Skytjenester – bruk dem gjerne, men bruk dem riktig

Bjørn Erik Thon | direktør | Datatilsynet

Personvernbloggen.no | @bjornerikthon | datatilsynet.no

29.10.2014

Datatilsynet

Dagens tema

- Bruk av skytjenester, og bevisst(løs) bruk
- Skytjenester og informasjonssikkerhet
- Datatilsynets krav til skytjenester
- Hvor trykker skoen i norske kommuner?
- Innebygd personvern

Mørketallsundersøkelsen

- Sterk økning i bruk av skytjenester de siste to år
- 2/3 av norske virksomheter bruker en eller annen form for skytjeneste
- 1/3 bruker gratistjenester, som f eks Dropbox og gmail
- 16% bruker skytjenester i utlandet, fordelt på 6% offentlige og 20% private.

Mørketallsundersøkelsen

- Kun 20% av private virksomheter har databehandleravtaler, og 50% av offentlige
- 20% av virksomhetene vet ikke om skyleverandører kan bruke dataene til eget bruk
- 20% vet ikke hvor dataene er lagret
- 33% av daglige ledere vet ikke om de har inngått databehandleravtaler.
- 75% har tillit til at skyleverandøren har logging av uautorisert tilgang og sletterutiner

Hva finner vi så på tilsyn der vi sjekker informasjonssikkerhet?


17
87
VARDOËNSIS INSIGNIA URBIS
CEDANT TENEBRA SOLI
17
42
BONA
CAUSA

29.10.2014

Hvor har vi vært?

- Kontroller
  - 5 kommuner i Nord-Troms
  - 6 kommuner på Sør-Helgeland
  - 2 kommuner i Sogn og Fjordane
  - 4 kommuner på Sør- og Vestlandet
  - 2 kommuner i Øst-Finnmark
- Råd og veiledning
  - Fosenregionen
  - Kongsbergregionen
  - Nordre Nordland
  - Fjellregionen (FARTT)
  - Nordland fylkeskommune
- Planlegger i løpet av høsten å besøke
  - 3 kommuner i Lofoten/Vesterålen/Ofoten/Sør-Troms

Hvor trykker skoen?

- Manglende oversikt over egne behandlinger
- Hull i kunnskapen om innsyn og informasjon
- Manglende eller for dårlige risikovurderinger
- Vertskommuner i regionale samarbeid er ikke alltid bevisst sin rolle som databehandler for de øvrige kommunene
- I noen tilfeller tror man behandlingsansvaret overføres til vertskommunen (Hvilket er riktig hvis samarbeidet er etter kommuneloven § 27)
- Databehandleravtaler

Kan skytjenester medføre økt risiko?

- Mindre kontroll med dataene kan gjøre det vanskeligere å avsløre avvik
- Data kan overføres til land med dårligere beskyttelsesnivå enn vårt
- Avtalene er kompliserte og vanskelig å trenge inn i / overskue konsekvensene av
- Det er vanskelig å kontrollere om databehandleren bruker dataene for egne formål
- Ansvarskjeden: Skytjenester innebærer bruk av underleverandører, og er de like troverdige og aktsomme som hovedleverandøren?
- Tilsyn med egne data kan bli vanskeligere
- Utenlandske myndigheters tilgang til data

Informasjonssikkerhet

- Ansvar for informasjonssikkerheten påhviler egen virksomhet
- Man kan ikke flytte ansvaret ut i skyen
- Må forvisse seg om tilstrekkelig sikkerhet i produktet som kjøpes

Er skytjenester usikre?

- På generelt grunnlag – nei

- Informasjonssikkerheten skyleverandørene tilbyr kan være bedre enn hva en liten kommune kan

- Men hovedoverskriften på vårt arbeid er allikevel informasjonssikkerhet – og de kravene som loven stiller opp for å sikre god informasjonssikkerhet

Narvik-saken, og bruk av Google Apps

- Saken har vært behandlet som en tradisjonell forvaltningssak

  - Hvilke personopplysninger behandles i Google Apps?
  - Den risikovurdering kommunen har fortatt
  - Kopi av avtalen + ev databehandleravtale
  - Segmentering av data
  - Lagringssted
  - Hvem har tilgang hos Google?

