Massale cyberaanvallen aanpakken met regulering softwaremarkten

WannaCry-gijzelsoftware niet bestrijden met meer geld en spionagebevoegdheden

Axel Arnbak

ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIEELE DAGBLAD

Nadat ziekenhuizen, fabrieken en ministeries wereldwijd dagenlang waren getroffen door een mondiale cyberaanval, is het grootste gevaar van het WannaCry-virus geweken. Nu rijst natuurlijk de vraag hoe we de volgende cyberstorm voorkomen en wie verantwoordelijk is voor schade. In onze informatiesamenleving ontstaat in rap tempo een digitaal kerkhof van miljarden onveilige internetapparaten: niet alleen pc's, maar ook webcams, fabrieksmachines, MRI-scanners en andere internetdingen. Zo'n digitaal kerkhof is het doelwit én het instrument van cybercriminelen en dat poets je niet weg met spionagebevoegdheden en geld. Leveranciers moeten internetapparaten veilig op de markt brengen en houden. Tijd voor softwareregulering.

WannaCry beheerste een paar dagen wereldwijd het nieuws, maar grootschalige ransomware-aanvallen, DDoS-blokkades van internetbankieren en spamtsunami's van Nigeriaanse prinsen teisteren de digitale wereld al decennialang. Experts zien in het WannaCry-incident niet iets nieuws, alleen een bevestiging dat de schaal en de impact van zulke aanvallen toenemen.

In de jaren 80 en 90 waren cyberaanvallen vooral het product van hobbyhackers die opschepten over hun kunsten of leveranciers wilden dwingen de gapende gaten in hun software te repareren. Sinds de internetexplosie medio jaren 90 zijn serieuze cybercrime-syndicaten ontstaan die miljoenen buitmaken met gestolen creditcardgegevens en gijzelsoftware. Met de opkomst van het 'internet der dingen' richten zij hun pijlen niet alleen op data, maar ook op de fysieke wereld. WannaCry legde de productielijn van Renault, het Spaanse Telefónica en hartpompen in Britse ziekenhuizen lam. Naast doelwit, zijn deze kwetsbare internetapparaten ook het aanvalswapen van cybercrime. Als een griep verspreidt cybercrime zich juist via slecht beveiligde internetdingen.

Connectiviteit en cybercrime gaan dus al decennia hand in hand, maar de beveiligingsvereisten voor software blijven steevast achter. Al jarenlang mogen leveranciers miljarden onveilige webcams, ijskasten en auto's op de markt brengen en bestaat er geen harde juridische verplichting hun software up-to-date te houden. Juist in het internet der dingen zijn structurele software-updates, het belangrijkste wapen tegen massale cyberaanvallen, niet de regel maar de uitzondering. Bij gebrek aan wetgeving geldt namelijk de tucht van de markt van netwerktechnologie: zo snel mogelijk een halfbakken product lanceren en gebruikers aan je platform binden, en daarna misschien de beveiligingslekken dichtplakken met updates. Maar zulke updates zijn geen verplichting, soms onmogelijk en voor gebruikers vaak vermoeiend. En zo is een mondiaal kerkhof van miljarden digitale zombieapparaten ontstaan dat een gevaar vormt voor zichzelf en de gehele digitale omgeving.

Kwetsbaarheid zit in de onveilige software van internetapparaten zelf

Na cyberaanvallen hoor je altijd weer dezelfde cyberconsultants in de media pleiten voor 'meer geld' (dus meer opdrachten) of traditionele veiligheidsexperts, zoals Ko Colijn van Clingendael, voor inlichtingendiensten die continu het hele internet afluisteren om cyberboeven te vangen (NRC 15 mei). Dat plan is door de decentrale en open opzet van internet niet alleen technisch onuitvoerbaar, maar ook de kernbom onder onze grondrechten en de grootste wens van dictators. Beide schijnoplossingen poetsen het mondiale digitale kerkhof niet weg.

De kern van de kwetsbaarheid zit in de onveilige software van de internetapparaten zelf. Kersverse cybersecuritywetten uit Brussel en nu in behandeling in de Eerste Kamer verplichten 'kritieke infrastructuren' als energiebedrijven, (lucht)havens en banken in vage termen IT-systemen op orde te hebben. Maar zij zijn slechts afnemers van IT. Recht en beleid moeten voor IT-leveranciers veiligheidsnormen, updateverplichtingen en aansprakelijkheid bij verwijtbare fouten voorschrijven. Uiteraard is tolerantie voor complexiteit en ademruimte voor innovatie essentieel. Als het digitale kerkhof maar wordt opgeruimd. De markt produceert niet als vanzelf cybersecurity en de aanvallen nemen in schaal en ernst toe.

Cybersecurity is geen technisch probleem, maar een vraagstuk van marktordening. Leveranciers hebben onvoldoende marktprikkels om software veilig te krijgen en te houden. Cybersecurity is een publiek goed en het mondiale digitale kerkhof een uitwas van marktfalen. Meer geld voor overlegclubs en spionnen maken onze informatiesamenleving niet veiliger, scherpere internationale regulering van softwarekwaliteit wel.

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