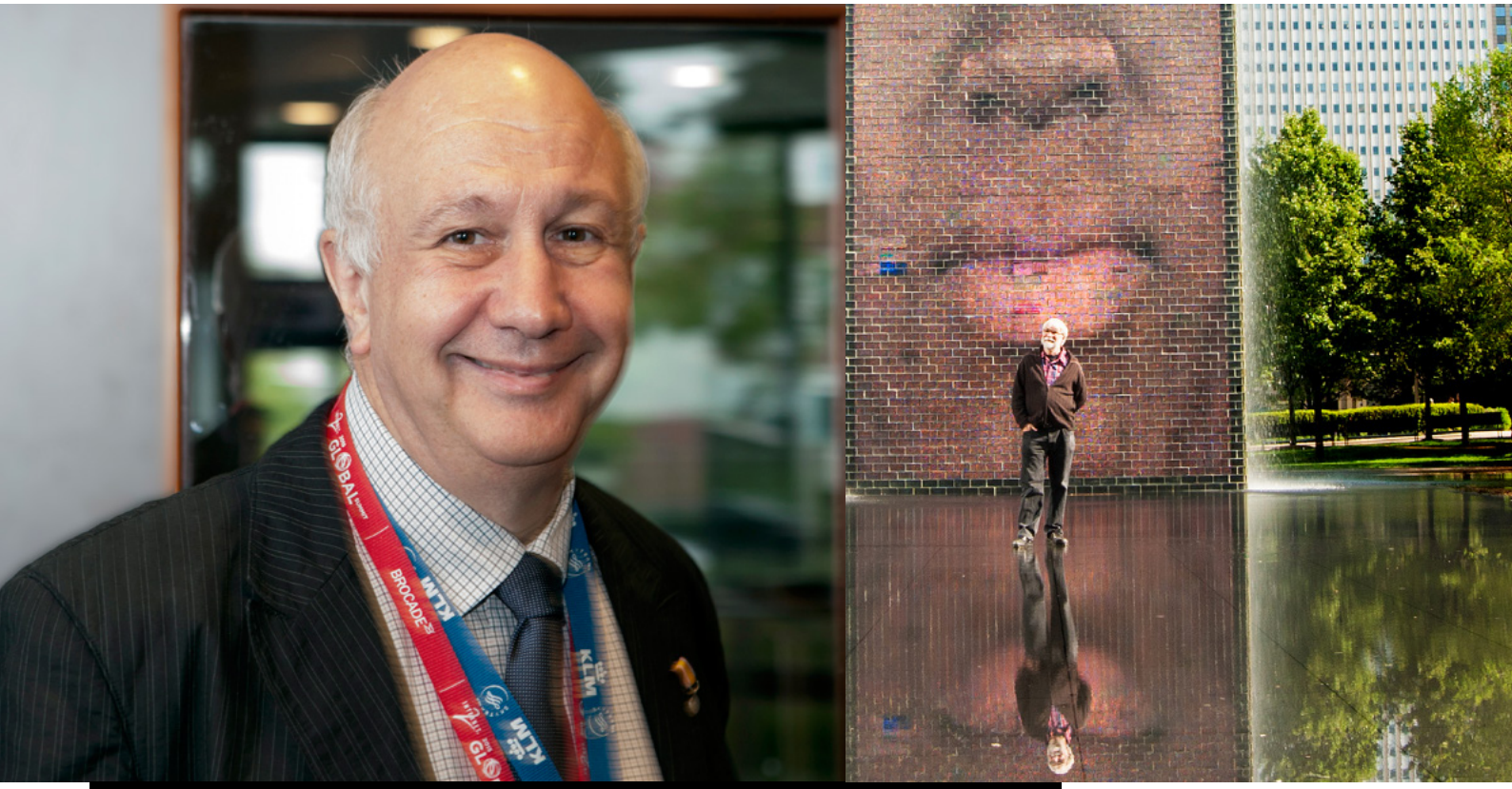
Virtuele en programmeerbare netwerken kunnen zichzelf steeds zodanig aanpassen dat ze cyberaanvallen kunnen ontwijken, terwijl de functionaliteit behouden blijft. Een aanval op een website krijgt daardoor het effect van een zwaarddans; het netwerk pareert elke aanval door hem elegant te ontwijken. Naast nieuwe technologie vereist deze benadering organisatorische samenwerking en juridische oplossingen. Het SARNET-project gaat deze uitdagingen aan, vertellen Cees de Laat en Leon Gommans. *Door Leendert van der Ent*

Het netwerk als zwaarddanser



Leon Gommans, KLM (links) en Cees de Laat, UvA (rechts) werken samen binnen SARNET.

Rond internet zijn twee tegengestelde trends gaande. Enerzijds communiceren bedrijven en overheid steeds meer via internet. Anderzijds ondermijnen internetcriminaliteit en storingen in al hun verschijningsvormen in toenemende mate het vertrouwen van burgers en consumenten in datzelfde internet. Is de site die ik zie wel de echte webshop? Komt deze mail wel van de bank? Cees de Laat, hoogleraar Systeem- en Netwerkengineering aan de Universiteit van Amsterdam: 'De leden van het SURF Computer Emergency Response Team (SURFCERT) bij de UvA zien bij universiteiten en de overheden tientallen grote en tienduizenden kleine incidenten per jaar langskomen. Dit varieert van virusbesmettingen en wachtwoordhacks tot grote botnets.' >>

Leon Gommans: 'Het gaat ons bij cyber security niet om patenten, maar om kennisdelen om tot efficiënte en kosteneffectieve beveiligingsstrategieën te komen.'

Cees De Laat, UvA

Cees De Laat: 'Je kunt een aanval het beste meteen afhandelen zodra hij in de vorm van kleine stroompjes data bij de internetdienstverlener binnenkomt.'

Het aantal incidenten neemt toe en de aanvallen worden steeds geraffineerder. 'Er is een bewapeningswedloop tussen aanvallers en verdedigers aan de gang,' schetst De Laat. 'Daarbij observeren de 'goeden' tegenwoordig steeds meer details van aanvallen, worden er systemen getest en vinden ze zo nu en dan zelfs informatie over nieuwe potentiële hacks, die soms ook weer uitlekt naar de 'bad guys'. Zo is er een continue strijd gaande met steeds verfijndere maatregelen en tegenmaatregelen. Daarbij krijgen de 'slechten' via cloud providers tegenwoordig gemakkelijk en goedkoop toegang tot grote capaciteit en infrastructuren om hun aanvallen uit te voeren; de *hack as a service*.'

Daarom is het belangrijk om technologie te ontwikkelen die vandalisme en criminaliteit terugdringt en het vertrouwen in het medium internet bij gebruikers weer kan versterken. Security Autonomous Response in programmable Networks (SARNET) is één van de gehonoreerde projecten uit de tweede door NWO-EW georganiseerde cyber security research call die daarvoor moeten zorgen. Nederland heeft een relatief groot belang op dit gebied, omdat we een goede internetinfrastructuur hebben en een groot internetknooppunt. Die koppositie brengt ons land wereldwijd helaas ook op de vierde plek in de ranking van slachtoffers door cybercriminelen.

Manipuleerbaar Netwerk

De Laat: 'SARNET neemt een bijzondere plek in binnen het geheel van monitorings-, detectie- en bestrijdingsprojecten. Wij willen technologie voor programmeerbare en virtualiseerbare netwerken gebruiken om ervoor te zorgen dat bijvoorbeeld tijdens een DDoS-aanval met bots op een website de functionaliteit overeind blijft. Het algemene uitgangspunt daarbij is dat alle elementen van een netwerk programmeerbaar moeten zijn. Dat is nog niet het geval, zo'n systeem moeten we de komende jaren daadwerkelijk gaan ontwikkelen. Daarbij moet het netwerk zichzelf softwarematig kunnen aanpassen, bijvoorbeeld door

zaken op te schalen en te verplaatsen, waardoor het een aanval geautomatiseerd kan ontwijken. In het model dat wij voor ons zien wisselt een conglomeraat van gebruikers en dienstverleners daarbij informatie uit die een georkestreerde tegenreactie mogelijk maakt.'

In deze benadering komen drie aspecten samen, elk de basis voor een eigen promotie-onderzoek. Het eerste aspect is zorgen dat het netwerk onafhankelijk van hardware reageert, zoals een drone die obstakels ontwijkt, maar het doel in het oog blijft houden. Het tweede aspect is om te achterhalen wat er gaande is om vervolgens geautomatiseerd op basis van een kosten-batenanalyse het beste antwoord op de aanval te bepalen – en dit geselecteerde antwoord uit te voeren.
Het derde aspect ligt op de grens van agent-technologie en rechten. Toepassing van de strategie vraagt om samenwerking tussen de verschillende netwerk- en cloudproviders in de keten en gebruikers. Hoe organiseer je het zo, dat partijen elkaar zodanig vertrouwen dat ze het afwegingsmechanisme in hun operatie willen invoeren? Bij dit deel van het project is hoogleraar Juridisch Kennismanagement Tom van Engers van het Leibniz Center for Law van de UvA betrokken. Naast de UvA doen ook netwerkspecialist Ciena, TNO en KLM als projectpartners mee in het project.

Grote stroom voorkomen

KLM is één van de bedrijven die in de praktijk de impact van een aanval hebben ondervonden. Voor de duidelijkheid: het gaat niet om vliegtuig-gerelateerde zaken, maar om 'denial of service' van hun diensten aangeboden via de website. In 2013 legde een DDoS-aanval de KLM-website, waarmee reizigers onder meer tickets boeken en inchecken voor hun vlucht, een tijdje plat. 'Iedere minuut dat een dergelijk cruciaal systeem offline is, betekent ongemak voor onze klanten, extra kosten, reputatieschade en omzetverlies,' zegt Leon Gommans van KLM.

Een dergelijk groot bedrijf heeft 24/7 een Operations Team paraat. Zo'n team moet bij een aanval eerst op basis van sporenanalyse en verkeerspatronen uitzoeken om welk van de vele mogelijke soorten aanvallen het gaat. Vervolgens moet het de verdedigingsstrategie bepalen: bijvoorbeeld andere firewall- en netwerk-configuraties toepassen om zo de aanval om te leiden naar een zwart gat. Gommans: 'Dat is arbeidsintensief en gaat relatief langzaam – zowel de analyse als de beantwoording van zo'n aanval kost een aantal uren. Het is veel efficiënter als je dat kunt automatiseren.'

Nog veel handiger is het als niet elke partij afzonderlijk zo'n verdediging opzet, maar als alle partijen in een keten samenwerken om dit te doen, vindt hij. De Laat vult aan: 'Op een hoger niveau heeft een aanval de vorm van kleine stroompjes data die bij de internetdienstverlener via de randen binnensijpelen. Pas bij de voordeur van het bedrijf waarop de aanval gericht is, komen die stroompjes samen om één grote klomp te vormen. Zo'n klomp is veel moeilijker te keren dan de kleine stroompjes die bij de randen via de firewalls doorsijpelen. Je kunt een aanval dus het beste 'upstream' afhandelen.'

'Het model voor ketensamenwerking dat SARNET voorstelt,' zegt De Laat, 'is ook toepasbaar op de wereldwijde samenwerking van wetenschappers die data verwerken in grote computercentra. In Amerika bij Internet2 en het GENI project reageert men enthousiast op het idee om het model daarop toe te passen.'

SARNET – en verder

De Laat: 'Buiten het kader van SARNET kun je verder nog denken aan fundamenteel onderzoek om de veiligheid van internet verder te vergroten. Aangezien vertrouwen een kernpunt is, kun je eraan denken om wiskundige grondslagen toe te passen op internet, ongeveer op een manier zoals dat bij Bitcoin nu al gebeurt. Een lastig punt is dat gebruikers vermoedelijk alleen evolutionaire stappen zullen accepteren – zodat ze niet al hun sites opnieuw hoeven te bouwen – terwijl technologisch gezien een revolutionair andere basis onder internet waarschijnlijk wenselijker is.'

Eén voor allen, allen voor één

Gebruikers en Internet Service Providers (ISPs) kunnen als ze samenwerken veel sneller en adequater op aanvallen reageren. Gommans 'Vanuit het principe 'een aanval op één is een aanval op allen' kun je veel meer doen en bijvoorbeeld al bij de ingang van de ISP een blokkade opzetten die alle klanten vrijwaart.'

De aanval uit 2013 was een belangrijke motivatie voor KLM om in SARNET te participeren. Ook persoonlijke contacten droegen eraan bij – Gommans promoveerde bij De Laat. Gommans: 'De vraag hoe we op lange termijn met dergelijke aanvallen omgaan is bij ons actueel. Vanuit een maatschappelijk verantwoordelijkheidsgevoel vinden we het belangrijk bij te dragen aan de ontwikkeling en verspreiding van relevante kennis op het gebied van internet-veiligheid. Het SARNET-project past daarin. Het gaat ons bij cyber security

>>

niet om patenten, maar om kennisdelen om tot efficiënte en kosteneffectieve beveiligingsstrategieën te komen. En dan is al snel duidelijk dat de beste verdediging niet bij het eindpunt ligt, maar bij de ISP. Daarom moet je wel samenwerken om een effectieve verdediging op te zetten.'

Grote belangstelling

De verdediging aanpakken in een samenwerking tussen gebruikers en service providers is volgens De Laat en Gommans technologisch effectief. In de praktijk is dit echter niet zo gemakkelijk te organiseren. Wie betaalt welke kosten? Hoe zorg je voor het vertrouwen van de ketenpartners? Welke juridische implicaties zijn er? Gommans: 'Dergelijke vragen borduren deels verder op mijn proefschrift. Daarom zal ik naast Van Engers en De Laat als copromotor optreden voor de promovendus die dit deel van het onderzoek gaat uitvoeren.'

Volgens Gommans is de gecombineerd technologisch-juridische insteek van SARNET op netwerkgebied wereldwijd behoorlijk uniek: 'We hebben het project de afgelopen tijd in Amerika gepresenteerd en de belangstelling is groot.'

Summary

Government and economy nowadays depend on internet – and internet depends on justified trust. The Security Autonomous Response in programmable Networks (SARNET) project is one of the projects within the framework of the National Cyber Security Research Agenda II to secure trust. It involves three different aspects to withstand attacks on vital websites. The first is to make software defined networks (SDN) and use network function virtualization (NFV) in such a way, that networks can flexibly be changed to evade attacks and at the same time maintain their original functionality. The second aspect is to develop an automated decision support mechanism, connected to automated cost-effective countermeasures. The final aspect involves the collaboration within the supply chain that is necessary to introduce such a model, including vital components such as trust and legal basis.

Start en finish

Na de zomer moet het consortium compleet zijn en gaan de promovendi van start. De Laat: 'Ruwweg zullen we het eerste jaar besteden om een wereldwijd programmeerbaar netwerk-laboratorium te creëren waarmee we later het concept kunnen testen op 'dummy ISPs'. Het tweede jaar hebben we nodig om multidomeinfuncties uit te voeren en het derde jaar om het afwegingsmechanisme en de afweer uit te werken.'

Welk resultaat zou Gommans over pakweg enkele jaren graag zien? 'Een prototypesysteem dat cyberaanvallen geautomatiseerd kan afslaan op meerdere netwerkniveaus in de keten, zowel bij gebruikers als bij netwerkdienstverleners. Dat is het model waar iedereen de voordelen van inziet: het vergt veel minder mankracht en de snellere reparatietijd beperkt de mogelijke directe en indirecte schade. Met een kosteneffectief systeem kunnen bedrijven gezamenlijk kosten besparen.' I/O