Alina Gil*, Tomasz Karoń**

ANALIZA ŚRODKÓW I METOD OCHRONY SYSTEMÓW OPERACYJNYCH

Streszczenie. W pracy przeanalizowane zostały środki i metody ochrony systemów operacyjnych. Sama ochrona systemu operacyjnego jest tylko elementem szerszego zagadnienia, jakim jest ochrona informacji. Na wstępie opisane zostały zagrożenia, na jakie jest narażony system operacyjny wskazując tym samym na zakres ochrony, jaką powinien być on objęty. Następnie dokonano analizy metod ochrony wskazując na rodzaj zagrożenia, któremu zapobiegają. Ochrona systemu operacyjnego jest realizowana przy użyciu mechanizmów samego systemu jak i przy użyciu programów zewnętrznych. W pracy główną uwagę koncentruje się na mechanizmach ochrony systemu operacyjnego natomiast specjalistyczne programy omówione zostały w mniejszym zakresie.

Słowa kluczowe: system operacyjny, ochrona informacji, bezpieczeństwo danych, administracja systemu.

WIADOMOŚCI WSTĘPNE

Współczesne komputery to rozbudowane urządzenia składające się często z dwu lub więcej systemów mikroprocesorowych oraz wielu urządzeń wejściowo – wyjściowych. Sterowanie komputerem, czyli zmuszenie go do wykonywania określonej aplikacji to skomplikowane zadanie, które jest realizowane w tzw. trybie jądra przy użyciu oprogramowania zwanego systemem operacyjnym.

Ogólnie rzecz biorąc system operacyjny realizuje dwa zadania:

- rozdział zasobów komputera tak, aby na komputerze mogło pracować wielu użytkowników i wiele programów. Z punktu widzenia ochrony systemu operacyjnego powinien on dysponować mechanizmami pozwalającymi w precyzyjny sposób określać zakres praw dostępu do systemu dla poszczególnych użytkowników a poprzez to uruchomionych przez nich procesów. Brak takich mechanizmów prowadzi często do unieruchomienia systemu operacyjnego i przejęcia kontroli nad komputerem poprzez inny kod.
- tworzenie maszyny wirtualnej z dostępnego sprzętu - czyli tworzenie interfejsu programistycznego umożliwiającego dostęp do sprzętu i samego systemu w sposób niezależny od architektury komputera, na którym. Realizowane jest to np. poprzez pamięć wirtualną, która powoduje rozszerzanie funkcjonalności sprzętu, na którym działa system

* Instytut Edukacji Technicznej i Bezpieczeństwa, Akademia im. Jana Długosza w Częstochowie, a.gil@ajd.czest.pl

** Zespół Szkół Mechaniczno-Elektrycznych im. K. Pułaskiego w Częstochowie

operacyjny. Komputer może dysponować ograniczoną pamięcią operacyjną a jednak z punktu widzenia użytkownika jest ona nieograniczona, ponieważ system operacyjny potrafi wykorzystywać urządzenia pamięci masowej do jej rozszerzenia. Innym przykładem jest tzw. pętla zwrotna, czyli symulowany interfejs sieciowy pozwalający między innymi na sprawdzenie poprawności działania mechanizmów sieciowych a także programów korzystających z sieci komputerowych.

Analizując ten zakres działania systemów operacyjnych pod kątem bezpieczeństwa należy uwzględnić ochronę zasobów i obsługę błędów. Ochrona zasobów powinna być tak zorganizowana, aby zapewniała bezpieczeństwo zasobów współużytkowników przed błędami lub złośliwością innych współużytkowników. Obsługa błędów powinna natomiast zapobiegać propagacji błędu na inne elementy systemu operacyjnego. Taki sposób ochrony jest w zasadzie uzupełnieniem ochrony zasobów.

System operacyjny jest, zatem oprogramowaniem działającym na komputerze na szczególnych prawach i zapewniającym łatwość obsługi a także zwiększenie możliwości komputera. Ze względu na tę specyficzną rolę powinien on podlegać ochronie, przy czym mechanizmy ochrony powinny być wbudowane w sam system a także powinny działać poza systemem chroniąc go niejako z zewnątrz.

Ochrona systemu operacyjnego jest tylko środkiem do celu, jakim jest ochrona informacji przechowywanej i przetwarzanej przez ten system. W związku z tym wszelkie rozważania na temat zagrożeń bezpieczeństwa systemów operacyjnych jak i środków zapobiegawczych należy prowadzić w kontekście ochrony informacji znajdujących się w komputerze.

ZAGROŻENIA BEZPIECZEŃSTWA SYSTEMÓW OPERACYJNYCH

Udostępnianie poufnych danych

Udostępnianie poufnych danych ma miejsce wtedy, gdy nieuprawnieni użytkownicy zyskują dostęp do danych dostępnych dla ściśle określonej grupy użytkowników (dostęp polega tu tylko na odczycie tych danych bez możliwości dokonania zmian).

Poufnymi danymi może być rodzaj i wersja systemu operacyjnego działającego w systemie komputerowym. Ma to szczególne znaczenie w sytuacji, gdy dany system pracuje w charakterze serwera w sieci. Informacja taka ma dużą wartość dla atakującego, gdyż dzięki temu potrafi on dobrać właściwe metody ataku. Dysponując wersją systemu operacyjnego można poznać jego słabe strony poprzez zaznajomienie się z informacjami umieszczonymi na witrynie producenta lub wydawcy.

Najprostszą metodą uzyskania informacji o zdalnym systemie operacyjnym jest wykorzystanie usługi udostępniania stron witryn World Wide Web. Niektóre programy obsługujące tę usługę wysyłają, bowiem w nagłówkach odpowiedzi na żądanie strony szczegółową informację o systemie, na którym pracują (przykład takiej informacji zamieszczono na rysunku 1).

Przy dostępie lokalnym użytkownik wie, z jakim systemem operacyjnym ma do czynienia. Nie powinien już jednak mieć możliwości ustalenia dokładnej jego wersji. Podobnie,

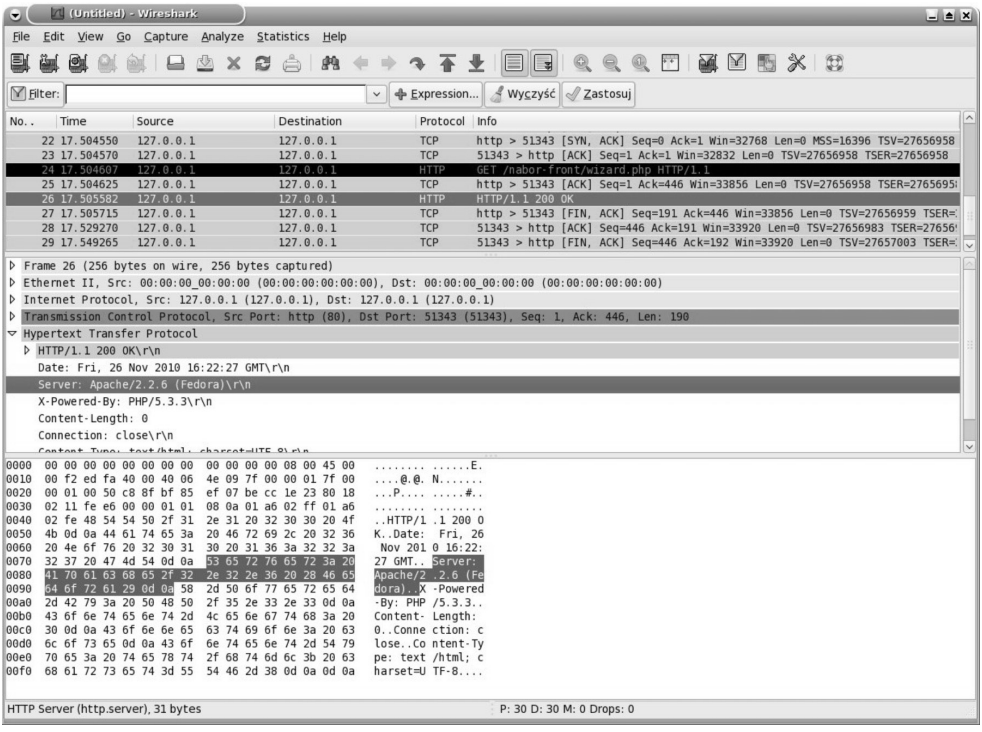
bowiem jak w przypadku dostępu zdalnego może próbować wykorzystać słabość systemu operacyjnego do uzyskania dostępu do poufnych danych.

