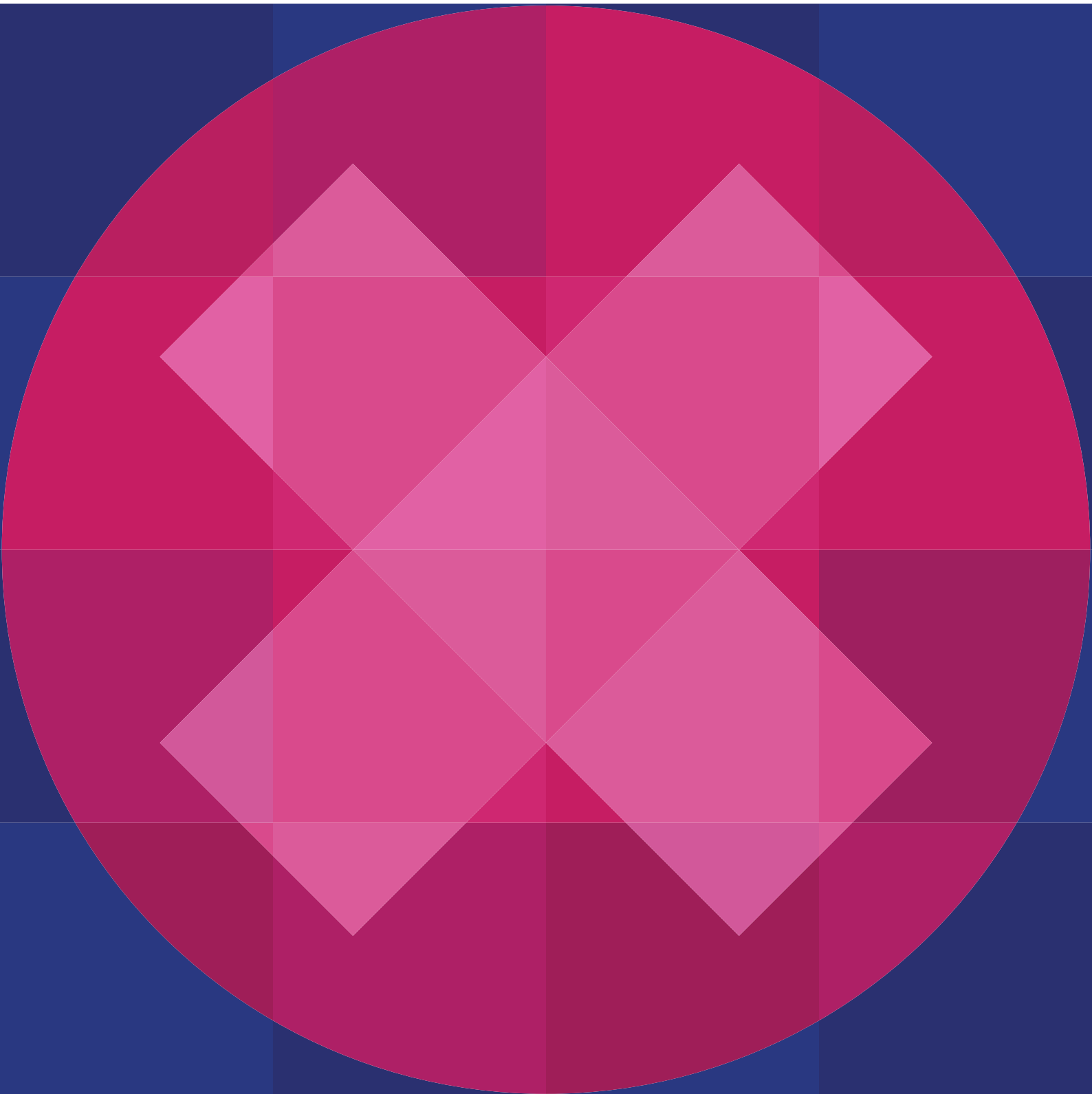
RAPORT 2020

NASK

dyżurnet.pl

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, realizujący działania w ramach CSIRT NASK na podstawie dotacji podmiotowej i będący częścią Polskiego Centrum Programu Safer Internet**

Korekta: **Anna Hernik-Solarska**

Opracowanie graficzne: **Aleksandra Więcierzewska**

Współfinansowane przez Unię Europejską
Instrument „Łącząc Europę”

SPIS TREŚCI

DZIAŁAMY

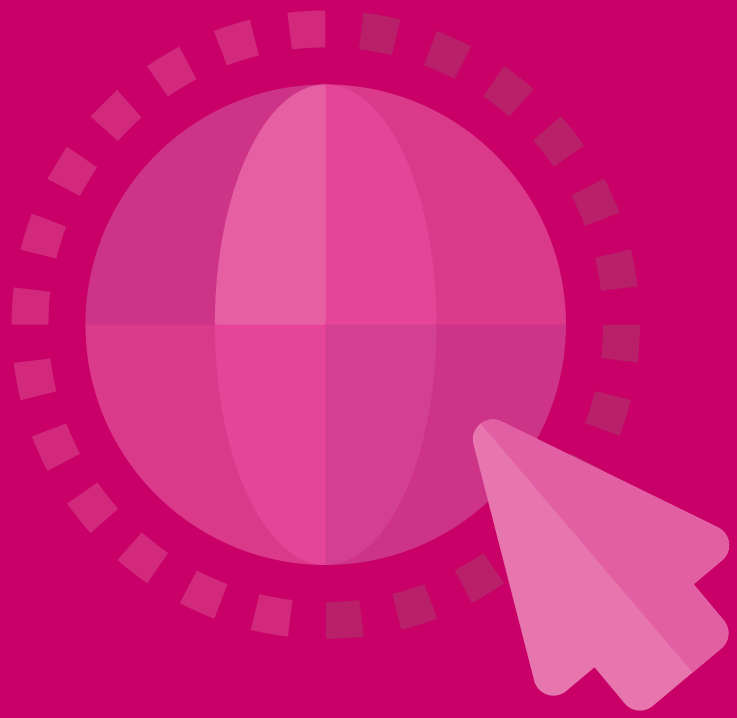
NA RZECZ TWORZENIA
BEZPIECZNEGO INTERNETU

REAGUJEMY

NA NIELEGALNE I SZKODLIWE
TREŚCI W INTERNECIE

POPULARYZUJEMY

BEZPIECZNE KORZYSTANIE
Z INTERNETU



NASK dyżurnet.pl

WSTĘP

Szanowni Państwo,

Zespół Dyżurnet.pl powstał w 2005 roku w NASK i zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa od 2018 roku realizuje zadania CSIRT NASK.

Rok 2020 był dla nas okazją do celebracji **#15 lat** Zespołu. Powodem inicjatywy było zauważenie konieczności podejmowania interwencji wobec treści internetowych przedstawiających seksualne wykorzystywanie dzieci. Zaczynaliśmy przede wszystkim od reagowania na zgłoszenia, z czasem rozwijając działania edukacyjne i popularyzatorskie aktywizując pedagogów, opiekunów, policjantów oraz same dzieci w trosce o bezpieczeństwo w internecie.
Po #15 latach działania rozwijamy również narzędzia, dzięki którym wykrywanie niepożądanych materiałów będzie łatwiejsze i szybsze.

Miniony rok 2020 był dla nas wszystkich wymagający. Był to rok wyzwań, również pod względem operacyjnym. Pandemia, izolacja w domach, nowa organizacja zajęć szkolnych spowodowały pojawienie się nowych zagrożeń oraz nasilenie tych, które są obserwowane od dawna.

Od kilku lat zwracamy Państwa uwagę na problem produkcji treści pornograficznych przez młodych użytkowników sieci. Przygotowaliśmy kampanię społeczną, w której zwracamy uwagę na to, że ofiary są #bezbronne, #szantażowane, #wykorzystywane. Pierwsza odsłona kampanii skierowana była do dorosłych – opiekunów, użytkowników internetu, ale również do administratorów i moderatorów, ponieważ tylko wtedy, gdy my dorośli będziemy mieć wspólne stanowisko i przejawiać zaangażowanie, możemy wspomóc młodych w podejmowaniu trafnych wyborów. W kolejnym roku planujemy drugą odsłonę kampanii, tym razem skierowaną właśnie do młodych użytkowników internetu, natomiast już dziś zapraszamy do jej wsparcia.

Naszą ambicją jest również to, aby rok 2020 był zapamiętany jako początek debaty o terminologii używanej w przestrzeni publicznej w odniesieniu do zjawiska seksualnego wykorzystywania dzieci w cyberprzestrzeni. Zaczynamy ją przyglądając się w raporcie określeniu „sextortion".

Apel o wrażliwość i empatię nie był nigdy tak aktualny jak teraz. Dlatego też podsumowując **#15 lat** naszej działalności dziękujemy za sympatię, słowa otuchy oraz wsparcie, którego doświadczamy każdego dnia.

Zapraszamy do lektury Raportu!

Z poważaniem

Krzysztof Silicki
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

O NAS

DZIAŁAMY - REAGUJEMY - POPULARYZUJEMY

Dyżurnet.pl działa w ramach NASK PIB już od 15 lat. Misją zespołu jest zapewnienie bezpieczeństwa w internecie, zwłaszcza najmłodszym jego użytkownikom, a jego działalność oparta jest na **Ustawie o Krajowym Systemie Cyberbezpieczeństwa** (z dnia 5 lipca 2018 r.). Zespół Dyżurnet.pl to jedyny wyspecjalizowany zespół w Polsce odpowiedzialny za przyjmowanie zgłoszeń o materiałach przedstwiajacych seksualne wykorzystywanie dzieci publikowanych w internecie. Ponadto Zespół przyjmuje i analizuje zgłoszenia dotyczące innych nielegalnych i szkodliwych treści.

Od początku działalności Zespół należy do **Stowarzyszenia INHOPE** – globalnej sieci zrzeszającej zespoły reagujące z różnych krajów, prowadzące współpracę (m.in. z Interpolem) w celu przeciwdziałania internetowym treściom prezentującym seksualne wykorzystywanie dzieci. Celem Stowarzyszenia jest eliminacja materiałów przedstawiających seksualne wykorzystywanie dzieci oraz wsparcie krajowych procedur na rzecz jak najszybszego usuwania nielegalnych materiałów.

Dyżurnet.pl jest także częścią **Polskiego Centrum Programu Safer Internet** organizowanego w ramach programu Komisji Europejskiej (*Connecting Europe Facility*).

NASK razem z Fundacją Dajemy Dzieciom Siłę prowadzi w Polsce działalność edukacyjną, organizując kampanie i konferencje, udostępniając publikacje oraz narzędzia pomagające w zwiększaniu świadomości Polaków na temat zagrożeń wynikających z korzystania z internetu. Fundacja Dajemy Dzieciom Siłę prowadzi również telefon zaufania, pomoc można uzyskać pod numerami telefonów:

telefon zaufania:
116 111, 800 100 100

Działania Polskiego Centrum Safer Internet są wspierane przez przedstawicieli instytucji rządowych, środowiska naukowego oraz biznesu w ramach **Komitetu Konsultacyjnego**.
www.saferinternet.pl

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.
- a od roku 2020 również poprzez dodatek/wtyczkę do przeglądarki Firefox: **Zgłoś Treść do Dyżurnet.pl**!

Kategorie, które są objęte procedurą reagowania:

- **Materiały przedstawiające seksualne wykorzystywanie dziecka**: art. 202 §3, 4, 4a, 4b k.k. - prawo polskie zabrania 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 prezentowaniem 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;

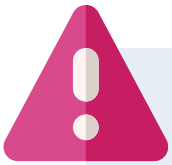
- **Inne nielegalne treści**: treści niedotyczące żadnej z powyższych kategorii, ale skierowane przeciwko bezpieczeństwu dzieci np. propagowanie lub pochwalanie zachowań o charakterze pedofilskim (art. 200b k.k.), uwodzenie dziecka poniżej 15 r.ż. przez internet, tzw. grooming (art. 200a k.k.), zjawisko szantażu na tle seksualnym (określane również jako „sextortion") - wykorzystanie materiałów o charakterze erotycznym i intymnym do wyłudzenia, najczęściej pieniędzy, dodatkowych materiałów lub doprowadzenia do obcowania płciowego czy poddania się innej czynności seksualnej.

Większość zgłoszeń przekazywanych przez użytkowników internetu do zespołu Dyżurnet.pl dotyczy treści potencjalnie przedstawiających seksualne wykorzystanie 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 rozpowszechniania materiału.

W każdym zgłoszeniu liczy się czas podjęcia reakcji.

Zespół Dyżurnet.pl podejmuje również działania wobec innych nielegalnych i szkodliwych treści internetowych, między innymi zawierających tzw. „twardą pornografię" oraz treści rasistowskich.

- W pierwszej kolejności materiał analizowany jest pod kątem jego legalności i jeżeli narusza polskie prawo oraz znajduje się na polskim serwerze, informacja przekazywana jest do Komendy Głównej Policji.
- W przypadku, gdy materiał jest legalny, ale mimo to narusza regulamin danego serwisu i został przez zespół Dyżurnet.pl uznany za szkodliwy, specjaliści kontaktują się z administratorami lub moderatorami serwisu z prośbą o założenie odpowiedniego ostrzeżenia lub usunięcie treści.

Ze względu na potencjalną szkodliwość nielegalnych treści zespół Dyżurnet.pl odradza samodzielne wyszukiwanie ich w internecie.

INHOPE

Skuteczna i szybka reakcja wobec materiałów przedstawiających seksualne wykorzystywanie dzieci jest możliwa dzięki działaniom podejmowanym przez krajowe organy ścigania oraz członków **Stowarzyszenia INHOPE**. Szczególnie ważne jest to w krajach rozwijających się i budujących społeczeństwo informacyjne oraz tworzących przepisy prawne, które regulują również internet.

