



Audyt Systemu Antywirusowego (AV)

Cel

Celem Audytu Systemu AV jest zapewnienie zasobom informatycznym Klienta należytej ochrony proceduralnej i technicznej przed wirusami, robakami i innymi formami złośliwych programów.

Charakterystyka usługi

Audyt Systemu AV jest przeznaczonym dla Klientów posiadających zaimplementowane rozwiązanie z rodziny produktów antywirusowych, którzy chcą ocenić poprawność i skuteczność jego funkcjonowania. Usługa jest wykonywana przez konsultantów Qumak-Sekom i obejmuje zarówno zagadnienia techniczne, jak również organizacyjne i proceduralne, związane z przedmiotem audytu.

W ramach prac związanych z badaniem funkcjonowania systemu AV w sferze organizacyjno-proceduralnej, konsultanci Qumak-Sekom zbadają m.in. następujące zagadnienia:

- Zarządzanie systemem AV (poziom administratora),
- Zasady aktualizacji oprogramowywania AV w poszczególnych miejscach systemu teleinformatycznego (stacje robocze, komputery przenośne, serwery poczty, bramki, serwery plików itp.),
- Obowiązek systematycznej kontroli antywirusowej wszystkich koniecznych elementów systemu IT,
- Raportowanie i procedury eskalacji w przypadku infekcji,
- Procedury awaryjne na wypadek infekcji,
- Kontrola wewnętrzna systemu AV.

Warto dodać, że część z powyższych zagadnień będzie badane w formie testów praktycznych.

Z kolei audyt zagadnień technicznych jest podzielony na dwie zasadnicze części:

1. Ocenę architektury systemu AV w kontekście zapewnienia maksymalnej ochrony systemowi IT Klienta.
2. Serię testów praktycznych pozwalających na ocenę rzeczywistego poziomu bezpieczeństwa systemu AV.

Architektura systemu AV jest jednym z kluczowych elementów, które stanowią o skuteczności ochrony antywirusowej w ramach danej organizacji. Nawet najlepsze oprogramowanie AV może się bowiem okazać nieskuteczne, w przypadku błędnych założeń projektowych. Konsultanci Qumak-Sekom dokonają szczegółowej analizy przepływu informacji elektronicznych Klienta (identyfikacja potencjalnych źródeł infekcji) i na tej podstawie wykonują ocenę architektury systemu AV.

Testy praktyczne polegają m.in. na kontrolowanym wprowadzeniu wirusów do systemu teleinformatycznego Klienta (poprzez wszystkie możliwe źródła infekcji) i sprawdzeniu skuteczności ochrony antywirusowej, jak również na weryfikacji aktualności oprogramowania AV w wybranych elementach systemu IT Klienta.

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 AV opartych na produktach następujących producentów:

- Network Associates (NAI),
- Trend Micro,
- Symantec.

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)¹,
- 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.

¹ W przypadkach, w których nie jest możliwe lub zasadne zastosowanie metod komplementarnych, badanie jest jednostopniowe.

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 ciągle 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