

# System zabezpieczony czy system bezpieczny?

Tomasz Barbaszewski  
ABA Kraków  
e-mail: tomekb@aba.krakow.pl

**Abstrakt:** Bezpieczeństwo systemów jest prasowym tematem dnia. Że problem jest istotny, można się przekonać przeglądając chociażby stronę <http://hacking.pl/hacked>, na której są prezentowane strony www zmienione przez hackerów lub portal <http://wirusy.onet.pl>, który nieomal codziennie podaje informacje o nowych wirusach lub ich mutacjach. Z drugiej strony wydatki, które ponoszą użytkownicy systemów komputerowych na ich zabezpieczenia ciągle rosną, a skutków jakoś nie widać, albowiem wszelkie dostępne statystyki podają, że rosną także straty spowodowane włamaniami do systemów komputerowych. Gdzieś musi więc tkwić podstawowy błąd, który powoduje powstawanie efektu "błędnego koła". Przedstawiane opracowanie stanowi próbę konstruktywnego rozwiązania sygnalizowanego powyżej problemu. Opierając się na danych statystycznych dostępnych w sieci Internet zanalizowano główne zagrożenia i wyciągnięto wnioski, że ofiarami ataków (pomimo stosowania różnego typu zabezpieczeń) padają głównie systemy skomplikowane o znacznych możliwościach konfiguracyjnych, jednym słowem takie, których twórcy dołożyli wszelkich starań, aby udostępnić ich Użytkownikom jak największą liczbę usług sieciowych. Dążenie do uniwersalizacji systemów powoduje poważne osłabienie ich odporności na ewentualne ataki. Dotyczy to zarówno systemów komercyjnych, jak również rozpowszechnianych na zasadzie "Open Source" i skutkuje znacznym zwiększeniem prawdopodobieństwa wystąpienia błędów w samym oprogramowaniu, jak i przy jego konfigurowaniu. W streszczanym opracowaniu zostanie przedstawiona koncepcja budowy systemów wykazujących naturalną odporność na ataki. Wbrew głoszonym na łamach prasy codziennej i specjalistycznej opiniom realizacja takich systemów jest całkowicie możliwa i co najważniejsze nie wymaga ponoszenia wielkich nakładów finansowych. Niezbędna jest jednak zmiana mentalności i świadoma rezygnacja z wyposażania systemu w funkcje, które nie są absolutnie niezbędne dla jego poprawnego działania, a spełniają jedynie zadania pomocnicze. Na poparcie powyższej tezy zostaną przytoczone konkretne przykłady udanych ataków, których można było uniknąć stosując koncepcję "Wrodzonej Bariery Immunologicznej Systemu".

Wydatki ponoszone przez użytkowników na zabezpieczanie systemów komputerowych stale rosną. Równocześnie wzrasta jednak liczba skutecznych ataków na systemy komputerowe prowadzona zarówno w sposób bezpośredni lub poprzez dystrybucję złośliwych programów znanych pod popularną nazwą wirusów lub robaków komputerowych.

Ostatnio (tekst ten powstaje w połowie sierpnia) byliśmy świadkami "sukcesów" robaka o nazwie Code Red i jego odmian. Sporo zamieszania uczynił również inny złośliwy programik o nazwie SirCam. Więcej szczegółów znajdziecie Państwo na specjalistycznych stronach internetowych (np. [www.mks.com.pl](http://www.mks.com.pl)). Informacje o programach, których nazwy podałem powyżej znajdą się zapewne już w archiwum, albowiem mam statystyczną pewność, że pojawią się nowe, jeszcze bardziej złośliwe mutacje wirusów.

Twórcy wirusów nie znają litości i próżną także w wakacje. Serwis firmy MKS doniósł w dniu 22 sierpnia o wirusie o nazwie XPMsg, który atakuje środowisko MS Office XP. Robak ten został napisany w języku Visual Basic, i reprodukuje się wykorzystując książkę adresową poczty elektronicznej oraz niszczy wszystkie pliki (nadpisuje je własnym kodem) o rozszerzeniach htm, hta oraz html.

Jednak wirusy to nie wszystko. Coraz popularniejsze są ataki na serwery WWW. "Żli chłopcy" upodobili sobie szczególnie firmę TP S.A. Tylko w pierwszej połowie sierpnia "padły" trzy serwery regionalne tej firmy - Gdańsk, Gdynia oraz Radom. Wyniki można obejrzeć na [www.hacking.pl/hacked](http://www.hacking.pl/hacked).

To jednak tylko wierzchołek góry lodowej. Oprócz spektakularnych i szeroko opisywanych skutków działania wirusów oraz zmian treści stron WWW mamy do czynienia z coraz większą liczbą "ciemnych ataków", których autorzy nie szukają rozgłosu. Są to (niestety często skuteczne) ataki na systemy bankowości internetowej, systemy autoryzacji kart kredytowych itp.

Ataki na systemy komputerowe są również dokonywane w celu zdobycia istotnych i możliwych do wykorzystania informacji. Instytucjonalny podsłuch sieci związany z projektem Echelon zwrócił uwagę wielu osób na potencjalne źródło dobrego zysku, jakim może być sprzedaż informacji zdobytych w wyniku ataków na systemy komputerowe. Ataki te są zazwyczaj trudne do wykrycia, ponieważ z samej zasady nie są atakami destrukcyjnymi. Uzyskana informacja jest oferowana różnym osobom - od dziennikarzy począwszy na firmach konkurencyjnych skończywszy. Docelowy rynek zależy oczywiście od charakteru zdobytej informacji.

Prowadząc od kilku lat badania bezpieczeństwa (audyty) systemów sieciowych i komputerowych największych firm w Polsce mogę z całą odpowiedzialnością stwierdzić, że bezpieczeństwo ich systemów komputerowych pozostawia co najmniej bardzo wiele do życzenia. Jest to w wielu przypadkach wynikiem bezgranicznej wiary użytkowników i administratorów w rozwiązania oferowane im przez wielkie firmy. Tymczasem nawet oprogramowanie przeznaczone do nadzoru i sprawdzania bezpieczeństwa sieci kosztujące kilkaset tysięcy dolarów nie jest wolne od błędów, które niekiedy wzbudzają wesołość wśród specjalistów. Na przykład jeden z szeroko reklamowanych (i bardzo drogich!) programów do badania bezpieczeństwa sieci "wykrył" w trakcie jednego z naszych audytów wirusa oprogramowania MS Office rezydującego rzekomo na routerze CISCO serii 2500 co wzbudziło salwę śmiechu zespołu audytorskiego.

Z oczywistych względów nie ujawniam zarówno nazw audytowanych Instytucji jak programów, zaś zdobyte (głównie w trakcie pisania raportów "Executive Summary") doświadczenia skłoniły mnie do podzielenia się z Państwem kilkoma ogólnymi spostrzeżeniami dotyczącymi bezpieczeństwa systemów komputerowych i sieciowych.

### **Po pierwsze - skuteczne zabezpieczenie wielu systemów jest w praktyce niemożliwe**

Pracujące w Polsce systemy komputerowe są w niemal 100% oparte o sieci komputerów PC z systemem operacyjnym MS WINDOWS. Sieć taka jest szczególnie trudna, a w przypadku, gdy nie stosujemy wyłącznie WINDOWS NT (lub 2000) w praktyce niemożliwa do skutecznego zabezpieczenia, a co najgorsze w przypadku standardowej konfiguracji stanowi wręcz idealne środowisko do powielania wirusów. Wystarczy się przyjrzeć chociażby typowej konfiguracji systemu poczty elektronicznej w takiej sieci.

*Do obsługi poczty elektronicznej służy serwer z odpowiednim oprogramowaniem realizujący funkcję Post Office Protocol (POP). Niezależnie od wersji wykorzystywanego oprogramowania oraz systemu operacyjnego serwera pocztowego jego funkcja polega na wysyłaniu poczty otrzymanej od użytkowników oraz na wydawaniu "na życzenie" poczty dla nich przeznaczonej.*

*Zasadą pracy systemu jest dostarczanie poczty na dyski komputerów Użytkowników, a więc cała docierająca do firmy poczta "ląduje" w końcu na stacjach roboczych, gdzie też jest otwierana.*

*Trudno znaleźć środowisko bardziej przyjazne dla wirusa przesyłanego w poczcie elektronicznej! Wraz z przesyłkami pocztowymi jest on kierowany wprost na dysk zazwyczaj słabo zabezpieczonej stacji roboczej, którą obsługuje na ogół osoba znająca jedynie podstawy pracy z komputerem (co nie oznacza bynajmniej małej sprawności w tworzeniu np. arkuszy kalkulacyjnych lub profesjonalnych dokumentów). Gdy zaś wirus znajdzie się już na stacji roboczej to "hulaj dusza!" Może łatwo "zarazić" inne komputery w sieci lokalnej, sprawdzić pliki z adresami poczty elektronicznej Użytkownika (np. programu Outlook Express) i rozpocząć wysyłanie swego kodu do następnych ofiar. W taki sposób rozpowszechnił się na przykład robak o nazwie SirCam. Jeśli do dnia 16 października nie usuniemy tego robaka z naszego komputera (a może on się na nim*

znajdować w stanie uśpienia, albowiem uruchamia się jedynie 8000 razy) to z prawdopodobieństwem 1/20 stracimy całą zawartość dysku C:

*Ktoś może stwierdzić, że są przecież programy antywirusowe, które mają zapobiec podobnym przypadkom. Ano są, ale jednak SirCam zaatakował skutecznie setki tysięcy komputerów na Świecie. Dlaczego tak się stało? Przyczyna jest bardzo prosta. Oprócz bardzo prymitywnych mutacji już znanych wirusów program antywirusowy może wykryć jedynie coś, co już zna. Nowy rodzaj wirusa może zatrzymać jedynie nowa "szczepionka", która z natury rzeczy może powstać dopiero "post factum". Jeśli wirus jest w stanie rozpowszechniać się odpowiednio szybko, to nim powstanie nowe zabezpieczenie ilość zainfekowanych komputerów idzie już w setki tysięcy, a nawet w miliony.*

*Co gorsza, wirus SirCam spełnił przepowiednię Jamesa Woolsey'a, byłego szefa CIA, że wkrótce powstaną wirusy, których zadaniem będzie rozsyłanie po Świecie poufnych lub tajnych wiadomości (szczegóły [www.ipsec.pl](http://www.ipsec.pl)). SirCam dotknął zarówno FBI, jak i urzędy na Ukrainie rozsyłając po Świecie pliki, które powinny pozostać poufne! Nie wierzę, aby FBI nie posiadało lub nie aktualizowało systemów antywirusowych!*

Powyższy przykład jest typowy, a więc warto poświęcić mu nieco uwagi. Dlaczego taki robak jak SirCam mógł tak łatwo się rozmnażać?

Nie mogę się ustrzec od porównania "biologicznego", które zresztą narzuca sama nazwa "wirus" lub "robak". Otóż stonka ziemniaczana znalazła warunki do rozmnażania się na szeroką skalę w wyniku wprowadzenia wielkich plantacji ziemniaków, w których krzaczek rośnie obok krzaczka na kilku, a czasem kilkudziesięciu hektarach. Pożywienie jest ogólnie dostępne zaś przemieszczanie się z krzaczka na krzaczek bardzo proste i praktycznie nie związane z ryzykiem.

Podobne warunki znajduje wirus w lokalnej sieci komputerowej dużej organizacji lub przedsiębiorstwa. Gdy już uda mu się dostać do sieci lokalnej, co może nastąpić na wiele różnych sposobów, z których jednym, często w ogóle nie zauważanym jest komputer notebook (niekiedy samego Szefa), to rozmnażanie się nie przedstawia większych problemów. O ile stało się już regułą sprawdzanie poczty przychodzącej (co jednak w przypadku nowych wirusów jest nieskuteczne) o tyle bardzo mało firm sprawdza pocztę wychodzącą. Tak więc łatwo można stać się źródłem zakażenia dla innych.

### **Co z tym można zrobić?**

Można oczywiście stosować coraz narastające restrykcje za pomocą Polityki Bezpieczeństwa, można wydać majątek na programy antywirusowe i można w końcu odłączyć sieć od Internetu (ale co notebookami, które są wykorzystywane na zewnątrz firmy, a potem podłączane do sieci LAN?).

Wszystkie powyższe i im podobne działania są usuwaniem skutków, a nie przyczyny, która leży w wadliwej koncepcji obsługi poczty elektronicznej! Najprostszym i co najważniejsze skutecznym sposobem zatrucia wirusom życia jest po prostu rezygnacja z dostarczania plików poczty elektronicznej na komputery PC w sieciach lokalnych. Likwiduje się w ten sposób środowisko sprzyjające propagowaniu się wirusów poprzez zarażanie kolejnych komputerów, na które dostarczana jest poczta elektroniczna.