Działalność Stowarzyszenia jest wspierana przez Interpol, Europol, Virtual Global Taskforce, European Financial Coalition, INSAFE, ECPAT oraz globalne firmy sektora informatycznego. Stowarzyszenie jest współfinansowane przez Komisję Europejską.

www.inhope.com

Quality assurance INHOPE

Jako członek stowarzyszenia INHOPE zespół Dyżurnet.pl podlega audytowi, który stanowi część INHOPE's Quality Assurance Programme i ma na celu zapewnienie jak najwyższych standardów działalności zespołów typu hotline. Audyt jest przeprowadzany przez członka zespołu INHOPE lub przez zewnętrznego ewaluatora. Tegoroczny audyt ze względu na pandemię COVID-19 odbywał się online. Sprawdzeniu podlegały przede wszystkim aspekty pracy hotline, zawarte w dwóch grupach:

- kontekst operacyjny pracy Zespołu – sekcja miała na celu wyjaśnienie i sprawdzenie wszelkich kwestii związanych z działaniem hotline, pomagając oceniającemu lepiej zrozumieć strukturę i działanie zespołu;

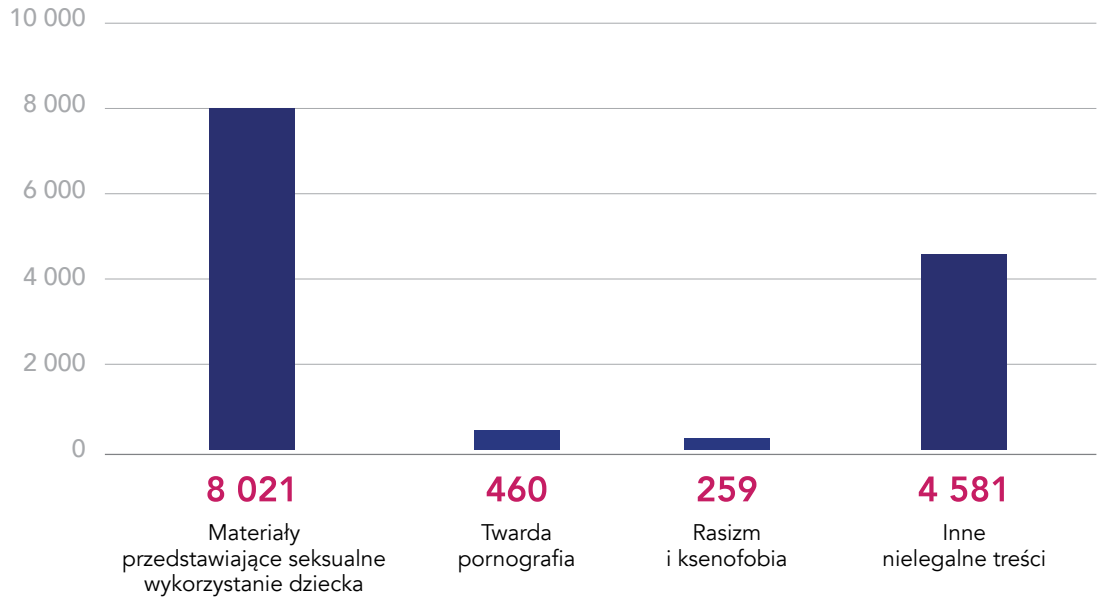
- zarządzanie i administracja – w tej sekcji audytor sprawdzał w jaki sposób działa zespół i jak jest zarządzany (jaka jest struktura zespołu, jakie są procedury zatrudnienia itp.).

Zespół Dyżurnet.pl spełnia wymagane normy i tym samym otrzymał certyfikat oceny jakości INHOPE.

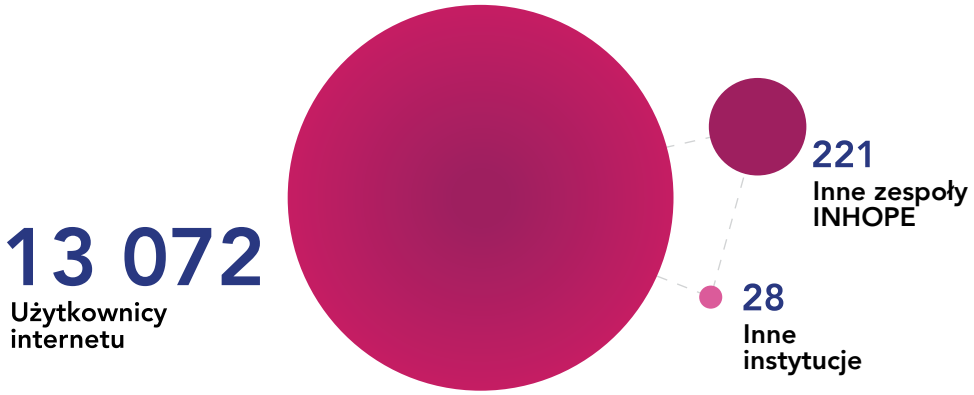
STATYSTYKI
DYŻURNET.PL ZA ROK 2020

ZGŁOSZENIA OTRZYMANE PRZEZ ZESPÓŁ DYŻURNET.PL

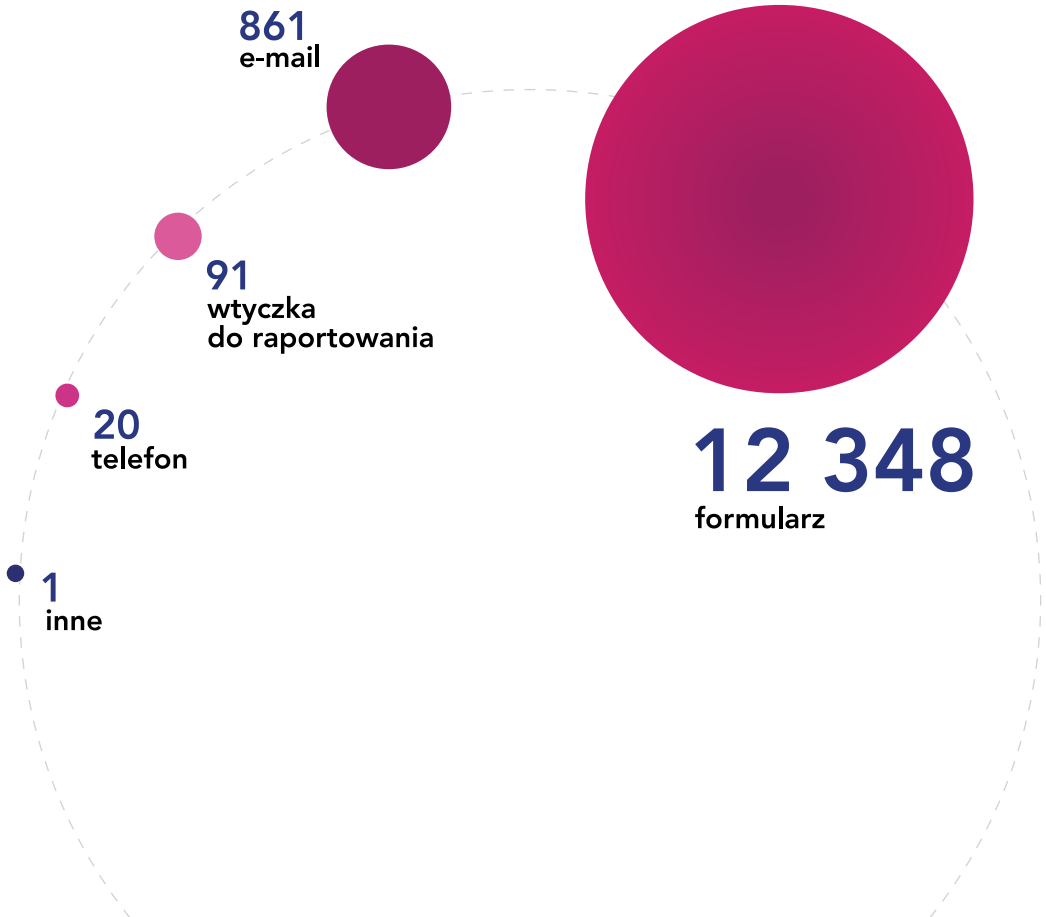
1 **Liczba zgłoszeń otrzymanych przez Dyżurnet.pl - rodzaj potencjalnie nielegalnych treści**



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

2 517

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.).

878

CSEM

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

22

PROPAGOWANIE PEDOFILSKIEJ AKTYWNOŚCI

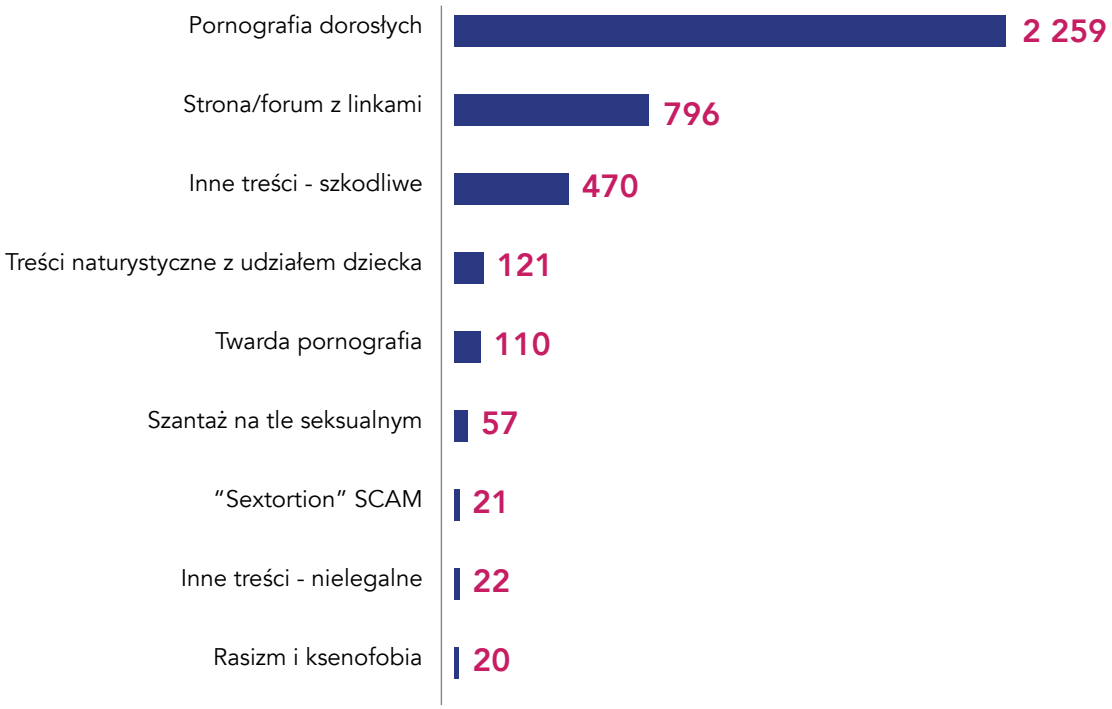
Propagowanie pedofilskiej aktywności
Publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim; nielegalne wg polskiego prawa (art. 200b k.k.).

8

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 drastyczne, wulgarne, obraźliwe, radykalne światopoglądowo, homofobiczne, autodestrukcyjne, propagujące samobójstwo lub przemoc.

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.).

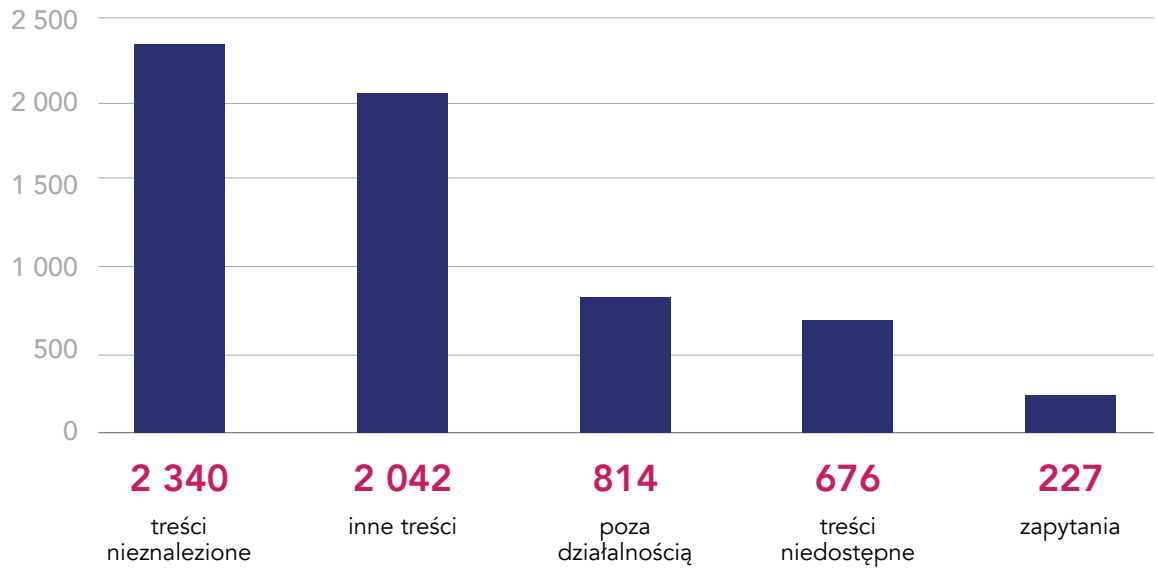
Szantaż na tle seksualnym („sextortion")
Seksualne wymuszenie, szantaż związany z uzyskaniem od ofiary materiałów multimedialnych o charakterze seksualnym pod groźbą ich szerszego udostępnienia; może wiązać się uzyskiwaniem materialnych korzyści.

„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.

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

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



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

Inne treści
Treści spoza wymienionych kategorii, niebędące treściami szkodliwymi ani nielegalnymi.

Poza działalnością
Zniesławienia, znieważenia, naruszenia dóbr osobistych i wizerunku, wyłudzenia danych osobowych, wyłudzenia i oszustwa finansowe (w tym fałszywe sklepy internetowe), włamania na konta i kradzież danych, naruszenia praw autorskich, gry hazardowe, handel narkotykami i środkami psychoaktywnymi, dystrybucja innych farmaceutyków poza obrotem aptecznym, informacje o dostępności zabiegów lub środków przerywania ciąży, publikowanie potencjalnie fałszywych informacji.

Treści niedostępne
Treści zabezpieczone hasłem, pliki do pobrania znajdujące się na serwerach 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

2 484
ZGŁOSZONE DO ODPOWIEDNIEGO ZESPOŁU INHOPE ORAZ INTERPOL

183
ZGŁOSZONE POLICJI

329
ZGŁOSZONE DO ADMINISTRATORÓW SERWISÓW

47
ZGŁOSZONE DO ISP

20
ZGŁOSZONE DO WŁAŚCICIELA TREŚCI

104
PRZEKAZANE INNEMU PODMIOTOWI (GŁÓWNIE CERT POLSKA)

Zgłoszone do odpowiedniego zespołu INHOPE oraz Interpol
Przesłane poprzez bazę ICCAM lub formularz kontaktowy do zespołów reagujących właściwych dla lokalizacji serwera, zrzeszonych w Stowarzyszeniu INHOPE; treści z kategorii baseline 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.

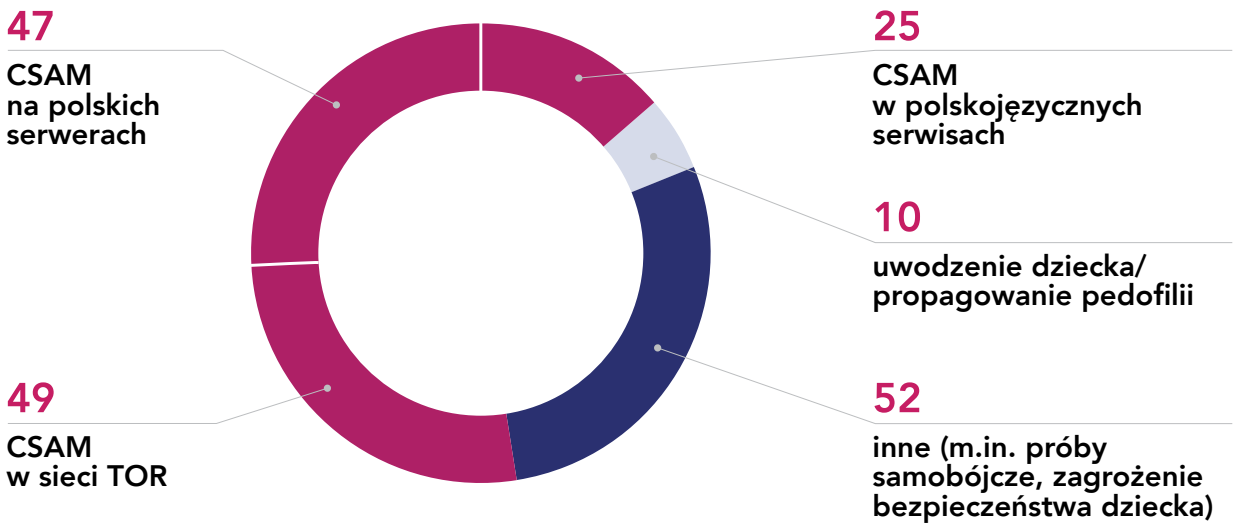
Zgłoszone do ISP
Przesłanie zawiadomienia o treściach o charakterze bezprawnym (dotyczących CSAM) zgodnie z art. 14 Ustawy o świadczeniu usług drogą elektroniczną w przypadku hostingodawcy w Polsce lub poinformowanie hostingodawcy znajdującego się poza zasięgiem INHOPE o bezprawnych treściach (dotyczących 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 oraz Fundacja Dajemy Dzieciom Siłę).

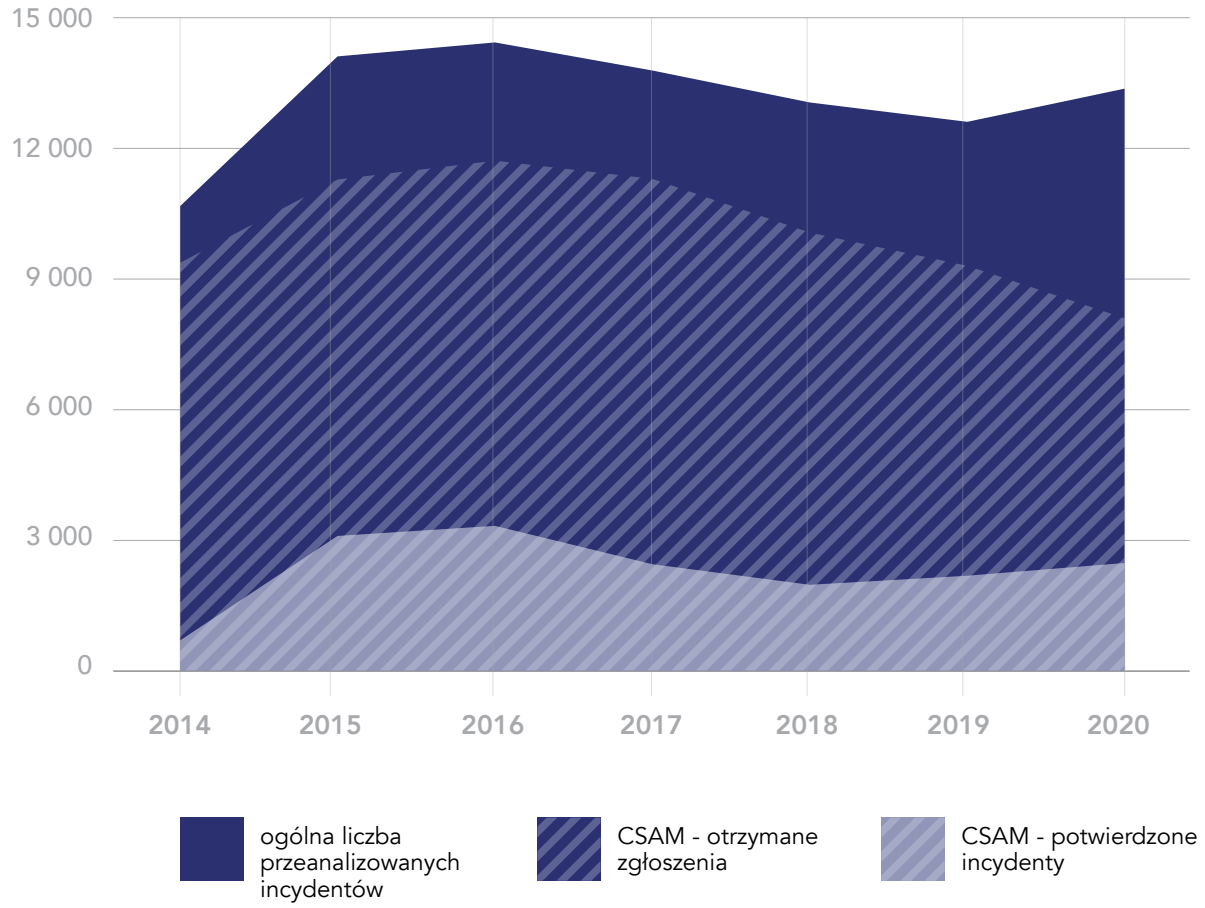
Zgłoszone Policji
Przekazane do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji.

8 | Klasyfikacja incydentów przekazanych do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji



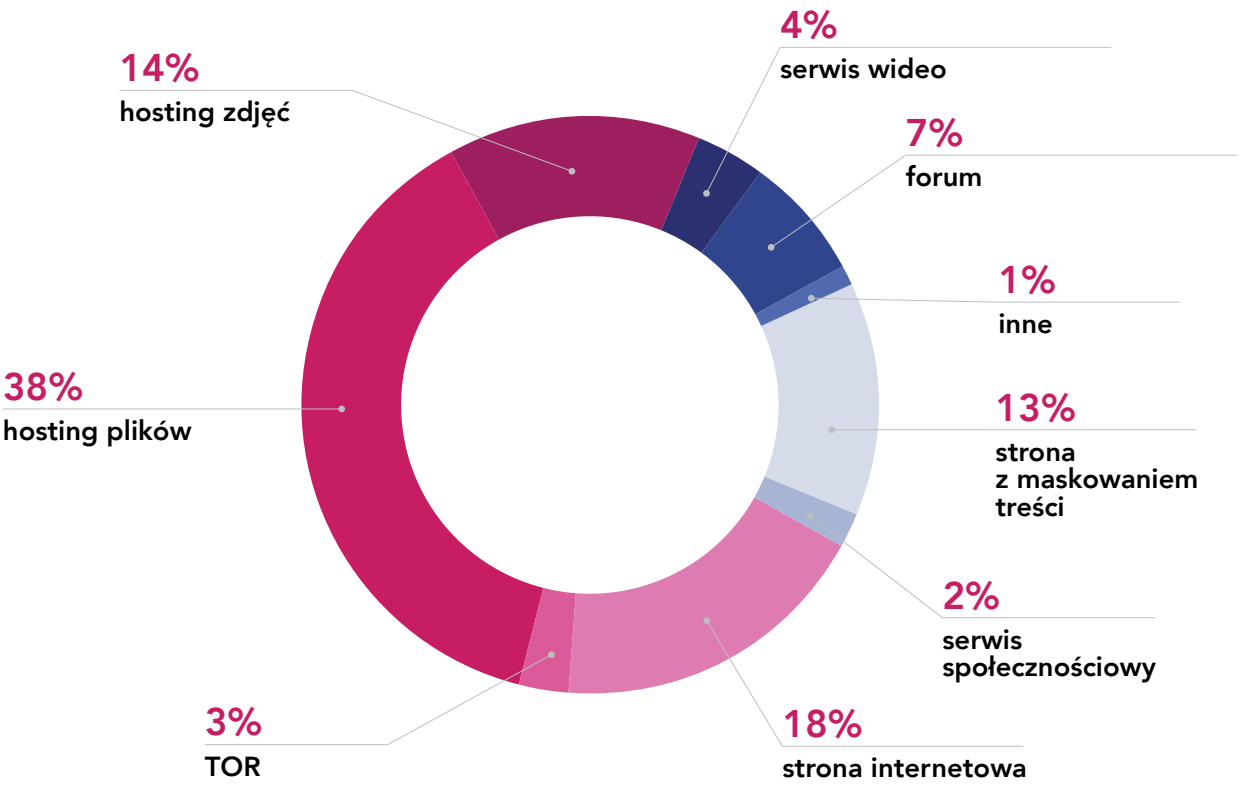
ANALIZA TREŚCI CSAM

9 Liczba zgłoszeń dotyczących potencjalnych materiałów typu CSAM oraz potwierdzonych incydentów CSAM na tle ogólnej liczby przeanalizowanych incydentów w latach 2014-2020



	2014	2015	2016	2017	2018	2019	2020
Ogólna liczba przeanalizowanych incydentów wszystkich kategorii	11 063	14 277	14 298	13 962	13 239	12 517	13 400
CSAM - otrzymane zgłoszenia z tej kategorii	9 117	11 227	11 759	11 457	10 784	9 194	8 021
CSAM - potwierdzone incydenty z tej kategorii	1 395	3 029	3 126	2 459	1 998	2 295	2 517

10 | CSAM analizowany przez Dyżurnet.pl - lokalizacja w usługach internetowych (n=2 517)



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.

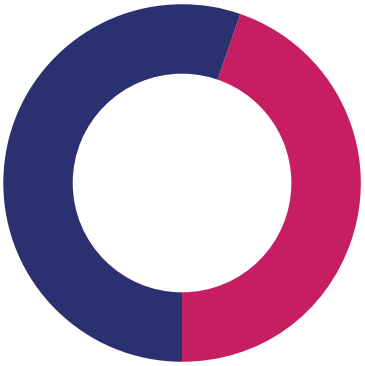
Forum
fora dyskusyjne znajdujące się w otwartych zasobach internetu poświęcone określonej tematyce; mogą zawierać pliki multimedialne.

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.

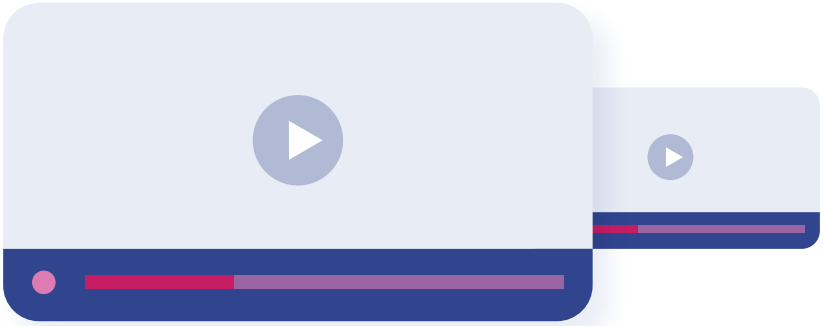
TOR (*The Onion Router*)
zasoby znajdujące się w zanonimizowanej sieci TOR, dostępne wyłącznie za pomocą dedykowanej przeglądarki; większość powyższych usług internetowych może mieć swój odpowiednik w sieci TOR. Adresy zasobów w sieci TOR (tzw. hidden services) zawierają pseudodomenę najwyższego poziomu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

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

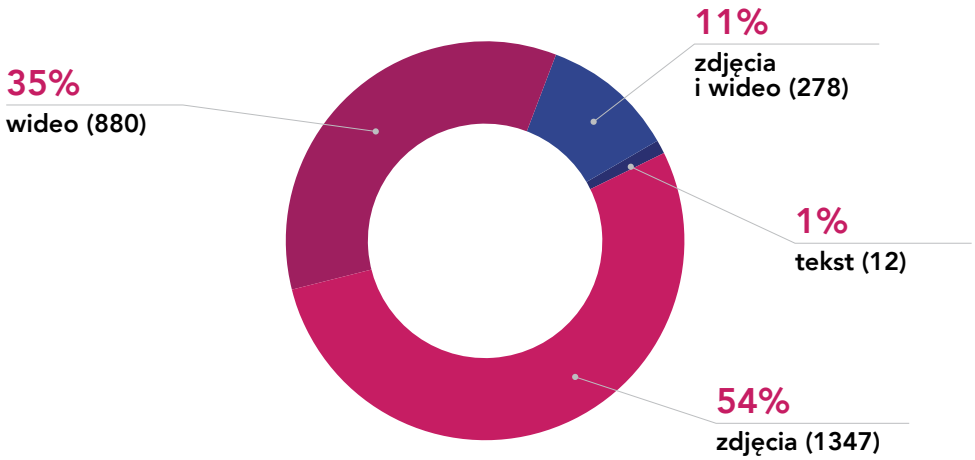


5 086
ROZPOZNANE WCZEŚNIEJ PRZEZ ZESPOŁY INHOPE

4 113
ANALIZOWANE PO RAZ PIERWSZY PRZEZ DYŻURNET.PL

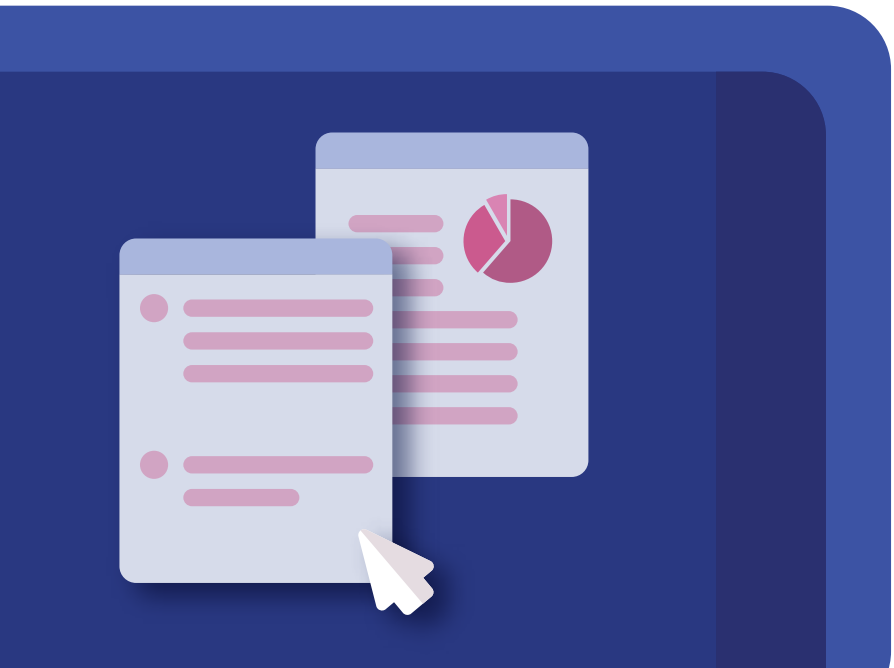


12 | CSAM analizowany przez Dyżurnet.pl – rodzaj treści (n=2 517)

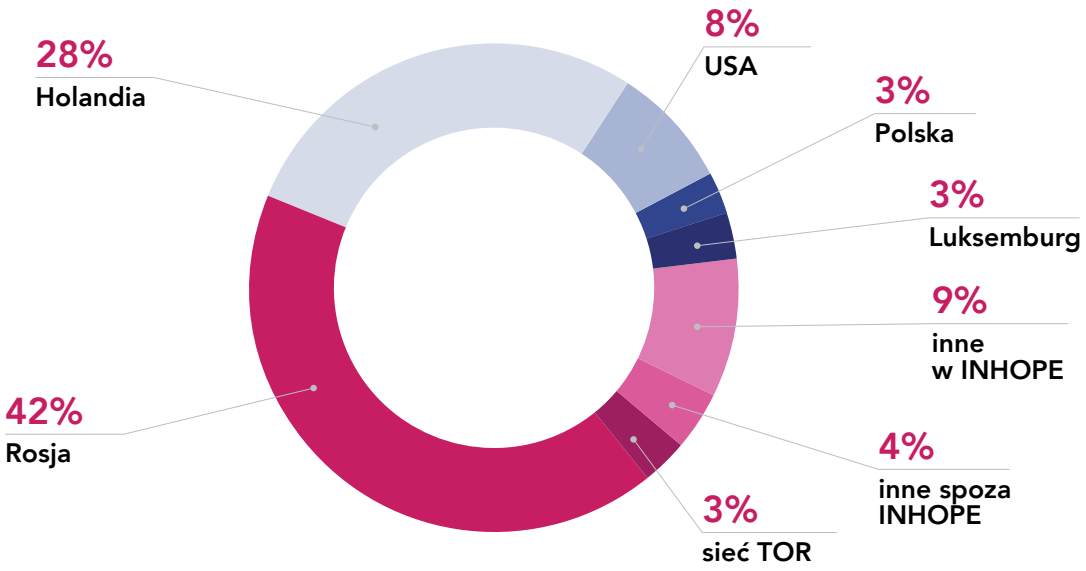


Baza ICCAM opiera się na rozpoznawaniu hash value (cyfrowego odcisku) plików. Obrazy i filmy, które zostały przeanalizowane i odpowiednio zaklasyfikowane nie są już wyświetlane przy ponownym wprowadzeniu do bazy ICCAM. Dzięki temu rozwiązaniu unika się powielania pracy analityków i poddawania ich czynnikom 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.

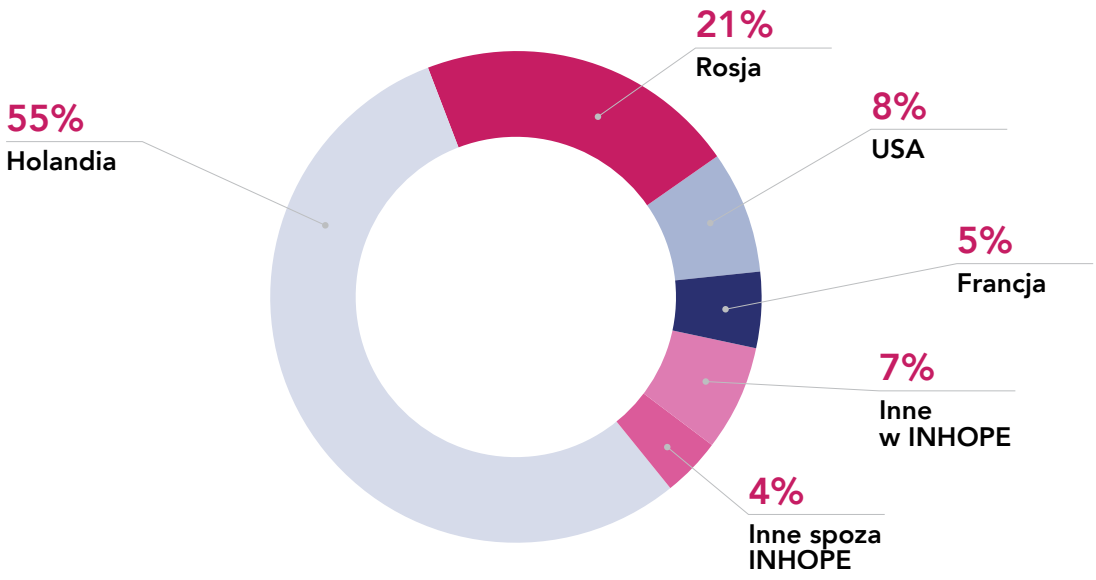


13 CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do adresów URL (n=2 517)

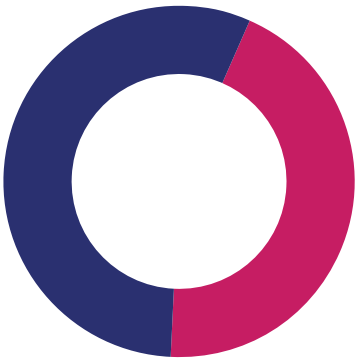


Lokalizacja serwera z treścią CSAM jest kluczowa dla skutecznej reakcji. Zespół Dyżurnet.pl wyróżnia dwa rodzaje lokalizacji: w odniesieniu do adresu URL oraz w odniesieniu do plików foto/wideo. Przykładowo – strona http://abc.com znajduje się na serwerze zlokalizowanym w USA. Lokalizację tego typu pokazuje 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=4113)



15 | CSAM analizowany przez Dyżurnet.pl – podział ze względu na kategorię treści (n=4 113)



56%
BASELINE CSAM

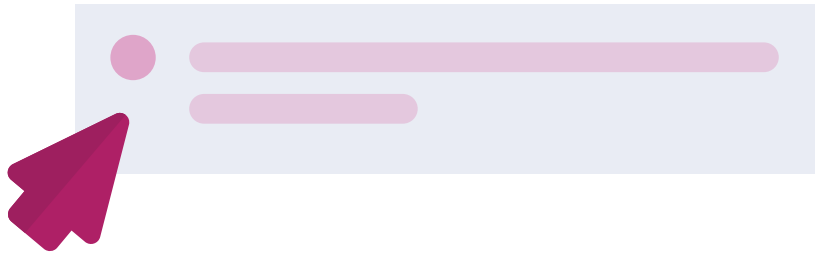
44%
NATIONAL CSAM

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. (te 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 – treści o charakterze pornograficznym wytworzone przez ofiary (*self-generated content*) w CSAM (n=2 517)

86%

NON SELF-GENERATED CONTENT (2162)

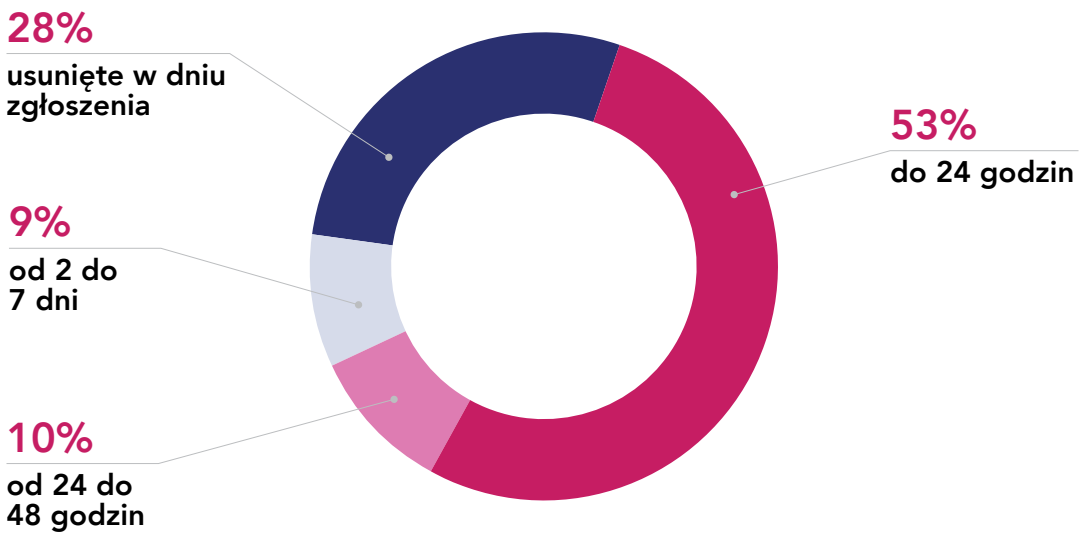
14%

SELF-GENERATED CONTENT (355)

Self-generated sexual content
Materiał foto/wideo wytworzony samodzielnie przez ofiarę, uzyskany za zgodą lub bez zgody małoletniego, przedstawiający go 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”[1] oraz na stronie 27.

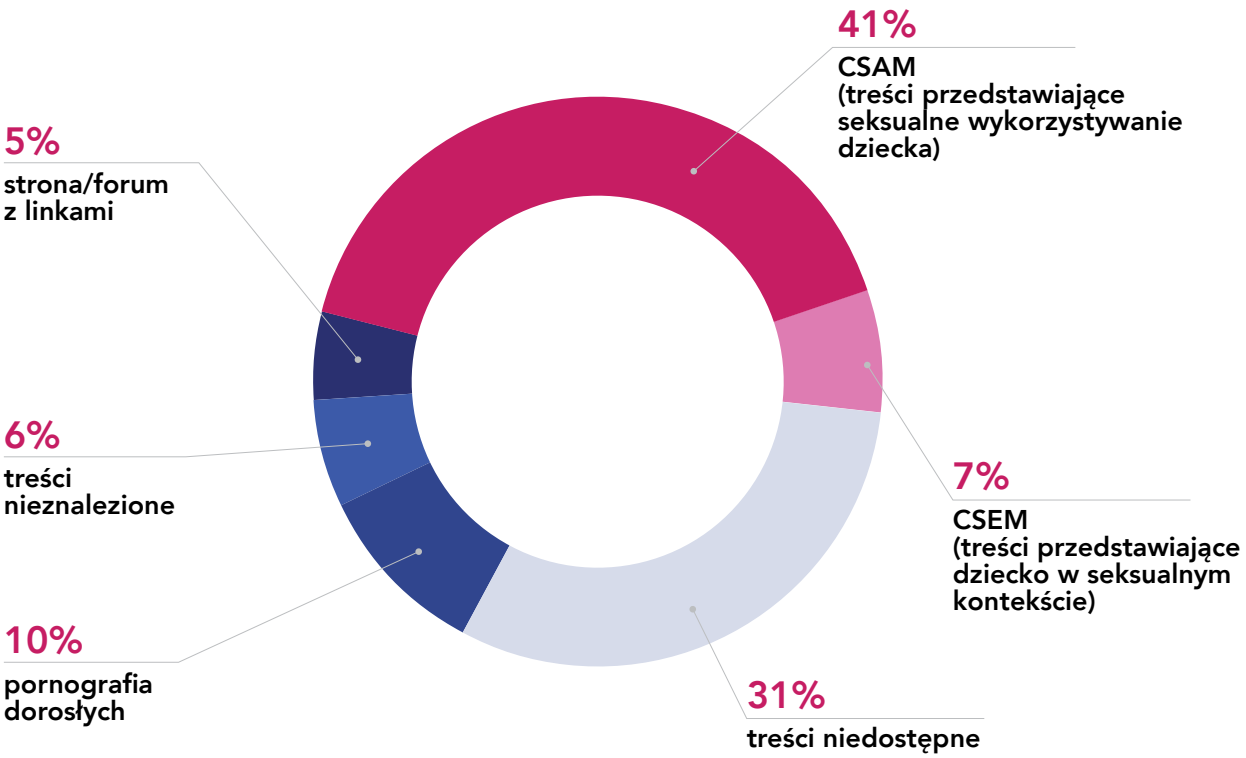
Warto zaznaczyć, że liczba tego typu incydentów wzrosła z 202 w roku 2019 do 355 w roku 2020.

17 | Czas publicznej dostępności CSAM/CSEM zlokalizowanych w Polsce i zgłoszonych do Dyżurnet.pl przez inne zespoły INHOPE (n=57)

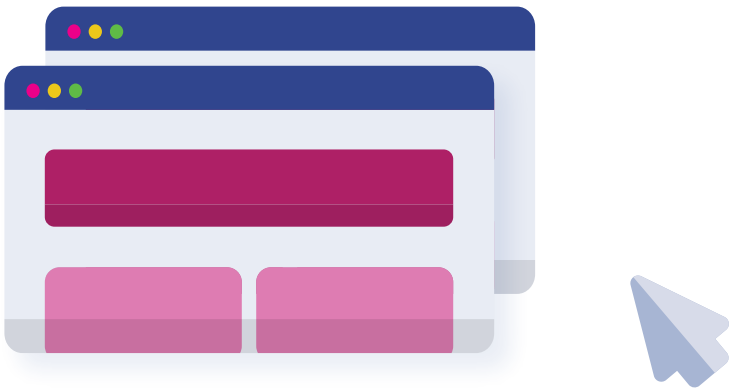


1. https://dyzurnet.pl/uploads/2020/04/Ryzykowne_zachowania_na_www.pdf

18 | Klasyfikacja stron maskujących swoją treść (n=784)



Liczba stron maskujących swoją treść analizowanych przez zespół Dyżurnet.pl w roku 2020 wyniosła 784 (w roku 2019 – 670). W przeszło połowie przypadków (53%) eksperci Dyżurnet.pl odblokowali ukrytą treść, a następnie zgłosili taką stronę właściwemu zespołowi reagującemu. W roku 2019 było to 61% skuteczności. Aby zwiększać odsetek odblokowywanych i następnie zgłaszanych stron tego typu, zespół Dyżurnet.pl udostępnił wtyczkę do raportowania, która pozwala skutecznie zgłaszać strony maskujące swoją treść (patrz str. 51).



DZIAŁANIA PODEJMOWANE PRZEZ DYŻURNET.PL WOBEC NIELEGALNYCH I SZKODLIWYCH TREŚCI

Od 2015 r. zespoły reagujące zrzeszone w INHOPE korzystają ze zintegrowanej bazy wymiany informacji dotyczących CSAM. Baza ICCAM posiada innowacyjne rozwiązania związane z analizą i klasyfikacją plików graficznych i wideo. 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 (tzw. *baseline*)**. Informacja o najbardziej drastycznych materiałach przekazywana jest bezpośrednio do bazy ICSE (*International Child Sexual Exploitation*[2]), umożliwiając podjęcie działań w celu identyfikacji zarówno ofiar, jaki i sprawcy.

W roku 2020 eksperci Dyżurnet.pl wprowadzili do ICCAM 2 187 raportów dotyczących nowych adresów URL zawierających nielegalne treści. Znajdowało się tam ogółem 9 199 plików graficznych i nagrań wideo, zaklasyfikowanych jako treść przedstawiająca seksualne wykorzystanie dziecka. W 1 117 przypadkach adres URL został już wcześniej zgłoszony do bazy ICCAM przez inny zespół reagujący sieci INHOPE.

