

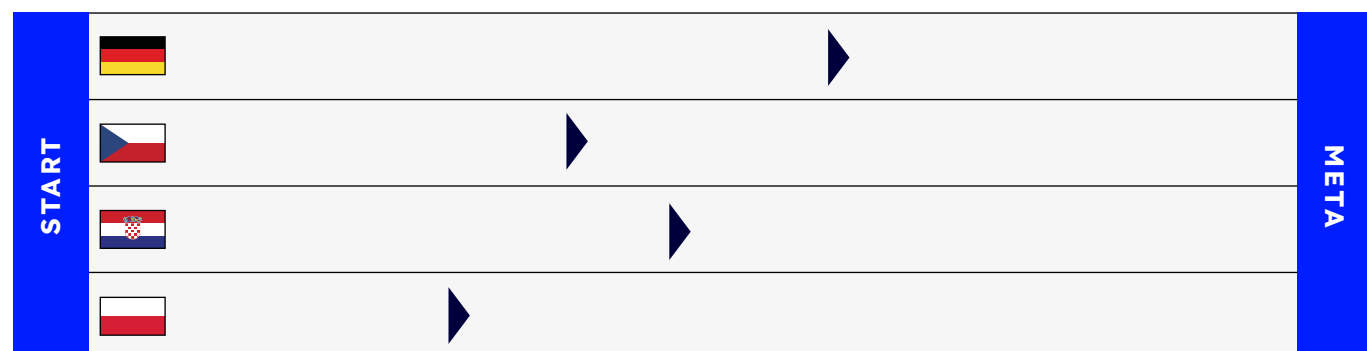
DYREKTYWA NIS2

Poznaj nowe rozporządzenia w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej

Chcąc nadążyć za rosnącą cyfryzacją i zmieniającym się krajobrazem zagrożeń dla podmiotów publicznych i prywatnych, unijne przepisy dotyczące cyberbezpieczeństwa, zostały zaktualizowane **dyrektywą NIS2**.

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci **obowiązkiem stosowania produktów, usług bądź procesów**, objętych tymi schematami certyfikacyjnymi.

DYREKTYWA NIS2 - WYŚCIG Z CZASEM:



NIS2 – CEL I KIERUNEK:

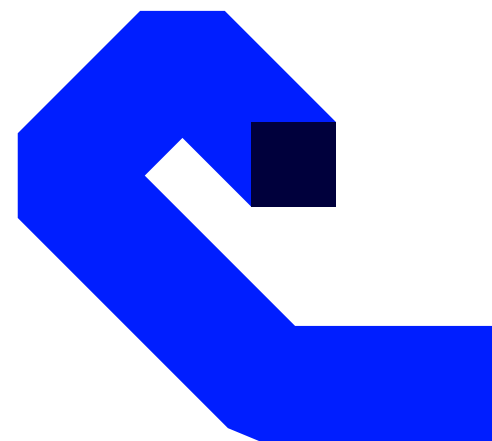
- Podstawowym kryterium jest wielkość przedsiębiorstwa działająca na terenie UE
- Podział podmiotów publicznych i prywatnych na dwie kategorie: kluczowe oraz ważne, które objęte zostaną tymi samymi minimalnymi wymogami bezpieczeństwa.
- Nadzór zarządu: **brak odpowiedniego nadzoru może skutkować nałożeniem kar przez organy właściwe. Zarządy muszą zaaprobować miary, nadzorować implementację oraz wdrożyć odpowiednią strategię z zakresu analizy i zarządzania ryzykiem**
- System kar administracyjnych:
 - podmioty kluczowe – minimum 10 mln EUR lub 2% rocznego obrotu
 - podmioty ważne – minimum 7 mln EUR lub 1,4 % rocznego obrotu.

KLUCZOWE OBSZARY KONTROLNE:

- Dyrektywa wprowadza określony zakres środków zaradczych bezpieczeństwa, które organizacje są zobowiązane wdrożyć, aby zapewnić efektywne zarządzanie ryzykiem:
- Zarządzanie ryzykiem i polityka bezpieczeństwa systemów informatycznych
- Zapewnienie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych
- Bezpieczeństwo łańcucha dostaw
- Podstawowe praktyki z zakresu cyberhigieny i szkoleń
- Ujawnianie i zarządzanie podatnościami
- Zapewnienie wykorzystywania kryptografii szyfrowania
- Zarządzanie ryzykiem i polityka bezpieczeństwa systemów informatycznych

Jak AltKom Akademia może wesprzeć Twoją organizację w dostosowaniu się do NIS2?

Nasza firma szkoleniowa oferuje kompleksowe szkolenia dla pracowników, które pomogą Twojej firmie zrozumieć i wdrożyć wymogi dyrektywy NIS2. Nasze kursy są zaprojektowane tak, aby dostarczyć praktycznej wiedzy i umiejętności niezbędnych do skutecznego dostosowania się do nowych przepisów.



GŁÓWNE FILARY EDUKACJI:

Zarządzanie ryzykiem i polityki bezpieczeństwa systemów informatycznych	<ul style="list-style-type: none"> ■ Warsztaty z Comptia Security + (przygotowanie do egzaminu SY0-701) ■ Warsztaty z Comptia Cybersecurity Analyst (CYSA+) (przygotowanie do egzaminu CS0-003) ■ Certified Ethical Hacker (CEHV12) ■ Bezpieczny administrator - praktyczny warsztat z bezpieczeństwa IT (BS.IT 04) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10 (Security MS) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2022 w połączeniu z Windows 11 (Security MS_2022) Stacjonarnie / Distance Learning ■ Bezpieczeństwo systemu Windows 10 (Security Windows 10) ■ Bezpieczeństwo systemu Windows 11 (Security Windows 11) Stacjonarnie / Distance Learning ■ Bezpieczeństwo aplikacji webowych (BEZP_WEB)
Zarządzanie incydentami security: zapobieganie, wykrywanie i reagowanie na nie	<ul style="list-style-type: none"> ■ Warsztaty z Comptia Security + (przygotowanie do egzaminu SY0-701) ■ Warsztaty z Comptia Cybersecurity Analyst (CYSA+) (przygotowanie do egzaminu CS0-003) ■ Certified Ethical Hacker (CEHV12) ■ Bezpieczny administrator - praktyczny warsztat z bezpieczeństwa IT (BS.IT 04) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10 (Security MS) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2022 w połączeniu z Windows 11 (Security MS_2022) Stacjonarnie / Distance Learning ■ Bezpieczeństwo systemu Windows 10 (Security Windows 10) ■ Bezpieczeństwo systemu Windows 11 (Security Windows 11) Stacjonarnie / Distance Learning ■ Bezpieczeństwo aplikacji webowych (BEZP_WEB)
Zapewnienie bezpieczeństwa w procesie nabywania rozwoju i utrzymania sieci i systemów informatycznych	<ul style="list-style-type: none"> ■ ITIL® 4 Foundation - akredytowane szkolenie z egzaminem (ZP-ITIL4-FX) ■ ITIL® 4 Specialist: Plan, Implement and Control - akredytowane szkolenie z egzaminem (ZP-ITIL4-PIC) ■ ITIL® 4 Practices: Monitor, Support and Fulfil (MSF) - akredytowane szkolenie z egzaminem (ZP-ITIL4-MSF) ■ DevSecOps Foundation - akredytowane szkolenie z egzaminem (ZP-DSOF-DOI) ■ Warsztaty praktyczne Comptia Network+ (przygotowanie do egzaminu N10-008) ■ Podstawy działania sieci opartych na modelu TCP/IP (TCP/IP) ■ Analiza ruchu sieciowego w modelu TCP/IP (TCP/IP_poziom 2) ■ Configure SIEM security operations using Microsoft Sentinel (SC-5001)
Podstawowe praktyki z zakresu cyberhygieny i szkoleń	<ul style="list-style-type: none"> ■ Warsztaty z cyberbezpieczeństwa (BS.IT CS) ■ Bezpieczny pracownik - wykłady cyber awareness dla pracowników biurowych (BS.IT 00) ■ Wprowadzenie do zagadnień bezpieczeństwa IT (BS.IT 01) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10 (Security MS) ■ Bezpieczeństwo systemów w domenie Active Directory Windows Server 2022 w połączeniu z Windows 11 (Security MS_2022) Stacjonarnie / Distance Learning ■ Bezpieczeństwo systemu Windows 10 (Security Windows 10) ■ Bezpieczeństwo systemu Windows 11 (Security Windows 11) Stacjonarnie / Distance Learning ■ Bezpieczeństwo w pracy biurowej (BEZ_OFF)
Zapewnienie wykorzystywania kryptografii szyfrowania	<ul style="list-style-type: none"> ■ Warsztaty z Comptia Security + (przygotowanie do egzaminu SY0-701) ■ Wprowadzenie do zagadnień bezpieczeństwa IT (BS.IT 01) ■ Certified Ethical Hacker (CEHV12)
Ciągłość działania i zarządzanie kryzysowe	<ul style="list-style-type: none"> ■ Budowa planów ciągłości działania (PCD)
Ujawnianie i zarządzanie podatnościami	<ul style="list-style-type: none"> ■ Warsztaty z Comptia Security + (przygotowanie do egzaminu SY0-701) ■ Warsztaty z Comptia Cybersecurity Analyst (CYSA+) (przygotowanie do egzaminu CS0-003) ■ Certified Penetration Testing (CPENT) ■ Bezpieczny administrator - praktyczny warsztat z bezpieczeństwa IT (BS.IT 04)