Dodatek nr 1

W dokumencie „Trasted Computer Standards Evaluation Criteria", znanym także jako „Orange Book", Departament Obrony USA zdefiniował siedem poziomów bezpieczeństwa komputerowego systemu operacyjnego. Kolejne poziomy określają różne sposoby zabezpieczania sprzętu, oprogramowania i danych. Klasyfikacja ma charakter „zawierania", co oznacza, że wyższe poziomy mają wszystkie cechy poziomów niższych, a dodatkowo — uzupełnienia.

D1 — to najniższy poziom bezpieczeństwa określający także całkowity brak wiarygodności systemu. Poziom ten nie wymaga certyfikacji, bowiem oznacza po prostu brak jakichkolwiek zabezpieczeń. Do tej klasy należą także systemy pozornie bezpieczne, czego przykładem może być procedura autoryzacji dostępu w sieciowych komputerach zaopatrzonych w system operacyjny Microsoft Windows. Użytkownik pytany jest tylko o identyfikator i hasło (wystarczy podać dane „z sufitu"), by uzyskać dostęp do lokalnych zasobów komputera. Trochę lepiej wygląda to w tym przypadku zabezpieczania zasobów przed dostępem z innych komputerów w Sieci i w tym ujęciu Microsoft Windows nie należy jednak do klasy D1.

C1 — jest to najniższy poziom bezpieczeństwa. System operacyjny kontroluje uprawnienia użytkowników do odczytu i zapisu plików oraz kartotek. Ponadto dysponuje mechanizmem autoryzacji dostępu. System taki nie ma na ogół zdefiniowanego tzw. super-użytkownika. Poziom ten pozbawiony jest także mechanizmów rejestrowania zdarzeń (auditing, logging).

C2 — to poziom , który gwarantuje automatyczne rejestrowanie wszystkich istotnych — z punktu widzenia bezpieczeństwa — zdarzeń i zapewnia silniejszą ochronę kluczowych danych systemowych, takich jak np. baza danych haseł użytkowych.

B1 — jest to klasa, która obsługuje bezpieczeństwo na kilku poziomach, takich jak — „tajne" i „ściśle tajne". Ma wdrożone mechanizmy uznaniowej kontroli dostępu do zasobów systemu, co może na przykład sprowadzić się do braku możliwości zmiany charakterystyki dostępu do plików i kartotek przez określonego użytkownika.

B2 — jest to klasa, który wymaga przypisania każdemu obiektowi systemu komputerowego etykiety bezpieczeństwa określającej status tego obiektu w odniesieniu do przyjętej polityki bezpieczeństwa (na przykład gdy obiekt „użytkownik" żąda dostępu do obiektu „plik", system ochrony akceptuje lub odrzuca to żądanie na podstawie porównania zawartości etykiet bezpieczeństwa tych obiektów). Etykiety te mogą zmieniać się dynamicznie w zależności od tego, co jest aktualnie użytkowane.

B3 — jest to rozszerzenie problemu bezpieczeństwa na sprzęt komputerowy. W tym przypadku bezwzględnie obowiązkowe jest chronienie zarówno przechowywanej, jak i przesyłanej informacji. Przykładowo: terminale mogą być połączone z serwerem tylko za pośrednictwem wiarygodnego okablowania i specjalizowanego sprzętu gwarantującego, że nikt nie będzie w stanie „podsłuchać" klawiatury.

A1 — jest to najwyższy poziom bezpieczeństwa. Cała konfiguracja sprzętowo-programowa wymaga matematycznej weryfikacji. Zarówno sprzęt, jak i oprogramowanie musi podlegać specjalnej ochronie w trakcie transportu zapewniającej jego nienaruszalność.

W tym miejscu należy zwrócić uwagę na problem wzrostu obciążenia systemu operacyjnego związanego z uaktywnieniem opcji bezpieczeństwa. W szczególności może okazać się, że mało wydajne serwery nie będą w stanie obsłużyć wszystkich użytkowników po uruchomieniu programów zabezpieczających, ze względu na duże zużycie zasobów CPU i powierzchni dyskowej.