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 2020 miała miejsce w przypadku **349** incydentów.

W **47** 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 organów ścigania, które również są powiadamiane.

Ze względu na zakres wykraczający poza ramy działalności Dyżurnet.pl **104** sprawy zostały przekazane innym podmiotom - m.in. działającemu w ramach NASK PIB zespołowi CERT Polska czy telefonom interwencyjnym prowadzonym przez Fundację Dajemy Dzieciom Siłę.

183 incydenty zostały zgłoszone do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Dotyczyły one przede wszystkim seksualnych nadużyć wobec dzieci. Zgłoszenia związane z CSAM stanowiły 67% przekazanych incydentów (na polskich serwerach – 26%, w polskojęzycznych serwisach – 14%, w sieci TOR – 27%). 10% przesłanych spraw dotyczyło uwodzenia dziecka i pochwalania zachowań o charakterze pedofilskim. 28% pozostałych spraw zgłoszonych do Policji obejmowało inne treści znajdujące się na serwerach w Polsce (próby samobójcze, treści rasistowskie i nacjonalistyczne, zagrożenie bezpieczeństwa dziecka).

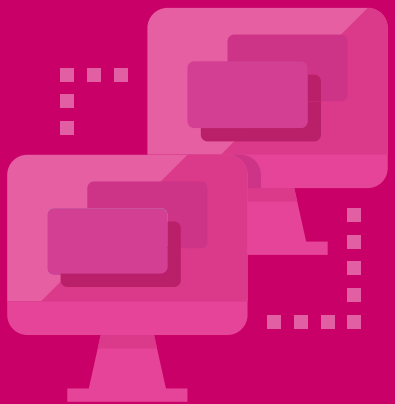
2. https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

ZMIANA ORGANIZACJI PRACY W TRAKCIE PANDEMII

Rok 2020 i nowa sytuacja spowodowana obostrzeniami wynikającymi z pandemii COVID-19, wymagała od Zespołu nowego sposobu pracy i dostosowania się do niej w bardzo krótkim czasie. Zespół Dyżurnet.pl w czasie pandemii pracuje głównie zdalnie. Jednak w trosce o utrzymanie płynnej obsługi zgłoszeń dotyczących treści potencjalnie przedstawiających seksualne wykorzystywanie dzieci oraz mając na uwadze przyjęte standardy bezpieczeństwa, wprowadzone zostały dyżury analityków w biurze stacjonarnym.

Statystyki pokazują, że nowy tryb pracy nie wpłynął negatywnie na efektywność zespołu oraz liczbę analizowanych zgłoszeń. W porównaniu do roku 2019, liczba zidentyfikowanych incydentów CSAM w roku 2020 wzrosła o blisko 10% z 2 295 do 2 517. I to pomimo niższej o 12% liczby otrzymanych zgłoszeń z tej kategorii (8 021 w roku 2020 do 9 194 w roku 2019).

Jednocześnie analitycy pozostający w warunkach pracy zdalnej stanęli przed wyzwaniem obsługi zdecydowanie zwiększonej liczby zgłoszeń z innych kategorii. Liczba zgłoszeń innych treści wzrosła o ponad 60% (z 3 250 w roku 2019 do 5 300 w roku 2020). Z tej liczby aż 2 042 incydentów zostało ocenione przez analityków jako treści legalne i nienoszące oznak szkodliwości.



TRENDY I ZJAWISKA

INTYMNE TREŚCI WYTWORZONE PRZEZ MŁODYCH UŻYTKOWNIKÓW

Już w ubiegłorocznym Raporcie Dyżurnet.pl informowaliśmy o intensywnie rozwijającym się zjawisku *self-generated sexual content*. Zjawisko to obejmuje wytworzenie materiałów (foto lub wideo) przez osobę nieletnią świadomie angażującą się w aktywność seksualną lub erotyczną. W tym roku Zespół zauważył wzrost liczby zgłoszeń zawierających materiały pornograficzne wytworzone przez osoby nieletnie. Analiza materiałów nie zawsze daje pewność, kto jest ich autorem ujęcia - „z ręki", odbicia w lustrze, zapis transmisji online wskazują na materiały wytworzone samodzielnie. Zgłoszenia otrzymane przez Dyżurnet.pl dotyczą przede wszystkim zdjęć z utrwalonych transmisji online, które następnie zostały opublikowane na poświęconych takiej tematyce forach. Materiały mogą przedstawiać jedno lub kilka osób małoletnich, którzy uczestniczą w aranżacji przekazu lub znacznie młodsze dzieci, które znajdują się tam przypadkowo i nie rozumieją kontekstu sytuacji.

Intymne treści wytwarzane samodzielnie (self-generated sexual content) mogą obejmować treści przedstawiające wykorzystywanie seksualne dzieci utrwalone za pomocą kamer internetowych, często w pokoju dziecka, a następnie udostępnione online.

Powody wytwarzania tego typu materiałów mogą być różne, od wymiany treści intymnych określanej jako sexting, przez chęć zaistnienia w grupie znajomych do tworzenia materiałów intymnych w procesie uwodzenia małoletniego (*child grooming*) lub jako konsekwencja użytej wobec niego groźby (szantażu na tle seksualnym). Niestety często materiały zamieszczone w sieci lub przesłane komuś w zaufaniu zostają upublicznione w internecie, co może prowadzić do późniejszego ich pojawienia się na stronach pornograficznych. Ostatecznie mogą dostać się również w ręce osób o skłonnościach pedofilskich. Opublikowanie materiałów intymnych może prowadzić do kolejnych nadużyć wobec dziecka, np. agresywnych i wulgarnych komentarzy, dalszej seksualizacji oraz cyberprzemocy. Dlatego ważne jest, aby każdorazowo reagować na obecność osób małoletnich na portalach erotycznych, nie zachęcać ich do podejmowania nieodpowiednich zachowań oraz zgłaszać do moderacji. Zgłoszeń niepokojących materiałów można dokonywać poprzez kontakt z administratorem serwisu lub przesyłając zgłoszenie do zespołu Dyżurnet.pl.

Warto zaznaczyć, że materiał wytworzony samodzielnie nie oznacza materiału wytworzonego dobrowolnie. Tak jak w przypadku uwodzenia dziecka w sieci (*child grooming*) wytworzenie materiałów może być wynikiem przemyślanej manipulacji dzieckiem lub też wymuszenia przez

sprawcę groźbą (np. w wyniku szantażu na tle seksualnym). Może to być również skutek powszechnego dostępu do treści erotycznych i pornograficznych oraz coraz wyższego poziomu seksualizacji mediów.

Według polskiego prawa utrwalanie i publikacja treści pornograficznych z udziałem osoby poniżej 18. roku życia jest nielegalne.

Skala zjawiska self-generated sexual content według badań brytyjskiej organizacji Internet Watch Foundation[3] w liczbach prezentuje się następująco:

- 27% stron zgłoszonych i przeanalizowanych przez IWF oceniono jako zawierające *self-generated sexual content*,
- 96% tych treści przedstawiało dzieci znajdujące się w domowym otoczeniu, przeważnie w pokojach lub sypialniach dziecka,
- 98% materiałów przedstawiało dzieci w wieku 13 lat i mniej,
- 73% tych materiałów pojawiło się na forach specjalizujących się w udostępnianiu płatnych plików wideo przedstawiających seksualne zachowania dzieci zarejestrowane z transmisji przeprowadzonych na żywo.

Eksperci zespołu Dyżurnet.pl apelują o każdorazowe zgłaszanie do odpowiednich podmiotów materiałów utrwalających osobę prawdopodobnie nieletnią, angażującą się w aktywność erotyczną lub pornograficzną.

3. https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf

„SEXTORTION" I ZMIANA NAZWY ZJAWISKA

Rozwój internetu w ostatnich latach zaowocował wieloma zmianami w życiu społecznym, w tym pojawieniem się nowych form przestępczości *online*. Jedną z nich jest wymierzony w dzieci szantaż na tle seksualnym odbywający się online, najczęściej popełniany przez sprawców motywowanych seksualnie lub finansowo. Zjawisko to wymyka się próbom zdefiniowania go, niewiele jest też badań, które je opisują, tymczasem wpływ tego fenomenu na ofiary jest w większości przypadków druzgocący. Zachowanie tutaj opisywane jest często określane w przestrzeni publicznej jako „sextortion", jednak takie postępowanie spotyka się z coraz większą krytyką ze strony ekspertów w tym zakresie, patrzących na nie z punktu widzenia ofiary. Ze względu na powagę zjawiska oraz to, jakie może pociągać za sobą konsekwencje dla ofiary, Zespół Dyżurnet.pl proponuje zmianę nazwy zjawiska na **szantaż na tle seksualnym**. To posunięcie jest pierwszym krokiem Zespołu Dyżurnet.pl na drodze do rozpoczęcia debaty nad terminologią stosowaną w odniesieniu do zjawiska seksualnego wykorzystywania dzieci w cyberprzestrzeni.

Bezpośrednie wzmianki o szantażu polegającym na wykorzystaniu zdjęcia lub nagrania osoby w celu zmuszenia jej do określonego zachowania, z reguły polegającego na przekazaniu materiałów o treściach seksualnych prezentujących tę osobę, bądź gratyfikacji finansowej, pojawiły się około 2012 r., choć nie znaczy to, iż nie występowało ono wcześniej.

Kluczowym zagadnieniem w przebiegu procesu szantażu jest posiadanie przez sprawcę zdjęć lub filmów video utrwalających intymne zachowania przyszłej ofiary.[4] Bez ich istnienia proces opierający się na późniejszych groźbach nie miałby miejsca. Zdjęcia, filmy video, czy nawet fragment konwersacji wygenerowany samodzielnie przez nieletniego dla celów prywatnych, np. w celu nawiązania lub podtrzymania seksualnej relacji. Udokumentowane są również przypadki pozyskania takich materiałów przez sprawcę za pośrednictwem złośliwego oprogramowania[5] bądź *hackingu*[6].

Aby pozyskać kompromitujący materiał sprawca ucieka się do oszukańczych praktyk, często je łącząc lub używając zamiennie. W raporcie NCMEC[7] zostały one bliżej scharakteryzowane[8]:

- wzajemność: „pokażę ci, jeśli ty pokażesz mnie",
- ofiarowywanie czegoś dziecku, np. pieniędzy lub narkotyków w zamian za materiał,
- udawanie, że jest się pracownikiem agencji modelingowej,
- wypracowanie więzi z dzieckiem poprzez ustanowienie przyjacielskiej lub romantycznej relacji,
- używanie wielu tożsamości w celu skontaktowania się z dzieckiem.

4. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime
5. B. Wittes, C. Poplin, Q. Jurecic and C. Spera, Center for Technology Innovation at Brookings, Sextortion: Cybersecurity, teenagers, and remote sexual assault (Brookings' report), 2016, s. 6 https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/
6. https://www.fbi.gov/file-repository/stop-sextortion-brochure.pdf/view
7. National Center for Missing and Exploited Children (NCMEC) to prywatna organizacja non-profit założona w 1984 roku przez Kongres Stanów Zjednoczonych, zajmuje się zwalczaniem nielegalnych treści w internecie.
8. http://www.missingkids.org/theissues/sextortion

W przypadku finansowo motywowanych sprawców materiał służący do szantażu jest w większości przypadków wykreowany jako część seksualnie nacechowanej konwersacji online, do której często dochodzi poprzez stosowanie technik manipulacyjnych przez sprawcę.

Będąc w posiadaniu materiałów o treściach seksualnych prezentujących przyszłą ofiarę sprawca szantażu na tle seksualnym posuwa się następnie do sformułowania groźby, najczęściej w postaci publikacji tych materiałów w serwisach społecznościowych czy też przesłania ich znajomym lub rodzinie. W ten sposób sprawca zmusza swoją ofiarę do określonego zachowania.

Szantaż na tle seksualnym online skierowany przeciwko dzieciom ma miejsce, ponieważ sprawca chce od nich uzyskać coś, co stanowi dla niego określoną wartość. Dostępne źródła wymieniają najczęściej dwa rodzaje tej wartości: są to seksualne materiały uzyskane od dziecka lub możliwość spotkania się z nim w rzeczywistości albo coś, co ma wartość materialną. Żądania sprawcy mogą mieć różny charakter – mogą dotyczyć określonego typu materiałów intymnych, określonej ilości lub szczególnych treści w nim zawartych. Zdarzają się również przypadki, kiedy sprawca wymusza na swojej ofierze zaangażowanie w seksualne akty innych dzieci, rodzeństwa lub znajomych[9].
W większości przypadków dziecko błędnie zakłada, że dostosowanie się do żądań sprawcy zatrzyma przestępczy proceder.

Gdzie szukać pomocy w przypadku doświadczania opisanych powyżej zachowań?

116111.pl - telefon zaufania dla dzieci i młodzieży.

Infolinia dla dzieci, młodzieży, rodziców i pedagogów prowadzona przez fundację ITAKA – **800 080 222**.

Opisane powyżej zachowanie jest przestępstwem i powinno być zgłoszone Policji.

9. Europol 2017, s.13.

ODPOWIEDZIALNA ROLA WŁAŚCICIELI SERWISÓW W KWESTII ZWALCZANIA CSAM

Zdecydowana większość zgłoszeń do zespołu Dyżurnet.pl kierowana jest przez zwykłych użytkowników internetu, raportujących potencjalnie nielegalne treści. Zdarza się jednak, że do Dyżurnet.pl zwracają się również przedstawiciele serwisów, którzy zanotowali potencjalnie przestępczą aktywność ich użytkowników. Tak stało się w przypadku jednego z serwisów umożliwiających zamieszczanie zdjęć.

Administratorzy platformy zauważyli, że jeden z użytkowników od dłuższego czasu umieszcza tam niepokojące treści o charakterze pedofilskim prezentujące prawdopodobnie osoby nieletnie. Moderacja na bieżąco usuwała materiały, natomiast użytkownik zakładał nowe konta i ponownie je udostępniał.

Administracja była w posiadaniu adresu IP użytkownika oraz zabezpieczyła wszelkie dane na potrzeby organów ścigania.

Eksperci zespołu Dyżurnet.pl skontaktowali przedstawicieli serwisu z funkcjonariuszami Wydziału do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji właściwej dla siedziby firmy, po czym doszło do spotkania roboczego, podczas którego ustalono dalsze działania.

Tak odpowiedzialne postępowanie serwisów internetowych, niestety, nie jest zbyt częste. Administratorzy koncentrują się na usuwaniu bezprawnych treści, nie dążąc do przekazania odpowiednim organom informacji służących identyfikacji zamieszczających je osób.

Zespół Dyżurnet.pl służy w tej kwestii pomocą i zwraca się z apelem do właścicieli serwisów o nieignorowanie problemu zamieszczania treści przedstawiających seksualne wykorzystywanie dzieci oraz identyfikacji popełniających to przestępstwo użytkowników.

SZTUCZNA INTELIGENCJA POMAGA W WALCE Z CSAM

Statystyki wszystkich organizacji zajmujących się walką z przemocą seksualną wobec nieletnich wskazują, że z roku na rok zwiększa się liczba materiałów przedstawiających seksualne wykorzystywanie dzieci udostępnianych w internecie. Firmy zajmujące się szeroko rozumianym hostingiem i dostawcy usług cyfrowych nie mają wystarczających zasobów ludzkich do sprawdzania i analizowania wszystkich plików zapisywanych na ich serwerach przez użytkowników.

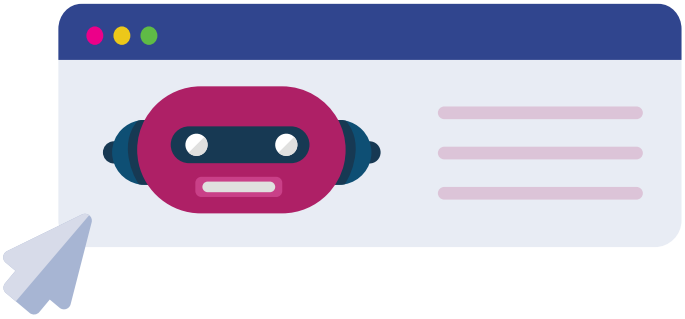
Postęp technologiczny i szybki rozwój algorytmów sztucznej inteligencji otwiera nowe możliwości zwiększenia skuteczności wykrywania, a w efekcie usuwania materiałów CSAM z serwerów, których treści udostępniane są użytkownikom w internecie.

Głębokie sieci neuronowe, a w szczególności modele sieci konwolucyjnych, umożliwiają analizę obrazu pod kątem rozpoznawania konkretnych cech. Mówiąc w dużym uproszczeniu, jesteśmy w stanie stworzyć algorytm, który będzie wykrywał potencjalną obecność treści pornograficznych z udziałem małoletnich (zdjęcia, filmy wideo) i automatycznie raportował tego typu incydenty administratorom serwisów, co z kolei da możliwość szybkiego zablokowania dostępu do nich i wysłania odpowiedniego zgłoszenia na policję.

Zaletą tego typu metod jest ich szybkość, czyli możliwość sprawdzenia wielu plików w krótkim czasie, działanie bez zaangażowania ludzi, a także coraz większa trafność. Szczególną wartość ma zwolnienie pracowników z obowiązku przeglądania dużych ilości szkodliwych treści.

Algorytmy sztucznej inteligencji coraz lepiej radzą sobie z rozpoznawaniem takich cech obrazu, jak np. wiek znajdujących się na nich osób, sylwetki ludzi, występowanie nagości, wykonywanie określonych czynności przez osoby widoczne na zdjęciach lub wideo, a nawet konkretnych emocji.

Ilość danych, które w ciągu doby przesyłane są między serwerami jest zbyt duża, żeby analizą treści zajmowali się wyłącznie ludzie. Sztuczna inteligencja może w niedalekiej przyszłości okazać się doskonałą pomocą pełniącą rolę strażnika, który będzie na bieżąco filtrował, rozpoznawał i blokował potencjalnie nielegalne treści.



Do analizy obrazu coraz częściej dołączają udoskonalane modele języka naturalnego, które mogą okazać się bardzo pomocne w rozpoznawaniu stylu, a nawet kontekstu całych zdań. Tego typu algorytmy mogą pomagać administratorom popularnych czatów na przykład w rozpoznawaniu prób uwodzenia osób małoletnich (tzw. *grooming*). Odpowiednio wytrenowane modele mogą w przyszłości zapewnić lepszą ochronę dzieci i młodzieży w internecie.

PANDEMIA I JEJ WPŁYW NA CSAM

Już na początku marca 2020 r., kiedy w wielu krajach zamykano szkoły i miejsca pracy, wyspecjalizowane instytucje i organizacje ostrzegały przed możliwością nasilenia się zjawiska seksualnego wykorzystania dzieci jako następstwa wprowadzenia restrykcji społecznych, takich jak całkowity lub częściowy *lockdown*[10]. Zdaniem tych instytucji okoliczności te powodują zwiększone ryzyko narażenia na szkodliwe kontakty za pośrednictwem mediów społecznościowych, czatów w aplikacjach, gier online czy też mniej bezpiecznych aplikacji edukacyjnych.

Samotność i izolacja dzieci mogą potencjalnie działać na korzyść osób seksualnie nimi zainteresowanych. W obliczu nieznanych dotąd trudności dziecko może być bardziej podatne na wpływy, przez co osobom o złych intencjach łatwiej nawiązać z nim intymną relację, a następnie wykorzystać ją dla krzywdzących dziecko celów. Brak tradycyjnych kontaktów interpersonalnych z rówieśnikami może prowadzić starsze dzieci do angażowania się w bardziej ryzykowne zachowania online, jak np. sexting czy dzielenie się wytworzonymi samodzielnie intymnymi materiałami w postaci zdjęć lub wideo. Materiały te, wydostając się poza ich kontrolę, mogą narazić przedstawiające je osoby na nękanie, szantaż czy publiczne upokorzenie. Ponadto, więcej czasu spędzanego online zarówno przez dorosłych jak i dzieci – bardzo często bez odpowiedzialnego nadzoru rodziców – może szczególnie sprzyjać zjawisku uwodzenia (*child grooming*) i nagabywania online, jak również seksualnym wymuszeniom w cyberprzestrzeni.

Obok sugerowanego związku pomiędzy wprowadzonymi restrykcjami a zwiększoną liczbą przestępstw o podłożu seksualnym online, pandemia może również wpływać na skalę seksualnego wykorzystywania dzieci w realnym świecie. W warunkach pandemicznych trudniej jest zidentyfikować ofiarę takiego przestępstwa, ponieważ dzieci wykluczone są ze społecznych kontaktów, nie uczestniczą też w zajęciach w szkole: miejscu, w którym przestępstwa tego typu są najczęściej identyfikowane i zgłaszane odpowiednim instytucjom. W przypadku dzieci, wobec których stosowana jest różnego rodzaju przemoc w środowisku domowym szkoła niejednokrotnie staje się przecież jedyną bezpieczną przystanią. W warunkach narzuconych przez pandemię zostają one pozbawione tego schronienia i zmuszone do przebywania w domach razem ze swoimi oprawcami.W wielu krajach organy ścigania oraz instytucje wspomagające zanotowały od początku pandemii wzrost liczby zgłoszeń dotyczących przestępstw o podłożu seksualnym wobec dzieci[11]. Wskazuje się również na wzrost aktywności online, zarówno jeśli chodzi o próby kontaktu z dziećmi ze strony osób seksualnie nimi zainteresowanych, w zakresie wymiany peer-to-peer, gdzie intymne materiały są dobrowolnie i samodzielnie tworzone przez małoletnich użytkowników, jak również w obszarze aktywności dotyczącej seksualnego wykorzystywania dzieci w darknecie. Zaobserwowano także zwiększoną aktywność

10. NetClean, Covid-19 Impact 2020. A Report About Child Sexual Abuse Crime, s.15.
11. NetClean 2020, s. 6, 15, 20.

w kontekście poszukiwania materiałów prezentujących seksualne wykorzystanie dzieci oraz większą liczbę stron zablokowanych ze względu na zawartość nielegalnych treści, w tym materiałów przedstawiających seksualne wykorzystanie dzieci. Ponadto, na forach użytkowanych przez osoby seksualnie zainteresowane dziećmi pojawiło się więcej nagrań z kamerek internetowych[12]. Mowa tutaj o treściach pornograficznych z wymuszonym udziałem dzieci, materiałach dobrowolnie wytworzonych przez małoletnich i udostępnionych na portalach społecznościowych, a także takich, które zostały nagrane i rozpowszechnione bez wiedzy i zgody dziecka. W Stanach Zjednoczonych liczba zgłoszeń dotyczących uwodzenia dzieci online, w okresie od marca do sierpnia 2020 r. uległa podwojeniu w porównaniu z poprzednim rokiem[13]. W niektórych kręgach popularne stały się relacje na żywo z przestępstwa seksualnego dokonanego na dziecku przez członka rodziny. Ponadto wzrost popularności relacji na żywo jest prognozowany ze względu na wprowadzone restrykcje dotyczące podróży i przemieszczania się.

Istnienie związku pomiędzy zwiększoną ilością czasu spędzanego przez dzieci online z uwagi na warunki narzucone przez pandemię a ich podatnością na zjawiska z obszaru wykorzystywania seksualnego wydaje się być prawdopodobne. Możliwa jest również korelacja pomiędzy nasiloną podczas pandemii aktywnością dzieci w cyberprzestrzeni a produkcją nowych materiałów prezentujących ich seksualne wykorzystywanie, jednak posiadane w tym momencie informacje są niepotwierdzone badaniami empirycznymi. Realna ocena negatywnych skutków pandemii, również w tym obszarze, jest zatem kwestią do rozstrzygnięcia w najbliższej przyszłości.

12. https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic
13. NetCelan 2020, s. 28.

SERWISY SPOŁECZNOŚCIOWE I ZAWODNE FILTRY

Technologia i sztuczna inteligencja coraz częściej i skuteczniej wspomagają nas w walce z nielegalnymi treściami w internecie. Sztuczna inteligencja jest stosowana w miejscach i sytuacjach, gdzie do tej pory zadania musiał wykonywać człowiek. Jednakże, należy pamiętać, że technologia bywa zawodna i wymaga udoskonaleń. Jak ważna jest praca nad nowymi rozwiązaniami pokazuje doświadczenie Zespołu. Zdarza się, że interwencja człowieka jest konieczna.

Pod koniec czerwca 2020 r. do Dyżurnet.pl zaczęły docierać niepokojące zgłoszenia, których dokonało blisko pięćdziesiąt osób. Zgłaszane były zdjęcia dziewczynek w wieku około 9-11 lat, bez ubrania, bez bielizny, czasami z nałożoną w miejscach intymnych grafiką (gwiazdy), dostępną w opcjach korygowania zdjęć na Instagramie. Eksperci Dyżurnet.pl natychmiast podjęli odpowiednie działania, zgłaszając profile do administratorów serwisu oraz na policję.

Serwisy społecznościowe korzystają z wysoko rozwiniętych mechanizmów automatycznej klasyfikacji i moderacji niepożądanych materiałów. Jednak ingerencja w postaci dodania grafiki cenzurującej zaburzyła ocenę stosowanych algorytmów i wpłynęła na ich błędną klasyfikację.

Ta sytuacja pokazała dwie bardzo ważne rzeczy – po pierwsze, algorytmy, sztuczna inteligencja, które nie powinny dopuścić do opublikowania takich zdjęć zostały „oszukane" za pomocą graficznych nakładek. Ważniejsza jednak jest druga konkluzja – internauci są coraz bardziej świadomi niebezpiecznych zjawisk, które pojawiają się w internecie i czują się odpowiedzialni za ich zgłaszanie.

NADUŻYCIA PODCZAS LEKCJI ONLINE #RIDING, #BOMBING CZY #TROLLING

Pandemia COVID-19 wymusiła wprowadzenie zajęć lekcyjnych prowadzonych w formie online. Pierwsze tygodnie zajęć wiązały się z nowym zagrożeniem, jakim było specjalne przeszkadzanie i przerywanie lekcji prowadzonych online.

Dzieci i nastolatki, znudzone dłużącymi się lekcjami, próbowały urozmaicić zajęcia, dokonując trollingu, rajdów, bombingu. Warto podkreślić, że zakłócanie wideokonferencji nie dotyczy tylko i wyłącznie szkół, ale w tym środowisku jest najbardziej widoczne i szkodliwe.

Samo zjawisko typu riding/bombing/trolling wyrosło ze środowiska graczy, gdzie przeciwnicy starali się popsuć innym rozgrywkę. Nuda, chęć zrobienia dowcipu, niezrozumienie szkodliwości zachowań czy poczucie anonimowości w internecie sprzyjają szerzeniu się zjawiska.

Niektóre z zachowań tylko zakłócały przebieg spotkania online i polegały na puszczaniu głośnej muzyki, złośliwym komentowaniu przebiegu lekcji, przedrzeźnianiu osób zabierających głos. Inne zachowania były wymierzone w nauczycieli lub osoby, które współuczestniczyły w zajęciach, zaobserwować można było obraźliwe i wulgarne komentarze czy złośliwe przeróbki zarejestrowanego materiału.

Jedne z najbardziej niepokojących sytuacji dotyczyły zachowań, które mogą być nielegalne, a na pewno są wysoce szkodliwe. Udostępnianie pornografii – również twardej, drastycznych materiałów, prezentowanie nagości to tylko niektóre z treści, które były zgłaszane do Dyżurnet.pl. Nagrania z lekcji publikowane były z kolei w internecie, stając się powodem do kolejnej fali cyberprzemocy.

W przypadku łamania prawa, np. poprzez prezentowanie treści pornograficznych osobom małoletnim, należy sprawę zgłosić organom ścigania, jednak jest to reakcja, która może przynieść jedynie odsunięte w czasie konsekwencje. Konieczne jest natychmiastowe zablokowanie treści, krótkie skomentowanie ich szkodliwości oraz poinformowanie rodziców i dyrekcji szkoły o wystąpieniu takiego incydentu. Bardzo ważne jest, aby dzieci, które funkcjonują w izolacji społecznej, gdy poziom lęku społeczeństwa jest znacznie wyższy niż zazwyczaj, miały przestrzeń do porozmawiania i odreagowania trudnej sytuacji. W przypadku drastycznych treści mogą się pojawiać lęk, strach, bezsenność.

OBYWATELSKA CZUJNOŚĆ NIE ZAWSZE W ZASIĘGU REAKCJI DYŻURNET.PL

W roku 2020 wielokrotnie do zespołu Dyżurnet.pl zwracali się użytkownicy, zgłaszając podejrzane zachowania innych użytkowników, które według nich miały pedofilski charakter. Były to przykładowo profile osób dorosłych w serwisach społecznościowych, które wśród znajomych miały wiele profili należących do dzieci. Zgłaszane były również profile osób, które zawodowo zajmowały się wykonywaniem zdjęć dzieci i w ramach castingu zwracały się z prośbą o zdjęcia np. w bieliźnie. Zgłoszenia dotyczyły też osób, które „wstawiają zdjęcia młodych dziewczyn z nieodpowiednimi podpisami, które mogą być dwuznaczne". Zgłaszający zwracali się do Dyżurnet.pl z prośbą o sprawdzenie, czy osoby te nie wykorzystują nieletnich.

Inną grupą tego typu zgłoszeń było raportowanie konwersacji z potencjalnym pedofilem, tzn. z rozmówcą, który rzekomo miał składać seksualne propozycje osobie poniżej 15 roku życia. Przy czym okazywało się, że „ofiarą" była osoba dorosła, w ramach „obywatelskiej prowokacji" podająca się za dziecko.

