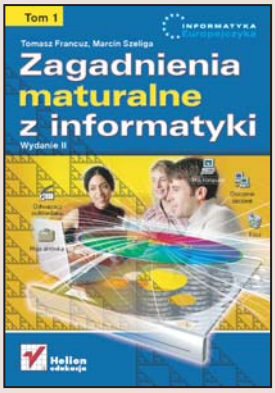
Zagadnienia maturalne z informatyki. Wydanie II. Tom I



Autorzy: Tomasz Francuz, Marcin Szeliga
ISBN: 83-7361-925-9
Format: B5, stron: 336

Przystąp do matury odpowiednio przygotowany

- Opanuj wszystkie wymagane zagadnienia
- Rozwiąż przykładowe zadania
- Poznaj zasady działania komputera

Jeśli przygotowujesz się do egzaminu maturalnego z informatyki, chcesz pogłębić wiedzę informatyczną, którą zdobywasz w szkole, lub poznać budowę komputera i zasady programowania – zajrzyj do tej książki. Znajdziesz tu wszystkie informacje, jakich możesz do tego potrzebować. Przeczytasz o głównych elementach komputera, urządzeniach peryferyjnych, systemach operacyjnych, sieciach, aplikacjach i programowaniu.

Opracowując „Zagadnienia maturalne z informatyki. Wydanie II", autorzy wykorzystywali materiały udostępnione przez Ministerstwo Edukacji Narodowej, zadania z olimpiad informatycznych oraz podręczniki szkolne. Dzięki temu przedstawione w książce zagadnienia są dostosowane do zakresu tematycznego zadań maturalnych.

- Budowa komputera
- Urządzenia peryferyjne
- Systemy operacyjne i ich zadania
- Rodzaje sieci komputerowych
- Internet
- Bezpieczeństwo systemów komputerowych i danych
- Prawa autorskie i zagadnienia etyczne związane z informatyką
- Arkusze kalkulacyjne
- Bazy danych i język SQL
- Grafika komputerowa

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Tom I

Rozdział 5.

Bezpieczeństwo systemów komputerowych

W pierwszych systemach komputerowych problem bezpieczeństwa praktycznie nie istniał — dostęp do nich miała bardzo ograniczona grupa ludzi (pracownicy firm komputerowych oraz wykładowcy i studenci uczelni technicznych), a udostępniane w tych sieciach fachowe zasoby były traktowane jak wspólne, w dobrym tego słowa znaczeniu.

W ciągu ostatnich lat nastąpił lawinowy wzrost liczby ataków na komputery — **w 2003 roku odnotowano ich ponad 900 milionów**, pięć lat wcześniej, **w roku 1998, „tylko" 100 milionów**. Szacunkowe **dane z roku 1990 mówią o kilkudziesięciu tysiącach** ataków.

Sytuacja zmieniła się wraz z upowszechnieniem komputerów i internetu oraz coraz liczniejszymi zastosowaniami komputerów. Dziś na podłączonym do sieci komputerze przechowujemy prywatne dane (nie tylko listy, ale również zdjęcia, deklaracje podatkowe, hasła do kont bankowych itd.), a uszkodzenie czy po prostu przerwa w działaniu komputera uniemożliwiają nam pracę i wiążą się ze stratą naszego czasu i pieniędzy. Co najważniejsze, dostęp do sieci, zamiast wąskiego grona fachowców, zyskały szerokie masy, w tym osoby, które z nudów, głupoty lub złośliwości próbują zaatakować nasze komputery, a internet stał się gigantyczną agencją reklamową.

Typowe zagrożenia

Żeby skutecznie chronić system komputerowy, trzeba poznać typowe zagrożenia. Ze względu na sposób przeprowadzenia ataku, dzielimy je na:

1. **Przypadkowe**, automatycznie przeprowadzane za pomocą specjalnych programów i niewymierzone w konkretny system (np. wirusy atakujące wszystkie, a nie wskazane komputery).
2. **Celowe**, też z reguły przeprowadzane przy użyciu specjalistycznych narzędzi, ale bardzo rzadko w całości zautomatyzowane i wymierzone w konkretny system (np. zdobycie przesyłanych w sieci informacji uwierzytelniających i wykorzystanie ich do złamania hasła użytkownika).

Wirusy

Wirusy to niewielkie, z reguły dołączane do innych programów lub plików programy, które są uruchamiane bez wiedzy użytkownika komputera. Działanie wirusów sprowadza się do dwóch czynności:

1. Niewidocznego dla użytkowników rozpowszechniania się (infekowanie kolejnych komputerów).
2. Ujawnienia się i zaatakowania komputera (rodzaj ataku zależy jedynie od umiejętności, fantazji i złośliwości twórcy wirusa — może to być wyświetlanie denerwujących komunikatów, skopiowanie określonych danych, uszkodzenie systemu operacyjnego czy przeprowadzenie ataku na inny komputer).

Jedyną skuteczną ochroną przed wirusami jest bezustanne sprawdzanie, czy uruchamiane i kopiowane pliki nie zostały wcześniej zainfekowane. Zadanie to wykonują skanery antywirusowe — programy, które chronią przed uruchomieniem wirusa, i które umożliwiają sprawdzenie, czy na dyskach twardych nie znajdują się zainfekowane pliki.

Niechciane programy

Wirusy to tylko jedne z wielu niechcianych (tj. takich, których użytkownik świadomie nie uruchomiłby na swoim komputerze) programów. Do niechcianych programów zaliczamy ponadto:

1. **Programy szpiegowskie** (ang. *SpyWare*) — ich działanie polega na zbieraniu informacji, które mogą ułatwić atak na komputer albo zostać wykorzystane przeciwko jego użytkownikowi — na przykład haseł do systemu operacyjnego, odwiedzanych stron internetowych czy serwerów pocztowych, numerów kart kredytowych, danych o konfiguracji systemu operacyjnego, czy po prostu sekwencji naciskanych przez użytkownika klawiszy.

Od połowy 2003 roku gwałtownie wzrasta liczba programów, których zadaniem jest ujawnienie atakującemu poufnych danych. Jednocześnie programy tego typu są coraz groźniejsze — np. **Bugbear.B** rozprzestrzeniał się w postaci załącznika do wysyłanych przez siebie wiadomości elektronicznych, które dzięki wykorzystaniu błędu w programach Microsoft Outlook i Microsoft Outlook Express były odczytywane i wykonywane bez wiedzy użytkownika. Po uruchomieniu Bugbear.B wyłączał **znane sobie skanery antywirusowe** i zarażał znajdujące się na dysku twardym pliki.

2. **Programy dodatkowe** (ang. *AdWare*) — instalowane albo z darmowymi bądź demonstracyjnymi wersjami najróżniejszych programów, albo automatycznie, bez wiedzy odwiedzającego strony WWW użytkownika, programy o najróżniejszym działaniu — od wyświetlania reklam, poprzez zbieranie informacji o odwiedzanych stronach WWW, aż po zmiany w ustawieniach programów i systemu operacyjnego.

Niektóre z takich programów są wykrywane i usuwane przez skanery antywirusowe, jednak zdecydowana większość nie jest uznawana za wirusy, co nie oznacza, że nie są one niebezpieczne. Dlatego **oprócz skanera antywirusowego każdy komputer powinien być chroniony za pomocą specjalnego programu antyszpiegowskiego.**

Ujawnienie hasła

W większości systemów komputerowych hasło jest jedynym sposobem sprawdzenia, czy dana osoba jest tą, za którą się podaje. Wynika z tego, że jeżeli ktokolwiek pozna Twoje hasło, to będzie mógł skutecznie podszyć się pod Ciebie i uzyskać w ten sposób dostęp do wszystkich Twoich danych i skonfigurowanych przez Ciebie programów. Dlatego **należy używać wyłącznie bezpiecznych haseł**.

Bezpieczne są takie hasła, które znasz tylko Ty, a które nie mogą zostać zdobyte przez inne osoby. W większości wypadków do zdobycia hasła atakujący wykorzystują specjalne programy, umożliwiające sprawdzanie kilkudziesięciu, a nawet kilkuset tysięcy kombinacji na minutę, tak więc **hasło typu *Jacek1* albo *1234* zostanie przez nich odkryte w ciągu paru sekund**.

Atakujący do zdobycia hasła wykorzystują:

1. Swoją wiedzę o użytkowniku, np. datę urodzenia, przezwisko czy drugie imię.
2. Plik słownika — kolejne sprawdzanie wszystkich zapisanych w nim słów ujawni hasło będące dowolnym wyrazem języka polskiego albo jakiegokolwiek innego języka.
3. Program, który będzie sprawdzał wszystkie możliwe kombinacje liter, cyfr i znaków specjalnych. Atak tego typu (**atak pełnego przeglądu**, ang. *Brute Force*) wymaga sprawdzenia ogromnej liczby kombinacji (np. *Aa1*, *A1a*, *aA1*, *a1A*, *1Aa*, *1aA*), co nie znaczy, że jest nieskuteczny.

Znając sposoby zdobywania haseł, możemy określić wymogi, jakie powinny spełniać hasła, aby ich zdobycie było praktycznie niemożliwe:

1. Po pierwsze, **hasło nie może w ogóle przypominać:** nazwy użytkownika, Twojego imienia, nazwiska, daty urodzenia, adresu, imienia ulubionego zwierzęcia, autora, tytułu filmu czy książki.
2. Po drugie, **hasło nie może być wyrazem jakiegokolwiek języka** — hasła *inwentaryzacja*, *agrokultura* czy *uporządkowywanie* są prawie tak samo łatwe do zdobycia jak hasła typu *1234*.
3. Po trzecie, **hasło nie może być krótsze niż ośmioznakowe,** a jeżeli nie ma żadnych specjalnych przeciwwskazań, długość hasła powinna wynosić co najmniej 12 znaków.
4. Po czwarte, hasło powinno zawierać przynajmniej kilka
   a. wielkich liter alfabetu (od *A* do *Z*);
   b. małych liter alfabetu angielskiego (od *a* do *z*);
   c. cyfr (od *0* do *9*);
   d. znaków specjalnych (np. *:*, *!*, *$*, *#*, *%*).

Najbezpieczniejsze, a jednocześnie łatwe do zapamiętania są hasła wielowyrazowe, np. *Jak ja nie lubię poniedziałków* czy *Jeszcze tylko 315 minut lekcji*. Jeżeli z obawy, że zapomnisz hasła stosujesz słabe hasła, zapisz je i schowaj kartkę z nimi tam, gdzie przechowujesz inne ważne dokumenty — w portfelu. To nie zapisywanie haseł, a zostawianie ich ogólnie dostępnych w pobliżu komputera jest powszechnym błędem.

Ataki lokalne

Najprostszym i najskuteczniejszym sposobem zdobycia kontroli nad komputerem jest zapewnienie sobie do niego lokalnego dostępu. O skali zagrożenia atakami lokalnymi może świadczyć fakt, że fachowcy od zabezpieczeń zgodnie przyznają, że **osobę, która miała okazję usiąść przed klawiaturą komputera należy uznać za administratora danego systemu, znającego wszystkie hasła i tajne dane poszczególnych użytkowników**.

Nie ma systemu operacyjnego, który osobie dysponującej odpowiednią wiedzą i zapasem czasu uniemożliwiłby zdobycie pełnej kontroli nad dostępnym fizycznie komputerem.

Z tego powodu **najskuteczniejszym sposobem ochrony komputera przed atakami lokalnymi jest ograniczenie dostępu do niego innym osobom**. Absolutnym minimum jest **blokowanie pozostawionego bez nadzoru, włączonego komputera**.

Ataki zdalne

Podłączenie komputera do sieci wiąże się z dodatkowymi zagrożeniami:

1. Pierwsza grupa zagrożeń jest związana z przesyłaniem danych przez sieć — wysłane pakiety mogą być przechwycone lub podsłuchane przez niepowołane osoby. Do tej grupy zagrożeń zalicza się:
   a. **Podsłuchiwanie** (ang. *Sniffing, Eavesdropping*) **pakietów przesyłanych przez sieć**. W ten sposób atakujący może poznać wszystkie informacje przesyłane jawnym tekstem.
   b. **Przechwytywanie** (ang. *Spoofing*) **przesyłanych pakietów w celu ich modyfikacji i odesłania do komputera docelowego**. Pozwala to atakującemu na podszywanie się pod zaufanego użytkownika sieci.
   c. **Nakłonienie użytkownika do nawiązania połączenia z wrogim komputerem** (ang. *Man-in-the-middle attack*) **i monitorowanie przesyłanych** przez to połączenie, nawet szyfrowanych **danych**.
2. Druga grupa zagrożeń wynika z udostępnienia Twojego komputera innym użytkownikom sieci — każdy z nich będzie mógł próbować połączyć się z Twoim komputerem i zdalnie uruchomić wrogi program. Do tej grupy zagrożeń zaliczamy:
   a. **Włamanie do komputera i przejęcie nad nim kontroli**. Zdecydowana większość ataków tego typu jest przeprowadzana za pomocą zautomatyzowanych narzędzi — wirusów lub koni trojańskich.
   b. **Odmowę obsługi** (ang. *Denial of Service*). Atak polegający na zablokowaniu komputera poprzez wysłanie do niego dużej liczby spreparowanych pakietów.

Socjotechnika

Nawet najlepsze zabezpieczenia komputera nie będą wiele warte, jeżeli jego użytkownik, świadomie lub nieświadomie, ujawni niepowołanym osobom informacje mające wpływ na jego bezpieczeństwo. **Duża część ataków na systemy komputerowe jest wymierzona właśnie w ich użytkowników** — często najprostszym sposobem włamania okazuje się przekonanie użytkownika, żeby zdradził swoje hasło.

Socjotechnika lub inżynieria socjalna (ang. *Social Engineering*) to jeden z najskuteczniejszych sposobów zdobywania poufnych informacji, polegający na wykorzystaniu wiedzy z psychologii, naszej ufności (dlaczego uważamy, że każda osoba w niebieskim mundurze jest policjantem?) i nieumiejętnego oceniania ryzyka (dlaczego sądzimy, że w znanym otoczeniu, np. w domu nie może stać nam się krzywda?) oraz podstawowych danych o użytkownikach atakowanego systemu.

Przykładowy atak socjotechniczny polega na dzwonieniu do wybranych osób i nakłanianiu ich (groźbami — podawanie się za nauczyciela lub administratora, prośbami — podawanie się za kolegę w potrzebie bądź obietnicami — podawanie się za osobę mającą określone wpływy) do zdradzenia hasła. Innym często spotykanym typem ataku jest rozsyłanie wiadomości e-mail, które pod pretekstem przeprowadzenia testów, usunięcia problemu (np. odblokowania konta) lub zbierania informacji mają przekonać do zdradzenia hasła.

Innym sposobem ujawnienia hasła jest jego pozostawienie w pobliżu komputera — nawet najbardziej skomplikowane hasło, które zostało zapisane na karteczce przyklejonej do monitora, schowanej pod klawiaturą lub w leżącym obok komputera kalendarzu jest nic niewarte.

