mgr inż. Dariusz Wojdas
http://www.wojdas.24x7.pl

TECHNIKI ZAGRAŻAJĄCE SIECIOM KOMPUTEROWYM
(hacking, cracking and viruses)

Praca dyplomowa

Studia Podyplomowe
Politechnika Śląska – Instytut Informatyki

Gliwice 2004

Spis treści

1. Wprowadzenie

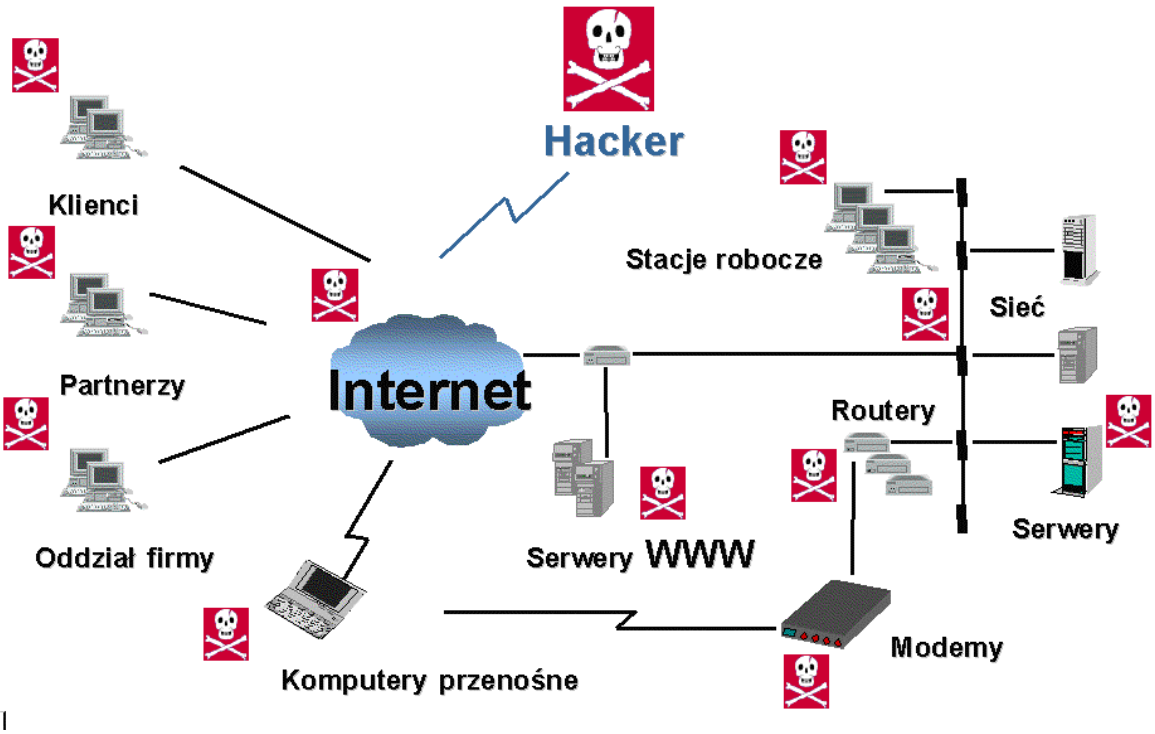
Do najpopularniejszych zjawisk bezpośrednio zagrażającym systemom komputerowym można zaliczyć wirusy, ataki oraz awarie sprzętu i oprogramowania.

Awarie to zdarzenia występujące losowo na które nie mamy wpływu ale możemy minimalizować zarówno prawdopodobieństwo jak i skutki wystąpienia ich poprzez balansowanie obciążeń, dublowanie poszczególnych elementów naszej sieci oraz odpowiednie tworzenie i przechowywanie kopii zapasowych naszych danych.

Wirusy komputerowe występują w różnych odmianach ale generalnie możemy przyjąć że jest to szkodliwy program mający zdolności samo powielania się po uruchomieniu go na danym komputerze który staję się wtedy zarówno ofiarą jak i nosicielem. Wirusy ogólnie możemy podzielić na ***destrukcyjne*** (które powodują całkowite lub częściowe zniszczenie danych, programów jak i systemu operacyjnego na zaatakowanym komputerze) oraz ***nie destrukcyjne*** (które zazwyczaj powodują generowanie dużego ruchu w sieci lub do sieci co skutkuje znacznym spowolnieniem sieci lub jej całkowitym zablokowaniem).

Ataki na sieci komputerowe są zjawiskiem które pojawiło się tuż po uruchomieniu pierwszych sieci komputerowych. W tych czasach zabezpieczenia były albo bardzo prymitywne albo w ogóle ich nie było. Jednakże problem ataków na sieci komputerowe dotyczy również czasów obecnych. Pomimo to że obecnie stosowane technologie zabezpieczeń są dużo bardziej doskonałe to istnieją nadal możliwości włamań nawet do najnowocześniejszych systemów sieciowych. Ataki są świadomym działaniem - nie ma przypadkowego ataku składającego się z kilku elementów. Włamanie można zdefiniować jako nieautoryzowany dostęp do zasobów sieci.

Co może być celem ataku ?



Celem ataku może być każde urządzenie (router, switch, firewall, IDS, modem, access point, PBX), każdy system operacyjny, każda usługa sieci (pliki, bazy danych, WWW, poczta), każdy serwer jak i każda stacja robocza oraz systemy zarządzania siecią.

Możemy wyróżnić dwa główne nurty ataków.

Pierwszy to ataki na system operacyjny pojedynczego komputera pozwalające uzyskać dostęp do zasobów w nim zgromadzonych. Na tego rodzaju ataki podatne są sieci w których jest stosowany model ochrony poszczególnych komputerów. Model ten jest najszerzej stosowany i przede wszystkim trudno skalowalny. Związane jest to z tym że występują różne systemy operacyjne a także ich wersje są zróżnicowane pod względem zaimplementowanych mechanizmów bezpieczeństwa. Administrowanie bezpieczeństwem w takiej sieci jest trudne i mało efektywne dlatego model ten nie nadaje się dla dużych systemów.

Drugi to ataki na system operacyjny sieci w celu uzyskania pełnego dostępu do wszystkich zasobów zgromadzonych w całej sieci. Na tego rodzaju ataki narażone są duże systemy sieciowe oparte o model ochrony w skali całego systemu. Mechanizmy bezpieczeństwa w tym modelu polegają na kontrolowaniu dostępu do wszystkich komputerów i usług. Narzędziami stosowanymi w takim modelu są usługi katalogowe połączone z filtrowaniem, kontrolowaniem i szyfrowaniem ruchu w poszczególnych warstwach modelu OSI/DoD

Całość włamań można podzielić na trzy grupy.

Pierwszą z nich stanowią ***penetracje systemów*** – jest to nieautoryzowany dostęp do zasobów sieci w celu pozyskania (kradzieży) informacji lub własności intelektualnej. Ten rodzaj włamań nie niszczy ani nie zmienia danych do których uzyskał dostęp włamywacz.

Drugim rodzajem włamań są ***włamania destrukcyjne*** – polegają one na zniszczeniu całości lub części informacji zawartych na zaatakowanym systemie lub ich celowej zmianie lub zamianie.

Trzecim rodzajem włamań są ***włamania w celu wykorzystania zaatakowanego systemu*** do przeprowadzenia pewnych operacji. Do operacji tych możemy zaliczyć uzyskanie dostępu z zaatakowanego systemu do innego systemu który współpracuje z zaatakowanym systemem lub też uruchamia na zaatakowanym systemie pewne procesy wpływające destrukcyjnie na zaatakowany system lub inne wybrane systemy.

Ze względu na miejsce uzyskania dostępu do atakowanej sieci, włamania możemy podzielić na dwie podgrupy.

Do pierwszej należą włamania realizowane „frontowymi drzwiami" . Jest to dostęp realizowany przez główny styk sieci wewnętrznej z przestrzenią ogólnodostępną (np. Internet-em). Agresor zazwyczaj wykrywa słabe punkty zabezpieczenia tego styku i uzyskuje dostęp do wnętrza sieci lub powoduje wyłączenie pewnych mechanizmów bezpieczeństwa styku. Większość włamań jest prowadzona w ten sposób.

Do drugiej należą włamania realizowane „tylnymi drzwiami" . Dostęp do atakowanej sieci w tej metodzie jest uzyskiwany przez omijanie głównego punktu styku sieci wewnętrznej z przestrzenią ogólnodostępną. W metodzie tej wykorzystywane są albo urządzenia sieci mające dostęp do sieci ogólnodostępnych (np. modemy, Access Point-y) będące składnikami sieci albo urządzenia takie zostają podstawione przez agresora. Metodę stosuje się wtedy gdy główny styk jest bardzo dobrze chroniony.

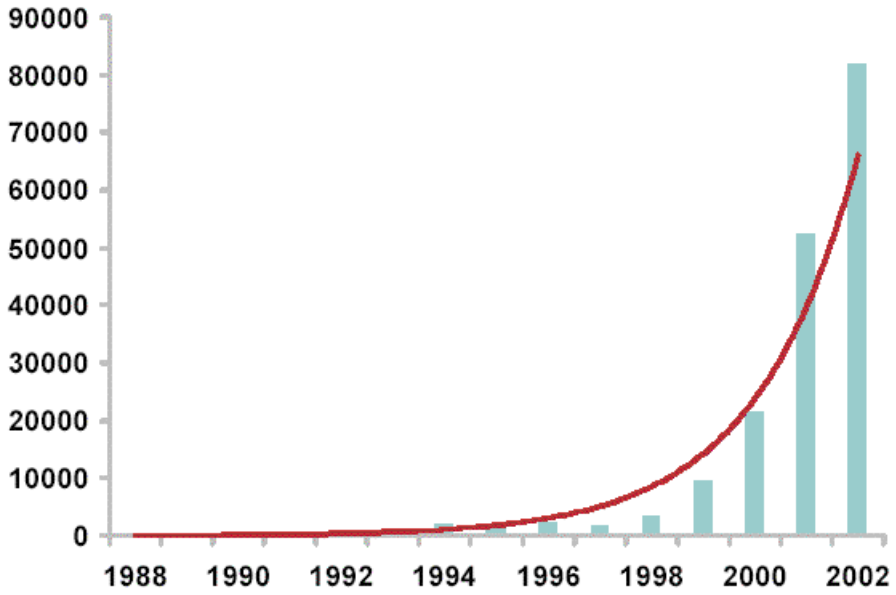
Koszty i ilość odnotowanych przestępstw komputerowych w USA

Typ przestępstwa	2001	2002
Kradzież tajemnic firmy	$151.2	$170.8
Przekłamania finansowe	$92.9	$115.7
Atak na siec od wewnątrz	$45.3	$49.9
Sabotaż	$5.2	$15.1
Nieautoryzowany dostęp od wewnątrz	$6.1	$4.5
Kradzież laptopów	$8.8	$11.7
Denial of Service	$4.3	$18.4
Penetracja systemów od zewnątrz	$19.0	$13.0
RAZEM	**$378M**	**$456M**

Źródło: FBI 2002 Report on Computer Crime

CERT—Ilość odnotowanych ataków (*)

http://www.cert.org/stats/cert_stats.html#incidents



(*) Jeden atak może dotyczyć jednej, setek a nawet tysięcy lokalizacji; ponadto część ataków ma/miała wpływ na działania organizacji w długim okresie czasu

2. Podstawowe wymogi bezpieczeństwa :

Do podstawowych wymogów bezpieczeństwa możemy zaliczyć:

- istniejąca i dobrze zdefiniowaną politykę bezpieczeństwa
- skuteczne mechanizmy wymuszające realizację polityki bezpieczeństwa
- identyfikację i opis obiektów z uwzględnieniem poziomu ochrony i praw dostępu
- audyt w celu umożliwienia wykonania dokładnej analizy ewentualnych zagrożeń
- pewność sprzętowych i/lub programowych mechanizmów zabezpieczeń
- ciągła ochrona mająca na celu utrzymanie odpowiedniego poziomu ochrony

Polityka bezpieczeństwa jest formalnym i spisanym określeniem reguł, do których muszą się zastosować osoby otrzymujące dostęp do technologii i zasobów informacyjnych organizacji. Definiuje ona sposoby wykorzystania kont użytkowników i danych przetwarzanych w systemie. Określaniem polityki bezpieczeństwa zajmują się zarządy firm lub organizacji w ścisłej współpracy a administratorami bezpieczeństwa. Określenie strategii realizacji polityki bezpieczeństwa należy do wyżej wymienionych administratorów, natomiast zadania opracowania i realizacji taktyk współdzielą administratorzy poszczególnych elementów sieci i użytkownicy końcowi.

Zrozumienie i zaakceptowanie polityki bezpieczeństwa jest niezbędne przed rozpoczęciem wdrożenia jakiegokolwiek rozwiązania.

Projektując politykę bezpieczeństwa należy uwzględnić koszty jakie zostaną poniesione na jej realizację oraz jej wpływ na funkcjonalność sieci komputerowej.
Ponadto należy ją ciągle dostosowywać do zmieniających się potrzeb firmy lub instytucji. Polityka bezpieczeństwa musi być racjonalna i klarowna tak aby mogła być zrozumiana i realizowana zarówno przez administratorów jak i użytkowników. Wszyscy pracownicy muszą podlegać obowiązkowi zaznajomienia się z polityką bezpieczeństwa.

Co powinna zawierać spisana polityka bezpieczeństwa ?

- informacje o organie wprowadzającym politykę bezpieczeństwa i jej zakres
- politykę dotyczącą "normalnej" eksploatacji sieci/zasobów
- politykę dotyczącą identyfikacji i uwierzytelnienia
- politykę dotyczącą zasad korzystania z zasobów zewnętrznych, np. Internetu
- politykę dotyczącą dostępu do sieci kampusowej, korporacyjnej i przemysłowej
- politykę dotyczącą zdalnego dostępu do sieci
- politykę dotyczącą reagowania na ataki/incydenty

Aby polityka bezpieczeństwa była realizowana w założony sposób musimy posiadać skuteczne mechanizmy wymuszające jej realizację.
Dla każdego obiektu obecnego w systemie musi być określony poziom ochrony poprzez zakwalifikowanie go do odpowiedniej grupy, określonej poprzez kryteria bezpieczeństwa oraz muszą być określone jego prawa do innych obiektów i ich własności. Obiekty muszą być tak nazywane aby była możliwość szybkiej identyfikacji.
W celu obserwacji określonych przez nas działań dla wybranych użytkowników musimy rejestrować, gromadzić i przetwarzać dane z audytu i na ich podstawie dokonywać analizy ewentualnych zagrożeń.

Każdy system komputerowy na którym chcemy wymusić określone wymogi bezpieczeństwa musi zawierać sprzętowe i/lub programowe mechanizmy zabezpieczeń, które możemy w sposób niezależny ocenić pod względem spełniania wyżej wymienionych wymogów.

Mechanizmy zwiększające bezpieczeństwo muszą być specjalnie chronione przed nieautoryzowanym dostępem zarówno z zewnątrz jak i wewnątrz systemu informatycznego. Należ też ciągle monitorować wszystkie mechanizmy bezpieczeństwa a szczególnie ich wyłączenia i zmiany konfiguracji.

3. *Strategie realizacji polityki bezpieczeństwa :*

Do najważniejszych strategii służących realizacji polityki bezpieczeństwa należy zaliczyć:

- zapewnianie bezpieczeństwa dzięki wielowarstwowemu mechanizmowi ochrony
- różnicowanie typów mechanizmów ochrony
- hierarchizacja uprawnień użytkowników systemu
- wydzielanie i monitorowanie punktów wymiany informacji systemu z otoczeniem
- blokowanie systemu w przypadku wykrycia włamania
- analiza sytuacji, zatrzymanie pracy całego lub części systemu, poinformowanie użytkowników
- konieczność wcześniejszego opracowania planu działania w przypadku awarii

Podstawową rzeczą w strategii bezpieczeństwa jest stosowanie wielowarstwowego mechanizmu ochrony. Polega to na tym że nie wystarczy ominąć jedno zabezpieczenie aby uzyskać nieautoryzowany dostęp. Pierwszą warstwą w wielowarstwowym mechanizmie ochrony powinna stanowić ochrona fizyczna urządzeń jak i kontrolowany dostęp do pomieszczeń w których się znajdują. Kolejną warstwą może być procedura uwierzytelniania użytkownika rozpoczynającego pracę na wyznaczonym dla niego sprzęcie i/lub w sieci komputerowej. Kolejnym poziomem bezpieczeństwa jest autoryzacja w bazach danych lub w programach korzystających z baz danych. Czy bardziej ważne dane tym więcej warstw modelu ochrony.

Dobrym dodatkiem do wielowarstwowego mechanizmu ochrony jest stosowanie produktów zwiększających bezpieczeństwo pochodzących od różnych producentów ponieważ poznanie słabego punktu danego zabezpieczenia nie ma krytycznego znaczenia dla całego systemu zabezpieczeń. Należy pamiętać że administrowanie wielowarstwowymi i zróżnicowanymi mechanizmami bezpieczeństwa jest o wiele bardziej skomplikowane i pracochłonne niż monolitem dostarczanym przez jednego producenta.

W każdym systemie informatycznym musi być hierarchizacja uprawnień użytkowników systemu. Najlepiej stosować się do zasady nadawania tylko uprawnień które są potrzebne, dzięki temu na niebezpieczeństwo lub błędy w zarządzaniu narażone są tylko określone fragmenty systemu.

Wszystkie punkty styku naszej sieci z sieciami potencjalnie uznawanymi za niebezpieczne (nie zarządzane przez nas) powinny być pod szczególnym nadzorem oraz dodatkowymi zabezpieczeniami. Punkty wymiany informacji z sieciami zewnętrznymi powinny być monitorowane na poziomie treści jakie są odbierane jak i wysyłane z naszej sieci.

Każdy dobry system zabezpieczeń powinien w porę wykrywać zagrożenia i im przeciwdziałać, uniemożliwiając napastnikowi wyrządzenie szkód lub odfiltrowywać informacje lub programy które nie powinny dostać się lub wydostać z naszego systemu informatycznego. Oprócz tego powinien też zarejestrować wszystkie działania które doprowadziły do sytuacji zagrożenia w tym informacji o intruzie oraz poinformować o tym fakcie wszystkie określone osoby.

Ważną sprawą jest przygotowanie planu działania w przypadku naruszenia bezpieczeństwa systemu lub w przypadku awarii który uwzględnia informowanie zarówno administratorów jak i użytkowników o zaistniałych sytuacjach.

4. Rodzaje zagrożeń dla poszczególnych obszarów :

1. Zagrożenia sprzętu :

- kradzież
- dobieranie się (rekonesans, nielegalne przeróbki, użycie niezgodne z przeznaczeniem)
- zniszczenie
- uszkodzenie
- nieuprawnione korzystanie

2. Zagrożenia oprogramowania :

- usuniecie
- kradzież
- błędy

3. Zagrożenia informacji :

- usunięcie
- kradzież
- modyfikacja

4. Zagrożenia operacji sieci :

- przerwania
- interferencje
- przeładowanie
- włamania

5. Poziomy bezpieczeństwa :

Poziom 1 - Fizyczna ochrona sprzętu, nośników i dokumentacji

- inteligentne budynki (kontrolowany i monitorowany dostęp do pomieszczeń, systemy alarmowe)
- punkty dystrybucyjne muszą posiadać dodatkową fizyczną ochronę
- tunele kablowe muszą być chronione przed dostępem do okablowania
- serwery powinny być w zamkniętych szafach lub przytwierdzone trwale do podłoża
- sam serwer powinien być zabezpieczony przed zdjęciem obudowy
- dyski twarde powinny być zabezpieczone przed wyjęciem
- stacja zarządzające muszą podlegać takiej samej ochronie jak sam serwer
- hasło BIOS serwera i stacji roboczej
- hasła blokujące konsolę serwerów, stacji roboczych i urządzeń zarządzalnych
- kopie zapasowe muszą podlegać takiej samej ochronie jak urządzenia na których się znajdują
- dokumentacja sieci, usług i serwerów musi podlegać określonej ochronie
- nośniki instalacyjne systemów operacyjnych i systemów zabezpieczeń powinny podlegać szczególnej ochronie

Poziom 2 - Zabezpieczenie systemu operacyjnego

autoryzowany i kontrolowany dostęp do :

- systemu operacyjnego stacji roboczej
- do zasobów sieciowych

Poziom 3 - Zabezpieczenie aplikacji

- wszelkie prace administracyjne powinny być wykonywane na dedykowanych stacjach zarządzających
- wszelkie oprogramowanie zarządzające powinno być dostępne tylko na stacjach zarządzających
- użytkownicy powinni mieć dostępne tylko te aplikacje które są im niezbędne do codziennej pracy
- aplikacje mające dostęp do danych powinny być dostępne po autoryzacji użytkownika i w zależności od tego powinny udostępniać i blokować odpowiednie funkcje swojego działania, niezależnie od praw nadanych dla użytkownika do poszczególnych obiektów baz danych
- centralny system zarządzania i dystrybucji aplikacji
- odebranie użytkownikom możliwości instalacji oprogramowania

Poziom 4 - Ochrona baz danych

autoryzowany i kontrolowany dostęp do baz danych :
- w oparciu o globalny system autoryzacji
- w oparciu o system operacyjny serwera
- w oparciu o własny system autoryzacji dostępny w danej bazie danych

Poziom 5 - Ochrona obiektów baz danych

autoryzowany i kontrolowany dostęp do obiektów baz danych :
- tabel
- widoków
- zapytań
- formularzy
- raportów
- procedur
- funkcji
- wyzwalaczy
- pól

Poziom 6 - Aktywna i pasywna ochrona sieci

- FW *(rodzaje : SPF, SPI, BL7F, BAF, DDR, NAT, PAT, Proxy)*

Zapora sieciowa jest urządzeniem lub oprogramowaniem zaprojektowanym zapobiegającym niepowołanemu dostępowi do sieci. Zadaniem jej jest kwalifikowanie, filtrowanie i logowanie określonych zdarzeń dotyczących ruchu począwszy od warstwy L2 po L7. Kwalifikacji żądania połączenia dokonywać można na podstawie: protokołu warstwy L3, adresu L3 hosta źródłowego jak i docelowego, źródłowego lub docelowego portu L4, adresu źródłowej lub docelowej sieci, interface źródłowego lub docelowego, adresu URL, użytkownika, grupy, MAC adresu, protokołu warstwy aplikacji L7, czasu, treści danych. Filtrowanie polega na przepuszczeniu lub odrzuceniu i logowaniu odpowiednio zakwalifikowanych pakietów.

- IDS *(rodzaje : NIDS, HIDS)*

Systemy wykrywania zagrożeń są urządzeniami lub oprogramowaniem służącym do wykrywania ataków na system komputerowy i samoczynnego przeciwdziałania tym że zagrożeniom. Systemy te możemy podzielić na działające na sieci i działające na hoście. Systemy te monitorując system potrafią rozpoznawać sygnatury ataków i w sposób aktywny im przeciwdziałać.

- AV *(rodzaje : skanery, monitory, szczepionki, sumy)*

Programy antywirusowe przeciwdziałają rozpowszechnianiu się wirusów. Praca monitorów polega na ciągłym monitorowaniu serwerów plików, poczty jak i stacji roboczych. W przypadku wykrycia odpowiednich sygnatur wskazujących na obecność wirusa, robaka czy konia trojańskiego, programy te podejmują określone zadania dotyczące zainfekowanych danych jak i informują różnymi metodami zainteresowane osoby. Skanery jako najprostsze programy wirusowe służą do sprawdzania nośników danych czy nie ma w danych jakie są na nich zapisane szkodliwych programów lub dokumentów.

- QoS *(rodzaje : CoS, ToS, DSCP, ICR, ECR, RSVP, NBAR, RED)*

Usługa zapewnienia jakości usług polega na odpowiednim zarządzaniem pasmem sieciowym począwszy od L2 po L7, tak aby wszystkie potrzebujące aplikacje miały zapewnione odpowiednie pasmo. Kształtowanie ruchu można realizować stosując reguły dla ruchu przychodzącego i wychodzącego, równoważenie obciążeń oraz realizując odpowiedni routing. Realizuje się to przez procesy rozpoznawania, klasyfikowania, oznaczania i zapobiegania zatorom określonych pakietów lub rezerwacji pasma pomiędzy odpowiednimi urządzeniami sieci. Rozpoznawanie może być prowadzone w oparciu o: protokołu warstwy L3, adresu L3 hosta źródłowego jak i docelowego, źródłowego lub docelowego portu L4, adresu źródłowej lub docelowej sieci, interface źródłowego lub docelowego, użytkownika, grupy, MAC adresu, protokołu warstwy aplikacji L7, czasu. Zapobieganie zatorom realizuję się metodami odrzucania pakietów i metodami ich kolejkowania.

- VLAN

Technologia wirtualnych sieci LAN polega na separacji grup roboczych w warstwie L2, gdzie przełączanie pomiędzy odseparowanymi grupami roboczymi odbywa się w warstwie L3. Oprócz separacji grup roboczych stosuję się do separacji kanałów głosowych i danych.

- VPN *(rodzaje : IP VPN, Internet VPN, FR VPN, ATM VPN)*

Wirtualne sieci prywatne są technologią która umożliwia sprzętową lub programową realizację szyfrowanych tuneli w warstwie L2 i L3. Są one niezbędne jeżeli chcemy zachować poufność przesyłanych danych a aplikację wyższych warstw nie mają żadnych mechanizmów związanych z zapewnieniem poufności i integralności.

- rozproszony i replikowalny system globalnej autoryzacji *(NDS, ADS, NIS/YP, LDAP)*

Polega na jednej autoryzacji dla stacji roboczej, serwerów plikowych, serwerów baz danych, usług Internet-owych, urządzeń i innych systemów operacyjnych serwerów jak i sieci

- dodatkowe systemy autoryzacji dla zdalnych użytkowników *(PAP, CHAP, RADIUS, TACACS, Kerberos)*

- bezpieczne zarządzanie *(rodzaje : EIB, OOB)*

W rozbudowanych systemach sieciowych zarządzanie powinno się odbywać na odseparowanych fizycznie łączach lub w przypadku zarządzania na tych samych łączach co przesył danych ruch zarządzający powinien być szyfrowany ze względu na możliwość podsłuchu.

- rejestrowanie zdarzeń i serwery logów *(rodzaje : syslog, ODBC, OLE-DB, BDE)*

W każdym systemie sieciowym powinno odbywać się rejestrowanie zdarzeń na wszystkich poziomach modelu OSI - począwszy od rejestracji zdarzeń dotyczących użytkowania i dostępu do aplikacji czy usługi sieci, poprzez rejestrację zdarzeń i dostępu do sieci a kończywszy na rejestrowaniu połączeń telefonicznych przez które były przesyłane dane. Jeżeli chodzi o rejestrację zdarzeń dla aplikacji to mechanizmy rejestracji musi wspierać sama aplikacja a w przypadku rejestrowania zdarzeń sieci rejestrowanie powinno być realizowane na wszystkich urządzeniach warstwy L2, L3 i L4 ze szczególnym uwzględnieniem punktów styków naszej sieci z sieciami zewnętrznymi. Zapisywanie tych zdarzeń może się odbywać poprzez standardowe mechanizmy na danej maszynie lub na specjalnych serwerach logów czy też bazach danych. Jednak standardowe mechanizmy nie dają odpowiedniego poziomu bezpieczeństwa bo włamywacze potrafią modyfikować wpisy w celu maskowania swojej działalności i nawet powstały narzędzia pozwalające na automatyzację maskowania pracy włamywacza poprzez zmianę wpisów w dziennikach. Dlatego lepiej stosować dodatkowe mechanizmy a w szczególności bazy danych które mają dodatkowe mechanizmy ochrony.

Poziom 7 - Kontrola dostępu do Internet-u

- spisane reguły dostępu do sieci Internet
- rejestrowanie działań użytkowników w Internecie
- możliwość wizualnego podglądu działań użytkownika w Internecie
- kontrolowany dostęp do Internet-u poprzez autoryzację
- analiza danych wysyłanych i pobieranych z Internet-u

Każda próba skorzystania z sieci Internet powinna być autoryzowana poprzez podanie identyfikatora i hasła. Autoryzowani użytkownicy powinni być podzielenia na odpowiednią liczbę grup dostępu.

Najwyższy poziom dostępu (czyli brak jakichkolwiek ograniczeń w korzystaniu z sieci Internet) powinni posiadać ludzie ze ścisłego kierownictwa firmy lub organizacji (np. członkowie zarządu, kadra dyrektorska i kadra kierownicza IT).

Następny poziom przeznaczona dla kadry kierowniczej średniego szczebla powinien zakładać już pewne restrykcję dotyczące czasu jak i treści (blokowane serwisy dla dorosłych, multimedialne, hazard i potencjalnie niebezpieczne oraz ograniczenia czasowe).

Poziom zabezpieczenia na którym powinni pracować pracownicy biurowi powinien im umożliwiać tylko kontakt z określonymi partnerami biznesowymi w określonym czasie.

Ostatni poziom powinien blokować wszystko i ten poziom powinien być domyślnie nadawanym dla nowych użytkowników i grup. W przypadkach uzasadnionych powinna być możliwość podglądu ekranu stacji roboczej użytkownika bez powiadamiania go o tym.
Wszelkie działania użytkowników muszą być rejestrowane a dane wysyłane powinny być analizowane pod kątem zawartości i w razie potrzeby powinna być możliwość samoczynnej blokady.

Poziom 8 - Bezpieczny dostęp użytkowników przez Internet do zasobów sieci własnej

- dostęp do plików *(protokoły standardowe NFS, SMB/CIFS, NCP, FTP, HTTP)*

Jeżeli chodzi o dostęp poprzez sieć Internet do plików znajdujących się w zasobach własnej sieci to korzystając z tradycyjnych protokołów takich jak FTP, HTTP, NFS czy SMB/CIFS należy pamiętać że dane są przesyłane bez żadnego zabezpieczenia. Możliwe jest przechwycenie danych a także ich modyfikacja a w protokole FTP jest możliwość przechwycenia nawet hasła gdyż jest ono przesyłane jawnym tekstem. Ponadto oprócz protokołu HTTP w którym jest możliwość używania SSL, pozostałe wymienione nie mają możliwości zaimplementowania żadnych metod zwiększających poufność i integralność danych. Dlatego jeżeli chcemy aby dostęp do plików poprzez sieć Internet był bezpieczny należy stosować oprogramowanie działające w architekturze klient-serwer które to w większości przypadków działa na protokole HTTP i umożliwia zarówno synchronizację plików, szyfrowanie transmisji jak i szyfrowanie danych zapisywanych na serwerach.

- dostęp do baz danych *(aplikacje natywne i WWW)*

Jeżeli chodzi o bazy danych to w przypadku komunikowania się klienta przyłączonego poprzez Internet z własnym serwerem bazy danych to w przypadku aplikacji natywnych nie ma możliwości zabezpieczenia poufności i integralności przesyłanych danych gdyż ani klient ani serwer bazy danych nie posiadają standardowo takich mechanizmów. W przypadku korzystania z aplikacji WEB-owych istnieje możliwość używania protokołu SSL.

- dostęp do wiadomości i poczty

Standardowe protokoły poczty takie jak SMTP, POP3 nie posiadają żadnych mechanizmów bezpieczeństwa zarówno dotyczących przesyłania haseł jak i danych. Ale istnieje możliwość zastosowania tuneli SSL do bezpiecznego przesyłania haseł jak i danych. Wszystkie najbardziej popularne przeglądarki są przystosowane do wspierania tuneli SSL. Jeżeli nie mamy do dyspozycji tuneli SSL lub chcemy dodatkowo zwiększyć poufność i integralność przesyłanych danych możemy zastosować podpis elektroniczny wraz a szyfrowaniem. Nie należy zapominać również o uwierzytelnianiu użytkownika w serwerze poczty wychodzącej co zapobiega wysyłaniu obcej poczty z naszego konta. W przypadku korzystania ze stron WWW do wymiany wiadomości należy pamiętać że w normalnym trybie dane nie są szyfrowane i w celu uzyskania poufności i integralności należy używać szyfrowania SSL.

- zdalne administrowanie *(telnet, r*, ssh, X-terminal, Windows Terminal, WEB)*

Programy takie jak telnet czy wszystkie r* (rlogin, rcp, rsh) nie posiadają żadnych mechanizmów ochrony danych jak i ochrony przesyłanych haseł. Polecanym narzędziem do zdalnego

administrowania jest SSH który posiada zarówno ochronę przesyłanych haseł jak i chroni przesyłane dane poprzez różne rodzaje szyfrowania. Usługi zdalnego administrowania oparte o aplikacje X-window wykorzystujące do komunikacji SSH możemy również uznać za bezpieczne. Jeżeli chodzi o Terminale Windows oparte na standardowym oprogramowaniu dostępnym w systemie to oprogramowanie to nie prowadzi szyfrowania danych. W przypadku wykorzystywania aplikacji WEB-owych do zdalnego administrowania jak i do przeprowadzania operacji wymagającej poufności i integralności należy używać szyfrowania SSL które wspierają standardowo wszystkie poważne serwery WWW i wszystkie najbardziej popularne przeglądarki WWW.

6. Metody autoryzacji

Autoryzacja ma za zadanie ochronę zasobów naszej sieci przed nielegalnym dostępem. Generalnie metody autoryzacji możemy podzielić na autoryzację urządzeń i autoryzację użytkowników.

Autoryzacja urządzeń przeważnie jest realizowana w oparciu o warstwę L2 i L3 modelu OSI. Polega ona na uwierzytelnieniu danej maszyny na podstawie np.: jej adresu sprzętowego karty sieciowej lub interfejsu sieciowego (adresu MAC) czy też jej adresu sieciowego (adresu IP lub IPX). Istnieje także możliwość uwierzytelniania urządzeń poprzez przedstawiane przez nie certyfikaty SSL.

Autoryzacja użytkowników polega na przedstawieniu się użytkownika. Tą metodę autoryzacji możemy podzielić na trzy rodzaje.

Pierwszy z nich to autoryzacja na poziomie zasobu lub urządzenia. Polega ona na podaniu hasła i w zależności od hasła uzyskujemy odpowiednie prawa dostępu do danego zasobu lub urządzenia. Autoryzacja ta nie rozróżnia użytkowników w związku z tym nie ma możliwości kontrolowania działań użytkowników.

Drugim rodzajem jest autoryzacja na poziomie użytkownika. Polega ona na podaniu identyfikatora i hasła użytkownika. Autoryzacja ta rozróżnia użytkowników i każdy użytkownik może posiadać dowolnie nadane prawa przez administratora systemu. Autoryzacja to może być prowadzoną zarówno przez lokalną bazę użytkowników danej maszyny jak i przez system globalnej autoryzacji.

Trzecim rodzajem autoryzacji jest przedstawienie się użytkownika certyfikatem SSL które w połączeniu z metodą przedstawienia się serwera certyfikatem SSL daje możliwość dwustronnej autoryzacji. Ten rodzaj autoryzacji najczęściej stosuje się przy komunikacji WEB-owej.

Jeżeli chodzi o metodę autoryzacji urządzeń (za wyjątkiem certyfikatów SSL) to jest to najprostszy i najbardziej zawodny sposób autoryzacji. Nie daje on możliwości użytkownikowi przemieszczania się (pracy na różnych maszynach lub zdalnie). Metoda ta jest stosowana jako metoda dodatkowa przy autoryzacji użytkowników w celu zmniejszenia ilości miejsc z których użytkownik może uzyskać dostęp do zasobów.

Jeżeli chodzi o metodę autoryzacji użytkowników to najczęściej stosowanym rodzajem jest autoryzacja na poziomie użytkownika. Daje ona możliwość pracy użytkownikowi na dowolnych stacjach roboczych z tymi samymi prawami.

Aby autoryzacja ta zapewniała odpowiedni poziom bezpieczeństwa musimy przyjąć odpowiednią politykę dotyczącą haseł dla poszczególnych zasobów.

W skład tej polityki muszą wchodzić takie zagadnienia jak tworzenie haseł, historia hasła, okres ważności hasła, ograniczona ilość prób logowania.

Jeżeli chodzi o tworzenie haseł to mamy dwie możliwości. Pierwsza z nich polega na tym że użytkownicy sami tworzą i zmieniają sobie hasła a druga zobowiązuje administratora do nadawania i zmieniania haseł. Hasła powinny wykazywać odpowiedni stopień zawiłości tzn. co najmniej 6 znaków w tym cyfry przemieszane z literami oraz nie powinny być oczywiste. Nie można dopuszczać haseł które wywodzą się z nazw lub opisu użytkownika (np. nazwisko, imię, pseudonim, przezwisko, data urodzenia, imiona małżonka, dzieci, pasa, nazwy ulubionych marek).

W przypadku zmiany hasła istotną rzeczą jest okres ważności hasła i historia haseł. Użytkownicy nie lubią zmiany haseł dlatego starają się posługiwać małą ilością haseł lub poprzez podwójną zmianę w krótkim odstępie czasu wracają do starego hasła. Aby uniemożliwić użytkownikom takie działania stosuje się historię haseł oraz minimalny i maksymalny okres ważności haseł.

W przypadku zrzucenia obowiązku tworzenia i zmiany hasła na użytkownika musimy uruchomić mechanizmy które będą kontrolowały procesy tworzenia i zmiany haseł. Podstawowe mechanizmy znajdują się w każdym nowoczesnym systemie uwierzytelniania (np. NDS, ADS, NIS/YP). Istnieje także szereg narzędzi dodatkowych zarówno dostarczanych przez producentów naszego systemu uwierzytelniania jak i narzędzi niezależnych producentów.

Należy pamiętać że jeżeli za bardzo zaostrzymy restrykcję dotyczące tworzenia i zmiany haseł przez użytkowników lub skomplikowane hasła będzie tworzył i zmieniał administrator to możemy doprowadzić do sytuacji że użytkownicy będą mieli kłopoty z zapamiętaniem haseł i zaczną zapisywać je np. na przyklejonej żółtej karteczce do monitora lub pod klawiaturę.

Innymi sposobami autoryzacji użytkowników mogą być metody wykorzystujące inteligentne karty lub metody bazujące na identyfikacji biometrycznej (np. odcisk palca, geometria dłoni, wizerunek oka lub całej twarzy, rozpoznawanie głosu, pismo odręczne).

Jeżeli chodzi o karty inteligentne mogą one przypominać karty telefoniczne czy bankomatowe które mogą być rozpoznawane stykowo (poprzez włożenie ich do czytnika) lub bezstykowo oraz mogą być podobne do kalkulatorów. Karty te mają wyświetlacz i klawiaturę. Zastosowanie ma tu silne, 2-elementowe uwierzytelnienie oparte na czymś co wiesz” oraz “czymś co masz”. Po podaniu odpowiedniego hasła czy też PIN-u karta ta generuje nam jednorazowe hasło.

Istotną sprawą jest to ile prób autentykacji do różnych zasobów musi zrealizować użytkownik. Związane jest to z ilością haseł które musi znać użytkownik oraz które zgodnie z polityką haseł dla różnych zasobów ulegają zmianom lub użytkownik zobowiązany jest je zmieniać. Zapamiętanie większej ilości haseł jest nie wygodne dla użytkownika co powoduje powstanie słabości w systemie bezpieczeństwa. Dlatego przy większych systemach informatycznych zaleca się stosowanie mechanizmów umożliwiających jednokrotne logowanie (single sign-on) do wszystkich zasobów do których potrzebuje mieć dostęp użytkownik. Mechanizmy te możemy wzbogacić dodatkowo o metody wieloetapowego uwierzytelniania w zależności od ważności zasobów. Dla zasobów zwykłych wystarcza tylko hasło, do zasobów ważniejszych hasło i token a do zasobów najważniejszych hasło, token i jedna z metod biometrycznych. Ponadto w przypadku posiadania różnych platform sprzętowo-programowych wchodzących w skład własnej sieci nieodzowne jest posiadanie systemów ułatwiających zarządzanie dostępem do wszystkich tych platform.

7. Komputerowe techniki zagrażające systemom informatycznym :

1. Techniki związane z rozszyfrowaniem hasła :

Posługujemy się tu specjalnymi programami łamiącymi hasła. Do grupy tej możemy zaliczyć każdy program omijający zabezpieczenia hasłem bądź kluczem, poprzez jego ujawnienie. Programy te stosują następujące techniki :

- crack prosty

większość algorytmów kryptograficznych jest jednokierunkowa i hasła tak zakodowane są nie dekodowalne. Jeżeli chcemy odnaleźć hasło musimy zastosować narzędzi symulujące działające w oparciu o ten sam algorytm, który został użyty do zaszyfrowania oryginalnego hasła. Ta metoda polega na sprawdzaniu czy hasłem nie jest jakaś dana zawarta w systemie. Mogą to być identyfikatory, nazwiska, imiona, daty urodzin, nazwy stacji roboczych i inne informacje o użytkowniku. Metoda bardzo szybka pozwalająca znajdywać złe/słabe hasła.

- crack słownikowy

polega na szukaniu hasła kodując słowo po słowie z dużymi prędkościami. Nie sprawdza się wszystkich kombinacji lecz wyrazy do kodowania pobierane są ze specjalnie przygotowanego do takich okazji słownika który jest zawarty w pliku zewnętrznym.

- crack inkrementalny (brute force)

polega na sprawdzaniu wszystkich możliwych kombinacji jedno, dwu, ..., ośmio literowych i cyfrowych, kodując je na odpowiednią liczbę sposobów. Jeżeli znajdzie się kombinacja który będzie zgodna po zakodowaniu z ciągiem znaków znajdującym się w naszej zakodowanej bazie danych użytkowników to ta kombinacja będzie szukanym hasłem. Metoda bardzo czasochłonna.

2. Techniki związane z pozyskiwaniem informacji :

Posługujemy się tu bardzo dużą gamą programów programami zarówno standardowych dostępnych w systemach operacyjnych jak i specjalnie do tego stworzonych o bardzo wyrafinowanych możliwościach. Możemy rozróżnić następujące techniki :

- fingering

pozwala na ustalenie kto jest obecny w systemie oraz pozwala na pozyskanie pewnych informacji przydatnych do ataku o danym użytkowniku. Pewna błędna konfiguracja demona finger pozwala na odczytanie dowolnego pliku z systemu plików.

- fingerprinting

polega na odkrywaniu przez skaner rodzaju systemu operacyjnego i jego wersji zainstalowanej na danej maszynie. Dysponując wiedzą o lukach i najczęściej popełnianych błędach przy konfiguracji, włamywacz ma ułatwione zadanie.

- scanning

proste skanowanie w celu poznania adresów IP i nazw aktywnych maszyn dostępnych w interesującej nas sieci lub podsieci.

- port scanning

skanowanie określonych maszyny w celu zapoznania się z udostępnionymi portami TCP/UDP i usługami na nich dostępnymi. Ma to na celu zlokalizowanie znanych, trudnych do obrony serwisów. Najnowsze programy umożliwiają skanowanie sieci schowanych za ścianami ogniowymi.

- error scanning

skanowanie ukierunkowane na znalezienie błędów w konfiguracji lub luk w oprogramowaniu zarówno systemu operacyjnego jak i serwisów udostępnionych przez daną maszynę. Programy te posiadają bazy danych o zagrożeniach i bazy te możemy aktualizować. Są to najbardziej dopracowane narzędzia wśród gamy wszystkich skanerów.

- sniffing

pozwala na przechwytywanie i zapisywanie wszystkich lub wybranych pakietów podróżujących po sieci do której ma dostęp dana maszyna. Analizie mogą podlegać różne protokoły. Istnieje możliwość przechwytywania zarówno haseł jak i danych co może służyć do zdobycia dostępu do sieci i usług. Istnieje również możliwość rekonstrukcji sesje i strumieni.

- airsnort

technika stosowana do nielegalnego dostępu do sieci bezprzewodowych poprzez wszelkie urządzenia WLAN. Polega ona na przechwyceniu określonej liczby pakietów i znalezieniu statycznego klucza służącego do autoryzacji i szyfrowania sprzętowego. A następnie możemy prowadzić przechwytywanie danych lub uzyskać nielegalny dostęp do danej sieci WLAN poprzez kartę sieciową WLAN, telefon bezprzewodowy IP a nawet bridge WLAN.

- starvation (DHCP starvation)

polega na instalacja fałszywego serwera DHCP wykorzystując brak autentykacji dla protokołu DHCP. Pozwala to na po przydzielanie innych adresów IP niż te które miały być pierwotnie przydzielono co może mieć wpływ na routing, FW, NAT, QoS i inne mechanizmy bazujące o adresy IP a także przydział do określonych grup roboczych warstwy L2.

- cache flushing

polega na odczytaniu hasła z pamięci operacyjnej które jest buforowane do ewentualnego późniejszego wykorzystania. Istnieje również możliwość wymuszenia zapisania zbuforowanego hasła do pliku wymiany

3. Techniki związane z podszywaniem :

Podszywania jest to wyszukany sposób uwierzytelnienia danej maszyny wobec innej poprzez fałszowanie pakietów zawierających adres uprawnionego nadawcy. Włamywacz musi uśpić maszynę pod której adres chce się podszyć i połączyć się z celem ataku jako wiarygodny klient. Możemy wyróżnić następujące poziomy podszywania :

- IP spoofing

polega na podszywaniu się jednego urządzenia pod drugi przez odpowiednią zamianę adresów IP. Sposób ten umożliwia na dostęp do innych maszyn będących w relacjach zaufania opartych na warstwie L3 a także zdobycia uprawnień związanych z routingiem, FW, QoS i innym opartymi tylko na warstwie L3

- ARP spoofing

technika która zmienia bufor protokołu ARP. Bufor ten zawiera informacje o odwzorowaniach adresów sprzętowych MAC na adresy IP. Można zmienić adres fizyczny (adres warstwy L2) komputera upoważnionego na adres maszyny włamywacza co daje możliwości podobne jak IP spoofing.

- DNS spoofing

polega na zmianie lub nadpisaniu poprawnych wpisów w DNS a także wyeksportowaniu fałszywych wpisów DNS do innych serwerów DNS. Umożliwia to w przypadku używania adresowania URL na podmianę adresów IP co skutkuję dostępem do nieodpowiednich maszyn.

- hijacking

technika ta polega na porwaniu sesji TCP poprzez jej przechwycenie. Umożliwia to podszycie się pod uwierzytelnioną już maszynę podczas bezpośredniej komunikacji.

- VLAN hopping

polega na tym że stacja może udawać przełącznik z obsługą protokołu ISL lub 802.1Q. Efektem tego może być to że stacja może należeć do wszystkich VLAN-ów przez co uzyskuję dostęp do wszystkich grup roboczych jak i kanałów telefonii IP. Działa to nawet wtedy, gdy trunk na porcie jest wyłączony.

4. Techniki związane z uruchomieniem skryptów/programów :

Programami w tego rodzaju atakach są prawidłowo działające programy z dołączonym obcym kodem który realizuje nieznane użytkownikowi i niepożądane funkcje. Nielegalne funkcje jakie realizują te programy mogą być różnorakiego rodzaju. Począwszy od komicznych i śmiesznych poprzez prowadzące do uzyskania nielegalnego dostępu do zasobów sieci aż do silnie destrukcyjnych. Są trudne do wykrycia i mogą występować w plikach binarnych jak i skryptowych, pracujących pod kontrolą systemu operacyjnego lub pracujące pod kontrolą innych aplikacji jak np.: serwer WWW, przeglądarka WWW

- trojan horses / back door

są typowymi prawidłowo działającymi programami (przeważnie pod kontrolą systemu operacyjnego ofiary) z dołączonym obcym kodem który realizuje nieznane użytkownikowi i niepożądane funkcje. Programy tego typu podrzuca się nieświadomym użytkownikom a oni je użytkują. Umożliwiają intruzowi na zdobywanie interesujących go danych jak i nielegalne wejście do systemu i wykonywanie tam nielegalnych operacji.

- CGI , DSO, ISAPI, NSAPI, PHP, ASP

są to programy działające pod kontrolą serwerów WWW. Mogą być programami samodzielnymi jak i bibliotekami czy modułami wywoływanymi przez serwer WWW. Włamywacz może wykorzystać słabość takiego programu (błędy programistów) i może zdobyć możliwość uruchamiania programów w systemie operacyjnym. Istnieje możliwość także podłożenia specjalnie przygotowanych programów tego typu który realizuje nieznane użytkownikowi i niepożądane funkcje na jego serwerach.

- ActiveX

jedna z najniebezpieczniejszych technologii WEB-owych działających pod kontrolą przeglądarki WEB. Kontrolka ActiveX może stwarzać pozory dokumentu utworzonego przy użyciu danej aplikacji przez co może doprowadzić do uruchomienia określonego programy a następnie może zdalnie kontrolować ten program. Cały proces jest nie widoczny dla użytkownika. Ponadto szkodliwy komponent może przeprowadzać dowolne operacje na plikach. ActiveX powinno być bezwzględnie odfiltrowywane już na zaporach ogniowych.

- Java Control

przeglądarka pod kontrolą apletu Java może przeprowadzać operacje na lokalnym systemie plików oraz ma możliwość odczytywania zmiennych środowiskowych, przeglądania danych użytkownika i zbierania innych informacji o użytkowniku. Istnieje też możliwość wykonania innych funkcji np. zmiana konfiguracji firewall czy innych zabezpieczeń.

- VBScript / JavaScript

jeżyki te mają możliwości wykonywania pewnych niebezpiecznych operacji zarówno pracując po stronie serwera jak i klienta bez względu na reakcję użytkownika.

- sploit /exploit

szkodliwe programy lub programy udające działanie standardowych programów systemu operacyjnego Linux/UNIX

- rootkit

pakiety które podmieniają oryginalne programy na specjalnie spreparowane programy tworzące tylne drzwi do systemu a co ciekawsze pakietu umożliwiają ukrycie pracy agresora.

- wirusy (viruses)

5. Techniki powodujące zablokowanie usług :

Techniki powodujące zablokowanie usług nie stanowią bezpośredniego zagrożenia dla danych znajdujących się w atakowanym systemie komputerowym ale stanowią prawdziwe utrapienie dla jego użytkowników gdyż utrudniają lub nawet uniemożliwiają korzystanie z zasobów sieci komputerowej legalnym użytkownikom. Możemy wyróżnić następujące rodzaje ataków :

- DoS (Denial of service)

standardowy atak tego typu charakteryzuje się paraliże usług, wyłączeniem systemu lub sieci. Możemy wyróżnić dwa rodzaje ataków. Pierwszy z nich to ataki na urządzenia i zadaniem jego jest obniżenie wydajności urządzenia lub jego zablokowanie. Charakteryzuje się on dużą ilością małych pakietów. Drugim rodzajem jest atak na łącze który powoduję spadek przepustowości i charakteryzuje się dużą wielkością pakietów. Celem ataków mogą być serwery lub urządzenia sprzętowe takie jak routery, firewall-e czy switche (w niektórych przypadkach może dojść nawet do fizycznego uszkodzenia sprzętu podczas takiego ataku). Objawami takiego typu ataku jest ciągłe przeciążenie procesora urządzenia, utraty pakietów, wzrost ruchu. Ataki te mogą być prowadzone przez wirusy, robaki i w sposób ręczny przez nawet jedno urządzenie, wykorzystując słabości systemów operacyjnych oraz użytkowników. Obrona przed atakami DoS jest bardzo trudna i wymaga zastosowania wielu metod ze sobą współpracujących oraz dużej praktyki administratora.

- DDoS (Distributed DoS)

ataki tego typu są udoskonaloną formą ataków DoS i są prowadzone z wielu maszyn i z wielu miejsc równocześnie. Praktycznie żaden router nie poradzi sobie z tym oraz istnieje nawet możliwość paraliżu urządzeń rdzeniowych sieci kampusowych. Ataki DDoS nie mogą być powstrzymane przez samą zaatakowaną sieć i powodują obniżenie wydajności nie tylko atakowanego systemu.

- STP DoS

powstanie pętli w sieci Ethernet, sprawia że ruch typu broadcast zmienia się w sztorm i ramki krążą w nieskończoność blokując tym samym komunikację w całym segmencie.

- gratuitous ARP

polega na wykorzystywaniu do samoczynnie i bez zapytania rozgłaszania własnych adresów IP co powoduję spadek wydajności segmentu sieci w której znajduje się napastnik.
Przyczyną tego jest brak mechanizmu bezpieczeństwa w protokole ARP

- flooding (MAC flooding)

powoduje to zjawisko zalew danych pochodzących z odwołań po ICMP. Następuje przepełnienie tablicy CAM w przełączniku co objawia się spadkiem wydajności sieci

- SYN-flood

polega na wysyłaniu dużej liczby tzw. SYN pakietów lub wysyłanie pół-otwartych żądań połączenia co w efekcie powoduje wypełnienie kolejki połączeń oczekujących i maszyna nie akceptuje następnych zgłoszeń. Następować może zajętość dużej liczby portów i powodzie TCP SYN/TCP ACK, ARP, DHCP

- fragmentation

jest to próba nadpisania danych w nagłówku pakietu TCP lub wysyłanie celowo uszkodzonych pakietów. Zmianie ulega pole CID.

- SMTP bug

wykorzystanie luk w oprogramowaniu serwera SMTP lub przeładowanie systemu wiadomościami.

- e-mail bombers

wysyłamy do danego serwera pocztowego większą ilość przesyłek, tak dużą że jesteśmy w stanie znacząco spowolnić działanie serwera lub zablokować cały serwer. Inną uciążliwością jest to że przy wolnych łączach odebranie tych „śmieci" zajmuje dużo czasu i znacząco obciąża sieć. Tego typu ataki nie wpływają na utratę danych. Inną odmianą tego typu ataku jest zapisanie atakowanego adresu poczty na wiele grup dyskusyjnych które generują dużą liczbę wiadomości.

- spam

rozsyłanie niechcianej poczty i reklamy powoduje duży ruch w sieci, zajmowanie miejsca na serwerach poczty oraz trudności z korzystania z poczty elektronicznej.

- buffer overflow

techniki powodujące przepełnienie stosu pamięci przydzielonej procesowi która może spowodować w sprzyjających warunkach wykonanie jakiegoś polecenia lub uruchomienie dowolnego procesu.

6. Techniki psychologiczno-socjotechniczne :

- polityka haseł dostępu
- przekazywania haseł i kluczy
- niszczenia dokumentów
- dostęp do stacji dyskietek, nagrywarek, dysków twardych, modemów
- dostęp do Internetu

Człowiek jest najsłabszym ogniwem systemu bezpieczeństwa. Pewne powszechne cechy charakteru pozwalają na łatwy dostęp do informacji pozwalających na dokonanie agresji. Działania takie najczęściej są powodowane brakiem odpowiedniej świadomości istniejących zagrożeń. Technika wykorzystująca ludzkie słabości została nazwana 'Social Engineering' czyli inżynierią społeczną.

W ‘Social Engineering’ (inżynierii społecznej) można wyróżnić dwie metody.

Pierwsza z nich to użycie środków programowo-sprzętowych do których można zaliczyć uruchomienie odpowiednio zmodyfikowanych usług udających prawdziwe serwery, usługi lub zasoby sieci (np. rozmieszczenie stron WWW zawierających odpowiednio umotywowaną prośbę o podanie identyfikatora oraz hasła) lub przesłanie programu który przechwyci hasło i wyśle je do intruza. Metodą tą posługują się osoby biegłe w informatyce gdyż wymagana jest tu duża wiedza z zakresu IT.

Druga bazuje na bezpośrednim kontakcie osobistym lub telefonicznym. Tutaj jest wiele metod i zależą one tylko od pomysłowości włamywacza. Np. intruz może podawać się z jakąś ważną osobę w firmie i zażądać nowego hasła, może podszywać się pod pracownika serwisu komputerowego i podczas rzekomej naprawy poprosić o hasło ale najczęstszą metodą są bliskie kontakty towarzyskie z ofiarą (na przyjęciach, bankietach, przy alkoholu) – napastnik wzbudza takie zaufanie że może pozwolić sobie na pozyskanie każdej informacji.

Jeżeli posiadamy odpowiednie narzędzia przeciwdziałające atakom, zarówno sprzętowe jak i programowe, to zdobywanie informacji metodami tradycyjnych włamań można szybko ujawnić oraz natychmiast reagować na zaistniałe zdarzenie poprzez odłączenie intruza.
Posiadając również aktualizowane oprogramowanie antywirusowe jesteśmy w stanie nie dopuścić do przeniknięcia do naszej sieci szkodliwych programów.
Ale w przypadku zdobycia hasła przez intruza żadne zabezpieczenia sprzętowe jak i programowe nie uchronią nas przed kłopotami.

8. Wirusy komputerowe

Wirus komputerowy jest programem który przyłącza się zazwyczaj do plików na komputerze który udało mu się zaatakować. Większość wirusów działa jak programy rezydentne, pozostają aktywne podczas pracy systemu operacyjnego i czekają na zaistnienie ściśle określonych warunków a następnie prowadzi infekcję plików. Infekcja polega na tym że kod wirusa zostaje dopisany do zawartości określonych plików danych, programów i plików systemowych. Zainfekowany plik staje się nosicielem i sam zaraża następne pliki które mogą znajdować się na lokalnej maszynie lub komputerach w sieci. Proces ten może być całkowicie niewidoczny i może trwać aż do zarażenia wszystkich plików na danej maszynie w między czasie przenosząc się na inne maszyny i doprowadzając do zarażenia całej populacji. Po czasie infekcji następuję aktywowanie się ukrytych w wirusie funkcji na wszystkich zainfekowanych maszynach na raz. Mogą to być procedury destrukcyjne lub prowadzące różnej maści ataki na inne systemy.

Pierwsze wirusy jakie powstały były łatwe do wykrycia ponieważ miały one charakterystyczny ciąg bajtów który był taki sam dla każdego zarażonego pliku. Znajdował się on (był dopisywany podczas infekcji) przeważnie na końcu pliku i był to kod właściwy wirusa. Ponadto jeszcze w nagłówku plików uruchamiających się znajdowało się odniesienie do kodu wirusa a w kodzie wirusa była procedura powrotu do wykonania właściwego programu. W ten sposób zainfekowany program przez nas uruchamiany oddawał na początku kontrolę procedurom wirusa (np. infekującym i/lub destrukcyjnym) a następnie po wykonaniu się procedur wirusa kontrola została oddana właściwym procedurom programu. Proste skanowanie plików wykrywało zawsze wirusa i potrafiło go unieszkodliwić w taki sposób aby działanie właściwego programu było nadal poprawne.