W przypadku dostępu lokalnego najprostszą metodą uzyskania informacji o wersji systemu operacyjnego, na której się pracuje jest przeglądniecie zawartości katalogów zawierających pliki związane bezpośrednio z systemem np. w systemie Linux będą to katalogi /boot i /lib/modules (rys. 2).

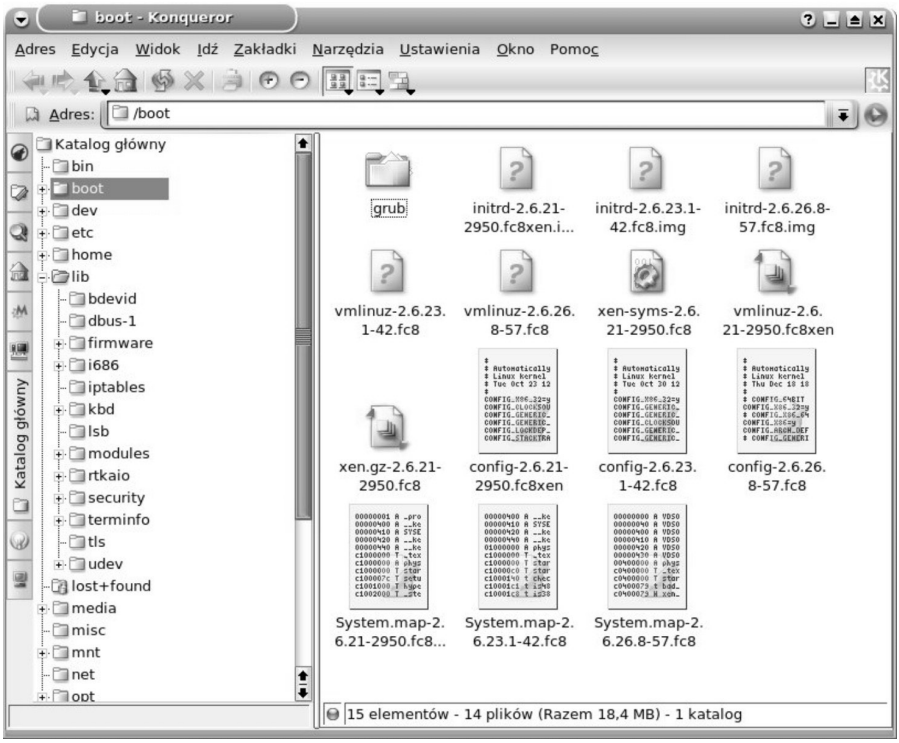
Innym rodzajem poufnych danych są logi systemowe i programów działających w systemie a także ich pliki konfiguracyjne. Podobnie jak poprzednio, zapoznanie się z logami systemu operacyjnego pozwala na odkrycie jego słabych stron. Atakujący ma tu ułatwione zadanie gdyż często system operacyjny dokładnie informuje o problemach i szczegółach swojego działania.

Analogicznie sprawa wygląda w przypadku logów i plików konfiguracyjnych programów działających w systemie operacyjnym. I tu analiza zapisów zdarzeń może pozwolić na odkrycie słabych stron programu, co może prowadzić np.: do ujawnienia innych poufnych danych.

Ostatnim rodzajem chronionych danych są różnego rodzaju dokumenty np.: plany, opisy, bazy danych itp. Często są to dokumenty dla przetwarzania których powstał konkretny



Rys. 1. Zrzut ekranowy z programu Wireshark, który przechwycił sesję połączenia z serwerem WWW uruchomionym na lokalnym hoście – informacja o systemie operacyjnym jest podświetlona



Rys. 2. Katalog /boot. Widoczne pliki obrazów jądra systemu operacyjnego oznaczone numerami wersji

system komputerowy. Bardzo często ich poufność zależy od poufności wcześniej wymienionych rodzajów danych. Nie trudno wyobrazić sobie atakującego, który po zdobyciu danych dotyczących konta legalnego użytkownika systemu podszywa się pod niego i zapoznaje się z danymi, do których normalnie nie powinien mieć dostępu.

Chronić przed niepowołanym dostępem należy w zasadzie każdą informację przechowywaną i związaną z systemem operacyjnym. Zawsze istnieje możliwość, że intruz z pomocą, z pozoru błahych informacji uzyska dostęp do tych najważniejszych i najbardziej chronionych.

Uszkodzenie danych

Uszkodzenie danych ma miejsce wtedy, gdy nieuprawnieni użytkownicy zyskują możliwość zmiany, usunięcia lub dodania danych. Oznacza to między innymi możliwość zamiany istniejących danych na dane fałszywe.

Jest to jedno z największych i najtrudniejszych do wykrycia zagrożeń związanych z danymi, wymaga nie tylko konieczności rozpoznania fałszywych danych, ale i rozpoznania samego faktu uszkodzenia danych. Przykładem może być zapisanie w systemie plików

pliku zawierającego kod polecenia naruszającego w jakiś sposób bezpieczeństwo systemu. Jest to bardzo często spotykana sytuacja w przypadku zainfekowania komputera złośliwym oprogramowaniem. Zasadniczym celem takiego działania jest chęć zachowania w systemie plików kopii kodu wywołującego niepożądane działanie. Jedynym działaniem, które w tej sytuacji może pomóc jest długotrwałe, obciążające wydajność systemu komputerowego przeglądanie plików pod kątem zawartości kodów uznanych za szkodliwe. Wykorzystuje się w tym celu specjalnie utworzoną bazę próbek kodów uznanych za szkodliwe.

Innym zagrożeniem jest stworzenie w systemie operacyjnym dodatkowego konta systemowego lub zmiana konfiguracji programów świadczących usługi w systemie operacyjnym. Podobnie jak w przypadku zainfekowania złośliwym oprogramowaniem tak i tu niezbędne jest długotrwałe skanowanie plików. W tym przypadku jest to działanie trudniejsze gdyż, aby wykryć zmiany w systemie należy dysponować samodzielnie utworzoną bazą plików konfiguracyjnych systemu. Bez takiej bazy wykrycie zmian w systemie będzie się sprowadzało do ręcznego przeglądnięcia wszystkich plików konfiguracyjnych przez administratora systemu komputerowego, co jest działaniem długotrwałym i narażonym na błędy.

Innym rozwiązaniem jest nadpisanie plików konfiguracyjnych plikami przechowywanymi w kopii zapasowej. Rozwiązanie to ma jednak tę wadę, że usuwa także ślady dokonanych zmian, przez co może utrudnić nie tylko wskazanie sprawcy, ale i odnalezienie luki w systemie bezpieczeństwa, z wykorzystaniem której dokonano zmian. W efekcie, po dokonanej poprawce, zmiany mogą „pojawić" się znowu.

Często zmiana danych w systemie nie powoduje jakiś spektakularnych efektów w działaniu systemu i bez specjalistycznego oprogramowania wykrycie tej zmiany jest wręcz niemożliwe. W wielu przypadkach jedynym celem atakujących dany system jest uzyskanie do niego dostępu a nie jego uszkodzenie. System operacyjny, który nie potrafi zapewnić nam integralności danych jest mało użyteczny.

Blokada usługi

Blokada usługi to działanie polegające na zakłóceniu działania systemu operacyjnego w taki sposób, aby stał się on bezużyteczny, np. nie będzie odpowiadał na polecenia operatora.

Analogicznie jak w przypadku uszkodzenia danych jest to działanie trudne do zablokowania. Przykładem może być atak polegający na zarzuceniu konkretnego programu bardzo dużą ilością żądań. Próba ich przetworzenia prowadzi do takiego obniżenia wydajności, że z punktu widzenia użytkownika program przestaje działać.

