



LIFE IS FOR SHARING.

Kontakt

Zespół Cybersecurity

e-mail: B2B\_Security\_Squad@t-mobile.pl

# Analiza nadzoru nad punktem styku z Internetem



## Ocena wrażliwości bezpieczeństwa punktu styku z Internetem

Punkt styku z siecią Internet pełni podstawową rolę w zapewnieniu cyberbezpieczeństwa oraz identyfikacji zagrożeń. To pośrednik w ruchu komunikacyjnym, łączący ze światem zewnętrznym, który powinien być ściśle nadzorowany i traktowany jako punkt graniczny. Bezpośredni nadzór nad ruchem wychodzącym oraz przychodzącym to jeden z filarów skutecznego monitoringu infrastruktury teleinformatycznej. Brak właściwego monitoringu i analizy zdarzeń na styku z Internetem to jedna z podstawowych przyczyn występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego.

## Autorska metodyka badania wrażliwości

Dokonaj oceny wrażliwości na zagrożenia, badając infrastrukturę brzegową.

### Badanie ma na celu:

- Analizę architektury brzegowej.
- Weryfikację możliwości wykrywania w ruchu sieciowym aplikacji i treści o wysokim ryzyku.
- Sprawdzenie funkcjonalności IPS – wykrywanie i blokowanie znanych zagrożeń typu exploit.
- Wykrywanie zagrożeń na poziomie modułów funkcjonalnych firewall.

### Wynikiem przeprowadzonego badania będzie raport zawierający:

- Wrażliwość systemu na próby przesyłania szkodliwej zawartości w ruchu sieciowym.
- Identyfikację zagrożeń na brzegu z siecią Internet.
- Wytyczenie kierunku rozwoju oraz zmian koniecznych w celu zwiększania poziomu cyberbezpieczeństwa organizacji.

## Dlaczego Twoja firma potrzebuje takiego badania?

- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrożenia cyberbezpieczeństwa.