

HANS FREDERIKS

Loskomen van BIG TECH

**Je eigen cloud met
een Synology NAS**

VANDUUREN
MEDIA

Loskomen van Big Tech

Hans Frederiks

VANDUUREN
MEDIA

ISBN: 978-94-6356-420-5

NUR: 987

Trefw.: Hardware, beveiliging, thuisnetwerk

Omslag: Bruggn Design, Purmerend

Opmaak: Van Duuren Media, Culemborg/Barcelona

Druk: Veldhuis Media, Meppel

Eerste druk: januari 2026

Dit boek is gedrukt op een papiersoort die niet met chloorhoudende chemicaliën is gebleekt. Hierdoor is de productie van dit boek minder belastend voor het milieu.

© Copyright 2026 Van Duuren Media B.V.

Van Duuren Informatica is een imprint van Van Duuren Media B.V.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande toestemming van de uitgever.

Voorzover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, St.b. 351, zoals gewijzigd bij Besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht. Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatie- of andere werken (artikel 16 Auteurswet 1912), in welke vorm dan ook, dient men zich tot de uitgever te wenden.

Ondanks alle aan de samenstelling van dit boek bestede zorg kan noch de redactie, noch de auteur, noch de uitgever aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout in deze uitgave.

Microsoft, Microsoft Windows, Microsoft Office, het Microsoft-logo en andere Microsoft-beeldmerken en -handelsnamen zijn handelsmerken of geregistreerde handelsmerken van Microsoft Corp.



Inhoud

■ 1	Waarom zelf hosten?	1
	Wat lees je in dit hoofdstuk?	1
	Het Big Tech-probleem	1
	Wat Google werkelijk ziet in jouw foto's	2
	Cloud Act: jouw data onder Amerikaanse controle	3
	Mijn eigen Big Tech-verslaving	4
	Microsoft: Office en OneDrive onder Amerikaanse controle	5
	Apple: privacymarketing versus Cloud Act-realiteit	6
	Advanced Data Protection: een stap vooruit	6
	Kostenaspect	7
	De andere kant van de medaille	7
■ 2	De keuze voor Synology	9
	Wat lees je in dit hoofdstuk?	9
	Meer dan alleen opslag	9
	Wat kun je ermee? Veel meer dan je denkt!	10
	QuickConnect: eenvoudig overal toegang	10
	Misschien zijn Synology's eigen apps wel genoeg	11
	Container Manager: voor wie meer wil	11
	Kosten: wat ga je uitgeven?	12
	Wat werkt goed, wat minder?	12
	Beveiliging: jij bent de systeembeheerder	13
	Voor wie is een NAS geschikt?	14
	Beperkingen waar je rekening mee moet houden	14
	Back-ups: juist bij zelf hosten essentieel	14
	Balans tussen gebruiksvriendelijkheid en zelf hosten	15
	Waarom geen andere oplossing?	15
	De Synology DS224+ die we in dit boek gebruiken	16
	Update 2025: de nieuwe DS225+	16

■ 3	Synology DS224+: aanschaf en installatie	19
	Wat lees je in dit hoofdstuk?	19
	Van een ingewikkeld plan terug naar de eenvoud	19
	RAID 1: waarom twee schijven beter zijn dan één	20
	RAID 1: spiegeling voor veiligheid	20
	Andere RAID-opties	21
	Perfect is voor beginners	21
	Aanschaf	21
	Netwerkverbinding regelen	23
	Hardware-installatie: eenvoudiger dan je denkt	23
	Wat zit waar op de DS224+?	23
	Fysieke installatie	25
	DSM-installatie en -configuratie	25
	Stap 1: Het eerste contact met je NAS	25
	Stap 2: DiskStation Manager (DSM) installeren	26
	Stap 3: Administratoraccount maken	27
	Stap 4: Update-instellingen configureren	29
	Stap 5: Synology-account (optioneel)	29
	Stap 6: QuickConnect instellen	30
	Stap 7: Essentiële apps downloaden en voorbereiden	31
	Stap 8: Extra services (optioneel)	32
	Stap 9: Extra garantie	32
	Stap 10: Tweefactorauthenticatie instellen	33
	Stap 11: Opslagconfiguratie	35
	Stap 12: Storage Creation Wizard	36
	Stap 13: RAID 1 configureren	36
	Stap 14: Synology's waarschuwing over third-party schijven	37
	Stap 15: RAID 1 wordt ingesteld, het eindresultaat	38
	Stap 16: Volume maken, de eigenlijke 'schijf'	38
	Stap 17: Apps installeren via Package Center	41
	Nog wat extra instellingen	42
	Taal	42
	E-mailnotificaties configureren	43
	Welkomstberichten aanpassen	44
	De installatie is voltooid	46

