

Online veiligheid

- Het aantal fraudedossiers waarin de internetrechercheurs van de *Internet Referral Unit* (i2-IRU) tussenkwamen, steeg aanzienlijk.
- Ook voor de Federal Computer Crime Unit (FCCU) was 2020 een bijzonder jaar. De Covid-19-pandemie had een grote impact op onder meer de internationale werking, de steundossiers en de opleidingen.
- Onder de koepel van de Europese Politieacademie CEPOL ontwikkelden de experts van FCCU een nieuwe doorgedreven opleidingsmodule rond het *dark web* voor Europese politiediensten.

Internetrecherche

De sectie i2-IRU (Internet Referral Unit) van de Directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) voert verschillende opdrachten uit:

- internetrecherche;
- het blokkeren van websites en/of content (in samenwerking met providers en webplatformen);
- communicatie over preventie;
- opleiding, het geven van informatie en het delen van expertise;
- deelname aan de acties van Europol.

Voor terro-dossiers (terroristische propaganda en aanverwante gewelddadige extremistische activiteiten op het internet) werkt i2-IRU samen met de Internet Referral Unit opgericht door Europol (IRU EU). Europol beschikt over een geautomatiseerde tool om opgespoorde propaganda ontoegankelijk te maken. Dossiers met een link naar België worden verder door i2-IRU behandeld.

i2-IRU verleende in 2020 in 1 099 dossiers steun aan de eenheden. Dat is een stijging met 88 dossiers ten opzichte van 2019 (1 011). De opmerkelijke stijging voor een aantal fenomenen is gelinkt aan COVID-19: de illegale verkoop van producten (fraude), de oproep tot ongehoorzaamheid (openbare orde) en het 'fake news' met betrekking tot vaccins en valse remedies voor de bestrijding van COVID-19.

1 099



dossiers

Fenomenen	2019	2020
Terrorisme	314	244
Informatie	132	151
Fraude	118	194
Diefstal	91	32
Poging zelfmoord	66	69

Fenomenen	2019	2020
Kindermisbruik	54	53
Mensenhandel	47	35
Drugs	40	57
Openbare orde	40	97
Cyberhaat	37	47
Cybercrime	31	37
Wapens	26	20
Verdwijningen	/	23
Hormonen	13	15
Moord	2	16
Patrimonium	/	6
Fake news	/	2
Wraakporno	/	1
Totaal	1 011	1 099

Federal Computer Crime Unit

De opdracht van de Federal Computer Crime Unit (FCCU) bestaat erin complexe en georganiseerde vormen van cybercriminaliteit te bestrijden, inzonderheid wanneer deze een impact hebben op kritieke infrastructuur of aanbieders van essentiële diensten. Daarnaast ontwikkelt de FCCU een expertise in bepaalde hoogtechnologische materies en levert zij gespecialiseerde steun aan de centrale onderzoeksdiensten en de inspectiediensten (AIG/Comité P) bij het onderzoeken van digitale gegevensdragers. Ten slotte draagt FCCU, samen met de Directie van de communicatie (CGC), ook bij tot het informeren en sensibiliseren van de bevolking over cybersecurity, over actuele digitale dreigingen en online veiligheid, onder meer via de socialemediakanalen van de Federale Politie.

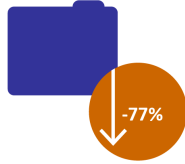
2020 was een bijzonder jaar; de coronapandemie had een grote impact op onder meer de internationale werking, de steundossiers en de opleidingen.

Desalniettemin steeg de effectieve capaciteit van FCCU in 2020 met 22% (van 23 naar 28 medewerkers). Een niet onaardige prestatie, aangezien ICT-specialisten zeer gegeerd zijn op de arbeidsmarkt. De focus ligt voornamelijk op het verbeteren van de interne processen en dienstverlening aan onze partners.

Qua internationale samenwerking is FCCU nog altijd piloot voor een EMPACT-project aangaande het ontwikkelen van een doorgedreven dark web opleidingsmodule. Het vorige trainingspakket werd alvast zeer positief onthaald.

FCCU heeft in 2020:

- 28 eigen dossiers behandeld (tegenover 121 in 2019, inclusief steunopdrachten voor andere eenheden);
- 50 meldingen ontvangen in de ransomware-webapplicatie (tegenover 171 in 2019). Deze terugval is echter voornamelijk te wijten aan onderrapportering (zowel intern als extern) want ransomware tiert nog steeds welig. Bij de modus 'ransomware' installeren afpersers op een slinkse manier een virus op een toestel buiten het medeweten van de eigenaar om. De kwaadaardige software houdt het toestel en de bestanden 'gegijzeld' (geëncrypteerd) en de afpersers eisen losgeld.



dossiers cybercriminaliteit



Success Story

Veroordelingen in omvangrijk kindermisbruikdossier

In een van de grootste kindermisbruikdossiers ooit in België zijn door de correctionele rechtbank van Oost-Vlaanderen, afdeling Dendermonde, op 31 maart 2020 vijf verdachten tot gevangenisstraffen veroordeeld. Maar dit was geen eindpunt. De hoeveelheid inbeslaggenomen beeldmateriaal was ongezien en leidde wereldwijd tot de identificatie van tientallen slachtoffers en daders. Het dossier is een mooi voorbeeld van samenwerking tussen de Federale Politie, de Lokale Politie, Europol en Interpol.

De bal ging aan het rollen in 2015 met de aanhouding van een man die op het strand foto's nam van naakte spelende kinderen. De politiezone VLAS (Kortrijk/Kuurne/Lendeledede) startte een onderzoek en trof digitale beelden van kindermisbruik aan. De onderzoekers stelden ook vast dat de verdachte contact had met een man uit het Oost-Vlaamse Wetteren met wie hij beelden uitwisselde. Het parket en de Federale Gerechtelijke Politie (FGP) Oost-Vlaanderen startten een onderzoek naar deze man. In opdracht van de onderzoeksrechter te Dendermonde werd een huiszoeking uitgevoerd en die resulteerde in de inbeslagname van ongeveer 15 terabyte (TB) aan beeldmateriaal! Doorgedreven onderzoek liet toe om nog drie verdachten in het vizier te krijgen.

Gezien de enorme hoeveelheid bestanden en de vele contacten in besloten kring, via het **dark web**, was het noodzakelijk om het onderzoeksteam uit te breiden en een internationale samenwerking op te starten. Er kwam steun van de Computer Crime Unit, de centrale dienst Child Abuse van de Federale Politie, FGP West-Vlaanderen en de politiezone VLAS. Op internationaal vlak leverde Europol een bijdrage in de analyse van de gegevens. Interpol begeleidde de berichten naar de collega's buiten Europa.

De intensieve samenwerking tussen het onderzoeksteam en Europol heeft ertoe geleid dat er wereldwijd meer dan 110 slachtoffers en 90 verdachten geïdentificeerd werden. In meer dan 40 landen werden onderzoeken opgestart of kon de informatie bijdragen tot een lopend onderzoek. Dit leidde wereldwijd tot arrestaties en veroordelingen. Heel wat onderzoeken zijn nog lopende.

tot arrestaties en veroordelingen. Meer wat onderzoeken zijn nog ropende.