Handel in geheime digitale lekken

Prins, J.E.J.

Published in:
Nederlands Juristenblad

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

Geheime handel in digitale lekken

17 Vorige maand maakte het Europese Hof van Justitie duidelijk dat de bevoegdheid van opsporingsinstanties om zgn. verkeersgegevens op te kunnen vragen (met welk telefoonnummer wordt naar welk nummer gebeld, vanaf welke locatie en hoe lang?) op proportionele wijze moet worden ingezet.[1] Het Hof stelde vast dat het vergaren van verkeersgegevens weliswaar kan bijdragen aan het bestrijden van zware criminaliteit en terrorisme, maar dat de wijze waarop dat nu gebeurt in strijd is met de eis van proportionaliteit. In commentaren werd er direct op gewezen dat de uitspraak past in een omslag van denken over het belang van privacy. Maar op min of meer hetzelfde moment dat het Europese Hof het privacybelang weer in het zadel hees, werd duidelijk dat de Amerikaanse NSA jarenlang gebruik heeft gemaakt van een internet-beveiligingslek genaamd Heartbleed. In plaats van het bij relevante partijen te melden, zodat deze de nodige aanpassingen in de systemen konden doorvoeren, bleef men heimelijk door de opening meegluren en schond daarmee wereldwijd de privacy van velen.

Het bericht kreeg ruim media-aandacht. Maar wie bekend is met de wereld waarin bedrijven als Vupen (vupen.com) en ReVuln (revuln.com) opereren, was niet verrast. In deze wereld wordt dik geld verdiend met handel in beveiligingslekken. De minimumprijs voor een zgn. zero-day exploit ligt rond de 50.000 dollar. Kort samengevat is een zero-day exploit een software-applicatie die speciaal is ontwikkeld om misbruik te maken van een beveiligingslek bij bijvoorbeeld een internetdienst. Met behulp van een zero-day exploit valt het ICT-systeem binnen te dringen zonder dat de aanbieder van dit systeem daar weet van heeft. Kortom, wie de beschikking heeft over een exploit kan heimelijk observeren, gegevens aftappen, virussen installeren, etc. De term zero-day exploit is afgeleid van de leeftijd van de software-applicatie die het lek benut. Inherent aan de applicatie is namelijk dat deze het lek misbruikt vóór de eerste dag (dus dag 0) dat de aanbieder van het systeem zich bewust wordt van het lek. Vanaf dat moment heeft deze aanbieder immers de kans een herstelapplicatie voor het lek naar gebruikers te distribueren en is de exploit niets meer waard.

Over de handel in zero-day exploits is weinig bekend, maar een lezenswaardige analyse van Reuters over deze schemerige markt maakt duidelijk dat inlichtingendiensten tot de belangrijke afnemers behoren.[2] Interessant is ook de maffia-achtige opstelling (van twee walletjes eten) van diverse aanbieders[3]: ze profileren zich als verdedigers tegen gevaarlijke exploits, maar ontwikkelen tegelijkertijd zelf exploits om ze aan te bieden vanuit de (al dan niet commercieel ingegeven) houding 'als je niet betaalt, zetten we de deur bij je open'.

De economische en sociale afhankelijkheid van verknoopte digitale systemen in combinatie met de groeiende onzekerheid over cyberterreur en digitale 'oorlogsvoering', brengt zowel veiligheidsdiensten als defensie tot voorheen onbekende strategieën. Of en in welke mate, zero-day exploits tot het nieuwe instrumentarium behoren, is onduidelijk. Het vorige week gepresenteerde AIVD-Jaarverslag rept er met geen woord over. Maar uit de brief die de minister van Defensie op 17 maart j.l. naar de Tweede Kamer zond valt op te maken dat "het ontwikkelen van het vermogen om offensieve cyberoperaties uit te voeren" een speerpunt vormt in de Defensie Cyber Strategie.[4] Ze vervolgt: "Offensieve cybercapaciteiten zijn de digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten. De inzet valt onder het desbetreffende mandaat en de geldende *Rules of Engagement*. De juridische kaders zijn niet anders dan die voor de inzet van conventionele middelen."

Mocht ook ons land zero-day exploits inzetten, wat impliceert de simpele vaststelling dat de "geldende *Rules of Engagement*" van toepassing zijn dan precies? Welk beoordelingskader hanteert men, nu de inzet van zero-day exploits per definitie de veiligheid van burgers en bedrijven op het spel zet? Volgens voormalig cyber-security adviseur van de regering Obama, Clarke, benut de Amerikaanse overheid zero-day exploits zonder een solide beoordelingskader.[5] Natuurlijk zijn criteria hier ontzettend lastig te formuleren, maar welke argumenten liggen dan in een concrete situatie ten grondslag aan de keuze om kennis over een lek in te zetten voor een offensieve strategie (het lek benutten om handelen van tegenstanders te beïnvloeden) of juist een defensieve (voorkomen dat kwaadwillenden het lek benutten en aanbieders waarschuwen)? En hoe transparant kan en wil men zijn over de mate waarin dit middel wordt ingezet?

Het hoofd van de AIVD, Bertholee, stelt in zijn voorwoord bij het Jaarverslag 2013: "We zijn een geheime dienst, maar we willen niet geheimzinnig zijn. Onze taken en bevoegdheden zijn vastgelegd in de wet, over ons handelen wordt in het openbaar verantwoording afgelegd. Dit jaarverslag is daarvan een onderdeel. Slechts een gedeelte van ons handelen is geheim en dat is ook met reden: om bronnen te beschermen of om te voorkomen dat onbevoegden kennis nemen van onze activiteiten. De controle op dat geheime deel van ons werk is gelukkig ook goed belegd." Mogelijk valt de inzet van zero-day exploits onder het geheime deel van het werk van de AIVD en ook Defensie. Daar zullen dan goede redenen voor zijn. Tegelijkertijd mag de samenleving erop vertrouwen dat ook bij dit nieuwe instrument de controle op de inzet en de afwegingen goed, en dus zoals het een rechtsstaat betaamt, functioneert.

Corien Prins

1. http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=313923
2. http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews
3. Zie voor een overzicht van deze bedrijven: http://wikileaks.org/the-spyfiles.html
4. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/03/17/kamerbrief-over-offensieve-cybercapaciteit-defensie.html
5. http://in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews