

Załącznik nr
do Zarządzenia Nr/2020/2021
Dyrektora ZSO w Wydminach
z dnia

**PROCEDURY REAGOWANIA
W PRZYPADKU WYSTĄPIENIA
W SZKOLE ZAGROŻEŃ
BEZPIECZEŃSTWA CYFROWEGO**

SPIS TREŚCI

- I. Dostęp do treści szkodliwych, niepożądanych, nielegalnych.
- II. Cyberprzemoc.
- III. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły.
- IV. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu.
- V. Nawiązywanie niebezpiecznych kontaktów w Internecie – uwodzenie, zagrożenie pedofilią.
- VI. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich.
- VII. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam.
- VIII. Łamanie prawa autorskiego.
- IX. Zagrożenia bezpieczeństwa technicznego sieci komputerów i zasobów online.

I. Dostęp do treści szkodliwych, niepożądanych, nielegalnych

Podstawy prawne uruchomienia procedury

Kodeks Karny, Statut szkoły

Rodzaj zagrożenia objętego procedurą

Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych).

Telefon/kontakty alarmowe: Zgłaszanie nielegalnych treści: dyzurnet.pl, tel. 801 615 005, Policja 997

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Opis okoliczności, analiza, zabezpieczenie dowodów

Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.

W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję.

2. Identyfikacja sprawcy(-ów)

W identyfikacji sprawców kluczowe znaczenie odgrywać będą zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści (np. pornografii) oraz osoby, która udostępniły je dziecku. Często osobami tymi są rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.

3. Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły

W przypadku udostępniania (szerowania, dzielenia się) treści opisanych wcześniej jako szkodliwych/ niedozwolonych/nielegalnych i niebezpiecznych dla zdrowia przez ucznia należy przeprowadzić z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działań. Działania szkoły powinny koncentrować się

jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) należy złożyć zawiadomienie o zdarzeniu na Policję.

4. Aktywności wobec ofiar zdarzenia

Dzieci - ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji - otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie należy ustalić okoliczności uzyskania przez ofiarę dostępu do ww. treści.

Należy koniecznie powiadomić ich rodziców lub opiekunów prawnych o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.

W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuszanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego. Np. kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy.

5. Aktywności wobec świadków

W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie, czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych.

6. Współpraca z Policją i sądami rodzinnymi

W przypadku naruszenia prawa np. rozpowszechniania materiałów pornograficznych z udziałem nieletniego lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą należy – w porozumieniu z rodzicami dziecka - niezwłocznie powiadomić Policję .

7. Współpraca ze służbami i placówkami specjalistycznymi

Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymi dziecka.

II. Cyberprzemoc

Podstawy prawne uruchomienia procedury

Kodeks Karny, Statut szkoły

Rodzaj zagrożenia objętego procedurą:

Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanых mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, media społecznościowe, grupy dyskusyjne, SMS i MMS

Telefony alarmowe krajowe i lokalne

Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka 800 12 12 12

Telefon Zaufania dla Dzieci i Młodzieży - **116 111**, <https://11611.pl/>

Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100**,
<https://800100100.pl/>

Zgłaszanie nielegalnych treści: dyzurnet.pl, dyzurnet@dyzurnet.pl, 810 615 005.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele). W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. Podziękować za zaufanie i zgłoszenie tej sprawy.

- Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości i poszanowaniem jej uczuć. Potwierdzić, że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność. Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrekcji).
- Jeśli osobą zgłaszającą nie jest ofiara, na początku prosimy o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach przed byciem kapusiem, obawa o własne bezpieczeństwo).

W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/powtarzalność). Realizując procedurę należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami, etc. Trzeba

dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu nie dopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń, etc.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem.

3. Identyfikacja sprawcy(-ów)

Identyfikacja sprawcy(ów) często jest możliwa dzięki zebranym materiałom – wynikiem rozmów z osobą zgłaszającą, z ofiarą, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niego cyberprzemoc.

Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK)

4. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy).

Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m. in. w statucie, kontrakcie, regulaminie). Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej” przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp.

5. Aktywności wobec ofiar zdarzenia

W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i zaopiekowana przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu.

Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić, że dobrze zrobił ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić, że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo.

Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbanie o podstawowe zasady bezpieczeństwa on-line (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku etc).

Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać” nad jej bezpieczeństwem, np. zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy.

W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom.

W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy Policji.

6. Aktywności wobec świadków

Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć – obawy przed przypięciem łatki „donosiciela”, strachu przed staniem się kolejną ofiarą sprawcy itp.

7. Współpraca z Policją i sądami rodzinnymi

Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu i/lub regulaminu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia).

Kontakt z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły.

8. Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi

Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123).

III. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły

Podstawy prawne uruchomienia procedury: Kodeks Karny (art. 190a), RODO

Rodzaj zagrożenia:

Zagrożenie to polega na naruszeniu prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. Należy zwrócić uwagę, iż podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle polskiego prawa przestępstwem. Najczęstszymi formami wyłudzenia lub kradzieży danych jest przejście profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź fotomontaż), szantażu (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających dobry wizerunek ofiary), dokonania zakupów i innych transakcji finansowych (np. w sklepach internetowych na koszt ofiary) Często naruszenia prywatności łączy się z cyberprzemocą.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

Gdy sprawcą jest uczeń - kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem szkoły, wychowawcą lub Szkolnym Mentorem Bezpieczeństwa Cyfrowego. W przypadku, gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku dziecka dochodzi ze strony dorosłych osób trzecich, rodzice winni skontaktować się bezpośrednio z Policją i powiadomić o tym szkołę (zgodnie z Kodeksem Karnym ściganie następuje tu na wniosek pokrzywdzonego). Istotne dla ścigania sprawcy będzie uzyskanie dowodów, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania - w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms). Równolegle należy dokonać zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności - w działaniu tym ucznia powinna wspierać osoba dorosła. Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary, bądź w innych celach niezgodnych z prawem należy dążyć do wyjaśnienia tych działań i usunięcia ich skutków, także tych widocznych w Internecie. Likwidacja stron internetowych czy profili w portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody musi odbywać się

za zgodą Policji (o ile została powiadomiona). Szczególnej uwagi wymagają incydenty kradzieży tożsamości w celu posłużenia się nią np. podczas zakupu towarów *online* lub dokonania transakcji finansowych. W tym przypadku należy skontaktować się ze sklepem lub pożyczkodawcą i wyjaśnić charakter zdarzenia. O czynach niezgodnych z prawem należy powiadomić Policję.

3. Identyfikacja sprawcy(-ów)

W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę oraz na spełnianie przesłanki, iż sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej należy je zabezpieczyć i przekazać Policji. W przypadku, gdy trudno to ustalić, identyfikacji dokonać winna Policja.

W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, szkoła powinna dążyć do rozwiązania problemu w ramach działań wychowawczo –profilaktycznych uzgodnionych rodzicami.

4. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania profilaktyczne , zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał. Jednym z elementów takich działań powinno być zadośćuczynienie osobie poszkodowanej.

Celem takich działań winno być nie tylko nabycie odpowiedniej wiedzy przez ucznia na temat wagi poszanowania prywatności w codziennym życiu, ale trwała zmiana jego postawy na akceptującą szacunek dla wizerunku i prywatności. Działania takie szkoła winna podjąć niezależnie od powiadomienia Policji/ sądu rodzinnego.

Dyrekcja szkoły winna podjąć decyzje w sprawie powiadomienia o incydencie Policji, biorąc pod uwagę rodzaj czynu oraz wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu , opinie wychowawcy i pedagoga. Dobrym rozwiązaniem jest uzyskanie interpretacji prawnej radcy prawnego.

