2. Metody pozyskiwania informacji i wyrządzania szkód

Niniejszy rozdział rozpatruje kolejny problemy szczegółowy, który przedstawiono we wprowadzeniu tzn.:

Jakie zagrożenia (i w jaki sposób) stwarza przestępczość komputerowa?

Problematyka drugiego rozdziału ukazuje szeroką gamę przestępstw komputerowych, które czasami się łączą nawet z socjotechniką w celu bycia jeszcze skuteczniejszymi. Przestępstwa wymienione w podrozdziałach ukazują wiele możliwości pozyskiwania informacji, jej preparowania lub blokowania. Dodatkowo rozdział uwzględnia problematykę wyrządzania szkód i ich wpływ na bezpieczeństwo marki danej organizacji. Rozdział prezentuje również możliwość pozyskiwania informacji i dostępu informatycznego poprzez podszywanie się przestępców różnymi sposobami.

Pozyskiwanie informacji w wojskowych sieciach teleinformatycznych jest złożone, a wymagania wobec bezpieczeństwa informacji w danych sieciach, opiewają na następujące obszary: bezpieczeństwa personalnego, bezpieczeństwa źródeł informacji, kontroli dostępu do zasobów sieci teleinformatycznej. Rozpatrując bezpieczeństwo personalne, osobowe dostosowuje się odpowiednio rekrutację i sprawdzenie personelu, który może posiadać dostęp do informacji niejawnych przekazywanych z wykorzystaniem sieci teleinformatycznych. Można tutaj mówić o osobach, które są odpowiedzialne za obsługę lub serwisowanie sprzętu informatycznego, może również to być personel sprzątający lub sfrustrowany, przekupny pracownik. Wspomniane przykłady podkreślają, jak ważna staje się odpowiednia weryfikacja i spełnienie wymagań w celu otrzymania poświadczenia bezpieczeństwa. Wymagania będą ciągle ewaluowały wraz ze zmianami postępującymi w technologii i informatyce. Kolejnym obszarem budującym podstawy bezpieczeństwa w obszarze wojskowych sieci teleinformatycznych jest bezpieczeństwo źródeł informacji, które jest swoistym rodzajem dokumentowania obiegu informacji, uprawnień. Potrzeba dokumentacji źródeł informacji jest związana z aspektem ochrony informacji od chwili jej powstania i nadania odpowiedniej klauzuli. Inny problem nasuwa się wraz z mobilnością jednostek wojskowych i ich działania na stanowiskach dowodzenia. Na tych stanowiskach powinny być przygotowane odpowiednio chronione miejsca (pojazdy, wozy dowodzenia), gdzie informacje są gromadzone i ochraniane przez bariery uniemożliwiające przechwycenie informacji. Dane bariery oprócz ochrony mają kolejny równie ważny cel, który polega na obronie informacji przed ich naruszeniem, zmianą, manipulacją. Ostatnim ważnym aspektem działania sieci teleinformatycznych jest kontrola dostępu do jej zasobów. Powinna ona się opierać na odpowiednim dopasowywaniu uprawnień użytkowników. Dowódca danej jednostki odpowiada

za organizację kontroli dostępu za pośrednictwem pełnomocnika do spraw ochrony informacji niejawnej. Zadaniem pełnomocnika jest natomiast określanie klauzuli informacji niejawnych, przygotowywanie identyfikatorów wymaganych do dostępu do stref bezpieczeństwa, przydzielanie kodów i haseł, ewidencjonowanie pracy (wejść i wyjść).[1]

Bezpieczeństwo informatyczne i informacji wraz z coraz szerszym dostępem do Internetu, rozwojem źródeł informacji i rosnącą jej ilością staje się podatniejsze na ataki z otoczenia organizacji. W dalszej części rozdziału zostaną przedstawione zagrożenia wynikające z czynnika ludzkiego, jak również i technologicznego. Istnienie różnych zagrożeń sprawia, że organizacje stają się pod wieloma względami podatne na szkodę. Poznanie natomiast możliwych zagrożeń pozwala na odpowiednie dostosowanie polityki bezpieczeństwa informacji do aktualnych rozwiązań technicznych i wymogów względem informacji. W Wojsku Polskim, jako organizacji rządowej, stającej na straży suwerenności Rzeczypospolitej Polskiej, wymagane jest ciągłe i jak najlepiej dostosowane optymalizowanie bezpieczeństwa informacji, ponieważ przekłada się ono na bezpieczeństwo Państwa. Pragnąc zapewnić wysoki poziom bezpieczeństwa informacyjnego i informatycznego wymagane jest przygotowanie odpowiednich zabezpieczeń, zasad bezpieczeństwa, szkoleń z zakresu bezpieczeństwa informacji i pojawiających się zagrożeń. Wymogi zaś, powinny być jasno sformułowane, sprawdzalne i swoim zakresem obejmować każdego żołnierza i pracownika cywilnego. Takie działania stają się czasochłonne i kosztowne, ale pozwolą budować odpowiednią świadomość bezpieczeństwa w Wojsku Polskim.

2.1. Pozyskiwanie informacji poprzez podszywanie się

Rozwijające się firmy i instytucje państwowe wraz ze wzrostem ilości osób pracujących w obrębie danej organizacji i napływem nowych technologii, narażone są coraz częściej na ataki przestępców. Cele ataków mogą być różne, ale głównym celem będzie zawsze pozyskanie informacji, która ma posłużyć do realizacji innych działań. Istotnym czynnikiem zagrażającym bezpieczeństwu informacji w obrębie organizacji i życia prywatnego pracownika danej organizacji jest człowiek. Kevin Mitnick w opisie swojej książki mówi: „Łamałem ludzi, nie hasła”[2] - jest to ważny punkt zaczepienia do dalszych rozważania i przedstawiania problemu bezpieczeństwa informacji w kontekście człowieka podatnego na socjotechnikę. Mówi się, że zespół, organizacja, jest tak silna, jak jej najsłabsze ogniwo. Myśląc o bezpieczeństwie informacji, można stwierdzić, że najsłabszym ogniwem jest człowiek. Niewyszkolony

[1]Andrzej Wisz, 'Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych', w *Biuro Bezpieczeństwa Narodowego*<www.bbn.gov.pl/download.php?s=1&id=1002> [dostępne: 6 luty 2012]
[2]Kevin Mitnick i William Simon, *Sztuka podstępu* (Gliwice: Helion, 2003).

pracownik pod względem bezpieczeństwa, stwarza bardzo duże ryzyko i staje się podatny na ataki polegające na podszywaniu, manipulacji, zachęcaniu do skorzystania z różnych stron internetowych, programów. Buduje to nowe możliwości dla przestępców, którzy przez odpowiednie przygotowanie się i zapoznanie się pod względem wszelkich informacji prywatnych z osobą atakowaną - preparują strony internetowe, wiadomości e-mail i uzyskują newralgiczne dane.

Metoda pozyskująca informacje poprzez podszywanie się, fałszowanie witryn, wiadomości, dokumentów elektronicznych, adresów internetowych nazywa się **Phishing** (ang. password harvesting fishing – łowienie haseł). W wolnym tłumaczenie może też oznaczać „łowienie ludzi na przynętę", ma na celu pozyskanie informacje przez stworzenie wiernych kopii zaufanych witryn, różniących się przeważnie miejscem dostarczania danych. Przykładowy atak polega na przygotowaniu wiadomości e-mail lub strony internetowej, która zachęca ofiarę ataku do skorzystania z podanego linku, zalogowania się do serwisu bankowego lub innego serwisu, gdzie będzie potrzebne podanie loginu i hasła. Po takim działaniu użytkownika może nastąpić przekierowanie do właściwego serwisu i zamonitowaniu błędu o błędnie wprowadzonym haśle. Jednak podczas całego procesu osoba atakująca zdążyła przechwycić dane do swojej bazy danych.[3] Jest to technika bardzo czasochłonna, wymagająca dużej wiedzy i przygotowania od przestępcy. Wymaga zabezpieczenia się przed: namierzeniem, rozpoznaniem nielegalnej strony, ponadto wymusza posiadanie wiedzy programistycznej. Efekty takiego ataku uzyskują powodzenie dopiero w skali makro, gdzie wiadomość lub spreparowana strona dociera do powyżej kilkudziesięciu tysięcy użytkowników. Potwierdzeniem takiego stanu rzeczy są statystki zebrane przez Kaspersky Lab przedstawione w tabeli 2.1.

[3] Por. Maciej Szmit i inne, *13 najpopularniejszych sieciowych ataków na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie.* (Gliwice: Helion, 2008).

Tabela 2.1 3 zasoby internetowe, które najczęściej zawierały przekierowania do szkodliwych odsyłaczy w trzecim kwartale 2011

Nazwa strony	Typ strony	Średnia liczba prób przekierowania dziennie
Facebook	Największy portal społecznościowy na świecie	96 000
Google	Największa na świecie wyszukiwarka	30 000
Yandex	Największa wyszukiwarka w rosyjskojęzycznym Internecie	24 000

Źródło: Kaspersky Lab, '3 zasoby internetowe, które najczęściej zawierały przekierowania do szkodliwych odsyłaczy w trzecim kwartale 2011', w *Viruslist*<http://www.viruslist.pl/analysis.html?newsid=690#13> [dostępne: 15 luty 2012]

Możliwości wraz z pozyskaniem dostępu do komputera ofiary rodzi się bardzo wiele. Najważniejszym czynnikiem określającym szkodliwość ataku jest jego celowość. Przestępca komputerowy w XXI wieku skupia się głównie na korzyściach majątkowych. Przestępcy o większej wiedzy i zdolnościach programistycznych w językach internetowych (Java, PHP, MySQL, Perl, Python) wykorzystają komputery zwykłych użytkowników w celach budowania sieci komputerów określanych mianem Zombie (komputer zarażony niebezpiecznym programem, przeważnie bez wiedzy użytkownika, dającym osobom postronnym wysokie uprawnienia). Przez ataki typu Phishing, gdzie użytkownik jest oszukiwany przez odpowiednio przygotowany dokument w różnej postaci nieświadomie traci zabezpieczenia i zastrzeżony dostęp do swojego systemu i komputera.

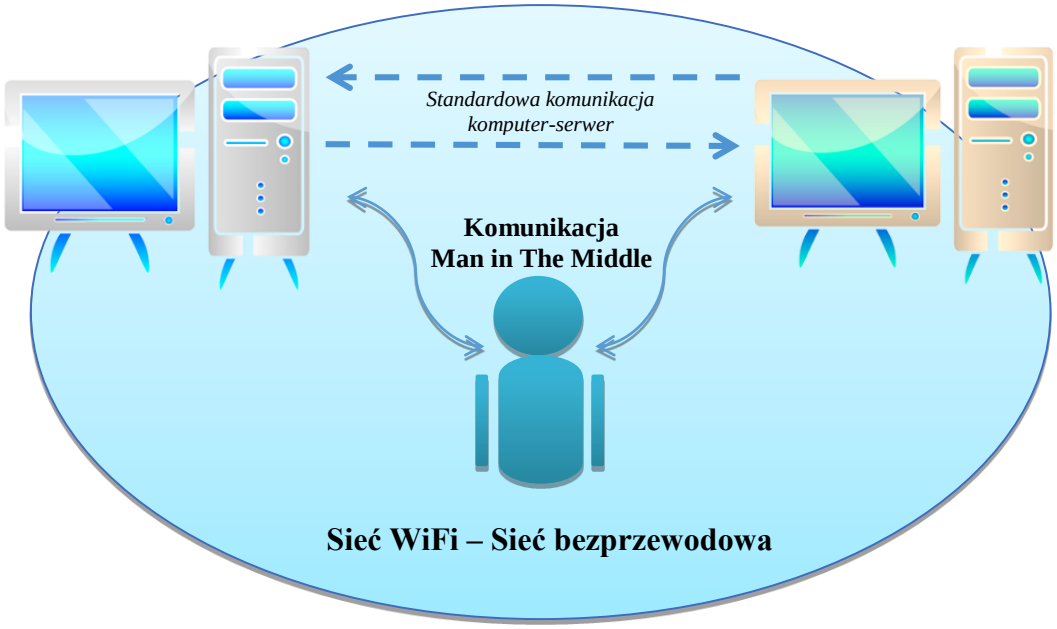
Skutki takiego zdarzenia w Wojsku Polskim mogą sprawić, że: zaczną wyciekać pospolite dane lub dane z klauzulą tajności, komputery żołnierzy lub pracowników cywilnych staną się źródłami przestępstw na skalę masową, zostaną wykorzystane do dalszych ataków, do szerszej inwigilacji danej jednostki wojskowej. W takim aspekcie odpowiednia polityka bezpieczeństwa i system zarządzania bezpieczeństwem powinien zapobiegać owym zdarzeniom. Natomiast, gdy nastąpi tego typu atak, albo zostaną wykryte częste połączenia (na niestandardowych portach i numerach ip), powinien monitować o zdarzeniach i przedstawiać, które komputery w danej sieci są zagrożone.

Podszywanie się w sieciach bezprzewodowych

Ludzkość stwarza nowe rozwiązania, wdraża nowe technologie by ułatwiać sobie życie. Tak samo dzieje się w przypadku bezprzewodowych rozwiązań, które mają swoje wady

i zalety. Głównymi zaletami sieci bezprzewodowych są: łatwa dostępność, ułatwiony sposób łączenia się między komputerami, przesyłanie danych bez okablowania, duży zasięg sieciowy, łatwa rozbudowa, łatwa konfiguracja. Oprócz wymienionych zalet są i wady, które wpływają znacząco na bezpieczeństwo działania sieci bezprzewodowych. W budowie sieci bezprzewodowych główną wadą jest to, że dostęp do punktów dostępowych ma każdy, pomimo, że są zabezpieczone. Komunikacja sieciowa oparta jest na komunikacji radiowej, gdzie urządzenia radiowe (karty wifi, routery, access pointy) ze sobą się komunikają. Takie rozwiązanie stwarza zagrożenie nie autoryzowanego: dostępu do sieci i podsłuchiwania danych (nawet zaszyfrowanych). Przykładem działania przestępczego w sieciach bezprzewodowych mogą być techniki **DNS-spoofing** i **Man In The Middle**.[4] Technika DNS-spoofing oparta jest na technologii domain name service, której zadaniem jest translacja adresów IP na adres w postaci nazw i odwrotnie. Zadaniem DNS w Internecie jest odpowiednie przypisanie nazwy, przykładowo www.wojsko-polskie.pl na IP odpowiedniego serwera DNS (ns2.nabino.pl – 195.26.13.16), który wskaże u siebie stroną internetową. Przestępca wykorzystując taką technikę, może podstawić fałszywą stronę, podczas gdy użytkownik będzie myślał, że odwiedził odpowiednią witrynę. W sieciach bezprzewodowych taki atak jest łatwiej wykonać wykorzystując technikę Man In The Middle, która polega na wejściu w interakcje pomiędzy klienta (komputer użytkownika), a serwer.[5] W takim wypadku przestępca „wpychając się" w sieci radiowej pomiędzy nadajnik (router, serwer, access point) udaje nadajnik i staje się pośrednikiem w procesie przesyłania danych, obrazuje to rys. 2.1. Z racji coraz większych odległości dostępnych w sieciach bezprzewodowych zagrożenia staje się coraz bardziej realne. Przestępca nie musi fizycznie mieć dostępu do routera lub gniazda sieciowego, może znajdować się poza budynkiem jednostki lub nawet jej ogrodzeniem. Mimo coraz lepszych zabezpieczeń i standardów szyfrowania haseł dostępowych do sieci, są one łamane, po przechwyceniu pakietów dostępnych w eterze sieciowym. Dlatego wykorzystywanie sieci bezprzewodowych, które są podatne na ataki Man in The Middle powinno być dobrze zaplanowane i ograniczone sygnałowo w ramach jednostki wojskowej.

[4] Por. Bob Toxen, *Bezpieczeństwo w Linuxie. Podręcznik administratora* (Gliwice: Wydawnictwo Helion, [n.d.]).
[5]Por.Mariusz Gliwiński i Robert Dylewski, *Ataki na sieci bezprzewodowe. Teoria i praktyka.* (Kwidzyn: Wydawnictwo CSH, 2010).



Rys. 2.1 Schemat ataku Man in The Middle

Źródło: opracowanie własne

Przestępca komputerowy, który złamie zabezpieczenia do sieci nie musi koniecznie wykorzystywać techniki MITM albo DNS-spoofing, czasem wystarczy, że wykorzysta programy do skanowania zasobów sieci i dzięki nim pozyska podstawowe/wstępne dane do dalszych ataków. Może to być zlokalizowanie komputera (adresu IP i systemu operacyjnego) i nazwy użytkownika dowódcy jednostki. Dowodem na niską świadomość płynących zagrożeń i braku zabezpieczeń w sieciach bezprzewodowych mogą być dane zebrane przez Kaspersky Lab zaprezentowane w tabeli 2.2 dane ukazują ,w jak wielu miastach na terenie Polski, istnieje niezabezpieczonych sieci bezprzewodowych, prawie co czwarta sieć działa bez szyfrowania klucza dostępu. Takie sieci pozwalają, przy odpowiednich zasobach i wiedzy, na przemyślane ataki z wykorzystaniem komputerów, gdzie przestępca jest nienamierzalny, ponieważ podszywa się pod czyiś adres IP.

Tabela 2.2 Wykorzystywane mechanizmy szyfrowania – tabela

	WPA/WPA2 (2010-11)	**WPA/WPA2 (2009)**	**WEP (2010-11)**	**WEP (2009)**	**Bez szyfrowania (2010-11)**	**Bez szyfrowania (2009)**
Toruń	56,10%	44,20%	25,27%	33,50%	18,63%	22,30%
Katowice	51,63%	50,00%	18,24%	29,30%	30,13%	20,75%
Kraków	42,64%	44,23%	23,95%	29,49%	33,41%	26,27%
Częstochowa	35,47%	-	31,35%	-	33,18%	-
Łódź	52,73%	50,60%	18,27%	24,50%	29,00%	24,90%
Warszawa	46,39%	53,61%	21,56%	26,73%	32,04%	19,66%
Lublin	64,00%	49%	16,60%	23,79%	19,40%	27,21%
Trójmiasto	67,77%	58,95%	16,06%	25,53%	17,17%	15,52%
Kielce	64,65%	-	15,66%	-	19,69%	-
Poznań	59,21%	44,61%	20,94%	35,04%	19,85%	20,35%
Wrocław	65,06%	-	16,21%	-	18,73%	-
Podsumowanie	**55,06%**	**49,40%**	**20,28%**	**28,48%**	**24,66%**	**22,12%**

Źródło: Kaspersky Lab, 'Bezpieczeństwo sieci WiFi w Polsce 2010/2011: Podsumowanie', w *Viruslist*<http://www.viruslist.pl/analysis.html?newsid=682> [dostępne: 20 luty 2012]

Wykorzystując sieci bezprzewodowe w jednostce wojskowej, bez ograniczeń zasięgu i o niskich zabezpieczeniach może dojść do naruszenia bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji. Przestępcy komputerowi mogą wykorzystywać sieci bezprzewodowe do podszywania się pod inne komputery w sieci lub do podsłuchiwania ruchu sieciowego. Trudno zatem jest optymalizować poziom bezpieczeństwa teleinformatycznego i informacyjnego w obrębie danej jednostki wojskowej. Mimo nawet wysokiego standardu szyfrowania, sieć, która jest rozległa zasięgiem, nie stanowi problemu do inwigilacji i może podlegać próbom złamania hasła dostępu bez wiedzy administratorów sieci. Odpowiedzią na przedstawiony problem powinno być dostosowanie polityki bezpieczeństwa i systemu zarządzania bezpieczeństwem, tak ,aby sprzyjał pracy informatycznej na jednostce wojskowej, jak i bezpieczeństwu teleinformatycznemu.

Podszywanie się telefoniczne

Telefon wpisał się w standardy życia codziennego. Posiadają go już nastolatkowie, czasem nawet dzieci, które są kontrolowane przez rodziców. Dzisiaj brak telefonu, kojarzy się z pewnego rodzaju niebezpieczeństwem, ponieważ nie mając go, może się tak zdarzyć, że trzeba będzie wezwać pomoc. Osoby często korzystające z telefonu, posiadają przeważnie dwa numery, jeden domowy/rodzinny, a drugi służbowy, wykorzystywany w kontaktach związanych z pracą. Można by się zastanowić, jak sam telefon może zaszkodzić, bądź kontakt telefoniczny. Tutaj warto powrócić do działań socjotechnicznych i wpływu psychologii na zachowania ludzkie.

Ingracjacją określa się zjawisko w którym człowiek pragnie sobie zjednać inne osoby. Witkowski w swojej książce określa techniki takie jak: konformizm, podnoszenie wartości partnera, manipulacje związane z autoprezentacją, które odpowiednio zrozumiane ułatwiają manipulacje. Człowiek jest osobą z natury społeczną, poszukującą wspólnot.[6] Pragnie mieć poczucie wsparcia, jedności, zrozumienia, pozytywnej komunikacji. Takie uczucia pragnie wywołać przestępca, socjotechnik wykorzystując telefon. Oprócz podstawowych technik, mogą zostać wykorzystane inne, które w połączeniu, spotęgują efekt manipulacji, perswazji rozmówcą. Ponadto sam rodzaj komunikacji telefonicznej ułatwia zadanie przestępcy, a jest za to utrudnieniem dla osoby atakowanej. Odbierając telefon można zidentyfikować zazwyczaj rozmówcę po głosie lub numerze połączenia. Niestety jest za mało cech, które dają stu procentową identyfikację. Inny problem się pojawia przy ilości odbieranych telefonów, mianowicie problem braku czasu, który jest wymagany przy identyfikacji. Pragnąc wyłudzić informację od rozmówcy socjotechnik wykorzysta wcześniej wspomniane techniki manipulacji. Często będzie pracował odlegle w czasie, nie będzie pytał się wprost lub od razu prosił o pomoc. Wywrze dobre wrażenie, zdobędzie zaufanie, pozna wcześniej slang korporacyjny, a dopiero następnie w utajnionych (niezauważalnych) pytaniach, będzie starał się zdobyć niby mało istotne informacje.[7] Dlatego kluczowym aspektem, który nie powinien być nigdy pomijany jest odpowiednia **identyfikacja** rozmówcy, osoby z którą się komunikujemy. Dodatkowo nie powinno się ujawniać nawet mało znaczących informacji, nawet pospolitych w przedsiębiorstwie.

Podszywanie się w świecie internetowym i rzeczywistym nie jest czymś niecodziennym. Wiele osób nie raz słyszało o różnych incydentach w gazetach lub telewizji.

---

[6]Por. Tomasz Witkowski, *PSYCHOMANIPULACJE - Jak je rozpoznawać i jak sobie z nimi radzić.*, wydanie pierwsze edn ([n.p]: Oficyna Wydawnicza UNUS, 2000).

[7] Por. William Chestwick, Steven Bellovin i Aviel Rubin, *Firewall-e i bezpieczeństwo w sieci. Vadamecum profesjonalisty* (Gliwice: Helion, [n.d.]).

Często pewnie związanych z wyłudzeniem danych bankowych lub danych osobowych. Głównym problem zjawiska wyłudzania danych przez podszywanie się jest człowiek. To on staje się tutaj słabym ogniwem, gdyż przez swoje uwarunkowania psychologiczne, otoczenie jest łatwym celem. Podatność ludzka zwiększa się wraz ze zmęczeniem danej osoby lub z przeciążenia pracą. Wtedy taka osoba jest roztargniona, nieskupiona i często przestaje logicznie myśleć. Takim sytuacjom, niestety, nie da się zapobiec, ale z odsieczą powinny przychodzić wyuczone nawyki dotyczące procedur polityki bezpieczeństwa, które nie raz były testowane w przedsiębiorstwie. W innym przypadku, przedsiębiorstwo jest narażone na nadużycie dotyczące możliwości socjotechnicznych lub wad sieci bezprzewodowych i utratę mniej lub bardziej cennych informacji.

2.2. Pozyskiwanie informacji z wykorzystaniem luk bezpieczeństwa

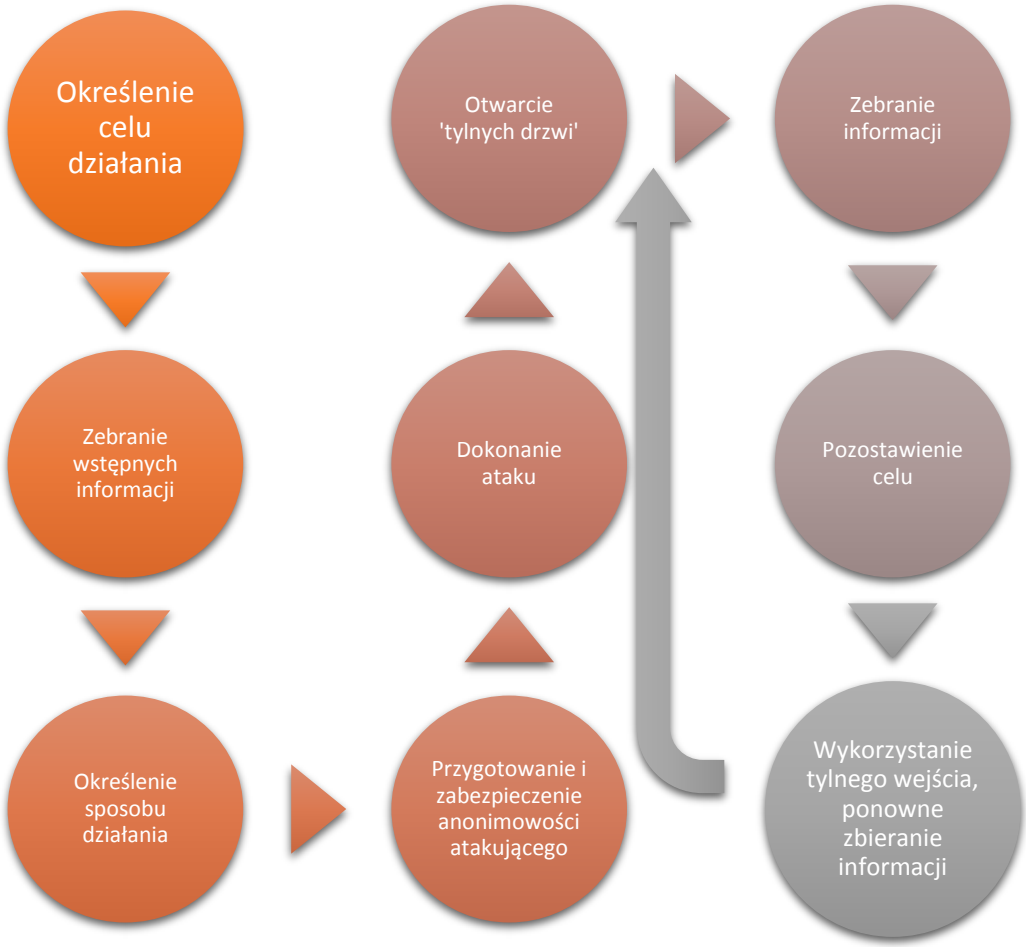
Programiści tworząc każde oprogramowanie nie są w stanie ustrzec się błędów, dlatego są wydawane uaktualnienia, poprawki błędów, stosuje się badanie programów, zbieranie informacji o błędach od użytkowników. Można ująć, że prawdopodobnie nie ma programu w pełni bezpiecznego, wolnego od skaz programistycznych w zakresie bezpieczeństwa. Zatem patrząc dalej, trzeba spojrzeć na całe systemy operacyjne, które oparte na jądrze i wielu programach wspierających, będą posiadać statystycznie więcej błędów. Takie błędy stają się pożywką dla przestępców, którzy pragną wykraść informacje lub przeprowadzić atak mający wyrządzić szkodę przedsiębiorstwu.[8] W dalszej części tego podrozdziału zostaną przedstawione sposoby działania, luki bezpieczeństwa i programy wykorzystywane w celach pozyskiwania informacji. Pozyskiwanie informacji w oparciu o błędy programowe jest bardzo skomplikowanym procesem, który wymaga wiedzy specjalistycznej. By dokonać jakiegoś ataku, nie wystarcza wiedza jednej osoby. Często takich ataków, dokonują grupy przestępcze w których to osoby komunikują się między sobą w celu znalezienia luk bezpieczeństwa.

Nie można pozyskać informacji, wykryć luk bezpieczeństwa nie stosując się do logicznego modelu postępowania. Taki model ma swój cel, określoną drogę zbierania informacji, analizę celu, utajnienia włamywacza, zabezpieczenia „tylnych drzwi" / „tylnego wejścia". Sposobów na osiągnięcie danego celu (przechwycenie informacji), może być przeważnie kilka, zależnych przeważnie od wykorzystywanych programów, technologii lub

[8]John Viega, *Mity bezpieczeństwa IT* (Gliwice: Helion, 2010).

zabezpieczeń. Niestety nie ma stu procentowych zabezpieczeń, gdyż gdy coś zostaje opracowane, pojawiają się osoby, które szukają i analizują błędy w danym opracowaniu.

Na rys. 2.2 przedstawiono schemat, który jest wyjściem do dalszych interpretacji działań przestępców wykorzystujących luki, błędy w programach, systemach operacyjnych. Mogło by się wydać, że włamanie do komputera/programu/systemu operacyjnego jest to krótki proces. Niestety rozważny przestępca, który nie chce pozostawić śladów swojej działalności lub jeśli już pozostawia, to prowadzące do błędnych osób. **Określenie celu działania** jest to zestaw czynności i procesów myślowych skupiających się na odpowiedzi na takie pytania jak: co chcę dokonać?; czy chcę uzyskać dostęp, czy może pozyskać dane?; jakie dane pozyskać?; czy chcę spreparować dane?; czy mam pozostawić ślady?; jeśli tak to jaki?. Po uzyskaniu odpowiedzi na powyższe przykładowe pytania, przestępca przechodzi przeważnie do kolejnego etapu, czyli **zebrania wstępnych informacji** (może ten etap zostać pominięty, wtedy gdy przestępca działa na zlecenie i posiada już wstępne dane), etap ten został przedstawiony w rozdziale pierwszym pracy naukowej. Kolejnym krokiem działania w procesie pozyskiwania informacji jest **określenie sposobu działania**. Problemem w tym miejscu dla przestępcy jest znalezienie odpowiedzi (mając wstępne informacje) na pytania: w jaki sposób mam osiągnąć cel?; jakie technologie może wykorzystać?; jakie posiada możliwości względem posiadanych informacji?; czy zna luki w zabezpieczeniach celu ataku?; czy może zostać namierzony?; czy wstępne informacje są wystarczające by dokonać pewnego ataku?. Odpowiedzenie na podane pytania może być bardzo trudne i nie wystarczające, aby przejść do kolejnych etapów. Dlatego czasem wymagane jest ponowne zebranie wstępnych informacji wykorzystując szersze działania (socjotechnika, podszywanie się).



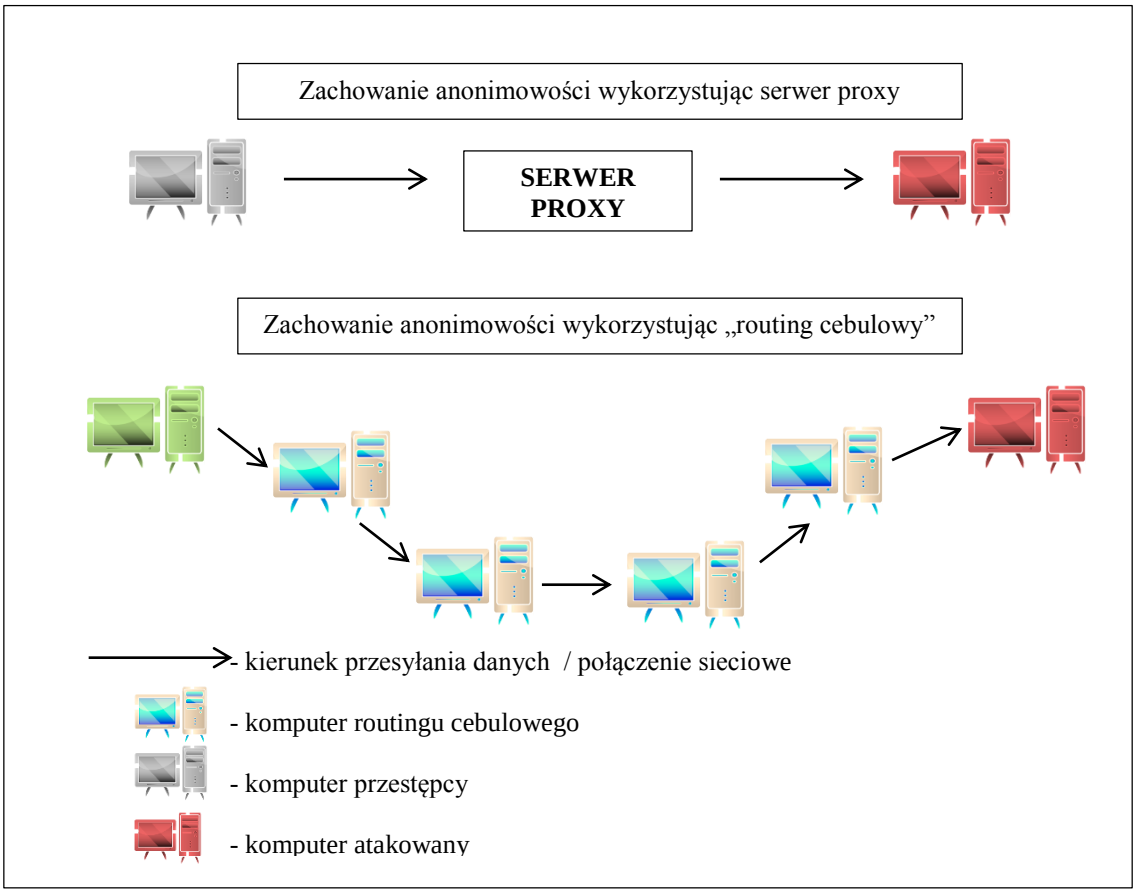
Rys. 2.2 Schemat pozyskiwania informacji z wykorzystaniem luk bezpieczeństwa.

Źródło: opracowanie własne

Kolejnym obszarem działania jest zabezpieczenie **anonimowości** (skrytości) ataku, które opiera się na wykorzystaniu innych adresów IP do wykonania ataku. Jest to niezbędne, gdyż wiele komputerów, sieci i dostawców internetowych posiada zabezpieczenia nie tylko w postaci zapór sieciowych, ale i rejestru logów i połączeń. Dzięki takiemu rejestrowi można odnaleźć przestępcę po odczytaniu czasu zdarzenia i numeru IP. Do podania fałszywego adresu IP wykorzystywane są serwery PROXY lub komputery wykorzystujące „routing cebulowy" (rys. 2.3).[9] Niestety takie rozwiązania nie dają stu procentowej pewności bo są obciążone ograniczeniami. Szyfrowana komunikacja opiera się wyłącznie po TCP, natomiast UDP już nie. Po UDP są przesyłane komunikaty DNS. Przez to anonimowość staje w takim wypadku pod znakiem zapytania. Można jednak i temu zaradzić wykorzystując program Tor

[9] Por. Maciej Szmit i inne, *13 najpopularniejszych sieciowych ataków na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie.* (Gliwice: Helion, 2008).

z programem Privoxy.[10]Wykorzystanie serwera proxy lub „routingu cebulowego" zakłóca identyfikację sprawcy ataku, ponieważ mając nawet rejestr logu wskazywane są IP tylko komputerów pośredniczących w ataku. Można by jednak pomyśleć, że wystarczy zgłosić się do dostawców internetowych tych komputerów, lecz tutaj przeważnie pojawia się przeszkoda międzynarodowa. Komputery pośredniczące w ataku będą przeważnie pochodziły z poza kraju atakującego, dlatego nie łatwo będzie namierzyć bez pomocy administratora komputera pośredniczącego ,skąd pochodziło połączenie atakującego. Problem wzrasta jednocześnie wtedy, gdy komputerów pośredniczących było kilka lub kilkanaście. Dlatego nawet posiadanie odpowiedniego systemu logowania połączeń przychodzących i wychodząc nie pozwoli stwierdzić, kto wykradł informacje.



Rys. 2.3 Schemat zachowywania anonimowości w sieci.

Źródło: opracowanie własne

Jeśli zostaną już zebrane odpowiednie informacje, określi się sposób działania i zabezpieczy anonimowość zostaje wykonany atak na cel. Do wykonania ataku na cel jest wymagana luka bezpieczeństwa lub wcześniej przygotowane „tylne wejście". Pragnąc odnaleźć lukę bezpieczeństwa w atakowanym komputerze można wykorzystać wiele sposobów

[10] Tamże

i programów. Część zostało wymienionych w rozdziale pierwszym. Warto jednak przytoczyć ich definicje, które pozwolą pojąć skalę zagrożeń. W Internecie każdego dnia powstają nowe formy i odmiany wirusów komputerowych, które są programami należącymi do programów złośliwych (malware) i wymagają programu nosiciela do którego się je dołącza. Można je podzielić na podtypy takie jak: gnieżdżące się w boot sektorze dysku twardego; plikowe; EPO (ang. Entry-Point Obscuring), rezydentne; towarzyszące.
W zależności od typu różnią się one miedzy sobą działaniem. Potrafią pozostawać w pamięci komputera, tworzyć osobne pliki, wykonywać skok do innego fragmentu kodu w danym programie, dopisywać się na początku pliku wykonywalnego. Wirusy są przeważnie masowo rozsyłane i rozpowszechniane, często mają na celu uruchomienie Trojana (konia trojańskiego), który w ukryciu będzie wykonywał polecenia z zewnątrz (od przestępcy). Innym rodzajem złośliwego oprogramowania są programy typu Backdoor, których zadaniem jest tworzenie luki w zabezpieczeniach, poprzez otwieranie portu na zaatakowanym komputerze i nasłuchiwanie w oczekiwaniu na polecenia. Innym wartym uwagi i popularnymi programami w sieci są oprogramowania szpiegowskie (ang. spyware), które są zamieszczane w darmowych programach. Mogą służyć do zbierania informacji marketingowych lub zbierania informacji o zasobach systemowych, bez zgody właściciela systemu. Niebezpieczny program, który często jest bardzo dobrze kamuflowany po zainfekowaniu komputera nazywa się keyloggerem. Zadaniem tego programu jest gromadzenie, zapisywanie i wysyłanie do przestępcy wykonanych działań na atakowanym komputerze (naciskane klawisze, kliknięcia myszki, uruchomione programy). Dzięki takiemu programowi może dojść do pozyskanie loginu i hasła przez przestępcę do systemu komputerowego, poczty internetowej lub serwisów społecznościowych.[11] Chcąc wykonać atak komputerowy nie jest obecnie wymagana znajomość programowania, choć może przyczynić się do skuteczniejszego wykonania ataku. Wspomniane w rozdziale pierwszym programy, systemy operacyjne mogą w pełni posłużyć do wykonania ataku, w szczególności jeśli cel ataku nie utrzymuje odpowiedniego poziomu aktualności oprogramowania.

Trudniejszym aspektem po dokonaniu ataku jest przygotowanie sobie „tylnego wejścia". Wykonanie i zabezpieczenie „tylnego wejścia" ma kilka celów. Jednym z głównych celów jest umożliwienie ponownego dostępu do zaatakowanego komputera. Pozwoli to na ciągłe wykradanie, przeglądanie, analizowanie powstających danych na danym komputerze. Innym celem przygotowania „tylnych drzwi" może być utworzenie z zaatakowanego

[11]Maciej Szmit i inne, *13 najpopularniejszych sieciowych ataków na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie.* (Gliwice: Helion, 2008).

komputera - komputera „Zombie", który będzie współdziałał z siecią botnet. Taki komputer może zostać wykorzystany do innego ataku (np. wykorzystany w celu bycia anonimowym – wykorzystując inny adres IP) lub w celu przeprowadzenia ataku DDOS (ang. distributed denial of service). Po takim ataku i zabezpieczeniu **„tylnego wejścia"** przejmuje w pełni i na stałe kontrolę nad komputerem i systemem operacyjnym. Taka kontrola będzie występowała tak długo dopóki nie zostanie wykryty lub nie ulegnie uszkodzeniu system właściciela zaatakowanego komputera. Rozwiązaniem wśród przestępców jest wykorzystywanie phishingu i rozsyłanie wielu tysięcy wiadomości e-mail. Dzięki temu, co jakiś czas zdobywają dostęp do jakiegoś komputera, następnie analizują jego zawartość. Pragnąc się ustrzec przed działaniem przestępców i powracaniem do przejętego komputera, warto działać w sieci wykorzystującej dodatkowe zabezpieczenia takie jak: zapora sieciowa lub translacje adresów (ang. NAT). Pozwala to na utrudnienie działania przestępcom, ponieważ dobrze zabezpieczona sieć będzie blokować niepożądane działania. Ważnym aspektem przy budowaniu dostępu teleinformatycznego w jednostce wojskowej, jest określenie polityki bezpieczeństwa wraz z systemem zarządzania bezpieczeństwem. Niestety samo utworzenie dokumentów nie będzie miało żadnego wpływu na optymalizację bezpieczeństwa, jeśli nie będzie w sposób ciągły podnoszona świadomość bezpieczeństwa informacyjnego i informatycznego. Wartym uwagi rozwiązaniem jest wykonywanie zewnętrznych (obiektywnych) audytów bezpieczeństwa przez firmy z dużym doświadczeniem i wiedzą. Inną opcją jest odpowiednie przeszkolenie informatyków jednostki wojskowej i nakazanie wykonywania testów penetracyjnych. Takie testy mogą polegać na okresowych próbach „wykradania" informacji z jednostki. Oczywiste jest, że powinny być przygotowywane z odpowiednią dokumentacją, za zgodą dowódcy jednostki i pełnomocnika ochrony. Przedstawione rozwiązania są tylko zalążkiem przykładów, które mogą wspierać zabezpieczanie się przed atakami i ich skutkami w jednostce wojskowej. Pozostaje jednak ciągle problem czysto technologiczny, gdzie niektóre rozwiązania stają się przestarzałe, a czynnik ludzki przestaje mieć znaczenie. Wtedy programiści zaczynają wykorzystywać różnego rodzaju luki bezpieczeństwa.

Rozdział pierwszy pracy naukowej przedstawiał określenia problemów bezpieczeństwa informatycznego. Przy problematyce podszywania się z wykorzystaniem luk bezpieczeństwa, warto rozwinąć czym są owe luki, jak są definiowane, jak oddziałują na system i zabezpieczenia systemowe.

„***Eksploit (ang. exploit)*** *– narzędzie (najczęściej kod lub zestaw instrukcji), służące do wykorzystania podatności (słabego punktu) programu,*”[12] Na początku powstawania systemów komputerowych i sieci komputerowych, wykorzystywano proste narzędzia dostarczane głównie wraz z systemem Windows. Służyły one do testowania łącza, odczytywania różnych parametrów sieciowych. Obecnie wraz z rozwojem nowych procesorów, wzrostu możliwości obliczeniowych programy stają się bardziej złożone i zarazem bardziej odporne. Niestety, gdy coś zostaje zabezpieczone, przestępcy o wysokiej wiedzy informatycznej (w szczególności programistycznej na poziomie procesora), szukają błędów w oprogramowaniu i opracowują nowe Eksploity.

„***Słaby punkt, podatność (ang. vulnerability)*** *– wada algorytmu (samego mechanizmu lub jego implementacji) systemu bądź aplikacji, której poprawne wykorzystanie przez atakującego (hakera) może doprowadzić do działania, które nie zostało przewidziane przez projektantów systemu. Zazwyczaj działanie takie owocuje przejęciem kontroli nad systemem lub aplikacją, zmianą uprawnień użytkownika (tzw. Podniesienie uprawnień) lub po prostu niestabilnym działaniem zaatakowanego systemu lub aplikacji,*”[13] Jak zostało wspomniane w rozdziale pierwszym i w przedstawionym przykładzie strony internetowej www.exploit-db.com podatności i informacji dostępnych o nich w Internecie jest bardzo dużo, ponadto każdego dnia są odkrywane coraz nowsze. Dlatego coraz ważniejszy staje się proces **aktualizacji** każdego oprogramowania zainstalowanego na danym stanowisku pracy (w szczególności jeśli jest połączony bezpośrednio lub pośrednio z Internetem). Aktualizacje oprogramowania nie mogą zostawać odwlekane lub pomijane. W przyszłości mogą skutkować wyciekiem, uszkodzeniem lub spreparowaniem danych.

