PORADNIK DLA SZKÓŁ OGÓLNOPOLSKIEJ SIECI EDUKACYJNEJ

BEZPIECZEŃSTWO ONLINE W SZKOŁACH OGÓLNOPOLSKIEJ SIECI EDUKACYJNEJ

Warszawa 2019

OGÓLNOPOLSKA SIEĆ EDUKACYJNA
NASK
Ministerstwo Cyfryzacji

SPIS ZAGADNIEŃ

Redakcja
Marek Sowala, dr Agnieszka Wrońska

Autorzy
Anna Borkowska, Oliwia Chojnacka, Anna Kwaśnik, Katarzyna Kujawa, Julia Piechna, Marek Sowala, Marta Witkowska, Agnieszka Wrońska

Korekta
Katarzyna Gańko

Projekt okładki, opracowanie graficzne, skład
Agnieszka Staręga

Warszawa 2019

ISBN: 978-83-65448-18-7

NASK Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

WSTĘP

Zgodnie z zapisami Ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (OSE) w ciągu najbliższych lat do wszystkich placówek oświatowych w Polsce doprowadzony zostanie światłowodowy symetryczny internet o przepływności 100 Mb/s. **Zarówno cele programu OSE, jak i zadania jego operatora zdefiniowane w powyższej Ustawie kładą duży nacisk na zagadnienie cyberbezpieczeństwa. Do zadań operatora sieci OSE należy m.in. świadczenie szkole usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz promowanie zasad bezpiecznego korzystania z technologii cyfrowych.** Jednocześnie art. 27 Ustawy Prawo oświatowe z dnia 14 grudnia 2016 r. nakłada na szkoły i placówki zapewniające uczniom dostęp do internetu obowiązek podejmowania działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. W szczególności szkoły obowiązane są zainstalować i aktualizować oprogramowanie zabezpieczające.

Korzystanie przez młodych użytkowników z sieci oraz coraz większa obecność internetu w edukacji i w procesach komunikowania w szkole i poza nią powinny iść w parze zarówno z edukacją dotyczącą bezpiecznego korzystania z sieci, jak i tworzeniem i wdrażaniem zasad profilaktyki oraz procedur reagowania na zagrożenia cyberprzestrzeni. Najważniejsze znaczenie dla zapewnienia podstaw bezpieczeństwa cyfrowego w szkole mają działania edukacyjne i profilaktyczne. Ważnym jest posiadanie przez szkołę opracowanych modeli reagowania w sytuacjach kryzysowych.

W poradniku zaprezentowane zostały informacje o wybranych zagrożeniach oraz propozycje procedur postępowania w przypadku ich wystąpienia. Zachęcamy szkoły do włączenia ich do szkolnej polityki bezpieczeństwa cyfrowego. W materiale poruszono następujące zagadnienia: cyberprzemoc, nadużywanie internetu i gier, szkodliwe treści, sexting i treści tworzone przez młodych użytkowników, nielegalne treści, naruszenia prywatności, niebezpieczne kontakty, naruszenia prawa autorskiego, szkodliwe oprogramowanie, oszustwa komputerowe, ataki kierowane na sieci szkolne w celu zablokowania ich działania, jak również nieuprawnionego dostępu (lub zmiany) do informacji.

Układ treści kolejnych rozdziałów obejmuje: krótki opis zagrożenia, odwołanie do wyników badań i przepisów prawa oraz porady.

Dodatkowo piktogramy ułatwiają określenie, czy dane zagrożenie podlega ochronie w ramach usług bezpieczeństwa OSE, a także wskazują, które zagadnienia wymagają podjęcia działań edukacyjnych czy interwencyjnych.

Wyjaśniaj, edukuj, ostrzegaj, korzystaj z porad ekspertów

Zgłoś do Dyżurnetu (dyzurnet.pl)

Usługi Bezpieczeństwa OSE

Planowane Usługi Bezpieczeństwa OSE

Gdzie uzyskać pomoc?

- Centrum Kontaktu OSE – informacja o usługach bezpieczeństwa OSE: **+48 22 182 55 55**
- Dyżurnet.pl **www.dyzurnet.pl** – anonimowe zgłaszanie nielegalnych bądź szkodliwych treści w internecie
- **800 100 100** – Telefon dla rodziców i nauczycieli
- **116 111** – Telefon zaufania dla dzieci i młodzieży
- **Administratorzy serwisów internetowych**

CYBERPRZEMOC

Anna Borkowska

Opis zjawiska

Cyberprzemoc to agresywne zachowania lub działania realizowane za pomocą środków elektronicznych i technologii informacyjno-komunikacyjnych, głównie internetu i telefonii komórkowej, podejmowane z intencją wyrządzenia krzywdy drugiej osobie.

Najczęstsze formy cyberprzemocy to: wyzywanie, wyśmiewanie, straszenie, zamieszczanie w sieci lub rozsyłanie upokarzających zdjęć i filmów, podszywanie się pod kogoś, nękanie uporczywymi telefonami lub SMS-ami, wykluczanie z grona znajomych w internecie itp.

Zjawisko cyberprzemocy najczęściej odnosi się do przemocy rówieśniczej i jest bardzo często przedłużeniem konfliktów przeniesionych ze środowiska offline – z klasy lub szkoły.

Długofalowe konsekwencje internetowego prześladowania dotykają zarówno ofiary cyberprzemocy, jak i jej sprawców. U dzieci doświadczających przemocy częściej występują problemy psychosomatyczne, depresja, lęk, obniżone poczucie własnej wartości. W skrajnych przypadkach mogą pojawić się myśli lub próby samobójcze. W przypadku sprawców obserwuje się utrwalanie agresywnych zachowań i obniżenie poczucia odpowiedzialności za własne działania. Może też nasilać się u nich skłonność do zachowań aspołecznych w przyszłości.

Ochrona przed zagrożeniem zostanie zapewniona w ramach planowanych Usług Bezpieczeństwa OSE.

Skala zjawiska

- 76,5% nastolatków w wieku 13–17 lat zetknęło się z przejawami agresji elektronicznej, a prawie połowa (48,8%) doświadczyła jej osobiście (Bochenek, Lange, 2019).
- Około 7% polskich uczniów doświadcza najpoważniejszych ataków internetowej agresji (z ang. cyberbullyingu) – regularnego, systematycznego i długotrwałego nękania w sieci przez rówieśników (Pyżalski i in., 2019).

Przepisy prawa

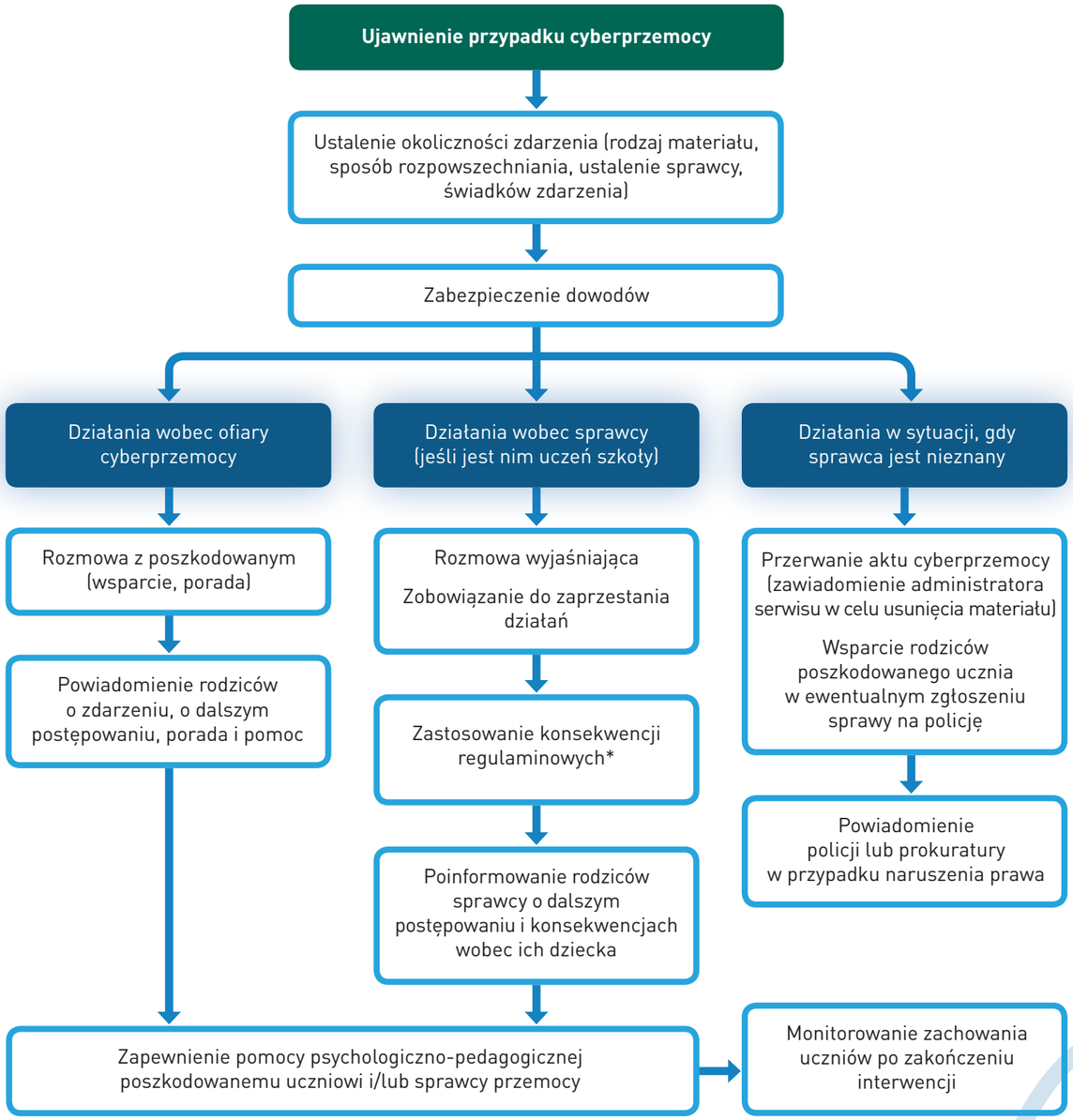
Niektóre akty cyberprzemocy stanowiące naruszenie prawa mogą być ścigane na wniosek pokrzywdzonego (w przypadku dzieci do 18 r.ż. na wniosek rodziców lub opiekunów prawnych). Są to: groźba karalna (art. 190 Kodeksu karnego – dalej k.k.), zmuszanie groźbą do określonego działania (art. 191 k.k.), uporczywe nękanie – stalking (art. 190a k.k.), naruszenie wizerunku (art. 23 i 24 Kodeksu cywilnego), zniesławienie/znieważenie (art. 216 i 212 k.k.), włamanie (art. 267 i 268a k.k.).

Czyny karalne ścigane z urzędu powinny być niezwłocznie zgłoszone na policję lub do prokuratury. Dotyczy to sytuacji takich jak rozpowszechnianie zdjęć lub filmów z udziałem osoby nieletniej mających cechy pornograficzne czy publikowanie materiałów prezentujących seksualne wykorzystywanie nieletnich (art. 202 k.k.).

