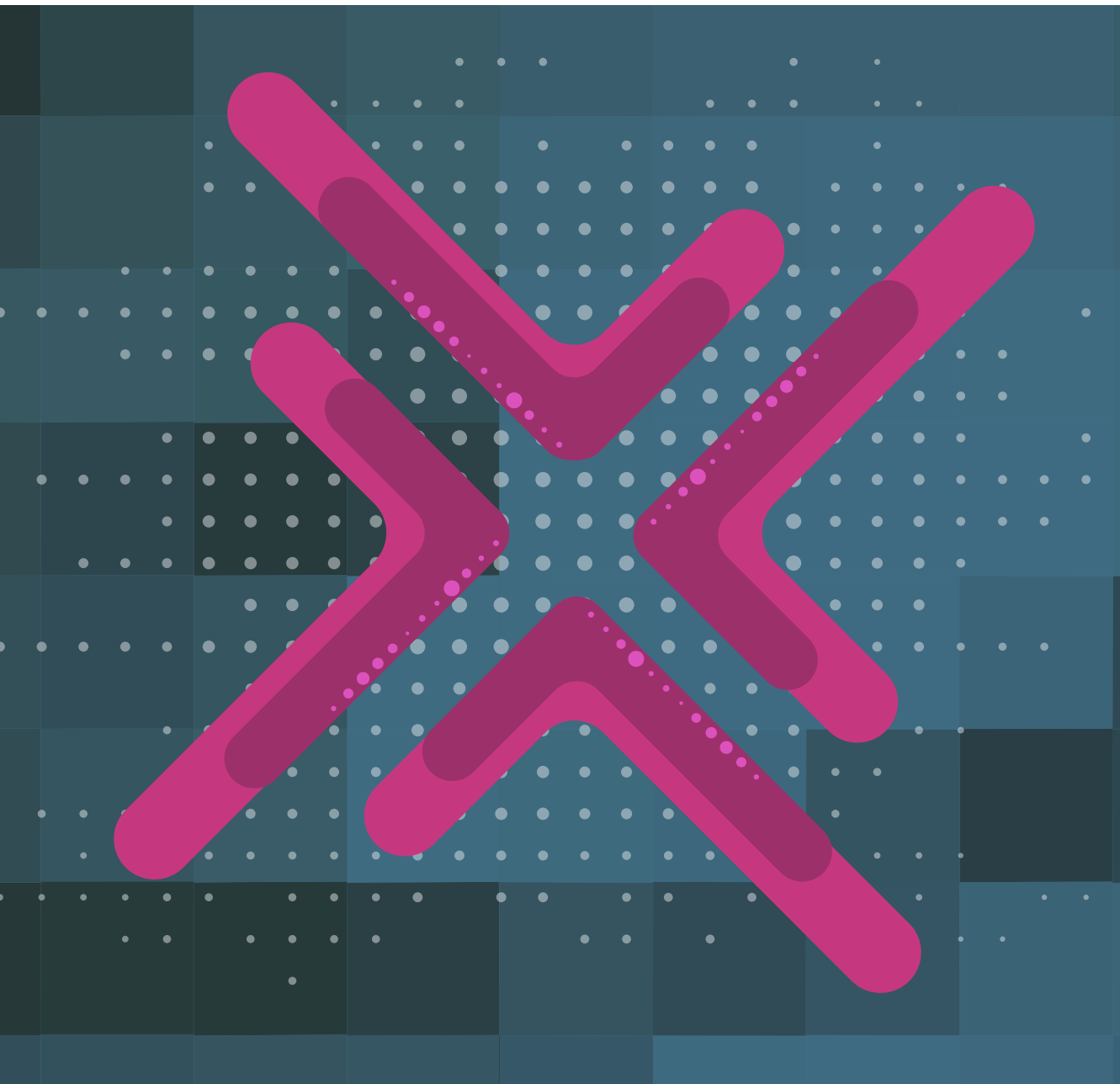
dyżurnet.pl NASK

CSIRT NASK

RAPORT 2022



Wydawca

NASK

Państwowy Instytut Badawczy

ul. Kolska 12
01–045 Warszawa

e-mail: info@nask.pl, info@dyzurnet.pl

ISNN 2084-7785

Tekst | Zespół Dyżurnet.pl, realizujący działania w ramach CSIRT NASK na podstawie dotacji podmiotowej.

Korekta | Anna Maria Hernik-Solarska

Opracowanie graficzne | Agnieszka Makowska

dyżurnet.pl NASK

INHOPE

saferinternet.pl

Dofinansowane przez Unię Europejską

Spis treści

DZIAŁAMY

na rzecz tworzenia
bezpiecznego internetu

REAGUJEMY

na nielegalne i szkodliwe
treści w internecie

POPULARYZUJEMY

bezpieczne korzystanie
z internetu

dyżurnet.pl
NASK

WSTĘP

Szanowni Państwo,

dla NASK-PIB działania na rzecz bezpieczeństwa w internecie mają niezmiennie priorytetowy charakter. Ich niezwykle ważną częścią jest przeciwdziałanie produkcji i dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci. Od 2005 roku potwierdza to każdy rok pracy Zespołu Dyżurnet.pl, w tym uwzględnienie jego działalności w Ustawie o Krajowym Systemie Cyberbezpieczeństwa w 2018 roku oraz wpisanie jego zadań w rolę CSIRT NASK, zespołu reagowania na poziomie krajowym.

Tegoroczny Raport zwraca uwagę na skalę zmian internetowych trendów. Pociąga to za sobą konieczność takiego dostosowania działań, które skutecznie będą zapobiegać przestępstwom seksualnym dotykającym dzieci. Potrzeba ta zauważana jest globalnie – na poziomie Unii Europejskiej aktualnie projektowane są nowe regulacje prawne, do wdrożenia których zobligowana będzie także Polska. Ponadto opracowywany jest krajowy plan działania, uwzględniający zmiany legislacyjne i systemowe, których celem jest przeciwdziałanie przemocy seksualnej wobec dzieci. W obu tych procesach swój istotny udział ma Dyżurnet.pl.

Analiza zgłoszeń i treści w ramach bieżącej pracy, a także wysiłki badawcze Zespołu w 2022 roku pokazują, że wraz z powstawaniem nowych usług czy przestrzeni takich jak Metawers, zagrożenia wobec bezpieczeństwa dzieci przybierają zupełnie nowe formy. Kluczowa jest więc nie tylko wiedza dotycząca funkcjonowania takich usług, ale też umiejętność przewidywania zachowań użytkowników w nowych przestrzeniach usług oraz potencjalnych zagrożeń. Dlatego wspólnie z partnerskimi instytucjami eksperci Dyżurnet.pl pracują nad rozwiązaniami technologicznymi, takimi jak system klasyfikacji danych oparty na sztucznej inteligencji czy projekt globalnego ujednolicenia systemów kategoryzacji nielegalnych treści.

O tym wszystkim, a także o innych zjawiskach i wyzwaniach, z którymi mierzył się Dyżurnet.pl w 2022 roku, przeczytają Państwo w niniejszym raporcie. Mamy nadzieję, że pozwoli to przybliżyć Państwu tę tematykę, abyśmy wszyscy – jako rodzice, opiekunowie, dorośli odpowiedzialni za dobro dzieci – mogli skutecznie dbać o bezpieczeństwo najmłodszych i nieustannie udzielać im wsparcia.

Z poważaniem

Krzysztof Silicki
Dyrektor ds. Strategicznego Rozwoju Cyberbezpieczeństwa

O NAS

Działamy – reagujemy – popularyzujemy

Zespół **Dyżurnet.pl** został powołany w 2005 roku w NASK. Jest jedynym w Polsce zespołem reagującym na nielegalne i szkodliwe treści w internecie, który w ramach swojej działalności, na podstawie Ustawy o Krajowym Systemie Cyberbezpieczeństwa, przyjmuje zgłoszenia dotyczące materiałów przedstawiających seksualne wykorzystywanie dzieci.

Od początku działalności **Dyżurnet.pl** należy do Stowarzyszenia INHOPE https://inhope.org/ – globalnej sieci zrzeszającej zespoły reagujące z różnych krajów, prowadzącego współpracę z międzynarodowymi organami ścigania, m.in. z Interpolem oraz firmami branży internetowej. Celem Stowarzyszenia jest wsparcie krajowych hotline'ów przeciwdziałających dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci.

Zespół **Dyżurnet.pl** od 2005 roku realizuje strategię Komisji Europejskiej Better Internet for Children, **współtworząc Polskie Centrum Programu Safer Internet (PCPSI)** https://www.saferinternet.pl/. Tworzą je: NASK Państwowy Instytut Badawczy (koordynator PCPSI) oraz Fundacja Dajemy Dzieciom Siłę. Strategia wdrożona w większości krajów europejskich (https://www.betterinternetforkids.eu/) ma na celu promowanie bezpiecznego korzystania z internetu i nowych technologii oraz wsparcie reagowania w przypadku zagrożeń online dotykających najmłodszych.

Telefony zaufania:

- 116 111 – telefon zaufania dla dzieci i młodzieży
- 116 123 – telefon zaufania dla osób dorosłych
- 800 100 100 – telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci

W 2022 roku Dyżurnet.pl w ramach współpracy z innymi zespołami interwencyjnymi wpierał rozwój telefonu zaufania dla osób dorosłych *Niebieska Linia*, finansowanego ze środków Skarbu Państwa będących w dyspozycji Ministra Cyfryzacji. Dostępne są trzy kanały komunikacji:

1. Telefon zaufania 116 123 – infolinia działa całodobowo, 7 dni w tygodniu, przez cały rok. Dostępna jest anonimowo i bezpłatnie.
2. Formularz kontaktowy – umożliwia otrzymanie porady mailowej. Konsultanci dokładają starań, aby jak najszybciej przesłać odpowiedź (w ciągu 48h od otrzymania zgłoszenia).
3. Czat – indywidualne rozmowy online ze specjalistami, dostępne od poniedziałku do piątku w godz. 17:00-22:00 (w przyszłości działający całodobowo, przez 7 dni w tygodniu).

Obsługa
zgłoszeń

Jak działamy?

Dyżurnet.pl przyjmuje zgłoszenia poprzez:

- formularz znajdujący się na stronie internetowej **www.dyzurnet.pl**
- adres mailowy **dyzurnet@dyzurnet.pl**
- automatyczną infolinię **801 615 005**
- wtyczkę do przeglądarki Google Chrome: Zgłoś nielegalną treść do Dyżurnet.pl
- wtyczkę do przeglądarki Mozilla Firefox: Zgłoś treść do Dyżurnet.pl

Ze względu na szkodliwość oraz możliwość poniesienia konsekwencji karnych z powodu uzyskiwania dostępu do nielegalnych treści zespół Dyżurnet.pl odradza samodzielne wyszukiwanie ich w internecie.

Kategorie, które są objęte procedurą reagowania[1]:

- Materiały przedstawiające seksualne wykorzystywanie dziecka: art. 202 §3, 4, 4a, 4b k.k. – prawo polskie zabrania produkowania, utrwalania, sprowadzania, rozpowszechniania, prezentowania, przechowywania, uzyskiwania dostępu oraz posiadania treści pornograficznych z udziałem małoletniego;
- Materiały przedstawiające twardą pornografię: art. 202 §3 k.k. – prawo polskie zabrania rozpowszechniania i publicznego prezentowania pornografii związanej z wykorzystaniem przemocy lub posługiwaniem się zwierzęciem;

1. Artykuły Kodeksu Karnego w brzmieniu niepełnym

- Treści propagujące rasizm i ksenofobię: art. 256 k.k. – polskie prawo zabrania propagowania faszystowskiego lub innego totalitarnego ustroju państwa oraz nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych lub ze względu na bezwyznaniowość;

- Inne nielegalne treści: treści niedotyczące żadnej z powyższych kategorii, ale skierowane przeciwko bezpieczeństwu dzieci, na przykład:

    - propagowanie lub pochwalanie zachowań o charakterze pedofilskim (art. 200b k.k.),

    - uwodzenie dziecka poniżej 15 r.ż. przez internet, tzw. child grooming (art. 200a k.k.),

    - zjawisko szantażu na tle seksualnym (określane również jako „sextortion").

Najważniejszą grupę zgłoszeń przekazywanych przez użytkowników internetu do zespołu Dyżurnet.pl stanowią treści przedstawiające seksualne wykorzystywanie dziecka.

W zależności od klasyfikacji zgłoszenia oraz lokalizacji serwera, na którym przechowywane są zgłoszone treści, zespół zgodnie z procedurą podejmuje następujące działania:

- jeżeli materiał przedstawiający seksualne wykorzystywanie dziecka znajduje się na serwerze zlokalizowanym w Polsce, to informacja jest przekazywana do Komendy Głównej Policji oraz do Interpolu;

- jeżeli materiał przedstawiający seksualne wykorzystywanie dziecka znajduje się na serwerze w kraju objętym działaniem Stowarzyszenia INHOPE, informacja ta przekazywana jest do zespołu reagującego właściwego dla kraju lokalizacji serwera oraz do Interpolu;

- jeżeli materiał przedstawiający seksualne wykorzystywanie dziecka znajduje się na serwerze poza zasięgiem INHOPE, ta informacja przekazywana jest do Komendy Głównej Policji oraz do Interpolu.

Wszystkie materiały (zdjęcia i filmy) prezentujące seksualne wykorzystywanie dzieci są przekazywane do bazy ICCAM, aby służyły identyfikacji ofiar i sprawców.

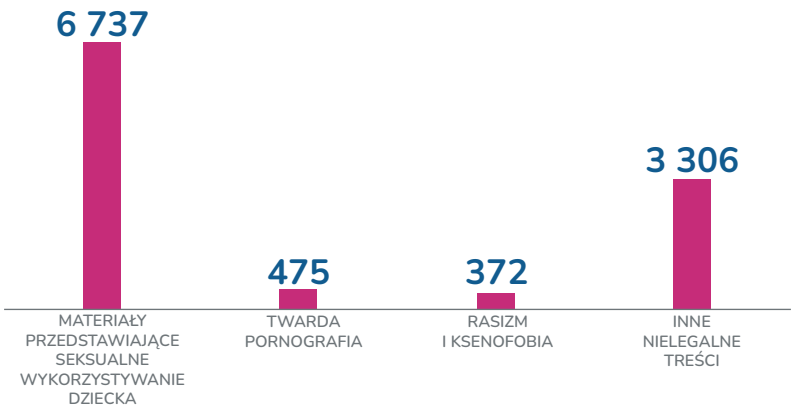
Działania wszystkich zespołów reagujących oraz współpracujących z nimi organów ścigania zmierzają do jak najszybszego zidentyfikowania sprawcy oraz ofiary seksualnego wykorzystania. Zgłoszenie przez użytkownika oraz niezwłoczne podjęcie działań przez administratora pozwalają na znaczne ograniczenie dalszego rozpowszechniania materiału przedstawiającego seksualne wykorzystywanie dziecka.

Statystyki

Dyżurnet.pl za rok 2022

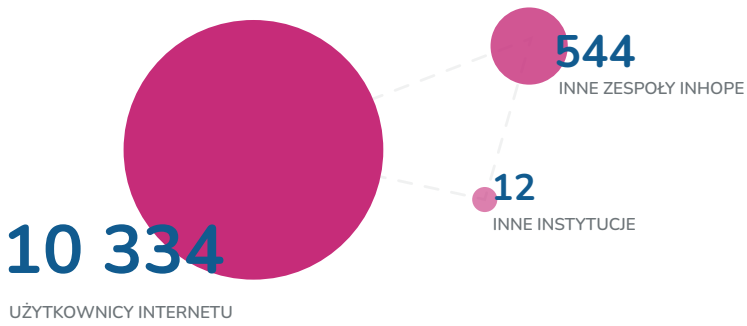
Zgłoszenia otrzymane przez zespół Dyżurnet.pl

1 | Liczba zgłoszeń otrzymanych przez Dyżurnet.pl - rodzaj potencjalnie nielegalnych treści



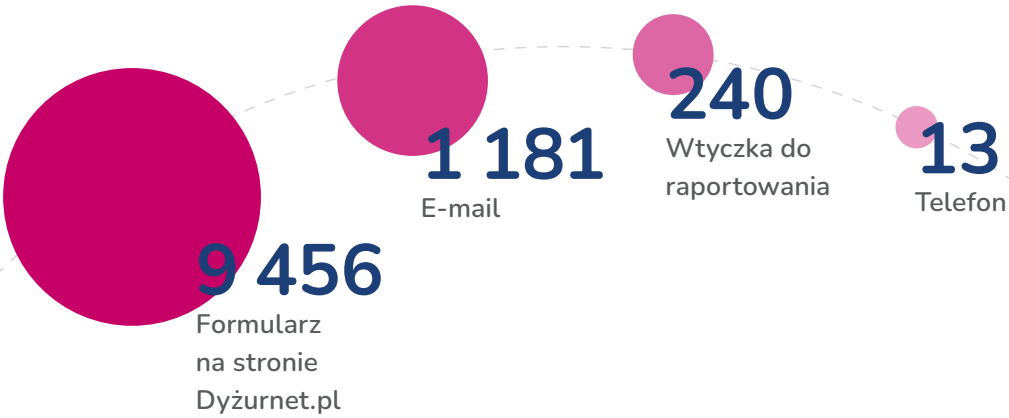
Zgłoszenia dotyczące treści potencjalnie przedstawiających seksualne wykorzystywanie dziecka od samego początku funkcjonowania Dyżurnet.pl stanowią największą część wszystkich zgłoszeń. Skuteczna współpraca w ramach Stowarzyszenia INHOPE oraz z krajowymi hostingodawcami i policją pozwala na szybką reakcję wobec takich treści. W porównaniu do poprzedniego roku liczba zgłoszeń dotyczących kategorii CSAM, twardej pornografii oraz treści rasistowskich utrzymuje się na podobnym poziomie. Wyraźnie natomiast zmniejszyła się liczba zgłoszeń z kategorii „inne" z 7 128 w roku 2021 do 3 306 w roku 2022.

2 | Liczba zgłoszeń otrzymanych przez Dyżurnet.pl - rodzaj zgłaszającego



Użytkownicy internetu od lat stanowią zdecydowaną większość przesyłających zgłoszenia do Dyżurnet.pl. Zespoły w ramach Stowarzyszenia INHOPE wysyłają mniej zgłoszeń, głównie dlatego, że względnie rzadko CSAM pojawia się na serwerach w Polsce.

3 | Liczba zgłoszeń otrzymanych przez Dyżurnet.pl - źródło zawiadomienia



Najczęściej wybieranym kanałem zgłaszania jest internetowy formularz znajdujący się na stronie www.dyzurnet.pl. Pomimo uruchomienia w roku 2020 wtyczki do raportowania dla przeglądarek Chrome i Firefox pomagającej w demaskowaniu i podejmowaniu reakcji wobec ukrytych treści CSAM, liczba zgłoszeń przy jej użyciu jest podobna jak w poprzednim roku i, niestety, stanowi względnie małą część wszystkich zgłoszeń.

Analizowane incydenty i działania podjęte przez zespół Dyżurnet.pl

4 | Klasyfikacja incydentów związanych z wykorzystaniem seksualnym małoletnich

2 861
CSAM

CSAM (*child sexual abuse materials*) – treści przedstawiające seksualne wykorzystywanie dzieci. Zgodnie z polskim prawem nielegalne, definiowane jako treści pornograficzne z udziałem małoletniego (art. 202 § 3, 4, 4a, 4b k.k.).

479
CSEM

CSEM (*child sexual exploitation materials*) – treści prezentujące dziecko w kontekście seksualnym, niekwalifikujące się jako CSAM. Obejmuje tzw. „modeling" i „seksualne pozowanie".

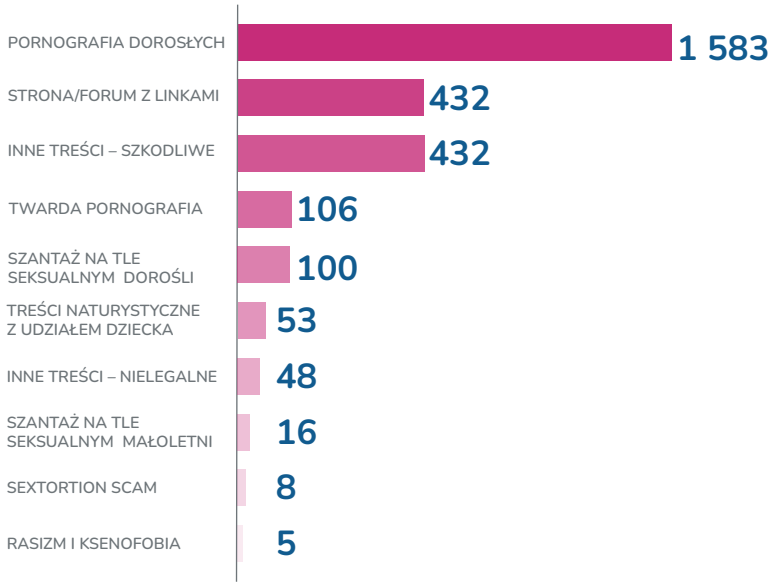
53
Propagowanie pedofilskiej aktywności

Propagowanie pedofilskiej aktywności – publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim; nielegalne wg polskiego prawa (art. 200b k.k.).

12
Uwodzenie dziecka

Uwodzenie dziecka – nawiązywanie kontaktu z małoletnim poniżej 15 r.ż. celem obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych; zgodnie z polskim prawem nielegalne (art. 200a k.k. [Elektroniczna korupcja seksualna małoletniego]).

5 | Klasyfikacja incydentów związanych z innymi treściami nielegalnymi i szkodliwymi



Pornografia dorosłych – treści o charakterze pornograficznym z udziałem osób wyglądających na pełnoletnie.

Strona/forum z linkami – strony lub fora internetowe zawierające wyłącznie linki do zewnętrznych zasobów.

Inne treści – szkodliwe - treści szkodliwe dla osób do 18 r.ż.: treści drastyczne, wulgarne, obraźliwe, radykalne światopoglądowo (również sekty), homofobiczne, autodestrukcyjne, propagujące samobójstwo lub przemoc, pro-ana, patostreamy, środki psychoaktywne (niezidentyfikowane jednoznacznie jako narkotyki).

Treści naturystyczne z udziałem dziecka – treści prezentujące nagie dzieci bez intencjonalnego seksualnego kontekstu, zazwyczaj treści nudystyczne czy naturystyczne o neutralnym charakterze.

Twarda pornografia – treści pornograficzne z udziałem osób wyglądających na pełnoletnie, zawierające sceny związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem; nielegalne wg polskiego prawa (art. 202 § 3 k.k.).

Szantaż na tle seksualnym – seksualne wymuszenie, szantaż związany z uzyskaniem od ofiary materiałów multimedialnych o charakterze seksualnym pod groźbą ich szerszego udostępnienia; może wiązać się uzyskiwaniem materialnych korzyści. Klasyfikacja jest podzielona na sprawy dotyczące osób dorosłych i osób małoletnich.

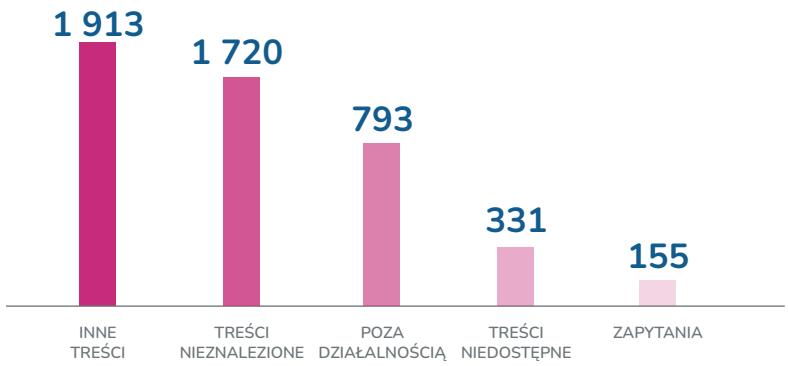
Inne treści – nielegalne – treści penalizowane przez polski Kodeks Karny i zagrażające bezpieczeństwu dzieci, wchodzące w zakres reagowania zespołu Dyżurnet.pl.

Sextortion scam – wysyłana masowo korespondencja dotycząca rzekomo pozyskanych materiałów o charakterze seksualnym z udziałem adresata; jedna z form wyłudzeń finansowych skierowana do osób, które padły ofiarą wycieku danych do logowania.

Rasizm i ksenofobia – treści publicznie propagujące totalitarny ustrój państwa, nawołujące do nienawiści oraz znieważające ze względu na przynależność narodową, etniczną, rasową, wyznaniową lub ze względu na bezwyznaniowość; zgodnie z polskim prawem nielegalne (art. 256 oraz 257 k.k.).

W porównaniu do roku 2022 i lat poprzednich Dyżurnet.pl obserwuje ciągły wzrost liczby incydentów dotyczących szantażu na tle seksualnym. W przypadku osób dorosłych dotkniętych tym zjawiskiem i które zdecydowały się zgłosić to do Dyżurnet.pl, liczba ta wzrosła z **69** w roku 2021 do **100** w roku 2022. W przypadku osób małoletnich, które osobiście lub poprzez rodziców szukały pomocy, liczba wzrosła z **3** do **16**.

6 | Klasyfikacja pozostałych kategorii incydentów



Inne treści – treści spoza wymienionych kategorii, nie będące treściami szkodliwymi lub nielegalnymi.

Treści nieznalezione – w momencie podjęcia analizy przez Dyżurnet.pl treści nie zostały znalezione, najprawdopodobniej zostały już usunięte.

Poza działalnością – Sprawy będące naruszeniami prawa, ale wykraczające poza zakres interwencji Dyżurnet.pl: zniesławienia, znieważenia, stalking,

groźby, naruszenia dóbr osobistych i wizerunku, sprawy dotyczące danych osobowych (wyłudzenia, udostępnianie bez zgody), wyłudzenia i oszustwa finansowe (w tym fałszywe sklepy internetowe), włamania na konta i kradzież danych, naruszenia praw autorskich, gry hazardowe, dystrybucja farmaceutyków poza obrotem aptecznym, informacje o dostępności zabiegów lub środków przerywania ciąży, publikowanie potencjalnie fałszywych informacji, fałszywe profile instytucji, fałszywe dokumenty,

Treści niedostępne – treści zabezpieczone hasłem, pliki do pobrania znajdujące się na serwerach znajdujących się poza Polską, strony zidentyfikowane jako skutecznie maskujące swoją treść.

Zapytania – pytania użytkowników internetu oraz innych instytucji dotyczące nielegalnych i szkodliwych treści publikowanych w sieci.

Liczba treści legalnych zgłaszanych do Dyżurnet.pl w roku 2022 zdecydowanie spadła z 5 484 w poprzednim roku do niecałych dwóch tysięcy. Wskutek masowego ich przesyłania w krótkim czasie oraz powtarzalnych domen, nie można wykluczyć, że ta kategoria zgłaszana była przez boty w celu zakłócenia procesu analizy zgłoszeń treści nielegalnych.

7 | Działania podjęte przez Dyżurnet.pl wobec wszystkich kategorii incydentów

2 460
Zgłoszone do odpowiedniego zespołu INHOPE oraz do Interpolu

290
Zgłoszone do administratorów serwisów

55
Zgłoszone do ISP

2
Zgłoszone do właściciela treści

182
Przekazane innemu podmiotowi (głównie CERT Polska)

167
Zgłoszone Policji

Zgłoszone do odpowiedniego zespołu INHOPE oraz do Interpolu – przesłane poprzez bazę ICCAM lub formularz kontaktowy do zespołów reagujących

właściwych dla lokalizacji serwera, zrzeszonych w Stowarzyszeniu INHOPE; treści z kategorii *baseline* (materiały stanowiące treść nielegalną we wszystkich krajach zrzeszonych w INHOPE) przekazywane są do bazy ICSE *(International Child Sexual Exploitation Database)* w Interpolu.

Zgłoszone do administratorów serwisów – zgłoszenie przesłane do administratorów lub działu moderacji serwisu internetowego, dotyczące treści niebędącej treścią nielegalną, jednak niezgodną z regulaminem serwisu.

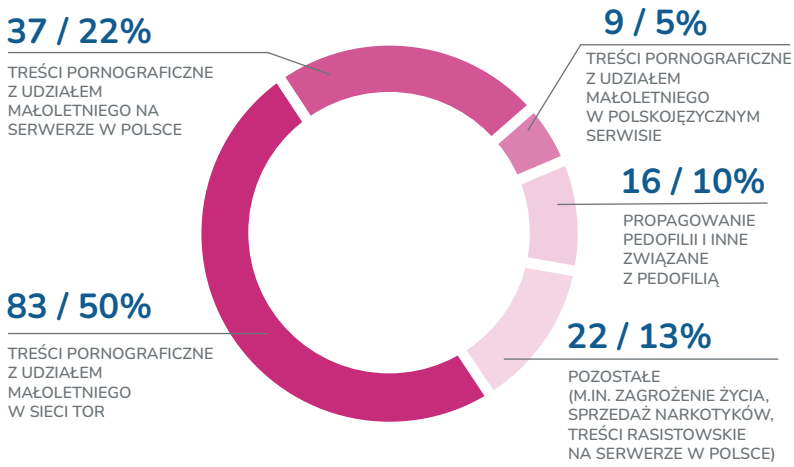
Zgłoszone do ISP - przesłanie zawiadomienia o treściach o charakterze bezprawnym (dotyczących CSAM) zgodnie z art. 14 *Ustawy o świadczeniu usług drogą elektroniczną* w przypadku hostingodawcy w Polsce lub poinformowanie hostingodawcy znajdującego się poza zasięgiem INHOPE o bezprawnych treściach (dotyczących CSAM) znajdujących się na jego serwerach.

Zgłoszone do właściciela treści – zgłoszenie dotyczące treści o szkodliwym charakterze skierowane do autora treści w celu rozważenia założenia odpowiedniego ostrzeżenia lub ich usunięcia.

Przekazane innemu podmiotowi – przekazane do współpracujących instytucji zgodnie z zakresem ich działania (głównie CERT Polska w ramach CSIRT NASK oraz Fundacji Dajemy Dzieciom Siłę).