„***0day*** *– eksploit dla danej podatności, której istnienie nie jest publicznie znane. Eksploity tego typu stanowią ogromne zagrożenie dla bezpieczeństwa komputerowego,*”[14] Najgorszym problemem rozszerzającym się na skalę globalną staje się czarny rynek. Jest on powiązany z eksploitami typu 0day, które nigdy nie zostały wykorzystane. Wiąże się to z wieloma możliwościami działań przestępczych. Eksploity 0day są sprzedawane w celu przeprowadzenia wcześniej przygotowanego ataku, którego celem jest osiągnięcie wysokich korzyści. Celami w których mogą zostać zakupione eksploity 0day mogą być: wykradzenie tajnych informacji z firmy konkurencyjnej, zniszczenie zaplecza bazodanowego, włamanie się do wielu komputerów w celu ciągłego szpiegowania pracowników konkurencyjnego

[12]Por. Piotr Planeta i Bogdan Drozdowski, *Bezpieczeństwo aplikacji Windows 7, Vista, XP* (Kwidzyn: Wydawnictwo CSH, 2012).
[13] Tamże
[14] Tamże

przedsiębiorstwa(armii). Eksploity 0day przeważnie nie będą wykorzystywane w mniej korzystnych celach, ponieważ wykrycie luk w oprogramowaniu jest czasochłonne i wymaga wiedzy z konkretnej dziedziny informatyki. Innym problemem związany z eksploitami 0day jest taki, że po zgłoszeniu do producenta o istnieniu takiej luki jest wymagany czas, przeważnie tydzień i więcej. W tym czasie niestety przestępca komputerowy ma wolną rękę działania, albo przedsiębiorstwo jest zmuszone do wyłączenia danego oprogramowania.[15] Wiąże się to niestety z kosztami, a czasem nawet z zaprzestaniem pracy danej firmy. Problem staje się mniejszy, jeśli następuje odpowiednia reakcja ze strony informatyka. Taka sytuacja zmusza jednocześnie do zastosowania odpowiedniej procedury, która minimalizuje skutki incydentu. Niestety w przedsiębiorstwach, które nie posiadają odpowiednich systemów zarządzania bezpieczeństwem informacji lub nie są one odpowiednio aktualizowane, reakcja na incydent z wykorzystaniem eksploitu 0day jest znikoma albo opóźniona.

Innym znaczącym zjawiskiem, który staje się nową bronią w armiach świata jest wykorzystanie eksploitu do działań wywiadowczych i przygotowujących do cyberwojen. Polega ono na tworzeniu pododdziałów informatycznych i szkoleniu ich w tworzeniu eksploitów, wykorzystywaniu ich i budowania sieci zainfekowanych komputerów, które mogę być wykorzystywane w różnych celach. Takie działania mogą z czasem zagrażać bezpieczeństwu informatycznemu państw. Celami takich działań może być destabilizacja dostępu do pieniędzy mieszkańców w bankach (co wywołuje straty gospodarcze)[16]. Z czasem gdy nowe rozwiązania informatyczne wkroczą bardziej w przestrzeń energetyczną, można będzie wykonywać ataki mające na celu wstrzymania dostaw energii elektrycznej w infrastrukturze krytycznej. Kolejnym ważnym zagrożeniem może być zakłócanie działania sieci telekomunikacyjnych lub rejestrowanie i przechwytywanie informacji.

Rootkit jest zestawem narzędzi, programów pozwalających wykorzystywać kody programistyczne na ciągłą i niezauważalną obecność w komputerze. Celem głównym działania rootkitu jest utrzymać uzyskany dostęp do systemu. Spełniał on dodatkowo dwie funkcje: zdalnej kontroli i podsłuchiwania programów. Wykorzystywać zdalną kontrolę można np. do ponownego uruchamiania zainfekowanego komputera, wywoływania błędów systemowych lub uzyskiwania dostępu do wiersza poleceń. Natomiast podsłuch z wykorzystaniem rootkita pozwala na śledzenie naciśnięć klawiszy, przyglądanie pakietów sieciowych, przechwytywanie haseł, przeglądanie kluczy szyfrujących. Koncepcją działania

[15]Por. John Viega, *Mity bezpieczeństwa IT* (Gliwice: Helion, 2010).
[16] Por. Infosec Island, 'Bank of America Hit By Anonymous DDoS Attack', w *Infosec Island* <http://www.infosecisland.com/blogview/10542-Bank-of-America-Hit-By-Anonymous-DDoS-Attack.html> [dostępne: 22 Kwiecień 2012]

rootkita jest modyfikacja oprogramowania tak, by podejmowało niewłaściwe decyzje. Czasem niektóre programy tak infekują inne oprogramowanie i zmienią kody, nawet przeglądarek internetowych, są wtedy trudne do wykrycia a nazywa się je **spyware** (oprogramowaniem szpiegującym). Takie oprogramowanie czyta strony internetowe użytkownika i przesyła do przestępcy. Problem dopisywania kodu staje się groźniejszy w oprogramowaniu wolno dostępnym, gdzie kody źródłowe są dostępne dla każdego. Złośliwe modyfikacje mogą być wprowadzane w uaktualnieniach i takich programów powinny unikać organizacje powiązane z bezpieczeństwem państwa Rootkit nie jest eksploitem, natomiast może być stosowany wraz z nim. Wiąże się to z tym, że rootkity to przeważnie zestawy narzędzi i najczęściej nie wykorzystują błędów zawartych w oprogramowaniu (typu błędy przepełnienia bufora). Może on za to w sobie zawierać części korzystające z błędów w oprogramowaniu, ponieważ przeważnie rootkit wymaga dostępu do jądra systemu, przez co przeważnie zawiera jakiś program systemowy. Nie jest on również też wirusem, który samoistnie się rozpowszechnia. Różni się też tym, że nie tworzy swoich kopii i nie posiada tak jakby swojej „woli". Działa pod kontrolą atakującego, natomiast wirusy przeważnie działają według automatycznych procedur.[17]

Pozyskiwanie informacji, tworzenie dostępu do danych po przez wykorzystanie luk w zabezpieczeniach jest poważnym zagrożeniem. Przedstawiono w rozdziale programy, rozwiązania, które ukazują istnienie niebezpieczeństwa związanego z dostępem do Internetu. Oprócz programów przedstawiono model działania i myślenia przestępcy, który pozwala poznać skuteczność jego działania i ciągłego inwigilowania. Przejawia się to tym, że raz uzyskany dostęp nie jest tracony, ale ciągle wykorzystywany poprzez „tylne wejście". Niestety poza wykorzystaniem luk w zabezpieczeniach do wykradania informacji mogą one być wykorzystywane w wielu innych celach w tym i do wyrządzania szkody, która zostanie opisane w kolejnym podrozdziale.

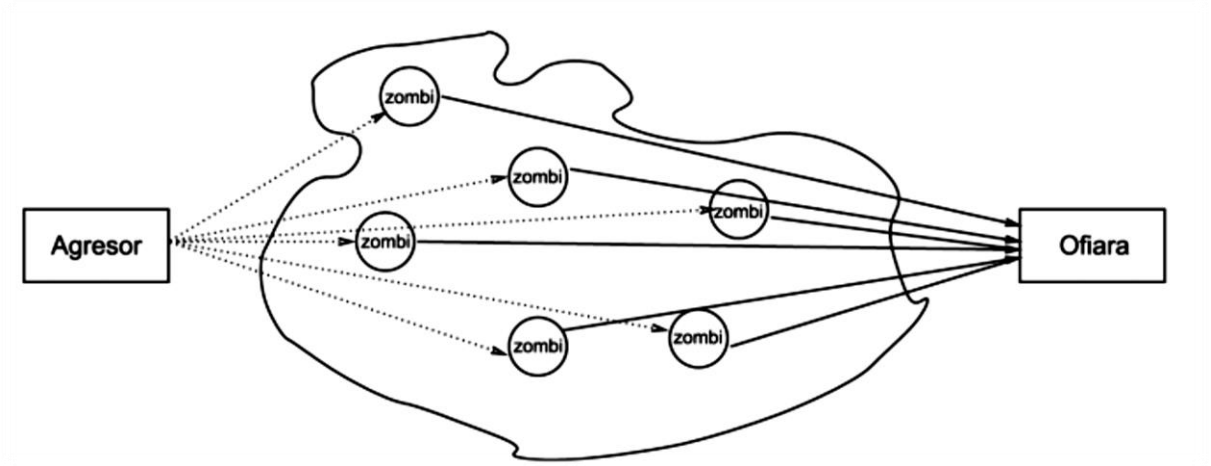
2.3. Wyrządzanie szkody

Częstym procederem występującym w sieci internetowej zamiast pozyskiwania informacji jest wyrządzanie szkody informacjom, danym lub dostępowi do informacji. Wykorzystywane są wtedy ataki komputerowe mające na celu przeważnie zablokowanie, zniszczenie lub spreparowanie ważnych danych. Takie ataki mogą być wykonywane przez firmy konkurencyjne, mające na celu opóźnić wprowadzenie produktu na rynek lub dokonaniu spekulacji na rynku pieniężnym. Innym celem takich ataków może być podważenie

[17]Greg Hoglund i Jamie Butler, *Rootkity: sabotowanie jądra systemu windows* (Gliwice: Helion, 2006).

ekskluzywności i prestiżu danej marki. Może to bardzo szybko doprowadzić do utraty klientów i wiarygodności. Społeczeństwo powierzając dane osobowe różnym firmom lub instytucjom, interesuje się jak są zabezpieczone i czy są bezpieczne. Wtedy, gdy dane zostaną wykradzione, szkodą dla tego przedsiębiorstwa, uszczerbkiem na marce będzie to zdarzenie.[18]

Atakami wykorzystywanymi przy takich celach nazywa się przewaznie **rozproszonymi atakami odmowy usług**(ang. distributed denial of service) lub **atakami odmowy usług** (ang. denial of service). Wykorzystują one przygotowane pakiety zawierające dane, które po odebraniu przez atakowany cel wywołują błędy w usługach.



Rys. 2.4 Rozproszony atak odmowy usług. Napastnik wysyła komunikat do programu głównego. Program główny rozsyła komunikaty do zombich, którzy z kolei zasypują cel swoimi pakietami

Źródło: William Chestwick, Steven Bellovin i Aviel Rubin, *Firewall-e i bezpieczeństwo w sieci. Vadamecum profesjonalisty* (Gliwice: Helion, [n.d.]).

Atak DDoS polega na wykorzystaniu moc i łączy innych komputerów (zombi) w oparciu o wcześniej zainstalowane szkodliwe oprogramowanie. Następnie agresor korzystając z programów sterujących przepuszcza atak na ofiarę, którego zadaniem jest wywołanie błędów w działających procesach. Ponadto często oprogramowanie sterujące posiada mechanizmy szyfrujące, które utrudniają odnalezienie sprawcy.

Innym szkodliwym działaniem dla firm lub instytucji państwowych jest blokowanie dostępu do informacji, blokowanie łącza do przesyłania danych. W takim momencie powstaje **blokada informacyjna** i zostaje zakłócona praca danej organizacji. Takie zdarzenie w obecnej dobie informatyzacji społeczeństwa, może zagrozić życiu społecznemu, jego

[18] Niebezpiecznik, 'Sony przeprasza za atak na PSN i wyjaśnia szczegóły', w *Niebezpiecznik* <http://niebezpiecznik.pl/post/sony-o-szczegolach-ataku-na-psn/> [dostępne: 22 Kwiecień 2012]

płynności i stabilizacji. Przykładem może być zablokowanie dostępu do płatności elektronicznych lub do systemu wypłacania pieniędzy (w przyszłości mogą to być ataki wykorzystywane w wojnach cybernetycznych), przestoje w działaniach banków niosą ze sobą wysokie koszty, a jeśli zostaną odpowiednio długo blokowane, mogą przynieść szkody zdrowotne dla społeczeństwa. Będzie to spowodowane przykładowo tym, że społeczności biedniejsze nie mają zabezpieczenia w fizyczne środki pieniężne, co skutkuje brakiem dostępu do środków pierwszej potrzeby lub środków podstawowych, niezbędnych do egzystencji (pożywienie, środki higieny itp.). Wyrządzanie szkody informacyjnej lub informatycznej jest przeważnie planowane i przygotowywane, ma określony swój cel. Pragnąc się bronić przed takimi zdarzeniami wymagane jest dostosowanie polityki bezpieczeństwa (w szczególności działu zabezpieczeń informatycznych), tak aby określały reakcje na incydenty blokady informacyjnej i usługowej. Powinna zostać przygotowana procedura reagowania i odzyskiwania stanu funkcjonowania, a następnie przetestowana przez zewnętrzną firmę audytorską. Jest to odpowiednie rozwiązanie, które pozwoli sprawdzić działanie zaplecza informatycznego bez strat spowodowanych prawdziwym atakiem.

Cyberterroryzm

Obecna globalna infrastruktura informacji dostarcza możliwości terrorystom działających na wielkich odległościach, by móc się porozumiewać głosowo (telefonicznie, satelitarnie, telefonią internetową), przesyłać pliki, pocztę elektroniczną. Internet może być również używany do rekrutacji i w rozpowszechnianiu struktur, dzięki temu technologie komunikacji stały się krytycznym majątkiem dla organizacji terrorystycznych. Dzięki globalnej sieci terroryści mogą działać na większych regionach geograficznych. Jednocześnie ta sama sieć pozwala utrzymywać dostęp informacyjny z innymi podobnymi grupami, zbierania wiedzy metodycznej i technicznej. Takie działanie również umożliwia uzupełniać zasoby ludzkie. Innym atutem Internetu jest to, że między grupami terrorystycznymi powstają przymierza. Kierując się takimi rozwiązaniami powstają nowe rodzaje podziału informacji, zasobów logistycznych i kontaktów między liderami grup. Jednocześnie grupy terrorystyczne dla bezpieczeństwa dzielą dostęp na odcinki lub ograniczając. Segmentacja pomniejsza ryzyko inwigilacji grupy.[19]

Terroryści wykorzystują sieć globalną i nie jest to wyłącznie Internet. Powoduje to, że działają jak międzynarodowa organizacja i wykorzystują wiele węzłów informacji. Można przez to stwierdzić, że grupy terrorystyczne posiadają osoby wykształcone, potrafiące

[19]Andrew Michael Colarik, *Cyber Terrorism: Political and Economic Implications* ([n.p]: Idea Group Publishing, 2006).

organizować połączenie sieciowe i zapewniają bezpieczeństwo własnej organizacji. Wymaga to natomiast traktowania tych cech i możliwości, jako kolejnych zagrożeń wpływających na bezpieczeństwo teleinformatyczne. Dodatkowo trzeba mieć na względzie, że komunikacja jest wstępem do dalszych działań. Powstaje ryzyko, że grupy terrorystyczne łącząc się i zawierając pakty, sojusze, będą szkoliły swoich informatyków do zadań wywiadowczych. Kolejnym zagrożeniem, które może wynikać z dostępu do sieci przez grupy terrorystyczne jest publikowanie materiałów z egzekucji i innych działań terrorystycznych, tworząc tym samym kolejny rodzaj terroru i oddziaływania psychologicznego na społeczeństwo.

Wnioski:

Na podstawie analizy przeprowadzonej w rozdziale drugim nasuwają się następujące wnioski:

1. Techniką przenoszącą wiele informacji z różnych źródeł w oparciu o manipulacje jest podszywanie się pod wiarygodne instytucje lub osoby.
2. W celu wykonania skutecznego ataku komputerowego wymagane jest stosowanie się do odpowiedniego schematu działania i opracowanie planu ataku.
3. Systemy komputerowe niosą ze sobą zawsze luki bezpieczeństwa, które niezabezpieczane poprzez aktualizacje mogą doprowadzić do penetracji systemu komputerowego i osadzenia złośliwego oprogramowania.
4. Przestępstwa komputerowego mogą mieć dodatkowy cel oprócz pozyskania informacji. Celem tym jest wyrządzenie szkody organizacji poprzez blokadę działania usług informatycznych.

W ten sposób pozyskano odpowiedź na drugi problem szczegółowy.

Przestępstwa komputerowe wraz z rozwojem wielu technologii stają się coraz poważniejszym i groźniejszym zagrożeniem dla bezpieczeństwa informatycznego i informacyjnego wśród żołnierzy. Podstawą funkcjonowania i korzystania z zasobów informatycznych jest odpowiednia wiedza o możliwych zagrożeniach i ich efektach działania.