Sikkerhedsgruppen

Talgildu Føroyar

Samleikin

IT-sikkerhedskrav

Sikkerhedsgruppens opgave er at lave en oversigt over it-sikkerhedskrav til 'Talgilda Samleikan' ud fra lovgivning, standarder samt risikovurderinger.

Kravene er baseret på følgende kilder:

- Færøsk lovgivning
- ISO/IEC 27002 (2013)
- Europa-kommisionens gennemførelsesforordninger 2015/1501 og 1502
- Europa-kommisionens gennemførelsesafgørelser 2015/1505 og 1506
- Certifikatpolitik for OCES-personcertifikater, version 4
- Egne risikovurderinger

Kravene er opdelt som kapitlerne i ISO/IEC 27002 (se bilag 1).

Vedlagt er:

- Et kompendium med krav

- Bilag med krav

    - 'Fylgiskjal 5' (generelle sikkerhedskrav i forbindelse med outsourcing). Fylgiskjal 5' er ikke ajourført i henhold til den nyeste ISO/IEC27002. Inden nye aftaler bliver indgået, bør dokumentet ajourføres.

    - Sammendrag af udvidede krav fra ISO/IEC27002, DS484, EU, OCES og egne risikovurderinger.
        - Risikovurderinger og overordnede tegninger over Trygdarkjarnan, Lyklaumsiting, Mobil-id, Felagsinnritan, Lyklakort og Fulltrú.
        - ISO/IEC27002 krav i tabelform
        - OCES/EU/DS484 krav i tabelform

    - Klassificering – en skabelon med nogle eksempler (under udarbejdelse)

    - Oversigt over krav, hvor procedurer kan indgå

Listen med krav, som Trygdarbólkurin har identificeret, kan ikke regnes som udtømmende, idet den planlagte løsning ikke er beskrevet i detaljer, men på et forholdsvis overodnet niveau.

Sikkerhedsgruppens bemærkninger

Det er positivt, at sikkerhedsaspekterne allerede er taget med i denne fase, fremfor at blive hevet frem til sidst, når alle væsentlige beslutninger er taget.

Arbejdet har været præget af, at man på nuværende tidspunkt ikke er fuldt ud klar over f.eks

- Systemernes funktioner
- Kommunikationen
- Borgernes muligheder
- Data
- Geografisk placering

derfor er de risici, som Sikkerhedsgruppen har afdækket, af forholdsvis generel art.

Det har ikke været muligt at få fat på EU's specifikke EU krav, derfor har vi kun haft mulighed for at forholde os til de overordnede krav. Gruppen har dog fået oplyst, at der er auditører, der besøger installationer i EU, og at der i Nederland er en godkendt installation. Derfor må der forefindes specifikke krav.

Sikkerhedsgruppens overordnede betragtning

Systemets eksistensberettigelse beror på, at borgerne, færøske myndigheder og EU har tillid til, at systemet lever op til de høje sikkerhedskrav om fortrolighed, integritet og tilgængelighed, som bliver stillet systemer af samme vigtighed. Der skal kun få uheldige hændelser til, før denne tillid svækkes. Derfor må man allerede i startfasen indarbejde tiltag i systemerne mod potentielle trusler, og man må fra opstart af systemet leve op til de krav, som EU stiller.

I dag er cyber space en stor trussel mod IT-sikkerheden, og den bliver ikke mindre i fremtiden. Derfor er det nødvendigt at imødegå denne trussel ved hjælp af standardbeskyttelse som antivirus, firewall m.m. og med samarbejdsaftaler med ekspertorganisationer som f.eks. Center for Cybersikkerhed i Danmark.

Resterende sikkerhedsopgaver

Hvis projektet fortsætter ser vi følgende opgaver:

- EU krav
  Dokumentere specifikke EU krav til løsningen
- Risikovurderinger
  Under systemernes videre udformning er det nødvendigt at evaluere risikovurderingerne regelmæssigt
- Politikker
  Udarbejde nødvendige politikker
- Procedurer
  Udarbejde nødvendige procedurer

- Kontroller
  Etablere nødvendige kontroller
- Systemdokumentation
  Sikre at nødvendig dokumentation forefindes
- Driftsdokumentation
  Sikre at nødvendig dokumentation forefindes
- Samarbejdsaftaler
  Udarbejde ny version af 'Fylgiskjal 5' og dokumentere hærdede krav
- Aftaler om revision
  Sikre at aftale er om nødvendig IT-revision
- CA's sikkerhedskrav
  Udarbejde CA's sikkerhedskrav (a'la OCES), som bl.a. stiller krav om at leverandør skal dokumentere sin sikkerhedsløsning
- Cyber sikkerhed
  Da truslen fra cyber er voksende, er det nødvendigt på Færøerne at etablere et organ i offentlig regi, hvis opgave er at koordinere Færøernes cybersikkerhedsinitiativ og etablere kontakt til ekspertorganisationer f.eks. Center for Cybersikkerhed i Danmark
- Kvalification
  Sikre at CA har adgang til nødvendig kvalificerede ressourcer til at tage hånd om systemerne, drift, IT-sikkerhed og IT-revision
- Oplysning til borgere
  Sikre at borgere får nødvendige oplysninger om sikker håndtering af deres identitet

Sikkerhedsgruppens rapporter og bilag er beregnet til at bygge videre på, hvis projektet fortsætter.

Hermed betragter gruppen sit arbejde som afsluttet.

Sikkerhedsgruppen

Dorit Reinert Jógvan Joensen Jóhan Martin Jacobsen

Bilag 1.

Opdeling af sikkerhedskravene

Kravene er opdelt som vist nedenfor i henhold til ISA/IEC 27002:

- 5 Informationssikkerhedspolitikker
- 6 Organisering af informationssikkerhed
- 7 HR sikkerhed
- 8 Håndtering af aktiver
- 9 Adgangskontrol
- 10 Kryptering
- 11 Fysisk og miljømæssig sikkerhed
- 12 Sikkerhed vedrørende drift
- 13 Sikkerhed vedrørende kommunikation
- 14 Anskaffelse, udvikling og vedligeholdelse af systemer
- 15 Leverandørforhold
- 16 Styring af sikkerhedshændelser
- 17 Informationssikkerhedsmæssige aspekter ved beredskabsstyring
- 18 Overensstemmelse