urządzenie jest w stanie rozpoznać odłączenie od sieci

Jedno z urządzeń stosowanych w informatyce śledczej
Fot. Fairycherry, commons.wikimedia.org

i zmienić status managera pamięci, który będzie nadpisywał dane nowymi[16].

Większość rozwiązań służących do pozyskiwania danych ma charakter komercyjny i składa się z programowania i sprzętu, bardzo często połączonych ze sobą i zautomatyzowanych.

Badania i analizy

Coraz więcej urządzeń mobilnych wykorzystuje systemy pliku wyższego poziomu, podobne do systemu plików znanych z komputerów. Metody i narzędzia służące do analizy mogą być te same (niektóre po drobnych zmianach) co w przypadku kryminalistyki dysków twardych[17].

System plików FAT jest powszechnie stosowany przy wykorzystaniu pamięci typu NAND.[18] Różnicą jest rozmiar użytego bloku, który jest większy niż 512 bajtów, w przypadku dysków twardych. W zależności od zastosowanego rodzaju pamięci, rozmiar bloku wynosi 64, 128 lub 256 kilobajtów dla pamięci typu NOR oraz 16, 128, 256 lub 512 kB dla pamięci typu NAND.

Do pozyskiwania danych z obrazu pamięci mogą służyć różne narzędzia programowe. Można do tego

celu użyć zautomatyzowanych, specjalistycznych programów do analizy śledczej, lub zwykłych edytorów i przeglądarek plików w formacie szesnastkowym, przeszukując pliki pod kątem konkretnych, charakterystycznych nagłówków. Zaletą edytorów heksadecymalnych jest głębszy wgląd w zarządzenie pamięcią, lecz praca z nim wymaga wielu zabiegów wykonywanych ręcznie oraz sporej wiedzy o budowie nagłówków plików. W przeciwieństwie do tego, zautomatyzowane oprogramowanie śledcze upraszcza wyszukiwanie i ekstrakcję danych, lecz może się zdarzyć, że oprogramowanie pominie jakiś plik. Przykładowymi programami do ekstrakcji danych z obrazu pamięci mogą być AccessData, Sleuthkit czy EnCase[19]. Ponieważ nie ma obecnie oprogramowania, które wyodrębni wszystkie możliwe dane, zaleca się, aby przeprowadzić analizę kilkoma różnymi programami po sobie[20].

Typy przejęcia danych

Wyodrębnianie danych z telefonów komórkowych może być sklasyfikowane według pewnej własności, która mówi, że kolejne metody będą coraz bardziej techniczne, narzędzia będą coraz droższe, analizy będą trwały więcej czasu, a śledczy będą musieli przebyć więcej szkoleń, niektóre metody staną się też bardziej inwazyjne.[21]

Pozyskanie ręczne

Śledczy wykorzystuje interfejs użytkownika, aby zbadać zawartość pamięci telefonu, dlatego urządzenie używane jest normalnie, a śledczy filmuje lub fotografuje jego zawartość. Metoda ta ma tą zaletę, że system operacyjny sprawia, iż nie potrzeba żadnych specjalistycznych narzędzi lub sprzętu, by przekształcić surowe dane na takie, które są możliwe do zrozumienia przez człowieka. W praktyce, metoda ta jest stosowana dla telefonów komórkowych, PDA czy nawigacji GPS[22]. Wadą tej metody jest to, że tylko dane widoczne w systemie operacyjnym urządzenia mogą być odzyskane.

Dane pozyskane z wykorzystaniem tej metody są w formie zdjęć lub filmu, a sama metoda jest bardzo czasochłonna.

Pozyskanie logiczne

Pozyskanie logiczne oznacza wykonanie kopii logicznej (bit za bitem) obiektów, np. plików czy katalogów, znajdujących się w przestrzeni logicznej urządzenia (np. na partycji systemowej).

Pozyskanie logiczne ma tą zaletę, że struktury danych są łatwiejsze do przeglądania i wyodrębniania z nich danych przez różnego rodzaju programy. Wyodrębnianie logiczne polega na wykorzystaniu narzędzi dostarczonych przez producenta sprzętu do synchronizacji danych między urządzeniem mobilnym a komputerem osobistym. Pozyskiwanie logiczne, jest stosunkowo łatwe, lecz specjalista śledczy, jest w stanie pozyskać więcej informacji podczas ekstrakcji fizycznej (ręcznej).

Przejęcie systemu plików

Ekstrakcja logiczna zazwyczaj nie pozwala na wyodrębnienie jakichkolwiek usuniętych danych, które zostały usunięte przez system telefonu. Jednak w niektórych przypadkach, szczególnie w przypadku systemów opartych i SQLite, czyli iOS oraz Android, telefon może zachować pliki baz danych i oznaczyć je jako usunięte, do późniejszego nadpisania. W przypadku dostępu tylko z poziomu oprogramowania do synchronizacji, nie jest możliwy dostęp do tego typu danych. Przejęcie systemu plików jest przydatne do ustalenia i zrozumienia struktury katalogów i plików, umożliwia przejrzenie historii przeglądanych stron czy używanych aplikacji. Umożliwia również śledczym analizę w bardziej tradycyjny sposób, znany z informatyki śledczej[23].

Fizyczne przejęcie

Przejęcie fizyczne oznacza dokładną (bit za bitem) kopię całego fizycznego nośnika danych, np. pamięci flash, metoda ta jest najbardziej podobna do badania komputerów osobistych. Przejęcie fizyczne ma tę zaletę, że można zbadać pozostałości usuniętych danych czy plików. Podczas wyodrębniania fizycznego uzyskiwane informacje pochodzą bezpośrednio z pamięci urządzenia.

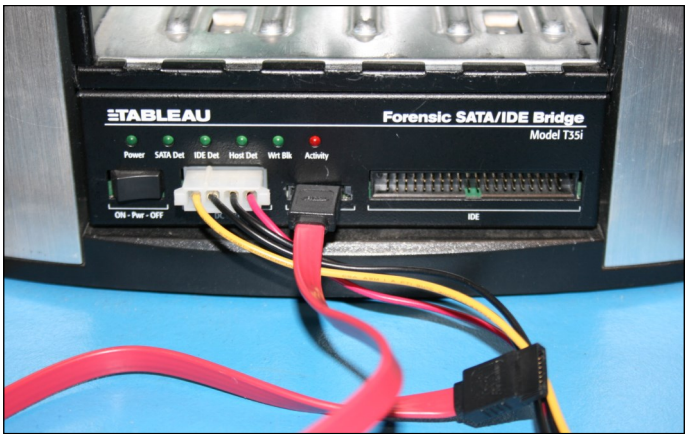
Jest to dość wymagające i trudne rozwiązanie, gdyż producenci sprzętu zwykle zabezpieczają sprzęt przed bezpośrednim dostępem do pamięci, dlatego też, urządzenie może być zablokowane a dostęp do niego może być możliwy tylko dla konkretnego operatora. W celu obejścia tego rozwiązania, narzędzia służące do analizy urządzeń mobilnych zawierają swój własny boot loader (program rozruchowy), dający narzędziu dostęp do pamięci, często obchodząc hasła użytkownika czy wzór klucza[24].

Na przejęcie fizyczne składają się dwie fazy: faza zrzutu, gdzie klonowana (zrzucana) jest zawartość pamięci urządzenia oraz faza faktycznego dekodowania danych.

Narzędzia

Wczesne śledztwa bazowały na ręcznej analizie działających urządzeń mobilnych, podczas której śledczy fotografowali lub opisywali przydatne materiały dowodowe. Z pominięciem fotografii rozwiązania takie jak Fernico ZRT, eDEC Eclipse czy Project-a-Phone posiadały niezaprzeczalną wadę: istniało wysokie ryzyko modyfikacji zawartości urządzenia, jak i to, że narzędzia te pozostawiały części własnego systemu operacyjnego w pamięci urządzenia.

W ostatnich latach pojawiło się wiele oprogramowania czy sprzętu potrafiącego dokonać przejęcia logicznego czy fizycznego z urządzeń mobilnych. Wiele z tych narzędzi to zarówno oprogramowanie jak i sprzęt, włączając w to odpowiednie kable połączeniowe do telefonów różnych producentów. Oprogramowanie tych narzędzi jest w stanie wyodrębnić, zewidencjonować i często przeanalizować odzyskane dane.



Jedno z urządzeń stosowanych w informatyce śledczej
Fot. Errantx, commons.wikimedia.org

Dziedzina narzędzi analizy śledczej urządzeń przenośnych dobrze się rozwija w ostatnich latach. Ma to związek między innymi z zapotrzebowaniem jednostek antyterrorystycznych i wojskowych szybkiego rozpoznawania jednostek terrorystycznych, zbierania danych w miejscach przestępstw, wyszukiwania powiązań czy podczas natychmiastowego przeszukania. Narzędzia takie muszą być też zdolne do pracy w trudnych warunkach, np. na polu bitwy a ich konstrukcja wzmocniona (wodoodporna, odporna na uderzenia, itd.)[25].

Ogólnie rzecz biorąc, z powodu niemożliwości stworzenia przez obecną technikę jednego narzędzia zdolnego analizować wszystkie typy urządzeń przenośnych, zalecane jest, by specjaliści śledczy mieli opracowane zestawy składające się z narzędzi komercyjnych, Open-Source, o szerokim i wąskim spektrum kompatybilnych urządzeń oraz akcesoriów takich jak baterie czy ładowarki, torby Faradaya lub innych środków tłumiących sygnał itp[26].

Narzędzia komercyjne

Do narzędzi komercyjnych należą m. in:

- AccessData's MPE+,
- Logicube CellXtract,
- Cellebrite UFED,
- Micro Systemation XRY,
- MOBILedit! Forensic,
- FINALDATA FINALMobile Forensics,
- Radio Tactics' Athena,
- Oxygen Forensic Suite,
- Paraben Device Seizure,
- Susteen SecureView
- produkty Aceso.

Niektóre narzędzia zostały wyprodukowane specjalnie do analizy urządzeń produkowanych w Chinach, czyli tak zwanych „chińskich podróbek". Urządzenia takie są oparte o chipsety Mediatek (MTK), Mstar i Spreadtrum. Narzędzia te mają wbudowane rozwiązania Cellebrite's CHINEX oraz eDEC's Tarantula, podczas gdy inne rozwiązania mają po prostu dodaną obsługę kilku chińskich telefonów do oprogramowania.

Narzędzia Open Source

Większość Open Source'owych narzędzi analizy śledczej urządzeń mobilnych jest zorientowanych na analizę konkretnej platformy smartfonów. Przykładowymi aplikacjami są:

- iPhone Analyzer,
- Katana Forensics' Lantern Lite imager,
- viaForensics' Open Source Android Forensics,
- the Mobile Internal Acquisition Tool
- TULP2G.

Aplikacja BitPim, choć nie została zaprojektowana jako narzędzie śledcze, jest szeroko stosowana z telefonami CDMA, LG VX440, LG VX6000 oraz wieloma telefonami Sanyo Sprint[27].

Narzędzia fizyczne

Wylutowanie

Technika powszechnie znana jako „Chip-Off", jest ostatnią, najbardziej inwazyjną metodą dostępu do obrazu pamięci urządzenia. Metoda ta polega na wylutowaniu kości nie ulotnej pamięci i podłączeniu jej do czytnika. Użycie tej metody niesie ze sobą potencjalne ryzyko całkowitej utraty danych, gdyż jest możliwe zniszczenie całej kości pamięci w związku z ciepłem potrzebnym podczas procesu wylutowywania.

Wylutowanie kości jest procesem wolnym i wymagającym uwagi, by nie zniszczyć pamięci i danych. Przed przystąpieniem do wylutowania płytka drukowana jest wygrzewana, by odparować z niej ewentualne drobiny wilgoci. Zapobiega to tak zwanemu efektowi popcornu, w którym woda lub wilgoć może uszkodzić kość podczas wylutowywania.

Są trzy podstawowe metody topienia cyny:

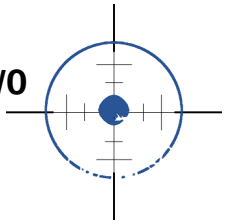
- gorące powietrze,
- światło podczerwone
- parowa.

Technologia podczerwona działa na zasadzie skupionego światła podczerwonego skierowanego na konkretny podzespół i jest stosowana do małych kości. Metody parowa i gorącego powietrza nie mogą być skupione na konkretnej kości, jak w przypadku metody podczerwonej.

Ponowne wlutowanie

Po wylutowaniu kości, proces ponownego wlutowania rozpoczyna się od czyszczenia jej oraz dodania nowych kulek cyny na styki. Ponowne wlutowanie można przeprowadzić na różne sposoby.

Pierwszym jest użycie wzornika. Wzornik jest zależny od kości i musi idealnie pasować. Następ-



nie nakładana jest na niego cienka warstwa pasty lutowniczej. Po wystudzeniu wzornik jest usuwany i w razie potrzeby następuje ponowny proces czyszczenia.

Drugą metodą jest wlutowanie laserowe[28, 29, 30]. Tutaj wzornik jest zaprogramowany w jednostce lutującej. Głowica lutująca automatycznie ładuje kulkę cyny z pojemnika, następnie kulka ta jest ogrzewana laserowo do momentu przejścia w stan ciekły i spływa na oczyszczony układ. Natychmiast po stopieniu kulki laser wyłącza się, a nowa kulka cyny wpada do głowicy lutującej. Podczas przeładowania głowicy zmienia ona jednocześnie pozycję nad inny pin do przylutowania.

Zaletą wylutowania przez śledczych jest to, że urządzenie nie musi być sprawne a i tak można wykonać kopię bez wprowadzania zmian w danych. Wadą natomiast jest to, że ponowne wlutowanie jest drogie, przez co proces ten jest kosztowny i niesie ze sobą ryzyko całkowitej utraty danych. Wylutowanie podczas dochodzenia powinno być wykonane jedynie w laboratoriach posiadających doświadczenie w rozwiązywaniu tego typu problemów.[31]

JTAG

Istniejące, ustandaryzowane interfejsy odczytu danych są zbudowane dla pojedynczych typów urządzeń, przykładowo do odczytania pozycji z lokalizatorów GPS czy do pobrania informacji z jednostki sterującej poduszkami powietrznymi[32].

Nie wszystkie urządzenia mobilne zapewniają taki ustandaryzowany interfejs, nie istnieje też standardowy interfejs dla wszystkich urządzeń mobilnych. Producenci mają jeden wspólny problem - miniaturyzację. Otwartą kwestią jest to, jak automatycznie testować funkcjonalność i jakość lutowanych elementów. Z tego powodu grupa JTAG (Joint Test Action Group) opracowała technologię testową zwaną skanowaniem granic (boundary scan).

Pomimo normalizacji przed interfejsem JTAG są stawiane cztery zadania. Technologia ta może być użyta do odzyskania pamięci. By znaleźć poprawne bity podczas skanowania granic rejestru należy wiedzieć, które układy procesora i pamięci są stosowane oraz jak są podłączone do magistrali systemowej. Jeżeli nie są dostępne z zewnątrz, należy znaleźć punkty testowe JTAG na płytce drukowanej oraz określić, którego testu można użyć dla konkretnego sygnału. Porty dostępowe TAG nie zawsze są wlutowane razem ze stykami, czasem konieczne jest otwarcie urządzenia i przelutowanie ich[33]. Protokół odczytu pamięci musi być znany, ostateczne poprawne napięcie musi być wymuszone, by zapobiec uszkodzeniu urządzenia[34].

Skanowanie granic daje kompletny obraz ulotnej i nieulotnej pamięci. Ryzyko zmiany danych jest zminimalizowane, a kość pamięci nie musi być wylutowana. Generowanie obrazu może być procesem czasochłonnym, ponadto nie wszystkie urządzenia mobilne posiadają aktywny JTAG, co za tym idzie, znalezienie portu dostępowego może to być trudne[35].

Narzędzia linii komend – Komendy systemowe

Urządzenia mobilne nie wspierają możliwości uruchamiania bądź rozruchu z dysku CD, podłączonego udziału sieciowego bądź innego urządzenia. Z tego powodu polecenia systemowe mogą być jedyną drogą do zapisu trwałej pamięci urządzenia. Ryzyko zmodyfikowania pamięci przez wykonanie poleceń systemowych musi być określone, jeśli dane pamięci ulotnej są istotne. Podobny problem pojawia się, gdy żadna sieć nie jest podpięta i nie ma możliwości podpięcia żadnej dodatkowej pamięci do urządzenia, gdyż pamięć ulotna musi być od razu zapisana w wewnętrznej pamięci nieulot-

nej, w której przechowywane są również dane użytkownika i najprawdopodobniej ważne, usunięte dane zostaną nadpisane i utracone. Polecenia systemowe to najtańsza metoda, lecz może oznaczać pewne ryzyko utraty danych. Każde użyte polecenie musi zostać udokumentowane wraz z wykorzystanymi opcjami.

Komendy AT

Polecenia AT są poleceniami używanymi w starych modemach, przykładowo zestaw poleceń Hayes oraz polecenia telefonów AT Motorola mogą być wykorzystywane tylko na urządzeniach modemowych. Przy pomocy tych poleceń można uzyskać informacje tylko o systemie operacyjnym, żadne usunięte dane nie mogą zostać odzyskane[36].

DD

Dla pamięci zewnętrznych i urządzeń USB typu Flash odpowiednie oprogramowanie, przykładowo polecenie dd występujące w powłoce systemów Unix/Linux, może wykonać kopię na poziomie bitów. Ponadto kości USB z ochroną pamięci nie wymagają dodatkowego sprzętu i mogą być podpięte do dowolnego komputera. Wiele dysków USB i kart pamięci posiada blokadę zapisu w formie fizycznego przełącznika na obudowie, przełącznik ten może zostać użyty jako zabezpieczenie przed zmianami w pamięci podczas wykonywania kopii.

Jeżeli dysk USB nie posiada przełącznika zabezpieczającego można użyć trybu montowania dysku tylko do odczytu, lub w wyjątkowych przypadkach, kość pamięci może zostać wylutowana. Karty SIM i karty pamięci wymagają użycia specjalnego czytnika do wykonania kopii. Karty SIM są gruntownie analizowane, możliwe jest wykonanie kopii (odzyskanie) usuniętych kontaktów czy wiadomości tekstowych[37].

Komercyjne narzędzia niespecjalistyczne: Narzędzie flasher

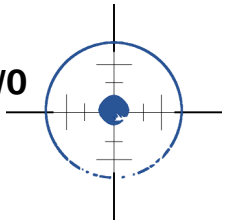
Narzędzie „flasher" jest programistycznym narzędziem, które może zostać użyte do oprogramowania pamięci, przykładowo EEPROM lub pamięci flash. Narzędzia te pochodzą głównie od producentów, centrów diagnostycznych lub serwisowych. Mogą one zastąpić pamięć nieulotną, a niektóre, zależnie od producenta lub urządzenia, mogą również odczytać pamięć czy wykonać jej kopię. Pamięć może być zabezpieczona przed odczytem przykładowo za pomocą oprogramowania bądź przez zniszczenie bezpieczników w obwodzie odczytu[38].

Uwaga, to nie przeszkadza zapisywać w pamięci lub używać pamięć wewnętrzną przez CPU. Narzędzia flasher są proste w podłączeniu i użyciu, jednak niektóre mogą zmieniać dane, zawierać niebezpieczne opcje lub nie wykonywać kompletnej kopii[39].

Podsumowanie

Generalnie nie istnieje standard wspierający wszystkie urządzenia. Doprowadziło to do sytuacji, w której komponenty różnych producentów są inaczej obsługiwane. Sytuacja ta znacznie utrudnia porównywanie z listą wspieranych urządzeń. Przykładowo: urządzenie, w którym logiczna ekstrakcja umożliwia wyodrębnienie wykonanych połączeń może być wymienione jako wspierane, podczas gdy inne urządzenie, również znajdujące się na liście, dostarczy znacznie mniej informacji.

Ponadto, różne produkty mogą wyodrębniać różne ilości informacji z różnych urządzeń. Prowadzi to do złożoności prób ich pozyskania. Na ogół prowadzi to do sytuacji, w której testowanie produktu przed zakupem jest zdecydowanie obszer-



niejsze i nie sprowadza się do testów jednego urządzenia lub oprogramowania, lecz do dwóch lub więcej, wzajemnie się uzupełniających.

Przeciwdziałanie śledczym jest dość trudne ze względu na małe rozmiary urządzeń oraz ograniczenia użytkownika[40]. Niemniej jednak istnieją sposoby zabezpieczenia sprzętowego pamięci oraz zabezpieczenie obwodów CPU i kości pamięci nawet do tego stopnia, że kość nie będzie działać po wylutowaniu[41 42].

Przypisy

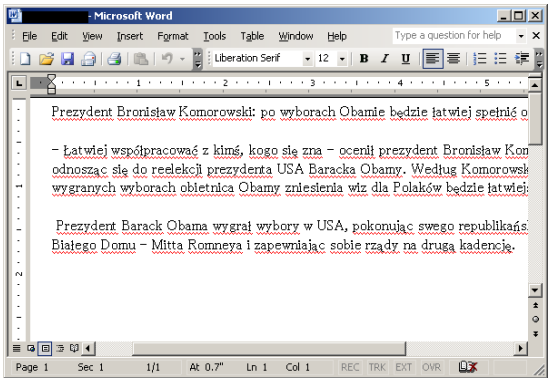
1 E. Casey, Cyfrowe Dowody i przestępstwa komputerowe, 2004.
2 C. Murphy, Cellular Phone Evidence Data Extraction and Documentation, http://www.mobilhttp://www.mobileforensicscentral.com/mfc/documents/Cell%20Phone%20Evidence%20Extraction%20Process%202.0%20with%20forms.pdf z dnia 10.04.2013.
3 T. Hayley, Two-thirds of mobile buyers have smartphones,
4 E. Casey, Cyfrowe Dowody i przestępstwa komputerowe, 2004.
5 E. Casey, Cyfrowe Dowody i przestępstwa komputerowe, 2004.
6 J. Wayne, D. Aurélien, M. Ludovic, Overcoming Impediments to Cell Phone Forensics, 2008.
7 T. John, Flasher Boxes: Back to Basics in Mobile Phone Forensics, 2010 http://www.dfinews.com/article/flasher-boxes-back-basics-mobile-phone-forensics z dnia 10.03.2013.
8 E. Casey, Cyfrowe Dowody i przestępstwa komputerowe, 2004.
9 S. Fiorillo, Theory and practice of flash memory mobile forensics, 2009, http://www.theosecurity.com/pdf/Fiorillo.pdf.
10 C. Miller, The other side of mobile forensics, 2008.
11 Tamże.
12 C. Murphy, Cellular Phone Evidence Data Extraction and Documentation, http://www.mobilhttp://www.mobileforensicscentral.com/mfc/documents/Cell%20Phone%20Evidence%20Extraction%20Process%202.0%20with%20forms.pdf.
13 Wayne, Jansen., & Ayers, Rick. (May 2007). Guidelines on cell phone forensics. http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.
14 Murphy, Cynthia, Cellular Phone Evidence Data Extraction and Documentation, http://www.mobilhttp://www.mobileforensicscentral.com/mfc/documents/Cell%20Phone%20Evidence%20Extraction%20Process%202.0%20with%20forms.pdf.
15 Wayne, Jansen., & Ayers, Rick. (May 2007). Guidelines on cell phone forensics. http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.
16 Willassen, Svein Y. (2006). Forensic analysis of mobile phone internal memory.
17 R. van der Knij. (2007). 10 Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics. http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf.
18 R. Ayers, Wayne Jansen, Nicolas Cilleros, and Ronan Daniellou. (October 2005) Cell Phone Forensic Tools: An Overview and Analysis. National Institute of Standards and Technology. http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf.
19 R. Ayers, Wayne Jansen, Nicolas Cilleros, and Ronan Daniellou. (October 2005) Cell Phone Forensic Tools: An Overview and Analysis. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistir/nistir-7250.pdf.
20 S. Fiorillo, Theory and practice of flash memory mobile forensics, 2009, http://www.theosecurity.com/pdf/Fiorillo.pdf.
21 Brothers Sam "iPhone Tool Classification" http://www.appleexaminer.com/files/iPhone_Levels.pdf 21 lipiec 2012.
22 Eoghan Casey. Handbook of computer crime investigation - forensic tools and technology. Academic Press, 2. edition, 2003.
23 Henry, Paul. "Quick Look - Cellebrite UFED Using Extract Phone Data & File System Dump" http://computer-forensics.sans.org/blog/2010/09/22/digital-forensics-quick-cellebrite-ufed-extract-phone-data-file-system-dump/ z dnia 30 lipieca 2012.
24 Vance, Christopher. "Android Physical Acquisitions using Cellebrite UFED" http://blog.csvance.com/?p=183 z dnia 1 sierpinia 2012.
25 "Mobile Digital Forensics for the Military" http://www.youtube.com/watch?v=jIKFqh73lKM z dnia 21 lipica 2012.
26 Daniels, Keith. "Creating a Cellular Device Investigation Toolkit: Basic Hardware and Software Specifications" http://www.search.org/files/pdf/celldevicetoolkit101309.pdf.
27 "The Electronic Evidence Information Center" http://www.e-evidence.info/cellular.html z dnia 25 sierpnia 2012.
27 Homepage of Factronix http://www.factronix.com/index.php?view=content&id=146&themeid=279&parentid=56&tpl=1&bild=1 z dnia 1.09.2012.
29 http://www.factronix.com/_downloads/BGA-Reballing-Animation.wmv.
30 http://www.factronix.com/_downloads/BGA-Reballing-Video.wmv.
31 Ronald van der Knij http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf z dnia 3.10.2012.
32 Eoghan Casey. Handbook of computer crime investigation - forensic tools and technology. Academic Press, 2. edition, 2003.
33 Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knij?, and Mark Roelos Forensic Data Recovery from Flash Memory. Small I Scale Digital Device Forensics Journal, Volume 1 (Number 1) http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf z dnia 10.12.2012.
34 Willassen, Svein Y. (2006). Forensic analysis of mobile phone internal memory.
35 Ronald van der Knij 10 Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf.
36 Willassen, Svein Y Forensic analysis of mobile phone internal memory
37 Tamże.
38 Tom Salt and Rodney Drake. US Patent 5469557 Code protection in microcontroller with EEPROM fuses http://www.patentstorm.us/patents/5469557/description.html.
39 Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knij and Mark Roelos Forensic Data Recovery from Flash Memory. Small I Scale Digital Device Forensics Journal, Volume 1 (Number 1) http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf
40 Ronald van der Knij 10 Good Reasons Why You Should Shift Focus to Small Scale Digital Device Forensics http://www.dfrws.org/2007/proceedings/vanderknijff_pres.pdf.
41 Secure Boot Patent . http://www.freepatentsonline.com/5937063.html.
42 Harini Sundaresan OMAP platform security features http://focus.ti.com/pdfs/vf/wireless/platformsecuritywp.pdf.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 2/2013 (14)]

BERNADETTA TERLECKA

Operacja „Czerwony październik”

Cel:	Agendy rządowe i dyplomatyczne.
Typ:	Cyber szpiegostwo.
Czas trwania:	Maj 2007 do nadal.
Urządzenia:	Stacje robocze i urządzenia mobilne.
Obszar zainteresowań:	Przede wszystkim informacje niejawne, dane wywiadowcze geopolityczne.



Rysunek 1. Plik skierowany w stronę Polskiego odbiorcy. http://niebezpiecznik.pl/wp-content/uploads/2013/01/redoctober3.png,

Kaspersky Lab na prośbę jednego z partnerów przeprowadziło analizę ataków typu *spear phishing* oraz *malware'ów* dzięki temu wykryło kampanię Rocra (Czerwony Październik). Kampania cyberszpiegowska od około pięciu lat odnosi sukcesy w infiltracji sieci rządowych i dyplomatycznych agend oraz jednostek naukowych. Celem ataku prócz klasycznych stacji roboczych są również urządzenia sieciowe (w tym CISCO) oraz urządzenia mobilne. Plikami będącymi w obszarze zainteresowań atakujących są te z rozszerzeniami txt, csv, eml, doc, odt, docx, rtf, pdf, xls, key, crt, cer, pgp, gpg, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa. Zwłaszcza pliki z rozszerzeniem acid* ponieważ są plikami programu „Acid Cryptofiler”, który używany jest przez Unię Europejską i NATO do szyfrowania.

Złośliwe oprogramowanie skierowane jest głównie do instytucji w Europie Wschodniej (Rosja, kraje byłego ZSRR), Azji Środkowej, Europy Zachodniej, Ameryki Północnej i Południowej (Rysunek nr 1). Szacuje się, że na świecie wystąpiło około 200 zakażeń tymi *malware'ami*. Niektóre elementy kodu mogą sugerować, że za atakami stoją chińscy lub rosyjscy hakerzy, choć równie prawdopodobnym jest wykorzystanie *exploit'ów* chińskich hakerów i celowe wstawienie rosyjsko - językowych fragmentów do kodu, w celu zmylenia analityków co do pochodzenia ataków.

Data rejestracji domen i głównych serwerów sugeruje, że ataki rozpoczęły się w okolicach maja 2007 roku. Do połowy stycznia tego roku sprawcy mieli zarejestrowane około 60 domen w C&C. Lokalizacje serwerów zarejestrowanych na tę sama osobę jest kilka i mieszczą się zazwyczaj w Rosji i Niemczech.

Wszystkie zebrane w tym czasie informacje są wykorzystywane do dalszych ataków. Przykładem jest kradzież poświadczeń i późniejsze ich wykorzystanie w przypadku, gdy w innej lokalizacji niezbędne było posiadanie poświadczenia. System jest odporny na przejęcie serwerów głównych i umożliwia odzyskanie kontroli atakujących nad zainfekowanymi maszynami za pomocą alternatywnych kanałów komunikacji.

Pracownicy Kaspersky Lab zaobserwowali użycie 3 różnych *exploit'ów* wykorzystujących znane luki i są nimi CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) i CVE-2012-0158 (MS Word).

Dokumenty wykorzystane podczas ataku były tworzone nie przez samych autorów systemu, a przez innych atakujących dla celów innych cyber napadów. W dokumentach zmienił się oczywiście plik wykonywalny jaki został umieszczony w dokumencie. Na rysunku 2 przedstawiono przykładowy dokument wykorzystywany podczas ataku. Podczas ruchu poprzecznego w sieci atakujący wdrażali moduły, których celem było aktywne skanowanie sieci. Dzięki temu hakerzy mogli znaleźć urządzenia podatne na MS08-067 oraz na atak na dostęp grupowy.

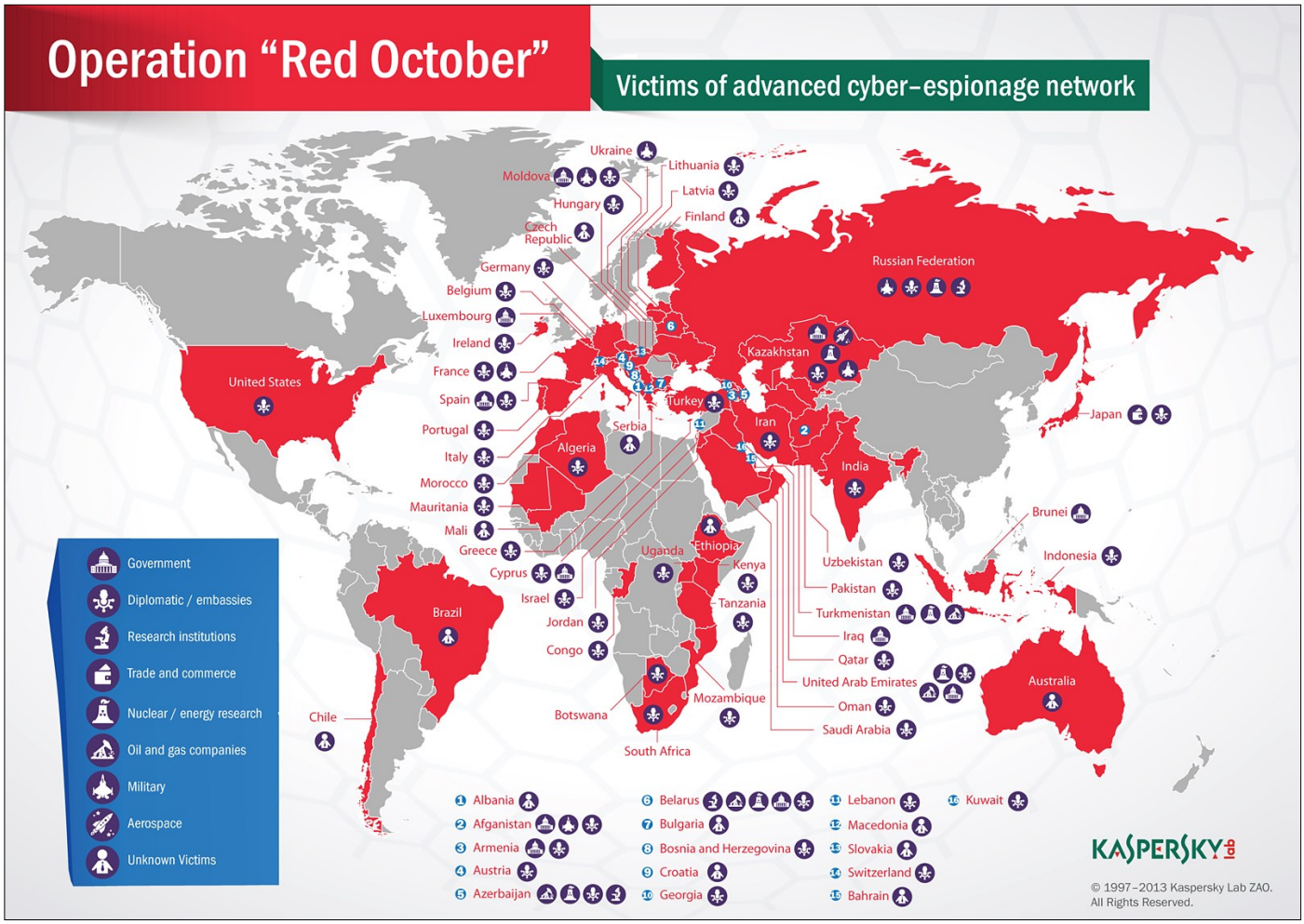
Jak już wcześniej wskazałam *exploity* służące do dokonania ataków wykorzystywały znane od dawna luki w oprogramowaniu Excel i Word. Nigdy w 5 letniej historii działania atakujący nie wykorzystywali *exploit'ów* zero-day. Należy zastanowić się czemu hakerzy wykorzystują tylko znane od dawna luki w oprogramowaniu? Czy mają zbyt małe fundusze, jakie mogą przeznaczyć na tę operację, a może ma to zmylić analityków, aby uznali, że za atakami stoją najzwyklejsi rzezimieszkowie[1].

Wobec Polaków (lub osób mówiących po polsku) również były skierowane takie ataki. Nie wiemy jednak czy skutecznie zadziałały, ponieważ Polski nie ma w statystykach jakie podaje Kaspersky Lab. Nie ma również informacji czy na serwery C&C docierają pliki z Polski (nie ma połączeń z Polski).

Pomimo posiadanych wskazówek ciężko jest jednoznacznie określić skąd pochodzą atakujący. Pewnym jest natomiast, że informacje jakie zbierają są cennymi danymi wywiadowczymi. Najprawdopodobniej więc grupa nastawiona jest na handel nimi z rządami niektórych państw. Takie grupy zwykło nazywać się *przesiewaczami informacji*[2].

Przypisy

1 Niebezpiecznik.pl, Kaspersky Lab, 2013.02.22.
2 Niebezpiecznik.pl, 2013.02.22.



Rysunek 2. Mapa terenu działania hakerów w operacji „czerwony październik”
Źródło: http://www.securelist.com/en/images/pictures/klblog/208194085.png, 2013.02.22

ZOBACZ WIĘCEJ: HTTP://WWW.SECURELIST.COM/EN/DOWNLOADS/VLPDFS/REDOCTOBER-INDICATORSOFCOMPROMISE.PDF

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 5/2012 (5)]

JACEK KOWALSKI

Szacowanie, analiza i zarządzanie ryzykiem

Wskutek przeobrażeń cywilizacyjnych, informacja nabrała statusu autonomicznego dobra prawnie chronionego. Nie oznacza to, że informacja wcześniej nie podlegała ochronie. Informacje chroniono od momentu, gdy tylko zaistniała. Ochrona ta obejmowała tajemnicę korespondencji, tajemnicę państwową, służbową oraz zawodową. Natomiast od momentu zautomatyzowania procesu przetwarzania informacji zaistniała potrzeba zapewnienia ochrony jej w zdigitalizowanej formie.

Ze względu na coraz większe znaczenie tego rodzaju informacji w życiu codziennym oraz w dzisiejszej gospodarce, preferencją staje się zapewnienie ochrony prawnej przetwarzanej informacji. W dzisiejszych czasach informacja ma ogromne znaczenie, utrata zaś informacji może przynieść wymierne szkody. Trzeba zadać sobie pytanie, jak zabezpieczyć informację przed ujawnieniem, ponieważ raz ujawniona nie posiada znamion informacji przeznaczonej wyłącznie dla uprawnionych, a staje się dostępna dla innych. Jednym ze sposobów zapobiegania i przeciwdziałania utracie informacji jest szacowanie i zarządzanie ryzykiem. Wybór metody zależy od nas samych. To jednak z jaką rzetelnością przeprowadzimy szacowanie i zarządzanie ryzykiem umożliwi nam skuteczną ochronę i może pomóc w przeciwdziałaniu utraty informacji.

Ryzyko można szacować na wiele sposobów, jednakże chciałbym pokrótce zaprezentować metodę opisaną przez mgr inż. Marka Anzela, który w swoim opracowaniu „Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych, przykład metody analizy ryzyka opartej na gotowych macierzach", wydane przez PHU ONE Poznań 2011. Według metody CRAMM (Crisis Risk Analisys and Management Method), ryzyko szacuje się jakościowo w oparciu o wybrany poziom bezpieczeństwa, związany z ochroną poufności, integralności i dostępności informacji. Stratę według metody CRAMM można obliczyć według poniższego wzoru **R = S x P.** Jego Którego składowe oznaczają:

R – wielkość oczekiwanej straty związanej z danym ryzykiem;
S – wielkość straty, gdy wystąpi rozpatrywane zdarzenie;
P – prawdopodobieństwo wystąpienia rozpatrywanego zdarzenia;

Dla obliczonych wartości liczbowych można przyjąć następujący poziom wielkości ryzyka:

niski (1 – 20)
średni (21 – 60)
wysoki (61 – 80)

W przypadku przekroczenia wartości 20, ryzyko należy obowiązkowo analizować.

By prawidłowo ocenić zagrożenia należy dobrze poznać Globalne Środowisko Bezpieczeństwa (GŚB) i przeprowadzić analizę jego otoczenia, zastosowane w nim środki bezpieczeństwa fizyczne i techniczne oraz możliwe zagrożenia. Drugim aspektem jest analiza Lokalnego Środowiska Bezpieczeństwa (LŚB), kto i w jaki sposób ma bezpośredni dostęp do pomieszczeń chronionych, gdzie przetwarzane są informacje, jakie uprawnienia posiada uprawniony personel i na jakie zagrożenia jest on podatny oraz jakie są możliwe zagrożenia dla LŚB.

Następny etap to przeprowadzenie identyfikacji zasobów wymagających ochrony i powinna ona obejmować zarówno dobra materialne jak i niematerialne.

Przykładowa lista zasobów, które mają zasadnicze znaczenie dla bezpieczeństwa informacji niejawnych (tabela 1).

Numer zasobu	Rodzaj zasobu	Miejsce przetwarzania, przechowywania i udostępniania	Klauzula tajności	Wartość informacji
ZS-1	**Kancelaria tajna**	Pomieszczenia nr ……	-	niska
ZS-2	Rejestry kancelaryjne	Pomieszczenia nr ……	JAWNE	średnia
ZS-3	Materiały niejawne	Pomieszczenia nr ……	TAJNE	wysoka
ZS-4	Materiały niejawne	Pomieszczenia nr ……	POUFNE	średnia
ZS-5	Materiały niejawne	Pomieszczenia nr ……	ZASTRZEŻONE	niska

Tabela 1. Opracowanie własne

Oszacowanie wartości informacji powinno być przeprowadzone na podstawie opinii osób odpowiedzialnymi za przechowywanie, dystrybucję i wytwarzanie informacji.

Następny krok to identyfikacja i oszacowanie zasobów w ustalonym zakresie, winna ona zawierać:

- wyposażenie środowiska;
- wykonawcy;
- dobra materialne;
- dobra niematerialne (personel)

I tak lista zasobów systemu uporządkowana według hierarchii ważności dla wykonania zadań przykładowej firmy X:

- materiały niejawne:
- dyski twarde wykorzystywane w systemach teleinformatycznych;
- magnetyczne nośniki danych;
- kancelaria tajna wraz z wyposażeniem;
- pomieszczenia w których umiejscowione są systemy teleinformatyczne;
- pełnomocnik ochrony;
- personel kancelarii tajnej;
- pracownicy ochrony;
- administrator systemu i sieci teleinformatycznych;
- inspektor bezpieczeństwa teleinformatycznego;
- użytkownicy (wykonawcy);
- itp.

Gdy opracujemy listę zasobów, możemy przystąpić do identyfikacji skutków utraty naszych zasobów pod względem ochrony poufności, integralności i dostępności informacji. W tym celu można przyjąć wymienione wartości liczbowe dla każdej z tych kategorii i tak dla:

Poufności (dopasowane do ustawowych klauzul):

- jawne (0);
- zastrzeżone (1-3);
- poufne (4-5);
- tajne (6-7);
- ściśle tajne (8-10);

Integralności:

- niskie (1-3);
- średnie (4-7);
- wysokie (8-9);
- bezwzględne (10);

Dostępności:

- **niskie wymagania (1-3)** – oznacza to, że jeśli informacje nie będą dostępne, nie będzie to miało większego wpływu na realizację zadań przez firmę XXXY w większym przedziale czasu;
- **średnie wymagania (4-6)** – oznacza to, że niedostępność informacji może mieć znaczący wpływ na realizację zadań przez firmę X, a dostęp musi nastąpić w ciągu kilki dni;

- **wysokie wymagania (4-6)** – oznacza to, że niedostępność informacji może spowodować duże szkody w realizacji zadań przez firmę X, a dostęp musi nastąpić w ciągu kilku godzin;
- **ekstremalne wymagania (9)** – oznacz to, że niedostępność informacji może sparaliżować realizację zadań przez firmę X, a dostęp musi nastąpić w ciągu kilku minut;
- **absolutne wymagania (10)** – oznacza to, że nie dopuszcza się niedostępności do informacji w każdej chwili.

Biorąc pod uwagę wymienione wyżej kryteria, można oszacować prawdopodobieństwo ewentualnych strat dla firmy X, oszacowanie należy przeprowadzić oddzielnie dla poufności, integralności i dostępności (tab. 2).

Przykładowe składowe **S** dla wzoru **R = S x P**

Identyfikację zagrożeń i określenie ich poziomu należy określić zarówno dla Globalnego Środowiska Bezpieczeństwa jak i dla Lokalnego Środowiska Bezpieczeństwa. Poniżej przykłady zagrożeń.

Dla Globalnego Środowiska Bezpieczeństwa:
- zagrożenia ze strony grup przestępczych, chuligańskich;
- zagrożenia ze strony obcych służb specjalnych;
- zagrożenia terrorystyczne;
- zagrożenia naturalne (pożary, powodzie, wyładowania atmosferyczne, wichury, gradobicia);
- zagrożenia środowiskowe (katastrofy komunikacyjne, wypadki w bezpośrednim sąsiedztwie firmy X, awarie elektrowni i ciepłowni, awarie linii elektrycznych i gazowych, awarie w zakładach produkcyjnych wykorzystujących techniczne środki przemysłowe);
- uwarunkowania geopolityczne (zagrożenia rozruchami, niepokojami społecznymi, położenie firmy X w danym regionie czy miejscowości, najbliższe sąsiedztwo, bliskość granic państwowych itp.).

Dla Lokalnego Środowiska Bezpieczeństwa:
- zagrożenia ze strony osób, które mogą mieć dostęp do pomieszczeń chronionych;
- częstotliwość i charakter wizyt osób spoza firmy X (zwłaszcza obywateli obcych państw, w związku z realizacją podpisanych umów międzynarodowych);
- stanu etatowego i kadrowego firmy X (zastępowalność kluczowego personelu dla funkcjonowania systemu ochrony informacji niejawnych);
- poziomu wyszkolenia personelu odpowiadającego za zapewnienie właściwego bezpieczeństwa ochrony informacji niejawnych;
- stopnia wyszkolenia wykonawców posiadających uprawnienia do dostępu do informacji niejawnych;
- poziom świadomości wykonawców i personelu pionu ochrony.

Numer zasobu	Nazwa zasobu	Poufność	Integralność	Dostępność
ZS-1	**Kancelaria tajna**	0	0	8
ZS-2	Rejestry kancelaryjne	0	8	8
ZS-3	Materiały niejawne	7	10	8
ZS-4	Materiały niejawne	5	9	8
ZS-5	Materiały niejawne	3	9	8

Tabela 2. Opracowanie własne

Numer zagrożenia	Zagrożenie	Czynnik	Poziom zagrożenia
ZG-1	Pożar	P, U, N	niski
ZG-2	Zalanie	P, U, N	niski
ZG-3	Zanieczyszczenie	P, U, N	średni
ZG-4	Wypadek	P, U, N	niski
ZG-5	Zniszczenie urządzeń lub nośników	P, U, N	średni
ZG-6	Pył, korozja, wychłodzenie, przegrzanie	P, U, N	niski
ZG-7	Zjawiska klimatyczne	N	średni
ZG-8	Zjawiska sejsmiczne	N	niski
ZG-9	Zjawiska wulkaniczne	N	niski
ZG-10	Zjawiska pogodowe	N	niski
ZG-11	Powódź	N	niski
ZG-12	Awaria w dostawie wody	P, U	średni
ZG-13	Utrata dostaw prądu	P, U, N	średni
ZG-14	Awaria urządzeń telekomunikacyjnych	P, U, N	średni
ZG-15	Promieniowanie elektromagnetyczne	P, U, N	średni
ZG-16	Promieniowanie cieplne	P, U, N	niski
ZG-17	Impuls elektromagnetyczny	P, U, N	średni
ZG-18	Przechwycenie sygnałów na skutek zjawiska interferencji	U	średni
ZG-19	Szpiegostwo zdalne	U	wysoki
ZG-20	Podsłuch	U	wysoki
ZG-21	Kradzież nośnika lub materiałów	U	średni
ZG-22	Kradzież urządzenia	U	niski
ZG-23	Odtworzenie danych z powtórnie wykorzystanych nośników	U	niski
ZG-24	Ujawnienie	P, U	średni
ZG-25	Dane z niewiarygodnych źródeł	P, U	niski

Tabela 3. Opracowanie własne

Przykład typowych zagrożeń, które mogą stanowić istotne zagrożenia dla wskazanych zasobów przedstawia tabela 3.

Oznaczenia czynnika zastosowanego w tabeli;

N – siły natury, zdarzenia nie wynikające z działalności człowieka;

U – umyślne działanie człowieka skierowane przeciwko zasobom;

P – działanie człowieka, które w sposób przypadkowy mogą zniszczyć, uszkodzić zasoby.

Oznaczenie poziomu zagrożenia zastosowanego w tabeli;

- niski;
- średni;
- wysoki;

Listę zagrożeń dla informacji niejawnych i zasobów należy uporządkować według prawdopodobieństwa wystąpienia zagrożeń, tak by można było wytypować obszary, w których środki ochrony należy zastosować w pierwszej kolejności lub gdzie należy dokonać poprawy zastosowanych środków ochrony. W dalszej kolejności, celem identyfikacji podatności na ryzyko, należy opracować listę słabych punktów (podatność) firmy X. Przy identyfikacji podatności należy wziąć pod uwagę funkcjonujące środki bezpieczeństwa.

Poziom podatności polega na przypisaniu każdej zdefiniowanej słabości odpowiedniej wartości: niski, średni, wysoki. Dla oszacowania poziomu podatności można przyjąć następujące wartości punktowe:

- brak (0);
- niski poziom (1-4);
- średni poziom (5-7);
- wysoki poziom (8-9);

I tak dla pary zasobów i zagrożeń (ZS / ZG) przyporządkowujemy poziom podatności P (tabela 4).
Jest to składowa **P** gdzie **R = S x P**

Identyfikacja i oszacowanie ryzyka

Z założenia, celem identyfikacji ryzyka jest wykrycie jego źródeł i usystematyzowanie według przyjętych kategorii.

Niski	(1 – 20)
Średni	(21 – 60)
Wysoki	(61 – 80)

Tabela 5. Opracowanie własne

Dla obliczonych wartości liczbowych możemy przyjąć następujące poziomy wielkości ryzyka:

Na podstawie oszacowanych wartości opracowujemy tabelę macierzy, każda dla poufności (tab. 6), integralności (tab. 7) i dostępności (tab. 8).

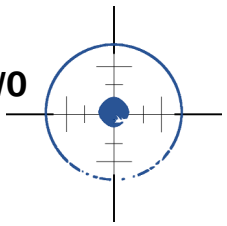
Przykłady opracowanych tabel macierzy dla zasobów od ZS-1 do ZS-5 przy zagrożeniach od ZG-1 do ZG-15, gdzie wartość ryzyka to iloczyn skutków i podatności, jest to wielkość możliwej straty obliczonej według wzoru:

R = S x P

Przykład: R=ZS-3xZG-1 (7x3=21), R=21

ZS/ZG	P	ZS/ZG	P	ZS/ZG	P	ZS/ZG	P	ZS/ZG	P
ZS-1/ZG-1	3	ZS-2/ZG-1	3	ZS-3/ZG-1	3	ZS-4/ZG-1	3	ZS-5/ZG-1	3
ZS-1/ZG-2	0	ZS-2/ZG-2	1	ZS-3/ZG-2	1	ZS-4/ZG-2	1	ZS-5/ZG-2	1
ZS-1/ZG-3	0	ZS-2/ZG-3	0	ZS-3/ZG-3	0	ZS-4/ZG-3	0	ZS-5/ZG-3	0
ZS-1/ZG-4	0	ZS-2/ZG-4	0	ZS-3/ZG-4	0	ZS-4/ZG-4	0	ZS-5/ZG-4	0
ZS-1/ZG-5	2	ZS-2/ZG-5	2	ZS-3/ZG-5	2	ZS-4/ZG-5	2	ZS-5/ZG-5	2
ZS-1/ZG-6	2	ZS-2/ZG-6	0	ZS-3/ZG-6	0	ZS-4/ZG-6	0	ZS-5/ZG-6	0
ZS-1/ZG-7	2	ZS-2/ZG-7	2	ZS-3/ZG-7	2	ZS-4/ZG-7	2	ZS-5/ZG-7	2
ZS-1/ZG-8	1	ZS-2/ZG-8	0	ZS-3/ZG-8	0	ZS-4/ZG-8	0	ZS-5/ZG-8	0
ZS-1/ZG-9	0	ZS-2/ZG-9	0	ZS-3/ZG-9	0	ZS-4/ZG-9	0	ZS-5/ZG-9	0
ZS-1/ZG-10	2	ZS-2/ZG-10	2	ZS-3/ZG-10	2	ZS-4/ZG-10	2	ZS-5/ZG-10	2
ZS-1/ZG-11	0	ZS-2/ZG-11	0	ZS-3/ZG-11	0	ZS-4/ZG-11	1	ZS-5/ZG-11	3
ZS-1/ZG-12	0	ZS-2/ZG-12	0	ZS-3/ZG-12	0	ZS-4/ZG-12	0	ZS-5/ZG-12	0
ZS-1/ZG-13	3	ZS-2/ZG-13	0	ZS-3/ZG-13	0	ZS-4/ZG-13	0	ZS-5/ZG-13	1
ZS-1/ZG-14	0	ZS-2/ZG-14	0	ZS-3/ZG-14	0	ZS-4/ZG-14	0	ZS-5/ZG-14	2
ZS-1/ZG-15	0	ZS-2/ZG-15	0	ZS-3/ZG-15	0	ZS-4/ZG-15	0	ZS-5/ZG-15	0
ZS-1/ZG-16	1	ZS-2/ZG-16	1	ZS-3/ZG-16	1	ZS-4/ZG-16	1	ZS-5/ZG-16	1
ZS-1/ZG-17	3	ZS-2/ZG-17	0	ZS-3/ZG-17	0	ZS-4/ZG-17	0	ZS-5/ZG-17	3
ZS-1/ZG-18	0	ZS-2/ZG-18	0	ZS-3/ZG-18	0	ZS-4/ZG-18	0	ZS-5/ZG-18	0
ZS-1/ZG-19	3	ZS-2/ZG-19	0	ZS-3/ZG-19	0	ZS-4/ZG-19	0	ZS-5/ZG-19	3
ZS-1/ZG-20	3	ZS-2/ZG-20	0	ZS-3/ZG-20	0	ZS-4/ZG-20	0	ZS-5/ZG-20	0
ZS-1/ZG-21	4	ZS-2/ZG-21	3	ZS-3/ZG-21	3	ZS-4/ZG-21	3	ZS-5/ZG-21	3
ZS-1/ZG-22	2	ZS-2/ZG-22	0	ZS-3/ZG-22	0	ZS-4/ZG-22	0	ZS-5/ZG-22	0
ZS-1/ZG-23	4	ZS-2/ZG-23	0	ZS-3/ZG-23	0	ZS-4/ZG-23	0	ZS-5/ZG-23	1
ZS-1/ZG-24	1	ZS-2/ZG-24	1	ZS-3/ZG-24	1	ZS-4/ZG-24	1	ZS-5/ZG-24	1
ZS-1/ZG-25	0	ZS-2/ZG-25	1	ZS-3/ZG-25	1	ZS-4/ZG-25	1	ZS-5/ZG-25	1

Tabela 4. Opracowanie własne



Macierz poziomów ryzyka dla poufności

Zasoby		Zagrożenia														
		INTEGRALNOŚCI														
rodzaj zasobu	Szacowanie	ZG-1	ZG-2	ZG-3	ZG-4	ZG-5	ZG-6	ZG-7	ZG-8	ZG-9	ZG-10	ZG-11	ZG-12	ZG-13	ZG-14	ZG-15
ZS-1	skutki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	podatność	3	0	0	0	2	2	2	1	0	2	0	0	3	0	0
	ryzyko	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
ZS-2	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	**24**	**8**	**0**	**0**	**16**	**0**	**16**	**0**	**0**	**16**	**0**	**0**	**0**	**0**	**0**
ZS-3	skutki	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	**30**	**10**	**0**	**0**	**20**	**0**	**0**	**0**	**0**	**20**	**0**	**0**	**0**	**0**	**0**
ZS-4	skutki	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
	podatność	3	1	0	0	2	0	2	0	0	2	1	0	0	0	0
	ryzyko	**27**	**9**	**0**	**0**	**18**	**0**	**18**	**0**	**0**	**18**	**9**	**0**	**0**	**0**	**0**
ZS-5	skutki	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
	podatność	3	1	0	0	2	0	2	0	0	2	3	0	1	2	0
	ryzyko	**27**	**9**	**0**	**0**	**18**	**0**	**18**	**0**	**0**	**18**	**27**	**0**	**9**	**18**	**0**

Tabela 6. Opracowanie własne

Macierz poziomów ryzyka dla integralności

Zasoby		Zagrożenia														
		DOSTĘPNOŚCI														
rodzaj zasobu	Szacowanie	ZG-1	ZG-2	ZG-3	ZG-4	ZG-5	ZG-6	ZG-7	ZG-8	ZG-9	ZG-10	ZG-11	ZG-12	ZG-13	ZG-14	ZG-15
ZS-1	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	0	0	0	2	2	2	1	0	2	0	0	3	0	0
	ryzyko	**24**	**0**	**0**	**0**	**16**	**16**	**16**	**8**	**0**	**16**	**0**	**0**	**24**	**0**	**0**
ZS-2	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	**24**	**8**	**0**	**0**	**16**	**0**	**16**	**0**	**0**	**16**	**0**	**0**	**0**	**0**	**0**
ZS-3	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	**24**	**8**	**0**	**0**	**16**	**0**	**16**	**0**	**0**	**16**	**0**	**0**	**0**	**0**	**0**
ZS-4	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	1	0	0	0	0
	ryzyko	**24**	**8**	**0**	**0**	**16**	**0**	**16**	**0**	**0**	**16**	**8**	**0**	**0**	**0**	**0**
ZS-5	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	3	0	1	2	0
	ryzyko	**24**	**8**	**0**	**0**	**16**	**0**	**16**	**0**	**0**	**16**	**24**	**0**	**8**	**16**	**0**

Tabela 7. Opracowanie własne

Macierz poziomów ryzyka dla dostępności

Zasoby		Zagrożenia														
		DOSTĘPNOŚCI														
rodzaj zasobu	Szacowanie	ZG-1	ZG-2	ZG-3	ZG-4	ZG-5	ZG-6	ZG-7	ZG-8	ZG-9	ZG-10	ZG-11	ZG-12	ZG-13	ZG-14	ZG-15
ZS-1	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	0	0	0	2	2	2	1	0	2	0	0	3	0	0
	ryzyko	24	0	0	0	16	16	16	8	0	16	0	0	24	0	0
ZS-2	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	24	8	0	0	16	0	16	0	0	16	0	0	0	0	0
ZS-3	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	0	0	0	0	0
	ryzyko	24	8	0	0	16	0	16	0	0	16	0	0	0	0	0
ZS-4	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	1	0	0	0	0
	ryzyko	24	8	0	0	16	0	16	0	0	16	8	0	0	0	0
ZS-5	skutki	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	podatność	3	1	0	0	2	0	2	0	0	2	3	0	1	2	0
	ryzyko	24	8	0	0	16	0	16	0	0	16	24	0	8	16	0

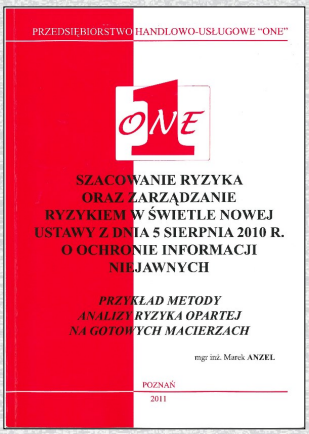
Ocena ryzyka

Po opracowaniu macierzy należy przystąpić do oceny wyliczonego ryzyka R, wskazanego w tabelach dla poufności, integralności i dostępności. Szczegółowo należy przeanalizować ryzyko po przekroczeniu wyliczonej wartości 20 (zgodnie z przyjętą punktacją) a po przekroczenie wartości 60, podjąć natychmiastową i bezwzględnej reakcję.

Jak dalej postępować z ryzykiem, możemy dowiedzieć się z przestawionej przeze mnie literatury, którą polecam. Jest to szczegółowe opracowanie, które jest niezmiernie przydatne przy tak mozolnym procesie jakim jest analiza, szacowanie i zarządzanie ryzykiem. Oczywiście każdy może mieć inny pogląd na przedstawioną metodę, jednak należy pamiętać, że jakiej metody nie użylibyśmy, to dużo zależy od kierownika jednostki organizacyjnej i jego zespołu, świadomości i odpowiedzialności za ochronę informacji i przeciwdziałaniu stwierdzonemu poziomowi ryzyka.

Jacek Kowalski

BIULETYN POLECA:



Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle nowej ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, M. Anzel.
Poznań 2011,
ss. 98.

ARTYKUŁ ARCHIWALNY
[e-Terroryzm nr 3/2013 (15)]

TOBIASZ MAŁYSA

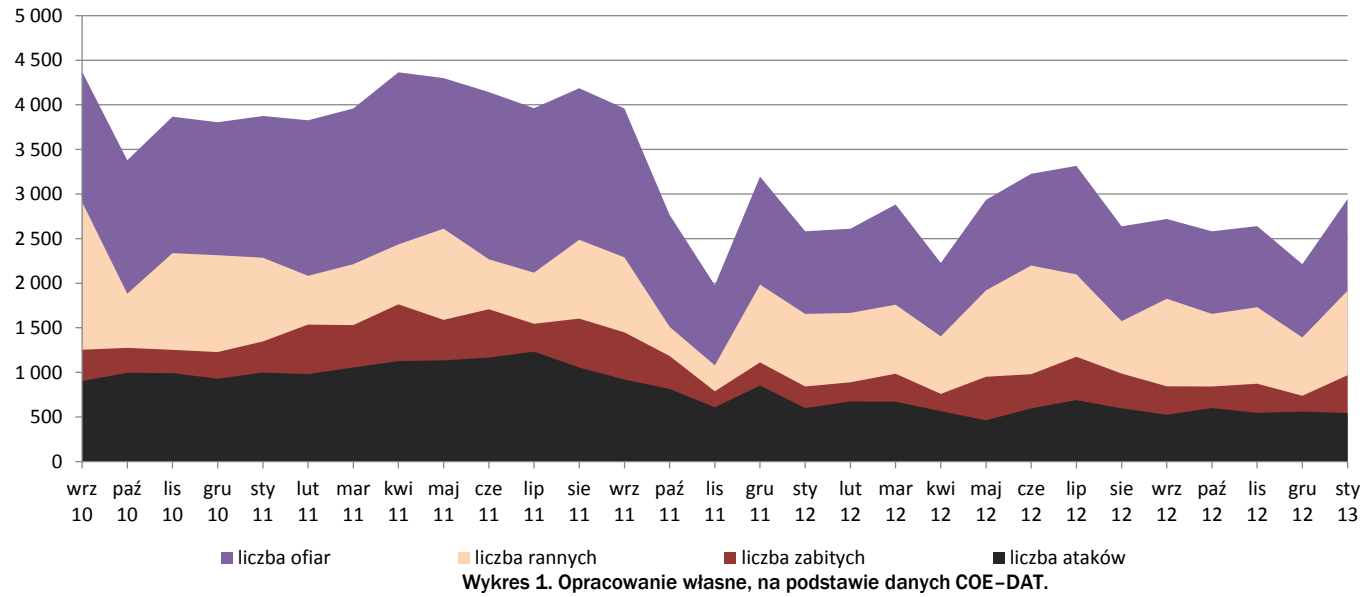
Globalne trendy zamachów terrorystycznych (wrzesień 2010 - styczeń 2013)

COEDAT to Centrum Wywiadowcze Obrony Przeciwko Terroryzmowi, akredytowane przez NATO. Mieści się ono w stolicy Turcji, Ankarze. Działając od 2005 roku Centrum od września 2010 publikuje globalne statystyki aktów terrorystycznych w formie raportów miesięcznych. Korzystając z nich, za okres wrzesień 2010 - styczeń 2013 (łącznie: 29 raportów) dokonaliśmy własnego podsumowania.

Pod uwagę wzięto globalne statystyki COEDAT poszczególnych rodzajów aktów terrorystycznych, z informacjami na temat liczby ataków danego rodzaju, liczby zabitych, rannych oraz porwanych w każdym miesiącu. Część danych została zaprezentowana w ujęciu miesięcznym, część w kwartalnym, a niektóre z diagramów i tabel są całościowymi zestawieniami dla omawianego okresu, uwzględniając zarówno poszczególne rodzaje ataków terrorystycznych, jak i całość.

W czasie od września 2010 r. do stycznia 2013 r. doszło na świecie do 23 393 aktów terrorystycznych, w których śmierć poniosło 33 997 osób, 57 608 zostało rannych, a 3 853 uprowadzonych. Z poszczególnych rodzajów ataków, doszło do 708 porwań, 5 695 ataków zbrojnych, 459 podpaleń, 3 735 konfliktów, 63 cyberataków, 1 080 egzekucji, 111 fałszywych alarmów, 1 407 przypadków ognia pośredniego, 7 614 eksplozji IED, 89 aktów piractwa, 471 napadów, 750 ataków samobójczych i 1 211 przypadków użycia VBIED (samochodu-pułapki). W ujęciu miesięcznym, ogólną ilość ataków terrorystycznych oraz ofiar zaprezentowano na wykresie 1. Natomiast wykres 2 (na następnej stronie) przedstawia ilość ich poszczególnych rodzajów. Jak pokazują statystyki, w omawianym okresie największa ilość aktów terrorystycznych oraz liczba ofiar dotyczy okresu od września 2010 r. do września-października 2011 r., po czym następuje ich znaczny spadek. Widoczny szczególnie przy atakach typu IED, ataku zbrojnym i konflikcie, a także ogniu pośrednim i napadach. Ilość ataków samobójczych odnotowała mniejszy spadek, a liczba eksplozji samochodów-pułapek w tym okresie wzrosła.

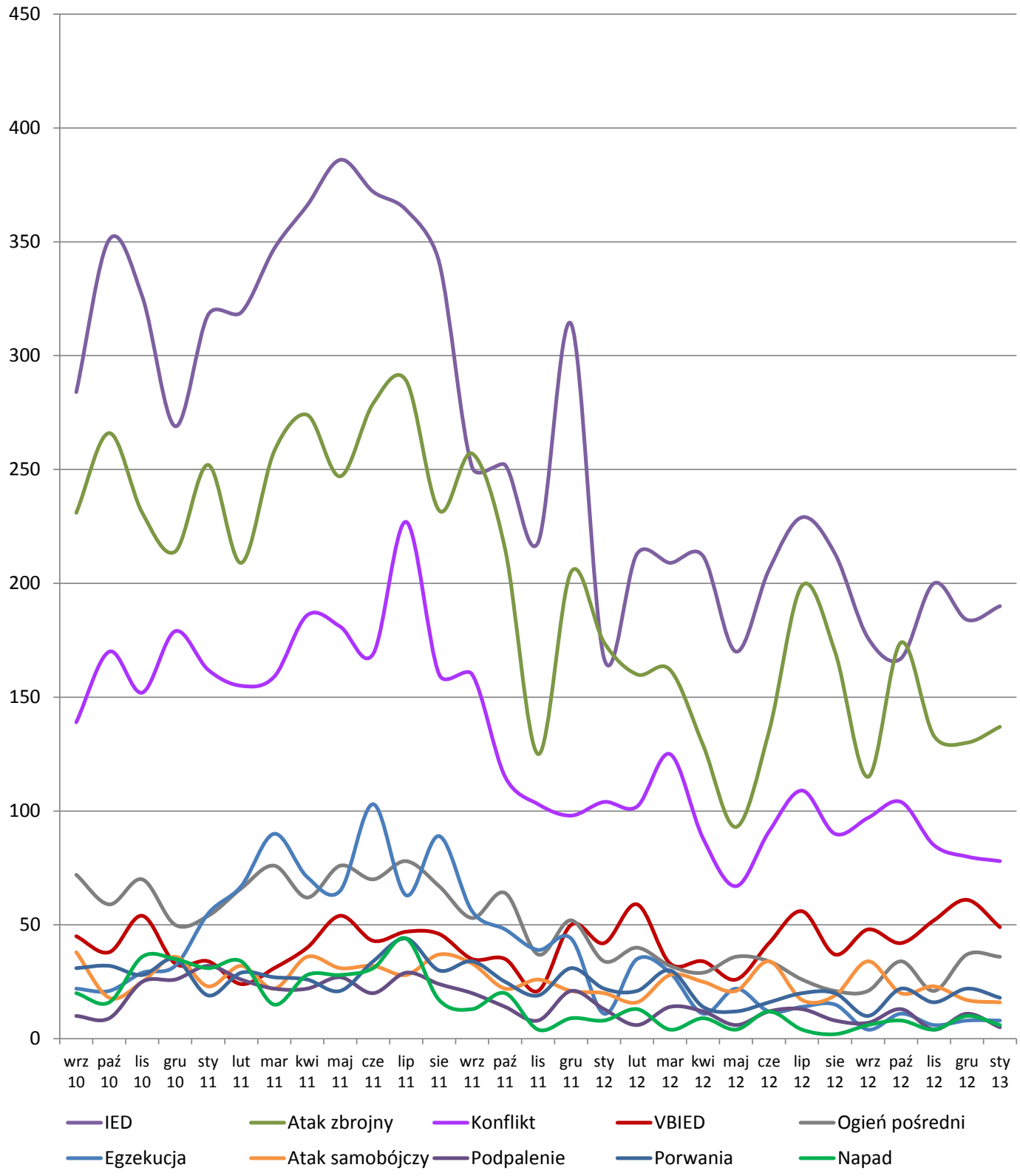
Liczba ataków terrorystycznych, ofiar (w tym porwanych)**, rannych i zabitych**



Wykres 1. Opracowanie własne, na podstawie danych COE–DAT.

Akty terrorystyczne - poszczególne rodzaje, liczba ataków*

*bez cyberataków, fałszywych alarmów oraz piractwa



Wykres 2. Opracowanie własne, na podstawie danych COE–DAT.

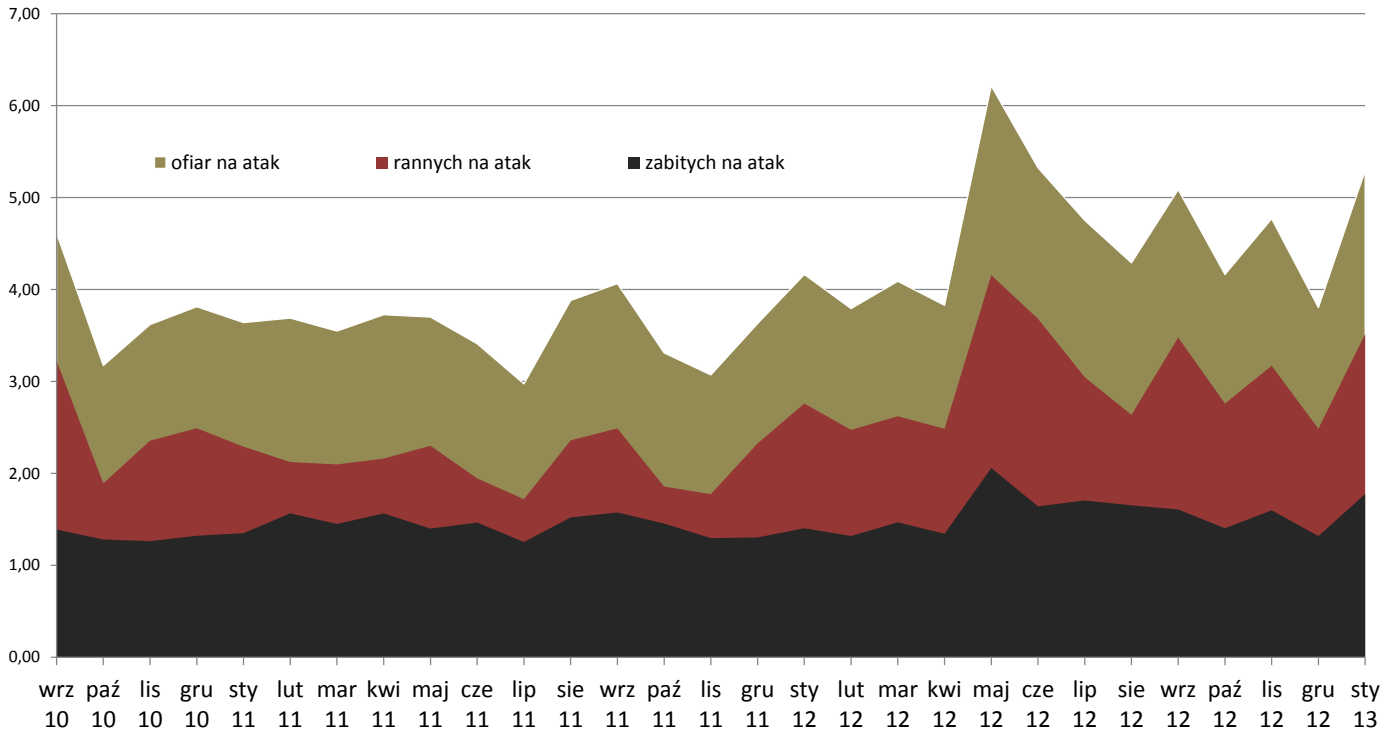
Globalne trendy zamachów terrorystycznych

Dane o liczbie zabitych, rannych oraz porwanych na każdy rodzaj ataku pozwoliły wraz z danymi o liczbie tych ataków (na każdy miesiąc) obliczyć średnią liczbę ofiar, rannych i śmiertelnych zarówno na każdy typ ataku, jak i ogółem. Średnia liczba ofiar (bez uwzględnienia porwanych), zabitych i rannych na atak terrorystyczny zaprezentowana została w ujęciu miesięcznym na wykresie 3. Analizując go da się zaobserwować wzrost średniej liczby ofiar, rannych i zabitych na pojedynczy atak terrorystyczny. W największym stopniu dotyczy to wzrostu liczby rannych. Wzrosła, chociaż w mniejszym stopniu również średnia liczba zabitych na jeden atak.

Dla wszystkich rodzajów ataków, stosunek procentowy ilości zabitych a rannych, w tym okresie pokazuje diagram 1. Przeciętnie, na atak terrorystyczny przypadło więc po 1,45 ofiar śmiertelnych, 2,46 rannych, oraz 4,08 ogółu ofiar (wraz z uprowadzonymi), przy czym na jeden atak przypadało po 0,16 uprowadzonych. Statystyki dotyczące porwań prezentowane są na wykresach 4, 5 i 6.

Na następnych stronach zaprezentowane zostaną kolejno: średnia liczba ofiar, zabitych i rannych (wykres 3), liczba uprowadzonych (wykres 4), średnia liczba uprowadzonych (wykres 5), liczba uprowadzeń a uprowadzonych w porwaniach (wykres 6), akty terrorystyczne w ujęciu za cały okres wrzesień 2010 - styczeń 2013 (tabela 1), zabici a ranni w atakach terrorystycznych (diagram 2), ataki terrorystyczne ogółem a % ofiar śmiertelnych (wykres 7), ataki terrorystyczne – ofiary śmiertelne a pozostałe (wykres 8), ataki terrorystyczne – średnia liczba zabitych na atak (diagram 3), udział w ilości zabitych (diagram 4), średnia liczba rannych na atak (diagram 5), udział w ilości rannych (diagram 6), średnia liczba ofiar na atak (diagram 7), udział w ilości ofiar (diagram 8), w ujęciu kwartalnym: udział poszczególnych rodzajów ataków w całości (wykres 9), % ofiar śmiertelnych (wykres 10), średnia liczba ofiar śmiertelnych (wykres 11), średnia liczba rannych (wykres 12), średnia liczba ofiar (wykres 13).

Średnia liczba ofiar (bez uprowadzonych)**, zabitych i rannych na atak terrorystyczny**



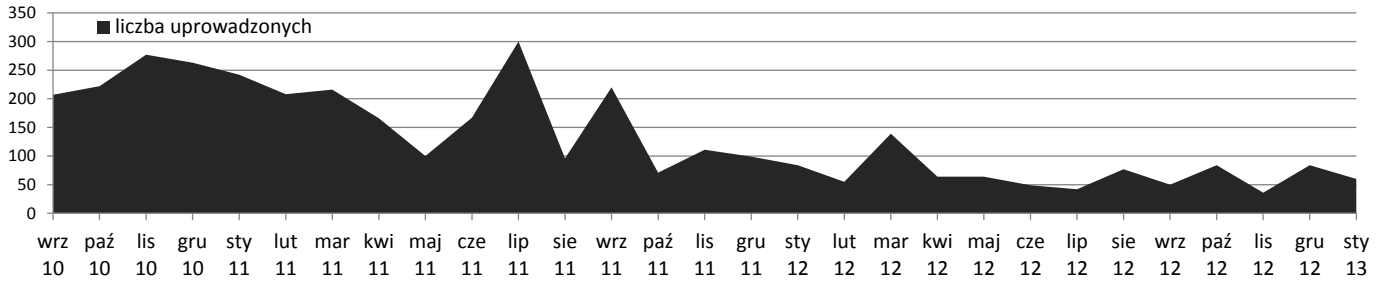
Wykres 3. Opracowanie własne, na podstawie danych COE–DAT.

Trzeba nadmienić, że wspominana wcześniej łączna liczba ofiar może być rozumiana na dwa sposoby. W pierwszym przypadku mogą być to wyłącznie ranni oraz zabici. W drugim przypadku, obejmie ona jeszcze liczbę uprowadzonych. Zdarza się bowiem, że np. podczas ataków część pozostałych przy życiu, zostaje przez napastników uprowadzona i stanowią oni niewątpliwie ofiary zamachów terrorystycznych, chociaż nie zaliczają się do rannych i zabitych, a sam typ ataku nie został odnotowany jako porwanie. W większości uwzględniano zatem liczbę uprowadzonych do ogólnej liczby ofiar (traktując wtedy uprowadzonego jako rannego), chyba, że przy wykresach albo diagramach wskazano inaczej.

Przeciętna liczba uprowadzonych w porwaniach na jedno porwanie wyniosła 3,52 osoby. W omawianym okresie akty piractwa (od II połowy 2011 roku gwałtownie zmniejszyła się liczba notowanych przypadków) sięgnęły natomiast 11,44 uprowadzonych osób na jeden akt. Najwięcej ofiar uprowadzonych zostało w porwaniach (65%) oraz piractwie (26%), napadach (5%), konflikcie (2%), IED (1%) i ataku zbrojnym (1%).

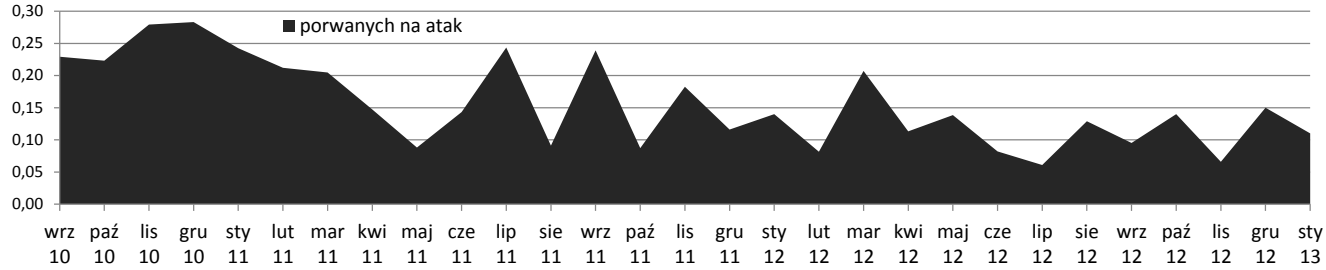
Największy stosunek uprowadzonych do ogółu ofiar oprócz uprowadzeń (99,7%) i piractwa (99,2%) przypadał na napad (7,8%) i podpalenie (6,5%). Przy innych rodzajach ataków udział uprowadzonych wynosi poniżej 1%. Nie odnotowano uprowadzonych przy atakach VBIED, samobójczych, cyberatakach i fałszywych alarmach. Dane te zaprezentowane są dalej (tabela 1).

Liczba uprowadzonych we wszystkich atakach terrorystycznych



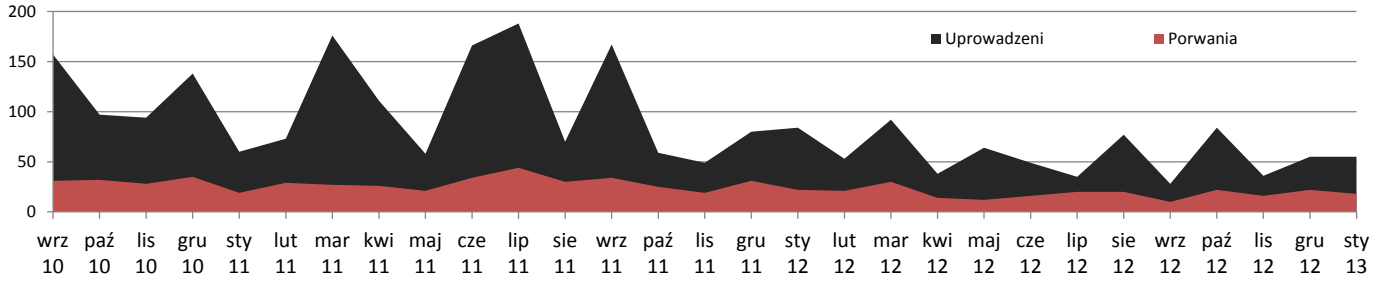
Wykres 4. Opracowanie własne, na podstawie danych COE–DAT.

Średnia liczba uprowadzonych na atak terrorystyczny



Wykres 5. Opracowanie własne, na podstawie danych COE–DAT.

Liczba uprowadzeń a uprowadzonych w porwaniach (bez piractwa i innych ataków)



Wykres 6. Opracowanie własne, na podstawie danych COE–DAT.

Akty terrorystyczne w ujęciu za cały okres wrz 2010 – sty 2013

	% ataków:	ataki	% zabitych	zabici	% rannych	ranni	% ofiar	ofiar	% porwanych	porwani
Porwania	3,03%	708	0%	3	0%	5	3%	2 501	65%	2 493
Atak zbrojny	24,34%	5 695	27%	9 282	8%	4 791	15%	14 106	1%	33
Podpalenie	1,96%	459	0%	49	0%	23	0%	77	0%	5
Konflikt	15,97%	3 735	16%	5 399	12%	6 713	13%	12 174	2%	62
Cyberatak	0,27%	63	0%	0	0%	0	0%	0	0%	0
Egzekucja	4,62%	1 080	8%	2 756	0%	178	3%	2 948	0%	14
Fałszywy alarm	0,47%	111	0%	0	0%	0	0%	0	0%	0
Ogień pośredni	6,01%	1 407	3%	1 069	7%	3 853	5%	4 927	0%	5
IED	32,55%	7 614	20%	6 952	34%	19 319	28%	26 298	1%	27
Piractwo	0,38%	89	0%	5	0%	3	1%	1 026	26%	1 018
Napad	2,01%	471	4%	1 218	2%	1 086	3%	2 500	5%	196
Atak samobójczy	3,21%	750	14%	4 663	20%	11 808	17%	16 471	0%	0
VBIED	5,18%	1 211	8%	2 601	17%	9 829	13%	12 430	0%	0
łącznie:	100%	23 393	100%	33 997	100%	57 608	100%	95 458	100%	3 853

	średnio na atak:				ranni, zabici a porwani w %		
	zabitych	**rannych**	**ofiar łącznie** (bez porwanych)	**porwanych**	**zabici**	**ranni**	**porwani**
Porwania	0,00	0,01	0,01	3,52	0,12%	0,20%	99,68%
Atak zbrojny	1,63	0,84	2,47	0,01	65,80%	33,96%	0,23%
Podpalenie	0,11	0,05	0,16	0,01	63,64%	29,87%	6,49%
Konflikt	1,45	1,80	3,24	0,02	44,35%	55,14%	0,51%
Cyberatak	0	0	0	0	0%	0%	0%
Egzekucja	2,55	0,16	2,72	0,01	93,49%	6,04%	0,47%
Fałszywy alarm	0	0	0	0	0%	0%	0%
Ogień pośredni	0,76	2,74	3,50	0,00	21,70%	78,20%	0,10%
IED	0,91	2,54	3,45	0,00	26,44%	73,46%	0,10%
Piractwo	0,06	0,03	0,09	11,44	0,49%	0,29%	99,22%
Napad	2,59	2,31	4,89	0,42	48,72%	43,44%	7,84%
Atak samobójczy	6,22	15,74	21,96	0,00	28,31%	71,69%	0,00%
VBIED	2,15	8,12	10,26	0,00	20,93%	79,07%	0,00%

Tabela 1. Opracowanie własne, na podstawie danych COE–DAT.

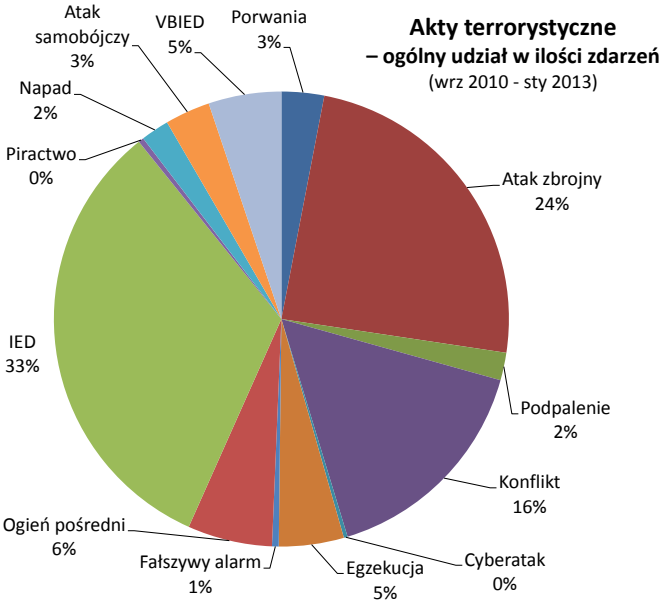


Diagram 1. Opracowanie własne, na podstawie danych COE–DAT.

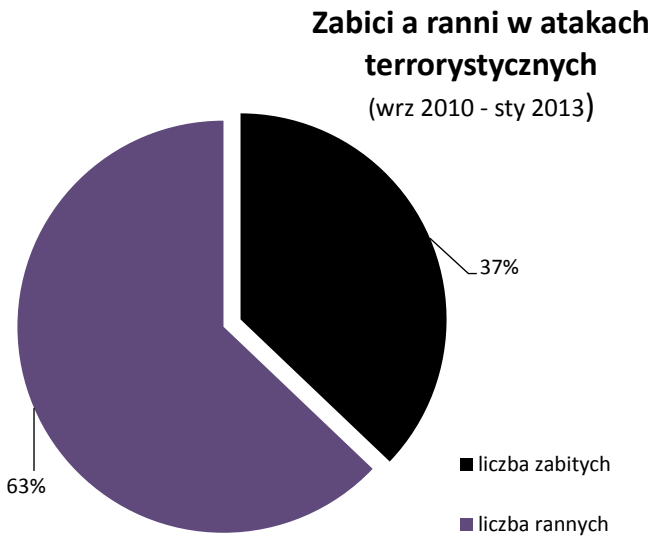
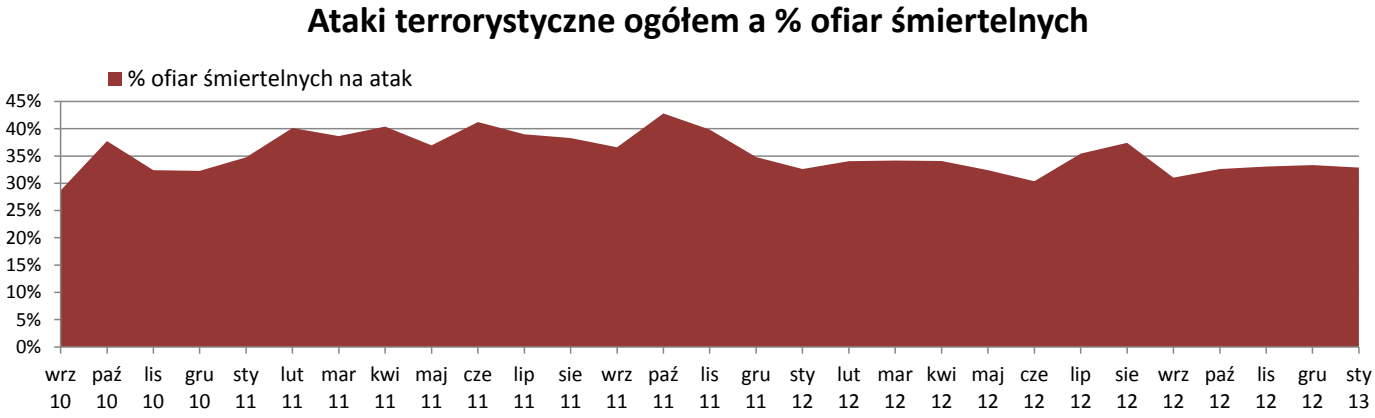
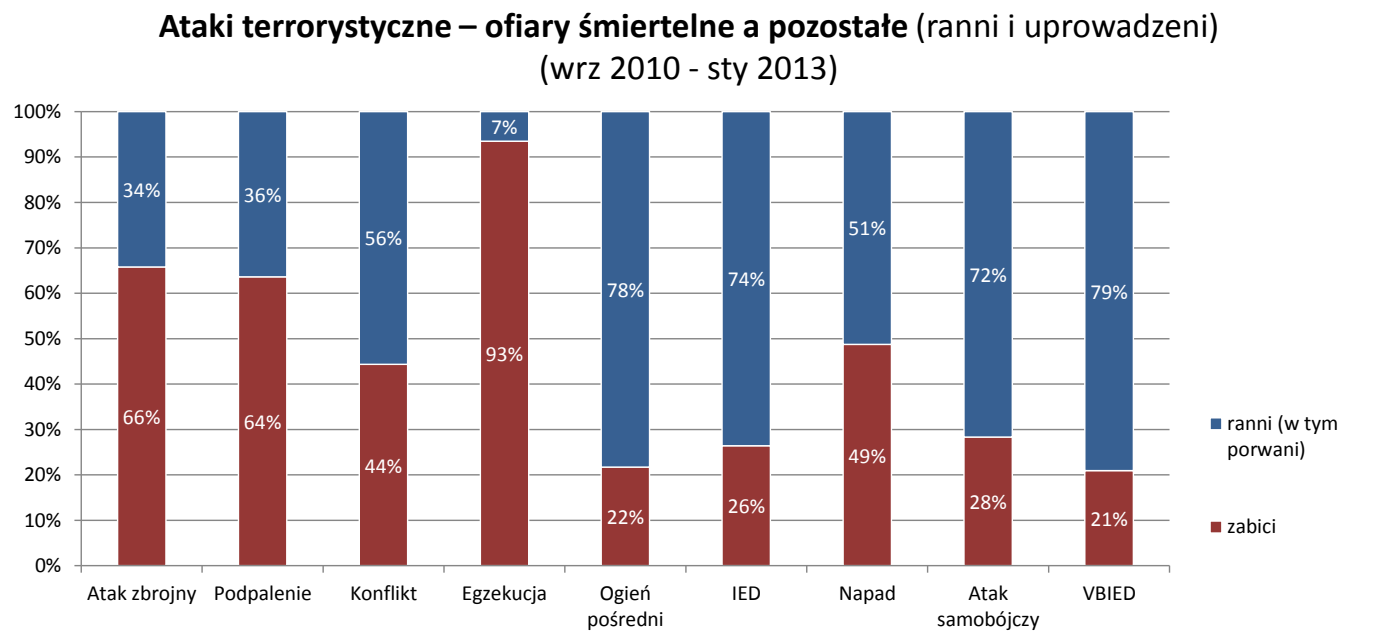


Diagram 2. Opracowanie własne, na podstawie danych COE–DAT.



Wykres 7. Opracowanie własne, na podstawie danych COE–DAT.



Wykres 8. Opracowanie własne, na podstawie danych COE–DAT.

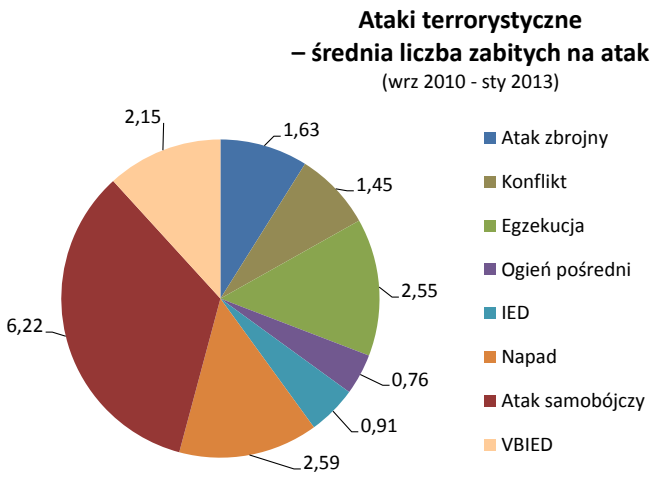


Diagram 3. Opracowanie własne, na podstawie danych COE–DAT.

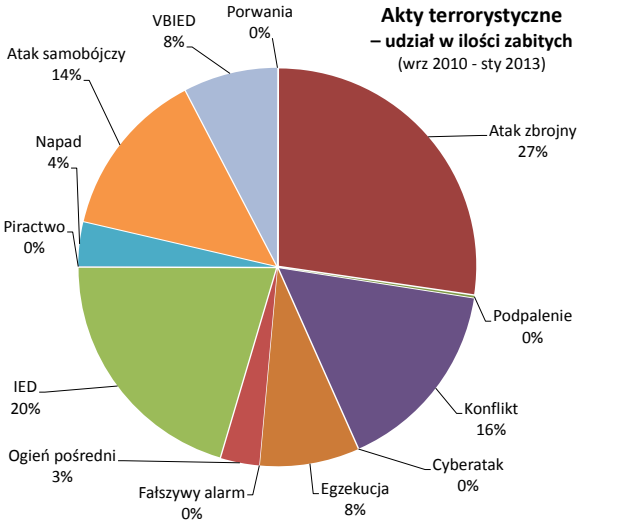


Diagram 4. Opracowanie własne, na podstawie danych COE–DAT.

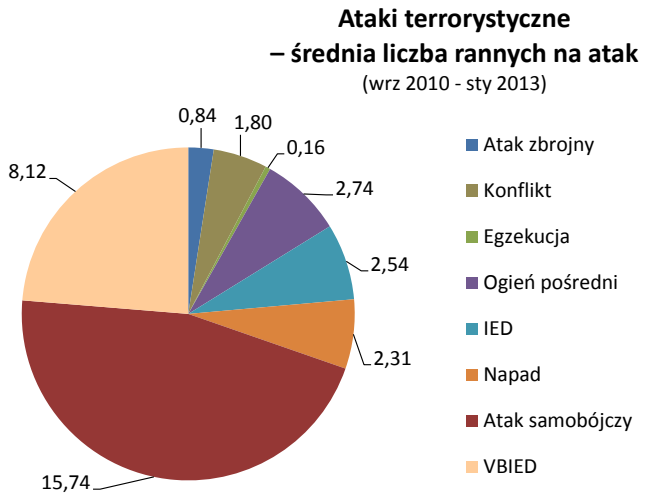


Diagram 5. Opracowanie własne, na podstawie danych COE–DAT.

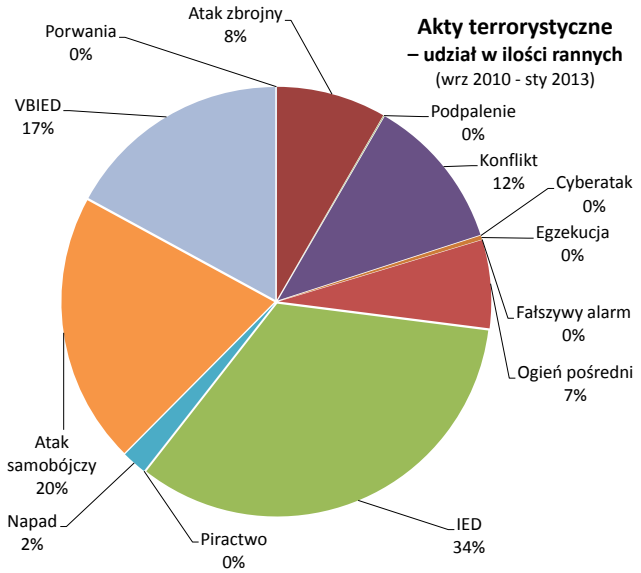


Diagram 6. Opracowanie własne, na podstawie danych COE–DAT.

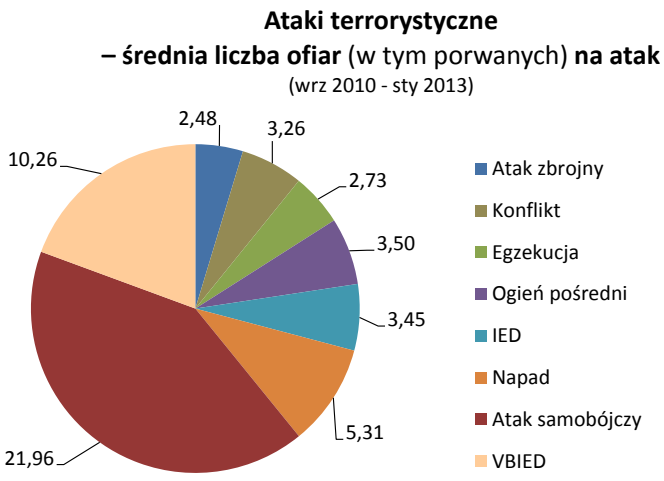


Diagram 7. Opracowanie własne, na podstawie danych COE–DAT.

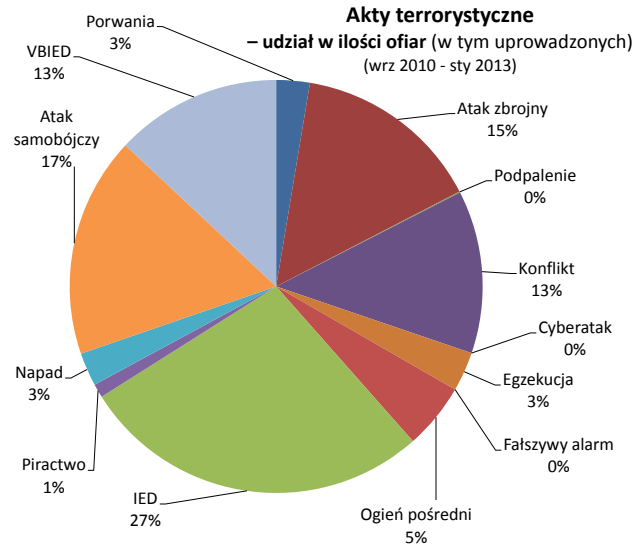
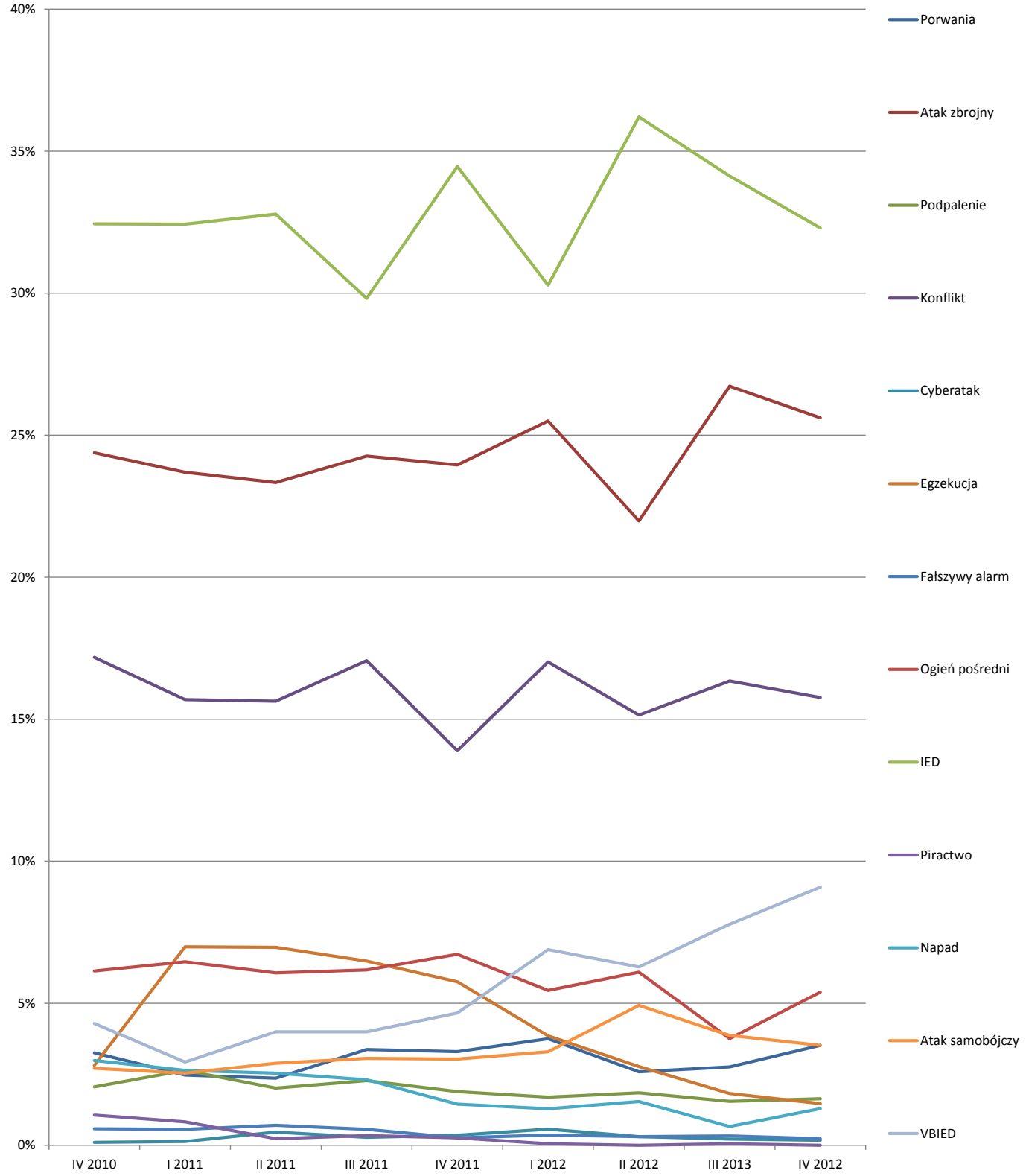
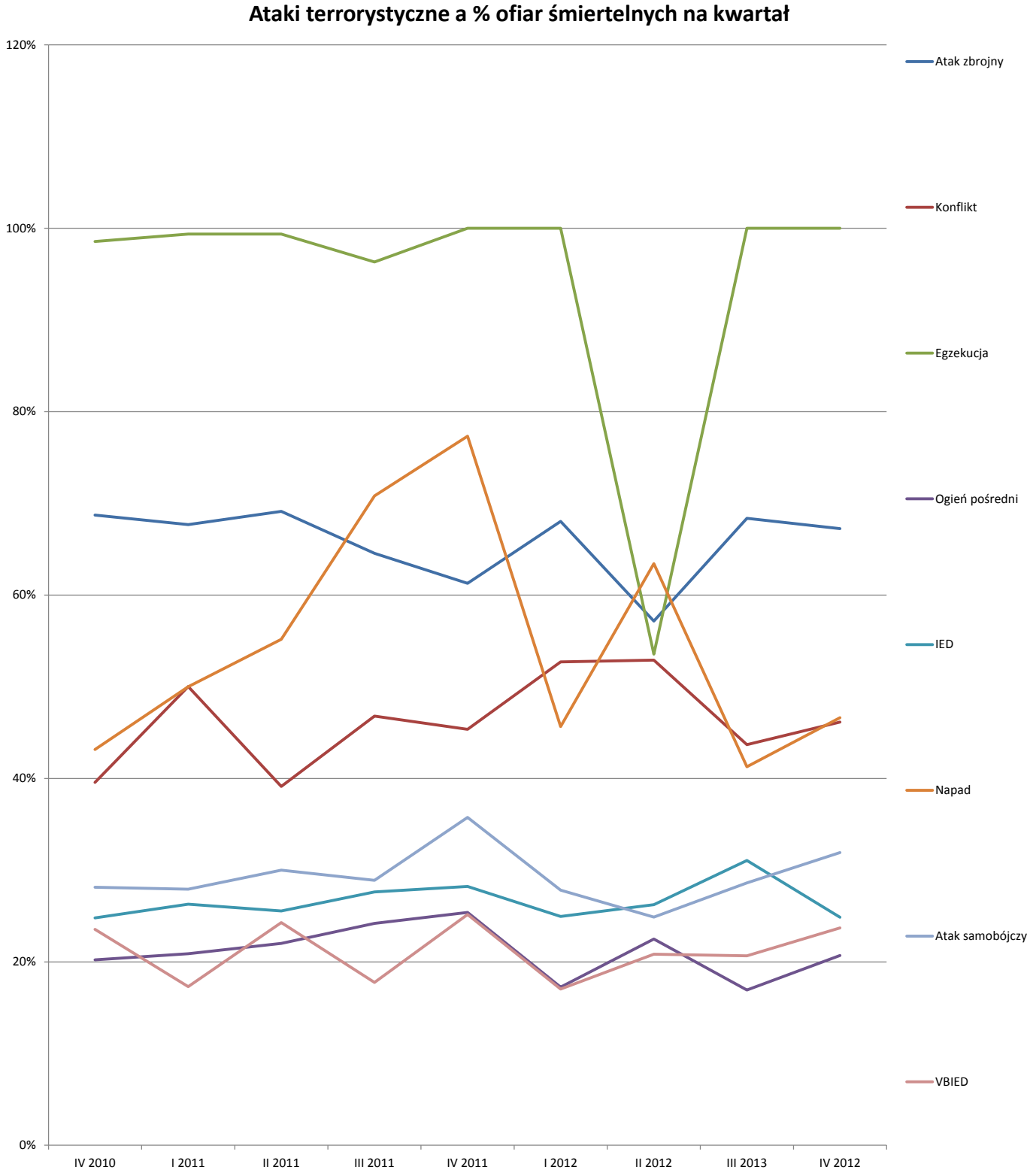


Diagram 8. Opracowanie własne, na podstawie danych COE–DAT.

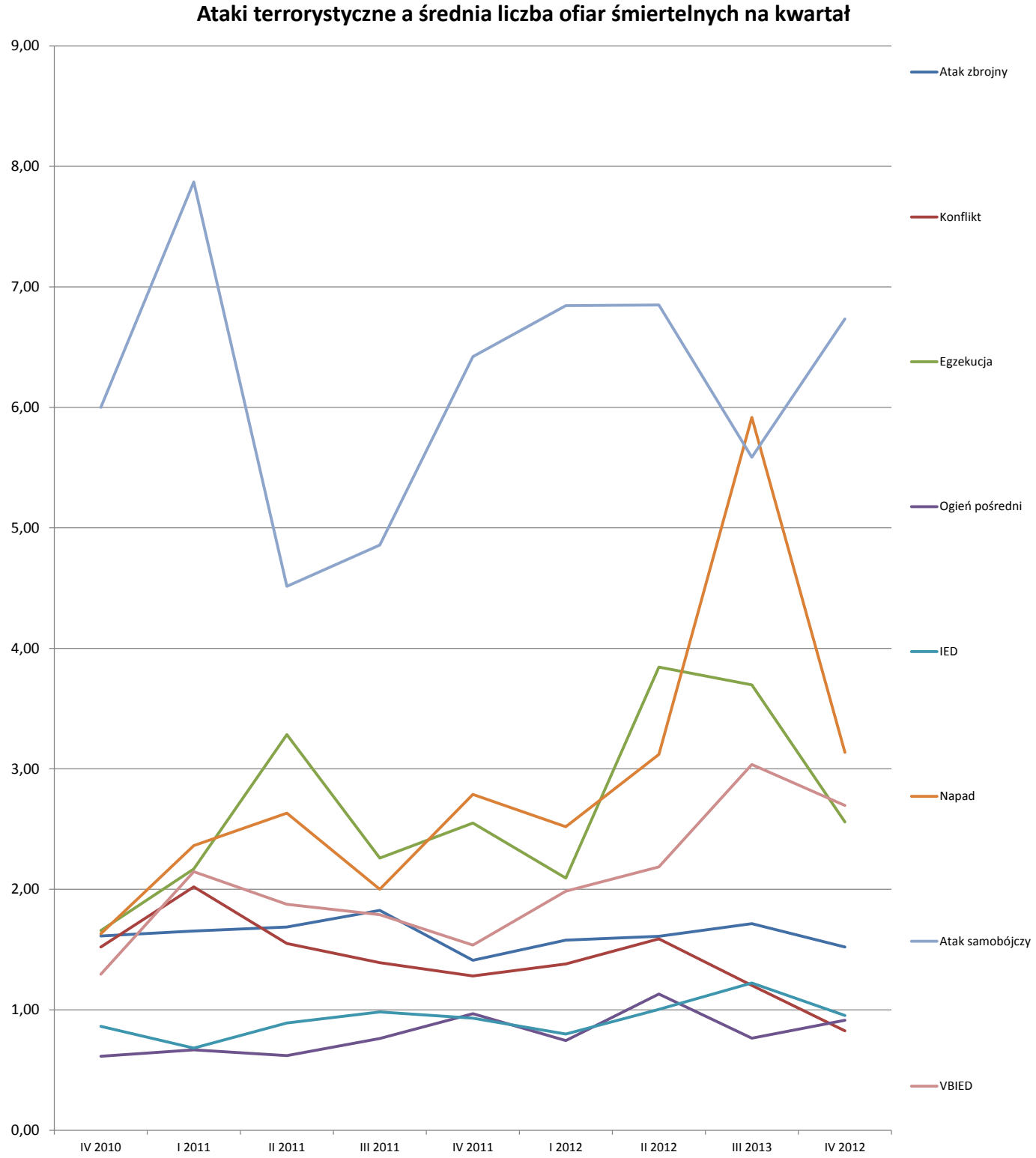
Udział poszczególnych rodzajów ataków w całości, na każdy kwartał



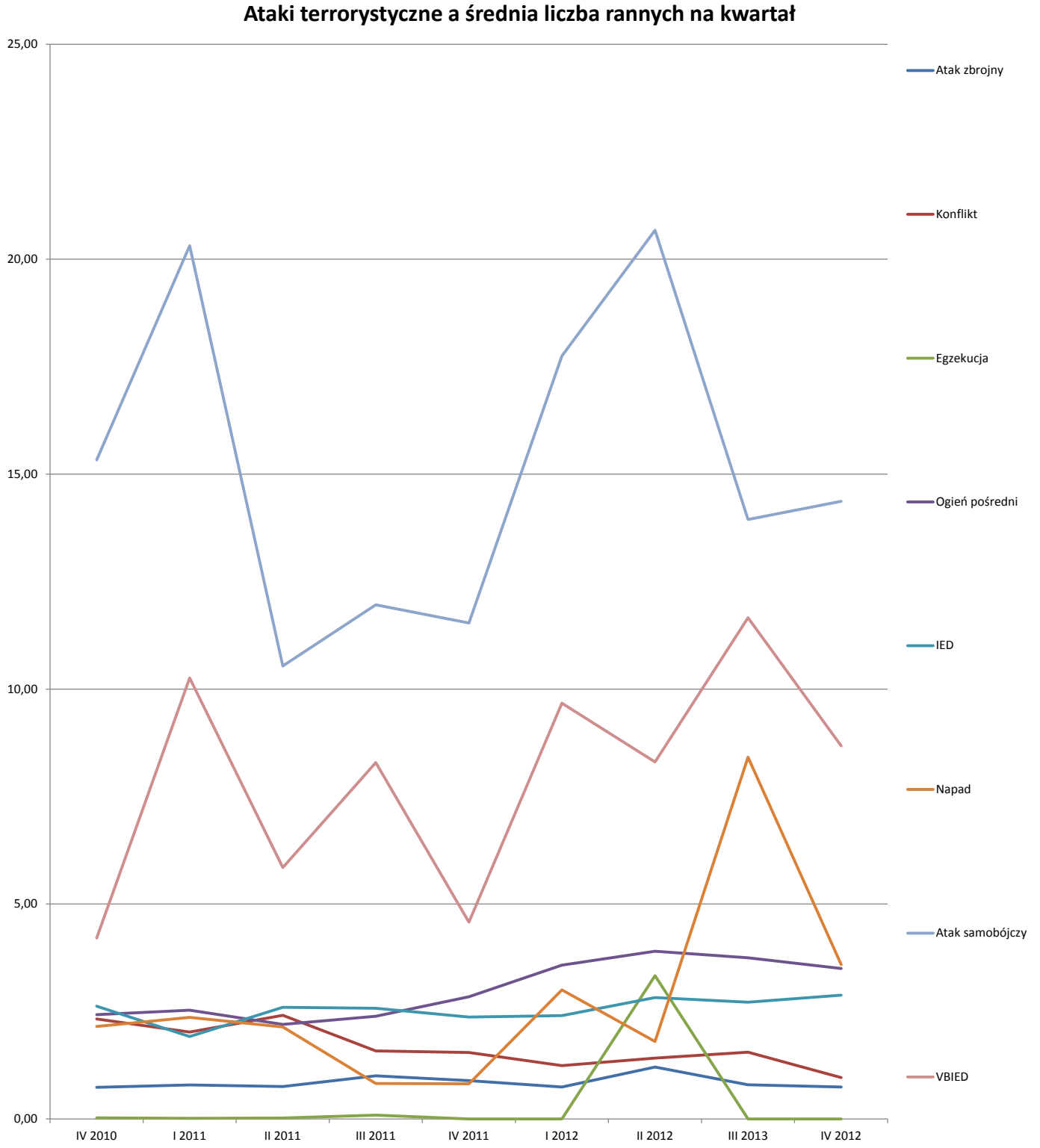
Wykres 9. Opracowanie własne, na podstawie danych COE–DAT.



