backupdagen 31. mars

Nasjonale datasenter vs. internasjonale

– norske personvernlover gir elektroniske data svært god beskyttelse

Flere land vurderer tiltak som skal sørge for at elektroniske data holdes på nasjonale datasentre. Et lovforslag som nå vurderes i den brasilianske nasjonalforsamlingen tar til orde for at internettaktører som er aktive i Brasil, som for eksempel Facebook og Google, må sette opp lokal infrastruktur i landet slik at data knyttet til brasilianske brukere lagres i Brasil og ikke i vilkårlige datasentre i utlandet. Videre vurderer Brasil, i likhet med Tyskland, å etablere nasjonale, krypterte e-posttjenester.

Geografisk plassering av data er viktig fordi det bestemmer hvilken jurisdiksjon dataene kommer inn under. For eksempel vil data som en nordmann lagrer på en tjeneste i USA komme inn under amerikansk lovgiving som ”the USA Patriot Act”.

Dersom amerikanske myndigheter får tilgang til dataene gjennom denne loven, har ikke tjenestetilbyder lov til å fortelle nordmannen at dataene er blitt brukt på denne måten. Geografisk plassering er derfor viktig for å sikre dataene gjennom nasjonal lovgivning. Det kan muligens også bidra til å heve terskelen for overvåking fra andre land.

Man bør sette krav til hvor data lagres og hvilket sikkerhetsnivå en cloud leverandør dokumenterer på sine tjenester. Transport og lagring vil være det letteste områdene man kan stjele eller hacke data uten god sikkerhet. Alle data bør sendes komprimert og kryptert med 256 bit AES kryptering før de forlater kundes maskiner. Alle data må lagres kryptert på det datasenteret leverandøren bruker til lagring. Det er kun kunden som sitter på krypteringsnøkkel for dekryptering av data.

Sikkerhetsnivået på norske datasentre som brukes av anerkjente cloud leverandører, er av de beste. Dessuten gir norske personvernlover et svært godt vern av all lagret datainformasjon. Norske datasentre har også blitt ettertraktet som lagringsplass for utenlandske selskaper på grunn av den beskyttelsen norske lover gir.