Det 7. norske arkivmøtet

Informasjonssikkerhet i endringsprosesser

6. April 2016

devoteam

Innovative technology consulting for business

Agenda

1. Informasjonssikkerhet
2. Klassifisering
3. Risikoanalyse og kontinuitetsplanlegging i endringsprosesser
4. Personvern i endring

Linda Charlotte Nedberge
CISSP

Informasjonssikkerhet er mer enn IT-sikkerhet

- **Konfidensialitet** – sikre at uvedkommende ikke får adgang/tilgang til informasjonen
- **Integritet** – sikre at ingen, enten med vilje eller ved en feil, endrer informasjonen
- **Tilgjengelighet** – sikre at informasjonen er tilgjengelig for dem som trenger den, når de trenger den

Gjelder all informasjon

- Papirbasert
- Muntlig
- Digitalt

- **Informasjonen** har verdi!

- Cybercrime er den moderne mafia – Cybercrime Is Now More Profitable Than The Drug Trade
- En undersøkelse fra McAfee sier at datakriminalitet koster den globale økonomien mer enn 3300 billioner kroner hvert år, og at det fortsatt øker. Bare i Norge har 150.000 blitt utsatt for ID-tyveri de siste to årene

Hva kan skje hvis informasjonssikkerheten er dårlig?

- Ingen reell styring eller oppfølging av infosikkerheten
- Tiltak som finnes er tilfeldige, og «skrudd til» maksimalt
- Ingen opplæring av ansatte
- Ansatte opplever de fleste tiltak som tidstyver og forsøker å omgå dem

Konsekvensene kan bli store og omfattende

- Brudd på personvernet (ID-tyveri etc)
- Omdømmetap
- Økonomiske tap
- Liv og helse (Rikets sikkerhet?)

Hva må gjøres?

- Sette ting i system, benytte eksisterende prinsipper som allerede er etablert, eks. HMS og annet sikkerhetsarbeid, kvalitet
- Få oversikt over trussel- og sårbarhetsbildet, gjøre noen vurderinger på bakgrunn av dette og etablere hensiktsmessige tiltak
  - stramme inn og løsne opp i takt med trussel- og sårbarhetsbildet

- CISO
- Styringssystem for informasjonssikkerhet (ISMS)
- Risikostyring
- Internkontroll (personvern)

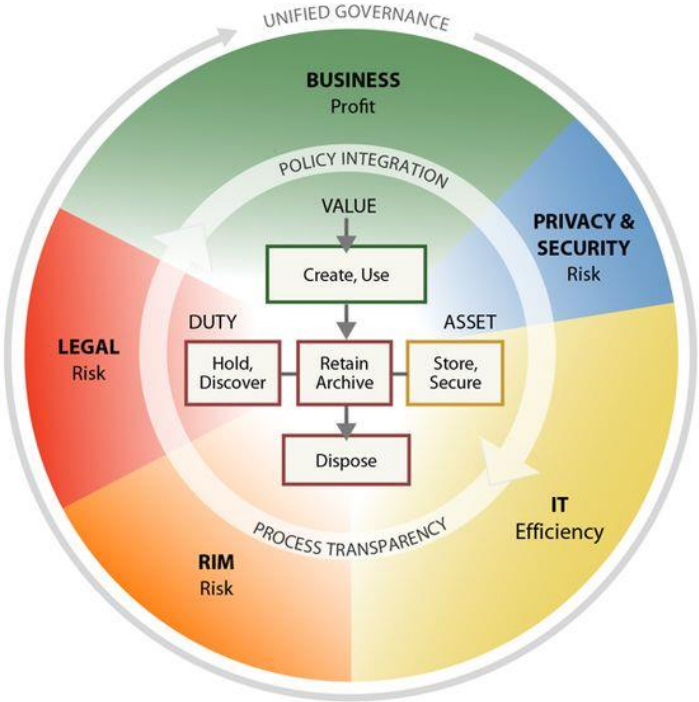
- ISO standarder for informasjonssikkerhet
- Personvernlovgivning

Gevinster med god infosikkerhet?

