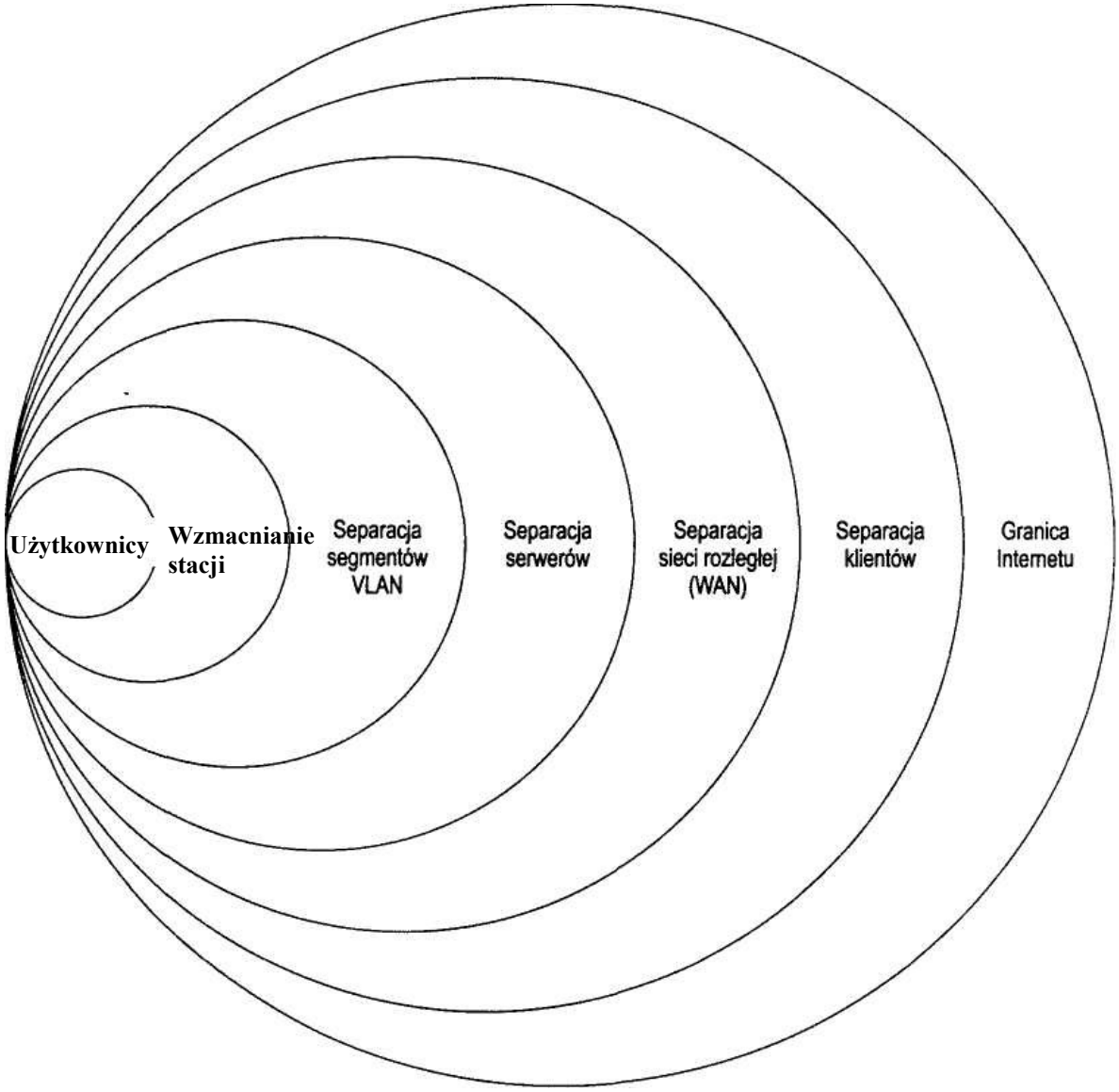
Wykl 4.

4. Bezpieczeństwo systemu operacyjnego i aplikacji

Bezpieczeństwo systemu operacyjnego jest ważnym elementem bezpieczeństwa sieciowego w organizacji. Stacja robocza w strategii ochrony dogłębnej stanowi kluczową pozycję. Schemat strategii ochrony dogłębnej został przedstawiony na rysunku 1.



Rys.1. Metodologia ochrony dogłębnej

Ochrona dogłębna jest metodologią mającą na celu opóźnianie i utrudnianie napastnikowi zadania. Może również wpłynąć na zmniejszenie szkód wyrządzonych wskutek ataku lub innego incydentu związanego z bezpieczeństwem. Jeśli jeden z mechanizmów kontrolnych (ochronnych) zawiedzie, ochrona dogłębna zapewnia, że atak nadal nie będzie skuteczny, ponieważ napastnikowi zostanie do pokonania jeszcze kilka warstw zabezpieczeń. Takie podejście daje administratorowi czas na odkrycie próby włamania i podjęcie odpowiedniej reakcji.

Warstwy ochronne

Zarządzanie użytkownikami — czujność użytkowników i ich świadomość powagi zagadnień bezpieczeństwa może być kluczowym czynnikiem skuteczności innych mechanizmów kontroli.
Wzmocnienie stacji — domyślne opcje instalacyjne stanowią podstawowy cel ataków. Napastnicy zawsze wybierają pierwszą dziesiątkę najpoważniejszych luk na listach słabych punktów systemów.
Separacja wirtualnych sieci lokalnych (VLAN) — należy ufać lecz warto odseparować. Nikt poza pracownikami związanymi z naliczaniem płac nie powinien mieć dostępu do podsieci, w której znajdują się stacje robocze zawierające informacje dotyczące płac.
Separacja serwerów — najcenniejsze cele ataków należy umieścić w podsieci o podwyższonym poziomie bezpieczeństwa.
Separacja sieci rozległej (WAN) — należy opracować kryteria typu „potrzebny dostęp" pomiędzy stacjami roboczymi a serwerami.
Separacja klientów — należy założyć, że żaden użytkownik i stacja poza siecią organizacji nie jest obiektem bezpiecznym.
Obszar Internetu — Internet co prawda niesie wiele zagrożeń, lecz badania instytucji bezpieczeństwa (np. FBI) udowadniają, że większość ataków pochodzi od wewnątrz jednostki.
Bezpieczeństwo systemu komputerowego
Bezpieczeństwo fizyczne
Bezpieczeństwo systemów operacyjnych
Bezpieczeństwo aplikacji
Bezpieczeństwo ludzi

Warstwa ochrony oprogramowania użytkowego odpowiada za zabezpieczenie dostępu do aplikacji oraz zapewnienie nienaruszalności oraz integralności jej zasobów.
Wyróżniamy następujące zagadnienia związane z bezpieczeństwem oprogramowania:
– Zapewnienie identyfikacji pojedynczego użytkownika aplikacji.
– Ustalenie praw poszczególnych grup użytkowników.
– Monitorowanie i rejestrowanie wykorzystanego oprogramowania.
– Kontrolę dostępu do tabel, kolumn i wierszy (relacyjnej) bazy danych.
– Ochronę konfiguracji oprogramowania.
– Pielęgnację kodu aplikacji.
– Replikacje danych, tworzenie kopii zapasowych – BACK-UP.
– Integrację mechanizmów ochrony systemu operacyjnego z wewnętrznymi zabezpieczeniami baz danych.
– Testowanie oprogramowania.
– Diagnostykę antywirusową.
– Bezpieczna administracja oprogramowania.

Bezpieczeństwo oprogramowania zależy od tego, czy oprogramowanie to zostało wykonane zgodnie z formalną metodyką tworzenia oprogramowania oraz czy posiada odpowiednio prowadzoną dokumentację.
W odniesieniu do danych aplikacji ważnym zagadnieniem są także jasno zdefiniowane więzy integralności oraz normalizacja baz danych.
Dodatkowe aspekty bezpieczeństwa oprogramowania to usuwanie błędów oraz wykrywanie blokad.

System operacyjny komputera (np. Unix, Windows XP/Vista, Linux) oferuje określone dla swojej klasy bezpieczeństwa usługi zabezpieczające.

4.1. Bezpieczeństwo systemów MS Windows

Bezpieczeństwo systemu Windows jest ważnym elementem bezpieczeństwa sieciowego w organizacji. Stacja robocza z systemem Windows w strategii ochrony dogłębnej stanowi kluczową pozycję.

- Zalecenia firmy Microsoft
- Wzmacnianie świeżo zainstalowanego systemu
- Instalacja aplikacji
- Przyłączanie stacji roboczych do sieci
- Bezpieczne użytkowanie systemu Windows
- Aktualizacja systemu i poprawki
- Utrzymanie i testowanie zabezpieczeń
- Ataki na stacje robocze w systemie Windows

4.1.1. Zalecenia firmy Microsoft

Firma Microsoft na swojej oficjalnej stronie poświęconej ochronie *http://www.microsoft.com/security/protect* zaleca przestrzeganie trzech zasad utrzymania wysokiego poziomu bezpieczeństwa systemu:

- stosowanie zapory sieciowej;
- systematyczne pobieranie aktualizacji systemu;
- wykorzystanie aktualnego oprogramowania antywirusowego.

Zalecenia firmy Microsoft stanowią ważne elementy zabezpieczenia stacji roboczej z systemem Windows.

Wzmacnianie systemu w sieci wiąże się z przestrzeganiem poniższych zaleceń.

- Należy opracować plan wzmacniania każdego systemu, który będzie miał kontakt ze światem zewnętrznym, w tym również stacje robocze z systemem Windows, przyłączone do sieci lokalnej (LAN) lub wymieniające pliki z innymi komputerami.
Należy koniecznie opracować procedurę, która będzie uwzględniała częste aktualizacje.
- Nie należy umieszczać świeżo zainstalowanego systemu w sieci lokalnej, chyba że będzie to bardzo bezpieczna, testowa sieć LAN. Producenci sprzętu (OEM) przygotowują swoje wersje instalacji Windows z myślą o szerokiej rzeszy odbiorców. Do bezpiecznych zastosowań system musi być okrojony do niezbędnego minimum, wystarczającego do realizacji funkcji biznesowych.
- Nigdy nie wolno umieszczać w sieci lokalnej systemu Windows, który miał bezpośrednią styczność z Internetem. Każdy system, który był przyłączony do Internetu bez specjalistycznych zabezpieczeń przez okres dłuższy od godziny powinien być uznany za podejrzany i potencjalnie stanowiący zagrożenie. W przypadku umieszczenia takiego systemu w sieci LAN będzie stanowił ryzyko dla wszystkich innych stacji roboczych. Każdy system Windows, który był przyłączony do Internetu bez zabezpieczeń powinien zostać zainstalowany na czysto przed umieszczeniem w zaufanym środowisku.
- Należy wyłączyć zbędne porty. Do sprawdzenia aktywnych portów można posłużyć się specjalizowanymi narzędziami, na przykład nmap czy nessus, służącymi do skanowania

komputera w sieci. W samym systemie Windows polecenie netstat -a i netstat -an uruchomione z wiersza poleceń spowoduje wypisanie numerów otwartych portów.
• Na stacji Windows należy wyłączyć zbędne usługi, nawet takie, które nie otwierają portów.
• Należy pobierać poprawki systemowe z użyciem mechanizmu Windows Update.
• Należy zainstalować dobry program antywirusowy i systematycznie aktualizować jego bazy.
• Należy zainstalować osobistą zaporę sieciową w systemie Windows. To jest element zgodny ze strategią ochrony dogłębnej, który dla napastnika stanowi dodatkową przeszkodę. Istnieją darmowe wersje programów tego typu.
• Nie należy bez biznesowego uzasadnienia uruchamiać na stacji roboczej zwracających uwagę serwerów sieciowych (WWW, poczty elektronicznej, udostępniania plików, wymiany informacji, np. LDAP, FTP). Należy przeprowadzić szczegółową analizę potrzeb stosowania każdej instalacji tego typu oprogramowania.
• Nie należy używać usług, które posiadają bezpieczniejsze i godne zaufania zamienniki. Na przykład zamiast telnet należy stosować ssh, zamiast POP3 lepiej użyć IMAP, zamiast FTP — SFTP.
• Należy zidentyfikować aplikacje krytyczne do realizacji misji organizacji i zarządzać poprawkami bezpieczeństwa dla tych aplikacji.
• Należy skonfigurować program wykonujący skanowanie systemu w poszukiwaniu nowo otwartych portów. W optymalnej konfiguracji stacja robocza powinna być skanowana co kwadrans.
• Należy stosować mocne hasła. Hasła powinny być zmieniane stosunkowo często — zaleca się okres 60 dni lub częściej.
• Należy użytkować system w sposób bezpieczny. Nie wolno otwierać dokumentów ani uruchamiać aplikacji, których pochodzenie nie jest w stu procentach pewne. Nie należy otwierać poczty elektronicznej od osób nieznajomych. Otwieranie niespodziewanych załączników poczty elektronicznej jest bardzo nierozważne.
• Należy usuwać zbędne dane i historie plików ze stacji roboczej. Powinno się stosować szyfrowanie danych.
• Należy obserwować zmiany wydajności systemu. Jeśli system nie został wyposażony w narzędzia służące do kontroli wydajności, należy je zainstalować.

4.1.2. Wzmocnienie świeżo zainstalowanego systemu

Świeże instalacje systemu Windows są ulubionymi celami ataków dlatego przed instalacją systemu należy fizycznie odłączyć stację roboczą od sieci. Po zainstalowaniu należy udokumentować wprowadzone zmiany - powinno się usunąć zbędne usługi, udokumentować zmiany i zapisać obraz systemu.
•Sprawdzić i zamknąć porty, które nie są bezpośrednio wymagane do realizacji zadań zabezpieczanej stacji roboczej.
•Zlokalizować i zamknąć wszelkie udostępniane zasoby, które nie są niezbędne do realizacji funkcji stacji roboczej. Otwarte zasoby współużytkowane można wypisać przez wywołanie polecenia net share z wiersza poleceń. Współużytkowanie zasobu można wyłączyć.
•Instalowane oprogramowanie należy ograniczyć do niezbędnego minimum, następnie udokumentować zmiany i ponownie zapisać obraz systemu.
•Zainstalować osobistą zaporę sieciową na stacji roboczej.
•Dokładnie przetestować system.

Szczegółowe zagadnienia wzmacniania systemu

Poniższa lista zawiera bardziej szczegółowe zalecenia dotyczące poprawiania bezpieczeństwa stacji roboczej z systemem Windows:

•włączyć obsługę szyfrowanego systemu plików EFS *(Encrypting File System)*w ramach NTFS;
•zablokować opcję Enable LMhosts lookup;
•zablokować opcję NetBIOS over TCP/IP;
•zablokować opcję ncacn_ip_tcp;
•ustawić MaxCachedSockets (REG_DWORD) na wartość 0;
•ustawić SmbDeviceEnabled (REG_DWORD) na wartość 0;
•ustawić AutoShareServer na wartość 0;
•ustawić AutoShareWks na wartość 0;
•w gałęzi NullSessionPipes usunąć wszystkie wartości;
•w gałęzi NuilSessionShares usunąć wszystkie wartości;
•jeśli stacja robocza jest wyposażona w dużą ilość pamięci RAM, należy wyłączyć wykorzystanie pliku wymiany (ang. *swap)*. Zwiększy to wydajność i bezpieczeństwo, ponieważ niejawne dane nie będą zapisywane na dysku twardym bez wiedzy użytkownika;
•ustawić dostęp do udostępnionych folderów określonym użytkownikom. Spowoduje to, że pozostali użytkownicy (oprócz administratorów) nie będą mieli dostępu do tych zasobów;
•ustawić rozsądną liczbę użytkowników uprawnionych do jednoczesnego dostępu do folderu współużytkowanego na rozsądną wartość. Jeśli do folderu ma mieć dostęp tylko jedna osoba, należy tę liczbę ustawić na 1;
•jeśli jest dostępna opcja szyfrowania zawartości folderów (Windows XP Professional), należy jej użyć;
•zabezpieczyć rejestr przed anonimowym dostępem;
•skonfigurować oczyszczanie pliku stronicowania przed zamknięciem systemu;
•wyświetlać stosowną informację o konsekwencjach prawnych przed zalogowaniem użytkownika w systemie;
•skonfigurować solidną politykę haseł;
•skonfigurować politykę blokowania kont;
•umożliwić audyt błędnych prób logowania i odrzuconych żądań dostępu;
•Nie stosować opcji AUTORUN. Wynikiem działania mechanizmu *autorun* może być uruchomienie podejrzanego kodu bez wiedzy użytkownika. W niektórych przypadkach napastnik może włożyć dysk CD do systemu i spowodować automatyczne uruchomienie własnego skryptu.

Bezpieczeństwo związane z systemem plików
Wiele z mechanizmów zabezpieczeń w domyślnych instalacjach systemów operacyjnych MS Windows pozostaje włączonych, lecz z powodu dużej liczby możliwych kombinacji konfiguracji sieciowych większość funkcji bezpieczeństwa nie jest domyślnie aktywna. Jedną z głównych funkcji bezpieczeństwa, która jest udostępniana przez system Windows oraz jest dla niego unikalna jest system plików NTFS, pozwalający na wykorzystanie zaawansowanych uprawnień do plików. Każdy administrator powinien stosować NTFS i wykorzystywać udostępniane przez ten format ustawienia uprawnień do plików.
Kolejną ważną i często pomijaną procedurą bezpieczeństwa jest zablokowanie uprawnień dostępu do plików na serwerze. W domyślnej konfiguracji system Windows nie stosuje restrykcji na żadnym z lokalnych plików lub folderów. Grupa *Wszyscy* posiada pełne prawa dostępu prawie do każdego zasobu systemu. W celu wzmocnienia bezpieczeństwa systemu operacyjnego grupa ta musi zostać usunięta a prawa dostępu do plików muszą być definiowane z wykorzystaniem precyzyjnie zdefiniowanych grup użytkowników.

Użytkownika, który jest dodawany do systemu, należy odpowiednio przypisać do właściwej grupy, w zależności od specyfiki wykonywanych przez niego zadań.
Zaleca się jednak, aby nie stosować do tego celu grup domyślnie zakładanych w systemie. Należy natomiast utworzyć nowe grupy z jasno określonymi uprawnieniami, niezbędnymi do realizacji poszczególnych zadań.
Jeśli konta zwykłych użytkowników nie zostały założone podczas instalacji systemu, należy tego dokonać jak najwcześniej. Jeśli to możliwe, należy konta skonfigurować jako zwykłe (nienależące do grupy *Administratorzy*). Nie należy stosować takich samych haseł do kont administratorów, co do kont zwykłych użytkowników.

Należy ustawić następujące opcje dla wszystkich użytkowników:
•w celu rozpoczęcia pracy z komputerem użytkownik musi podać nazwę konta i hasło;
•maksymalny okres ważności hasła — 60 dni (lub mniej);
•minimalny okres ważności hasła — 0 dni;
•minimalna długość hasła — 14 znaków;
•hasło musi spełniać wymagania co do złożoności — włączony;
•zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego — wyłączony;
•próg blokady konta — 3 nieudane próby załogowania;
•czas trwania blokady konta — 15 minut;
•wyzeruj licznik blokady konta po — 15 minut;
•przeprowadź inspekcję zdarzeń logowania — sukces, niepowodzenie;
•przeprowadź inspekcję zarządzania kontami — sukces, niepowodzenie;
•przeprowadź inspekcję zdarzeń logowania na kontach — sukces, niepowodzenie;
•przeprowadź inspekcję dostępu do obiektów — sukces, niepowodzenie;
•przeprowadź inspekcję zmian zasad — sukces, niepowodzenie;
•przeprowadź inspekcję zdarzeń systemowych — sukces, niepowodzenie.

Należy zadbać o to, aby użytkownicy nie używali ciągle tych samych haseł. Brak określonego czasu ważności hasła znacznie obniża poziom bezpieczeństwa, dając napastnikowi nieograniczony czas na złamanie hasła a w przypadku jego złamania, nieograniczony czas na jego wykorzystanie. Oprócz tego należy usunąć nieużywane konta. Takie konta, na które można się załogować ale których nikt nie używa, są często tworzone z jakąś formą domyślnego hasła i mogą być drogą uzyskania nieautoryzowanego dostępu do systemu. Wszystkie konta powinny być regularnie kontrolowane w celu sprawdzenia, czy ich czas ważności nie upłynął.

Zabezpieczanie typowej biznesowej stacji roboczej z systemem Windows
Windows jest systemem operacyjnym ogólnego zastosowania. Jednak typowy użytkownik stacji roboczej nie potrzebuje wcale ogólnego narzędzia.
Typowa biznesowa stacja robocza z systemem Windows realizuje poniższe funkcje:
• Edycja tekstów i zadania biurowe
• Poczta elektroniczna
• Przeglądanie WWW
• Przesyłanie plików
• Współużytkowanie plików

Edycja dokumentów, poczta elektroniczna, przeglądanie WWW i przesyłanie plików nie wymagają dostępu z zewnątrz do stacji roboczej. Z tego powodu skonfigurowana osobista zapora sieciowa powinna blokować cały dostęp z zewnątrz.
Współużytkowanie plików niestety wymaga dostępu z zewnątrz. To oznacza, że zapora sieciowa powinna zezwalać na tego typu połączenia do stacji roboczej. Aby uniknąć wyłomu w osobistej zaporze sieciowej, należy skonfigurować dedykowany serwer do współużytkowania plików i unikać udostępniania zasobów dyskowych na stacjach.

4.1.3. Instalacja aplikacji

Po wzmocnieniu systemu operacyjnego można przystąpić do instalacji aplikacji niezbędnych do realizacji zadań stacji roboczej. Ze względów bezpieczeństwa aplikacje przeznaczone dla stacji roboczych z systemem Windows ogranicza się do niezbędnego minimum. Polega to po prostu na ograniczeniu ryzyka przez usunięcie potencjalnych celów lub dróg ataku.

Niebezpieczeństwa

Aplikacje a szczególnie gry umożliwiają wprowadzenie do systemu obcego kodu w sposób prawie nie kontrolowany. Złośliwy kod (ang. *malcode*) to takie oprogramowanie i oprogramowanie sprzętowe (ang. *firmware*), które jest instalowane z zamiarem wyrządzenia szkód. Niektóre formy złośliwego kodu to bomby logiczne, konie trojańskie, robaki i wirusy.

Zabezpieczenie antywirusowe

Wirus jest programem komputerowym osadzonym w innym programie lub w pliku danych. Wirus jest zaprojektowany w taki sposób, że kopiuje się (samopowiela się) do innych plików podczas otwierania lub uruchamiania pliku przez system. Oprócz rozprzestrzeniania się wirusy mogą realizować inne zadania, od niegroźnych, takich jak zmiana kolorów na ekranie komputera, po szkodliwe, na przykład usuwanie plików z dysku twardego. Po zainfekowaniu komputera wirusem usunięcie szkodnika z systemu może być bardzo trudne. Często próby usunięcia wirusa sprowadzają się do usuwania skutków, a nie samego wirusa.
Robak – stoi o stopień wyżej w ewolucji. Nie potrzebuje już żywiciela i to odróżnia go od klasycznego wirusa. Samodzielnie dba o swoje uruchamianie.
Trojan (koń trojański) – najczęściej pojawia się w postaci niewinnie wyglądającej gry czy też wygaszacza ekranu. Niestety, po jego uruchomieniu oprócz spodziewanego efektu program potajemnie wykonuje dodatkowe działania np. pobiera na nasz komputer serwer FTP.

Wirusy i robaki rozprzestrzeniają się z wykorzystaniem środków dostępnych standardowo w sieci lokalnej lub środowisku pracy komputera.
We współczesnym środowisku pełnym zagrożeń należy zabezpieczyć przed infekcją wirusową wszystkie stacje robocze z systemem Windows.

Zabezpieczenie antywirusowe powinno skupiać się na:

- **Wykorzystaniu aplikacji antywirusowych** — zabezpieczenie przed wirusami może być realizowane przez oprogramowanie antywirusowe z częstymi aktualizacjami sygnatur wirusów.
- **Konfiguracji systemu Windows** — rozprzestrzenianie się wirusa może być powstrzymane przez zablokowanie słabych punktów stacji roboczej, takich jak zasoby sieciowe NetBIOS. Wirus może wykorzystywać zasoby NetBIOS, opierając się na zaufaniu pomiędzy klientem a systemem udostępniającym zasób.
- **Szkoleniu i świadomości użytkowników** — świadomy użytkownik, który w porę rozpozna symptomy zakażenia, może powstrzymać większość wirusów (oraz robaków i koni trojańskich).

4.1.4. Przyłączenie stacji roboczej do sieci

Stacja robocza z systemem Windows nie powinna zostać przyłączona do sieci przed przeprowadzeniem odpowiednich przygotowań, dostosowanych do istniejącego poziomu ryzyka. Lokalny atak na stację roboczą z systemem Windows jest kwestią kilku sekund, zatem należy dołożyć wszelkich starań, aby przed przyłączeniem do jakiejkolwiek sieci stacja była jak najlepiej zabezpieczona.

Testowanie wzmocnionej stacji

Przed przyłączeniem do niezaufanej sieci świeżo wzmocnionej stacji z system Windows, należy przetestować jej system na interfejsie sieciowym. Testy powinny składać się z kontroli otwartych portów oraz skanowania słabych punktów w systemie Windows. Każdy otwarty port powinien być rozpoznany i jeżeli jest nieużywany - zablokowany

Zapora sieciowa

Sieć, w której zostanie umieszczona stacja robocza z systemem Windows, powinna być zabezpieczona przed niezaufanymi sieciami (takimi jak Internet) za pomocą zapory sieciowej. Po wzmocnieniu ogólnym systemu operacyjnego oraz stacji roboczych, nadal występuje podatność na ataki związana z niewłaściwym wykorzystaniem możliwości stacji, takich jak przekazywanie *(replay),* podszywanie się lub ataki pośredniczące *(man-in-the-middle).* Jednym z najlepszych sposobów zabezpieczenia się przed atakami tego typu jest ochrona lokalnego segmentu sieci, do którego przyłączono stację. Do tego celu doskonale nadaje się centralna zapora sieciowa.

Osobiste zapory sieciowe

Osobista zapora sieciowa (ang. *personal firewall)* jest oprogramowaniem działającym na stacji roboczej. Zadaniem tego oprogramowania jest kontrola wchodzącego i wychodzącego ruchu sieciowego.

Poprawnie skonfigurowana osobista zapora sieciowa może w zabezpieczaniu stacji roboczej być bardziej skuteczna od zapory centralnej. Z punktu widzenia ruchu do i ze stacji roboczej użytkownika, zapora centralna jest z reguły skonfigurowana w zbyt ogólny sposób. Właściwie skonfigurowana zapora osobista może zawierać bardzo indywidualne opcje, wymagane do ochrony konkretnej stacji w sieci lokalnej.

Prawidłowy sposób konfiguracji zapory osobistej polega na zablokowaniu wszelkiego ruchu z i do stacji. Gdy użytkownik zetknie się z informacją o próbie transferu, może zdecydować, czy można zezwolić na dany ruch. W krótkim okresie użytkownik odblokuje wszelki ruch niezbędny mu do pracy. Od tego momentu konfiguracja osobistej zapory sieciowej będzie uwzględniała wszystkie specyficzne potrzeby danego użytkownika.

Bezpieczne usługi – usługi szyfrowane

- **Secure Shell (SSH)**
- **Secure FTP**
- **Pretty Good Privacy**

Secure Shell (SSH)

Usługa SSH (ang. *Secure Shell)* zabezpiecza połączenia sieciowe wykorzystując szyfrowanie przesyłanych haseł i innych danych. Program SSH służy do łączenia się z systemami zdalnymi i do wykonywania na nich poleceń. Wszelki ruch przesyłany w sesji jest szyfrowany. SSH początkowo miał służyć jako mechanizm zastępujący protokół telnet. Program ten ma za zadanie zastąpienie rlogin oraz rsh i udostępnienie bezpiecznej, szyfrowanej komunikacji pomiędzy niezaufanymi stacjami za pośrednictwem niezaufanej sieci. Za pomocą SSH można również przesyłać dane wykorzystując technikę tunelowania ruchu przez zabezpieczony kanał.

Wprowadzenie do SSH funkcji przekazywania portów *(port forwarding)* znacznie jednak poszerzyło jego możliwości. Technika ta powszechnie jest stosowana w celu zabezpieczania transmisji poczty elektronicznej.

Secure FTP

Program sFTP *(Secure FTP)* jest programem klienckim, który umożliwia przesyłanie plików pomiędzy stacją roboczą Windows a serwerem SSH. Wykorzystuje więc ten sam mechanizm uwierzytelniania i szyfrowania co program ssh. sFTP jest implementacją protokołu FTP za pośrednictwem SSH, zapewnia zatem połączenie bezpieczeństwa SSH z funkcjami znanymi z FTP. Oprócz przesyłania plików, sFTP może być stosowany do usuwania plików, tworzenia i usuwania katalogów i zmiany uprawnień do plików i katalogów.

