CRYPTO WARS 2.0

De unieke sleutel tot onze digitale informatie

Axel Arnbak

De nieuwste iPhone's en iPad's zijn standaard zo beveiligd dat alleen de gebruiker de unieke sleutel tot zijn gadget krijgt. Voortaan kan Apple er niet meer in. En dus ook de Amerikaanse autoriteiten niet. De FBI brieste vorige week dat Apple hiermee de dood van kinderen, terroristische aanslagen en ander gezelligs op zijn geweten heeft. Beveiligingsexperts buitelden over elkaar heen om de krankzinnige angstzaaierij af te kraken. En Apple erop te wijzen dat gebruikers ook de unieke sleutel tot de iCloud moeten krijgen. De iCloud zit immers in het Prism-programma — zo onthulde Snowden — en bleek deze zomer ook nog zo lek als een zeef. Cybercriminelen zetten naaktfoto's van beroemdheden online. Niemand weet wat nog meer is buitgemaakt. Tussen marketing, angst en beveiliging worden de messen geslepen voor de Crypto Wars, versie 2.0.

De eerste Crypto Wars woedden medio jaren '90. De inzet: wetenschap. Een naïef standaardwerk over die geschiedenis heeft een veelzeggende titel: *Crypto:How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. Steven Levy tekent een sprookje op over coole geeks en hippies, die tijdens roadtrips langs de West Coast filosoferen over versleuteling en anoniem geld — Bitcoin avant la lettre. Onderweg testten ze hun ideeën op de computers van topuniversiteiten. Het was de geboorte van openbare versleuteling.

Tot die tijd, al eeuwenlang, bewaakten overheden versleuteling met staatsgeheimen, publicatie- en exportverboden. De Koude Oorlog was nog maar net voorbij. Maar de wetenschappelijke doorbraken waren niet meer te stoppen. Geholpen door financiële- en E-Commercebedrijven die het nut van versleuteling inzagen, werden de verboden na jarenlang actievoeren opgeheven. Iedereen mocht zichzelf nu beveiligen. Privacy gered, aldus Levy in 2001.

Heerlijk leesvoer, gevaarlijk naïef. In feite speelde de Amerikaanse overheid een geniaal dubbelspel. In het publieke debat voedde men de angst. Zo durfden politici robuuste beveiliging niet bij wet te verplichten. Ondertussen werden saaie standaardorganisaties — zoals IETF en NIST — systematisch geïnfiltreerd om niet de theorie, maar de implementatie in massa-infrastructuur en producten te manipuleren. Ook werden beveiligingsbedrijven als RSA, waarvan u op werk allicht zo'n kek inlogsleuteltje heeft, omgekocht om achterdeurtjes in hun waar te maken. Door Snowden weten we het zeker: standaard internettechnologie is fundamenteel onveilig.

De techno-elite had geen geduld voor saaie standaarden en het volk. Iedereen kan zichzelf toch beveiligen? Gewoon vanaf de command line je PGP-sleutels, PKI-certs, Linux-distro en eigen servertje managen! Slechts enkelen zagen in dat cybersecurity en privacy steeds meer kwesties van business opportunity, geopolitiek, grondrechten en gebruiksvriendelijkheid zijn. De technologie bleef beschikbaar, maar wordt nauwelijks en verkeerd gebruikt.

Door Snowden weten we het zeker: standaard internettechnologie is fundamenteel onveilig

Na de eerste Crypto Wars sloot alles en iedereen zich aan op het web. Onder de illusie van veiligheid. De FBI en NSA luisteren gretig mee. Eerst schuilde het Westen onder de 'nuclear umbrella' van de V.S. als bescherming tegen Russische kernwapens. Nu heeft Amerika met een 'information umbrella' westerse bondgenoten weer afhankelijk gemaakt. Informatie is macht.

Na alle iCloud-blunders en Snowdensaga's vechten Amerikaanse marktleiders voor ons vertrouwen. Gadget control is winst, maar onze apparaten liggen altijd aan het infuus van de cloud. Zonder de unieke cloudsleutel blijft de schatkist wagenwijd open.

Dat is het cruciale punt van beveiliging: iedere aanvaller kan ieder gat of achterdeurtje exploiteren. Of het nu de cloudprovider, concurrent, NSA, Belastingdienst, politie, Poetin of een cybercrimineel is. Een technisch hiaat maakt geen onderscheid tussen goed en kwaad. Beveiliging moet mooi, meteen 'aan' en transparant zijn. Met unieke sleutels. De iPhone biedt dat niet. Als start ups Blackphone en IndiePhone het waarmaken, wachten gouden bergen.

Tijdens de eerste Crypto Wars stond de theorie op het spel, nu de implementatie. Maken we het internet veilig voor iedereen, of kwetsbaar voor alle aanvallers? De belangen zijn kolossaal, vaak verhuld achter krankzinnig doemdenken. Wie krijgt de unieke sleutel tot onze informatie? De Crypto Wars 2.0 zijn begonnen.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IViR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak