



Audyt Systemu IDS

Cel

Celem Audytu Systemu IDS jest zapewnienie systemowi informatycznemu Klienta należytej ochrony, poprzez skutecznie i sprawnie działające mechanizmy wykrywania naruszeń i zagrożeń (IDS).

Charakterystyka usługi

Audyt Systemu IDS jest skierowany do Klientów posiadających wdrożone rozwiązanie z dziedziny wykrywania naruszeń i zagrożeń (IDS), 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 przypadku systemów IDS niezwykle ważne są zagadnienia organizacyjne i proceduralne, które w znacznym stopniu mogą stanowić o skuteczności funkcjonowania całego rozwiązania. Współczesne systemy IT są bowiem źródłem wielu zdarzeń, spośród których należy wyselekcjonować te noszące znamiona naruszenia zasad bezpieczeństwa i w odpowiedni sposób je obsłużyć – szczególnie na poziomie proceduralnym.

Mając na uwadze znaczenie kwestii organizacyjnych i proceduralnych w ramach Audytu Systemu IDS zbadane zostaną m.in. następujące zagadnienia:

- Zarządzanie systemem IDS (poziom administratora);
- Raportowanie i eskalacja:
 - W stanie normalnej pracy systemu,
 - W przypadku wykrycia naruszeń zasad bezpieczeństwa.
- Archiwizacja danych systemu IDS;
- Kontrola wewnętrzna.

Audyt Systemu IDS w sferze technicznej obejmuje dwa podstawowe zagadnienia:

1. Poprawność architektury systemu IDS pod kątem potrzeb Klienta oraz dobrych praktyk.
2. Skuteczność wykrywania nieuprawnionych działań i naruszeń zasad bezpieczeństwa.

W ramach części pierwszej ocenie poddana zostanie architektura systemu IDS, a w szczególności jej zdolność do ochrony systemu teleinformatycznego Klienta i kluczowych jego elementów oraz zgodność architektury z powszechnie przyjętymi standardami dotyczącymi budowy systemów IDS (*host-based, network-based* itp.).

Druga część stanowi praktyczną weryfikację skuteczności działania systemu IDS i obejmuje przeprowadzenie szeregu kontrolowanych ataków i prób naruszeń zasad bezpieczeństwa. W ramach tej części prac konsultanci Qumak-Sekom zrealizują ustalony wcześniej z Klientem scenariusz działań, który pozwoli na ocenę:

- Zgodności działania systemu IDS z założeniami polityk i procedur,
- Jakości implementacji systemu IDS względem zestawu dobrych praktyk, przygotowanych przez Qumak-Sekom.

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 IDS dla następujących produktów/rozwiązań:

- RealSecure firmy Internet Security Systems,
- IntruShield firmy NAI,
- Cisco IDS.

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