

Procedury reagowania w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego

Spis procedur:

1. Procedura – dostęp do treści szkodliwych, niepożądanych i nielegalnych
2. Procedura – cyberprzemoc
3. Procedura – naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły
4. Procedura – zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu
5. Procedura – nawiązywanie niebezpiecznych kontaktów w Internecie – uwodzenie, zagrożenie pedofilią
6. Procedura – seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich
7. Procedura – bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam
8. Procedura – łamanie prawa autorskiego
9. Procedura – zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online

Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole.

Systematycznie prowadzone działania profilaktyczne w znacznej mierze ograniczają zakres zagrożeń uczniów występujących w cyberprzestrzeni, nie są jednak w stanie ich całkowicie wyeliminować. **W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechować powinna otwartość w działaniu, szybka identyfikacja problemu – określenie szkodliwych lub niezgodnych z prawem zachowań – i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.** Podobnie asertywnie, bez zwłoki, merytorycznie – z wykorzystaniem wiedzy ekspertów i dobrych praktyk z innych placówek – szkoła powinna zareagować w przypadku wystąpienia problemów wynikających z deficytu lub braku wiedzy ucznia, np. na temat prawa autorskiego.

Zagrożenia bezpieczeństwa cyfrowego w szkole oraz problemy ucznia w świecie cyfrowym mogą mieć różnorodny charakter. W niniejszym opracowaniu nie podejmowano próby ich systematycznego opisu, natomiast dokonano analizy służącej określeniu procedur reagowania na występujące zagrożenia lub deficyty kompetencji, eksperci korzystali przede wszystkim z wartościowych publikacji: *Standard bezpieczeństwa online placówek oświatowych*.

Warto przy tym podkreślić, iż nie istnieje „złota recepta”, którą zastosować można we wszystkich przypadkach wystąpienia zagrożeń spowodowanych przez uczniów. Dyrektorzy i nauczyciele muszą uwzględniać kontekst indywidualnych przypadków, a także ich szkolne i środowiskowe tło i reagować adekwatnie do poziomu odpowiedzialności i winy ucznia.

Obligatoryjne działania interwencyjne, będące następstwem wystąpienia zagrożenia, zawsze podzielić można na 3 grupy:

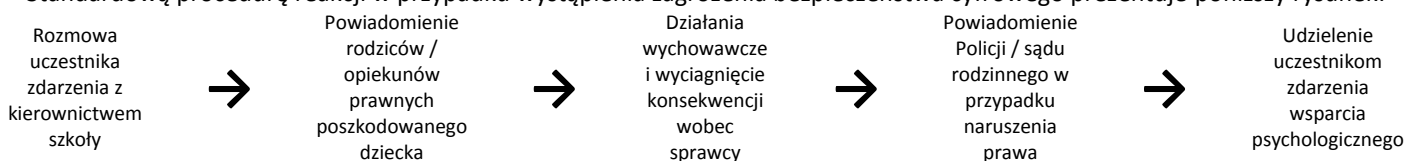
- 1) **działania wobec aktu / zdarzenia** – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring pointerwencyjny,
- 2) **działania wobec uczestników zdarzenia** (ofiara / sprawca / świadek, rodzice),
- 3) **działania wobec instytucji / organizacji / służb pomocowych i współpracujących** – Policji, wymiaru sprawiedliwości, służb społecznych.

Na każdą procedurę reakcji na wystąpienie danego typu zagrożenia cyberbezpieczeństwa w szkole muszą składać się działania tego typu – podjęte przez dyrekcję szkoły oraz nauczycieli, pedagogów / psychologów szkolnych. Ich szczegółowy opis znajduje się w opracowaniu: *Standard bezpieczeństwa online placówek oświatowych* opracowanym przez zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie. Publikacja opracowana została w ramach realizowanego przez Fundację Odkrywców Innowacji projektu *Działania na rzecz bezpiecznego korzystania z Internetu* (<http://bezpiecznyinternet.edu.pl/produkty/standard/>).

Działania wobec aktu / zdarzenia polegają przede wszystkim na zachowaniu (nie usuwaniu) dokumentacji cyfrowej: wiadomości SMS, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów w blogu i plików filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach, linki (konkretne adresy URL) oraz dane o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania w stosownym protokole.

Przez **działania wobec uczestników zdarzenia** rozumie się aktywności podejmowane wobec **ofiar** (osób poszkodowanych), **sprawców** i **świadków zdarzenia**. W szkole osobami poszkodowanymi będą w przeważającym odsetku przypadków dzieci (nieletni). Dlatego jako kolejną grupę pośrednich uczestników zdarzenia wyróżniamy ich rodziców / opiekunów prawnych.

Standardową procedurę reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego prezentuje poniższy rysunek:



Działania szkoły adresowane do instytucji / organizacji / służb zewnętrznych są niezbędne w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Pośród nich należy wyróżnić szczególnie współpracę z:

- 1) Policją i sądami rodzinnymi,
- 2) służbami społecznymi i placówkami specjalistycznymi oraz
- 3) dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć co najmniej poniższymi działaniami:

- 1) Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał. W trakcie takiej rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające ze statutu szkoły lub wprowadzonego kontraktu / umowy). W trakcie rozmowy sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości, w tym usunięcia skutków swoich działań (np. publikacji w portalu społecznościowym). Sprawca powinien również zostać objęty odpowiednią pomocą psychologiczną-pedagogiczną w celu zrozumienia konsekwencji swojego zachowania oraz zmiany postawy i dalszego postępowania. Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.
- 2) Należy zadbać o to, żeby osoba reprezentująca szkołę (pedagog, psycholog, wychowawca) ograniczyła się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować Rada Pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać dyrektor szkoły. Ważne jest zatem oddzielenie osoby pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.

Celem sankcji wobec sprawcy jest przede wszystkim zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Sankcje mają na celu także pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła jest w stanie skutecznie zareagować w tego rodzaju sytuacji. Podejmując decyzję o sankcjach, należy wziąć pod uwagę:

- ✓ **rozmiar i rangę szkody** – np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;
- ✓ **czas trwania prześladowania** – czy było to długotrwałe działanie, czy pojedynczy incydent;
- ✓ **świadomość popełnianego czynu** – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie; np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
- ✓ **motywację sprawcy** – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami lub opiekunami prawnymi – powinni oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją na temat dalszego postępowania ze sprawcą (np. na temat sankcji). Warto, aby rodzice współpracowali ze szkołą w zakresie rozwiązywania sytuacji kryzysowej, aby stali się jej sojusznikami, a nie przeciwnikami. Rodzice sprawcy powinni również zostać poinformowani, że rodzice ofiary mają prawo zgłosić sprawę na Policję.

Jeśli sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców / opiekunów prawnych) o przysługujących jej prawach (np. zgłoszenie popełnienia przestępstwa na Policję). Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.