Niestety, dodatkowe bezpieczeństwo niesie również niewygody. Mechanizm sFTP wymaga osobnego serwera plików.

Pretty Good Privacy

Pretty Good Privacy (PGP) jest pakietem programów, który służy do szyfrowania z użyciem techniki klucza publicznego w celu zabezpieczania danych i poczty elektronicznej. Pakiet ten pozwala na bezpieczną wymianę danych pomiędzy osobami posiadającymi wzajemnie swoje klucze publiczne. Klucze publiczne są danymi jawnymi, można je przesyłać pocztą, umieszczać na publicznych serwerach lub stronach WWW.

PGP dobrze integruje się z większością klientów poczty elektronicznej. Posiadacz klucza publicznego adresata może wysłać mu zaszyfrowaną wiadomość, która będzie czytelna tylko dla niego.

4.1.5. Bezpieczne użytkowanie systemu Windows

Nie wystarczy tylko wzmocnić stację roboczą Windows przed atakami, należy ją przede wszystkim użytkować w sposób bezpieczny. Po wzmocnieniu stacja robocza musi być w stanie realizować określone zadania. Jeżeli użytkownik nie przestrzega określonych reguł bezpiecznego użytkowania to może zostać narażony na atak.

Bezpieczne użytkowanie systemu Windows

- Ochrona fizyczna stacji roboczych i serwera.
- Konfiguracja
  - ograniczanie praw użytkowników
  - wykorzystanie zabezpieczenia antywirusowego
  - kontrola konfiguracji
- Minimalizacja wykorzystywania konta administratora
- Wykonywanie częstych kopii kluczowych danych

4.1.6. Aktualizacja wersji systemu i poprawki

Bezpieczeństwo wiąże się z ciągłymi zmianami. Napastnicy dostosowują się do tych zmian i ciągle poszukują nowych sposobów dokonywania włamań. Duży wpływ na tę sytuację mają coraz nowocześniejsze technologie, udostępniane wraz z nowymi wersjami systemów operacyjnych i aplikacji. W ten sposób ryzyko typowej stacji roboczej z systemem Windows także wzrasta wraz z upływem czasu.

Obserwuje się zwiększenie świadomości istotności zabezpieczeń przez dostawców systemów. Coraz większa liczba i częstotliwość dostarczania nowych wersji i poprawek jest wynikiem potrzeby poprawiania luk bezpieczeństwa systemów. Z tego powodu ważne jest, aby administratorzy i użytkownicy utrzymywali systemy w jak najlepszym stanie, wykorzystując aktualizacje wersji (ang. *upgrade)* i poprawki (ang. *patch).*

4.1.7. Utrzymanie i testowanie zabezpieczeń

Zagrożenia stacji roboczej z systemem Windows stale ulegają zmianom i mają tendencję do narastania. Coraz większa liczba napastników eksperymentuje z narzędziami do włamań. Dostępność tego typu narzędzi jest również coraz większa. To oznacza, że administrator systemu Windows musi zachować czujność w utrzymywaniu i testowaniu systemu zabezpieczeń stacji roboczej.

Poszukiwanie słabych punktów

System Windows powinien być okresowo sprawdzany w poszukiwaniu słabych punktów oraz otwartych portów. Można w tym celu wykorzystać kilka wysokiej jakości darmowych narzędzi skanujących, na przykład nmap czy nessus bądź ich komercyjne odpowiedniki. Każdą lukę bezpieczeństwa czy otwarty port należy przeanalizować i określić skutki jej usunięcia z punktu widzenia biznesowego.

Testowanie niepewnych aplikacji

Za każdym razem, gdy wystąpi konieczność instalacji na stacji roboczej aplikacji o wątpliwych cechach z punktu widzenia bezpieczeństwa, należy ją najpierw przetestować. Jeśli pochodzenie aplikacji nie jest znane, należy ją automatycznie potraktować jako potencjalnie niebezpieczną. Produkty dostępne na półkach w sklepach z oprogramowaniem komputerowym można natomiast uznać za stosunkowo bezpieczne. Programy pobierane z Internetu oraz oprogramowanie dostępne za darmo należy uznać za ryzykowne lub niepewne. Administrator systemu Windows powinien korzystać z komputera testowego, uważanego za niepewną stację i traktowanego w specjalny sposób. Każde nowe oraz niepewne oprogramowanie należy w pierwszej kolejności instalować na tego typu stacji. Stację i zainstalowane oprogramowanie należy stale sprawdzać pod kątem występowania wirusów i innych problemów.

Przebudowa systemu

Stacja robocza Windows będzie charakteryzować się najwyższą wydajnością i poziomem bezpieczeństwa wyłącznie zaraz po instalacji i wzmocnieniu. Wraz z upływem czasu bezpieczeństwo systemu będzie się obniżać. Powodem tego będą zmiany zachodzące w systemie, niektóre oczywiste, jak dodawanie aplikacji, inne bardziej subtelne, ujawniające się głównie wpisami w rejestrze systemowym. Zaleca się, aby użytkownik lub administrator okresowo analizował stan bezpieczeństwa stacji roboczej z systemem Windows. Jeśli takie procedury będą odbywały się systematycznie, mogą zwiększyć bezpieczeństwo.

Ponowna analiza bezpieczeństwa systemu Windows jest wskazana w przypadku wystąpienia określonych zdarzeń, między innymi:

- dodanie lub usunięcie użytkownika z systemu;
- instalacja poprawek lub aktualizacji systemowych;
- przy zmianie czasu.

Zaleca się również systematyczne sporządzanie kopii zapasowych systemu i dokonywanie jego ponownych instalacji. Częstotliwość wykonywania tej procedury zależy od wielu czynników, między innymi:

- od liczby eksperymentów przeprowadzanych na systemie;
- od liczby różnych gier instalowanych w systemie;
- od wykorzystania systemu do tworzenia oprogramowania;
- częstotliwości niecodziennych zachowań i awarii systemu.

Przy niskim stopniu wykorzystania systemu, na przykład w zastosowaniach domowych, system Windows wystarczy instalować od nowa raz na rok. W przypadku systemów wykorzystywanych bardzo intensywnie, należy go instalować częściej.

Monitorowanie
Wzmacnianie systemu Windows i zabezpieczanie sieci dotyczą określonych dziedzin problemów. Administrator systemu Windows musi jednak zachować stałą czujność, aby odpowiednio reagować również na nieoczekiwane zagrożenia. Zastosowanie odpowiednich mechanizmów monitorujących pozwala na wykrycie ataków na system, jak również niewłaściwych praktyk obsługi systemu przez legalnych użytkowników.
System powinien być monitorowany adekwatnie do poziomu zagrożenia danych oraz skutków utraty jego produktywności. Jeśli utrata danych lub produktywności jest nie do przyjęcia, monitorowanie musi odbywać się w trybie ciągłym. Jeśli zastosowano odpowiednie praktyki bezpieczeństwa, monitorowanie może odbywać się okresowo.

Administrator systemu musi zwracać uwagę na zagadnienia związane z zagrożeniami systemu,
przede wszystkim:
- analizować dzienniki systemowe;
- analizować dzienniki systemu poczty elektronicznej;
- śledzić nieudane próby dostępu do systemu;
- śledzić błędy aplikacji;
- analizować modyfikacje kluczowych plików;
- kontrolować uprawnienia do kluczowych plików;
- wykonywać testy wydajności;
- kontrolować zajętość dysków.

Administrator systemu Windows powinien włączyć funkcje zapisu dzienników systemowych w jak największym zakresie, jednak pod warunkiem, że nie wpłynie to negatywnie na wydajność i zasoby systemu. Należy jednak pamiętać, że nadmiar danych może obniżyć wydajność mechanizmów monitorujących system.
Dzienniki powinny być analizowane w sposób systematyczny.
Należy przede wszystkim monitorować przypadki ponownego uruchamiania systemu. Analiza takich zdarzeń i powiązanie ich z innymi problemami może znacznie uprościć pracę związaną z zabezpieczaniem systemu.

Oczyszczanie systemu
Do dobrych praktyk zalicza się okresowe oczyszczanie systemu Windows. Stacja robocza z czasem gromadzi różne elementy, które należy co jakiś czas usuwać. Wykonywanie oczyszczania systemu może wpłynąć na poprawę bezpieczeństwa stacji roboczej gdyż pozwoli to na usunięcie zbędnych plików tymczasowych. W ten sposób można również usunąć zapisane na dysku twardym lokalne kopie stron internetowych *(cache* przeglądarki). Usuwanie tego typu danych jest ważne przede wszystkim dlatego, że mogą posłużyć napastnikowi do pozyskania danych potrzebnych do prowadzenia ataków socjotechnicznych. Należy również przeanalizować potrzebę i ewentualnie usunąć wszelkie dane prywatne zapisane na stacji roboczej.

Przygotowanie na wypadek ataku
Pomimo nawet najskuteczniejszych wysiłków włożonych we wzmocnienie systemu Windows na stacji roboczej, nie można do końca wykluczyć incydentów związanych z bezpieczeństwem. Dlatego dobrze być przygotowanym na taki potencjalny atak.
Przygotowania do zareagowania na potencjalny atak należy rozpocząć od przeanalizowania

różnego rodzaju zagrożeń. Następnie należy opracowanie planu postępowania w przypadku ataku.

