Nasjonal kommunikasjons-myndighet

Tilsynsrapport, IKT-sikkerhet i datasenter

Kartleggingstilsyn datasenter 2025

Rapport

9. februar 2026

Sammendrag

Nasjonal kommunikasjonsmyndighet (Nkom) gjennomførte et kartleggingstilsyn høsten 2025 med 17 datasenteroperatører, basert på deres egenvurdering av sikkerhet. De utvalgte representerer bredden av bransjen slik den eksisterer i Norge i dag, og ble valgt ut på bakgrunn av forskjellige kategorier som type datasenter; hyperscale (store, dedikerte datasenter), colocation (samlokaliseringsdatasenter) og edge (mindre installasjoner), geografisk beliggenhet med mer.

Formålet med tilsynet var å introdusere Nkom som sektormyndighet overfor datasenteroperatører som nå er underlagt ekomloven fra og med 1. januar 2025, og sjekke modenheten i bransjen med fokus på IKT-sikkerhet. Nkom vil blant annet legge funnene fra denne kartleggingen til grunn for fremtidige tilsyn.

NSM har utviklet verktøyet cybersjekk som alle virksomheter kan bruke for egenkontroll av egen IKT-sikkerhet. Nkom så det som formålstjenlig å ta i bruk dette verktøyet for tilsynet. Tilsynsobjektene fikk gjennom NSMs Cybersjekk raskt oversikt over status i sitt arbeid med digital sikkerhet, og de fikk direkte veiledning og tilbakemelding på anbefalte prioriterte sikkerhetstiltak for å forbedre sikkerhetsarbeidet. Rapportene fra de enkelte datasenteroperatørenes cybersjekk har vært gjenstand for Nkom i tilsynsvurderingen.

Resultatet fra tilsynet viste at det er en spredning i arbeidet med digital sikkerhet for datasenteroperatørene som var underlagt kartleggingen. Dette er delvis forventet da det er variasjon i deres risikobilde, størrelse, brukere og tjenesteleveranse. Sikkerhetsarbeidet må tilpasses det samlede risiko- og sårbarhetsbildet den enkelte virksomhet står overfor. De bør gjennomgå rapporten de har fått fra NSMs Cybersjekk, og se denne i sammenheng med egne verdivurderinger og risiko- og sårbarhetsanalyser.

Generelt vurderer datasenteroperatørene at de scorer godt innen kategoriene sikkerhetskultur, overordnet verdikartlegging og kartlegging av IKT. Derimot peker kategoriene «servere og klienter», og «verifisering og sikkerhetsovervåkning» seg ut med størst forbedringspotensial for flest datasenteroperatører. Dette er områder hvor flere av dem bør iverksette tiltak for å heve sikkerheten.

Nkom vil anbefale at alle datasenteroperatører, også de som ikke var underlagt tilsynet, å gjennomføre NSMs cybersjekk. Nkom forutsetter at den enkelte datasenteroperatør gjennomgår sin rapport og gjør disse vurderingene knyttet til egen virksomhet.

Nkom forventer at det iverksettes tiltak der det er nødvendig for å levere forsvarlig sikkerhet innen IKT-sikkerhet. Nkom vil følge opp resultatet fra dette tilsynet i fremtidige tilsyn.

Innhold

1 Innledning 4

1.1 Hjemmel for tilsyn 4

1.2 Bakgrunn for tilsynet 4

1.3 Mål for tilsynet 5

1.4 Kriterier for tilsynet 5

1.5 Omfang av tilsynet 5

1.6 Gjennomføring av tilsynet 6

1.7 Tilsynsmetodikk 6

2 Gjennomgang av resultater fra NSMs Cybersjekk 6

2.1 Styringssystem for sikkerhet 8

2.2 Ledelse 9

2.3 Risikostyring 10

2.4 Sikkerhetskultur 12

2.5 Overordnet verdikartlegging 13

2.6 IKT kartlegging 14

2.7 IKT arkitektur 15

2.8 Servere og klienter 17

2.9 Tilgang, rettigheter og brukere 18

2.10 Verifisering og sikkerhetsovervåkning 19

2.11 Leverandørforhold 20

2.12 Hendelsesberedskap 21

3 Virksomhetens dokumentasjon 23

1 Innledning

Datasenterbransjen ble underlagt ny ekomlov 1. januar 2025. I tråd med Nkoms mandat som sektormyndighet for sikkerhet i ekomsektoren, førte Nkom tilsyn med en rekke datasenteroperatører høsten 2025.

