



TESTY BEZPIECZEŃSTWA SYSTEMÓW IT

Systemy IT ze względu na wrażliwość danych jakie zawierają, mogą stać się łatwym celem różnego rodzaju ataków mających na celu uzyskanie dostępu do zasobów przez niepowołane osoby. Im więcej podatności zawiera system tym lepsze stwarza warunki do udanych ataków. Skutki niepożądanych działań mogą mieć poważny wpływ na procesy biznesowe organizacji, dlatego tak ważne jest właściwe zaprojektowanie mechanizmów bezpieczeństwa systemów. Jednocześnie zaleca się identyfikację i analizę zagrożeń oraz ryzyk jak najwcześniej w cyklu życia systemu informatycznego, przed wprowadzeniem rozwiązania do środowiska produkcyjnego. Najskuteczniejszym sposobem żeby to wykonać jest przeprowadzenie testów bezpieczeństwa rozwiązania informatycznego.

Testy bezpieczeństwa pomagają określić potrzeby w zakresie bezpieczeństwa, mogą być zalecane w celu spełnienia prawnych wymogów ochrony informacji, konieczność przeprowadzenia testów często narzucają dokumenty określające politykę bezpieczeństwa organizacji, a także bywa to warunkiem wstępnym do przeprowadzenia audytu finansowego.

Dobłą praktyką stosowaną najczęściej przez organizacje jest zlecenie przeprowadzenia testów bezpieczeństwa niezależnym audytorom. Zaangażowanie niezależnych firm pozwala oszacować realne zagrożenia dla systemów.

Safe Computing posiada bardzo duże doświadczenie w przeprowadzaniu audytów bezpieczeństwa i oferuje szeroki ich zakres, w szczególności testy bezpieczeństwa w następujących obszarach:

- aplikacje
- systemy operacyjne
- bazy danych
- urządzenia sieciowe

Wszystkie audyty przeprowadzane są według własnej metodologii, jednocześnie korzystamy z uznanych metodyk audytowych, np. OWASP (*Open Web Application Security Project*) oraz WASC (*Web Application Security Consortium*).

Ocenę zastosowanych zabezpieczeń przeprowadzamy za pomocą następujących testów:

BLACK-BOX – zakłada minimalną wiedzę audytorów o badanym systemie, porównywalną z wiedzą przeciętnego użytkownika aplikacji. Testy polegają na przeprowadzaniu symulacji ataków na system przy użyciu znanych i powszechnie stosowanych metod.

GRAY-BOX – zakłada niepełną wiedzę o badanym systemie, ale większą, niż podczas testów black-box (np. w przypadku audytu aplikacji audytorzy posiadają dostęp do dokumentacji systemu, ale nie dysponują kodem źródłowym aplikacji).

WHITE-BOX – zakłada pełną wiedzę o badanym systemie. Audytorzy mają dostęp do badanych systemów z uprawnieniami takimi jak ich administratorzy, posiadają dokumentację do systemów oraz kod źródłowy (audyt aplikacji), mają możliwość zbierania informacji od personelu klienta poprzez wywiady i ankiety. Dzięki takiemu podejściu możliwa jest bardziej szczegółowa analiza bezpieczeństwa.

Najlepszą metodą z punktu widzenia oceny bezpieczeństwa jest połączenie dwóch rodzajów testów: white-box oraz black-box, dzięki której możliwe jest znalezienie największej liczby podatności przy założonym poziomie zaangażowania zasobów.

Większość prac związanych z identyfikacją podatności prowadzona jest ręcznie, jednak nasi audytorzy korzystają także z narzędzi pozwalających zautomatyzować wiele czynności w trakcie audytu. Safe Computing dysponuje odpowiednimi narzędziami komercyjnymi, typu „open source” oraz własnej produkcji. Automatyczne narzędzia identyfikują podatności oraz pozwalają wstępnie oszacować poziom bezpieczeństwa. Podatności wykryte automatycznymi narzędziami są weryfikowane przez audytorów w celu usunięcia zjawiska false positive – czyli wykrywania przez narzędzia podatności, które w rzeczywistości nie istnieją.

Po zakończeniu prac audytowych Klient otrzymuje Raport z testów bezpieczeństwa, który oprócz opisu wykrytych podatności zawiera m.in. wstępne zalecenia dotyczące usunięcia podatności oraz redukcji ryzyka do akceptowanego poziomu.

Testy bezpieczeństwa systemu nie powinny być ograniczone do jednorazowego przedsięwzięcia. Bezpieczeństwo nie jest czymś stałym, wciąż bowiem pojawiają się nowe zagrożenia. W Internecie publikowane są opisy wykrytych podatności oraz metody ich wykorzystania, stąd konieczne jest stałe lub okresowe badanie bezpieczeństwa systemów.

Audytorzy Safe Computing to wysokiej klasy specjaliści posiadający wieloletnie doświadczenie w przeprowadzaniu audytów w różnorodnych środowiskach. Wielu z nich jest członkami organizacji ISACA (Information Systems Audit and Control Association) oraz posiada uznawane na całym świecie certyfikaty bezpieczeństwa:

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CISA (Certified Information Systems Auditor)

Dzięki temu jesteśmy w stanie zapewnić najwyższą jakość audytów niezależnie od wdrożonych rozwiązań IT u Klienta. Ponadto nasi audytorzy utrzymują stały kontakt z zagranicznymi firmami audytorskimi dzięki czemu mogą stale pogłębiać swoją wiedzę i wymieniać się doświadczeniami.