Trudność w zablokowaniu takiego działania polega na konieczności oddzielenia żądań zwykłych użytkowników od żądań, których celem jest blokada usługi. Często jest to rzecz niemożliwa do realizacji, ponieważ żądania, których celem jest blokada usługi wyglądają dokładnie tak samo jak żądania zwykłych użytkowników.

W większości przypadków do blokady usługi dochodzi poprzez sieć komputerową. Nie jest to jednak regułą. W systemach operacyjnych działają programy, które, mimo że nie wykorzystują sieci komputerowej to pracują z wykorzystaniem architektury klient – serwer. Dobrym przykładem może być serwer X. W systemach z rodziny Linux zapewnia

on obsługę w formie graficznej. Jego klientami są menadżery okien np. Gnome, KDE itp. W sytuacji, w której zostaje on zarzucony żądaniami dochodzi do jego blokady, co można zauważyć na ekranie.

Zatem do blokady usługi dochodzi przy zarzuceniu programu żądaniami, których nie jest on w stanie przetworzyć. Działanie takie jest dość łatwe do wykrycia, lecz trudne do zablokowania. Żądania mogą bowiem pochodzić w dużej mierze od legalnych użytkowników chcących po prostu wykorzystać daną usługę. Zdarzają się jednak sytuacje, w których większość żądań pochodzi z jednego tylko źródła. W takiej sytuacji wystarczy odciąć dopływ żądań by odblokować usługę.

Jeśli jednak chroniony system operacyjny pada ofiarą ataku Denial of Service to często bywa tak, że żądania napływają z wielu różnych źródeł, co utrudnia ich odcięcie. Aby przeprowadzić taki atak napastnicy przejmują inne komputery i zmuszają do wysyłania żądań do innego systemu.

Przejęcie systemu przez wirusy

Z przejęciem systemu przez wirusy mamy do czynienia w sytuacji, w której system komputerowy wykonuje głównie kod oprogramowania wirusa a żądania operatora wykonuje w drugiej kolejności lub wcale.

Jest to sytuacja potencjalnie niebezpieczna gdyż operator często nie ma kontroli nad oprogramowaniem, co może prowadzić do nieuprawnionego dostępu do chronionych danych a ponad to system komputerowy może stanowić zagrożenie dla innych systemów, jeśli mamy do czynienia z pracą w sieci komputerowej.

System komputerowy przejęty przez wirusy, lecz odłączony od sieci komputerowej utrudnia pracę, lecz nie umożliwia przesłania chronionych danych do innego komputera a często także i „zarażania" innych systemów.

W większości przypadków przejęcie przez wirusy łatwo rozpoznać. System komputerowy nagle, bez konkretnych przyczyn zmniejsza wydajność pracy, nie jest to jednak regułą. Gdy napastnikowi zależy na ciągłym dostępie do danego komputera wówczas z premedytacją działa tak, aby nie zwrócić na siebie uwagi uprawnionego operatora systemu.

Wbrew pozorom przejęcie systemu przez wirusy nie jest błahym przypadkiem zagrożenia bezpieczeństwa. Często bowiem użytkownik nie potrafi lub nie może rozpoznać symptomów, a program antywirusowy jest bezradny do czasu wprowadzenia do jego bazy wirusów próbki kodu. W takiej sytuacji pomóc mogą tylko metody pośrednie np. analiza logów systemu operacyjnego, ruchu sieciowego i tym podobne.

MECHANIZMY OCHRONY SYSTEMÓW OPERACYJNYCH

Bezpieczeństwo fizyczne

Zasadniczą kwestią z punktu widzenia ochrony informacji przechowywanej i przetwarzanej przez system komputerowy jest bezpieczeństwo fizyczne, czyli zapewnienie urzą-

dzeniu pracy w warunkach uwzględniających brak czynników szkodliwych np. wysokiej temperatury, pyłów, przepięć i tym podobnych, jak i zabezpieczenie go przed kradzieżą lub zniszczeniem.

Współczesne systemy komputerowe w trakcie swojej pracy wydzielają duże ilości ciepła. Brak możliwości odprowadzenia wydzielanej energii cieplnej z urządzenia prowadzi do podnoszenia ich temperatury i w końcu do termicznego uszkodzenia elementów elektronicznych.

Najprostszą i najczęściej wykorzystywaną metodą odprowadzania ciepła jest wykorzystanie radiatorów chłodzonych przepływającym wokół nich powietrzem. W efekcie ciepło przepływa od nagrzanego kryształu krzemu, tworzącego układ elektroniczny, poprzez radiator do opływającego go powietrza. Taki przepływ jest możliwy, gdy powietrze ma niższą temperaturę niż chłodzony układ, co oznacza, że musi istnieć możliwość rozproszenia pobranego ciepła w otoczeniu. W sytuacji, gdy system komputerowy znajduje się w małym pomieszczeniu lub w pomieszczeniu znajduje się większa ilość urządzeń wydzielających ciepło zachodzi potrzeba zainstalowania klimatyzatora.

Z chłodzeniem powietrzem wiąże się także problem zapylenia. Powietrze z dużą zawartością pyłów może doprowadzić to do ich osadzania się na radiatorach oraz łożyskach wiatraków wymuszających przepływ powietrza, co w efekcie prowadzi do spadku wydajności tych urządzeń a nawet zatarcia pyłami.

Nadmiar pyłów w urządzeniu może również doprowadzić do zwiększenia oporów elektrycznych na skutek zabrudzenia styków krawędziowych i innych. Prowadzi to do błędów w działaniu urządzenia a nawet do jego unieruchomienia. I tu najlepszym rozwiązaniem jest klimatyzacja zaopatrzona w odpowiednie filtry powietrza. Alternatywnie można co jakiś czas usuwać zgromadzony w urządzeniu pył i kurz.

Komputery to urządzenia elektryczne, dlatego dostarczenie energii elektrycznej niespełniającej określonych norm może prowadzić do uszkodzenia systemu komputerowego lub braku jego działania. Ważnym elementem związanym z bezpieczeństwem systemu operacyjnego jest właściwie zaprojektowana sieć elektryczna. Powinna ona zawierać komplet zabezpieczeń chroniących system komputerowy przed przekroczeniem wartości krytycznych parametrów zasilania (np. przepięcia), a także zabezpieczających personel przed skutkami uszkodzenia izolacji (porażenie prądem elektrycznym).

Szczególnie ważny sprzęt komputerowy powinien być zasilany z innego obwodu niż inne ogólnie dostępne urządzenia np.: radia, czajniki itd., gdyż awaria tych urządzeń może doprowadzić do wyłączenia systemu komputerowego na skutek zadziałania zabezpieczeń. Istotnym elementem związanym z zasilaniem jest ciągłość działania, czyli zapewnienie dostarczenia energii z kilku niezależnych źródeł. W dużych centrach komputerowych zasilanie doprowadzane jest za pomocą co najmniej dwu niezależnych linii elektroenergetycznych przyłączonych do dwu różnych i niezależnych od siebie nawzajem punktów systemu elektroenergetycznego. Niezależnie od tego w samym centrum komputerowym istnieje system zasilania awaryjnego z UPS. W mniejszych ośrodkach stosuje się najczęściej punkt zasilania przyłączony do systemu elektroenergetycznego za pomocą jednej linii elektroenergetycznej oraz mały zasilacz UPS zapewniający energię na kilka godzin pracy.

Jedną z metod ochrony przed zniszczeniem będącym efektem zdarzeń losowych np. pożaru, powodzi itp. jest stosowanie rozmaitych czujników wykrywających takie zagrożenia.

Bardzo często oprócz zwykłego powiadamiania uruchamiają one także odpowiednie systemy zabezpieczające np. czujnik dymu, który uruchomi odpowiednie urządzenie gaśnicze wykorzystujące gazy obojętne takie jak: azot, dwutlenek węgla czy węglowodory halogenopodobne np. HFC-127ea.

Inną metodą ochrony jest tworzenie kopii zapasowych danych na urządzeniach znajdujących się w innym pomieszczeniu, a najlepiej budynku niż chroniony system.

System komputerowy należy także chronić przed kradzieżami a więc zamykać drzwi pomieszczenia, w którym znajduje się chroniony komputer, na klucz, stosować karty magnetyczne lub zamki elektromagnetyczne.

