RÅDET FOR DIGITAL SIKKERHED

Retsudvalgets høring om myndigheders behandling af personoplysninger

Sikkerheden i den outsourcede it-drift

Christiansborg, 21. oktober 2014

Birgitte Kofod Olsen, Formand
Partner, phd, Carve Consulting

Robust sikkerhed

Effektiv beskyttelse af borgernes data kan kun opnås gennem

- Konkret vurdering af sikkerhedsbehovet
- Præcise krav til leverandører
- Forventningsafstemning og løbende dialog

#1 Konkret vurdering af sikkerhed

Sikkerheden i den outsourcede it-drift

Sikkerheden i outsourcing afhænger af

- det konkrete behov for at outsource drift
- forhold hos kunden - datatype, it-drift, organiastion, procedurer
- forhold hos leverandøren –, geografi, organisation, procedurer, it-drift, brug af privacy enhancing techonologies, PETs

Vurderingen heraf skal være på plads før den rigtige beslutning kan træffes.

#2 Præcise krav til leverandører

Sikkerheden i den outsourcede it-drift

Den offentlige myndighed skal stille specifikke sikkerhedskrav i udbudsmateriale og i kontrakten:

- Sikkerhedsniveau for almindelige hhv følsomme persondata
- Krav om privacy by design
- Udarbejdelse af risikovurdering, evt. sammen med leverandøren, herunder Privacy Impact Assessment, PIA
- Udarbejdelse af plan til forebyggelse og mitigering af sikkerhedsbrud
- Sikkerhedsprocedurer, herunder kontrol og rapportering

#3 Forventningsafstemning

Sikkerheden i den outsourcede it-drift

Sikker outsourcing kræver forventningsafstemning og løbende dialog mellem offentlig myndighed og leverandør om:

- opfyldelse af konkrete formål med at outsource
- det relevante sikkerhedsniveau
- nødvendige justeringer

Forventningsafstemningen mangler i dag – derfor ser vi:

- lavere sikkerhed, end den der er brug for
- udgifter til højere sikkerhed, end der reelt er brug for
- outsourcing vælges fra

Bilag

- Privacy Impact Assesment
- ISO27001
- ISO27018

Privacy Impact Assesment

- Identifikation af al persondata, der håndteres i et system og af måden data anvendes på
- Vurdering af nødvendigheden og proportionaliteten af anvendelse og opbevaring
- Kortlægning af, hvordan persondata håndteres efter indsamling (adgang, logning)
- Identifikation af privacy risici og risikoniveauet
- Formulering af løsninger til at eliminere eller reducere privacy risici til et acceptabelt niveau.

Læs mere om den canadiske metode og den danske vejledning her:

http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp

http://www.digst.dk/~/media/Files/Arkitektur%20og%20standarder/Informationssikkerhed%20efter%20ISO27001/Guide%20til%20konsekvensvurdering%20af%20privatlivsbeskyttelsen_ver3.pdf

ISO 27001

Information Security Management System

- Context of the organisation
- Planning
  - Actions to adress risks and opportunities
  - Information security risk treatment
- Support
- Operation
- Performance evaluation
- Improvement

ISO 27001 Control objectives and controls: (A.9-12)

Access control – User access management

System and application access control

- Information access restrictions
- Secure log-on-procedures
- Password managment system ”ensure quality PWs”

Crytographic controls

- Policy on the use of cryptographic controls
- Key management

Backup

Protection from malware

- Implementation of detection, prevention and recovery controls
- User awareness

Logging and monitoring

- Events
- Protection of log-info
- Administrator and system operator log

ISO 27001 Privacy

Classification of information (A.8.2.1)

- Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification

Compliance – control (A.18.14)

- Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable

- http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO 27018 personally identifiable information in public clouds

ISO/IEC 27018:2014

- Information technology
- Security techniques
- Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

- http://www.iso27001security.com/html/27018.html

Kontaktinformation

Rådet for Digital Sikkerhed

Toldbodgade 12

1253 København K

Formand

Birgitte Kofod Olsen

Mobil +45 41 42 83 81

Mail birgitte.kofod.olsen@digitalsikkerhed.dk

Web digitalsikkerhed.dk