  - ...sett i lys av bl.a. sikkerhetsforskriftens krav til risikovurdering og sikkerhetsrevisjon

Nettskyen – Narvik-saken – Google Apps

- Varsel om vedtak mot kommunen i januar 2012

  - Usikkerhet rundt risikovurderinger
  - Ingen databehandleravtale (avtalen hensikt, formål, plikter, forhold til underleverandør, sikkerhet, revisjon mv)
  - Vet ikke i hvilket land dataene er lagret
  - Kan ikke gjennomføre sikkerhetsrevisjoner
  - Hvem har tilgang hos Google?
  - Uklarhet rundt segmentering

Hva ble endret i Narvik-saken fra den startet til den ble avgjort?

- Risikovurderinger
- Databehandleravtale
- Revisjon av tredjeparter
- Databehandleravtalen må trumfe Googles generelle vilkår
- Klarhet om overføring til utlandet

Risikovurderinger

- Personopplysningsforskriftens § 2-4

- *Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.*

Risikovurderinger

- Narvik kommune:

- *"En flytting av e-postløsning til Google Apps vil på enkelte aspekter gi likt risikobilde som for gammel, men på mange områder innebærer ny løsning redusert risiko. Lagring av e-post data utenfor kommunens datasenter vil gi en lavere risiko med hensyn til konfidensialitet, integritet og tilgjengelighet."*

Risikovurderinger

- *Datatilsynet anser risikovurderingen som tilfredsstillende men ønsker å påpeke viktigheten av at kommunen gjennomfører ny risikovurdering ved endringer som har betydning for informasjonssikkerheten*

- *I tillegg: Viktig hvilken type opplysninger som behandles i tjenesten*

Revisjon fra tredjeparter

- Loven stiller krav om at det skal gjennomføres sikkerhetsrevisjoner og at resultatet av sikkerhetsrevisjonen skal offentliggjøres

- Berlin –gruppen og WP29 har åpnet for at sikkerhetsrevisjoner kan gjennomføres av tredjeparter

- Tredjepartsrevisjonen må tilfredsstille en del vilkår
  - Uavhengig, regelmessig, kommunen må motta rapporter som er relevant for de data som behandles pva kommunen osv

Databehandleravtaler

- Rettslig grunnlag: POL § 15
- Grunnkrav til databehandleravtaler:
- *Avtalens hensikt, formål, databehandlers plikter, bruk av underleverandør, sikkerhet, sikkerhetsrevisjoner, avtalens varighet, ved opphør, meddelelser, samt*
- *lovvalg og verneting*.

- Særlig viktig: Formålsavgrensninger, forbud mot å utlevere data til andre, informasjonssikkerhetstiltak

- Datatilsynet fant at databehandleravtalen oppflyte lovens krav

Databehandleravtalen må trumfe Google/Microsofts generelle vilkår

- - .....når det gjelder utveklsing av data på tvers av disse (og andre) selskapers tjenester