Bezpieczeństwo systemu plików

System plików jest mechanizmem ograniczającym, przechowującym oraz dającym dostęp do informacji zawartych w różnych urządzeniach pamięci masowych np.: dyskach twardych, CD-ROM'ach, pendrive'ach itp. W systemie plików oprócz danych użytkownika przechowuje się także dane związane z systemem operacyjnym np.: obraz jądra systemu, moduły jądra w systemie operacyjnym GNU/Linux itd. Co ważniejsze standardowo kod obsługujący systemy plików wbudowany jest w sam system operacyjny - stanowi jego część.

Omawiając kwestię bezpieczeństwa systemu operacyjnego, jako część szerszego zagadnienia związanego z ochroną informacji nie można pominąć kwestii bezpieczeństwa systemu plików. Od niego zależy bowiem nienaruszalność obrazu systemu operacyjnego przechowywanego w pamięci masowej a później uruchamianego.

Kluczową sprawą jest dostępność danych przechowywanych w pamięci masowej. Na skutek naruszenia spójności systemu plików, może dojść do wymieszania danych zawartych w kilku plikach lub zniknięcia z dysku niektórych plików.

Sprawdzenia spójności systemu plików można dokonać stosując program fdisk lub fsck celem przeglądnięcia zawartości całego dysku i naprawienia ewentualnych błędów (rys. 3).

Jednak w przypadku współczesnych dysków twardych o pojemnościach rzędu 1TB operacja taka może trwać długo, dlatego stosuje się rozwiązanie alternatywne –system plików z kroniką. Metoda ta polega na prowadzeniu dla systemu plików specjalnego dziennika – kroniki, w którym zapisuje się wszystkie operacje wykonywane na plikach. Zmiany wprowadzane do systemu plików są rejestrowane w dzienniku przed ich realizacją a także po zrealizowaniu. Jeśli więc w trakcie dokonywania zmian w systemie plików zabraknie prądu i nie zostaną one zakończone to po restarcie systemu będzie można zakończyć ich realizację, natomiast gdyby prądu zabrakło w trakcie zapisywania zmian do kroniki to wciąż będziemy

```
[root@komp ~]# fsck -v /dev/sdb8
fsck z pakietu util-linux-ng 2.17.2
e2fsck 1.41.10 (10-Feb-2009)
/dev/sdb8: czysty, 12/4194304 plików, 309301/16761811 bloków
[root@komp ~]#
```

Rys. 3. Przykład uruchomienia narzędzia fsck w systemie GNU/Linux

dysponowali spójnym systemem plików. Rozwiązanie to nie gwarantuje oczywiście, że nigdy nie dojdzie do utraty danych np. w wyniku zaniku zasilania, lecz zmniejsza prawdopodobieństwo takiego zdarzenia do minimum.

Kwestię bezpieczeństwa systemu plików należy rozpatrywać także z punktu widzenia dostępu do plików przez nieuprawnionych użytkowników podczas działania systemu operacyjnego. Wszystkie nowoczesne systemy plików posiadają mechanizmy pozwalające na dokonanie weryfikacji praw konkretnego użytkownika do konkretnego pliku. Prawami tymi są prawo do odczytu, zapisu oraz wykonania pliku. W większości przypadków taki prosty mechanizm weryfikacji praw wystarcza.

Dostęp do plików rozpatruje się również z punktu widzenia dostępu do nich podczas działania innego, obcego systemu operacyjnego. Ze zdarzeniem takim mamy do czynienia w sytuacji naruszenia fizycznego bezpieczeństwa komputera i jego rozruchu np. z płyty CD-ROM lub pendrive'a lub w przypadku, gdy w systemie komputerowym zainstalowano dwa lub więcej systemów operacyjnych mających dostęp do wszystkich partycji i dysków.

Dobrym rozwiązaniem w tej sytuacji jest zastosowanie szyfrowania. Szyfrować można zarówno całe partycje czy dyski jak i pojedyncze pliki i katalogi. Należy jednak pamiętać, że w przypadku zaszyfrowania całej partycji, na której znajduje się system operacyjny należy zadbać o prostą metodę, automatycznego podawania hasła. Można to zrealizować za pomocą pendrive'a z certyfikatem osobistym. Jeśli w trakcie uruchomienia systemu operacyjnego, nie będzie w którymś slocie USB pendrive'a, to system nie wystartuje gdyż nie dostanie się do głównego systemu plików. Co więcej po uruchomieniu obcego systemu plików na komputerze informacje będą bezpieczne gdyż będą się znajdowały na zaszyfrowanej partycji. Jedyną wadą rozwiązania jest konieczność asysty człowieka przy uruchamianiu komputera, co może być problemem w przypadku serwerów, które powinny działać non stop przez 24 godziny na dobę.

Rozwiązaniem pośrednim jest więc szyfrowanie tylko tych partycji lub katalogów, w których znajdują się ważne dane. Wadą tych rozwiązań jest możliwość zmiany konfiguracji systemu operacyjnego i uzyskania dostępu do tych danych przez nieuprawnionych użytkowników w trakcie normalnej pracy systemu.

Bezpieczeństwo systemu plików jest zagadnieniem kluczowym dla bezpieczeństwa informacji. Istnieje wiele metod zapewnienia tego bezpieczeństwa, lecz wszystkie one charakteryzują się narzuceniem dodatkowych operacji, które system operacyjny musi wykonać nim udostępni dane. Oznacza to, że projektując systemy bezpieczeństwa należy uwzględnić czy koszty ekonomiczne związane z zakupem wydajniejszych urządzeń są porównywalne z wartością przechowywanych i przetwarzanych danych oraz stopień prawdopodobieństwa narażenia systemu na poszczególne rodzaje zagrożeń.

Bezpieczeństwo sieci

Większość współczesnych systemów komputerowych pracuje w sieci komputerowej i tu bezpieczeństwo działających w nim programów wykorzystujących sieć komputerową jest równie ważne jak poprawna konfiguracja systemu operacyjnego do pracy w sieci.

Jeśli komputer jest przyłączony do kablowej sieci komputerowej LAN poprzez kartę sieciową wykorzystującą technologię Ethernet, dane z sieci docierają do karty sieciowej w postaci tzw. ramek Ethernetowych, czyli ciągów bitów, w których można wyróżnić nagłówek oraz dane. W nagłówku ramki Ethernetowej znajduje się między innymi adres MAC, czyli unikalny adres fizyczny każdej karty sieciowej. Konkretna ramka Ethernetowa jest odbierana, jeśli adres odbiorcy zgadza się z adresem karty sieciowej lub jest to tzw. adres rozgłoszeniowy, czyli skierowany do wszystkich.

Odebrane ramki są przekazywane do procedur obsługi tzw. stosu sieciowego, czyli zestawu funkcji, za pomocą których zaimplementowano obsługę poszczególnych protokołów sieciowych w systemie operacyjnym. W przypadku protokołów sieciowych nie mówi się już o ramce, lecz o pakiecie danych. Podobnie jak w przypadku ramki, pakiet składa się z nagłówka charakterystycznego dla konkretnego protokołu oraz danych. Jeden pakiet może być wynikiem złożenia danych zawartych w kilku ramkach Ethernetowych.

Cały proces przekazywania danych poprzez sieć realizuje system operacyjny. Kwestią zasadniczą, pod względem bezpieczeństwa jest ustalenie czy wszystkie informacje, z których korzystają procedury przekazywania danych są prawidłowe. Chodzi tu głównie o adres IP, maskę sieciową i adres bramy. Podmiana tych informacji może w efekcie poskutkować przekazywaniem pakietów sieciowych poprzez komputer, który pełni rolę podsłuchu.

Problem ten nabiera szczególnego znaczenia w przypadku pobierania tych informacji z wykorzystaniem protokołu dynamicznego konfigurowania hostów, czyli DHCP. Proces ten jest automatyczny i często nie dysponujemy metodą pozwalającą na stwierdzenie czy przebiegł prawidłowo, to jest, że otrzymaliśmy prawidłowe informacje.

