

T Business

# PAKIETY KSC (NIS2)



Choć przepisy ustawy o KSC, implementujące dyrektywę NIS2, najczęściej są kojarzone z dużymi organizacjami oraz sektorami infrastruktury krytycznej, w praktyce ich oddziaływanie jest znacznie szersze. Bezpieczeństwo przestaje być wyłącznie obowiązkiem regulacyjnym – staje się warunkiem współpracy.

Firmy będące częścią łańcucha dostaw organizacji objętych NIS2 lub KSC coraz częściej muszą dokumentować swoją dojrzałość w obszarze cyberbezpieczeństwa.

## Kto powinien sięgnąć po Pakiety KSC (NIS2)?

- **Firmy objęte KSC/NIS2**, które chcą spełnić wymagania regulacyjne.
- **Dostawcy i podwykonawcy organizacji regulowanych** – pod presją wymogów bezpieczeństwa w łańcuchu dostaw.
- **Wszystkie firmy, które chcą utrzymać ciągłość działania** i zapewnić bezpieczeństwo realnie dopasowane do swojego biznesu, bez nadmierowej złożoności.

## Jak pakiety wesprą Twoją organizację w spełnianiu wymagań ustawy KSC (NIS2)?



COMPLIANCE



DOSTĘPNOŚĆ  
USŁUG



BEZPIECZEŃSTWO  
URZĄDZEŃ



SZKOLENIA  
I ŚWIADOMOŚĆ



MONITORING  
I REAKCJA



SKANOWANIE  
PODATNOŚCI



OCHRONA  
DANYCH



Connecting  
your world.

## KSC (NIS2) Ready

Szybkie, podstawowe podniesienie poziomu bezpieczeństwa użytkowników i ruchu

### Cyber Check

Jednorazowy, szybki przegląd zgodności z wymaganiami dyrektywy NIS2.

### vCISO Lite

Wirtualny Dyrektor ds. bezpieczeństwa informacji.

### Bezpieczny Internet

Firewall, Antywirus, Ochrona przed intruzami, Antymalware, Kontrola aplikacji, Filtrowanie www.

### AntyDDoS Bronze

Blokowanie złośliwego ruchu.

### Cyber Guard® Lite

Analiza ruchu sieciowego i blokowanie złośliwej transmisji danych.

### MDM Gold

Zarządzanie i ochrona floty telefonów.

### Cyber Know (platforma szkoleniowa)

Edukacja pracowników – szkolenia na dedykowanej platformie.

### Cyber Know (phishing i smishing)

Budowanie świadomości przez testowe kampanie phishing i smishing.

### SOC Lite

Automatyczny monitoring bezpieczeństwa, zbieranie, korelacja i analiza zdarzeń oraz generowanie alertów.

### Business Backup

Szyfrowane kopie zapasowe, szybkie przywracanie danych.

## KSC (NIS2) Secure+

Centralna kontrola sieci i ochrona usług (kilka lokalizacji)

### Cyber Check

Jednorazowy, szybki przegląd zgodności z wymaganiami dyrektywy NIS2.

### vCISO Lite

Wirtualny Dyrektor ds. bezpieczeństwa informacji.

### Zarządzany Firewall Silver

Zapora sieciowa nowej generacji – monitoring, filtracja i blokada ruchu sieciowego.

### AntyDDoS Silver

Blokowanie złośliwego ruchu.

### Cyber Guard® Silver

Analiza ruchu sieciowego i blokowanie złośliwej transmisji danych.

### MDM Gold

Zarządzanie i ochrona floty telefonów.

### Cyber Know (platforma szkoleniowa)

Edukacja pracowników – szkolenia na dedykowanej platformie.

### Cyber Know (phishing i smishing)

Budowanie świadomości przez testowe kampanie phishing i smishing.

### SOC Lite/SOC

Całodobowy monitoring i reagowanie na incydenty bezpieczeństwa w systemach IT przez dedykowany zespół ekspertów.

### Testy penetracyjne

Kontrolowane ataki symulujące rzeczywiste działania cyberprzestępców.

### Skonowanie podatności

Przeszukiwanie infrastruktury IT w celu identyfikacji wszelkich potencjalnych luk w zabezpieczeniach.

### DRAAS

Zapasowe uruchomienie systemów w chmurze na czas awarii.

## KSC (NIS2) Pro

Wysoka dostępność usług online i odporność na ataki

### Doradztwo/vCISO

Wirtualny Dyrektor ds. bezpieczeństwa informacji, przegląd zgodności z wymaganiami ustawy KSC (NIS2).

### Audyty cyberbezpieczeństwa

- Audyt bezpieczeństwa
- Audyt zgodności

### Zarządzany Firewall Gold

Zapora sieciowa nowej generacji – monitoring, filtracja i blokada ruchu sieciowego.

### AntyDDoS Gold

Blokowanie złośliwego ruchu.

### Cyber Guard® Gold

Analiza ruchu sieciowego i blokowanie złośliwej transmisji danych.

### MDM Gold

Zarządzanie i ochrona floty telefonów.

### Cyber Know (platforma szkoleniowa)

Edukacja pracowników – szkolenia na dedykowanej platformie.

### Cyber Know (phishing i smishing)

Budowanie świadomości przez testowe kampanie phishing i smishing.

### SOC

Całodobowy monitoring i reagowanie na incydenty bezpieczeństwa w systemach IT przez dedykowany zespół ekspertów.

### Testy penetracyjne

Kontrolowane ataki symulujące rzeczywiste działania cyberprzestępców.

### Skonowanie podatności

Przeszukiwanie infrastruktury IT w celu identyfikacji wszelkich potencjalnych luk w zabezpieczeniach.

### DRAAS + Business Backup

Zapasowe uruchomienie systemów w chmurze na czas awarii.

## Wyzwania dla Twojej organizacji

- Rosnąca liczba zapytań o bezpieczeństwo.
- Rosnące wymagania regulacyjne i audytowe.
- Konieczność dokumentowania podstawowych zabezpieczeń.
- Brak kompetencji i wdrożonej strategii bezpieczeństwa.
- Ryzyko kar i utraty kontraktów.

## Kogo dotyczy KSC?

Nowe przepisy obejmują kluczowe i ważne podmioty, kwalifikowane na podstawie:

- **kryterium wielkościowego** – co do zasady średnie i duże przedsiębiorstwa (min. 50 pracowników lub >10 mln euro obrotu/bilansu),
- **kryterium sektorowego** – prowadzenie działalności w sektorach wskazanych w ustawie.

**KSC (NIS2) to nie tylko regulacja, lecz także wymóg rynkowy.**

**Firmy niepodlegające regulacjom mogą być rozliczane przez:**

- dużych klientów,
- łańcuch dostaw,
- procesy zakupowe i przetargi.

T-Mobile Polska  
ul. Marynarska 12  
02-674 Warszawa

Więcej informacji o usługach:  
[www.biznes.t-mobile.pl](http://www.biznes.t-mobile.pl)

