TEMAMØDE
Sikkerhedshændelser

Introduktion v/Gitte Melph

AALBORG UNIVERSITET

Rammerne for sikkerhed på AAU

- AAU´s informationssikkerhedsudvalg (ISU) har indstillet og ledelsen besluttet at følge ISO standard 27001
- AAU har derfor opbygget sin politik og sikkerhedshåndbog i h.t. standarden
- 14 hovedområder:
  - Informationssikkerhedspolitikker
  - Organisering af informationssikkerhed
  - Personalesikkerhed
  - Styring af aktiver
  - Adgangsstyring
  - Kryptografi
  - Fysisk sikring
  - Driftssikkerhed
  - Kommunikationssikkerhed
  - Anskaffelse, udvikling og vedligeholdelse af systemer
  - Leverandørforhold
  - Styring af informationssikkerhedsbrud / -hændelser
  - Nød-, beredskab- og reetablering, sikkerhedsaspekter
  - Overensstemmelse (compliance)

Hvad er en sikkerhedshændelse?

- en bred definition

En sikkerhedshændelse er en hændelse, der indikerer, at systemer, data eller bygninger er blevet kompromitteret eller at beskyttelsesforanstaltninger er blevet omgået eller sat ud af funktion.

Kompromittering af TILGÆNGELIGHED - FORTROLIGHED - INTEGRITET

Eksempler:

- Forstyrrelse eller utilgængelighed til services
- Forsøg på uautoriseret adgang til systemer eller data
- Forsøg fra uautoriserede kilder for at få adgang til systemer eller data
- Skadelig kode – ex. i form at virus og orme
- Uautoriseret adgang til data – ex. til at gemme eller tilgå data
- Uautoriserede ændringer til udstyr, services, data
- Sikkerhedshuller i software (sårbarheder, der kan udnyttes)
- Mistet udstyr
- …….. og meget, meget andet

Hvad kan man gøre for at undgå sikkerhedshændelser?

Initiativer af forebyggende - opdagende - udbedrende/korrigerende karakter.

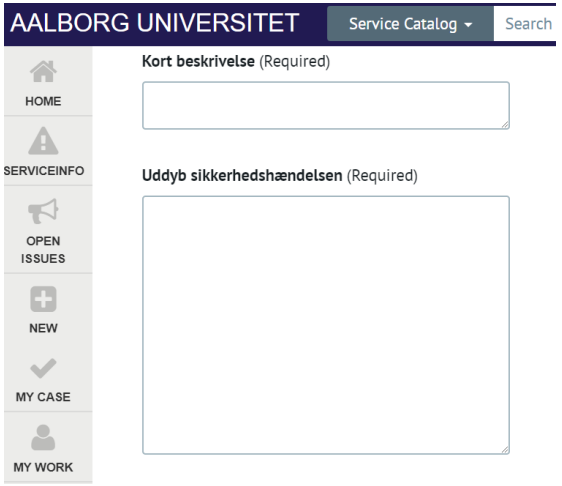
Fra sikkerhedsfunktionens side ser man typisk på følgende tiltag:

- Krav om sikkerhed i processer, fx softwareudvikling, krav til leverandører etc.
- Sikre, at der er etableret og indarbejdet (implementeret) processer for hændelseshåndtering – og at de testes
- Awareness træning af medarbejderne
- Logning og analyse af logfiler
- Løbende kontroller og tests
- Tekniske værktøjer

AAU´s proces for sikkerhedshændelser

Sikkerhed.aau.dk → formular øverst på forsiden: ”Anmeldelse af sikkerhedshændelse”

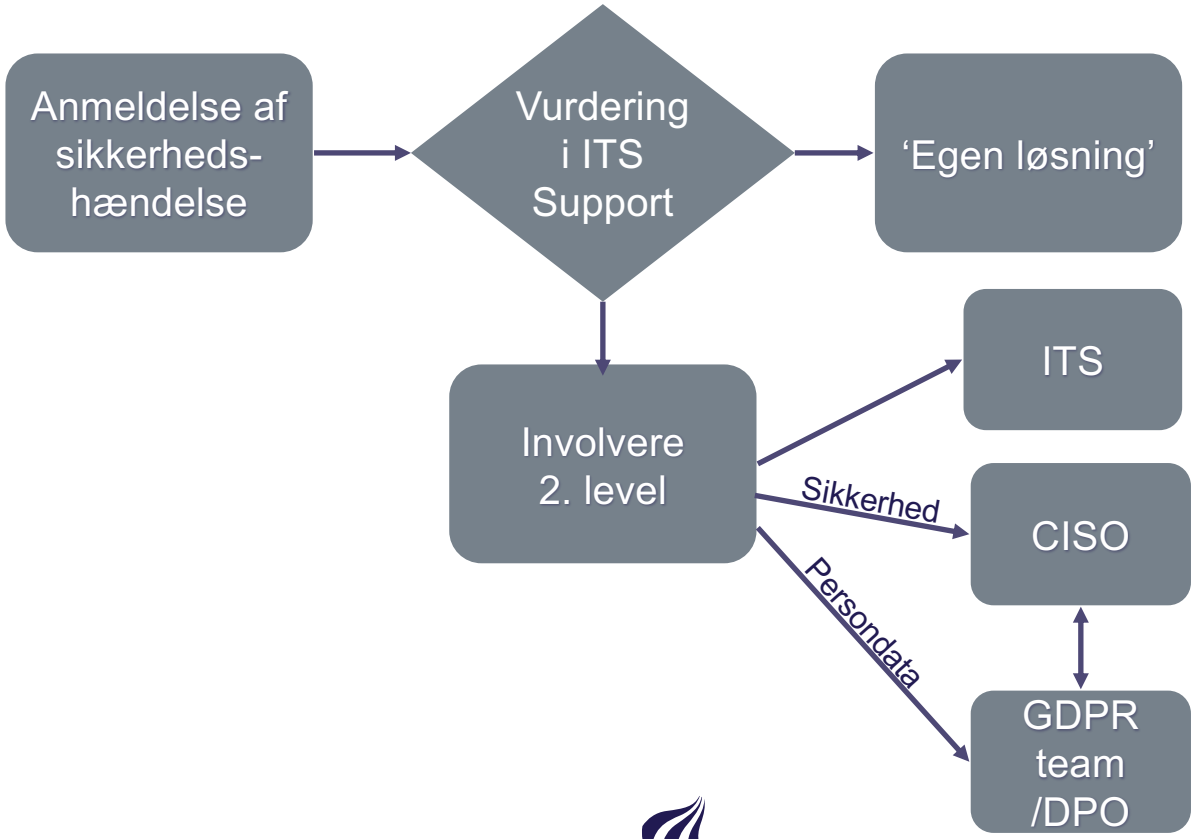
Simpel proces og simpel formular, der pt. ligner en almindelig mail: Emnefelt + beskrivelse



Hvad skal rapporteres/anmeldes?

- En aktuel hændelse (mistet pc, stjålet telefon, ransomware: ”Din computer er låst, betal….”, jeg kom til at klikke, fundet fortrolig print i printerrummet, fundet USB-nøgle (aflevere i on-site support), sendt mail med fortrolig eller følsom informationer osv.
- En formodet hændelse (modtaget phishing mail, men har ikke klikket, ny og underlig oplevelse af service etc.)

Proces efter din anmeldelse



AALBORG UNIVERSITET