IT-SIKKERHEDSEFTERSYN

Baseret på ISO27000 og praktisk erfaring

Hvordan sikrer jeg, at min organisations IT-sikkerhed er tilstrækkelig?

HVORFOR ET IT-EFTERSYN?

Virksomheder og organisationer er afhængige af, at IT-systemerne virker. Altså, at man kan kommunikere og arbejde digitalt internt i organisationen og i cyberspace. At man gennem anvendelse af netværk, servere, printere, computere og programmer mv. kan løse de opgaver, som gør at organisation fungerer. At det kan ske uforstyrret og sikkert uden at andre kan misbruge ens data og systemer.

Spørgsmålet er, om IT-systemerne og den tilhørende organisation er robust og sikker nok, hvis der skulle ske et utilsigtet datatab, kompromittering af data eller en menneskelig fejl. Dette vil et IT-sikkerhedseftersyn give svar på.

FORMÅLET MED ET IT-EFTERSYN

Formålet med INFORMI A/S IT-sikkerhedseftersyn er at afdække de områder som virksomheden skal fokusere på for at opnå en tilfredsstillende IT-sikkerhed.

Desuden kan formålet være at forberede virksomheden på en egentlig ISO27000 certificering.

HVAD ER ET IT-EFTERSYN?

INFORMI A/S IT-sikkerhedseftersyn består af en gennemgang af virksomhedens IT-mæssige forhold, herunder organisering, politikker, regler, processer, adfærd og kontroller mv. Dette med henblik på at afdække de områder, hvor organisationen bør foretage forbedringer.

IT-sikkerhedseftersynet giver forslag til forbedringer og opstiller en konkret handlingsplan. Gennemgangen bygger på ISO27000 (SOA)[1] og best practice.

Efter aftale kan IT-sikkerhedseftersynet suppleres med en gennemgang af virksomhedens GDPR-forhold.

INFORMIS IT-SIKKERHEDSEFTERSYN KOMMER RUNDT OM ALLE DE VIGTIGE OMRÅDER

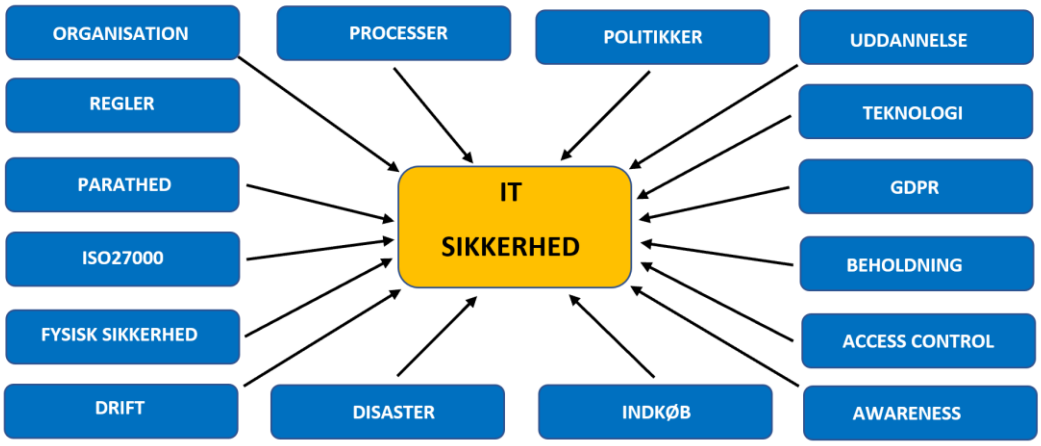

Fig. 1: Komponenter der er indeholdt i IT-sikkerhed

[1] ISO27000 er en international standard for IT-sikkerhed, der er markedsstandard for større private og offentlige virksomheder.

HVORDAN GENNEMFØRES ET IT-SIKKERHEDSEFTERSYN?

Sikkerhedseftersynet gennemføres som en dialog med udgangspunkt i et spørgeskema baseret på ISO27000 SOA[2]. Det indledes med en overordnet afdækning af organisationens overordnede rammer og nuværende IT-forhold. Herefter følger en gennemgang af de områder, der er betydende for IT-sikkerheden, og for hvert område foretages en afdækning af omfang og tilstrækkelighed i forhold til de i SOA anførte kontrolmål.

Sidste del af processen er en afklaring af, hvad organisationen bør gøre for at opnå en tilfredsstillende IT-sikkerhed, samt udarbejdelse af en handleplan med ressourceestimater.

Sikkerhedseftersynets omfang og varighed vil være afhængig af organisationens størrelse og kompleksitet, men et standardforløb for en ikke for kompleks virksomhed vil kunne gennemføres inden for ca. en uge af en til to konsulenter.

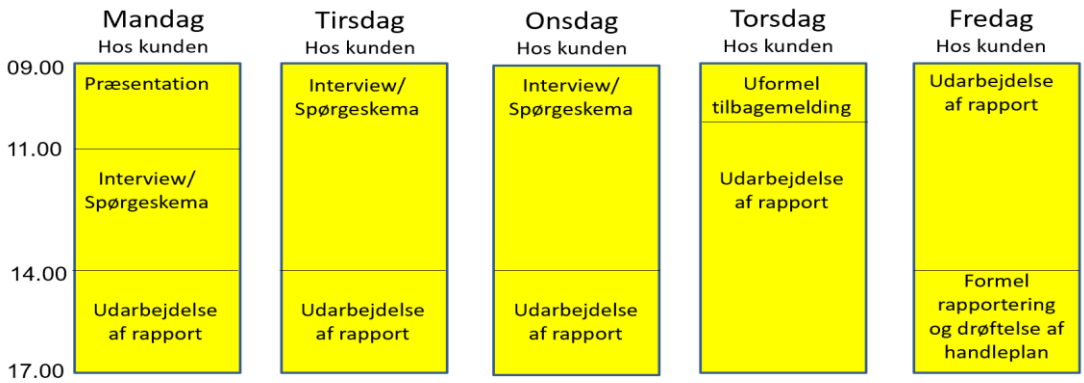

Fig. 2: Generisk tidsplan

AFGRÆNSNING

Den proces som Informi A/S gennemfører med kunden er ikke en ISO-certificering, men en proces der i praksis vedrører alle de elementer som ISO27000-SOA omhandler, samt de elementer der evt. tilføjes som særlige områder af interesse i forbindelse med den enkelte virksomhed.

HVAD KOSTER ET IT-EFTERSYN?

Prisen på et IT-eftersyn fastsættes individuelt og er afhængig af organisationens størrelse og kompleksitet.
For en organisation med en begrænset kompleksitet udgør prisen ca. 60.000 kr.

HVORDAN KOMMER JEG VIDERE?

For yderlig information og vejledning:

Claus Ejlersen, Partner,
tidligere chef for infrastruktur i
Forsvarets Koncern IT
Email: claus.ejlersen@informi.com
Tel.: +45 53 79 39 49

Lars Bæhr, Partner
tidligere chef i Forsvarets Koncern IT
Email: lars.baehr@informi.com
Tel.: +45 28 30 16 77

Bernt Christiansen, Seniorkonsulent
tidligere chef i Forsvarets Efterretningstjeneste
og ansvarlig for IT-sikkerhed i Forsvaret
Email: bernt.christiansen@informi.com
Tel.: +45 24 42 92 09

[2] Statement of Applicability