4.1.8. Zagrożenia i ataki na stacje robocze z systemem Windows

Dopóki system Windows pozostanie najpopularniejszym systemem operacyjnym dopóty będzie jednym z ulubionych celów ataków. Systemy operacyjne z rodziny Windows cechują się zróżnicowaną podatnością na ataki. Wystarczy odwiedzić specjalistyczne strony WWW dotyczące tych zagadnień, jak np. *SecurityFocus,* aby stwierdzić, że lista znanych słabych punktów tych systemów powiększa się każdego dnia.

Oprócz omawianego wcześniej zagrożenia związanego ze złośliwym kodem należy wspomnieć o zagrożeniach ze strony oprogramowania szpiegowskiego i reklamowego. Oprogramowanie szpiegowskie (ang. *spyware)* należy do grupy aplikacji zbierających informacje o stacjach roboczych i ich użytkownikach. Informacje tego typu są wysyłane do twórców i dystrybutorów programów szpiegowskich w celu dalszego wykorzystania np. kampanii marketingowych.
Oprogramowanie szpiegowskie stanowi znacznie większe zagrożenie, ponieważ dane zgromadzone za jego pomocą są o wiele bardziej szczegółowe. Takie prywatne informacje mogą być wykorzystane do wielu celów bez wiedzy i zgody użytkownika. Warto też podkreślić, że dostęp do niektórych danych zapisanych na dysku twardym może znacznie ułatwić tzw. kradzieże tożsamości.

Stacja robocza z systemem Windows zapisuje w wielu miejscach pewne informacje osobiste, wykorzystywane przez różne programy działające w systemie. Najpowszechniej spotyka się dane wprowadzane w formularzach stron WWW, zapisywane na dysku w postaci plików *cookies*.
Pliki *cookies* mogą potencjalnie zawierać szeroki zakres danych osobistych. Wszystko, co wpisujemy w formularzach na stronach WWW, może zostać zachowane przez serwer WWW na dysku twardym użytkownika w postaci pliku *cookies*.
Informacje, które często zdarza się wprowadzać do formularzy na stronach WWW:
•imię, nazwisko i adres;
•numery telefonów, adresy e-mail, identyfikatory komunikatorów;
•numery polis ubezpieczeniowych, numery kont bankowych, numery PIN;
•imiona dzieci, nazwisko rodowe matki, imię zwierzaka;
•nazwa pracodawcy i wysokość zarobków;
•numery nadwozia i silnika samochodu, jego marka i model.

Istnieje możliwość zablokowania zapisu plików *cookies* przez przeglądarkę WWW na komputerze użytkownika. Spowoduje to jednak, że większość serwisów internetowych nie będzie działać prawidłowo. Technika ta bowiem jest wykorzystywana przez większość stron WWW do obsługi użytecznych i w pełni legalnych funkcji serwera WWW.

Oprogramowanie szpiegowskie typu „Wielki Brat"

Termin *oprogramowanie szpiegowskie* jest stosowany również w stosunku do aplikacji służących do celowo podsłuchiwania lub monitorowania działania użytkownika w sposób dla niego niewidoczny. Omawiane narzędzia przesyłają do ich twórców informacje o działaniach użytkownika komputera.

W skład podsłuchiwanych danych mogą wchodzić następujące:
Naciśnięcia klawiszy — wykorzystywane między innymi do przechwytywania haseł i innych poufnych danych.

Kopie listów elektronicznych — wysyłane lub otrzymywane wiadomości e-mail są przekazywane do osób trzecich bez wiedzy użytkownika.
Kopie rozmów wykonywanych z użyciem komunikatorów internetowych — każda informacja przesyłana do lub z komputera może zostać skopiowana i przesłana do autora programu szpiegowskiego.
Zrzuty ekranów — nawet w przypadku wykorzystania szyfrowanej komunikacji dane prędzej czy później zostaną wyświetlone na ekranie. Program szpiegowski może zatem wykonać graficzny zrzut ekranu i wysłać taki obraz do wskazanego miejsca.
Inne ważne informacje — czasy załogowania i wylogowania z systemu, adresy odwiedzonych stron WWW — to tylko przykłady informacji, którymi mogą być zainteresowani szpiedzy komputerowi.

Oprogramowanie szpiegowskie wykorzystuje różne techniki ukrywania się w systemie. Gdyby użytkownik wiedział, że taka aplikacja działa w jego komputerze, natychmiast by ją usunął, zmienił ustawienia pracy lub w inny sposób starał się uniknąć skutków takiego monitoringu.
Istnieje kilka programów komercyjnych usuwających oprogramowanie szpiegowskie. Produkty tego typu wykorzystują bazę danych znanych aplikacji zawierających mechanizmy szpiegowskie. Programy te są użyteczne do usuwania znanych i szczególnie bezczelnych przypadków oprogramowania szpiegowskiego, lecz nie można liczyć na to, że są w stanie zwalczyć wszelkie przejawy takiej działalności.

Ataki fizyczne

Istnieje kilka typów ataków fizycznych, na które są podatne stacje robocze z systemem Windows. Większość specjalistów do spraw bezpieczeństwa informatycznego uważa, że gdy napastnik uzyska fizyczny dostęp do systemu, mechanizmy bezpieczeństwa takiego systemu można automatycznie uznać za naruszone.

Do ataków fizycznych zalicza się między innymi:

- Uruchomienie systemu z dyskietki lub rozruchowego dysku CD. W takim przypadku intruz może uzyskać dostęp do bazy haseł SAM oraz innych informacji przydatnych w łamaniu haseł. Włamywacz może też usunąć hasło i ustawić własne. Takie uruchomienie umożliwia również wystartowanie własnej wersji systemu Windows, dostosowanej do potrzeb włamywacza.
- W komputerze mogą zostać zainstalowane urządzenia podsłuchowe, na przykład przechwytujące naciśnięcia klawiszy w celu przejęcia poufnych danych, takich jak hasła i wpisywane dokumenty.
- Ruch sieciowy do i ze stacji roboczej może być podsłuchany dzięki koncentratorowi sieciowemu wpiętemu pomiędzy stacją roboczą a siecią lokalną. Można tego dokonać również dzięki wprowadzeniu modyfikacji w przełącznikach sieciowych.

Ataki TEMPEST

Ataki TEMPEST (ang. *Transient Electromagnetic Pulse Emanation Standard)* polegają na przechwytywaniu promieniowania elektromagnetycznego wytwarzanego podczas pracy urządzeń elektronicznych. Ataki te obecnie polegają głównie na analizie promieniowania wydzielanego przez monitory komputerowe. Zasięg ataków TEMPEST wynosi dziesiątki metrów, więc w przypadku bardzo poufnych danych można je uznać za poważny problem.

Najlepsze zabezpieczenia przed atakami TEMPEST polegają na:
•unikaniu korzystania z urządzeń niezgodnych ze standardami FCC *(Federal Communications Commission)*. FCC jest organizacją regulującą kwestie emisji elektromag-netycznej komputerów i innych urządzeń w celu mini-malizacji zakłóceń transmisji radiowej;

•przetwarzania najbardziej poufnych danych na urządzeniach skonstruowanych z myślą o odporności na ataki TEMPEST np. ekranowane komory lub pomieszczenia;
•zachować czujność w stosunku do otoczenia fizycznego organizacji;
•jeśli wystąpi podejrzenie wystąpienia problemu, należy przetestować otoczenie w poszukiwaniu emisji TEMPEST.

Tylne drzwi

„Tylne drzwi" są jednym ze sposobów uzyskania dostępu do systemu Windows. Często przeprowadzenie ataku na stację roboczą Windows jest utrudnione, szczególnie w przypadku zastosowania zapory sieciowej i mechanizmów detekcji włamań. Napastnik może więc zainstalować (lub nakłonić do tego użytkownika systemu) aplikację, która pozwoli mu na dostęp do systemu. Tego typu „tylne drzwi" (ang. *backdoor)* są często bardzo dobrze ukryte.

Jeśli stacja robocza Windows jest przyłączona do Internetu bez specjalnych zabezpieczeń dłużej niż jeden dzień, najprawdopodobniej została przejęta i zainstalowano już na niej co najmniej jedne tylne drzwi. W takim przypadku najlepszy sposób postępowania polega na ponownej instalacji systemu Windows. Tylne drzwi można często wykryć korzystając ze skanerów portów, jednak nigdy nie można mieć pewności, że na stacji nie dokonano innych, bardziej subtelnych modyfikacji. Niektóre zmiany w jądrze lub sterownikach urządzeń nie są łatwe do wykrycia. Niektóre konie trojańskie również bywają trudne do wykrycia bez dokonania szczegółowego porównania plików z wiarygodnymi wzorcami.

Ataki typu DoS

Jak wiemy bezpieczeństwo systemów informaty-cznych zajmuje się trzema zagadnieniami: poufnością, integralnością i dostępnością danych. Gdy użytkownik utraci dostęp do danych lub usług systemu, sytuacja taka zostaje zakwalifikowana do problemów bezpieczeństwa. Gdy utrata dostępu do danych lub usług jest wynikiem działań napastnika, mamy do czynienia z atakiem typu DoS (ang. *Denial-of-Service).*

Atakom typu DoS bardzo trudno zapobiec. Każdy komputer, jak i inne urządzenia, charakteryzuje się ograniczonymi możliwościami. Wiele ataków typu DoS wykorzystuje ten fakt zmuszając urządzenia do pracy poza pułapem ich możliwości, doprowadzając je do awarii. Ataki DoS często odbywają się w taki sposób, że do usługi są wysyłane w pełni legalne żądania, lecz z tak dużą częstotliwością, że dostęp do danej usługi staje się niemożliwy (np. zawieszeniu programu serwera), legalni użytkownicy nie mają możliwości skorzystania z urządzenia — następuje więc blokada dostępu do usługi.

Ataki typu DoS na stacje robocze Windows można ograniczyć stosując się do następujących zaleceń:
•zainstalować osobistą zaporę sieciową;
•wykorzystywać centralną zaporę sieciową chroniącą całą sieć lokalną;
•ograniczyć liczbę usług działających w stacji roboczej. Poniższe usługi w większości przypadków są zupełnie zbędne na stacji roboczej, powinny więc zostać usunięte lub zablokowane przed automatycznym uruchamianiem podczas rozruchu systemu:
- serwer WWW;
- serwer poczty;
- serwer FTP;
- serwer plików.

Podsłuchiwanie pakietów

Stacje robocze z systemem Windows są podatne na ataki przechwytywania ruchu sieciowego przez inne stacje robocze przyłączone do tego samego segmentu LAN. W przypadku zastosowania przełączników sieciowych, narzędzia wykorzystują tzw. atak pośredniczący

(ang. *man-in-the-middle),* w którym ruch jest przechwytywany przez napastnika, po czym odsyłany do prawdziwego adresata.

Podsłuchiwanie pakietów pozwala na odczyt całego ruchu sieciowego wysyłanego lub odbieranego przez stację roboczą. Dotyczy to poczty elektronicznej, komunikatorów internetowych i ruchu związanego z WWW. Na przykład w przypadku podsłuchanego ruchu WWW napastnik może oglądać każdy ekran dokładnie w takiej samej postaci, jak użytkownik.
Najlepsze zabezpieczenie systemu Windows przed podsłuchiwaniem pakietów polega na wykorzystaniu technik szyfrowania w tych wszystkich przypadkach, gdy to jest możliwe. Napastnik nadal może przechwycić ruch sieciowy, lecz nie będzie w stanie odszyfrować jego treści.

Przechwytywanie i wznawianie sesji

Przechwytywanie sesji (ang. *session hijacking)* jest techniką ataku, która polega na obserwacji i przechwytywaniu sesji TCP/IP przez program podsłuchujący. Każda sesja sieciowa posiada dwie strony komunikacji: nadawcę (komputer nawiązujący sesję) i odbiorcę. Napastnik może modyfikować ruch sieciowy, aby udawać system, z którym miała zostać nawiązana sesja. Ruch jest przesyłany pomiędzy napastnikiem a nadawcą.

Wznawianie sesji (ang. *session replay)* występuje wtedy, gdy program podsłuchujący odczyta parametry sesji. Napastnik modyfikuje nieco odpowiednie parametry sesji (niektóre nie muszą być modyfikowane, na przykład w przypadku transferu środków z konta bankowego) i dokonuje ponownego połączenia z serwerem podszywając się pod oryginalnego nadawcę.

Socjotechnika

Socjotechnika jest metodą uzyskiwania wartościowych informacji na temat systemu od jego legalnych użytkowników. Napastnik stosuje odpowiednie połączenie informacji o systemie i technik manipulacyjnych, aby wzbudzić zaufanie ofiary. W efekcie ofiara jest skłonna ujawnić napastnikowi więcej dodatkowych informacji potrzebnych do kontynuacji ataku. Na przykład intruz może udawać osobę upoważnioną i zadzwonić do centrum pomocy z prośbą o przypomnienie zapomnianego hasła, które jest niezbędne do uzyskania natychmiastowego dostępu do systemu. Dodatkowym argumentem może być, przykładowo, obawa o utratę ważnego klienta. Atakujący może wymyślić wiele sytuacji w zależności od zakresu posiadanych już informacji o organizacji i określonych aplikacjach. W niektórych przypadkach napastnik stosuje grę emocjami i wywiera nacisk na personel, nie dając czasu na zastanowienie. W takich przypadkach łatwo jest wykorzystać efekt zaskoczenia w celu szybkiego uzyskania informacji.

Należy założyć, że napastnik zdecydowany na dokonanie ataku w konkretnym celu (niekoniecznie niszczycielskim, również szpiegowskim) zawsze posłuży się socjotechnika, aby uprościć sobie zadanie.
Nie należy ujawniać publicznie żadnych informacji, które są związane z realizacją misji stacji roboczej. Te informacje mogą znacznie uprościć zadanie napastnika stosującego socjotechnikę. Na przykład nazwy i identyfikatory użytkowników nie powinny być wyświetlane w sposób łatwy do odczytania przez obce osoby.

Ataki polegające na wykorzystaniu socjotechniki są najtrudniejsze do uniknięcia i — potencjalnie — najpoważniejsze w skutkach. Nawet najlepiej wyszkoleni użytkownicy są skłonni do udzielania informacji, jeśli sądzą, że w ten sposób będą mogli skuteczniej wykonywać swoją pracę. Napastnik może za pomocą tej informacji dokonać wielu zniszczeń.

Jeśli informacja uzyskana metodami socjotechniki zawiera identyfikatory i hasła, napastnik ma dokładnie takie same możliwości posługiwania się stacją roboczą, co ofiara takiego ataku.

Podsumowanie

Stacja robocza z systemem Windows bywa często najsłabiej zabezpieczonym elementem sieci w organizacji. Dzieje się tak z wielu powodów, najważniejsze z nich to:
•Typowy użytkownik systemu Windows nie jest wystarczająco dobrze przeszkolony z zakresu bezpieczeństwa, lecz ma bardzo duże uprawnienia w systemie stacji roboczej.
•Standard PC został opracowany z myślą o bardzo ogólnych zastosowaniach. To powoduje, że istnieje wiele obszarów, w których włamywacze mogą poszukiwać słabych punktów.
•Firma Microsoft zaprojektowała swój system operacyjny w taki sposób, żeby standardowa instalacja zaspokajała jak najszerszy zakres potrzeb użytkowników. Cecha pożądana dla jednej grupy użytkowników bywa jednak zupełnie zbędna i stanowi zagrożenie bezpieczeństwa dla innej.
•Większość pracy wykonywanej w organizacji odbywa się z użyciem stacji roboczych z systemem Windows. Istnieje oczywisty konflikt pomiędzy poziomem bezpieczeństwa a wygodą obsługi. Często kompromis pomiędzy tymi potrzebami jest osiągany kosztem bezpieczeństwa, co powoduje, że stacja robocza stanowi najsłabsze ogniwo w zabezpieczeniach sieci.

Stację roboczą z systemem Windows można jednak zabezpieczyć. Najważniejsze sposoby realizacji tego celu obejmują:
•wzmocnienie systemu operacyjnego;
•instalację aplikacji zwiększających bezpieczeństwo, między innymi oprogramowania antywirusowego;
•odpowiednią konfigurację sieci, do której zostanie przyłączona stacja robocza;
•bezpieczne wykorzystanie stacji;
•systematyczną instalację poprawek i aktualizacji systemu oraz kluczowych aplikacji;
•częste testowanie i monitorowanie zabezpieczeń stacji roboczej.

4.2. Bezpieczeństwo systemów Unix

Unix, Linux i inne pokrewne systemy operacyjne zdobywają coraz większą popularność i udział w rynku. Unix jest nadal dominującym systemem operacyjnym serwerów, wzrost popularności systemów Unix i Linux dotyczy przede wszystkim stacji roboczych.

Większość zagadnień bezpieczeństwa dotyczących stacji roboczych, omówione w poprzednim wykładzie, odnosi się również do maszyn pracujących w systemie Unix i Linux. W tym wykładzie zostaną omówione zagadnienia dotyczące głównie systemów Unix.

Unix, Linux, FreeBSD, AIX i inne pokrewne systemy operacyjne (określane po prostu jako Unix) charakteryzują się wielkim potencjałem, zarówno pod względem wysokiego bezpieczeństwa, jak i podatności na ataki. Niektóre z tych cech, które powodują, że systemy Unix są tak podatne na ataki, stanowią o ich wielkiej elastyczności i mogą być wykorzystane również do ich wzmocnienia w celu zapewnienia bezpieczeństwa pracy.

Unix jako cel ataku

Podstawowe powody, dla których komputery pracujące w systemach Unix i Linux stają się celami ataków to:
•Linux ma jawny kod źródłowy (ang. *open source*);

•system Unix i Linux jest zwykle oprogramowaniem niedrogim (często darmowym) i przez to łatwo dostępnym;
•większość narzędzi wykorzystywanych przez włamywaczy jest dostępna dla systemów Unix;
•Unix stanowi dobre środowisko wymiany kodu.

Narzędzia sieciowe i programistyczne
Kolejną atrakcyjną dla włamywacza cechą systemów Unix i Linux jest wręcz nadmierna liczba dostępnych narzędzi sieciowych. Większość takich narzędzi jest tworzona w pierwszej kolejności dla systemów Linux i FreeBSD, dopiero potem są przenoszone na inne systemy operacyjne.
Oprócz narzędzi sieciowych Unix udostępnia bardzo funkcjonalne środowisko programistyczne. Wszystkie kompilatory oraz biblioteki niezbędne do kompilacji jądra i systemu operacyjnego są dostępne na zasadzie otwartych licencji. Dzięki temu włamywacz może wygenerować sobie dowolne narzędzia, od spreparowanych modułów jądra udostępniających prawa konta użytkownika *root (root kit),* po zaawansowane i specjalizowane narzędzia do prowadzenia ataków.

