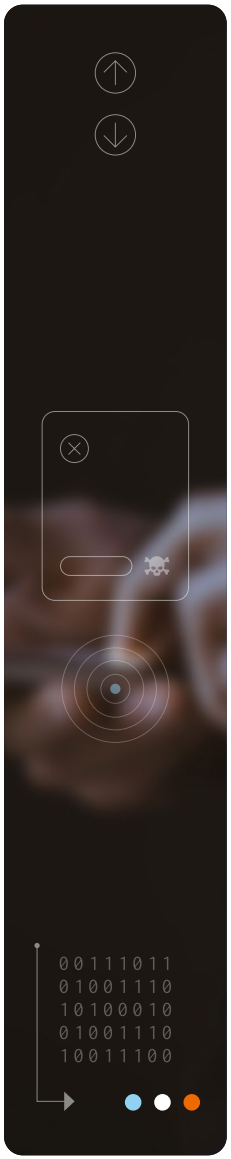
OPENBAAR MINISTERIE POLITIE

CYBER CRIME BEELD NEDERLAND 2024



01/02

Samenvatting

Cybercrime effectief bestrijden kan alleen als dat gebeurt op een breed terrein en als Openbaar Ministerie (OM), politie, publieke én private partners intensief samenwerken. Brede bestrijding van cybercrime draait om opsporing en vervolging, maar ook om het tegenhouden van criminaliteit (verstoring), het beperken van schade (via notificatie) en het voorkomen van dader- en slachtofferschap (preventie). Voor deze brede bestrijding is essentieel dat alle partijen urgentie geven aan de aanpak van cybercrime.

Het Cybercrimebeeld Nederland (CCBN) schetst een beeld van het cybercrimedomein, specifiek vanuit het unieke perspectief van OM en politie, aangevuld met informatie uit openbare bronnen. Het is de eerste editie van een tweejaarlijkse monitor van de grote ontwikkelingen op het terrein van cybercrime.

In deze eerste editie ligt de focus op het complexere gedeelte van online criminaliteit dat primair gericht is op ICT: cybercrime.

De doelgroep zijn beleidsmakers en bestuurders van publieke én private partners die actief zijn in de brede bestrijding van cybercrime.

De belangrijkste bevindingen in het CCBN 2024 zijn:

01

Het cybercrimelandschap is complex

Doordat cybercrime vele verschijningsvormen kent die constant in ontwikkeling zijn, is geen standaard aanpak mogelijk. Cybercrime is een internationale vorm van criminaliteit met lokale componenten. De aanpak van cybercrime is een specialisme in ontwikkeling.

Terwijl het voor OM en politie kennis, kunde, tijd en focus vergt om cybercrime te bestrijden, wordt het voor criminelen juist steeds eenvoudiger om in te stappen in deze vorm van criminaliteit. Je hoeft geen meesterbrein te zijn om aan de slag te gaan als cybercrimineel.

Dit komt doordat technisch onderlegde criminelen hun diensten, producten en handleidingen aanbieden: *cybercrime-as-a-service*. Dit maakt het mogelijk voor allerlei criminelen om cybercrime te plegen. Denk daarbij bijvoorbeeld aan DDoS aanvallen of zelfs volledige phishingpanels, die kant en klaar te koop zijn.

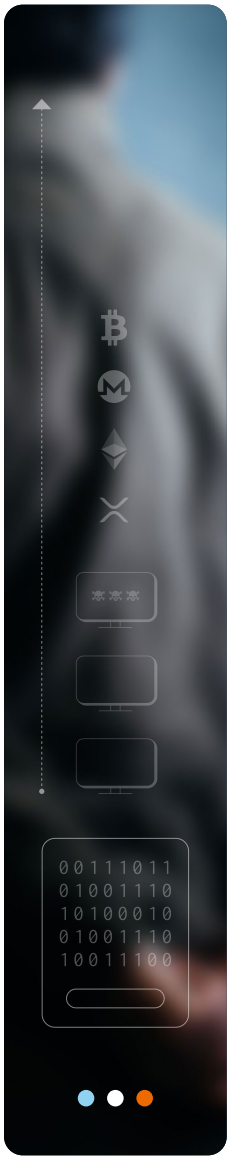
02

Trends en ontwikkelingen 2024

OM en politie zien in de praktijk dat de volgende ontwikkelingen bijdragen aan zowel de omvang als de impact van cybercrime:

I. Zorgwekkend aandeel jonge cybercrimeverdachten
OM en politie maken zich zorgen over het aandeel jonge verdachten van cybercrime. De helft van de cybercrimeverdachten die zich voor de rechter moeten verantwoorden is 25 jaar of jonger.

II. Opkomst van datadiefstal en -handel
Cybercriminelen stappen in toenemende mate af van het versleutelen van data als afpersingstactiek. In plaats daarvan kopiëren zij de data, waarna gelijk wordt overgegaan tot afpersing. De data wordt vervolgens verrijkt door bijvoorbeeld datasets met elkaar te combineren om de waarde, nauwkeurigheid of bruikbaarheid te vergroten en door te verkopen aan andere criminelen.



02/02

Samenvatting

02

Trends en ontwikkelingen 2024

III. Vermenging met traditionele criminaliteit
Cyber-officieren van justitie zien in hun onderzoeken dat de grens tussen cybercrime en andere, meer traditionele, vormen van criminaliteit vervaagt. Verdachten houden zich niet uitsluitend bezig met cybercrimedelicten. Zo worden geregeld wapens, munitie en explosieven aangetroffen bij - soms zelfs minderjarige - verdachten. Het beeld dat cybercriminelen zich slechts bewapenen met een toetsenbord is dan ook niet altijd juist.

IV. Nederland als host van criminele infrastructuur
Nederlandse datacenters en hostingbedrijven spelen een belangrijke rol in het voorkomen en bestrijden van cybercrime. Er zijn partijen die zich legitiem voordoen maar weinig verantwoordelijkheid nemen om de hoeveelheid strafbaar materiaal op de eigen servers te beperken, met de eigen diensten adverteren op de criminele markt en zo actief cybercrime faciliteren. Ondanks verbeterde wetgeving die de Digital Services Act (DSA) biedt, blijft er ruimte voor twijfelachtige verdienmodellen.

03

De impact op slachtoffers wordt onderschat

Uit onderzoek blijkt dat particuliere slachtoffers van cybercrime meer emotionele dan financiële schade ondervinden en dat de acute stress groter is dan bij vergelijkbare traditionele delicten.

Daarnaast bestaat de schade voor bedrijven niet alleen uit de initiële materiële schade, maar ook uit naweeën als reputatieschade of privacyschendingen en aanhoudende psychische problemen bij werknemers. Bovendien is de strafrechtketen niet ingericht op het massaal slachtofferschap als gevolg van de inherente schaalbaarheid van cybercrime, waarbij met één druk op de knop vele slachtoffers tegelijk kunnen worden gemaakt.

04

Brede bestrijding is noodzakelijk voor een effectieve aanpak van cybercrime

Publieke én private partners spelen een cruciale rol in de bestrijding van cybercrime. Het cybercriminele systeem is flexibel en veerkrachtig. Waar mogelijk zijn lokale interventies in het systeem belangrijk, maar ze hebben niet per definitie grote impact op het totale systeem van cybercrime.

De bestrijding van cybercrime vraagt daarom om een integrale en systemische aanpak, waarbij de verschillende partners eigen expertise en verantwoordelijkheden hebben. OM en politie zijn een belangrijk onderdeel en sluitstuk van die brede aanpak, maar ook andere publieke en private partijen spelen een cruciale rol.

Een integrale, systemische aanpak draait niet alleen om opsporing en vervolging van cybercriminelen, maar ook om verstoren van hun activiteiten, informeren van slachtoffers en preventie die erop is gericht om te voorkomen dat mensen slachtoffer worden van cybercrime en dat nieuwe daders opstaan.