RAPORT 2021

dyżurnet.pl
NASK

CSIRT NASK

WYDAWCA

NASK Państwowy Instytut Badawczy

ul. Kolska 12
01-045 Warszawa
e-mail: info@nask.pl, info@dyzurnet.pl

issn 2084-7785

Tekst: Zespół Dyżurnet.pl

Korekta: Anna Hernik-Solarska

opracowanie graficzne i ilustracje: Agnieszka Malinowska

dyżurnet.pl
NASK

INHOPE

saferinternet.pl

Współfinansowane przez Unię Europejską
Instrument „Łącząc Europę”

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,

Raport z działalności Zespołu Dyżurnet.pl jest okazją do refleksji na temat zagrożeń, które mają miejsce w internecie oraz są związane z nowymi technologiami. Dla NASK PIB zawsze ważne były działania na rzecz podnoszenia poziomu bezpieczeństwa internetu czy technologii, a założenie w 2005 roku zespołu Dyżurnet.pl pokazało, że przeciwdziałanie materiałom przedstawiającym seksualne wykorzystywanie dzieci jest koniecznym krokiem. Od 2018 roku działalność Dyżurnet.pl jest wpisana w Ustawę o Krajowym Systemie Cyberbezpieczeństwa, a Zespół realizuje zadania CSIRT NASK.

Wyjątkowość Zespołu polega na tym, że analizuje treści, które nie są powszechnie dostępne, ale również dlatego, że jest łącznikiem pomiędzy użytkownikami, platformami internetowymi, organami ścigania czy instytucjami rządowymi. Nasza perspektywa pozwala na analizę zjawisk, które dla innych mogą być nieuchwytne. W tegorocznym raporcie ważny jest, z naszego punktu widzenia, alarmujący przekaz zwracający uwagę na treści seksualne samodzielnie wyprodukowane przez dzieci. Samodzielnie nie znaczy dobrowolnie, dziecko nie ma wystarczającego doświadczenia i wiedzy, aby rozumieć cały kontekst sytuacji. Dlatego konieczne jest wsparcie wszystkich osób i instytucji, aby przeciwdziałać powstawaniu intymnych treści oraz jak najskuteczniej przeciwdziałać skutkom dystrybucji zdjęć czy filmów prezentujących seksualne wykorzystanie najmłodszych.

Mamy nadzieję, że raport obrazujący skalę zjawisk związanych z nadużyciami w sieci, nielegalnymi i nieodpowiednimi treściami, a także zawierający opisy naszej działalności będzie dla Państwa inspiracją do przemyśleń o wyzwaniach, jakie stawia przed nami cyfrowy świat. Bądźmy w nim razem, ponieważ tylko wtedy jest możliwe zadbanie o najmłodszych użytkowników cyberprzestrzeni.

Z poważaniem
Krzysztof Silicki
Dyrektor ds. Cyberbezpieczeństwa i Innowacji NASK

SPIS TREŚCI

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, prowadząc współpracę z międzynarodowymi organami ścigania,
m.in. z Interpolem oraz firmami branży internetowej. Celem Stowarzyszenia jest wsparcie krajowych hotlinów 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 (www.betterinterntetforkids.eu)
ma na celu promowanie bezpiecznego korzystania z internetu i nowych technologii oraz wsparcie reagowania w przypadku zagrożeń online dotykających najmłodszych.

telefon zaufania:
116 111
800 100 100

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*:

- 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;
- 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 np. 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.

* Artykuły Kodeksu Karnego w brzmieniu niepełnym

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.

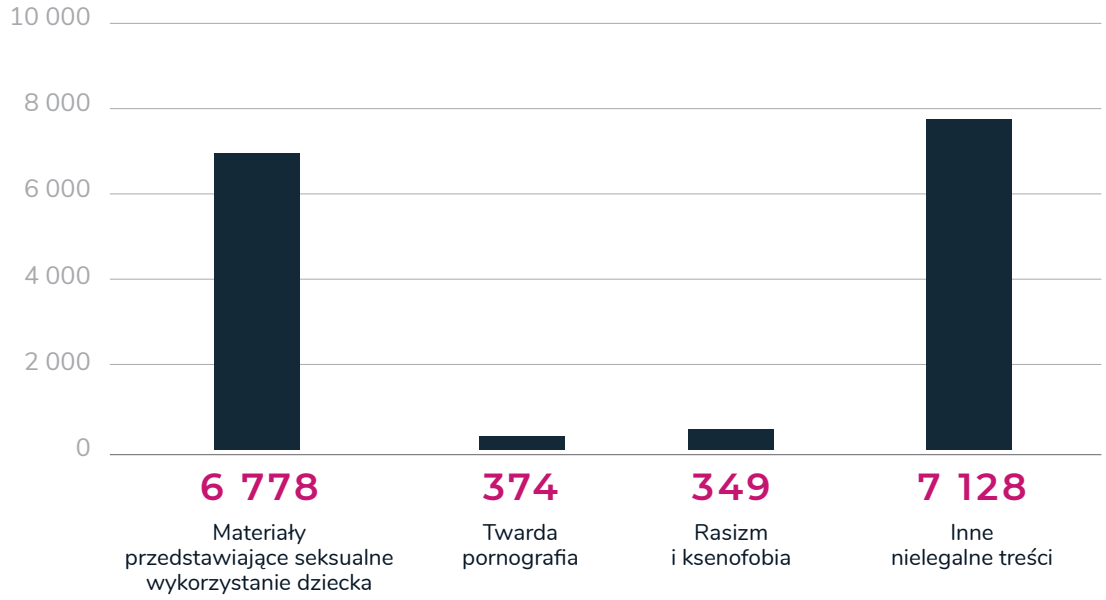
Działania wszystkich zespołów reagujących oraz współpracujących z nimi organów ścigania zmierzają do jak najszybszego zidentyfikowania sprawcy oraz ofiary seksualnego wykorzystania. Zgłoszenie przez użytkownika oraz niezwłoczne podjęcie działań przez administratora pozwalają na znaczne ograniczenie dalszego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

STATYSTYKI

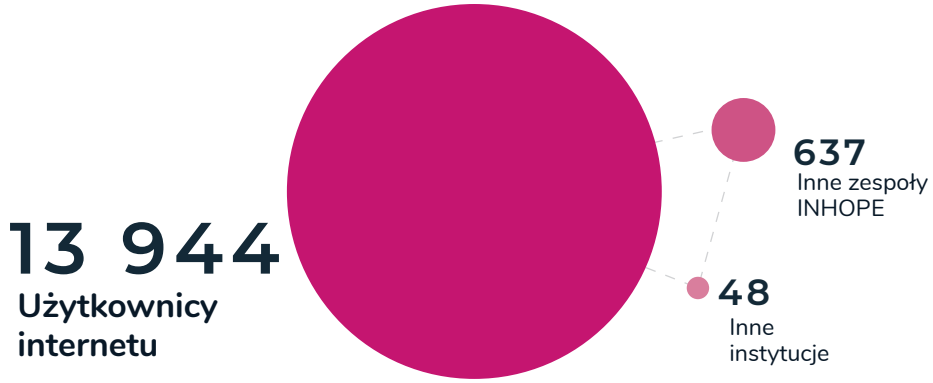
Dyżurnet.pl za rok 2021

Zgłoszenia otrzymane przez zespół Dyżurnet.pl

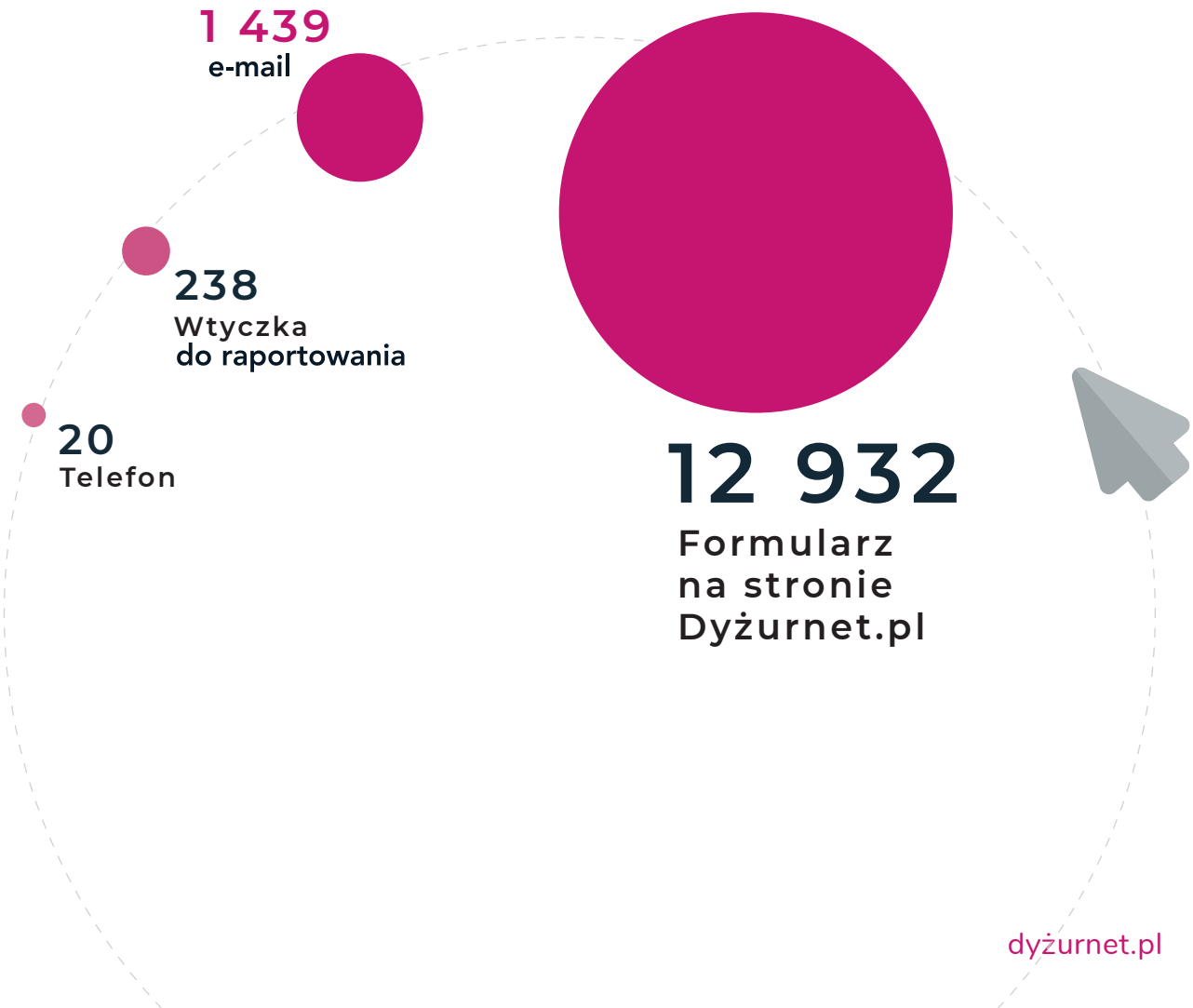
1 | Liczba zgłoszeń otrzymanych przez Dyżurnet.pl - rodzaj potencjalnie nielegalnych treści



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



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



Analizowane incydenty i działania podjęte przez zespół Dyżurnet.pl

4 | Klasyfikacja incydentów związanych z wykorzystaniem seksualnym małoletnich

2069

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.).

409

CSEM

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

18

Propagowanie pedofilskiej aktywności

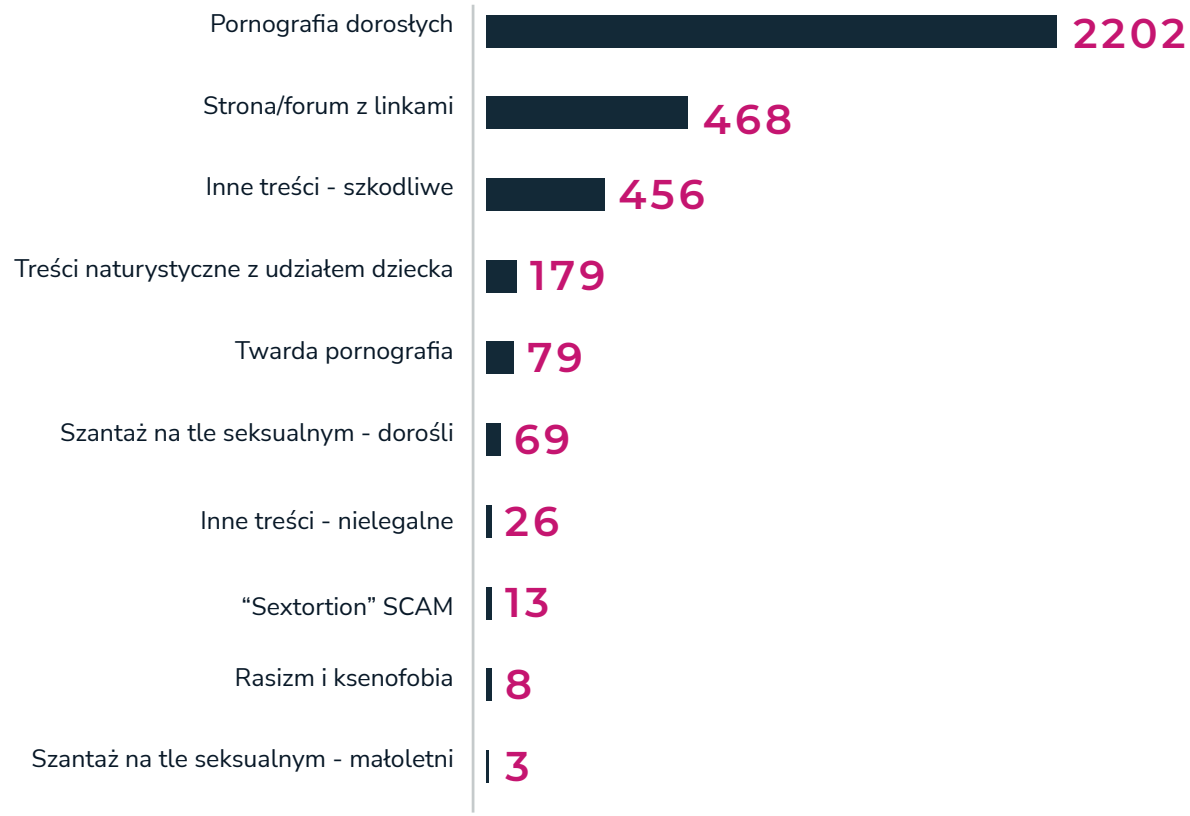
Propagowanie pedofilskiej aktywności
Publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim; nielegalne wg polskiego prawa (art. 200b k.k.).