Haker

Nie sposób pisać o bezpieczeństwie systemów komputerowych z pominięciem hakerów (ang. *Hacker*). **Haker to osoba o wyjątkowych zdolnościach, doskonale znająca tajniki języków programowania**. Zajmuje się tworzeniem systemów operacyjnych, programów oraz ich ulepszaniem.

Początkowo synonimem słowa haker był zwrot *real programmer* — w ten sposób określano tych inżynierów lub absolwentów wydziałów matematyki czy fizyki, którzy zafascynowani możliwościami powstającej informatyki pisali programy w asemblerze, Fortranie i kilku innych językach programowania, których nazw nawet nikt już nie pamięta. Do tej grupy należeli m.in. Seymour Cray, Stan Kelly-Bootle czy David E. Lundstrom.

Lata 80. to okres, w którym powstaje odrębna subkultura hakerów — w roku 1978 Randy Sousa i Ward Christiansen zakładają pierwszy **BBS**, powstaje charakterystyczny żargon (*http://www.tuxedo.org/jargon*) i etykieta tego środowiska. W tym czasie systemy PDP-10 zostają zastąpione komputerami pracującymi pod kontrolą opracowanego przez hakera Kena Thompsona systemu Unix, a **hakerzy zyskują potężne narzędzie w postaci opracowanego przez hakera Dennisa Ritchiego języka programowania C**. Ci dwaj panowie w roku 1974 opublikowali wynik wspólnej pracy — pierwszy system operacyjny napisany w języku wysokiego poziomu.

Niedługo później **Richard M. Stallman (znany pod pseudonimem RMS), twórca EMACSa, osoba uznawana za „ostatniego prawdziwego hakera", zakłada fundację wolnego oprogramowania (FSF)**. W roku 1982 rozpoczynają się prace nad projektem GNU, w ramach którego powstanie bezpłatna wersja systemu Unix napisana w języku C. W roku 1991 haker Linus Torvalds udostępnia utworzone z wykorzystaniem narzędzi FSF bezpłatne jądro wersji systemu Unix przeznaczone dla komputerów z procesorem INTEL 386.

W latach 90. powstają takie grupy hakerów, jak założony przez Leksa Luthora *Legion of Doom* oraz *Master of Deception*. Coraz częściej poszczególne grupy i hakerzy „walczą" między sobą, atakując m.in. serwery rządowe czy firmowe. Media i niektóre korporacje zaczynają promować inne, negatywne znaczenie terminu haker — według nich **haker to niebezpieczny maniak komputerowy, wręcz groźny przestępca**.

Hakerzy to ścisła elita świata informatyki. Jeżeli któryś z nich chciałby zaatakować dowolny system komputerowy, prawie na pewno udałoby mu się to. Na szczęście bardzo znikoma część ataków przeprowadzana jest przez hakerów. Około 30% ataków jest dziełem krakerów, pozostałe 70% — lamerów.

Kraker (ang. *Cracker*) **— to osoba zajmująca się łamaniem zabezpieczeń oprogramowania**. Dotyczy to zarówno włamań do systemów komputerowych (łamanie zabezpieczeń serwerów), jak i, o wiele częściej, łamania zabezpieczeń programów np. w celu uniknięcia opłaty licencyjnej.

Lamer (ang. *Lammer*) **to osoba z niewielkim zasobem wiedzy informatycznej, która przeprowadza ataki za pomocą ogólnie dostępnych narzędzi** — niewiedza nie pozwala mu na analizę zabezpieczeń i opracowanie własnych sposobów ich ominięcia. Charakterystyczną cechą jest używanie przez nich przydomków zawierających dużą liczbę wielkich liter np. *SuPeRHaCkEr*.

Zagrożenie charakterystyczne dla systemu GNU/Linux

Paradoksalnie, **największe zagrożenie dla systemu GNU/Linux wynika z przekonania o jego bezpieczeństwie**. Pogląd ten rozpowszechniany jest zwykle przez adeptów GNU/Linux i prawdopodobnie bierze się z pewnego błędu statystycznego — użytkowników różnych dystrybucji GNU/Linux i, co za tym idzie, potencjalnych krakerów jest znacznie mniej niż użytkowników systemów MS Windows.

Zagrożenia systemu GNU/Linux można podzielić na cztery kategorie:

1. **Instalowanie niepotrzebnych usług i pozostawianie otwartych portów**. Jest to najczęstszy błąd popełniany przez użytkowników tego systemu. Większość osób, instalując oprogramowanie domyślnie wybiera kompletną instalację. W efekcie mamy system przypominający śmietnik z dużą liczbą niepoprawnie skonfigurowanych usług.

Instaluj wyłącznie programy, których używasz. Jeśli w przyszłości będziesz chciał skorzystać z nowej usługi, zawsze możesz ją dodać.

2. **Używanie oprogramowania bez uaktualnień.** System dostępny na płycie CD lub pobrany z internetu to system bez poprawek, które wyszły już po jego wydaniu.

Zawsze należy dbać o uaktualnienie systemu i używanie programów w najnowszych wersjach.

3. **Nieuważne administrowanie**. Systemu sieciowego po zainstalowaniu nie można zostawić samemu sobie. Należy przeglądać dzienniki usług, dbać o jego aktualizacje i poprawną konfigurację.