We wszystkich powyższych przypadkach właściwym organem, który może podjąć wymagane w takich sytuacjach czynności dochodzeniowo-śledcze jest policja.

Zespół Dyżurnet.pl może podjąć interwencję wyłącznie w sytuacji opisanej w art. 200a , czyli kiedy realne dziecko poniżej 15 roku życia otrzyma poprzez internet propozycję o charakterze seksualnym, a zrzuty ekranu, dokumentujące taką konwersację, zostaną przesłane na adres: **dyzurnet@dyzurnet.pl**

O takiej sytuacji niezwłocznie powiadomiona zostanie policja, która podejmie kroki umożliwiające identyfikację potencjalnego pedofila.

ZGŁOSZENIA DOTYCZĄCE TREŚCI LEGALNYCH

Rok 2020 to również rok, w którym Zespół po raz pierwszy zetknął się ze zmasowanymi zgłoszeniami powiązanych tematycznie, jednak nieszkodliwych i zupełnie legalnych, treści. Dyżurnet.pl otrzymał w ostatnich miesiącach setki powielonych wiadomości, które nie wymagały żadnej interwencji ze względu na neutralność wskazanych materiałów.

Liczba zgłoszeń innych treści wzrosła aż o przeszło 60% (z 3 250 w roku 2019 do 5 300 w roku 2020). Z tej liczby aż 2 042 incydenty zostały ocenione przez analityków jako treści legalne i nienoszące oznak szkodliwości.

Tego typu wielokrotne zgłoszenia tych samych lub bardzo podobnych materiałów to duże wyzwanie dla Zespołu, który, radząc sobie z tak dużymi wolumenami materiałów dostarczonych przez jednego tylko użytkownika, a nie wymagających reakcji ze strony organów ścigania, musi w odpowiednio krótkim czasie zareagować także na zgłoszenia, od których naprawdę może zależeć los dziecka.

Dużą rolę może tutaj odgrywać różny poziom wrażliwości użytkowników internetu. Niektóre materiały mogą wydawać się niepokojące lub szkodliwe i jednocześnie nie budzić tego typu wątpliwości czy podejrzeń u innych osób i być całkowicie legalnymi na terenie naszego kraju. Warto jednak przy zgłaszaniu potencjalnie nielegalnych treści mieć na uwadze to, że Zespół Dyżurnet.pl ze szczególnym oddaniem działa przede wszystkim na rzecz wykorzystywanych seksualnie dzieci i został powołany do tej misji z nadzieją, że czujność użytkowników internetu pomoże w jej realizacji.

DZIAŁALNOŚĆ EDUKACYJNO-POPULARYZATORSKA

Wydarzenia

14.01.2020 R.

Szkolenie prowadzone przez Interpol

Delegacja zespołu Dyżurnet.pl wzięła udział w szkoleniu skierowanym do pracowników analizujących materiały przedstawiające seksualne wykorzystywanie dzieci. Szkolenie było organizowane i prowadzone przez Interpol.

11.02.2020 R.

DBI „Dzień Bezpiecznego Internetu: Działajmy razem!"

Konferencja z okazji Dnia Bezpiecznego Internetu odbyła się 11 lutego w Teatrze Palladium w Warszawie. Wydarzenie to zgromadziło ok. 700 przedstawicieli sektora edukacyjnego, profesjonalistów pracujących z dziećmi oraz mediów. Organizatorem konferencji było Polskie Centrum Programu Safer Internet (PCPSI), które tworzą NASK i Fundacja Dajemy Dzieciom Siłę. Głównym partnerem wydarzenia była Fundacja Orange. Obchody DBI wspierane były przez Facebook Polska i Google Polska.

10.04.2020 R.

Uruchomienie nowej strony internetowej Dyżurnet.pl

W kwietniu 2020 r. przekazaliśmy do Państwa użytku nową stronę internetową naszego Zespołu. Zmianie uległa cała szata graficzna, logo oraz organizacja treści na stronie.

12.05, 14.05.2020 R.

Webinar Dyżurnet.pl - „Child grooming, sexting i sextortion. Niebezpieczne kontakty w internecie"

Wraz z zamknięciem szkół z powodu pandemii COVID-19 komputer stał się dla dzieci narzędziem służącym do nauki, kontaktu z nauczycielami i kolegami ze szkoły. Młodzi użytkownicy internetu, chcąc pozostać w kontakcie ze znajomymi i poznawać nowe osoby bez wychodzenia z domu, ulegają presji otoczenia, ogólnie panującej modzie, manipulacji. Dlaczego problem umieszczania w internecie intymnych materiałów przez dzieci jest tak ważny i wymagający reakcji? Webinarium poprowadziła ekspertka z zespołu Dyżurnet.pl.

19 - 21.05.2020 R.

INHOPE

Spotkanie INHOPE

22.07.2020 R.

INHOPE

Walne Zgromadzenie Stowarzyszenia INHOPE

#15lat NASK dyżurnet.pl

15-lecie zespołu Dyżurnet.pl

Z okazji tego jubileuszu życzenia, wspomnienia i słowa uznania w formie nagrań i wideo przesłali liczni współpracownicy i partnerzy Dyżurnet.pl – nagrania można było oglądać w social mediach oraz na stronach internetowych NASK. Opublikowany został również film pokazujący najważniejsze wydarzenia z 15 lat działalności Zespołu oraz zostały opublikowane informacje prasowe licznie cytowane przez media.

29.09. - 02.10.2020 R.

14. Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w internecie"

Konferencja poświęcona jest szerokiemu spektrum zagadnień związanych z bezpieczeństwem dzieci i młodzieży w internecie. Adresatami wydarzenia są przedstawiciele sektora edukacyjnego, organizacji pozarządowych, wymiaru sprawiedliwości i organów ścigania oraz dostawców usług i treści internetowych. Podczas konferencji zaprezentowane zostały między innymi wyniki najnowszych badań poświęconych bezpieczeństwu online, a także najnowsze trendy i wyzwania z zakresu bezpieczeństwa internetowego.

11.12.2020 R.

Digital Youth Forum

Digital Youth Forum to wydarzenie organizowane dla uczniów klas 7-8 szkół podstawowych i klas 1-3 szkół ponadpodstawowych. Poświęcone jest edukacji w zakresie bezpiecznego, kreatywnego i pozytywnego korzystania z internetu i nowych technologii.

GRUDZIEŃ 2020 R.

Kampania self-generated sexual content

Kampania porusza problem wytwarzania intymnych obrazów lub filmów przez osoby małoletnie intencjonalnie angażujące się w erotyczną lub seksualną aktywność oraz prezentowania takich treści w internecie, rozsyłania ich do osób bliskich oraz nieznajomych (tzw. *self-generated sexual content*).

W 2020 R. PRZEDSTAWICIELE DYŻURNET.PL DZIELILI SIĘ SWOIMI DOŚWIADCZENIAMI I WIEDZĄ PODCZAS WYDARZEŃ:

Luty

24.02.2020 r.
Warsztaty dla dzieci
Szkoła Podstawowa nr 2 w Łomiankach

Marzec

04.03.2020 r.
Komitet Konsultacyjny

05.03.2020 r.
Webinar: Jak reagować na zagrożenia w internecie, aby był przyjaznym miejscem?

05.03.2020 r.
Jak przeciwdziałać ryzykownym zachowaniom seksualnym w Internecie

Kwiecień

01.04.2020 r.
XI Dni Kryminalistyki
„Materiały owiane tajemnicą - treści przedstawiające seksualne wykorzystywanie dzieci"

03.04.2020 r.
Insafe Training meeting

Maj

12 i 14.05.2020 r.
Webinar Dyżurnet.pl - „Child grooming, sexting i sextortion. Niebezpieczne kontakty w internecie."
Webinar dla rodziców

Czerwiec

17.06.2020 r.
Webinar z cyklu „Bezpiecznie i kreatywnie w internecie, czyli jak..."

23.06.2020 r.
Czy to tylko trolling? – rajdy podczas zajęć online

Sierpień

04.08.2020 r.
Podcast - Rozmowy internetowe „O zdjęciach dzieci"

25.08.2020 r.
Akademia Cyfrowego Rodzica - „Ryzykowne zachowania dzieci w sieci - sexting"

Wrzesień

08.09.2020 r.
Seminarium Równowaga online i offline - wyzwania dla rodziców i szkoły

Październik

29.10.2020 r.
Ogólnopolska Konferencja Naukowa „Przemoc w rodzinie w ujęciu interdyscyplinarnym"

02.10.2020 r.
Warsztaty podczas konferencji międzynarodowej: Aplikacje mobilne - bezpieczny czy niebezpieczny plac zabaw?

Listopad

16.11.2020 r.
Podcast - Bądź z innej bajki „child grooming"

17.11.2020 r.
Konferencja lokalna „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online"

19.11.2020 r.
Sexting - w pandemii stajemy się mniej czujni

25.11.2020 r.
Seminarium - „Wrażliwość użytkowników na szkodliwe treści"

Grudzień

01.12.2020 r.
Szkodliwe treści w internecie - rozpoznawanie i przeciwdziałanie

16.12.2020 r.
Bezpieczeństwo w internecie – wyzwania wobec szkoły i zdalnego nauczania.
Bezpieczeństwo w internecie – wyzwania świata wobec ucznia

KALENDARZ WYDARZEŃ UNIJNYCH W ROKU 2020

Rok 2020 obfitował w wydarzenia istotne dla zwalczania seksualnego wykorzystywania dzieci, dlatego poświęcamy temu zagadnieniu miejsce w naszym raporcie.

Ważne daty

24.07.2020 R.

Ogłoszenie strategii unijnej dotyczącej bardziej efektywnej walki z seksualnym wykorzystywaniem dzieci. Strategia zakłada działania w dwóch obszarach i opiera się na ośmiu priorytetach:

Obszar I Implementacja i rozwijanie właściwych ram prawnych dla ochrony dziecka

1. Zapewnienie kompletnej implementacji Dyrektywy 2011/93/EU
2. Zapewnienie, że legislacja unijna umożliwia efektywną odpowiedź na problem seksualnego wykorzystywania dzieci
3. Identyfikacja luk legislacyjnych, *best practices* i priorytetowych przedsięwzięć w tym obszarze

Obszar II Wzmocnienie odpowiedzi organów ścigania oraz ulepszenie współpracy między partnerami

4. Wzmocnienie starań organów ścigania na poziomie krajowym i unijnym
5. Umożliwienie krajom członkowskim lepszej ochrony dzieci poprzez prewencję
6. Możliwość utworzenia europejskiego Centrum Ochrony Dzieci
7. Pobudzenie wysiłków sektora prywatnego w celu zapewnienia należytej ochrony dzieci w jego usługach
8. Poprawa globalnej ochrony dzieci poprzez wielostronną współpracę partnerów

2-3.12.2020 R.

Komisja Europejska rozpoczęła drogę konsultacji (*road map*), aby określić obowiązki odpowiednich dostawców usług internetowych, wymagające od nich wykrywania i raportowania do właściwych instytucji przypadków ujawniania materiałów przedstawiających seksualne wykorzystywanie dzieci. Kolejna runda konsultacyjna została przewidziana na pierwszy kwartał 2021 r.

15.12.2020 R.

Komisja Europejska przedstawiła kompleksowy zestaw przepisów dotyczących wszystkich usług cyfrowych działających w Unii Europejskiej – Kodeks usług cyfrowych (*Digital Services Act*), który określa zasady funkcjonowania wszystkich usług cyfrowych w UE oraz Akt o rynkach cyfrowych (*Digital Markets Act*), który określa zasady funkcjonowania platform internetowych w sektorze cyfrowym.

21.12.2020 R.

To ważna data z uwagi na wejście w życie zapisów *European Electronic Communications Code*, które spowodowały, że pewne internetowe serwisy komunikacyjne, takie jak webmail czy messaging services, zostały objęte *Dyrektywą e-Privacy*. Taka sytuacja wpłynęła na ograniczenie tym serwisom możliwości dobrowolnego wykrywania i raportowania przypadków obecności w ich zasobach materiałów z kategorii seksualnego wykorzystywania dzieci. Komisja Europejska, próbując zapobiec tej sytuacji przygotowała rozwiązanie tymczasowe, pozwalające na ściśle określone odstępstwo od artykułów 5(1) i 6 *Dyrektywy e-Privacy,* pracując jednocześnie nad długofalowym rozwiązaniem legislacyjnym. Nie osiągnięto jednak porozumienia w sprawie tego rozwiązania w ramach procedury Trilog, która miała miejsce 17 grudnia 2020 r.

Zgodnie z danymi udostępnionymi przez amerykańskie centrum National Center for Missing and Exploited Children (NCMEC), odnotowało ono 46% spadek w liczbie raportów dotyczących obszaru Unii Europejskiej przekazanych przez sektor prywatny w 3-tygodniowym okresie porównawczym przed i po 21 grudnia 2020 r., czyli datą wejścia w życie zapisów *European Electronic Communication Code*. Uregulowanie tego obszaru będzie jednym z najważniejszych wyzwań w 2021 roku.

KAMPANIA DYŻURNET.PL

W grudniu 2020 r. miało miejsce rozpoczęcie Kampanii Dyżurnet.pl realizowanej w ramach działań **Polskiego Centrum Programu Safer Internet**.

Kampania ma na celu poruszenie problemu *self-generated sexual content* oraz zaznaczenia potrzeby reakcji ze strony użytkowników, gdy są świadkami niepokojącego zachowania online osoby nieletniej. Jak informowaliśmy wcześniej w raporcie (strona 23) w ciągu ostatniego roku nastąpił wzrost liczby zgłoszeń dotyczących wytwarzania intymnych obrazów lub filmów przez osoby małoletnie, intencjonalnie angażujące się w erotyczną lub seksualną aktywność oraz prezentowania takich treści w internecie, rozsyłania ich do osób bliskich oraz nieznajomych (*self-generated sexual content*). Kampania kierowana jest głównie do dorosłych użytkowników serwisów internetowych i portali społecznościowych, zwłaszcza tych, na których można prowadzić transmisję na żywo oraz do administratorów i moderatorów serwisów internetowych. Działania kampanijne mają również na celu uwrażliwienie rodziców i opiekunów w kwestii narastającego problemu wytwarzania przez dzieci i młodzież materiałów o charakterze seksualnym i upubliczniania ich w internecie.

Realizatorem akcji jest **NASK Państwowy Instytut Badawczy** w ramach działań **Polskiego Centrum Programu Safer Internet** (PCPSI). Centrum powołane zostało w 2005 r. i obecnie funkcjonuje w ramach programu Komisji Europejskiej Connecting Europe Facility. Tworzą je **NASK** (koordynator PCPSI) oraz **Fundacja Dajemy Dzieciom Siłę**. Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii (kampanie społeczne, konferencje, szkolenia, publikacja materiałów edukacyjnych). W ramach Centrum udzielana jest pomoc psychologiczna młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z internetu oraz telefonów komórkowych przez dzieci i młodzież (telefony zaufania: 116 111, 800 100 100).