Najnowszą generacją wirusów są wirusy polimorficzne (samo mutujące się) które nie mają żadnych ciągów bajtów charakterystycznych. Uzyskano to przez zastosowanie kodowanie wirusa jak również przez zakodowanie samej procedury dekodującej znajdującej się przed kodem właściwym wirusa. Każda następna kopia wirusa nie ma żadnych charakterystycznych bajtów. W przypadku wirusów polimorficznych również jest modyfikowany nagłówek pliku uruchamiającego się tak aby spowodować przeskok do procedury dekodującej wirusa. Procedura ta dekoduje kod wirusa jak i generator polimorficzny. Następnie następuje działanie wirusa który w przypadku infekcji uruchamia generator polimorficzny który koduje procedurę dekodującą, kod wirusa i sam siebie a następnie wprowadza zmiany w następnym zaatakowanym pliku uruchamiającym się. Po procedurze infekcji może wykonać jeszcze inne niepożądane działanie a następnie uruchamia właściwy program. W przypadku tego rodzaju wirusów proste skanowanie już nie wystarcza i nie zawsze jest możliwość wyleczenia zainfekowanego pliku w taki sposób aby program właściwy działał poprawnie.

8.1 Rodzaje wirusów :

1. Wirusy pasożytnicze (*parasite infectors*)

Są to wirusy które wykorzystują swoje ofiary (czyli pliki wykonywalne) do transportu, modyfikując ich strukturę wewnętrzna.

- dołączające (*appending*) lub lokujące (*end of file*)
dołączają się do końca pliku, wzrasta wielkość pliku i powodują że program który zainfekowały nadal będzie poprawnie pracował oraz istnieje możliwość pełnego wyleczenia

- nadpisujące (*overwrite*)
nie wzrasta wielkość pliku, nadpisują zawartość zainfekowanego pliku co uniemożliwia całkowite wyleczenie, program zainfekowany nie będzie poprawnie pracował

- nadpisujące puste obszary (*cave*)
nie wzrasta wielkość pliku, nadpisują miejsca w których nie niszczą żadnych informacji zainfekowanego pliku, program zainfekowany nadal będzie pracował poprawnie

- dopisujące się do jednostki alokacji pliku (*slack space*)
wirus wykorzystujący do zapisania swojego kodu ostatnią jednostkę alokacji która zazwyczaj nie jest wypełniona do końca, nie wzrasta wielkość zajmowanego miejsca przez plik na dysku oraz zainfekowany program działa dalej poprawnie

2. Wirusy towarzyszące (*companion infectors*)

Są to wirusy które korzystają z hierarchii uruchamiania przez system DOS programów gdy nie podajemy pełnej nazwy programu (brak rozszerzenia)

- uruchamiane przed właściwym plikiem (*.com, *.exe, *.bat)
w przypadku gdy programem właściwym jest plik o rozszerzeniu exe, uruchomieniu podlega plik o tej samej nazwie ale z rozszerzeniem com który jest kodem wirusa a następnie wirus uruchamia właściwy plik programu

- uruchamiane z poprzedzającego katalogu (path)
technika ta jest podobna do poprzedniej z tym wyjątkiem że pierwszy zostaje uruchomiony plik o tej samej nazwie który jest wirusem ale dostępny w katalogu który jest umieszczony w zmiennej środowiskowej PATH

3. Wirusy plików wsadowych (*batchviruses*)

Są to wirusy które używają do transportu pliki o rozszerzeniu bat. Po uruchomieniu pliku wsadowego bat, tworzy plik o rozszerzeniu com lub exe i uruchamia go.

4. Wirusy makrosów (*macroviruses*)

Są to wirusy przenoszone we wszelkiej maści dokumentach w których można definiować makrodefinicję. Wirusy te nie infekują programów wykonywalnych lecz pliki zawierające makrodefinicję. Po uruchomieniu zainfekowanego dokumentu, wirus kopiuje się do szablonu np. normal.dot, personal.xls i wtedy infekuje wszystkie dokumenty przetwarzane przez dany program. Wirusy te mogą przeszukiwać dyski, operować na plikach, wysyłać pocztę.

5. Robaki (*worm*)

Działanie robaków sprowadza się do tworzenia ogromnych ilości własnych kopii na dysku lokalnym i do rozsyłania ich po sieci powodując wielkie natężenie ruch w sieci. Robaki same w sobie nie posiadają mechanizmów destrukcyjnych ale powodują zapychanie dysków twardych co może doprowadzić do upadku serwera zaatakowanego robakiem.

6. Konie trojańskie (*trojan horses*)

Są to programy które oprócz normalnego działania wykonują niewidoczne i niepożądane funkcje z punktu widzenia użytkownika. Często one mają zdolności do samo powielanie się i/lub prowadzenia działalności destrukcyjnej.

7. Bomby logiczne (*logical bombs*)

Są to programy podobne do koni trojańskich ale do aktywacji dochodzi po spełnieniu pewnych warunków narzuconych przez autora bomby.

8. Dialery

Są to programy które prawie samoistnie i w niewidoczny sposób instaluje się w systemie i powoduje samoistne (bez jakiegokolwiek powiadomienia) wdzwanianie się modemem w wysoko płatne serwisy co naraża użytkownika na spore koszty. Działań destrukcyjnych i samo powielających programy te nie wykonują ale są kłopoty z ich usunięciem.

8.2 Podział wirusów :

1. Niezydentne (*non resident*)

Jest to najprostsza odmiana wirusów, która po uruchomieniu nosiciela wyszukuje w bieżącym katalogu i katalogach określonych w zmiennej środowiskowej ofiar i je infekuje. Podczas działanie nie przechwytuje przerwań. Wraz z zamknięciem programu nosiciela wirus przestaje działać.

2. Rezydentne (*resident*)

Przebywają po uruchomieniu w pamięci operacyjnej komputera i monitoruje wszystkie operacje systemu operacyjnego przez przechwytywanie odpowiednich przerwań.
Na szybkość infekcji wpływa parametr który jest stosunkiem liczby infekcji do liczby uruchomień wirusa. Im ten parametr większy tym szybciej będzie się rozprzestrzeniał.
Rozróżniamy :

- **szybkie infektory (*fast infectors*)**
  nastawione są na jak najszybsze zainfekowanie jak największej liczby plików
- **wolne infektory (*slow infectors*)**
  nastawiają się na jak najdłuższe przeżycie w zainfekowanym systemie i mogą stosować techniki przeciwdziałające wykrywaniu

3. Między platformowe

Znacząca większość wirusów jest pisana z myślą o atakowaniu określonego systemu operacyjnego (99,9% wirusów atakuję systemy rodziny Windows) ale ze względu na rosnącą popularność systemów rodziny Linux zaczynają pojawiać się i na tę platformę wirusy. Aby usprawnić infekcję na oby platformach równocześnie stworzono wirusy :

- międzysystemowe (*multisystem viruses*)
  wirusy tego rodzaju mogą atakować wiele systemów operacyjnych
- międzysprzętowe (*multiplatform viruses*)
  najbardziej doskonałe wirusy jakie udało się obecnie stworzyć – są w stanie infekować wszystko niezależnie od platformy sprzętowej i systemowej

8.3 Nosiciele wirusów :

1. Pliki

Najczęstszą drogą jak się przenoszą wirusy są pliki. Najlepszymi plikami są pliki posiadające jakieś instrukcje sterujące oraz funkcje operujące na strukturze systemu plików. Do grupy tych plików zaliczają się pliki wykonywalne, pliki wsadowe, pliki sterowników, pliki z modułami wykonywalnymi a także pliki dokumentów z definicjami makr.
Rodzaje w plików mogących przenosić wirusy :

- pliki programów (*.exe, *.com)
- pliki systemowe (*.sys, *.bin, *.drv, *.vxd, *.386)
- pliki bibliotek i inne (*.dll, *.ov?, *.lib, *.obj, *.bgi)
- pliki dokumentów (*.doc, *.xls, *.mdb, *.sam)

2. Sektory systemowe

Zainfekowanie sektorów systemowych dysku twardego polega na dopisaniu do niego kodu który będzie uruchamiał wirusa. Istnieją pewne różnice między infekcja MBR i BS polegające na różnym rozmieszczeniu kodu ładującego względem informacji o strukturze dysku.
Nosicielem może być :

- główny rekord ładujący (*Master Boot Record*)
- rekordy ładujące (*Boot Sector*)

8.4 Techniki utrudniające wykrywanie wirusa :

Twórcom wirusa zależy na tym aby ich wirus jak najdłużej pozostawał nie wykryty przez użytkownika zainfekowanego systemu, gdyż wykrycie wirusa zwykle kończy się napisaniem na niego szczepionki przez twórców programów antywirusowych jeszcze przed właściwą aktywacją.

1. Technika Stealth

Wirus w większości przypadków modyfikuje pliki i w związku z tym zmienia się ich długość i zawartość. Aby zmiany dokonane przez wirusa na pliku (czyli infekcja) nie były widoczne wirus podczas próby dostępu do pliku, potrafi leczyć go w locie tak że do pamięci operacyjnej trafia plik o zawartości i długości odpowiadającej oryginałowi.

2. Kontrola przerwania

Technikę tę można stosować do odczytu zainfekowanych MBR (Master Boot Record) i BOOT-sector. W tym przypadku już na etapie przerwań sprzętowych które są odwołaniami do dysków, następuje zmiana rozkazu tak aby odczytać inne sektory zawierające oryginalny MBR.

3. Szyfrowanie (*polimorfizm*)

Polega na szyfrowaniu zarówno kodu wirusa jak i jego procedury dekodującej poprzez generator polimorficzny wskutek tego wirus nie ma żadnej charakterystycznej sygnatury rozpoznawczej.

4. Antydebuggowanie

Żeby utrudnić życie programistom piszącym programy antywirusowe twórcy wirusów stosują procedury blokujące przerwania sprzętowe w momencie wykonywania kodu wirusa co powoduje problemy przy analizowaniu kodu wirusa lub procedury wykrywające próbę analizowania i zastosowania w danym momencie określonej destrukcyjnej procedury.

5. Antydeasemblowanie

Aby utrudnić dostęp do uzyskania kodu źródłowego wirusa stosuje się szyfrowanie lub odpowiednie kombinację instrukcji powodujące trudności w zrozumieniu uzyskanego kodu.

6. Antyemulacja

Jest to metoda dla utrudnienia wykrywania wirusów polimorficznych. Dekoderowi próbuje się nadać wygląd programu napisanego w języku programowania wysokiego poziomu co potrafi zmylić programy antywirusowe.

7. Antyheurystyka

Metoda ta polega na odpowiedniej manipulacji kodem wirusa na różne sposoby wykonującym ostatecznie te same działania, programy antywirusowe z heurystyką mają wtedy problemy z rozpoznaniem szkodliwego kodu.

8. Rekonstruktura

Wiele z najnowocześniejszych wirusów w aktywny sposób potrafi walczyć z programami antywirusowymi. Wirusy te potrafią kasować pliki z sumami kontrolnymi, modyfikować programy antywirusowe a nawet je deinstalować z pamięci w niewidzialny sposób dla użytkownikach a nawet wpływać na dane wyprowadzane przez te programy do użytkownika.

Postacie pod jakimi można spotkać wirusy:

- jawna

Wirusy występują w postaci jawnej (niezaszyfrowanej). Wtedy już na poziomie sieci jest możliwość wykrycia i nie dopuszczenia do przeniknięcia ich do chronionego systemu sieciowego.

- ukryta

Wirus występują w postaci zaszyfrowanej lub jest spakowany przy użyciu programu kompresującego który umożliwia zabezpieczenie hasłem. Zaszyfrowany plik lub spakowany z hasłem (zaszyfrowany hasłem) jest przez programy antywirusowe działające na sieci nie wykrywalny. Dopiero użytkownik podczas dekompresji pliku jeżeli ma program antywirusowy zabezpieczający jego stację roboczą może odkryć wirusa.

Źródła wirusów:

- Internet (strony WWW, poczta, FTP, chaty)
- płyty CD
- płyty DVD
- dyskietki
- wyjmowalne dyski twarde
- ZIP-y
- kasety bibliotek taśmowych

W jaki sposób można doprowadzić do zainfekowania:

- pobierając i uruchamiając zainfekowany program pochodzący z Internet-u (np. WWW, FTP, KaZaA)
- uruchamiając zainfekowany załącznik poczty
- uruchamiając zainfekowany program z nośnika
- otwierając zainfekowany dokument
- wkładając do stacji zainfekowany CD/DVD
- wkładając do stacji zainfekowaną dyskietkę lub przenośny napęd dyskowy

Znana zasada bezpieczeństwa mówi że im większa elastyczność i łatwość obsługi systemu operacyjnego tym bardziej narażony jest na samoistne infekcje.

Co nas czeka w przyszłości ?

- wirusy w plikach graficznych (*.gif, *jpg, *.png) atakujące przeglądarki Internet-owe i system operacyjny na którym pracuje przeglądarka
- wirusy w plikach muzycznych (*.mp3) atakujące programy do dystrybucji i odtwarzania wraz z systemem operacyjnym pod którego kontrolą pracują
- wirusy zawarte w filmach DVD, VCD
- wirusy atakujące telefony GSM i UMTS
- wirusy rozprzestrzeniające się poprzez sieć energetyczną (~230V)

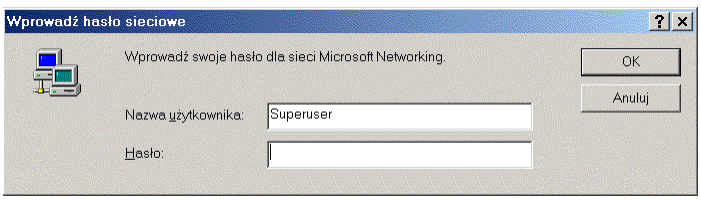
9. Nowoczesne metody ataków na systemy IT

Metody profesjonalistów zazwyczaj są stosowane przez ludzi lub grupy, zawodowo zajmujących się hackingiem w celach komercyjnych. Celem jest przechwycenie lub kradzież ściśle określonych danych zamawianych przez ich klientów (np. nielegalny handel danymi osobowymi, danymi o partnerach handlowych). Metody ich działania są na tyle wyrafinowane że w większości przypadków są nie zauważalne a ofiarami najczęściej są instytucje i organizacje rządowe a nawet służby powołane do dbania o porządek i bezpieczeństwo kraju.

Techniki stosowane do tego rodzaju działalności można nazwać już technologią włamań. Na początku prowadzi się szeroko zakrojony rekonesans zarówno fizyczny jak i elektroniczny ale w sposób mało zwracający uwagę (np. jedni zatrudniają się jako sprzątaczki a inni nawiązują kontakty towarzyskie a jeszcze inni prowadzą wywiad elektroniczny). Następnym krokiem będzie badanie celu ataku i rozpoznanie wszystkich rodzajów zabezpieczeń poprzez bezpośrednie interakcję z celem ataku ale poprzez maszyny z jakiegoś egzotycznego kraju lub już opanowane maszyny które dla atakowanego systemu są uważane za zaufane. Tego rodzaju działania dobry administrator powinien już zauważyć i poczynić pewne kroki w celu dobrego przygotowania się na ewentualny atak. Po tym etapie działań następuje „cisza przed burzą" i w czasie tej „ciszy" poddaje się analizie wszystkie zdobyte informacje na temat celu ataku i zostaje opracowany dokładny plan ataku. Następnie faza zbierania i tworzenia specjalnie pod tą „okazję" oprogramowania i prowadzenia symulacji. Po zakończeniu tego etapu następuje atak na cel.

Może on przyjmować formę ataku bezpośredniego w którym w krótkim czasie zostaję przejęta kontrola nad systemem jeszcze nim zdąży to zauważyć administrator i następują wszelkie działania maskujące atak przed administratorem a w międzyczasie wyprowadzane są dane. Po wyprowadzeniu danych maskowana są wszelkie operacje jakie zostały przeprowadzone przez włamywaczy na danym systemie i opuszczają bezzwłocznie system. Ataki takie są prowadzane z komputerów najczęściej będące poza granicami kraju w którym znajdują się włamywacze i cel ataku oraz została już wcześniej przejęta nad nimi kontrola a po ataku zawartość ich pamięci zostaje wyzerowana.

W przypadku dobrze zabezpieczonych systemów stosowana jest metoda stopniowego pozyskiwania uprawnień. Pierwsza faza tej metody bazuje na niskiej świadomości użytkowników systemu i polega na wprowadzenia na stację użytkownika lub użytkowników specjalnego oprogramowania będącego po trochę wirusem, po trochę koniem trojańskim własnej produkcji najczęściej poprzez pocztę lub płyty CD. Ten specjalny program potrafi systematycznie pozyskiwać lub zdobywać uprawnienia aż do momentu zdobycia wszystkich interesujących intruza uprawnień. Oprócz tego potrafi wykonywać wiele ciekawych sztuczek jak na przykład przechwytywanie wszelkich haseł i wysyłanie ich do włamywaczy, rekonfigurowanie systemów zabezpieczeń, kopiowanie danych aż nawet do przejęcia zdalnej kontroli nad systemem zarządzania siecią.



Czy to na pewno jest okno logowania MSN czy może koń trojański ?

Programy te mogą być na tyle inteligentne że potrafią wykonać całość zadań związanych z atakiem, pobraniem danych, zamaskowaniem ataku i ulec destrukcji lub pozwalają na zdobycie odpowiednich uprawnień i osłabienie systemu bezpieczeństwa w celu ułatwienia ataku bezpośredniego.

10. Strategie obrony przed atakami

Jeżeli chodzi o metody administrowania systemami informatycznymi jak i mechanizmami bezpieczeństwa to możemy wyróżnić dwa zasadnicze podejścia administratorów. Pierwsze z nich nazywane jest administrowaniem reaktywnym i polega na reagowaniu na zaistniałe zdarzenia po ich nastąpieniu. Drugim z nich jest administrowanie proaktywne polegające na planowaniu, przewidywaniu i szacowaniu podatności na ataki jak i poziomu zagrożeń.

Istnieje parę rodzajów strategii obrony przed atakami.

Pierwsza z nich polega na pasywnym odparciu ataku poprzez mechanizmy bezpieczeństwa. Strategia ta pozwala na skuteczne odparcie ataku poprzez zablokowanie atakującej maszyny ale nie przeciwdziała próbom następnych ataków prowadzonymi tymi samymi metodami lub przez te same maszyny.

Następna metoda polega na odparciu ataku ale pozwala zrobić rekonesans jeżeli chodzi o źródło ataku jak i sygnatury ataku. Strategia ta pozwala uczyć system ochrony jak przeciwdziałać próbom następnych podobnych ataków oraz zbiera wszelkie informację potrzebne organom ścigania. Najbardziej profesjonalnymi metodami obrony są metody „wpuszczenia w maliny" i ataku zwrotnego. Metody te stosuję się przeciwko profesjonalnym atakom w których nie ma możliwości namierzenia włamywacza poprzez zwykłe metody.

Metoda „wpuszczania w maliny" polega na tym że system bezpieczeństwa wykrywa atak i przełącza intruza na spreparowaną specjalnie do tego celu infrastrukturę IT umożliwiając pobranie spreparowanych danych które mają dezinformować. Włamywacz jest oczywiście niczego nie świadomy i dostarcza skradzione dane swojemu klientowi. Następnie oczekuję się kto będzie wykorzystywał te spreparowane dane i do jakich celów.