Czy taka konfiguracja systemu jest możliwa? Oczywiście, i to bez konieczności rezygnacji ze standardowego środowiska MS Office. Poczta można przeglądać na serwerze, który może być znacznie lepiej zabezpieczony od stacji roboczych. Ponieważ użytkownicy serwera, niezależnie od wykorzystywanego systemu operacyjnego posiadają ograniczone uprawnienia systemowe (nie mogą zapisywać dowolnych plików lub wykonywać dowolnych programów). Uszkodzenia, których może dokonać wirus są więc ograniczone i przy prawidłowej konfiguracji mało prawdopodobne.

Skuteczne zabezpieczenie jednego lub kilku serwerów w korporacji jest oczywiście o wiele łatwiejsze niż skuteczne zabezpieczenie kilkudziesięciu lub kilkuset komputerów PC.

### **Serwery uniwersalne czy specjalizowane?**

Producenci oprogramowania systemowego starają się obecnie udostępnić jak najwięcej funkcji serwera. Niezależnie od tego, czy jest to WINDOWS 2000, system rodziny UNIX (np. SUN Solaris, HP/UX, SCO - obecnie CALDERA) czy też LINUX mamy do dyspozycji szereg funkcji sieciowych systemu - serwera plikowego, serwera WWW, poczty elektronicznej, DHCP, drukarek, DNS, usług terminalowych, baz danych itp. Jest to głównie spowodowane względami marketingowymi - wiele razy byli zapewne Państwo obecni na prezentacjach, na których podkreślano uniwersalność oferowanego systemu. Niezależnie od osobistych sympatii musimy stwierdzić, że prym wiodą tu dostawcy tak zwanych dystrybucji systemu LINUX.

W efekcie administrator systemu musi zabezpieczyć skutecznie system o ogromnej funkcjonalności, co oczywiście wiąże się z koniecznością usuwania zbędnych funkcji. Operacja ta nosi czasem nazwę "utwardzania" (hardening) systemu operacyjnego.

Poprawne przeprowadzenie takiej procedury nie jest proste. Konieczna jest dokładna znajomość samego systemu, powiązań bibliotek i odwołań oraz duża doza wyobraźni, albowiem wielokrotnie okazuje się, że pozostawiona usługa staje się bramą umożliwiającą atak na system.

Tymczasem oczywiste jest, że skuteczne zabezpieczenie urządzenia, którego funkcjonalność została świadomie ograniczona jest znacznie prostsze niż urządzenia uniwersalnego. Jeśli zdecydujemy się na przykład na zastosowanie odrębnego komputera do obsługi poczty elektronicznej nie ma żadnej potrzeby uruchamiania na nim usług niezwiązanych z realizacją obsługi E-mail. W oczywisty sposób ułatwia to administrację systemu, zapewnia o wiele większe bezpieczeństwo oraz ogranicza skutki ewentualnego ataku lub awarii.

Ceny sprzętu (zwłaszcza PC) są obecnie tak niskie, że markowy komputer PC można już kupić za ok. 2000 zł netto, zaś możliwości konfiguracji oprogramowania typu OpenSource umożliwiają budowanie specjalizowanych serwerów realizujących nieomal dowolne funkcje w sieci. Powyższa filozofia znajduje swe odzwierciedlenie w strategii wielu firm, takich jak SUN, INTEL, COMPAQ itp., oferujących tak zwane "Network Appliances". Wiele z tych urządzeń jest przeznaczonych do pracy w zestawach 19", a więc otrzymujemy w wyniku zestaw specjalizowanych serwerów, który nie zajmuje wiele miejsca, jest prosty w administracji i może zapewnić znacznie większy poziom bezpieczeństwa niż pojedynczy serwer realizujący wiele funkcji.

Wykorzystywanie specjalizowanych serwerów umożliwia również bardziej bezpieczną konfigurację sieci poprzez wykorzystywanie sieci nierutowalnych oraz serwerów typu PROXY.

Urządzenia typu "Network Appliances" mogą być realizowane w oparciu o dowolny system operacyjny. Zazwyczaj są one wyposażane w przyjazne interfejsy administratora ułatwiające i przyspieszające ich konfigurowanie. Dostępne są urządzenia o różnych stopniach specjalizacji - od systemów, na których zainstalowano wiele funkcji przeznaczonych do skonfigurowania przez administratora (mikroserwery Cobalt) do urządzeń realizujących jedynie wybraną funkcję (Bezpieczny serwer WWW firmy ABA).

Bezpieczne urządzenia typu "Network Appliances" charakteryzują się przede wszystkim tym, że ich system operacyjny jest budowany z wybranych modułów i mieści się zazwyczaj na nośniku o pojemności kilku megabajtów. Producenci często wykorzystują jako nośnik systemu pamięć typu FLASH. Specjalnie przygotowany system jest wyposażony jedynie w funkcje niezbędne do realizacji zadań, do których został zbudowany, zaś pozbawiony wszelkich zbędnych usług i protokołów. Zmniejsza to bardzo znacznie prawdopodobieństwo skutecznego ataku na system.

Urządzenia typu "Network Appliances" są na ogół bardzo proste w administracji i przeznaczone do ciągłej pracy bez dozoru, a więc ich obsługa administracyjna może być zlecana podmiotom zewnętrznym (outsourcing).

*Przykład:*

*W miesiącach wakacyjnych sporo zamieszania czyni robak o nazwie CodeRed. Jego kolejne mutacje (CodeRed I, II, a ostatnio III) sięgają spustoszenia w serwisach WWW wykorzystujących oprogramowanie Microsoft ISS. O ile początkowe wersje ograniczały się jedynie do blokowania usług (Denial of Service), o tyle późniejsze wersje robaka umożliwiają przejęcie kontroli nad maszyną. Pomimo, że od dawna dostępna jest poprawka (na stronach firmy Microsoft) uniemożliwiająca działanie tego robaka rozprzestrzenia się on nadal i straty spowodowane jego działaniem szacuje się już na ponad miliard dolarów!*

Powyższy przykład daje sporo do myślenia. CodeRed zaatakował skutecznie największe korporacje, które zapewne posiadały szczegółowo opracowane dokumenty Polityki Bezpieczeństwa. Nie chce mi się wierzyć, aby nie było w nich zalecenia regularnego sprawdzania błędów i instalacji poprawek w eksploatowanych systemach. A jednak...

Posiadanie Polityki Bezpieczeństwa to jedno, a jej przestrzeganie to drugie, a z tym jak widać na całym Świecie nie jest najlepiej i nie należy się spodziewać, aby Polska była chlubnym wyjątkiem. Jedynym praktycznie skutecznym rozwiązaniem jest taka budowa systemu, aby prawdopodobieństwo pojawienia się w nim błędu było jak najmniejsze. Jest to realne jedynie w bardzo prostych, specjalizowanych systemach. Teoria niezawodności ma pełne zastosowanie także w inżynierii oprogramowania!

Stąd też wynika rosnąca popularność "Internet Appliances", których specjalizowane systemy operacyjne są trudne do zaatakowania.

### **Zdalna administracja - wygoda czy pułapka?**

Centralizacja działów informatyki, którą można zaobserwować w wielu Instytucjach i Przedsiębiorstwach spowodowała bardzo znaczne zainteresowanie możliwościami zdalnej administracji systemami komputerowymi. Jest to oczywiście bardzo wygodne, jednakże wprowadzenie systemu zdalnej administracji wiąże się zawsze ze wzrostem ryzyka dla bezpieczeństwa sieci, jeśli bowiem administrator może wpływać zdalnie na konfigurację i sposób pracy urządzenia, to może to zrobić także atakujący, któremu uda się przełamać system zabezpieczeń.

Konfigurując system zdalnego zarządzania należy zawsze o tym pamiętać i najlepszym rozwiązaniem jest unikanie konieczności zdalnego administrowania jakimikolwiek urządzeniami sieciowymi. Ryzyko przejęcia kontroli nad urządzeniem jest w przypadku stosowania zdalnej administracji znaczne i niekoniernie wymaga znacznej wiedzy specjalistycznej. Najczęstszą metodą wykorzystywaną do przejęcia kontroli administracyjnej nad siecią jest wykorzystywanie ludzkiej gadatliwości połączonej z nieświadomością (social engineering).