10

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.).

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 i kwalifikowane do blokowania w sieci OSE: treści drastyczne, wulgarne, obraźliwe, radykalne światopoglądowo (również sekty), homofobiczne, autodestrukcyjne, propagujące samobójstwo lub przemoc, pro-ana, patostreamy, środki psychoaktywne (nie zidentyfikowane 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.).

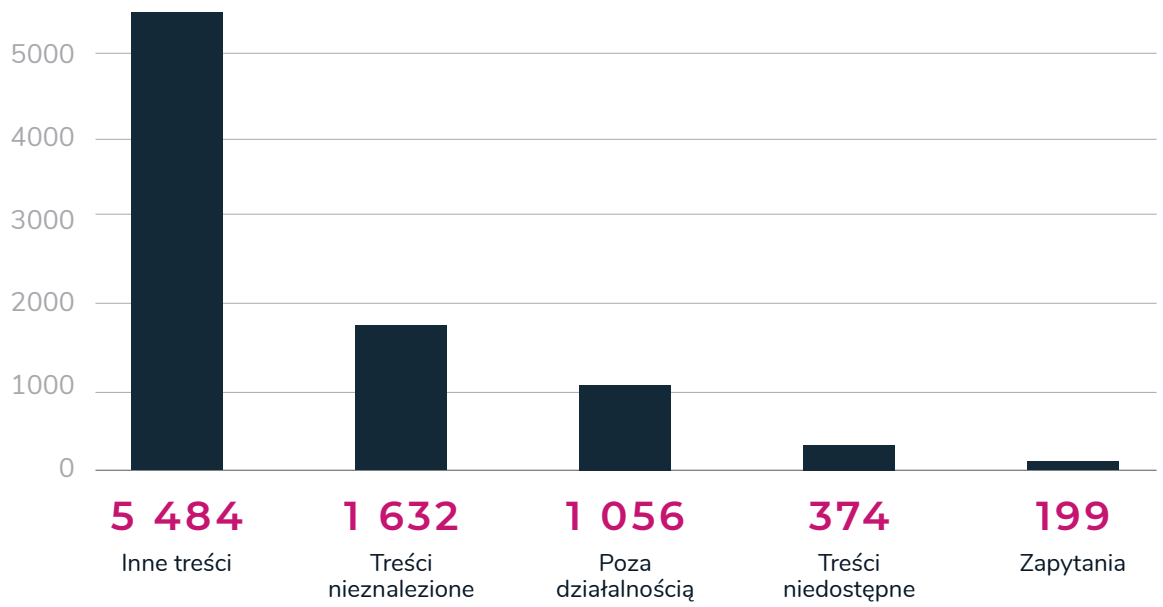
Szantaż na tle seksualnym („sextortion”)
Seksualne wymuszenie, szantaż związany z uzyskaniem od ofiary materiałów multimedialnych o charakterze seksualnym pod groźbą ich szerszego udostępnienia; może wiązać się uzyskiwaniem materialnych korzyści.
Klasyfikacja jest podzielona na sprawy dotyczące osób 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.).

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.

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

1 975
Zgłoszone do odpowiedniego zespołu INHOPE oraz do Interpolu

281
Zgłoszone do administratorów serwisów

51
Zgłoszone do ISP

12
Zgłoszone do właściciela treści

107
Przekazane innemu podmiotowi (głównie CERT Polska)

145
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.

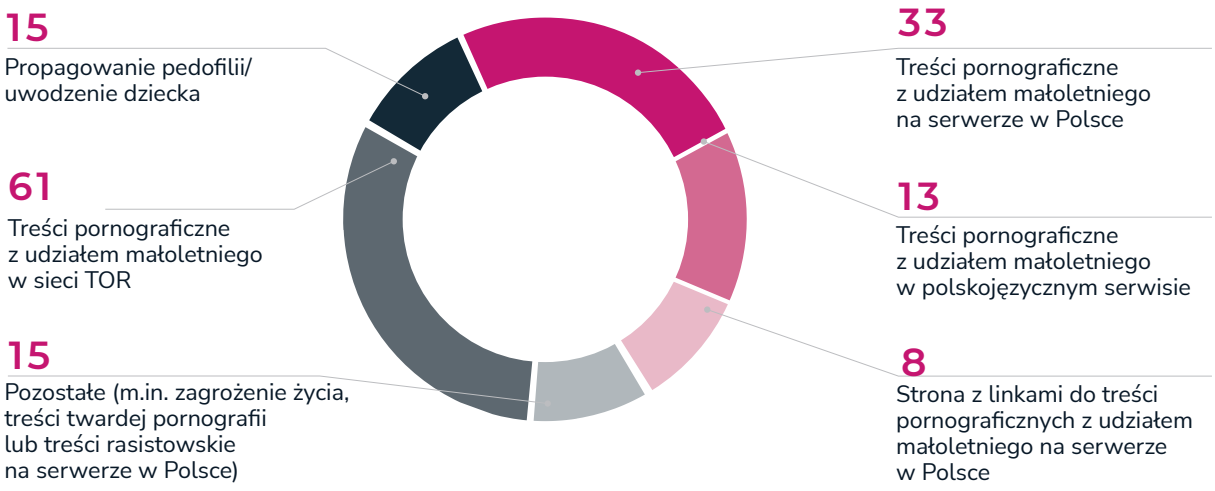
Zgłoszone do ISP
Przesłanie zawiadomienia o treściach o charakterze bezprawnym (dotyczących CSAM) zgodnie z art. 14 Ustawy o świadczeniu usług drogą elektroniczną w przypadku hostingodawcy w Polsce lub poinformowanie hostingodawcy znajdującego się poza zasięgiem INHOPE o bezprawnych treściach (dotyczących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

Zgłoszone do właściciela treści
Zgłoszenie dotyczące treści o szkodliwym charakterze skierowane do autora treści celem 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 Fundacja Dajemy Dzieciom Siłę).

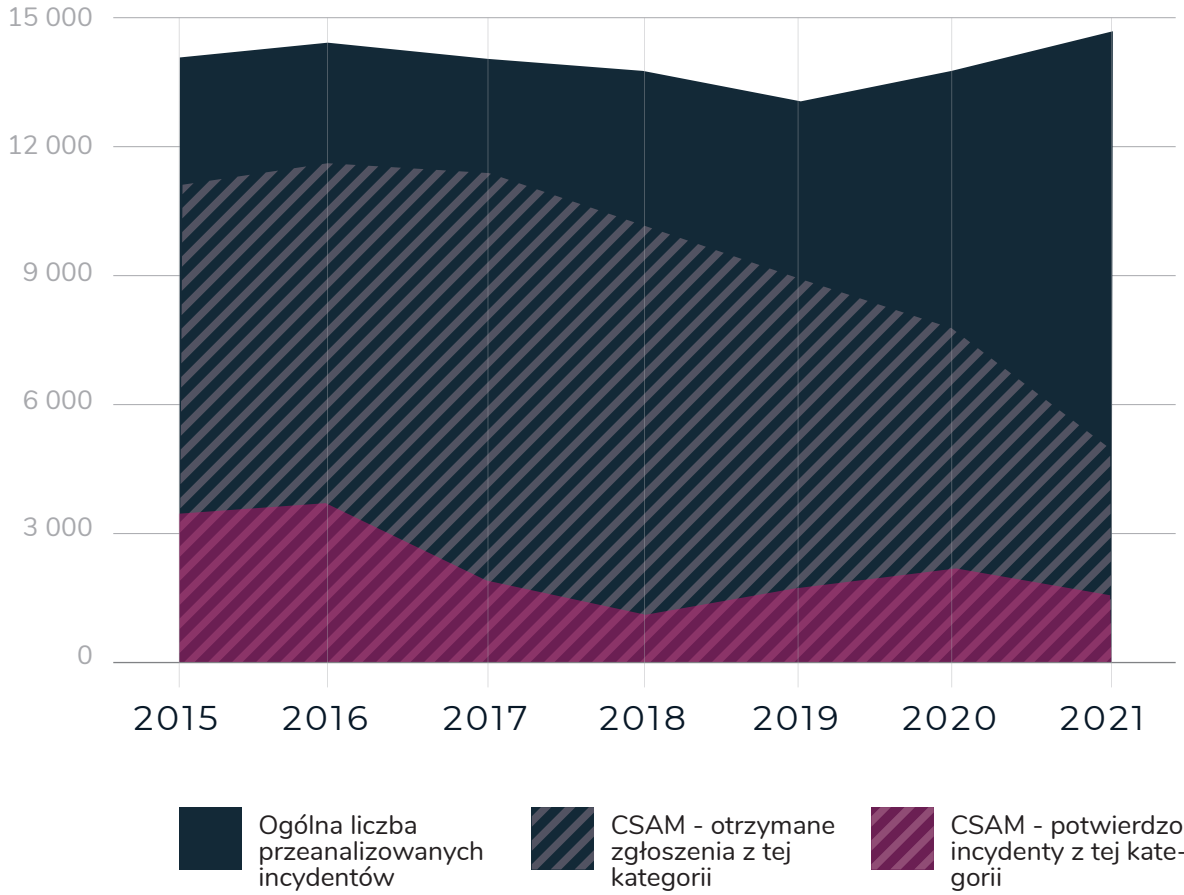
Zgłoszone Policji
Przekazane do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji.

8 | Zgłoszenia przesłane do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji



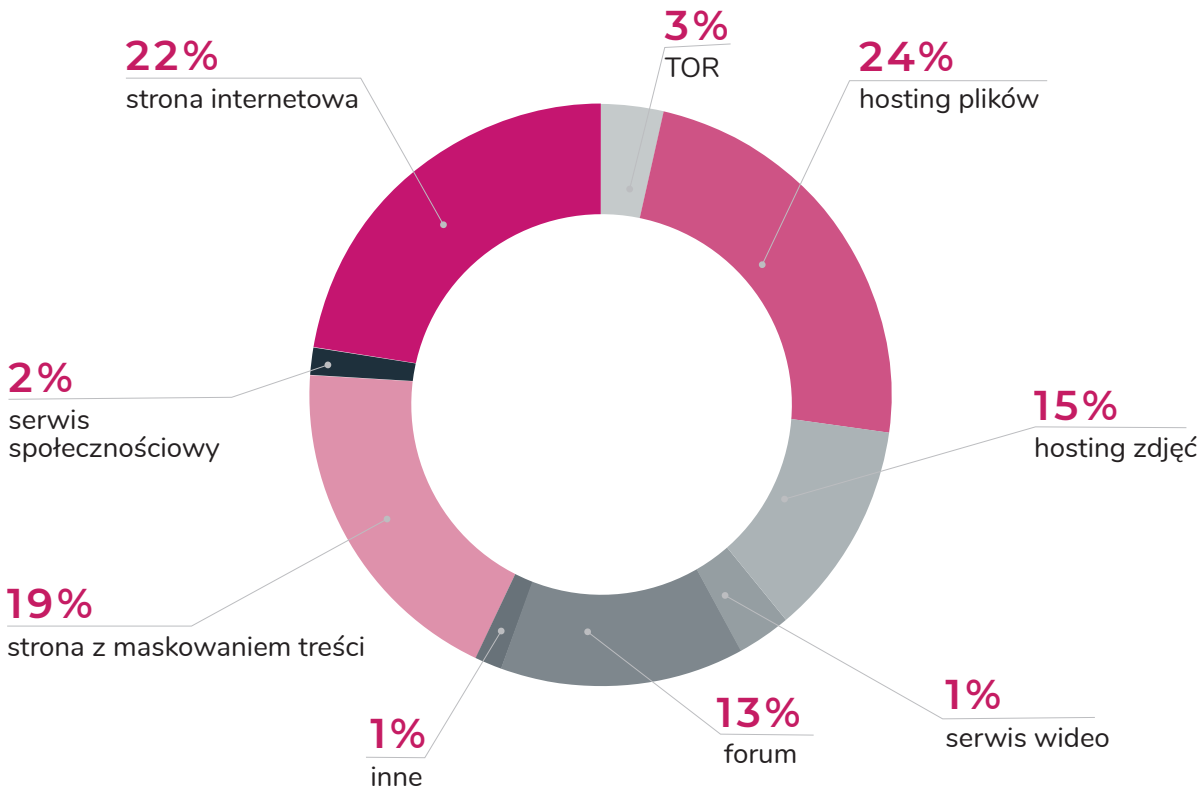
Analiza treści CSAM

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



	2015	2016	2017	2018	2019	2020	2021
Ogólna liczba przeanalizowanych incydentów wszystkich kategorii	14 277	14 298	13 962	13 239	12 517	13 400	14 754
CSAM - otrzymane zgłoszenia z tej kategorii	11 227	11 759	11 457	10 784	9 194	8 021	6 778
CSAM - potwierdzone incydenty z tej kategorii	3 029	3 126	2 459	1 998	2 295	2 517	2 069

10 CSAM analizowany przez Dyżurnet.pl - lokalizacja w usługach internetowych (n=2069)



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*".

Warto zaznaczyć, że z ogólnej liczby 2065 adresów url, na których eksperci Dyżurnet.pl zidentyfikowali CSAM, 1930 było unikalnych. Innymi słowy, powtórzenia stanowiły 7 procent ogólnej liczby incydentów CSAM i dotyczyły głównie stron maskujących swoją treść. Specyfika tych stron wymaga podania 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

5 594

Rozpoznane wcześniej przez zespoły INHOPE

3 782

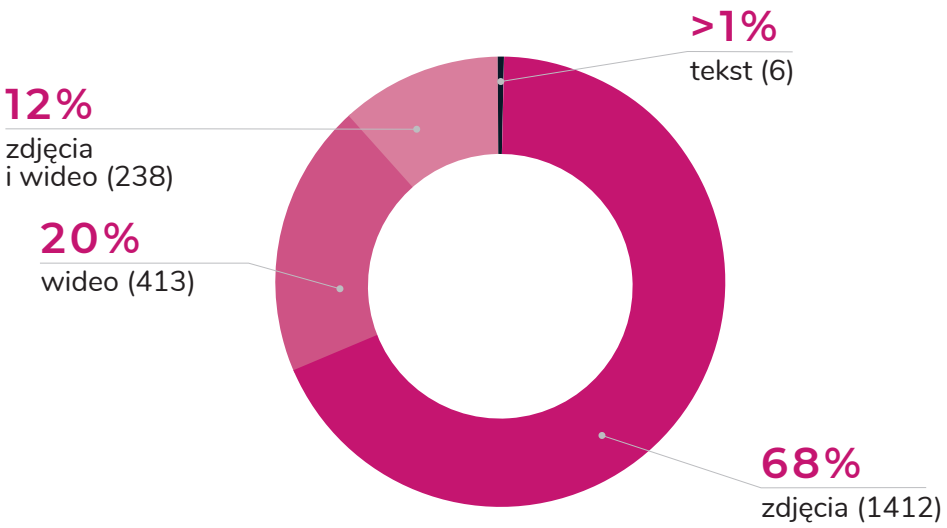
Analizowane po raz pierwszy przez Dyżurnet.pl

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.

