Belle van der Velde
500906306
27/09/2026

Weekopdracht individueel - Reflectie

Eigen onderzoek
De bron die ik het meest interessant vindt, is die over Meta en Google. Ik wist vooraf wel dat Google en Meta veel geld verdienen met advertenties, maar ik had niet verwacht dat de bedragen zo hoog zouden zijn. Hierdoor werd mij duidelijk dat de advertentieveilingen heel groot zijn.
Ik wist dat je advertenties krijgt te zien die aangepast zijn aan jouw online gedrag. Ook dat Google en Meta hierin erg groot zijn. Hoe het precies in zijn werk gaat en hoe snel het gebeurt wist ik nog niet.
Ik heb vooral geleerd hoe snel de veilingen plaatsvinden en welke partijen hier allemaal bij komen kijken. Ook had ik niet eerder over programmatic advertising gehoord en dat real time bidding daar een onderdeel van is.
Wat mij aan het denken heeft gezet is de hoeveelheid gegevens die gebruikt worden. Daarbij weet je ook niet langs hoeveel partijen de gegevens gaan, waardoor het niet erg transparant is. Ik ga steeds bewuster nadenken over waar mijn gegevens allemaal voor worden gebruikt en op welke manier dat gaat.

Presentatie AT-protocol – David en Helena

Wat wist ik al?
Ik wist al dat Bluesky en Eurosky bestonden en had een ongeveer beeld van hoe ze werkten.

Wat heb ik geleerd dat nieuw voor me was?
Het AT Protocol bleek redelijk nieuw te zijn. Ik wist ook niet dat het protocol zo open is opgezet, waardoor je heel makkelijk bij de data van iedereen kunt komen. Alle berichten, likes en het hele sociale netwerk zijn openbaar en toegankelijk. Ook nieuw was dat je met dit protocol makkelijk van platform kunt wisselen zonder je volgers of berichten kwijt te raken, omdat je gegevens niet vastzitten aan één bedrijf zoals nu bij Instagram of X wel het geval is.

Wat heeft me aan het denken gezet, en waarom?
Ik ga vooral nadenken over waarom iemands data zo makkelijk toegankelijk is voor anderen en of daar iets aan te doen valt. Aan de ene kant snap ik dat die openheid juist het doel is, zodat niet een bedrijf alle controle heeft en mensen makkelijk kunnen overstappen. Maar aan de andere kant vraag ik me af of gebruikers zich wel altijd bewust zijn van hoe openbaar hun gegevens dan zijn.

End to end encryptie

End-to-end encryptie betekent dat een bericht al op jouw eigen telefoon wordt vergrendeld en pas op de telefoon van de ontvanger weer open kan. Daarvoor heeft iedereen twee sleutels, een publieke en een privésleutel. Met de publieke sleutel van de ontvanger vergrendel je het bericht, en alleen de privésleutel van de ontvanger kan het weer openen. Bij gewone versleuteling, zoals Telegram die standaard gebruikt, wordt het bericht bij het bedrijf zelf eerst geopend en daarna opnieuw dichtgedaan om door te sturen. Daardoor kan het bedrijf in principe meelezen. Bij end-to-end encryptie kan dat niet, en dus kan het bedrijf de berichten ook niet aan de anderen geven.

Toch is end-to-end encryptie niet perfect. De inhoud van een bericht blijft geheim, maar de gegevens eromheen niet. Dat heet metadata en het gaat om wie wanneer met wie appte en vanaf welk IP-adres. Die informatie kan wel worden bewaard en door justitie worden opgevraagd. Een back-up in de cloud kan ook een zwak punt zijn. Je chats zijn op je telefoon dan wel versleuteld, maar de kopie in de cloud niet altijd. Ook is de versleuteling niet sterk meer als iemand toegang heeft tot je telefoon. Als iemand toegang krijgt tot je telefoon, maakt het niet meer uit hoe goed de berichten versleuteld zijn.
Daarnaast bestaat er ook een truc waarbij een hacker zich tussen twee mensen in wringt en doet alsof hij de ontvanger is, zodat hij de sleutels kan onderscheppen voordat het gesprek goed en wel begint.

