STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 3271
31 januari
2018

Richtlijn voor strafvordering cybercrime

Rechtskarakter: Aanwijzing i.d.z.v. artikel 130, lid 6 Wet RO
Van: College van procureurs-generaal
Aan: Hoofden van de OM-onderdelen
Registratienummer: 2018R001
Datum inwerkingtreding: 01-02-2018
Publicatie in Stcrt.:
Vervallen: –
Relevante beleidsregels OM: Aanwijzing kader voor strafvordering en OM-afdoeningen (2015A001)
Wetsbepalingen: Art. 138ab, 138b, 139d en 350a Wetboek van Strafrecht (Sr)
Bijlage(n): -

Inleiding

De computer en het internet zijn niet meer weg te denken uit onze samenleving. Deze nieuwe technologie heeft het dagelijks leven veranderd. Steeds meer voorwerpen zijn aangesloten op het internet (Internet of Things, IoT) en kunnen gegevens uitwisselen. Dit brengt kansen voor criminelen en daarmee veiligheidsrisico's voor burgers, bedrijven en overheidspartijen met zich mee. Het aantal gevallen van cybercrime blijft toenemen. Computers worden niet alleen als middel ingezet, maar zijn ook doelwit van aanvallen. Dankzij de technologische mogelijkheden kunnen cybercriminelen in korte tijd vanaf elke plek ter wereld grote aantallen slachtoffers maken. Om een veilig digitaal domein te creëren en effectief tegen cybercrime te kunnen optreden, is een zichtbare, integrale en toekomstgerichte aanpak nodig.

Deze eerste richtlijn cybercrime biedt handvaten voor de op zitting te eisen straffen.
De richtlijn ziet op de verschillende verschijningsvormen van cybercrime (o.a. computervredebreuk, de DDoS aanval, ransomware, malware, defacing) en bevat criteria aan de hand waarvan in individuele zaken een strafeis geformuleerd kan worden.

De omschrijving van de diverse vormen van cybercrime die terugkomen in deze richtlijn staan genoemd in de legenda onderaan.

De richtlijn onderscheidt daarnaast de volgende categorieën:
– Cybercrime in de relatiesfeer (ex-partners, ex-werknemers, etc.)
– Cybercrime met als oogmerk diefstal van vermogen (diefstal internetbankieren, art. 139d Sr, crypto/ransomware)
– Cybercrime met als oogmerk het overnemen van gegevens ((bedrijfs)spionage, tentamenfraude, etc)
– Cybercrime met een ideologisch (niet zijnde terroristisch) oogmerk (DDos, art. 350a Sr, defacing)

Beschrijving

Deze richtlijn heeft betrekking op diverse vormen van cybercrime. Er is een tabel voor cybercrime eenmaal gepleegd en een tabel voor meermalen gepleegd.

Basiscasus/delict

Cybercrime, alleen en eenmalig gepleegd.

Cybercrime in relatiesfeer (ex-partners, ex-werknemers, etc.)	**first offender**	**1x recidive***
Inbreken in een (social media of mail) account of (bedrijfs)server (art. 138ab Sr)	TS 20–80 uur	TS 30–120 uur en een voorwaardelijke gevangenisstraf
Wijzigen wachtwoorden/ ontoegankelijke maken van gegevens (art. 350a Sr)	TS 20–100 uur	TS 30–150 uur en een voorwaardelijke gevangenisstraf
Verwijderen / ontoegankelijk maken van gegevens/ toevoegen van gegevens (art. 350a Sr / 138ab Sr)	TS 20–120 uur	TS 30–180 uur en een voorwaardelijke gevangenisstraf

DDoS aanval met beperkte impact** (art. 138b Sr)	TS 60 uur	TS 90 uur
Het versturen van een smadelijk/lasterlijk bericht vanuit het account van je (ex-)partner (smaad en computervredebreuk)	TS 120 uur	TS 180 uur en een voorwaardelijke gevangenisstraf
Cybercrime met oogmerk diefstal vermogen (diefstal internetbankieren, art. 139d Sr, crypto/ransomware)	**first offender**	**1x recidive***
Diefstal internetbankieren (art. 311 Sr / 138ab Sr) – tot € 10.000,-	TS tot 120 uur/ GS 1 week tot 2 mnd	GS 10 weken tot 4 mnd
– van € 10.000,– t/m € 100.000,–	TS vanaf 120 uur/ GS 2 tot 5 mnd	GS 4 mnd tot 6 mnd
– meer dan € 100.000,-	GS vanaf 5 mnd	GS vanaf 7 mnd
Voorhanden hebben van malware / wachtwoorden / inloggegevens (art. 139d lid 2 sub a en b Sr)	GS 2 weken	GS 3 wkn
Gebruik van crypto- en ransomware (art. 326/284 Sr)	GS 3 maanden	GS 4 mnd
Hacken van een server ten behoeve van b.v. phishen (art. 138ab Sr)	GS 1 maand	GS 6 wkn
Cybercrime met oogmerk overnemen gegevens ((bedrijfs)spionage, tentamenfraude, etc)	**first offender**	**1x recidive***
Inbreken in account met het oogmerk gegevens over te nemen (art. 138ab Sr)	GS 2 maanden	GS 3 maanden
Het voorhanden hebben van malware (art. 139d lid 2 sub a en b SR)	GS 1 maand	GS 6 wkn
Cybercrime met ideologisch (niet zijnde terroristisch) oogmerk (DDos, art. 350a Sr, defacing)	**first offender**	**1x recidive***
Defacen website (art. 350a Sr)	TS 60 uur	TS 90 uur en een voorwaardelijke gevangenisstraf
DDoS aanval met beperkte impact** (art. 138b Sr)	TS 60 uur	TS 90 uur
Bijzonderheden Uitgangspunt is dat de dader de schade vergoedt. Strafverzwarende/verminderende factoren o.a .: – gebruik malware – schade / herstel – aard van gegevens – kwetsbaar slachtoffer – verbeurdverklaring computers/gegevensdragers – meermalen recidive (maatwerk) * Let op evt. taakstrafverbod (art. 22b Sr) ** De impact is afhankelijk van de financiële schade en in hoeverre diensten zijn getroffen.		

Basiscasus/delict

Cybercrime, meermalen gepleegd, veelal in georganiseerd verband en in combinatie met andere strafbare feiten

Cybercrime met oogmerk diefstal vermogen (diefstal internetbankieren, art. 139d Sr, crypto/ransomware)	**first offender**	**1x recidive**
Medeplegen van diefstal met valse sleutel en computervredebreuk, bestaande uit het inloggen op een bankrekening en het vervolgens overmaken van geld naar rekening van derde(n), met inloggegevens waartoe dader niet gerechtigd was. Meestal zijn de inloggegevens (deels) verkregen dmv phishing en/of malware (art. 138ab/139d/311/326/420bis Sr)	GS 3 jaar	GS 4 jaar
Grootschalige ransomware-campagne	GS 3 jaar	GS 4 jaar
Bijzonderheden Uitgangspunt is dat de dader de schade vergoedt. Strafverzwarende/verminderende factoren o.a.:		

– Mate van inbreuk op de privacy van het slachtoffer
– Aantal slachtoffers
– Mate van georganiseerdheid
– Hoogte schade
– meermalen recidive (maatwerk)

Legenda

Malware = Samentrekking van malicious software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.

Ransomware = Type malware dat systemen en/of informatie daarop blokkeert en alleen tegen betaling van losgeld toegankelijk maakt.

Cryptoware = Type ransomware dat bestanden op een computer of in een netwerk versleutelt. De sleutel wordt alleen tegen betaling vrijgegeven.

Phishing = Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor identiteitsdiefstal. Spearphishing is een variant die zich richt op één persoon of een zeer beperkte groep personen in bijvoorbeeld een organisatie, die specifiek worden uitgekozen op basis van hun toegangspositie om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.

Defacing = Bij defacing worden websites door hackers gewijzigd, beschadigd of vervangen.

DDoS = (Distributed) Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.

Afkortingen

TS = Taakstraf
GS = gevangenisstraf

Voor een toelichting op de onderstreepte begrippen zie de Aanwijzing kader voor strafvordering en OM-afdoeningen.