

NASK ...
dyżurnet x pl



RAPORT 2018

issn 2084-7785

NASK

Wydawca:

NASK

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

Tekst:

Zespół Dyżurnet.pl

Korekta:

Anna Maj

Opracowanie graficzne:

KLKAM
Piotr Klicki

SPIS TREŚCI

| | |
|---|----|
| O nas | 8 |
| Obsługa zgłoszeń | 10 |
| Statystyki Dyżurnet.pl | 14 |
| Analiza treści CSAM | 22 |
| Trendy i zjawiska | 27 |
| Sexting i sextortion | 28 |
| Treści CSAM jako narzędzie destabilizacji i dyskredytacji | 29 |
| Próby wyłudzeń typu „sextortion scams” | 30 |
| Prywatność dzieci łamana przez rodziców | 31 |
| Patostreamy | 32 |
| Działalność edukacyjno-popularyzatorska | 33 |
| Wydarzenia | 33 |
| O NASK | 38 |

NASK ...
dyżurnet  pl

Działamy na rzecz tworzenia bezpiecznego internetu

REAGUJEMY

na nielegalne i szkodliwe treści internetowe
skierowane przeciwko
bezpieczeństwu dzieci i młodzieży

POPULARYZUJEMY

bezpieczne korzystanie z internetu

Szanowni Państwo,

Z wielu obszarów, na których koncentruje się NASK, jednym z najważniejszych jest troska o bezpieczeństwo internetu. Dlatego tak istotne było wejście w życie ustawy o Krajowym Systemie Cyberbezpieczeństwa w sierpniu 2018 r. Regulacja precyzuje odpowiedzialności i zadania, umożliwiające sprawne działania na rzecz wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP.

Ustawa nałożyła na NASK PIB, rolę CSIRT NASK – jednego z trzech CSIRT poziomu krajowego, który w ramach reagowania na incydenty naruszające cyberbezpieczeństwo jest odpowiedzialny także za przyjmowanie i analizowanie zgłoszeń dotyczących treści pornograficznych z udziałem dzieci, którą to rolę pełni zespół Dyżurnet.pl – już od 2005 r.

Podkreślenie działań reagujących na niepożądane treści typu CSAM w obowiązkach ustawowych stanowi nie tylko uznanie społecznej użyteczności pracy naszych specjalistów czy stworzenie nowych możliwości działania dla zespołu Dyżurnet.pl. Jest to przede wszystkim uznanie walki z rozpowszechnianiem materiałów dokumentujących krzywdę dziecka za sprawę najwyższej wagi.

Miniony rok był dla nas czasem intensywnej współpracy z moderatorami i administratorami serwisów internetowych. Uczestniczyliśmy w spotkaniach, mających na celu wymianę doświadczeń oraz wypracowanie sposobów efektywniejszego reagowania na niepożądane treści i niebezpieczne zachowania użytkowników. To szczególnie ważne w kontekście treści legalnych, ale szkodliwych, których dostępność zależy od decyzji właścicieli serwisów.

Działalność zespołu Dyżurnet.pl jest możliwa dzięki współpracy z różnymi podmiotami, dla których kluczowe jest podnoszenie poziomu bezpieczeństwa w internecie – w tym instytucji publicznych, przedstawicieli edukacji i szkolnictwa wyższego oraz przedsiębiorstw branży teleinformatycznej. Opublikowanie raportu z kolejnego roku pracy Dyżurnet.pl jest najlepszą okazją do podziękowania Państwu za współpracę i za zainteresowanie przeciwdziałaniem krzywdzie najmłodszych.

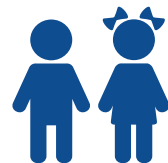
Z poważaniem
Krzysztof Silicki
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

NAJWAŻNIEJSZE DANE Z DZIAŁALNOŚCI DYŻURNET.PL

Jedyny Zespół w Polsce, który **reaguje na treści przedstawiające seksualne wykorzystywanie dzieci**. Został założony w NASK w 2005 roku i od samego początku należy do **międzynarodowego stowarzyszenia INHOPE**, które skupia zespoły reagujące z całego świata.

W sierpniu 2018 roku działania podejmowane przez Zespół wpisano na mocy ustawy do **Krajowego Systemu Cyberbezpieczeństwa**.

NASK
dyżurnet.pl



13 239

przeanalizowanych incydentów,
w tym prawie **2000** dotyczyło
treści prezentujących seksualne
wykorzystywanie dzieci (CSAM)



1 466

spraw zgłoszonych
do INHOPE i Interpolu

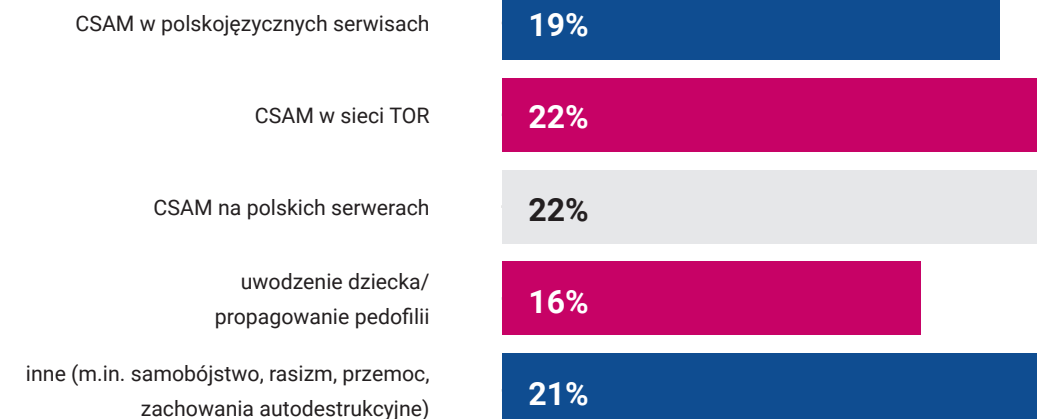
INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE



167

spraw zgłoszonych
do polskiej policji

Incydenty przekazane do policji



50% monitorowanych incydentów CSAM było usuwanych w ciągu 7 dni od zgłoszenia do Dyżurnet.pl,
a kolejne 18 procent w przeciągu drugiego tygodnia

Trendy i zjawiska Sexting/sexortion | sextortion scam | patostreamy | trollparenting



Dyżurnet.pl to jedyny zespół w Polsce, który reaguje na treści przedstawiające seksualne wykorzystywanie dzieci. Został założony w NASK w 2005 roku i od samego początku należy do międzynarodowego stowarzyszenia INHOPE, które skupia podobne zespoły reagujące z całego świata. Zespół, oprócz działań operacyjnych, które są związane z analizą treści, podejmuje inicjatywy podnoszące poziom świadomości o zagrożeniach internetowych oraz bezpieczeństwie w sieci.

W sierpniu 2018 roku działania podejmowane przez Zespół wpisano na mocy ustawy do **Krajowego Systemu Cyberbezpieczeństwa** (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560).

Od początku swojej działalności Dyżurnet.pl realizuje strategię Komisji Europejskiej *Better Internet for Children* współtworząc **Polskie Centrum Programu Safer Internet** (PCPSI).

Strategia wdrożona w większości krajów europejskich (www.betterinternetforkids.eu) ma na celu promowanie bezpiecznego korzystania z internetu i nowych technologii oraz wsparcie reagowania w przypadku zagrożeń sieciowych dotyczących najmłodszych.

W Polsce strategia finansowana w ramach *Connecting Europe Facility* jest realizowana przez NASK (który jest koordynatorem PCPSI) oraz Fundację Dajemy Dzieciom Siłę.

W ramach programu realizowane są projekty:

Saferinternet.pl – zwiększający poziom świadomości społecznej na temat zagrożeń, poprzez działania informacyjne i edukacyjne przeznaczone dla dzieci i młodzieży, a także skierowane do specjalistów m.in. nauczycieli, policjantów jak również rodziców i opiekunów;

116 111 – telefon zaufania dla dzieci i młodzieży oraz **800 100 100**, telefon dla rodziców i nauczycieli, dzięki którym można uzyskać pomoc w sprawach bezpieczeństwa online;

Dyżurnet.pl – punkt kontaktowy do zgłaszania informacji o treściach nielegalnych i szkodliwych publikowanych w internecie.

Kompleksowe działania podejmowane przez PCPSI bazują na wieloletnim doświadczeniu, prowadzonych badaniach oraz interwencjach. Jest to szczególnie ważne w ciągle rozwijającym się środowisku internetowym. Przy Polskim Centrum Programu Safer Internet działa **Komitet Konsultacyjny**, w skład którego wchodzi przedstawiciele ministerstw, policji, środowiska naukowego i biznesowego. Celem Komitetu jest wspieranie inicjatyw prowadzonych przez Centrum.

Skuteczne i szybkie reagowanie na nielegalne treści związane z seksualnym wykorzystywaniem dzieci jest możliwe dzięki współpracy z polskimi organami ścigania oraz innymi zespołami reagującymi zrzeszonymi w **Stowarzyszeniu INHOPE**. Blisko 50 organizacji z całego świata, dzięki zachowaniu najwyższych standardów bezpieczeństwa oraz działaniu według wspólnych wytycznych, tworzy sieć zaufanych podmiotów. Każdy z nich blisko współpracuje z przedstawicielami krajowych organów ścigania, wspierając przy tym środowisko edukacyjne i biznesowe.

W 2018 r. Dyżurnet.pl pomyślnie przeszedł audyt *Quality Assurance Programme*, potwierdzający spełnienie standardów wymaganych przez INHOPE.

www.saferinternet.pl

www.116111.pl

www.dyzurnet.pl

www.inhope.org

Zespół Dyżurnet.pl podejmuje również działania wobec treści internetowych, które zawierają tzw. „twardą pornografię” oraz treści ksenofobiczne i rasistowskie.

- **jeśli materiał jest nielegalny i znajduje się na polskich serwerach** – informacja przekazywana jest do Komendy Głównej Policji;
- **jeśli zgłoszony materiał jest legalny, ale narusza regulamin danego serwisu lub materiał jest szkodliwy i nie powinien znajdować się w szerokim dostępie** – specjaliści kontaktują się z administratorami lub moderatorami serwisu z prośbą o przeniesienie treści czy założenie odpowiedniego ostrzeżenia.

