INTERVIEW

‘Niemand kan grote ict-projecten managen’

Krakkemikkige websites, een gekraakte ov-chipkaart en falende internetbeveiligingen. De overheid gedraagt zich vaak als een digitale brokkenpiloot. Toch is het vooral de mens die moeite heeft met ict-veiligheid, vindt hoogleraar ict-veiligheid **Bart Jacobs**.

Door Herbert Blankesteijn

Is een website van de overheid wat hij zegt te zijn? In september bleek dat het systeem van digitale certificaten waarmee sites hun identiteit bewijzen, was ondermijnd. Diginotar, een Nederlandse maker van zulke certificaten, was gehackt en had geprobeerd dat stil te houden, hoewel het bedrijf wist dat er certificaten waren vervalst. Toen dat bekend werd, maakte minister Donner op een nachtelijke persconferentie bekend dat de betrouwbaarheid van overheidswebsites niet kon worden gegarandeerd.

Is dat het zoveelste voorbeeld van falen van de overheid bij automatiseringsprojecten? Is een behoorlijk niveau van veiligheid eigenlijk wel haalbaar? Prof.dr. Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen, heeft in het verleden gewaarschuwd voor de ondeugdelijkheid van verschillende digitale systemen, zoals de stemcomputer en de ov-chipkaart.

Hoe werkt dat systeem van certificaten waar Diginotar onderdeel van was?
‘Als ik wil gaan internetbankieren, vraagt mijn pc aan die van de bank: bewijs maar eens dat jij van de bank bent. Die bankcomputer doet dat door een certificaat te overhandigen. Zo’n 600 bedrijven in de wereld verstrekken zulke digitale bewijzen, dat zijn de zogenoemde *certificate authorities*. Die certificaten worden vertrouwd door alle grote browsers in de wereld, zoals Internet Explorer, Firefox, Chrome en Safari.’

En wie bepaalt welke bedrijven *certificate authority* mogen zijn?
In essentie bepalen Microsoft, Apple, Mozilla en Google dat, de makers van de browsers dus. Zij bepalen welke bedrijven ze vertrouwen.’

‘Als ik bij de Chinese geheime dienst zou werken, maakte ik apps als *Angry Birds*’

Hoe zag het gat in de beveiliging bij Diginotar eruit?
‘Een hacker wist binnen te komen en die is erin geslaagd certificaten ondertekend te krijgen van organisaties die helemaal geen klant zijn bij Diginotar, met name Google. Daarmee wist de Iraanse overheid vervolgens de data van Gmail-gebruikers te onderscheppen.

‘Als er iets fout gaat bij een certificaatprovider als Diginotar, moet je direct de onjuiste certificaten op een zwarte lijst zetten. Dan is er in feite niks aan de hand. Maar Diginotar heeft het stilgehouden. Daardoor was niet duidelijk wat er wel of niet op de zwarte lijst moest komen. En toen heeft de internationale gemeenschap gezegd: wij vertrouwen geen enkel certificaat van Diginotar meer.’

Dus certificaatinstanties worden gekozen door grote internetbedrijven. Een van die gelukkigen, Diginotar, heeft zijn beveiliging niet op orde. En daardoor komt de Nederlandse overheid in de problemen. De overheid zelf heeft dus niet gefaald?
‘Inderdaad. De overheid is van alles aangerekend waar ze niet verantwoordelijk voor was. Indirect heeft de overheid wel een rol omdat ze verantwoordelijk is voor het toezicht in Nederland op partijen als Diginotar. Dus daar zit een afgeleide verantwoordelijkheid. Maar het zijn grotendeels private partijen die besluiten hoe ze dat doen.’

De overheid krijgt vaak de wind van voren, ze zou geen grote ict-projecten kunnen managen. Maar wie kan dat wel?
‘Volgens mij kan niemand dat. Bij de overheid valt me op dat ambtenaren op het middenniveau vaak behoorlijke technische kennis hebben. Op de hogere niveaus

RADBOUD UNIVERSITEIT

wordt daar vaak niet naar geluisterd. Dat is een deel van het probleem.

'Interessant aan de Diginotar-crisis is dat de eerstverantwoordelijke ministers Donner en Opstelten hier helemaal niks van weten. En ze waren juist erg geneigd te luisteren naar hun ambtenaren. Daardoor is het probleem goed opgelost.'

Het lijkt erop dat computersystemen zo complex zijn dat er altijd wel ergens een gat zit. Is waterdichte beveiliging nog mogelijk?
'De samenleving is afhankelijk geworden van digitale processen. De digitale beveiliging is dus cruciaal. Maar daar hebben we niet zo'n goede intuïtie voor. Als op straat een vreemde aan jou vraagt: mag ik je huissleutel, dan lach je hem uit. Mensen hebben een redelijk gevoel voor fysieke beveiliging. In de digitale wereld hebben we dat nog niet.'

Als je mensen op straat naar hun wachtwoord vraagt, krijg je het vaak nog ook. Dat is in diverse onderzoeken aangetoond.
'De meeste mensen hebben intussen wel door dat je op je Hyves-pagina niet én moet zetten wanneer je op vakantie gaat, én op welk adres je woont. Maar de ontwikkelingen gaan zo snel dat je je kunt afvragen of mensen dit bijhouden.

'Neem de smartphones. Dat vind ik werkelijk een *security*-ramp. Als je ziet wat mensen daar allemaal aan apps op kunnen zetten… Als ik bij de Chinese geheime dienst zou werken, maakte ik apps als Angry Birds en Whatsapp. Dan zit je bij honderden miljoenen mensen op de smartphone. Die programma's vragen bij installatie: geeft u toestemming dat uw locatie, uw contactgegevens en dergelijke doorgegeven worden? Iedereen klikt vervolgens 'ja.' Het is dweilen met de kraan open.'

De vraag is dus eigenlijk: wat is het zwakste punt, de techniek of de mens?
'Ja, en bovendien: wie zijn de *stakeholders*. Want je ziet dat de partijen die zulke apps schrijven, totaal geen belang hebben bij beveiliging.'

Kun je met wet- en regelgeving goede beveiliging afdwingen?
'Daar is wel winst te halen. In de fysieke wereld is veel gebeurd in de afgelopen eeuw. De auto is een voorbeeld. In de eerste 50 jaar dat auto's werden geproduceerd, was er geen belangstelling voor beveiliging – in de zin van bescherming van de inzittenden. Op een gegeven moment is dat van de grond gekomen, door een combinatie van afdwingen van regulering en bewustzijn van de rijders. Bij een auto zijn veiligheidseisen relatief makkelijk te stellen: een rem moet het gewoon doen, en binnen zoveel meter moet je stilstaan. Dat soort zaken zijn ontstellend lastig in de computerwereld.'

Al was het maar omdat die stomme dingen zich zo snel ontwikkelen. Elke regel die je bedenkt is morgen verouderd.

Bart Jacobs

1963 Geboren in Nuenen

1981 Studies wiskunde en filosofie in Nijmegen

1991 Promotie in theoretische computerwetenschappen

2002 Hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen

2002 Toekenning Pionier-subsidie van 1,8 miljoen euro

2007 Lid van commissie-Korthals Altes, die adviseert de stemcomputer af te schaffen

2008 Jacobs' groep toont aan dat de Mifare Classic-chip, onderdeel van de ov-chipkaart, onveilig is.

▶ **Bart Jacobs kraakte in 2008 met zijn onderzoeksgroep de ov-chipkaart.** HH

'Dat is één ding. Daarnaast hebben computers niet een eenduidig doel. De kracht is juist dat je hem op allerlei manieren kunt programmeren en dat je dus geen doelgerelateerde eisen kunt stellen.

'Daarnaast heb je nog de omstandigheid dat software-aansprakelijkheid nooit van de grond is gekomen. Als ik een strijkijzer koop en het is niet goed, dan kan ik terug naar de winkel. Als je dat doet met een computer met een blauw scherm, dan lachen ze je uit. Wat wel interessant is: de kosten van auto's zitten de laatste jaren vooral in software en niet meer in staal. Dáár stellen consumenten eisen aan: dezelfde eisen die ze gewend zijn aan auto's te stellen. Die moeten betrouwbaar zijn en veilig.'

Want daar zijn levens mee gemoeid in plaats van bankrekeningen.
Daarom staat er druk op dat die software beter functioneert. Maar vooralsnog kan die kwaliteit niet worden geleverd. De incidenten met auto's van de laatste jaren, zoals de '*unintended acceleration*' bij Toyota, hebben in veel gevallen met software te maken.

Waar valt het meest te halen, bij regelgeving, techniek of de menselijke factor?
'Bij wet- en regelgeving valt zeker wat te halen. Maar dan moeten we eerst consensus hebben over de eisen. In mijn vak zijn modellen in omloop van zogeheten *common criteria* voor software. Die hebben zeven niveaus van eisen die je aan software kunt stellen. Het laagste niveau is dat er documentatie moet zijn. Dat is niet altijd vanzelfsprekend. Andere niveaus zijn bijvoorbeeld eisen voor een duidelijke omschrijving van het doel, een functioneel ontwerp, een functionele test die moet worden uitgevoerd, een beveiligingsmodel dat moet zijn getest enzovoort. In de wereld van smartcards wordt dat al gebruikt. Zulke criteria komen uit de militaire- en inlichtingenwereld, waar ze nog steeds worden toegepast.'

'Mensen klikken op van alles en geven al hun privégegevens aan Facebook'

Waar de eisen hoog zijn, anders komt een product er gewoon niet in?
'Inderdaad. Bescherming van staatsgeheimen mag alleen via apparatuur die aan strenge eisen voldoet.'

Valt te verwachten dat het daarvandaan doorsijpelt naar de hele computermarkt?
'Ja, je ziet wel dat het verder komt, maar het drijft de kosten op en leidt ook tot een zekere verstarring. Je kunt je voorstellen dat als een bepaald apparaat met bepaalde software is goedgekeurd, de goedkeuring vervalt zodra er ook maar een patch (*een stukje software dat wordt gebruikt om fouten op te lossen of updates te verrichten aan de software, red.*) wordt uitgevoerd.'

Laat staan wanneer je echt gaat innoveren.
'Inderdaad! Het is de vraag of dat wel zinvol en vol te houden is.'

Dan kun je het ook omdraaien en zeggen dat een groot deel van de innovaties van de afgelopen decennia te danken is aan gebrek aan veiligheid.
'Het heeft te maken met software-economie. Als je applicaties wilt verkopen, is het ontzettend belangrijk snel een groot marktaandeel te krijgen. Daardoor is een houding ontstaan van: *sell tomorrow and patch in version 5*. Pas als je de consument hebt gevangen, kun je aan kwaliteit gaan denken.'

Dus regels kunnen we wel verwachten, maar er is een grens aan wat je daarmee kunt doen. Kun je dingen goed dichttimmeren met techniek?
'In principe wel, ja. Maar het is complex, en je moet goed kijken waar je op vertrouwt. Je kunt zelf een veilig programma schrijven, maar zo'n programma wordt in laatste instantie door een compiler (*een vertaalprogramma, red.*) gemaakt. Als zo'n compiler is besmet en stiekem dingetjes toevoegt, krijg je ook problemen. Dus je moet de compiler vertrouwen. Dan het besturingssysteem waar je computer op draait. Als je helemaal paranoïde bent moet je ook de hardware vertrouwen…'

…die nogal eens uit China komt…
'Precies. Dus het is ontzettend moeilijk die hele keten in de gaten en onder controle te houden.'

En dan de factor mens. Wat gaan we daarmee doen?
'Afschaffen. Mensen klikken op van alles en nog wat, geven al hun privégegevens aan Facebook, zijn slordig met hun wachtwoorden en laten zich met leuke features naar een onveilig product lokken. Beveiliging vereist een juiste combinatie van technische, organisatorische en juridische middelen. Maar de mens blijft voorlopig de zwakste plek.' ■