Z drugiej strony, liczba analizowanych po raz pierwszy plików pokazuje wkład zespołu Dyżurnet.pl w budowanie bazy rozpoznanych już plików zawierających CSAM.

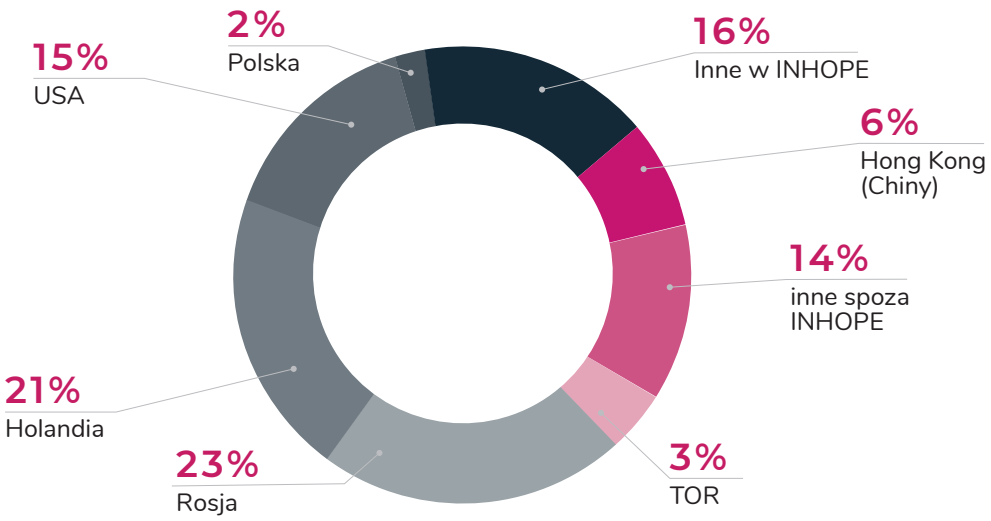
W roku 2021 udział treści analizowanych po raz pierwszy przez Dyżurnet.pl wynosił 40 procent.

12 | CSAM analizowany przez Dyżurnet.pl – rodzaj treści (n=2069)



61 incydentów z ogólnej liczby 2069 dotyczyło treści przedstawiających wytworzony lub przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej. Takie zazwyczaj wygenerowane komputerowo i względnie 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=2069)

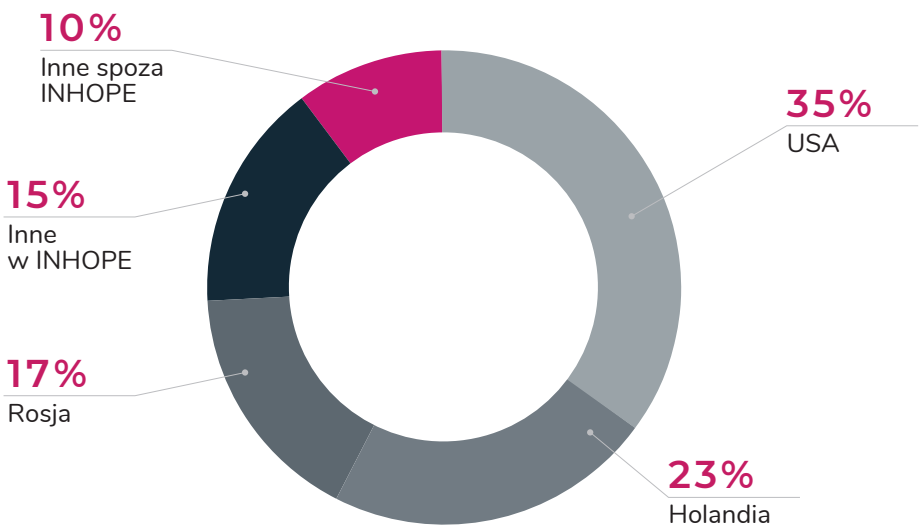


Lokalizacja serwera z treścią CSAM jest kluczowa dla skutecznej reakcji. Zespół Dyżurnet.pl wyróżnia dwa rodzaje lokalizacji:

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

Przykładowo – strona http://abc.com 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 Rosji. Lokalizację plików CSAM pokazuje wykres nr 14.

14 | CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do plików foto/wideo (n=3782)



W roku 2021 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 2021 było to 23 procent (2020 – 7 procent, 2019 – 11 procent)

W odniesieniu do plików foto/wideo w roku 2021 było to 10 procent (2020 i 2019 – po 4 procent)

W związku z tą tendencją wypracowane zostały nowe standardy i procedura pozwalająca określonym zespołom Stowarzyszenia interweniować bezpośrednio u zagranicznego hostingodawcy w celu usunięcia treści CSAM.

15 | CSAM analizowany przez Dyżurnet.pl – podział ze względu na kategorię treści (n=3782)

57%

BASELINE CSAM

43%

NATIONAL CSAM

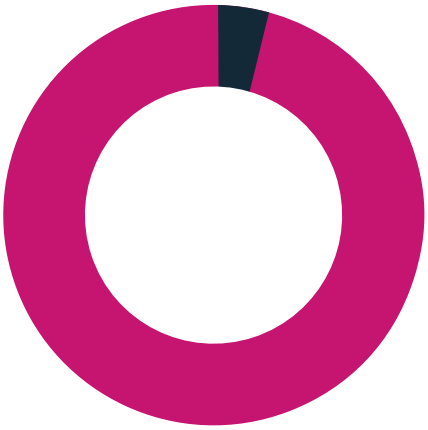
Baseline CSAM (kryteria nielegalności we wszystkich państwach współpracujących z Interpolem):

- 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. (materiały z osobami młodszymi klasyfikowane są jako Baseline CSAM)
- Treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej

16 | CSAM analizowany przez Dyżurnet.pl – udział treści o charakterze pornograficznym wytworzonych przez ofiary (self-generated sexual content) (n=2069)



92%

NON SELF-GENERATED CONTENT (1908)

8%

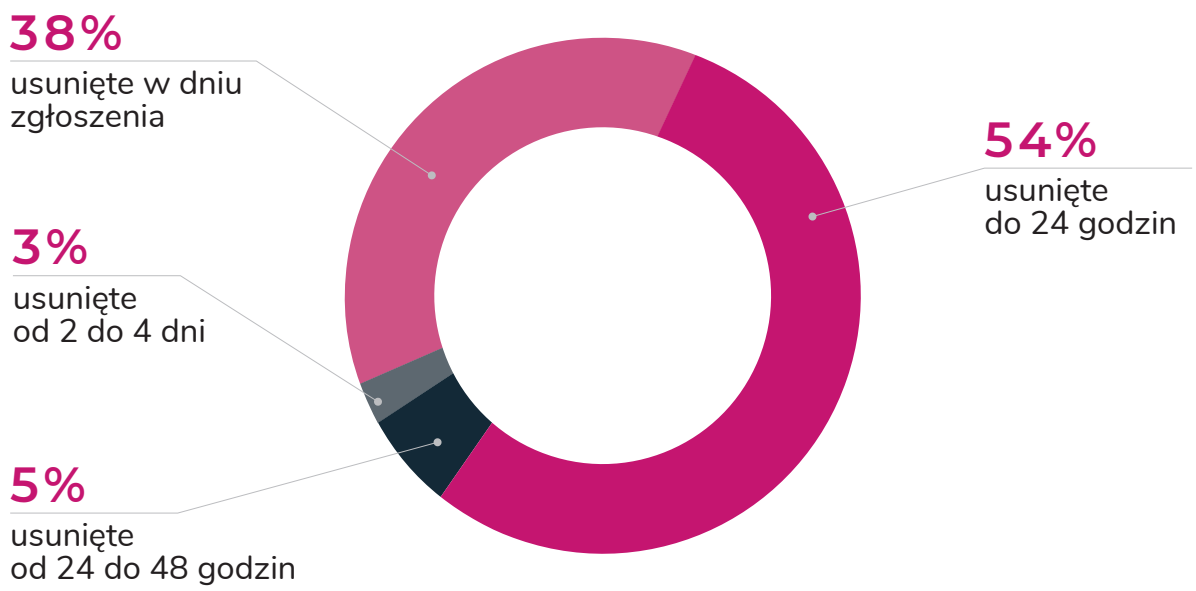
SELF-GENERATED CONTENT (161)

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."[4]

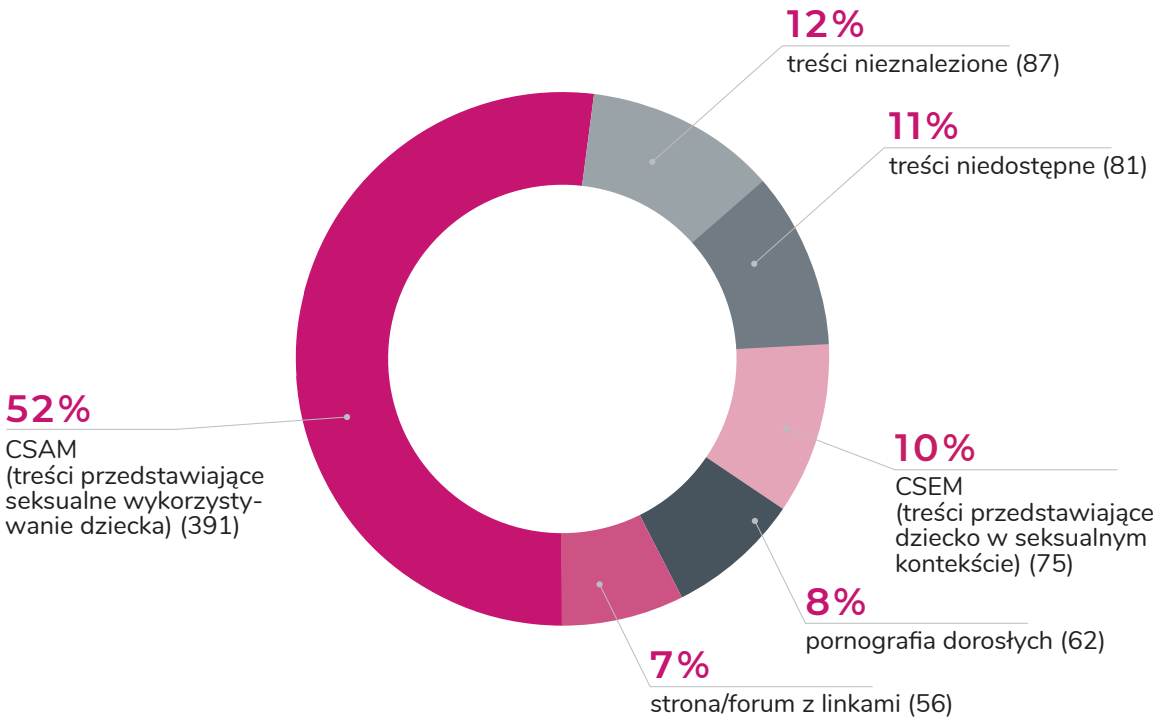
Po obserwowanym przez ekspertów Dyżurnet.pl wzroście udziału tego typu materiałów w ogólnej liczbie CSAM z 9 procent w roku 2019 do 14 procent w roku 2020, liczba zaklasyfikowanych w ten sposób treści spadła do 8 procent i okazała się najmniejsza w przeciągu 3 lat. Warto jednak zaznaczyć, że pojedyncze 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.

4. 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=37)



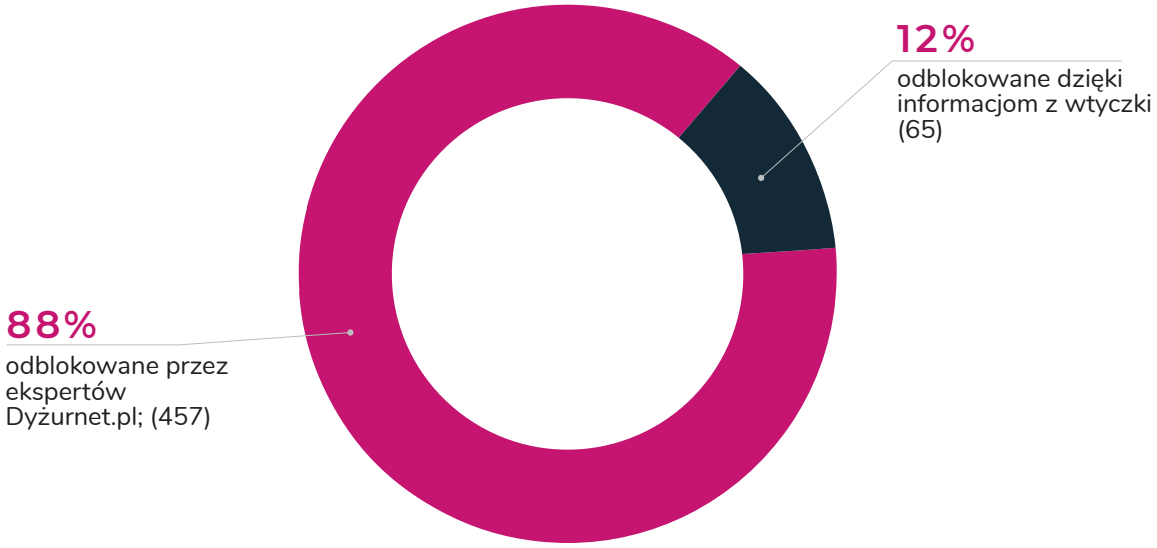
18 | Klasyfikacja stron maskujących swoją treść (n=752)



Liczba stron maskujących swoją treść analizowanych przez zespół Dyżurnet.pl w roku 2021 wyniosła 752, czyli porównywalnie do roku poprzedniego (w roku 2020 – 784). Ekspertom Dyżurnet.pl udało się odblokować ukrytą treść w 70 procentach przypadków, co stanowi zdecydowanie lepszy wynik niż w roku poprzednim, gdy ukrytą treść udało się odblokować w 53 procentach (jako odblokowaną traktuje się stronę, która wyświetliła treść z następujących kategorii: CSAM, CSEM, strona/forum z linkami).

W pewnym stopniu do poprawy skuteczności przyczyniła się większa ilość zgłoszeń przesyłanych poprzez wtyczkę do raportowania, która została opracowana specjalnie do zgłaszania stron maskujących swoją treść. W roku 2020 zespół Dyżurnet.pl za jej pomocą otrzymał 91 zgłoszeń, natomiast w roku 2021 już 238. Liczba stron odblokowanych dzięki informacjom przekazanym za pomocą wtyczki wyniosła 65, co stanowi 12 procent ogólnej liczby odblokowanych stron maskujących swoją treść.

19 | Udział stron maskujących swoją treść odblokowanych dzięki informacjom przekazanym poprzez wtyczkę do raportowania (n=522)



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 database***[6]), umożliwiając podjęcie działań w celu identyfikacji zarówno ofiar, jak i sprawców.

W roku 2021 eksperci Dyżurnet.pl wprowadzili do ICCAM 1 850 raportów dotyczących adresów URL zawierających nielegalne treści. Znajdowało się tam ogółem 9 376 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 2021 miała miejsce w przypadku 281 incydentów.

W 51 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 107 spraw zostało przekazanych innym podmiotom - m.in. działającemu w ramach NASK-PIB zespołowi CERT Polska czy telefonom interwencyjnym prowadzonym przez Fundację Dajemy Dzieciom Siłę.

145 incydentów zostało zgłoszonych do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Dotyczyły one przede wszystkim seksualnych nadużyć wobec dzieci. Zgłoszenia związane z CSAM stanowiły 80 procent przekazanych incydentów (na polskich serwerach – 29 procent, w polskojęzycznych serwisach – 9 procent, w sieci TOR – 42 procent). 10 procent przesłanych spraw dotyczyło uwodzenia dziecka i propagowania zachowań o charakterze pedofilskim.
10 procent pozostałych spraw zgłoszonych do Policji obejmowało inne treści znajdujące się na serwerach w Polsce (treści twardej pornografii, treści rasistowskie lub sprawy związane z zagrożeniem życia).

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

TRENDY I ZJAWISKA

Czy wiesz co twoje dziecko nagrywa na YouTube?

Od wiosny 2021 roku zespół Dyżurnet.pl odnotował zwiększoną liczbę zgłoszeń dotyczących materiałów wideo nagrywanych przez kilkuletnie dzieci, zazwyczaj dziewczynki. Według osób zgłaszających, mogły być one narażone na niebezpieczny kontakt ze strony osób seksualnie zainteresowanych dziećmi.

Nagrania te w przeważającej części stanowiły „urywki" lub „pamiętniki" z życia dziecka, takie jak oprowadzanie po swoim pokoju ***(„room tour")***, tańce czy wokalny playback do ulubionej muzyki, prezentacja nowego łóżka, nowej fryzury, ubrań, „gra w grę" czy luźne komentarze. Materiały te nagrywane są zazwyczaj samodzielnie w pokoju dziecka, choć zdarzają się też nagrywane wspólnie z innymi nieletnimi osobami. Są względnie słabej jakości z powodu nagrania smartfonem lub tabletem.

Oglądalność takich filmów jest różnorodna – od kilku do kilkuset w ciągu pierwszych dni od publikacji, jeden z materiałów miał aż ćwierć miliona odsłon. Pada tam symptomatyczne stwierdzenie dobrze prezentujące sposób myślenia niektórych z autorów takich materiałów: ***„Nie wiemy co robić, ale to nasze życie. I tak musimy (...) się nagrywać, bo w ogóle nasze życie na tym zależy. Jak nie będziemy się nagrywać, nie będzie kasy (...) Mówimy to na żywo. YouTube jest najlepsze na świecie!"***

Duża część dzieci prezentuje w nagranych przez siebie materiałach odzwierciedlenie zachowań swoich vlogowych idoli. Pojawiają się stwierdzenia typu: ***„witam was na moim kanale***", prośby o ***„łapki w górę"*** i ***„subskrypcje***".

Warto przytoczyć też jedną z wypowiedzi około dziewięcioletniej autorki materiału: ***„Jeżeli macie tiktoka to wpadajcie na konto, mam już 2K tylko błagam nie banujcie mi bo się powieszę. 2 lata pracowałam na 2K. Jeżeli mnie zbanujecie to obiecuję Wam, że wtedy się zabiję".***

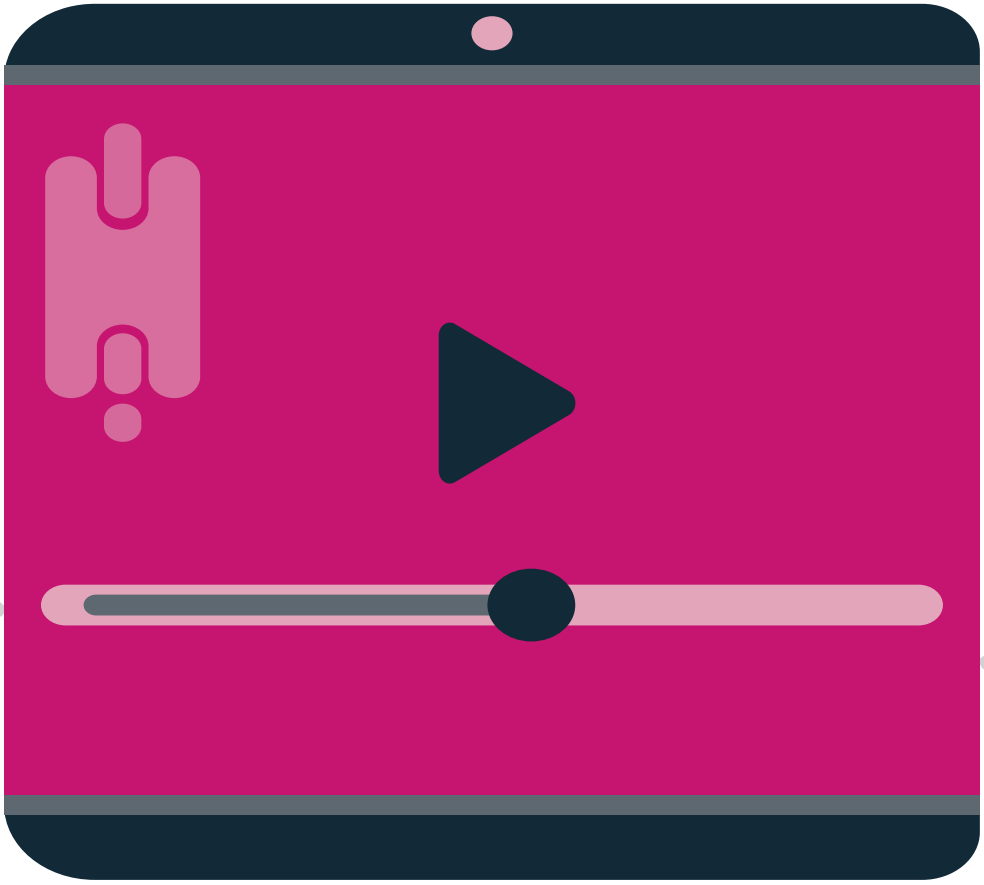
Przy czym w rzeczywistości prawdziwe konto autorki miało niecałą setkę obserwujących, a w materiale odnosiła się do konta innej „influencerki". Widać zatem potrzebę zwrócenia na siebie uwagi lub nawet wywołania sensacji tak silną, że autor jest skłonny do zamieszczania informacji wprowadzających w błąd postronnych obserwatorów.

Od końca sierpnia 2021 roku licznie zaczęły pojawiać się materiały w trochę innym typie. Tym razem w postaci kanałów dziewczynek nagrywających i publikujących codziennie po kilka filmików. Trwają one maksymalnie 15 sekund i prezentują taniec lub muzyczny playback. Kanały te mają po kilka tysięcy subskrybentów, a niektóre filmiki po kilka tysięcy wyświetleń. Zdarzają się układy taneczne, kiedy to dziewczynki w trakcie tańca zdejmują bluzki i pokazują bieliznę lub eksponują pośladki. Powody powstania tego typu materiałów mogą być różne, od chęci zwrócenia na siebie uwagi, przez nudę, po możliwość bycia dziecka w procesie child groomingu (uwodzenie dziecka w sieci). Często młode osoby motywowane chęcią zdobycia popularności na znanych serwisach podejmują takie aktywności.

Poprzez ustawienie tego typu sprzętu na podłodze i nagranie „od dołu” zdarza się, że stojącym lub tańczącym dziewczynkom widać bieliznę, co faktycznie może interesować osoby seksualnie zainteresowane dziećmi.

W przypadku materiałów o charakterze seksualnym, zespół Dyżurnet.pl podejmuje interwencje i zgłasza je do serwisu YouTube, który niezwłocznie je usuwa. Istotne jest, że w zdecydowanej większości materiałów tworzonych przez dzieci zablokowana jest możliwość zamieszczania komentarzy.

Warto pamiętać, że upublicznianie przez dziecko swojego wizerunku w sieci może wiązać się z ryzykiem zarówno ze strony rówieśników mogących poddać je surowej krytyce, jak i przyciągnąć uwagę wymienionych na wstępie osób o skłonnościach pedofilskich. Warto towarzyszyć dziecku w jego internetowej aktywności, wspierać i kontrolować podczas drogi do „bycia słynnym influencerem”.



Uwodzenie dziecka w internecie

Problem uwodzenia nieletnich, tzw. „***child grooming***" wraz z postępem technologii, anonimowością w świecie wirtualnym, brakiem świadomości i kontroli rodzicielskiej przybrał niepokojące rozmiary[6].

Choć w otrzymywanych przez Zespół danych można zauważyć powtarzające się schematy interakcji wykorzystywane przez sprawców, warto zaznaczyć, że zarówno sposób prowadzenia rozmowy, jak również reakcje małoletnich nie są jednolite. Sprawcy mogą być osobami uciekającymi się do szantażu, ale też mogą oferować wynagrodzenie w zamian za „przysługi". Mogą podszywać się np. pod agencję modelingową lub autorytet (choćby administrację serwisu), udawać osoby w wieku bliskim ofiary, ale też mogą być osobami wprost informującymi o swoim prawdziwym wieku. Część z nich to osoby kryjące się za fałszywymi kontami od samego początku konwersacji, żądające intymnych zdjęć oraz przesyłające własne fotografie czy wideo (często wyraźnie posługując się automatycznym tłumaczeniem wiadomości z innego języka), część to osoby znane dziecku z innego serwisu lub z życia poza internetem.

Przykładowa treść konwersacji (pisownia oryginalna):

„ - masz poważne kłopoty
- 😬😱😬
- Wyślę teraz nasze rozmowy, zdjęcia i filmy, aby nagrać całą Europę, możesz zobaczyć swoją twarz i ciało nago, nie polecam blokowania
TERAZ 👍"

Zdarzają się też interakcje dążące do zaprzyjaźnienia się lub symulowania związku, budujące bliskość i zaufanie – jednak widać w nich niepokojące elementy dążenia do utrzymania relacji w tajemnicy – „niemówienia nikomu", „naszej tajemnicy", „obawy, bo to nielegalne". Często też mimo pozornej ugodowości widać silny nacisk na treści seksualne w rozmowie i ciągłe nawracanie do tej tematyki – a przy tym naruszanie i przesuwanie granicy komfortu osoby małoletniej.

Przykładowa treść konwersacji (pisownia oryginalna):

„ - Mogę z Tobą pisać
Nie powiesz nikomu
- Nie
Zrobię co mi karzesz
Wszystko tylko nie zglaszaj
👍
Wszystko proszę
Co zechcesz
Jak chcesz to pokaże Ci na ksmerce
Wszystko zrobię proszę
Co zechcesz Nie zgłosisz? Proszę"

6. https://repozytorium.uph.edu.pl/bitstream/handle/11331/2671/Wrobel-Delegacz.W.Grooming_zagrozenie.pdf?sequence=1 – strona 12

Dla części przypadków charakterystyczne mogą być gwałtowne zmiany nastroju – sprawca bardzo szybko przechodzi od czułego i proszącego do wściekłego i atakującego tonu, zwłaszcza gdy jego żądania nie są spełniane. W większości sprawcy są świadomi grożących im konsekwencji – nie zawsze są chętni do podania swoich prawdziwych danych osobowych lub zdjęć twarzy, ale zależy im na uzyskaniu zdjęć dziecka.

Cel rozmowy może być różny – niektórzy sprawcy pragną zdalnego zaspokojenia fantazji poprzez sexting (niekoniecznie zawierający wysyłanie zdjęć), inni dążą do spotkania z dzieckiem, jeszcze inni pragną zdobyć jak najwięcej zdjęć lub filmów.

Reakcje dzieci na tego typu interakcje są również bardzo zróżnicowane, często zdają się być konsekwencją niewiedzy lub odrazy wynikających ze zbyt młodego wieku lub też ciekawości i zainteresowania tematami seksualnymi, dotyczy to zwłaszcza dzieci w wieku nieco starszym. Niektórzy młodzi ludzie wprost odrzucają nowe znajomości ze względu na ich zbytnią natrętność lub bezpośredniość, a czasem też ze względu na sam wiek sprawcy – nie chcą kontynuować rozmowy z dorosłym. Część młodzieży zostaje wciągnięta w silnie nacechowaną seksualnie interakcję. Czasami młode osoby poszukują online bliskości, nie zawsze są świadome wieku osoby, z którą angażują się w relację – takie osoby mogą zostać wciągnięte w narrację, że wymiana intymnych materiałów jest niezbędna i bezpieczna (w końcu wysyłane są tylko dla „znajomego", który obiecał dyskrecję). W niektórych przypadkach można odnieść wrażenie, że dziecko nie ma świadomości, że rozmowę, która staje się niekomfortowa można zakończyć w każdym momencie, a także zablokować zbyt natrętnego interlokutora.

Częstym elementem manipulacji wprowadzanym przez sprawców jest wywołanie u młodej osoby poczucia dumy lub potrzeby dorównania rówieśnikom – objawia się ona w stwierdzeniach typu „znam osoby w twoim wieku, które już to robią", „wstydzisz się?", „boisz się?", a także w kładzeniu nacisku na swoje doświadczenie w sprawach seksualnych, możliwość nauki czegoś przyjemnego i „dorosłego", przyjemność płynącą z tego typu spotkań, a nawet potencjalne bezpośrednie korzyści dla młodego człowieka - wynagrodzenie rzeczowe lub pieniężne. Tematy związane z seksualnością zostają przez sprawcę maksymalnie spłycone, ale ciągle do nich powraca, nawet mimo chęci dziecka do zmiany tematu. Często występuje też natarczywe sprawdzanie obecności drugiej strony na czacie.

Przykładowa treść konwersacji (pisownia oryginalna):

„Z kim kotek
Z kim idziesz kotem
Jesteś kochanie
😍😍😍😍😍😍😍😍😍😍
Czemu nie piszesz kotek
Jestes tam kochanie 😍😍😍😍😍😍😍
Czemu nie piszesz kotek
Jestes zla na mnie kochanie"

Innym sposobem manipulowania dzieckiem w celu uzyskania intymnych materiałów jest dążenie w konwersacji do zdejmowania z siebie odpowiedzialności, zrzucanie winy na ofiarę – „jeżeli chcesz, to wyślę ci...", „jeżeli chcesz, możesz mi wysłać...", „on/ona sama chciała", a także ukazywanie popędu seksualnego jako siły niezależnej od osoby – „tylko ty mi możesz pomóc... już nie wytrzymuję". Mimo że temat seksualności najczęściej inicjowany jest wyłącznie przez sprawcę, sposób prowadzenia rozmowy wywiera presję na współuczestnictwo i ma na celu obarczenie winą ofiary. Oczywiście, nawet w wypadkach inicjowania sekstingu przez osobę małoletnią, nie jest to w żadnym stopniu okolicznością łagodzącą ani usprawiedliwieniem.

Przykładowa treść konwersacji (pisownia oryginalna):

> *„- Ona sama się mnie zapytała czy jej pokaże*
> *- Sama tego chciała"*

Otrzymane w trakcie tego typu rozmów zdjęcia mogą być wykorzystane do bezpośredniego zaspokojenia osobistych potrzeb sprawcy, ale mogą też trafić do puli zdjęć wymienianych pomiędzy osobami seksualnie zainteresowanymi dziećmi lub posłużyć do szantażu ofiary na późniejszych etapach relacji w celu uzyskania większej liczby zdjęć pod groźbą udostępnienia dotychczasowych zbiorów rodzinie i znajomym młodego człowieka. Dlatego wyjątkowo ważne jest ostrożne dysponowanie swoim wizerunkiem, zwłaszcza tym, który wyjęty z kontekstu może być kompromitujący lub wysoce problematyczny.

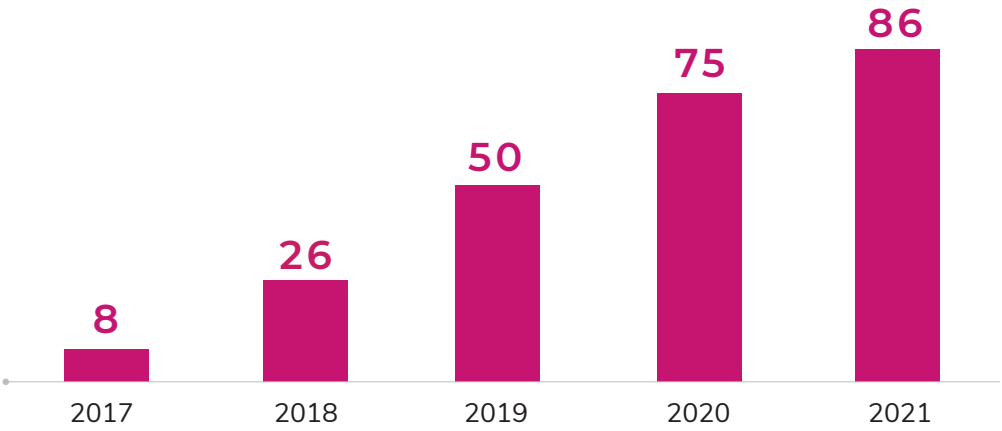
Poza ograniczeniem zaufania względem ludzi poznanych online (niekoniecznie są oni tymi, za których się podają), ważne jest zwrócenie uwagi na własne odczucia i motywacje – czy motywacja jest własna czy spowodowana zewnętrzną presją wywieraną na różne sposoby przez drugą osobę – poprzez powoływanie się na przyjaźń, warunkowanie tym istnienia związku, wzbudzanie współczucia i chęci pomocy. Czy na podstawie wysłanego zdjęcia można łatwo zidentyfikować osobę na nim uwiecznioną? Czy po ewentualnym „wycieku" zdjęć będzie można zidentyfikować źródło wycieku? Sprawcom może zależeć na wyraźnej identyfikacji osoby na zdjęciu oraz „unikalności" zdjęcia.

Udostępniając informacje o sobie w internecie należy się liczyć z tym, że mogą one zostać powielone i rozpowszechnione dalej, a ich całkowite usunięcie z sieci będzie właściwie niemożliwe.

Szantaż na tle seksualnym

Szantaż na tle seksualnym to problem coraz powszechniej odnotowywany przez ekspertów zespołu Dyżurnet.pl. W raporcie za rok 2020 zjawisko zostało szeroko ujęte i opisane. W tym raporcie uwaga zostanie zwrócona na skalę zjawiska.

W 2021 roku zespół odnotował 52 zgłoszenia dotyczące tego procederu oraz 34 tak zwane „**sextortion SCAM**", czyli zgłoszenia dotyczące automatycznych, masowo wysyłanych wiadomości udających szantaż na tle seksualnym w celu wyłudzenia pieniędzy. W sumie w roku 2021 zostało odnotowane 86 zgłoszeń. Jak widać na poniżej załączonej tabeli trend zgłoszeń dotyczących szantażu na tle seksualnym (biorąc pod uwagę również „sextortion SCAM") w podziale na lata jest wzrostowy. Zgłoszenia związane były głównie z osobami pełnoletnimi. Jedynie trzy otrzymane zgłoszenia dotyczyły osób poniżej 15 roku życia.



Zgłoszenia szantażu na tle seksualnym i sextortion SCAM w podziale na lata

Statystyka ta pokazuje, że ofiarami szantażu na tle seksualnym bardzo często padają osoby dorosłe, które powinny dysponować wiedzą oraz umiejętnością oceny ryzyka, pozwalającymi na ustrzeżenie się przed tego typu zagrożeniem. Co więcej, w pewnym stopniu ciąży na tych osobach obowiązek edukowania w tym zakresie najmłodszych użytkowników internetu, najczęściej własnych dzieci. Tymczasem brak świadomości oraz zainteresowania tematem cyfrowych zagrożeń nierzadko skutkuje podejmowaniem niebezpiecznych aktywności online również przez dorosłych, dlatego warto uzupełniać wiedzę na temat tego zjawiska. Więcej informacji na temat szantażu na tle seksualnym jest dostępne w publikacji: *Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu*[7]. oraz w artykułach zespołu Dyżurnet.pl dostępnych na stronie. Poruszana jest w nich skala problemu, sygnalizowane jest jak łatwo paść ofiarą tego typu działalności bez odpowiedniej świadomości oraz wskazane są „dobre praktyki", które pozwolą zabezpieczyć się przed szantażem na tle seksualnym.

7. Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki, Seria: Internet – Edukacja – Bezpieczeństwo, Warszawa, 2019

Moderacja treści i regulaminy serwisów a dystrybucja materiałów CSAM

Mimo iż w polskim prawie nie znajdziemy regulacji odnośnie procedur reagowania na incydenty związane z dystrybucją materiałów CSAM, to jednak można zaobserwować pozytywne postawy moderatorów włączających się w działania na rzecz krzywdzonych dzieci. Jako przykład można wskazać moderatorów jednego z polskich portali, którzy wzorowo zareagowali na zaistniały w ich witrynie incydent. W ubiegłym roku portal padł bowiem ofiarą zorganizowanej akcji, w ramach której na stronie udostępniano linki prowadzące do materiałów przedstawiających seksualne wykorzystywanie dzieci. Co więcej, użytkownicy udostępniający te treści podszywali się pod państwowe instytucje i organizacje działające na rzecz bezpieczeństwa w internecie. Cała sytuacja została przez administrację serwisu zgłoszona bezpośrednio do Zespołu Dyżurnet.pl.

Nie jest to jednak często spotykana reakcja, a zalecenia Komisji Europejskiej w obszarze przeciwdziałania rozprzestrzenianiu materiałów przedstawiających seksualne wykorzystywanie dzieci sięgają nawet dalej[8]. Rekomendowana jest nie tylko bezpośrednia współpraca między dostawcami usług internetowych a zespołami reagowania na tego typu incydenty, ale podkreślana jest również potrzeba wprowadzenia działania opartego na tzw. ***trusted flaggers***, czyli zaufanych podmiotach zgłaszających, uwzględniającego uproszczone, a przede wszystkim skuteczniejsze procedury, pozwalające na szybsze usunięcie nielegalnych treści. Wprowadzenie ***trusted flaggers*** w systemach dostawców usług pozwala na priorytetyzowanie zgłoszeń pochodzących od zaufanych instytucji, a co za tym idzie, natychmiastową reakcję.

Dodatkowo, zgodnie z modelem WeProtect[9] , każdy serwis umożliwiający użytkownikom udostępnianie własnych treści powinien udostępnić również łatwą drogę ich zgłaszania, mechanizm pozwalający reagować w przypadku incydentów, przede wszystkim tych związanych z bezpieczeństwem dzieci. Informacja o zakazie udostępniania materiałów przedstawiających seksualne wykorzystywanie dzieci powinna być również uwzględniona w regulaminie serwisu z wyszczególnieniem zakazu zarówno produkcji, dystrybucji, jak i wyświetlania takich materiałów. Taki portal powinien dysponować również jednostką – czy to konkretnym pracownikiem czy całym zespołem – odpowiedzialną za przetwarzanie zgłoszeń dotyczących materiałów CSAM. Jednocześnie jednak każdy pracownik przyjmujący zgłoszenia powinien być przygotowany na sytuację, w której będzie miał kontakt z nielegalnymi i destrukcyjnymi treściami, powinien być poinformowany o ryzyku, dobrowolnie wyrazić na nie zgodę, a także posiadać odpowiednią wiedzę i umiejętności, aby takie zgłoszenie przyjąć i poddać analizie. Każdy taki pracownik powinien mieć również zapewnione odpowiednie warunki pracy oraz wsparcie, ze szczególnym uwzględnieniem wsparcia psychologicznego.

8. Study on Framework of best practices to tackle child sexual abuse material online, 2017
9. www.weprotect.org/frameworks/industry

Prawa dziecka w środowisku cyfrowym

Ogromne ilości danych o użytkowniku, które powstają wraz z korzystaniem z usług cyfrowych wymagają tworzenia oraz ciągłej aktualizacji praw użytkowników. Ze względu na konieczność szczególnej ochrony, dzieci powinny mieć zapewnione najwyższe standardy bezpieczeństwa i stosowania istniejących regulacji, równocześnie dające im przestrzeń do realizacji praw takich jak: prawo dostępu do środowiska cyfrowego, prawo do swobodnej wypowiedzi i do informacji online, prawo do uczestnictwa i do zabawy, prawo do nauki i edukacji medialnej, prawo do ochrony i bezpieczeństwa oraz prawo do prywatności i ochrony danych.

Dzieci wykorzystują internet zależnie od swoich potrzeb, które realizują za jego pomocą i które wpływają na wiele aspektów życia na różnych poziomach, np. potrzeba interakcji, ekspresji, przynależności itp. oraz jako przestrzeń do spędzenia czasu wolnego i rozrywki. Poza wieloma zaletami postępująca cyfryzacja niesie również zagrożenia, np. ułatwia nowe rodzaje dyskryminacji, takie jak cyberbullying (przemoc w internecie) lub mowę nienawiści, które szerzą się w sieci. Młode osoby należy przede wszystkim chronić przed materiałami szkodliwymi i nielegalnymi dostępnymi online, na które mogą trafić intencjonalnie lub przypadkowo.

Dlatego też tworzenie aplikacji lub serwisów, których użytkownikami są lub mogą być dzieci powinno realizować zasadę polegającą na budowaniu tych narzędzi w oparciu o zapewnienie jak najwyższego bezpieczeństwa najmłodszym użytkownikom. Wiele popularnych serwisów, z których korzystają najmłodsi stosuje jedynie weryfikację wieku poprzez wpisanie daty urodzenia, co może nie być wystarczającym zabezpieczeniem przed korzystaniem z tych narzędzi przez osoby, dla których nie są one przeznaczone ze względu na wiek. Wynikający z nieświadomości zagrożeń, brak weryfikacji aplikacji i serwisów użytkowanych przez dziecko ze strony rodziców i opiekunów, również może być czynnikiem prowadzącym do kontaktu młodych użytkowników z materiałami szkodliwymi lub nielegalnymi.

Warto zaznaczyć, że rodzice lub opiekunowie często podejmują zachowania ryzykowne lub szkodliwe w sieci, które w przyszłości mogą zaszkodzić najmłodszym. Ważną sprawą, którą należy zaznaczyć jest kwestia prywatności, ponieważ dzieci mają również prawo do prywatności online, co oznacza, że publikacja materiałów z dzieckiem w internecie powinna być z nim wcześniej uzgodniona.

Budowanie bezpieczeństwa dzieci i młodzieży w internecie powinno opierać się na współpracy osób tworzących serwisy, rodziców i opiekunów oraz edukatorów. Znajomość zagrożeń i niebezpieczeństw w internecie oraz tego, jak się przed nimi chronić jest podstawą budowania i tworzenia internetu.

Czy internet może zapomnieć?

Niejednokrotnie do Zespołu Dyżurnet.pl zgłaszane są treści, które nie są nielegalne, a jedynie w sposób nielegalny udostępnione, np. zdjęcia upublicznione bez zgody osoby na nich uwiecznionej. Tego typu zgłoszenia nie wchodzą w zakres działalności Zespołu, ponieważ brak jest podstawy prawnej do podjęcia konkretnych czynności – w takich przypadkach może to zrobić tylko osoba poszkodowana. Podobnie jest z upublicznieniem danych wrażliwych, np. danych dotyczących kart kredytowych czy konta bankowego oraz informacji medycznych. W takich okolicznościach można skorzystać z prawa do bycia zapomnianym, które przysługuje każdej osobie na podstawie rozporządzenia unijnego RODO, gwarantuje ono każdej osobie fizycznej prawo żądania usunięcia swoich danych osobowych przez administratora tych danych. Co więcej, administrator danych zobowiązany jest nie tylko dane te usunąć, ale również powiadomić o takim żądaniu wszystkie inne podmioty, którym te dane udostępnił. W szczególnych przypadkach usunięcie danych osobowych jest jednak niemożliwe. Sytuacja taka może się zdarzyć np. w obszarze działalności dziennikarskiej – jeśli dane zostaną uznane za istotne dla interesu publicznego mogą pozostać nieusunięte z uwagi na prawo do wolności wypowiedzi i informacji. Usunięcie danych może być także niemożliwe z powodu uwarunkowań prawnych, np. istnieje przepis prawa pracy wymagający przechowywania danych osobowych zatrudnianych pracowników przez wskazany okres, nawet po zakończeniu stosunku pracy. Podobne przepisy obowiązują sprzedawców internetowych oraz przetwarzanych przez nich danych osobowych klientów.

Prawo do zapomnienia przysługuje również w przypadku wyników podawanych przez wyszukwiarki Google i Bing. Tutaj również możemy zażądać usunięcia wszelkich wrażliwych danych. Zgodnie z instrukcjami udostępnianymi przez Google, brane jest także pod uwagę, czy dane są „niedokładne, nieadekwatne, nieistotne lub przesadzone", weryfikowany jest też wspomniany już interes publiczny. Każdy użytkownik, który zauważy w wynikach wyszukiwania Google wrażliwe lub nieprawdziwe dane na swój temat lub trafi w wyszukiwarce obrazów na zdjęcia opublikowane bez jego zgody może zgłosić ten fakt bezpośrednio do suportu Google, wypełniając stosowny formularz. Każda taka sprawa rozpatrywana jest indywidualnie, a osoba zgłaszająca informowana jest o podjętej decyzji. Warto jednak pamiętać, że wyszukiwarka jest jedynie agregatem treści w internecie. Usunięcie ich spośród wyników wyszukiwania oznacza więc jedynie deindeksację stron, na których informacje te się pojawiają, co oznacza że nie są one już widoczne w wynikach wyszukiwania danej wyszukiwarki, nadal jednak są dostępne online. W celu faktycznego usunięcia treści należy skontaktować się bezpośrednio z administracją serwisu czy strony internetowej, na której zdjęcia zostały udostępnione, ponieważ tylko administratorzy mogą usunąć materiały zamieszczane w ich witrynie.

Chociaż formalnie możliwe jest usunięcie zdjęć spośród wyników wyszukiwania grafiki Google, to jednak zdarza się, że pojawiają się trudności. Zgłoszenie może zostać odrzucone przez Google ze względu na wadliwy link URL lub inne problemy techniczne, ale może się też zdarzyć, że dany obraz występuje na jednej lub kilku stronach w kilku lub nawet kilkudziesięciu kopiach – wtedy usunięcie jednej z nich nie wywołuje widocznego efektu, każdy z tych materiałów należałoby deindeksować indywidualnie. Jeśli obraz przypisany jest do założonego w przeszłości konta internetowego, łatwiej może być usunąć wspomniane konto i w ten sposób próbować zapobiec wyświetlaniu się niepożądanych treści w wynikach wyszukiwania. Może także pomóc zmiana ustawień takiego konta. Kiedy pojawią się trudności przy egzekwowaniu prawa do bycia zapomnianym, warto szukać alternatywnych rozwiązań i być może zlikwidować materiał u źródła.

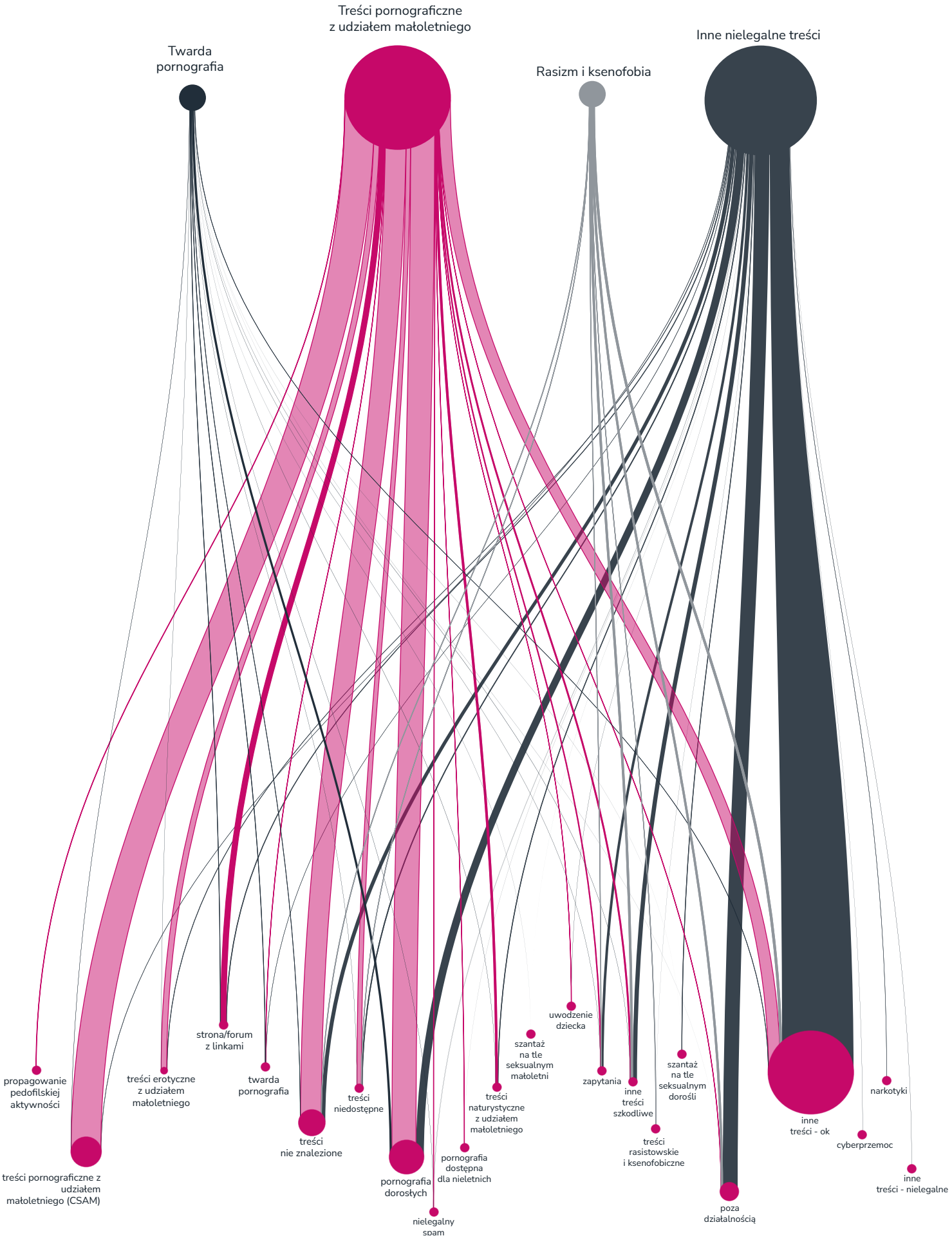
Zgłoszenia dotyczące treści legalnych

W ubiegłym roku po raz pierwszy odnotowano mniej zgłoszeń dotyczących materiałów przedstawiających seksualne wykorzystywanie dzieci niż incydentów z pozostałych kategorii. Zgłoszenia zdjęć i wideo CSAM stanowiły jedynie 46% zgłoszonych treści. Pozostałe zgłoszenia najczęściej dotyczą tematów związanych z seksualnością - kulturą japońską lub artystycznymi sesjami zdjęciowymi, jednak nie mające nic wspólnego z seksualnym wykorzystywaniem dzieci. Warto zauważyć, że dodatkowo forma tych zgłoszeń często uniemożliwia faktyczną ich analizę, ponieważ link URL prowadzi do wyników wyszukiwania, a one mogą zmieniać się w zależności od wielu różnych czynników.

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 (patrz Statystyki Dyżurnet.pl za rok 2021). 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, znaczącą większość 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.

Około połowę wszystkich zgłoszeń stanowią zgłoszenia treści potencjalnie przedstawiających seksualne wykorzystywanie dzieci. Statystycznie w co piątym przypadku udaje się potwierdzić obecność takich materiałów pod wskazanych adresem, często jednak treści nie są już dostępne. Bardzo często również zgłaszane materiały nie są materiałami CSAM, ale pornografią z udziałem osób dorosłych, a więc ponownie – materiałami legalnymi.


Treści pornograficzne z udziałem małoletniego
Twarda pornografia
Rasizm i ksenofobia
Inne nielegalne treści
propagowanie pedofilskiej aktywności
treści pornograficzne z udziałem małoletniego (CSAM)
treści erotyczne z udziałem małoletniego
strona/forum z linkami
twarda pornografia
treści nie znalezione
treści niedostępne
pornografia dorosłych
pornografia dostępna dla nieletnich
nielegalny spam
treści naturystyczne z udziałem małoletniego
szantaż na tle seksualnym małoletni
uwodzenie dziecka
zapytania
inne treści szkodliwe
treści rasistowskie i ksenofobiczne
szantaż na tle seksualnym dorośli
poza działalnością
inne treści - ok
narkotyki
cyberprzemoc
inne treści - nielegalne

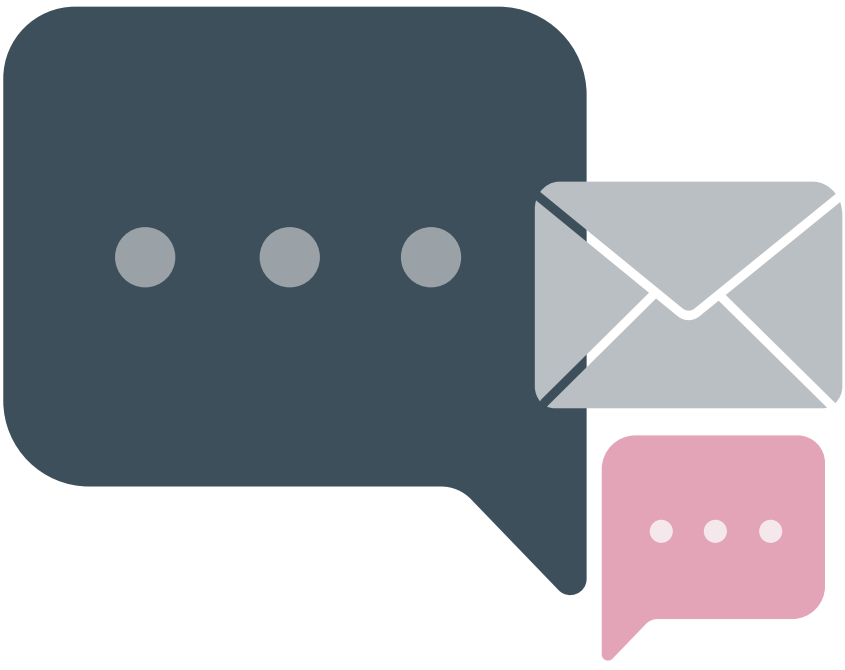
Niebezpieczne wyzwania internetowe

W raportach oraz publikacjach zespołu Dyżurnet.pl wielokrotnie pojawiały się informacje na temat szkodliwych lub przeciwnie, niosących pozytywne przesłanie internetowych wyzwań. Wyzwania („***challenge***") zazwyczaj są promowane głównie w social mediach, często przez osoby posiadające duże zasięgi – gwiazdy, influencerów, celebrytów, polityków. Zabawa może mieć na celu szerzenie świadomości, np. na temat choroby, problemów społecznych lub po prostu zrzeszać jak największą liczbę osób w celu rozrywkowym.

Niestety w sieci pojawiają się również wyzwania, których podejmowanie czy naśladowanie może wiązać się z niebezpieczeństwem utraty zdrowia lub życia – Tide Pot Challenge, polegające na zjedzeniu kapsułki ze środkiem do prania, posypanie ciała solą i przyłożenie kostki lodu do skóry (Salt and Ice Challenge) czy też bardzo niebezpieczna forma wyzwania, jakim było Ultimate Selfie Challenge, polegające na zrobieniu sobie selfie w brawurowej sytuacji lub groźnym miejscu, np. na krawędzi wysokiej skarpy.

Jednym z nowszych wyzwań, które pojawiło się w mediach społecznościowych i zatacza coraz większe kręgi jest Skull Breaker Challenge. „Zabawa" w tym wyzwaniu wygląda następująco: trzy osoby stojące w rzędzie podskakują z czego dwie po zewnętrznych stronach podcinają nogi osoby będącej w środku, w trakcie podskoku. Skutki takiej „zabawy" to najczęściej siniaki, złamania, a w wielu przypadkach także ciężkie uszkodzenia ciała lub kalectwo.

Ważne jest towarzyszenie dzieciom oraz nastolatkom w ich internetowych wyborach i namawianie ich do nieulegania modom. Czasami z pozoru niewinna zabawa może prowadzić do kalectwa l ub śmierci. Warto uświadamiać młodych ludzi, że bycie bezpiecznym w internecie wiąże się również z nieangażowaniem się i nienaśladowaniem niebezpiecznych zachowań w realnym życiu.



Szkodliwe treści popularne wśród dzieci i młodzieży

Na szkodliwe treści w internecie można trafić na wiele różnych sposobów, materiały takie mogą znaleźć się wśród proponowanych przez portal „popularnych" wideo, na portalach społecznościowych, może to być złośliwe przekierowanie z innej strony lub link przesłany przez znajomego lub nawet osobę, której nie znamy. Jedną z form szkodliwych treści są patostreamy. Są to relacje na żywo, prezentujące zachowania określane i postrzegane jako patologiczne, np. relacje z libacji alkoholowych, materiały prezentujące agresywne zachowania lub zachęcające do takich zachowań wobec innych osób lub konkretnych grup społecznych, wyzwiska, bójki i inne zachowania niebezpieczne.

Niestety zjawisko jest nadal obecne w sieci, a walka z nim często nierówna. Patostreamy stanowią materiały szkodliwe, ale rzadko same w sobie stanowią treści naruszające prawo, dlatego w takich przypadkach usunięcie lub specjalne oznaczenie treści (np. jako materiały nieprzeznaczone dla dzieci) zależy od woli administratora serwisu.

Dlaczego patostreamy są groźne?

- promują niebezpieczne i szkodliwe zachowania,
- treści w nich zawarte mogą być nielegalne,
- mogą powodować negatywne emocje u odbiorcy,
- nakłaniają do wpłacania pieniędzy,
- pokazują zakłamany obraz rzeczywistości,
- młodzi ludzie zachęceni popularnością swoich „idoli" mogą angażować się w podobne aktywności w celu uzyskania rozpoznawalności i sławy.

Twórcy patotreści zachęcani wpłatami od oglądających, popularnością i rozgłosem decydują się na podejmowanie coraz śmielszych zachowań. Wraz z rozwojem zjawiska, w materiałach dochodziło do nękania lub znęcania się nad innymi osobami lub podpaleń i niszczenia przedmiotów.

Walka z patostreamami, aby przynosiła efekty, powinna opierać się na budowaniu świadomości na temat szkodliwości zjawiska i jego negatywnego wpływu na młode osoby oraz niepromowaniu tego typu materiałów w sieci przez serwisy, na których są zamieszczane.

W ostatnim czasie media kilkukrotnie donosiły o czasowym aresztowaniu znanych patostreamerów, co pokazuje, że podejmowanie działań mających na celu uchronienie młodych osób przed kontaktem z treściami szkodliwymi przynosi wymierne efekty.

Regulacje prawne dotyczące nowych technologii a bezpieczeństwo

Pod koniec grudnia 2020 roku instytucje, organizacje, przedstawiciele branży sektora prywatnego oraz niezależni eksperci zaangażowani w przedsięwzięcia mające na celu zapobieganie i zwalczanie wykorzystywania seksualnego dzieci, z niepokojem obserwowali wejście w życie z dniem 21 grudnia 2020 roku Europejskiego Kodeksu Łączności Elektronicznej (**ang. *European Electronic Communications Code***)[10] Konsekwencją jego pełnej aplikacji była sytuacja, w której niektóre internetowe serwisy komunikacyjne, takie jak ***webmail*** czy ***messaging services***, zostały objęte ***Dyrektywą e-Privacy***[11]. To z kolei odebrało im możliwość dobrowolnego wykrywania i raportowania przypadków obecności w ich produktach i usługach materiałów z kategorii CSAM.

Jeszcze we wrześniu 2020 roku Komisja Europejska, dążąc do zapobieżenia tej sytuacji, przygotowała propozycję rozwiązania tymczasowego, zgodnie z którym dostarczyciele internetowych serwisów komunikacyjnych mogliby kontynuować swoje dobrowolne starania służące wykrywaniu, raportowaniu, a następnie usuwaniu CSAM[12]. Głównym argumentem, mającym przekonać do przyjęcia tej propozycji było zapewnienie, iż daje ona gwarancję ochrony prywatności i danych personalnych. Dodatkowym uzasadnieniem było również to, że poufność komunikacji nie powinna chronić sprawców seksualnego wykorzystywania dzieci. Niestety, na wejście w życie tego rozwiązania trzeba było czekać aż do sierpnia 2021 roku. Tyle czasu zajął bowiem proces negocjacyjny zanim został uzgodniony ostateczny kształt tych przepisów[13].

Dlaczego interwencja Komisji Europejskiej była potrzebna?

Dążenia sektora prywatnego do ograniczenia obecności CSAM w ich produktach i usługach stanowią nieoceniony wkład w starania międzynarodowej społeczności, której przyświeca wizja Internetu wolnego od treści tego rodzaju. Praktyki sektora prywatnego polegające na stosowaniu technologii pozwalających na automatyczne wykrywanie materiałów wcześniej sklasyfikowanych jako CSAM[14] dzięki porównywaniu danych hash, uzupełniają równoległe działania infolinii, takich jak Dyżurnet.pl, zrzeszonych w INHOPE.

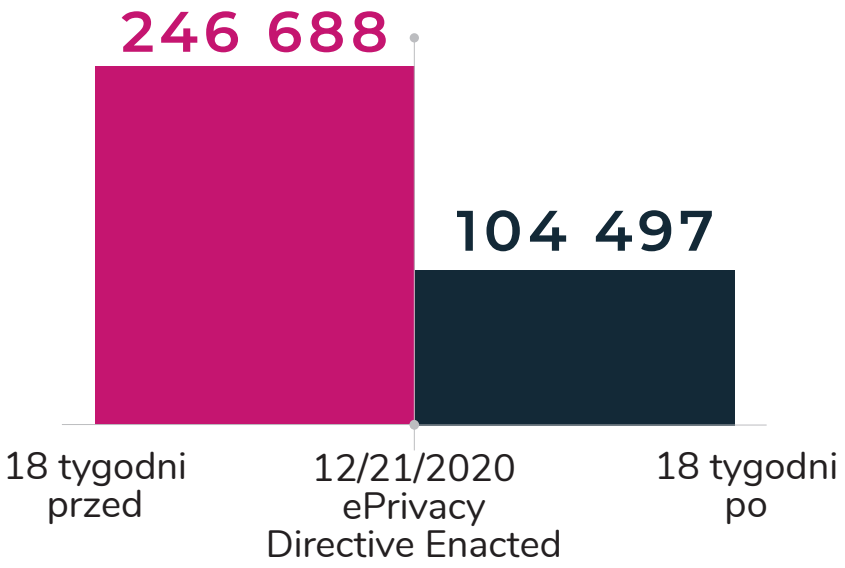
W staraniach mających na celu nakreślenie skali wyzwania warto powołać się na dane publikowane przez National Center for Missing & Exploited Children w USA[15] . Zgodnie z amerykańskim prawem federalnym, lokalne podmioty sektora prywatnego mają obowiązek raportowania do zarządzanej przez to centrum infolinii – CyberTipline - przypadków ujawnienia w ich zasobach materiałów mogących przedstawiać seksualne wykorzystywane dzieci. Jest to wyjątkowa regulacja, niemająca do tej pory swojego odpowiednika nigdzie indziej na świecie. Liczby publikowane przez tę organizację są alarmujące: w 2020 roku CyberTipline otrzymała ponad 21.7 miliona raportów, co stanowi przyrost w wysokości 28% w porównaniu z rokiem 2019[16] .

10. https://eur-lex.europa.eu/eli/dir/2018/1972/2018-12-17
11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
12. c.europa.eu/home-affairs/news/eu-will-continue-protect-children-child-sexual-abuse-online-2020-09-10_en
13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.274.01.0041.01.ENG
14. c.europa.eu/home-affairs/news/eu-will-continue-protect-children-child-sexual-abuse-online-2020-09-10_en
15. https://www.missingkids.org/HOME
16. https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers

Sytuację, jaka miała miejsce w grudniu 2020 roku, należy określić jednoznacznie: bez tymczasowych przepisów, pozwalających na odstępstwo od wyszczególnionych w nich artykułów Dyrektywy e-Privacy, terytorium Unii Europejskiej mogłoby zostać nieograniczonym centrum dystrybucji CSAM online. Nic więc dziwnego, że propozycja Komisji Europejskiej spotkała się z ogromnym poparciem ze strony przedstawicieli środowiska zaangażowanego w przedsięwzięcia mające na celu zapobieganie i zwalczanie seksualnego wykorzystywania dzieci. Stowarzyszenie INHOPE uruchomiło kampanię „See no evil, hear no evil", w ramach której zachęcano do nagłośnienia tej sytuacji[17] . Pomimo tego, iż problem dotyczył Unii Europejskiej, w starania te włączyło się również przywołane już tutaj amerykańskie centrum NCMEC. Oprócz uruchomienia dedykowanej kampanii[18] , przedstawiciele tego centrum wysłali ponad 200 listów do członków Parlamentu Europejskiego.

Jaką lekcję można wyciągnąć z okresu, w którym tak pożądane praktyki sektora prywatnego zostały częściowo zarzucone?

Zgodnie z danymi opublikowanymi przez NCMEC nastąpił znaczący spadek, tj. aż o 58 procent,, liczby raportów dotyczących krajów Unii Europejskiej przekazanych do CyberTipline, porównując okres 18 tygodni przed i po 21 grudnia 2020 roku, co zostało przedstawione na zamieszczonym poniżej wykresie [19]:



Przyjęcie rozwiązania tymczasowego Komisji Europejskiej jest chwilowym zażegnaniem kryzysu, gdyż ma ono ograniczony czas obowiązywania – do 3 sierpnia 2024 roku. Aktualnie trwają prace nad nowym pakietem przepisów, które regulowałyby ten obszar. Ich ogłoszenie ma nastąpić w najbliższych miesiącach.

17. https://inhope.org/EN/articles/e-privacy-directive-temporary-derogation
18. https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety oraz change.org/childsafetyfirst
19. https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

Rozwiązania technologiczne

APAKT – postęp prac w projekcie

W roku 2021 Zespół Dyżurnet.pl kontynuował realizację projektu APAKT, który jest realizowany razem z naukowcami NASK i naukowcami Politechniki Warszawskiej oraz firmy technologicznej Enamor International, a finansowany ze środków Narodowego Centrum Badań i Rozwoju. Celem projektu jest stworzenie narzędzi do analizy i detekcji treści multimedialnych oraz materiałów tekstowych udostępnianych w cyberprzestrzeni, przedstawiających seksualne wykorzystywanie dzieci.

Wypracowane metody oparte będą na modelach klasyfikacji treści zbudowanych przy zastosowaniu algorytmów sztucznej inteligencji, których zadaniem będzie m.in. klasyfikacja i priorytetyzacja zgłoszeń dotyczących treści publikowanych w internecie pod kątem obecności materiałów przedstawiających seksualne wykorzystywanie dziecka.

Warunkiem powodzenia projektu jest zgromadzenie ogromnej ilości danych, które posłużą do trenowania modeli opartych na sieciach neuronowych. Dane w postaci zdjęć, filmów wideo oraz tekstów muszą zostać odpowiednio sklasyfikowane oraz oznaczone (otagowane). Każdy element analizowanego materiału, który wpływa na jego klasyfikację, zostanie odpowiednio opisany zgodnie z przyjętym i uzgodnionym wcześniej systemem znaczników (tzw. tagów).

Proces doboru znaczników do poszczególnych rodzajów treści jest niezmiernie ważnym elementem gromadzenia danych służącym do uczenia modeli sztucznej inteligencji. Błędne oznaczenia lub ich nieodpowiedni wybór może zaważyć na końcowym efekcie, czyli zdolności danego modelu do prawidłowej klasyfikacji treści. Duże doświadczenie Zespołu Dyżurnet.pl w analizie i klasyfikacji treści CSAM pozwoliło na dokładne określenie specyficznych cech występujących w analizowanych treściach. Określono wszystkie cechy, które determinują przynależność danej treści do konkretnej klasy materiałów.

Następnym krokiem było wypracowanie w każdej z grup materiałów (obrazy, wideo, teksty) list tagów, które umożliwią wytrenowanie modeli sztucznej inteligencji opartych na sieciach neuronowych. Na tym etapie Zespół Dyżurnet.pl ściśle współpracował z zespołami naukowymi NASK oraz Politechniki Warszawskiej.

Firma ENAMOR INTERNATIONAL Sp. z o.o. przygotowała pierwszą wersję systemu informatycznego, dzięki któremu możliwe będzie zbieranie danych, które następnie zostaną sklasyfikowane, oznaczone wybranymi wcześniej zestawami odpowiednich tagów i w takiej wersji na bieżąco przekazywane będą do procesu uczenia modeli AI.

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 uczynić proces zgłaszania treści łatwiejszym i sprawniejszym dla użytkownika Zespół Dyżurnet.pl stworzył specjalną wtyczkę, która po zainstalowaniu umożliwia zgłoszenie nielegalnych lub szkodliwych treści 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. Dodatkowo, tak jak w przypadku formularza, zgłoszenia mogą być dokonywane anonimowo i gwarantowane jest pełne bezpieczeństwo danych.

- Wtyczkę do przeglądarki Mozilla Firefox: Zgłoś treść do Dyżurnet.pl [20]
- Wtyczkę do przeglądarki Google Chrome: Zgłoś nielegalną treść do Dyżurnet.pl [21]

Współpraca z OSE

Państwowy Instytut Badawczy NASK jest operatorem sieci OSE (ose.gov.pl). Ogólnopolska Sieć Edukacyjna daje szkołom w całej Polsce możliwość podłączenia szybkiego, bezpłatnego i bezpiecznego internetu. Projekt został stworzony przez Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej.

Eksperci Dyżurnet.pl realizują zadania związane z podnoszeniem poziomu bezpieczeństwa w sieci, w tym wspomagając definiowanie polityki bezpieczeństwa, przyjmując incydenty bezpieczeństwa związane z nielegalnymi treściami oraz współtworząc materiały edukacyjne i promocyjne.

Aplikacja SYWENTO

Analitycy Dyżurnet.pl w trakcie swojej pracy gromadzą duże ilości danych, których ewentualne wykorzystanie mogłoby ułatwić pracę innym profesjonalistom zajmującym się materiałami prezentującymi seksualne wykorzystanie nieletnich. W tym celu w roku 2020 powstała aplikacja SYWENTO, narzędzie stworzone przez NASK PIB z przeznaczeniem dla biegłych sądowych z zakresu informatyki. Wspomaga analizę danych pod kątem uzyskania informacji, czy pod danym adresem internetowym (tzw. URL) znajdowały się treści pornograficzne z udziałem małoletniego. Po wysłaniu zapytania zawierającego listę adresów internetowych odwiedzanych przez podejrzanego, SYWENTO dostarcza informację zwrotną z listą adresów URL zidentyfikowanych wcześniej przez Zespół Dyżurnet.pl jako strony zawierające treści pornograficzne z udziałem małoletnich z podaniem daty, kiedy dana strona była analizowana przez Dyżurnet.pl. Baza systemu SYWENTO obejmuje wyłącznie adresy URL, które były przedmiotem zgłoszenia i zostały przeanalizowane i sklasyfikowane przez Dyżurnet.pl. Taka informacja może być pomocna w przypadku konieczności analizy dużej ilości materiałów pozyskanych z nośników danych osób podejrzanych o pedofilię. Wynik zapytania daje nam odpowiedź, czy i jak często podejrzany przeglądał strony internetowe, na których według analityków Dyżurnet.pl znajdowały się nielegalne treści.

20. https://addons.mozilla.org/pl/firefox/addon/zglos-tresc-do-dyzurnet-pl/
21. https://chrome.google.com/webstore/detail/report-illegal-content-to/djegpdbohfkhkiebfdikclmmbpgdblbh

DZIAŁALNOŚĆ
edukacyjno-popularyzatorska

Kampania

Media społecznościowe w obecnych czasach są przestrzenią, w której młode osoby tworzą i budują relacje, kształtują własną tożsamość, wyrażają siebie i poznają otaczający świat. Wraz z rozwojem cyfryzacji naturalną konsekwencją jest to, iż do świata online przeniosło się również budowanie relacji intymnych. Z roku na rok rośnie liczba materiałów erotycznych wytwarzanych przez młode osoby, tendencja wzrostowa zjawiska jest zauważalna na całym świecie. Według badań przeprowadzonych przez THORN[22] w USA:

- 2 na 10 dziewcząt (w wieku 13-17) udostępniło swoje intymne materiały;
- 1 na 10 chłopców (w wieku 13-17) udostępnił swoje intymne materiały;
- 40% z badanych dzieci zgadza się ze stwierdzeniem „to normalne dla osób w moim wieku, aby dzielić się intymnymi materiałami z innymi".

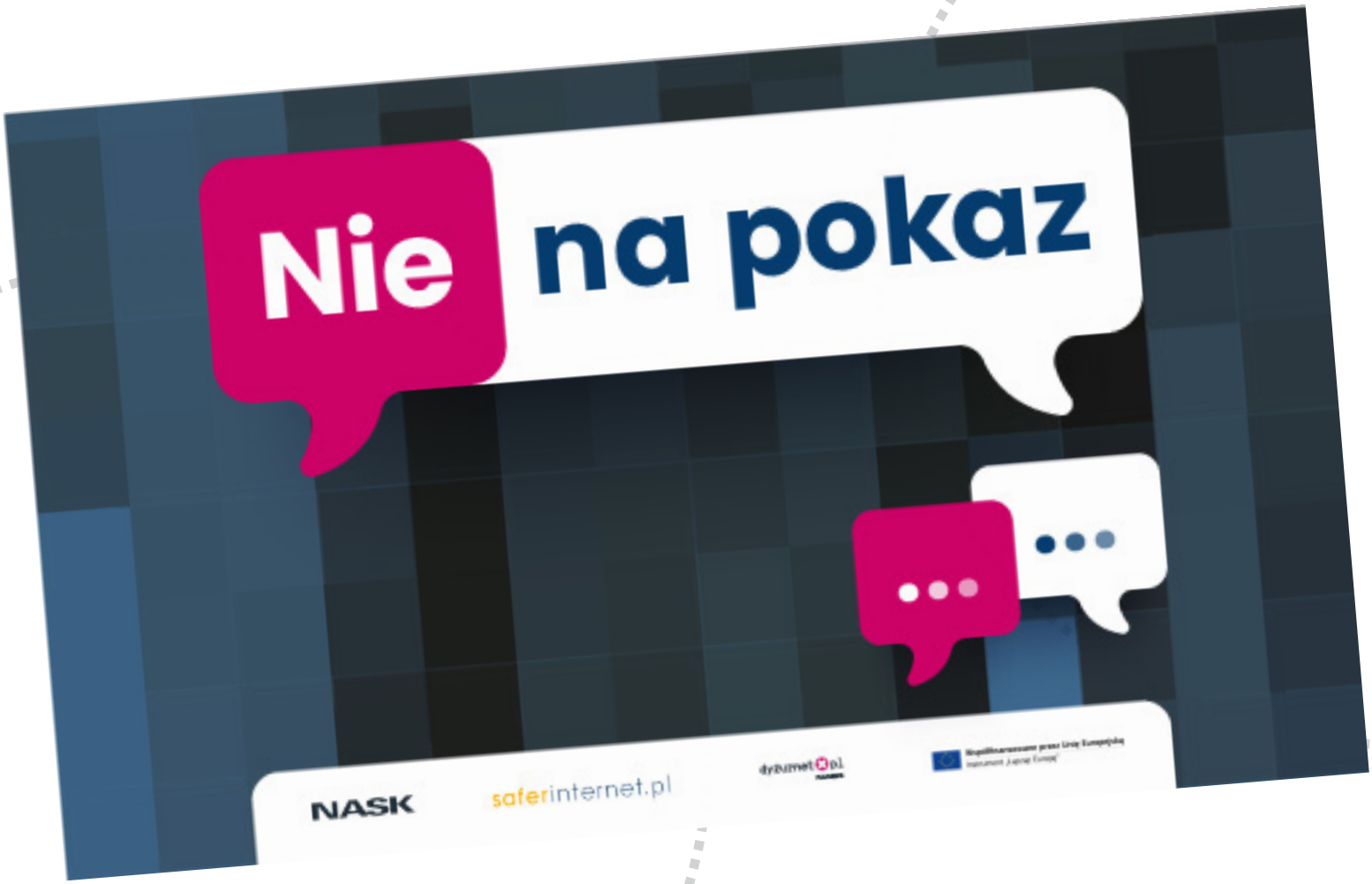
Wiele młodych osób potwierdzało pozytywne odczucia o swoich doświadczeniach dzielenia się materiałami intymnymi, takie jak zwiększenie pewności siebie czy zwiększenie poczucia zaufania. Intymne relacje i flirty w sieci ulegają normalizacji, jednakże równocześnie wzrasta przestrzeń dla osób, które chcą tę sytuację wykorzystać. Wymiana materiałów intymnych online naraża dzieci na nadużycia ze strony dorosłych, którzy mogą starać się je wykorzystać w różnych celach, ale też na nękanie ze strony rówieśników, którzy mogą przekazać materiały dalej, do osób postronnych lub je upublicznić. Według badań przeprowadzonych przez NASK w 2021 roku "Nastolatki 3.0"[23] , otrzymanie materiałów intymnych potwierdziło 8,3% respondentów. Młode osoby często nie zdają sobie sprawy, że materiały mogą zostać upublicznione bez ich zgody oraz że osoba poznana w internecie nie zawsze ma dobre zamiary i niekoniecznie jest kimś za kogo się podaje. Najbardziej zagrażająca jest utrata kontroli nad tym, co z danym materiałem się wydarzy po jego wysłaniu lub upublicznieniu. Młode osoby są narażone na przemoc ze strony rówieśników lub dorosłych, materiały mogą również dostać się w ręce osób o skłonnościach pedofilskich. Młodzi ludzie równie często stają się ofiarami otrzymywania niechcianych materiałów intymnych od innych osób, czasami nieznajomych, poprzez wiadomości na portalach społecznościowych lub platformach gamingowych.

22. https://www.thorn.org/self-generated-child-sexual-abuse-material-attitudes-and-experiences/
23. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html

W odpowiedzi na rosnący problem NASK przygotował kampanię, która porusza temat popularności dzielenia się materiałami o charakterze intymnym wśród młodych ludzi i będzie adresowana głównie do nastolatków (w wieku 13-17 lat). Poprzez działania kampanijne zostały wskazane niebezpieczeństwa wynikające z podejmowania takich aktywności oraz miejsca, gdzie można szukać pomocy, a także co zrobić w sytuacji, gdy materiały zostaną upublicznione przez osoby, które uzyskały do nich dostęp.

Ważnym aspektem kampanii jest edukacja młodych osób skierowana na rozwijanie świadomości możliwości dokonania wyboru – jeśli nie chcą dzielić się materiałami intymnymi, to zawsze mogą powiedzieć „nie" – badanie pokazało, że postawa asertywna i odmowa nie zawsze jest brana pod uwagę przez młode osoby, często wypływa to z poczucia zobowiązania.

Kampania została realizowana przez Państwowy Instytut Badawczy NASK w ramach działań Polskiego Centrum Programu Safer Internet (PCPSI).



PUBLIKACJE

PRZYGOTOWANE

PRZEZ DYŻURNET.PL

Cyfrowy Ślad Małego Dziecka

W lipcu 2021 roku ukazała się publikacja zespołu Dyżurnet.pl pt. „Cyfrowy Ślad Małego Dziecka[24]". Jest to ważny raport utworzony przez ekspertów Zespołu, który powstał na podstawie obserwacji treści zgłaszanych przez użytkowników internetu. Eksperci Zespołu na co dzień w swojej pracy mają kontakt z kolekcjami materiałów o charakterze pedofilskim. Oprócz treści łamiących polskie prawo mają do czynienia z materiałami legalnymi i pozornie neutralnymi materiałami prezentującymi dzieci. Są to zdjęcia i filmy w dużej mierze zebrane z różnego rodzaju serwisów społecznościowych. Większość z nich została zamieszczona w sieci przez niefrasobliwych rodziców, którzy nie zdają sobie sprawy z tego, w jaki sposób materiały te mogą zostać później wykorzystane.

Raport pokazuje na jak dużą skalę publikowane są przez rodziców zdjęcia i filmy, na których prezentowane są dzieci. Najlepiej obrazuje to poniższy cytat:

„Wśród przebadanych 168 polskich kont w serwi¬sach społecznościowych w 2015 r. prawie 40% publikowało więcej niż 100 zdjęć swojego dziecka, a aż 90% podało imię dziecka i prawie 84% datę jego urodzenia. Im więcej informacji, tym pełniejszy wizerunek można zbudować, co ostatecznie może prowadzić nawet do kradzieży tożsamości. Badania przeprowadzone w 2019 r. pokazują, że 40% Polaków regularnie publikuje zdjęcia swoich pociech na różnego rodzaju portalach społecznościowych. Co ciekawe, 81% rodziców ocenia udostępnianie zdjęć własnych dzieci pozytywnie lub neutralnie. Aż 57% bada¬nych deklaruje, że o prywatności dziecka decy¬dują rodzice i nie ma nic złego we wrzucaniu do internetu zdjęć lub filmów z jego udziałem. Niepokojące jest również, że aż 60% dzieli się dokumentacją z dorastania własnych dzieci przynajmniej raz w miesiącu, a tylko około 25% zapytało dziecko o zgodę na udostępnianie jego zdjęć" (s. 7).

Najważniejsze wnioski publikacji „Cyfrowy Ślad Małego Dziecka":

- Publikacja ukazuje zagrożenia płynące z nieostrożnego publikowania wizerunku dzieci.
- Przedstawia zestaw dobrych praktyk, które pomogą rodzicom najmłodszych dzieci umiejętnie zarządzać wizerunkiem swoich pociech.
- Podkreśla, jak ważna jest prywatność dziecka.
- Dodatkowo raport skierowany jest również do placówek opiekuńczych i przedstawia najważniejsze aspekty prywatności wizerunku dzieci, na które placówki powinny zwrócić szczególną uwagę.

24. https://dyzurnet.pl/uploads/2021/07/Cyfrowy_slad_malego_dziecka.pdf

APLIKACJE MOBILNE

czy nasze dzieci są bezpieczne?

Z roku na roku następuje coraz większa wirtualizacja otaczającej nas rzeczywistości. Aplikacje mobilne służą wielu osobom w codziennym życiu na każdym kroku, a popularność urządzeń z interfejsem dotykowym sprawia, że aplikacje są coraz prostsze w obsłudze. Interfejs wielu z nich, pozwala na intuicyjną nawigację nawet najmłodszym użytkownikom.

Aplikacje spełniają wiele celów – służą do rozrywki, edukacji, umożliwiają kontakt. Korzystanie z nich i z ich funkcjonalności umożliwia zaspokajanie potrzeb na różnych poziomach – takich jak potrzeba przynależności, potrzeba kontaktu z innymi czy potrzeba ekspresji. Dlatego też najmłodsi tak często i chętnie sięgają po produkty, które są przeznaczone dla starszych grup wiekowych. Zdarza się, że dzieci zachęcone popularnością sięgają po aplikacje przeznaczone dla starszych użytkowników, zawyżając swój wiek do celów instalacji produktu, co może prowadzić do kontaktu z treściami przeznaczonymi dla starszych użytkowników. Niestety mała świadomość opiekunów, w jaki sposób prawidłowo konfigurować urządzenia i profile, aby ograniczyć kontakt z nieodpowiednimi treściami wpływa na to, że dzieci i młodzież korzystają z aplikacji przeznaczonych dla starszych grup wiekowych na podstawowych ustawieniach – niechroniących młodszych użytkowników przed niewłaściwymi dla nich treściami czy też kontaktem z nieznajomym.

Korzystanie z nieodpowiednich aplikacji może narazić najmłodszego użytkownika na kontakt z zagrożeniami takimi jak:

- kontakt z nieodpowiednimi – szkodliwymi i nielegalnymi – treściami;
- kontakt z niebezpiecznymi osobami;
- ujawnienie i wyciek prywatnych informacji;
- utrwalanie niebezpiecznych zachowań i nawyków;
- nadużycia finansowe;
- wirusy i ataki hackerskie.

Wybór aplikacji, z której może korzystać dziecko nie jest łatwy dla jego opiekunów. Atrakcyjny interfejs, popularność korzystania wśród innych dzieci, brak czasu na zapoznanie się z aplikacją i małe kompetencje cyfrowe rodziców sprawiają, że instalacja i jakość treści dostępnych w aplikacji nie przechodzi weryfikacji ze strony opiekunów. Często też w przypadku młodszych dzieci, a na pewno nastolatków – dziecko samo je instaluje bez wiedzy i zgody rodzica.
W raporcie zostały wskazane rekomendacje dla opiekunów i rodziców oraz ogólne potencjalne zagrożenia i zasady bezpieczeństwa korzystania z aplikacji mobilnych przez dzieci i młodzież. Zachęcamy do zapoznania się z Raportem na stronie Dyżurnet.pl.

Wydarzenia

W 2021 roku przedstawiciele Dyżurnet.pl dzielili się swoimi doświadczeniami i wiedzą między innymi podczas wydarzeń:

09.02.2021

DBI - Samodzielnie, nie znaczy dobrowolnie - treści internetowe wytworzone przez młodzież

17.03.2021

Sexting i nagie zdjęcia w sieci – bezpieczni w sieci z OSE

13.04.2021

Samodzielnie nie znaczy dobrowolnie dla Przystań w Sieci

18.05.2021

DBI - Konferencja lokalna Safer Internet

23.11.2021

Self -generated sexual content - konferencja lokalna Safer Internet

Ponadto Eksperci Zespołu wraz z Wirtualną Katedrą Etyki i Prawa współorganizowali webinaria:

- Zjawisko seksualnego wykorzystywania dzieci w cyberprzestrzeni oraz publiczno-prywatna odpowiedź na związane z nim wyzwania.
- Analiza stanu implementacji Dyrektywy 2011/93/EU.
- Analiza konsekwencji wejścia w życie postanowień European Electronic Communications Code.
- Analiza konsekwencji ogłoszenia zestawu przepisów dotyczących wszystkich usług cyfrowych działających w Unii Europejskiej – Kodeks usług cyfrowych (Digital Services Act), który określa zasady funkcjonowania wszystkich usług cyfrowych w UE.
- Analiza nowego pakietu przepisów ogłoszonych przez Komisję Europejską w ramach realizacji strategii unijnej dotyczącej bardziej efektywnej walki z seksualnym wykorzystywaniem dzieci (w przypadku ogłoszenia przed datą webinarium).

O NASK

NASK jest państwowym instytutem badawczym nadzorowanym przez Kancelarię Prezesa Rady Ministrów.

Kluczowym polem aktywności NASK są działania związane z zapewnieniem bezpieczeństwa Internetu. Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci w Polsce i koordynacją działań w tym obszarze zajmuje się Pion Centrum Cyberbezpieczeństwa, w którego skład wchodzi m.in. zespół CERT Polska (www.cert.pl). Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK-PIB został wskazany jako jeden z 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. NASK współtworzy także zaplecze analityczne oraz badawczo-rozwoje dla krajowego systemu cyberbezpieczeństwa.

NASK prowadzi też działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Tym, co wyróżnia nasz instytut badawczy od ściśle komercyjnych przedsiębiorstw jest podejście do tworzenia rozwiązań dla obecnych i przyszłych potrzeb klientów. W instytucie NASK 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. 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).

NASK

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.

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 przekazywana jest informacja 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.

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

dyżurnet.pl

NASK