Porady

- Reaguj w przypadku każdego aktu przemocy. Nie czekaj, aż niepokojące zachowanie samo się skończy.
- Pamiętaj, że głównym celem interwencji jest przerwanie procesu przemocy, otoczenie opieką ofiar agresji i powstrzymanie sprawców.
- Współpracuj z rodzicami, zarówno ofiar, jak i sprawców cyberprzemocy.
- W przypadku naruszenia prawa zawiadom policję lub prokuraturę.
- Podejmuj systematyczne działania wychowawcze i profilaktyczne zanim w twojej placówce pojawi się przemoc – buduj pozytywny klimat szkoły i dobre relacje w społeczności szkolnej.

Schemat: Procedura reagowania w przypadku ujawnienia cyberprzemocy w szkole



Sporządzenie dokumentacji:

- Notatka służbowa zawierająca opis okoliczności przebiegu zdarzenia oraz podjętych czynności
- Zabezpieczone dowody (wydruki, opis itp.)

* W przypadku, gdy uczeń – sprawca cyberprzemocy przejawia zachowania świadczące o demoralizacji bądź popełnił czyn karalny, szkoła zobowiązana jest do podjęcia współpracy z policją lub sądem rodzinnym i nieletnich.

NADUŻYWANIE NOWOCZESNYCH TECHNOLOGII I FOMO

Marta Witkowska

Opis zjawiska

FOMO (ang. fear of missing out) to lęk przed odłączeniem, wypadnięciem z obiegu. FOMO, choć pierwotnie niewiązane z nowymi technologiami, łączone jest obecnie z intensywnym rozwojem mediów społecznościowych. Skutkuje przymusem nieustannego bycia online.

Nadużywanie nowoczesnych technologii (telefonu, internetu i gier komputerowych) to problem coraz powszechniej dotykający dzieci i młodzież. Wszystkie te nałogowe czynności charakteryzuje:

- silnie odczuwany wewnętrzny przymus wykonywania określonych czynności, np. grania w grę lub przeglądania profili w mediach społecznościowych;
- uporczywe ich powtarzanie, nawet jeśli powodują szkody, np. prowadzą do wyczerpania, problemów zdrowotnych i zaniedbywania innych sfer funkcjonowania, takich jak nauka, kontakty z rówieśnikami czy pasje i zainteresowania; nieprzyjemne uczucia i stany (nuda, niepokój, smutek, rozdrażnienie, złość itp.) podczas prób ograniczania lub zakończenia czynności nałogowych. Próby te kończą się niepowodzeniem, ulgę przynosi powrót do używania nowoczesnych technologii.

Zarówno FOMO, jak i nadużywanie internetu i gier mogą mieć poważne konsekwencje dla prawidłowego rozwoju uczniów.

- Szkoła: pogorszenie wyników w nauce, częste spóźnienia, liczne nieobecności, wagary, brak promocji do następnej klasy, a nawet niewywiązywanie się z obowiązku szkolnego i załamanie ścieżki edukacyjnej.
- Zdrowie fizyczne: bóle głowy, oczu, kręgosłupa, nadgarstka i inne.
- Zdrowie psychiczne: znaczne obniżenie samooceny i uzależnienie jej od czynności i kontaktów online, pogłębiający się stan izolacji i wyobcowania, problemy (lub zanik) relacji interpersonalnych, stany depresyjne, depresja.
- Podejmowanie ryzykownych zachowań w sieci: upublicznianie zbyt wielu informacji o sobie, częstsze poszukiwanie pornografii online i angażowanie się w hazard online (Węgrzecka-Giluń, 2013).

Ochrona przed zagrożeniem zostanie zapewniona w ramach planowanych Usług Bezpieczeństwa OSE.

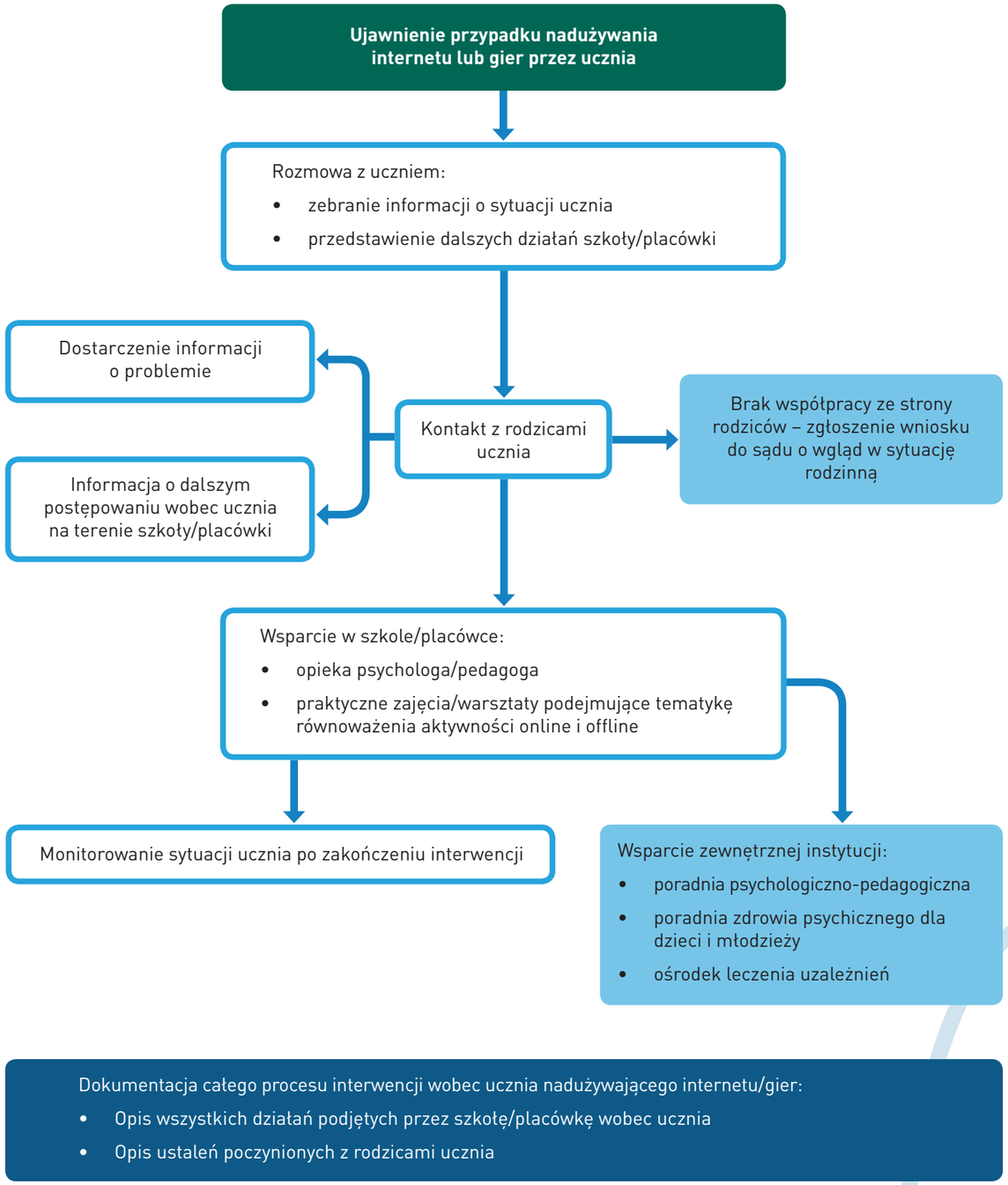
Skala zjawiska

- W najmłodszej grupie polskich internautów (od 15 do 24 roku życia) aż 21% młodych ludzi doświadcza wysokiego poziomu FOMO (Jupowicz-Ginalska i in., 2018).
- Aż 56% nastolatków uważa, że powinno mniej korzystać z telefonu, a 36% podejmowało nieudane próby ograniczania się (Bochenek, Lange, 2019).
- Około 12% nastolatków, a więc co ósmy badany, może być zagrożony uzależnieniem – czyli nadużywać internetu (Makaruk i in., 2012).
- Około 1% nastolatków w Polsce może przejawiać symptomy uzależnienia od internetu (Pyżalski i in., 2019).

Porady

- Wejdź w ścisłą współpracę z rodzicami ucznia nadużywającego internetu lub gier – wiele szkodliwych zachowań uczeń podejmuje poza szkołą.
- Rozmawiaj z uczniami o konieczności zachowania równowagi pomiędzy aktywnościami online i offline.
- Rozważ wprowadzenie do szkoły/placówki zajęć dla uczniów i ich rodziców, podejmujących tematykę nadmiernego i szkodliwego korzystania z sieci.

Schemat: Procedura reagowania w sytuacji nadużywania nowoczesnych technologii



SZKODLIWE TREŚCI W INTERNECIE

Julia Piechna

Opis zjawiska

Treści szkodliwe to takie, które mogą wywołać negatywne emocje u odbiorcy, a także destrukcyjnie wpływać na rozwój i psychikę dzieci i młodzieży. Promują niebezpieczne zachowania i dlatego są nieodpowiednie dla młodego odbiorcy. Dzieci mogą trafiać na te treści celowo lub przypadkiem, np. poprzez mylne wyniki wyszukiwania, spam czy reklamę.

Do szkodliwych treści zalicza się m.in.: treści obrazujące przemoc, obrażenia fizyczne bądź śmierć; treści nawołujące do samookaleczeń, samobójstw lub zachowań szkodliwych dla zdrowia; treści dyskryminacyjne, zawierające postawy wrogości a nawet nienawiści; treści pornograficzne; fałszywe wiadomości (tzw. fake news), często o charakterze sensacyjnym, publikowane w mass mediach w celu zmanipulowania i wprowadzenia odbiorcy w błąd oraz patostreamy, czyli relacje na żywo w sieci, prezentujące zachowania określane i postrzegane jako patologiczne (np. libacje alkoholowe, zażywanie narkotyków, bójki).

Do najważniejszych konsekwencji należą: obniżenie poczucia bezpieczeństwa, wypaczony obraz rzeczywistości, pogorszenie nastroju, demoralizacja i wspieranie zachowań sprzecznych z normami społecznymi, znieczulenie na losy ofiar przemocy oraz ryzykowne zachowania.

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

Skala zjawiska

- 42,6% dzieci w wieku 11–17 lat miało styczność z krwawymi i brutalnymi obrazami w internecie (Pyżalski i in., 2019).
- 43% dzieci w wieku 11–18 lat miało kontakt z pornografią w internecie (Makaruk i in., 2017).
- 23,4% nastolatków ogląda patostreamy w internecie (Bochenek, Lange, 2019).