In de politiek zijn ze al langere tijd aan het discussiëren over end-to-end encryptie. Ze willen een chatcontrole, waarbij je zou moeten meekijken met chatberichten. Dit willen ze om bijvoorbeeld criminaliteit en kindermisbruik tegen te gaan. Door de end-to-end encryptie is het lastiger misdaden op te sporen, omdat criminelen onderling vrij contact kunnen houden over zaken. End-to0end ecryptie is dus goed voor de vrijheid en privacy van mensen, maar brengt ook nadelen met zich mee.

https://hcc.nl/kennis/kennis/vraag-van-de-week/hoe-werkt-end-to-end-encryptie-en-wat-zijn-de-risico-s

https://nieuws.crypto.nl/net-binnen/eu-verlengt-chatcontrole-tot-2028-wat-betekent-dit-voor-privacy-en-encryptie/

Reflectievragen
Wat wist ik al?
Ik wist al dat WhatsApp en Signal versleutelde berichten gebruiken, en dat dit betekent dat een berichtendienst niet zomaar kan meelezen met je gesprekken.

Wat heb ik geleerd dat nieuw voor me was?
Nieuw voor mij was dat Telegram dit standaard niet doet en dat je daar zelf een geheime chat voor moet starten om berichten echt end-to-end versleuteld te krijgen. Ook wist ik niet dat een cloud-back-up van je chats soms niet versleuteld is, terwijl de berichten zelf dat wel zijn.

Wat heeft me aan het denken gezet, en waarom?
Het meest heeft me aan het denken gezet dat end-to-end encryptie eigenlijk twee kanten heeft. Aan de ene kant beschermt het gewone mensen tegen meekijkende bedrijven of overheden, maar aan de andere kant maakt het opsporen van criminelen ook moeilijker. Ik vond het lastig om daar zelf een mening over te vormen, want ik snap beide kanten.

Cloud
De cloud is eigenlijk niets anders dan de computers van een ander bedrijf. Je bestanden staan niet op je eigen apparaat, maar in datacenters. Dat zijn grote gebouwen vol harde schijven die over de hele wereld staan. Je komt erbij met een account en een wachtwoord. Meestal staan er meerdere kopieën op verschillende plekken, zodat je

bestanden er nog zijn als één datacenter uitvalt.

Het probleem zit vooral bij wie de cloud beheert. 67 procent van 16.500 onderzochte Nederlandse websites is gekoppeld aan minstens één Amerikaanse clouddienst. Door de Amerikaanse CLOUD Act kan de Amerikaanse overheid gegevens opvragen bij Amerikaanse bedrijven ook als die gegevens op servers in Europa staan. Nederlandse organisaties kunnen zelfs buitengesloten worden van hun eigen gegevens, met grote gevolgen voor de samenleving. Echter is de kans dat de VS via deze wet echt bij Europese persoonsgegevens komt in de praktijk klein. Een ander risico zit in de vraag of je kunt controleren dat er geen verborgen toegang in de techniek is ingebouwd, waardoor er toch een weg is naar je gegevens.

https://3bplus.nl/cloud/hoe-werkt-de-cloud-de-cloud-uitgelegd/

https://nos.nl/artikel/2599837-nederlandse-cloud-binnen-handbereik-tweede-kamer-wil-haast-maken

Reflectievragen

Wat wist ik al?
Ik wist al dat de cloud betekent dat je bestanden niet op je eigen apparaat staan maar ergens op een server, en dat je daar via internet bij kunt. Ik gebruik zelf ook clouddiensten zoals Google Drive en wist dat die bestanden dan ergens in een datacenter staan.

Wat heb ik geleerd dat nieuw voor me was?
Nieuw voor mij was dat zoveel Nederlandse websites afhankelijk zijn van Amerikaanse cloudbedrijven. Ik wist ook niet dat er een Amerikaanse wet bestaat, de CLOUD Act, die ervoor zorgt dat de Amerikaanse overheid gegevens kan opvragen bij Amerikaanse bedrijven, zelfs als die gegevens op servers in Europa staan.

Wat heeft me aan het denken gezet, en waarom?
Het verraste me dat de locatie van een server dus niet alles zegt, het gaat er meer om welk bedrijf de server beheert. Dat vond ik best confronterend, want ik had daar zelf nooit bij stilgestaan als ik iets in de cloud zet. Ik ga dan toch beter nadenken wat ik zelf gebruik en welk bedrijf dat beheert.