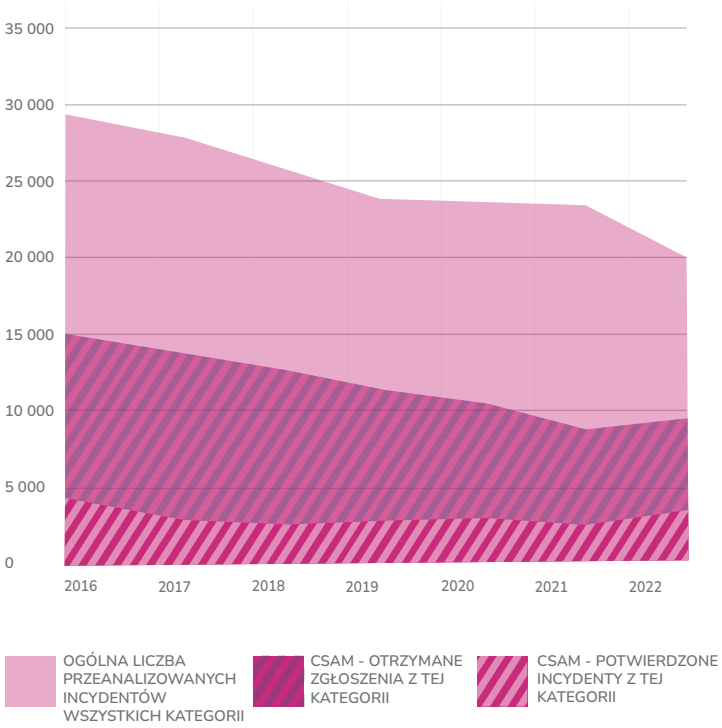
Zgłoszone Policji – przekazane do Centralnego Biura Zwalczania Cyberprzestępczości

8 | Zgłoszenia przesłane do Centralnego Biura Zwalczania Cyberprzestępczości KGP



Analiza treści CSAM

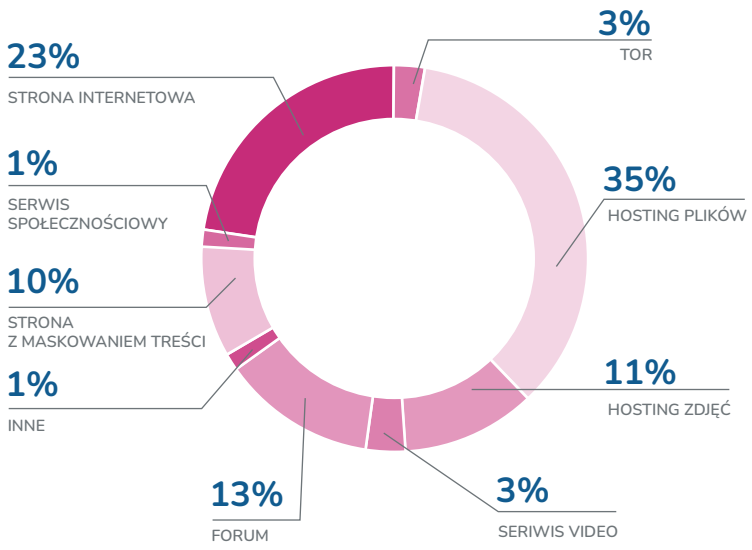
9 | Liczba zgłoszeń dotyczących potencjalnych materiałów typu CSAM oraz potwierdzonych incydentów CSAM na tle ogólnej liczby przeanalizowanych incydentów w latach 2015-2021



Rok 2022 przyniósł zdecydowany spadek liczby przesłanych zgłoszeń, jednak jak pokazuje rys. 1 zmniejszeniu uległa liczba zgłoszeń kategorii „inne treści". Jednak po ich analizie okazało się, że większość z nich nie dotyczyła ani szkodliwych, ani tym bardziej nielegalnych materiałów publikowanych w internecie.

Jednocześnie nastąpił wzrost potwierdzonych incydentów dotyczących obecności treści przedstawiających seksualne wykorzystywanie dzieci. Jest on najwyższy od roku 2016 pomimo spadku prawie o połowę liczby zgłoszeń tego typu materiałów.

10 | CSAM analizowany przez Dyżurnet.pl – lokalizacja w usługach internetowych (n=2861)



Strona internetowa – strona www znajdująca się w otwartych zasobach internetu.

Hosting plików – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie, oglądanie i pobieranie przez użytkowników plików różnego rodzaju.

Hosting zdjęć – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie, oglądanie i pobieranie przez użytkowników zdjęć oraz grafik.

Serwis wideo – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie i oglądanie przez użytkowników plików wideo bez konieczności ich pobierania.

Forum – fora dyskusyjne znajdujące się w otwartych zasobach internetu poświęcone określonej tematyce; mogą zawierać pliki multimedialne.

Serwis społecznościowy – serwis, w ramach którego użytkownicy zakładają własne profile i dzielą się zamieszczanymi przez siebie treściami z innymi użytkownikami.

Strona z maskowaniem treści – strona www znajdująca się w otwartych zasobach internetu, wyświetlająca ukrytą treść po wprowadzeniu odpowiedniego odsyłacza *(http referrer)* lub pliku *cookie*.

TOR *(The Onion Router)* – zasoby znajdujące się w zanonimizowanej sieci TOR, dostępne wyłącznie za pomocą dedykowanej przeglądarki; większość powyższych usług internetowych może mieć swój odpowiednik w sieci TOR. Adresy zasobów w sieci TOR (tzw. *hidden services*) zawierają pseudodomenę najwyższego poziomu „*.onion*".

W porównaniu do roku ubiegłego spadł udział stron z maskowaniem treści (z 19 do 10 procent) oraz hostingu zdjęć (z 15 do 11 procent). Zwiększył się natomiast udział serwisów hostingu plików multimedialnych (z 24 do 35 procent) oraz serwisów video (z 1 do 3 procent). Pozostałe udziały nie zanotowały większych zmian.

Z ogólnej liczby 2861 adresów URL, pod którymi eksperci Dyżurnet.pl zidentyfikowali CSAM, 2674 było unikalnych. Innymi słowy, powtórzenia stanowiły 7 procent ogólnej liczby incydentów CSAM i wartość ta jest identyczna jak w roku poprzednim. Większy udział w powtórzeniach mają strony maskujące swoją treść (17 procent powtórzeń). Wynika to z faktu, że wyświetlana na takiej stronie treść zależy od wprowadzenia odpowiedniego odsyłacza (adresu URL), który może się zmieniać w czasie. Dlatego takie strony mogą być raportowane wielokrotnie.

11 | CSAM analizowany przez Dyżurnet.pl – liczba plików foto/wideo analizowanych przez Dyżurnet.pl i rozpoznanych już wcześniej przez zespoły INHOPE

1 677
33%
Rozpoznane wcześniej przez zespoły INHOPE

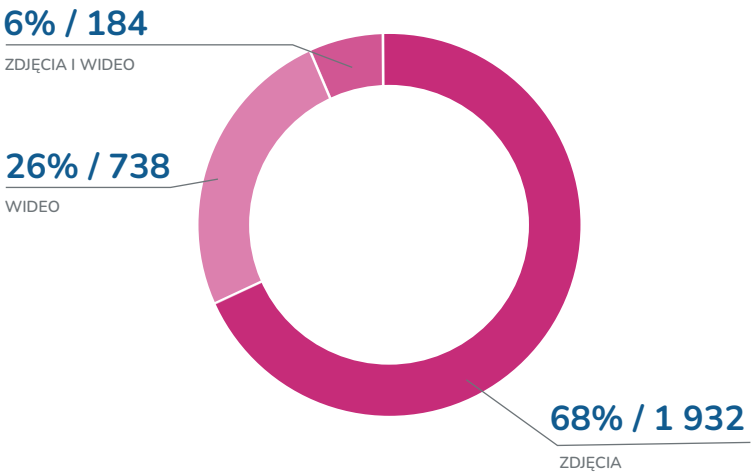
3 340
67%
Analizowane po raz pierwszy przez Dyżurnet.pl

Baza ICCAM opiera się na rozpoznawaniu *hash value* (cyfrowego odcisku) plików. Dane te uzyskiwane są poprzez zastosowanie funkcji skrótu, pozwalającej na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych

zbiorów danych. Obrazy i filmy, które zostały zanalizowane i odpowiednio zaklasyfikowane nie są już wyświetlane przy ponownym wprowadzeniu do bazy ICCAM. Dzięki temu rozwiązaniu unika się powielania pracy analityków i poddawania ich czynnikom stresogennym wynikającym z analizy treści, a sama analiza przebiega szybciej.

W roku 2021 udział treści analizowanych po raz pierwszy przez Dyżurnet.pl wynosił 40 procent, co świadczy o pojawieniu się dużej ilości nowo wytworzonych materiałów ukazujących dzieci w trakcie czynności seksualnych.

12 | CSAM analizowany przez Dyżurnet.pl – rodzaj treści (n=2854)



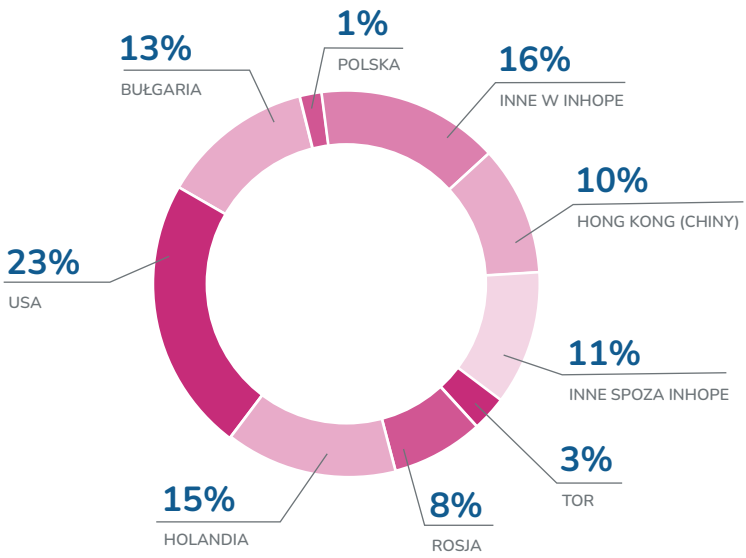
Po raz pierwszy w przedstawionej statystyce dotyczącej rodzaju treści CSAM nie ma kategorii „tekst". Wynika to ze zmiany spowodowanej orzeczeniem Sądu Najwyższego, gdzie mowa o nielegalności „jakiegokolwiek materiału, który **wizualnie** przedstawia dziecko uczestniczące w rzeczywistej lub udawanej czynności wyraźnie seksualnej lub jakiekolwiek przedstawiania narządów płciowych dziecka głównie w celach seksualnych"[2].

41 incydentów z ogólnej liczby 2 861 dotyczyło treści przedstawiających wytworzony lub przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej. Takie zazwyczaj wygenerowane komputerowo i względnie

2. Postanowienie SN z 15.01.2020 r., V KK 655/19, LEX nr 2777419

realistycznie wyglądające treści, w wielu państwach nie są uznawane za nielegalne, dlatego ciągle są obecne w internecie.

13 | CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do adresów URL (n=2861)

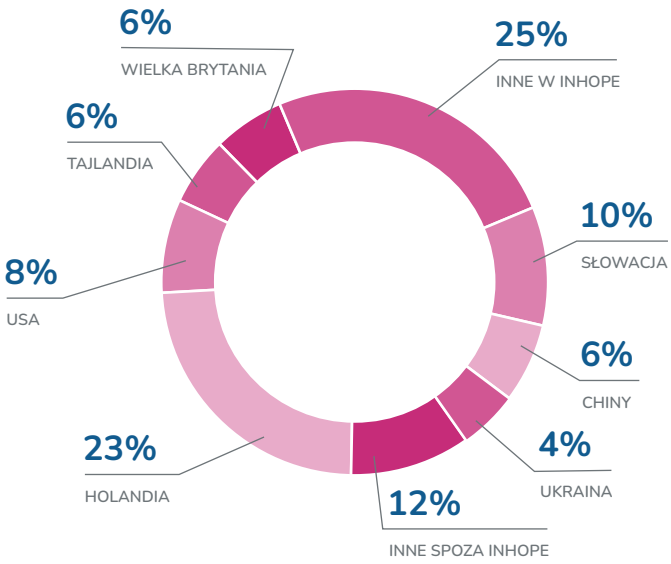


Lokalizacja serwera z treścią CSAM jest kluczowa dla skutecznej reakcji. Zespół Dyżurnet.pl wyróżnia dwa rodzaje lokalizacji:

- w odniesieniu do adresu URL,
- w odniesieniu do plików foto/wideo.

Przykładowo – strona internetowa znajduje się na serwerze zlokalizowanym w USA. Lokalizację tego typu pokazuje wykres nr 13. Jednak nielegalne pliki foto lub wideo wyświetlane przez tę stronę znajdują się na serwerach innych państw, np. Holandii lub USA. Lokalizację plików CSAM pokazuje wykres nr 14.

14 | CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do plików foto/wideo (n=3340)



Rok 2022 był kolejnym, w którym eksperci Dyżurnet.pl zauważyli coraz częstsze lokowanie stron oraz plików z treściami CSAM poza zasięgiem działalności zespołów reagujących zrzeszonych w Stowarzyszeniu INHOPE.

W odniesieniu do adresów URL w roku 2022 było to 24 procent (2021 - 23 procent, 2020 – 7 procent, 2019 – 11 procent).

W odniesieniu do plików foto/wideo w roku 2022 było to 32 procent (2021 - 10 procent, 2020 i 2019 – po 4 procent). Na duży wzrost liczby plików poza zasięgiem Stowarzyszenia INHOPE niewątpliwie wpłynęło opuszczenie Stowarzyszenia przez zespół ze Słowacji. W roku 2023 Słowacja ma ponownie dołączyć do INHOPE z nowo utworzonym zespołem.

Rok 2022 był pierwszym kiedy obowiązywały nowe standardy i procedura pozwalająca określonym zespołom Stowarzyszenia interweniować bezpośrednio u zagranicznego hostingodawcy w celu usunięcia treści CSAM. Niewątpliwie wpływa to na zwiększenie odsetka treści CSAM, które są usuwane z serwerów.

15 | CSAM analizowany przez Dyżurnet.pl – podział ze względu na kategorię treści (n=3340)

48%

National CSAM

52%

Baseline CSAM

Baseline CSAM (kryteria nielegalności we wszystkich państwach współpracujących z Interpolem):

- Obraz prawdziwego, realnego dziecka. Obrazy wygenerowane komputerowo, narysowane lub w jakikolwiek inny sposób wytworzone czy przetworzone nie są uwzględniane.
- Dzieci przedstawione w sytuacjach seksualnego wykorzystania są w okresie przedpokwitaniowym (nie osiągnęły 13 r.ż.).
- Przedstawienie sytuacji seksualnego kontaktu lub zogniskowanie na rejonie genitalnym lub analnym dziecka.

National CSAM

- Treści o charakterze pornograficznym z udziałem osób małoletnich powyżej 13 r.ż. (treści z osobami młodszymi klasyfikowane są jako Baseline CSAM).
- Treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej.

W roku 2022 odsetek najbardziej drastycznych treści kategorii Baseline spadł z 57 do 52 procent w porównaniu do 2021 roku.

