



Audyt Systemu Operacyjnego

Cel

Celem Audytu Systemu Operacyjnego jest zapewnienie Klientowi najwyższego poziomu bezpieczeństwa poprzez wykonanie niezależnej oceny bezpieczeństwa dla systemu operacyjnego będącego przedmiotem audytu.

Charakterystyka usługi

Audyt Systemu Operacyjnego jest audytem skierowanym do Klientów posiadających systemy operacyjne, jako platformę dla aplikacji i baz danych. Polecany jest także, jako audyt doskonale uzupełniający pozostałe rodzaje audytów proponowanych przez Qumak-Sekom w ramach swojej oferty.

Usługa jest wykonywana przez konsultantów Qumak-Sekom i obejmuje zarówno zagadnienia techniczne, jak również organizacyjne i proceduralne, związane z przedmiotem audytu.

W ramach części dotyczącej kwestii organizacyjnych i proceduralnych audytowi poddane zostaną m.in. następujące zagadnienia:

- Zarządzanie:
 - Systemem operacyjnym (poziom administratora),
 - Prawami dostępu dla użytkowników.
- Kopie zapasowe i odtwarzanie systemu,
- Awarie i procedury awaryjne,
- Kontrola wewnętrzna.

System operacyjny, jako platforma dla aplikacji i baz danych jest niezwykle kluczowym elementem z punktu widzenia bezpieczeństwa. Jego kompromitacja¹ w prosty sposób prowadzi do możliwości uzyskania kluczowych informacji, najczęściej przechowywanych w bazach danych lub/i przetwarzanych przez różnorodne aplikacje. Dlatego tak ważne i nieodzowne jest zapewnienie systemowi operacyjnemu najwyższego poziomu bezpieczeństwa.

Techniczna część audytu systemu operacyjnego jest podzielona na kilka zasadniczych faz:

1. Badanie podatności na ataki.
2. Weryfikacja bezpieczeństwa konfiguracji systemu.
3. Badanie aktualności oprogramowania systemowego.
4. Badanie stosowanych praktyk w zakresie kopii zapasowych i odtwarzania.

Badanie podatności na ataki odbywa się najczęściej (o ile to technicznie możliwe) poprzez przeprowadzenie dwóch niezależnych testów opartych na automatycznych narzędziach:

- operujących na poziomie sieci (Network Based Testing),
- operujących na poziomie badanego systemu (Host Based Testing).

Dodatkowo, o ile to uzasadnione, konsultanci Qumak-Sekom mogą wykonać „ręczne” próby podatności na ataki.

¹ Przelamanie istniejących w systemie operacyjnym mechanizmów zabezpieczeń.

Weryfikacja bezpieczeństwa konfiguracji systemu jest zazwyczaj wykonywana dwuetapowo:

- Przy wykorzystaniu automatycznych narzędzi badających,
- Poprzez „ręczny” przegląd konfiguracji systemu przez konsultanta Qumak-Sekom celem weryfikacji stopnia spełnienia zestawu dobrych praktyk.

W ramach niniejszego etapu badane są m.in. takie parametry systemu operacyjnego, jak:

- Prawa dostępu do plików i katalogów,
- Prawa dostępu do systemu operacyjnego,
- Poziom utwardzenia systemu operacyjnego,
- Logowanie zdarzeń i accounting.

Badanie aktualności oprogramowania systemowego jest wykonywane przez konsultanta Qumak-Sekom i pozwala na sprawdzenie stosowanych aktualnie wersji systemu operacyjnego oraz ewentualnych serwerów usług na nim uruchomionych.

Ostatnim, ale bardzo ważnym testem, jest badanie kwestii związanych z wykonywaniem kopii zapasowych i zdolnością odtworzenia systemu po ewentualnej utracie danych.

Klient otrzymuje

Jako wynik wykonania usługi Klient otrzymuje *Raport z Audytu* zawierający:

- Listę wykrytych błędów i niezgodności opatrzonych komentarzem audytora, uzasadniającym ich uwzględnienie w raporcie,
- Klasyfikację wykrytych błędów i niezgodności w zależności od stopnia ich krytyczności dla bezpieczeństwa Klienta,
- Sugerowaną przez audytora metodę usunięcia błędu lub niezgodności,
- Zalecenia pozwalające na podniesienie poziomu bezpieczeństwa przedmiotu audytu.

Raport jest przekazywany Klientowi w dwóch egzemplarzach, z których jeden posiada formę klasycznego dokumentu (wydruk na papierze), a drugi jest plikiem źródłowym w wersji elektronicznej (plik .pdf na nośniku CD).

Wspierane rozwiązania

Qumak-Sekom oferuje Audyt Systemu Operacyjnego dla następujących produktów/rozwiązań:

- Solaris (Intel, Sparc),
- Windows (NT 4.0, 2000, XP, 2003),
- Linux (RedHat, Debian, SlackWare, SuSe),
- Nokia IPSO,
- Cisco IOS/CatOS.

Metodologia Q-Security

Wszystkie audyty wykonywane przez Qumak-Sekom realizowane są według jednej, spójnej metodologii **Q-Security**. Dzięki temu wyniki audytu są powtarzalne, cechują się bardzo wysoką jakością merytoryczną oraz obejmują szeroki zakres zagadnień (w tym również nietechniczne).

Podstawowe założenia metodologii **Q-Security**:

- Stosowanie komplementarnych metod weryfikacji poziomu bezpieczeństwa w obrębie zagadnień technicznych (badanie dwustopniowe)²,
- Prowadzenie audytu zarówno w obszarze technicznym, jak również w obszarach organizacyjnym i proceduralnym,
- Zunifikowany proces realizacji audytu.

Badanie dwustopniowe polega na wykorzystaniu podczas audytu zarówno narzędzi automatycznych np. dedykowanych skanerów i testerów, jak i wiedzy oraz doświadczenia konsultantów, wspieranej przez dostęp do baz wiedzy producentów. Takie podejście pozwala na uzyskanie znacznie bardziej miarodajnych wyników prac, a poza tym umożliwia skrócenie całkowitego czasu realizacji audytu, co przyczynia się do obniżenia jego kosztów.

O poziomie bezpieczeństwa systemu informatycznego decyduje zarówno jakość i skuteczność działania zaimplementowanych rozwiązań technicznych, jak również sprawna organizacja i efektywne procedury, związane z codzienną pracą. Dlatego podczas przeprowadzania audytów bezpieczeństwa przez Qumak-Sekom kładziemy nacisk na oba te obszary, które są ze sobą nierozdzielnie połączone. Podejście metodologii **Q-Security** jest oparte na światowych standardach i normach związanych z zapewnianiem bezpieczeństwa systemom informatycznym.

Proces realizacji każdego audytu oferowanego przez Qumak-Sekom jest identyczny i przebiega w następującym cyklu:

- Gromadzenie danych i przygotowanie szczegółów audytu,
- Przeprowadzenie audytu (najczęściej dwustopniowo),
- Wykonanie Raportu z Audytu w wersji 1,
- Spotkanie z przedstawicielami Klienta i analiza wyników Raportu z Audyt w wersji 1,
- Przygotowanie ostatecznej wersji Raportu z Audytu.

Możliwe jest także przeprowadzenie dodatkowego, drugiego audytu, zwanego Audytem Sprawdzającym, którego celem jest zweryfikowanie działań naprawczych lub/i korygujących wykonanych przez Klienta (lub podmiot przez niego upoważniony) na podstawie Raportu z Audytu.

Warto także podkreślić, że audyt powinien mieć charakter cykliczny, co umożliwia ciągłe utrzymywanie wysokiego poziomu bezpieczeństwa badanego obszaru.

Kontakt

W celu uzyskania dodatkowych informacji prosimy o kontakt z konsultantem Qumak-Sekom pod numerami telefonów (12) 254 58 00 lub (22) 519 08 00 oraz pod adresem email:

security@qumak.pl

² W przypadkach, w których nie jest możliwe lub zasadne zastosowanie metod komplementarnych, badanie jest jednostopniowe.