Metoda ataku zwrotnego jest najbardziej wyrafinowaną obroną przed atakami i umożliwia zarówno namierzenie włamywacza w bezpośredni sposób i udaremnienie w odpowiedniej chwili włamania. Polega na tym że podczas próby ataku którą wykrywamy niemal nie zwłocznie, nasz system przeprowadza atak na maszyny atakujące w celu pobrania z nich różnych „ważnych i ciekawych" informacji i bez względu czy maszyny atakujące nasz system są maszynami włamywacza czy tylko „użyczonymi" przez niego uzyskujemy cenne informacje oraz istnieje możliwość zniszczenia zarówno maszyn włamywacza jak i maszyn pośredniczących w ataku. Wszystkie te działania są wykonywane wtedy gdy włamywacz usiłuje penetrować nasz system i niczego się nie spodziewa. Metodę tę często łączy się z metodą „wpuszczania w maliny". Na ogół te dwie ostatnio prezentowane metody eliminuję włamywacza lub grupę włamywaczy z „rynku" poprzez ujawnienie publiczne zarówno osób dokonujących włamania jak i klientów korzystających z tego rodzaju usług.

11. Odniesienie zagrożeń do modelu OSI

Efekt Domino - jeżeli bezpieczeństwo jednej z warstw zostanie przełamane, transmisja przestaje by bezpieczna ...

OSI	CEL ATAKU	METODY i SKUTKI ATAKU	METODY OCHRONA
L1	hasła BIOS komputerów i hasła urządzeń (np.: router, switch, FW, IDS, AP)	możliwość usunięcia sprzętowo lub programowo a nawet możliwość programowego znalezienia i rozkodowania	fizyczna ochrona pomieszczeń i samego sprzętu, stosowanie silnych bezpiecznych haseł
	partycje dyskowe (np.: NTFS, EXT2, EXT3, NWFS, NSS)	odczytywanie partycji spod poziomu innego systemu operacyjnego lub innej maszyny daje możliwość uzyskania danych, plików z hasłami, certyfikatów i kluczy, na skutek ominięcia kontroli praw dostępu	fizyczna ochrona pomieszczeń, samego sprzętu i dysków
			szyfrowanie systemu plików
	urządzenia peryferyjne (np.: CD/DVD, RHDD, FDD, ZIP)	możliwość wprowadzania jak i wyprowadzania nielegalnych danych i programów	kontrolowany dostęp do urządzeń peryferyjnych i wejść/wyjść komputera
	serwery usług (np.: plików, drukarek, WWW, poczty, FTP)	zablokowanie lub unieruchomienie serwera usług i podstawienie serwera który udaje serwer usług i autoryzuje próby dostępu co umożliwia pozyskanie haseł.	fizyczna ochrona budynku, pomieszczeń i samego sprzętu, autoryzacja do portu w warstwie L2
	certyfikaty i klucze	kradzież poprzez fizyczny dostęp do plików zawierających certyfikaty i klucze	fizyczna ochrona pomieszczeń, samego sprzętu i dysków, kontrolowany dostęp do urządzeń peryferyjnych, , zabezpieczenie kluczy i certyfikatów hasłem (szyfrowanie w magazynie certyfikatów)
		wykorzystanie ich na opanowanych maszynach w celu podpisywania dokumentów	
	dokumentacja sieci komputerowej, usług i serwerów	skopiowanie lub fizyczna kradzież w celu niepożądanego wykorzystania	fizyczna ochrona pomieszczeń i szaf w których jest przechowywana dokumentacja
	kopie zapasowe danych	skopiowanie lub fizyczna kradzież w celu uzyskania danych, plików z hasłami, certyfikatów i kluczy szyfrujących	fizyczna ochrona pomieszczeń i szaf w których jest przechowywana kopia zapasowa
			kopia zapasowa powinna być przechowywana w pewnej odległości od maszyn na których są oryginalne dane ze względu na klęski żywiołowe lub działania terrorystyczne
	sieć komputerowa, architektura LAN i WAN	podstawienie urządzenia przewodowych jak i bezprzewodowych oraz radiowych wewnątrz atakowanego systemu w celu uzyskania dostępu	fizyczna ochrona budynku, pomieszczeń, sprzętu, tuneli kablowych, szaf dystrybucyjnych, autoryzacja do portu w warstwie L2, dynamiczne klucze szyfrowania dla bezprzewodowych
		podstawienie urządzenia przewodowych jak i bezprzewodowych oraz radiowych wewnątrz atakowanego systemu w celu analizy ruchu i przechwytywania danych	
	dyski twarde i macierze dyskowe serwerów	fizyczna kradzież tych podzespołów lub dobranie się do nich z pod poziomu innego sprzętu lub systemu operacyjnego w celu uzyskania danych, plików z hasłami, certyfikatów i kluczy szyfrujących	fizyczna ochrona budynku, pomieszczeń i samego sprzętu
		zniszczenie lub uszkodzenie fizyczne	kopia zapasowa
		naprawa, kasacja lub zbycie dysków lub macierzy	w przypadku oddawanie do naprawy, kasacji lub zbycia należy usunąć dane w sposób uniemożliwiający ich odtworzenie
	urządzenia sieciowe i okablowanie	awarie, przerwanie okablowania lub rozłączenie, kradzież	fizyczna ochrona tuneli kablowych, szaf dystrybucyjnych, sprzętu
			bezpieczne systemy zasilanie

	urządzenia zasilające	awarie, kradzieże, uszkodzenia połączeń	fizyczna ochrona pomieszczeń w których znajdują się urządzenia zasilające
			zabezpieczenia zwarciowe przeciwprądowe, przepięciowe, agregaty prądotwórcze, akumulatory, przetwornice
	urządzenia osobiste : laptopy, komunikatory	kradzież, zniszczenie, dobieranie się w celu uzyskania danych, plików z hasłami, certyfikatów i kluczy szyfrujących	ochrona fizyczna urządzenia, autoryzacja w systemie operacyjnym, szyfrowanie ważnych danych
	monitory	przechwytywanie promieniowania elektromagnetycznego urządzeń prezentujących dane	ekranowanie pomieszczeń i budynków w których pracują monitory prezentujące krytyczne dane
		przechwytywanie obrazu poprzez kamery systemu monitoringu budynku jak i zainstalowane celowo do tego celu	ochrona fizyczna pomieszczeń i ustawianie monitorów w sposób uniemożliwiający obserwowanie go przez kamery monitoringu
	telefony IP - przewodowe - software-owe - bezprzewodowe	nieautoryzowane podłączenia	stosowanie VLAN-ów głosowych, autoryzacja użytkownika oparta o RADIUS, TACACS, autoryzacja do portu L2 i VLAN-u
		nielegalne korzystanie	
		podsłuchiwanie rozmów – VOMIT. Większość urządzeń telefonii IP nie wspiera mechanizmów ochrony poufności przesyłanych informacji	
	sieci SAN	dedykowane ataki na SAN, umożliwiające przechwytywanie i manipulowanie danymi dostępnych na mediach magneto-optycznych (np. macierzach, bibliotekach masowych)	ochrona logiczna i fizyczna sieci SAN oraz urządzeń SAN
	sieci NAS	ataki na sieć LAN są zagrożeniem dla danych przesyłanych do urządzeń pamięci masowych	ochrona fizyczna i logiczna sieci LAN i WAN wraz z urządzeniami NAS
	konsole urządzeń	pozostawione bez opieki i zabezpieczenia przed nielegalnym użyciem	ochrona fizyczna pomieszczeń, automatyczne blokowanie konsoli na której wykrywany jest brak działań
L2	VLAN	uzyskanie dostępu do innych grup roboczych, urządzeń i przywilejów w warstwach L2 i L3	odpowiednia architektura warstwy L2, prawidłowa konfiguracja separacji grup roboczych oraz kanałów głosowych i danych
		uzyskanie dostępu do kanałów głosowych w celu podsłuchu lub nielegalnego dostępu	
	FR VPN	ataki na certyfikaty i klucze szyfrujące	odpowiednia architektura warstwy L2, silna ochrona dostępu do certyfikatów i kluczy
	ATM VPN	ataki na certyfikaty i klucze szyfrujące	
	WLAN	uzyskanie dostępu	uwierzytelnianie portu przełącznika
			dynamiczne klucze szyfrowania ramek
	adresy MAC	podszywanie się pod adresy MAC w celu skorzystania z relacji zaufania jakie są realizowane na warstwach L2	odpowiednia architektura warstwy L2, fizyczna ochrona pomieszczeń, łączy, szaf dystrybucyjnych i urządzeń, VLAN, uwierzytelnianie do portów L2
	Ethernet	odmowa usług lub zakłócenia w działaniu	odpowiednia architektura warstwy L2, uwierzytelnianie do portów L2
		analiza ruchu i przechwytywanie ramek	przełączniki, VLAN, VPN
	grupy robocze	uzyskanie nieautoryzowanego dostępu do innych grup roboczych warstwy L2	VLAN i trasowanie w warstwie L3 pomiędzy grupami roboczymi
	STP	drzewa i zapętlenia powodujące DoS na L2	odpowiednia architektura warstwy L2, ochrona fizyczna urządzeń przełączających i trasujących oraz ochrona na poziomie sytemu operacyjnego
	ARP	zmiana odwzorowań adresów MAC na adresy IP w tablicy urządzenia przełączającego lub trasującego w celu uzyskania dostępu	
	PVC i SVC	przechwytywanie kanałów lub zmiana punktów końcowych na zwrotnicach FR i ATM w celu przechwycenia danych	ochrona fizyczna zwrotnic i na poziomie systemu operacyjnego
L3÷L4	identyfikatory i hasła do usług sieci	poprzez podsłuchanie nieszyfrowanej ich transmisji	szyfrowanie na poziomie aplikacji
	dane		szyfrowanie na poziomie sieci
			stosowanie VLAN-ów
	sieć, architektura	zablokowanie lub ograniczenie funkcjonalności atakami DoS	odpowiednia architektura warstwy L3, stosuję się wiele metod równocześnie np.: limitowanie transmisji, filtrowanie pakietów, rozwiązywanie nazw
		penetracja i skanowanie sieci i usług (skanowanie warstwy L3 i L4)	ściany ogniowe poziomu aplikacji
			translacja adresów i portów

			mechanizmy wykrywające skanowanie, NIDS
		dystrybucja szkodliwego oprogramowania	programy antywirusowe
		zapychanie pakietami aplikacji P2P	odpowiednia architektura warstwy L3, zarządzaniem pasmem sieciowym w warstwach od L2 po L7
		niepowołany dostęp	ściany ogniowe, NIDS, systemy autoryzacji
		szkodliwe pakiety	HIDS i NIDS
		podszywanie się za stacje zarządzające przy pracy na nie szyfrowanych wspólnych łączach	odpowiednia architektura warstwy L3, tworzenie tablic maszyn które są uprawnione do zarządzania danymi urządzeniami
	adresy IP	podszywanie się pod adresy IP w celu skorzystania z relacji zaufania jakie są realizowane na warstwach L3	odpowiednia architektura warstwy L3, fizyczna ochrona pomieszczeń, łączy, szaf dystrybucyjnych i urządzeń, VLAN, uwierzytelnianie do portów L2, kontrolowanie adresów IP w sieci
	FW	próby omijania i oszukania tych urządzeń, próby wyłączenia lub zablokowania tych urządzeń	odpowiednia architektura warstwy L3
	IDS		filtracja właściwych adresów i pakietów w warstwie dystrybucyjnej i dostępowej
			szacowanie odporności na ataki
			fizyczna ochrona urządzeń, szaf dystrybucyjnych, łączy
	VPN	ataki służą pozyskaniu kluczy szyfrujących i na ich podstawie odszyfrowaniu przechwyconych danych lub zestawianie tuneli	ochrona fizyczna jak i elektroniczna certyfikatów i kluczy szyfrujących
	routing	zmiany w tablicach trasowanie mogą spowodować spowolnienie sieci lub nawet jej zablokowanie poprzez nieokreślone zmiany tras a także do przeprowadzania ataków przez ściany ogniowe	odpowiednia architektura warstwy L3, ochrona fizyczna pomieszczeń i routerów oraz ochrona spod poziomu systemu operacyjnego routera, monitorowanie tablic trasowania
	porty TCP i usług	poprzez translację portów TCP możemy wyprowadzać lub wprowadzać ruch który jest ograniczony odpowiednimi mechanizmami bezpieczeństwa takimi jak ściana ogniowa, sterowanie przepustowością czy IDS-y	odpowiednia architektura warstwy L3, kontrola i monitorowanie na poziomie L4 używanych portów TCP zarówno przez serwery, stacje robocze jak i inne urządzenia warstwy L4
	wydajność sieci	aplikację P2P stosowane do wymiany plików multimedialnych (np.: mp3, mpg, jpeg) mogą pożerać całe pasmo sieciowe i uniemożliwiać pracę normalnym użytkownikom	odpowiednia architektura warstwy L3, stosowanie usług QoS na warstwach od L2 do L7
L5÷L7	hasła plików (np.: dokumentów, arkuszy, plików spakowanych, zaszyfrowanych)	istnieją techniczne możliwości znalezienia hasła lub odczytania dokumentu zahasłowanego	szyfrowanie plików zarówno składowanych jak i przesyłanych
	bazy danych użytkowników sieciowego systemu operacyjnego i urządzenia (np.: NDS, ADS, IOS, NIS/YP)	w każdym systemie operacyjnym muszą istnieć pliki w których zapisana jest baza danych użytkowników, ich hasła, uprawnienia i inne istotne rzeczy. W bazach tych oprócz przechowywania własnych haseł mogą być przechowywane identyfikatory i hasła dostępu do innych systemów operacyjnych, baz danych jak i innych urządzeń sieci. Bazy te są z reguły szyfrowane i zabezpieczone przed skopiowaniem lub podejrzeniem. Istnieją dwie metody na ominiecie tego typu przeszkody. Pierwsza z nich polega na podmianie lub uszkodzeniu tych plików i w ten sposób uzyskanie nielegalnego dostępu a druga pozwala na dobranie się, rozkodowanie tych plików i uzyskanie z nich istotnych informacji.	fizyczna ochrona pomieszczeń i sprzętu,
			ochrona tych plików z pod poziomu systemu operacyjnego
	bazy danych użytkowników mających dostęp do serwerów baz danych SQL (np.: Oracle, SQL Server, InterBase, MySQL, Access)	o ile autoryzacja do bazy danych nie jest prowadzona w oparciu o system operacyjny to system bazy danych posiada pliki w których zapisana jest baza danych użytkowników, ich hasła, uprawnienia i inne istotne rzeczy. Pliki te są szyfrowane, jednakże są swobodnie widzialne przez system operacyjny serwera i nie ma żadnych przeszkód aby je skopiować i rozkodować ale najlepszym sposobem jest ich podmiana na spreparowane odpowiednio przez włamywacza własne pliki.	fizyczna ochrona pomieszczeń i sprzętu

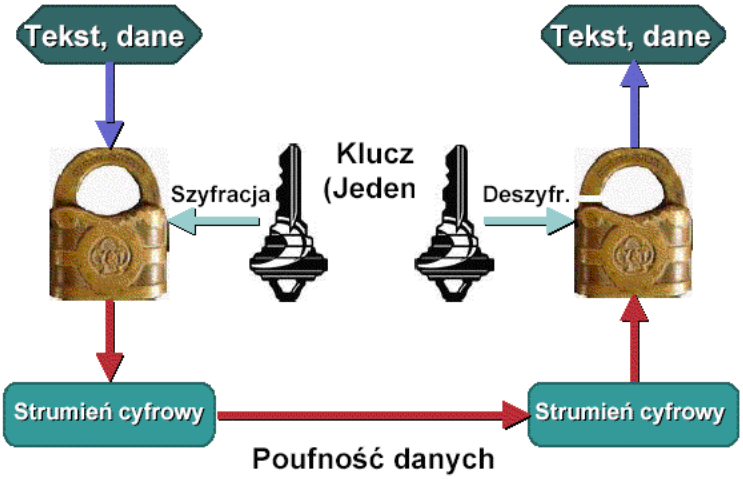
			ochrona tych plików z pod poziomu systemu operacyjnego
	bazy danych użytkowników mających dostęp do usług sieci (np.: WWW, poczta, FTP, chat, zdalny dostęp)	podobnie jak w przypadku baz danych użytkowników systemu operacyjnego, (o ile autoryzacja jest prowadzona o własne mechanizmy), tak i usługi posiada pliki w których zapisana jest baza danych użytkowników, ich hasła, uprawnienia i inne istotne rzeczy. Pliki te są swobodnie widzialne przez system operacyjny serwera i nie ma żadnych przeszkód aby je skopiować i rozkodować ale najlepszym sposobem jest ich podmiana na spreparowane odpowiednio przez włamywacza własne pliki.	fizyczna ochrona pomieszczeń i sprzętu
			ochrona tych plików z pod poziomu systemu operacyjnego
	programy i biblioteki	celowa zmiana kodu źródłowego programów lub bibliotek aby mogły wykonywać niepożądane z punktu widzenia użytkownika funkcje	fizyczna ochrona sprzętu
		zmiany w programach prowadzących autoryzację lub ich podmiana w celu realizacji zadań służących ujawnieniu haseł	instalacja oprogramowania z pewnych źródeł, kontrolowana instalacja oprogramowania,
			audyt na poziomie kodu źródłowego programów
	luki w systemach operacyjnych	luka jest dowolnym sprzętowym lub programowym defektem systemu, który umożliwia włamywaczowi uzyskanie nielegalnego dostępu. Zjawisko występowania luk dotyczy nie tylko oprogramowania komputerów ale także takich urządzeń dedykowanych jak routery, switche, firewall.	śledzenie zarówno informacji od producentów i dostawców oprogramowania i sprzętu jak i pozyskiwanie informacji ze źródeł niezależnych na temat luk
			jak najszybsza instalacja uaktualnień i pakietów naprawczych
	narzędzia bezpieczeństwa (np.: FW, AV, IDS)	wyłączenie ich, deaktywacja ich funkcji, zmiana konfiguracji	monitorowanie wszelkich prób restartów i zmiany konfiguracji urządzeń służących zwiększaniu bezpieczeństwa
		szyfrowanie danych i programów w celu ich wprowadzenia lub wyprowadzenia z sieci	monitorowanie i kontrolowanie szyfrowania
	system operacyjny serwera	infekcja wirusami, robakami i koniami trojańskimi w celu zniszczenia danych przetwarzanych przez dany system, ograniczenia funkcjonalności a nawet przejęcia zdalnej kontroli	programy antywirusowe, HIDS, zapory ogniowe różnych poziomów
	system operacyjny stacji roboczej		
	system operacyjny urządzenia sieciowego	zmiana konfiguracji wpływająca na realizowane funkcje przez urządzenie oraz monitorowanie sieci	ochrona z pod poziomu systemu operacyjnego, kontrola zmian konfiguracji i restartów urządzeń
	systemy zarządzania siecią (np.: SMNP, telnet, r*)	większość narzędzi i protokołów do zarządzania siecią, serwerami i urządzeniami stosuje protokoły nie posiadające żadnych zabezpieczeń zarówno jeżeli chodzi o przechwycenie hasła i danych jak i systemu uwierzytelniania	stosowania do zarządzania dedykowanych łączy OOB
			szyfrowanie transmisji zarządzających EIB
	oprogramowanie	skasowanie lub kradzież	kopie zapasowe i ochrona na poziomie systemu operacyjnego oraz szyfrowanie danych
	dane	usuniecie lub kradzież	
	hasła konsoli	wyciągnięcie hasła z systemu operacyjnego, z systemy plików lub podsłuchanie	ochrona na poziomie systemu operacyjnego i systemu plików
	aplikacje	możliwość użycia aplikacji przez agresora w celu wykonania operacji na systemie	powinny być zabezpieczone hasłem i poziomem uprawnień
	bazy danych	wprowadzanie, modyfikacja, wyprowadzanie, kasowanie danych i obiektów z pod poziomu języka SQL poprzez aplikacje natywne lub poprzez serwery WEB współpracujące z bazami danych	obiektu baz danych i dane powinny być zabezpieczone na każdym poziomie przez system zarządzania bazą danych niezależnie od zabezpieczeń aplikacji
	obiekty baz danych		dzienniki transakcji i inspekcja określonych zdarzeń w bazie dabych
	SNMP	słabe zabezpieczenia i brak szyfrowanie	dedykowane łącza lub szyfrowanie oraz uwierzytelnianie na poziomie L3
			stosowanie trudnych nazw społeczności
			stosowanie innych nazw społeczności przy odczycie i zapisie

