

[Home](#) / [Veiligheid](#) / Online veiligheid

Online veiligheid

Internetrecherche

914



dossiers

De internetrechercheurs van de cel i2-IRU van de Federale Politie hebben in 2018 steun verleend in 914 dossiers, dat zijn gemiddeld 75 opdrachten per maand.

De meeste steunopdrachten hebben te maken met terrorisme. Zo heeft de cel i2-IRU onder coördinatie van het Federaal Parket meegewerkt met (inter)nationale rekerchediensten aan de inbeslagname van servers gebruikt door de Islamitische Staat.

De cel houdt zich ook bezig met de melding, met het oog op verwijdering, van inhoud die betrekking hebben op propaganda, terrorisme, radicalisme, gewelddadig extremisme en haatdragende taal. In 2018 werden 1621 terroristische inhoud gemeld. 1 193 maakten het voorwerp van een verwijdering uit. Er werden bovendien 129 inhoud in verband met haatdragende taal vermeld, waarvan er 77 konden worden verwijderd. De rest kon niet worden verwijderd door de platforms.

Veel steunaanvragen hadden betrekking op nog een ander fenomeen: seksueel misbruik van minderjarigen. Vorig jaar ontving de cel 494 profielen. Van 163 wordt de identiteit nog onderzocht. Er zijn 191 identificaties verricht, waarbij een proces-verbaal werd opgesteld. Het verschil, 140 profielen, komt overeen met niet-geïdentificeerde of niet-identificeerbare profielen (bv. profielen die niet meer bestaan of afgesloten werden).

Opgemerkt dient te worden dat de meldingen aan de platforms, om de verwijdering van inhoud te vragen, geen gerechtelijke vorderingen zijn. Het staat de platforms dus vrij om de gemelde inhoud al dan niet te verwijderen.

Qua blokkering van websites en/of inhoud ontving de cel i2-IRU 33 aanvragen met betrekking tot 67 adressen. De meeste aanvragen hebben te maken met illegale ticketverkoop op het internet.

Cybercriminaliteit

De Federale Politie speurt in cyberspace naar nieuwe vormen van oplichting. In het kader van preventie worden waarschuwingen uitgestuurd in de media, met name via de uitzending "Surfons tranquille" (RTBF). Deze waarschuwingen trekken veel publieke belangstelling. Zo werd een waarschuwing voor een phishingcampagne tegen een Belgische bank in 24 uur tijd gelezen door 180 125 personen en talloze keren gedeeld.

Phishing* en ransomware** in 2018

1478



websites offline gehaald voor phishing***

171



processen-verbaal met modus ransomware****

* **Phishing** : vorm van oplichting waarbij criminelen geld aftroggelen van nietsvermoedende mensen aan de hand van frauduleuze mails en websites die bijvoorbeeld lijken alsof ze van een bankinstelling afkomstig zijn.

** **Ransomware** : virus dat wordt geïnstalleerd op een toestel zonder dat de eigenaar daarvoor toestemming gaf. Het gijzelvirus houdt het toestel en de bestanden gegijzeld (geëncrypteerd) en vraagt losgeld.

*** Tegenover 648 522 meldingen via Safeonweb.be van het Centre for Cyber Security Belgium (CCB).

**** Tegenover 437 meldingen bij het Meldpunt van de Federale Overheidsdienst (FOD) Economie.

De cijfers over cybercrime zijn relatief, omdat de aangiftebereidheid bij de bevolking laag is. Slachtoffers van cybercrime stappen niet vaak naar de politie om klacht neer te leggen. In 2018 registreerden de politiediensten 24 582 feiten. Via de bevraging voor de Veiligheidsmonitor gaf 8% van de bevolking te kennen het afgelopen jaar minstens eenmaal slachtoffer te zijn geweest van 'oplichting op het internet'. Slechts één op vijf deed hiervan aangifte. Er is dus een groot *dark number*.



Federale Politie

✉ federal.contactcenter@police.belgium.eu

🌐 www.federalepolitie.be

Archief

[Jaarverslag 2017](#)

[Jaarverslag 2016](#)

Taalkeuze

[Nederlands](#)

[Français](#)

Copyright ©2019 | Ontworpen door [Federale Politie](#)