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



INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

Stowarzyszenie INHOPE to sieć zaufanych zespołów reagujących. Co roku przyjmuje nowych członków, poszerzając tym samym zasięg swojego wpływu. Celem Stowarzyszenia jest eliminacja materiałów przedstawiających seksualne wykorzystywanie dzieci oraz wspieranie tworzenia krajowych procedur służących jak najszybszemu usuwaniu nielegalnych treści. 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 Task Force, European Financial Coalition, INSAFE, ECPAT oraz globalne firmy sektora informatycznego. Działalność Stowarzyszenia jest współfinansowana przez Komisję Europejską.

www.inhope.org

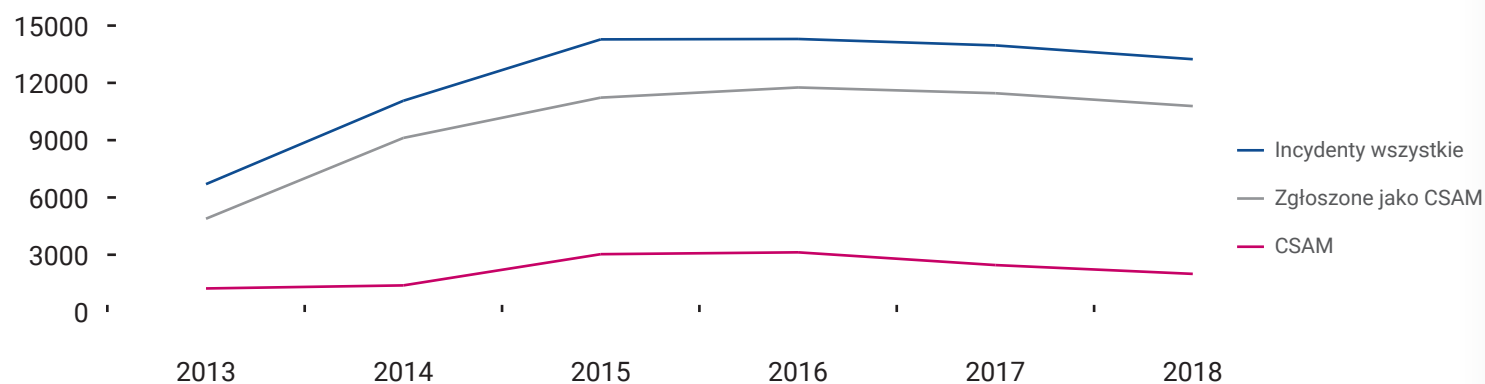
Podstawowym zadaniem zespołu Dyżurnet.pl jest analiza i reagowanie na zgłoszenia dotyczące potencjalnie nielegalnych treści w internecie, z których najważniejszymi są treści przedstawiające seksualne wykorzystywanie dzieci.

Taki zakres kompetencji znajduje odzwierciedlenie w zgłoszeniach, które otrzymuje Dyżurnet.pl. W roku 2018 zgłoszenia dotyczące treści potencjalnie przedstawiających seksualne wykorzystywanie dziecka stanowiły **83 procent ogólnej liczby zgłoszeń** i proporcja ta od lat utrzymuje się na stałym poziomie.

Zdecydowanie najczęstszym sposobem zgłaszania jest użycie formularza znajdującego się na stronie www.dyzurnet.pl. Ta droga pozwala wysłać zgłoszenie w sposób anonimowy. Aż 96 procent zgłoszeń otrzymanych przez Dyżurnet.pl pochodzi z tego źródła.

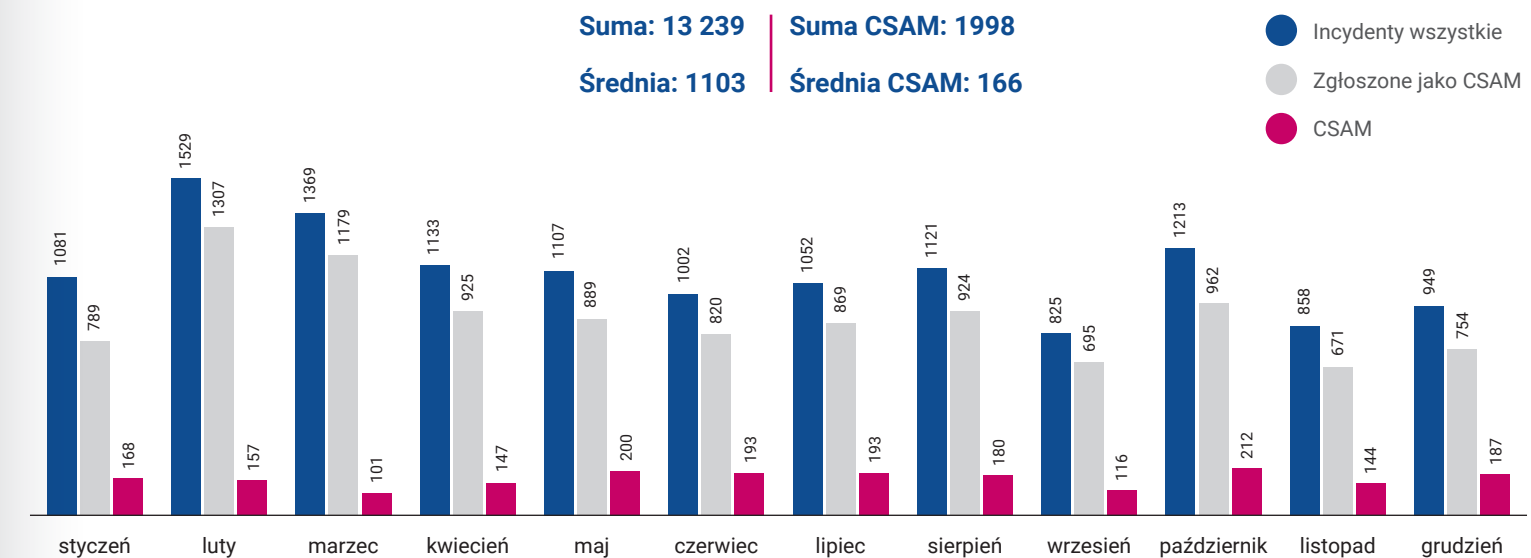
Zgłoszenia, które zostały nadesłane e-mailem (na adresy: dyzurnet@dyzurnet.pl lub info@dyzurnet.pl) stanowiły 4 procent zgłoszeń. To dwukrotnie więcej niż w roku 2017. Ten sposób komunikacji wykorzystywany jest głównie do przekazywania kopii podejrzanej korespondencji e-mail, przesyłania załączników dokumentujących potencjalnie nielegalne zachowania użytkowników, do opisywania bardziej złożonych spraw, jak również do zadawania pytań.

Potencjalnie nielegalne treści zgłaszane są przede wszystkim przez użytkowników internetu, 99 procent zgłoszeń pochodzi właśnie od nich. Pozostały procent stanowią zgłoszenia z innych zespołów reagujących zrzeszonych w INHOPE lub innych instytucji.



Rys. 1 Zgłoszenia i incydenty CSAM w latach 2013-2018

Rys. 1 przedstawia rozkład zgłoszeń i incydentów analizowanych przez Dyżurnet.pl w latach 2013-2018. Widoczne jest, że po gwałtownym wzroście w roku 2014 (wzrost o 65 procent) oraz w roku 2015 (wzrost o 30 procent), w 2016 nastąpiła stabilizacja, a od roku 2017 lekki spadek zauważalny w każdej z kategorii.



Rys. 2 Incydenty w poszczególnych miesiącach roku 2018



Zgłoszenie

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



CSAM

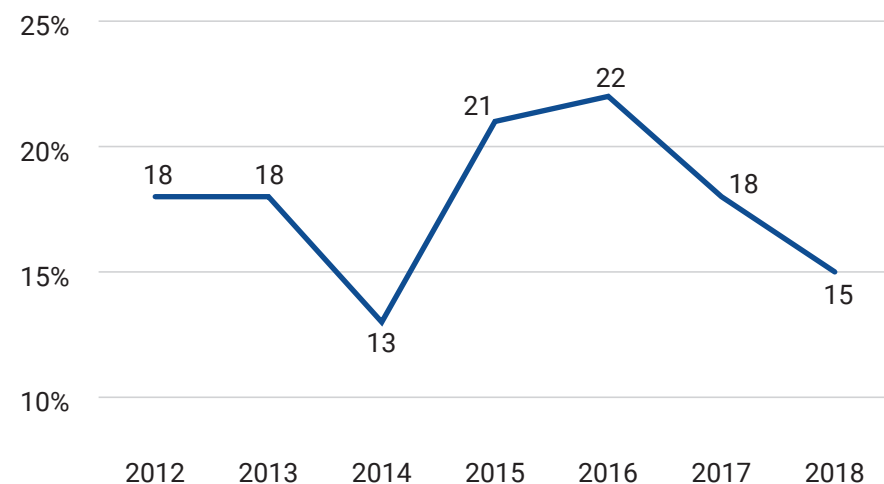
(child sexual abuse materials) Materiały przedstawiające seksualne wykorzystywanie dziecka



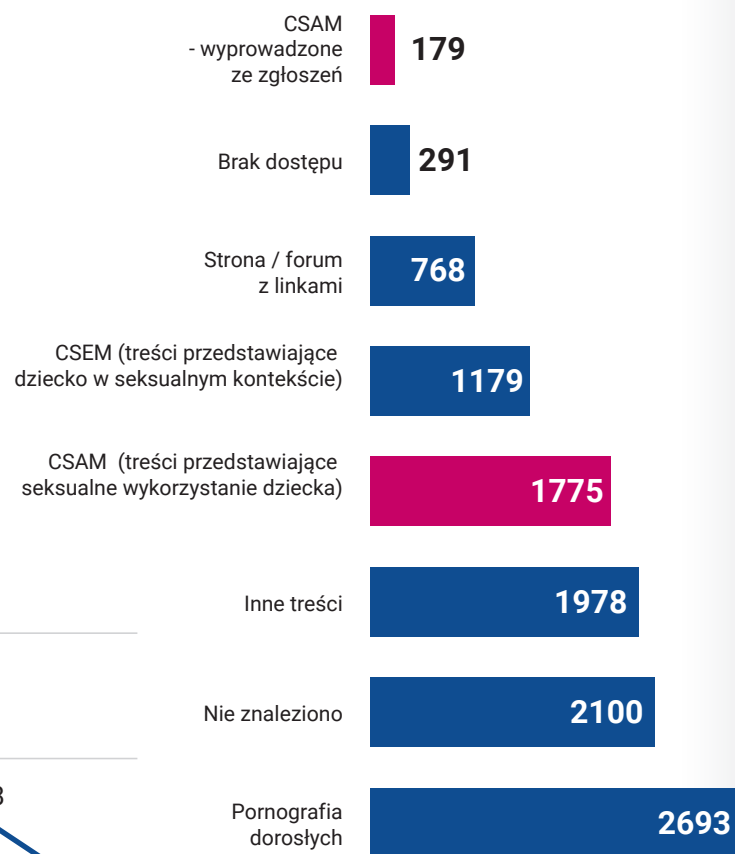
Incydent

Zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl

W roku 2018 eksperci zespołu Dyżurnet.pl przeanalizowali łącznie 13 239 incydentów. Z tej liczby 1 998 zostało zaklasyfikowane jako treści przedstawiające seksualne wykorzystanie dzieci. Rozkład procentowy udziału incydentów CSAM w ogólnej ich liczbie prezentuje Rys. 3. Zauważyć można, że po wzroście w latach 2015-2016, stosunek treści CSAM do ogółu przeanalizowanych incydentów spadł do poziomu 15 procent. Wynika to nie tylko ze zmniejszającej się liczby potwierdzonych przez ekspertów Dyżurnet.pl incydentów CSAM, ale ponad dwukrotnego wzrostu liczebności kategorii „Inne treści” wśród treści zgłoszonych jako potencjalny CSAM w roku 2018.



Rys. 3 Procent CSAM w ogólnej liczbie incydentów w latach 2013-2018



Rys. 4 Klasyfikacja incydentów zgłoszonych jako CSAM w roku 2018

Spośród wszystkich zgłoszeń dotyczących treści potencjalnie przedstawiających seksualne wykorzystanie dziecka, eksperci Dyżurnet.pl potwierdzili faktyczną obecność takich materiałów w 1 775 przypadkach. Dodatkowo w 179 przypadkach wykazano powiązanie z pierwotnymi zgłoszeniami kolejne przedstawienia nadużyć seksualnych wobec dzieci (CSAM – wyprowadzone ze zgłoszeń).

Wszystkie te przypadki, w zależności od lokalizacji serwera (patrz Rys. 11), zgłoszone zostały do Interpolu przez bazę ICCAM, do adekwatnych zespołów reagujących oraz Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Ogólna liczba incydentów CSAM (1 998) jest wyższa niż wykazana na wykresie, gdyż niektóre z nich zostały zgłoszone jako „inne treści”.

1 179 incydentów zaklasyfikowanych zostało jako CSEM (*child sexual exploitation material*) – treści przedstawiające dziecko w seksualnym kontekście. Ta klasyfikacja zastępuje określenia „erotyka dziecięca” oraz „nudyzm dziecięcy”, które nie są adekwatne w definiowaniu zjawiska. Tego typu treści nie są jednak kwalifikowane jako pornograficzne i przez to nie są nielegalne. Temat ten szerzej omówiony został w raporcie Dyżurnet.pl z 2017 roku.



CSAM

Materiał prezentujący seksualne wykorzystanie dziecka (ang. *child sexual abuse material*) - stanowi dowód przestępstwa i sam w sobie jest nielegalny.



CSEM

Materiał prezentujący dziecko w seksualnym kontekście (ang. *child sexual exploitation material*) - stanowi nadużycie wobec dziecka, jednak w większości krajów, w tym w Polsce, jest materiałem legalnym.

Najliczniejszą grupą są incydenty zakwalifikowane jako „pornografia dorosłych”. Stanowiły one 2 693 przypadków. Dotyczą one treści o charakterze pornograficznym z udziałem osób wyglądających na pełnoletnie, wobec których nie było potwierdzonych informacji, że mają mniej niż 18 lat.

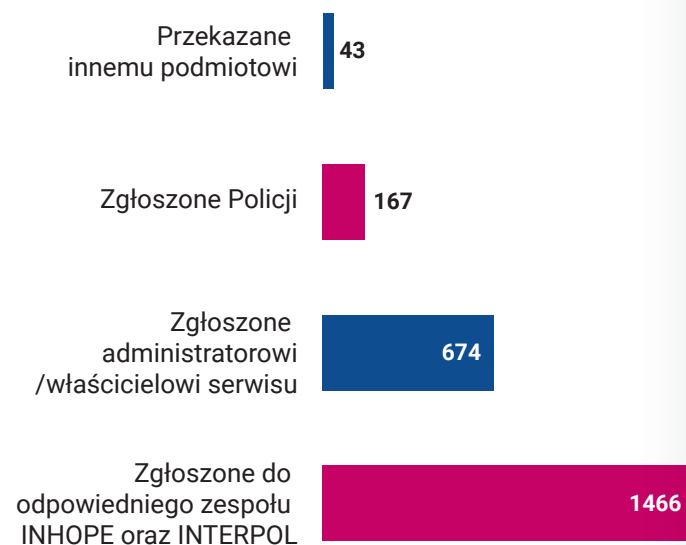
2 100 incydentów zakwalifikowanych zostało jako „nie znalezione” i dotyczyło treści, które były już niedostępne w momencie analizy przez ekspertów Dyżurnet.pl. Pokazuje to, jak istotna jest szybka reakcja hostingodawców, administratorów serwisów oraz innych zespołów reagujących w eliminowaniu takich treści z internetu.

768 przypadków dotyczyło stron lub forów zamieszczających wyłącznie linki z treściami wskazującymi na możliwość dotarcia do treści z małoletnimi. W większości przypadków tego typu strony prowadzą do innych podobnych sobie (tzw. *link farm*). W sytuacji, gdy taka strona faktycznie prowadziła do treści CSAM, tworzony był incydent „CSAM - wyprowadzone ze zgłoszeń”.

W 291 przypadkach eksperci Dyżurnet.pl nie mieli dostępu do zgłoszonej treści. Mogło to być spowodowane:

- brakiem znajomości hasła chroniącego dostęp do zgłoszonego zasobu,
- koniecznością rejestracji konta użytkownika w celu uzyskania dostępu,
- dotyczyło pliku, którego zawartość mogła być weryfikowana wyłącznie po pobraniu, a znajdował się on na zagranicznym serwerze.

Zgodnie z procedurą działania, Dyżurnet.pl nie pobiera takich plików, lecz zawiadamia o tym zespół reagujący właściwy dla lokalizacji serwera.



Rys. 5 Działania podjęte przez Zespół Dyżurnet.pl w roku 2018

Główne metody interwencji wobec zgłoszonych treści pokazuje Rys. 5. W związku z faktem, że zdecydowana większość treści zlokalizowana jest na serwerach poza granicami Polski, najczęściej informacja jest przekazywana do zespołu właściwego dla kraju lokalizacji serwera, zrzeszonego w Stowarzyszeniu INHOPE. Dodatkowo, jeśli informacja dotyczy treści CSAM, przekazywana jest ona poprzez bazę ICCAM do Interpolu.

W roku 2018 eksperci Dyżurnet.pl wprowadzili do ICCAM 1 429 raportów dotyczących nowych adresów URL zawierających nielegalne treści. Znajdowało się tam ogółem 7 681 plików graficznych i nagrań wideo, zaklasyfikowanych jako treść przedstawiająca seksualne wykorzystanie dziecka. W 508 przypadkach adres URL został już wcześniej zgłoszony do bazy ICCAM przez inny zespół reagujący sieci INHOPE.

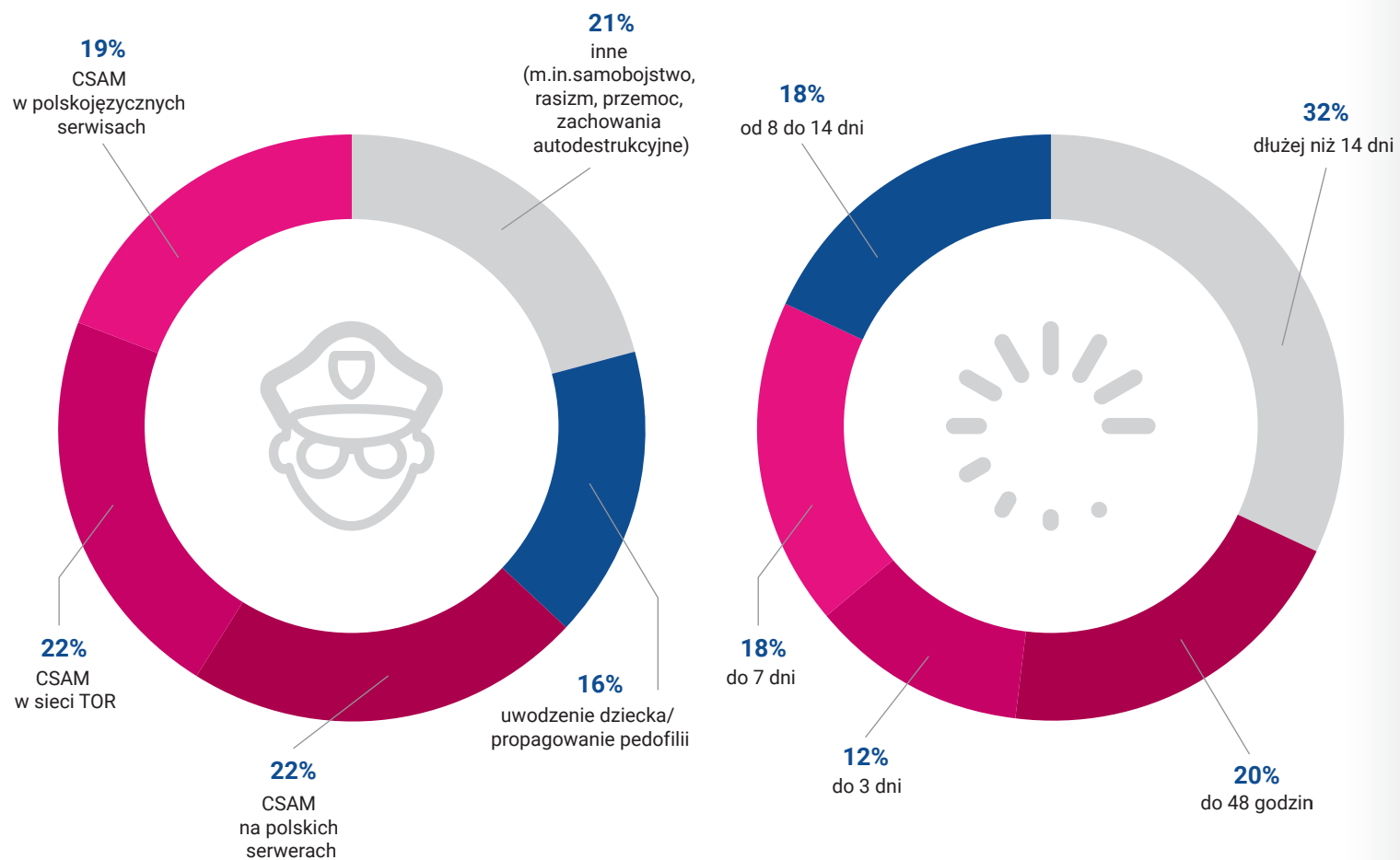
Drugą najczęstszą metodą interwencji, podejmowaną przez ekspertów Dyżurnet.pl, jest bezpośredni kontakt z moderatorami, administratorami lub właścicielami serwisów. Dotyczy to zazwyczaj treści legalnych, ale naruszających regulamin lub zasady społeczności. Taka interwencja podejmowana jest zarówno wobec stron polskich, jak i zagranicznych i w roku 2018 miała miejsce w przypadku 674 incydentów.

Ze względu na zakres wykraczający poza ramy działalności Dyżurnet.pl, 43 sprawy zostały przekazane innym podmiotom - m.in. działającemu w NASK zespołowi CERT Polska czy telefonom interwencyjnym prowadzonym przez Fundację Dajemy Dzieciom Siłę.

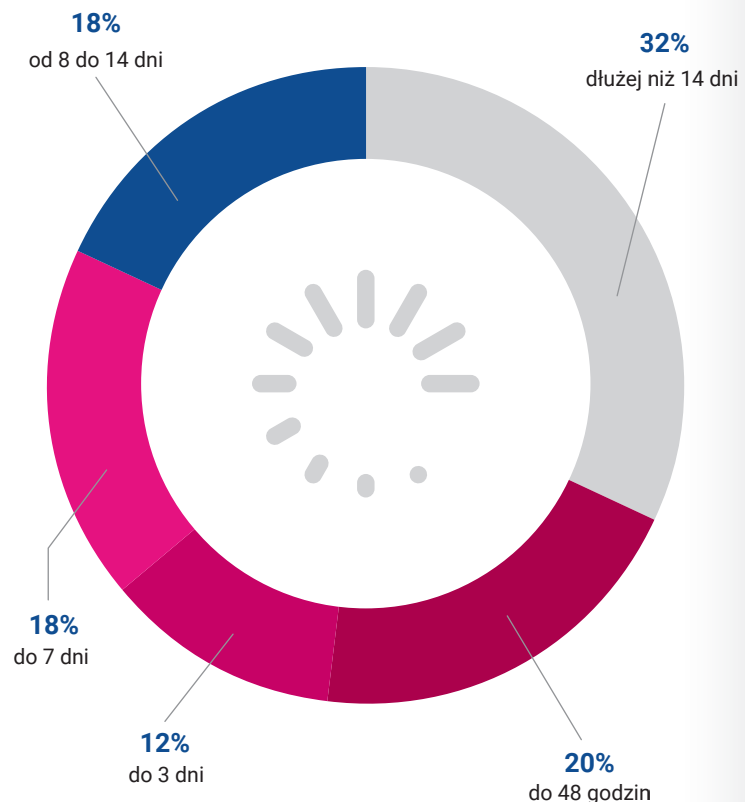
167 incydentów zostało zgłoszonych do Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Dotyczyły one przede wszystkim seksualnych nadużyć wobec dzieci. Zgłoszenia związane z CSAM stanowiły 63 procent przekazanych incydentów (na polskich serwerach - 22 procent, w polskojęzycznych serwisach - 19 procent, w sieci TOR - 22 procent). 16 procent przesłanych spraw dotyczyło uwodzenia dziecka i pochwalania zachowań o charakterze pedofilskim. 21 procent pozostałych spraw zgłoszonych do Policji obejmowało inne treści znajdujące się na serwerach w Polsce (zachowania zagrażające życiu lub zdrowiu, treści rasistowskie, twarda pornografia itp.).

Od 2015 roku 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* - www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification), umożliwiając podjęcie działań w celu identyfikacji zarówno ofiar, jak i sprawcy.

W ostatnich latach szczególną uwagę zwraca się na kwestię analizy materiału i możliwości identyfikacji sprawcy i ofiary. Jednak nadal istotne jest jak najszybsze usunięcie treści CSAM z publicznego dostępu.



Rys. 6 Incydenty przekazane do policji w roku 2018



Rys. 7 Czas dostępności CSAM po zgłoszeniu do Dyżurnet.pl w roku 2018

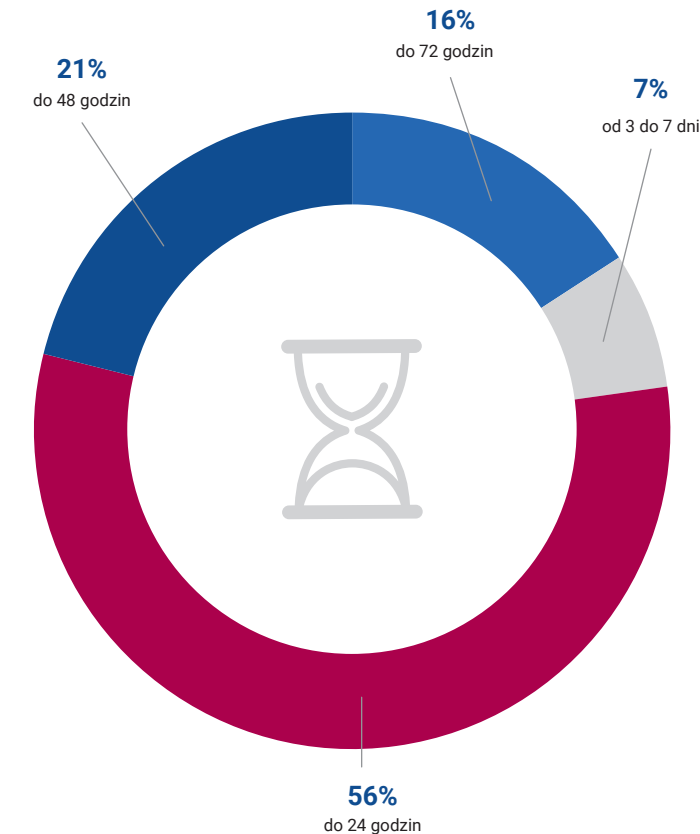
W roku 2018 monitoringowi ze względu na czas dostępności poddane zostało 68 procent ogółu incydentów zakwalifikowanych jako CSAM. Pozostała część znajdowała się w sieci TOR lub została już wcześniej zgłoszona przez inny zespół reagujący, bądź treści nie były nielegalne w kraju serwera i zostały wyłączone z monitoringu (np. treści pornograficzne prezentujące wytworzony wizerunek dziecka).

Z poddanych monitoringowi incydentów **CSAM 50 procent było usuwanych w ciągu 7 dni od zgłoszenia** do Dyżurnet.pl, a kolejne 18 procent w przeciągu drugiego tygodnia. Treści obecne w sieci dłużej niż dwa tygodnie stanowiły 32 procent. Ten zwiększony w stosunku do lat poprzednich odsetek wynika głównie z dużej liczby zgłoszonych stron typu chan (patrz Rys. 10). Te internetowe fora, na których posty zamieszczane są głównie w formie plików graficznych czy zdjęć, nie znikają z publicznego dostępu, mimo ustawicznego publikowania na nich nielegalnych treści.

W roku 2018 Zespół Dyżurnet.pl uzyskał status *trusted flagger* u jednego z większych dostawców usługi tzw. serwera pośredniczącego. Usługa ta umożliwia ukrycie faktycznej lokalizacji serwera wskazując na serwer pośredniczący. Status „zaufanego zgłaszającego” zdecydowanie skrócił czas oczekiwania na uzyskanie informacji na temat faktycznego adresu IP serwera z nielegalnymi treściami.

Wykres czasu dostępności CSAM po zgłoszeniu do Dyżurnet.pl dotyczy wszystkich tego typu treści, niezależnie od lokalizacji serwera. W tym raporcie Dyżurnet.pl po raz pierwszy prezentuje dane odnośnie czasu dostępności treści zlokalizowanych w Polsce, które zostały zgłoszone przez inne zespoły reagujące INHOPE w 2018 roku. Dotyczą one materiałów prezentujących zarówno seksualne wykorzystywanie dzieci (CSAM), jak i materiałów prezentujących dziecko w seksualnym kontekście

(CSEM). W tym drugim przypadku, mimo że treści nie były nielegalne, Dyżurnet.pl zwracał się do administratorów stron o ich usunięcie. Ogółem Dyżurnet.pl otrzymał powiadomienia dotyczące 57 plików. Ponad 75 procent materiałów zostało usuniętych z sieci maksymalnie po 48 godzinach od zgłoszenia do Dyżurnet.pl.



Rys. 8 Czas dostępności treści zgłoszonych do Dyżurnet.pl przez inne zespoły INHOPE w roku 2018

ANALIZA TREŚCI CSAM

Już trzeci rok z rzędu eksperci Dyżurnet.pl przeprowadzili pogłębioną analizę treści CSAM ze względu na ich charakter, lokalizację oraz sposób dystrybucji. Analiza dotyczyła treści znajdujących się w zasobach otwartej sieci internet i nie uwzględnia materiałów z anonimowej sieci TOR.

Przy ocenie treści CSAM zespoły zrzeszone w Stowarzyszeniu INHOPE stosują podstawowe rozróżnienie – treści spełniające kryteria wyznaczone przez INTERPOL (www.interpol.int/Crime-areas/Crimes-against-children/Internet-crimes) i bezwzględnie nielegalne we wszystkich krajach stowarzyszenia określane są jako *baseline*. Dotyczą one dzieci przed rozpoczęciem okresu pokwitania, które poddane zostały najpoważniejszym formom wykorzystania seksualnego (najwyższe stopnie skali COPINE – Por. [Treści pornograficzne z udziałem dzieci. Zarys problematyki, Warszawa 2016](#)).

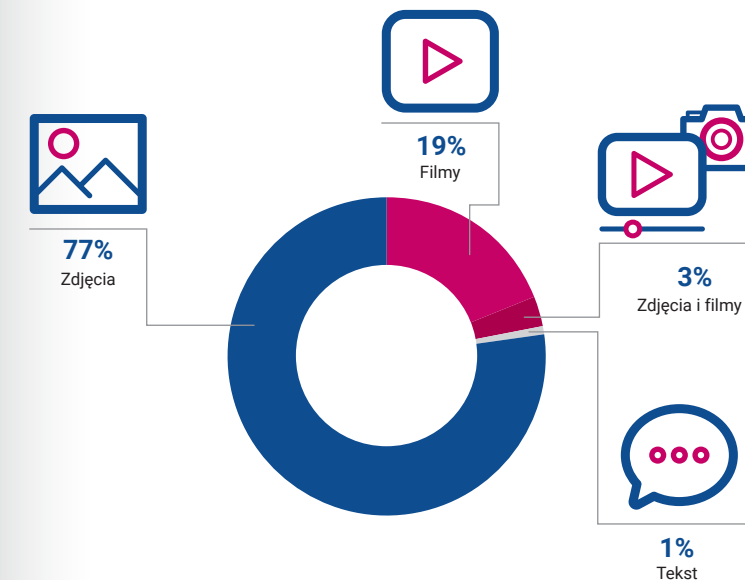
Druga kategoria *national CSAM* uwzględnia regulacje prawne obowiązujące w kraju, gdzie analizowany jest materiał, jednocześnie nie spełniając wytycznych dla treści *baseline*. Przykładowo, w Polsce nielegalne są treści pornograficzne przedstawiające wytworzony lub przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej. Ta kategoria obejmuje też osoby po rozpoczęciu okresu pokwitania, ale prawdopodobnie przed osiągnięciem pełnoletności.

W ocenie ekspertów Dyżurnet.pl rozkład obydwu kategorii uległ zmianie w porównaniu do 2017 roku. O ile w 2017 podział był praktycznie równy, to w 2018 treści zakwalifikowane jako *national CSAM* stanowią 64 procent, a treści *baseline* - 36 procent.

Dane prezentujące strukturę wieku ofiar wykorzystania seksualnego oraz podział na płeć udostępniane są w raporcie Stowarzyszenia INHOPE (www.inhope.org/tns/news-and-events/news/18-06-25/INHOPE_Annual_Report_2017.aspx).

Podział ze względu na rodzaj analizowanej treści prezentuje Rys. 9. Nie uległ on większej zmianie i nadal zdecydowaną większość stanowią zdjęcia (77 procent). Materiały wideo to 19 procent, a obecność zarówno filmów jak i zdjęć na analizowanej stronie stwierdzono w 3 procentach incydentów CSAM. Natomiast 1 procent stanowi tekst opisujący seksualne wykorzystywanie dziecka.

Po raz pierwszy eksperci Dyżurnet.pl przeanalizowali udział treści przedstawiających wytworzony lub przetworzony wizerunek dziecka uczestniczącego w czynności seksualnej w ogólnej liczbie treści CSAM. W roku 2018 były to 44 incydenty czyli 2 procent ogółu CSAM. Prezentowały one głównie animowane komputerowo obrazy (grafika 3D). W Polsce takie treści są nielegalne (art. 202 § 4b. k.k.), niestety inne kraje nie penalizują takiej twórczości i tam też zlokalizowane są serwery hostujące tego typu strony.



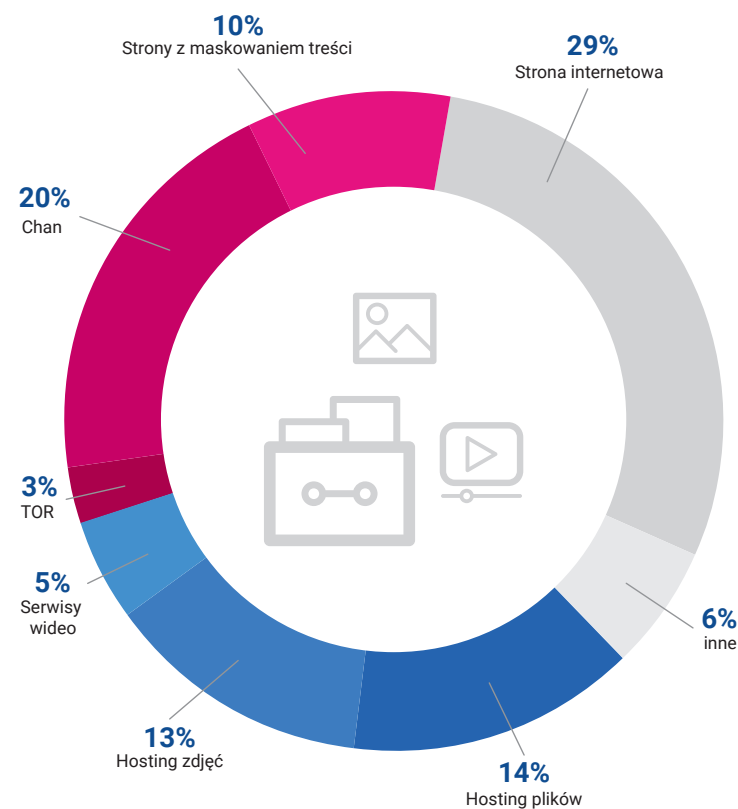
Rys. 9 CSAM analizowany przez Dyżurnet.pl w roku 2018 – rodzaj treści

Sposób dystrybucji w internecie analizowanych treści w roku 2018 przedstawia Rys. 10. Na przestrzeni ostatnich lat zaobserwować można było malejący udział ogólnodostępnych, darmowych serwisów hostingowych w dystrybucji CSAM. W roku 2016 lokalizacja CSAM w tego typu usługach stwierdzona była w 68 procentach przypadków. Rok później w 54 procentach, a w roku 2018 w 32 procentach. Może mieć to związek z coraz efektywniejszym wprowadzaniem przez największych dostawców usług, list opartych o tzw. *hashvalue* czyli identyfikator pliku. Listy zawierające identyfikatory rozpoznanych plików zawierających CSAM są coraz częściej używane do weryfikowania przesyłanych danych i w efekcie, do uniemożliwienia zamieszczenia treści o takim charakterze.

Prawie nie zmienił się natomiast procent stron maskujących nielegalną zawartość. Wyświetlają one treści przedstawiające seksualne wykorzystywanie dzieci tylko przy spełnieniu określonych warunków, np. na przesłaniu nagłówka (tzw. *referer*) z innej, odsyłającej strony. W przypadku bezpośredniego wejścia na taki adres URL wyświetlają się treści legalne, zazwyczaj prezentujące pornografię osób pełnoletnich lub informujące o zawieszeniu działalności witryny. Dopiero po wprowadzeniu odpowiedniego odsyłacza wyświetlają one ukrytą treść. Takie strony w roku 2017 stanowiły 9 procent, w roku 2018 - 10 procent. Warto jednak zwrócić uwagę, że treść przedstawiającą seksualne nadużycia wobec dzieci eksperci stwierdzili w 248 przypadkach spośród całości 506 stron oszacowanych jako maskujące swą zawartość. Zatem w 258 przypadkach nie udało się uzyskać odpowiedniego odsyłacza, „odblokowującego” nielegalną zawartość. Odnotować należy, że z tej części 41 maskowanych stron zgłoszonych zostało do bazy ICCAM przez inne zespoły reagujące.

Obecnie każda strona zgłoszona jako zawierająca treść CSAM jest sprawdzana przez ekspertów Dyżurnet.pl jako potencjalnie służąca do maskowania treści. Dyżurnet.pl zachęca do przekazywania w zgłoszeniu również referera do potencjalnie nielegalnych treści.

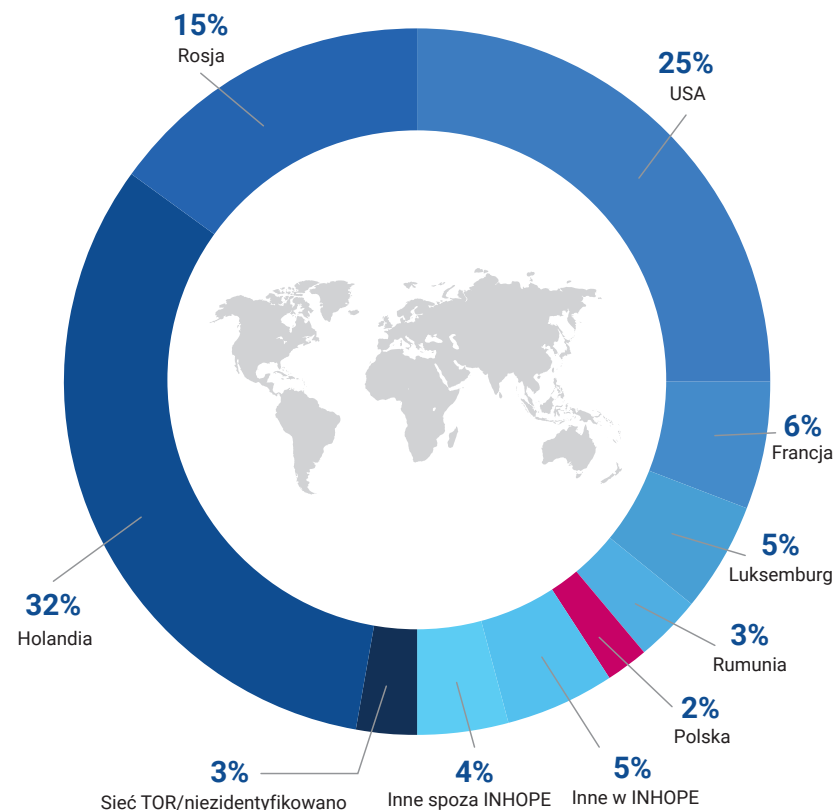
Największy wzrost zgłoszeń treści CSAM, związanych z usługami internetowymi, obserwowany jest od lat w przypadku tzw. chanów, czyli internetowych forów, na których posty zamieszczane są głównie w formie plików graficznych czy zdjęć. W roku 2016 stanowiły one 4 procent, w roku 2017 już 9 procent, a w roku 2018 aż 20 procent. Wzrost liczebności tej grupy niestety związany jest z problemem w usuwaniu treści, mimo ich regularnego zgłaszania do właściwego dla kraju lokalizacji serwera zespołu reagującego, a za jego pośrednictwem, do miejscowej policji. Przyczyny takiego stanu rzeczy nie są znane.



