Rondetafelgesprek: computercriminaliteit III
Ronald Prins - Fox IT

Dank voor uw uitnodiging. Ik zal mijn betoog beperken tot de bevoegdheid tot hacken voor de politie.

Noodzaak

Sinds 2010 wordt al over een hackbevoegdheid gediscussieerd. Wat er vaak in die discussies ontbreekt is een uiteenzetting over de noodzaak. Ik doe hier een poging.

Cybercrime is een groeiend probleem. We zien hackers beter en slimmer worden. We zien andere spelers, zoals buitenlandse inlichtingendiensten, die ook van hack technieken gebruik maken. Er is dan ook veel van waarde te halen online. Een hele simpele regel uit de criminologie is dat als er voor een delict geen pakkans is en de opbrengst alleen maar groter wordt dat de criminaliteit dan zal groeien.

Ik zie in Nederland een hoop digitale politie erbij komen, maar zelden wordt een serieuze cybercrimineel aangehouden. De mensen die bij de politie werken hebben prima technische en recherche vaardigheden, maar ze moeten met hun handen op rug gebonden achter de criminelen aangaan.

Waarom loopt de politie vast online? In de basis komt dat omdat het heel makkelijk is om je online te verstoppen achter vage ip-adressen en aliassen. Waar de politie in de fysieke wereld heel veel bevoegdheden (dna, observatie, taps, huiszoeking) heeft om daders te identificeren en bewijs te verzamelen lukt dat in het digitale domein totaal niet. De meeste onderzoeken stoppen bij een vaag ip-adres ergens in het buitenland. En als dan al via een rechtshulp verzoek na 8 weken naar boven komt wie er achter schuil zou gaan, dan blijkt een gehuurde server te zijn, die betaald wordt met gestolen creditcards of bitcoins.

Juist het instrument van hacken geeft de politie de mogelijkheid om wel zicht te krijgen op de daders. Door de criminele infrastructuur te hacken, sla je heel veel tussenliggende landen over en vind je wel sporen die lijden naar een echte identiteit of locatie. Pas dan kan de politie zijn traditionele bevoegdheden weer inzetten.

Ik weet van twee zaken waarbij de politie al ‘geoefend’heeft. Het heeft beide keren geleid tot succes dat anders niet was gelukt. In beide gevallen is het instrument van hacken ingezet om identiteiten van daders te vinden en niet als surveillancetool (Bredolab (2010), Descartes (2012 kp)

Een ander voor de hand liggende oplossing tegen criminele hackers, is het veiliger maken van onze digitale omgeving. Ondanks dat je het altijd moet blijven proberen, denk ik niet dat

daar de oplossing ligt. Onze digitale wereld is te complex om werkelijk veilig te krijgen. Het zal alleen maar complexer worden en daarmee onveiliger.

We zien andere landen de bevoegdheid al succesvol toepassen. De Fransen hebben het bijvoorbeeld ingezet om camera's te hacken in een supermarkt waar een terrorist 15 joodse gijzelaars vast hield.

Hackers, pionnen, activisten, terroristen: iedereen hackt, behalve de politie.
Zoals een wapen in de fysieke wereld gebruikt door criminelen om macht uit te oefenen, zo is hacken dat in cyberspace. Op straat heeft de politie ook een pistool als antwoord daarop. Waarom mogen ze dat online dan niet?

techniek

Veel kritiek op het voorstel is gebaseerd op het gebruik van 0days door de overheid. Dit zijn nog onbekende zwakheden in software. Met een 0day in de hand heb je min of meer garantie dat je in een computer kan binnendringen. De critici hanteren het argument dat de overheid er nu baat bij heeft om onbekende kwetsbaarheden voor zichzelf te houden in plaats van te delen zodat de software leverancier zijn product kan verbeteren.

Twee dingen daarover:

- Het product wordt niet per se veiliger. In de meeste platformen zit het nog vol met onbekende kwetsbaarheden die met een beetje moeite door goede hackers (inlichtingendiensten) te vinden zijn.
- Om effectief te kunnen hacken is het helemaal niet nodig om gebruik te maken van deze 0days. Er zijn bijna altijd wel bekende kwetsbaarheden voorhanden waarmee het ook lukt om binnen te dringen. Dit ervaart Fox IT dagelijks bij het uitvoeren van ethical hacking testen voor onze klanten. Maar ook het hoofd van de hackingunit van de NSA gaf op een hackersconferentie een uniek inkijkje in hun technieken aan dat ze helemaal geen 0days nodig hebben om effectief te zijn.

NSA: We can do it without the zero days. There are so many more attack vectors that are easier, less risky and quite often more productive.

Internationaal / jurisdictie

Doordat hackers hun criminele infrastructuur op een ondoorzichtige manier aan elkaar koppelen weet je als politie niet altijd in welk land je de hack daadwerkelijk uitvoert. Dat maakt het ook niet mogelijk om de bevoegdheid te beperken tot Nederland. In de praktijk zie je dat criminele infrastructuur juist gehuurd wordt in landen waar de politie op basis van samenwerkingsverdragen niet effectief mee kan schakelen.
Zodra de dader en een land in zicht komt, zal de politie moeten schakelen met de lokale autoriteiten op basis van rechtshulpverzoeken op hun onderzoek succesvol te kunnen afronden.

Scoping. Voor welke delicten?

Mijn betoog hiervoor dekt vooral cybercrime en kinderporno delicten. Het hacken door de politie is daarbij een essentieel middel om een zaak rond te krijgen. Hacking moet daarbij vooral gebruikt worden om daders en lokaties in beeld te krijgen en niet zo zeer als surveillance middel. Daarvoor heeft de politie een heel palet aan andere bevoegdheden tot zijn beschikking.

Daarnaast zie ik het als instrument in zeer ernstige zaken. Het Franse voorbeeld van de camera's in de supermarkt is daarvan een voorbeeld. Maar ook bijvoorbeeld het hacken van een forum waarop jihadstrijders overleggen over terroristische activiteiten.

Een derde categorie zou zijn het hacken om cryptografische sleutels te achterhalen. Nu de huidige bewindspersoon, Klaas Dijkhoff, gelukkig het decryptie bevel geschrapt heeft, zal de politie een ander mechanisme moeten hebben om bijvoorbeeld sleutels van harde schijven te achterhalen voordat ze een huiszoeking doen.

Ik vind het belangrijk dat bij elke inzet van dit paardenmiddel een duidelijk omschreven concreet doel vastgelegd wordt. Dus bij het bijvoorbeeld binnendringen in een 'anonieme' computer om zijn echte locatie vast te stellen, moet niet ook gelijk maar een kopietje van de harde schijf gemaakt worden. Alleen als die data niet op een andere manier met minder verdergaande bevoegdheden achterhaald kan worden, zou dat eventueel wel kunnen.

Het toepassen van de hack bevoegdheid moet een laatste redmiddel zijn. Bij cybercrime zaken is dat het al snel, bij andere zaken moet er een serieuze hobbel zijn voordat dit middel wordt ingezet. Hacken is relatief een goedkoop en effectief middel. Maar dat houdt niet automatisch in dat andere middelen die meer resources vragen maar minder ingrijpend zijn, niet eerst ingezet moeten worden.

Afsluitend

Dagelijks wordt onze privacy geschonden door hackers en andere actoren die uit zijn op gevoelige data. Door de politie de hack bevoegdheid te geven, zal cyberspace niet onveiliger worden zoals sommigen zeggen, maar juist veiliger. Het is dan wel belangrijk dat de machtigingen die rechters vooraf ondertekenen nauwkeurig beschreven hebben waarvoor de last verstrekt wordt. Dat vergt mogelijk nog wel wat educatie.