baramundi

CHECKLISTY BARAMUNDI zapewniają zwięzłe i szczegółowe wskazówki ekspertów odnoszące się do częstych pytań i problemów. Więcej z nich można znaleźć na stronie www.baramundi.com/checklisty

Audyt IT: 7 kroków do zwiększenia bezpieczeństwa cyfrowego

Cyberprzestępcy szukają luk w zabezpieczeniach, aby przeprowadzać ataki i osiągać zyski z wykorzystaniem oprogramowania ransomware. Systematyczny i dokładny audyt ujawni potencjalne zagrożenia i niedociągnięcia w IT. Dzięki temu możliwe będzie zabezpieczenie użytkowników i systemów, zapewnienie zgodności z przepisami i zwiększenie produktywności firmy.

Zaplanuj

Od sprzętu po zarządzanie danymi, zidentyfikuj obszary i systemy do audytu. Zdefiniuj konkretne cele, takie jak zapewnienie zgodności, udokumentowanie istniejących praktyk bezpieczeństwa lub zwiększenie świadomości na temat cyberbezpieczeństwa wśród użytkowników.

Dokumentuj

Utrzymuj aktualną i kompletną inwentaryzację całego sprzętu, oprogramowania, komponentów sieciowych i konfiguracji systemów. Dzięki temu możliwa będzie ocena aktualnego stanu i postępów.

Sprawdź efektywność zabezpieczeń

Zaangażuj zaufane podmioty do przeprowadzenia pentestów i analiz podatności istniejących środków bezpieczeństwa IT, takich jak firewalle i programy antywirusowe. Koniecznie przejrzyj konfiguracje serwerów i komponentów sieciowych.

Sprawdź zgodność

Upewnij się, że Twoje IT jest zgodne ze wszystkimi obowiązującymi przepisami, standardami branżowymi lub wewnętrznymi wymaganiami dotyczącymi bezpieczeństwa, ochrony danych i ciągłości działania. Pomoże to szybko wznowić operacje po wystąpieniu sytuacji awaryjnej.

Zoptymalizuj efektywność

Przeanalizuj, czy wydajność systemu i infrastruktura sieciowa spełniają bieżące potrzeby biznesowe i są wystarczająco skalowalne, aby obsługiwać okresy wysokiego zapotrzebowania, w tym podczas odzyskiwania danych.

Stwórz plan działania

Zdefiniuj działania i potrzebne zasoby w oparciu o priorytet lub pilność. Wyznacz jasne obowiązki i terminy, a następnie zajmij się zidentyfikowanymi słabościami i niedociągnięciami.

Zaraportuj

Ostatnim krokiem jest raport z audytu, który zawiera ustalenia, zalecenia i priorytety dotyczące usprawnień. Stanowi on podstawę dla wszystkich kolejnych działań. Raport należy udostępnić odpowiednim zainteresowanym stronom.

W pigułce: Regularne audyty IT pozwalają zidentyfikować zagrożenia dla bezpieczeństwa cyfrowego. Niezależnie od tego, czy chodzi o inwentaryzację, skanowanie podatności czy zarządzanie aktualizacjami, baramundi Management Suite zagwarantuje powodzenie audytu w każdym obszarze IT.