

NRC HANDELSBLAD

@

Veilig en democratisch

Marie-José Klaver



Wat hebben informatiebeveiliging en democratie met elkaar te maken? Veel, vindt de pas benoemde hoogleraar computerbeveiliging Bart Jacobs. In zijn vrijdag uitgesproken inaugurale rede aan de universiteit van Nijmegen pleit Jacobs, wiens leeropdracht beveiliging en correctheid van programmatuur is, voor meer openheid in de computerbeveiliging.

Geheime beveiligingstechnieken zijn op den duur een gevaar voor de democratie, betoogt Jacobs, omdat computersystemen ook worden gebruikt om te stemmen en om rechters te ontlasten. Bij de Europese verkiezingen volgend jaar is er ruimte om op afstand per computer te stemmen. „Hoe kunnen burgers erop vertrouwen dat hun elektronisch uitgebrachte stem aantoonbaar bijdraagt aan het eindresultaat, maar toch geheim blijft?” vraagt Jacobs zich af.

Jacobs maakt zich ook zorgen over de elektronische handtekening die binnenkort dezelfde status krijgt als de handtekening op papier. Een elektronische handtekening moet volgens de wet worden gezet met een „veilig middel”. Een vage bepaling, vindt Jacobs.

De hoogleraar stoort zich met name aan nieuwe wetgeving die het controleren van computerbeveiligingsmethoden bemoeilijkt en in bepaalde gevallen zelfs strafbaar stelt. Het doorbreken en omzeilen van beveiligingsmechanismen en het publiceren over lekken wordt in de Europese Unie verboden. Volgens nieuwe wetgeving, die sterkt lijkt op bestaande Amerikaanse wetgeving, prevaleren de rechten van softwaremakers en leveranciers van content (spelletjes, films, boeken) boven de rechten van nieuwsgierige hackers en wetenschappers die digitale beveiligingsmethoden graag onder de loep nemen en hun vondsten openbaar willen maken.

De nieuwe Auteurswet heeft volgens Jacobs desastreuze gevolgen voor zijn vak. „Wetenschappelijk onderzoek naar correctheid en beveiliging van computersystemen is er inherent op gericht om fouten te vinden. Een verbod om vervolgens zulke gebreken te rapporteren leidt tot een wezenlijke beperking van dergelijk onderzoek.”

De overheid realiseert zich volgens Jacobs onvoldoende dat ook computers gecontroleerd moeten worden. Gebrek aan transparantie heeft volgens hem direct invloed op de democratie. Als allerlei procedures die essentieel zijn voor de democratie, zoals rechtspraak en openbaar bestuur, afgehandeld worden door computers in black boxes, met „misschien een stickertje van TNO”, weet niemand wat er precies gebeurt, aldus Jacobs. „De in () stemcomputers gebruikte mechanismen zijn niet openbaar. Iets technischer, de broncode van de gebruikte software is niet openbaar. Wij hebben als burgers het recht om het tellen van gewoon met potlood en papier uitgebrachte stemmen bij te wonen en te controleren, maar wij hebben geen inzage in de werking van deze stemcomputers.”

Wat er mis kan gaan als software niet controleerbaar is, blijkt uit de rechtszaak tegen de Koerdische drugshandelaar Hüseyin Baybasin. In zijn zaak speelden door geheime diensten afgetapte telefoongesprekken een grote rol. De software die in Nederlandse tapkamers wordt gebruikt is afkomstig van de Israëlische geheime dienst. Omdat de broncode van de tapprogramma's geheim is, kan volgens Jacobs door de verdediging nooit worden vastgesteld of de als bewijs aangedragen tapverslagen betrouwbaar zijn. Ondanks onduidelijkheden over de betrouwbaarheid van de

afgetapte gesprekken werd Baybasin tot twintig jaar gevangenisstraf veroordeeld.

Om de transparantie te bevorderen moet de overheid ervoor zorgen dat er zoveel mogelijk open source software gebruikt wordt, meent Jacobs. Software waarvan de broncode openbaar en aanpasbaar is, is gemakkelijker te controleren dan computerprogramma's van commerciële bedrijven als Microsoft en Adobe die er alles aan doen om de receptuur van hun programma's geheim te houden.

Maar open source software gebruiken is niet genoeg. Het belangrijkste is de wet. En die wordt steeds vaker in Europees verband gemaakt, zodat de invloed van de Nederlandse overheid (en kiezer) gering is. De nieuwe Auteurswet, die onder meer het publiceren over gevonden zwakheden in digitale beveiligingstechnieken verbiedt, is de implementatie van een Europese richtlijn. Zelfs als de Nederlandse overheid haar standpunt zou herzien als gevolg van Jacobs' oratie, is de kans op aanpassing van de wet gering.

Website: www.cs.kun.nl/~bart

[klaver@nrc.nl] Vragen over internet? Ga naar www.nrc.nl/klaver

19 mei 2003

© Op dit artikel berust auteursrecht

 **print**