



# Audyty i Testy Penetracyjne

AUDYTY BEZPIECZEŃSTWA

AUDYTY SYSTEMÓW  
BEZPIECZEŃSTWA

ANALIZA RYZYKA

TESTY PENETRACYJNE

TESTY BEZPIECZEŃSTWA  
SYSTEMÓWANALIZY WYKORZYSTANIA  
INTERNETUSYSTEMY ZARZĄDZANIA  
BEZPIECZEŃSTWEM  
INFORMACJISYSTEMY MONITOROWANIA  
INTERNETUSYSTEMY BEZPIECZNEGO  
PRZESYŁANIA INFORMACJI

PLANY CIĄGŁOŚCI DZIAŁANIA

OCHRONA DANYCH  
OSOBYCHOCHRONA TAJEMNICY  
PRZEDSIĘBIORSTWA

ZARZĄDZANIE PROJEKTAMI

DORADZTWO

SZKOLENIA

WDROŻENIA

**Zapewnienie bezpieczeństwa** przetwarzanym informacjom to istotny element każdej działalności biznesowej. Przy obecnym tempie rozwoju technologii i pojawianiu się nowych zagrożeń, nawet najlepsze systemy zabezpieczeń technicznych i organizacyjnych nie gwarantują zapewnienia optymalnego poziomu bezpieczeństwa.

W celu utrzymania właściwego poziomu bezpieczeństwa konieczna jest okresowa weryfikacja jego rzeczywistego stanu. To, co zapewniało bezpieczeństwo pół roku temu, dziś może wymagać pilnych działań korygujących. Oferujemy wykonanie takiej weryfikacji poprzez przeprowadzenie odpowiednich audytów lub testów.

## Korzyści biznesowe z wykonywania audytów to:

- o eliminacja strat finansowych spowodowanych: błędami aplikacji, konfiguracją urządzeń, awariami, cyberprzestępczością, niedbalstwem lub brakiem świadomości pracowników,
- o optymalizacja kosztów poprzez lepsze wykorzystanie zasobów, materiałów, ludzi,
- o racjonalizacja i redukcja wydatków w obszarze informatyki (np. poprzez rezygnację z utrzymywania zbędnych licencji lub urządzeń, dopasowanie umów serwisowych do rzeczywistych potrzeb).

**Naszymi ekspertami** są profesjonalni audytorzy oraz pentesterzy, posiadający prestiżowe certyfikaty zawodowe i ogromne doświadczenie w realizowaniu prac dla dużych firm różnych sektorów.

## Przeprowadzamy Audyty:

- o Stanu obszaru IT (kadra, organizacja, dokumentacja, sprzęt, oprogramowanie, umowy z dostawcami)
- o Bezpieczeństwa we wszystkich obszarach zarządzania i przetwarzania informacji
- o Systemów Zarządzania Bezpieczeństwem Informacji
- o Funkcjonowania i efektywności systemów zabezpieczeń technicznych i organizacyjnych
- o Planów Ciągłości Działania i Procedur Awaryjnych
- o Identyfikujące źródła wycieku danych
- o Zgodności z obowiązującymi aktami prawnymi, normami i standardami
- o Przestrzegania wewnętrznych przepisów dotyczących bezpieczeństwa informacji
- o Procesu zarządzania użytkownikami i ich uprawnień w systemach informatycznych
- o Wykorzystania Internetu przez pracowników

## Wykonujemy testy penetracyjne:

Testy penetracyjne są jednym z głównych sposobów badania bezpieczeństwa systemów informatycznych. Testy, wykonywane metodami „black box”, „gray box”, „white box” wykrywają błędy w: oprogramowaniu, usługach, serwerach, urządzeniach sieci komputerowej oraz w ich konfiguracji. Testy wykrywają luki, które mogą być wykorzystane do przeprowadzenia włamania przez osoby nieuprawnione.

## Wykonujemy testy bezpieczeństwa aplikacji i serwisów internetowych:

Testy umożliwiają wykrycie istniejących luk w bezpieczeństwie aplikacji oraz serwisów dostępnych dla każdego z sieci Internet, które mogą zagrażać prywatności użytkowników lub zagrazić bezpieczeństwu danych oraz reputacji właściciela aplikacji/serwisu. Testy sprawdzają zabezpieczenia na poziomie baz danych, aplikacji oraz przesyłania informacji do/z aplikacji/serwisu. Weryfikują bezpieczeństwo gromadzenia informacji, mechanizmów uwierzytelniających, zarządzania sesjami, walidacji wprowadzanych danych oraz odporność na ataki odmowy usługi (ang. „Denial of Service”).

**Nasze raporty zawierają przydatne rekomendacje działań eliminujących wykryte podatności lub minimalizujących skutki potencjalnych ataków.**

**Ratels to gwarancja wysokiej jakości w rozsądnej cenie!**

Zapraszamy do zapoznania się z pełną ofertą naszych usług:

<http://www.ratels.pl/DoPobrania/OfertaRatels.pdf>