

Veileder i sikkerhetsarkitektur

For virksomheter som behandler personopplysninger og sensitive personopplysninger.

August 2011



Innhold

Innledning	3
Krav i regelverket	5
Hva er informasjonssikkerhet?	8
Risikovurderinger og akseptkriterier	9
Generelle sikkerhetsprinsipper	11
Systemteknisk sikkerhet – Innledning	15
Systemteknisk sikkerhet – Soner	20
Systemteknisk sikkerhet – Prinsipper for nettverksoppsett.....	23
Systemteknisk sikkerhet – Sikkerhetsbarrierer	27
Bruk av databehandler.....	29
Definisjoner fra personopplysningsloven	30
Ordliste.....	33

Innledning

Denne veilederen gjelder for offentlige og private virksomheter som behandler store mengder personopplysninger, men kan også være nyttig virksomheter som tilbyr tjenester som innebærer behandling av personopplysninger og sensitive personopplysninger¹. Dette kan for eksempel være omsorgsrelaterte virksomheter eller databehandlere.

Veilederen fokuserer på hvordan en virksomhet bør implementere teknologiske tiltak for informasjonssikkerhet etter at informasjonssikkerhetsarbeid for internkontroll er gjennomført. Den retter seg i hovedsak mot IT- og sikkerhetspersonell og tar utgangspunkt i regelverkets krav om forholdsmessig sikring av personopplysninger. Tilsynet har lagt vekt på å skissere hensiktsmessige og funksjonelle tekniske løsninger, hvor man bygger på tilsynets erfaringer fra kontrollvirksomhet, saksbehandling, råd- og veiledningsmøter samt tidligere veiledere. Prinsippet om separate nettverk som Datatilsynet har presentert i tidligere veiledere, har ikke endret seg. En slik løsning anses som en fleksibel og arbeidseffektiv løsning som gjenspeiler tilgjengelige produkter og ny teknologi. Veilederen erstatter derfor "Datatilsynets veileder for kommuner og fylker".

Utgangspunktet for veilederen er prinsipper fra, og tolkninger av, personopplysningslovens § 13 og helseregisterlovens § 16 om sikring av personopplysninger. De to bestemmelsene er ganske like. Datatilsynet har derfor, i denne veilederen, valgt å ta utgangspunkt i personopplysningslovens bestemmelser. Veilederen må ses i sammenheng med personopplysningsforskriftens kapittel 2 med kommentarer.

For helserelaterte virksomheter, for eksempel leger, sykehus, tannlege og fysioterapeuter vil denne veilederen vil være et supplement til Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren når det gjelder overordene prinsipper for virksomhetens informasjonssikkerhet (Normen). Normen er utarbeidet av representanter for sektoren, og Helsedirektoratet koordinerer dette arbeidet. Normen og tilhørende faktaark er tilgjengelig på normen.no

Denne veilederen gir ingen fullstendig oversikt over alle tilgjengelige teknologier for informasjonssikkerhet. Den tar utgangspunkt i Datatilsynets vurderinger av utvalgte teknologier og metoder, og presenterer hovedprinsipper for tilrettelegging for eksempel ved bruk av terminalserver, virtuelle servere, SAN og ekstern pålogging. Ut fra dette illustrer veilederen Datatilsynets anbefalte overordende metoder for etablering av tilfredsstillende informasjonssikkerhet ved:

¹ Se definisjoner fra personopplysningsloven s. 30

- elektronisk behandling av personopplysninger i virksomhetens informasjonssystem.
- tilkobling av virksomhetens informasjonssystem til eksterne datanettverk.
- ekstern datakommunikasjon, herunder ekstern kommunikasjon av sensitive personopplysninger.
- ekstern tilgang til virksomhetens informasjonssystem.

For å forklare de tekniske tiltakene som foreslås i veilederen nærmere, har Datatilsynet laget temaark. Disse gir eksempler på metoder for utforming av ulike løsninger. Eksempelene og metodene som er oppgitt er ikke den eneste måten å løse dette på og temaarkene er derfor ment som en veiledning eller et utgangspunkt, heller enn en fasit.

Krav i regelverket

Personopplysningslovens § 13 og helseregisterlovens § 15 har overordnede bestemmelser om informasjonssikkerhet. Denne veilederen skal hjelpe virksomheter til å sikre at de oppfyller tekniske tiltak for å etterleve følgende bestemmelse; *”Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.”*

Personopplysningsforskriftens kapittel 2 er en felles forskrift om informasjonssikkerhet for personopplysningsloven og helseregisterloven.

Nedenfor er bestemmelsene som gjelder tekniske tiltak gjengitt *i kursiv*. Kravene i forskriften er, det dette er nødvendig, utdypet med merknader til de enkelte paragrafer i forskriften og supplerende tekst. Dette er for å klargjøre forskriftskravene.

§ 2-4 om risikovurdering

Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger.

Det er virksomhetens ansvar å sette akseptkriteriene for risiko, men slike beslutninger kan ifølge § 2-2 overprøves av Datatilsynet. Denne veilederen legger til grunn de akseptkriterier som Datatilsynet benytter i sin praktiske veiledning, og er ikke å regne som et vedtak fattet av Datatilsynet.

Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd.

Det stilles ikke stilt krav om ”risikoanalyse”, kun en risikovurdering. Denne veilederen er begrenset til hvilke viktige momenter en risikovurdering av tekniske tiltak bør inneholde.

§ 2-7 om organisering

Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.

En konfigurasjon omfatter informasjonssystemets utforming, det vil si utstyr og program samt sammenkobling av disse. Denne veilederen viser sentrale elementer for konfigurering i en sikkerhetsarkitektur.

§ 2-14 om sikkerhetstiltak

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk.

Veilederen beskriver eksempler på tekniske tiltak for å hindre sikkerhetsbrudd.

Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.

Den behandlingsansvarlige må etablere tiltak som fungerer uavhengig av medarbeidernes handlinger. Sikkerhetstiltak bør tilpasses slik at minimum to uavhengige tiltak må påvirkes før et sikkerhetsbrudd får betydning. Siden regelverket krever tilfredsstillende sikring, har veilederen som prinsipp at det er nødvendig med to uavhengige tekniske tiltak mellom omverdenen og sikret sone. I tillegg er en slik sikring ment som et tiltak for sikring av øvrige soner i informasjonssystemet.

§ 2-11 om sikring av konfidensialitet

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig.

Bestemmelsen pålegger behandlingsansvarlige å hindre uautorisert innsyn i personopplysninger. Definisjon av hvilke opplysninger som krever konfidensialitet og hvilke sikkerhetstiltak som må etableres for å oppfylle dette, vil være et resultat av risikovurderingen. Veilederen gir eksempler på tiltak som hindrer uautorisert tilgang til personopplysninger både internt i virksomheten, for eksterne og ved uautorisert utlevering av personopplysninger.

§ 2-12 om sikring av tilgjengelighet

Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig.

Bestemmelsen pålegger behandlingsansvarlige å sikre nødvendig innsyn i opplysninger for å kunne gjennomføre avtalt behandling av personopplysninger. Definisjonen av hvilke opplysninger som skal ha sikret tilgang og hvilke sikkerhetstiltak som må etableres vil være et resultat av risikovurderingen. Veilederen utdyper hovedprinsipper for tilgang, men går ikke i detalj om tilgangsstyring og logging i ulike applikasjoner.

§ 2-13 om sikring av integritet

Det skal treffes tiltak mot uautorisert endring av personopplysninger hvor integritet er nødvendig.

Denne bestemmelsen pålegger behandlingsansvarlige å hindre tilfeldig endring av personopplysninger. Resultatet av risikovurderingen vil definere hvilke opplysninger det skal sikres integritet for og hvilke sikkerhetstiltak som må etableres. Veilederen omtaler kun hovedprinsipper for sikring av integritet.

Det skal treffes tiltak mot ødeleggende programvare.

Behandlingsansvarlige skal sørge for at systemet/virksomheten er beskyttet mot ødeleggende program, for eksempel "datavirus".

Hva er informasjonssikkerhet?

Informasjonssikkerhet ved behandling av personopplysninger skal være en tilpasset sikring av tekniske og fysiske informasjonssystemer. Informasjonssikkerheten skal bygges ut fra virksomhetens utføring og dokumentasjon av følgende hovedelementer:

1. **Risikovurdering** - en vurdering av hvilken risiko bruk av informasjonssystemet medfører for de ulike opplysninger som behandles i virksomheten. Ut fra resultatet av risikovurderingen skal det iverksettes nødvendige organisatoriske og tekniske tiltak for å oppnå et akseptabelt risikonivå.
2. **Internkontroll** - dokumentasjon og gjennomføring av nødvendige rutiner i samsvar med risikovurdering og kravene i personopplysningsforskriftens kapittel 2.
3. **Tekniske tiltak** - dokumentasjon og gjennomføring av de tekniske sikkerhetstiltak som risikovurderingen krever for å oppnå tilfredsstillende informasjonssikkerhet.

Internkontroll og tekniske tiltak skal iverksettes ut fra resultatet av risikovurderingen.

Datatilsynet har utarbeidet flere veiledere om organisering av arbeidet med å ivareta kravene til personopplysningsloven med forskrift, for eksempel:

Risikovurdering

Veilederen "Risikovurdering av informasjonssystem" er beregnet på alle virksomheter. Dette er en utdypende veiledning i risikovurdering som Datatilsynet anbefaler å bruke som støtte for gjennomføring av en nødvendig risikovurdering, som igjen er grunnlaget for å iverksette de tekniske tiltak vi behandler i denne veilederen.

Internkontroll

"En veiledning om internkontroll og informasjonssikkerhet" gir utdypende veiledning i arbeidet med å sikre ivaretagelse av kravene til internkontroll og informasjonssikkerhet i personopplysningsloven med forskrift. Veilederen er beregnet for større virksomheter, og virksomheter som behandler store mengder personopplysninger om andre enn egne ansatte. Tilsynet anbefaler å bruke denne som støtte for å iverksette nødvendige organisatoriske tiltak i tillegg til de tekniske tiltak som er beskrevet i den veiledning du nå leser.

Tekniske tiltak

Veileder i sikkerhetsarkitektur gjelder for tekniske tiltak som bør iverksettes i tillegg til organisatoriske tiltak. Denne veilederen i tekniske tiltak fritar på ingen måte virksomheten for organisatoriske tiltak, men skal sikre at de også gjenspeiles i informasjonssystemet.

Risikovurderinger og akseptkriterier

For å kunne gjøre en risikovurdering må det etableres en oversikt over hvilke behandlinger av personopplysninger som utføres i virksomheten. Etter å ha gjennomført en risikovurdering vil en virksomhet sitte med en oversikt over hvilke behandlinger som krever sikkerhetstiltak.

Ved utarbeidelse av nivåer for akseptabel risiko, anbefaler Datatilsynet at virksomheten tar utgangspunkt i en skala for konsekvens og sannsynlighet. Virksomhetens vurdering av akseptable konsekvenstyper kan rangeres på en skala fra 1 til 4 (fra ubetydelig til kritisk) og samme vurdering gjøres for sannsynlighetsskalaen, som oftest går fra 1 til 4 (usannsynlig til sannsynlig).

Ved å kombinere (multiplisere) hva virksomheten definerer som maksimal akseptabel konsekvens med det som er definert som maksimal akseptabel sannsynlighet, defineres nivå for akseptabel risiko. Dette gir et tall eller tallområde for akseptkriterier. Det anbefales at virksomheten utdypet tallene for akseptabel risiko skriftlig slik at analysen blir lettere tilgjengelig også for de som ikke har vært med på gjennomføringen av risikoanalysen.

Det kan være nyttig å tenke på at det vil være virksomhetens leder som skal stå frem for å forsvare akseptabel risiko ved for eksempel å si;

“vår virksomhet aksepterer at dette spesielle uhellet skjer 1 gang hvert ... år. Dette er normalt og vi ser derfor ingen grunn til å iverksette spesielle tiltak ...”

Datatilsynets erfaring er at bedriftens leder oftest står frem og sier;

“dette uhellet er et brudd på våre sikkerhetsbestemmelser og vi vil iverksette forsvarlige tiltak slik at dette ikke ...”

I den siste uttalelsen gis det ikke noe inntrykk av virksomhetens risikovurdering. En risikovurdering innebærer at virksomheten gjør en konkret vurdering av alle enkeltkomponenter i sikkerhetsløsningen. Denne vurderingen bidrar til en god risikovurdering fordi konfigurasjonskart og funksjonsforklaring vil vise de enkelte komponentene i en overordnet sikkerhetsarkitektur.

Akseptkriterier benyttet i sikkerhetsarkitekturen for sikret sone

Her følger noen eksempler på akseptkriterier benyttet i sikkerhetsarkitekturen i virksomheter hvor det skal gjøres planlagte behandlinger av sensitive personopplysninger. Datatilsynet understreker at virksomheten selv må definere hvilke akseptkriterier som skal legges til grunn.

Konfidensialitet skal sikres for å unngå at noen utenfor virksomheten, uansett ressurser, skal få tilgang til sensitive personopplysninger. Ansatte skal heller ikke ha tilgang til eller mulighet til å kunne utlevere sensitive opplysninger, uten å bryte tekniske sperrer.

Systemtilgjengelighet for autorisert personell skal ytes i X% av tiden på alle arbeidsdager.

Integritet i systemene skal sikres slik at det ikke er mulig for personer eller ondsinnet programvare utenfor virksomheten, uansett kompetanse og hjelpemidler å forårsake endring eller ødeleggelse av opplysninger.

Akseptkriterier benyttet i sikkerhetsarkitekturen for intern sone

Eksempler på akseptkriterier som benyttes i virksomheter hvor det er planlagt å bruke personopplysninger sammen med taushetsbelagte opplysninger, men hvor det ikke foregår planlagt behandling av sensitive personopplysninger.

Konfidensialitet skal sikres for å unngå at noen utenfor virksomheten med kjente teknikker, skal få tilgang til personopplysninger i intern sone. Ansatte skal heller ikke få tilgang til personopplysninger, uten nødvendig autorisasjon uten at dette blir oppdaget. Autorisert personell skal ikke kunne utlevere opplysninger uten å bryte organisatoriske sperrer.

Systemtilgjengelighet for autorisert personell skal ytes i X% av tiden på alle arbeidsdager.

Integritet i systemene skal sikres slik at det ikke er mulig for personer eller ondsinnet programvare utenfor virksomheten å forårsake endring eller ødeleggelse av opplysninger.

Veilederen gir ikke spesielle akseptkriterier for DMZ (**Demilitarisert sone**) eller åpen sone. Dette er fordi veilederen, som tidligere nevnt, kun gir generelle råd.

Generelle sikkerhetsprinsipper

Sikkerhet forbindes oftest med tilgangsstyring, men like viktig som dette er:

- Personellsikring
- Fysisk sikring av lokaler og utstyr
- Systemteknisk sikkerhet

Her følger en nærmere beskrivelse av disse tre punktene.

Personellsikring

Krav til kompetanse

Alle medarbeidere som bruker, administrerer, vedlikeholder eller utvikler informasjonssystemene eller på annen måte påvirker informasjonssikkerheten, skal ha nødvendig kompetanse for å utføre sine oppgaver. Medarbeidere som har overordnet operativt ansvar for drift av informasjonssystemet eller informasjonssikkerheten, skal kunne dokumentere nødvendig og relevant kunnskap om teknologien virksomheten benytter i sitt informasjonssystem.

Virksomheten skal utarbeide rutiner som sørger for at denne kompetansen vedlikeholdes og utvikles. Sentrale elementer i slike rutiner består av at virksomheten har:

- oversikt over den enkelte medarbeiders kompetanse.
- oversikt over kompetansekrav for de ulike oppgaver og funksjoner
- årlige planer for kompetanseutvikling.

De årlige medarbeidersamtalene er et godt utgangspunkt for å drøfte status for og videreutvikling av kompetanse hos medarbeidere.

Taushetsplikt

Medarbeidere som har tilgang til sensitive personopplysninger eller til informasjon om sikring av slike opplysninger, er underlagt taushetsplikt og skal undertegne taushetserklæring. Dette kravet vil også omfatte databehandlere og andre eksterne som for eksempel servicepersonell som har tilgang til informasjonssystemer hvor personopplysninger behandles. Dette gjelder alle informasjonssystemer virksomheten er behandlingsansvarlig for.

Alle som har skrevet under taushetserklæringen skal informeres om taushetspliktens omfang og varighet samt hvilke konsekvenser det vil få om den brytes. Det skal også dokumenteres hvem som har inngått taushetserklæring med virksomheten. Denne oversikten må til enhver tid være oppdatert slik at det finnes en oversikt over hvem i virksomheten som kan gjennomføre hvilke arbeidsoppgaver i systemer hvor personopplysninger blir behandlet.

Autorisasjon

Med utgangspunkt i virksomhetens sikkerhetsstrategi, skal medarbeidere bare gis adgang til systemområder eller tilgang til personopplysninger som er nødvendig for at de skal kunne utføre sine pålagte oppgaver.

Formålet med autorisasjonsrutinen er å sikre at de som har et tjenestelig behov for adgang til områder og utstyr samt tilgang til soner, data og programmer. De dette gjelder skal også til enhver tid ha nødvendig autorisasjon til dette. En rutine for autorisasjonstildeling skal omfatte:

- autorisasjon av nyansatte, vikarer og partnere i henhold til tjenstlige behov.
- behov for endringer ved forandring av oppgaver, herunder sletting av autorisasjon når noen ikke lenger har tjenstlige behov for tilgang, for eksempel når en medarbeider slutter i virksomheten.
- kontroll med at tildelte autorisasjoner fungerer etter forutsetningene satt i virksomhetens internkontroll.

Fysisk sikring av lokaler og utstyr

Virksomheten skal sørge for at lokaler og utstyr den benytter er forsvarlig sikret.

Dette gjelder særlig for de rommene hvor det er plassert utstyr for behandling eller sikring av sensitive personopplysninger, for eksempel tjenermaskin, kommunikasjons- og nettverksenheter. For å sikre at sikkerhetstiltakene er tilpasset den enkelte virksomhets behov og trusselbilde, må det gjennomføres en risikovurdering. Denne vil identifisere nødvendige tiltak.

Fysisk sikring ved behandling av sensitive personopplysninger er en vesentlig del av det totale sikkerhetskonseptet. Trusler som kan utløses ved for dårlig fysisk sikring kan være:

- at uvedkommende får tilgang til utstyr hvor sensitive personopplysninger behandles.
- tyveri av PC-er eller sikkerhetskopier både i og utenom arbeidstid.
- sabotasje eller hærverk mot vitale deler av informasjonssystemet.

Selv om ingen kan sikre seg 100 % mot uautorisert adgang må virksomheten velge sikkerhetsløsninger som oppdager forsøk på inntrenging, samt rapportere disse som avvik. Tiltakene bør være gode nok til at slike forsøk forsinkes tilstrekkelig, slik at respons på utløst alarm kan gi de ansatte mulighet til å avverge eller begrense konsekvensene av et sikkerhetsbrudd.

Virksomheten må også påse at tilsvarende sikkerhetskrav for behandling av sensitive personopplysninger stilles til eventuelle databehandlere. Dette bør etableres i en databehandleravtale.

Adgangskontroll

Alle som får adgang til lokaler og utstyr der personopplysninger behandles skal kontrolleres. Lokaler og utstyr der sensitive personopplysninger behandles, eller der man har informasjon om sikring av slike opplysninger, skal ha spesielle sikringstiltak.

Virksomheten må vurdere om det er behov for å innføre fysisk områdeinndeling av lokaler for å skille områder som trenger spesiell beskyttelse fra andre områder. Sikringen kan gjennomføres ved bruk av adgangskontroll til lokaler eller ved innføring av spesielle sikringsmekanismer knyttet til bruk av selve utstyret. Kun personell med behov skal ha adgang til dedikerte rom med driftsutstyr (servere og utstyr). Medarbeideres adgang til virksomhetens lokaler skal i størst mulig grad begrenses til den enkeltes tjenestelige behov.

Virksomheter som tar imot eksternt besøk må definere i hvilke deler av virksomhetens lokaler adgangskontroll skal benyttes, og i hvilken grad sikring skal kobles til bruk av utstyret.

Områdesikret adgangskontroll

Der virksomheten bruker områdesikret adgangskontroll for områder hvor sensitive personopplysninger behandles, skal det kontrolleres at kun autorisert personell har adgang. Det betyr at autorisert personell ikke vil kunne ta med seg uautorisert personell inn i området.

Dette innebærer at:

- områder der sensitive personopplysninger behandles skal kontrolleres av et adgangskontrollsystem.
- nøkkelasvarlig skal ha mottatt skriftlig autorisasjon før den enkelte får nøkler og koder for adgang.
- den enkeltes tildelte adgangsrettigheter er begrenset til det som er nødvendig ut fra tjenestelig behov, og tilgangen fjernes når arbeidsforholdet opphører.
- besøkende alltid følges av ansatte som er autorisert for adgang til området, og blir aldri etterlatt alene.

Adgang til utstyr

Når virksomheten benytter sikkerhetsmekanismer i utstyret for å begrense adgang til sensitive opplysninger, skal kun medarbeiderne som har tjenestelig behov for tilgang

til disse opplysningene kunne bruke utstyret. Dette gjelder både arbeidsstasjoner, skrivere, kopimaskiner, telefaks og annet utstyr.

Virksomheten må sikre at dette gjennomføres i praksis, gjennom å etablere gode rutiner og teknisk sikring som hindrer uautorisert bruk av utstyret, samt egnede tiltak mot innsyn.

Risikovurdering av lokaler og utstyrs plassering

Risikovurderingen må ta utgangspunkt i de konkrete fysiske arealene som skal sikres mot uautorisert adgang. Den bør belyse et eventuelt behov for å dele virksomhetens areal inn i ulike soner. En sonemodell som definerer internt og eksternt personells fysiske adgang til personopplysninger kan defineres slik:

Åpen sone. arealer hvor publikum har fri adgang, for eksempel korridorer, venterom, fellesarealer eller områder med alminnelig ferdsel.

Indre sone. åpne arbeidsplasser (områder med begrenset ferdsel), arealer beregnet kun for medarbeidere i virksomheten eller eventuelt publikum i følge med medarbeidere, resepsjonsarbeidsplassen, kontorer og vaktrom.

Sikret sone. arealer hvor kun spesielt godkjente (autoriserte) medarbeidere har adgang for eksempel datarom, rom med nettverk, servere og kommunikasjonsutstyr.

For mindre virksomheter der soneinndeling ikke er mulig, må en risikovurdering belyse risikoen for at uvedkommende kan få adgang til personopplysninger innen virksomhetens areal.

Systemteknisk sikkerhet - Innledning

Systemteknisk sikkerhet kan deles inn i to hovedområder. Sikkerhet i datakommunikasjon på protokoll- og nettverksnivå og logiske sikkerhetstiltak i selve databasen, applikasjonen eller systemet. Sistnevnte vil typisk være tilgangsstyring. De to hovedområdene har flere underliggende områder som vil beskrives etter en gjennomgang av de overordnede områdene.

Datakommunikasjon

For at ulike nettverkskomponenter og løsninger skal kunne kommunisere med hverandre, opprettes det ulike kommunikasjonskanaler i nettverket, basert på OSI-modellen. Disse kanalene bruker også ulike kommunikasjonsporter² (1 til 65535). For eksempel bruker LDAP i Active Directory både port 389 og en rekke andre porter for å kommunisere³. Dette er ikke unikt for denne kommunikasjonsprotokollen ettersom mange nettverkskomponenter og mye programvare er avhengig av å kommunisere med slike autentiseringsløsninger.

Manglende kontroll over datakommunikasjon innebærer klare risikoelementer. Åpne porter eller kommunikasjonskanaler som ikke er rett konfigurert eller ingen har kontroll over, kan føre til lavere sikkerhet for personopplysningene som blir behandlet. Det er også svært viktig å ha kontroll over datakommunikasjon ved bruk av flere soner, særlig mellom intern og sikret sone. Dersom det er en mulighet for at informasjon flytter utilsiktet mellom soner, har man ikke kontroll på hvilken datakommunikasjon som går imellom de enkelte sonene. Dersom det benyttes fellesløsninger for begge sonene, for eksempel skrivere, vil slike løsninger kunne omgå sikkerheten satt opp i brannmurer mellom sonene. Her er det viktig å være bevisst på sikkerheten og datakommunikasjonen på selve skriveren opp mot personopplysningenes normale soneplassering. I dette tilfellet vil det si at dokumenter fra intern sone og sikret sone ikke bør ende opp samme fysiske sted. Dette prinsippet gjelder for alle slike fellesløsninger mellom soner.

Et annet viktig prinsipp Datatilsynet har ved bruk av sikret sone, er hvilken vei kommunikasjonen initieres. Tilsynets utgangspunkt er at all kommunikasjon skal initieres fra sikret sone og ikke inn mot sonen utenfra. Dette ivaretar prinsippet om at sonen er sikker og at de to sikkerhetsbarrierene fungerer som forutsatt. Det kan gjøres unntak fra dette prinsippet, for eksempel med DMZ og terminalserver eller andre lignende tekniske tiltak som forhindrer direkte kommunikasjon inn mot sikret sone.

² http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

³ [http://technet.microsoft.com/en-us/library/dd772723\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd772723(WS.10).aspx)

Datakommunikasjonen i et nettverk byr på mange problemstillinger. Særlig nevneverdig er brukerautentisering på tvers av soner og programmer eller såkalt "Single Sign-On". Denne spesifikke problemstillingen gjennomgås i veilederens temaark.

Logisk sikkerhet i systemer

Logisk sikkerhet skal supplere sikkerheten i datakommunikasjonen gjennom blant annet tilgangsstyring i systemer og applikasjoner. Det er viktig for funksjonalitet knyttet til logisk sikkerhet at datakommunikasjon ligger i bakgrunnen. Utelukkende logisk sikkerhet innebærer store risikoelementer som kan bety utilfredsstillende sikring av opplysninger. For eksempel:

”For å bidra til en enklere hverdag for saksbehandlere i en kommune, ønsker man å beskytte sensitive personopplysninger i sakssystemet ved kryptering av databasen. I tillegg legges det opp til tilgangstyring på et tilfredsstillende nivå. Kommunen bestemmer også at den krypterte databasen flyttes ut av sikret sone for å skape en lettere infrastruktur i nettverket.”

Dette eksemplet har noen helt klare utfordringer.

- Hvor ligger krypteringsnøkkelen?
- Hvor dekrypteres informasjonen og hva er sikkerhetsnivået?
- Er datakommunikasjonen sikret?
- Hva med e-post og internett, er det avgjørende for risikobildet?
- Virus og skadevare, er det et større problem utenfor sikret sone?
- Mister man reell kontroll over hvordan saksbehandler håndterer opplysningene?
- Er manuelle rutiner godt nok?

En vurdering av svarene på disse spørsmålene gir grunnlag for en mer detaljert konsekvensanalyse. En slik analyse må også omfatte tilgangsstyring og logging.

Generelt

Tilgang til tjenester og informasjon i et nettverk skal kun gis etter tjenstlig behov. I utgangspunktet skal alle tjenester være sperret. En mulig sikkerhetsarkitektur vil i prinsippet omfatte enkle løsninger med et fysisk skille mellom risikoutsatte tjenester og sensitive personopplysninger. Der det er behov for en mer integrert nettverksløsning for bruk av ulike opplysninger vil løsningene bli stadig mer omfattende.

Hvorvidt virksomheten har mulighet til å iverksette en tilstrekkelig sikkerhetsløsning vil bestemme graden av integrasjon og funksjonalitet i informasjonssystemet. Dette vil i hovedsak være avhengig av hvilke fysiske og logiske sikkerhetsmekanismer som til enhver tid eksisterer.

Dagens teknologiske utvikling har hatt sterkt fokus på logisk sikkerhet, særlig med hensyn til tilgangsstyring og logging. Logisk sikkerhet bygger i hovedsak på konfigurasjonsinnstillinger i programvaren som benyttes i løsningen. Det vil parallelt

med dette også være fysisk datakommunikasjon mellom enheter og tjenere i et nettverk for eksempel mellom soner, brannmurer, terminalservere og rutere. Om den fysiske datakommunikasjonen ikke klarer å gjenspeile den logiske sikringen man ønsker å etablere, vil løsningen som helhet sannsynligvis ha risikomomenter som innbærer utilstrekkelig sikring av personopplysninger.

Logisk sikring i seg selv er ikke godt nok for å sikre personopplysninger fordi den fysiske datakommunikasjonen kan ha svakheter som åpner for at den logiske sikringen omgås. Om den fysiske datakommunikasjonen ikke er avklart i forkant av systemdesignet, vil den sannsynligvis skape problemer for funksjonalitet hvis den må korrigeres i etterkant. Det er derfor bedre å bygge opp sikkerhetsmodellen fra bunnen av. Først når virksomheten har kontroll på kommunikasjonsflyten, kan denne overbygges med logisk sikring.

Et ytterligere informasjonssikkerhetstiltak som har gjort seg gjeldende i senere tid, er kryptering av databaser/filområder for å simulere sikre soner i form av beskyttede siloer som autoriserte med nøkkel kan åpne. Disse "sikre sonene" har færre fysiske tiltak for å oppnå ønsket sikkerhet. Utfordringen med denne typen siloer er at den krypterte informasjonen kan bli eksponert når siloen blir åpnet og tilgjengeliggjort. Det må derfor vurderes hva som kan skje med informasjonen hvis den eksponeres, og om kontrollnivået og nivå for akseptabel risiko er tilfredsstillende.

Bruk av kortsystemer for printerløsninger tas i bruk i et stadig større omfang. Et slikt system innebærer at utskrifter ikke blir skrevet ut før bruker har autentisert seg med kort og/eller PIN-kode på skriveren. Det er en økende tendens til at slike printerløsninger blir felles for personopplysninger og sensitive personopplysninger. Slike løsninger kan ha sikkerhetsmangler som øker risikobildet. Å bruke en felles printer omgår sikkerhetsmekanismer som er etablert mellom to adskilte soner fordi printere har egne harddisker, ftp, webserver, faks etc. Kommunikasjon kan derfor flyte fra en sone til en annen, som igjen kan utgjøre en uønsket risiko for at personopplysninger gjøres tilgjengelig mellom sonene. En felles printer blir derfor et sikkerhetshull i nettverket.

Hvorvidt virksomheten har mulighet til å iverksette tilstrekkelige sikkerhetsløsninger, vil bestemme graden av integrasjon og funksjonalitet i informasjonssystemet.

Kort oppsummert mener Datatilsynet at logisk sikkerhet alene ikke er godt nok for å sikre personopplysninger. Det er svært viktig at virksomheten samtidig ser på datakommunikasjonen som sikrer gjennomføringen av den logiske sikkerheten. Er det svakheter i noen av disse delene bør virksomheten revurdere den valgte løsningen eller tilpasse den slik at det tas hensyn både til logisk sikring og til datakommunikasjonen som sikrer gjennomføringen av den logiske sikringen.

Om det eksisterer konkrete trusler i den valgte løsningen bør disse kompenseres med riktige tiltak slik at risikoen blir akseptabel. Tiltakene bør baseres på en kombinasjon av sikkerhet i datakommunikasjon og logiske tiltak. Eksempler på en slik tilnærming presenteres i neste avsnitt om sikkerhetsarkitektur og i veilederens temaark.

Systemteknisk sikkerhet – Soner

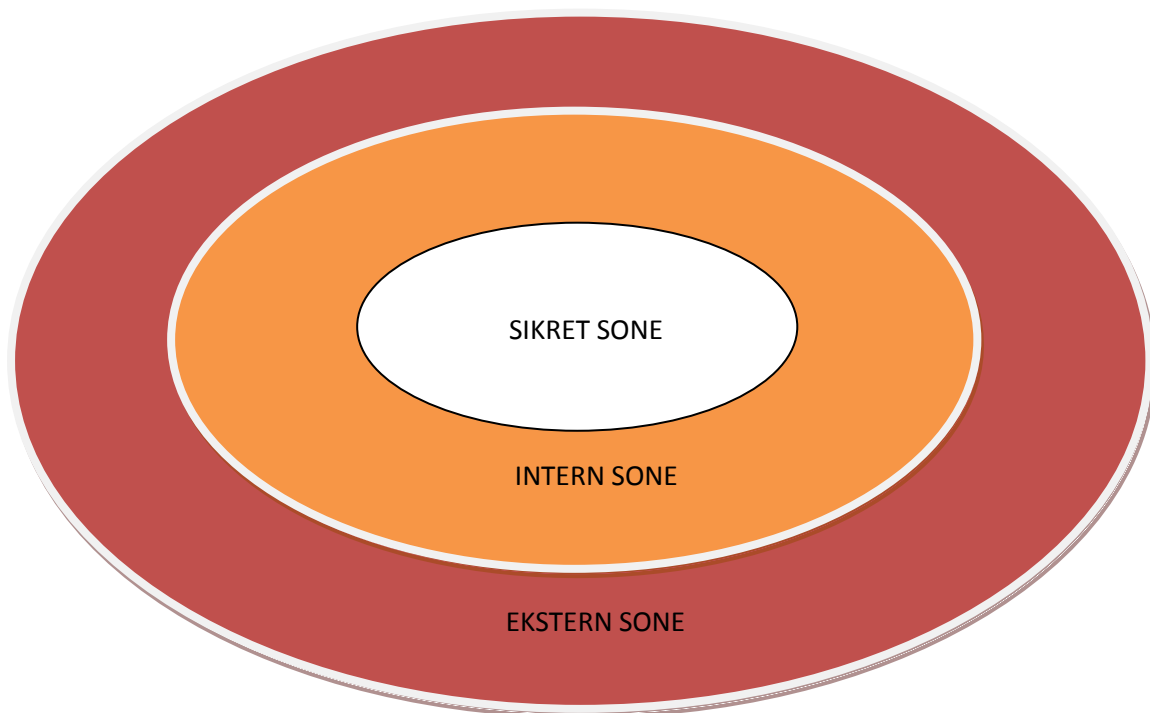
Sikkerhetsarkitektur. Inndeling i soner

Datatilsynet mener at sikkerhetsarkitekturen skal deles inn i adskilte soner. En sone er et adskilt segment eller del av et informasjonssystem med tilhørende enheter, som kun kan kommunisere seg imellom. Soner opprettes etter at virksomheten har kartlagt hvilke behandlinger virksomheten gjør, gjennomført en risikovurdering av behandlingen, og avklart hvilke personopplysninger virksomheten behandler. I hovedsak skal virksomhetens interne sikkerhetsarkitektur deles opp i følgende soner (ref. figur 1):

- 1. Sikret sone.** Sone der sensitive personopplysninger behandles (ved behov skal det opprettes flere sikrede soner i virksomheten). Den enkelte sikrede sone skal være sikkerhetsmessig atskilt både fra resten av det interne nettverket og fra eventuelle andre sikrede soner.
- 2. Intern sone.** Sone der hvor ikke-sensitive personopplysninger behandles. Denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt (ved behov skal det opprettes flere interne soner i virksomheten).
- 3. Ekstern sone.** Sone der åpen informasjon og tilgjengelig informasjon (typisk Internettbaserte tjenester) befinner seg. Denne sonen er plassert utenfor virksomhetens ytre brannmur, og inkluderer eksterne kommunikasjonskanaler som for eksempel e-post. Sonen benyttes også for ekstern pålogging mot tjenester virksomheten tilbyr sine ansatte eller sine kunder. Tjenestene ligger normalt i en DMZ sone på ekstern brannmur. Dette er for at virksomheten skal kunne styre kommunikasjonen og ivareta sikkerheten for servere internt i virksomheten.

Datatilsynet forutsetter at sonene er adskilt med minimum to uavhengige tekniske barrierer, en mellom hver sone.

Virksomhetens interne informasjonssystemer vil med stor sannsynlighet også kommunisere med de eksterne sonene virksomheten benytter, men ikke kontrollerer. Figur 1 viser derfor både en sikret, en intern og en ekstern sone.



FIGUR 1: Sikkerhetsarkitektur. Inndeling i soner

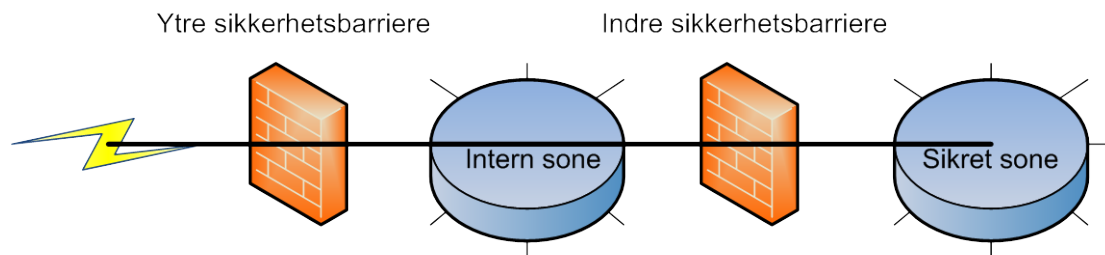
Virksomhetens sikkerhetsarkitektur skal ivareta følgende:

- Sensitive personopplysninger skal behandles og lagres i sikrede soner som kun autoriserte brukere har tilgang til. En virksomhet kan opprette flere sikrede soner avhengig av behov.
- Skillet mellom sikret sone og intern sone skal være slik at det ikke er mulig for brukere å overstyre oppsatte begrensninger. Som et minimum må det være én teknisk sikkerhetsbarriere mellom sikret sone og intern sone.
- Skillet mellom eksterne nettverk og sikret sone skal ivaretas av to uavhengige tekniske sikkerhetsbarrierer.
- Ingen tjenester skal kunne initieres fra andre soner og inn i sikret sone. Kun autoriserte tjenester skal kunne initieres utenfra med særskilte tekniske sikkerhetstiltak.
- Ingen nettverkskomponenter, utstyr, databaser eller lignede skal kunne omgå oppsatte sikkerhetsbarrierer, for eksempel at utstyr brukes som fellesløsning for både sikret og intern sone.

- Den fysiske kommunikasjonsflyten skal ikke kunne kompromittere implementerte sikkerhetsmekanismer, for eksempel ved at det kun benyttes logisk sikkerhet uten at den fysiske kommunikasjonen støtter oppunder sikkerhetsmekanismene
- Data skal krypteres ved ekstern formidling av sensitive personopplysninger. Dette gjelder også informasjon om hvordan slike opplysninger skal sikres. Krypteringen skal skje i sikret sone og den skal skje "ende til ende".
- Krypteringsnøkler for systemer (for eksempel VPN) skal håndteres like sikkert som opplysningene krypteringen beskytter. Tilgangen til krypteringsnøklerne skal reguleres av tjenstlig behov.
- Ved ekstern tilkobling til informasjonssystemet for å behandle sensitive personopplysninger, må sikkerheten som er etablert i sikret sone ivaretas i alle ledd der opplysningene behandles. Dette gjelder særlig for mobile enheter som smarttelefoner, bærbare pc og annet mobilt utstyr.
- Den indre brannmuren skal både forhindre ekstern inntrenging til sikret sone, og sikre kommunikasjon ut fra sonen. Kun autoriserte tjenester skal kunne kommunisere ut fra sikret sone. Autoriserte tjenester er systemer som virksomheten har risikovurdert, konfigurert og godkjent for ekstern kommunikasjon.

Systemteknisk sikkerhet – Prinsipper for nettverksoppsett

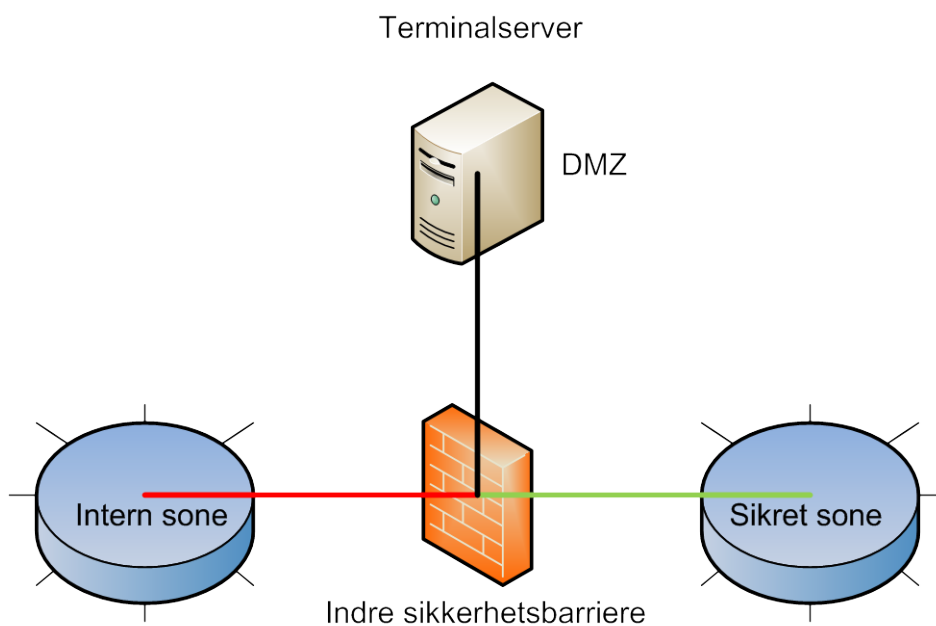
Bruk av ny teknologi, spesielle oppsett av sonene og bruk av andre typer sikkerhetsbarrierer/mekanismer tas opp i veilederens temaark.



FIGUR 2: Overordnet prinsipp for bruk av soner og sikkerhetsbarrierer.

I figur 2 skisseres et overordnet prinsipp for bruk av soner og sikkerhetsbarrierer. De fleste virksomheter behandler personopplysninger og sensitive personopplysninger i tillegg til å være tilknyttet et eksternt nettverk, normalt Internett. Systemteknisk sikkerhet skal ivaretas ved følgende sikkerhetstiltak:

- Ha en ytre sikkerhetsbarriere i form av en sikkerhetsløsning mellom eksternt nettverk og intern sone.
- Ha en indre sikkerhetsbarriere, i form av en sikkerhetsløsning mellom internt nettverk og sikret sone.



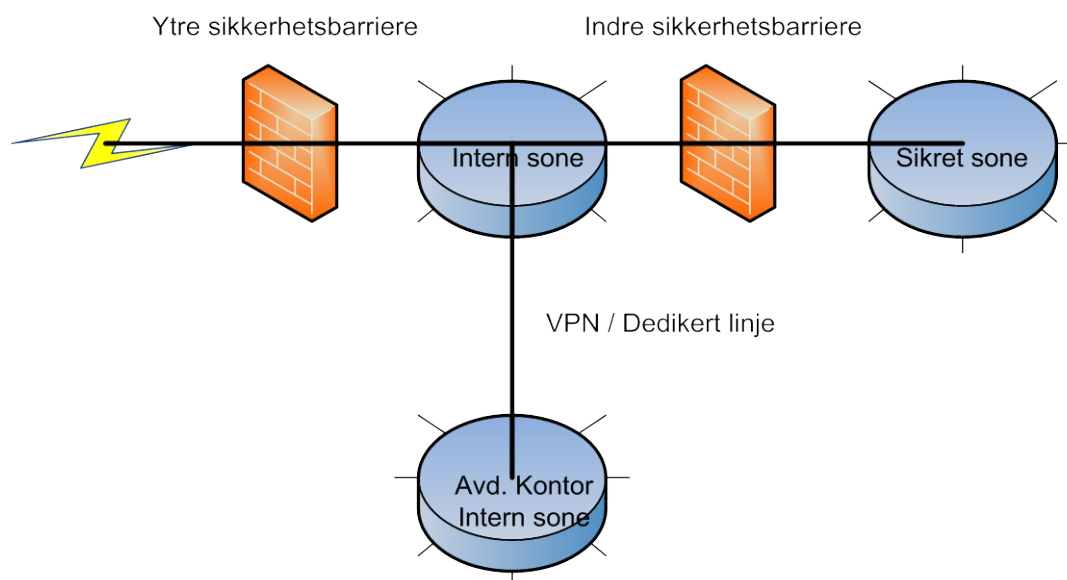
FIGUR 3: Oppsett av terminalserver i DMZ mot sikret sone

Tilgang til sikret sone som vist i figur 3, styres av sikkerhetsmekanismer tilknyttet den indre sikkerhetsbarrieren i en DMZ. Dette kan for eksempel være en terminalserver som er tilstrekkelig sikret mot informasjonsflyt mellom sonene som for eksempel klipp og lim av tekst, utskrifter, filoverføringer eller oppsett av nettverkspor og nettverksstasjoner.

Når minimumstiltakene som vist i figur 3 er ivaretatt, er det ikke behov for unike datamaskiner for hvert nett. Brukerne kan være i intern sone og jobbe inn mot sikret sone.

Hvordan brukere plasseres i en slik skisse er opp til virksomheten, men sikkerheten rundt opplysningene i sikret sone skal ikke nedgraderes slik at risikonivået virksomhetens ledelse har satt, senkes. Dette gjelder alle for ledd der opplysningene behandles, lagres eller på annen måte beveger seg gjennom.

For virksomheter med eksternt adskilte lokaler, kan et overordnet prinsipp, som vist figur 4 benyttes.

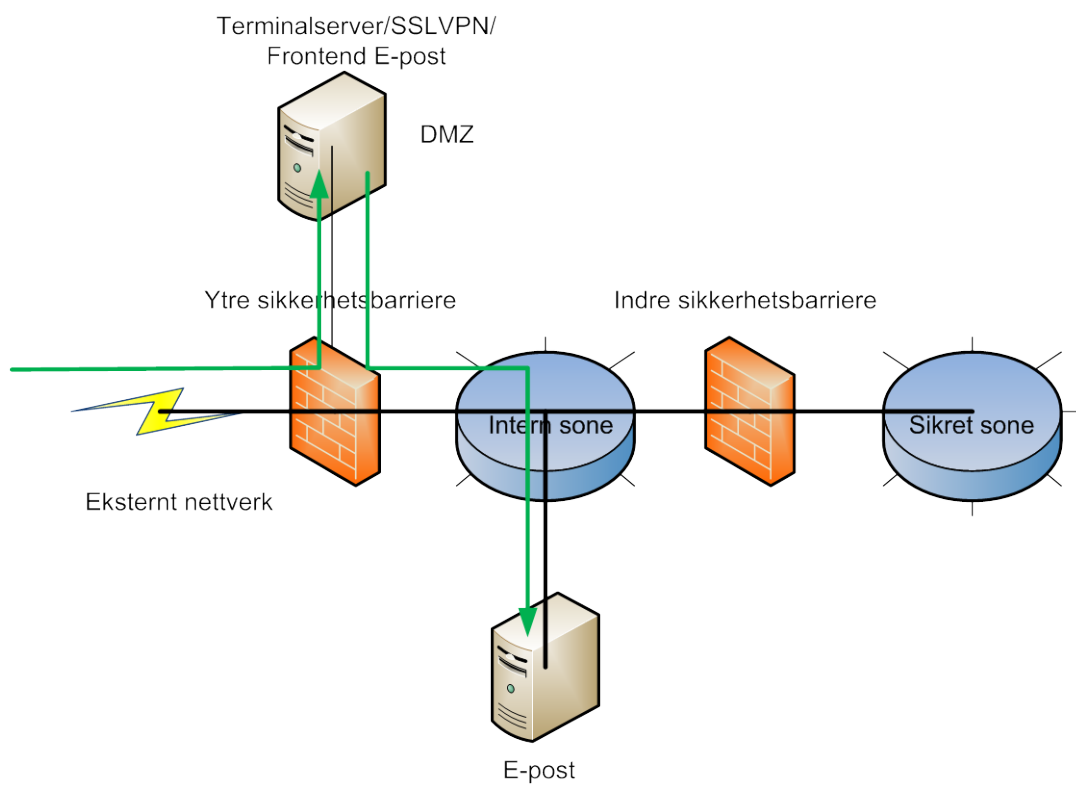


FIGUR 4: Overordnet prinsipp for soneinndeling og sikkerhetsbarrierer for virksomheter med eksternt adskilte lokaler.

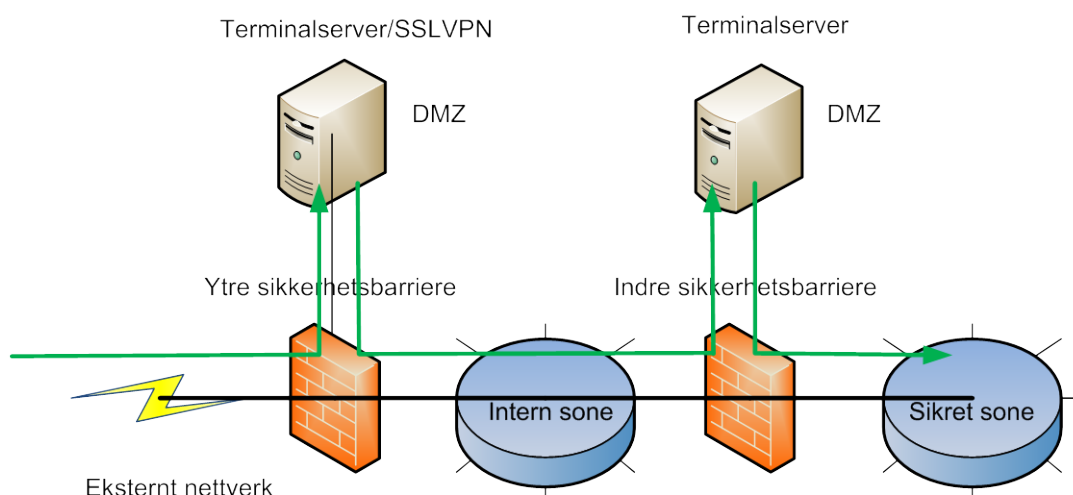
I eksternt adskilte lokaler, der medarbeidere har tilgang til intern sone og også kan eller skal ha tilgang til sikret sone ved autorisasjon, kan følgende løsning benyttes:

- Den interne sonen kobles til virksomhetens sentralsystem via en kryptert forbindelse. Dette kan enten gjøre med ytre sikkerhetsbarrierer eller med annet teknisk utstyr som sikrer tilstrekkelig kryptering av datakommunikasjonen mellom sonene.
- Ved tilgang til sikret sone benyttes prinsippene vist i figur 3.

Kryptering av forbindelsen mellom intern sone og virksomhetens sentralsystem er en forutsetning for tilgang. Dette er fordi informasjonen fra sikret sone i form av skjermbilder, overføres til brukerne på avdelingskontoret via intern sone. Veilederens temaark tar opp problemstillinger rundt blant annet utskrift og filoverføring.



FIGUR 5: Eksempel på nettverksoppsett ved ekstern tilgang til informasjonssystem ved hjelp av terminalserver/SSLVPN i DMZ på ytre sikkerhetsbarriere.



FIGUR 6: Eksempel på nettverksoppsett ved ekstern tilgang til informasjonssystem ved hjelp av terminalserver/SSLVPN i DMZ på ytre sikkerhetsbarriere og bruk av terminalserver mot sikre sone.

Systemteknisk sikkerhet – Sikkerhetsbarrierer

Datatilsynet forutsetter at tilgang fra intern til sikret sone går igjennom minst en sikkerhetsbarriere med tilhørende tekniske tiltak. Dette er både for å sikre integriteten til sikret sone og for å sikre opplysningene som er lagret der. I tillegg forutsetter tilsynet at en intern sone har minimum en sikkerhetsbarriere ut mot eksterne nettverk.

Et eksempel på en slik sikkerhetsbarriere kan være en løsning med et fysisk skille mellom sikret sone og intern sone. En slik løsning krever ingen ytterligere systemtekniske tiltak for å skille mellom sonene.

Dersom løsningen ikke har et fysisk skille mellom sonene, må det iverksettes tekniske tiltak for å skille disse. Bruk av virtuelle brannmurer for ytre og indre sikkerhetsbarriere er etter Datatilsynets oppfatning ikke like tilfredsstillende som to tekniske separate sikkerhetstiltak. Dette er fordi brannmurene deler fysisk plattform. Hvis den fysiske plattformen kompromitteres eller på annen måte opphever de implementerte sikkerhetsmekanismene, vil det innebære en for stor risiko.

Indre sikkerhetsbarriere

En indre sikkerhetsbarriere er plassert mellom intern og sikret sone. Denne lukker i utgangspunktet all trafikk mellom sonene. Etter en vurdering av risiko og tekniske samt logiske tiltak kan sikkerhetsbarrieren likevel åpnes for kommunikasjon. Et

typisk teknisk tiltak for indre sikkerhetsbarriere er å bruke terminalserver i DMZ for tilgang til sikret sone.

Ytre sikkerhetsbarriere

En ytre sikkerhetsbarriere er plassert mellom intern sone og eksternt nettverk, hvor sistnevnte normalt er utenfor virksomhetens fysiske kontroll, for eksempel Internett. Virksomheter åpner som regel for trafikk inn og ut for eksempel for e-post og bruk av Internett. For denne typen sikkerhetsbarriere er det ikke nødvendig å benytte DMZ-soner for virksomhetens utgående trafikk, men det kan være nyttig for å redusere direkte risiko mot interne systemer ved å benytte utstyr i DMZ for trafikk utenfra og inn til virksomheten.

DMZ

DMZ(demilitarisert sone) er et nettverkssegment som benyttes til å isolere tjenester og styre trafikk mellom sikkerhetssoner ved hjelp av teknisk utstyr. DMZ kan blant annet inneholde terminalserver eller SSLVPN til annet teknisk utstyr som vil oppnå tilfredsstillende sikkerhet i kommunikasjonen, og dermed også adgangskontroll mellom to adskilte soner.

Bruk av databehandler

Det er ikke forskjell på behov for soneinndeling og sikkerhetstiltak for virksomheter som bruker databehandler for betjening av informasjonssystemet og som de betjener eget informasjonssystem. Virksomhetens forhold til en databehandler skal reguleres i en databehandleravtale ([www.datatilsynet.no\databehandler](http://www.datatilsynet.no/databehandler)).

Virksomheter som inngår en databehandleravtale må se denne i sammenheng med virksomhetens internkontroll og behandlingsansvar. Sistnevnte har særlig betydning for segmentering av informasjonssystemene og sammenblanding av informasjon som tilhører andre behandlingsansvarlige. I utgangspunkt skal hver enkelt behandlingsansvarlig ha et separat informasjonssystem, selv om det dreier seg om virtuelle systemer. I slike virtuelle systemer må informasjonen skilles slik at sikkerheten tilsvarer sikkerheten ved to fysisk separate informasjonssystemer. En slik adskilling av informasjonssystemene er også viktig ved sikkerhetskopiering.

Definisjoner fra personopplysningsloven

Personopplysningsloven gir følgende førende definisjoner:

- 1. Personopplysning:** Opplysninger og vurderinger som kan knyttes til en enkeltperson. For eksempel navn, fødselsnummer, e-post og aidentifiserte opplysninger (se dette begrepet forklart i uttrykk og begreper brukt).
- 2. Behandling av personopplysninger:** Enhver bruk av personopplysninger, som foreksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder.
- 3. Personregister:** Register, fortegnelser med videre der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.
- 4. Behandlingsansvarlig:** Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes i behandlingen.
- 5. Databehandler:** Den som behandler personopplysninger på vegne av den behandlingsansvarlige. En databehandler er en ekstern person eller virksomhet som befinner seg utenfor den behandlingsansvarliges virksomhet.
- 6. Registrert:** Den enkeltperson en personopplysning kan knyttes til.
- 7. Samtykke:** En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.

- 8. Sensitive personopplysninger:** Opplysninger om:
- a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
 - b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
 - c) helseforhold
 - d) seksuelle forhold
 - e) medlemskap i fagforeninger
- 9. Fødselsnummer (11 siffer):** Fødselsnummer er en unik identifikator som har en særlig bestemmelse om nødvendig bruk i personopplysningsloven § 12. Det skal kun brukes der det er saklig behov for sikker identifisering og metoden er nødvendig for slik identifisering. I tillegg er det en særbestemmelse om kryptering ved elektronisk kommunikasjon i personopplysningsforskriften § 10-2.
- 10. Akseptkriterier:**
- Fastlegging av kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. Personopplysningsforskriften § 2-4 første ledd og § 2-2.
- 11. Avvik:** Med avvik menes enhver håndtering av *personopplysninger* som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd. Avvik meldes Datatilsynet i henhold til personopplysningsforskriften § 2-6.
- 12. Konfidensialitet:** Konfidensialitet betyr at personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.

- 13. Integritet:** Med integritet menes at personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.
- 14. Tilgjengelighet:** Tilgjengelighet betyr at personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.
- 15. Internkontroll:** Med internkontroll menes planlagte, systematiske og dokumenterte tiltak som skal sikre at personopplysninger blir behandlet i samsvar med personopplysningsloven med forskrift.

Ordliste

- 1. Aidentifiserte personopplysninger:** Opplysninger er aidentifiserte dersom navn, personnummer eller andre personentydige kjennetegn er erstattet med et nummer, en kode, fiktive navn eller lignende, som viser til en atskilt liste med de direkte personopplysningene.
- 2. Datakommunikasjon:** Elektronisk flyt av data i et informasjonssystem.
- 3. Ekstern datakommunikasjon:** Datakommunikasjon der kommunikasjonskanalen er utenfor virksomhetens kontroll betegnes som ekstern datakommunikasjon.
- 4. DMZ (Demilitarisert sone):** En sone datakommunikasjon kan rutes igjennom for å hindre eksponering av beskyttede nettverkssoner mot eksterne og interne parter. Benyttes også til å plassere terminalservere i.
- 5. Eksternt nettverk:** Datanettverk utenfor virksomhetens egen kontroll.
- 6. Internt nettverk:** Datanettverk innenfor virksomhetens egen kontroll.
- 7. Sone:** Oppdeling av internt nettverk i adskilte soner for opplysninger med forskjellig sikkerhetsbehov. Opplysningene er i ulike systemer og har ulik tilgangstyring. Oppdelingen i soner vil øke kontrollen på datakommunikasjonen. Oppdeling skjer etter en risikovurdering og analyse av behov.

- 8. Intern sone:** En nettverksone som normalt håndterer personopplysninger med lavere krav til informasjonssikkerhet enn sensitive personopplysninger.
- 9. Sikret sone:** En nettverksone som normalt håndterer sensitive personopplysninger med høyere krav til informasjonssikkerhet.
- 10. Teknisk sikkerhetsbarriere (eks. Ruter, Brannmur, SSL VPN):** Fysisk utstyr og programvare benyttet for tilgangs- og kommunikasjonskontroll mellom virksomhetens informasjonssystem og eksterne nettverk, eller mellom forskjellige soner internt i virksomhetens informasjonssystem.
- 11. Virksomhet:** Benyttes både om offentlig og private virksomheter.
- 12. Virtuell server:** En fysisk server som har en grunnplattform i form av programvare. Disse tillater samtidig kjøring av ulike logiske adskilte serversystemer som deler på fysiske ressurser.
- 13. Virtuell brannmur:** En fysisk komponent som har en grunnplattform i form av programvare. Disse tillater samtidig kjøring av ulike logiske adskilte brannmurer som deler på fysiske ressurser.

- 14. Virtuell database:** En fysisk server som har en grunnplattform i form av programvare. Disse tillater samtidig kjøring av ulike logisk adskilte databaseinstanser som deler på fysiske ressurser.
- 15. Terminalserver:** En fysisk server/komponent med tilhørende programvare som oppretter virtuelle skrivebord for tilgang til interne og eksterne ressurser. Kan også benyttes for å begrense brukermulighetene i form av konfigurasjonsendringer.
- 16. Filsluse:** Begrep som benyttes om teknisk løsning for overføring av filer mellom to separate soner.
- 17. SAN (Storage area network):** Tilkobling av eksterne lagringsmedium til servere som fungerer som om de er lokale. Benyttes i stor grad opp mot virtuelle servere.
- 18. NAS (Network attached storage):** Se SAN. Forskjellen ligger i måten de er tilkoblet servere og nettverket på.
- 19. Sikkerhetskopiering:** Begrep som benyttes om en teknisk og/eller programvarebasert løsning for å ta kopi av elektronisk lagret informasjon i et informasjonssystem.
- 20. Kvalifisert sertifikat og signatur:** Autentisering og signering som gir en juridisk rettsvirkning i samsvar med lov om digital signatur.
- 21. Ødeleggende programvare:** Begrep som benyttes om virus, trojanere, ormer, skadevare og annen programvare laget for å skade eller få

tilgang til et informasjonssystem.

22. Konfigurasjon:

Med konfigurasjon menes informasjonssystemets utforming. Dette inkluderer alt fra teknisk utstyr, sikkerhetstiltak til programvare.