

50 jaar internet: tijd voor herziening

Het internet is een wereldwijd netwerk van computernetwerken, waarvan onze maatschappij steeds meer afhankelijk is. Enkele fundamentele ontwerp-problemen gaan nu steeds meer opspelen. Cristian Hesselman (SIDN Labs) en Jesse Robbers (Quantum Delta NL) nemen ons mee in de belangrijkste uitdagingen.

Door **Amanda Verdonk**

We staan er niet bij stil als we een e-mail verzenden, een Instagrambericht plaatsen, op een website klikken of Spotify of Netflix streamen. Maar op al die momenten schieten er razendsnel datapakketjes heen en weer tussen ons *device* en dataservers waar dan ook ter wereld. Internetinfrastructuur zorgt ervoor dat al dat dataverkeer mogelijk is. De infrastructuur bestaat niet alleen uit de hardware zoals kabels, antennes en serverkasten, maar ook uit een onzichtbare tussenlaag van software. Die tussenlaag is in feite het echte internet: een netwerk van aan elkaar gekoppelde computernetwerken die volgens afgesproken protocollen informatie uitwisselen.

Er wordt veel gesproken over problemen op het internet, bijvoorbeeld op het gebied van privacy en *fake news*. Maar meestal gaan die problemen – en de mogelijke oplossingen – over diensten zoals sociale media die gebruikmaken van internet. Dat neemt niet weg dat ook die tussenlaag, de internetinfrastructuur, aan herziening toe is zodat het beter aansluit bij nieuwe maatschappelijke behoeften, zoals meer digitale autonomie.

“Aan het basisontwerp is weinig veranderd en dat wordt in toenemende mate een probleem”

Uit de hand gelopen

Het oorspronkelijke internetontwerp stamt uit begin jaren zeventig, vertelt Cristian

Hesselman, directeur van SIDN Labs. “Het internet werd toen vooral op universiteiten gebruikt, bijvoorbeeld voor het versturen van berichten of gezamenlijk gebruik van apparatuur. Beveiliging was toen nog geen punt, want iedereen kende elkaar.” Die paar universiteitscomputers zijn inmiddels in 50 jaar tijd uitgegroeid tot meer dan 70.000 aan elkaar gekoppelde netwerken wereldwijd, die in Nederland in beheer zijn bij bedrijven zoals KPN, T-Mobile en VodafoneZiggo. Al die tijd is er aan het basisontwerp weinig veranderd. En dat wordt in toenemende mate een probleem, omdat steeds meer kritische toepassingen aan het internet gekoppeld worden. Denk bijvoorbeeld aan energienetwerken, auto's, medische apparatuur, fabrieken, drinkwaterinstallaties en bruggen. Zulke diensten vereisen een betrouwbare internetinfrastructuur die de aanbieders van deze diensten meer grip biedt op hoe ze data over het internet kunnen versturen (*data in transit*).

Maar het internet is zodanig ontworpen dat het zelf besluit hoe de datapakketjes door de netwerken reizen. Het kiest de kortste route, met zo min mogelijk tussenliggende netwerken, en stuurt de data automatisch via een andere route als ergens een storing optreedt. Dat is een handige eigenschap, maar het betekent wel dat die routing en gebruikte netwerken een *black box* zijn. En dat is een fundamenteel probleem, aldus Hesselman. “De netwerken veranderen continu. Er kan bijvoorbeeld een kwetsbaarheid in de netwerksoftware

Weergave van een deel van het internet netwerk in 1990

ontstaan of routes kunnen onverwacht via gebieden met een andere rechtsmacht lopen die de zender van de data niet vertrouwt. Spanningen tussen landen kunnen een rol spelen. Zo is er nu discussie over vermeende kwetsbaarheden en risico op spionage als telecombedrijven in Europa 5G-apparatuur van Chinese bedrijven installeren.”

Lacune

Volgens Hesselman moeten beheerders van kritische toepassingen dan ook meer inzicht in en controle over de infrastructuur krijgen om hun digitale autonomie te vergroten. Net zoals je een postpakketje kunt tracken en traceren, zo zou je met behulp van certifi-



Cristian Hesselman is directeur van SIDN Labs, een onderzoeksteam dat tot doel heeft de betrouwbaarheid van de internetinfrastructuur te vergroten. SIDN Labs is onderdeel van SIDN, de operator en beheerder van het .nl-domein. Daarnaast is hij universitair hoofddocent aan de Universiteit Twente en voorzitter van het bestuur van NLnet Labs.

cristian.hesselman@sidn.nl

caten of *tokens* ook de route van het dataverkeer beter moeten kunnen traceren. Beheerders kunnen op basis van die informatie kiezen om bepaalde routes die ze niet vertrouwen niet te gebruiken. “Als je weet welke partij jouw data afhandelt, kun je kijken naar het beveiligingsniveau, de locatie, de jurisdictie en de gebruikte software. Is die bijvoorbeeld *open source* (vrije toegang tot en inzage in de broncode, red.) en zijn er geen ‘achterdeurtjes’?” Om traceerbare en controleerbare datastromen mogelijk te maken is SIDN Labs verbonden met SCION, een experimentele internetinfrastructuur van de technische universiteit ETH Zürich in Zwitserland. Daar is *open source* software ontwikkeld die de gebruiker meer controle geeft over de te gebruiken netwerken. De software wordt al in een testomgeving gebruikt bij netwerkbeheerder Swisscom en enkele banken en ambassades. Maar de ontwikkeling bevindt zich nog in een pril stadium. Hesselman: “Er is nog heel weinig Europese aandacht voor de internetinfrastructuur, dat is een lacune. Net als *Responsible AI*, waarmee je meer inzicht krijgt in de beslissingen van algoritmes, zou ook een *Responsible Internet* op de agenda moeten komen.”

Inherent veilig

Met alleen een beter traceerbaar internet zijn we er nog niet. Op dit moment wordt gewerkt met encryptie- of versleutelingstechnieken die over een aantal jaren niet meer houdbaar zijn. Dat heeft te maken met de komst van de quantumcomputer. Zulke supercomputers bestaan nu nog niet, maar er



Jesse Robbers is medeoprichter en directeur van Quantum Delta NL, een samenwerkingsverband ter bevordering van de ontwikkeling van quantumtechnologie in Nederland. Ook is hij senior consultant bij TNO op het gebied van digitale infrastructuur.

jesse.robbers@quantumdelta.nl

wordt hard aan gewerkt en de verwachting is dat ze over tien tot vijftien jaar in bedrijf zullen zijn. Quantumcomputers werken met quantumbits (qubits) die meerdere posities kunnen aannemen en tegelijk 0 en 1 kunnen zijn. Hierdoor hebben ze veel meer rekenkracht dan gewone computers en kunnen ze de huidige versleuteling kraken. Dat is een grote zorg. Niet alleen voor de toekomst, maar nu al, meent Jesse Robbers, directeur van QuantumDelta NL. “Versleutelde data van bijvoorbeeld overheden of banken kunnen nu al worden afgeluisterd en opgeslagen, ook al is die informatie nog niet toegankelijk. Met behulp van quantumcomputers wordt die informatie in de toekomst wel toegankelijk en kunnen bijvoorbeeld staatsgeheimen of bankgegevens uitlekken.” Daarom wordt er nu al gewerkt aan Quantum Key Distribution. De verzender en ontvanger krijgen beide een unieke sleutel bestaande uit qubits die onstabiel worden als je ze probeert te onderscheppen. Dat maakt het systeem inherent veilig.

“Quantuminternet heeft veiligheid én snelheid als belangrijkste troeven”

De volgende stap is een geheel netwerk dat draait op qubits, oftewel een quantuminternet. Onlangs werd daarvoor in Delft weer een belangrijke stap gezet, toen wetenschappers voor het eerst een quantuminternetverbinding tussen drie locaties tot stand wisten te brengen. Quantuminternet heeft veiligheid én snelheid als belangrijkste troeven. Die snelheid maakt het mogelijk om enorme hoeveelheden informatie te versturen, veel meer dan nu mogelijk

is. Robbers: “Doordat de quantumbits verstrengeld zijn, hebben ze aan beide zijden dezelfde status. Daardoor hoef je waarschijnlijk niet gehele datasets te versturen, maar slechts delen.” Vanwege veiligheidsoverwegingen zullen overheden en banken tot de eerste gebruikers behoren, verwacht Robbers. Wetenschappers en bedrijven die werken met complexe datamodellen zullen snel volgen. “Denk aan het ontwikkelen van nieuwe klimaatmodellen, medicijnen of chemische formules. Dat zijn toepassingen die extreem veel rekenkracht vereisen.” Deze ontwikkeling zal zich grotendeels op de achtergrond voltrekken, want Robbers verwacht dat er geen schop voor in de grond hoeft. Naar verwachting kunnen ook de huidige glasvezelkabels de qubits transporteren. Over enkele jaren verwacht hij dat de eerste quantumnetwerken al in bedrijf zullen zijn. Ook nu zullen de universiteiten, net als vijftig jaar geleden, tot de eerste gebruikers behoren.

Onzichtbaar

Burgers merken voorlopig nog niets van de technische ontwikkelingen naar een traceerbaar, veiliger en sneller (quantum)internet. Al denken zowel Hesselman als Robbers dat dat op termijn wel zal gebeuren. Robbers: “Quantumtechnologie zal uiteindelijk ook de huishoudens in kruipen. Denk bijvoorbeeld aan de beveiliging van data uit slimme thermostaten of zelfrijdende auto’s die met het internet zijn verbonden. Maar dan zijn we wel tien of twintig jaar verder.” Volgens Hesselman moeten gebruikers meer grip op hun data krijgen. Ze moeten niet alleen kunnen zien wie hun data transporteert, maar ook waar deze staat en wat ermee gebeurt. “Als je een apparaat bij de Mediamarkt koopt zou daar een bijsluitertje bij moeten zitten. Daarop staat dan welke informatie het apparaat verstuurt, naar welke locatie en met welk doel. Slimme apparaten worden namelijk steeds onzichtbaarder, waardoor je op een gegeven moment niet eens meer weet waar ze zitten. Misschien wel in de deurklink of in de vloer van je badkamer. Meer autonomie over onze data is cruciaal voor het vertrouwen van organisaties, overheden en burgers in onze digitale infrastructuur.” •



Kijktip!

Wie heeft het internet uitgevonden? En waarom? De internethistorie in een notendop.

<https://youtu.be/21eFwbb48sE>