Przykłady darmowych narzędzi sieciowych, które mogą być wykorzystane przez włamywaczy w poszukiwaniu słabych punktów systemów i w celu tworzenia *exploitów.*
tcpdump — aplikacja, która przechwytuje dane przesyłane w sieci i pracuje na niskim poziomie (program ten działa w warstwach: 2., 3. i 4. sieciowego modelu ISO OSI). Program tcpdump wchodzi w skład standardowych instalacji systemów Unix i obsługuje szeroki zakres nośników sieciowych warstwy 2. tcpdump jest powszechnie dostępny, zatem wyniki jego działania są często wykorzystywane jako dane wejściowe narzędzi analizujących ruch sieciowy.
Ethereal — aplikacja służąca do podsłuchiwania ruchu sieciowego. Ethereal posiada interfejs umożliwiający pracę z danymi dostarczanymi przez inne narzędzia działające na niskim poziomie, jak tcpdump.
tcpreplay — pozwala na wysyłanie z powrotem do sieci danych przechwyconych przez program tcpdump. Pozwala to włamywaczom na dokładniejszą analizę ruchu sieciowego i lepsze testowanie własnych aplikacji.
nmap — popularne narzędzie skanujące porty. Sprawdza stan portów w systemie próbując się z nimi połączyć. Istnieje wiele metod aktywacji portów, nmap może również być uruchamiany w trybach mniej lub bardziej agresywnych.
Nessus — skaner sprawdzający podatność na włamania. W pierwszej kolejności wykorzystuje nmap do wykrycia otwartych portów, następnie sprawdza otwarte porty pod kątem możliwości przeprowadzenia znanych ataków. Skaner nessus implementuje ponad 500 testów i potrafi wykryć większość znanych dziur w systemie zabezpieczeń.
Perl, sh, ksh —języki skryptowe, które w rękach zdolnego włamywacza mogą stać się potężnymi narzędziami, pozwalającymi na automatyzację powtarzalnych procedur.

Unix i Linux jako trudny cel ataków
Unix posiada również kilka cech, dzięki którym jego atrakcyjność jako obiektu ataków zmniejsza się. Do tych cech należą między innymi:
•istnieje wiele odmian, wersji i kompilacji tego systemu;
•użytkownicy systemów Unix są z reguły bardziej doświadczeni;
•uruchomienie skryptów w atakowanym systemie jest niełatwym zadaniem (w porównaniu do wykorzystania błędów programu MS Outlook);

•atrybuty uprawnień do plików znacznie utrudniają rozprzestrzenianie się w systemie złośliwego oprogramowania.

Wiele odmian, wersji i kompilacji

Kod i sposoby włamań łatwo rozpowszechnić, lecz określone *exploity* mogą nie działać jednakowo ze wszystkimi wersjami systemów Unix. Wymaga to znacznych umiejętności konfiguracyjnych, co z reguły nie należy do cech typowego złośliwego włamywacza. W wyniku tego faktu dla systemów Unix istnieje, co prawda, spora liczba *exploitów,* lecz naprawdę groźnych jest niewiele.

Zaawansowani użytkownicy

Unix jak do tej pory nie zdobył sobie popularności w charakterze systemu biurkowego dla masowych odbiorców. Jego głównymi zastosowaniami są serwery, systemy wbudowane oraz platformy programistyczne. Wszystkie te sposoby pracy wymagają od średnio zaawansowanego użytkownika znacznie większego zakresu wiedzy. Z tego powodu doświadczenie przeciętnego użytkownika systemu Unix jest większe niż większości osób pracujących w systemie Windows. Włamywacze komputerowi, podobnie jak ich odpowiednicy w większości innych dziedzin, z reguły poszukują ścieżki najmniejszego oporu. Atakowanie stacji roboczej wykorzystywanej przez użytkownika o niewielkich umiejętnościach technicznych będzie z oczywistych przyczyn łatwiejszym zadaniem od atakowania systemu obsługiwanego przez eksperta. Z tego powodu ataki na platformy uniksowe są rzadsze.

Niełatwe uruchamianie skryptów

W systemach Unix można wykorzystać wiele technik skryptowych. Jednakże w przeciwieństwie do systemu Windows, mechanizmy skryptowe nie są tu zintegrowane z powszechnie wykorzystywanymi aplikacjami (jak MS Outlook czy Word). To powoduje, że Unix jest mniej podatny na ataki od systemu Windows, w którym działa MS Outlook pozwalający na uruchamianie skryptów języka Visual Basic z prawie nieograniczonymi uprawnieniami.

Uprawnienia dostępu do plików

Pospolitą techniką stosowaną przez złośliwe programy jest wykorzystywanie często uruchamianych aplikacji do propagacji ataku. W tych przypadkach wirus czy robak dopisuje swój kod do programu, który jest następnie uruchamiany przez nieświadomego użytkownika. Ten typ ataku jest możliwy, ponieważ w celu wykorzystania niektórych zasobów systemu zwykli użytkownicy muszą uruchamiać programy działające z prawami użytkownika *root*. Taka sytuacja ma miejsce również w systemie Unix.

Unix jednak posiada tę przewagę, że uprawnienie do uruchomienia programu jest niezależne od prawa własności względem pliku. Choć użytkownik ma prawo uruchamiania aplikacji, z reguły nie jest właścicielem samego pliku i nie będzie miał możliwości modyfikacji tego programu. Brak możliwości modyfikowania programu wykonywalnego przez zwykłego użytkownika jest poważnym ograniczeniem dla wirusów i koni trojańskich, które często tego wymagają w celu rozprzestrzeniania się.

Bezpieczna obsługa systemu Unix

Unix jest bardzo dobrze wyposażonym systemem operacyjnym, udostępniającym wiele narzędzi i możliwości, lecz nawet dobrze skonfigurowany i wzmocniony system operacyjny może nadal stanowić zagrożenie, jeśli użytkownicy i procesy nie są właściwie kontrolowane i monitorowane.

Każdy atak na stację roboczą związany z siecią prędzej czy później kończy się uruchomieniem jakiegoś kodu. Kod ten można zaklasyfikować do jednej z następujących kategorii:

kod złośliwy — obejmuje wirusy, robaki i konie trojańskie. Kod tego typu może być uruchomiony w imieniu legalnego użytkownika przez aplikację obsługującą skrypty, na przykład przez przeglądarkę WWW;
usługi sieciowe — w tym przypadku napastnik włamuje się do systemu przez sieć i uzyskuje dostęp do stacji roboczej poprzez otwarty port.

W celu zabezpieczenia się przed złośliwym kodem można zastosować dwa sposoby: wykorzystać oprogramowanie antywirusowe i unikać ryzykownych działań. Zagadnienie to zostało szczegółowo już omówione, warto wspomnieć o tym i tutaj. Unikanie ryzykownych działań obejmuje przestrzeganie następujących zaleceń.
♦ Nie należy otwierać, uruchamiać a nawet pobierać z sieci zasobów, co do których istnieją jakiekolwiek podejrzenia. Innymi słowy nie należy „rozmawiać z nieznajomymi". Taki sposób postępowania należy wymuszać na wszystkich poziomach organizacji. Zasada najsłabszego ogniwa ma w tym przypadku szczególne zastosowanie.
♦ Gdy to tylko możliwe, należy wyłączyć funkcje obsługi skryptów w programach klientów pocztowych, edytorach tekstów i innych programach biurowych.

System zabezpieczeń wielu stacji roboczych może być usprawniony przez użycie szyfrowania. Zagadnienie to będzie omówione później.

Kontrola procesów
We wczesnych latach systemów Unix instalacja systemu składała się wyłącznie z podstawowych elementów. Wraz ze wzrostem popularności Uniksa i Linuksa równocześnie zaczęto udostępniać coraz większą liczbę różnorodnych funkcji. Wszystkie te dodatkowe funkcje i aplikacje są potencjalnymi zagrożeniami.
Procesy można z punktu widzenia bezpieczeństwa podzielić na trzy kategorie.
Unikać, o ile to tylko możliwe — niektóre usługi są przestarzałe lub niebezpieczne i dlatego należy unikać ich lub stosować rozwiązania alternatywne.
Używać, o ile to konieczne — niewielka grupa usług jest prawdopodobnie na tyle wartościowa, że można podjąć ryzyko ich stosowania.
Prawdopodobnie niepotrzebne — większość procesów można zaliczyć właśnie do tej kategorii. W niektórych przypadkach mogą znaleźć zastosowanie, lecz nie powinny być instalowane w większości stacji roboczych z systemem Unix.

Usługi, których należy unikać
W celu zapewnienia bezpieczeństwa stacji roboczej z systemem Unix w sieci, administrator powinien kontrolować działające procesy. Wiele aplikacji w systemach Unix, które działają w trybie demona lub serwera, mogą stać się obiektami ataków jako potencjalne sposoby dostępu do systemu.
Jedna z zasad bezpieczeństwa mówi, że niepotrzebne aplikacje lub usługi nie powinny być uruchamiane. Poniżej wymieniono kilka przykładów tego typu aplikacji, które często są standardowo instalowane w systemie i w większości przypadków nie są wykorzystywane.
FTP (vsftp lub wuftpd) — FTP jest bardzo rozpowszechnionym sposobem przesyłania plików. Duża liczba słabych punktów tego protokołu ujawnia się w przypadku anonimowego dostępu. Poważną wadą FTP jest przesyłanie haseł w postaci nieszyfrowanej. Z tych powodów zaleca się stosowanie bardziej bezpiecznych metod przesyłania plików, jak scp oraz sFTP.
Network File System (NFS) — zaprojektowany w celu współużytkowania plików w sieci, lecz nie w Internecie. NFS jest usługą wykorzystującą protokół RPC i usługę portmap. Protokół NFS ułatwia napastnikowi rozprzestrzenianie złośliwego kodu.

nfslock — usługa blokowania plików udostępnianych protokołem NFS.
Jeśli NFS nie jest wykorzystany, ta usługa powinna zostać wyłączona.
RPC *(Remote Procedure Call)* — ten protokół może powodować poważne problemy bezpieczeństwa i powinno się go unikać, jeśli nie jest niezbędny. Istnieje kilka aplikacji wykorzystujących RPC. Większość użytkowników jednak pracuje na swoich stacjach roboczych bez żadnej potrzeby stosowania RPC. Z tego powodu zaleca się wyłączenie usług RPC, chyba że protokół ten jest wymagany z jakiegoś powodu. Większość implementacji RPC obsługuje zadania zdalnego sterowania komputerem lub przetwarzania rozproszonego. Przypadki takie jednak są rzadkie.
portmap — ta usługa stosuje RPC i jest wykorzystywana przez nfslock.
polecenia rsh, rep, rlogin — są to programy sieciowe stosujące słabe uwierzytelnianie. Przesyłają informacje bez szyfrowania (w tym hasła). Istnieją znacznie lepsze zamienniki tych poleceń, jak ssh czy scp.
telnet — ta bardzo prosta usługa pozwala na zdalny dostęp do stacji roboczej. Informacje są przesyłane bez szyfrowania, zatem jest możliwe przechwycenie haseł przez osoby postronne. Sesję telnet można ponadto z łatwością przechwycić i wykorzystać lub przekierować do innego systemu.

Użyteczne usługi
Wykorzystanie wymienionych niżej usług jest zalecane jedynie w przypadku, gdy są potrzebne. Niekiedy można je dodatkowo wzmocnić blokując dostęp z sieci do portów przez nie wykorzystywanych.
iptables — filtr pakietów obsługiwany przez jądro. Wykorzystuje reguły kontrolujące pakiety na wejściu, wyjściu oraz w razie ich przekazywania do interfejsów sieciowych stacji roboczej. Program iptables stanowi dodatkową warstwę zabezpieczeń i jest ważnym elementem strategii obrony dogłębnej stacji roboczych z systemem Unix.
kudzu — program wykrywający sprzęt uruchamiany podczas rozruchu systemu. Jeśli stacja robocza nie podlega częstym zmianom konfiguracji sprzętowej, można wyłączyć tę usługę.
network — skrypt uruchamiający interfejsy sieciowe. Jest wymagany w przypadku przyłączenia stacji roboczej do sieci.
demony wydruku (cupsd, Ipd) — usługi te umożliwiają drukowanie ze stacji z systemem Unix na dowolnej drukarce. Usługi te umożliwiają również drukowanie sieciowe, lecz nie powinny być udostępniane w ten sposób. W celu zablokowania dostępu sieciowego do tych usług można posłużyć się usługą i ptables.
rawdevices — ta usługa umożliwia dostęp do „surowych" urządzeń wejścia—wyjścia (IO).
sshd — serwer umożliwiający zdalne logowanie się z użyciem klienta ssh. Jeśli dostęp do stacji nie jest potrzebny, usługę te można wyłączyć.
syslog — obsługa zapisu dzienników systemowych, działająca również sieciowo, na przykład na podstawie centralnego serwera dzienników z funkcjami analizy i audytu.
imaps — usługa udostępniająca pocztę w standardzie IMAP przez szyfrowane połączenie SSL (ang. *Secure Socket Layers)*. Klientami obsługującymi ten standard są na przykład Netscape Communicator oraz fetchmail.
rexec — serwer usługi rexec. Serwer ten udostępnia możliwość zdalnego uruchamiania programów z uwierzytelnianiem polegającym na użyciu nazwy użytkownika i hasła.
rlogin — serwer usługi rlogin. Serwer ten pozwala na zdalne logowanie się do systemu z uwierzytelnianiem opartym na uprzywilejowanych numerach portów z zaufanych hostów.
rsh — serwer usługi rcmd. Serwer ten umożliwia zdalne połączenia z uwierzytelnianiem opartym na uprzywilejowanych numerach portów z zaufanych hostów.
rsync — serwer umożliwiający synchronizowanie plików z wykorzystaniem sum kontrolnych CRC.

servers — usługa, która wypisuje nazwy aktywnych procesów serwera. Zagadnienie to jest szerzej omówione w dalszej części.
sgi_fam — demon monitorujący pliki. Może być użyty w celu informowania administratora o zmianach wprowadzonych w plikach.

Wykrywanie usług
Administrator systemu powinien zablokować wszelkie zbędne usługi systemowe, musi więc mieć możliwość wykrywania i zarządzania tymi usługami. Do tego celu służą polecenia: ps, netstat oraz nmap.

Kontrola użytkowników
Oprócz kontroli procesów ważne jest, aby sprawdzać użytkowników stacji roboczej. Czynności z tym związane obejmują kontrolę dostępu użytkownika do plików i możliwości uruchamiania procesów. Mechanizm uprawnień do plików w typowy dla systemów Unix sposób określa zakres możliwego dostępu użytkownika do danego pliku. Ograniczanie dostępu użytkownika do procesów opiera się na kontroli dostępu do praw konta *root.*

Uprawnienia do plików
Założeniem obowiązującym w systemie Unix jest, że użytkownicy logują się w stacji roboczej z wykorzystaniem własnych identyfikatorów (UID) i haseł. Uprawnienia do plików polegają na wykorzystaniu trzech kategorii, co oznacza, że każdy plik w systemie Unix posiada zdefiniowane uprawnienia dla trzech rodzajów użytkowników. Procedura logowania się w systemie musi jednoznacznie zaklasyfikować użytkownika do odpowiedniej kategorii: *wszyscy, grupa, właściciel.*

Dostęp do konta root
Wcześniej wspomniano, że jądro systemów Unix pracuje w dwóch trybach: administratora *(root)* oraz zwykłego użytkownika. Konto *root* ma pełny dostęp do całej stacji roboczej. Użytkownik uzyskuje jedynie ograniczony dostęp, co więcej, w przypadku próby skorzystania z pamięci zastrzeżonej dla użytkownika *root* za pomocą programu działającego z uprawnieniami zwykłego użytkownika, zostanie wywołany błąd segmentacji i program zostanie unicestwiony.

Zagrożenia i ataki na stacje robocze z systemem Unix
Ataki na systemy Unix koncentrują się na próbach uzyskania uprawnień konta *root.* W celu zmniejszenia ryzyka dla stacji roboczej, administrator systemu powinien unikać udostępniania zwykłym użytkownikom praw konta *root.*

• Wynikiem dostępu zwykłych użytkowników do konta *root* mogą być poniższe problemy. Użytkownicy z prawami konta *root* mogą modyfikować konfigurację stacji roboczej i potencjalnie zmieniać mechanizmy bezpieczeństwa skonfigurowane przez administratora. Na przykład, określona usługa mogła zostać skonfigurowana do pracy wyłącznie w środowisku *chroot* (polecenie chroot umożliwia wirtualną zmianę katalogu głównego procesu), to oznacza, że istnieje jedynie ryzyko nielegalnego dostępu do alternatywnego katalogu głównego. Jeśli użytkownik nieświadomie uruchomi tę usługę z wiersza poleceń, zabezpieczenie zapewniane przez mechanizm *chroot* nie będzie już skuteczne.
•Użytkownicy mogą uruchamiać usługi narażające stację roboczą na ataki. Na przykład serwer WWW jest bardzo łatwo osiągalnym celem i wymaga zabiegów wzmacniających i przygotowania bezpiecznej konfiguracji. Typowy użytkownik nie zapewni odpowiedniego

poziomu zabezpieczeń dla samodzielnie skonfigurowanego serwera WWW, uruchamianego na stacji roboczej.
•Proste błędy popełniane przez użytkownika mogą mieć nieproporcjonalne poważne konsekwencje np.. uruchomić polecenie rm -rf * - taka operacja spowoduje usunięcie wszystkich niekrytych plików oraz podkatalogów w katalogu bieżącym bez zadawania dodatkowych pytań. Ten przykład stanowi najlepszy dowód konieczności pracy zwykłych użytkowników na kontach o minimalnym zakresie uprawnień. Użytkownik nadal może oczywiście wyrządzić sporo szkód, lecz przynajmniej nie usunie plików, których właścicielem jest *root.*

W celu minimalizacji używania uprawnień konta *root* na stacji roboczej można zastosować kilka zabiegów. Najczęściej stosuje się:
•Ograniczenie dostępu do stacji roboczej bezpośrednio z konta *root* - wszyscy użytkownicy powinni logować się na swoje konta o zwykłych uprawnieniach.
•Ograniczenie zdalnego dostępu do konta *root*.

Szyfrowanie i certyfikaty
Strategia zabezpieczania dogłębnego wymaga od administratorów, aby podjęli wszelkie niezbędne działania w celu poprawy bezpieczeństwa. Jednym z ważnych usprawnień ochrony systemu jest stosowanie na szeroką skalę technik kryptograficznych.
Należy stosowac:
- GNU Privacy Guard – odpowiednik PGP.
- SSH.

Wzmacnianie systemu Unix
Każda stacja robocza przyłączona do sieci musi zostać wzmocniona przed atakami. Ogólne zalecenia dotyczące takiego wzmacniania są następujące:
•założenie, że domyślna instalacja dowolnej dystrybucji nie jest bezpieczna i że należy ją wzmocnić;
•ograniczenie do minimum zainstalowanego oprogramowania, uruchomionych procesów itp., tak aby realizowały zadania stacji roboczej i nic ponad to;
•konsekwentne stosowanie bezpiecznych alternatyw usług, które nie są uznawane za bezpieczne (na przykład ssh jako bezpieczna alternatywa usługi telnet);
•bieżące instalowanie poprawek bezpieczeństwa i aktualizacje pakietów oprogramowania;
•wykorzystanie również prywatnej zapory sieciowej iptables.

Podsumowanie
Systemy Unix są bardzo rozbudowanymi systemami operacyjnymi, które za pomocą wiedzy i odpowiednich środków można uczynić bardzo bezpiecznymi. Równocześnie, wskutek braku umiejętności lub bezmyślności mogą łatwo stać się bardzo podatnymi na ataki. Przestrzeganie omówionych zasad bezpieczeństwa, dzięki którym systemy Unix można doprowadzić do tego, że będą skutecznie zabezpieczane.