Koniecznym staje się więc zastosowanie zabezpieczeń uniemożliwiających zakłócenie procesu konfiguracji hosta np.:

- konfiguracja serwera DHCP polegająca na spowodowaniu, aby DHCP przydzielał konkretny adres IP dla konkretnego adresu MAC. Rozwiązanie to staje się kłopotliwe przy dużej liczbie komputerów przyłączonych do serwera. Jego zaletą jest możliwość kontroli konfiguracji sieci z jednego miejsca.
- zastosowanie tak zwanego DHCP Snooping polegające na wykorzystaniu specjalnie oprogramowanego switcha sieci, tzw. switcha zarządzalnego. Switch dba, aby każdy host w sieci otrzymywał przypisany sobie adres IP, kontroluje adres MAC i adres IP w ramkach Ethernetowych i nagłówkach pakietów IP a także sprawdza czy kombinacja adres MAC – IP przychodzi do niego poprzez konkretne, ustalone przez administratora, gniazdo. Ponadto dba, aby po sieci krążyły odpowiedzi DHCP wysyłane tylko przez komputer przyłączony do określonego gniazda w switchu, a więc przez serwer wskazany przez administratora.

Niezależnie od powyższych rozwiązań konieczna jest także okresowa kontrola dziennika serwera DHCP pod kątem prawidłowości przyznawania adresów IP.

Ważną sprawą z punktu widzenia bezpieczeństwa systemu operacyjnego jest kontrola usług w nim działających. Chodzi tu nie tylko o kontrolę dostępu, tzn. kto i kiedy może korzystać z usługi, ale i o kontrolę samego faktu realizacji usługi.

Każda usługa – program realizowany przez system operacyjny może doprowadzić do narażenia systemu operacyjnego wynikające z faktu błędnej konfiguracji usługi. Aby je ograniczyć możemy zmniejszyć liczbę potencjalnych usługobiorców, określić godziny, w których realizowana jest usługa a także zmniejszyć jej prawa dostępu do plików systemowych. Zmniejszamy w ten sposób liczbę potencjalnych ataków a także umożliwiamy ustalenie sprawcy ataku, co ma fundamentalne znaczenie wobec odpowiedzialności karnej. Często powyższych ograniczeń nie da się nałożyć na usługę z poziomu jej pliku konfiguracyjnego i tu z pomocą przychodzi program superserwera xinetd (rys. 4).

Niezależnie od stosowanej metody uruchamiania zalecane jest użycie narzędzia nmap do kontroli, na jakich portach nasłuchuje system. Przykład użycia tego narzędzia pokazano na rysunku 5. Program nmap korzysta z protokołu ICMP do ustalenia nasłuchujących gniazd, a więc sprawdza komputer niejako z zewnątrz.

```
# default: off
# description: The CVS service can record the history of your source \
#              files. CVS stores all the versions of a file in a single \
#              file in a clever way that only stores the differences \
#              between versions.
service cvspserver
{
.       disable.        .       = yes
.       port.   .       .       = 2401
.       socket_type.    .       = stream
.       protocol.       .       = tcp
.       wait.   .       .       = no
.       user.   .       .       = root
.       passenv.        .       = PATH
.       server. .       .       = /usr/bin/cvs
.       env.    .       .       = HOME=/var/cvs
.       server_args.    .       = -f --allow-root=/var/cvs pserver
#.      bind.   .       .       = 127.0.0.1
}
```

Rys. 4. Plik konfiguracyjny jednej z usług obsługiwanych przez xinetd

```
Starting Nmap 4.20 ( http://insecure.org ) at 2011-01-04 11:28 CET
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 1691 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
10000/tcp open  snet-sensor-mgmt

Nmap finished: 1 IP address (1 host up) scanned in 0.168 seconds
```

Rys. 5. Wyniki zwrócone przez program nmap

Kwestia uruchomionych usług jest też ważna na etapie samej instalacji systemu operacyjnego, bowiem od rodzaju i ilości usług a także stopnia ich wykorzystania zależy sposób doboru sprzętu komputerowego oraz konfiguracja samego systemu operacyjnego.

Zakres uruchamianych usług w danym systemie operacyjnym jest na tyle kluczowy, że w planach bezpieczeństwa zawsze uwzględnia się kwestie związane z:

- potrzebą działania konkretnych usług sieciowych;
- zasadami dostępności usług sieciowych np. na żądanie lub stale;
- zakresem dostępności poszczególnych usług: dla wszystkich lub tylko dla niektórych;
- zakresem tworzenia zapisów zdarzeń zachodzących w programie usług sieciowych tak zwanych dzienników.

Niezależnie od powyższych ważna jest także okresowa kontrola dzienników usług sieciowych pod kątem nieprawidłowości związanych z bezpieczeństwem.

Bezpieczeństwo sieci granicznej

Lokalne sieci komputerowe są z reguły przyłączone do sieci Internet. Oznacza to, że systemy operacyjne pracujące w tych komputerach są narażone na zagrożenia, o których mowa w rozdziale 2 niniejszej pracy.

Celem ochrony przed tymi zagrożeniami stosuje się zapory sieciowe, których działanie polega na ograniczeniu przepływu danych z jednego systemu operacyjnego do drugiego. Dzielą się one na:

- ściany ogniowe w warstwie sieciowej – bramy filtrowania;
- ściany ogniowe w warstwie transportu;
- ściany ogniowe w warstwie aplikacji.

Celem działania bramy filtrowania jest podjęcie decyzji co do dalszych losów pakietu IP na podstawie adresu IP nadawcy i odbiorcy. Ściana ogniowa w warstwie sieci może zadecydować o: zagubieniu pakietu bez wysyłania informacji zwrotnej; zagubieniu pakietu z wysłaniem informacji zwrotnej; przekazaniu pakietu do następnego punktu; rejestracji pakietu. Ostatnie działanie może być realizowane łącznie z wszystkimi poprzednimi.

Celem działania ściany ogniowej w warstwie transportu jest filtrowanie pakietów na podstawie tożsamości użytkownika. Rozwiązania takie są użyteczne, gdy w lokalnej sieci istnieją takie obszary, które wymagają bardziej restrykcyjnego podejścia od innych. Zasadniczą wadą tego rozwiązania jest konieczność doinstalowania na wszystkich komputerach korzystających z takiego filtru specjalnego oprogramowania.

Ściany ogniowe w warstwie aplikacji, popularnie nazywane proxy, mają na celu filtrowanie pakietów na podstawie ich zawartości. Rozwiązanie to pozwala np. przeglądać przychodzące dane pod kątem zawartości wirusów. Dodatkową zaletą tych rozwiązań, jest także buforowanie przychodzących danych, co może być wykorzystane do przyspieszenia działania sieci. Wykorzystuje się tutaj fakt, że połączenia sieci LAN są dużo szybsze niż połączenia pomiędzy siecią Internet a LAN.

Ze względu na sposób budowy ściany ogniowe można podzielić na:

- Filtr pakietów, czyli rozwiązanie działające jako brama filtrowania. Cechą charakterystyczną jest takie umiejscowienie filtra w strukturze sieci, że wymusza ono przepływ całego ruchu przez filtr. Zasadniczymi wadami tego rodzaju firewalli są: możliwość podszywania się pod adres IP występujący w sieci LAN, co prowadzi do przepuszczania pakietów normalnie blokowanych; reguły filtracji oparte tylko o zawartość nagłówka pakietu; mało rozbudowane możliwości zapisu dzienników.
- Duall homed gateway - to rozwiązanie wykorzystujące komputer wyposażony w dwa interfejsy sieciowe. Pozwala ono na dokonywanie filtrowania z wykorzystaniem warstwy sieciowej, transportu i aplikacji a także stosowanie usługi typu NAT. Zasadniczą wadą tego rozwiązania jest koszt – wymaga ono bowiem wydajnego komputera. Dodatkowo przejęcie takiego komputera prowadzi do utraty zabezpieczenia.
- Screened – subnet to rozwiązanie łączące filtr pakietów i dual home gateway. Ma ono wiele zalet, do których należy między innymi: ochrona komputera realizującego filtrowanie w warstwie sieci, transportu i aplikacji przez filtr pakietów; duża pewność działania zabezpieczenia, gdyż do całkowitej utraty zabezpieczenia można doprowadzić jedynie poprzez przejęcie wszystkich urządzeń. Wadami tego rozwiązania są wysokie koszty oraz trudności w odnalezieniu błędu konfiguracji takiego zabezpieczenia.

