# #616: Verantwoordelijkheid van derden voor cybercriminaliteit: bulletproof hosting

In een recente zaak bij de rechtbank Rotterdam (ECLI:NL:RBROT:2025:2488 en ECLI:NL:RBROT:2025:2492) stond een bulletproof hostingprovider en haar bestuurders terecht vanwege de actieve rol die hun infrastructuur speelde bij het hosten en verspreiden van de beruchte Mirai-botnetmalware. De rechtbank boog zich over de vraag of de verdachten medeplichtig waren aan computervredebreuk en de verdere verspreiding van de malware. Deze kwestie werpt een interessant licht op de grenzen van strafrechtelijke aansprakelijkheid voor hostingproviders, zeker nu er (nog) geen formele wettelijke regels bestaan die deze sector reguleren.

**De kern van de zaak**

De rechtbank stelt voorop dat de online sector voor het grootste deel zelfregulerend is. Omdat algemeen bekend is dat hostingpartijen (on)bewust faciliterend kunnen zijn aan cybercriminaliteit, nemen zij zelf maatregelen om te voorkomen dat er misbruik wordt gemaakt van hun virtuele diensten, aldus de rechtbank. Uit het vonnis blijkt dat de verdachten bekend waren met de risico's van misbruik en de bestaande Gedragscode voor hostingproviders, waarin onder meer staat dat hostingpartijen '*alles moeten doen wat in hun mogelijkheden ligt om misbruik te bestrijden*'. Desondanks namen zij nauwelijks maatregelen tegen de vele abusemeldingen die dagelijks binnenkwamen – 8.012 mails in ongeveer een halfjaar, waarvan 138 specifiek over Mirai en gerelateerd aan een

bepaald IP-blok. Bovendien bleek dat deze hostingprovider anonieme klantregistratie toestond, betaalmethodes in Bitcoins faciliteerde en zelfs instructies gaf aan klanten over hoe ‘malware binary’s’ te verbergen. Aan misbruikmeldingen werd vaak geen gevolg gegeven; in de communicatie tussen de hostingprovider en klant werd expliciet gezegd ‘niet om abuse te geven’, terwijl de genoemde IP-adressen gewoon actief bleven.

**Medeplichtigheid**

De vraag is, welke omstandigheden leiden nu tot een medeplichtigheid aan de strafbare feiten? Voor medeplichtigheid (art. 48 Sr) moet de verdachte opzettelijk behulpzaam zijn bij het plegen van een delict, of opzettelijk gelegenheid, middelen of inlichtingen verschaffen. Cruciaal is dat het opzet (al dan niet in voorwaardelijke vorm) niet alleen gericht is op het aanbieden van servers, maar ook op het onderliggende strafbare feit. In deze zaak ging het om computervredebreuk en de verspreiding/het hosten van het Mirai-botnet.

Bij voorwaardelijk opzet aanvaardt de verdachte bewust de aanmerkelijke kans dat zijn handelen of nalaten zal leiden tot het strafbare feit. De rechtbank oordeelde dat de verdachten in kwestie de grote hoeveelheid abusemeldingen kenden, wisten van het hosten van Mirai en zelfs actief meewerkten aan het faciliteren van deze malware door actief instructies te geven. Daarmee aanvaardden zij volgens de rechtbank bewust de aanmerkelijke kans dat hun diensten werden gebruikt voor het hacken en verspreiden van dit botnet.

**Rol van gedragscodes en (afwezige) KYC**

Eén van de opmerkelijke punten is dat er geen wettelijke plicht bestaat om klanten te identificeren, noch een algemene wettelijke verplichting om abusemeldingen op te volgen. De Gedragscode – die door de sector zelf is opgesteld – legt geen

wettelijke verplichting op, maar laat zien dat hostingproviders zich bewust moeten zijn van het risico dat hun diensten kunnen worden misbruikt en welke maatregelen ze zouden kunnen nemen. De rechtbank heeft die kennis en het feit dat er niet werd opgetreden ondanks die kennis, meegewogen bij de beoordeling van de opzet.

In deze context is de vraag gerechtvaardigd hoeveel meldingen nodig zijn voordat een dienstverlener in de gevarenzone van strafrechtelijke aansprakelijkheid belandt, en of het negeren van abusemeldingen voldoende is of dat er meer nodig is. Het strafrecht is in beginsel het 'ultimum remedium', niet bedoeld om op onduidelijke wijze zorgplichten binnen een sector af te dwingen. Dat schept onzekerheid en kan lijken op een vorm van risicoaansprakelijkheid.

**Eigen bijdrage als factor**

Wat mij betreft is cruciaal in deze zaak dat de hostingprovider niet slechts passief optrad, maar concreet instructies gaf om de malware verborgen te houden. Deze actieve ondersteuning maakte aannemelijk dat de verdachten (voorwaardelijk) opzet hadden op de onderliggende strafbare feiten. Enkel stilzitten of wegkijken was in deze zaak kennelijk niet aan de orde.

**Conclusie**

Deze zaak onderstreept voor mij de noodzaak van heldere regels over wat wel en niet mag, zodat dienstverleners weten wanneer zij strafrechtelijke risico's lopen. Totdat die regelgeving er is, leert deze zaak dat hostingpartijen die evident criminele activiteiten faciliteren én zelfs actief ondersteunen, een grote kans lopen te worden veroordeeld voor medeplichtigheid. Het strafrecht zet hiermee een duidelijk signaal af, maar de gewenste rechtszekerheid vraagt om meer. Het strafrecht moet niet te snel worden ingezet om bepaalde zorgplichten in een sector af te dwingen, terwijl die niet wettelijk zijn

vastgelegd.

Heb je vragen over het voorgaande of wil je hierover van gedachten wisselen met ons? Neem dan contact op via vaklunch@hertoghsadvocaten.nl.