Openbaar Ministerie

College van procureurs-generaal

Parket-Generaal

Postadres: Postbus 20305, 2500 EH Den Haag.

Bezoekadres:
Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 70 33 99 600
Telefax +31 70 33 99 851

Aan alle parkethoofden

Onderdeel	Beleid & Strategie
Contactpersoon	
Doorkiesnummer(s)	
Datum	18 maart 2013
Ons kenmerk	PaG/B&S/16708
Bijlage	1
Onderwerp	Responsible Disclosure (hoe te handelen bij 'ethische' hackers?)

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Beste collega's,

Onlangs is door het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie een handreiking gepresenteerd voor organisaties (overheid en bedrijfsleven) en `ethische` hackers om op verantwoorde manier kwetsbaarheden in informatiesystemen en (software)producten te melden en af te handelen. Deze handreiking is getiteld: 'Leidraad om te komen tot een praktijk van Responsible Disclosure' (zie bijlage). Doel van deze leidraad is het bieden van bouwstenen voor organisaties om een beleid voor Responsible Disclosure te kunnen vaststellen. Dit beleid geeft de `ethische` hacker duidelijkheid hoe door de desbetreffende organisatie zal worden omgegaan met door die hacker aangetoonde en/of gemelde kwetsbaarheden in de ICT systemen en biedt getroffen bedrijven de mogelijkheid om kwetsbaarheden te verhelpen en schade te beperken vóórdat de hacker met zijn daad naar buiten treedt. Het verantwoord melden van een kwetsbaarheid vrijwaart de melder, indien hij bij het aantonen van de kwetsbaarheid een strafbaar feit heeft gepleegd, geenszins van de mogelijkheid dat de politie, op gezag van het OM, een strafrechtelijk onderzoek instelt en/of dat wordt overgegaan tot vervolging. In deze brief wordt een aantal uitgangspunten geformuleerd die de officier van justitie dient te betrekken bij de afweging van de vraag of er wel of geen vervolging tegen de hacker/melder van een kwetsbaarheid dient te worden ingesteld.

In het Wetboek van Strafrecht komt het begrip 'ethisch' hacken niet voor in de bepalingen die computervredebreuk regelen. De wet voorziet ook niet in een

specifieke strafuitsluitingsgrond voor een hacker die handelt uit ideologische/ethische motieven. Hoewel de wet hierin dus niet voorziet, wil dat niet zeggen dat 'ethische' motieven geen rol kunnen spelen bij de beoordeling van de strafbaarheid van het handelen of de dader. Als een hacker een lek vindt in de beveiliging van een informatiesysteem van een bedrijf en dit meldt aan het betreffende bedrijf, dan heet dat — in beginsel — gewetensvol of 'ethisch' hacken. In principe wordt geen strafrechtelijk onderzoek ingesteld wanneer sprake is van rechtsherstel tussen de melder en het betreffende bedrijf . Echter, als een hacker een lek meldt, maar er aanwijzingen zijn dat de hacker bewust dan wel onbewust meer heeft gedaan dan alleen melden van het beveiligingslek aan het betreffende bedrijf, dan dient dat wel degelijk verder te worden uitgezocht. Te denken valt aan het overnemen van gevoelige (persoons-) gegevens of het achterlaten van 'malware' op het systeem. Het toetsingskader dienaangaande is vergelijkbaar met de situaties waarin door journalisten strafbare feiten worden gepleegd met het oog op nieuwsgaring. Op dit toetsingskader wordt hierna ingegaan.

De leidraad regelt in principe niets meer of minder dan hoe bij voorkeur dient te worden opgetreden wanneer informatie wordt verkregen over een kwetsbaarheid in een ICT-systeem. De wijze waarop die informatie is verkregen speelt bij Responsible Disclosure (voortaan: RD) op zich geen rol. Het doel van RD is het bijdragen aan het verhogen van veiligheid van ICT systemen door (mogelijke) kwetsbaarheden op verantwoorde wijze te melden en deze meldingen zorgvuldig af te handelen, zodat schade zoveel mogelijk kan worden voorkomen of beperkt.

RD is dan ook geen 'gegeven' of 'beleid' waar eenieder zich zondermeer op kan beroepen. Evenmin is RD uniform. Er is sprake van RD, wanneer het gehackte bedrijf ook een RD-beleid heeft. Wanneer daar geen sprake van is, is er ook geen sprake van RD. Vanzelfsprekend kan bij de beoordeling van de casus wel worden gekeken naar de algemene uitgangspunten die bij RD worden gehanteerd en die in de Handleiding zijn beschreven. Dikwijls is nader (strafrechtelijk) onderzoek nodig om na te gaan of een melding die is gedaan door een hacker, onder de gegeven omstandigheden noodzakelijk en proportioneel was. Als een hacker direct en veilig communiceert met de eigenaar van het ICT systeem over een aangetroffen lek in de beveiliging en er geen gegevens zijn verwijderd of gemanipuleerd, kan er sprake zijn van RD en is er geen aanleiding om (verder) strafrechtelijk onderzoek of vervolging in te stellen. Daar waar wel gegevens zijn verwijderd, gemanipuleerd of gekopieerd, dan wel op onevenredige wijze is gehandeld bij het toegang verschaffen tot het ICT-systeem, is er geen sprake van RD en is verder strafrechtelijk onderzoek en eventuele strafrechtelijke vervolging geïndiceerd.

Kortom: de officier van justitie zal bij de afweging van de vraag of er al dan niet sprake is van strafbare gedragingen rekening moeten houden met de volgende omstandigheden:

- Was het handelen van de verdachte noodzakelijk binnen een democratische samenleving (was er een zwaarwegend algemeen belang)?
- Heeft de verdachte bij zijn handelen proportioneel gehandeld (stond het gekozen middel in verhouding tot het te bereiken doel)? Met andere woorden: hoe heeft de hacker toegang verkregen tot het ICT-systeem? Indien daarvoor op onevenredige wijze is gehandeld, bijvoorbeeld zoals omschreven in de Leidraad (blz. 8 onder 4.2.), is geen sprake van een 'ethische' hack.
- Heeft de verdachte subsidiair gehandeld (waren er andere mogelijkheden om te handelen)? Met andere woorden: is de hack direct gemeld aan de eigenaar van het ICT-systeem of heeft de hacker dit niet terstond gedaan om bijvoorbeeld sporen te wissen, gegevens te manipuleren, te kopiëren of te verwijderen? Indien sporen zijn gewist, gegevens zijn gemanipuleerd, gekopieerd of verwijderd is er geen sprake van een ethische hack.

Als het antwoord op bovenstaande vragen positief is, kan de officier van justitie afzien van een strafrechtelijk onderzoek, dan wel geen vervolging instellen.

Zoals hierboven reeds opgemerkt kan het noodzakelijk zijn om toch eerst een strafrechtelijk onderzoek in te stellen en om de hacker als verdachte aan te merken om antwoord te kunnen krijgen op de hierboven genoemde vragen. Bij twijfel kan de zaaksofficier in overleg treden met de cybercrime-officier op zijn/haar parket en/of het Kennis- en Expertisecentrum Cybercrime bij het Landelijk Parket. Het verdient aanbeveling om de overwegingen t.a.v. het hierboven omschreven kader (ten minste) te journaliseren, opdat de vervolgingsbeslissing ter terechtzitting zal kunnen worden toegelicht.

Mocht u n.a.v. deze brief nog vragen en/of opmerkingen hebben dan kunt u contact (laten) opnemen met de afdeling Beleid & Strategie van het Parket-Generaal.

Ik vertrouw erop u voor dit moment voldoende te hebben geïnformeerd.

Met collegiale groet,
Het College van procureurs-generaal,

H.J. Bolhaar