16 | CSAM analizowany przez Dyżurnet.pl – udział treści o charakterze pornograficznym wytworzonych przez ofiary (*self-generated sexual content*) (n=2861)

2 444

85%

non self-generated content;

417

15%

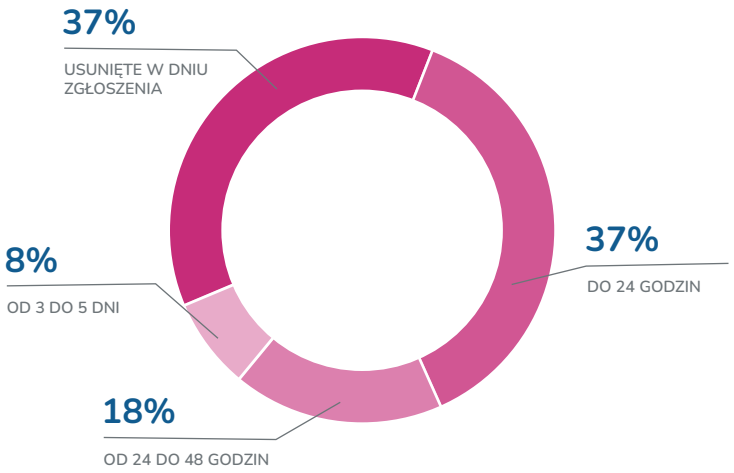
self-generated content;

Self-generated sexual content – materiał foto/wideo wytworzony samodzielnie przez osobę małoletnią, uzyskany za jej zgodą lub bez jej zgody, przedstawiający ją w trakcie czynności o charakterze seksualnym. Więcej na ten temat znajduje się w naszej publikacji *Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki*[3].

Po chwilowym spadku udziału tego typu materiałów w roku 2021 do 8 procent, rok 2022 przyniósł powrót do procentu zbliżonego do tego, jaki eksperci Dyżurnet.pl obserwowali w roku 2019. Wtedy było to 14 procent, w roku 2022 – 15 procent, a liczba incydentów tego typu wzrosła przeszło dwukrotnie. Warto zaznaczyć, że pojedyncze incydenty zazwyczaj dotyczą forów, na których umieszczane są tysiące tego typu materiałów, wytwarzanych zarówno przez nastolatki, jak i dzieci w wieku wczesnoszkolnym. Pod tym względem eksperci obserwują coraz wcześniejszą „inicjację" w tworzeniu przez dzieci treści o charakterze seksualnym.

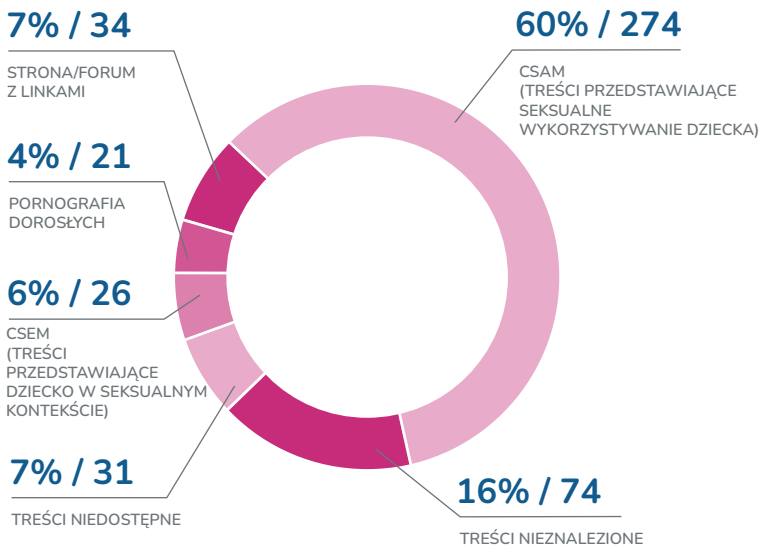
3. https://dyzurnet.pl/uploads/2020/04/Ryzykowne_zachowania_na_www.pdf

17 | Czas publicznej dostępności CSAM/CSEM zlokalizowanych w Polsce i zgłoszonych do Dyżurnet.pl przez inne zespoły INHOPE (n=40)



W roku 2022 polscy hostingodawcy wydłużyli proces usuwania treści CSAM ze swoich serwerów po zawiadomieniu przez Dyżurnet.pl. O ile liczba treści usuniętych w dniu zawiadomienia pozostaje zbliżona do tej z roku 2021 (38 procent, obecnie 37), to już procent treści usuniętych w przeciągu 24 godzin spadł z 54 do 37 procent. Niestety wzrostowi uległy udziały treści usuwanych od 24 do 48 godzin (z 5 do 18 procent) oraz od 3 do 5 dni (z 3 do 8 procent). **Istotne jest, że 100 procent treści zgłoszonych do Dyżurnet.pl przez inne zespoły INHOPE zostało usuniętych z internetu**.

18 | Klasyfikacja stron maskujących swoją treść (n=460)



Liczba stron maskujących swoją treść analizowanych przez zespół Dyżurnet.pl w roku 2022 wyniosła 460 i była mniejsza niż w latach ubiegłych (rok 2021 – 752, rok 2020 – 784).

Ekspertom Dyżurnet.pl udało się odblokować ukrytą treść w 73 procentach, co jest wynikiem lepszym o 3 procent niż w roku poprzednim (jako odblokowaną traktuje się stronę, która wyświetliła treść z następujących kategorii: CSAM, CSEM, strona/forum z linkami).

Od roku 2020 dostępna jest do pobrania wtyczka do raportowania dla przeglądarek Chrome i Firefox. Wtyczka ta została opracowana specjalnie do zgłaszania stron maskujących swoją treść. W roku 2022 Dyżurnet.pl za jej pomocą otrzymał 240 zgłoszeń, a dzięki zawartym tam informacjom o odsyłaczu, ekspertom Dyżurnet.pl udało się odblokować 99 stron. Liczba ta stanowi jedną trzecią wszystkich odblokowanych stron maskujących swoją treść. Dla porównania w roku 2021 było to zaledwie 12 procent.

Doceniając pomoc zgłaszających w zwalczaniu maskowanych stron, niezmiennie apelujemy o częstsze korzystanie właśnie z tego sposobu raportowania treści CSAM.

19 | Udział stron maskujących swoją treść odblokowanych dzięki informacjom przekazanym poprzez wtyczkę do raportowania (n=297)

99
33%

odblokowane dzięki informacjom z wtyczki

198
67%

odblokowane przez ekspertów Dyżurnet.pl

Działania podejmowane przez Dyżurnet.pl wobec nielegalnych i szkodliwych treści

Od 2015 roku zespoły reagujące zrzeszone w INHOPE korzystają ze zintegrowanej bazy wymiany informacji dotyczących CSAM. Baza ICCAM pozwala na klasyfikację plików foto i wideo zamieszczonych pod określonym adresem URL Materiały klasyfikowane są ze względu na cechy ofiary, takie jak płeć oraz przybliżony wiek. Najistotniejsze jest **rozpoznanie materiałów stanowiących treść nielegalną we wszystkich krajach zrzeszonych w INHOPE (*baseline*).** Informacja o najbardziej drastycznych materiałach przekazywana jest bezpośrednio do bazy ICSE (*International Child Sexual Exploitation databse*[4]), umożliwiając podjęcie działań w celu identyfikacji zarówno ofiar, jaki i sprawców.

W roku 2022 eksperci Dyżurnet.pl wprowadzili do ICCAM 2 322 raporty dotyczące adresów URL zawierających nielegalne treści. Znalazło się tam ogółem **5 017** plików graficznych i nagrań wideo zaklasyfikowanych jako treść przedstawiająca seksualne wykorzystanie dziecka.

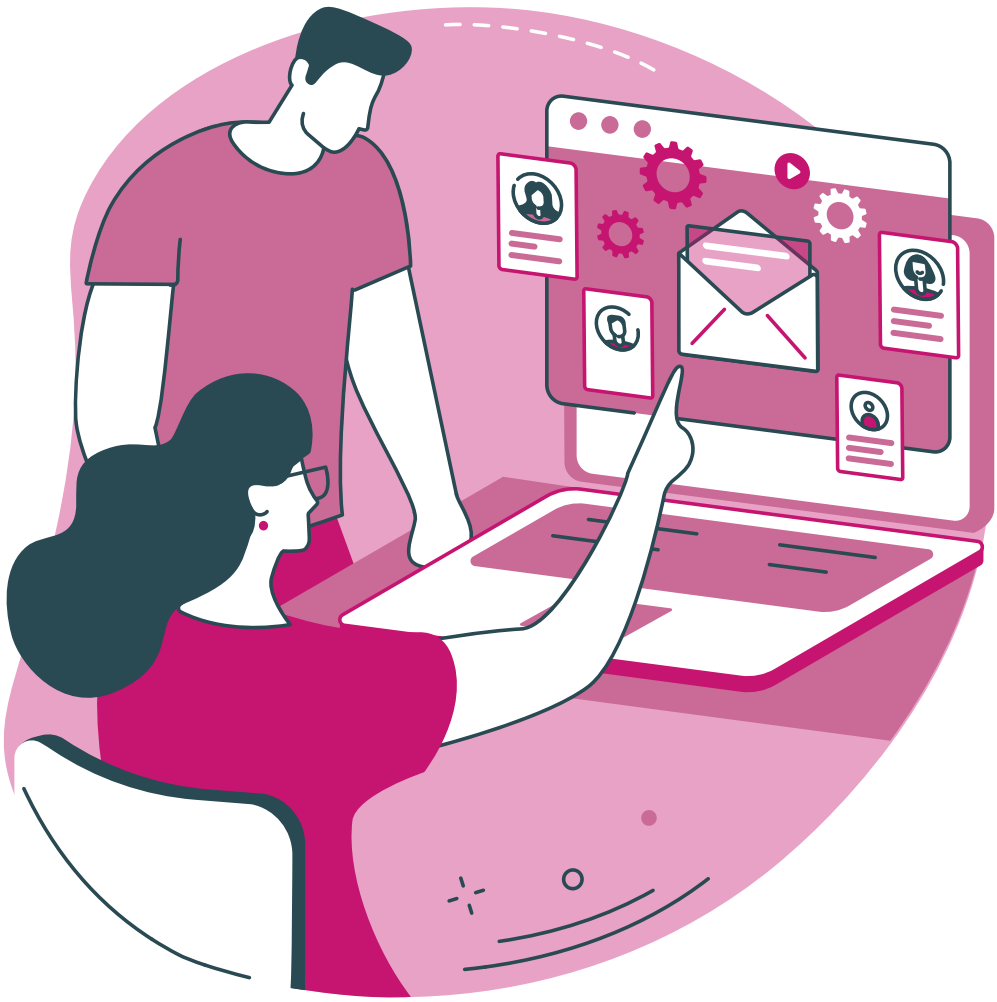
Drugą najczęstszą metodą interwencji podejmowaną przez ekspertów Dyżurnet.pl jest **bezpośredni kontakt z moderatorami, administratorami, właścicielami serwisów lub autorami treści.** Dotyczy to zazwyczaj treści legalnych, ale naruszających regulamin lub zasady społeczności. Taka interwencja podejmowana jest zarówno wobec stron polskich, jak i zagranicznych i w roku 2022 miała miejsce w przypadku **290** incydentów, a zgłaszane treści są usuwane bądź przenoszone do odpowiednich kategorii

W **55** przypadkach zespół Dyżurnet.pl kontaktował się bezpośrednio z hostingodawcami w celu poinformowania o treściach bezprawnych (dotyczących CSAM) znajdujących się na ich serwerach. Publiczny dostęp do treści zostaje zablokowany, a odpowiednie dane zostają zabezpieczone na potrzeby działań organów ścigania, które również są powiadamiane.

Ze względu na zakres wykraczający poza ramy działalności Dyżurnet.pl **182** sprawy zostały przekazane innym podmiotom - m.in. działającym w ramach NASK-PIB zespołom CERT Polska lub zespołowi przeciwdziałającemu dezinformacji czy telefonom interwencyjnym prowadzonym przez Fundację Dajemy Dzieciom Siłę.

4. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

167 incydentów zostało zgłoszonych do utworzonego w roku 2022 Centralnego Biura Zwalczania Cyberprzestępczości KGP. Dotyczyły one przede wszystkim seksualnych nadużyć wobec dzieci. Zgłoszenia związane z CSAM stanowiły 77 procent przekazanych incydentów (na polskich serwerach – 22 procent, w polskojęzycznych serwisach – 5 procent, w sieci TOR – 50 procent). 10 procent przesłanych spraw dotyczyło propagowania pedofilii i innych spraw powiązanych z pedofilską aktywnością użytkowników internetu. 13 procent pozostałych spraw zgłoszonych do Policji obejmowało inne treści znajdujące się na serwerach w Polsce (sprawy związane z zagrożeniem życia, sprzedażą narkotyków czy treściami o charakterze rasistowskim).

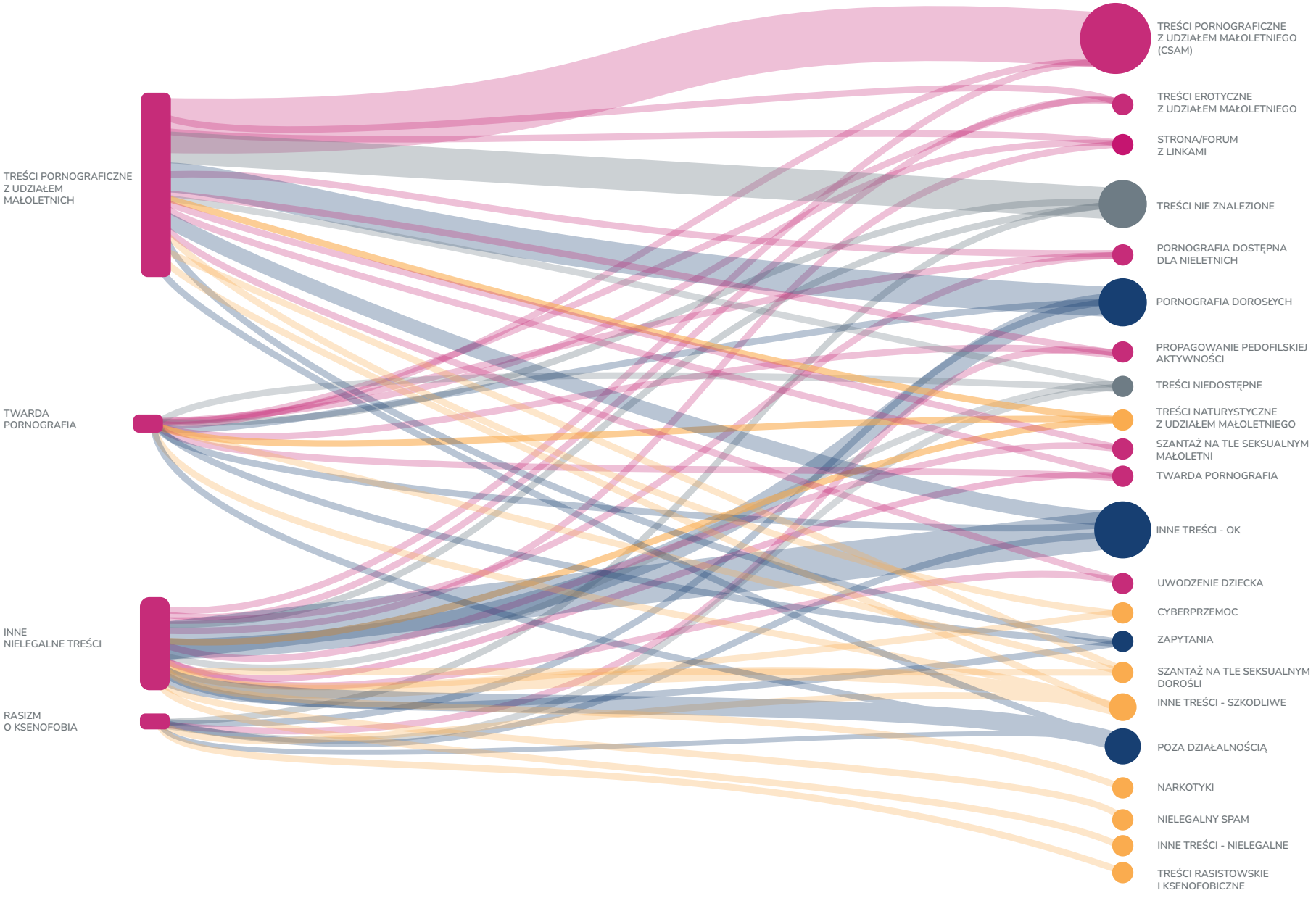


Zgłoszenia dotyczące treści legalnych

Wszystkie otrzymane przez zespół zgłoszenia są analizowane indywidualnie, a każdy taki przypadek znajduje swoje odzwierciedlenie w utworzonych incydentach, a co za tym idzie – w ich liczbie i rozkładzie kategorii. W ten sposób zgłoszenia dotyczące wyników wyszukiwania, które obejmują zupełnie nieszkodliwe i legalne treści, wpływają w znaczący sposób na końcowe statystyki dotyczące funkcjonowania zespołu.

