



Cykl konferencji nt. bezpieczeństwa

Rola szkół i placówek w systemie obrony cywilnej (zgodnie z ustawą OLiOC) – zadania i wyzwania w obliczu współczesnych zagrożeń

Kraków - 24.11.2025
Tarnów - 04.12.2025
Nowy Sącz - 09.12.2025

Wykładowcy: kadra naukowo-dydaktyczna Wydziału Nauk o Bezpieczeństwie UAfM
oraz współpracownicy - specjaliści w zakresie OLiOC.

Konferencje realizowane pod Honorowym Patronatem:
Wojewody Małopolskiego dr Krzysztofa Klęczara, Małopolskiego Kuratora Oświaty dr Gabrieli Olszowskiej
Rektora Uniwersytetu Andrzeja Frycza Modrzewskiego dr Macieja Kluza

**U
A
F
M** UNIwersytet
Andrzeja Frycza Modrzewskiego
w Krakowie



Bezpieczeństwo cybernetyczne w systemie oświaty

dr Marcei HERMAN
Wydział Nauk o Bezpieczeństwie
Uniwersytet Andrzeja Frycza Modrzewskiego,
ul. Herlinga-Grudzińskiego 1,
30 – 705 Kraków



CEL WYKŁADU

1. Wzmocnienie świadomości przedstawicieli systemu oświaty w kontekście zagrożeń cybernetycznych;
2. Identyfikacja i klasyfikacja zagrożeń cybernetycznych w placówkach oświatowych;
3. Przedstawienie algorytmów postępowania w sytuacji zagrożenia dla infrastruktury cybernetycznej w systemie oświaty.





CYBERBEZPIECZEŃSTWO - ZNACZENIE DEFINICYJNE

„odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”.



KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA - ZNACZENIE DEFINICYJNE

„ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów”.

PODSTAWY PRAWNE BEZPIECZEŃSTWA CYBERNETYCZNEGO W SYSTEMIE OŚWIATY



Ustawa z dnia 5 lipca 2018 r.
o krajowym systemie cyberbezpieczeństwa

Ustawa z dnia 14 grudnia 2016 r.
Prawo oświatowe

Ustawa z dnia 10 maja 2018 r.
o ochronie danych osobowych

Narodowe Standardy Cyberbezpieczeństwa
(NSC)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA (NSC)

1. NSC 199, Standardy kategoryzacji bezpieczeństwa
2. NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych
3. NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych
4. NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne
5. NSC 800-34, Poradnik Planowania Awaryjnego
6. NSC 800-46, Przewodnik po telepracy w podmiocie publicznym



objawy wskazujące na zainfekowanie jednostki teleinformatycznej

komputer wolniej pracuje



nie można uruchomić niektórych programów



skrzynka pocztowa zawiera wiele wiadomości
bez nagłówka lub adresu e-mail nadawcy



samoczynne działanie urządzenia

objawy wskazujące na infekcję/atak



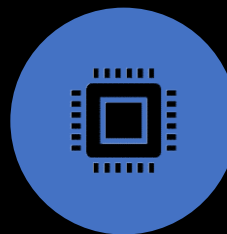
na pulpicie komputera
pojawiają się różne
komunikaty z reklamami
czy ostrzeżeniami



w systemie pojawiają się
nowe, nieznane programy



komputer generuje
przypadkowe dźwięki



samoczynnie otwiera i
zamyka się napęd CD-
ROM;

Rodzaje zabezpieczeń

1. Antywirus,
antyspyware oraz
firewall

2. Zabezpieczenia
behawioralne

3. Usuń śmieci i
próbki

4. Aktualizuj swoje
oprogramowanie

5. Załóż konto do
kontroli wszystkich
kont

6. Zabezpiecz sieć
oraz przeglądarkę

7. Ustaw punkt
przywracania
systemu

8. Uświadom
innych
użytkowników
komputera

9. Fizyczne
zabezpieczenie

10. Bądź uważny i
rozważny

Źródła ataku / pobudki

zemsta byłego
pracownika/ucznia/
studenta;

oszustwo ukierunkowane
na korzyści finansowe
bądź skompromitowanie
placówki;

atak terrorystyczny,
którego celem jest
spowodowanie jak
największej szkody

atak terrorystyczny o
charakterze pośrednim,
którego celem
odwrócenie uwagi od
ataku właściwego

szpiegostwo, pozyskanie
danych, które mają jakąś
wartość (rynkową bądź
intelektualną);

zabawa, testowanie
bezpieczeństwa, chęć
przerwania egzaminów

IDENTYFIKACJA I KLASYFIKACJA ZAGROZEŃ CYBERNETYCZNYCH W PLACÓWKACH OŚWIATOWYCH



Serwisy społecznościowe



Bezpieczeństwo dzieci w
internecie



Bezpieczeństwo urządzeń
mobilnych



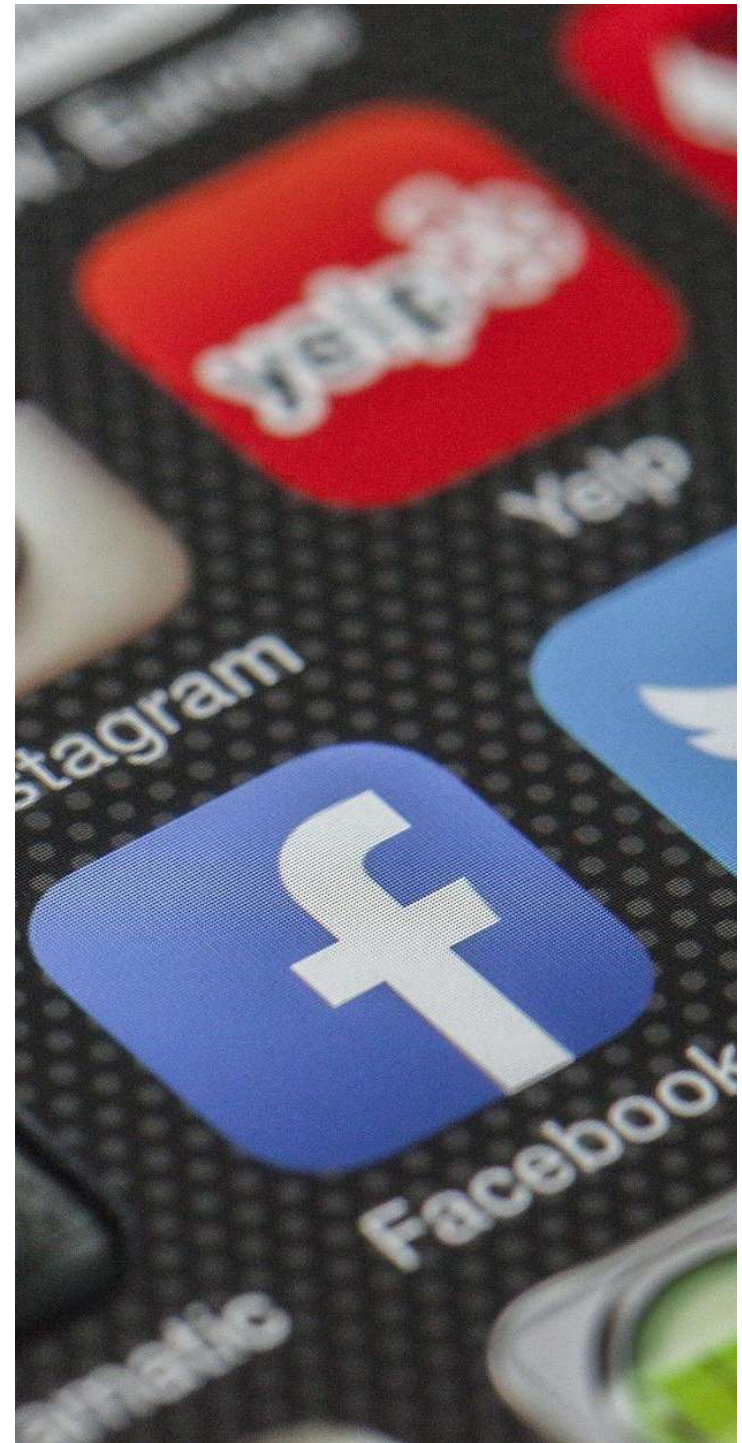
Ataki na infrastrukturę placówek
oświatowych



[To zdjęcie](#), autor: Nieznany autor, licencja: [CC BY-SA-NC](#)

PROPONOWANE REKOMENDACJE BEZPIECZEŃSTWA CYBERNETYCZNEGO DLA: Serwisów społecznościowych

1. Bezpieczeństwo informacji;
2. Silne hasło;
3. Konfiguracja ustawień prywatności;
4. Udostępnianie danych (gry, quizy);
5. **WYCHOWANIE/ZAINTERESOWANIE
DZIECKIEM**
 1. rozmowy uświadamiające,
 2. bezwzględne reagowanie w przypadkach zagrożeń,
 3. zwiększenie rygorystyczności w ustawieniach prywatności
 4. monitorowanie zachowań dziecka



**PROPONOWANE REKOMENDACJE
BEZPIECZEŃSTWA CYBERNETYCZNEGO DLA:**
Bezpieczeństwa dzieci w internecie



1. Kompleksowa konfiguracja urządzenia przekazanego dziecku:
 - a. program antywirusowy, filtry kontroli rodzicielskiej, automatyczne płatności, ograniczenia czasowe
2. Monitorowanie zachowania w sieci;
 - a. rodzaj publikowanych treści;
 - b. odwiedzane strony;
 - c. nawiązywane znajomości

PROPONOWANE REKOMENDACJE BEZPIECZEŃSTWA CYBERNETYCZNEGO DLA: Bezpieczeństwa urządzeń mobilnych

1. Pierwszy krok: Pomyśl – Połącz;
2. Zadbaj o ich bezpieczeństwo danych:

 1. Chronić urządzenia przed niepowołanym dostępem
 2. Wybór aplikacji
 3. Hotspoty WiFi
3. Urządzenia zawsze aktualne:
 1. Aktualizacje
 2. Jednorazowe wykorzystanie aplikacji



Najczęstsze cyberzagrożenia w szkołach

Malware i Ransomware

to złośliwe oprogramowania mogące sparaliżować systemy szkolne, powodując utratę danych i zakłócenia.

Nieautoryzowany dostęp

Nieautoryzowany dostęp do systemów szkolnych stanowi poważne zagrożenie dla bezpieczeństwa danych uczniów i personelu.

DDoS (rozproszona odmowa usługi) atakujący przytłaczają sieć organizacji lub witrynę internetową ruchem, obciążając jej funkcjonowanie



Ataki socjotechniczne — phishing, inżynieria społeczna

Ataki socjotechniczne

polegają na manipulacji ludźmi w celu uzyskania poufnych informacji lub dostępu;

Phishing

to podszywanie się pod zaufane źródła w celu wyłudzenia danych, często przez fałszywe e-maile lub strony;

Wpływ na systemy szkolne

Phishing i inżynieria społeczna mogą zagrozić bezpieczeństwu danych i dostępowi do systemów edukacyjnych.



Procedury reagowania na incydenty



To zdjęcie, autor: Nieznany autor, licencja: [CC BY](#)

**proponowany
algorytm
postępowania
awaryjnego w
przypadku ataku
cybernetycznego**

Przygotowanie na
incydent

Identyfikacja ataku

Izolowanie
zagrożenia

Testowanie procedur

Regularne aktualizacje

Szkolenia pracowników

Wsparcie zewnętrzne

Współpraca z CERT, policją, organami administracji publicznej



1. Policja – Centralne Biuro Zwalczania Cyberprzestępczości;
2. CERT.PL;
3. CSIRT GOV;
4. CSIRT MON;
5. CSIRT NASK;
6. ABW;
7. SKW;
8. Żandarmeria Wojskowa

PROPONOWANE REKOMENDACJE PRZEDSTAWICIELI SYSTEMU OŚWIATY

-
1. Świadomość zagrożeń infrastruktury cybernetycznej;
 2. Wdrażanie polityk bezpieczeństwa;
 3. Szkolenia personelu



PODSUMOWANIE

- 1. scharakteryzowano objawy ataku cybernetycznego**
- 2. dokonano identyfikacji i klasyfikacji zagrożeń cybernetycznych w placówkach oświatowych**
- 3. wskazano proponowane algorytmy postępowania na wypadek ataku na system oświaty (lokalny, ogólnopolski)**





DZIĘKUJĘ ZA UWAGĘ

dr Marcei HERMAN
Wydział Nauk o Bezpieczeństwie
Uniwersytet Andrzeja Frycza Modrzewskiego,
ul. Herlinga-Grudzińskiego 1,
30 – 705 Kraków
tel. 606-717-029