Warto zapisać się na listy dystrybucyjne związane z bezpieczeństwem używanego systemu.

4. **Uruchamianie niebezpiecznych usług**. Do takich usług zaliczamy FTP, Telnet czy serwer poczty elektronicznej. Powstały one w czasach, kiedy problemom bezpieczeństwa nie poświęcano wiele uwagi. Do uwierzytelniania używają one haseł przesyłanych otwartym tekstem, a więc łatwych do przechwycenia.

Jeśli istnieje konieczność korzystania z tych usług, to należy je zastąpić bezpiecznymi odpowiednikami (SFTP, SSH, SSMTP oraz SPOP).

Rozprzestrzenianie się wirusów w systemach GNU/Linux jest stosunkowo trudne ze względu na dużą zmienność tego systemu. Praktycznie każda dystrybucja wprowadza pewne zmiany położenia kluczowych plików, różne wersje oprogramowania, często z charakterystycznymi dla dystrybucji rozszerzeniami, co praktycznie uniemożliwia napisanie wirusa mogącego atakować w sposób uniwersalny ten system. Nawet epidemia robaka **Slapper** w 2002 roku była spowodowana niefrasobliwością administratorów i niezainstalowaniem udostępnionych przed wybuchem epidemii uaktualnień.

Budowa podsystemu wejścia-wyjścia nie umożliwia, inaczej niż w systemach Windows, kontrolowania zapisywanych i odczytywanych danych, jednej z podstawowych funkcji skanerów antywirusowych.

GNU/Linux jest narażony na ataki spowodowane uruchamianiem programów z niepewnego źródła. Dla tego systemu charakterystyczne jest rozwijanie aplikacji przez wielu niezależnych programistów, co wraz z bezgranicznym zaufaniem części użytkowników do oprogramowania pobranego z internetu może mieć katastrofalne skutki. Przeciwnicy wolnego oprogramowania argumentują, że jest ono z definicji bardziej narażone na próby włamania. Kraker, dysponując kodem źródłowym, ma większe możliwości znalezienia potencjalnych błędów do wykorzystania. **Fakty nie potwierdzają tych zarzutów — dostęp do kodu źródłowego powoduje szybkie znajdywanie potencjalnych niebezpieczeństw i ich usuwanie**. Dotyczy to jednak dużych, prawidłowo zarządzanych projektów. Projekty rozwijane przez pojedynczych użytkowników zwykle cechują się marną jakością kodu i wieloma błędami.

Kilka cech systemu GNU/Linux czynią go stosunkowo odpornym na próby ataków:

- **System od początku był systemem wieloużytkownikowym**. Od samego początku użytkownicy byli separowani od aplikacji i środowiska innych użytkowników. Aplikacje uruchamiane są z prawami użytkownika, co ogranicza możliwość potencjalnych szkód. Również wykorzystywane przez aplikacje biblioteki są wykonywane z prawami użytkownika. Dzięki temu atakujący nie może wykorzystać błędów np. w module obsługi formatu graficznego GIF do uzyskania kontroli nad systemem. Dostosowanie aplikacji do pracy z ograniczonymi uprawnieniami powoduje, że rzadko trzeba korzystać z konta administracyjnego.
- **Aplikacje są modułowe**. Dzięki temu (z wyjątkiem **KDE** i **Gnome**) nie są zależne od siebie i błąd jednego modułu nie wpływa na pracę innych.
- **GNU/Linux nie jest oparty na modelu RPC** (ang. *Remote Procedure Call*). RPC wykorzystywany jest do komunikacji pomiędzy programami, ale może też być poważną luką w bezpieczeństwie. RPC umożliwia nakazanie innej aplikacji, często pracującej z zupełnie innymi uprawnieniami, by wykonała pewne czynności. Wykorzystując błędy w oprogramowaniu, użytkownik może wykonać czynności, do których normalnie nie posiadałby wystarczających uprawnień. Aplikacje w systemie GNU/Linux w większości mogą prawidłowo działać z wyłączonym RPC.

Zagrożenia związane z technologiami RPC i DCOM zostały ograniczone dopiero w drugim pakiecie serwisowym dla systemu Windows XP i pierwszym dla systemu Windows Server 2003.

- **Domyślnie praktycznie wszystkie aplikacje mają wyłączoną obsługę sieci lub też realizują połączenia wyłącznie z lokalnego komputera**. Włączenie potencjalnie niebezpiecznych funkcji wymaga aktywności użytkownika i świadomego wyboru.
- **Praktycznie nie występują aplikacje lub usługi wymagające do działania uprzywilejowanego konta administracyjnego**. Dzięki temu nawet poważny błąd danej usługi ogranicza możliwości ataku wyłącznie do konta, z którego ona działała.
- **Istnieją specjalne rozszerzenia jądra zwiększające bezpieczeństwo**. Do takich rozszerzeń należą np. **openwall** lub **Selinux**. Szczególnie ta ostatnia nakładka znacznie rozszerza bezpieczeństwo systemu, poprzez wprowadzenie list **ACL** (ang. *Access Control Lists*), co umożliwia stworzenie precyzyjnych ról. Dzięki temu zadania administracyjne można rozdzielić, np. stworzyć osobne konto administracyjne do zarządzania użytkownikami, osobne do uaktualniania systemu itd.

Istnieje wiele dystrybucji systemu GNU/Linux. Każda z nich cechuje się nieco innym podejściem do problemów bezpieczeństwa i domyślnie instalowanych aplikacji.

Zagrożenie charakterystyczne dla systemu Windows

Systemy Windows 9x powstały kilkanaście lat temu — w czasach, kiedy nie było internetu, a moc obliczeniowa komputerów domowych była tak mała, że nawet słabe szyfrowanie zabezpieczało poufne dane przed ich ujawnieniem. **Dzisiaj systemy te nie gwarantują żadnego bezpieczeństwa, a jedynym sposobem na jego zapewnienie jest aktualizacja systemu operacyjnego**.

W ciągu ostatnich dwóch lat podejście firmy Microsoft do kwestii bezpieczeństwa uległo jednak radykalnej zmianie — możliwe, że zmiana ta dokonała się zbyt późno i niektóre osoby nie zmienią już swojej opinii na ten temat.

W ramach projektu **wiarygodnych technik komputerowych** (ang. *Trustworthy Computing*) firma Microsoft:

1. **Szkoli programistów,** pozostałych pracowników i partnerów w zakresie tworzenia bezpiecznego kodu źródłowego oraz identyfikacji luk w zabezpieczeniach.
2. **Zmieniła domyślną konfigurację swoich produktów z funkcjonalnej na bezpieczną**.
3. **Opracowała narzędzia pozwalające na automatyczne zarządzanie zabezpieczeniami**, w tym automatyczną aktualizację oprogramowania, ocenę bezpieczeństwa systemu i jego poprawę.
4. **Udostępnia zalecenia, w postaci wskazówek i podręczników,** ułatwiające administratorom i użytkownikom zabezpieczenie używanego oprogramowania.
5. **Promuje rozwiązania gwarantujące poufność informacji** — wszystkie nowe serwery i systemy firmy Microsoft umożliwiają zabezpieczenie przechowywanych w nich danych.

Niestety, systemy Windows nadal padają łatwą ofiarą ataków i kolejnych epidemii wirusów. Dlaczego tak jest? **Przede wszystkim dlatego, że stanowią większość wszystkich używanych systemów operacyjnych** (ponad 95% komputerów domowych działa pod kontrolą jakiejś wersji systemu Windows). W kilkudziesięcioletniej historii systemów operacyjnych zawsze najczęściej atakowane były te najpopularniejsze — tak było z systemami komputerów PDP-11 TOPS-10 i TOPS-20, z systemem komputerów VAX VMS, z najpopularniejszym później systemem Unix i tak jest teraz z systemem Windows. Monokultura jest zawsze mniej odporna, a epidemie rozpowszechniają się w niej o wiele szybciej i pochłaniają więcej ofiar niż w środowiskach mieszanych.

1 stycznia 2004 znanych było mniej więcej pięć i pół tysiąca programów zagrażających bezpieczeństwu systemów Windows — narzędzi umożliwiających zautomatyzowany atak lub najróżniejszego typu wirusów.

Drugim powodem jest wysoki poziom standaryzacji — skoro większość systemów jest tak samo zainstalowana i skonfigurowana, to udane włamanie do jednego z nich może być powtórzone podczas atakowania kolejnych.

Trzecim powodem jest zauważalna niechęć wielu osób do firmy Microsoft. Pojawia się coraz więcej i to coraz groźniejszych wirusów atakujących systemy Windows — tylko w ciągu drugiego półrocza 2003 roku ujawniono ponad 1700 nowych wirusów. Właściwie nie ma miesiąca, żeby nie wybuchła nowa ogólnoświatowa epidemia — dla porównania, pierwsza poważna epidemia wirusów systemu GNU/Linux miała miejsce w roku 1998 (wirus **Linux.ADM.Worm**), a druga (i do momentu przygotowania tej książki, ostatnia) — w roku 2002 (wirus **Slapper**).

Czwartym powodem jest błędne przekonanie, że administrowanie tym systemem nie wymaga specjalnej wiedzy. To prawda, że łatwiej jest uruchomić np. serwer zdalnego dostępu w systemie Windows niż na serwerze GNU/Linux, ale to nie znaczy, że tak uruchomione usługi będą bezpieczne. Zabezpieczenie systemu operacyjnego, nawet z pomocą narzędzi i na podstawie opublikowanych wskazówek, wymaga pracy i wiedzy.

Ciekawe artykuły poświęcone bezpieczeństwu systemu Windows publikowane są w polskiej wersji Technetu pod adresem *http://www.microsoft.com/poland/technet/article/default.mspx*.

Obrona

Dzisiaj internet jest niebezpiecznym miejscem, w którym nieustannie toczą się walki. Pouczające może być wyobrażenie go sobie jako świata z filmów i książek historycznych czy mitologicznych — duże miasta (sieci korporacji) są jeszcze względnie bezpieczne, ale poza ich murami, w małych miasteczkach (sieciach osiedlowych) nikt (żaden komputer) nie jest bezpieczny.

Jak nie istnieje bezbłędnie napisany program, tak nie istnieje stuprocentowo bezpieczny system komputerowy. Jedyne, co możemy w tej sytuacji zrobić, to **zmniejszyć ryzyko udanego ataku**.

Strategia wielu warstw

Raz jeszcze odwołamy się do przenośni internetu jako pola walki. Gdybyśmy, dysponując skromnymi środkami, chcieli ochronić nasz dom (komputer), moglibyśmy otoczyć go palisadą (zaporą połączenia internetowego). Takie rozwiązanie nie zabezpieczy nas przed wszystkimi atakami, ale przed niektórymi — tak.

Żeby zabezpieczenia systemu komputerowego były skuteczne, muszą być szczelne. W naszym przykładzie z wielu kijów zbudowaliśmy palisadę, ale nie wbiliśmy przed domem jednego, ogromnego pala w nadziei, że atakujący, zamiast go ominąć, nadzieją się na niego. Niestety, wielu administratorom brakuje wyobraźni i zabezpieczenie systemu sprowadzają do szyfrowania wszystkich danych długim, najlepiej 4-kilobajtowym kluczem. Z doświadczenia wiemy, że atakujący, zamiast zgodnie z oczekiwaniami administratora spędzić eony lat na próbach jego złamania, poświęcą kilka godzin na zdobycie interesujących ich danych w inny sposób.

Pewna część ataków, których nie zatrzyma palisada może być zatrzymana poprzez zamontowanie ciężkich, szczelnych drzwi[1] (zablokowanie nieużywanych usług i nieuruchamianie pochodzących z niepewnego źródła programów). W ten sposób stworzylibyśmy **drugą linię obrony** — z filmów wszyscy wiemy, że skuteczne strategie obrony składają się z kilku elementów (klasyczny przykład to przepaść, stroma góra, fosa, mur, następny mur, wąska ścieżka nad przepaścią, ciężkie drzwi, cały czas strażnicy i wreszcie skarb).

W następnej kolejności powinniśmy zamontować w drzwiach solidny zamek (zaimplementować bezpieczne protokoły uwierzytelniania). Jego rola jest inna niż drzwi czy palisady — zamiast wszystkim, ma uniemożliwić wejście (dostęp) nieznanym osobom.

Nie ma żadnych powodów, dla których tej sprawdzonej strategii nie mielibyśmy stosować do obrony systemów komputerowych. Przecież funkcjonalny model komputera przedstawia go jako systemem wielowarstwowy (rysunek 5.1).

Rysunek 5.1. *Poszczególne warstwy systemu komputerowego*

W każdej z warstw należy wprowadzić inne środki bezpieczeństwa:

1. **Użytkownicy to najczęściej atakowany element systemu komputerowego**. Niezbędne zabezpieczenia obejmują:
   a. uświadomienie im zagrożeń i sposobów ich unikania;
   b. nauczenie ich wykrywania wszelkiego rodzaju mistyfikacji (np. fałszywych maili z prośbami o podanie poufnych danych);
   c. nauczenie ich rozpoznawania ataków socjotechnicznych i obrony przed nimi.
2. **Bezpośredni, fizyczny dostęp do komputerów, urządzeń sieciowych, a nawet okablowania musi być ograniczony do niezbędnego minimum**. W innym przypadku pozostałe zabezpieczenia będą nieskuteczne — atakujący z łatwością je ominie.
3. **Linia graniczna zawiera wszystkie komputery i urządzenia sieciowe bezpośrednio podłączone do publicznej sieci** (komputerowej lub telefonicznej)[2]. Tak jak na większości granic, na granicy systemu komputerowego również należy blokować niepożądany ruch, i sprawdzać poprawność przesyłanych, danych.

[1] Albo fosy, w każdym razie nie kolejnej palisady. Ryzyko, że atakujący sforsuje dwie różne przeszkody jest o wiele mniejsze, niż gdy ma do pokonania kilka takich samych.

[2] Typowymi urządzeniami linii granicznej są routery.

4. **Zdalny dostęp do komputera musi być kontrolowany**. Wiara w to, że wszystkie próby ataku zostaną zatrzymane na linii granicznej jest taką samą naiwnością, jak wiara w to, że straż graniczna zatrzyma wszystkich złodziei, a skoro rodacy są uczciwi, to nie musimy zamykać samochodów. W sieci lokalnej należy:

   a. blokować niepożądane dane,

   b. szyfrować poufne dane,

   c. sprawdzać tożsamość zdalnych komputerów.

5. Częstym (statystycznie trzecim, po użytkownikach i typowych usługach, np. serwerach WWW) celem ataków jest system operacyjny. Żeby się przed nimi obronić, należy:

   a. na bieżąco aktualizować system;

W 2003 roku wykrytych zostało ponad trzy tysiące poważnych luk w zabezpieczeniach systemów operacyjnych. Co więcej, ponad 70% luk było bardzo łatwych do wykorzystania — przeprowadzenie ataku nie wymagało specjalistycznej wiedzy i często sprowadzało się do uruchomienia ogólnie dostępnego w internecie programu.

   b. kontrolować dostęp użytkowników do zasobów systemu, przede wszystkim nie korzystać na co dzień z konta administratora;

   c. systematycznie monitorować bezpieczeństwo systemu.