■ 4	Back-ups instellen voordat het serieus wordt	47
	Wat lees je in dit hoofdstuk?	47
	3-2-1-regel	48
	Lokale back-up: de externe schijf	48
	Cloudback-up: Amerikaanse versus Europese keuze	48
	Europese alternatieven	49
	Hyper Backup configureren	49
	Externe schijf voorbereiden	49
	Back-up instellen	51
	Cloudback-up configureren	52
	Je data op de NAS zijn nu veilig	53
	Praktische tips	53
	Alternatieve oplossingen voor cloudback-up	53
	Back-up testen en verifiëren	53
	Een back-up die je niet test, is geen back-up	53
	Methode 1: Herstelwizard (voor complete mappen)	54
	Methode 2: Hyper Backup Explorer (veilig testen)	56
	Cloudback-up testen: Backblaze B2	59
	Configuratieback-up: DSM-instellingen	60
	Waarom is dit belangrijk?	60
	Automatische back-up naar je Synology-account	60
	Handmatige export naar je computer	61
	Wanneer gebruik je dit?	61
	Hele systeemherstel: alleen voor Vault en C2	62
	Back-ups via de 3-2-1-regel (en regelmatig testen)	62
■ 5	Gebruikers toevoegen en rechten instellen	63
	Wat lees je in dit hoofdstuk?	63
	Een dilemma: één account of twee?	64
	Tweefactorauthenticatie aanzetten voor iedereen	64
	Account toevoegen	65
	Aan het werk met de NAS	70

■ 6 Synology Photos, Audio Station, Drive en Office 71

Wat lees je in dit hoofdstuk?	71
Synology Drive en Synology Office	72
Synology Drive en Office installeren	72
NAS en Chromebook	74
Synology Photos: je eigen Google Foto's	74
Installatie en eerste indruk	75
Mobiele app Synology Photos gebruiken	76
Gezichtsherkenning in de praktijk	77
Onderwerpen en automatische herkenning	77
Albums maken en delen	77
Verschillen met Google of Apple Foto's	79
Overstappen van Google/Apple Foto's of niet?	79
Audio Station: je eigen muziekstreaming	80
Waarom weg van Spotify?	80
Gedeelde map music	81
Je eigen map met muziek	82
Mijn muziekcollectie uploaden	83
Technische mogelijkheden	83
DS Audio onderweg	83
Audio Station voor iedereen?	84
Praktijkvoorbeeld: 25.000 mp3's uploaden	84
Synology Office	85
Google Docs vergeleken met Synology Documents	85
Spreadsheet en Dia's	86
Synology Office versus Google/Microsoft	87
Synology AI Console	87
De afweging	88
Synology-apps: het NAS-experiment gaat verder	88

■ 7 Eigen domein voor je NAS 91

Wat lees je in dit hoofdstuk?	91
Drie manieren	92
Het verschil zit vooral in certificaten en Docker	92
Wat te kiezen?	93
Belangrijk keuzemoment	94
Nog een waarschuwing	94
Ziggo's modem	95

Stap voor stap je eigen domein instellen voor je NAS	95
Stap 1: DNS-configuratie bij je domeinaanbieder aanpassen	95
Stap 2: Port forwarding configureren in je router	96
Poorten beveiligen: de deuren naar je digitale huis	98
Welke poorten heb je nodig?	99
Essentiële beveiligingsmaatregelen	99
Monitoren en onderhouden	100
Geoblocking instellen	101
Stap 3: DSM-configuratie	102
DSM-poorten controleren	102
Externe toegang configureren	103
Stap 4: SSL-certificaat aanvragen	104
Certificaat toewijzen aan services	105
Van afhankelijkheid naar onafhankelijkheid	106
 ■ 8 Docker begrijpen: de eerste container	 107
Wat lees je in dit hoofdstuk?	107
Mogelijkheden van Docker	108
Containers versus 'gewone' applicaties	109
Wat Container Manager precies doet	109
Functie	109
Images, containers en volumes	110
Images (het statische softwarepakket)	110
Container (de dynamische, actieve instantie)	110
Volume (de permanente datakoppeling)	110
Container Manager installeren	111
Installatie via Package Center	111
Wat is dat brugnetwerk?	111
Interface	112
Eerste container: Jellyfin-mediaserver	113
Waarom Jellyfin en niet Plex?	114
Jellyfin installeren als je eerste container	115
Basisprincipes van Docker	124
Probleemoplossing	124
Container start niet	124
Jellyfin is onbereikbaar	125
Jellyfin ziet mijn mediabestanden niet	125
Container crasht steeds	125

