15. Maj 2021

GDPR, Schrems II - og det ingen tør sige højt

Der bliver lavet en masse politisk og juridisk tankearbejde for at komme uden om den temmelig store udfordring, som Schrems II har efterladt.

Vi tager her et kik på udfordringen fra en teknisk og praktisk vinkel.

Lad os starte med at se på, hvad problemet egentligt er.
Lidt firkantet sagt har GDPR pålagt alle virksomheder og myndigheder at sørge for, at deres data om ansatte og brugere/borgere/kunder ikke kommer i hænderne på uvedkommende.

På den anden side har vi blandt andre diverse efterretningstjenester (og her ignorerer jeg lige efterretningstjenesterne fra EU lande). Disse tjenester har en meget stor opgave i at skaffe sig adgang til alt det data, de overhovedet kan, uanset hvordan.

I Schrems (I og II) er USA 'fjenden', fordi vi i EU gerne vil bruge deres kommercielle services. I USA har de Patriot's Act som - i pixie versionen - giver diverse efterretningstjenester ret til tre ting, nemlig

1. pålægge enhver amerikansk virksomhed at udlevere alt det data virksomheden på nogen måde kan få fingre i

2. pålægge enhver amerikansk virksomhed at holde fuldstændigt tæt med ovenstående

3. gøre livet rigtigt, rigtigt surt for enhver amerikansk virksomhed, der ikke retter ind (hemmelige domstole og den slags)

Efter at have kridtet banen op med 'The good guys', dvs. EU med databeskyttelse for øje og 'The bad guys', dvs. stort set alle andre, som vil have fat i vores data, skal vi se på, hvad det helt praktisk betyder.

Lad os starte blødt med den allesteds nærværende cloud. I lyset af ovenstående kan man ikke bruge nogen form for service, der ejes af et ikke-EU firma. Man kan heller ikke bruge en service, hvor en ikke-EU virksomhed har bestemmende (del)ejerskab.

Nu kunne man forledes til at tænke, at en ikke-EU virksomhed bare kunne oprette et EU datterselskab og så er alt godt. Men det er så her, alt det tekniske kommer ind.

Det er overvejende sandsynligt at den kode, som servicen i EU selskabet kører på, enten er en 1-til-1 kopi af den kode, som kører i moderselskabet med alle de bagdøre, der måtte være i den. Faktisk vil det nok endda være ikke-EU moderselskabet, som i praksis kører koden og EU datterselskabet er en frontend salgs- og supportskal.

Under alle omstændigheder kan en CxO fra moderselskabet nok godt møde op i datterselskabet og bede om diverse data på en USB-stick - sådan helt diskret.

Så ikke-EU cloud er yt. Men så kan vi da bare køre det hele hos en EU udbyder eller internt! Mjaaah... måske.

I Danmark/EU kører vores PC'ere og servere mest Microsoft Windows, en del Apple macOS/iOS på iPhone/iPad og en smule Google ChromeOS/Android på telefoner og tablets (jeg ser lige bort fra Linux et øjeblik). Og hvor er det nu Microsoft, Apple, Google og selv RedHat har hovedkvarter? Jep, USA. Og så må vi jo bare erkende, at de har fuldstændig kontrol over vores maskiner via deres operativsystemer. Via deres operativsystemer kan (og gør!) de kopiere hvad som helst fra en hvilken som helst maskine til en server i USA uden at vi kan finde ud af det.

Så, rent teknisk, kan vi ikke beskytte vores data, hvis vi bruger et ikke-EU operativsystem.

Og, nå ja, det samme gælder selvfølgelig alle de programmer, der måtte køre oven på et hvilket som helst operativsystem, som f.eks. kontorpakker, browsere, databaser, ESDH'er osv.

Okay, så må vi lave et EU operativsystem og EU applikationer, så er alt godt, ikke sandt? Mjaaah... måske.

Der er jo også noget, der hedder hardware, f.eks. CPU, RAM, harddiske, grafikkort, netværkskort osv. Hvis vi nøjes med at se på CPU er de to store leverandører Intel og AMD. Og de er jo fra USA! Og resten har et 'Made in China' mærkat.

Det meste hardware har efterhånden en del regnekraft og ingen ved hvad der foregår der.

Så, rent teknisk, kan vi ikke beskytte vores data, hvis vi bruger ikke-EU hardware.

Så, hvis vi virkelig skal gøre noget ved databeskyttelse, skal vi i EU lave vores egen hardware og vores egen software.

Det kan virke langt ude at skulle stå for det hele selv, men der er faktisk en række lande, som ønsker at undgå amerikansk hardware og software. Lande som Rusland, Kina og Nordkorea arbejder på egen hardware og software.

Så når politikere og jurister sidder og nørkler med en tekst på et stykke papir, som skal sikre vores data, så vil det, rent teknisk, aldrig virke.

Til gengæld kan de (måske) finde en tekst, som gør det muligt for virksomheder og myndigheder at fortsætte med at bruge ikke-EU services, software og hardware, i hvert fald indtil vi får en Schrems III.

Hvis du vil vide mere er gode søgetermer: "Edward Snowden", "Apple FBI dispute", "Intel backdoor", "Red Flag Linux", "Red Star Linux", "China CPU", "Russia CPU"

PS Lidt ekstra info på Version2 https://www.version2.dk/artikel/max-schrems-dumper-nyt-microsoft-setup-nsa-har-stadig-adgang-dine-data-1092605