

God it-sikkerhed i kommuner

En vejledning til kommuner om at skabe et godt fundament for tryk og sikker behandling af kommunens og borgernes oplysninger. Vejledningen beskriver, hvordan DS484-baseret it-sikkerhedsledelse indføres pragmatisk.

Vejledningen er udgivet af Neupart A/S og må frit anvendes af kommuner.

KL må publicere den.

Indhold

| | |
|---|----|
| IT Governance, DS484 og andre standarder | 3 |
| Et DS484-projekt..... | 4 |
| It-sikkerhedshåndbog | 4 |
| Dokumentationsfasen | 5 |
| Implementeringsfasen | 6 |
| Driftsfasen..... | 6 |
| Risikostyring..... | 7 |
| De 5 trin | 7 |
| Hvad skal komme først – håndbog eller risikovurdering?..... | 8 |
| Opfølgning og løbende forbedringer | 9 |
| Omfang af DS484-projekter | 10 |
| Om Neupart..... | 11 |
| SecureAware® KV hjælper kommunen godt på vej | 11 |
| SecureConsult : Skræddersyede konsulentytelser | 11 |
| Fordele til kommunen..... | 12 |
| Kontakt-information | 13 |

IT Governance, DS484 og andre standarder

Den nuværende udgave af den danske standard for informationssikkerhed blev lavet i 2005 inspireret af den daværende internationale standard for informationsikkerhed, ISO17799.

Siden er ISO-standarden omdøbt og gjort til en del af ISO27000-familien, og en række andre standarder for ledelse af informationssikkerhed er tilføjet. I dag er der følgende standarder:

- ISO27001: Krav til et ISMS (Ledelsessystem for informationssikkerhed)
- ISO27002: God skik for informationssikkerhed
- ISO27005: God skik for risikostyring
- ISO27006: Krav til ISMS auditors

På IT Governance området er det passende at nævne Cobit 4.1, som er et "IT Governance Framework". Cobit udgives af IT Governance Institute (www.ITGI.org), som er stiftet af ISACA, en international non-profit-organisation med rødder i revisionsbranchen. Cobit er i dag mapet sammen med både ITIL og ISO2700x, og dermed også med DS484.

*DS484 og ITIL
supplerer
hinanden godt*

For kommuner er DS484 den mest interessante standard, dels fordi KL anbefaler den, fordi staten har valgt at følge den, -og så er den på dansk. I forhold til ITIL drejer DS484 sig primært om ledelse af it-sikkerheden hvor ITIL primært drejer sig om stabile it-services. De to supplerer hinanden godt. Man kan sige, at ITIL bl.a. hjælper kommunen med at efterleve tilgængelighedskravene i DS484.

Efterlevelse – "compliance" på engelsk - med DS484 kan være særdels omfattende, og derfor anbefaler Neupart at DS484 indføres pragmatisk i kommunerne, og at sikkerheden doseres rigtigt med respekt for vigtigheden i at passe ordentligt på kommunens og borgernes informationer.

Kommunens fordele med DS484 efterlevelse er, at fortrolighed, integritet og tilgængelighed for informationerne sikres, og at det er nemmere for kommunen at efterleve sikkerhedskravene i persondatalovgivningen. DS484 er kort sagt god skik for informationssikkerhed.

Et DS484-projekt

DS484-efterlevelse består af mange elementer. Hos Neupart er det vores erfaring, at kommunerne med fordel kan koncentrere sig om følgende discipliner, som alle kræves som en del af DS484:

- It-sikkerhedshåndbog, og den vigtige forankring.
- Risikostyring
- Opfølgning og løbende forbedringer

I de følgende afsnit gennemgår vi disse discipliner, der samtidigt er hovedingredienserne i kommunens it-sikkerhedsledelse (ISMS – Information Security Management System). Neupart's produktlinie SecureAware hjælper kommuner med DS484-efterlevelse, men fremgangsmåden der beskrives i dette dokument er generel og kan også anvendes uden brug af Neuparts løsninger.

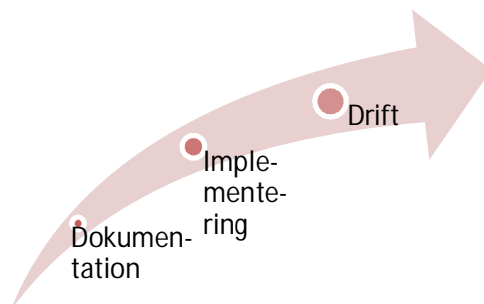
*It-sikkerheds-
forum mødes
regelmæssigt*

Vi anbefaler at etablere et it-sikkerhedsforum tidigt i forløbet. Et it-sikkerhedsforum er en gruppe personer fra forskellige dele af kommunen, som skal mødes regelmæssigt, for eksempel hvert kvartal. Dette er med til at forankre DS484-aktiviteterne.

It-sikkerhedshåndbog

Kært barn har mange navne. It-sikkerhedspolitik, It-sikkerhedshåndbog, politik for informationssikkerhed. I dette dokument bruger vi begrebet "it-sikkerhedshåndbog", og definerer det som en fællesbetegnelse for den overordnede politik, med tilhørende regelsæt (hvad må vi, hvad må vi ikke, nogle gange kaldet retningslinier), samt procedurer, der beskriver hvordan de besluttede regler i praksis efterleves.

Vi opdeler nu DS484-projektet i nogle underprojekter. Det første kalder vi dokumentationsfasen, som efterfølges af implementeringsfasen. Når disse underprojekter er gennemført, går kommunen over i almindelig "drift", forstået på den måde, at informationssikkerheden er blevet integreret i kommunens daglige rutiner og øvrige aktiviteter.



Dokumentationsfasen

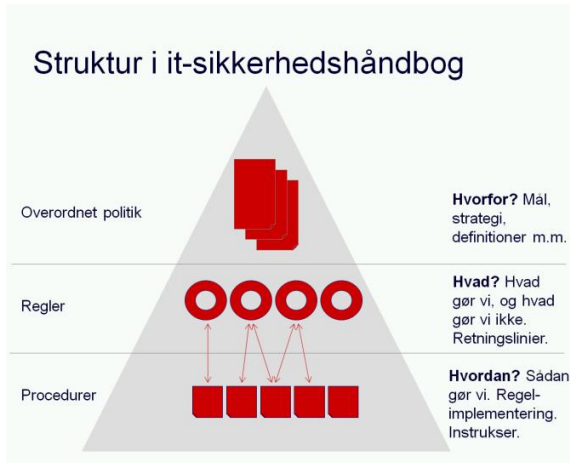
I dokumentationsfasen skal vi opdatere kommunens regler og procedurer, så relevante sikkerhedskrav er efterlevet. Her gennemgås DS484 afsnit for afsnit. DS484 indeholder 135 sikringsforamtalninger, der hver har et antal implementeringsretningslinier. For at en kommune kan påberåbe sig "at efterleve DS484", skal hver eneste sikringsforanstaltning og alle såkaldte basale implementeringsretningslinier efterleves. Det giver ca. 400 krav (!), og derfor anbefaler Neupart som udgangspunkt ikke en fuld efterlevelse. I stedet vurderes de 135 sikringsforanstaltningers relevans for kommunen, hvorefter passende regler og procedurer etableres. Eksisterende regler og procedurer genbruges selvfølgelig, og de relateres til de enkelte DS484-sikringsforanstaltninger.

*Fuld DS484
efterlevelse er
for nogen et
urealistisk
scenarie*

Hvis omfanget af kommunens nuværende dokumentation er så stort, at der ikke rigtigt er et overblik, kan en egentlig dokumentationskortlægning udføres. Her kortlægger man, hvilke DS484-områder der allerede er beskrevet.

Læg mærke til, at DS484 ikke kan udgøre jeres it-sikkerhedspolitik eller –håndbog. DS484 beskriver krav, som skal eller kan følges, og oftest gives ikke konkrete formuleringsforslag til jeres regler og procedurer. Et af kravene er i øvrigt, at andre relevante sikkerhedskrav identificeres. Her kommer blandt andet persondatalovgivningen ind i billedet.

Det er endvidere væsentligt at etablere en god sammenhæng i hele it-sikkerhedshåndbogen. Sammenhængen kan skabes ved referencer, således at regler og procedurers indbyrdes afhængigheder tydeligt fremgår. Se figur "Struktur i it-sikkerhedshåndbog". Gentagelser skal undgås.



Implementeringsfasen

Når it-sikkerhedshåndbogen er opdateret, skal den forankres i organisationen. Kendskab er en forudsætning for, at ansatte i kommunen kan følge it-sikkerhedshåndbogen og dens regler og procedurer. Derfor indeholder DS484 også krav om oplysning, uddannelse og træning it-sikkerhedshåndbogens indhold.

Kommunikation og "awareness-programmer" er derfor naturlige aktiviteter i implementeringsfasen.

Ansvar for alle aktiviteter skal placeres. Uden ansvarsplacering kan man ikke forvente at ting bliver gjort, og det gælder ikke mindst for sikkerhedsaktiviteter, som næppe kan kaldes lystbetonede. Mange anser nærmere sikkerhed som et nødvendigt onde. Den positive udlægning er selvfølgelig, at sikkerhedsaktiviteter muliggør andre it-projekter og øvrige forretningsaktiviteter. Under alle omstændigheder kan awareness-programmer både øge kendskabet til it-sikkerhedshåndbogen og skabe forståelse for, hvorfor reglerne er etableret. Hvis vi får forklaret baggrunden for regler, kan de fleste af os bedre acceptere dem.

Driftsfasen

Kloge folk har udtalt, at it-sikkerhed ikke er et projekt, men en løbende proces. Sandt nok, og det er netop begrundelsen for at it-sikkerhed indarbejdes i relevante rutiner. Et projekt har en slutdato, i modsætning til løbende processer. Det kan således være et

Ingen ansatte kan forventes at efterleve krav, der ikke er tydeligt kommunikeret. Det er årsagen til at kommuner skal gennemføre Awareness-programmer

projekt, at etablere it-sikkerhedshåndbogen, eller at implementere DS484-krav i konkrete systemer, men den efterfølgende it-sikkerhedsledelse er ikke et projekt.

En del af driftsfasen for et system til it-sikkerhedsledelse indebærer, at risikovurderinger udføres løbende, at der regelmæssigt følges op på efterlevelsen, at it-sikkerhedshåndbogen holdes ajour, og at it-sikkerhedsforum mødes regelmæssigt, typisk 4 gange om året.

Risikostyring

Risikostyring er en løbende process, hvor risici mod kommunens informationsbehandling løbende vurderes og behandles. Nøgleordet her er *løbende*. I mange it-sikkerhedshåndbøger skriver man ofte, at "risikovurderinger skal udføres hvert år, ved anskaffelsen af nye systemer, eller ved ændringer i trusselsbilledet".

Risikovurderinger kan udføres efter mange forskellige metoder og på mange detaljeringsniveauer.

De 5 trin



Hos Neupart er vi tilhængere af en pragmatisk vurderingsform. Et risikovurderingsforløb kan se således ud:

Kommunens risiko vokser og falder med sandsynligheden for hændelser og med effekten af hændelserne

1. Kortlægning af væsentlige forretningsprocesser, væsentlige it-systemer og deres indbyrdes afhængighed. Med it-system menes applikationen, for eksempel ESDH, Mail/kalender, Websites med mere. Glem alt om at vurdere alt der har en ip-adresse, i hvert fald i første omgang.
2. Hvert systemer og proces skal have en ejer.
3. Vurder den forretningsmæssige konsekvens af hændelser, vurder sandsynlighed for, at hændelser opstår. Sandsynlighed hænger tæt sammen med sårbarhed: Jo mere sårbart et system er, des mere sandsynligt er det, at der sker en hændelse.

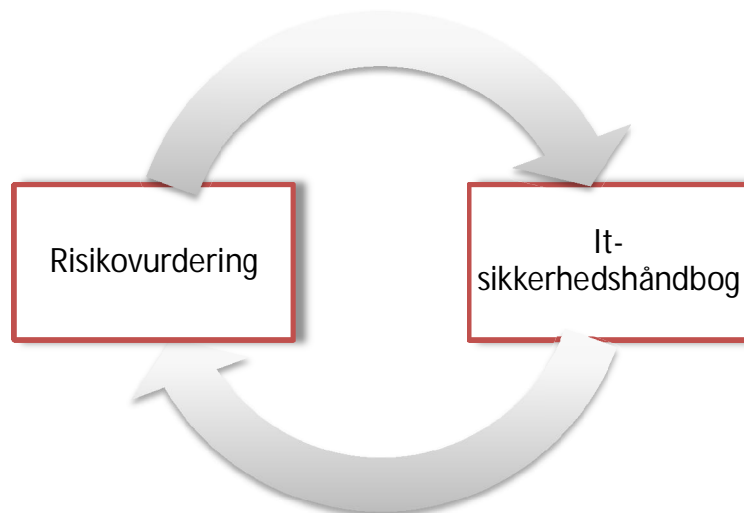
$$\text{Risiko} = \text{Konsekvens} * \text{Sandsynlighed}$$

Vurderingerne foretages per system og/eller process, og gennemføres for fortrolighed, integritet og tilgængelighed. En 1 – 5 skala kan anvendes. Det er typisk en forretningsansvarlig (fx systemejer), der vurderer konsekvens, og en teknisk person der vurderer sårbarhed eller sandsynlighed. Tag gerne udgangspunkt i et trusselskatalog for at sikre, at sårbarheden for relevante trusler vurderes; altså at I ikke glemmer at spørge ind til en væsentlig trussel og sårbarhed.

Risikoappetit
definerer hvor
meget sikkerhed
kommunen
ønsker.

4. Sammensæt resultaterne i overskuelige rapporter, gerne med forskellige detaljeringsgrader
5. Få ledelsens accept på det afdækkede risikobillede, og lav handlingsplan med aktiviteter på de områder, hvor ledelsen ønsker lavere risiko. Bemærk: 100% sikkerhed findes ikke. Det er et spørgsmål om "risikoappetit", altså hvor højt et sikkerhedsniveau, der ønskes.

Hvad skal komme først – håndbog eller risikovurdering?



Nogle konsulenthuse insisterer på først at lave en risikovurdering og dernæst skrive it-sikkerhedspolitik. Det er en udmærket fremgangsmåde, som kommuner også kan bruge,

Kommunen kan starte der hvor det passer den bedst

ligesom Neupart nogle gange også anvender denne fremgangsmåde. Risikovurdering og politik hænger imidlertid gensidigt sammen i en proces, hvor det, som står i it-sikkerhedshåndbogen, har indflydelse på resultatet af risikovurderingen, og risikovurderingen giver input til it-sikkerhedshåndbogen. Da dette er en cyklisk proces, kan kommunen hoppe ind i hjulet der, hvor det passer bedst til den enkelte kommunes situation.

Opfølgning og løbende forbedringer

Opfølgning er vigtigt i ethvert system, også i et system til it-sikkerhedsledelse. Opfølgningen kan finde sted på mange måder, og den afhænger til dels af virksomhedens kultur og vaner. Begreber som intern og ekstern revision, "self-assessments", erklæringer, stikprøver, afprøvning, behandling af hændelser, metrikker og målinger er typisk forbundet med opfølgningen. Nogle kommuner foretrækker en mere formel indgangsvinkel, hvor kontrol prioriteres, andre baserer sig i videre udstrækning på "self-assessments".

Vi anbefaler, at opfølgningsarbejdet i stor udstrækning baseres på kommunens it-sikkerhedspolitik. Ved hjælp af simple spørgeskemaer, der er baseret på kommunens faktiske regler og procedurer, kan kommunen danne sig et indtryk af, om der er et "gap" mellem virkeligheden og politikken. Hvis I lader udvalgte af kommunens ansatte svare på, hvorvidt de selv efterlever konkrete dele af politikken, får I "self assessments", som kan give jer gode hints om, hvor I har forbedringsmuligheder.

Det er vores erfaring, at medarbejdere, i organisationer, hvor man har en kultur baseret på tillid og respekt, i interviews svarer ærligt og bidrager konstruktivt omkring efterlevelse af regler.

Opgaveløsning skal registreres i sammenhæng med it-sikkerhedshåndbogen.

I kan vælge at få i udført revision på grundlag det samme spørgeskema, nemlig kommunens it-sikkerhedshåndbog. Det er simpelt at lade en revisor kontrollere punkterne i det samme spørgeskema, eller samme form for spørgeskema. På grund af koblingen til jeres it-sikkerhedspolitik, lettes opfølgningen på eventuelle afvigelser.

Uanset kontrol og "self-assessments" er der et område, der virkelig gør en forskel i jeres sikkerhedsarbejde: Opgaveløsning: At små og store opgaver bliver løst, og at det registreres, i hvilken grad de er løst. Det gælder både dag til dag opgaver, men i høj grad også tilbagevendende opgaver med længere intervaller, for eksempel et årligt review af it-sikkerhedshåndbogen, den årligt tilbagevendende risikovurdering, de kvartalsvise it-sikkerhedstest osv.

Organisatorisk kan kommunen med fordel etablere det nævnte it-sikkerhedsforum. Der vedtages en agenda, som bl.a. sikrer opfølgning på konkrete hændelser samt stillingtagen til, om it-sikkerhedsniveauet er tilstrækkeligt og passende (for eksempel baseret på vedtagne metrikker og målepunkter).

Omfang af DS484-projekter

Det kan være vanskeligt at sige noget generelt om varigheden af DS484-projekter. Det skyldes dels, at DS484 berører mange områder, men også at kommunerne kan have forskelligt "modenhedsniveau". Vi prøver alligevel 😊

Selvom konsulenthuse (inkl. Neupart) kan og vil rådgive mest muligt om DS484-projekter, kræver projekterne altid involvering fra kommunens egne folk. Med alle disse forbehold kan vi nævne, at erfarne it-sikkerhedskonsulenter kan skrive politik på dage og regler eller retningslinier på uger. Procedurer tager typisk lidt længere tid, men løses bedst med større involvering fra kommunens egne ansatte. Risikovurderinger kan, afhængig af detaljeringsgrad og antal systemer og processer, udføres fra 3 dage og op. Under alle omstændigheder er det vigtigt at fastslå, at it-sikkerhedsledelse ikke kan outsources 100% til en leverandør. Alle de nævnte områder kræver involvering for at få ordentlig forankring.

Officepakken er ikke egnet til it-sikkerhedsledelse

Værktøjer til it-sikkerhedsledelse giver fordele. En af fordelene er, at tidsforbruget kan nedbringes både indledningsvist og løbende. En Office-pakke er ikke et egnet værktøj. Den er uegnet til at lave målgruppe-opdelte it-sikkerhedshåndbøger, at holde styr på forskellige personers risikovurderinger eller "compliance"-besvarelser, at registrere om information er læst, at måle kendskab og kæde udførte opgaver sammen med it-sikkerhedshåndbogen.

Leverandør med
stor erfaring

Om Neupart

Neupart A/S hjælper kommuner med tryk og effektiv efterlevelse af it-sikkerhedskrav. Kommunens sikkerhedskrav kommer fra lovgivning, borgere, samarbejdspartnere, andre myndigheder eller kommunen selv. En stor del af kommunerne, staten og regionerne, samt en lang række store og små private virksomheder er kunder hos Neupart. Neupart er dansk-ejet, har egne datterselskaber i Tyskland og USA, samt forhandlere i en række andre lande. Neupart er ISO27001-certificeret. SecureAware® og SecureConsult® er Neupart's varemærker.

En standard-
løsning til
kommuner.

SecureAware® KV hjælper kommunen godt på vej

Med produktpakken SecureAware® KV får kommunen en komplet serie af løsninger, der kan anvendes samlet eller hver for sig alt efter den enkelte kommunes behov.

Modulerne i den nye SecureAware KV hjælper med it-sikkerhedsledelse:

- SecureAware Policy: It-sikkerhedshåndbog
- SecureAware BCP: It-beredskabsplan
- SecureAware Compliance Analysis II: DS484-efterlevelse
- SecureAware Compliance Workflow: Opfølgning og opgavestyring
- SecureAware Risk: Risikostyring
- SecureAware Awareness: Målrettet kommunikation til slutbrugere

SecureConsult : Skræddersyede konsulenttydelser.

SecureConsult er navnet på Neuparts konsulenttydelser, der effektivt hjælper kommuner til passende informationssikkerhed. Ikke for meget, ikke for lidt, men passende informationssikkerhed. Vi bruger værktøjer og metoder, så vores erfarne konsulenter kan hjælpe dig og dine kollegaer trygt og effektivt. Du kan få hjælp til selvhjælp, eller vi kan lave det meste af arbejdet for dig.

Fordele til kommunen

SecureAware KV giver blandt andet følgende fordele til kommunen:

DS484 i praksis: SecureAware KV hjælper kommuner med at efterleve DS484:2005 i praksis. Relevante dele af indholdet er udviklet i samarbejde med Dansk Standard.

Tryghed: Overblik over, om kommunen overholder relevante krav.

Gennemprøvet: SecureAware KV er danske kommuners foretrukne løsning til effektiv it-sikkerhedsledelse. Se de mange referencekunder på www.neupart.dk

Persondata-forvaltning: Det er enkelt at efterleve sikkerhedsbekendtgørelsens krav om interne uddybende sikkerhedsregler og andre krav på persondatalovens område.

Individuelt tilpasset: Kommuner er forskellige, med egne organisationskulturer og individuelle it-sikkerhedsbehov. Det er nemt at tilpasse SecureAware KV.

Bedre sikkerhed: Med SecureAware KV er det let at prioritere indsatsen og gøre it-sikkerhed operationel i hele forvaltningen.

Certificeret: Neupart er eneste danske it-sikkerhedsleverandør, der er certificeret af Dansk Standard i ISO27001.

Kontakt-information

Danmark (hovedkontor):
Neupart A/S
Hollandsvej 12
2800 Lyngby
Tel. +45 7025 8030
Fax +45 7025 8031
CVR nummer 26295092

Nordamerika:
Neupart Americas Inc
2553 Crescent St
Ferndale, WA 98248
Tel +1 360 820-2545
Fax + (360) 392-6078

Tyskland:
Neupart GmbH
Kaiserwerther Strasse 115
40880 Ratingen/Düsseldorf
Tel +49 2102 420926

Læs mere på www.neupart.dk, hvor I kan få gratis uddannelse i SecureAware, og høre hvad andre kunder siger om samarbejdet med Neupart.

Eller ring uforpligtende på telefon 7025 8030.