Containers beheren	126
Container stoppen en starten	126
Container verwijderen	126
Image bijwerken	127
Verder met Container Manager	127
 ■ 9 Portainer en Nginx Proxy Manager	 129
Wat lees je in dit hoofdstuk?	129
Rampspoed en gevloek	130
Wat is Docker Compose?	131
Waarom Portainer en niet Container Manager?	132
Docker Compose en het YAML-bestand	132
Toegang tot alle Docker-functionaliteit	134
Waarom hebben we toch Container Manager nodig?	135
Portainer installeren	135
Waarom SSH in plaats van de GUI?	135
Portainer installeren via SSH	136
Netwerk toevoegen in Portainer	140
Nginx Proxy Manager (NPM)	141
Machtigingen correct instellen voor Docker-containers	142
Deploy the stack	143
De NPM-YAML uitgelegd	143
NPM gaan gebruiken	144
Waarom NPM?	145
Het probleem met poortnummers	145
Wat doet een reverse proxy?	145
Waarom niet de reverse proxy van Synology?	146
Voor wie is NPM geschikt?	146
Port forwarding aanpassen voor NPM	147
Probleem in het kort	147
Port forwarding wijzigen in je router	147
Proxy hosts toevoegen	148
Voorbereiding: A-records controleren	149
Proxy host 1: eigendomein.nl naar DSM	150
Proxy host 2: npm.eigendomein.nl naar NPM	151
Proxy host 3: portainer.eigendomein.nl naar Portainer	152
Wat hebben we bereikt?	153

■ 10 Photoprism en Nextcloud	155
Wat lees je in dit hoofdstuk?	155
Photoprism als alternatief voor Immich	156
Photoprism installeren	156
Aan de gang met Photoprism	157
Apps voor automatische foto-upload naar Photoprism	159
Tevreden met Photoprism?	160
Nextcloud als complete cloudoplossing	160
Installatie van Nextcloud	161
Waarom Nextcloud toch niet voor me werkte	162
Conclusie: terug naar de tekentafel	164
■ 11 Immich: je eigen Google Foto's	165
Wat lees je in dit hoofdstuk?	165
Waarom juist Immich?	166
Andere oplossingen vielen tegen	166
Een vergelijking tussen Immich en Google Foto's	166
Immich installeren	167
Installatie-uitdagingen	167
Het probleem: de poort was veranderd	168
YAML en de proxy host	168
Immich: de eerste stappen	169
Google Cast: wel of niet aanzetten?	169
Denk aan je back-upstrategie	169
Immich-app gebruiken	170
Foto's uploaden naar de server	170
Let op: de eerste upload is zwaar werk voor je NAS	171
Gezichtsherkenning in Immich	171
Albums maken, albums en foto's delen en Partner Sharing	171
Immich is nog in ontwikkeling	172
■ 12 De balans opmaken: wat lukte en wat niet	173
Waarom ik dit wilde aanpakken	173
Wat ik gebouwd heb	174
De balans	175
Dockerfrustratie	176

Immich	177
Maar wordt het gebruikt?	178
De andere applicaties	178
Het echte probleem: timing	179
Privacy buiten de NAS	179
Sociale media en communicatie	179
Google Takeout: de grote export	180
E-mail: de Gmail-verslaving doorbroken	180
Wat zou er nodig zijn voor succes?	180
De eindbalans	181
Dit is geen eindpunt, dit is een startpunt	181
Voor jou, lezer	182
 A Lijst van gebruikte afkortingen in dit boek	 183
 B Extra veiligheidsmaatregelen voor Docker	 187
Tailscale en Synology VPN: de veiligste route	188
Rate limiting: bruteforceaanvallen blokkeren	188
Immich en 2FA	189
Authelia	189
 C Stacks en Portainer bijwerken	 191
Wat lees je in deze bijlage?	191
Stacks bijwerken	191
Wanneer werk je een Stack bij?	191
Stappen	191
Portainer bijwerken	192
Waarom kan Portainer zichzelf niet bijwerken?	192
Portainer bijwerken via SSH	192
Samenvatting: zo blijf je up-to-date	195
 Index	 197

Voorwoord

■ Loskomen van Big Tech

Begin juni vorig jaar schreef ik op het blog **computercreatief.nl** een blogpost met de titel *Een NAS voor zelf-hosten: je eigen cloud in de meterkast*. Het was een vervolg op een eerdere blogpost over het loskomen van Big Tech. Ik realiseerde me hoe afhankelijk we zijn van die Amerikaanse techgiganten. Wat weet Big Tech allemaal van ons? Wat weet Google van mij?

