NIEUWE KANSEN

# Stortvloed regels moet beveiliging internet verbeteren

Axel Arnbak

Met de aftrap van het Europese en Nederlandse politieke seizoen stormt nieuwe cybersecurityregulering vanuit alle windhoeken op ons af. In Europa zijn vijf wetsvoorstellen in behandeling. In Nederland tikt het College Bescherming Persoonsgegevens (CBP) organisaties steeds vaker op de vingers. Rechters stellen bedrijven als DigiNotar aansprakelijk voor geleden schade. Ondertussen staan de media bol van incidenten zoals gehackte naaktfoto's uit de iClouds van Hollywoodsterren. En nestelt het internet zich in de broekzak, cv-ketel en pacemaker van een bezorgde burger.

Niet hackers of technische complexiteit, maar een falende markt voor internetbeveiliging is de kern van het probleem. Aan de ene kant van de markt komen verkopers van hard- en software al decennialang weg met matig beveiligde producten en diensten. Aan de andere kant hebben kopers geen idee hoe cybersecurityproducten presteren, laat staan concurreren op cybersecuritygebied. Wil je onder de motorkap van je telefoon of besturingssysteem kijken en sleutelen aan je product, vervalt je garantie. Veel cybersecuritymarkten kennen bovendien maar een of twee dominante spelers. Overheden, bedrijven en consumenten zitten na hun eerste koop opgesloten in een jarenlange keten van producten van dezelfde maker. Overstappen is technisch of praktisch onmogelijk.

Ernstige lekken worden onder de pet gehouden. Crasht je systeem en liggen je bedrijfsgeheimen of naaktfoto's op straat, verwerpt de verkoper in de kleine lettertjes iedere aansprakelijkheid. Of het nu gaat om Microsoft Windows of de aan alle Apple-producten gekoppelde iCloud, beveiligingsexperts en beleidseconomen bewijzen al jaren dat verkopers handig inspelen op de falende cybersecuritymarkt.

Bij het 'internet der dingen' nemen de problemen en afhankelijkheid alleen maar toe. Cv-ketels kan je dan op afstand laten exploderen. Voormalig vice-president Dick Cheney van de VS heeft nog kunnen afdwingen dat zijn pacemaker niet benaderbaar is via internet, een nieuwtje waar hitserie *Homeland* op inspeelde. Maar voor ons gewone stervelingen rest de ijdele hoop dat hartendief een figuurlijke uitdrukking blijft.

Voor de Europese verkiezingen in mei behandelde de EU vijf nieuwe cybersecuritywetten op het gebied van privacy, telecom, encryptie, cybercrime en kritieke maatschappelijke infrastructuren. Opmerkelijk genoeg verschillen de voorstellen weinig van Europese initiatiefwetgeving in de jaren '90: (ietwat fletse) beveiligingseisen, meldplichten na incidenten en een verdeling van aansprakelijkheden. Net als toen heeft een briljant georganiseerde lobby de voorstellen zo weten uit te kleden dat iedereen straks de schuld krijgt, behalve verkopers.

Lobbyclubs als de Business Software Alliance hebben uitzonderingsposities weten te bedingen voor verkopers en lijken ook een centrale rol te krijgen bij de invulling van abstracte beveiligingsnormen en meldplichten. Omdat de media te druk waren met de Europese verkiezingen en kopers lagen te slapen, verandert de status quo nauwelijks: wij van WC-eend adviseren WC-eend.

**Door toenemende aandacht voor cybersecurity is er momentum om in politiek orde op zaken te stellen**

Uit andere hoeken is beter nieuws te berichten. Het CBP pioniert met handhavingsacties tegen Whatsapp, apotheken en hogescholen. In augustus oordeelde de Amsterdamse rechtbank dat de vorige eigenaren van DigiNotar de aankoopsom aan Vasco dienen terug te betalen wegens aansprakelijkheid voor de verwijtbare beveiligingsravage. Europese rechters vestigen langzamerhand een grondrecht op ICT-beveiliging. Internetbeveiliging is inderdaad essentieel voor het genieten van privacy en vrijheid van meningsuiting op internet.

De trends in toezicht en rechtspraak worden versterkt door de media-aandacht en consumentenzorgen, ook na de onthullingen van Snowden.

Door de toenemende aandacht voor cybersecurity zullen organisaties beveiligingsniveaus moeten oprikken. Al staat de wetgeving er niet best voor, bieden de wisseling van de wacht in de Europese Commissie en het Parlement nieuwe kansen om hogere eisen te stellen aan soft- en hardware. Hoog tijd dat de kopers van internetbeveiliging zich organiseren, met name in Brussel. Verwacht in de komende maanden niet alleen een stortvloed aan nieuwe incidenten, maar ook aan regulering die erop gericht dient te zijn een einde te maken aan structureel falende cybersecuritymarkten.

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