Szczególne niebezpieczne jest zdalne dokonywanie uaktualnień oprogramowania, zawsze bowiem istnieje możliwość, że "uaktualnienia" może dokonać atakujący wprowadzając do oprogramowania "konia trojańskiego", którego działanie umożliwi mu dalszą penetrację naszej sieci. Wbrew pozorom nie jest to wcale bardzo trudne - krótki programik przechwytyjący kody klawiszy naciskanych na klawiaturze i przesyłający je na określony adres sieciowy może spowodować, że pozornie niewinna końcówka sieciowa może się okazać urządzeniem przekazującym atakującemu hasła jej użytkowników.

Powyższy przykład jest bardzo prosty, lecz możliwe są oczywiście znacznie bardziej wyrafinowane metody.

Jeśli zamierzamy wykorzystać mechanizmy zdalnej administracji, powinniśmy się przede wszystkim zastanowić, czy jest to niezbędne konieczne, i czy nie możemy sobie poradzić inaczej. Zasadą powinno być takie konfigurowanie systemu, aby administracja była ograniczona do minimum! Pamiętajmy o prawie Murhy'ego - "Jeśli coś można zrobić, to zawsze znajdzie się ktoś, kto to zrobi!". Tak więc jeśli Administrator może zmieniać zdalnie konfigurację jakiegokolwiek urządzenia, to należy przyjąć, że może zrobić to także ktoś inny.

### **System z "barierą immunologiczną"**

Sprawnie działający organizm biologiczny potrafi się sam obronić przed wieloma infekcjami i nie jest konieczne podawanie mu lekarstw. W podobny sposób powinniśmy potraktować nasze systemy komputerowe. Wymaga to starannego przemyślenia konfiguracji całego systemu, albowiem nawet stosowanie rozwiązań, które charakteryzują się z zasady podwyższonym poziomem bezpieczeństwa nie stanowi żadnej gwarancji. Błędna konfiguracja systemu może obniżyć poziom bezpieczeństwa do niedopuszczalnych granic.

*W jednej z instalacji opartych o komputery sieciowe zastosowano dość dziwny mechanizm udostępniania użytkownikom ważnej aplikacji poprzez NFS. Tak więc system plikowy każdej końcówki posiadał dostęp do katalogów z kodem i danymi aplikacji. Co więcej, ponieważ końcówek było dużo nie zastosowano żadnej kontroli w pliku /etc/exports udostępniając aplikację wszystkim użytkownikom sieci!*

Teoretycznie spełniono wszelkie założenia bezpieczeństwa, ale zniweczyła to niepoprawna konfiguracja systemu.

Jakie więc działania należy podjąć, aby zbudować system bezpieczny?

1. Starannie przemyśleć konfigurację systemu.
2. Nie wykorzystywać zbyt wielu protokołów i usług sieciowych jednocześnie.
3. Wprowadzać w miarę możliwości serwery aplikacji oraz "Internet Appliances".
4. Ściśle określić funkcję poszczególnych serwerów.
5. Ograniczyć w miarę możliwości liczbę komputerów PC na stanowiskach pracy, a w ich miejsce zastosować terminale (współczesne terminale pracują sprawnie ze wszystkimi systemami w trybie graficznym z WINDOWS 2000 włącznie!).
6. Ograniczyć do niezbędnego minimum zdalną administrację urządzeniami sieciowymi, końcówkami i serwerami, a jeżeli już jest ona konieczna bezwzględnie stosować silne mechanizmy kryptograficzne (szyfrowanie transmisji, podpisy cyfrowe itp.).
7. Nie udostępniać bez potrzeby żadnych zasobów, a zwłaszcza zdalnych dysków.
8. Poczcie elektroniczną wykorzystywać w trybie terminalowym.
9. Konfiguracja przeglądarek internetowych powinna być wykonana przez Administratora i zabezpieczona przez zmiany przez Użytkowników systemu.
10. Przeprowadzić kompetentny audyt systemu nie tylko przy użyciu narzędzi automatycznych, ale przez kompetentny zespół specjalistów.

Jeśli nie będziemy przestrzegać powyższych reguł, to pomimo znacznych wydatków na oprogramowanie i urządzenia zabezpieczające system może stać się łatwo celem skutecznego ataku oraz źródłem ataków na inne systemy dostępne w sieci.