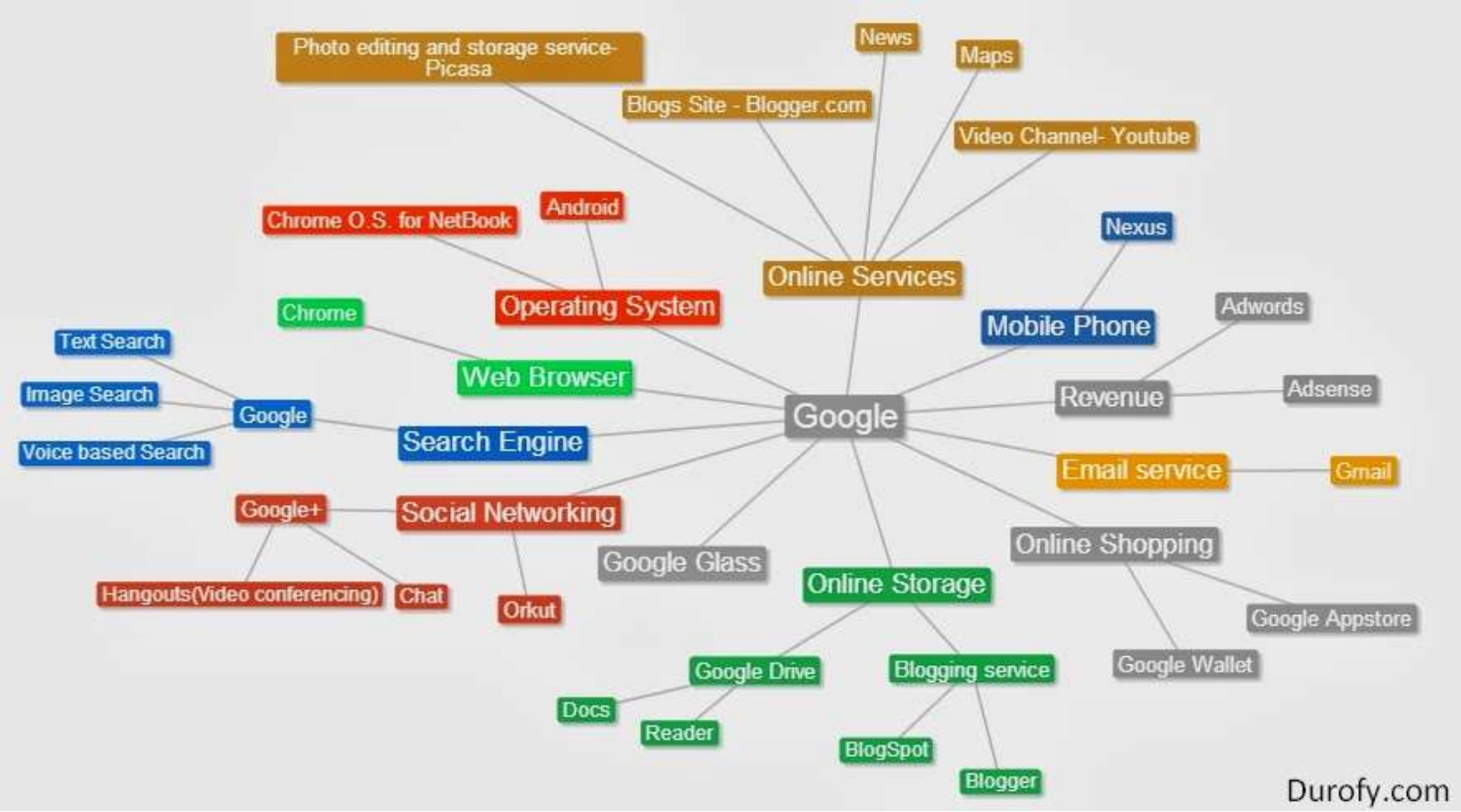
Photo editing and storage service- Picasa
News
Maps
Blogs Site - Blogger.com
Video Channel- Youtube
Chrome O.S. for NetBook
Android
Nexus
Online Services
Operating System
Chrome
Adwords
Mobile Phone
Text Search
Web Browser
Image Search
Google
Revenue
Adsense
Search Engine
Voice based Search
Email service
Gmail
Google+
Social Networking
Online Shopping
Google Glass
Online Storage
Hangouts(Video conferencing)
Chat
Orkut
Google Appstore
Google Drive
Blogging service
Google Wallet
Docs
Reader
BlogSpot
Blogger
Durofy.com


Microsoft
Windows 8
SharePoint
Office 365
Windows Azure
Microsoft Dynamics CRM
Microsoft SQL Server
Microsoft Dynamics AX
Lync
bing
msn
skype

Repetisjon: Mørketallsundersøkelsen

- Kun 20% av private virksomheter har databehandleravtaler, og 50% av offentlige
- 20% av virksomhetene vet ikke om skyleverandører kan bruke dataene til eget bruk
- 20% vet ikke hvor dataene er lagret
- 75% har tillit til at leverandøren har rutiner for logging av uautorisert tilgang og sletterutiner
- 1/3 av daglige ledere i private virksomheter vet ikke om de har inngått databehandleravtaler.

Regjeringen krever innebygd personvern i alle sektorer

- Det bør fastsetjast eit prinsipielt mål om innebygd personvern i alle sektorar
- Dei førehandsdefinerte standardinnstillingane på utstyr, i system og i program bør setjast til den mest personvernvenlege løysinga

Syv prinsipper for bruk av innebygd personvern

1. Man må ligge i forkant av utviklingen og se hva som kommer
2. Den personvernvennlige løsningen er forhåndsvalgt
3. Personvernet må være bygd inn i løsningen fra starten av
4. Innebygd personvern må skape en vinn-vinn situasjon for borger og næringsliv
5. Innebygd personvern skal gjelde fra vugge til grav
6. Åpenhet og etterprøvbarhet
7. Respekt for borgeren: brukervennlighet i design og informasjon

Takk for oppmerksomheten

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no