Overheid benadert hackers

'We willen het imago van de AIVD onder hackers verbeteren, misschien kan je daarbij een rol spelen', aldus Hans Turksma van Binnenlandse Zaken of de AIVD.

Augustus 2013, na afloop van de internationale hackersconferentie OHM2013 die in Oudkarspel plaatsvond, heeft AIVD'er 'Hans Turksma' geprobeerd hacker 'Stefan' te benaderen voor een vermoedelijke informantenrol. Stefan was die bewuste maandag niet thuis, maar Turksma dacht kennelijk dat hij zich verstopt had achter de vensterbank en bleef daarom wachten.

"Er stonden fietsen voor de deur en er lag een tas op tafel, er moet dus iemand thuis zijn geweest", vertelde Turksma de volgende dag over de telefoon aan de vader van Stefan, nadat hij eerder die dag voor de tweede maal voor niets had aangebeld bij de woning van Stefan. Aanvankelijk gaf Turksma zich uit voor een medewerker van het ministerie van Binnenlandse Zaken. De vader van Stefan vond dat nogal vreemd. Ambtenaren van Binnenlandse Zaken komen zelden aan de deur bij burgers, áls ze Den Haag al verlaten.

Stefan's vader concludeerde dat de man van de inlichtingendienst moest zijn. Turksma gaf in het telefoongesprek toe dat hij voor de AIVD (Algemene Inlichtingen- en Veiligheidsdienst) werkzaam was, maar niet of hij daadwerkelijk ook Hans Turksma heette (0681704511). Tevens vertelde de AIVD'er dat hij eigenlijk op een positieve missie was. Hij wilde Stefan spreken omdat de AIVD zo'n slechte reputatie heeft onder hackers, daar wil de dienst wat aan doen. De dienst wilde via Stefan in contact komen met hackers "in den lande". Waar Turksma hier precies op doelde, werd niet duidelijk. Later zou blijken dat de dienst ook andere hackers had benaderd, dus had Turksma Stefan daar niet voor nodig. De vader van Stefan beëindigde het korte gesprek met de boodschap dat de AIVD'er hem en zijn zoon niet langer lastig moest vallen.

Na deze mislukte benaderingspoging realiseerde Stefan zich recente voorvallen die mogelijk iets met inlichtingendiensten te maken kunnen hebben gehad. Een familielid was een paar maanden eerder gebeld door een "vriend van Stefan" met de vraag of hij Stefan's mobiele telefoonnummer had. Het familielid vond het maar een vreemde vraag en poeierde de beller af. Tijdens OHM2013 raakte Stefan zijn mobieltje kwijt terwijl hij er zeker van was dat hij die in zijn broekzak had gestopt. Uiteindelijk dook zijn telefoon op in de doos 'Lost and Found' van het festival.

In een tijd van WikiLeaks, de in juni 2013 ontmaskerde informant Sigurdur Thordarson die een jaar lang logs aan de FBI (Federal Bureau of Investigation) doorspeelde, de discussie voor en op OHM2013 over Fox-IT, de openbaarmaking van NSA (National Security Agency)-documenten door Edward Snowden, een politiek actief subkamp (Putting the Resistance back in OHM) en nieuwe al dan niet politieke initiatieven, zullen er regelmatig internetactivisten,

hackers en andere mensen die politiek actief zijn op het internet worden benaderd door de inlichtingendiensten.

Hoe positief de vraag van Turksma wellicht ook moge klinken, inlichtingendiensten hebben nooit eenduidige bedoelingen. Net als de volledige veiligheidsindustrie drijven zij op de angst voor het moslimgevaar, cybercrime, de georganiseerde misdaad en andere loodzware termen, maar zodra het om transparantie, controle, toezicht en verantwoording van diezelfde diensten gaat, blijven ze stil.

Sommige mensen verwarren de AIVD'ers die hackers benaderen met rekruteurs, werkzaam voor het ministerie van Defensie of andere overheidsinstanties. Maar zoals onderstaande chat tussen een medewerker van Defensie en twee reservisten ons laat zien, is de insteek anders. Rekruteurs zoeken naar talenten en binnen de hackersgemeenschap blijkbaar naar mensen die van 'speelgoed' houden. Veel *nerds* zijn weliswaar bekwaam, maar niet voldoende geschoold. Sommige hackers hebben ook een strafblad vanwege het inbreken in systemen of andere vergrijpen. Overheidsinstanties hebben daar moeite mee.

Rekruteurs van Defensie (of andere overheidsinstanties) en personen van de inlichtingendiensten die hackers benaderen, zijn niet inwisselbaar. De eerste benadert je voor een baan, de tweede om te klikken over je vrienden. Bijkomend probleem als je een baan accepteert en een strafblad hebt, is dat je ook chantabel bent. Wantrouwen van de overheid zal dan blijven bestaan, zoals uit de chat blijkt. Het kan zijn dat de MIVD een bewijs van goed gedrag levert, maar in ruil voor wat?

Doel van inlichtingendiensten is het in kaart brengen van gemeenschappen en netwerken. De geworven informant is slechts een minuscuul radertje in het web om de samenleving in kaart te brengen. Medewerkers van de diensten, zoals 'Hans Turksma', maken gebruik van leugens en bedrog om hun werk te rechtvaardigen. Een informant zal daar altijd in meegezogen worden en zijn vrienden en kennissen kwijtraken zodra bekend wordt dat hij of zij heeft geklikt.

Naast Stefan zijn er waarschijnlijk nog meer (waarschijnlijk drie) personen benaderd door de AIVD. Het is goed om de verhalen te delen en anderen te waarschuwen voor de praktijken van de diensten.

(Stefan is een gefingeerde voornaam)

'EEN *CHALLENGE* IS EEN OPTIE'

Chat tussen een medewerker van Defensie en twee 'cyberreservisten'

over het werven van hackers

reservisten: "Er is een groot deel wat niet zal voldoen aan de HBO-eis. Een grote groep MBO'ers heeft echte *skills* die we niet zouden willen missen, hier kunnen we een hoop van leren. Gewenste oplossing: Deze eis laten vallen en werven op basis van te testen competenties door middel van bijvoorbeeld een *cyber challenge*."

Defensie: "Dit is iets waar we over kunnen nadenken. Ik kan me voorstellen dat we HBO-werk en denkniveau vragen voor een cyberreservist, maar een *challenge* is een optie. Daarnaast zien we in het reguliere personeel goede mogelijkheden voor MBO'ers, dus dat is ook een optie. Moet nog verder aan gewerkt worden."

reservisten: "Wat zijn de kaders en doelen van een cyberreservist? De ontvangen info is nog te onduidelijk hier in. Het gaat de meesten niet om het geld, maar om het doel."

Defensie: "De kaders en doelen zijn goed verwoord in de studie cyberreservisten. We zullen hier een samenvatting van maken en die aan het infopakket van het CMI-commando moeten toevoegen."

reservisten: "Het informatiepakket wat ons is gestuurd, bevat info over bijvoorbeeld een AP fixen in Afghanistan zodat uitgestegen troepen met thuis kunnen emailen. Dit klinkt meer als een reservist met ICT-kennis. Omdat deze een paar keer werd genoemd: Er zijn 'goede' hackers met een strafblad. Is het mogelijk dat de MIVD voor bepaalde 'niet-crimineel bedoelde vergrijpen' niet direct een afkeuring geeft?"

Defensie: "Hier kan ik geen uitspraak over doen. Het is nu eenmaal zo dat een strafblad reden is tot het niet toekennen van een verklaring van geen bezwaar voor gegevens tot op de hoogste rubricering. Dat zijn wel de gegevens waarmee personeel binnen cyber mee in aanraking komt. Zal in elk geval op de korte termijn niet opgelost worden."

reservisten: "Toegang tot veel 'speelgoed'/Cyberlab is een voorwaarde wat de mensen prikkelt. Met een knipoog: Een bekende hacker hoopt op het ombouwen van een tank met 19" rackspace. Trainingen d.m.v. CaptureTheFlag events en certificeringen zien mensen als een reden om bij de reservisten te komen. Ook een middel om het nationale veiligheidsbewustzijn te verbeteren."

Defensie: "Voor beide voorgaande punten geldt dat we juist ook reservisten willen gebruiken om deze tools te maken. Uiteraard kijken we ook naar oefeningen waarbij we reservisten in het vakgebied kunnen trainen en daar zijn een lab en de door jou voorgestelde trainingen voor nodig. Ook willen we bijvoorbeeld bij staftrainingen *red teaming* activiteiten ontwikkelen waarbij we wellicht op kwetsbaarheden in onze systemen stuiten. Daarnaast kunnen dit soort activiteiten gebruikt worden om commandanten en hun staf kennis te laten maken met de gevolgen van een cyberaanval

of social engineering, of weghalen van gegevens (niet altijd hoeft vanaf *ground zero* gehackt te worden: informatie zoals toegang en wachtwoord kan ook gegeven worden)."

reservisten: "Sommigen willen ook graag persoonlijk hun ideeën kwijt over de cyberreservist tijdens een BBQ/of een ander event."

Defensie: "Dit is mogelijk op bijeenkomsten van het netwerk. Verder kunnen ideeën natuurlijk altijd gecommuniceerd worden via C-DCEC of via de mail rechtstreeks. Maar zoals je weet is het niet altijd mogelijk rechtstreeks met de Commandant zaken uit te wisselen. Daar zijn momenten voor maar is geen standaard. We zullen wel begin volgend jaar een borrel organiseren met daaraan voorafgaand een soort paneldiscussie voor de 'potentiële' reservisten."