6. Nawet najlepsze zabezpieczenie systemu operacyjnego nie jest wiele warte, jeżeli na komputerze są uruchamiane (możliwe, że bez wiedzy użytkownika) wrogie programy. Jednym z najczęstszych błędów jest **brak zabezpieczeń w warstwie aplikacji**. Najbardziej zagrożone są, umożliwiające zdalny dostęp, aplikacje internetowe — to właśnie w nie jest wymierzona prawie połowa wszystkich ataków. Drugi typ zagrożeń polega na uruchomieniu wrogiego programu — jeżeli atakującemu uda się do tego przekonać użytkownika, wszystkie zabezpieczenia będą nieskuteczne, bo system uzna, że użytkownik świadomie wykonał daną operację. Zabezpieczenia tej warstwy powinny obejmować:

   a. aktualizację oprogramowania;

   b. blokowanie niechcianych programów;

   c. ochronę antywirusową;

   d. uniemożliwienie uruchomienia wskazanych programów.

Sześć z dziesięciu ataków najczęściej przeprowadzanych w 2003 roku (dane nie uwzględniają ataków na użytkowników) odbyło się za pośrednictwem protokołu HTTP, a więc były to ataki wymierzone w aplikacje internetowe — przeglądarki, programy pocztowe lub serwery WWW.

7. **Od dwóch lat systematycznie rośnie liczba zagrożeń poufnych danych użytkownika** — w pierwszej połowie 2002 roku tylko dwa z dziesięciu najpopularniejszych ataków miały na celu zdobycie takich danych, w pierwszej połowie 2004 roku już osiem z dziesięciu najczęściej zgłaszanych ataków było wymierzonych w poufne dane użytkowników komputerów. O ile jeszcze parę lat temu zagrożenia dotyczyły prawie wyłącznie przechowywanych na dyskach danych, to współczesne ataki są wymierzone nie tylko w pliki, ale również w hasła, klucze szyfrujące czy sekwencje naciskanych klawiszy. Na bezpieczeństwo danych składają się:

   a. kontrola dostępu do plików i folderów;

   b. szyfrowanie poufnych danych;

   c. regularne tworzenie kopii zapasowych.

Efektem wdrożenia strategii niezależnego zabezpieczenia poszczególnych elementów systemu komputerowego jest wielokrotne zmniejszenie ryzyka i zwiększenie szansy wykrycia ataku. Rozpatrzymy przykład epidemii wirusa **Sasser**.

Wirus atakował komputery, wykorzystując lukę w bezpieczeństwie systemów Windows 2000, XP i 2003. Po zaatakowaniu Sasser kopiuje się do pliku *avserve.exe*, *avserve2.exe*, *skynetave.exe*, *lsasss.exe* lub *napatch.exe* i modyfikuje *Rejestr*, zapewniając sobie automatyczne uruchamianie podczas startu systemu. Następnie na zaatakowanym komputerze uruchamiany jest serwer FTP (numer portu zależy od wersji wirusa), a wirus rozpoczyna wyszukiwanie innych podatnych na atak komputerów. Po ich znalezieniu, wykorzystując lukę podsystemu zabezpieczeń LSASS, uruchamia na zdalnym komputerze wiersz polecenia, a wykorzystany do ataku komputer jest restartowany.

W przypadku próby ataku na zabezpieczony system komputerowy:

1. Prawdopodobnie trzy na cztery próby ataku przedostaną się przez zaporę linii granicznej (zatrzymanie ataku wymaga błyskawicznej reakcji administratora). Szansa, że uda się powstrzymać rozprzestrzenianie wirusa jest już dużo większa — w linii granicznej z reguły blokowany jest ruch adresowany na nietypowe numery portów.
2. Jeżeli nawet wirus przedostanie się do sieci lokalnej, to tylko jedna na dwadzieścia prób ataku nie zostanie zatrzymana przez zaporę komputera — w sumie 37 na 1000 (0,75∗0,05) ataków okaże się skutecznych — użytkownik może na przykład przypadkowo zezwolić na komunikację z zaatakowanym komputerem.
3. Jeżeli nawet wirus dostanie się do naszego komputera, to tylko jeden na dziesięć ataków nie zostanie wykryty i zatrzymany przez skaner antywirusowy — w sumie 4 na 1000 (0,037∗0,1) ataków okaże się skutecznych (zakładamy możliwość pojawienia się nowej, niewykrywanej jeszcze przez skanery odmiany wirusa. **Możemy zmniejszyć ryzyko, codziennie aktualizując sygnatury znanych wirusów**).

4. Jeżeli nawet do tego dojdzie, to zaktualizowany system operacyjny będzie odporny na dziewiętnaście z dwudziestu prób ataku (na tyle oceniamy ryzyko, że nowe odmiany wirusa wykorzystają nieujawnioną dotychczas lukę w zabezpieczeniach systemu).
5. W sumie, przyjmując pesymistyczny wariant, **ryzyko udanego ataku nie przekracza setnych części procentu** — w naszym przypadku 1 na 5000 (0,0037∗0,05 = 0,000185) ataków okazałby się skuteczny.