5. Aktywności wobec ofiar zdarzenia

Nieletnią ofiarę incydentów należy otoczyć – w porozumieniu z rodzicami/opiekunami prawnymi - opieką pedagogiczno-psychologiczną i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (np. usunięcie z Internetu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym). Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane tylko jej i rodzicom, szkoła winna zapewnić poufność działań, tak aby informacje narażające ofiarę na naruszenie wizerunku nie były rozpowszechniane.

6. Aktywności wobec świadków

Gdy kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę naruszania wizerunku ucznia – koleżanki lub kolegi oraz odpowiedzialność prawną.

7. Współpraca z Policją i sądami rodzinnymi

Gdy naruszenie prywatności, czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice ucznia winni o tym powiadomić Policję.

8. Współpraca ze służbami placówkami specjalistycznymi W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej.

IV. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu

Podstawy prawne uruchomienia procedury: Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe

Rodzaj zagrożenia objętego procedurą (opis):

Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgosłupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psychofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności, oraz osłabianiu relacji rodzinnych i społecznych.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

W przypadku nadmiernego korzystania z komputera lub podejrzenia infoholizmu konieczne jest podejmowanie działań pomocowych - głównie skierowanie ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej. Kluczowe są tutaj pozostałe objawy wskazane wyżej.

Nauczyciele w szkole także powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcającymi wolne chwile na kontakt *online* lub przychodzącymi do szkoły po nieprzespanej nocy. Rzadziej zgłoszeń można się spodziewać od rówieśników dziecka nadmiernie korzystającego z sieci.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Reakcja szkoły powinna polegać w pierwszych krokach na ustaleniu skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu - z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole.

3. Aktywności wobec ofiar zdarzenia

Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką pedagoga/psychologa szkolnego. Pierwszym jej etapem będzie rozmowa (rozmowy) ze specjalistą, która pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia w nałóg (np. sytuacja domowa, brak sukcesów edukacyjnych w szkole, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każde dziecko, u którego podejrzewa się nałóg korzystania z Internetu powinno zostać profesjonalnie zdiagnozowane za zgodą

rodziców/opiekunów prawnych przez psychologa szkolnego lub. Poradnię Psychologiczno-Pedagogiczną.

Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny - o jego sytuacji i specyfice uwarunkowań osobistych powinni zostać powiadomieni wszyscy uczący go i oceniający nauczyciele.

Z rodzicami/opiekunami prawnymi dziecka należy omówić wspólne rozwiązania trudnej sytuacji. Tylko synergiczne współdziałanie rodziców i szkoły może zagwarantować powodzenie podejmowanych działań wspierających dziecko.

4. Aktywności wobec świadków

Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o wsparcie dla dziecka dotkniętego problemem.

5. Współpraca ze służbami i placówkami specjalistycznymi

W przypadku zdiagnozowania przez psychologa uzależnienia od korzystania z zasobów Internetu dziecko powinno zostać skierowane we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej oferującej program terapeutyczny.

V. Nawiązywanie niebezpiecznych kontaktów w INTERNECIE – uwodzenie, zagrożenie pedofilią

Podstawy prawne uruchomienia procedury: Kodeks Karny, art. 200, 200a par 1 i 2, art. 286 par.1

Rodzaj zagrożenia objętego procedurą (opis):

Zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych).

Telefony alarmowe krajowe: Telefon Zaufania dla Dzieci i Młodzieży - **116 111**, <https://116111.pl/>

Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100**, <https://800100100.pl/>

Zgłaszanie nielegalnych treści: dyzurnet.pl, dyzurnet@dyzurnet.pl, **801 615 005**

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

Osobami najczęściej zgłaszającymi omawiany problem są rodzice/opiekunowie prawni dziecka lub osoby zajmujące się „poszukiwaniem pedofili”. W pierwszym przypadku informacja trafia najpierw do szkół, w drugim - na Policję. Zdarza się, że informacja uzyskiwana jest ze środowiska rówieśników ofiary.

