INTERNETKANON

Hoe slimme apparaten aanvallen

Axel Arnbak

Het is een tijdje stil geweest rondom DDoS-aanvallen. Een paar jaar terug waren websites van Nederlandse bedrijven, overheidsinstanties en maatschappelijke organisaties geregeld onbereikbaar door 'Distributed Denial of Service-attacks': het overbelasten van een website door tienduizenden aanvragen per milliseconde. Internetbeveiligers weten DDoS-aanvallen steeds beter te pararen, maar de recente — en in Nederlandse media onbesproken — cyberaanval op de website van cybercrime-journalist Brian Krebs geeft reden tot alarm. De krachtigste DDoS-aanval ooit waargenomen gebruikt namelijk het internet der dingen als internetkanon.

Voor het uitvoeren van een geslaagde DDoS-aanval moet je eerst beschikken over een netwerk van slecht beveiligde computers die samen een webserver kunnen overbelasten met aanvragen. Je kunt zelf een DDoS-netwerk bouwen, door het internet af te scannen naar lekke computers en daar malware op te installeren. Je kunt het ook aanschaffen op duistere internetfora, bijvoorbeeld bij cybercrime-syndicaat vDOS.

Nadat Krebs drie verhalen op zijn website gepubliceerd had over vDOS, opende het syndicaat prompt de aanval op zijn website. Deze aanval was qua bandbreedte veel groter dan het record tot dan toe. vDOS gebruikt als cyberwapen het internet der dingen, dat inmiddels uit miljarden slecht beveiligde huis-tuin-en-keukenapparaten bestaat. Krebs is aangevallen door circa 120.000 webcams, routers en printers. Het Franse internetbedrijf OVH claimde kort daarna ook door vDOS geraakt te zijn, door 150.000 apparaten. vDOS kon de 'slimme' apparaten kinderlijk eenvoudig hacken omdat de fabrikanten de internetdingen uitrusten met standaardwachtwoorden als 'admin' en '12345'.

DDoS-aanval

Wordt uitgevoerd met netwerk van simpel te hacken computers

Nieuw alternatief

Inschakelen van webcams, routers en printers

Slecht beveiligd

In het internet of things zijn deze apparaten slecht beveiligd

Alleen internetkrachtpatsers als Google en Akamai kunnen zulke grote aanvallen omleiden en afslaan. Alleen staten en grote bedrijven kunnen hun rekeningen betalen. De rest van ons moet hopen dat de internetverkeersleiders tijd en zin hebben om ons te beschermen. Akamai ondersteunde Krebs pro bono, maar moest al snel de handdoek in de ring gooien. De dienstverlening aan betalende klanten kwam namelijk in gevaar. De website van Krebs ging meteen kopje-onder, maar via vriendjes bij Google kwam hij snel weer online. Voor journalisten en organisaties die niemand bij Google kennen en, zeg, in een totalitair regime over corruptie of de onderdrukking van vrouwen publiceren, ligt dat anders. Hun afhankelijkheid van Akamai en Google is geen garantie voor hun vrije meningsuiting. Het internet der dingen geeft zo een impuls aan DDoS-aanvallen als krachtig wapen voor censuur.

De spectaculaire aanval geeft ook reden tot ernstige zorgen over cybersecurity. vDOS kan het internetkanon ook op internetdingen zelf richten. Dan staat het leven van een ceo in een connected car, de politicus aan een verbonden hartpomp of de volkswijk achter de genetwerkte watersluis op het spel. Zoals eerder betoogd op deze plek, en uitmuntend onderzocht en opgeschreven door Maurits Martijn en Dimitri Tokmetzis in hun bestseller *Je hebt wél iets te verbergen*, is een internet der dingen zonder robuuste beveiliging onverantwoord.

De oplossingen lijken simpel. 'Slimme' apparaten moeten aan hoge beveiligingsvereisten voldoen en up-to-date blijven. Maar de digitale wereld is al overspoeld met onveilige internetapparaten, die vDOS van digitaal kruit voorzien. Die apparaten kunnen moeilijk van de markt worden gehaald. Wetgeving, toezicht, zelfregulering door de sector, zelfs een keurmerk voor het internet der dingen is nog niet op de horizon. En als de DDoS-problematiek aanzwelt, moet het afwentelen ervan een overheidstaak zijn. Paradoxaal genoeg komt onlinecensuurbestrijding dan in overheidshanden. De gemarginaliseerde organisatie in een totalitair regime is bovendien niet geholpen bij deze aanpak.

Het medicijn tegen krachtige cyberwapens is dus theoretisch eenvoudig en praktisch complex. Niets doen is geen optie. vDOS heeft met een oorverdovend kanonschot de DDoS-stilte doorbroken. Makers van beleid en internetdingen moeten nu beveiliging prioriteren, voordat de vrije meningsuiting en de veiligheid van internetgebruikers nog meer schade ondervinden.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak