Prof. Bart Jacobs en **Dr. Klaus Kursawe** werken aan de Radboud Universiteit Nijmegen rond digitale beveiliging.

Wikileaks was geen toeval

Wanneer moet je gevoelige geheimen onthullen? Beveiligingsdeskundigen Bart Jacobs and Klaus Kursawe trekken parallellen tussen het onthullen van diplomatieke geheimen en het onthullen van fouten in software.

Wikileaks heeft de afgelopen weken de gemoederen stevig verhit. De aandacht richtte zich vooral op de opzienbarende inhoud van Amerikaanse diplomatieke berichten die Wikileaks publiceerde. Maar ook de werkwijze van de diverse betrokkenen (zoals Wikileaks, de Amerikaanse overheid, de Zweedse justitie en anonieme hackers) gaf aanleiding tot veel discussie.

Niet iedereen lijkt zich te realiseren dat Wikileaks er niet toevallig is gekomen. Het is een haast logisch gevolg van de infrastructuur die het internet biedt: je kunt anoniem informatie aanbieden, maar je kunt informatie niet zomaar laten verdwijnen, zeker niet als er veel belangstellenden zijn die de informatie zelf ook weer gaan verspreiden. Om dat onmogelijk te maken, moet de hele structuur van het internet overhoop gehaald worden en zullen fundamentele burgerrechten beknot moeten. We kunnen Wikileaks dus beter accepteren in plaats van bestrijden.

Wat verder direct opvalt, vanuit het perspectief van informatiebeveiliging, is dat de Amerikaanse diplomatieke berichten überhaupt konden uitlekken. De gegevens waren beschikbaar via het Amerikaanse geheime defensienetwerk SIPRNet, waartoe naar verluidt zo'n twee miljoen mensen toegang hebben. Het is uitgesloten dat al die mensen volledig betrouwbaar zijn. Als zovelen bij die informatie kunnen, mag je overigens aannemen dat concurrerende inlichtingendiensten er al lang over beschikken. Voor veel wereldleiders zal de inhoud dus geen verrassing vormen.

De Amerikaanse overheid toonde zich erg verontwaardigd over de publicatie. Minister van Buitenlandse Zaken Hillary Clinton noemde ze onverantwoordelijk, levensbedreigend en een aantasting van de nationale veiligheid. Echter, juist het slordig omgaan met de gevoelige gegevens is onverantwoordelijk en levensbedreigend.

Onze onderzoeksgroep in Nijmegen is ongeveer drie jaar geleden ook hard aangevallen over onze publicatie(plannen). Begin 2008 ontdekten we dat in de chipkaart 'Mifare Classic' cruciale ontwerpfouten zaten waardoor de kaart eigenlijk waardeloos was. Van de Mifare Classic zijn wereldwijd miljarden exemplaren verkocht die volop gebruikt worden in toegangspasjes voor gebouwen en voor betaling in het openbaar vervoer, zoals in de OV-chipkaart in Nederland. Onze conclusies publiceren was, vooral volgens de kaartfabrikant, 'onverantwoordelijk' en zou 'grote gevaren met zich meebrengen'. Men trok zelfs naar de rechter om een publicatieverbod te vragen. Tevergeefs.

'Wederzijds vertrouwen is vereist. Escalatie werkt niet'

Voortdurend worden fouten ontdekt in computerprogramma's. Wat moet je doen als je bijvoorbeeld een fout ontdekt in Windows? Het is in ieders belang dat zo'n fout zo snel mogelijk gerepareerd ('*gepatched*') wordt, zodat kwaadwillenden er geen misbruik van kunnen maken. Het ligt het meest voor de hand om de fabrikant zo snel mogelijk vertrouwelijk in te lichten. In de praktijk blijkt dat bij zo'n *restricted disclosure* de fabrikant die fout niet direct repareert. Een minder nette, maar vaak effectievere manier, is *full disclosure*: directe publicatie van de fout, mogelijk zelfs samen met software om er misbruik van te maken. Na zo'n publicatie blijken fabrikanten vaak wél snel te reageren en een patch beschikbaar te stellen.

Door de jaren heen is er op dit gebied brede overeenstemming gekomen over de beste handelwijze. Dat wordt *responsible disclosure* genoemd: je meldt de fout direct aan de fabrikant, en zegt daarbij dat je de details over een paar maanden zult publiceren.

Kunnen we hiervan leren in het geval van Wikileaks? Natuurlijk gaat de vergelijking maar gedeeltelijk op: Wikileaks' berichten zijn geen repareerbare softwarefouten, maar bevatten soms wel wantoestanden. Een eerste stap in de richting van een consensus over zulk soort onthullingen is de erkenning van een gemeenschappelijk belang, in de vorm van het repareren van softwarefouten of het voorkomen of bestraffen van misstanden. Een tweede stap is een verantwoordelijke onthulling, die duidelijk gericht is op dat gemeenschappelijke belang, zonder onnodige, gevaarlijke bekendmakingen. Ten derde is een zekere mate van wederzijds vertrouwen vereist, waarbij partijen elkaars rol erkennen en elkaar niet bestrijden zolang ze zich verantwoordelijk gedragen en zich richten op het gemeenschappelijke belang. De softwarewereld is daarin inmiddels verder gevorderd dan de internetwereld. Escalatie werkt niet.