- Tilliten vil øke
- Blir i stand til å digitalisere mer
- Reduserte kostnader
- Fornøyde ansatte

Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Information security management system (ISMS)

- Utvikles av informasjonssikkerhetsansvarlig, i samarbeid med
  - ledelsen
  - "subject matter experts" (f.eks. IT-personell, HR, legal)
- Oppfyller krav til god informasjonssikkerhet i Personopplysningsloven og Forskriften
- Bør baseres på ISO/IEC 27001:2013

- **ISO/IEC 27001** — Information technology - Security Techniques - Information security management systems — Requirements.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27017 — cloud services
- ISO/IEC 27018 —protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27032 — Guideline for cyber security
- ISO/IEC 27035 — Information security incident management

Controls

- Information Security policies
- Organization of Information Security
- Human Resource Security
- **Asset Management**
- Access Control
- Cryptography
- Physical and environmental security
- Operation Security-, Protection from malware, Backup, Logging and monitoring, Control of operational software, and Information systems audit coordination
- Communication security - Network security management and Information transfer
- System acquisition, development and maintenance - Security in development and support processes and Test data
- Supplier relationships
- Information security incident management
- Information security aspects of **business continuity management**
- Compliance - Compliance with legal and contractual requirements and Information security reviews

Klassifisering av informasjon

- For å vite rett nivå av beskyttelse.
- Hvilken informasjon trenger vi å beskytte? Hva er konsekvensene om noe går galt?
- Kan gjøre sikkerhet enklere, ved å gruppere informasjon og prioritere informasjonen som må beskyttes
- Målsettinger, kontrakter, lover og regler
- Del av en risikovurdering
- Konfidensialitet, integritet, tilgjengelighet
- Mulige konsevenser: lav, middels høy

Risikostyring

- Sørge for konfidensialitet, integritet og tilgjengelighet for all informasjon, samtidig som man sikrer **kostnadseffektive** tiltak
- Risikoen vurderes ut ifra kombinasjonen av **sannsynlighet** for at noe inntreffer, og **konsekvensene** om det faktisk inntreffer
- Identifisere aktiva. Informasjonseiere!
- Identifisere trusler (og sårbarheter)
- Identifisere risikoeiere
- Velge **tiltak**
- Vurdere risikoapetitt

Beredskaps- og kontinuitetsplanlegging

- Formål: hindre avbrudd i (virksomhets)prosesser og beskytte kritiske driftsprosesser fra konsekvensene av større feil i informasjonssystemer, og å sikre at de berørte prosessene kan gjenopptas i tråd med tilgjengelighetskravene.
- Risikovurderinger gjennomføres som en del av kontinuitetsplanleggingen for å identifisere hendelser som kan forårsake avbrudd i driftsprosesser, sannsynligheten for at disse inntreffer, samt hvilke konsekvenser de har for virksomhetsprosessene.
- Beredskaps- og kontinuitetsplanene må testes og oppdateres regelmessig (øve på samhandling og håndtering av krevende situasjoner, som driftsavbrudd, evakuering, brannslukking og andre hendelser)
- **BIA** (Business Impact Analysis):
  - Identifisere kjernevirksomheten, kritiske business prosesser (core business)
  - Hvilke ressurser/systemer som supporterer disse aktivitetene/prosessene?
  - Konsekvenser ved bortfall av disse?
  - Hvor lenge kan vi «overleve» uten?

Personvernlovgivning

- Personopplysningsloven
- Personopplysningforskriften

EU privacy regulation

- **Microsoft vs FBI**… (straff/bøter fra EU eller USA – et resultat av uharmoniserte lover)
- **Safe Harbour:** Max Schrems vs Facebook, NSA PRISM, USAs omfattende overvåking, ikke adekvat beskyttelse av borgere

devoteam

EU personvernforordning

- Erstatter direktivet fra 1995, i kraft 2018
- **One continent, one law**
- **Privacy officers**
- **Sanctions/penalties:** bøtene kan bli opptil 4% av global brutto konsernomsetning per overtredelse
- **Big data**: avledet bruk – blir også strengt regulert (identifiable metadata)
- **Transfer** of personal data outside EU (EEA), server location, but also location of support personnel
- **A right to be forgotten**
- **Right to data portability**
- **The right to know when your data has been hacked**: Du må melde inn ”breaches”, altså avvik til Datatilsynet innen 72 timer etter det er oppdaget.. I alvorlige tilfeller må bedriften også melde om avviket til de personene som det er frastjålet data om.
- **Data protection first, not an afterthought**
- **Større krav til generell IT-sikkerhet**
- **Certification**

Contact Information

Devoteam AS

Linda Charlotte Nedberge
Senior consultant
Phone: +47 906 60 251
E-mail: linda.nedberge@devoteam.com
www.devoteam.no

Locations in Norway:

Oslo: Addr.: Kronprinsens gate 17, 0251 Oslo, Phone: +47 23 25 33 00

Grimstad: Addr.: Terje Løvås vei 1, 4898 Grimstad, Phone: +47 37 80 00 00