Analizując rozwiązania zapór sieciowych można stwierdzić, że najlepszym pod względem dokładności działania jest rozwiązanie typu screened – subnet. Ze względu na duże koszty wskazanego rozwiązania, stosuje się rozwiązania nieco mniej rozbudowane np. rezygnuje się z filtracji w warstwie transportu.

Systemami operacyjnymi, które najczęściej są wykorzystywane jako podstawa do budowy zapory sieciowej jest GNU/Linux lub BSD. Wynika to stąd, że jądra tych systemów operacyjnych oferują niezbędną funkcjonalność do realizacji bramy filtrującej a także dodatkowych funkcji np. tłumaczenia adresów sieciowych – NAT. Dodatkowo istnieją pakiety oprogramowania opracowane pod te systemy, które oferują filtracje w pozostałych warstwach np. Squid, Fwtk itd. Oznacza to, że istnieje możliwość stosowania nietypowych rozwiązań zapór sieciowych trudniejszych do złamania.

Bezpieczeństwo aplikacji

Sam system operacyjny stanowi jedynie podstawę do przetwarzania danych, zapewnia miejsce ich składowania oraz ujednolica i ułatwia obsługę urządzeń peryferyjnych niezbędnych do ich przetwarzania a przetwarzaniem danych zajmują się aplikacje w nim uruchomione, czyli odpowiedzialność za bezpieczeństwo danych spada także po części na owe aplikacje.

Najbardziej podstawowym zagrożeniem, na jakie narażone są aplikacje użytkowe są inne programy określane często ogólnym mianem wirusów. Zgodnie z nieformalną definicją wirusa podaną przez dr Fredricka B. Cohena „wirus jest programem zdolnym do zarażania innych programów, poprzez modyfikowanie ich i dołączanie do nich własnej, być może zmo-

dyfikowanej kopii" [9]. Jest to definicja, która w miarę dobrze opisuje współczesne wirusy komputerowe występujące w wielu różnych formach i działające na wiele różnych sposobów.

Istnieje wiele różnych odmian wirusów, które mają różne cele działania od złośliwego utrudniania pracy, przez infekowanie innych komputerów po przesyłanie ważnych danych poprzez sieć komputerową.

Kluczową sprawą jest fakt, że wszystkie kody wirusów pracują w uruchomionym systemie operacyjnym. Oznacza to, że mogą mieć dostęp do wszystkich danych, jakie są przechowywane w komputerze, również tych zaszyfrowanych. Aby można było skorzystać z zakodowanych danych trzeba je najpierw odszyfrować, co często robi dobrowolnie użytkownik posłusznie wpisując hasła i wskazując odpowiednie certyfikaty. Sam wirus korzysta z odszyfrowanej informacji przechowywanej gdzieś w pamięci komputera.

Jedynym rozwiązaniem zabezpieczającym nas przed wirusami jest stosowanie oprogramowania antywirusowego. Programy te przeglądają pamięć operacyjną i pamięci masowe w poszukiwaniu kodu wirusa wykorzystując w tym celu bazę zawierającą próbki kodów znanych wirusów. Jeśli któraś z próbek wstępnie pasuje to dokonywana jest dokładniejsza analiza.

Działanie takie jest oczywiście bardzo czasochłonne. Nowoczesne programy antywirusowe wykonują je więc tylko raz zaraz po zainstalowaniu zapisując jednocześnie sumy kontrolne plików niezainfekowanych wraz z ścieżkami dostępu do nich do specjalnej bazy. Sumy kontrolne są generowane w taki sposób, aby były unikalne dla konkretnej zawartości, dla której zostały wygenerowane. Oznacza to, że drobna zmiana tej zawartości prowadzi do zmiany wartości sumy kontrolnej. Fakt ten wykorzystywany jest przez programy antywirusowe.

Ze względu na to, że generacja sumy kontrolnej trwa bardzo krótko to przy każdym skanowaniu systemu w poszukiwaniu wirusów programy te generują sumy kontrolne sprawdzanych plików i sprawdzają je z tymi zarejestrowanymi w bazie. W przypadku wykrycia różnic następuje dokładne sprawdzenie pliku z użyciem bazy wirusów. Taka metoda oszczędza czas i moc obliczeniową systemu. Pomimo tego programy do wykrywania wirusów i tak mają dużo pracy.

Celem zabezpieczania systemu przed infekcją programy antywirusowe muszą także przeglądać zawartość podłączanych do systemu pendrive'ów, innych pamięci masowych oraz danych ściąganych poprzez sieć komputerową. Otwarcie strony w przeglądarce powoduje bowiem ściągnięcie do katalogu tymczasowego na dysku twardym komputera całej jej zawartości, wśród której może znajdować się wirus.

Dodatkowo skuteczność oprogramowania antywirusowego uzależniona jest od zawartości bazy wirusów. Z tego powodu jednym z zaleceń dawanych użytkownikom tych programów jest częsta aktualizacja baz wirusów. Większość programów robi to automatycznie.

Instalacja oprogramowania od sprawdzonych producentów lub podpisanego cyfrowo a także ostrożne obchodzenie się z danymi pobranymi z sieci, w szczególności chodzi tu o załączniki do poczty elektronicznej mogące zawierać wirusy, zmniejsza ryzyko tzw. zawirusowania.

Większość technologii sieciowych, których działanie uzależnione jest od wykonania kodu po stronie użytkownika pracuje w tak zwanych sandboxach. Jest to technika pozwalają-

ca na izolowanie kodu w trakcie jego wykonywania. W dużym uproszczeniu sandbox (*z ang.* piaskownica), w którym izolowany jest obcy kod, ma uniemożliwić dokonanie przeskoku apletu do kodu spoza piaskownicy a także wyeliminować do minimum możliwość interakcji z samym systemem operacyjnym.

Dostęp i uwierzytelnianie

Celem uwierzytelniania jest ustalenie przez system operacyjny, z kim ma do czynienia i wskazanie na tej podstawie praw, jakimi ten ktoś dysponuje. Operację uwierzytelniania przeprowadza się w trakcie logowania do systemu. Ogólnie rzecz biorąc uwierzytelnianie polega na uzyskaniu od użytkownika:

- określonej informacji np. hasła;
- określonej rzeczy np. karty magnetycznej z zapisaną informacją;
- jakiejś jego cechy biometrycznej np. odcisku palca.

Pierwsza z wymienionych opcji jest najprostsza i najczęściej stosowana. Wymaga podania przez użytkownika jego identyfikatora w systemie – loginu oraz znanego tylko przez niego hasła. System operacyjny porówna dane wprowadzone przez użytkownika z danymi przechowywanymi w bazie użytkowników. Jeśli się zgadzają uruchamia powłokę systemową: graficzną lub tekstową, jeśli nie wyświetla stosowny komunikat. Z punktu widzenia bezpieczeństwa całego procesu należy zadbać między innymi o komunikaty o właściwej treści. System powinien informować użytkownika o nieudanej próbie uwierzytelnienia, lecz nie powinien podawać dokładnej przyczyny niepowodzenia. Utrudni to przeprowadzenie próby odgadnięcia hasła metodą prób i błędów. Ponadto wprowadzanie błędnego loginu i hasła po kilku pod rząd nieudanych próbach powinno skutkować dezaktywacją lub czasową blokadą możliwości zalogowania. Podczas wpisywania hasła komputer nie powinien wyświetlać żadnych znaków. Utrudnia to zwyczajne podpatrzenie hasła.

Opisana powyżej metoda uwierzytelniania jest najprostsza do zaimplementowania, lecz również najłatwiejsza do złamania. Zgodnie z badaniami opisanymi w pracach [10, 11] wystarczy sporządzić listę prawdopodobnych haseł złożoną z imion, nazwisk, nazw ulic i miast, słów z małych słowników, wulgaryzmów a także krótkich ciągów literowych by mieć pewność, że znajdzie się na niej około 86% stosowanych haseł. Istnieje, co prawda możliwość wymuszania na użytkowniku stosowania bardziej rozbudowanych haseł, lecz skutkuje to często zapisaniem hasła na karteczce, którą przylepia się do monitora.