Rys. 10 CSAM analizowany przez Dyżurnet.pl w roku 2018 – lokalizacja w usługach internetowych

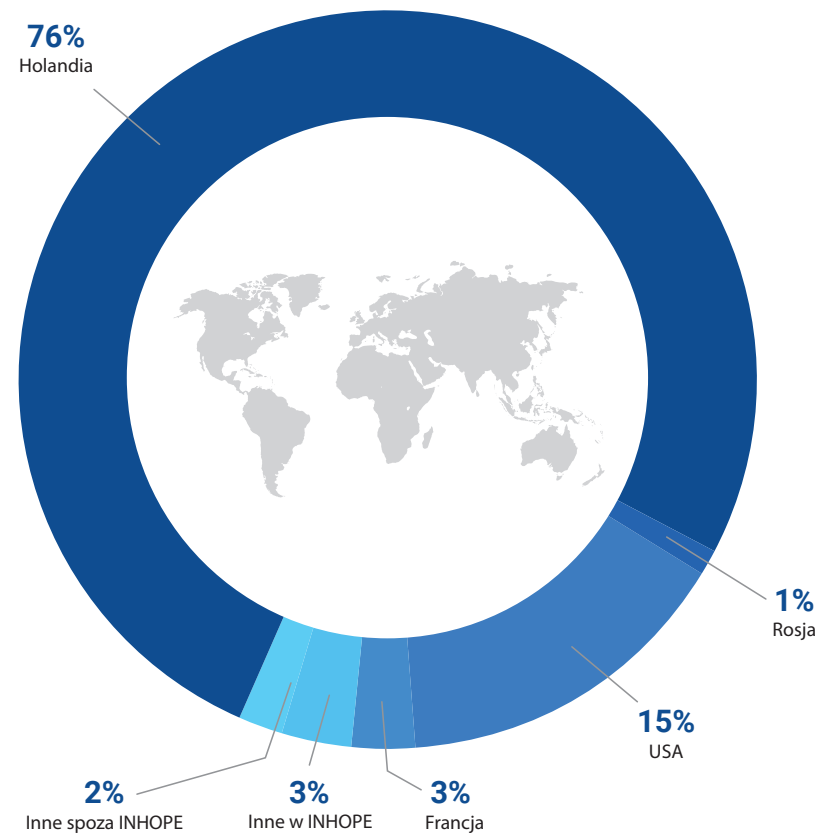
Nieźmiernie istotną kwestią jest właściwa analiza lokalizacji serwerów, na których znajdują się nielegalne treści. Od tego zależy szybkość reakcji danego zespołu. Pomyłki lub opóźnienia w tej kwestii mogą uniemożliwić zarówno analizę treści, jak i danych dotyczących zamieszczających je użytkowników.

Od roku 2017 Dyżurnet.pl prezentuje dwa wykresy, związane z lokalizacją. Pierwszy z nich dotyczy lokalizacji serwerów powiązanych ze zgłoszonym adresem URL. Drugi natomiast dotyczy lokalizacji plików graficznych i wideo. Przykładowo strona znajdująca się na serwerze w Federacji Rosyjskiej może prezentować osadzone potencjalnie nielegalne pliki znajdujące się na serwerach w Holandii i USA. Dodatkowo adres URL może wskazywać na jedną z kilkuset domen najwyższego poziomu. Obecnie jednak kwestia lokalizacji domen jest poza analizą Dyżurnet.pl, gdyż nie wpływa na proces obsługi zgłoszenia.



Rys. 11 CSAM analizowany przez Dyżurnet.pl w roku 2018 – lokalizacja serwerów w odniesieniu do adresów URL

Trzy kraje najliczniej hostujące strony z treściami CSAM od lat pozostają niezmiennie. To Holandia, USA i Rosja. Związane jest to głównie ze względnie łatwym i powszechnym dostępem do internetowej infrastruktury. Zasięg serwerów powiązanych z URL poza zasięgiem INHOPE spadł z 7 procent w roku 2017 do 4 procent w roku 2018. Jednocześnie zwiększył się (z 1 do 3 procent) udział stron, których lokalizacji nie można było ustalić, głównie ze względu na ich obecność w anonimowej sieci TOR (domeny .onion).



Rys. 12 CSAM analizowany przez Dyżurnet.pl w roku 2018 – lokalizacja serwerów w odniesieniu do analizowanych plików foto/wideo

Druga analiza lokalizacji odnosi się do umiejscowienia zdjęć i filmów przedstawiających seksualne wykorzystywanie dzieci. W porównaniu z poprzednim rokiem widać zdecydowany wzrost udziału serwerów zlokalizowanych w Holandii (z 26 do 76 procent). Tylko 2 procent materiałów w tzw. otwartym internecie, znajduje się poza zasięgiem reakcji zespołów zrzeszonych w INHOPE. Zatem nawet jeśli strona znajduje się w państwie, gdzie nie funkcjonuje zespół reagujący, inne zespoły mogą podjąć działania wobec plików zawierających treści CSAM zamieszczone na takiej stronie.



SEXTING I SEXTORTION

Sexting i sextortion to popularne zjawiska, z którymi spotykają się użytkownicy internetu, bez względu na wiek, płeć czy pochodzenie. W ostatnich latach zjawiska te są coraz częstsze oraz przyjmują bardzo różne formy. Jeszcze kilka lat temu zjawisko sextingu dotyczyło przesyłania intymnych materiałów między osobami, które łączył związek lub inna relacja. Obecnie nagie, często intymne i erotyczne materiały przesyłane są do różnych osób i traktowane są jako normalna, codzienna aktywność w sieci.

Przesyłanie i rozpowszechnienie takich materiałów niesie ze sobą wiele niebezpieczeństw i może wywołać negatywne konsekwencje. Przede wszystkim trzeba mieć na uwadze to, że dzieci i młodzież sami stają się twórcami, a przez to ofiarami dystrybucji materiałów przedstawiających seksualne wykorzystanie, które po dostaniu się do sieci, prawdopodobnie nigdy z niej nie znikną. Ponadto w wyniku nagrywania, utrwalania intymnych materiałów dzieci, nastolatki, a także osoby dorosłe mogą zostać ofiarami takich przestępstw jak grooming - uwodzenia czy sextortion - szantażu na tle seksualnym.

Podczas analizy zgłoszeń Zespół Dyżurnet.pl zauważył, że zwiększyła się liczba materiałów, które prawdopodobnie zostały wyprodukowane samodzielnie przez osoby na nich występujące. Mogą to być materiały o charakterze sextingowym, przesłane do kogoś i rozpowszechnione bez zgody i wiedzy ofiary. Ponadto mogą to być treści powstałe w wyniku child grooming, sextortion lub innej aktywności osób trzecich. Niepokojący jest fakt, że na materiałach samodzielnie wytwa-

rzanych przez dzieci i młodzież często występują osoby poniżej okresu pokwitania, czyli poniżej 13 roku życia, a takie treści można napotkać w szerokim dostępie.

Większość materiałów, które trafiła do analizy, to zdjęcia, filmy czy tzw. *screenshotty* (zrzuty ekranu) zrobione podczas pokazu online, a następnie rozpowszechnione i opublikowane na różnego rodzaju stronach internetowych (np. hosting zdjęć). Pokazy erotyczne online przeważnie prowadzone są na platformach streamingowych, a także portalach społecznościowych, gdzie można prowadzić wideokonferencję lub transmisję na żywo. Analizując zgłoszenia eksperci zwrócili uwagę na wpisy i komentarze publikowane pod materiałami, które wskazywały na brak reakcji administratorów serwisu i społeczności strony. W niektórych przypadkach użytkownicy wręcz namawiają nieletnich do podejmowania różnych aktywności, również tych seksualnych.

Eksperti z zespołu Dyżurnet.pl zwracają szczególną uwagę wszystkim użytkownikom internetu, aby podejmowali szybkie i stosowne reakcje wobec niewłaściwych zachowań na platformach.

Osoby niepełnoletnie mogą nie zdawać sobie sprawy z konsekwencji uczestniczenia w pokazach erotycznych online. Dlatego tak ważne jest wprowadzenie restrykcyjnej polityki bezpieczeństwa i szybkie podejmowanie działań przez platformy, a także przez użytkowników, którzy zgłaszając ryzykowane zachowania dzieci mogą ograniczyć negatywne konsekwencje.

TREŚCI CSAM JAKO NARZĘDZIE DESTABILIZACJI I DYSKREDYTACJI

Pod koniec roku 2018 Zespół Dyżurnet.pl otrzymał dużą liczbę zgłoszeń dotyczących publikacji treści CSAM na jednym z popularnych polskich serwisów internetowych. Treści te były zamieszczane z kont zarejestrowanych użytkowników. Zawierały materiały w oczywisty sposób nielegalne, pojawiał się też link prowadzący do pobrania całych archiwów. Posty te zamieszczane były w godzinach nocnych i w związku z tym były usuwane przez moderatorów dopiero po kilku godzinach od zamieszczenia, przy czym pliki graficzne pozostawały dalej na serwerach.

Jak się wkrótce okazało, była to zaplanowana akcja społeczności skupionej wokół jednego z internetowych chanów, która poprzez masowe zamieszczanie nielegalnych treści chciała wzbudzić oburzenie wśród użytkowników. Miało to skutkować wycofaniem się użytkowników oraz reklamodawców z serwisu, wpływając na jego kondycję finansową.

Sprawa ta pokazuje jak istotne są w walce z niepożądanymi treściami zarówno środki doraźne, jak i zapobiegawcze.

Metody doraźne:

- wzmocnienie całodobowej obsady moderatorów, mogących w czasie rzeczywistym skutecznie reagować na zgłoszenia użytkowników,
- zablokowanie ruchu z TOR i podejrzanych adresów IP.

Rozwiązanie pierwsze wiąże się z kosztami; rozwiązanie drugie nie jest doskonałe ze względu na zmienną liczbę węzłów TOR oraz niepełną „blacklistę” adresów IP. W tej sytuacji nie można całkowicie uniemożliwić ruchu z anonimowych źródeł. Warto wprowadzić również narzędzia automatycznego ostrzegania o nietypowym ruchu na serwerze, może być to skuteczne również w przeciwdziałaniu innym zagrożeniom sieciowym.

Bardziej zaawansowaną formą moderacji jest przyznawanie poszczególnym kategoriom użytkowników adekwatnych wag do ich zgłoszeń. W takim przypadku zgłoszenia użytkowników, którzy w przeszłości informowali o wielu trafnych incydentach są rozpatrywane priorytetowo (tzw. *trusted flagger*).

Metody zapobiegawcze:

- uniemożliwienie rejestracji kont z domen oferujących krótkoterminowe adresy e-mail,
- wprowadzenie weryfikacji sms przy rejestracji konta,
- ograniczenie zamieszczania zewnętrznych plików przez nowych (lub nieaktywnych dotąd) użytkowników,
- weryfikacja zamieszczanych plików foto/wideo przez odpowiednie narzędzia (np. Photo DNA) zgodnie z listą tzw. *hashvalue* rozpoznanych już plików zawierających nielegalne treści.

Więcej informacji na temat proaktywnych rozwiązań w walce w CSAM zamieszczonych zostało w Raporcie 2017.

PRÓBY WYŁUDZEŃ TYPU „SEXTORTION SCAMS”

W roku 2018 oba działające w NASK zespoły: CERT Polska oraz Dyżurnet.pl zaobserwowały zwiększoną liczbę zgłoszeń od użytkowników, którzy otrzymali niepokojącą korespondencję meilową. Autorzy korespondencji twierdzili, że poznali hasło stosowane przez użytkownika. W dalszej treści wiadomości informowali, że wskutek oprogramowania malware, zainstalowanego na jednej ze stron z treściami o charakterze pornograficznym, uzyskali dostęp do internetowej kamery, kontaktów serwisów społecznościowych i skrzynki pocztowej użytkownika. Przypadki początkowo dotyczyły korespondencji prowadzonej w języku angielskim, potem wysyłane mejle pisane były poprawną polszczyzną, co nie jest regułą przy tego typu wiadomościach, i dodatkowo uwiarygadniało przestępców.

Autorzy meila stosowali szantaż – wyznaczali krótki termin na wpłatę sumy ok. 1000 USD w formie Bitcoin pod podany adres portfela kryptowaluty. W przypadku braku wpłaty, grozili udostępnieniem materiału zarejestrowanego przez internetową kamerkę w trakcie odwiedzin strony pornograficznej osobom znajdującym się w na liście znajomych oraz w bazie kontaktów ze skrzynki pocztowej.

Próbę szantażu uwiarygadniało podane w korespondencji prawdziwe hasło dostępowe do jednego z popularnych serwisów internetowych, które w przeszłości stosowane było przez użytkownika. Hasła te pochodziły z wcześniejszych wycieków danych, nawet sprzed kilku lat.

Wiadomości tego typu wysłane zostały do tysięcy użytkowników, których hasła zostały wykradzione.

To, czy dla danego konta e-mail hasło zostało wykradzione, można samodzielnie sprawdzić na dedykowanych do tego stronach

W tego typu sytuacjach eksperci Dyżurnet.pl radzą:

- zmienić używane hasło na wrażliwych kontaktach,
- nie odpowiadać na przesłanego meila,
- nie dokonywać płatności,
- przeskanować urządzenie pod kątem szkodliwego oprogramowania,
- zakrywać obiektyw kamery każdorazowo, gdy nie jest w użyciu.

Samo zjawisko tzw. sextortion, czyli realnej groźby udostępnienia zarejestrowanego bez zgody użytkownika materiału o charakterze seksualnym, zostało opisane w rozdziale „Sexting i sextortion”.

Więcej na ten temat: www.dyzurnet.pl/baza-wiedzy/jestes-ofiara-sextortion-otrzymaj-pomoc.html

PRYWATNOŚĆ DZIECI ŁAMANA PRZEZ RODZICÓW

Od początków funkcjonowania portali społecznościowych zaobserwować można zjawisko zamieszczania przez rodziców zdjęć swoich dzieci dokumentujących niemal każdy moment życia. Bywa, że są to zdjęcia z sytuacji intymnych np. kąpiel dziecka lub krępujących np. uwieczniające sytuacje ośmieszające dziecko.

Należy pamiętać, że wrzucając zdjęcie lub film do sieci traci się nad nimi kontrolę i nie ma wpływu na to, co później się z nimi wydarzy, jak wiele razy zostaną skopiowane i do kogo trafią.

Niestety nawet materiały z pozoru wyglądające na niewinne mogą trafić w niepowołane ręce. Jednym z zagrożeń są działania osób o skłonnościach pedofilskich, które często pozyskują materiały z portali społecznościowych zamieszczanych przez niczego nieświadomych rodziców.

Innym zagrożeniem jest ośmieszanie dziecka, czego konsekwencje mogą się pojawić dopiero jak dziecko osiągnie wiek nastoletni, a materiały zamieszczone lata wcześniej przez rodziców mogą się stać narzędziem cyberprzemocy rówieśniczej. Publikowanie przez najbliższych intymnego czy ośmieszającego wizerunku dziecka może w dalszej perspektywie skutkować w jego zachowaniu brakiem poszanowania prywatności oraz szacunku wobec drugiego człowieka.

Przed opublikowaniem zdjęcia czy filmu, opiekunowie powinni zastanowić się nad potencjalnymi konsekwencjami takiej aktywności dla dziecka.

Zespół Dyżurnet.pl zaleca rozważę przy publikacji materiałów na portalach, ponieważ zdjęcie czy film raz wrzucony do sieci może z niej nigdy nie zniknąć. Warto również zastanowić się, czy instytucja, która sprawuje opiekę nad dzieckiem (żłobek, przedszkole, klubik dziecięcy, szkoła) może dysponować wizerunkiem dziecka w portalach społecznościowych i czy opiekunowie świadomie wyrażają na to zgodę.



Trollparenting – („troll” – trollowanie, wyśmiewanie, „parenting” – rodzicielstwo) wyśmiewanie dzieci przez rodziców w internecie. Zamieszczanie w sieci materiałów ośmieszających dzieci.



Sharenting – (połączeni słów „share” – udostępnianie, dzielenie się oraz „parenting” – rodzicielstwo) zamieszczanie przez rodziców zdjęć/filmów z wydarzeń z życia dzieci bez zgody dzieci.

PATOSTREAMY

Patostreamy to internetowe relacje na żywo (*streaming live*) prezentujące zachowania określone i postrzegane jako patologiczne. Są to, np. relacje z libacji alkoholowych, materiały prezentujące agresywne zachowania, wyzwiska, bójki. Autorzy i często również główni aktorzy relacji za zamieszczony materiał uzyskiwali od oglądających indywidualne wpłaty. Skutkowało to przekraczaniem przez nich kolejnych granic, głównie w celu zwiększenia zysków materialnych. Patostreamerzy bardzo szybko zorientowali się, że im bardziej wulgarne i szokujące były nagrania, tym więcej było oglądających i subskrybujących kanał.

Patostreamy są szczególnie szkodliwe dla dzieci i młodzieży, ponieważ promują niebezpieczne zachowania, a treści w nich zawarte mogą być nielegalne oraz mogą nawoływać do popełnienia przestępstwa. Natomiast dzieci często nie zdają sobie sprawy ze szkodliwości powielania takich zachowań. Naśladują swoich „idoli” w nadziei na uzyskanie takiej samej popularności w mediach społecznościowych, nie zdając sobie sprawy z konsekwencji. Niestety, przez dużą oglądalność i rosnącą liczbę subskrypcji, patostreamerzy byli promowani przez serwisy jako filmy proponowane do obejrzenia. Usuwani ze znanych serwisów wideo, szukali innych miejsc, gdzie mogliby bezkarnie zamieszczać swoje relacje. Wskutek tego, przenosili się do serwisów erotycznych i pornograficznych. Było to kolejne zagrożenie dla młodych użytkowników internetu, którzy podążając za swoimi idolami trafiali na platformy publikujące treści nieodpowiednie dla ich wieku.

W walce z patostreamami bardzo ważna jest szybka i zdecydowana reakcja administratorów serwisów. Pomocne może okazać się wprowadzenie ograniczenia wieku dla oglądających oraz wprowadzenie polityki braku akceptacji dla promowania zachowań szkodliwych i niebezpiecznych.

Zespół Dyżurnet.pl przypomina o zachowaniu rozwagi w internecie. Bardzo ważne jest, aby opiekunowie towarzyszyli nastolatkom, a szczególnie młodszym dzieciom w ich internetowych wyborach.

4

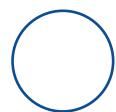
DZIAŁALNOŚĆ EDUKACYJNO-POPULARYZATORSKA



WYDARZENIA

Zespół Dyżurnet.pl organizuje i uczestniczy w wydarzeniach związanych z popularyzacją bezpiecznego korzystania z internetu skierowanych do różnych grup odbiorców.

Przedstawiciel Dyżurnet.pl wziął udział w szkoleniu dedykowanemu pracownikom analizującym materiały przedstawiające seksualne wykorzystywanie dzieci. Cykliczne szkolenie jest organizowane przez **Interpol** i odbyło się w jego siedzibie w Lyonie **19 lutego**.



Najważniejszym świętem promującym internet bez zagrożeń jest **Dzień Bezpiecznego Internetu**, którego główne obchody w 2018 r. odbyły się **6 lutego**. Hasło Tworzymy Kulturę Szacunku w Sieci miało zwrócić uwagę na to, że wszyscy tworzymy internet i wpływamy na poziom jego bezpieczeństwa.

W dniu **22 marca** w Faktycznym Domu Kultury w Warszawie odbyło się **Seminarium eksperckie Safer Internet YouTube – Szanse i zagrożenia dla dzieci i młodzieży**. Spotkanie było poświęcone zarówno pozytywnym, jak również szkodliwym formom korzystania z serwisów wideo. Seminarium było skierowane do nauczycieli, rodziców i osób zawodowo zajmujących się pracą z młodzieżą.

W ramach programu odbyło się również wiele konferencji lokalnych organizowanych z inicjatywy konsorcjum Programu Safer Internet. Były to między innymi Konferencje Lokalne Safer Internet w Białej Podlaskiej (**18 kwietnia**), we Włocławku (**23 kwietnia**), Kielcach (**20 listopada**).

W dniach **18-19 kwietnia** w Dublinie odbyło się **EMEA Child Safety**. Spotkanie organizowane przez Google i Facebook jest dedykowane przedstawicielom nauki, działaczom społecznym, politykom. W jego trakcie poruszane są m.in. zagadnienia związane z bezpieczeństwem użytkowników internetu, nowymi produktami i usługami.



W dniach **20-22 lutego** w Lyonie odbyło się **Zgromadzenie Generalne INHOPE**. Oprócz bieżących spraw dotyczących działalności Stowarzyszenia odbyły się prelekcje na temat przyszłości urządzeń mobilnych i treści CSAM oraz współpracy Stowarzyszenia INHOPE z operatorami sieci komórkowych w walce z CSAM. Kolejne spotkanie Stowarzyszenia INHOPE miało miejsce w dniach **10-15 czerwca** w Heraklionie. Spotkanie dotyczyło zagadnień z bieżącej działalności Stowarzyszenia, a członkowie tym razem mieli okazję wziąć udział w prelekcjach m.in. na temat Darknetu. Do członków Stowarzyszenia zostały przyjęte organizacje Alia2 z Hiszpanii, CNTI z Cypru oraz Net Patrola z Serbii. Podczas konferencji zorganizowane zostało szkolenie dla analityków treści, w którym wziął udział przedstawiciel zespołu Dyżurnet.pl.

Stowarzyszenie INHOPE kładzie bardzo duży nacisk na jakość i efektywność działań zespołów hotline. W związku z tym prowadzi program okresowego audytu działalności jego członków. W **lipcu 2018** roku Zespół Dyżurnet.pl pomyślnie przeszedł audyt przeprowadzony przez niezależnego, zewnętrznego audytora.

Przynależność do organizacji INHOPE stwarza możliwość bliskiej współpracy z zespołami reagującymi, działającymi w innych krajach. We **wrześniu 2018** roku Zespół Dyżurnet.pl podczas wizyty studyjnej dzielił się swoimi doświadczeniami z przedstawicielami hotline z Litwy Svarus Internetas.



W dniach **18-19 września** w Warszawie odbyła się **12. Międzynarodowa Konferencja Bezpieczeństwo dzieci i młodzieży w internecie**. Coroczne wydarzenie jest organizowane przy współpracy PCPSI z niemieckim konsorcjum realizującym projekt klikSAFE, w ramach programu Komisji Europejskiej Connecting Europe Facility. Adresatami wydarzenia byli przedstawiciele sektora edukacyjnego, organizacji pozarządowych, wymiaru sprawiedliwości i organów ścigania oraz dostawcy usług i treści internetowych. Podczas konferencji zaprezentowane zostały między innymi wyniki najnowszych badań poświęconych bezpieczeństwu online, wyzwania w zakresie bezpieczeństwa internetowego, a także nowe pomysły w zakresie dotyczące zastosowania nowych mediów i nowych technologii w procesie edukacji dzieci i młodzieży.

Eksperti Zespołu Dyżurnet.pl dzielą się swoją wiedzą podczas prelekcji i warsztatów organizowanych przez inne instytucje, którym bliski jest temat bezpieczeństwa dzieci i młodzieży w internecie. W 2018 roku brali udział m.in. w konferencjach organizowanych przez KWP w Katowicach: **Profilaktyka w obszarze cyberprzestrzeni (27 lutego)**, Wodzisław Śląski), oraz **Metody zwalczania oraz możliwości wykrywania przestępstw związanych z Cyberprzestępczością (27 września)**. Przedstawiciele Dyżurnet.pl brali również udział w konferencji szkoleniowej programu **Zagrożenia w sieci- profilaktyka, reagowanie** w ramach projektu organizowanego przez Wydział Prewencji KWP w Krakowie, Departament Zdrowia i Polityki Społecznej Urzędu Marszałkowskiego Województwa Małopolskiego oraz NASK (**1-2 października**), konferencji szkoleniowej **W świecie cyberprzestrzeni o zagrożeniach uświadamiamy, omamić nie pozwalamy** organizowanej dla funkcjonariuszy ds. profilaktyki społecznej z garnizonu mazowieckiego oraz pracowników Mazowieckiego Samorządowego Centrum Doskonalenia Nauczycieli (**13 grudnia**, Podgórze).

Wrzesień

Październik

Listopad

Grudzień

W ramach programu **CYBERPOL** NASK wraz z Prokuraturą Krajową zorganizował szkolenie dla prokuratorów oraz przedstawicieli innych służb dotyczące sieci DarkNet (**7 listopada**), podczas którego uczestnicy poznali zasady funkcjonowania tego obszaru internetu. Omawiane były również rodzaje przestępstw ze szczególnym uwzględnieniem dystrybucji treści przedstawiających seksualne wykorzystywanie dzieci.

W 2018 roku przedstawiciele Dyżurnet.pl dzielili się swoimi doświadczeniami i wiedzą podczas wydarzeń:

- Spotkania ze studentami Wydziału Psychologii, Uniwersytet Warszawski, 15 stycznia,
- warsztatów dla II klas Gimnazjum, Józefosław 19 lutego,
- spotkania z rodzicami w Gimnazjum w Jedlińsku, 12 marca,
- warsztaty dla uczniów Gimnazjum w Strykowicach Górnych, 19 marca,
- spotkania ze studentami Kół Naukowych, Uniwersytet Warszawski 14 marca oraz 25 kwietnia,
- warsztatów dla szkoły podstawowej nr 77, Warszawa, 27 kwietnia.

Warsztaty dla specjalistów

W 2018 roku w ramach działającego w NASK **Programu Partnerstwo dla Cyberbezpieczeństwa** eksperci zespołu przeprowadzili szereg warsztatów dla osób zajmujących się moderacją w portalach internetowych. Tematyka spotkań skupiała się wokół specyfiki korzystania z internetu przez dzieci i młodzież, zjawisk zagrażających bezpieczeństwu, sposobów reakcji wobec nielegalnych i szkodliwych treści.

Dyżurnet.pl przeprowadził również warsztaty dla pracowników banku NatWest w Warszawie, wspierając specjalistów zajmujących się bezpieczeństwem, którzy w ramach wolontariatu pracowniczego prowadzą zajęcia dla dzieci i młodzieży.



Cyberbezpieczeństwo i ochrona użytkowników

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 Centrum Cyberbezpieczeństwa, w którego skład wchodzi m.in. zespół CERT Polska (www.cert.pl) oraz zespół Dyżurnet.pl (www.dyzurnet.pl). Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK-PIB został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT, który koordynuje incydenty zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych i samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy.

Nauka i innowacje

NASK prowadzi działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Główny nurt badań wyznacza cyberbezpieczeństwo, 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. NASK prowadzi także rejestr nazw w domenie .pl (www.dns.pl).

Współpraca i zaufanie

NASK jest przykładem skutecznego połączenia zarówno badań naukowych, rynkowego sukcesu, jak i współpracy z administra-

cją publiczną. Instytut jest partnerem i wykonawcą projektów dla instytucji z sektora usług strategicznych, w tym między innymi systemu wczesnego wykrywania incydentów zagrażających cyberbezpieczeństwu dla administracji publicznej (ARAKIS GOV). We współpracy z Ministerstwem Cyfryzacji oraz Centralnym Ośrodkiem Informatyki NASK realizuje m.in. program mDokumenty i mLegitymacje.

Edukacja społeczna i rozwój społeczeństwa informacyjnego

Ważną rolę pełni działalność edukacyjna i popularyzacja idei społeczeństwa informacyjnego. W Akademii NASK (www.akademia.nask.pl) realizowane są projekty społeczne oraz unikatowe szkolenia dla firm i instytucji, ze szczególnym uwzględnieniem tematyki bezpieczeństwa ICT. Od lat realizowany jest program Komisji Europejskiej Safer Internet promujący bezpieczne korzystanie z nowych technologii i internetu wśród dzieci i młodzieży (www.saferinternet.pl). NASK prowadzi również portal e-learningowy IT Szkoła (www.it-szkola.edu.pl), skierowany do szkół ponadpodstawowych oraz osób zainteresowanych teorią i zastosowaniem ICT, pomagający w podnoszeniu poziomu kompetencji cyfrowych poprzez wykłady on-line i certyfikowane kursy. W ramach instytutu funkcjonuje Dyżurnet.pl (www.dyzurnet.pl), który przyjmuje zgłoszenia dotyczące nielegalnych treści w internecie, przede wszystkim związanych z materiałami przedstawiającymi seksualne wykorzystywanie dzieci. W 2017 r. instytut został operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE) – programu, którego celem jest podłączenie wszystkich szkół w Polsce do szybkiego i bezpiecznego internetu (www.ose.gov.pl/).

NASK ...
dyżurnet  pl