Aanpak Cybercrime

Een eerste introductie van cybercrime en de aanpak hiervan door de politie Oost-Nederland.

Hand-out voor gemeenten in Oost-Nederland.

Februari 2021

Cybercrime en gedigitaliseerde criminaliteit*

In de criminaliteitscijfers is een verschuiving zichtbaar van criminaliteit in de fysieke wereld naar criminaliteit welke online wordt gepleegd. Hierbij kan een onderscheid worden gemaakt tussen cybercrime en gedigitaliseerde criminaliteit.

Cybercrime

Cybercrime betreft strafbare feiten welke niet zonder tussenkomst van een computer en/of netwerk gepleegd kunnen worden. De criminaliteitsvormen zoals ransomware, hacken en DDoS-aanvallen vragen om een specialistische aanpak.

Gedigitaliseerde criminaliteit

Gedigitaliseerde criminaliteit betreft vooral bekende criminaliteitsvormen zoals fraude, oplichting en afpersing welke via de digitale weg zijn gepleegd. Bij deze criminaliteitsvorm spelen computers en/of netwerken een rol. De criminaliteitsvorm is niet nieuw, de wijze waarop deze wordt gepleegd wel. Vooral bij deze criminaliteitsvormen is een stijging van aangiften zichtbaar.

** In deze hand-out wordt de term cybercrime gehanteerd. Hiermee wordt zowel cybercrime als gedigitaliseerde criminaliteit bedoeld.*

"Iedereen kan slachtoffer worden van cybercrime"

Kenmerken

Veel slachtoffers

Cybercrime wordt onder andere gekenmerkt door het feit dat een dader eenvoudig en in korte tijd een groot aantal slachtoffers kan maken.

Grensoverschrijdend

Doordat de criminaliteit via de digitale weg plaatsvindt, is deze vaak grensoverschrijdend. Een dader kan vanaf één locatie slachtoffers door het hele land maken.

Georganiseerd verband

Veel cybercrime delicten worden in georganiseerd verband gepleegd, waarbij meerdere personen met verschillende rollen betrokken zijn.

Snelle ontwikkelingen

Cybercrime is continue in ontwikkeling. Daders verzinnen in hoog tempo nieuwe methoden om slachtoffers te maken. Een actueel beeld vandaag, kan volgende maand achterhaald zijn.

"Snelle ontwikkelingen vragen om een flexibele aanpak"

Veelvoorkomende cybercrime

Op basis van de politiecijfers uit 2020 kan gesteld worden dat er vijf vormen van cybercrime veel voorkomen in Oost-Nederland.

Helpdeskfraude

Een persoon doet zich telefonisch voor als medewerker van een helpdesk en beweegt het slachtoffer naar bepaalde rekeningen geld over te maken.

Fraude bankgegevens

Het slachtoffer heeft een bericht ontvangen om bijv. bankgegevens te verifiëren, een bankpas aan te vragen of een betaling te doen. Hierbij wordt het slachtoffer bewogen op een valse website bankgegevens in te vullen, welke door de dader worden misbruikt.

Vriend-in-noodfraude

Het slachtoffer wordt benaderd door een persoon die zich voordoet als een bekende van het slachtoffer en verzoekt het slachtoffer rekeningen te betalen.

Aan- en verkoopfraude

Oplichtingsvorm waarbij online gekochte goederen worden betaald, maar niet ontvangen. Of goederen zijn verstuurd, maar er wordt niet voor betaald.

Misbruik account voor bestellingen

Met het (webshop)account van het slachtoffer zijn bestellingen geplaatst voor goederen of diensten, welke niet door het slachtoffer zelf zijn gedaan.

Bestrijden cybercrime

Cybercrime is een geprioriteerd thema voor de Nationale Politie. Om snel te acteren op nieuwe trends en ontwikkelingen heeft elke politie eenheid een Cybercrimeteam. Deze teams ondersteunen de basisteams bij de lokale aanpak van cybercrime. Daarnaast is cybercrime grensoverschrijdend waardoor naast een lokale en regionale aanpak ook landelijk en internationaal wordt samengewerkt met andere politie eenheden. Hierbij wordt geïnvesteerd op onderstaande drie aspecten.

Voorkomen

Door de inzet van preventieve middelen gericht op slachtoffers en (potentiële) daders wordt zoveel mogelijk aan de voorkant getracht cybercrime te voorkomen.

Verstoren

Voor de aanpak van veelvoorkomende cybercrimedelicten worden fenomeenonderzoeken uitgevoerd. Deze onderzoeken maken inzichtelijk waar barrières opgeworpen kunnen worden om het criminele proces te verstoren.

Opsporen

Door politie onderzoeken worden in samenwerking met het Openbaar Ministerie verdachten opgespoord en vervolgd. Opsporen en vervolgen is een laatste middel om cybercrime aan te pakken.

"Gezamenlijk optrekken in de strijd tegen cybercrime”

Samen voorkomen en verstoren

Door in samenwerking met overheidspartners, zoals gemeenten, en private partners te investeren op het voorkomen en verstoren van cybercrime wordt deze effectiever en efficiënter bestreden. Hieronder een aantal voorbeelden van gerichte aanpakken. Hierbij het advies om waar mogelijk aan te sluiten bij bestaande initiatieven.

Slachtofferpreventie

Slachtofferpreventie richt zich op het voorkomen van slachtofferschap van cybercriminaliteit. Afhankelijk van de criminaliteitsvormen kan de preventie zich richten op specifieke doelgroepen als ouderen, jongeren of ondernemers.

Daderpreventie

Daderpreventie richt zich op het voorkomen van daderschap van cybercriminaliteit. Door in de bestrijding van cybercrime vroeg te investeren op (potentiële) daders wordt getracht te voorkomen dat zij in de toekomst het criminele pad op gaan.

Fenomeenaanpak

Om een specifiek fenomeen aan te pakken kunnen naast de politie ook andere publieke en private partijen barrières opwerpen om het criminele proces te verstoren.

"Bewustwording online gedrag en vergroten cyberweerbaarheid”

Cybercrimeteam Oost-Nederland

Multidisciplinair team

Oost-Nederland bestaat uit 5 districten en 27 basisteams welke in de aanpak van cybercrime worden ondersteund door het regionale Cybercrimeteam. Het Cybercrimeteam is een specialistisch multidisciplinair samengesteld opsporingsteam. Naast de verbinding met lokale teams, staat het Cybercrimeteam tevens in verbinding met Cybercrimeteams uit andere politie eenheden.

Netwerk

De strijd tegen cybercrime vraagt om een integrale aanpak. Ieder Cybercrimeteam houdt zich actief bezig met publiek-private-samenwerking om gezamenlijk cybercrime aan te pakken. Naast een regionale werkgroep cyber zijn er in diverse districten werkgroepen cyber waaraan onder andere politie, OM en gemeenten deelnemen.

Vragen?

Ieder basisteam heeft een aanspreekpunt voor het thema cybercrime. Daarnaast is ieder basisteam vertegenwoordigd in het cybernetwerk Oost-Nederland en heeft daarmee een directe verbinding met het Cybercrimeteam Oost-Nederland. Voor de aanpak op lokaal niveau is het advies om over dit geprioriteerde thema in gesprek te gaan met het basisteam.