Druga z wymienionych opcji polega na podawaniu przez użytkownika określonej rzeczy. Takie rozwiązanie stosowane jest np. w bankomatach. Użytkownik, klient banku, wprowadza do odpowiedniego slotu kartę magnetyczną i wpisuje swój PIN. Jeśli dane odczytane z karty oraz wprowadzone przez użytkownika odpowiadają tym przechowywanym w bazie danych banku to uzyskuje się dostęp do systemu. Można tu zauważyć pewną analogię do systemu z loginem i hasłem. W tym przypadku mamy do czynienia jednak z dwoma hasłami. Jednym długim i unikalnym zapisanym na karcie magnetycznej a drugim podawanym w formie PIN. Jest to na tyle dobra metoda, że do tej pory opracowano tylko metody kopiowa-

nia danych z karty i nagrywania naciskanych przez klienta klawiszy. Nikomu nie udało się przeprowadzić ataku w formie metody prób i błędów.

Pewną odmianą tej metody jest stosowanie tzw. kart inteligentnych, czyli wyposażonych w mikroprocesor. Uwierzytelnianie przy pomocy takich kart przeprowadzane jest jako szereg zapytań i odpowiedzi udzielanych przez kartę.

Trzecia z powyższych opcji polega na pobraniu od użytkownika pewnych danych biometrycznych służących uwierzytelnianiu. Mogą to być: odcisk palca, skan tęczówki oka, identyfikacja cech głosu itp. Jest to oczywiście najbardziej skuteczna, ale i najdroższa metoda. Jej zasadniczą wadą jest uzależnienie dopuszczenia użytkownika do systemu od cech, które mogą ulec zmianie np. w wypadku.

Wszystkie powyższe metody mają jednak słaby punkt w przypadku próby dostępu do systemu poprzez sieć komputerową, są bowiem możliwości podsłuchania danych lub zwyczajnego podszycia się pod zabezpieczany system.

Jedynym rozwiązaniem tego problemu jest uwierzytelnianie uczestników wymiany danych oraz ich komputerów za pomocą specjalnych certyfikatów a także szyfrowanie danych. Metoda ta polega na wymianie zestawu danych np. nazwy użytkownika, nazwy organizacji oraz nazwy domenowej hosta, z którym uzyskujemy połączenie. Ów zestaw nosi nazwę certyfikatu i jego zawartość jest poświadczona przez firmę trzecią, co jest sprawdzane w trakcie połączenia. Po upewnieniu się, że po drugiej stronie znajduje się maszyna i użytkownik, z którym chcemy nawiązać połączenie następuje uzgodnienie mechanizmu szyfrowania danych. Tym sposobem w sieci Internet powstaje zaszyfrowany kanał transferu informacji, którego zakończenia są przyłączone do zaufanych komputerów. Szyfrowanie takie wymaga istnienia w sieci firm, które zajmują się zawodowo poświadczaniem certyfikatów.

Rozwiązanie to stosowane jest jako rozszerzenie wielu znanych protokołów. O tym, że jest wykorzystywane informuje litera s na końcu skrótu nazwy protokołu, np.: https, smtps. Podobnie zamiast zwykłego protokołu telnet stosuje się protokół ssh.

Monitorowanie i audyt systemu, jako metoda ochrony

Jedną z ważniejszych czynności, jakie powinien realizować administrator systemu jest przegląd dzienników systemu operacyjnego. Działanie takie pozwala na wykrycie ewentualnych problemów i prób włamania i w związku z tym daje możliwość poprawy bezpieczeństwa systemu. Co prawda istnieje możliwość spenetrowania systemu w sposób pozwalający na unikniecie zapisów w dziennikach, lecz trudno tak zmodyfikować pliki historii by było to niezauważalne.

Kwestię monitorowania i audytu systemu operacyjnego przedstawimy na przykładzie systemu GNU/Linux. W systemie tym istnieje usługa *syslog*, której celem jest zbieranie danych pozwalających na diagnostykę systemu. Pliki konfiguracyjne *syslog* pozwalają na rozbicie informacji na pliki, z których każdy zawiera inny jej rodzaj. Standartowo dane zapisywane są w plikach:

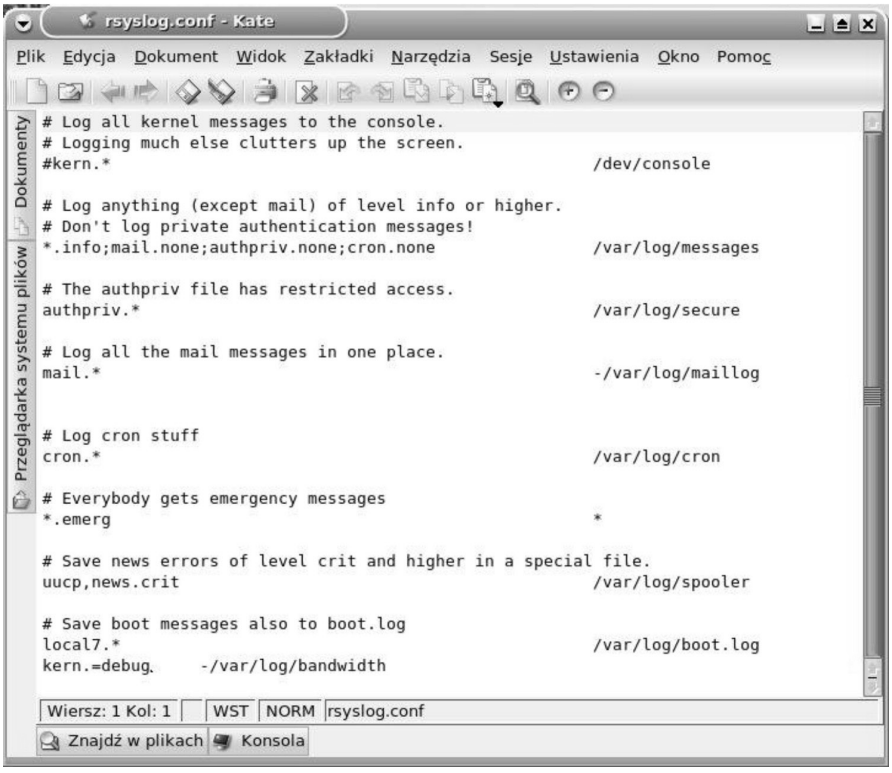
- Messages – ogólne informacje o działaniu systemu i różnych usługach;
- Secure – informacje z zakresu bezpieczeństwa systemu;

– Maillog – informacje od programu sendmail;
– Spooler – informacje od innych usług np. synchronizacji czasu;
– boot.log – informacje pojawiające się w czasie startu systemu;

Następcą programu *syslog* jest program *rsyslog* (Rys. 6), którego pozbawiono kilku wad poprzednika między innymi możliwości zablokowania dysku twardego danymi zapisywanymi do programu syslog.

Ze względu na to, że tworzone pliki są dość obszerne system regularnie uruchamia skrypt logrotate, który zapisane pliki przenosi do plików z rozszerzeniem odpowiednio 1,2 itd. oraz tworzy nowy czysty plik. Ilość plików z rozszerzeniami w postaci cyfr jest różna i zależy od ustawień skryptu. Z reguły jest to siedem pozycji.

Usługa *syslog* zapisuje bardzo dużą ilość danych. Przeglądanie czystych, nieprzetworzonych plików dzienników jest uciążliwe i narażone na błędy lub pominięcie ważnych informacji. Z tego powodu wykorzystuje się dodatkowe narzędzia np. *swatch* lub *logcheck* [rys. 7], których celem jest okresowe przeglądanie plików dzienników i poszukiwanie określonych wpisów. Wszystkie odnalezione wpisy narzędzia te wysyłają w formie emaila pod podany adres. W efekcie administrator systemu dostaje z każdego nadzorowanego systemu raport o problemach i zdarzeniach naruszających bezpieczeństwo.