Google verzamelt niet alleen je foto's, documenten en e-mails; ze analyseren ook wat er in en op staat. Die leuke vakantiekiekjes? Google weet waar ik ben geweest, met wie ik op de foto sta (gezichtsherkenning) en wat ik aan het doen was. Mijn Google Docs? Die worden gescand op content. Mijn Gmail? Idem dito.

Het is natuurlijk niet zo dat er een medewerker van Google over mijn schouder meekijkt, maar hun algoritmen kijken wel mee. En die informatie wordt gebruikt voor advertenties, productverbetering en wie weet wat nog meer. De Amerikaanse Cloud Act-wet zorgt er bovendien voor dat Amerikaanse bedrijven verplicht kunnen worden om data af te staan aan de overheid. Ook als die data op Europese servers staat. En die data kan alle informatie bevatten die Google of Microsoft over jou of mij heeft.

En laten we eerlijk zijn: in deze rare tijden weten we niet wat de huidige Amerikaanse regering van ons weet of wil weten. Met alle politieke spanningen en de onvoorspelbaarheid van het Amerikaanse beleid is het misschien wel verstandiger om niet volledig afhankelijk te zijn van Amerikaanse techgiganten. Zelf hosten betekent dat je data gewoon in Nederland blijven, onder Nederlandse en Europese wetgeving.

Ik som de problemen die ik heb met die diensten van Google en Microsoft even op.

- Ten eerste privacy: je data worden gescand, geanalyseerd en gebruikt voor doeleinden waar je misschien niet blij mee bent. Dan heb je het controleverlies: Google of Microsoft bepaalt wat je wel en niet kunt doen met je eigen bestanden. Account geblokkeerd? Pech gehad, je data zijn weg.

- Die ‘gratis’ diensten zijn bovendien alleen gratis tot je meer nodig hebt – dan betaal je maandelijks voor opslag die je zelf veel goedkoper kunt regelen.
- Je wordt ook afhankelijk van hun keuzes. Als Google besluit om een dienst stop te zetten, ben je de pineut.
- En niet te vergeten: je data staan op servers in andere landen, onder Amerikaanse wetgeving.

En dus wilde ik er vanaf. Stel je voor: je eigen Google Drive op een kastje in je meterkast. Een eigen Google Photos die alleen voor jou en je gezin is. Een eigen cloud voor je eigen bedrijf. Je eigen cloud waar geen algoritme meekijkt en waar jij de baas bent. Klinkt goed, toch?

■ Helemaal los van Big Tech?

En ik vond het goed klinken. Ik nam me voor om een eigen server te gaan draaien met daarop de cloud en de applicaties die je nodig hebt. Een server voor selfhosting helemaal zelf in elkaar zetten leek me te ingewikkeld en ik kwam uit bij de Synology NAS, een Synology DS224+ van zo’n € 750,- (inclusief harde schijven en geheugenuitbreiding).

Ik maakte mijn vrouw Linda, mijn dochter Lisa en zoon Rufus enthousiast over het idee ‘baas zijn over je eigen data’. Nu gaan we zien of het voor ons werkt. De basis is gelegd.

Als je dit boek hebt gelezen kun je weer baas worden over je eigen data en ben je minder afhankelijk van Big Tech. En misschien vind je het net zo leuk om die NAS op te zetten en te experimenteren met nieuwe applicaties. Ik heb nieuwe kennis opgedaan over Docker en containers, technieken waar ik voordat ik hieraan begon geen weet van had. En die kennis heb jij ook als je het boek uit hebt.

Ben ik zelf nu helemaal los van Big Tech? Nee, dan moet ik helemaal van internet af en terug naar een domme telefoon. Maar Google analyseert mijn data in ieder geval bijna niet meer. Over mijn foto’s en documenten ben ik in ieder geval weer de baas.