Przepisy prawa

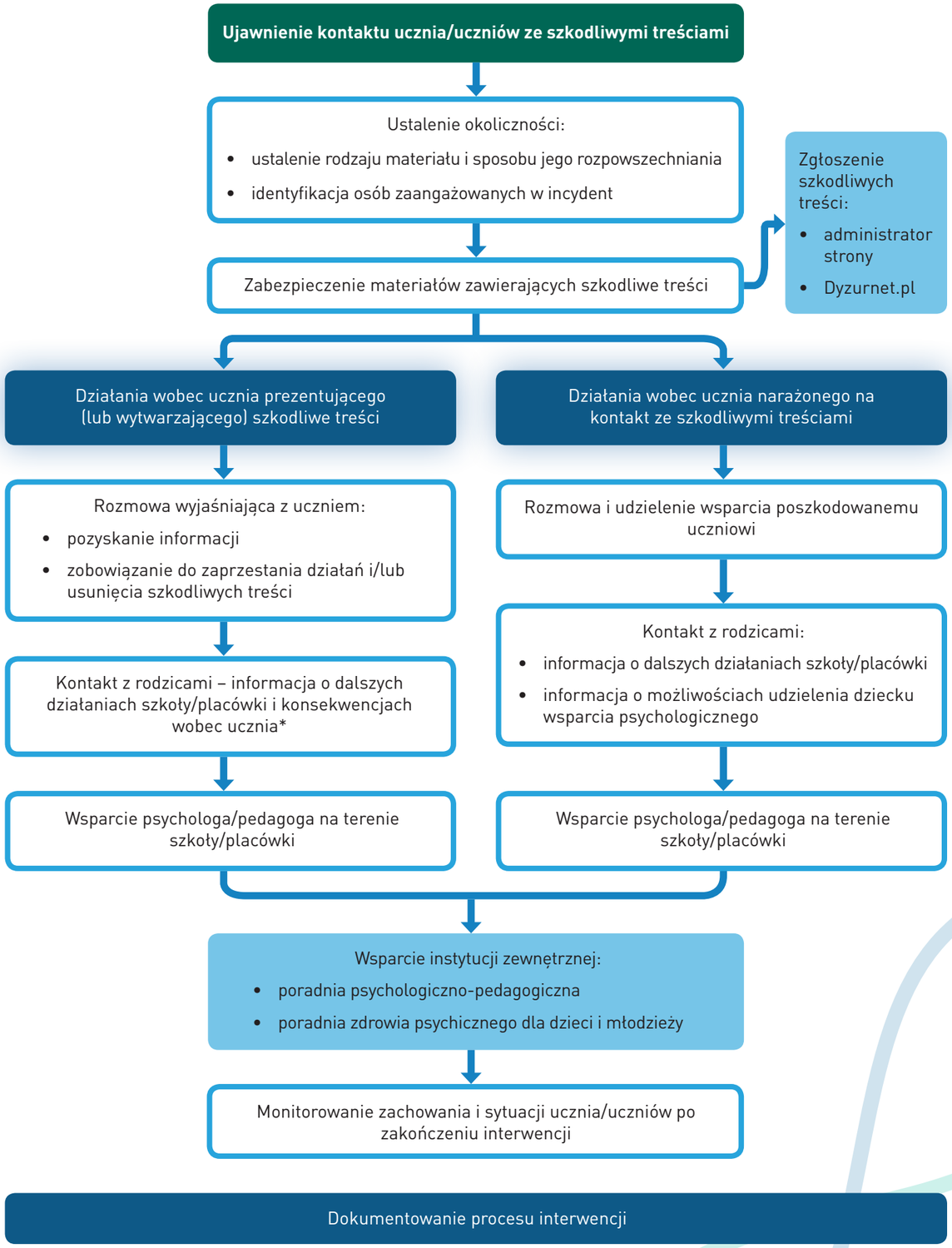
Szkodliwe treści internetowe nie zawsze naruszają prawo. Z tego powodu bardzo ważna jest rola moderatorów czy właścicieli domeny podczas publikacji treści oraz usuwania tych, które są szkodliwe lub łamią regulamin serwisu. Istnieje także kategoria treści szkodliych, naruszających przepisy polskiego prawa – zostały one przedstawione w rozdziale „Nielegalne treści" (s. 12).

Porady

Jak chronić dzieci przed szkodliwymi treściami w internecie?

- W szkole podłączonej do sieci OSE uruchom darmową usługę ochrony użytkownika OSE.
- W szkole niepodłączonej do sieci OSE zadbaj o odpowiednie oprogramowanie zabezpieczające.
- Wprowadź w szkole procedury reagowania na incydenty związane z kontaktem ucznia ze szkodliwymi treściami.
- Rozmawiaj z uczniami o ich aktywnościach online. Interesuj się, zapewniaj, że w trudnych sytuacjach mogą liczyć na wsparcie.
- Ucz dzieci krytycznego podejścia do treści dostępnych online.

Schemat: Procedura reagowania na incydenty związane z kontaktem ucznia ze szkodliwymi treściami



* W przypadku, gdy uczeń wytwarzający lub prezentujący szkodliwe treści przejawia zachowania świadczące o demoralizacji, szkoła zobowiązana jest do podjęcia współpracy z policją lub sądem rodzinnym i nieletnich.

SEXTING

Anna Kwaśnik

Opis zjawiska

Sexting to przesyłanie za pomocą nowoczesnych technologii swoich zdjęć, filmów bądź wiadomości o seksualnym charakterze. Termin powstał z połączenia słów „sex" i „texting", a początkowo odnosił się jedynie do wysyłania wiadomości SMS. Obecnie dotyczy również przesyłania treści za pomocą aplikacji, komunikatorów, serwisów społecznościowych, a także udostępniania pokazów erotycznych online.

Popularność zjawiska sextingu, zwłaszcza wśród osób młodych, wpływa na coraz większą liczbę treści definiowanych przez specjalistów jako self generated content, czyli nagich czy półnagich obrazów lub filmów wytworzonych przez osobę młodą (poniżej 18 roku życia), która świadomie angażuje się w erotyczną lub seksualną aktywność.

Motywy wysyłania takich treści mogą być bardzo różne. Do najczęstszych należą: przesyłanie takich treści do osoby, z którą nastolatek jest w związku; wysyłanie materiałów do osoby poznanej online; „to normalne, wszyscy tak robią"; nuda, zabawa; wyzwania internetowe, czyli tzw. challange.

Intymne treści mogą trafić do osób o skłonnościach pedofilskich, które wykorzystują je w różny sposób. W niektórych przypadkach dążą nawet do spotkania (zwłaszcza w przypadku młodszych dzieci). Dodatkowo rozpowszechnienie takich materiałów może nieść za sobą wiele niebezpieczeństw w życiu codziennym, w niektórych przypadkach prowadzi do zachowań autodestrukcyjnych, a nawet prób samobójczych. Inną konsekwencją rozsyłania intymnych materiałów jest rosnąca liczba csam (z ang. child sexual abuse materials), czyli treści przedstawiających seksualne wykorzystywanie dziecka. Przede wszystkim nie zapominajmy, że materiały udostępniane i rozpowszechniane w internecie mogą stamtąd nigdy nie zginąć.

Ochrona przed zagrożeniem zostanie zapewniona w ramach planowanych Usług Bezpieczeństwa OSE.

Skala zjawiska

- 42% młodych ludzi w wieku 15–18 lat otrzymało kiedyś od innej osoby jej nagie zdęcie lub film, a 13% wysłało swoje nagie zdjęcie lub film (Kamieniecki i in, 2017).
- W ciągu roku 3,8% 11–17-latków umieściło wiadomości związane z seksem z udziałem swoim lub innej osoby (Pyżalski i in., 2019).
- 25% badanych przyznaje, że wysyła materiały związane z seksem przynajmniej raz w miesiącu (Pyżalski i in., 2019).
- 57,1% nastolatków deklaruje zamieszczanie w sieci treści związanych z seksem w taki sposób, żeby inni mogli je zobaczyć (Pyżalski i in., 2019).
- 45,7% badanych przyznaje, że kilkukrotnie prosiło w sieci kogoś o przesłanie informacji związanych z seksem (Pyżalski i in., 2019).

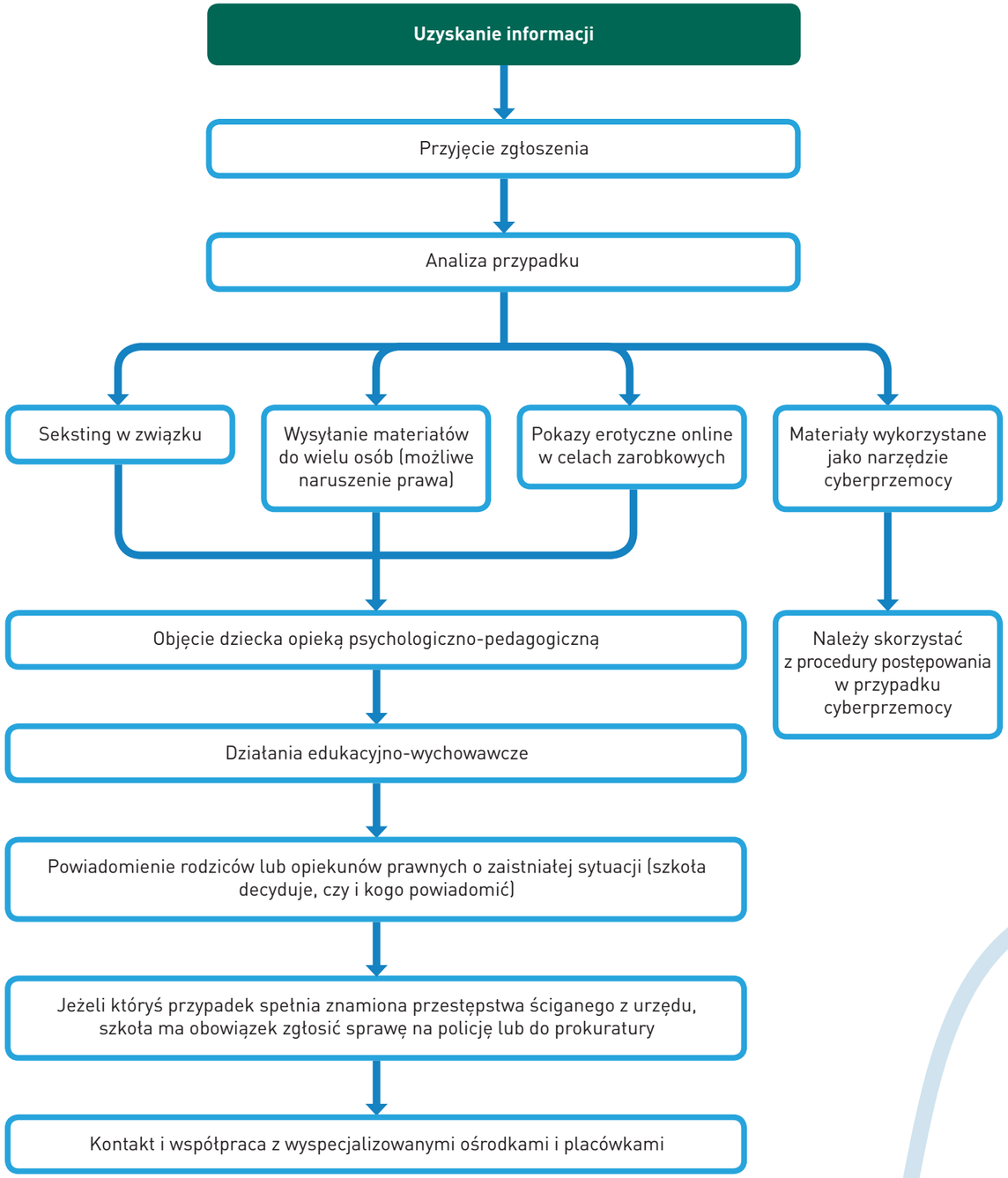
Przepisy prawa

Zjawisko sextingu i przesyłanie sobie nagich zdjęć, zwłaszcza w przypadku osób małoletnich, może się wiązać z łamaniem przepisów prawa (Kodeks karny, art. 200a, 202, a także 191, który dotyczy utrwalania i rozpowszechniania wizerunku bez zgody osoby występującej w danym materiale).

Porady

- Co zrobić, gdy twoje dziecko rozesłało swoje intymne zdjęcia?
- Porozmawiaj z dzieckiem o tym, co się stało, nie oceniaj, nie obwiniaj. Udziel potrzebnego wsparcia.
- Zgłoś sprawę administratorowi serwisu, aby usunął treści, a jednocześnie zachował informacje, które mogą być potrzebne policji w ewentualnym późniejszym postępowaniu.
- Jeżeli doszło do nadużycia wobec dziecka, zgłoś sprawę na policję.

Schemat: Procedura zgłaszania zjawiska sextingu w szkole



NIELEGALNE TREŚCI W INTERNECIE

Oliwia Chojnacka

Opis zjawiska

Treści nielegalne to materiały naruszające przepisy prawa, zarówno polskiego, jak i Unii Europejskiej. Przy ocenie treści zastosowanie znajdują przede wszystkim przepisy Kodeksu karnego (dalej k.k.).

Do nielegalnych treści w internecie zaliczają się m.in.:

- reklama lub promocja działalności polegającej na rozpowszechnianiu treści pornograficznych w sposób umożliwiający zapoznanie się z nimi małoletniemu poniżej lat 15 (art. 200 §5 k.k.);
- uwodzenie za pomocą internetu małoletniego poniżej lat 15 (grooming) (art. 200 §1 i §2 k.k.);
- publicznie propagowanie lub pochwalanie zachowań o charakterze pedofilskim (art. 200 b k.k.);
- treści pornograficzne z udziałem małoletniego oraz związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem (art. 202 §3 k.k.);
- treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej (art. 202 §4b k.k.);
- publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa, a także nawoływanie do nienawiści (art. 256 k.k.) oraz znieważanie grupy czy poszczególnych osób (art. 257 k.k.) na na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (art. 256 k.k.).

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

Skala zjawiska

W 2018 r. eksperci zespołu Dyżurnet.pl przeanalizowali łącznie 13 239 incydentów dotyczących potencjalnie nielegalnych treści w internecie, z czego 1998 zostało zaklasyfikowanych jako treści przedstawiające seksualne wykorzystywanie dzieci. Zdarza się, że to właśnie dzieci zostają twórcami treści pornograficznych. Wytworzenie materiału często następuje w procesie groomingu, dla zabawy lub z chęci wzbudzenia zainteresowania u płci przeciwnej. Według polskiego prawa, gdy osoba uwieczniona na materiale nie ma ukończonych 18 lat, wytwarzanie, przesyłanie lub publiczne udostępnianie materiału jest nielegalne (art. 202 §3 i §4 k.k.).

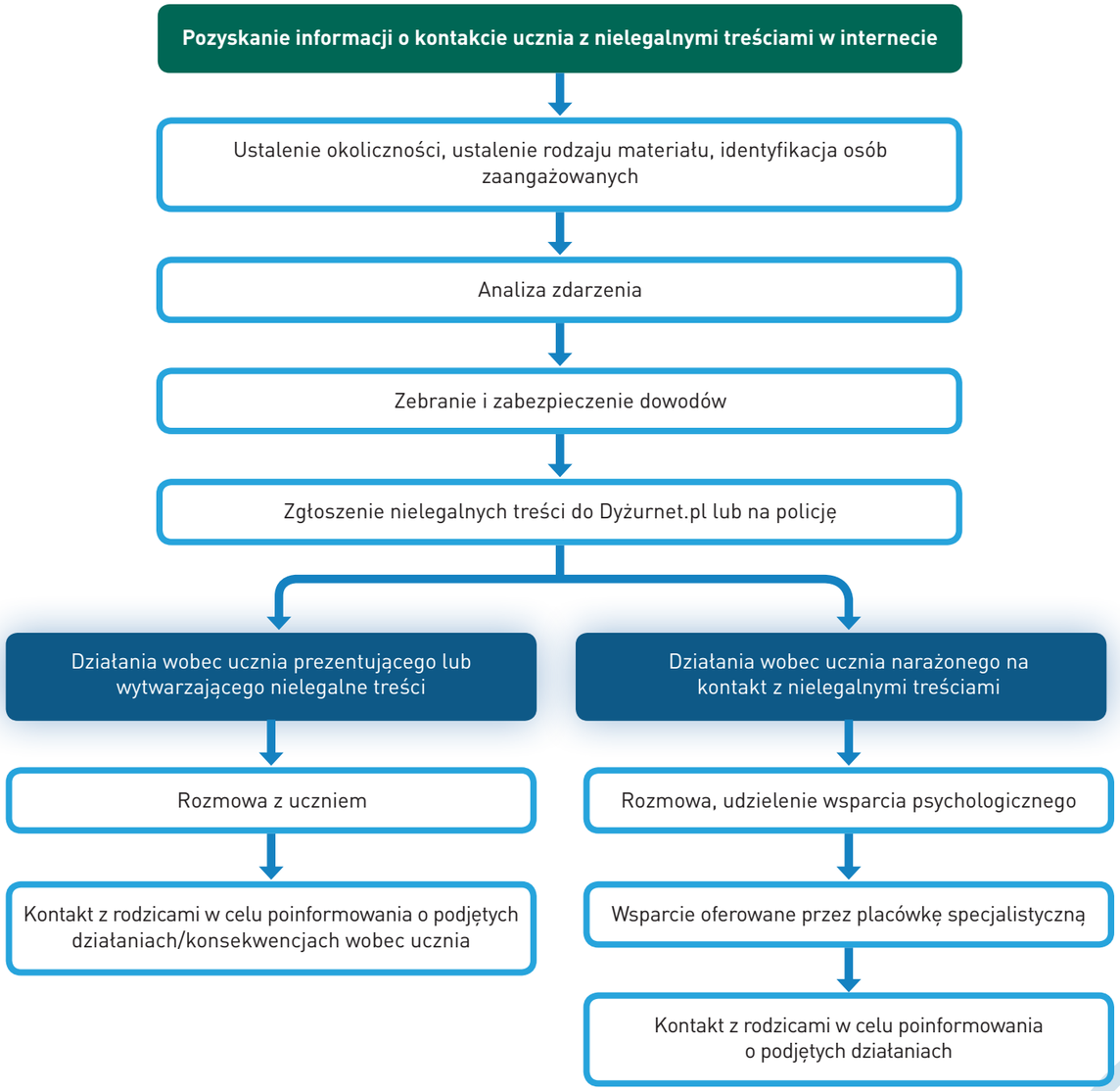
- 43% dzieci w wieku 11–18 lat miało kontakt z pornografią w internecie (Makaruk i in., 2017).
- 2 razy częściej z pornografią w internecie kontakt mają osoby, których rodzice nie ustalili żadnych zasad korzystania z internetu (Makaruk i in., 2017).
- Nastolatki w wieku 15–18 lat, które miały kontakt z pornografią, trzy razy częściej otrzymują nagie lub prawie nagie zdjęcia oraz pięć razy częściej je wysyłają (seksting).

Porady

Jak chronić dzieci przed kontaktem z nielegalnymi treściami w internecie?

- W szkole podłączonej do sieci OSE uruchom darmową usługę ochrony użytkownika OSE
- W szkole niepodłączonej do sieci OSE zadbaj o odpowiednie oprogramowanie zabezpieczające.
- Określ zasady korzystania z internetu, rozmawiaj z dziećmi/uczniami o ich aktywności w internecie.
- Aktywnie towarzysz w podejmowaniu internetowych wyborów, buduj atmosferę zaufania.
- Ustal i wprowadź procedury reagowania na incydenty związane z kontaktem ucznia z nielegalnymi treściami.

Schemat: Procedura reagowania na incydenty związane z kontaktem ucznia z nielegalnymi treściami



W całym procesie bardzo ważna jest również współpraca z policją, sądem rodzinnym, rodzicami, opiekunami prawnymi.

NARUSZENIA PRYWATNOŚCI

Agnieszka Wrońska

Opis zjawiska

Prywatność to prawo do zapewnienia sobie sfery wolnej od ingerencji innych osób oraz prawo do decydowania o tym, jak wiele informacji o sobie chcemy ujawnić. Prawo do ochrony osobistych informacji rozumiane jest również jako umiejętność takiego zachowania, które pomaga ludziom chronić swoje dane, ale też dane innych osób. Naruszenia prywatności mogą zatem dotyczyć zarówno ucznia, jak i nauczyciela; związane są z nieodpowiednim wykorzystaniem danych osobowych lub wizerunku osoby. Zgodnie z przepisami polskiego prawa działania takie jak: podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia szkody osobistej lub majątkowej są przestępstwem. Najczęstszym nadużyciem w tym obszarze jest przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja nieprawdziwych, ośmieszających informacji, modyfikacja treści i zdjęć).

Naruszenie prywatności ucznia często wiąże się również z cyberprzemocą równieśniczą (patrz s. 4) oraz jest traktowane jako forma żartu. Z kolei wyłudzenie lub kradzież danych mogą skutkować szantażem czy dokonaniem zakupów w sklepach internetowych. Prywatność może być przedmiotem ataków cyberprzestępców, którzy wykorzystując złośliwe oprogramowanie zaszyte w popularnych grach i aplikacjach, uzyskują dostęp do danych zapisanych na urządzeniach cyfrowych używanych przez dzieci. Ochrona prywatności bywa często rozumiana jako zachowanie niezależności wobec znanych osób (np. rodziców czy rodzeństwa), a nie wobec innych, często nieznanych użytkowników internetu.

Ochrona przed zagrożeniem dotyczącym sieci szkolnej zapewniona w ramach Usług Bezpieczeństwa OSE.

Skala zjawiska

- Jednym z najczęstszych naruszeń prywatności zgłaszanych przez dzieci i młodzież są przypadki przejęcia kont społecznościowych – aż 13% badanych doświadczyło kradzieży tożsamości;
- Młodzi użytkownicy często udostępniają dane, które powinny zostać poufne (np. numer telefonu udostępnia publicznie 14% nastolatków);
- Co piąty nastolatek nie dostrzega szczególnych zagrożeń związanych z utratą prywatności i nie ogranicza dostępu do swoich materiałów, a ponad jedna trzecia świadomie rezygnuje z narzędzi i działań chroniących prywatność w sieci;
- Jedynie 11% nastolatków regularnie zmienia swoje hasło dostępowe do kont e-mailowych oraz portali społecznościowych (Bochenek, Lange, 2019).

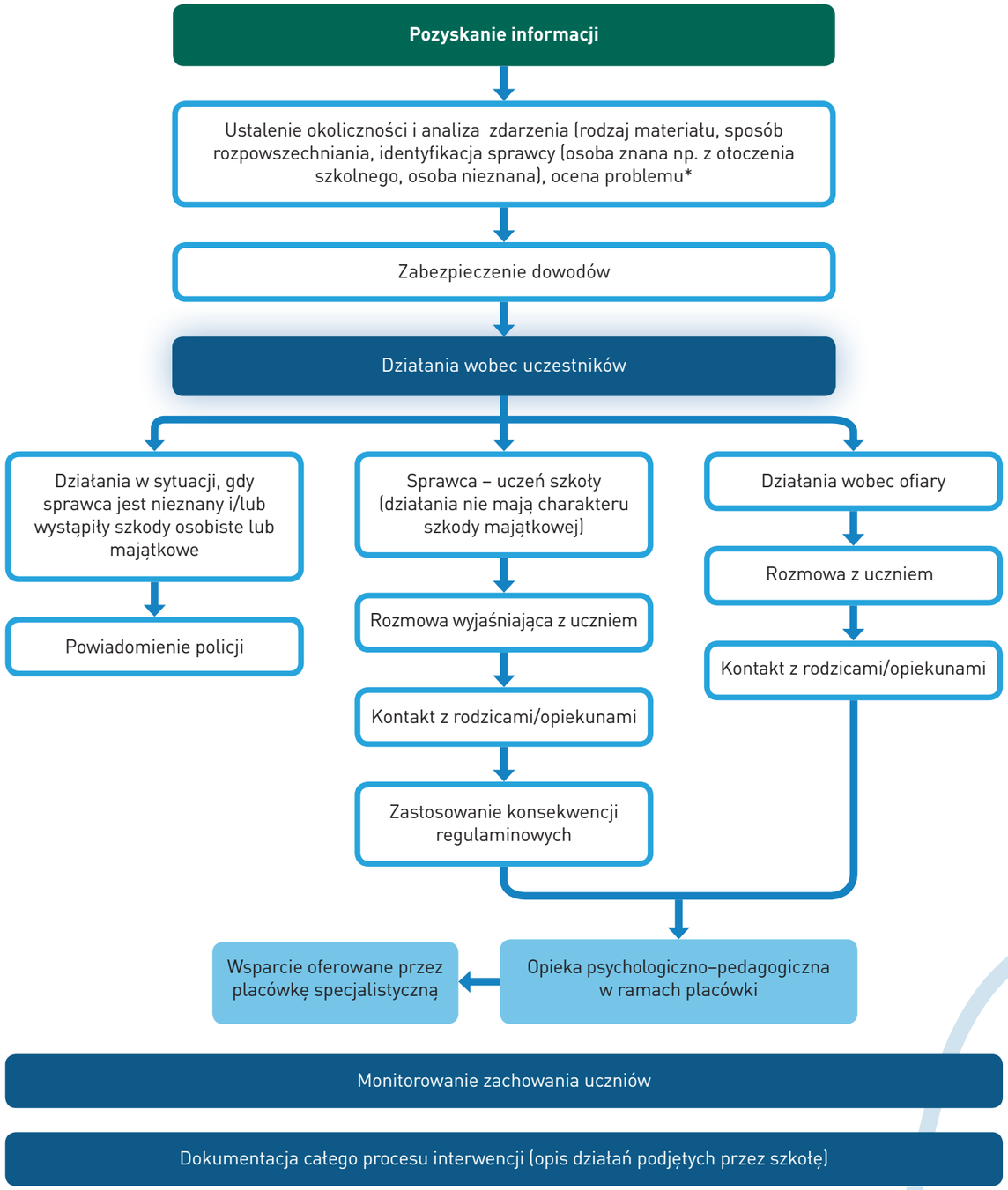
Przepisy prawa

Prywatność jest chroniona przez prawo, m.in. przez Konstytucję RP, w której w art. 47 pojawia się zapis: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Ochronę dóbr osobistych człowieka zapewnia również Kodeks cywilny (art. 23) oraz Kodeks karny (art. 190a §2). Ponadto artykuł 17 ust. 1 Rozporządzenia o ochronie danych osobowych (RODO) ustanawia prawo do usunięcia danych, znane również jako „prawo do bycia zapomnianym".

Porady

- Uświadamiaj, że każdy ma, zarówno prawo do ochrony prywatności, jak i obowiązek poszanowania prywatności innych osób.
- Korzystaj z ustawień prywatności udostępnianych przez serwisy.
- Pamiętaj, że rozporządzenie o ochronie danych osobowych (RODO) umożliwia zgłaszanie do administratorów żądania usunięcia danych („prawo do bycia zapomnianym").

Schemat: Procedura reagowania wobec naruszeń prywatności w internecie



* W przypadku wskazującym na sprawcę działającego w celu wyrządzenia ofierze szkody majątkowej lub osobistej, należy zabezpieczyć dowody i przekazać policji. W przypadku znanego sprawcy (np. ucznia szkoły, kolegi ofiary), który nie działał z powyższych pobudek, rekomenduje się rozwiązanie problemu w ramach działań wychowawczych.

NIEBEZPIECZNE KONTAKTY

Agnieszka Wrońska

Opis zjawiska

Niebezpieczne kontakty dotyczą nawiązywania relacji osób małoletnich z osobami nieznanymi w świecie offline (często dorosłymi o skłonnościach pedofilskich), jak również z jednostkami lub grupami nakłaniającymi do zachowań ryzykownych lub niezgodnych z prawem. Kontakty te podejmowane są w celu wyłudzenia od dziecka poufnych informacji wykorzystywanych później m.in. do działań przestępczych, inicjowania kontaktów seksualnych, skłaniania dziecka do zachowań niebezpiecznych dla jego zdrowia i życia (tj. samookaleczania, restrykcyjnej diety, stosowania substancji psychoaktywnych) lub zainteresowania daną tematyką, werbunku do grup o radykalnych poglądach, np. subkultur propagujących zachowania agresywne, sekt, grup przestępczych.

Do grupy wysoce niebezpiecznych kontaktów należy zaliczyć zjawisko uwodzenia dzieci w internecie (ang. child grooming), polegające na wytworzeniu relacji za pośrednictwem internetu między osobą dorosłą a małoletnią (poniżej 15 r.ż.) w celu uwiedzenia i wykorzystania. Działania podejmowane przez sprawcę nastawione są na nawiązanie więzi emocjonalnej z dzieckiem, tak aby zdobyć jego zaufanie, zmniejszyć opór, nakłonić do podejmowania czynności o charakterze seksualnym. Wykorzystanie i przemoc seksualna wobec dziecka nie dotyczą wyłącznie fizycznego aktu w świecie realnym, ale związane są również m.in. z prezentowaniem dziecku materiałów pornograficznych, prowadzeniem rozmów o charakterze erotycznym, składaniem propozycji seksualnych, nakłanianiem do wykonywania i wysyłania intymnych zdjęć lub filmów czy prezentowaniem zachowań seksualnych podczas chatów i wideotransmisji.

Uwodzenie dzieci w internecie jest często wieloetapowym procesem, podczas którego sprawca stosuje różne techniki manipulacji, używa również szantażu czy groźby. Opiekunom trudno jest zaobserwować próby uwodzenia ich dziecka w sieci. Pomocne mogą być pewne symptomy, tj. wycofanie się z relacji, posiadanie prezentów czy pieniędzy niewiadomego pochodzenia, zabezpieczanie dostępu do urządzeń, przechowywanie materiałów pornograficznych.

Ochrona przed zagrożeniem zostanie zapewniona w ramach planowanych Usług Bezpieczeństwa OSE.

Skala zjawiska

- Co dwudzieste dziecko (5%) było namawiane do zachowań o charakterze seksualnym przez osobę poznaną w internecie (Makaruk i in., 2017).
- Jedna czwarta nastolatków przyznaje, że zdarzyło im się spotkać z osobą dorosłą poznaną w internecie: 39% z nich poinformowało o tym rodziców, a 29% – nikogo (Kamieniecki i in, 2017).
- W roku 2018 eksperci zespołu Dyżurnet.pl przeanalizowali blisko 13 tys. incydentów. Z tej liczby 1 998 zostało zaklasyfikowane jako treści przedstawiające seksualne wykorzystywanie dzieci (Zespół Dyżurnet.pl, 2019).

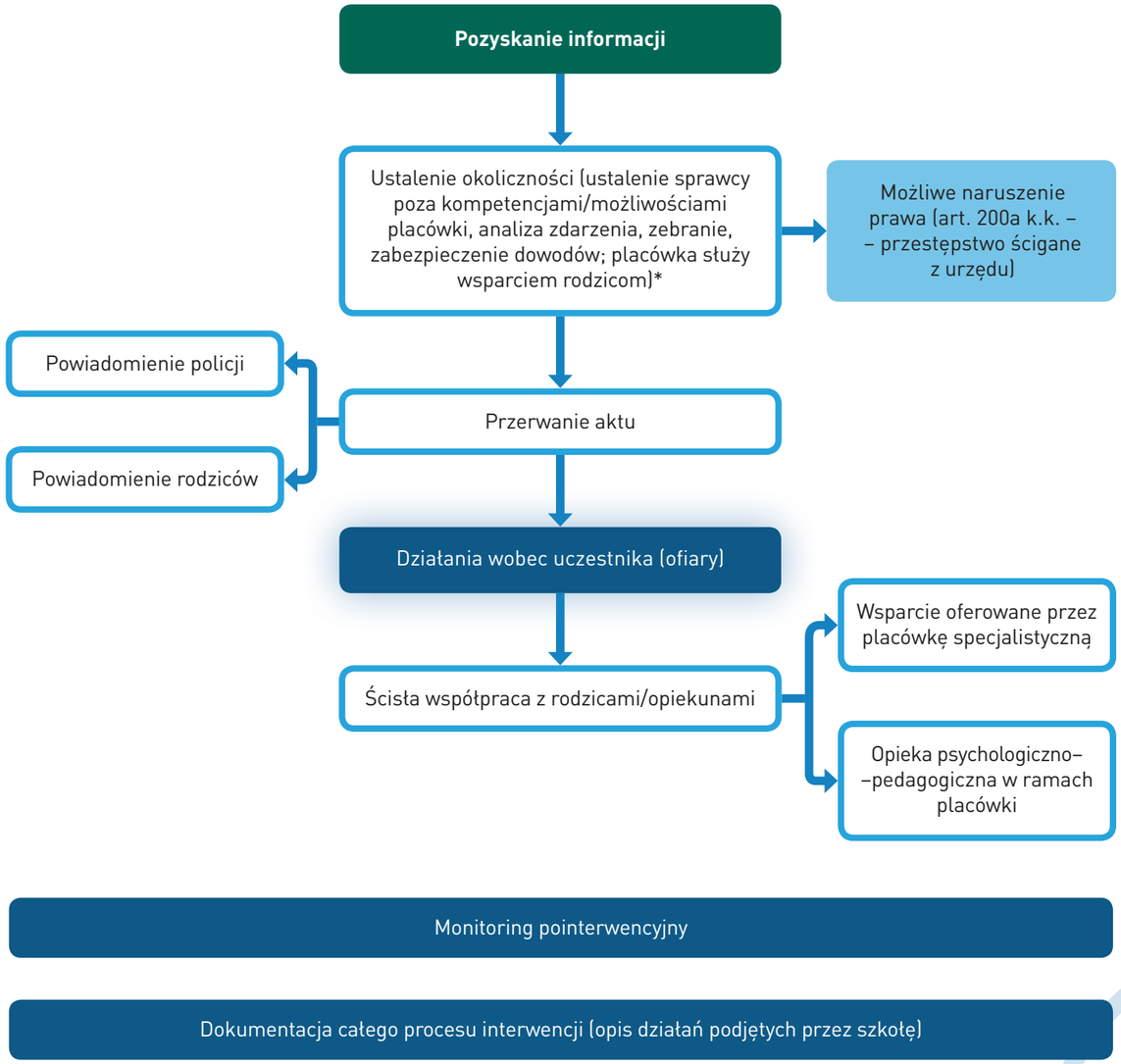
Przepisy prawa

Uwodzenie dzieci w internecie jest przestępstwem uregulowanym w art. 200a Kodeksu karnego (art. 200, 200a §1 i §2, art. 286 §1).

Porady

- Rozmawiaj o problemie uwodzenia w sieci, wyjaśnij metody działania osób o złych zamiarach.
- Obserwuj zachowanie dziecka, w przypadku uwiedzenia oraz próby uwodzenia otocz dziecko specjalistyczną opieką.
- Zabezpiecz dowody uwiedzenia (zapisy rozmów w komunikatorach, na portalach społecznościowych; SMS-y, MMS-y, zrzuty ekranowe, zdjęcia, wiadomości e-mail).
- Powiadom policję, zgłoś problem, skonsultuj się z ekspertem. W przypadkach naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie policji lub sądu rodzinnego.

Schemat: Procedura reagowania wobec niebezpiecznych kontaktów w internecie, w szczególności zjawiska uwodzenia dzieci w internecie (child grooming)



* W całym procesie bardzo ważna jest współpraca z policją, sądem rodzinnym, rodzicami, opiekunami prawnymi.

NARUSZENIA PRAWA AUTORSKIEGO

Katarzyna Kujawa

Opis zjawiska

Zagadnienia związane z prawem autorskim – a co za tym idzie z jego naruszeniami i możliwymi środkami obrony – zostały uregulowane przede wszystkim w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. Zgodnie z ustawą każdemu twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim oraz prawo do wynagrodzenia za korzystanie z utworu. Utwór, jako każdy przejaw działalności twórczej o indywidualnym charakterze, ustalonej w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia, jest chroniony w myśl powyższej ustawy.

Udostępnianie dzieł dla szerszej publiczności – czy to za pomocą internetu, telewizji czy innych mediów – zawsze niesie za sobą ryzyko naruszenia praw autorskich twórcy dzieła. Z kolei nieudostępnianie utworu skutkuje jego kompletną anonimowością i pozostawieniem w czterech ścianach pracowni czy w pamięci smartfona.

W związku z tym, że prawa autorskie dzielą się na prawa osobiste i majątkowe, odmiennie wygląda dochodzenie odszkodowania za naruszenie poszczególnych praw, a także przysługują im inne instytucje prawne. Polski ustawodawca w ustawie o prawie autorskim i prawach pokrewnych przewidział szereg możliwych narzędzi do obrony autorskich praw majątkowych, do których zaliczamy:

- roszczenia o zaniechanie naruszania;
- roszczenia o usunięcie skutków naruszenia;
- roszczenia o naprawienie wyrządzonej szkody na zasadach ogólnych albo poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej dwukrotności – a w przypadku gdy naruszenie jest zawinione: trzykrotności – stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu;
- roszczenia o wydanie uzyskanych korzyści.

W przypadku naruszenia autorskich praw osobistych twórca może żądać zaniechania tego działania poprzez wytoczenie powództwa o ochronę autorskich praw osobistych przed właściwym sądem.

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

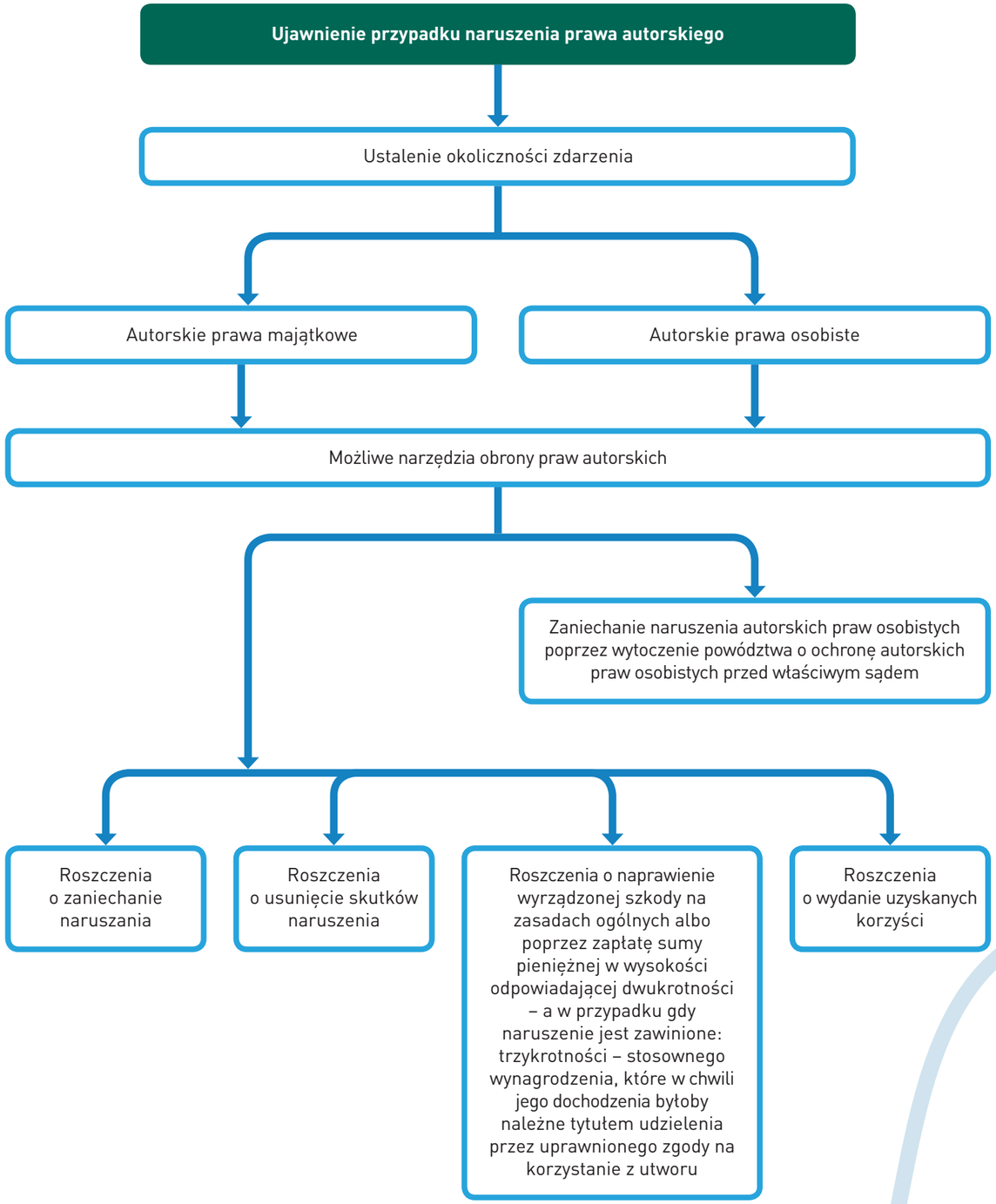
Przepisy prawa

Rozdziały 8–9 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U.2019.1231 t.j.).

Porady

- W przypadku wątpliwości, czy twoje prawa zostały naruszone, skontaktuj się z adwokatem lub radcą prawnym.
- Nie ignoruj naruszania swoich praw – w takich sytuacjach zawsze reaguj!
- Pamiętaj, że polskie prawo dopuszcza możliwość kumulowania roszczeń. Dzięki temu w tym samym czasie możesz zwrócić się do osoby, która bezprawnie wykorzystuje twoje dzieło, zarówno z roszczeniem o zaniechanie naruszeń, jak i z roszczeniem odszkodowawczym.

Schemat: Procedura reagowania w przypadku naruszenia prawa autorskiego



OSZUSTWA KOMPUTEROWE – WYŁUDZANIE DANYCH (PHISHING)

Marek Sowala

Opis zjawiska

Phishing to typ ataku, w którym przestępcy, używając specjalnie spreparowanych wiadomości, chcą wprowadzić ofiarę w błąd i nakłonić do wykonania czynności, której nie powinna wykonać, jak np. kliknięcie w złośliwy link, podanie hasła na niezaufanej stronie czy otwarcie zainfekowanego załącznika. Atakujący starają się wykorzystywać fałszywe informacje w taki sposób, by wzbudzić pożądane emocje, poczucie zaciekawienia lub potrzebę podjęcia natychmiastowego działania. W wiadomościach mogą podszywać się pod znajomego, którego dobrze znasz, czy firmę, z której usług regularnie korzystasz. Przestępcy potrafią podrobić logo instytucji (np. twojego banku) oraz wysłać wiadomość z adresu o łudząco podobnej nazwie (co dodatkowo zwiększa ich wiarygodność). Tego typu kampanie wysyłane są zazwyczaj na masową skalę. Im większa liczba adresatów, tym większe prawdopodobieństwo, że ktoś „połknie haczyk".

W przeciwieństwie do innych zagrożeń phishing nie wymaga szczególnie zaawansowanej wiedzy technicznej ani zaangażowania wielkich środków technicznych. To dlatego, że celem ataku jest człowiek. Przestępcy nie muszą szukać żadnych podatności w systemach komputerowych – używają technik inżynierii społecznej (ang. social engineering), ponieważ uważają, że najsłabszym ogniwem w systemie bezpieczeństwa jest człowiek, który nie sprawdza dokładnie, skąd pochodzi otrzymana wiadomość e-mail i nieświadomie wykona opisane w niej czynności oczekiwane przez przestępców, np. poda na podstawionej stronie banku swoje dane do logowania do systemu bankowego.

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

Porady

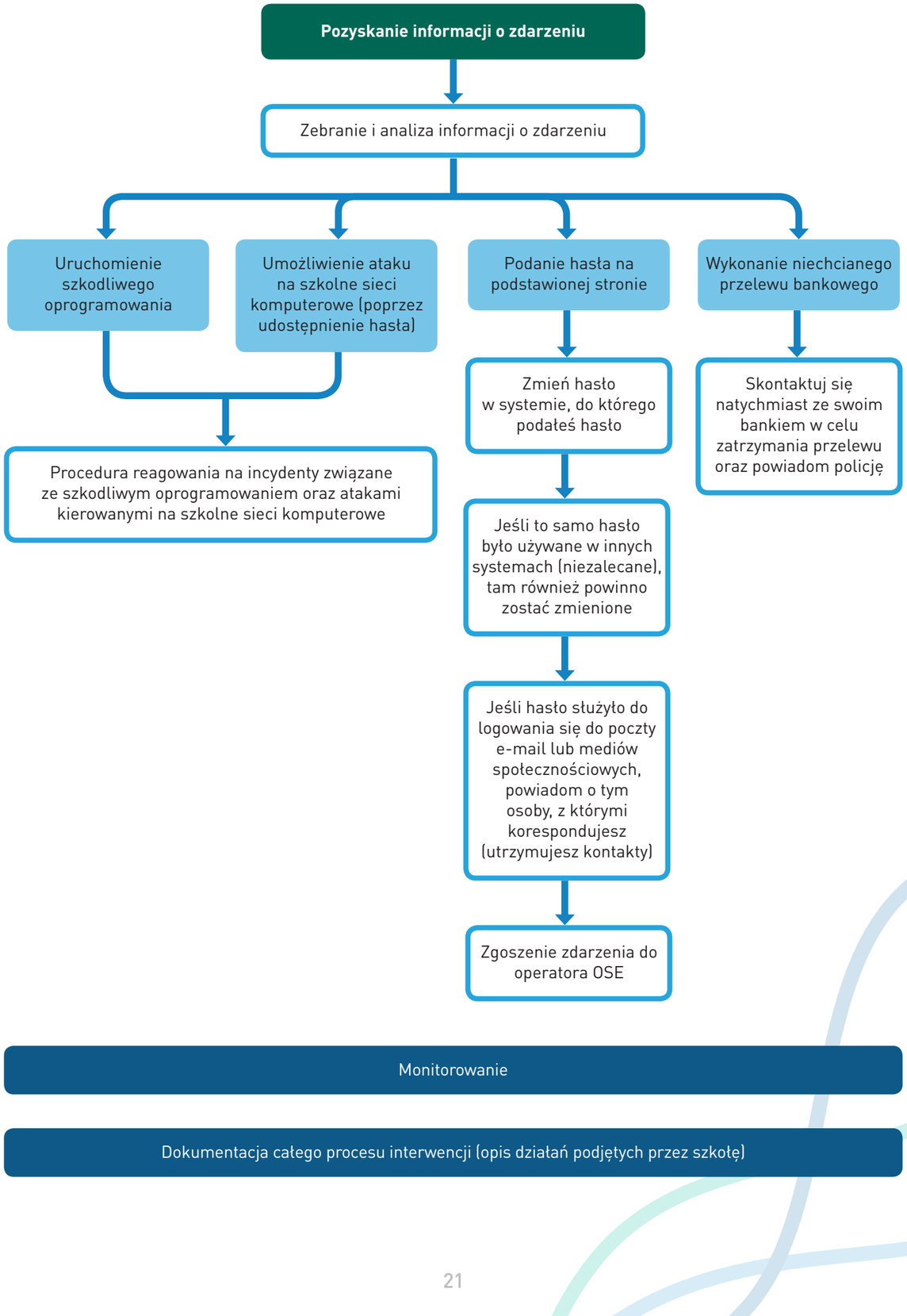
W przypadku phishingu otwarcie czy odczytanie wiadomości nie prowadzi jeszcze do niczego złego. Aby phishing był skuteczny, przestępcy muszą nakłonić ofiarę do wykonania oczekiwanej przez nich czynności. Podstawową linią obrony jest zdrowy rozsądek. Jeśli e-mail lub wiadomość wydają się podejrzane lub ich treść wskazuje na coś nieprawdopodobnego – może to wskazywać na atak phishingowy.

Na szczęście istnieją przesłanki mogące pomóc w odpowiednio wczesnym wykryciu ataku:

- Wiadomość wywołuje u odbiorcy potrzebę podjęcia natychmiastowego działania, gdyż w innym przypadku wydarzy się coś złego. Korzystając z tej metody, atakujący próbuje sprowokować ofiarę do wykonania nieprzemyślanych działań.
- Wiadomości phishingowe adresowane w sposób ogólny, np. „Szanowny Kliencie".
- Wiadomość zawiera pytanie o informacje, które nadawca powinien już znać, lub zapytanie dotyczące danych wrażliwych (takich jak numer karty płatniczej czy hasło).
- Nadawca twierdzi, że jest z dużej organizacji, ale e-mail zawiera dużo błędów językowych lub jest wysłany z ogólnodostępnych adresów: @gmail.com, @wp.pl lub @hotmail.com.
- Otrzymana wiadomość jest od znajomego, ale jej ton lub zastosowane zwroty nie pasują do tej osoby. Jeśli masz podejrzenia, zadzwoń do nadawcy i zweryfikuj, czy to on kontaktował się z tobą.

W szkole podłączonej do sieci OSE uruchom darmową usługę ochrony przed szkodliwym oprogramowaniem, która ma na celu zapewnienie ochrony dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego.

Schemat: Procedura reagowania na incydenty związane z phishingiem



ZŁOŚLIWE OPROGRAMOWANIE (MALWARE)

Marek Sowala

Opis zjawiska

Złośliwe oprogramowanie to program komputerowy stworzony w celu wykonania niepożądanej przez użytkownika czynności. Termin malware wywodzi się z języka angielskiego, powstał jako złożenie dwóch terminów: malicious (złośliwy) oraz software (oprogramowanie). Celem przestępców, którzy wykorzystują złośliwe oprogramowanie, jest przejęcie kontroli nad urządzeniem użytkownika lub/i uzyskanie dostępu do zapisanych na nim danych. Jeżeli przestępcy uda się zainstalować złośliwe oprogramowanie, może szpiegować użytkownika, czytać wymieniane przez niego wiadomości, oglądać i pobierać zdjęcia oraz inne ważne informacje, w tym np. hasła do systemów bankowości elektronicznej, które mogą zostać wykorzystane do kradzieży pieniędzy z konta bankowego.

Złośliwe oprogramowanie może też zostać wykorzystane do atakowania innych użytkowników internetu. Jednym z celów złośliwego oprogramowania jest również wymuszenie okupu od użytkownika poprzez szantaż wykorzystujący wrażliwe informacje znalezione na urządzeniu użytkownika lub wymuszenie okupu za przywrócenie dostępu do danych po uprzednim ich zaszyfrowaniu na dysku (i innych nośnikach pamięci). Wraz ze wzrostem wartości walut wirtualnych, tzw. kryptowalut (Bitcoin, Etherum, Monero) przestępcy bardzo często wykorzystują malware w celu przejęcia mocy komputera użytkownika do zdobycia krytowaluty i wytransferowania jej na własne konta. Użytkownik pozbawiany jest wówczas mocy obliczeniowej swojego komputera, a dodatkowo obciążany kosztami zużytej przez malware energii elektrycznej.

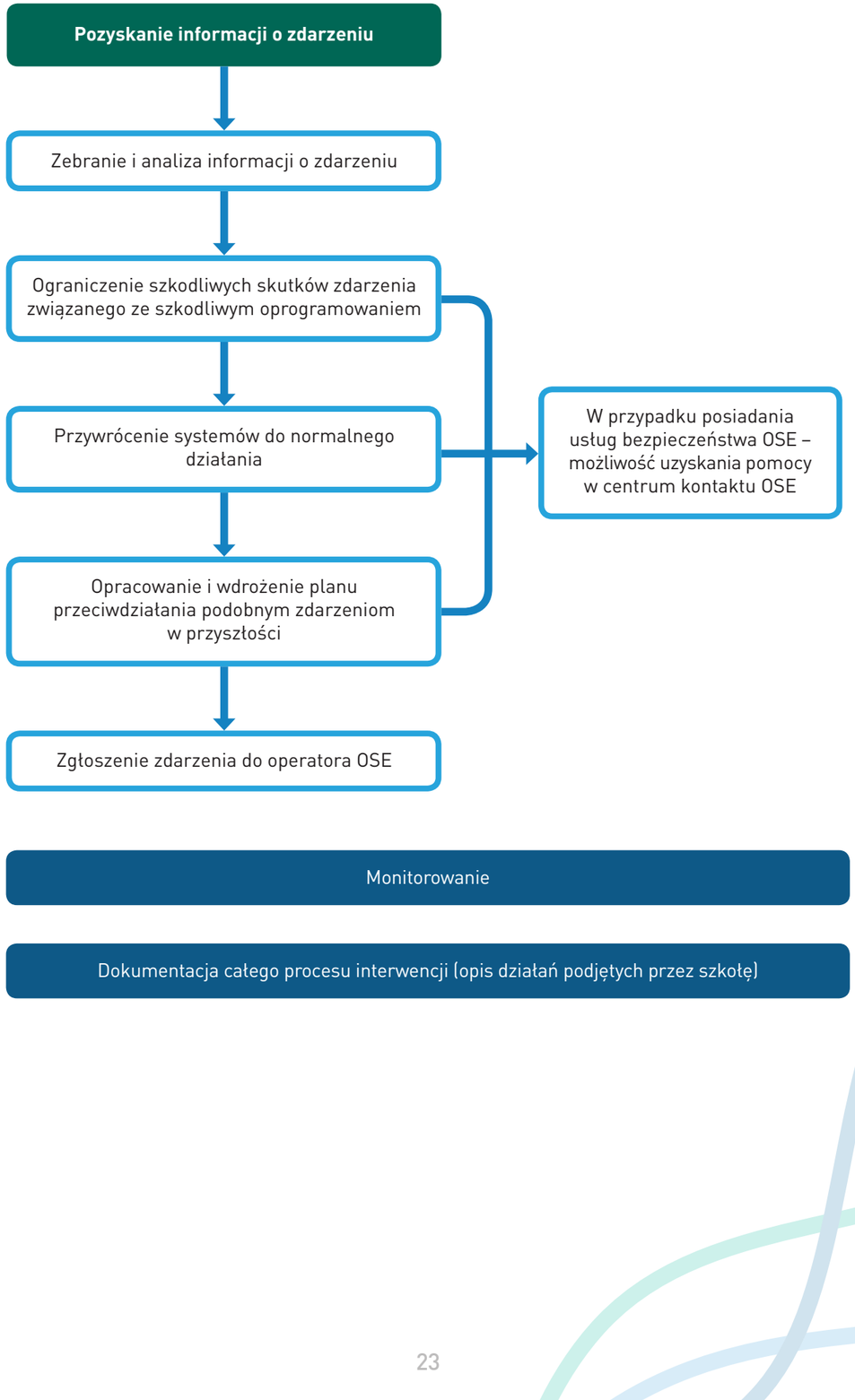
Jak możesz sprawdzić, czy masz na swoim urządzeniu złośliwe oprogramowanie? Komputer zaczyna działać dużo wolniej niż wcześniej, często się zawiesza, nagle bez powodu zmniejsza się dostępna ilość miejsca na dysku, a wykorzystanie zasobów systemu (pamięć RAM, procesor) jest wysokie niezależnie od tego, czy pracujesz intensywnie na urządzeniu, czy nie. Podczas przeglądania otwiera się wiele stron z denerwującymi reklamami (nie można w nie klikać!). To tylko niektóre oznaki, których może być znacznie więcej. Niestety, nawet jeśli nie zauważysz żadnego z powyższych objawów, nie oznacza to, że twoje urządzenie na pewno jest bezpieczne. Istnieje wiele rodzajów malware'u, które działają „po cichu" przez długi czas.

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

Porady

- W szkole podłączonej do sieci OSE uruchom darmową usługę mającą na celu zapewnienie ochrony dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego.
- Nie pracuj na koncie administratora na urządzeniach, które to umożliwiają. To znacznie utrudnia instalację złośliwego oprogramowania.
- Dbaj o aktualność systemu operacyjnego urządzenia, przeglądarek internetowych i innego używanego oprogramowania (np. czytnik plików pdf, pakiet Office).
- Pobieraj aplikacje (szczególnie dotyczy to aplikacji mobilnych) tylko z zaufanych źródeł.
- Nie klikaj łączy w wiadomościach e-mail, tekstowych i komunikatorach o nieznanym pochodzeniu. Nawet jeśli otrzymasz podejrzanie wyglądający link od znajomego, upewnij się, że ta osoba wysłała ci go intencjonalnie.
- Używaj dobrego programu do walki ze złośliwym oprogramowaniem i dbaj o jego aktualizacje.
- Jeżeli wszystkie powyższe metody zawiodą, warto mieć aktualną kopię zapasową danych. Poprawnie wykonane kopie zapasowe to często ostateczna i jedyna metoda odzyskania utraconych plików.

Schemat: Procedura reagowania na incydenty związane ze szkodliwym oprogramowaniem oraz atakami kierowanymi na szkolne sieci komputerowe



ATAKI KIEROWANE NA SZKOLNE SIECI KOMPUTEROWE

Marek Sowala

Opis zjawiska

Szkolne sieci komputerowe narażone są na wiele zagrożeń pochodzących zarówno z wewnątrz sieci, jak i z zewnątrz – z internetu. Ataki z wewnątrz sieci są dużo trudniejsze do wykrycia, ponieważ osoba atakująca znajduje się już w sieci, ma do niej fizyczny dostęp i skutki takiego ataku przeważnie są dużo poważniejsze. Nie zawsze ataki wewnętrzne są zamierzone, czasami spowodowane są niefrasobliwością użytkownika, który np. nieświadomie ściągnie i uruchomi złośliwe oprogramowanie na komputerze w szkole. Ataki zewnętrzne to przeważnie celowe działania mające na celu:

- kradzież informacji w celu ich nieuprawnionego użycia lub sprzedania. Szczególnym przypadkiem jest kradzież informacji osobistych wykorzystywanych do przejęcia czyjeś tożsamości i zaciągnięcia zobowiązań finansowych;
- zmianę i/lub zniszczenie informacji. Zmiana informacji to np. podmiana numeru rachunku bankowego kontrahenta na rachunek kontrolowany przez przestępcę lub podmiana informacji umieszczonych na szkolnym serwerze www. Przykładem utraty informacji może być np. zaszyfrowany dysk twardy komputera, na którym zostało uruchomione złośliwe oprogramowanie szyfrujące dane – ransomware;
- blokadę świadczenia usług sieciowych. Jeśli szkoła posiada własny serwer www lub poczty e-mail, atak na taki serwer może spowodować zaprzestanie jego działania.

Ataki wykonywane są za pomocą bardzo skomplikowanych technik i narzędzi informatycznych. Do najczęściej wykorzystywanych należą:

- podsłuchiwanie ruchu, skanowanie sieci w celu wykrycia podatnych na zagrożenia systemów;
- próby logowania się do serwerów www i poczty e-mail za pomocą podsłuchanych lub odgadniętych haseł;
- wysyłanie do serwera bardzo dużej ilości zapytań, często z wielu komputerów jednocześnie, co powoduje wzrost obciążenia serwera aż do – w skrajnym przypadku – zaprzestania jego działania;
- wykorzystywanie podatności (luk) w oprogramowaniu systemów komputerowych;
- wykorzystywanie szkodliwego oprogramowania (malware) – użytkownicy sieci są często przekonywani do jego ściągnięcia i uruchomienia poprzez phishing. Malware umieszczany jest również na zwykłych, odwiedzanych przez użytkowników stronach, wtedy infekcja odbywa się w tle, bez wiedzy użytkowników.

Ochrona przed zagrożeniem zapewniona w ramach Usług Bezpieczeństwa OSE.

Porady

- W szkole podłączonej do sieci OSE uruchom darmową usługę mającą na celu zapewnienie ochrony dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego.
- Nie pracuj na koncie administratora na urządzeniach, które to umożliwiają. To znacznie utrudnia instalację złośliwego oprogramowania.
- Dbaj o aktualność systemu operacyjnego urządzenia, używanych przeglądarek internetowych i innego oprogramowania (np. czytnik plików pdf, pakiet Office), a także systemu operacyjnego serwerów i urządzeń sieciowych wykorzystywanych w szkole oraz oprogramowania używanego na serwerach (np. www, poczty e-mail).
- Nie klikaj łączy w wiadomościach e-mail, tekstowych i komunikatorach o nieznanym pochodzeniu. Nawet jeśli otrzymasz podejrzanie wyglądający link od znajomego, upewnij się, że ta osoba wysłała ci go intencjonalnie.
- Używaj dobrego programu do walki ze złośliwym oprogramowaniem i dbaj o jego aktualizacje.
- Jeżeli wszystkie powyższe metody zawiodą, warto mieć aktualną kopię zapasową danych. Poprawnie wykonane kopie zapasowe to często ostateczna i jedyna metoda na odzyskanie utraconych plików.

USŁUGI BEZPIECZEŃSTWA OSE

NASK dostarcza usługę bezpieczeństwa, która ma na celu zapewnienie ochrony szerokopasmowego dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego. Ponadto NASK zapewnia wsparcie szkole w podejmowaniu działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. NASK, w ramach projektu OSE, udostępnia usługę ochrony użytkownika w sieci. Usługa ta chroni użytkownika OSE poprzez automatyczną ochronę przed treściami nielegalnymi, czyli treściami, których prezentacja i dystrybucja jest zabroniona i podlega karze, zgodnie z przepisami kodeksu karnego i ustaw właściwych, oraz innymi treściami szkodliwymi dla dzieci.

Usługi bezpieczeństwa OSE – korzyści dla szkoły

- Spełnienie wymagań art. 27 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, która nakłada na szkoły i placówki zapewniające uczniom dostęp do internetu obowiązek podejmowania działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. W szczególności szkoły obowiązane są zainstalować i aktualizować oprogramowanie zabezpieczające.
- Możliwość bezpłatnego korzystania z systemów bezpieczeństwa na najwyższym światowym poziomie, dotychczas dostępnych tylko dla instytucji dysponujących bardzo dużymi budżetami IT.
- Możliwość znaczącego ograniczenia wydatków przez szkoły na oprogramowanie zabezpieczające dostęp szkoły do internetu.
- Całość systemów zlokalizowana jest w centrach przetwarzania danych NASK i zarządzana przez personel operatora OSE, dzięki czemu szkoły nie muszą zatrudniać wykwalifikowanej kadry IT.
- Brak problemów z samodzielną instalacją i aktualizacją oprogramowania zabezpieczającego.

Uruchomienie przez szkołę usług bezpieczeństwa OSE oznacza, że:

- NASK zapewnia ochronę przed szkodliwym oprogramowaniem na poziomie sieci OSE. System mający na celu monitorowanie, wykrywanie i usuwanie znanych wirusów komputerowych działa w następujących procesach: korzystanie z poczty elektronicznej (sprawdzeniu podlegają wyłącznie załączniki), przeglądanie stron internetowych, pobieranie plików z sieci internet.
- NASK zapewnia ochronę na poziomie sieci przed zaawansowanymi atakami sieciowymi kierowanymi na sieć OSE.
- Usługi bezpieczeństwa OSE nie obejmują działaniem sieci LAN w szkołach, a tylko komunikację sieci LAN z siecią internet.
- Strony zawierające treści nielegalne oraz szkodliwe są zablokowane i nie będą dostępne dla użytkowników sieci OSE.
- NASK udostępnia dyrektorowi szkoły raporty dotyczące monitorowania zagrożeń i przypadków naruszeń bezpieczeństwa użytkowników OSE, zawierające dane o sposobie korzystania z internetu w szkole.
- NASK monitoruje zagrożenia i przypadki naruszeń bezpieczeństwa sieci wykryte przez systemy ochrony przed szkodliwym oprogramowaniem.
- Ze względów związanych z ochroną danych wrażliwych system ochrony przed szkodliwym oprogramowaniem nie będzie obejmować witryn z obszarów: bankowość i finanse, opieka zdrowotna oraz poczta elektroniczna.
- Zaawansowane funkcje bezpieczeństwa OSE wykonywane są na urządzeniach centralnych w sieci OSE. Do ich poprawnego działania wymagana jest inspekcja ruchu szyfrowanego SSL w celu analizy ruchu sieciowego przesyłanego w ramach komunikacji wymienianej z internetem. NASK udostępnia certyfikaty SSL, umożliwiające inspekcje ruchu szyfrowanego, które szkoła, korzystająca z usługi bezpieczeństwa, jest zobowiązana zainstalować na wszystkich komputerach oraz urządzeniach komputerowych (tablety, smartfony, laptopy).
- Z powodów niezależnych od NASK pewna część aplikacji sieciowych (głównie mobilnych, czyli instalowanych na urządzeniach takich jak tablety i smartfony) może nie działać poprawnie lub nie działać w ogóle.

BIBLIOGRAFIA

Bochenek M., Lange R. (red.), (2019), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów", Warszawa: NASK Państwowy Instytut Badawczy.

Jupowicz-Ginalska A., Jasiewicz J., Kisilowska M., Baran T., Wysocki A., (2018), „FOMO. Polacy a lęk przed odłączeniem – raport z badań", Warszawa: Wydział Dziennikarstwa, Informacji i Bibliologii.

Kamieniecki W., Bochenek M., Tanaś M., Wrońska A., Lange R., Fila M., Loba B., Konopczyński F., (2017), „Raport z badania. Nastolatki 3.0", Warszawa: NASK – Instytut Badawczy.

Makaruk K., Włodarczyk J., Michalski P., (2017), „Kontakt dzieci i młodzieży z pornografią", Warszawa: Fundacja Dajemy Dzieciom Siłę.

Makaruk K., Wójcik Sz., Konsorcjum EU NET ADB, (2012), „EU NET ADB. Badanie nadużywania internetu przez młodzież w Polsce", Warszawa: Fundacja Dzieci Niczyje.

Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk K., (2019), „Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski", Poznań: Wydawnictwo Naukowe UAM.

Węgrzecka-Giluń J., (2013), „Uzależnienia behawioralne. Rodzaje oraz skala zjawiska. Sygnały ostrzegawcze i skutki. Kompendium wiedzy dla Rodziców", Warszawa: ETOH Fundacja Rozwoju Profilaktyki, Edukacji i Terapii Problemów Alkoholowych.

Wrońska A., Lizut J. (red.), (2019), „Standardy bezpieczeństwa online placówek oświatowych", Warszawa: NASK Państwowy Instytut Badawczy.

Zespół Dyżurnet.pl (red.), (2019), „Raport 2018", Warszawa: NASK Państwowy Instytut Badawczy.

POLECAMY

ose.gov.pl
Ogólnopolska Sieć Edukacyjna

gov.pl/cyfryzacja
Ministerstwo Cyfryzacji

nask.pl
NASK

osehero.pl
OSEhero

lektury.gov.pl
Portal lektury.gov.pl

oseregio.pl
OSEregio

cert.pl
CERT Polska

dyzurnet.pl
Dyżurnet

akademia.nask.pl
Akademia NASK

Państwowy Instytut Badawczy NASK

Cyberbezpieczeństwo – innowacje – edukacja cyfrowa – OSE

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministerstwo Cyfryzacji. Prowadzi badania naukowe i prace rozwojowe na rzecz bezpieczeństwa systemów sieciowych, a także nad technologiami opartymi na najnowocześniejszych rozwiązaniach, wykorzystujących sztuczną inteligencję i zaawansowaną analizę danych. NASK na mocy ustawy o Krajowym Systemie Cyberbezpieczeństwa pełni zadania jednego z trzech Zespołów Reagowania na Incydenty Komputerowe (CSIRT) poziomu krajowego. Instytut realizuje strategiczne programy z obszaru cyfryzacji Polski, a także prowadzi rejestr domeny .pl, w którym znajduje się ponad 2,6 mln domen. NASK wypełnia misję edukacyjną, ekspercką i popularyzatorską na rzecz podnoszenia poziomu kompetencji cyfrowych oraz świadomości bezpieczeństwa użytkowników sieci.

Państwowy Instytut Badawczy NASK jest operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE) – programu Ministerstwa Cyfryzacji, którego celem jest budowa i podłączenie wszystkich szkół w Polsce do szybkiego, bezpiecznego i bezpłatnego internetu, a także tworzenie Ekosystemu OSE, wspierającego proces kształcenia poprzez dostarczanie nowoczesnych i wartościowych treści oraz narzędzi cyfrowych dla nauczycieli i uczniów.

NASK – współtworzymy rewolucję cyfrową w Polsce!

Kontakt

ul. Kolska 12
01-045 Warszawa

+48 22 182 55 55

ose@nask.pl

ose.gov.pl