Wykres 10. Opracowanie własne, na podstawie danych COE–DAT.

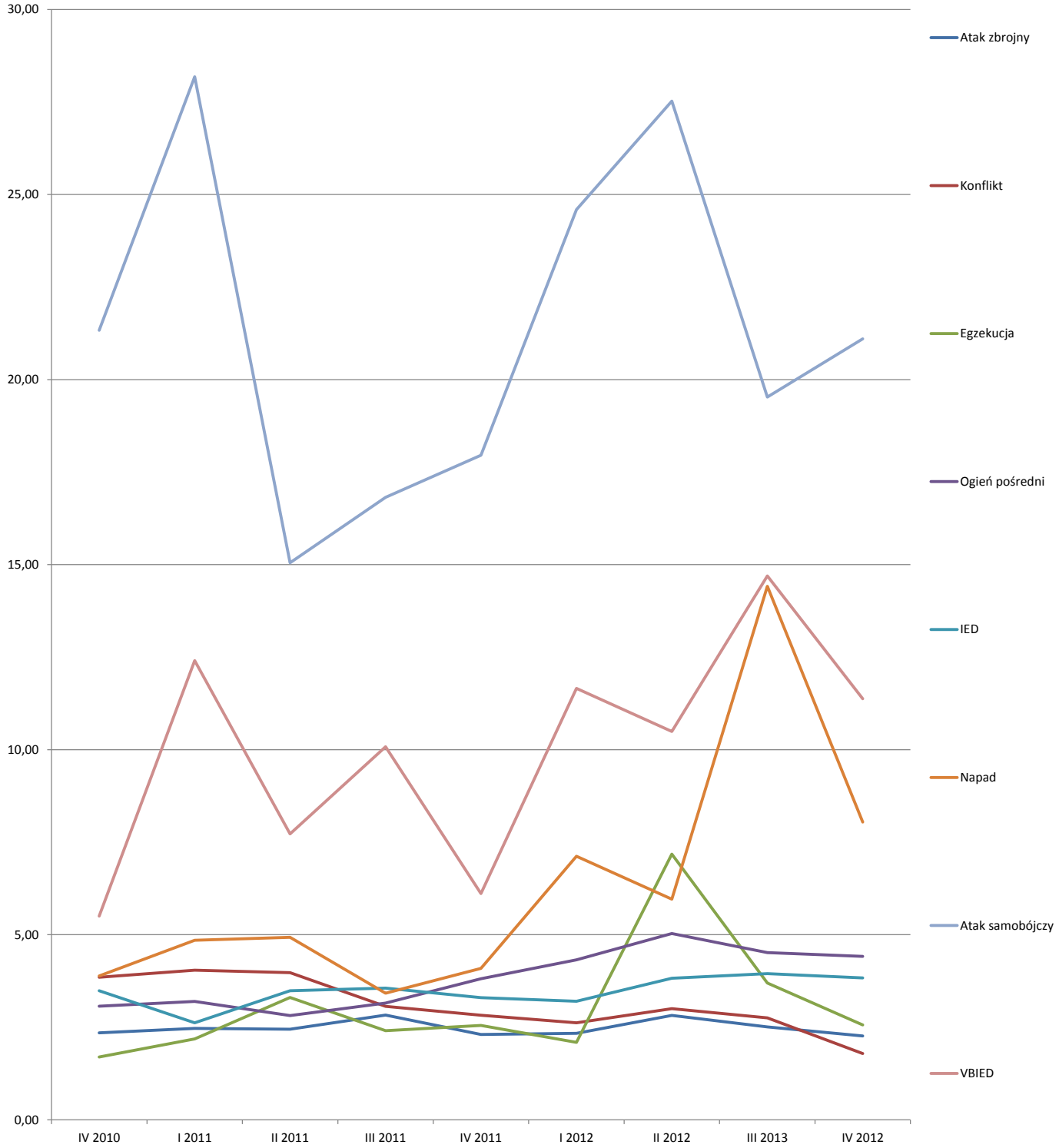


Wykres 11. Opracowanie własne, na podstawie danych COE–DAT.



Wykres 12. Opracowanie własne, na podstawie danych COE–DAT.

Ataki terrorystyczne a średnia liczba ofiar (w tym uprowadzonych) **na kwartał**



Wykres 13. Opracowanie własne, na podstawie danych COE–DAT.

Akty terrorystyczne w ujęciu kwartalnym – średnia zabitych, rannych i ofiar na atak

	IV 2010	I 2011	II 2011	III 2011	IV 2011	I 2012	II 2012	III 2013	IV 2012
średnio zabitych na atak	1,29	1,45	1,48	1,43	1,36	1,40	1,66	1,66	1,44
średnio rannych na atak	2,24	2,17	2,13	2,15	2,01	2,61	3,40	3,04	2,80
średnio ofiar (bez uprowadzonych) **na atak**	3,53	3,62	3,61	3,58	3,37	4,01	5,06	4,70	4,24

Tabela 2. Opracowanie własne, na podstawie danych COE–DAT.

Jak zobaczyliśmy wcześniej, rodzaje ataków terrorystycznych można rozpatrywać na różne sposoby. Gdyby za najgroźniejsze z nich uznać te, w których największy % ofiar to zabici, takimi atakami byłyby kolejno egzekucja (93%), atak zbrojny (66%), podpalenie (64%) oraz napad (49%) i konflikt (44%). Stosunkowo niewielka śmiertelność dotyczy ataku samobójczego (28%), IED (26%), ognia pośredniego (22%) i VBIED (21%). Z drugiej strony, najwięcej ofiar na przeciętny atak przypada kolejno na atak samobójczy (21,96), VBIED (10,26) napad (5,31) ogień pośredni (3,50), IED (3,45) i konflikt (3,26), egzekucję (2,73) i atak zbrojny (2,48). Przeciętna ilość zabitych wynosi najwięcej dla ataku samobójczego (6,22), napadu (2,59), egzekucji (2,55), VBIED (2,15), ataku zbrojnego (1,63), konfliktu (1,45), IED (0,91) i ognia pośredniego (0,76). Przeciętna ilość rannych była najwyższa dla ataku samobójczego (15,74), VBIED (8,12), ognia pośredniego (2,74), IED (2,54), napadu (2,31), konfliktu (1,80) i ataku zbrojnego (0,84), a na jedną egzekucję (co zrozumiałe) przypadało tylko po 0,16 rannych.

Wywnioskować można wysoką skuteczność zamachów samobójczych i VBIED, chociaż powodują więcej rannych niż ofiar śmiertelnych, a ataki samobójcze pod tym względem górują (28% do 21%). Napady, ataki zbrojne i konflikty cechują się wysoką śmiertelnością i stosunkowo niską średnią ofiar, co można tłumaczyć dużą ich brutalnością (celem jest zabicie ofiar, a nie ich zranienie). Ataki IED odznaczają się za to podobieństwem do ognia pośredniego - średnia ilość zabitych na atak jest niska (0,91 - 0,76), ale liczba rannych jest już wyższa (2,54 - 2,74), co w przypadku IED można wytłumaczyć pewną ochroną załogi pojazdu przed odłamkami, a w ogniu pośrednim - przypadkowością ofiar.

Podsumowanie

Czy zaprezentowane statystyki pozwalają zauważyć pewne trendy? Liczba zamachów terrorystycznych spada, ale rośnie ich skuteczność: średnia ilość rannych i zabitych na każdy atak jest w ostatnich 2-3 kwartałach wyższa niż rok - dwa lata temu. Tendencję rosnącą pod względem średniej liczby zabitych na atak wykazały atak samobójczy, napad, egzekucja, VBIED, IED i ogień pośredni, w przeciwieństwie do ataku zbrojnego i konfliktu, gdzie wskaźnik ten spada. Średnia liczba rannych wzrosła w atakach typu VBIED, napad i ogień pośredni. Stabilność lub niezauważalny wzrost dotyczy kategorii ataki samobójcze, IED i atak zbrojny. Spadek wartości nastąpił w przypadku konfliktu. Z kolei, wzrost średniej liczby ofiar (w tym uprowadzonych) nastąpił w VBIED, napadach, atakach samobójczych, egzekucjach, ogniu pośrednim i IED. Atak zbrojny cechuje się stabilnością, a tylko dla konfliktu nastąpił spadek, co można uznać za słabnącą skuteczność.

Rośnie ilość ataków typu VBIED (samochód-pułapka) oraz ich udział w ogólnej liczbie comiesięcznych zamachów. W mniejszym stopniu rośnie udział ataków IED oraz samobójczych, a także ataków zbrojnych. Liczba tych ataków spada, ale nie tak szybko jak pozostałych. Spada liczba uprowadzeń i uprowadzonych oraz ich udziału w liczbie ofiar, natomiast udział porwań w ogólnej liczbie ataków terrorystycznych utrzymuje się w równowadze. Liczba konfliktów (potyczek), egzekucji, ognia pośredniego, napadów i podpaleń oraz ich udział w comiesięcznej liczbie zamachów spadły. Na koniec, obok naszych rozważań nie możemy też przeoczyć smutnego faktu, iż za każdą z tych liczb stało życie człowieka i ludzkie tragedie.

Archiwalne numery e-Terroryzm.pl

– zapraszamy do zapoznania się!

Chcesz opublikować własny artykuł?

Wyślij go na e-mail: redakcja@e-terroryzm.pl

Zwyczajowa objętość artykułu to od 3 500 znaków (jedna strona) do 25 000 znaków (co odpowiada około 7-8 stronom). Można dostarczyć fotografie oraz tabele, wymagane są ich podpisy. Nie trzeba formatować tekstu. Formatowania oraz korekty dokonuje Redakcja.

Tematyka artykułu może poruszać sprawy powiązane z terroryzmem i bezpieczeństwem, a także politologią, zarządzaniem kryzysowym i ratownictwem, ochroną informacji niejawnych i infrastruktury krytycznej.

Nie jesteś pewien czy Twój artykuł odpowiada tematyce czasopisma? Przekonaj się o tym.

Na pewno odpowiemy na Twój list.

Redakcja zastrzega sobie prawo do skrótów oraz korekty.

Archiwalne numery dostępne na naszej stronie:

www.e-Terroryzm.pl

Strefa dobrej telekomunikacji

W ciągu 11 lat pokryli cały Śląsk siecią światłowodową. Wybudowali największe centrum przetwarzania danych w regionie. Mają już 1000 klientów i prawie 200 pracowników w kilku spółkach. Ich misją jest rozwój. Grupa 3S skutecznie tworzy na południu Polski strefę dobrej telekomunikacji.

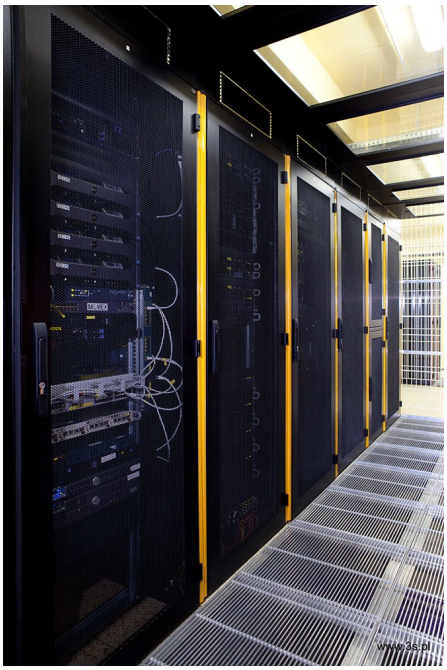
Światłowody dla każdego

Początek Grupie 3S dała spółka TKP S.A. założona w 2002 z zamiarem wybudowania na Śląsku sieci światłowodowej, gotowej by udostępniać ją każdemu, kto tego potrzebuje: operatorom dużym i mniejszym, biznesowi, czy administracji. Przez wiele lat spółka działała pod marką Śląskie Sieci Światłowodowe. Dostarczając hurtowy Internet lokalnym operatorom, znacząco przyczyniła się do spadku cen w tym sektorze, co przełożyło się na niższe ceny Internetu dla końcowego użytkownika. Do dziś, oferowanie infrastruktury jest podstawową działalnością firmy. Wraz z coraz gęstszą siecią, klientami 3S zostawało coraz więcej podmiotów biznesowych i instytucjonalnych. W krótkim czasie firma rozpoczęła współpracę z uczelniami wyższymi, bankami, czołowymi firmami przemysłu kolejowego, górniczego i energetycznego, a także z wieloma urzędami miast. W 2010 roku nastąpił rozwój usług dla klientów z sektora MSP, co przyczyniło się szybko do wzrostu liczby podłączonych adresów biznesowych.

Data center – biznes z przyszłością

Naturalną drogą rozwoju każdego operatora jest posiadanie własnego centrum przetwarzania danych. Budowa 3S Data Center ruszyła w 2009 roku na zakupionej działce w Katowicach, na terenie usytuowanym poza strefą zalewową. Wybór miejsca, na którym powstaje data center jest bardzo ważnym elementem tego rodzaju inwestycji. Pod uwagę brane są takie czynniki jak dojazd z dwóch stron do obiektu, sąsiedztwo dróg i innych obiektów, możliwość doprowadzenia podwójnych przyłączy światłowodowych i energetycznych oraz optymalne położenie względem autostrad i lotnisk. Liczy się także możliwość zaadaptowania terenu do wymagających norm Tier, określających dokładnie wszystkie parametry centrum danych. **3S Data Center** posiada 800m2 powierzchni kolokacyjnej, na której mieści się 220 szaf serwerowych. Z początkiem 2014 roku uruchomione zostanie dodatkowe 1000m2 w nowo budowanym obiekcie, fizycznie połączonym z istniejącym. Pojawi się zatem miejsce na kolejne 300 szaf pod kolokację serwerów.

Bezpieczeństwo ponad wszystko



3SData Center hołduje zasadzie, że bezpieczne centrum, to bezpieczne dane. W związku z tym, szczególną wagę przykłada się jak do zabezpieczeń fizycznych, tak i energetycznych, telekomunikacyjnych, a także do bezpieczeństwa środowiska pracy serwerów. 3S Data Center to monitorowany, chroniony teren oraz budynek wyposażony w strefy kontroli dostępu i systemy antywłamaniowe. Obiekt wyposażony jest w systemy przeciwpożarowe oraz systemy gaszenia dedykowane urządzeniom elektronicznym. Konieczne jest, by budynek tej klasy posiadał dwa niezależne przyłącza energetyczne SN o mocy 4MW każde od dwóch niezależnych dostawców energii elektrycznej, a także redundantne agregaty prądotwórcze i zasilacze UPS. Działanie wszystkich systemów monitoruje system SCADA. Kontroluje się w ten sposób parametry pracy urządzeń i systemów wspierających prawidłową pracę środowiska DC, zdarzenia mogące mieć wpływ na bezpieczeństwo, zu-

Fot. U.S. Marine Corps photo by Cpl. Ryan Walker