ZWARTE MARKT

Speltheorie in plaats van recht en ethiek

Axel Arnbak

Het was wereldnieuws twee weken geleden, behalve in Nederland. Zerodium, een dubieuze startup die hacking tools verkoopt, publiceerde via techblog Wired ineens zijn prijslijst voor cyberwapens. De prijslijst biedt een verontrustende en fascinerende inkijk in de zwarte handel in nog onbekende kwetsbaarheden in alledaagse software. Kopers met diepe zakken kunnen deze zogenaamde 'zero day' kwetsbaarheden gebruiken om kritieke systemen te hacken.

De bekendste smartphones, browsers, computerprogramma's en besturingssystemen prijken allemaal op de prijslijst. Het geruchtencircuit draaide al op volle toeren, maar nu weet de wereld dat aan een nog onbekende iPhone-kwetsbaarheid een prijskaartje hangt van $ 500.000.

Niemand weet welke bedrijven, overheden, organisaties en criminele bendes actief zijn op de markt voor cyberwapens. Het is zonneklaar dat deze schimmige handel direct aan banden gelegd moet worden. Maar de kopers, waaronder vele Navo-landen, opereren nog te graag ondergronds.

Het businessmodel van bedrijven als Zerodium is simpel. Je kunt een abonnement afsluiten, beginnend bij een half miljoen dollar per jaar en oplopend tot onbekende hoogtes, om toegang te krijgen tot (delen van) hun hacking tools. Met de tools kun je ongemerkt hacken. De prijslijst bevat geen verkoopprijzen, maar de aankoopprijs van Zerodium voor zero day kwetsbaarheden. Die koopt het bijvoorbeeld van cybercriminelen, werknemers van technologiebedrijven of onethische hackers. Hackercultuur schrijft juist voor om zero days openbaar te maken, zodat software-ontwikkelaars hun gaten kunnen dichten. Met een zero day voor Adobe's PDF-reader of webbrowser Chrome kun je $ 80.000 verdienen. Mobiel besturingssysteem Android? $ 100.000 dollar. Kassa.

De schade is immens. Het Italiaanse bedrijf Hacking Team en het Franse Vu-Pen verkochten hun hacking tools aan duistere regimes om politieke dissidenten op te sluiten en bedrijfsspionage te verrichten. Ook Nederland doet mee: de KLPD schafte in 2014 voor € 2,7 mln 16 licenties aan voor de FinFisher hacking tool van het Brits-Duitse bedrijf Gamma, ook gebruikt door de Egyptische en Oegandese collega's. De zwarte handel in cyberwapens heeft ook desastreuze gevolgen voor de cybersecurity op lange termijn: overheden en ethische hackers worden geprikkeld om, in plaats van gaten te dichten, een florerende markt en cultuur voor aanval te laten ontstaan.

Landen kunnen bedrijven die cyberwapens verkopen vervolgen, maar ze doen vrolijk mee aan het spel

Waarom neigen democratische staten naar aanval in plaats van verdediging? In mijn proefschrift, dat ik vorige week verdedigde, som ik een aantal redenen op. De meest beangstigende is dat waar het recht en ethiek niet bestaan, speltheorie de overhand neemt. In het recente artikel 'Timing of Cyber Conflict' laat de invloedrijke speltheoreticus Axelrod — die ook gezaghebbende analyses maakte van de inzet van nucleaire wapens — zien dat staten zero days zo snel mogelijk zullen inzetten. Voordat het nog onbekende lek is gedicht. Daarom laten staten op de korte termijn cyberoorlog escaleren.

Joost mag weten hoeveel inlichtingen- en politiediensten, dictators en cybercriminelen geabonneerd zijn op de hacking tools van Zerodium cum suis. Want behalve Zerodium, dat de prijslijst publiceerde, zullen de meeste bedrijven buiten de publiciteit willen blijven. Dat democratische landen zich mengen in zulke zwarte markten legitimeert hun businessmodellen. De beer, of de zwarte markt, is dus los.

Europese landen kunnen op basis van hun cybercrime-wetgeving de bedrijven mogelijk strafrechtelijk vervolgen, maar doen ondergronds mee. In een ideale wereld zouden landen als Nederland en Zweden, die in hun buitenlandbeleid cyberpeace prediken en in deze wapenwedloop toch niet meekunnen, het voortouw nemen en cybersecurity een enorme dienst bewijzen. Zoals het net aangekondigde klimaatfonds van $ 100 mrd, kan een onafhankelijke fonds gesticht worden om alle kwetsbaarheden op de markt op te kopen en direct te publiceren. Zo kan iedereen zijn gaten dichten.

Verbied en vervolg daarop meteen de zwarte handel in kwetsbaarheden en breng cyberwar binnen het domein van de rechtsstaat. Maar goed, aan zulke idealistische oplossing kleven duizend haken en ogen. In het cyberdomein zijn we vooralsnog overgeleverd aan de wetten van de speltheorie.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IVIR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak.