European Commission

# NACISKAMY PRZYCISK ODŚWIEŻANIA W SPRAWACH ZASAD BEZPIECZEŃSTWA CYBERNETYCZNEGO

## NIS2: WNIOSEK DOTYCZĄCY DYREKTYWY W SPRAWIE ŚRODKÓW NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU BEZPIECZEŃSTWA CYBERNETYCZNEGO W CAŁEJ UNII

16 GRUDNIA 2020

#SecurityUnion #DigitalEU

**Pierwsza ogólnounijna ustawa o bezpieczeństwie cybernetycznym**, dyrektywa NIS, weszła w życie w 2016 r. i pomogła osiągnąć wyższy i bardziej wyrównany poziom bezpieczeństwa sieci i systemów informatycznych w całej UE. W obliczu bezprecedensowej cyfryzacji w ostatnich latach, nadszedł czas na jej odświeżenie.

## Jak?

### Większe możliwości

| NIS | NIS 2 |
|---|---|
| Państwa członkowskie UE poprawiają swoje zdolności w zakresie bezpieczeństwa cybernetycznego. | Wprowadzono bardziej rygorystyczne środki nadzoru i egzekwowania prawa. |
| | Ustala się listę sankcji administracyjnych, w tym grzywien, za naruszenie obowiązków w zakresie zarządzania ryzykiem cyberbezpieczeństwa i raportowania. |

### Współpraca

| NIS | NIS 2 | |
|---|---|---|
| Zwiększona współpraca na poziomie UE. | Utworzenie europejskiej sieci organizacji łącznikowych ds. kryzysów cybernetycznych (EU- CyCLONe) w celu wspierania skoordynowanego zarządzania incydentami i kryzysami związanymi z bezpieczeństwem cybernetycznym na dużą skalę na poziomie UE | Zwiększona wymiana informacji i współpraca między organami państw członkowskich przy zwiększonej roli Grupy Współpracy. |
| | | Ustanawia się skoordynowane ujawnianie nowo odkrytych luk w zabezpieczeniach w całej UE. |

### Zarządzanie ryzykiem w zakresie cyberbezpieczeństwa

| NIS | NIS 2 | | |
|---|---|---|---|
| Operatorzy Istotnych Usług (OES) i Dostawcy Usług Cyfrowych (DSP) muszą przyjąć praktyki zarządzania ryzykiem i zgłaszać znaczące incydenty do swoich władz krajowych. | Wzmocnione wymogi bezpieczeństwa z listą ukierunkowanych środków, w tym reagowanie na incydenty i zarządzanie kryzysowe, obsługę i ujawnianie słabych punktów, polityki i procedury oceny skuteczności środków zarządzania ryzykiem w zakresie bezpieczeństwa cybernetycznego, podstawowe praktyki higieny komputerowej i szkolenia w zakresie bezpieczeństwa cybernetycznego, skuteczne stosowanie kryptografii oraz bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzanie aktywami. | Cyberbezpieczeństwo łańcucha dostaw kluczowych technologii informacyjnych i komunikacyjnych zostanie wzmocnione. | Odpowiedzialność kierownictwa firmy za przestrzeganie środków zarządzania ryzykiem w zakresie bezpieczeństwa cybernetycznego. |
| | | | Usprawnienie obowiązku zgłaszania incydentów z bardziej precyzyjnymi przepisami dotyczącymi procesu zgłaszania, treści i terminów. |

# SEKTORY OBJĘTE DYREKTYWĄ NIS

## NIS

- OCHRONA ZDROWIA
- TRANSPORT
- INFRASTRUKTURA RYNKU BANKOWEGO I FINANSOWEGO
- INFRASTRUKTURA CYFROWA
- DOSTAWY WODY
- ENERGIA
- DOSTAWCY USŁUG CYFROWYCH

## NIS 2

Rozszerzony zakres, aby objąć więcej sektorów i usług jako kluczowych lub ważnych jednostek.

- DOSTAWCY PUBLICZNYCH SIECI LUB USŁUG ŁĄCZNOŚCI ELEKTRONICZNEJ
- USŁUGI CYFROWE, TAKIE JAK PLATFORMY SERWISÓW SPOŁECZNOŚCIOWYCH I USŁUGI CENTRÓW DANYCH
- ŚCIEKI I GOSPODARKA ODPADAMI
- PRZESTRZEŃ KOSMICZNA
- PRODUKCJA NIEKTÓRYCH KRYTYCZNYCH PRODUKTÓW (TAKICH JAK FARMACEUTYKI, URZĄDZENIA MEDYCZNE, CHEMIKALIA)
- USŁUGI POCZTOWE I KURIERSKIE
- ŻYWNOŚĆ
- ADMINISTRACJA PUBLICZNA



Publications Office of the European Union

PDF ISBN 978-92-76-27602-9 doi: 10.2759/0630 KK-02-20-102-EN-N
BOOK ISBN 978-92-76-27603-6 doi:10.2759/7745526 KK-02-20-102-EN-C

Updated 2022-05-11