Zadanie
„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

Obowiązki szkół wyższych związane ze zgłaszaniem incydentów

Prelegent: dr Agnieszka Besiekierska

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Status uczelni/ incydent

- Uczelnie publiczne jako podmioty krajowego systemu cyberbezpieczeństwa (**podmioty publiczne)** – art.4 pkt 7 w zw. z art. 9 pkt 11 ustawy o finansach publicznych
- **Incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
- **incydent krytyczny** – incydent skutkujący **znaczną szkodą** dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, **klasyfikowany przez właściwy CSIRT**;

Obowiązki bezpośrednio związane z incydentami

- Jako **uczelnia publiczna** podmiot publiczny realizuje obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa:

1) zapewnia **zarządzanie incydentem** w podmiocie publicznym (zarządzanie incydentem obejmuje obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu);

2) zgłasza incydent w podmiocie publicznym **niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia do **CSIRT NASK;**

3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z CSIRT NASK, przekazując niezbędne dane, w tym dane osobowe;

Może przekazywać do CSIRT NASK informacje: 1) o innych incydentach; 2) o zagrożeniach cyberbezpieczeństwa; 3) dotyczące szacowania ryzyka; 4) o podatnościach; 5) o wykorzystywanych technologiach.

Obowiązki pośrednio związane z incydentami

*4) **zapewnia osobom,** na rzecz których zadanie publiczne jest realizowane, **dostęp do wiedzy** pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;*

5) przekazuje do właściwego CSIRT NASK dane osoby odpowiedzialnej za utrzymanie kontaktu w ramach ksc, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

Forma zgłoszenia

w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji;

Zawartość zgłoszenia – art. 23 uksc **https://incydent.cert.pl/**

- Czy incydent miał wpływ na realizację zadań publicznych? Jeśli tak, na jakie?
- Czy możesz określić dokładną lub przybliżoną liczbę osób, na które ma wpływ incydent?
- Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydentu?
- Czy możesz geograficznie określić obszar, którego dotyczy incydent?
- Czy ustaliłeś przyczynę incydentu?
- Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?
- Opisz najdokładniej jak potrafisz przebieg incydentu
- Czy podjęto działania zapobiegawcze w związku z incydentem? Jeśli tak, prosimy opisać te działania.
- Jakie działania naprawcze podjąłeś w związku z incydentem?
- Inne istotne informacje

Dziękuję za uwagę