



## Audyt Rozwiązania Firewall

### **Cel**

Audyt Rozwiązania Firewall ma za zadanie zapewnienie Klientowi najwyższego poziomu bezpieczeństwa poprzez wykonanie niezależnej oceny bezpieczeństwa dla stosowanego rozwiązania z rodziny firewall.

### **Charakterystyka usługi**

Audyt Rozwiązania Firewall jest przeznaczony dla Klientów posiadających zaimplementowane rozwiązanie z rodziny firewall, którzy chcą dokonać oceny jego poziomu bezpieczeństwa przez niezależnych ekspertów oraz uzyskać wytyczne i sugestie pozwalające na podniesienie poziomu bezpieczeństwa swojej organizacji. Usługa jest wykonywana przez konsultantów Qumak-Sekom i obejmuje zarówno zagadnienia techniczne, jak również organizacyjne i proceduralne, związane z przedmiotem audytu.

W ramach audytu sfery organizacyjnej i proceduralnej konsultanci Qumak-Sekom zbadają m.in. następujące obszary:

- Zarządzanie:
  - systemem firewall (poziom administratora),
  - prawami dostępu dla użytkowników/podmiotów.
- Monitorowanie działania:
  - Podczas pracy w stanie normalnych,
  - Podczas wystąpienia naruszeń i pojawienia się zagrożeń.
- Kopie zapasowe i odtwarzanie;
- Kontrola wewnętrzna.

Część techniczna Audytu Rozwiązania Firewall zazwyczaj obejmuje wykonanie trzech rodzajów testów:

1. Weryfikacja zgodności konfiguracji firewall z zapisami Polityki Bezpieczeństwa lub innymi wytycznymi Klienta.
2. Zbadanie realizacji dobrych praktyk zalecanych przez producenta danego produktu/rozwiązania.
3. Zbadanie realizacji dobrych praktyk zalecanych przez konsultantów Qumak-Sekom.

W ramach pierwszego etapu testów zweryfikowana zostanie aktualna konfiguracja firewalle pod kątem zgodności z odpowiednimi zapisami Polityki Bezpieczeństwa lub/i dokumentów jej towarzyszących. Możliwe jest również wykonanie tej części prac na bazie innych wytycznych posiadanych przez Klienta, określających zasady komunikacji sieciowej. W sytuacji braku powyższych zapisów lub wytycznych konieczne jest wykonanie dodatkowego wywiadu z wyznaczonymi pracownikami Klienta, celem zebrania informacji koniecznych do przeprowadzenia tej części prac audytowych.

Drugi etap audytu polega na sprawdzeniu przez konsultanta Qumak-Sekom, w jakim stopniu sposób implementacji produktu spełnia zalecenia i wytyczne producenta, a tym także sprawdzenie stosowanej wersji produktu, wymaganych przez producenta poprawek i uaktualnień.

Ostatnim etapem audytu jest zbadanie zgodności implementacji produktu/rozwiązania z zestawem dobrych praktyk, opracowanych i zalecanych przez konsultantów Qumak-Sekom na podstawie własnego doświadczenia i praktyki oraz na bazie światowych standardów powszechnie uznanych za obowiązujące.

### **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 Rozwiązania Firewall dla następujących produktów/rozwiązań:

- CheckPoint FireWall-1,
- Cisco Secure PIX Firewall,
- MS ISA Server,
- G2 Firewall,
- IPChains,
- IPTables,
- IPF.

### **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.

---

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

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 umożliwi 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](mailto:security@qumak.pl)