Kluczowe znaczenie w działaniach szkoły ma czas reakcji - szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu *online*, przeradzającego się w zachowania w świecie rzeczywistym: uwiedzenie i wykorzystanie seksualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadkach niebezpiecznych kontaktów inicjowanych w Internecie może dochodzić do zagrożenia życia i zdrowia dziecka, szantażu i przymusu realizacji czynności seksualnych.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Należy zidentyfikować i zabezpieczyć w szkole, w formie elektronicznej dowody działania dorosłego sprawcy uwiedzenia (zapisy rozmów w komunikatorach, na portalach społecznościowych; zrzuty ekranowe, zdjęcia, wiadomości e-mail).

Jednocześnie – bezzwłocznie - należy dokonać zawiadomienia na Policji o wystąpieniu zdarzenia.

3. Identyfikacja sprawcy(-ów)

Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje i możliwości szkoły w większości przypadków uwodzenia przez Internet.

4. Aktywności wobec sprawców ze szkoły/ spoza szkoły

Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ew. świadkami.

5. Aktywności wobec ofiar zdarzenia

W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpieczne zachowania, a także werbunku do grupy terrorystycznej należy przed wszystkim zapewnić ofierze opiekę psychologiczną i poczucie bezpieczeństwa. Podobne wsparcie winno być udzielone w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych), bowiem zachowania te mogą być inicjowane i wzmacniane poprzez kontakty w Internecie. O możliwym związku takich zachowań dzieci z inspiracją w Internecie należy powiadomić rodziców.

Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-pedagogiczną we współpracy szkoły z rodzicami/opiekunami. W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpieczne zachowania, a także werbunku do grupy terrorystycznej należy przed wszystkim zapewnić ofierze opiekę psychologiczną i poczucie bezpieczeństwa. Podobne wsparcie winno być udzielone w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych), bowiem zachowania te mogą być inicjowane i wzmacniane poprzez kontakty w Internecie. O możliwym związku takich zachowań dzieci z inspiracją w Internecie należy powiadomić rodziców.

Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-pedagogiczną we współpracy szkoły z rodzicami/opiekunami prawnymi. W trakcie rozmowy z dzieckiem prowadzonej w warunkach komfortu psychicznego przez wychowawcę/ pedagoga/psychologa/osobę ze szkoły, do której dziecko ma szczególne zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je Policji. Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany, a dziecko odzyskało poczucie bezpieczeństwa. Towarzyszyć temu powinna analiza sytuacji domowej (rodzinnej) dziecka, w której tkwić może źródło poszukiwania kontaktów w Internecie. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej.

Wszelkie działania szkoły wobec dziecka winny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.

6. Aktywności wobec świadków

Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy docenić jego prospołeczną postawę.

7. Współpraca z Policją i sądami rodzinnymi

W przypadkach naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie Policji lub sądu rodzinnego.

8. Współpraca ze służbami społecznymi i placówkami specjalistycznymi

W przypadkach uwiedzenia nieletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

VI. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich – procedura reagowania

Podstawy prawne uruchomienia procedury: Kodeks Karny (art. 191a i 202)

Rodzaj zagrożenia objętego procedurą:

Seksting to przesyłanie drogą elektroniczną w formie wiadomości MMS lub publikowanie np. na portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

Zgłoszeń przypadków sekstingu dokonują głównie rodzice lub opiekunowie prawni dziecka - ofiary. Czasami informacja dociera do szkoły bezpośrednio od ucznia lub z grona bliskich znajomych dziecka. W rzadkich wypadkach nauczyciele i inni pracownicy szkoły sami identyfikują takie zdarzenia w sieci. Delikatny charakter sprawy, a także odpowiedzialność karna sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji. Niekiedy zgłoszenia dokonują ofiary lub osoby je znające.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania:

Rodzaj 1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej.

Rodzaj 2. Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie.

Rodzaj 3. Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy.

3. Identyfikacja sprawcy (-ów)

Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów - przesyłanych zdjęć, czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a). Jako, że seksting jest karalny, skrupulatność i wiarygodność dokumentacji ma duże znaczenie. Należy przy tym przestrzegać zasad dyskrecji, szczególnie w środowisku rówieśniczym ofiary.

4. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie zostaną im przedstawione dowody ich aktywności. Niezależnie od zakresu negatywnych

zachowań i działań wszyscy sprawcy powinni otrzymać wsparcie pedagogiczne i psychologiczne. Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły.

Rodzaj 1. Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno-pedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne.

Rodzaj 2. Niektóre tego typu materiały mogą zostać uznane za pornograficzne, w takim wypadku na dyrektorze placówki ciąży obowiązek zgłoszenia incydentu na Policję. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (art. 202 Kodeksu Karnego), dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na Policję i/lub do sądu rodzinnego. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi.

Rodzaj 3. W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc.

5. Aktywności wobec ofiar zdarzenia

Pierwszą reakcją szkoły i rodziców, obok dokumentacji dowodów, winno być otoczenie opieką psychologiczno - pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych, w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym. Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana w warunkach komfortu psychicznego dla dziecka – ofiary sekstingu, z szacunkiem dla niego.

6. Aktywności wobec świadków

Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym – np. poprzez media społecznościowe czy MMS do uczniów tej samej szkoły lub klasy lub publikację w portalu społecznościowym, należy podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary.

7. Współpraca z Policją i sądami rodzinnymi

W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) kierownictwo szkoły jest zobowiązane do powiadomienia o tym zdarzeniu Policji lub sądu rodzinnego.

8. Współpraca ze służbami społecznymi i placówkami specjalistycznymi

Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog/pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

VII. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam

Podstawy prawne uruchomienia procedury: Ustawa z 14 grudnia 2016 r. – prawo oświatowe

Rodzaj zagrożenia objętego procedurą (opis):

Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w Internecie, bezkrytyczne uznawanie za prawdę też publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach. Taka postawa dzieci prowadzić może do zagrożeń życia i zdrowia (np. stosowania wyniszczającej diety, samookaleczeń), skutkować rozczarowaniami i porażkami życiowymi (w efekcie korzystania z fałszywych informacji), utrudniać lub uniemożliwiać osiągnięcie dobrych wyników w edukacji (korzystanie z upraszczających i zawężających temat „ściągi” i „bryków”), a także utrwalenia się u ucznia ambiwalentnych postaw moralnych.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

Uczniowie nie umiejący odróżniać prawdy od fałszu informacji publikowanych w Internecie winni być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów. Często taka postawa ujawnia się podczas przygotowania prac domowych i jest stosunkowo łatwa do zidentyfikowania przez oceniającego je nauczyciela.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych, każdorazowo winno być zauważone przez nauczyciela, przeanalizowane i sprostowane.

3. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Wystarczającą reakcją jest opublikowanie sprostowania nieprawdziwych informacji i - w miarę możliwości – rozpowszechnienie ich w Internecie, w portalach o zbliżonej tematyce.

4. Aktywności wobec ofiar zdarzenia i świadków

Szkoła powinna prowadzić działania profilaktyczne - edukację medialną (informacyjną), np. w trakcie zajęć nieinformatycznych (np. historii, języka polskiego,) przez wszystkie lata nauki ucznia w szkole lub lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji informatycznych. Edukacja medialna może być prowadzona również na zajęciach pozalekcyjnych.

VIII. Łamanie prawa autorskiego

Podstawy prawne uruchomienia procedury: Kodeks Karny

Rodzaj zagrożenia objętego procedurą (opis):

Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. *copyright trolling*).

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

W zależności od okoliczności oraz zaawansowania problemu, w którym doszło do ujawnienia sprawy, zdarzenie może zostać zgłoszone w sposób nieformalny (ustnie, telefonicznie, pocztą elektroniczną, na zamkniętym lub publicznym forum internetowym, na piśmie w postaci wezwania podpisanego przez domniemanego uprawnionego lub jego pełnomocnika) lub formalny (w postaci doręczenia odpisu pozwu lub innego pisma urzędowego np. wezwania z Policji lub prokuratury). Przyjęcie zgłoszenia dokonane w sposób nieformalny powinno zaowocować powstaniem bardziej formalnego śladu, w postaci np. notatki służbowej, zakomunikowania przełożonemu itd. w zależności od wagi sprawy.

Na wstępnym etapie należy przede wszystkim unikać wdawania się w argumentację, pochopnego przyznawania roszczeń lub spełniania żądań, piętnowania domniemych sprawców itd. bez ustalenia wszystkich okoliczności sprawy, w razie potrzeby w konsultacji z prawnikiem. Prawo autorskie jest regulacją skomplikowaną, a sądy decydują w sprawach o naruszenie praw autorskich często w bardzo odmienny sposób, dlatego w większości przypadków uzyskanie fachowej pomocy prawnej jest wysoce wskazane.

Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych przez uczniów szkoła nie może występować w roli sędziego - dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła powinna na każdym etapie skupić się na swojej roli edukacyjno-wychowawczej poprzez organizację lekcji na temat praw autorskich, zwracając przy tym uwagę, że powinny one rzeczowo i konkretnie informować, jakie czyny są dozwolone, a jakie zabronione prawem.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Należy zebrać informacje przede wszystkim o:

- osobie dokonującej zgłoszenia, czy jest do tego uprawniona (czy faktycznie przysługują jej prawa autorskie do danego utworu, czy posiada ważne pełnomocnictwo itd.)

- wykorzystanym utworze (czy faktycznie jest chroniony przez prawo autorskie, w jakim zakresie został wykorzystany i czy zakres ten mieści się w zakresie posiadanych licencji lub dozwolonego użytku)

Należy zweryfikować wszystkie informacje podawane przez zgłaszającego lub inne osoby. Jeżeli np. powołuje się on na toczące się w sprawie postępowanie karne, należy podjąć kontakt z odpowiednimi służbami celem ustalenia, czy takie postępowanie faktycznie się toczy, czego dokładnie dotyczy i jaka jest w nim rola poszczególnych osób. Taki kontakt najlepiej przeprowadzać za pośrednictwem adwokata lub radcy prawnego.

Należy sprawdzić, czy okoliczności podane w zgłoszeniu faktycznie miały miejsce i czy powoływane tam dowody nie zostały zmanipulowane.

3. Identyfikacja sprawcy (-ów)

Dochodzenie naruszeń praw autorskich realizowane jest, co do zasady, z inicjatywy samego uprawnionego przed sądami, a w przypadku naruszeń stanowiących przestępstwo dodatkowo zaangażowane mogą być Policja i prokuratura. Szkoła nie powinna wyręczać tych organów w ich rolach ani też wkraczać w ich kompetencje. Szkoła powinna skupić się na swojej roli wychowawczej i edukacyjnej, wykorzystując otrzymanie zgłoszenia rzekomego naruszenia do przekazania zaangażowanym osobom (a być może i wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat tego, jak faktycznie prawo reguluje tę konkretną sytuację.

4. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Zasadniczo o dochodzeniu roszczeń wobec sprawcy decyduje sam uprawniony (tzn. autor lub inna osoba, której przysługują prawa autorskie). Szkoła powinna natomiast podjąć działania o charakterze edukacyjno-wychowawczym, polegające na obszernym wyjaśnieniu, na czym polegało naruszenie oraz przekazaniu wiedzy, jak do naruszeń nie dopuścić w przyszłości.

5. Aktywności wobec ofiar zdarzenia

Jeżeli osobą, której prawa autorskie naruszono, jest uczeń należy rozważyć możliwość wystąpienia w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub inne kompromisowe zakończenie powstałego sporu. Np. w przypadku, gdy ofiarą jest osoba ze szkoły, autorytet szkoły może pomóc w skłonieniu sprawcy do zaprzestania naruszeń. Z kolei w przypadku, gdy ofiarą jest osoba spoza szkoły, szkoła może pomóc sprawcy w doprowadzeniu do zaniechania naruszeń i naprawienia ich skutków bez niepotrzebnej eskalacji sporu.

6. Aktywności wobec świadków

Stosownie do okoliczności, należy samodzielnie zebrać ich zeznania lub zadbać, aby zostały one zebrane przez uprawnione organy.

7. Współpraca z Policją i sądami rodzinnymi

Ponieważ, co do zasady dochodzenie roszczeń z tytułu naruszeń zależy od decyzji uprawnionego, to uprawniony musi samodzielnie zdecydować czy zawiadamić Policję lub składać powództwo. Stosownie do wskazanej wyżej roli mediatora, szkoła powinna zaangażować się natomiast przede wszystkim w ułatwianie zakończenia sporu bez takiej eskalacji.

8. Współpraca ze służbami społecznymi i placówkami specjalistycznymi

Warto rozważyć zorganizowanie szkoleń lub warsztatów z zakresu prawa autorskiego w intencji dla wszystkich zainteresowanych osób w szkole.

9. Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi

Zależnie od okoliczności, może być wskazana asysta sprawcy bądź ofiary przy kontakcie z tego typu podmiotami, np. w celu zablokowania dostępu do utworu umieszczonego w Internecie z naruszeniem prawa. Ponadto, stosownie do przepisów prawa, tego typu usługodawcy mogą zostać zobowiązani do przekazania szczegółów dotyczących naruszenia dokonanego z użyciem ich usług (do czego jednak może być potrzebne postanowienie sądowe).

IX. Zagrożenia bezpieczeństwa technicznego sieci komputerów i zasobów online

Podstawy prawne uruchomienia procedury: Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe, Statut szkoły

Rodzaj zagrożenia objętego procedurą (opis):

Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spectrum problemów: (1) ataki przez wirusy, robaki i trojany, (2) ataki na zasoby sieciowe (hakerstwo, spyware, crimeware, exploit, ataki słownikowe i back door, skanowanie portów, phishing, pharming, sniffing, spoofing, ataki Denial of service (DoS, DDoS rootkit) i ataki socjotechniczne. Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników np. używanie łatwych do odgadnięcia haseł, pozostawianie komputerów włączonych bez opieki, czy brak zabezpieczeń na wypadek braku energii elektrycznej.

Sposób postępowania w przypadku wystąpienia zagrożenia

1. Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową szkoły oraz dyrekcji. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.

2. Opis okoliczności, analiza, zabezpieczenie dowodów

Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego powinien zostać zawarty w dokumencie „**polityka bezpieczeństwa cyfrowego**” danej szkoły stanowiącej element **Szkolnego Planu Zapewnienia Bezpieczeństwa Cyfrowego**. W części przypadków szkoła poradzi sobie we własnym zakresie, w niektórych konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.

3. Identyfikacja sprawcy(-ów)

Identyfikację sprawców ataku należy pozostawić specjalistom – informatykom. W sytuacji, gdy incydent spowodował szkole straty materialne lub wiązał się z utratą danych należy powiadomić Policję, aby podjęła działania na rzecz zidentyfikowania sprawcy.

4. Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Jeśli sprawcami incydentu są uczniowie danej szkoły, o zaistniałej sytuacji należy powiadomić ich rodziców, zaś wobec nich podjąć działania wychowawcze. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły), należy taki przypadek zgłosić na Policję.

5. Aktywności wobec świadków

O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte sprawne działania, tak przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci.

6. Współpraca z Policją i sądami rodzinnymi

W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji.

7. Współpraca ze służbami społecznymi i placówkami specjalistycznymi

W przypadkach zaawansowanych awarii (np. wywołanych przez trojany) lub strat (np. utrata danych z e-dziennika) konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.