RIGSREVISIONEN

Status på datasikkerhed hos offentlige myndigheder

Beskytter statslige virksomheder fortrolige data tilstrækkeligt?

Steen Bernt Jensen, chefkonsulent

Beretning om hackerangreb fra 2013

De udvalgte statslige virksomheder:

- Energistyrelsen
  - Behandler fortrolige data via myndighedsopgaver.
- Statens It
  - Er driftscenter for 8 ministerier og ca. 80 virksomheder. De 80 virksomheder behandler tilsammen store mængder af fortrolige data, herunder persondata.
- Digitaliseringsstyrelsen
  - Har opgaver vedrørende informationssikkerhed i staten
  - Fører tilsyn med it-sikkerheden på ministerområdet
  - Behandler fortrolige data.
- Klima-, Energi-, og Bygningsministeriet
  - Ministerbetjeningen er fortrolig.
- Alle ovennævnte virksomheder håndterer persondata, fx i outlook og personalesager.

Slide nummer 2

SBJ2 det er vigtigt ikke kun at fokusere på persondata, da statslige virksomheder behandler mange fortrolige data som ikke er persondata. Så persondataloven er ikke svaret på hvordan virksomhederne beskytter andre typer af fortrolige data.

Steen Bernt Jensen; 15-10-2014

Beretning om hackerangreb fra 2013

Hvad viste Rigsrevisionens undersøgelse?

- Rigsrevisionen fandt, at de data, som de undersøgte statslige virksomheder var ansvarlige for, ikke var tilstrækkeligt beskyttede på undersøgelsestidspunktet. Der var med det konstaterede sikkerhedsniveau en unødig stor risiko for hackerangreb og misbrug af it-systemer og fortrolige data.

- Det var Rigsrevisionens vurdering, at undersøgelsens resultater kunne være gældende for en større kreds af statslige virksomheder, end de netop undersøgte.

- Statens It havde ikke i tilstrækkelig grad undersøgt risikoen for, at et hackerangreb på én virksomhed med utilstrækkelige sikringstiltag kunne sprede sig til andre virksomheder.

Rigsrevisionens revision vedr. persondata

- Vi begyndte at undersøge området for nogle år siden.

- Vi havde forventet at se en høj efterlevelse af persondataloven fordi:
  - Borgere registreres uanset om de ønsker det. Manglende efterlevelse af persondataloven er en krænkelse af borgernes rettigheder.

  - Statslige virksomheder udfolder normalt store anstrengelser for at efterleve Folketingets beslutninger i form af vedtagne love.

  - Potentialet ved digitalisering af den offentlige sektor er slet ikke udnyttet. Manglende efterlevelse af persondataloven kan medføre manglende vilje til at aflevere data, eller at borgere bevidst afleverer forkerte data. Manglende tillid til forvaltningen kan påvirke mulighederne for en fortsat digitalisering.

Hvad har revisionerne vist

- Kun én af de ca. 80 virksomheder, der er tilsluttet Statens It, har i dag indgået en tilstrækkelig databehandleraftale med Statens It. Det er kundens ansvar, at der indgås en databehandleraftale, og at der følges op på, at sikkerheden hos driftsleverandøren er tilstrækkelig.

- Problemet har været kendt siden 2011/2012.

- Digitaliseringsstyrelsen og Center for Cybersikkerhed har i august 2014 udgivet en rapport, som opsamler erfaringerne fra hackerangrebet hos CSC. Hovedanbefaling fra rapport: Ledelsen bør sikre, at myndigheden indgår aftaler om ønsket sikkerhedsniveau ved outsourcet drift.
  Vedrørende persondata vil det som minimum sige en databehandleraftale.

- Når vi undersøger statslige virksomheders efterlevelse af sikkerheds-bekendtgørelsen, konstaterer vi ofte eksempler på manglende efterlevelse.

Slide nummer 5

SBJ1 Når vi undersøger området, så ser vi ofte eksempler på manglende efterlevelse af sikkerhedsbekendtgørelsen.
Derfor har vi lavet en mere systematisk undersøgelse af om Rigspolitiet, Sundhedsstyrelsen, Socialstyrelsen, SKAT, Institut for Menneske-rettigheder, Forsvarskommandoen, Danmarks Statistik og Arbejdsskadestyrelsen efterlever sikkerhedsbekendtgørelsen.

Resultaterne af den undersøgelse vil fremgå af en beretning til Statsrevisorerne, som forventes behandlet på deres møde den 12. november 2014

Steen Bernt Jensen; 15-10-2014

Beskytter statslige virksomheder fortrolige data tilstrækkeligt?

Grundlag for konklusion:

- Rigsrevisionens hackerberetning fra 2013.
- Revisionerne vedrørende persondata i perioden 2011-2013.
- Kun én kunde har indgået en tilstrækkelig databehandleraftale med Statens It. Ca. 60 virksomheder, svarende til 1/3 af alle statslige virksomheder, er tilsluttet Statens It.

Konklusion:

- Det er Rigsrevisionens vurdering, at mange statslige virksomheder ikke har etableret de fornødne tekniske og organisatoriske tiltag for at beskytte fortrolige data.