Det var et ledd i å introdusere bransjen for Nkom som sektor- og tilsynsmyndighet og gi Nkom en oversikt over datasenterbransjen. Tilsynet var og ment til å danne et grunnlag for videre oppfølging av sektoren i form av f. eks. veiledning og tilsyn.

Nkom har i denne prosessen gjennomført et dokumenttilsyn hvor det ble valgt ut 17 ulike datasenteroperatører for å få et representativt utvalg. Faktorer lagt til grunn for utvelgelsen av virksomheter var størrelse, geografisk beliggenhet, kommersielle og virksomhetsinterne datasentre m.m.

Ekomloven skal bidra til å sikre brukerne i hele landet gode, rimelige og fremtidsrettede datasentertjenester med forsvarlig sikkerhet, legge til rette for bærekraftig konkurranse og effektiv bruk av samfunnets ressurser og stimulere til næringsutvikling og innovasjon, jf. lov 13. ekomloven formålsparagraf § 1-1.

Det legges til grunn at resultatene som er blitt identifisert hensyntas av den enkelte virksomhet. Datasenteroperatørene er selv ansvarlig for forsvarlig sikkerhet i sine datasentre.

1.1 Hjemmel for tilsyn

Nkom som sektormyndighet for sikkerhet i ekomsektoren skal føre tilsyn med at krav fastsatt i eller i medhold av loven er oppfylt, jf. ekomloven §15-1, jamfør datasenterforskriften § 3-1.

Nasjonal kommunikasjonsmyndighet fører tilsyn med at kravene i forskriften blir oppfylt, og kan blant annet innhente opplysninger og gjennomføre sanksjoner etter ekomloven kapittel 15.

1.2 Bakgrunn for tilsynet

Datasenter er en sentral del av den digitale grunnmuren i Norge. Regjeringen legger til grunn at datasentre er kritisk digital infrastruktur. Ny datasenterstrategi ble lansert i juni 2025, og bygger på den nasjonale digitaliseringsstrategien 2024 – 2030 Fremtidens digitale Norge. Ett av de overordnede målene i datasenterstrategien er at «*Datasenter skal ha forsvarleg tryggleik i fred, krise og krig. Noreg har robuste datasenter som sikrar både nasjonal og regional autonomi av datasentertenester. Dei mest kritiske digitale tenestene skal bli leverte frå datasenter i Noreg eller frå datasenter hos allierte.»*.[1]

[1] Datasenternæringa - ei berekraftig framtidsnæring for det digitale Noreg

I Nkom ROS 2025 vurderer Nkom risiko- og trusselbildet i sektoren, med særlig fokus på det digitale trusselbildet, og en økt usikkerhet grunnet de sikkerhetspolitiske endringene. Kritisk infrastruktur i Norge står fremdeles overfor vedvarende høy risiko, og samfunnets evne til å fungere er i stor grad avhengig av både fysisk og digital infrastruktur. Svikt i denne infrastrukturen og systemene vil medføre alvorlige konsekvenser for leveransen av kritiske varer og tjenester som innbyggere og myndigheter er avhengige av.

1.3 Mål for tilsynet

Tilsynet ble gjennomført for å vurdere bransjens egen forståelse av, og modenhet til, IKT-sikkerhet i dagens risiko og trusselbilde og kunne danne grunnlag for fremtidige risikobaserte tilsyn av bransjen.

Målet begrenser seg til et oversiktsbilde og inkluderer ikke individuell oppfølging av datasentrene eller kontroll på bakgrunn av tilsynet. Datasenteroperatørene har selv mottatt tilbakemelding på egen sikkerhetstilstand gjennom rapporten fra NSM cybersjekk, og bør benytte denne som et bidrag til virksomhetens arbeid med forsvarlig sikkerhet.

1.4 Kriterier for tilsynet

Kriterier som er lagt til grunn for tilsynet finnes i:

- Lov 13. desember 2024 nr. 76 om elektronisk kommunikasjon (ekomloven)
- Forskrift 18. desember 2024 nr. 3313 forskrift om datasenter (datasenterforskriften)

1.5 Omfang av tilsynet

Tilsynet har omfattet undersøkelser hos 17 datasenteroperatører som representerer bredden av bransjen slik den eksisterer i Norge i dag. Datasenteroperatørene er valgt ut på bakgrunn av forskjellige kategorier som type datasenter; hyperscale (store, dedikerte datasenter), colocation (samlokaliseringsdatasenter) og edge (mindre installasjoner), geografisk beliggenhet med mer.

Nkom har sett behov for å få en bredere oversikt over bransjens oppfølging av krav til digital sikkerhet.

Fokusområde har vært å vurdere datasenteroperatørenes arbeid med styringssystem for IKT-sikkerhet med følgende temaer:

- Ledelse
- Risikostyring
- Sikkerhetskultur
- Overordnet kartlegging
- Karlegging av kritikalitet
- IKT-arkitektur
- Servere og klienter
- Tilgang, rettigheter og brukere
- Verifisering av sikkerhetsovervåkning
- Leverandørforhold
- Hendelsesberedskap

1.6 Gjennomføring av tilsynet

Tilsynsobjekt:	Utvalgte datasenteroperatører
Varsel om tilsyn med pålegg om utlevering dokumentasjon:	25. september 2025
Pålegg om utlevering:	10. oktober 2025
Dokumentgjennomgang:	oktober - desember 2025
Rapport:	februar 2026

1.7 Tilsynsmetodikk

Tilsynet er gjennomført som dokumenttilsyn, med utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet og ved bruk av NSM sin tjeneste Cybersjekk. Det er således de individuelle datasenteroperatørene som har rapportert på egen sikkerhetstilstand.

Tilsynsrapporten fokuserer på, og beskriver, det aggregerte (modenhets) nivået basert på datasenteroperatørenes samlede besvarelser. Dette gir et bilde på egenvurdering av IKT-sikkerhetstilstanden for bransjen.

Rapporten viser hvordan bransjen vurderer egen IKT-sikkerhet. Dette vil danne grunnlag for kontinuerlig forbedring for de involverte aktørene, så vel som øvrige datasenteroperatører som ikke var omfattet av tilsynet. Det vil også gi aktørene en mulighet til å danne seg et bilde av hvordan deres arbeid står i forhold til andre aktører i bransjen.

Ved å benytte NSM sin Cybersjekk i dette tilsynet, ønsker Nkom å fremme NSM sin nye tjeneste. Vi håper dette motiverer flere datasenteroperatører til å benytte NSMs Cybersjekk for selv å få en oppdatert og god status over tilstanden på egen sikkerhet.

Det er datasenteroperatøren selv som er nærmest til å avdekke slike underliggende årsaker, og som må ta eierskap til disse prosessene. Datasenteroperatørene er selv ansvarlig for å ha forsvarlig sikkerhet i deres datasentre etter krav i lov og forskrift.

2 Gjennomgang av resultater fra NSMs Cybersjekk

Kapittel to i rapporten beskriver en sammenstilling av resultatene fra tilsynet. Rapporten tar for seg forhold knyttet til datasenteroperatøren sin håndtering av IKT-sikkerhet. Rapporten er videre delt inn i temaene: ledelse, risikostyring, sikkerhetskultur, overordnet kartlegging, kartlegging av IKT, IKT-arkitektur, servere og klienter, tilgang, rettigheter og brukere, verifisering og sikkerhetsovervåkning, leverandørforhold og hendelsesberedskap. Datasenteroperatørene har gjennom NSMs Cybersjekk oppnådd en poengscore, både totalt og enkeltvist pr tema, mellom null og ti med forslag til forbedringstiltak for hvert av temaene.