Poniższy wykres przedstawia rozkład zgłoszeń dokonywanych przez użytkowników między kategorie przypisywane przez analityków zespołu Dyżurnet.pl po analizie zgłoszenia. Jak widać, znaczną część klasyfikowanych materiałów stanowią treści neutralne (inne treści – ok), które zgłaszane są przez użytkowników jako treści nielegalne, jednak w rzeczywistości nie tylko nie łamią w żaden sposób prawa, ale również nie można ich uznać za treści szkodliwe. Spora część zgłoszeń dotyczy również kwestii wykraczających poza ramy działalności zespołu, czyli w szczególności sytuacji, w których prawo zostało złamane, jednak ściganie sprawcy następuje wyłącznie na wniosek poszkodowanego.

W niektórych przypadkach również po analizie zgłoszeń treści potencjalnie przedstawiających seksualne wykorzystywanie dzieci okazuje się, że zgłaszane materiały nie są materiałami CSAM, ale pornografią z udziałem osób dorosłych – a więc materiałami legalnymi.


TREŚCI PORNOGRAFICZNE Z UDZIAŁEM MAŁOLETNICH
TWARDA PORNOGRAFIA
INNE NIELEGALNE TREŚCI
RASIZM O KSENOFOBIA
TREŚCI PORNOGRAFICZNE Z UDZIAŁEM MAŁOLETNIEGO (CSAM)
TREŚCI EROTYCZNE Z UDZIAŁEM MAŁOLETNIEGO
STRONA/FORUM Z LINKAMI
TREŚCI NIE ZNALEZIONE
PORNOGRAFIA DOSTĘPNA DLA NIELETNICH
PORNOGRAFIA DOROSŁYCH
PROPAGOWANIE PEDOFILSKIEJ AKTYWNOŚCI
TREŚCI NIEDOSTĘPNE
TREŚCI NATURYSTYCZNE Z UDZIAŁEM MAŁOLETNIEGO
SZANTAŻ NA TLE SEKSUALNYM MAŁOLETNI
TWARDA PORNOGRAFIA
INNE TREŚCI - OK
UWODZENIE DZIECKA
CYBERPRZEMOC
ZAPYTANIA
SZANTAŻ NA TLE SEKSUALNYM DOROŚLI
INNE TREŚCI - SZKODLIWE
POZA DZIAŁALNOŚCIĄ
NARKOTYKI
NIELEGALNY SPAM
INNE TREŚCI - NIELEGALNE
TREŚCI RASISTOWSKIE I KSENOFOBICZNE

Trendy

i zjawiska

Grooming a napastowanie seksualne

Uwodzenie dziecka przez internet, czyli online *child grooming* w kodeksie karnym penalizowane jest w artykułach 200 oraz 200a. Uwzględniają one sytuacje, w których osoba poniżej 15 lat otrzymuje treści pornograficzne, propozycje wykonywania czynności seksualnych lub też propozycje spotkania w tymże celu. W Polsce i na świecie powstało dotąd wiele badań nad tym zjawiskiem, wskazujących przede wszystkim na jego powszechność oraz zróżnicowanie zachowań sprawców.

W klasycznym rozumieniu[5] grooming jest zjawiskiem rozciągniętym w czasie, gdzie sprawca przechodzi przez kilka podstawowych etapów interakcji, najpierw starając się zdobyć zaufanie i przyjaźń dziecka, a dopiero potem przechodząc do treści seksualizujących i bezpośrednich propozycji. Jednak fazy te nie muszą być równej długości, niekoniecznie występują w tej kolejności, a nawet nie zawsze występują wszystkie naraz. Według analiz rozmów na czatach w języku angielskim[6] [7], tylko w 2 z 44 badanych rozmów wystąpiły wszystkie z technik manipulacyjnych charakterystycznych dla konkretnych etapów, lecz w każdej pojawiła się co najmniej jedna. Średnio używano około pięciu.

5. *O'Connell, R. (2003). A typology of child cybersexploitation and online grooming practices.,* http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf

6. Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). *A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. Child abuse & neglect, 44,* 140-149. https://www.sciencedirect.com/science/article/pii/S0145213414004360

7. http://www.perverted-justice.com/ rozmowy sprawców przemocy seksualnej z osobami podającymi się za nieletnich

Badania NASK

Powszechność zjawiska potwierdzają raporty z badań NASK – *Nastolatki 3.0*[8], *Nastolatki wobec pornografii cyfrowej*"[9] oraz projektu *#nienapokaz*[10]. Wyniki pokazują, że około 24% badanych 16-latków i 9% 12- i 14-latków wysłało zdjęcia intymne – przy czym niemal dwukrotnie więcej otrzymywało propozycje przesłania takich materiałów. Blisko 30% złożonych propozycji pojawiło się w interakcjach z anonimowymi nieznajomymi, a około 20% z obcymi dorosłymi poznanymi online.

W niedawno przeprowadzonym przez NASK badaniu jakościowym (*#nienapokaz*) uwidoczniły się pewne niepokojące trendy w interakcjach online młodzieży. Znajomości nawiązywane online służą nawiązaniu bliskich relacji towarzyskich i zdobyciu poczucia akceptacji, którego brakuje zwłaszcza młodzieży należącej do mniejszości seksualnych z mniejszych miejscowości, nieodnajdującej się wśród rówieśników. Otwiera to możliwość osobom uwodzącym dzieci na pozorne zaspokojenie tych podstawowych potrzeb młodej osoby, a następnie wykorzystanie jej. Jednak klasyczny *child grooming* nie jest jedyną formą szkodliwej interakcji, na którą narażeni są młodzi. W badaniu pojawiły się opinie na temat otrzymywanych bez ostrzeżenia materiałów o treści seksualnej lub intymnej, które budzą różne reakcje – od traumy, przez zobojętnienie, do nienaturalnie zwiększonego zainteresowania seksualnością. Ankietowana młodzież zwróciła w szczególności uwagę na szkodliwość otrzymania takich materiałów, zwłaszcza przy braku zrozumienia sytuacji, swojej seksualności i celów rozmówcy. Przy powtarzalności takich sytuacji następowało zwykle zobojętnienie na tego typu treści, połączone z krytycznymi, czasem prześmiewczymi, odczuciami wobec wysyłających.

8. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html
9. https://www.nask.pl/pl/raporty/raporty/5077,Raport-Nastolatki-wobec-pornografii-cyfrowej.html
10. https://dyzurnet.pl/uploads/2022/02/Publikacja-Nie-na-pokaz.pdf

Dane Dyżurnet.pl

Analiza danych przeprowadzona przez zespół Dyżurnet.pl wykazała transformację procesu *child groomingu* z ostrożnego i powolnego uwodzenia osób małoletnich na bardziej gwałtowny, szybko przechodzący do żądań seksualnych (*online solicitation* – napastowanie seksualne online). Tutaj przytoczyć można kilka wybranych taktyk przestępców seksualnych i przykłady niepokojących interakcji, które szczególnie zwróciły uwagę ekspertów.

Młodzi ludzie spotykają się z sytuacjami, gdzie wysłane jest im zdjęcie męskich genitaliów bez żadnego wcześniejszego ostrzeżenia, a nachalne intymne pytania następują już w pierwszych wiadomościach konwersacji. Takie pytania oraz żądanie intymnych materiałów może pokazywać czy dana osoba odpowiada preferencjom sprawcy i czy jej deklarowany wiek odpowiada rzeczywistości – przy czym zdarza się, że zdjęć rozmówcy żądają także dzieci, które często nie mają chęci rozmawiać ze starszą osobą.

Wiele kampanii profilaktycznych podkreśla, że sprawcy przestępstw podają się za rówieśników. Jednak, jak pokazuje praktyka, sprawcy często nie ukrywają swojego wieku lub zaniżają go nieznacznie. Młoda osoba może być jednak potencjalnie bardziej skłonna do nawiązania relacji z rówieśnikiem niż z osobą dorosłą, pomimo alarmującego sposobu prowadzenia konwersacji (np. w sposób nacechowany seksualnie). W niektórych rozmowach wykazujących cechy *child groomingu* analizowanych przez Dyżurnet.pl dziecko nie zawsze wykazuje odpowiednią ostrożność i kontynuuje rozmowę, akceptując problemy sprzętowe „koleżanki" z aparatem czy kamerką, a nawet odpowiada na namowy i realizuje seksualizujące czynności. Zdarza się też, że sprawca buduje niespójny profil i w trakcie rozmowy podaje kilka różnych danych, np. dotyczących swojego wieku. To kolejne wskazówki, które mogą wzbudzić nieufność młodych osób, podobnie jak zdjęcia lub połączenia audio bądź wideo, na których trudniej zafałszować zbyt niski głos lub poważniejszy wygląd.

Jednak napastnik może odwrócić taką nieufność na swoją korzyść, jako pierwszy pytając, czy dziecko nie jest „fejkiem", podstawionym dorosłym-prowokatorem. Jest to okazja do zażądania zdjęć dziecka, czasem w większej liczbie – a następnie oskarżenia dziecka o ściągnięcie zdjęcia z internetu. Jeśli sytuacja potoczy się po myśli napastnika, może on zażądać specyficznej aranżacji i przygotowania zdjęcia np. ustawienia ciała lub zdjęć intymnych. Dziecko, którego szczerość została zakwestionowana, może w ten sposób zostać zmanipulowane, aby bronić się przed oskarżeniami, a jednocześnie przesuwać granice bezpiecznego zachowania w internecie.

Nagłe przejście do tematyki seksualnej jest szczególnie charakterystyczne dla profili ewidentnie zagranicznych, posługujących się niedoskonałym automatycznym tłumaczeniem wiadomości na język polski – na ich tłumaczenie z innego języka może wskazywać niestandardowy sposób budowania zdań, niepoprawność gramatyczna, a czasem i pojedyncze słowa w obcym języku, które przez przypadek nie zostały przetłumaczone. Inne jest także użycie emotikonów; osoby polskojęzyczne używają ich raczej oszczędniej – żartobliwie albo w późniejszej, nastawionej na relację romantyczną fazie rozmowy – zaś konta spamujące seksualnymi propozycjami używają ich w dużej ilości od samego początku. Pojawiają się tu ikony telefonu, bakłażana, brzoskwini, ust i serc, w zależności od wystosowywanych próśb. Nachalność wiadomości i niskie umiejętności prowadzenia dialogu sprawiają wrażenie rozmowy z botem lub półautomatycznym systemem, nienastawionym na budowanie relacji z dzieckiem, a raczej na zarzucenie szerokiej sieci na jak najwięcej młodych osób w nadziei, że chociaż niewielki procent z rozmów przyniesie zysk w postaci materiałów intymnych. Niestety, w kilku przypadkach faktycznie młodzież po nagabywaniu udostępnia swoje zdjęcia, jak tłumaczą – z nudy bądź w celu zakończenia interakcji.

Zarzucanie szerokiej sieci na młodzież jest dodatkowo ułatwiane przez algorytmy polecania znajomych[11] prezentujące sprawcy rówieśników młodego rozmówcy. Rozmowa z nimi może zostać uwiarygodniona poprzez posiadanie wspólnego znajomego z obcym. Także w bezpośrednich rozmowach z dziećmi zdarza się, że osoba uwodząca pyta wprost o rówieśników, na przykład o koleżanki, które potencjalnie byłyby zainteresowane wysyłaniem zdjęć bądź rozmową. Czasami dziecko spełnia rolę mediatora między dorosłym a koleżanką (rzadziej kolegą – jak wynika z danych dostępnych Dyżurnet.pl), przekazując prośby o kontakt, dodanie do znajomych lub odblokowanie.

11. https://www.riskyby.design/friend-suggestions

Grooming jako zjawisko rozproszone

Ze względu na opisane powyżej mechanizmy (a także wiele innych spełniających podobne funkcje), które występują w wielu interakcjach z różnymi ludźmi na przestrzeni lat, można mówić o „rozproszonym groomingu". Dzieci są przyzwyczajane do tematyki seksualnej nie przez jedną osobę, lecz przez wiele osób, które nękają równolegle wiele kont należących do młodych użytkowników, w nadziei, że choć kilkoro z nich odpowie w oczekiwany sposób – i często się tak dzieje. Analizowane rozmowy są przykładem konwersacji, w których dziecko nie potrafiło lub nie chciało zablokować rozmówcy i sytuacja rozwijała się w niebezpiecznym kierunku. Szczególnie u młodzieży stykającej się z tego typu napastnikiem po raz pierwszy często było widoczne zbytnie przywiązanie do konieczności usprawiedliwienia się lub wyjaśnienia sytuacji, podczas gdy drugiej stronie zależało wyłącznie na korzyściach seksualnych – co czyniło wszelkie dyskusje bezproduktywnymi.

Zatem wyuczone ignorowanie zaczepek sygnalizowane zarówno przez młodzież w badaniach, jak i bezpośrednio w analizowanych przez Dyżurnet.pl rozmowach ze sprawcami, może stanowić mechanizm obronny przed skrzywdzeniem – jednak nie bez znaczenia jest fakt, w jakich okolicznościach została wypracowana ta umiejętność.

Handel materiałami intymnymi

Wśród zgłoszeń analizowanych przez Dyżurnet.pl znajdują się treści nazywane *self-generated sexual content*, czyli materiały o charakterze seksualnym tworzone przez samego użytkownika. Z przeprowadzonego w drugiej połowie 2021 roku badania NASK *Nastolatki wobec pornografii cyfrowej* wynika, że 26 procent nastolatków otrzymało propozycję wysłania własnego zdjęcia o charakterze seksualnym. Niemal połowa takich próśb pochodziła od osób anonimowych czy takich, których ankietowani nie znają osobiście w „realnym" świecie. Co więcej, 24 procent badanych w wieku 16 lat oraz 9 procent w grupie 12 i 14 lat zdecydowało się na wysłanie własnego nagiego lub półnagiego zdjęcia czy filmu[12].

Motywacje wysyłania takich materiałów przez nastolatków mogą być różne, co szerzej opisuje opublikowana w 2022 roku publikacja *Nie na pokaz. Analiza wyników badania dotyczącego treści intymnych publikowanych przez młodzież*[13]. Przykładowo – osoby będące w związku i wysyłające sobie wzajemnie takie materiały, często wykazywały przekonanie o braku zagrożeń z tym związanych. Łączą to bowiem ze wzajemnym zaufaniem i oddaniem wynikającym z wiążącego ich uczucia. W przypadku wysyłania intymnych zdjęć czy filmów obcym osobom, wymieniane było chociażby dążenie do zyskania akceptacji czy komplementów.

