Waar zijn mijn data gebleven?

'Hello, I have to make an international transfer as soon as possible, pay an invoice. Can you do that for me? Let me know, then I can send you the details immediately. Sincerely, Martin Paul.'

Deze e-mail werd laatst gestuurd naar een collega van mij. De tekst was duidelijk in het Nederlands geschreven en daarna vertaald met Google Translate; een typisch geval van persoonsfraude.
Natuurlijk betaalde mijn collega niks. Een klik op het mailadres van de afzender bewees dat de boodschap niet van mijn account afkomstig was. Tegenwoordig weten mijn naaste collega's en de ondersteunende afdelingen op de universiteit exact hoe ze dit soort benaderingen, ook wel bekend als CEO-fraude, kunnen herkennen. En we hebben allerlei beveiligingssystemen waarmee we digitale bedreigingen voor de Universiteit Maastricht kunnen herkennen en blokkeren. Maar het bovengenoemde voorval is slechts één symptoom van onze kwetsbaarheid anno 2019, met de vele digitale sporen die we achterlaten, van social media tot allerhande databanken. Het is haast onmogelijk geworden om te weten waar onze data zijn opgeslagen en wat er precies mee gebeurt (en dus of er misbruik van gemaakt wordt).

Twee recente voorvallen die veel media-aandacht kregen, illustreren ook dat deze nepmail geen op zichzelf staand incident is. Vlak voor Kerstmis werd bekend dat de persoonsgegevens van honderden Duitse politici en anderszins bekende figuren 'gehackt' zijn, inclusief zeer gevoelige informatie als paspoort- en rekeningnummers. En vorige week maakte de hotelketen Marriott bekend dat een lek in hun database de diefstal mogelijk maakte van de gegevens van ruim 350 miljoen gasten die de afgelopen jaren bij hen overnachtten. Wederom inclusief paspoort- en telefoonnummers, maar ook creditcardnummers en andere gevoelige informatie, zoals werk- en privéadressen. Er zijn grote zorgen dat deze data gebruikt kunnen worden voor identiteitsfraude, gevolgd door diefstal.

Dit alles maakt duidelijk dat de bedreiging van dataprivacy een wereldwijde epidemie is. Maar ook, dat we ons moeten realiseren hoe afhankelijk onze samenleving is geworden van informatie uit social media, waardoor de publieke opinie heel effectief kan worden gemanipuleerd. De manier waarop robots op Facebook en andere platforms de laatste Amerikaanse presidentsverkiezingen konden beïnvloeden, is wat dat betreft nog maar het topje van de ijsberg.

De vraag is: hoe gaan we om met al deze digitale dreigingen? Strengere Europese richtlijnen voor regelgeving rond databeveiliging is maar één deel van de puzzel. Het is ook noodzakelijk dat grote IT-bedrijven zich aan de regels houden en dat de overheid zich bemoeit met het vergroten van de IT-veiligheid. Ik denk bijvoorbeeld aan voortdurende 'end-to-end encryptie' (waarmee berichten alleen gelezen kunnen worden door degene voor wie ze bedoeld zijn) en meer politieke steun en middelen voor organisaties die investeren in goede IT-beveiliging.

En we moeten het gesprek voeren over onze burgerrechten in een digitale samenleving, met aandacht niet alleen voor technologie, maar ook voor juridische en ethische aspecten.
Tenslotte, maar niet het minst belangrijk: we moeten ook onze eigen verantwoordelijkheid nemen voor cyberveiligheid op persoonlijk vlak en hoe en waar we onze data overhandigen. Het maken van sterke wachtwoorden die we regelmatig veranderen en encryptie-technologie zijn nog maar de eerste en eenvoudige stappen. Zoals we ons paspoort en onze rekeningoverzichten nooit aan volstrekte vreemden zouden overhandigen, moeten we ook voorzichtig zijn met hoe we onze digitale gegevens delen. Zwakke en te simpele wachtoorden zijn wat dat betreft een groot probleem. Om onze medewerkers hier op een ludieke manier van bewust te maken, gebruiken we binnen de UM een aantal slogans, waaronder deze: ´Behandel je wachtwoord als je ondergoed: deel het nooit met iemand, verwissel het regelmatig en laat het niet rondslingeren op je bureau.'

Met dit alles in het achterhoofd heb ik een van mijn goede voornemens voor dit jaar al gerealiseerd: ik heb opnieuw mijn wachtwoorden veranderd. Ook ga ik mijn social media-activiteiten beperken. Wat is uw voornemen?

Column De Limburger, 12 januari 2019