



## Audyt Bezpieczeństwa Styku z Siecią Internet

### **Cel**

Celem audytu styku z siecią Internet jest zapewnienie wysokiego poziomu bezpieczeństwa systemowi informatycznemu Klienta, połączonemu z siecią globalną, poprzez weryfikację bezpieczeństwa rozwiązania realizującego separację i kontrolę dostępu na styku z Internetem.

### **Charakterystyka usługi**

Audyt Bezpieczeństwa Styku z Siecią Internet jest przeznaczony dla Klientów posiadających połączenie z siecią globalną, w ramach którego zapewniany jest dostęp pracowników do zasobów Internetu lub/i użytkownikom zewnętrznym udostępniane są zasoby Klienta np. Web, poczta elektroniczna, DNS.

Audyt styku z siecią Internet stanowi połączenie:

- Audytów cząstkowych dotyczących systemów operacyjnych oraz firewalla,
- Testów penetracyjne wykonywanych z sieci Internet dla aplikacji i usług udostępnianych przez Klienta,
- Analizy architektury styku.

W ramach audytu badaniu zostaną poddane następujące elementy tworzące styk z siecią Internet:

- Router brzegowy:
  - Audyt systemu operacyjnego.
- Firewall:
  - Audyt systemu operacyjnego,
  - Audyt firewalla.
- Switch DMZ:
  - Audyt systemu operacyjnego.
- Serwer usług WWW, poczty elektronicznej, DNS:
  - Audyt systemu operacyjnego.

Ponadto powyższe testy zostaną uzupełnione o testy penetracyjne prowadzone z sieci Internet, których celem będzie zbadanie odporności systemu zabezpieczeń na ataki prowadzone z zewnątrz.

Ważnym elementem audytu jest przeprowadzenie przez konsultantów Qumak-Sekom analizy architektury posiadanego przez Klienta styku pod kątem:

- Spełnienia wymagań biznesowych:
  - Wydajność,
  - Niezawodność.
- Zgodności z dobrymi praktykami dotyczącymi zasad separacji i kontroli dostępu przy połączeniach między sieciami.

Zgodnie z metodologią Q-Security audyt bezpieczeństwa styku obejmuje zarówno sferę proceduralną i organizacyjną oraz zagadnienia technologiczne.

## **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).

## **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)<sup>1</sup>,
- 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,

---

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

- 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](mailto:security@qumak.pl)