Jednak niezależnie od tego, jakie były motywy takich aktywności, młode osoby zdają się zapominać o możliwych konsekwencjach wycieku materiałów intymnych, który nastąpi w następstwie ich wysłania. Sytuacja, w której samodzielnie wytworzona treść o charakterze seksualnym trafia do osoby, dla której nie była ona przeznaczona, może okazać się niezwykle niebezpieczna dla twórcy takiej treści, który staje się wtedy de facto ofiarą przestępstwa.

W kontekście dzielenia się intymnymi materiałami w związku, należy pamiętać o możliwości wystąpienia zjawiska *revenge porn*. Tak nazywa się upublicznianie – często jako forma zemsty za porzucenie przez drugą stronę – wspomnianych

12. https://www.nask.pl/pl/raporty/raporty/5077,Raport-Nastolatki-wobec-pornografii-cyfrowej.html
13. https://dyzurnet.pl/uploads/2022/02/Publikacja-Nie-na-pokaz.pdf

treści otrzymanych uprzednio od byłego już partnera. Wśród zgłoszeń trafiających do Dyżurnet.pl pojawiały się prośby o pomoc w usunięciu zdjęć dystrybuowanych na przykład w formie postów czy komentarzy na portalach społecznościowych.

Innym zagrożeniem jest wyciek materiałów intymnych na skutek wysłania ich osobie nieznanej i posługującej się fałszywą tożsamością. Takie osoby często nawiązują w internecie kontakt z małoletnimi, podszywając się pod ich rówieśników i posługując się wcześniej wykradzionymi zdjęciami – także intymnymi – w celu uwiarygodnienia. Budują zaufanie u swojej ofiary, aby po czasie pozyskać od niej materiały o charakterze seksualnym. Młodzi ludzie myślą, że wysyłają je osobie zainteresowanej zbudowaniem bliższej relacji, chociażby w świecie wirtualnym. W rzeczywistości mogą korespondować jednak z członkami zorganizowanych grup przestępczych, którzy kolekcjonują wspomniane nielegalne materiały w celach zarobkowych. Po otrzymaniu zdjęć czy filmów korespondencja może – niespodziewanie dla ofiary – urwać się, bądź sprawca dodatkowo może posunąć się do szantażu na tle seksualnym. Grożąc upublicznieniem materiałów, będzie żądał wynagrodzenia lub przesyłania kolejnych, coraz odważniejszych treści.

Tak pozyskane treści są następnie nielegalnie udostępniane w serwisach oferujących hosting plików. Pakowane są w archiwa lub foldery, zabezpieczane hasłem i wyceniane. W serwisach społecznościowych (także tych popularnych) umieszczane są oferty sprzedaży tych materiałów. Pojawiają się swoiste katalogi, rozróżniające foldery według płci czy wieku osób przedstawionych na zdjęciach lub filmach. Należy zauważyć, że na wspomnianych portalach nie pojawiają się same treści, a jedynie ich opis – co więcej, najczęściej podany skrótowo lub enigmatycznie. Uzyskanie dostępu do nielegalnych materiałów wymaga kontaktu z przestępcą w prywatnych wiadomościach, w których instruuje on jak dokonać płatności, po której wysyłane są link i hasło do folderu czy archiwum. Najczęściej wymagana jest płatność za pomocą kryptowaluty lub innego systemu zapewniającego anonimowość.

Dzięki szybkiej reakcji i współpracy danej platformy, usunięcie materiałów udostępnionych przez byłego partnera lub partnerki w formie zemsty może zminimalizować ryzyko negatywnych konsekwencji dla ofiary wycieku. Jednak w przypadku wycieku w celu nielegalnej sprzedaży, sytuacja jest bardziej złożona. Materiały, które trafiają w ręce przestępców, są wielokrotnie kopiowane. Po usunięciu ich z jednej platformy czy serwera, są udostępniane na innych. Sposób ich dystrybucji jest zawiły, co wydłuża dotarcie do przestępcy. Konta oferujące sprzedaż nielegalnych materiałów są raportowane do platform, na których działają – a w konsekwencji blokowane i zgłaszane do organów ścigania właściwych dla kraju operowania. Jednakże często na ich miejsce powstają nowe. Podobny schemat występuje przy udostępnianiu nowych kopii materiałów w nowych miejscach.

Warto pamiętać, że każde udostępnienie takiej treści to w praktyce kolejne upublicznienie zapisu przestępstwa. Wiele młodych osób wysyłających nieznajomym lub nowo poznanym osobom intymne materiały nie zdaje sobie sprawy z niebezpieczeństwa, jakim jest stanie się częścią opisanego procederu. Dlatego ważna jest edukacja w tej kwestii, a także intensywna współpraca organów ścigania, platform internetowych i zespołów reagujących w celu sprawnego rozpoznawania i usuwania nielegalnych materiałów w internecie.

Serwisy komunikacyjne o strukturze rozproszonej

Rok 2022 przyniósł zwiększoną liczbę zgłoszeń dotyczących zdecentralizowanych platform komunikacyjno–streamingowych, zaprojektowanych początkowo jako forma komunikatorów dla graczy komputerowych. Platformy te oparte są na rozproszonej strukturze, czyli takiej, w której portal znajduje się na więcej niż jednym serwerze (głównie na terenie Stanów Zjednoczonych). Umożliwiają one zakładanie zarówno publicznych, jak i prywatnych kanałów komunikacyjnych. Ze względu na fakt, że platformy te udostępniają jedynie narzędzie, to głównie do użytkowników będących administratorami poszczególnych kanałów należy tworzenie swoistych regulaminów – a w następstwie determinowanie charakteru udostępnianych na kanałach treści. Nielegalne materiały, pojawiające się na niektórych kanałach ze względu na brak moderacji, można podzielić na trzy grupy.

1 | Pierwszy typ incydentów dotyczy materiałów CSAM (zawierających treści prezentujące seksualne wykorzystywanie dzieci), które najczęściej przemieszane są z materiałami pornograficznymi przedstawiającymi osoby dorosłe. Jest to forma kamuflowania nielegalnych treści CSAM. Materiały tego typu są zazwyczaj częściowo publikowane na kanale z możliwością wykupienia dostępu do większej ich ilości zgromadzonej na zewnętrznym serwerze hostingowym.

2 | Drugi typ incydentów stanowią treści pornograficzne z udziałem osób dorosłych rozpowszechniane na kanałach platformy, do których mają dostęp osoby małoletnie lub wręcz na kanałach specjalnie przeznaczonych dla dzieci.

System komunikacyjny z takimi platformami rodzi szereg problemów dotyczących zarówno weryfikacji oraz raportowania nielegalnych treści, jak i pozyskiwania danych o polskojęzycznych potencjalnych sprawcach przez polskie organy ścigania.

- Aby wejść na prywatny kanał, potrzebne jest spersonalizowane zaproszenie od jego uczestnika. Zaproszenia te posiadają krótki, około 2-3 dniowy termin ważności. Oznacza to, że przesłane zgłoszenie o nielegalnych treściach do organów ścigania jest często niemożliwe do zweryfikowania.

- Polskojęzyczne grupy mogą znajdywać się na amerykańskich serwerach przez co, ze względu na specyficzny stan prawny, polska policja ma problem z ich wykryciem.

- Opisywane platformy nie posiadają programu *Trusted Flaggers*, który zakłada priorytetowe traktowanie zgłoszeń pochodzących od tak zwanych zaufanych podmiotów sygnalizujących – takim podmiotem mógłby być zespół reagujący na nielegalne treści w internecie, jakim jest Dyżurnet.pl. Z tego powodu jedynym sposobem komunikacji z administracją serwisu pozostaje ogólna forma zgłaszania nadużyć, która jest czasochłonna i nie zawsze skuteczna.

3 | Trzecim rodzajem incydentów są zewnętrzne strony, tak zwane CAP Sites, funkcjonujące na zasadzie zaproszeń. Na takich stronach umieszczane są materiały przedstawiające seksualne wykorzystywanie dzieci czy twardą pornografię. Najczęściej filmy czy zdjęcia są jednak tylko osadzone na danej stronie, podczas gdy fizycznie multimedia znajdują się na serwerach platformy komunikacyjnej, z której korzystają także dzieci. Użytkownicy zakładają konto na stronie, otrzymując pierwszy poziom dostępu. Każdy użytkownik ma możliwość rozsyłania zaproszeń na stronę – link powiązany jest z jego kontem. Po zarejestrowaniu odpowiedniej liczby użytkowników z danego linku polecającego, osobie zapraszającej przyznawane są kolejne poziomy dostępu, które odblokowują dostęp do większej liczby nielegalnych materiałów. Alarmujący jest fakt, że to właśnie wspomniana platforma komunikacyjna i kanały odwiedzane głównie przez osoby niepełnoletnie stały się jedną z podstawowych dróg dystrybucji linków zapraszających. Po pewnym czasie linki te zaczęły być rozsyłane także pomiędzy młodzieżą w formie niezwykle lekkomyślnego żartu. Do zespołu Dyżurnet.pl trafiają zgłoszenia dotyczące wyżej opisanych stron nadesłane przez – często poruszone i zaniepokojone – osoby niepełnoletnie. Poniżej zaledwie kilka przykładów zgłoszeń raportujących takie kanały (pisownia oryginalna):

*Dzień dobry... Boże Święty zawału można dostać.. jak przepraszam za zwrot – k**** można udostępniać takie rzeczy? Boże... dzieci gwałcić, seks z dzieckiem? Błagam, proszę się tym zająć... Ja mam 16 lat, przez przypadek trafiłem na to na serwerze na D***e.. przez to wszystko opuściłem ten serwer dodałem link do serwera... Proszę się tym zająć, złapać tych co to robią... chce mi się kurna płakać jak to widzę... przepraszam za słownictwo ale widząc to mam ochotę wymierzyć sprawiedliwość... Błagam, zajmijcie się tym... Nie wiem jak można takie coś robić*

Dzien dobry. Chciałbym zgłosić ważną jak nie bardzo ważną sprawę było tak że wszedłem na jakąś stronę internetową i z ciekawości się zalogowałem tam tylko trzeba było login i hasło i tyle wtedy zobaczyłem na filmiku dziecko dalej można sobie wyobrazić co było to jest smutne że są tacy ludzie co krzywdzą dzieci. Zastanawiam się cały czas o tym jak można tak robić i dlatego piszę bo nie mogę przestać o tym myśleć ale myślę że cos z tym zrobicie (...) na stronie może bylem z 5 min ale bardzo żałuję że w jakiegoś linka klikłem ale jedynie w taki sposób mogę pomóc

*Podczas przeglądania d***a natknąłem się na link z podpisem wyślij koledze aby go sprankować stwierdziłem spoko plan wysłałem koledze i nagle moje konto zostało zbanowane więc z ciekawości wszedłem w ten link myślałem że będzie to strona typu bardzo głośna muzyka z jakimś migającym obrazkiem którego nie da się zamknąć moim oczom ukazała się natomiast strona z dziecięcą pornografią. Przestraszony zamknąłem szybko stronę Po dłuższym namyśle zacząłem szukać w internecie co zrobić kiedy natknie się na to jedna że stron mówiła o opcji zgłoszenia tego na tą stronę*

*Znalazlem ten link link na jednym z serwerów *** znalezionym w internecie. Miało byc to zwykle nsfw wszedlem w ten link i po zalogowaniu zobaczylem cos czego nie powinienem. Takie rzeczy nie powinny krążyc po internecie. Na wejscie skusila mnie ciekawość i nie podejrzliwość bo w końcu to serwer *** co moze byc tam nie legalnego. Wahałem sie czy napisac (...) jednak to co sie tam dzieje przechodzi moje najśmielsze pojęcie*

*Znalazłem przez przypadek stronę z dziecięcą pornografia. Jestem graczem, użytkownikiem d***a, i ogólnie dosyć dużo używam komputera. Dzisiaj, jak każdego dnia, sprawdzałem co się dzieje na różnych serwerach, o czym piszą ludzie, próbując przyłączyć się do konwersacji. Gdy wszedłem na pewny serwer, ujrzałem na każdym z kanałów tekstowych link zamieszczony powyżej. (...) Wszedłem w link, ujrzałem panel rejestracji i zrobiłem konto*

> *(...) Gdy się zalogowałem, ujrzałem to, czego nigdy w życiu nie chciałbym widzieć. Praktycznie od razu z niej wyszedłem, ale i tak widziałem za dużo. Mam nadzieję, że tym pedofilom stojącym za tą stroną stanie się coś złego w życiu, i że bardzo prędko zostaną złapani*

Chociaż rozpoznawalność i zaufanie, którym młodzi ludzie obdarzają Dyżurnet.pl w tych przypadkach jest budująca, to są to zgłoszenia, do których należy podchodzić ze szczególną uwagą. Styczność z materiałami przedstawiającymi seksualne wykorzystywanie dzieci, szczególnie w młodym wieku może powodować wiele negatywnych emocji, niepokój czy nawet traumę. Dlatego jeśli zgłaszający pozostawia do siebie kontakt, a zespół Dyżurnet.pl posiada informację, że jest to osoba niepełnoletnia – poza informacjami o podjętych działaniach przekazywane jest jej wsparcie oraz kontakt do instytucji, gdzie może ona uzyskać pomoc psychologiczną. Jednym z takich kontaktów jest całodobowy, anonimowy telefon zaufania dla dzieci i młodzieży 116 111 (https://116111.pl). Należy tu wspomnieć o niezwykle ważnej roli rozmowy i obecności rodzica lub opiekuna w życiu dziecka – także w aspektach związanych z internetem – aby czuło ono pełne zaufanie i przekonanie o możliwości uzyskania wsparcia od osoby dorosłej w trudnych momentach.

Wyzwania we współpracy z administratorami platform społecznościowych

Nieodłącznym elementem pracy zespołu Dyżurnet.pl jest kontakt z administratorami różnego rodzaju serwisów internetowych. Są to w dużej mierze portale społecznościowe i platformy komunikacyjne.
Zagraniczne serwisy społecznościowe są w większości zarządzane przez duże korporacje, które dbając o swój wizerunek podejmują kroki, by osoby małoletnie były bezpieczne w ich przestrzeniach. Platformy te dysponują szerokim zakresem moderacji treści oraz, w większości, posiadają programy Trusted flaggers, umożliwiające takim zespołom jak Dyżurnet.pl zgłaszanie treści w specjalnym, priorytetowym trybie. Ponadto serwisy zarejestrowane w Stanach Zjednoczonych mają obowiązek raportowania wykrytych nielegalnych treści do National Center for Missing & Exploited Children14 (amerykańskiego zespołu reagującego, „odpowiednika" hotline'u, jakim jest Dyżurnet.pl).
W przypadku polskich serwisów społecznościowych sprawa wygląda inaczej. Portale te są dużo mniejsze i mają ograniczone możliwości finansowe, systemowe czy narzędziowe. Regulacje prawne nie nadążają za potrzebami wywołanymi przez zmiany technologiczne. Podstawowym problemem tego typu serwisów, zlokalizowanych na polskich serwerach jest bardzo słaba moderacja lub jej brak. Nie dysponują one też programami Trusted Flaggers, a kontakt z ich administracją jest bardzo utrudniony. Z tego powodu ważnym wyzwaniem stojącym przed polskimi serwisami społecznościowymi i komunikacyjnymi jest wprowadzenie poprawnie funkcjonujących działów typu abuse, reagujących na zgłoszenia użytkowników i współpracujących zarówno z organami ścigania, jak i zespołem Dyżurnet.pl w kwestii reagowania na nielegalne treści w internecie. Wyzwaniem jest również wprowadzenie premoderacji – szczególnie w miejscach bardzo wrażliwych społecznie ze względu na popularność serwisu wśród osób niepełnoletnich.

14. https://www.missingkids.org/HOME

Drugim, nie mniej ważnym problemem jest obecnie brak skutecznej weryfikacji wieku użytkowników, która pozwalałaby na dopasowanie treści i funkcjonalności (np. ustawienia prywatności) do wieku osoby korzystającej z usługi. Niektóre platformy umożliwiają również anonimowy kontakt pomiędzy użytkownikami, gdzie nie jest wymagane podanie personaliów użytkownika. Brak obowiązku rejestracji lub jej bardzo uproszczona forma również stanowi czynnik sprzyjający temu zjawisku. Takie warunki mogą stwarzać osobom o niekoniecznie czystych zamiarach możliwość nawiązania kontaktu z osobą niepełnoletnią i wykorzystania jej. Dlatego ważnym wyzwaniem stojącym przed administratorami takich serwisów jest rozwiązanie tego problemu. Społeczność internetowa powinna wymagać od administratorów/właścicieli jak największej dbałości o bezpieczeństwo użytkowników i zapewnienia możliwości podjęcia działań wobec użytkownika naruszającego regulamin lub prawo.

Działania w obszarze policy

Rok 2022 był dla Dyżurnet.pl ważny z uwagi na dwa przedsięwzięcia w obszarze *policy*, które mają szansę przyczynić się do poprawy krajowej odpowiedzi na problem wykorzystywania seksualnego dzieci, w tym w cyberprzestrzeni.

Pierwszym z nich jest kontynuacja prac *Zespołu do spraw przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich*, powołanego przez Ministra Sprawiedliwości we wrześniu 2021 roku. Zgodnie z treścią Zarządzenia[15] Ministra Sprawiedliwości, do zadań, które mają zostać zrealizowane przez ten Zespół do końca 2026 r. należą:

- analiza aktualnych rozwiązań krajowych w obszarze szeroko pojętego przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich;
- opracowanie krajowego planu działania na rzecz przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich;
- wypracowanie propozycji legislacyjnych w ww. zakresie oraz propozycji zmian systemowych.

W 2022 roku działania Zespołu skupiły się na opracowaniu krajowego planu działania (p.2), którego projekt zostanie następnie skierowany do dalszych prac legislacyjnych (uchwała Rady Ministrów). Reprezentanci NASK i Dyżurnet.pl zaproponowali szereg działań, które zostały uwzględnione w planie, jak również będą zaangażowani w realizację wielu z nich. Należy wśród nich wymienić:

- prowadzenie badań, analiz i gromadzenie danych statystycznych;
- działania legislacyjne;
- realizacja szkoleń;

15. Zarządzenie Ministra Sprawiedliwości z dnia 29 września 2021 r., Dz. U. Ministra Sprawiedliwości, poz. 221 z 2021 r. [Dostęp 05/12/22: https://www.gov.pl/web/sprawiedliwosc/du-21-233].

- wdrażanie rozwiązań technologicznych;
- rozbudowa platformy 116.

Drugim przedsięwzięciem była publikacja w maju 2022 roku wniosku Komisji Europejskiej, dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady, ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie.[16] Projektowany akt prawny ma nałożyć obowiązki na dostawców usług w zakresie oceny i ograniczania ryzyka wystąpienia wypadków niegodziwego traktowania dzieci w celach seksualnych oraz, w stosownych przypadkach, wykrywania, zgłaszania i eliminowania tego rodzaju materiałów w ramach świadczonych przez nich usług. Planowane jest również utworzenie *Unijnego Centrum ds. Zapobiegania Niegodziwemu Traktowaniu Dzieci w Celach Seksualnych i Jego Zwalczania*, które ma być organem udzielającym wsparcia krajowym organom koordynującym, ułatwiającym dokonywanie oceny ryzyka, wykrywanie, zgłaszanie, usuwanie i blokowanie treści oraz wymianę informacji. Centrum ma być ponadto upoważnione do tworzenia i utrzymywania baz danych zawierających informacje dotyczące zjawiska niegodziwego traktowania dzieci w celach seksualnych w cyberprzestrzeni, w tym treści przedstawiających takie traktowanie.

W 2023 roku prace nad rozporządzeniem będą kontynuowane. Należy spodziewać się, że jego wejście w życie pociągnie za sobą zmiany dotyczące funkcjonowania Dyżurnet.pl, zatem nasza uwaga będzie skupiona na tym obszarze.

16. COM(2022) 209 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022PC0209

Czym jest metawersum?

Tematy związane z *metawersum*, szansami, jakie daje i możliwymi zagrożeniami, jakie stwarza korzystanie z tego typu technologii, są przedmiotem zainteresowania ekspertów zajmujących się zarówno technologią, jak i profilaktyką zagrożeń. **Czym jest *metawersum*? Jaka jest jego przyszłość? Jakie zagrożenia stwarza?**

Metawersum to wirtualny świat, do którego dostęp możliwy jest poprzez użycie specjalnych gogli VR (*Virtual Reality*). Technologia ta ma stanowić odwzorowanie świata offline, co za tym idzie – pozwalać na podejmowanie różnych aktywności, często w interakcji z innymi użytkownikami. W światach *metawersum* użytkownik porusza się swoim awatarem, którego wygląd można dowolnie zmieniać i dostosowywać.

Jak estymują eksperci, za 10-15 lat technologia będzie powszechnie dostępna dla wszystkich i wykorzystywana w różnych miejscach np. przy nauce nowych procesów lub czynności, pozwoli doświadczać ograniczeń wynikających z choroby, ale też brać udział w nowych formach rozrywki. Obecnie VR ma również zastosowanie terapeutyczne – obiecująco wyglądają badania dotyczące wykorzystania VR w terapiach traum i autyzmu[17]. Już teraz w wirtualnej rzeczywistości możliwy jest zakup dla awatara cyfrowej wersji ubrań, biżuterii, elektroniki lub innych rzeczy, np. produktów ekskluzywnych od projektantów. Ponadto możliwy jest zakup nieruchomości, zwierzaka, jak również „wyjazd na wycieczkę" nawet w najbardziej egzotyczne miejsca, czy zwiedzenie muzeum i galerii, które mogą prezentować zbiory sztuki. Siła *Metawersum* polega na tym, że jest to miejsce, gdzie każdy może całkowicie kreować siebie – mieć wielu znajomych, podróżować dookoła świata, „mieszkać" w pięknym miejscu, posiadać i robić rzeczy, na które nie mógłby pozwolić sobie w życiu offline.

Eksperci zespołu Dyżurnet.pl poza wieloma zaletami, zauważają szereg zagrożeń związanych z bezpieczeństwem, przede wszystkim dzieci i młodzieży korzystających z tego typu technologii. Niedostateczna weryfikacja użytkowników oraz możliwość „bycia kim się chce" mogą być atrakcyjne dla osób seksualnie

17. Wiebe A., Kannen A., Selaskowski B., Mehrena A., Thöne A., *Virtual reality in the diagnostic and therapy for mental disorders: A systematic review*

zainteresowanych dziećmi lub tych, których intencje nie są dobre. *Metawersum*, ponieważ jest nowym rozwiązaniem technologicznym, nie ma jeszcze dostatecznie wypracowanych regulacji prawnych, problematyczna może okazać się również jurysdykcja. Kwestie zasad panujących na platformie często opierają się jedynie na regulaminie użytkowania. Wiele gier czy miejsc rozrywki, do których dostęp można uzyskać poprzez gogle VR, nie oferuje automatycznych, domyślnych ustawień o najwyższym stopniu prywatności dla osób małoletnich, co może stanowić „otwarte drzwi" do kontaktu dziecka z osobami dorosłymi lub prowadzić do innych nadużyć. Ujawnione zostały przypadki nadużyć polegających na prezentowaniu pornografii osobom nieletnim w światach VR oraz przypadki *child groomingu*, czyli uwodzenia dziecka online, na platformach tego typu. Przy stosowaniu gogli na uwagę zasługuje również wpływ korzystania z tego typu urządzeń na mózg, co nie zostało do tej pory dostatecznie zbadane.

W stosunku do każdej technologii, a w szczególności tej nowej, wskazane jest zachowanie ostrożności oraz stosowanie zasady ograniczonego zaufania. Zanim pozwolimy korzystać dziecku z gier czy aplikacji, w tym przede wszystkim tych umożliwiających kontakt z nieznajomymi lub których *content* nie jest weryfikowany przed upublicznieniem, warto przejść przez aplikację/grę i sprawdzić, co w sobie zawiera. Dobrą praktyką jest osobiste zweryfikowanie zawartości oraz funkcjonalności danej gry czy aplikacji lub przejście jej razem z dzieckiem.

Wraz z końcem roku 2022 zespół Dyżurnet.pl podjął się badania przestrzeni metawersum z poziomu użytkownika. Badane platformy podlegały sprawdzeniu empirycznemu pod kątem bezpieczeństwa i możliwych zagrożeń. Do badania zostały wybrane aplikacje, które są najbardziej popularne wśród użytkowników. Zespół przede wszystkim zwracał uwagę na platformy, za pomocą których możliwa jest interakcja z innymi użytkownikami, poziom ich bezpieczeństwa oraz sposoby weryfikacji użytkownika. Raport z badania będzie dostępny na stronie dyzurnet.pl.

Rozwiązania
technologiczne

Udział Dyżurnet.pl w międzynarodowym projekcie Global Standard

Świat wolny od wykorzystywania seksualnego dzieci oraz od treści CSAM jest wspólną wizją wszystkich organizacji i instytucji oraz opiekunów, którym zależy na dobru dziecka. Istotnym krokiem w kierunku urzeczywistnienia tej wizji jest międzynarodowy projekt *Global Standard* realizowany przez INHOPE i finansowany przez *Global Partnership to End Violence against Children*.

Celem projektu jest stworzenie wspólnej ontologii dla istniejących na świecie systemów kategoryzacji treści CSAM, która umożliwi automatyczną translację pomiędzy takimi systemami funkcjonującymi dzisiaj w różnych krajach i instytucjach. Wspólny język opisujący cechy charakterystyczne w poszczególnych kategoriach treści pozwoli wszystkim zaangażowanym instytucjom i podmiotom na efektywną wymianę danych bez konieczności ich ponownej analizy. Umożliwi również szybkie podjęcie decyzji o potencjalnej nielegalności każdej skategoryzowanej treści. Z systemu będą mogli korzystać zarówno analitycy hotline, funkcjonariusze policji, jak i specjaliści branży technologicznej.

Specjaliści Dyżurnet.pl brali aktywny udział w tworzeniu nowego standardu, dzieląc się wiedzą pozyskaną podczas pracy zespołu nad nowym systemem wdrażanym w projekcie APAKT. Doświadczenia zdobyte podczas kategoryzacji i anotowania obrazów i filmów do celów treningu modeli sztucznej inteligencji okazały się bardzo pomocne podczas prac grupy roboczej, w których Dyżurnet.pl brał udział. Wytyczne ontologii będą publikowane w połowie 2023 roku.

Projekt APAKT automatyczna analiza treści

Zakończył się trzeci rok prac na projektem APAKT – czyli narzędziem, którego celem będzie Automatyczne Przeszukiwanie, Analiza i Klasyfikacja Treści. APAKT, poprzez identyfikację materiałów przedstawiających seksualne wykorzystywanie dzieci, zarówno tych już rozpoznanych i sklasyfikowanych w przeszłości, jak i zupełnie nowych, ma przede wszystkim usprawnić proces obsługi zgłoszeń kierowanych do Dyżurnet.pl. Algorytmy detekcji treści CSAM będą miały również szerokie zastosowanie w innych systemach informatycznych, w których użytkownicy mają możliwość udostępniania plików.

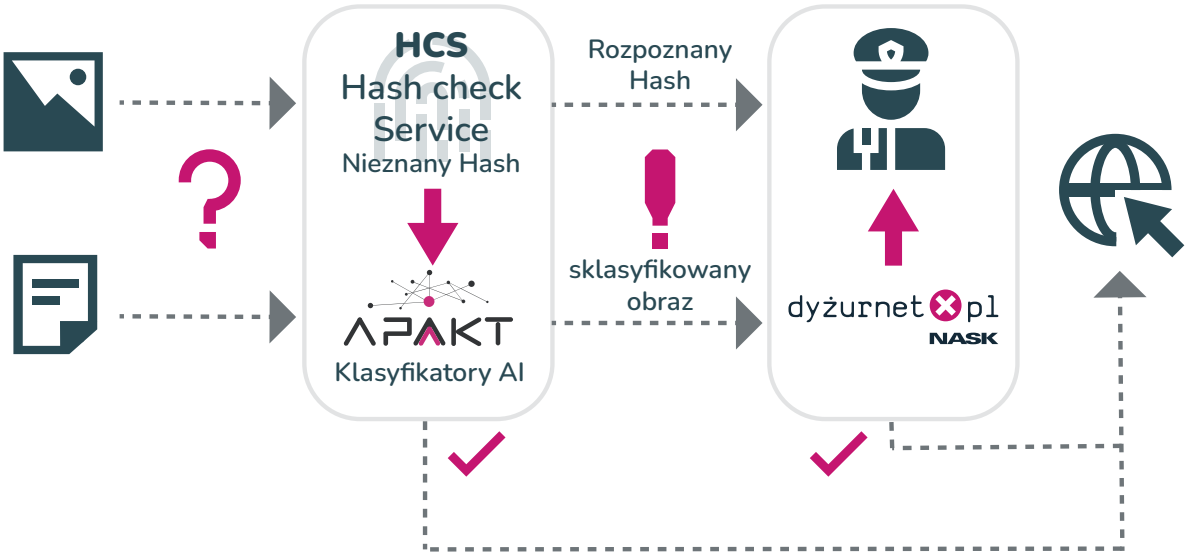
Przedsięwzięcie finansowane jest ze środków Narodowego Centrum Badań i Rozwoju, a w jego realizacji, oprócz zespołu Dyżurnet.pl i pracowników naukowych NASK, uczestniczą również Politechnika Warszawska oraz firma Enamor International Sp. z o.o.

W ramach odpowiednio zabezpieczonej infrastruktury zbudowana została baza danych wraz z zaawansowanym systemem do ich pobierania, filtrowania i analizy. Dane gromadzone w systemie są analizowane pod kątem ewentualnych duplikatów przy zastosowaniu kilku poziomów detekcji, od porównania sygnatur plików (tzw. hashy kryptograficznych) po wykorzystanie bardziej zaawansowanych hashy perceptualnych, częściowo odpornych na zmiany dokonane w obrazach. Zduplikowane lub bardzo podobne zdjęcia są automatycznie klasyfikowane bez udziału analityków, dzięki czemu zmniejsza się ekspozycja zespołu na szkodliwe treści. W trakcie trwania projektu sklasyfikowano ponad 21 tysięcy zdjęć i filmów oraz ponad tysiąc tekstów.

W trakcie roku zespoły naukowe wypracowały kilka modeli cząstkowych wykorzystujących sztuczną inteligencję i umożliwiających detekcję wybranych elementów obrazu. Po ich udoskonaleniu, modele te zostaną połączone w jeden algorytm, który umożliwi klasyfikację zdjęć i filmów pod kątem obecności treści CSAM.

System klasyfikacji i kategoryzacji danych został dostosowany do standardów międzynarodowych i jest na bieżąco dostrajany do ontologii tworzonej w projekcie *Global Standard*.

Narzędzia i ścieżka detekcji treści CSAM



Wtyczka do zgłaszania nielegalnych i szkodliwych treści

Na treści nielegalne lub szkodliwe w internecie można natrafić zupełnie przypadkiem, klikając w przesłany przez kogoś link lub reklamę. Zdarza się, że strony internetowe przekierowują do treści, do których użytkownicy świadomie nie zdecydowaliby się zajrzeć.

Aby proces zgłaszania treści był łatwiejszy dla użytkownika, zespół Dyżurnet.pl stworzył specjalną wtyczkę do przeglądarek internetowych, która po zainstalowaniu umożliwia przesłanie informacji o nielegalnych lub szkodliwych treściach za pomocą kilku kliknięć. Procedura wysyłania zgłoszeń za pomocą wtyczki nie wymaga przenoszenia adresu zgłaszanej strony internetowej do formularza zgłoszeń. Nie wymaga też żadnych dodatkowych kroków oprócz prostego kliknięcia w ikonę wtyczki. Wtyczka umożliwia również automatyczne przekazanie referera, czyli adresu strony internetowej, z której zostaliśmy na aktualnie przeglądaną stronę przekierowani. Dodatkowo, tak jak w przypadku formularza, zgłoszenia mogą być dokonywane anonimowo i gwarantowane jest pełne bezpieczeństwo danych.

Wtyczka jest dostępna dla przeglądarek:

- Mozilla Firefox: Zgłoś treść do Dyżurnet.pl[18],
- Google Chrome: Zgłoś nielegalną treść do Dyżurnet.pl[19].

18. https://addons.mozilla.org/pl/firefox/addon/zglos-tresc-do-dyzurnet-pl/

19. https://chrome.google.com/webstore/detail/report-illegal-content-to/djegpdbohfkhkiebfdikclmmbpgdblbh

Współpraca z OSE

Państwowy Instytut Badawczy NASK jest operatorem programu Ogólnopolskiej Sieci Edukacyjnej (OSE), który umożliwia szkołom w całej Polsce podłączenie szybkiego, bezpłatnego i bezpiecznego internetu.

Eksperci Dyżurnet.pl biorą udział w realizacji zadań związanych ze stałym podnoszeniem poziomu bezpieczeństwa sieci OSE poprzez:

1. współtworzenie i aktualizacje polityki bezpieczeństwa,

2. wspomaganie procesu wdrażania i rozwoju kolejnych poziomów usług bezpieczeństwa,

3. wymianę informacji o zgłaszanych incydentach, dzięki czemu możliwa jest jeszcze lepsza ochrona użytkowników sieci OSE przed treściami nielegalnymi i potencjalnie szkodliwymi.

Więcej informacji o programie: www.ose.gov.pl.

Działalność

edukacyjno-popularyzatorska

Kampania Nie na pokaz

W 2022 roku Dyżurnet.pl w ramach programu Safer Internet przygotował kampanię *Nie na pokaz*. Kampanię poprzedzały badania zrealizowane w czwartym kwartale 2021 roku wraz z firmą badawczą SW Research z wykorzystaniem jakościowych indywidualnych wywiadów pogłębionych (IDI). Realizacja wywiadów odbyła się od 2 do 22 września 2021 roku. W tym czasie przeprowadzono 37 indywidualnych wywiadów przy użyciu platformy ZOOM. W badaniu wzięły udział osoby w dwóch grupach wiekowych: 18-21 lat (28 respondentów) oraz 22-24 lata (9 respondentów). Łącznie przebadano 15 mężczyzn i 22 kobiety. Zadane zostały pytania zgodnie z profilem osób:

- osoba, która wysłała zdjęcie świadomie;
- osoba, która wysłała zdjęcie pod presją;
- osoba, której zdjęcie wyciekło i nie była tego świadoma przez pewien czas;
- osoba, która otrzymała materiał o charakterze intymnym, bo o to prosiła;
- osoba, która otrzymała materiał o charakterze intymnym poprzez *maillingfame* – ktoś chciał się pochwalić swoimi zdjęciami i wysłał je do większej liczby osób;
- osoba, która otrzymała przez przypadek materiały o charakterze intymnym;
- osoba, która nie wysłała, a była namawiana / osoba, która nie wysłała, a była pod presją.

Po dogłębnej analizie wywiadów powstał raport *Nie na pokaz*, wydany przez zespół Dyżurnet.pl, który jest podsumowaniem wyników badań oraz prezentacją skali i charakterystyki zjawiska treści intymnych produkowanych przez młodzież. Kampania skierowana do nastolatków była realizowana przez Polskie Centrum Programu Safer Internet, Dyżurnet.pl oraz Tik Tok Polska.

We wstępie do raportu czytamy:

> *Wyniki badania, mimo zakresu pracy zespołu Dyżurnet.pl i znajomości tematu zagrożeń, z jakimi mogą się zetknąć osoby niepełnoletnie w internecie, były zaskakujące. Okazało się, że zjawisko sextingu oraz wytwarzania treści „self-generated sexual content" przez osoby nieletnie jest dużo bardziej powszechne, niż wcześniej nam się zdawało.*

Ważnym tego aspektem jest dobrowolność decydowania się na produkcję i prezentację treści intymnych. **Należy zaznaczyć, że samodzielnie nie znaczy dobrowolnie.** Raport z badania, ale również zgłoszenia otrzymywane przez Dyżurnet.pl pokazują, że treści intymne powstają w różnych okolicznościach, nie zawsze użytkownicy zdają sobie sprawę z dalszych konsekwencji swojego postępowania i dopiero w sytuacji wycieku materiałów zastanawiają się nad grożącymi im konsekwencjami. Zdarzają się jednak sytuacje, gdy osoba nieletnia jest przymuszana szantażem do wytwarzania takich treści lub jej materiały intymne są publikowane w sieci bez jej zgody. Takie przypadki zawsze powinny budzić czujność rodziców i opiekunów, ponieważ może kryć się za nimi przemoc, zarówno ze strony rówieśników, jak i dorosłych.

Badanie dotyczące publikowania treści intymnych przez młodzież pokazało, że zarówno zbyt wczesny kontakt dziecka z treściami pornograficznymi, jak upublicznienie własnych intymnych materiałów mogą być dla młodej osoby przeżyciem traumatycznym. Podobnie dzieje się w sytuacji, gdy dziecko jest uwodzone lub szantażowane. W takich sytuacjach niezwykle ważna jest odpowiednia, wspierająca reakcja dorosłych – przede wszystkim rodziców, ale też nauczycieli. Młodzi ludzie wskazują też na dużą rolę wsparcia otrzymywanego od rówieśników.

Dlatego w podsumowaniu raportu znajdują się wskazówki dla dorosłych, jak odpowiednio reagować w sytuacji, w której dowiadują się, że dziecko miało kontakt z pornografią lub udostępniło treści intymne w sieci. W przypadku młodszych dzieci bardzo ważne jest odpowiednie skonfigurowanie i zabezpieczenie urządzeń, z których korzysta dziecko, trzymanie się zasad i regulaminów mediów społecznościowych, które określają minimalny wiek użytkowników, ale też kontrola treści i materiałów tworzonych przez dziecko. Warto też pamiętać o tym, że często sami rodzice udostępniają w sieci zdjęcia czy filmy ze swoimi dziećmi, które wydają im się niewinne, a mimo to mogą znaleźć się w galeriach osób seksualnie zainteresowanych dziećmi. O tym, że w sieci nic nie ginie, a każdy opublikowany tam materiał będzie już zawsze dostępny, powinni wiedzieć i pamiętać przede wszystkim dorośli. W przypadku młodzieży nacisk powinien być

położony na zasady cyberbezpieczeństwa, ale także poczucie własnej wartości i budowanie swojego wizerunku.

W raporcie czytamy:

> *Szacunek do własnego ciała oraz umiejętność asertywnego odmawiania są kluczowe w budowaniu pewności siebie oraz poczucia własnej wartości. Naucz dziecko umiejętności dokonywania dobrych wyborów przez diagnozowanie motywów działania (swoich i innych) oraz widzenia krótko- i długofalowych skutków. Nawet w potencjalnie bezpiecznej relacji dzielenie się materiałami intymnymi może być niebezpieczne. Pamiętaj, że najlepiej działają przykłady, dlatego rozmawiajcie o różnych sytuacjach, których doświadczają rówieśnicy. Starajcie się wspólnie znaleźć alternatywne rozwiązania.*

W raporcie wielokrotnie zostało podkreślone wsparcie, które jest bardzo ważne dla dziecka na każdym etapie. Nawet wówczas, gdy jego intymne materiały wyciekną do sieci, należy pamiętać, by nie obwiniać dziecka, nie karać, gdyż cała sytuacja jest dla niego wystarczająco trudna. W sytuacji, gdy dziecko jest ofiarą uwodzenia lub szantażu na tle seksualnym, taki incydent należy zgłosić do zespołu Dyżurnet.pl oraz na Policję.

Więcej informacji na temat zjawiska wytwarzania materiałów intymnych przez małoletnich jak i analiza przeprowadzonych badań dostępne są w raporcie na stronie: https://dyzurnet.pl/uploads/2022/02/Publikacja-Nie-na-pokaz.pdf

Wydarzenia

W 2022 roku przedstawiciele Dyżurnet.pl dzielili się swoimi doświadczeniami i wiedzą między innymi podczas wydarzeń:

- 21 kwietnia-6 maja – cykl szkoleń dla Szkoły Policji w Pile
- 25-26 maja – *INHOPE Roundtable* w Bratysławie
- 31 maja – *Instant Image Identifier Demonstration* w Brukseli
- 1-2 września – wizyta studyjna przedstawicieli słowackiego Ministestwa Pracy, Spraw Społecznych i Rodziny oraz Narodowego Ośrodka Przeciwdziałania Przemocy Wobec Dzieci
- 16 września – *XVIII Ogólnopolski Zjazd Socjologiczny* w Warszawie
- 28 września – *8. Forum Prawa Mediów Elektronicznych* na Uniwersytecie Śląskim
- 28-29 września – *16. Międzynarodowa Konferencja Bezpieczeństwo dzieci i młodzieży w internecie* Safer Internet
- 28-29 września – INHOPE Advanced Analysts Workshop w Amsterdamie
- 12-14 października – *EFNI Europejskie Forum Nowych Idei*
- 15 listopada – *INHOPE Annual General Meeting* w Lizbonie
- 15 listopada – konferencja Safer Internet *Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online*
- 17 listopada – konferencja online *SECURE Early Bird*

- 23 listopada – konferencja Wydziału Kryminalnego KWP w Szczecinie *Metody zwalczania przestępczości handlu ludźmi w kontekście migracji*

Ponadto eksperci zespołu prowadzili warsztaty i webinary, między innymi:

- 26 kwietnia – webinar poświęcony problematyce udostępniania w sieci treści intymnych przez młodych ludzi *Nie na pokaz* z udziałem gości: prof. Zbigniewa Izdebskiego i Jakuba Olka (TikTok)

- 12 maja – webinar dla rodziców *Rodzic 3.0 – jak chronić dziecko przed zagrożeniami w internecie na przykładzie pornografii*

- 21-22 lipca – warsztaty dot. bezpiecznego korzystania z internetu dla Związku Harcerstwa Polskiego w Szklarskiej Porębie

- 29 września – webinar *Popularne aplikacje – przewodnik dotyczący prywatności*

- 18 listopada – webinar *Ryzykowne zachowania online* dla uczniów szkół w powiecie ciechanowskim

- 12-13 grudnia – warsztaty dot. cyberbezpieczeństwa dla uczniów Zespołu Szkół Ogólnokształcących w Górze Kalwarii

O działaniach edukacyjno-popularyzatorskich Dyżurnet.pl można było dowiedzieć się także z audycji w mediach i podcastów.

O NASK

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministra Cyfryzacji w Kancelarii Prezesa Rady Ministrów.

Cyberbezpieczeństwo i ochrona użytkowników oraz działania związane z zapewnieniem bezpieczeństwa są kluczowym polem aktywności NASK. Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci i przyjmowaniem zgłoszeń o naruszeniach zajmuje się Zespół CERT Polska (www.cert.pl) oraz Dyżurnet.pl. Zgodnie z Ustawą o Krajowym Systemie Cyberbezpieczeństwa NASK-PIB został wskazany na poziomie krajowym jako jeden z trzech Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy internetu.

NASK współtworzy również zaplecze analityczne oraz badawczo-rozwojowe dla Krajowego Systemu Cyberbezpieczeństwa, prowadzi działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Działalność naukowo-badawcza NASK ma również wymiar wdrożeniowy i prorynkowy. W naszym instytucie badacze komercyjny problem ujmują w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, ale również innowacyjnych. Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie, analiza, przetwarzanie i transfer danych, a także złożone systemy sieciowe, w tym systemy IoT oraz mobilne sieci ad hoc. Obecnie rozwijany jest w badaniach obszar sztucznej inteligencji. Istotne miejsce zajmują badania dotyczące biometrycznych metod weryfikacji tożsamości w bezpieczeństwie usług. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki. NASK prowadzi także rejestr nazw w domenie .pl (www.dns.pl).

Słownik pojęć

CSAM

child sexual abuse materials – materiały przedstawiające seksualne wykorzystywanie dziecka. Kategoryzowane przez ekspertów Dyżurnet.pl jako treści pornograficzne z udziałem małoletnich (art. 202 k.k.).

CSEM

child sexual exploitation material – materiały prezentujące dziecko w seksualnym kontekście, będące nadużyciem wobec dziecka, jednak w większości krajów, w tym w Polsce, są to materiały legalne.

Baseline

kryterium opisujące materiały CSAM, które stanowią treść nielegalną we wszystkich krajach zrzeszonych w INHOPE.

Zgłoszenie

powiadomienie dotyczące potencjalnie nielegalnych treści w internecie przesłane przez użytkownika lub instytucję.

Incydent

zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl.

ICCAM

baza wymiany informacji dotyczących CSAM dostępna dla zespołów zrzeszonych w INHOPE, do której na bieżąco przekazywane są materiały zaklasyfikowane jako przedstawiające seksualne wykorzystanie dziecka.

ICSE

International Child Sexual Exploitation database – utrzymywana przez Interpol baza, do której przekazywane są informacje o najbardziej drastycznych materiałach w kategorii CSAM, dzięki czemu możliwe jest podjęcie działań w celu identyfikacji zarówno ofiar, jak i sprawców.

INHOPE

sieć zaufanych zespołów reagujących, której celem jest eliminacja materiałów przedstawiających seksualne wykorzystywanie dzieci oraz wsparcie krajowych procedur na rzecz jak najszybszego usuwania nielegalnych materiałów. Działalność Stowarzyszenia jest wspierana przez Interpol, Europol, Virtual Task Force, European Financial Coalition, INSAFE, ECPAT oraz globalne firmy sektora informatycznego.

APAKT

Automatyczne Przeszukiwanie, Analiza i Klasyfikacja Treści – projekt finansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu badawczo-rozwojowego CyberSecIdent, ukierunkowanego na podniesienie bezpieczeństwa cyberprzestrzeni RP. Celem projektu jest wypracowanie algorytmów, które będą skutecznie rozpoznawać i klasyfikować materiały przedstawiające seksualne wykorzystywanie dzieci z użyciem modeli tzw. sztucznej inteligencji.

Hash

sygnatura pliku, jego „cyfrowy odcisk".

Szantaż na tle seksualnym

(dawniej sextortion) jest to zjawisko, które polega na pozyskaniu przez sprawcę materiałów o charakterze seksualnym, a następnie wymuszenie od ofiary pieniędzy w zamian za nie udostępnienie materiałów w sieci. Czasami sprawca może żądać kolejnych filmów, zdjęć lub innego wynagrodzenia.