	DNS	fałszowanie wpisów wskazujące na inne urządzenia	ochrona na poziomie systemu operacyjnego i systemu plików, uwierzytelnianie wszystkich urządzeń na poziomie L2
	DHCP	nadawanie nielegalnych adresów IP w celu uzyskania dostępu do maszyny w tym adresem	
	WWW, CGI, DSO, ISAPI, NSAPI	uruchamianie szkodliwego oprogramowania pod kontrolą serwerów WWW	audyt na poziomie kodu źródłowego programów
			ochrona na poziomie systemu operacyjnego
	dane multimedialne	przechwytywanie głosu, obrazu	fizyczna ochrona sprzętu i łączy
	iSCSI	ataki na macierze SAN i biblioteki masowe, systemy hot-backup, przełączniki SAN w celu przechwytywania danych zapisywanych na nośnikach	ochrona fizyczna i logiczna sieci SAN
	serwery czasu	fałszowanie czasu w celu rozsynchronizowania sieci i podrabiania znaczników czasu	niezależne źródło dokładnego czasu oraz synchronizacja
	serwery logów	fałszowanie wpisów mających za zadanie maskowanie ataków lub prób nielegalnego dostępu	ochrona z pod poziomu systemu operacyjnego i systemu plików
			najlepiej umieszczać ten serwer na osobnych maszynach
	usługi	pobieranie informacji (skanowanie usług) o oprogramowaniu obsługującym dane usługi i jego wersji	zablokowanie podawania szczegółowych informacji lub podawanie spreparowanych
		złożoność aplikacji świadczących usługi powoduje iż są one narażone na błędy ludzkie	wnikliwa analiza zasad działania i zasad konfiguracji aplikacji usług
L8 (czynnik ludzki)	błędy w konfiguracji mechanizmów zabezpieczających	błędy w konfiguracji mogą powodować tworzenie się luk w tych systemach (np.: FW, IDS, AV, WWW, poczta, FTP, BGP, prawa dla plików, user-ów, grup i obiektów)	należy dokładnie przemyśleć koncepcję konfiguracji oraz poddać ją symulacjom i próbom
	hasło administratora i hasła użytkowników	patrzenie na ręce administratora lub użytkownika podczas próby logowania się	administrator nie powinien logować się z prawami administracyjnymi na innych stacjach niż do tego wydzielone lub stosowanie haseł jednorazowych
			zwracać uwagę na wszelkie formy podglądania np.: lusterka, kamery
		programy przechwytujące kody klawiatury (podstawienie programu zapisującego po wystąpieniu określonego zdarzenia jakie klawisze i w jakiej kolejności były naciskane np. podczas logowania)	administrator nie powinien logować się z prawami administracyjnymi na innych stacjach niż do tego wydzielone lub stosowanie haseł jednorazowych
			kontrola instalowanego oprogramowania
		zgadywanie łatwych haseł	kontrolowanie tworzonych haseł z pod poziomu systemu operacyjnego lub dodatkowych programów do tego służących.
			stosowanie się do polityki haseł
	administrator	doprowadzenie administratora do paranoi w tworzeniu zabezpieczeń co sprzyja wielu pomyłkom otwierającym „tylne drzwi”	wszelkie działania dotyczące rekonfiguracji dobrze działającego systemu zabezpieczeń powinny być dobrze przemyślane i poddane symulacjom
			nie należy przesadzać z zabezpieczeniami
	czas i wydajność pracy	działania w Internecie nie zawsze są związane z wykonywaną pracą. Wielu użytkowników większość czasu spędza na rozrywkach	stosować oprogramowanie do kontrolowania, monitorowania i rejestrowania działań użytkowników w Internecie
		działania na komputerach nie zawsze są związane z wykonywaną pracą. Wielu użytkowników większość czasu spędza na rozrywkach	stosować oprogramowanie do kontrolowania, monitorowania i rejestrowania działań użytkowników na stacjach roboczych
	ekran logowania	podstawienie nielegalnego ekranu logowania	kontrolowany dostęp do stacji, programy antywirusowe, HIDS, ściany ogniowe
	zdalny dostęp	należy z rozwagą używać programy pozwalające na przejmowanie zdalnej kontroli szczególnie na sieciach WAN, gdyż istnieje możliwość posłuchu haseł, danych a także przechwycenia sesji	szyfrowanie transmisji oraz stosowanie programów znanych i renomowanych producentów

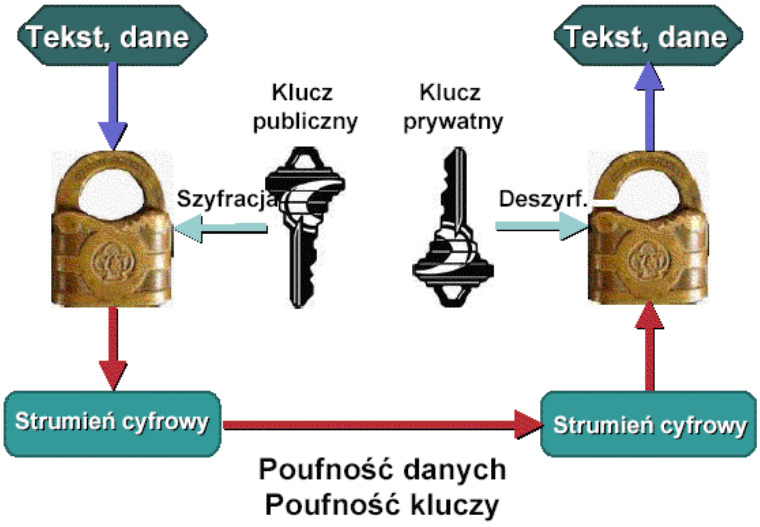
12. Szyfrowania w poszczególnych warstwach modelu OSI i systemie plików

Szyfrowanie możemy podzielić na symetryczne i asymetryczne. Symetryczne zapewnia poufność danych i odbywa się w oparciu o ten sam klucz służący do szyfrowania i deszyfrowania. W szyfrowaniu asymetrycznym możemy zapewnić poufność jak i integralność danych i mamy do czynienia z dwoma kluczami: publicznym (dostępnym dla nadawców i odbiorców) i prywatnym (dostępnym tylko dla właściciela).

Schemat szyfrowania symetrycznego



Schemat szyfrowania asymetrycznego



Każde szyfrowanie nawet na urządzeniach sprzętowych powoduje spadek wydajności przesyłania danych od 3 do 15 razy w zależności od szybkości transmisji (im szybkość transmisji jest większa tym spadek wydajności związany z szyfrowaniem rośnie)

Ze względu na to że algorytmy asymetryczne potrafią być do 400 razy wolniejsze od symetrycznych możliwe jest szyfrowanie z używaniem dwóch algorytmów symetrycznego i asymetrycznego. Algorytm asymetryczny służy do wymiany kluczy symetrycznych a następnie szyfruje się kluczami symetrycznymi. W ten sposób zyskujemy poufność i integralność kluczy symetrycznych, poufność danych i znacząco większą szybkość transmisji.

Należy też brać pod uwagę to że szyfrowanie programowe jest co najmniej o 10 razy wolniejsze od sprzętowego dlatego przy dużych transferach danych wymagających szyfrowania należy stosować urządzenia sprzętowe do tworzenia tuneli szyfrowanych.

Szyfrowanie w poszczególnych warstwach sieciowych

- szyfrowanie transmisji w warstwie aplikacji [L7] (SSL, podpis cyfrowy)

szyfrowanie w warstwie aplikacji wymaga aby obie komunikujące się ze sobą strony wspierały ten sam rodzaj szyfrowania. Większość protokołów warstwy aplikacji nie zostało zaprojektowanych z myślą o szyfrowaniu danych dlatego chcąc stosować tę metodę zwiększania integralności i poufności danych zarówno programy klienckie jak i oprogramowanie serwerów musi ulec stosownym modyfikacjom. Jednak nie zawsze istniej taka możliwość szczególnie jeżeli chodzi o usługi takie jak telnet, poczta czy ftp.

W przypadku usług WWW zarówno wszystkie najbardziej popularne serwery jak i przeglądarki mają zaimplementowane mechanizmy które umożliwiają obustronne rozpoznanie się i bezpieczną komunikację w architekturze klient-serwer. Jeżeli certyfikatem SSL dysponuje tylko serwer WWW to przedstawia się on nam swoim certyfikatem i przesyła swój klucz publiczny którym będziemy szyfrować wszystkie dane opuszczające naszą przeglądarkę do momentu ustalenia klucza sesyjnego. W przypadku gdy certyfikatami SSL dysponują obie strony to serwer WWW dodatkowo może rozpoznać co daje najwyższy poziom bezpieczeństwa.

W przypadku poczty elektronicznej najbardziej popularną metodą zapewniającą zarówno poufność jak i integralność wiadomości jest podpis cyfrowy wraz z szyfrowaniem. Metoda ta jest realizowana na poziomie aplikacji klienckich poczty. Poufność uzyskuje się przez szyfrowanie wiadomości kluczem publicznym odbiorcy a integralność poprzez podpisywanie własnym kluczem prywatnym nadawcy. W ten sposób uzyskujemy pewność że dokument który do nas dotarł jest wysłany przez tego nadawcę, że nikt go po drodze nie zmienił i nie czytał.

W przypadku zdalnej kontroli takiej jak w przypadku programów telnet, rcp, rlogin, rsh, zostały one zastąpione pakietem SSH który składa się z klienta i serwera. Program ten posiada różne rodzaje szyfrowania zarówno haseł jak i danych co zapewnia wystarczający poziom bezpieczeństwa zarówno dla normalnej pracy jak i zadań administracyjnych.

- szyfrowanie transmisji w warstwie sieciowej [L3] (IP VPN, IPSec)

jeżeli aplikacje które wykorzystujemy nie wspierają metod zwiększających poufność i integralności lub chcemy jeszcze bardziej zabezpieczyć transmitowane dane możemy budować bezpieczne tunele. Tunele te są przeźroczyste dla aplikacji. Tunele te można podzielić na dwa rodzaje. Pierwszy z nich to tunel sieć do sieci (S2S) i pozwala on zabezpieczyć dane przesyłane przez sieci uznawane z niebezpieczne a drugi to stacja do stacji lub sieci pozwala zabezpieczyć dane przesyłane z konkretnej maszyny na konkretną maszynę lub bramę bezpieczeństwa (RA). Drugi sposób stosuje się przy zdalnym dostępie przez sieci uznawane za niebezpieczne do zasobów sieciowych znajdujących się w firmie czy instytucji.

Oprócz tego możemy wyróżnić tunelowanie transportowe i właściwe. Tunelowanie transportowe polega na tym że szyfrowaniu podlegają tylko dane pakietu warstwy L3 a we właściwym tunelowaniu, szyfrowaniu podlega cały pakiet włącznie z nagłówkiem.

- szyfrowanie transmisji w warstwie łącza danych [L2] (FR i ATM VPN, WLAN)

jest to najniższy poziom modelu OSI na którym możliwe jest tylko sprzętowe szyfrowanie i jest ono dostępne tylko dla protokołów łączy komutowanych Frame Relay i ATM oraz w sieciach WLAN.

Szyfrowanie w systemie plików

- szyfrowanie systemu plików

większość nowoczesnych systemów operacyjnych umożliwia zaszyfrowanie zarówno całego systemu plików jak i poszczególnych katalogów i plików. Istnieje też dużo programów szyfrujących niezależnych producentów które umożliwiają stosowanie różnych algorytmów szyfrujących. Szyfrowanie to zabezpiecza pliki na naszych dyskach w przypadku uzyskania przez osoby niepowołane, fizycznego dostępu do urządzenia na którym znajduje się zaszyfrowany system plików. Należy pamiętać że nie powinno się szyfrować dysków/partycji na których znajduje się system operacyjny ze względu na spowolnienie spowodowane operacjami szyfrowania jak i odszyfrowywania oraz w przypadku awarii systemu operacyjnego może uniemożliwić jego naprawę i odzyskanie danych.

- szyfrowanie baz danych

niektóre systemy baz danych umożliwiają szyfrowanie plików z danymi co w przypadku ważnych danych może być uzasadnione ale powoduje to znaczące obniżenie wydajności bazy danych. Rozwiązania te są stosowane sporadycznie.

- szyfrowanie dokumentów

najbardziej rozpowszechnione jest szyfrowanie plików zawierających ważne dane. Ten rodzaj szyfrowania może realizować system operacyjny, aplikacja która przetwarza dany dokument lub inne programy do szyfrowanie.

Wszelkie problemy związane z bezpieczeństwem zarówno szyfrowanej transmisji danych jak i przechowywania szyfrowanych danych biorą się przeważnie z faktu że zostały ujawnione lub skradzione certyfikaty i/lub klucze. Certyfikaty i klucze są częstym celem ataków na systemy w których funkcjonuje szyfrowanie gdyż przełamanie tych systemów w inny sposób jest szczególnie trudne dlatego należy zwracać szczególną uwagę na miejsca gdzie są przechowywane zarówno w systemie plików jak i na kopiach zapasowych.

Należy pamiętać że szyfrowanie danych (zarówno podczas transmisji jak i składowania) może powodować obniżenie bezpieczeństwa. Szkodliwe oprogramowanie może niepostrzeżenie przedostawać się do naszej sieci podczas szyfrowanej transmisji na poziomie aplikacji lub w postaci zaszyfrowanej, przez co nie jest rozpoznawane przez sieciowe mechanizmy bezpieczeństwa. Również ważne dane mogą zostać wyprowadzone podczas szyfrowanej transmisji na poziomie aplikacji lub/i w postaci zaszyfrowanej co uniemożliwia ich identyfikację przez systemy kontroli zawartości przesyłek. Dlatego należy kontrolować dostęp użytkowników oraz maszyn do mechanizmów szyfrowania transmisji jak i programów szyfrujących składowane dane.

13. Problemy bezpieczeństwa w sieciach przemysłowych

Tradycyjne sieci przemysłowe oparte o takie metody dostępu do łącza jak : TOKEN-BUS, MASTER-SLAVE czy PDK (*przykładowy schemat w dodatkach do niniejszej pracy*) nie posiadają wielowarstwowych mechanizmów ochrony.

W sieciach tych brak jest jakichkolwiek mechanizmów aktywnej i pasywnej ochrony sieci takich jak :
- filtracja i inspekcja ruchu w sieci
- wykrywanie szkodliwych działań
- autoryzacja urządzeń i użytkowników
- integralność i poufność przesyłanych danych
- bezpieczne zarządzanie zarówno lokalne jak i zdalne
- rejestracja zdarzeń zachodzących w sieci jak i na urządzeniach

Jedyny poziom zabezpieczeń jakie można zastosować to fizyczna ochrona sprzętu i łączy polegająca na :
- kontrolowanym i monitorowanym dostępie do pomieszczeń
- fizycznej ochronie sprzętu : węzłów systemu, urządzeń zdalnej transmisji, stacji kontrolno-nadzorczych
- fizycznej ochronie tuneli kablowych : magistral sterowników, magistral kontroli urządzeń
- określonej ochronie dokumentacji sieci i urządzeń

Tradycyjne sieci przemysłowe możemy uznać za niebezpieczne ponieważ wystarczy przełamać tylko poziom zabezpieczeń fizycznych aby uzyskać pełny i nieograniczony dostęp zarówno do sieci jak i urządzeń oraz aplikacji na nich działających. W przypadku uzyskania dostępu np. do kabla magistrali sterowników lub magistrali kontroli urządzeń, może spowodować zatrzymanie lub zakłócanie pracy urządzeń lub danego segmentu sieci, zmienić konfigurację, podstawić dodatkowe urządzenia, fałszować informację przesyłane siecią i wiele innych szkodliwych działań.

Nowoczesne sieci przemysłowe (Industrial Ethernet) oparte o protokoły Ethernet i TCP/IP, (*przykładowy schemat w dodatkach do niniejszej pracy*) umożliwiają zapewnianie bezpieczeństwa zarówno komunikacji sieciowej jak i zarządzania, dzięki wielowarstwowemu mechanizmowi ochrony. W tego rodzaju sieciach istnieje możliwość zastosowanie wszelkich mechanizmów ochronnych przewidzianych dla sieci korporacyjnych co ułatwia nam ich integrację z nowoczesnymi sieciami przemysłowymi w jednolitą sieć w której działają jednolite mechanizmy ochrony. Wyżej wymieniona integracja ułatwia sprawne zarządzanie i monitorowanie mechanizmami zwiększającymi bezpieczeństwo całego systemu informatycznego.

Architektura Industrial Ethernet umożliwia nam stosowanie szerokiego spektrum mediów komunikacyjnych co może wpływać na podwyższenie bezpieczeństwa na poziomie ochrony fizycznej (np.: zastosowanie światłowodu czy łączy bezprzewodowych) a także zwiększyć zasięg dla stacji zarządzająco-monitorujących mechanizmy ochrony.

14. Uwagi końcowe

Komputery i systemy informatyczne mają zastosowania w każdej gałęzi gospodarki i stają się niezastąpionymi elementami nawet w tak strategicznych dziedzinach jak energetyka, gazownictwo, dostarczanie wody, transport, media, finanse i bankowość, medycyna, systemy alarmowe i wiele innych. Dlatego problemy zagrożeń dla systemów informatycznych są sprawą ważną nawet w aspekcie bezpieczeństwa narodowego, gdyż nietrudno sobie wyobrazić skutki włamania do wyżej wymienionych systemów w kontekście zamachu terrorystycznego. Skutki takiego zamachu mogą być o wiele bardziej dotkliwe niż jakiekolwiek działania terrorystyczne do tej pory spotykane.

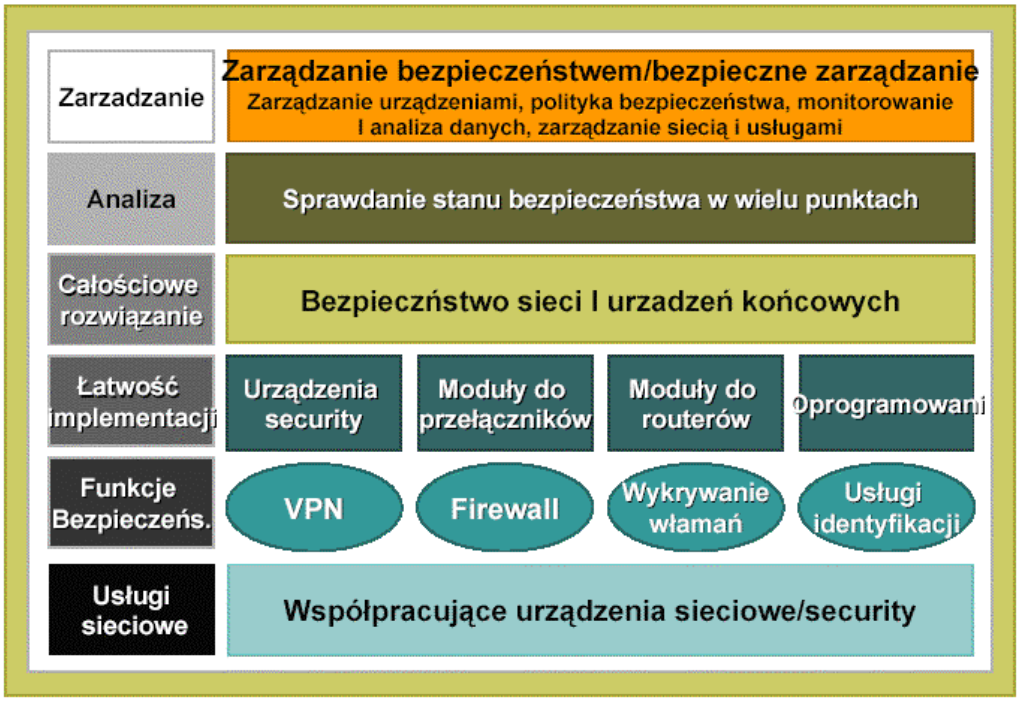
Twórcami wirusów są ludzie znający się bardzo dobrze na systemach operacyjnych oraz umiejący biegle programować. Część z nich pisze wirusy aby się wykazać że są dobrymi programistami inni robią to ze względów ideowych a jeszcze inni w ramach zemsty. Powodów dla których są tworzone wirusy jest tak wiele jak ich autorów. Twórcy wirusów bazują na niskiej świadomości ludzi wykorzystujących komputery do zabawy, rozrywki i pracy - gdyż bez „pomocy" zwykłych użytkowników komputerów wirusy nie mogły by się rozprzestrzeniać a coraz większa ilość połączonych między sobą komputerów ułatwia coraz szybsze rozprzestrzenianie się wirusów. Oprócz pisania wirusów pojawił się ostatnio nowy trend na tworzenie programów przy pomocy których każdy może stworzyć wirusa. Są to tak zwane kreatory wirusów, wzorowane na kreatorach obecnych w systemach okienkowych. Kreator pozwala na wybranie typu wirusa, efektów jakie ma prezentować, rodzaju infekcji oraz warunki w jakich ma nastąpić aktywacja. Kreatory tę są o tyle niebezpieczne że pozwalają każdemu stworzyć zupełnie nowego wirusa w ciągu paru minut, nawet polimorficznego.
Dlatego każdy zwykły użytkownik powinien zaopatrzyć się dobry program antywirusowy dla swojej stacji roboczej który dla spełniania swoich funkcji powinien być zawsze włączony, dobrze skonfigurowany oraz aktualizowany najpóźniej co dwa tygodnie. A w przypadku sieci komputerowych nieodzowne stają się programy antywirusowe działające na poziomie sieci i punktów styku z sieciami zewnętrznymi.

Należy wiedzieć że programy antywirusowe powstają na podstawie „schwytanych" wirusów czyli ujawnienia wirusa przebywającego na „wolności" w początkowej fazie jego rozprzestrzeniania się (autorzy programów antywirusowych badają schwytanego wirusa i wymyślają metodę jego rozpoznawania oraz antidotum na niego gdy już doszło do infekcji). Nie ma możliwości napisania programu antywirusowego który potrafi przewidzieć jakie wirusy pojawią się na „rynku". Zazwyczaj „szczepionka" pojawia się w okresie pomiędzy fazą infekcji a fazą aktywowania jego właściwych funkcji i powinna rozprzestrzeniać się znacznie szybciej niż sam wirus. Dlatego nie ma tak naprawdę pewnych metod sprzętowo-programowych na uniknięcie niebezpieczeństwa. Pewną metodą zwiększającą pewność jest używanie wielu programów antywirusowych pochodzących z różnych stron świata (np. Polski, Europy, Ameryki i Azji) gdyż rejon świata z którego wywodzi się wirus zostanie najprędzej zainfekowany co spowoduje tam najszybsze pojawienie się antidotum. W walce z wirusami najważniejsza jest świadomość użytkowników.

Jeżeli chodzi o ataki na sieci komputerowe to może ich dokonać każdy bez względu na poziom wiedzy informatycznej. Mogą to być uczniowie, niezadowoleni pracownicy wykorzystujący do tego gotowe programy powszechnie dostępne jak i profesjonalni hackerzy, działający na zlecenie obcych rządów czy konkurencyjnych firm, którzy na okoliczność ataku opracowują własną technologię (przeprowadzają szczegółowy rekonesans, sami piszą sobie oprogramowanie do przeprowadzenia ataku, przeprowadzają atak oraz stosują techniki maskujące atak jak i uniemożliwiające ich namierzenie).

Aby skutecznie odpierać wszelkie ataki należy zaopatrzyć się w specjalizowane urządzenia sprzętowe i oprogramowanie firm które specjalizują się w produkcji rozwiązań zwiększających bezpieczeństwo.

Co powinien zawierać kompleksowy system bezpieczeństwa ?



Każdy użytkownik jak i firma czy instytucja musi być świadoma zagrożeń jakie niosą ze sobą nowe technologie zarówno wewnętrznymi jak i zewnętrznymi. Uświadomienie użytkownikom problemów występujących podczas pracy z komputerem może zapobiec wielu niebezpiecznym incydentom. W dzisiejszym świecie informacja czy dane przekładają się bezpośrednio na dochody dlatego pozyskiwanie informacji i własności intelektualnej poprzez sieci komputerowe będzie się nasilało.

Celem wszelkich działań związanych z poprawą bezpieczeństwa jest ograniczanie ryzyka do minimum. Dbanie o bezpieczeństwo jest procesem który nigdy się nie kończy a jego najsłabszym ogniwem jest czynnik ludzki - użytkownicy. Żaden nawet najlepszy system zabezpieczeń nie spełni swoich zadań jeżeli użytkownicy nie będą mieli odpowiedniej świadomości oraz gdy będą ignorować podstawowe wymogi bezpieczeństwa dotyczące użytkowania sieci. W celu zwiększenia świadomości użytkowników należy prowadzić szkolenia uświadamiające ich o czyhających niebezpieczeństwach oraz wyjaśniać ich mechanizmy.

Podsumowanie

- Poprawę bezpieczeństwa uzyskuje się zwykle kosztem wygody i efektywności pracy w sieci komputerowej dlatego też nie należy przesadzać z zabezpieczeniami.

- Naruszenie bezpieczeństwa jednego urządzenia może w sposób lawinowy narazić na niebezpieczeństwo całą resztę sieci.

- Jeżeli bezpieczeństwo jednej z warstw modelu OSI zostanie przełamane, transmisja przestaje by bezpieczna

- Relacje pomiędzy poszczególnymi urządzeniami w sieci znaczą bardzo wiele (ich zrozumienie i przechwycenie – również)

- Należy dbać o systemy autoryzacji użytkowników i urządzeń

- Szyfrowanie transmisji jak i danych nie zawsze zwiększa bezpieczeństwo

- Nieautoryzowane kanały kontroli urządzeń są potencjalnym punktem ingerencji z zewnątrz

- Aktualizuj aplikacje, systemy operacyjne i sprawdzaj kod źródłowy.

- Niewiele firm ma silną politykę bezpieczeństwa a wiele jej w ogóle nie posiada.

- Zbyt mało profesjonalistów, którzy mogą zająć się problemami bezpieczeństwa.

- Budowanie systemu bezpieczeństwa trzeba zaczynać od pierwszej warstwy modelu OSI

- Włamywaczowi najłatwiej jest zaatakować sieć której użytkownicy nie mają odpowiedniej świadomości dotyczącej bezpieczeństwa nie wspominając świadomości administratorów dlatego tak ważne są szkolenia z zakresu bezpieczeństwa.

- Nie należy w bezpodstawne twierdzenia producentów sprzętu i oprogramowania, że to co produkują jest bezpieczne. Dążenie dostawców sprzętu i oprogramowania do odniesienia korzyści materialnych poprzez wykorzystywanie niewiedzy użytkowników.

- Należy pamiętać że programy dla włamywaczy które służą do agresji są najlepszymi programami dla administratorów do sprawdzania bezpieczeństwa systemów którymi administrują a najlepszymi specjalistami ds. bezpieczeństwa są ludzie którzy potrafią łamać wszelkie systemy zabezpieczeń.

15. Dodatki

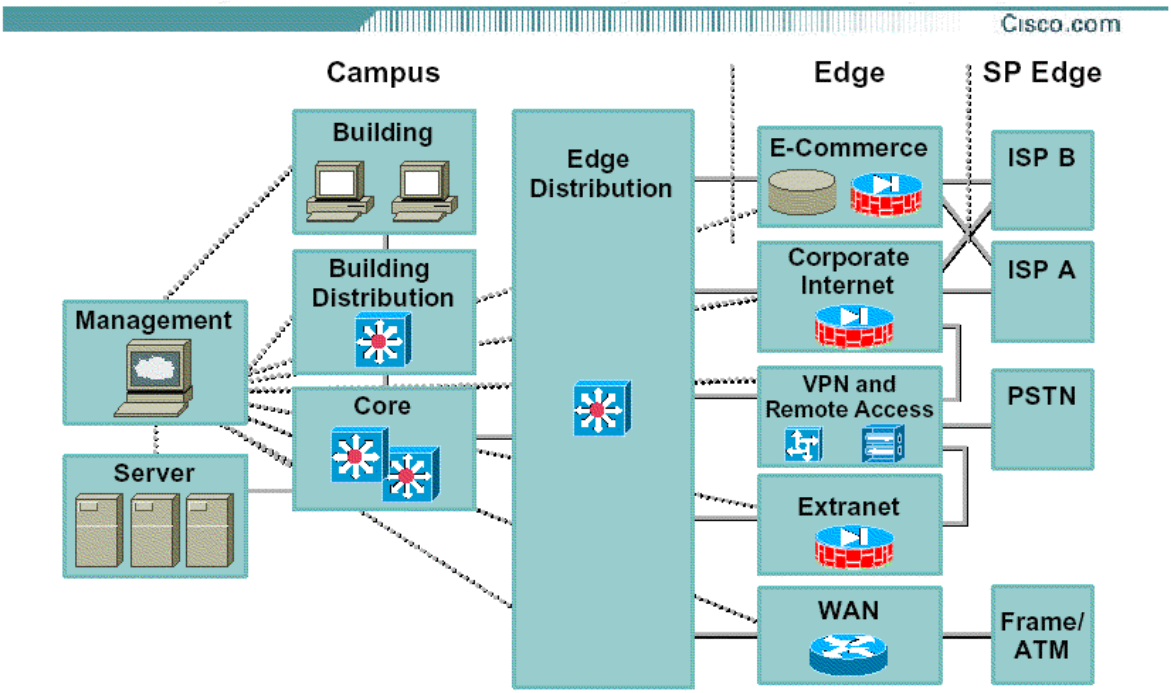
15.1 Przesyłanie haseł i danych w sieciach LAN i WAN

SEG.	USŁUGA SIECI	HASŁO LOGOWANIE	DANE	METODY ZABEZPIECZANIA
LAN	Klient **Microsoft Network** *(SMB/CIFS)*	zaszyfrowane	tekst jawny	VPN
	Klient **Novell Netware** *(NCP)*	zaszyfrowane	tekst jawny	VPN
	Klient **NFS**	zaszyfrowane	tekst jawny	VPN
	Klient **Microsoft Terminal**	zaszyfrowane	tekst jawny	VPN
INTERNET	Klient **WEB** *(HTTP)*	zaszyfrowane	tekst jawny	SSL/VPN
	Klient **FTP**	**tekst jawny**	tekst jawny	Kerberos/VPN
	Klient **MAIL** *(SMTP, POP3)*	**tekst jawny**	tekst jawny	S-MIME/SSL/VPN
	Klient **NEWS** *(NNTP)*	**tekst jawny**	tekst jawny	SSL/VPN
	Klient **TELNET**	**tekst jawny**	tekst jawny	Kerberos/VPN
	Klient **RLOGIN, RSH, RCP**	**tekst jawny**	tekst jawny	Kerberos/VPN
	Klient **SSH**	zaszyfrowane	zaszyfrowane	- -
	Klient **GOPHER**	**tekst jawny**	tekst jawny	VPN
	Klient **PROXY**	**tekst jawny**	tekst jawny	VPN
BAZY DANYCH	Klient **dBASE** *(BDE)*	brak	tekst jawny	VPN
	Klient **Paradox** *(BDE)*	zaszyfrowane	tekst jawny	VPN
	Klient **MS Access** *(BDE)*	zaszyfrowane	tekst jawny	VPN
	Klient **InterBase** *(BDE)*	zaszyfrowane	tekst jawny	VPN
	Klient **SQL Server**	zaszyfrowane	zaszyfrowane(*)	VPN
	Klient **Oracle Server**	zaszyfrowane	tekst jawny	VPN
	Klient **IBM DB2**	zaszyfrowane	tekst jawny	VPN
	Klient **MySQL Server**	**tekst jawny**	tekst jawny	VPN
	Klient **PostgreSQL Server**	zaszyfrowane(*) Kerberos	tekst jawny	VPN

15.2 Architektury bezpiecznych sieci korporacyjnych:

- *w/g Cisco*

Architektura Cisco SAFE może być wykorzystywana w sieciach małych, średnich jak i dużych, złożonych strukturach korporacyjnych. Jest ona sprawdzonym rozwiązaniem przy projektowaniu bezpiecznych sieci komputerowych. Składa się ona z trzech głównych części w skład których wchodzą : moduły sieci kampusowej (*Enterprise Campus*), moduły styku z sieciami zewnętrznymi (*Enterprise Edge*) i moduły brzegowe dostawców usług telekomunikacyjnych (*SP Edge*).



W skład modułów sieci kampusowej (*Enterprise Campus*) wchodzą :
- moduły dostępu w budynkach (*Building*)
- moduły dystrybucyjne w budynkach (*Building Distribution*)
- moduł rdzenia sieci (*Core*)
- moduł farmy serwerowej (*Server*)
- moduł brzegu sieci (*Edge Distribution*)
- moduł zarządzania (*Management*)

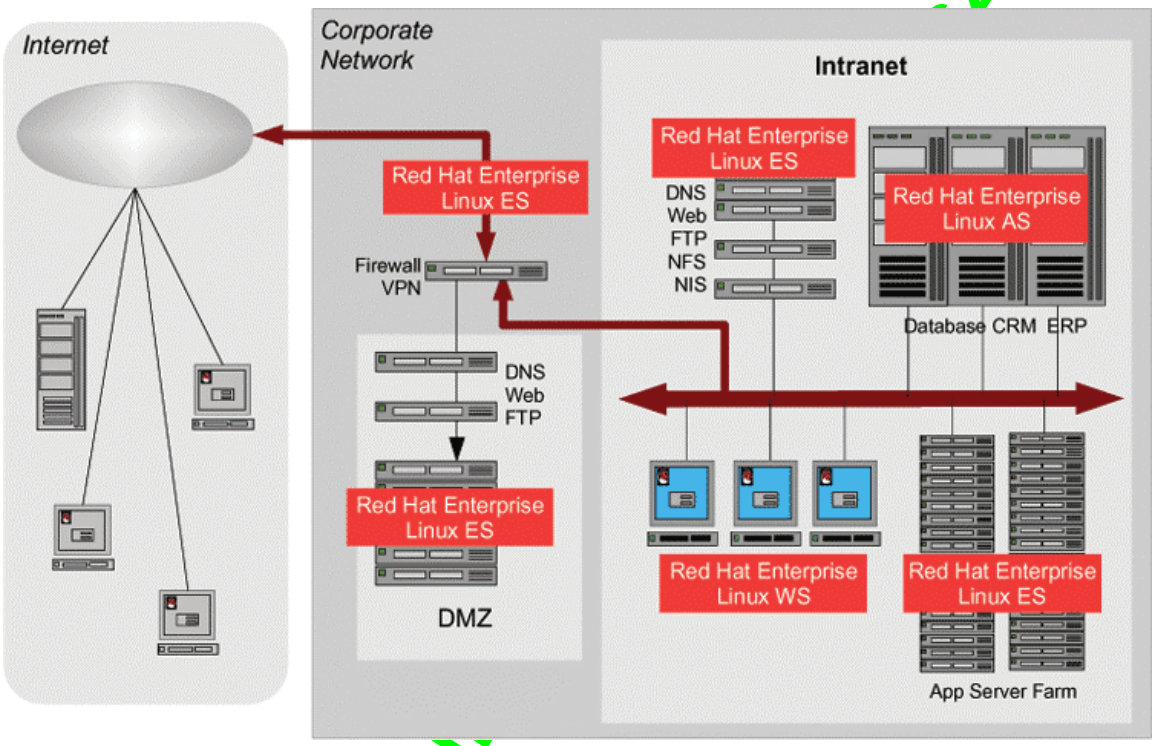
W skład modułów styku z sieciami zewnętrznymi (*Enterprise Edge*) wchodzą :
- moduł firmowego dostępu do Internet-u (*Corporate Internet*)
- moduł terminowania połączeń od partnerów biznesowych (*Extranet*)
- moduł handlu elektronicznego (*E-commerce*)
- moduł zdalnego dostępu i VPN (*Remote Access and VPN*)
- moduł sieci rozległych (*WAN*)

W skład modułów brzegowych dostawców usług telekomunikacyjnych (*SP Edge*) wchodzą :
- moduły łączy komutowanych (*ATM/FrameRelay*)
- moduły łączy dostawców usług Internet-owych (*ISP*)
- moduły łączy telefonicznych (*PSTN*)

Architektura Cisco SAFE jest niezależna sprzętowo i programowo.

- *w/g RedHat*

Architektura firmy RedHat może być wykorzystywana w sieciach małych, średnich jak i sieciach korporacyjnych. Jest ona zalecanym rozwiązaniem przy projektowaniu sieci komputerowych opartych o system operacyjny Linux. Składa się ona z dwóch głównych części w skład których wchodzą : moduł sieci wewnętrznej (*Intranet*) i moduł styku z sieciami zewnętrznymi (*DMZ*) oraz brzegu dostawcy usług Internet-owych.