Nog een paar zaken over de totstandkoming van dit boek. Ik had een paar meelezers die me adviezen gaven. Yoram, Linda en Michiel: dank daarvoor. En eigenlijk had ik nog drie andere meelezers: ik maakte veelvuldig gebruik van AI voor het uitzoeken van technische problemen. Het hele boek sloeg ik op in een project van Claude, die las alle hoofdstukken mee. Met Claude, Gemini en Perplexity loste ik de technische problemen op die ik tegenkwam. Daardoor draait bijvoorbeeld Immich nu op de NAS en gebruik ik Pi-hole om ons netwerk af te schermen van te veel advertenties. Er wordt veel gemopperd over AI,

dat het niet echt slim is bijvoorbeeld. Niet slim? Misschien is dat zo, maar samen losten we telkens toch een probleem op. (AI kreeg ik soms ook hele stomme antwoorden. En ja, AI is ook onderdeel van Big Tech; het is niet anders. En Europese AI is nog niet goed genoeg...)

Ik heb in ieder geval veel plezier gehad met het maken van dit boek. Ik hoop dat je dat erin terug kunt lezen.

Amsterdam, januari 2026

Hans Frederiks



Bonusmateriaal

Online heb ik nog drie bonusbijlagen voor je klaargezet plus een setje YAML-bestanden; wat je daarmee kunt lees je verderop in dit boek. Surf naar **mijn.cc/yaml** om alles in één keer te downloaden!

Waarom zelf hosten?

Als je dit leest heb je het boek Loskomen van Big Tech al gekocht en weet je al een beetje waarom je al je bestanden, je foto's en je data zelf op een veilige plek zou willen bewaren en toegankelijk maken. In dit eerste hoofdstuk zet ik op een rijtje waarom je zelf zou willen hosten en wat de mogelijkheden daartoe zijn met een moderne Synology NAS.

■ Wat lees je in dit hoofdstuk?

- Het Big Tech-probleem: waarom je afhankelijkheid van Google, Microsoft en Apple een risico vormt voor je privacy en controle over je eigen data, en hoe de Amerikaanse Cloud Act jouw Europese data onder Amerikaanse wetgeving brengt.
- De werkelijke kosten van 'gratis': hoe Google, Microsoft en Apple je persoonlijke gegevens analyseren en verkopen, en waarom een eigen NAS op lange termijn zowel privacyvriendelijker als goedkoper is dan cloudabonnementen.
- De realistische afwegingen: welke voordelen en verantwoordelijkheden komen kijken bij self-hosting, en waarom complete loskoppeling van Big Tech niet altijd haalbaar of praktisch is.

■ Het Big Tech-probleem

Je gebruikt bijvoorbeeld een telefoon met daarop Google Foto's, een computer waarop je Google Drive hebt staan, je gebruikt Gmail en Google Docs... je zit, kortom, volledig in het Google-universum. Dan raakt ineens je gratis opslag vol en moet je gaan betalen voor de opslag in de Google-cloud. Ondertussen lees je in de krant dat Microsoft de e-mail blokkeert van de hoofdaanklager van het Internationaal Strafhof (ICC). Het ICC in Den Haag wordt hard geraakt door de recente Amerikaanse sancties. Zo heeft hoofdaanklager Karim Khan geen toegang meer tot zijn Microsoft-e-mail-account. Je realiseert je dat je voor de meeste diensten die je gebruikt afhankelijk bent van Big Tech-bedrijven als Microsoft, Apple en Google. Dat jouw gegevens, jouw data, jouw foto's alle-

maal op servers staan in Amerika en dat zo'n bedrijf je zomaar, ineens, kan afsluiten.

Dat afsluiten van toegang tot je data is één reden om die dan maar zelf te gaan hosten. Een ander belangrijk argument om zelf te hosten is het aspect privacy. Neem Google. Wat weet dat bedrijf allemaal niet van jou!? Je gebruikt de Google-software, je reist met aanwijzingen van Google Maps en je gebruikt meeluisterende speakers van Amazon of Google. Ja, Google Foto's is zo handig en kan zo veel, maar heb je enig idee wat Google allemaal over je weet, dankzij die foto's?

■ Wat Google werkelijk ziet in jouw foto's

De programmeur Vishnu Mohandas, die jarenlang bij Google werkte, maakte bij zijn bedrijf Ente een tool waarmee je een foto kunt uploaden en die kunt laten analyseren. Die tool laat zien wat Google allemaal in die foto 'ziet'. Als je leest wat dat is en wat voor conclusies er worden getrokken, dan schrik je je een ongeluk. Ik probeer het nog eens met een foto van de afsluiting van het hockeyseizoen van mijn kleinzoon. Daarop staat een groepje kinderen dat net een medaille of diploma heeft gekregen. Google ziet daarin het volgende:

Op deze foto staat een groep kinderen trots na wat een sportevenement lijkt te zijn in Amsterdam. Op de voorgrond staan de kinderen met medailles om hun nek, sommigen met certificaten en een trofee, wat suggereert dat ze iets belangrijks hebben bereikt. Een net strekt zich uit over de scène, wat verwijst naar een hockeywedstrijd. Op de achtergrond zijn een zwart hek, bomen, fietsen en een auto te zien.

De kinderen zijn van verschillende rassen, waaronder overwegend blank en van gemengde etniciteit, en hun geschatte gezinsinkomen varieert van € 30.000 tot € 80.000 per jaar. Ze hebben waarschijnlijk een christelijke of seculiere achtergrond. Hun politieke voorkeuren, indien aanwezig, zijn waarschijnlijk gelieerd aan de VVD. De kinderen vertonen een scala aan emoties, van vreugde en opwinding tot kalme tevredenheid. Ze dragen een mix van sportkleding en vrijetijdskleding, wat een ontspannen, maar feestelijke sfeer suggereert. Hun interesses kunnen hockey en andere sporten, buitenactiviteiten, onderwijs en sociale interactie met vrienden zijn. Een mogelijke negatieve invloed kan overmatige schermtijd, ongezonde eetgewoonten en uitstelgedrag zijn.

Deze kinderen lijken extraverte eigenschappen, een matig zelfbeeld en een gemiddelde zelfbeheersing te bezitten. Daarom kunnen we ze targeten met sportuitrusting, educatief speelgoed en ervaringen die sociale interactie bevorderen, zoals: RitFit Hockey Training Set, educatief STEM-speelgoed van Lego, een Decathlon hockeystick, Nike sportkleding en BuitenSpeel buitenspeelgoed, McDonald's Happy Meals, Netflix Kids-programma's en educatieve boeken van Bol.com.



■ Wat Google allemaal kan zien op een foto.

Zeg nu zelf: de informatie die Google uit deze foto denkt te halen, gaat heel ver. Geschat inkomen, VVD, christelijk of seculier, targetten met allerlei spullen... doodeng. Ja, Google Foto's is gratis, maar dit is de prijs die je betaalt aan Google: info over jou en je familie, met het doel je spullen te verkopen. Veel mensen beseffen niet dat deze 'gratis' diensten eigenlijk betaald worden met hun persoonlijke data.

■ Cloud Act: jouw data onder Amerikaanse controle

Het kan nog erger. Wat als er iemand – jij, je kleinzoon of -dochter, of gewoon iemand die langsluip – een Palestijnse keffiyeh omheeft? Dat staat op een foto en die foto staat op je telefoon, of in de cloud. Je bent net geland in New York en je staat bij de immigratie. Hebben ze in opdracht van de Amerikaanse regering jouw foto's gescand om te kijken wat jouw politieke overtuiging is? Daar sta je dan, met die voorbijganger in die keffiyeh. Misschien/waarschijnlijk kom je daardoor het huidige Amerika helemaal niet in.

Dankzij de Cloud Act mag de Amerikaanse overheid kijken wat er op Amerikaanse servers in de cloud staat. Die Cloud Act-wet geeft de Amerikaanse regering het recht om toegang te eisen tot alle data die worden opgeslagen door Amerikaanse bedrijven, ook als die data op servers in Europa staan. Dus al die foto's die je zo netjes hebt opgeslagen in Google Drive 'in Nederland'? Ze vallen gewoon onder Amerikaanse wetgeving.

Stel je voor: je bent een kleine ondernemer en je bewaart klantdata bij Microsoft. Ineens besluit de Amerikaanse regering dat ze toegang wil tot bepaalde informatie. Microsoft moet die toegang geven, ook al staan die servers in Amsterdam. Jouw klantdata, hun privégegevens, zomaar overgedragen aan een buitenlandse regering. En jij als ondernemer hebt daar niets over te zeggen. Of neem het Internationaal Strafhof dat ik net noemde. Karim Khan kon ineens niet meer bij zijn Microsoft-account. Dat was geen technische storing, dat waren sancties. Zo makkelijk kan het gaan: je bent afhankelijk van een Amerikaans bedrijf, Amerika is het niet eens met wat je doet, en klaar is je digitale leven.

De Cloud Act maakt van alle data van Europese gebruikers eigenlijk Amerikaanse data. Het maakt niet uit dat Google zegt dat je gegevens "veilig in Europa" staan. Als Washington belt, gaan die data gewoon de oceaan over. En daar kun je als gebruiker helemaal niets tegen doen.