Rys. 6. Okno edytora z plikiem konfiguracyjnym rsyslog.conf

Ważną czynnością, która powinna być również wykonywana co jakiś czas jest audyt integralności plików konfiguracyjnych i innych systemu. Pracę tę może wykonać narzędzie o nazwie *tripwire*. Działanie tego narzędzia przypomina pracę programu antywirusowego, gdyż przegląda ono wskazane przez administratora pliki i sprawdza czy od czasu ostatniego audytu doszło do zmiany ich zawartości. Jeśli tak to szczegółowy raport na ten temat wysyłany jest do administratora.

Niezależnie od audytu i monitoringu samego systemu operacyjnego ważnym zadaniem jest też monitorowanie sieci. Monitoring sieci pozwala wykryć takie zdarzenia, w których dochodzi do transferu danych lub innych informacji np. spamu. Jednym z narzędzi, które mogą być użyte do tego celu jest *Ethereal* (Wireshark – rys. 1). Pozwala on na przechwytywanie i przeglądanie pakietów przesyłanych w sieci. Narzędzie to jest bardzo użyteczne nie tylko przy okresowym monitoringu sieci, ale także przy sprawdzaniu poprawności konfiguracji poszczególnych usług sieciowych.

Ważnym zadaniem administratora systemu jest także upewnienie się, że nadzorowany system operacyjny nie podlega właśnie zdalnemu skanowaniu pod kątem uruchomionych usług lub luk bezpieczeństwa. Narzędziem, które można do tego wykorzystać jest *PortSentry*. Pozwala ono wykryć fakt sprawdzania systemu, stworzyć dziennik zdarzeń oraz wysłać powiadomienie do administratora.

```
################### Logwatch 7.3.6 (05/19/07) ####################
       Processing Initiated: Tue Jan 11 15:46:30 2011
       Date Range Processed: yesterday
                             ( 2011-Jan-10 )
                             Period is day.
     Detail Level of Output: 0
             Type of Output: unformatted
         Logfiles for Host: sala307dd.szkola
 ##################################################################

--------------------- httpd Begin ------------------------

Requests with error response codes
   404 Not Found
      /favicon.ico: 6 Time(s)
      /nabor-fronton/: 1 Time(s)

---------------------- httpd End -------------------------


--------------------- pam_unix Begin ------------------------

su:
   Sessions Opened:
      (uid=500) -> root: 2 Time(s)

su-l:
   Sessions Opened:
      karont(uid=500) -> root: 2 Time(s)


---------------------- pam_unix End -------------------------
```

Rys. 7. Codzienny raport programu logwatch

Raz na jakiś czas administrator systemu powinien dokonać też audytu systemu pod kątem podatności na włamania. Służy do tego narzędzie *Nessus*, które za pomocą skryptów realizuje algorytmy znanych włamań. Audyt taki ma na celu, nie tylko wykrycie luk w konfiguracji bezpieczeństwa, ale i wykrycie ewentualnego pojawienia się nowych np. na skutek aktualizacji niektórych programów.

WNIOSKI

Ochrona systemu operacyjnego, mimo że sama w sobie jest tylko częścią szerszego zagadnienia, jakim jest ochrona informacji, jest zagadnieniem skomplikowanym i rozbudowanym. Wynika to głównie z ilości oraz rozmaitości zagrożeń, na jakie narażony jest system operacyjny. Są nimi: udostępnianie poufnych danych, uszkodzenie danych, blokada usługi oraz przejęcie systemu przez wirusy. Każde z powyższych zagrożeń może pojawić się łącznie z innymi, co prowadzi do wzrostu ich ilości.

Z tego względu mechanizmy ochrony systemu zostały podzielone na warstwy bezpieczeństwa: fizycznego, systemu plików, sieci, sieci granicznej, aplikacji, dostępu i uwierzytelniania. Każda z warstw posiada swoje mechanizmy ochrony i wymaga okresowego monitoringu działania a także audytu celem upewnienia się, że działa poprawnie. Podział na warstwy wprowadzono celem ułatwienia opracowania mechanizmów bezpieczeństwa. Od poprawności konfiguracji każdej z warstw zależy bezpieczeństwo całego systemu operacyjnego.

Opisane powyżej zagadnienie dobrze obejmuje tzw. polityka bezpieczeństwa, czyli dokument opisujący w spójny sposób zbiór precyzyjnych reguł i procedur, które są wykorzystywane do organizowania i zarządzania zasobami oraz systemami informatycznymi. Tworząc taki dokument, osoba odpowiedzialna za bezpieczeństwo informacji, musi uwzględnić w nim sposób zabezpieczania poszczególnych grup lub konkretnych systemów operacyjnych z uwzględnieniem roli, jaką pełnią one w całym systemie informatycznym. Oznacza to konieczność opracowania integralnej koncepcji zabezpieczenia z uwzględnieniem wszystkich warstw.

Na zakończenie warto wspomnieć o pewnym rodzaju zagrożenia, które opisano w wrześniowym numerze Świata Nauki z 2010 r. Zagrożenie to polega na takiej modyfikacji układów scalonych, z których zbudowany jest system komputerowy, aby pełniły one funkcje wirusa lub tylnego wejścia do systemu operacyjnego. W zasadzie, jeśli modyfikacja taka zostanie wykryta to jedyne, co można zrobić, to wyłączyć komputer. Autor artykułu opisuje, co prawda, kilka metod ochrony przed tego rodzaju zagrożeniami, lecz wszystkie sprowadzają się do rozbudowy istniejących układów scalonych o dodatkowe moduły realizujące ochronę przed „chipem trojańskim".

Kwestia bezpieczeństwa systemów operacyjnych jest otwarta. Wciąż, bowiem pojawiają się nowe zagrożenia a także rozwiązania pozwalające im zapobiegać. Oznacza to, ze bezpieczeństwo systemu operacyjnego to proces a nie stan i aby uzyskać właściwy poziom tego bezpieczeństwa trzeba na bieżąco śledzić wszystkie doniesienia o zagrożeniach oraz zabezpieczeniach.

BIBLIOGRAFIA

1. Liderman K.: Podręcznik administratora bezpieczeństwa teleinformatycznego. Wydawnictwo MIKOM, Warszawa 2003.
2. Tanenbaum A.S.: Systemy operacyjne. Wydawnictwo HELION, Gliwice 2010.
3. Hontanon R.J.: Bezpieczeństwo systemu Linux. Wydawnictwo MIKOM, Warszawa 2002.
4. Dostalek L. Bezpieczeństwo protokołu TCP/IP. Wydawnictwo Naukowe PWN, Warszawa 2006.
5. Szor P. Wirusy rozpoznawanie i obrona. Wydawnictwo Naukowe PWN, Warszawa 2006.
6. Lowe R. Kernel Linux – przewodnik programisty. Wydawnictwo HELION, Gliwice 2004.
7. Benevenuti C. Linux – mechanizmy sieciowe. Wydawnictwo HELION, Gliwice 2006.
8. Von Hagen W. Systemy plików w Linuksie. Wydawnictwo HELION, Gliwice 2002.
9. Dr Cohen F.B. A short Course on Computer Viruses. Wiley Professional Computing, Nowy Jork 1994.
10. Morris R., Thompson K. Password Security: A core history. Tom 22 Commun. of the ACM, 1979: 594–597.
11. Klein D.V. Foiling the Crakcer: A survey of, and Improvments to, Password Security. UNIX Security Workshop II 1990.
12. Villasenor J.: Haker w sercu komputera. Świat nauki, nr 9, 2010: 70–75.

ANALYSIS OF MEANS AND METHODS OF PROTECTION THE OPERATING SYSTEMS

Summary

The means and methods of protection the safety of operating systems were analyzed in this study. Protection of the operating system is only part of a wider problem – protection of the information. At the beginning, the risks to which the operating system is exposed were described indicating that it should be covered the extent of protection. Then, the analysis of methods of protection was done, pointing to the hazard, which prevents. Protecting the operating system is implemented using their own mechanisms as well as using external programs. In this paper the main attention is focused on operating system security mechanisms and specialized programs were discussed in lesser extent.

Key words: operating system, information assurance, data security, system administration.