W skład modułu sieci wewnętrznej (*Intranet*) wchodzą :
- farma serwerów aplikacji (*App Server Farm*)
- serwery baz danych i plików (*Database, CRM, ERP*)
- serwery usług sieciowych (*WEB, FTP, DNS, NFS, NIS, DHCP, SMTP, POP3, IMAP*)
- stacje robocze użytkowników (*Linux WS*)

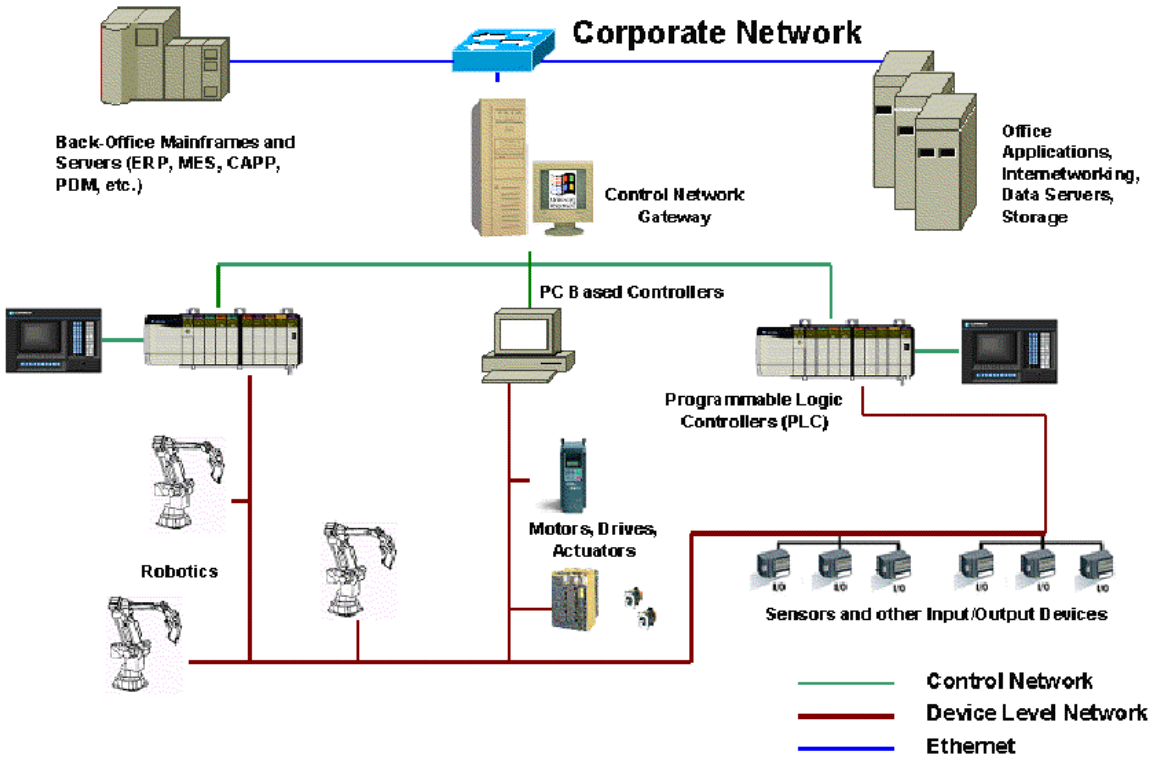
W skład moduł styku z sieciami zewnętrznymi (*DMZ*) wchodzą :
- serwery stron WWW (*WEB*)
- serwery plików (*FTP*)
- serwery nazw (*DNS*)
- serwery poczty (*SMTP, POP3, IMAP*)

W skład brzegu dostawcy usług Internet-owych wchodzą :
- zapory ogniowe (*Firewall*)
- urządzenia szyfrowania transmisji (*VPN*)

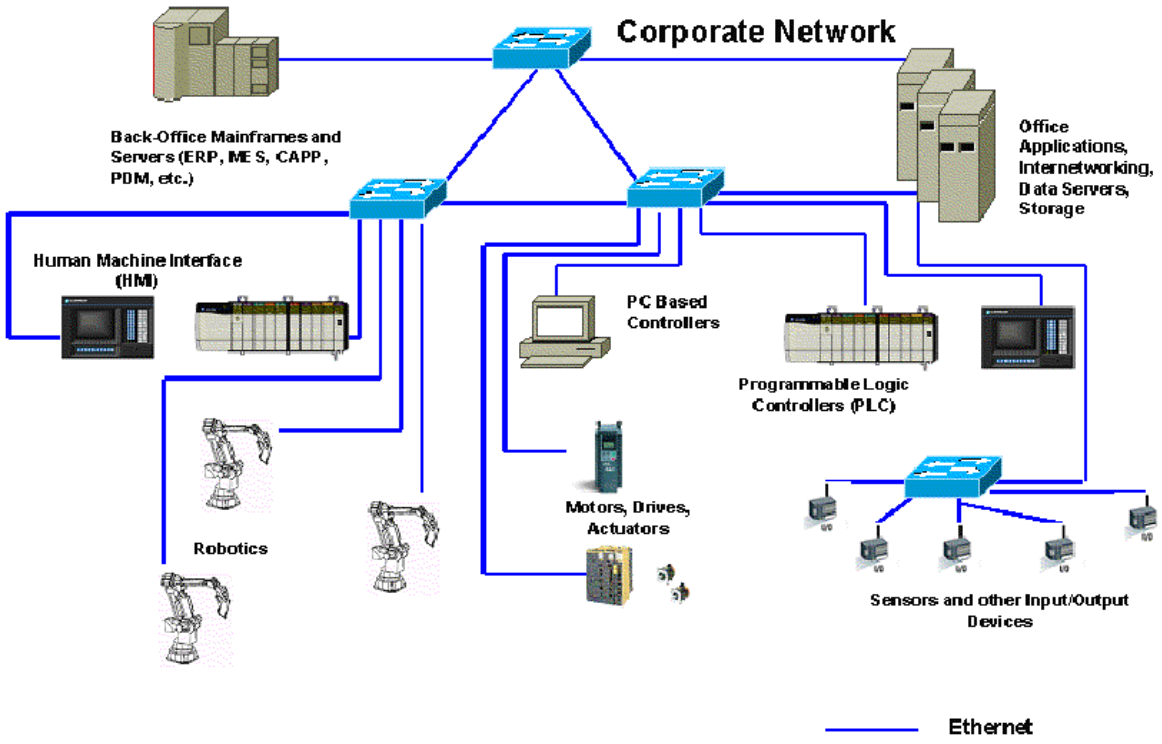
Architektura firmy RedHat jest niezależna sprzętowo i programowo.

15.3 *Architektury sieci przemysłowych:*

- *tradycyjnych*



- *w/g Cisco (Industrial Ethernet)*



15.4 Pliki związane z kryptografią :

***.key** - *Private Key (klucz prywatny certyfikatu [text] - Linux)*
***.crt** - *Internet Security Certificates X509 (certyfikat [text]- Linux)*
***.pem** - *Certificate PEM (certyfikat lub klucz prywatny [text] - Linux)*
***.ca** - *Encoded Files X509 (certyfikat - Linux)*
***.509** - *Encoded Files X509 (certyfikat - Linux)*
***.csr** - *Certificate Signing Request (kandydat na certyfikat [text] - Linux)*
***.crl** - *Certificate Revocation List (lista odwołanych certyfikatów [text] - Linux)*

***.p12** - *PKCS #12 Certificate (osobisty certyfikat [binarny] z kluczem prywatnym - Linux/Windows)*
***.pfx** - *Personal Information Exchange (osobisty certyfikat [binarny] z kluczem prywatnym - Linux/Windows)*
***.apf** - *Acrobat Personal Information Exchange (osobisty certyfikat [binarny] z kluczem prywatnym - Adobe Acrobat)*
***.p7** - *PKCS #7 Certificate (osobisty certyfikat - Linux)*
***.p7s** - *PKCS #7 Signed Certificate (osobisty certyfikat - Linux)*
***.usr** - *Certificate X509 (osobisty certyfikat z kluczem prywatnym - Linux)*

***.cer** - *Cetryficate X509 [DER lub BASE64] (certyfikat [binarny lub text] - Linux/Windows)*
***.fdf** - *Acrobat Data Exchange (certyfikat [binarny] - Adobe Acrobat)*
***.der** - *DER Encoded Binary Files X509 (certyfikat [binarny] - Linux/Novell)*
***.b64** - *BASE64 Encoded Files X509 (certyfikat [text] - Novell)*
***.req** - *Request Certificate (kandydat na certyfikat - Windows)*
***.p7b** - *PKCS #7 Certificate (osobisty certyfikat [binarny] bez klucza prywatnego - Windows)*
***.spc** - *PKCS #7 Cryptographic Message Syntax Standard (osobisty certyfikat [binarny] bez klucza prywatnego - Windows)*
***.key.db** - *Key Pair Files (baza danych kluczy prywatnych certyfikatów - Novell)*
***.cer.db** - *Certificate Files (baza danych certyfikatów - Novell)*
***.sst** - *Microsoft Serialized Certificate Store (magazyn certyfikatów seryjnych - Windows)*
***.stl** - *Certificate Trust List (lista zaufania certyfikatów - Windows)*

***.pgp** - *Pretty Good Privacy*
***.gpg** - *GNU Privacy Guard*
***.sig** - *plik podpisany elektronicznie GPG*
***.asc** - *plik podpisany elektronicznie "clearsign" GPG*

15.5 Składniki pakietu dokumentacji sieci

1. Schematy topologii fizycznej *(L1 - warstwa fizyczna modelu OSI)*
2. Schematy topologii logicznej *(L2 - warstwa łącza modelu OSI)*
3. Schematy adresacji sieciowej *(L3 - warstwa sieciowa modelu OSI)*
4. Inwentaryzacja wszystkich urządzeń sieciowych
5. Dokumentacje producenta na poszczególne urządzenia sieciowe
6. Wersje aktualnego oprogramowania urządzeń sieciowych
7. Dokumentacje oprogramowania urządzeń sieciowych
8. Wszystkie informacje pochodzące od ISP i/lub operatora telekomunikacyjnego *(parametry, ustawienia)*
9. Dokumentacja instalacji elektrycznej zasilającej urządzenia sieciowe i sprzęt komputerowy *(zasilacze bezprzerwowe, agregaty prądotwórcze)*
10. Jasna i dobrze zdefiniowana polityka bezpieczeństwa sieci
11. Szczegółowy opis instalacji urządzeń sieciowych
12. Aktualna konfiguracja urządzeń sieciowych
13. Szczegółowy opis czynności serwisowych i diagnostycznych urządzeń sieciowych
14. Statystyki ruchu i błędów
15. Dokumentacja dotycząca rozwiązywania problemów sieci
16. Instrukcja postępowania w sytuacjach awaryjnych dotyczących sieci
17. Lista osób odpowiedzialnych za poszczególne elementy sieci oraz sposoby kontaktu z nimi
18. Lista firm oferujących wsparcie techniczne dla elementów naszej sieci oraz sposoby kontaktu z nimi

15.6 Składniki pakietu dokumentacji usług sieci

1. Wykaz wszystkich usług sieci wraz z urządzeniami/serwerami na których działają
2. Protokoły używane przez poszczególne usługi sieci
3. Wykaz portów/gniazd statycznych i dynamicznych usług sieci
4. Dyski CD z aktualnym oprogramowaniem usług sieci wraz ze wszystkimi zainstalowanymi pakietami serwisowymi i korekcyjnymi
5. Dokumentacje oprogramowania usług sieci
6. Szczegółowy opis instalacji i konfiguracji oprogramowania usług sieci
7. Aktualna konfiguracja poszczególnych usług sieci
8. Szczegółowy opis czynności monitorowania i diagnozowania usług sieci
9. Dokumentacja dotycząca rozwiązywania problemów usług sieci
10. Instrukcja postępowania w sytuacjach awaryjnych dotyczących usług sieci
11. Lista osób odpowiedzialnych za poszczególne usługi sieci oraz sposoby kontaktu z nimi
12. Lista firm oferujących wsparcie dla poszczególnych usług sieci oraz sposoby kontaktu z nimi

15.7 Składniki pakietu dokumentacji serwera

1. Dokumentacja producenta na poszczególne podzespoły sprzętu komputerowego
2. Szczegółowy opis konfiguracji sprzętowej serwera
3. Dyski CD z aktualną wersją instalacyjną systemu operacyjnego oraz wszystkimi zainstalowanymi pakietami serwisowymi i korekcyjnymi
4. Dyskietki startowe i naprawcze
5. Dyski CD z aktualnymi wersjami sterowników urządzeń (karty graficzne, kontrolery napędów, karty sieciowe, modemy, itp)
6. Dokumentacja producenta systemu operacyjnego oraz oprogramowania sterowników urządzeń serwera
7. Szczegółowy opis instalacji i konfiguracji systemu operacyjnego serwera
8. Dyski CD z aktualnym oprogramowaniem usługowym wraz ze wszystkimi zainstalowanymi pakietami serwisowymi i korekcyjnymi
9. Dokumentacja producenta oprogramowania usługowego
10. Szczegółowy opis instalacji i konfiguracji oprogramowania usługowego
11. Szczegółowy opis czynności serwisowych i diagnostycznych serwera
12. Instrukcja postępowania w sytuacjach awaryjnych
13. Lista osób odpowiedzialnych za poszczególne elementy systemu oraz sposoby kontaktu z nimi
14. Lista firm oferujących wsparcie techniczne dla elementów naszego systemu

ponadto dla serwerów baz danych :

15. Dyski CD z aktualnym oprogramowaniem instalacyjnym klienta i serwera baz danych oraz dodatkowym oprogramowaniem zarządzającym wraz ze wszystkimi zainstalowanymi pakietami serwisowymi i korekcyjnymi
16. Dokumentacja producenta serwera baz danych
17. Szczegółowy opis instalacji i konfiguracji serwera baz danych
18. Szczegółowy opis instalacji i konfiguracji klienta bazy danych
19. Dyski CD z aktualnym oprogramowaniem aplikacji i interfejsów realizujących dostęp do danych w różnych formatach i z różnych źródeł *(np: BDE, ODBC32, unixODBC, JDBC, OLE-DB, dbExpress, PHP)*
20. Dokumentacja producenta aplikacji i interfejsów realizujących dostęp do danych
21. Szczegółowy opis instalacji i konfiguracji aplikacji oraz interfejsów realizujących dostęp do danych
22. Jasna i dobrze zdefiniowana polityka bezpieczeństwa danych
23. Projekt bazy danych
24. Szczegółowy opis czynności serwisowych i diagnostycznych na bazie danych
25. Lista osób odpowiedzialnych za poszczególne obiekty bazy danych oraz sposoby kontaktu z nimi
26. Lista firm oferujących wsparcie dla elementów naszego systemu baz danych

16. Słownik skrótów

ADO - *ActiveX Data Object*
ADS - *Active Directory Services (Windows 2000/2003 Server)*
ASP - *Active Server Page*
ATM - *Asynchronous Transfer Mode*
ATM VPN - *ATM Virtual Private Network (L2)*
AV - *AntiViruse*
BDE - *Borland Database Engine*
BL7F, BAF - *Basic Application Filter*
CA - *Certificate Authority*
CGI - *Common Gateway Interface*
CHAP - *Challenge Handshake Authentication Protocol*
CIFS - *Common Internet File System*
CoS - *Class of Service (L2)*
CPE - LAN + DMZ
DAO - *Data Access Object*
DDR - *Dynamic Document Review*
DMZ - *Demilitarized Zona (public services : HTTP, FTP, DNS, ...)*
DSCP - *Differentiated Services Codepoint Field*
DSO - *Dynamic Shared Object*
ECR - *Egress Commited Rate*
EIB - *Enctypted In Band Network Management*
FAP - *Firewall Authentication Proxy*
FR - *Frame Relay*
FR VPN - *Frame Relay Virtual Private Network (L2)*
FW - *Firewall*
GPG - *GNU Privacy Guard (uwierzytelnianie, integralność - podpis i szyfrowanie)*
HIDS - *Host IDS*
ICR - *Ingress Commited Rate*
IDS - *Intrusion Detection Systems*
IOS - *Internetworking Operating System (Cisco)*
IP VPN - *IP Virtual Private Network (L3)*
ISAPI - *Internet Information Server API*
iSCSI - *Internet SCSI (SCSI over TCP/IP)*
JSP - *JavaScript Server Page*
Kerberos - *protokół warstwy aplikacji (weryfikacja tożsamości, integralność i poufność)*
L1 - *OSI Layer 1 (warstwa fizyczna)*
L2 - *OSI Layer 2 (warstwa łącza danych)*
L3 - *OSI Layer 3 (warstwa sieciowa)*
L4 - *OSI Layer 4 (warstwa transportowa)*
L5 - *OSI Layer 5 (warstwa sesji)*
L6 - *OSI Layer 6 (warstwa prezentacji)*
L7 - *OSI Layer 7 (warstwa aplikacji)*
LDAP - *Lightweight Directory Access Protocol*

MAC - *Media Access Control*
NAS - *Network Attached Storage*
NAT - *Network Address Translation*
NBAR - *Network-Based Application Recognition*
NCP - *Netware Core Protocol*
NDS - *Novell Directory Services (Netware 4.x/5.x/6.x)*
NFS - *Network File System*
NIDS - *Network IDS*
NSAPI - *Netscape Server API*
NSS - *Netware Storage Service*
NTFS - *NT File System*
ODBC - *Open Database Connectivity*
OOB - *Out of Band Network Management*
OTP - *One Time Password*
P2P - *Peer-To-Peer*
PAP - *Password Authentication Protocol*
PAT - *Port Application Translation*
PGP - *Pretty Good Privacy (uwierzytelnianie, integralność - podpis i szyfrowanie)*
PHP - *Hypertext Preprocessor*
PKCS - *Public Key Cryptographic Standards*
PKI - *Public Key Infrastructure*
PKS - *Public Key System*
PSK - *Pre-Shared Key*
PWLAN - *Public WLAN*
PVC - *Permament Virtual Circuits*
QoS - *Quality of Service*
RADIUS - *Remote Access Dial-In User Scheme (zdalne uwierzytelnienia i rozliczania)*
RDO - *Remote Data Object*
RSVP - *Reservation Protocol*
S/MIME - *Secure Multipurpose Internet Mail Extensions (uwierzytelnianie, integralność - podpis i szyfrowanie)*
Samba - *SMB/CIFS (UNIX i Linux)*
SAN - *Storage Area Network*
SMB - *Server Message Block*
SMBS - *Server Message Block Signing*
SNMP - *Simple Network Management Protocol*
SPF - *Simple Packet Filter*
SPI - *Stateful Packet Inspection*
SSH - *Secure SH*
SSL - *Secure Sockets Layer*
STP - *Spanning Tree Protocol*
SVC - *Switched Virtual Circuits*
TACACS - *Terminal Access Controller Access Control System*
TLS - *Transport Layer Security*
ToS - *Type of Service (L3)*
WLAN - *Wireless LAN*
WWAN - *Wireless WAN*
VLAN - *Virtual LAN*
VPN - *Virtual Private Network (S2S i RA)*
YP/NIS - *Network Information System (UNIX i Linux)*

17. Źródła

Wydawnictwa książkowe:

Dudek Andrzej: *Jak pisać wirusy*, Read Me, Warszawa 1994
Dudek Andrzej: *Nie tylko wirusy*, Helion, Gliwice 1998
Błaszczyk Adam: *Pisanie wirusów i antywirusów*, Read Me, Warszawa 1998
A hacker's guide to protecting your Internet site and network, SAMS 1997
Internet. *Agresja i Ochrona*, Robomatic, Wrocław 1998

Konferencja i seminaria:

Kraut Michał: *Building SAFE Networks*, Seminarium Cisco Systems, Warszawa 2002
Kraut Michał: *Wprowadzenie do zagadnień bezpieczeństwa sieciowego*, Konferencja Cisco EXPO, Warszawa 2003
Baczyński Mariusz: *Bezpieczeństwo WLAN*, Konferencja Cisco EXPO, Warszawa 2003
Kontkiewicz Andrzej: *Bezpieczeństwo sieci komputerowych*, Seminarium Symantec Polska, Wrocław 2002
Bromirski Łukasz: *Pasywne i aktywne mechanizmy ochronne sieci komputerowej*, Seminarium bezpieczeństwa sieci komputerowych, Warszawa 2001
Szołkowski Piotr, Krzątala Grzegorz: *Budowa nowoczesnych i bezpiecznych sieci lokalnych*, Seminarium 3Com Polska, Wrocław 2002
Jakubiuk Mariusz: *Wykrywanie agresji i kontrola dostępu do zasobów Internetowych*, Seminarium Edusoft, Wrocław 2002
Sturniek Tomasz: *Nowoczesne metody zabezpieczania systemów informatycznych*, Seminarium Novell, Wrocław 2002
Wojdas Dariusz: *Problem Roku 2000*, Konferencja MSWiA, Opole 1999
Wojdas Dariusz: *Bezpieczeństwo systemów IT*, Konferencja SafeNet, Jesenik (CZ) 2002

Portale Internet-owe:

www.BezpieczenstwoIT.pl – Bezpieczeństwo IT
www.wojdas.24x7.pl – Encyklopedia Administratora Systemu Informatycznego