■ Mijn eigen Big Tech-verslaving

Het zijn twee onderdelen die met elkaar te maken hebben: jouw privacy en die Amerikaanse Cloud Act. Je wilt dat jouw data van jezelf zijn en dat ze niet voor het grijpen liggen voor wie dan ook, en zeker niet voor de Amerikaanse regering. Misschien moet je eens kijken wat er allemaal van jou in de cloud staat en welke apps je daarbij gebruikt. Voor mezelf zet ik het op een rijtje.

Ik gebruik nogal veel van Google. Drive en Docs bijvoorbeeld. Al mijn schrijfwerk schrijf ik in Google Docs (dat is zo handig en altijd overal beschikbaar enzovoort). Mijn bescheiden boekhouding staat in Google Sheets-documenten. En Google Foto's natuurlijk. Daarin staan meer dan 100.000 foto's van mijn familie, vakanties, mijn 'artistieke' prestaties tot op de dag van vandaag bijhouden en natuurlijk door Google geanalyseerd. We gebruiken Google Calendar, waarin allerlei privé-afspraken staan. Wanneer had ik een afspraak met de dokter, met welke vrienden, Google weet het allemaal.

Ik heb zoals zo veel mensen een Gmail-adres. Een handig e-mailadres dat je altijd en overal voor kunt gebruiken. Ik heb meer e-mailadressen en die had ik – tot voor kort – allemaal verzameld in de Gmail-app. Zo kwam alle mail daar samen. En – je begrijpt het al – Google kan al die e-mail ook analyseren. (Inmiddels gebruik ik Thunderbird op mijn Android-telefoon en -tablet voor mijn vijf mailadressen.)

Gmail is meer dan alleen e-mail: het is de sleutel tot het hele Google-universum. Mijn Gmail-account, eigenlijk je Google-account, is gekoppeld aan mijn Android-telefoon, Google Drive, YouTube en tientallen andere services. Gmail scant al mijn berichten voor advertenties en profilering, weet precies met wie ik contact heb en hoe vaak, en Gmail kan zomaar worden afgesloten als Google daar behoefte aan heeft. Het probleem: hoe kom je van Gmail af als het inmiddels de basis is geworden voor al je andere online accounts?

Google Maps is ook al zo handig, waardoor Google altijd weet waar je was en dat weer zo handig kan koppelen aan je foto's.

Om contactloos met mijn telefoon te betalen (ook al zo handig) moet ik van mijn bank gebruikmaken van Google Wallet. Google Wallet is 'veilig' voor mijn bankgegevens (ze weten niet het bedrag, mijn saldo en aan wie ik heb betaald), maar geeft wel meer informatie voor mijn profiel. Het kan met gps zien waar ik was en daar koopconclusies aan verbinden. Google Wallet is ook zo handig om je tickets in te bewaren, dus weet Google naar welk concert, welke tentoonstelling of welke theatervoorstelling ik ben geweest. Nog meer? Vast wel, maar is dit al niet genoeg? Ik zou best van mijn Gmail-account af willen, maar dat Gmail-account is essentieel voor alle apps en mogelijkheden die Google biedt.

■ **Microsoft: Office en OneDrive onder Amerikaanse controle**

Ik ben geen uitgebreide Microsoft-gebruiker. Maar als ik erover nadenk, zit ik voor een deel ook in dat universum. Ik heb een Microsoft-account, ik draai via Parallels Windows 11 op mijn Mac en ik weet dat Microsoft ook geen lieverdje is als het om privacy gaat. Als je Windows installeert, moet je door allerlei hoepels springen om te voorkomen dat ook Microsoft je privacy gaat schenden.

Gebruik je Microsoft 365? Staan je documenten in OneDrive? Voor OneDrive geldt hetzelfde als voor Google Drive: alles wat daarin staat kan worden gelezen door Microsoft en als de Amerikaanse justitie jouw documenten wil inzien, kan dat ook. Je mailaccount bij Microsoft kan dus zomaar worden afgesloten als de Amerikanen dat willen.

■ Apple: privacymarketing versus Cloud Act-realiteit

En Apple dan?, zul je zeggen. Die zijn toch zo voor privacy? Hun marketing-slogan *What happens on the iPhone stays on the iPhone* klinkt overtuigend, en Apple heeft inderdaad een betere privacyreputatie dan Google of Facebook. Maar als je de details bekijkt, is het verhaal genuanceerder.

Apple versleutelt veel data op je iPhone zelf. Je foto's, berichten en contacten zijn beschermd met sterke encryptie. Toen de FBI in 2016 wilde dat Apple een iPhone zou ontgrendelen na een aanslag, weigerde Apple dat: ze hadden letterlijk niet de sleutels om die encryptie te breken.

Maar dan komt iCloud. Het probleem begint zodra je iCloud inschakelt. Die handige back-up van je iPhone? Je foto's die automatisch synchroniseren? Die staan dan wél op Apple-servers in Amerika. En hoewel Apple deze data versleutelt tijdens transport en opslag, heeft Apple zelf wél de sleutels om je iCloud-data te ontsleutelen.

Dit betekent concreet: als de Amerikaanse overheid Apple om jouw iCloud-data vraagt, kunnen ze die gewoon geven. En dat doen ze ook. Apple heeft in 2022 aan meer dan 5000 verzoeken van Amerikaanse autoriteiten voldaan voor toegang tot iCloud-accounts.

Advanced Data Protection: een stap vooruit

Apple heeft wel geluisterd naar kritiek. Sinds 2023 bieden ze *Advanced Data Protection* aan, waarbij ook iCloud-data wordt versleuteld met sleutels die alleen jij hebt. Maar dit is:

- standaard uitgeschakeld; en
- niet beschikbaar in alle landen.

Bovendien: je bent je data kwijt als je je sleutels verliest.

De meeste Apple-gebruikers hebben dit dus niet ingeschakeld en vallen gewoon onder Amerikaanse Cloud Act-wetgeving.

Apples privacy is inderdaad beter dan Googles businessmodel van het verkopen van je data voor advertenties. Maar uiteindelijk zijn het allemaal Amerikaanse bedrijven onder Amerikaanse jurisdictie. Je betaalt Apple wel voor privacy, maar krijgt alleen échte privacy als je alles lokaal houdt en dat is niet hoe de meeste mensen hun iPhone gebruiken.

■ Kostenaspect

Van die diensten en apps is er heel veel gratis. Google Drive, OneDrive en iCloud zijn als je ermee begint gratis. Maar als je steeds meer documenten, foto's en films in de cloud opslaat, loopt die gratis opslagruimte vol en zul je moeten gaan betalen.

Voor een gezin of klein bedrijf kom je al snel uit op ongeveer € 120 per jaar bij alle drie de grote aanbieders:

■ Google One Familie (2 TB): € 120/jaar

■ Microsoft 365 Familie (6 TB + Office): € 120/jaar

Apple iCloud+ Familie (2 TB): € 120/jaar

Een Synology NAS met twee schijven van 6 TB kost eenmalig ongeveer € 750. Tel je daar de levensduur van ongeveer zes jaar bij op, plus eventuele schijfvervanging en back-upkosten, dan kom je alsnog goedkoper uit dan de cloud-abonnementen. Na ongeveer zes jaar heb je de investering terugverdiend, en daarna bespaar je elk jaar € 120. Maar laat ik eerlijk zijn: je doet het niet per se voor het geld. Het echte voordeel is je privacy en onafhankelijkheid van Big Tech. Het financiële voordeel is mooi meegenomen, maar je vrijheid is onbetaalbaar.

■ De andere kant van de medaille

Dat zijn de voordelen. Nu de redenen waarom je goed moet nadenken voordat je het gaat doen. Een belangrijk nadeel: het is jouw verantwoordelijkheid om je data en die van je medegebruikers veilig te houden. Je wordt de systeembeheerder; jij bent degene die ze vragen gaan stellen als iets niet werkt. Jij bent verantwoordelijk als je NAS wordt gehackt. Je moet je verdiepen in die problematiek, in de installatie en het onderhoud. De basismogelijkheden van Synology zijn best uitgebreid en zijn voor een beginner te doen. Maar je kunt dieper gaan met Docker en apps die daarbij horen, zoals Immich en dat wordt een stuk ingewikkelder.

Daarnaast moet je je realiseren dat niet alles haalbaar is. Wil je in de auto af van Google Maps? En die handig gedeelde kalender, die je met je gezinsleden of medewerkers deelt? Synology Photos is handig, maar in Google Foto's kun je de foto's meteen bewerken en krijg je steeds meer mogelijkheden. Loskomen van Big Tech gaat niet een-twee-drie. Als je hieraan begint, zul je telkens een afweging maken wat je wilt behouden en waar je je privacy wilt beschermen. Maar je leest deze inleiding in het boek, dus je wilt beginnen. In de twee volgende hoofdstukken lees je over de NAS die ik heb gekocht, de alternatieven en het draaiend krijgen van het apparaat.