Więcej o kampanii na stronie Safer Internet (**https://www.saferinternet.pl/dyzurnet/kampania.html**).

APLIKACJE MOBILNE

CZY NASZE DZIECI SĄ BEZPIECZNE?

Zespół Dyżurnet.pl przygotował raport podsumowujący kwestie bezpieczeństwa aplikacji, z których najczęściej korzystają dzieci i nastolatki w Polsce. Przeanalizowano przede wszystkim aplikacje społecznościowe oraz najpopularniejsze gry. Badano zarówno wrażenia użytkownika i łatwość dostępu do informacji zamieszczonych w aplikacji, jak i skalę dostępów oprogramowania oraz rodzaj treści i materiałów w nich zawartych.

Przy korzystaniu z nowoczesnych technologii powinniśmy mieć na uwadze ochronę prywatności naszej i dziecka. Zawsze przy instalacji nowej aplikacji należy zweryfikować dostępy, na które wyrażamy zgodę oraz rozważyć ich zasadność – wiele aplikacji korzysta z dostępu do kamery, mikrofonu, geolokalizacji czy plików zapisanych na naszym telefonie, co może stanowić poważne naruszenie naszej prywatności. Powinniśmy również pamiętać o tym, że kiedy wyrażamy zgodę na targetowanie reklam, aplikacja ma dostęp także do czynności, które wykonujemy poza nią, np. do haseł wyszukiwanych w przeglądarce. Większość aplikacji społecznościowych zachęca użytkowników do dzielenia się jak największą ilością danych prywatnych oraz wrażliwych. Warto zwrócić uwagę na to, kto ma dostęp do udostępnianych przez nas materiałów, czy można zmodyfikować zakres widocznych informacji na nasz temat lub zablokować możliwość kontaktu ze strony nieznanych nam osób.

W przypadku aplikacji, z których korzystają dzieci, jeszcze ważniejszą kwestią niż to, co udostępniamy, staje się to, co mogą udostępniać inni. Za każdym razem, kiedy mamy do czynienia z serwisem, w którym każdy użytkownik może udostępniać własne treści, istnieje ryzyko kontaktu z materiałami drastycznymi, pornograficznymi czy prezentującymi zachowania niebezpieczne. Kontakt z zawartością wielu aplikacji powoduje również, że coraz więcej młodych ludzi ma do czynienia z cyberprzemocą, problemy z uzależnieniami behawioralnymi czy uwarunkowaniem poczucia własnej wartości od opinii innych. W przypadku aplikacji, z których korzystają nasze dzieci powinniśmy zwrócić szczególną uwagę na możliwość kontaktu z nieznajomymi oraz obecność linków i reklam powodujących opuszczenie aplikacji i przejście do stron, które mogą zawierać treści nieodpowiednie dla najmłodszych.

Każdego dnia użytkownicy serwisów i aplikacji społecznościowych udostępniają setki tysięcy nowych materiałów, co utrudnia moderację nielegalnych i szkodliwych treści. Zgłoszenia, które otrzymuje Zespół Dyżurnet.pl dotyczą również materiałów udostępnianych w serwisach społecznościowych, dlatego dzieci, jeśli z nich korzystają, powinny to robić z dużą ostrożnością, pod kontrolą rodzica lub opiekuna.

KALENDARZ NA ROK 2021

9 LUTEGO	**Dzień Bezpiecznego Internetu** Obchodzony jest z inicjatywy Komisji Europejskiej od 2004 r. Początkowo wydarzenie to świętowały jedynie państwa europejskie, ale już od lat DBI przekracza granice Europy, angażując kraje z całego świata. Z pełną listą zaangażowanych państw i instytucji oraz podjętymi przez nie działaniami można zapoznać się na stronie **www.saferinternetday.org**.
30 KWIETNIA	**Światowy Dzień Sprzeciwu wobec Bicia Dzieci**
WRZESIEŃ	**Konferencja Międzynarodowa „Bezpieczeństwo dzieci i młodzieży w internecie"**
PAŹDZIERNIK	**Konferencja Dziecko Pokrzywdzone Przestępstwem**
18 PAŹDZIERNIKA	**Europejski Dzień Przeciwko Handlowi Ludźmi**
18 LISTOPADA	**Europejski Dzień Ochrony dzieci przed wykorzystywaniem seksualnym i niegodziwym traktowaniem w celach seksualnych**
19 LISTOPADA	**Międzynarodowy Dzień Zapobiegania Przemocy wobec Dzieci**
20 LISTOPADA	**Światowy Dzień Dziecka**
GRUDZIEŃ	**Digital Youth Forum**

ROZWIĄZANIA TECHNOLOGICZNE

STRONA INTERNETOWA

W kwietniu 2020 r. przekazaliśmy do Państwa użytku nową stronę internetową naszego Zespołu. Poza zmianami graficznymi, uległ zmianie również podział organizacyjny strony. Została ona podzielona na sekcje, a priorytet stanowiło ułatwienie i uproszczenie sposobu przesyłania do nas zgłoszeń dotyczących nielegalnych lub szkodliwych treści.

W nowej odsłonie strony znajdują się aktualności zawierające najświeższe informacje z zakresu naszej działalności, zarówno te dotyczące Polski, jak i świata. Tam też będą poruszane kwestie pojawiających się szkodliwych trendów internetowych mogących stanowić zagrożenie dla użytkowników.

Zmianie uległ również podział tematyczny strony – przygotowana została sekcja dla profesjonalistów, dla rodziców i opiekunów oraz dla pozostałych użytkowników internetu. Każda z sekcji poświęcona jest tematom najbardziej interesującym i najbliższym danemu typowi odbiorcy. Przeznaczono również specjalną przestrzeń na publikacje, która zawiera wszelkie nasze wydawnictwa. Polecamy zwrócić uwagę na słownik pojęć, w którym znajdą Państwo wyjaśnienia pojęć z zakresu cyberbezpieczeństwa oraz niebezpiecznych trendów internetowych. Na nowej stronie znajdą Państwo również odpowiedzi na najczęściej zadawane pytania – w sekcji FAQ.

Tworząc nową stronę naszym celem było, aby służyła ona Państwu jako miejsce, w którym można znaleźć wiedzę na temat treści nielegalnych oraz szkodliwych w internecie i rekomendacje dotyczące tego, jak się przed nimi bronić i jak je rozpoznać. Strona jest również bezpiecznym miejscem, w którym można anonimowo dokonać zgłoszenia treści.

APAKT AUTOMATYCZNE PRZESZUKIWANIE, ANALIZA I KLASYFIKACJA TREŚCI

Praca związana z wykrywaniem i klasyfikacją materiałów przedstawiających seksualne wykorzystywanie małoletnich stanowi ogromne wyzwanie nie tylko ze względu na wyjątkową szkodliwość dla osób mających kontakt z treściami CSAM, lecz także w związku ze stale rosnącą liczbą nowych, nielegalnych treści pojawiających się w cyberprzestrzeni.

System oparty o analizę przeprowadzaną przez ludzi staje się coraz mniej efektywny, dlatego istnieje potrzeba stworzenia narzędzi, które częściowo zautomatyzowałyby pracę nie tylko analityków takich zespołów jak Dyżurnet.pl, ale także policjantów prowadzących dochodzenia w przestępstwach związanych z pedofilią czy pracowników pełniących funkcje administracyjne u dostawców usług cyfrowych.

W przypadku zdjęć i filmów, które zostały wcześniej sklasyfikowane jako materiały CSAM, ich identyfikacja jest możliwa bez udziału człowieka dzięki zastosowaniu technologii PhotoDNA lub metody porównywania hashy, które są „cyfrowym odciskiem palca" plików. Metody te pozwalają na szybkie automatyczne przeszukiwanie dużej ilości materiałów zdjęciowych zgromadzonych na nośnikach cyfrowych, niestety nie sprawdzą się w przypadku nowych, jeszcze niezidentyfikowanych i niesklasyfikowanych zdjęć i filmów wideo.

Rozwój algorytmów sztucznej inteligencji z wykorzystaniem uczenia głębokiego, a w szczególności modeli analizy obrazu i tekstu daje realną możliwość stworzenia efektywnych narzędzi programistycznych znacznie usprawniających i przyspieszających wyszukiwanie, identyfikację oraz klasyfikację nielegalnych treści znajdujących się na nośnikach danych.

NASK PIB wielokrotnie realizował zaawansowane rozwiązania programistyczne w dziedzinie cyberbezpieczeństwa. W 2020 r., przy udziale Politechniki Warszawskiej oraz firmy ENAMOR INTERNATIONAL Sp. z o.o. Zespół Dyżurnet.pl wraz z pracownikami naukowymi Instytutu, rozpoczął prace nad opracowaniem informatycznych narzędzi detekcji i analizy zagrożeń związanych z propagowaniem nielegalnych i wrażliwych treści w cyberprzestrzeni z wykorzystaniem modeli klasyfikacji zbudowanych przy zastosowaniu algorytmów sztucznej inteligencji. Projekt nosi nazwę APAKT (Automatyczne Przeszukiwanie, Analiza i Klasyfikacja Treści) i realizowany jest w ramach programu badawczo-rozwojowego Narodowego Centrum Badań i Rozwoju - CyberSecIdent, ukierunkowanego na podniesienie bezpieczeństwa cyberprzestrzeni RP poprzez zwiększenie dostępności rozwiązań sprzętowych i programistycznych. Efekty prac projektowych spodziewane są w roku 2023.

Celem projektu jest opracowanie metod sztucznej inteligencji przeznaczonych do analizy zagrożeń występujących w cyberprzestrzeni polegających na udostępnianiu treści multimedialnych oraz tekstów przedstawiających seksualne wykorzystywanie dzieci – treści pornograficznych z udziałem dzieci, treści erotycznych z udziałem dzieci, treści pornograficznych z wytworzonym obrazem dziecka oraz stanowiących pornografię z udziałem dorosłych.

Dzięki przyszłemu wdrożeniu efektów projektu APAKT do systemu informatycznego Dyżurnet.pl powstanie narzędzie wspierające pracę Zespołu poprzez automatyczną klasyfikację zgłoszeń. System nie wykluczy zaangażowania ludzi, jednak zdecydowanie przyspieszy proces analizy treści ze względu na określenie prawdopodobieństwa wystąpienia w nich treści CSAM.

Rozwiązanie to będzie mogło zostać zaimplementowane zarówno do celów policyjnej analizy dochodzeniowej, jak i w różnego rodzaju usługach gromadzenia danych udostępnianych przez użytkowników internetu na platformach dostawców usług internetowych.

SYWENTO WSPÓŁPRACA Z PROFESJONALISTAMI

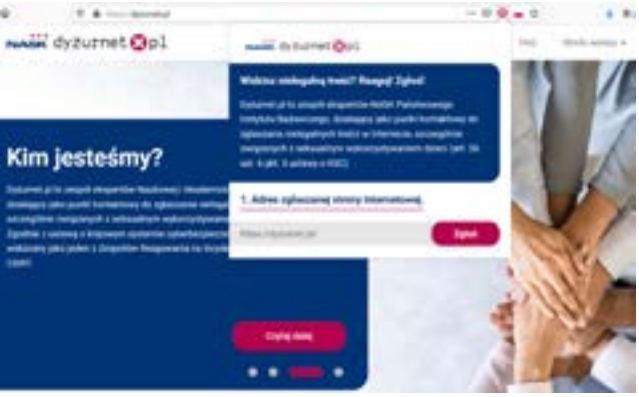
Analitycy Dyżurnet.pl w trakcie swojej pracy gromadzą duże ilości danych, których ewentualne wykorzystanie mogłoby ułatwić pracę innym profesjonalistom zajmującym się materiałami prezentującymi seksualne wykorzystanie nieletnich. W tym celu w roku 2020 powstała aplikacja SYWENTO, narzędzie stworzone 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.

WTYCZKA DO RAPORTOWANIA - SPOSÓB NA STRONY MASKUJĄCE SWOJĄ TREŚĆ

Wiele stron zawierających treści CSAM ukrywa swoją nielegalną zawartość (13% ogólnej liczby CSAM analizowanego przez Dyżurnet.pl w roku 2020). Próba sprawdzenia zawartości takiej strony internetowej często kończy się niepowodzeniem, ponieważ treści maskowane są przed przypadkowymi użytkownikami. Dopiero dostarczenie informacji o właściwym odsyłaczu (tzw. http referrer) „odblokowuje" ukrytą treść. Wiele przesyłanych do Dyżurnet.pl zgłoszeń niestety nie zawiera informacji na temat odsyłacza. Stanowi on zazwyczaj adres url jednej z odwiedzonych wcześniej stron, z której następnie zostało dokonane przekierowanie na stronę zgłaszaną.

Sposobem na strony maskujące swoją treść jest nowy program stworzony w 2020 r. przez programistów NASK – Wtyczka do raportowania. Jest to dodatek do przeglądarki Firefox, którego celem jest ułatwienie zgłaszania nielegalnych treści w internecie oraz zawarcie w zgłoszeniu informacji o referrerze, dzięki której możliwe jest „odblokowanie" ukrytych treści. Wtyczka, jak większość dodatków do przeglądarki Firefox, jest bardzo łatwa w instalacji i jest dostępna przez stronę Mozilli:
https://addons.mozilla.org/pl/firefox/addon/zglos-tresc-do-dyzurnet-pl/



Procedura wysyłania zgłoszeń za pomocą Wtyczki jest prosta i intuicyjna nie wymaga kopiowania adresu zgłaszanej strony internetowej do formularza zgłoszeniowego. Nie wymaga też żadnych dodatkowych kroków oprócz prostego kliknięcia w ikonkę Wtyczki, która po zainstalowaniu wyświetla się w prawym rogu paska adresowego przeglądarki.

Wtyczka to przydatne i proste narzędzie, które służy zarówno zgłaszającemu, jak i analitykom Zespołu Dyżurnet.pl. Narzędzie nie przekazuje danych związanych z prywatnością – nie śledzi użytkownika, nie zapisuje loginów i haseł. Obecnie Wtyczka przewidziana jest do stosowania z przeglądarką Firefox, jednak w planach są również wersje na inne przeglądarki.

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.

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

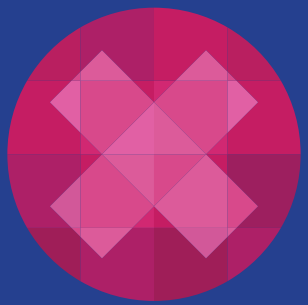
Incydent
Zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl.

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, „sextortion"
Jest to zjawisko, które polega na pozyskaniu przez sprawcę materiałów o charakterze seksualnym, prezentujących tą osobę a następnie zmuszaniu jej do określonego zachowania np. wytworzenia nowych materiałów z tej kategorii lub przekazania pieniędzy w zamian za nieudostępnienie materiałów w sieci.



NASK dyżurnet.pl