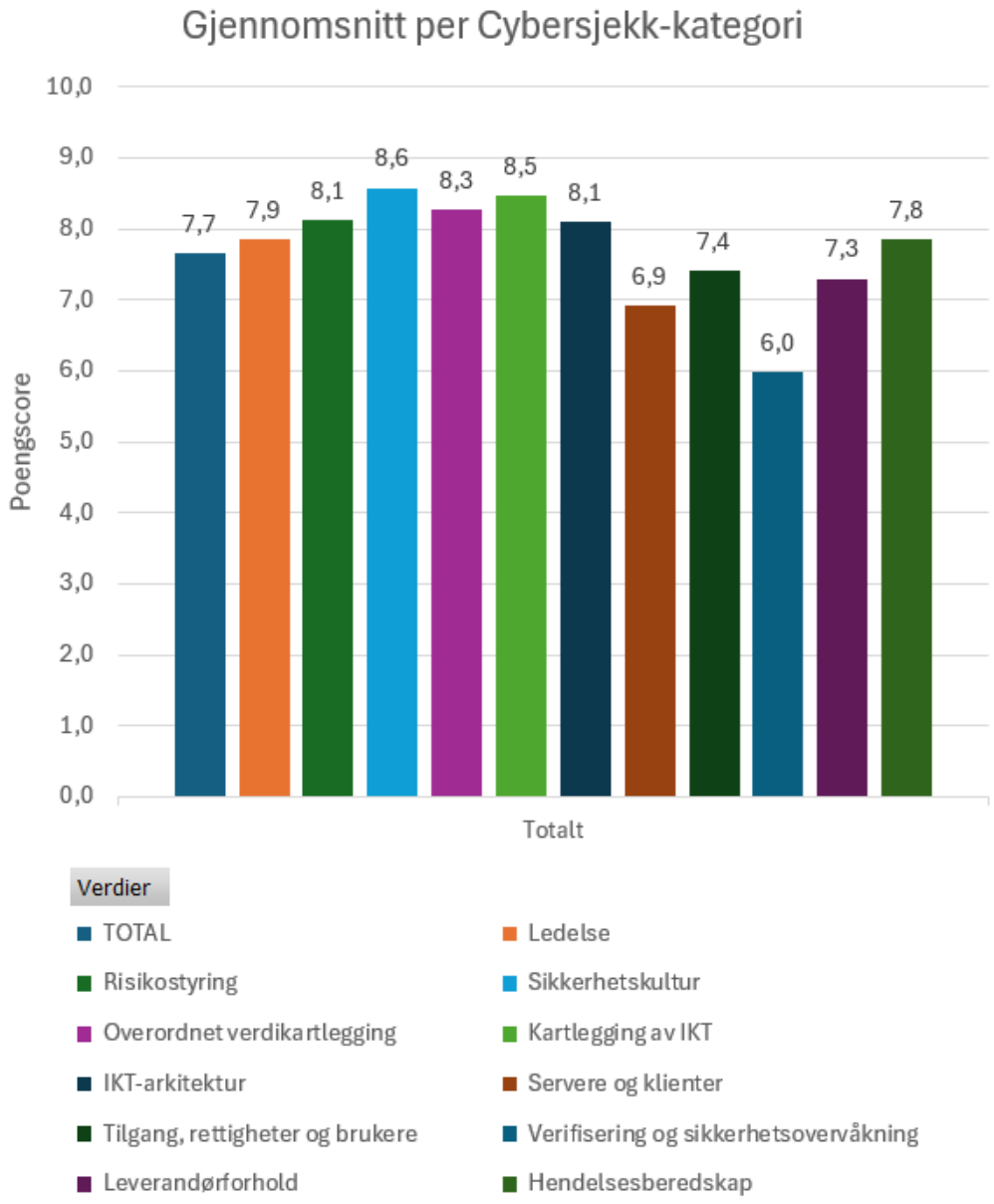
Under vil det bli presentert en kort redegjørelse for funksjonen til et styringssystem for sikkerhet, før hvert enkelt emne blir adressert med en graf som viser det aggregerte resultatet for alle

datasenteroperatørene som var en del av tilsynet. Det blir gitt en overordnet veiledning til emnet, med henvisning til NSMs grunnprinsipper for IKT-sikkerhet.

Hvordan datasenteroperatørene oppnår forsvarlig sikkerhet vil variere utfra verdivurdering og hvordan ulike risikoer kan påvirke verdiene. Det vil derfor være viktig at hver aktør har gjort sine verdivurderinger og ROS analyser samt hensyntar disse i sin drift og arbeid med sikkerhet.

Cybersjekk er en tjeneste hvor norske virksomheter kan sjekke egen digital sikkerhetstilstand. Verktøyet gir et raskt overblikk over virksomhetens digitale sikkerhet og deler en rapport med prioriterte tiltak tilpasset virksomheten som vil bedre sikkerhetsnivået ytterligere.

Diagrammet under viser gjennomsnittet av poengscorene for hvert tema for alle de 17 datasenteroperatørene som var en del av tilsynet:



Jevnt over er det gjennomsnittlige resultatet bra. Gjennomsnittet for alle kategoriene er 7,7. Kategoriene servere og klienter, og verifisering og sikkerhetsovervåkning peker seg ut hvor det kan være størst utfordring for enkelte datasenteroperatører, mens den høyeste gjennomsnittlige poengscoren er på kategorien sikkerhetskultur.

2.1 Styringssystem for sikkerhet

Et styringssystem for sikkerhet bidrar til å beskytte viktige verdier, og bidrar til kontinuerlig forbedring og utvikling i arbeidet, gitt den risikoen datasenteroperatøren er villig til å ta. Et styringssystem handler om hvordan datasenteroperatøren arbeider med sikkerhet, i tillegg til å beskrive hvordan datasenteroperatøren styrer og utfører tiltakene og aktivitetene sine.

Tre momenter som er avgjørende for å bygge opp og videreutvikle et styringssystem for sikkerhet: I) forankring, II) forpliktelse, og III) forståelse.

Gjennom systematisk arbeid vil ledelsen få jevnlig orienteringer om sikkerhetstilstanden, og slikt sett ta avgjørelser på et mer riktig grunnlag. Risikobasert sikkerhetsstyring bidrar proaktivt fremfor reaktiv styring. Det setter datasenteroperatøren i stand til å forebygge hendelser, i stedet for å måtte reagere etter at en uønsket hendelse har skjedd.

Sikkerhetsstyring er en kontinuerlig prosess bestående av planlegging, risikovurdering og risikoevaluering. Målet med sikkerhetsstyring er å identifisere farer og uønskede hendelser, analysere og evaluere risiko, for så å identifisere tiltak som kan redusere risikoen.

Her vil gjennomføringen av sikkerhetsrevisjoner være en grunnleggende forutsetning for en velfungerende forebyggende sikkerhetsarbeid. Resultater av sikkerhetsrevisjonene skal inngå som en del av virksomhetens leders evaluering av det forebyggende sikkerhetsarbeidet.

Planlegging, gjennomføring og oppfølging av interne sikkerhetsrevisjoner, innebærer at plan- og regelmessige sikkerhetsrevisjoner må gjennomføres for de ulike fagområdene innen forebyggende sikkerhet i løpet av en gitt periode. Ved de interne sikkerhetsrevisjonene kontrolleres det om pålagte eller besluttede sikkerhetstiltak faktisk er iverksatt, og om de virker etter hensikten.

Interne sikkerhetsplaner skal revideres jevnlig. Omfanget av den enkelte sikkerhetsrevisjon tilpasses virksomhetens størrelse og kompleksitet, og det er som regel en fordel å gjennomføre flere delrevisjoner per år. Resultatet av interne sikkerhetsrevisjoner skal dokumenteres.

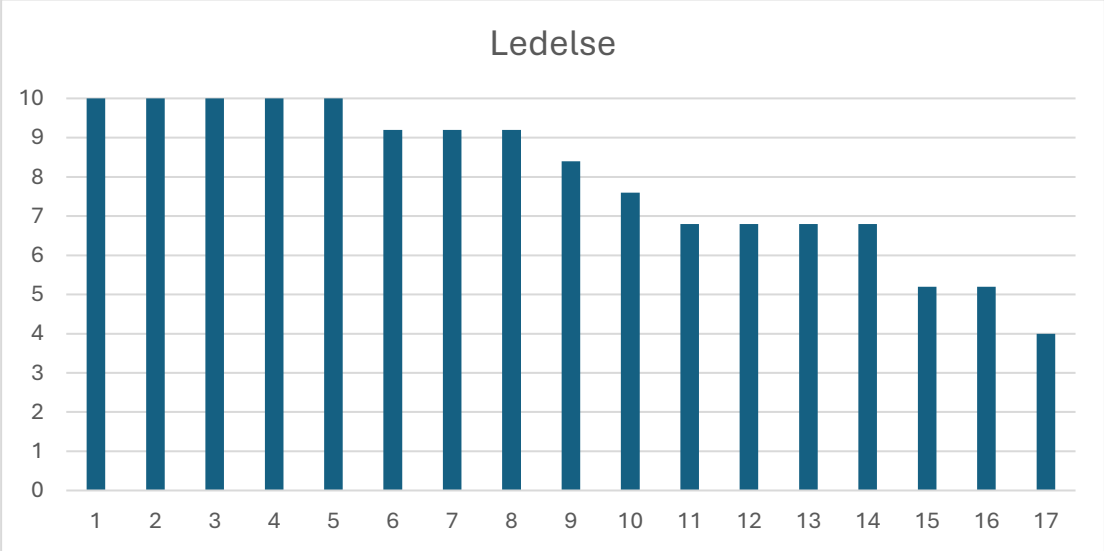
I denne rapporten beskriver vi de delene av styringssystemet som først og fremst gjelder IKT-sikkerhet. Disse sammenfaller med punktene i NSMs Cybersjekk som er benyttet som verktøy. Dette gir et overordnet bilde av aktørene systematiske arbeid innenfor områdene som bygger på NSMs grunnprinsipper for IKT-sikkerhet. Disse beskriver virksomhetens evne til å:

- **Identifisere og kartlegge** egen organisasjon for å holde oversikt over sikkerhetstilstanden. Hensikten er å forstå virksomhetens leveranser og tjenester, få oversikt over hvilke teknologiske ressurser som må sikres og de roller og brukere virksomheten består av, noe som er en forutsetning for å kunne dimensjonere og prioritere sikkerhetsarbeidet slik at de oppnår forsvarlig sikkerhet. Dette punktet er en forutsetning for de tre øvrige punktene.
- **Beskytte og opprettholde** de verdiene man har identifisert at virksomheten har og de leveransene som er identifisert som kritiske.
- **Oppdage** hvilke trusler som finnes, hvilke sårbarheter visksomheten har og hvorvidt man har hendelser som gjør at sikkerheten er truet. Gjennom å oppdage trusler kan man fjerne kjente sårbarheter og oppdage avvik.
- **Håndtere** sikkerhetshendelser effektivt, slik at normal drift gjenopprettes innenfor akseptable tidsrammer, og at man kan lære av disse slik at erfaringene kan brukes inn i et arbeid med kontinuerlig forbedring.

Kapitlene nedenfor beskriver de valgte temaene og funnene knyttet til datasenteroperatørenes resultater.

2.2 Ledelse

Dette punktet tar for seg hvorvidt virksomhetens ledelse tar aktiv del i sikkerhetsarbeidet, og om datasenteroperatøren mener de har etablert en sikkerhetsorganisasjon, med klart definerte roller, ansvar og mål.
Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



De aller fleste datasenteroperatørene rapporterer at de har god lederforankring. Imidlertid er det enkelte som rapporterer at de har et forbedringspotensialet.

2.2.1 Veiledning

Sikkerhetsoppgaver kan delegeres, men ansvaret forblir hos virksomhetens leder. Effektivt arbeid med forebyggende sikkerhet forutsetter derfor at virksomhetens ledelse holder seg orientert om sikkerhetstilstanden i virksomheten og prioriterer ressurser effektivt innenfor dette området.

For å etablere og opprettholde et forsvarlig sikkerhetsnivå er datasenteroperatøren avhengig av at ledelsen er involvert og tar ansvar for sikkerhetsarbeidet. Dette bidrar til at beslutninger om sikkerhet tas på riktig grunnlag, at tilstrekkelige og nødvendige ressurser tildeles og at ressurser brukes riktig.

Det er en klar sammenheng mellom sikkerhetsengasjerte ledere og sikkerhetstilstanden i virksomheten. Der ledelsen er fraværende i sikkerhetsspørsmål, blir avstanden til sikkerhetsarbeidet fort stor, og det blir vanskeligere å få besluttet, gjennomført og evaluert relevante tiltak. Leder skal engasjere seg, og skal legge til rette for gode rutiner og samarbeid som fremmer ønsket sikkerhet.

For at dette skal kunne realiseres anbefaler vi at det er god styring og tydelige styringsprosesser for sikkerhetsarbeidet, og at virksomheten har fastsatte roller, ansvar og rapporterings- og styringslinjer for sikkerhetsarbeidet.

Virksomheten bør ha en strategi og planer for IKT og IKT-sikkerhet som understøtter formål, oppdrag og virksomhetsprosesser. Det bør også være en egen strategi og plan for å modernisere IKT-plattformer og tjenester, som en integrert del av overordnede strategi og mål.

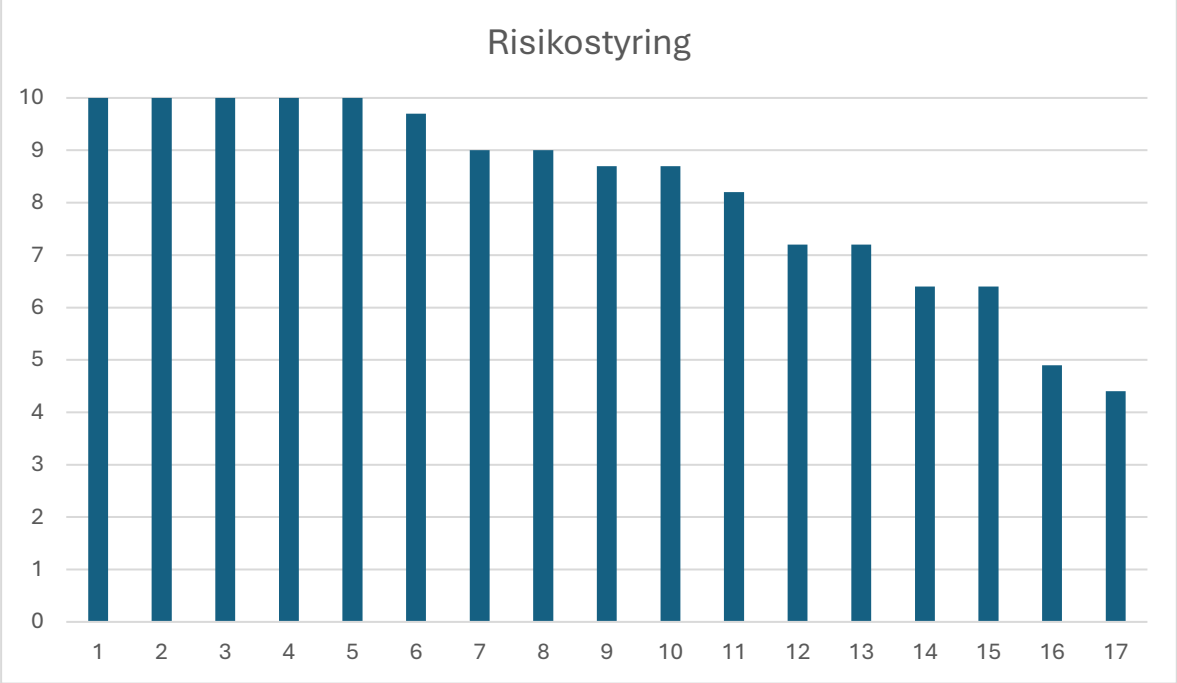
Mer anbefalt veiledning om ledelsens sikkerhetsstyring finnes i NSMs grunnprinsipp for IKT-sikkerhet, kapittel 1.1.[2]

2.3 Risikostyring

Risikostyring er en systematisk prosess for å identifisere, forstå, håndtere og følge opp risikoer som kan påvirke virksomhetens måloppnåelse, verdier og tjenester. Dette innebærer å forstå hvilke verdier som skal beskyttes, hvilke trusler og sårbarheter som kan påvirke dem, og å etablere hensiktsmessige sikkerhetstiltak som reduserer risiko til et akseptabelt nivå.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.

[2] Kartlegg styringsstrukturer, leveranser og understøttende systemer - Nasjonal sikkerhetsmyndighet



Resultatet viser at de fleste datasenteroperatørene rapporterer at de arbeider godt med risikostyring, men at enkelte bør øke innsatsen ytterligere på området.

2.3.1 Veiledning

Sentralt i arbeidet med risikostyring er periodisk oppdaterte verdivurderinger, risiko- og sårbarhetsanalyser (ROS) og beredskapsplaner som er forankret hos virksomhetens ledelse, tilgjengelig, lest og forstått av relevant personell.

Arbeid med IKT-sikkerhet bør starte med verdivurderinger og risikovurderinger. Disse bør gjennomføres på en strukturert måte og følge en metode som gjør arbeidet overkommelig, og sørg for at IKT-sikkerhet er inkludert.

Dette betyr at virksomheten bør ha oversikt over hvilke systemer som ikke bør, eller kan ha nedetid. Oversikten gjelder også hvilke data som bør sikkerhetskopieres og som ikke kan havne på avveie, og hvilke eksterne systemer og tjenester som virksomheten er avhengig av.

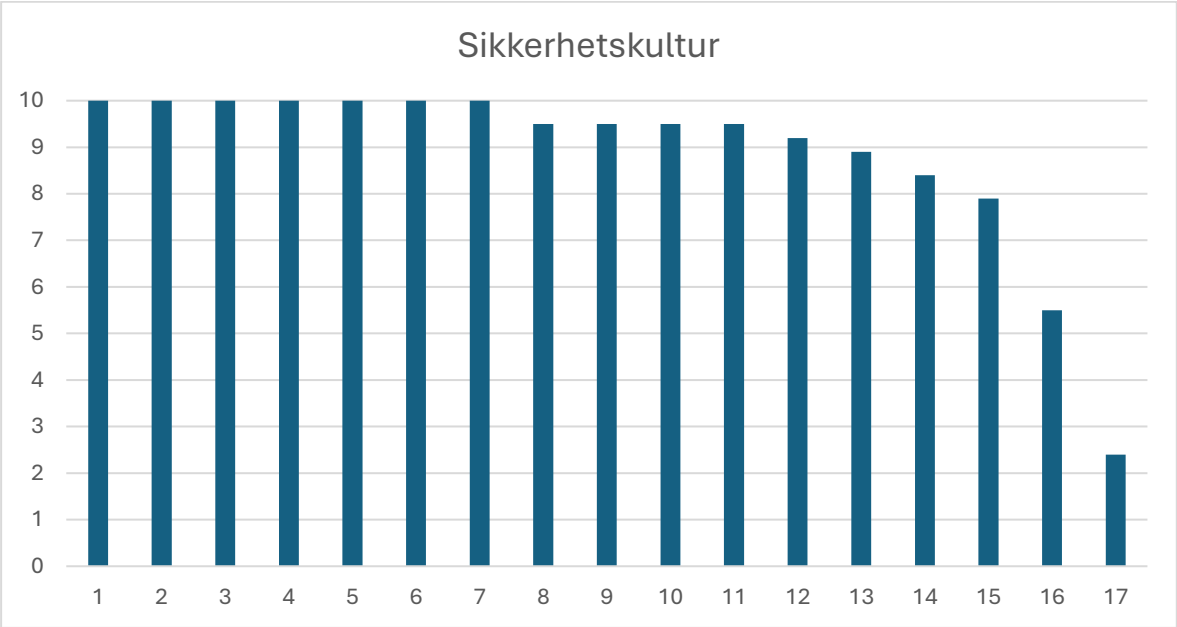
Toleransegrenser for hva virksomheten er villig til å risikere bør være definerte slik at man kan måle risikovurderingene opp mot denne, og iverksette sikkerhetstiltak som er tilpasset denne grensen. Når sikkerhetstiltak er iverksatt, bør disse jevnlig kontrolleres om de fungerer slik de er tenkt.

De siste årene har flere virksomheter blitt rammet av dataangrep. Det er viktig å kartlegge hvilke mulige konsekvenser dette ville fått for virksomheten, og utarbeide relevante risikoscenarier for å

kunne prioritere sikkerhetsarbeidet på en fornuftig måte. Vi anbefaler videre veiledning på NSM sin side om temaet digital utpressing[3].

2.4 Sikkerhetskultur

Sikkerhetskultur er de felles holdningene, verdiene, kunnskapen og adferd som bidrar til sikkerheten i en virksomhet.
Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser at datasenteroperatørene rapporterer at de har innført tiltak som etablerer, bygger og vedlikeholder sikkerhetskultur i organisasjonene. Det er viktig å jobbe systematisk med sikkerhetskultur, og datasenteroperatørene bør fortsette å prioritere dette.

2.4.1 Veiledning

En eller annen form for sikkerhetskultur eksisterer i alle organisasjoner. Den kan være god eller dårlig. Bevisstgjøring, utdanning og opplæring i grunnsikring, IKT-sikkerhet og informasjonssikkerhet er tiltak som er effektive for å bygge og bedre sikkerhetskultur, slik at både ledelse og ansatte forstår sin egen rolle i sikkerhetsarbeidet, er bevisst hvilken risiko som er til stede og aktivt bidrar til å forebygge, oppdage og håndtere hendelser. Dette gjelder også for innleide og konsulenter.

[3] Digital utpressing - Nasjonal sikkerhetsmyndighet

I forbindelse med ansettelser bør virksomheten ha gode rutiner for bakgrunnssjekk og inngåelse av taushetsavtaler, og ha gode rutiner for at de nye medarbeiderne får nødvendig sikkerhetsopplæring ved oppstart.

Sikkerhetskultur er ofte noe som blir tydeliggjort etter at vi opplever sikkerhetsbrudd eller sikkerhetstruende hendelser. Det er vesentlig at det er en god kultur for å rapportere om og håndtere avvik, og at det er tydelig hvilke konsekvenser som gjelder for brudd på virksomhetens regelverk. Man må generelt passe på at trussel om straff ikke hindrer rapportering. Det skal være trygt å rapportere, også når det gjelder egne brudd.

Som et minimum bør virksomheten legge til rette for sikkert arbeid hjemmefra, og ha regler i forbindelse med reise. Hva som gjelder for privat bruk av virksomhetens IKT-utstyr, og bruk av privat utstyr til jobbrelatert arbeid bør også være tydeliggjort.

For videre lesing anbefaler vi NSM-artikler om sikkerhetskultur[4] og deres temarapport om innsiderisiko[5].

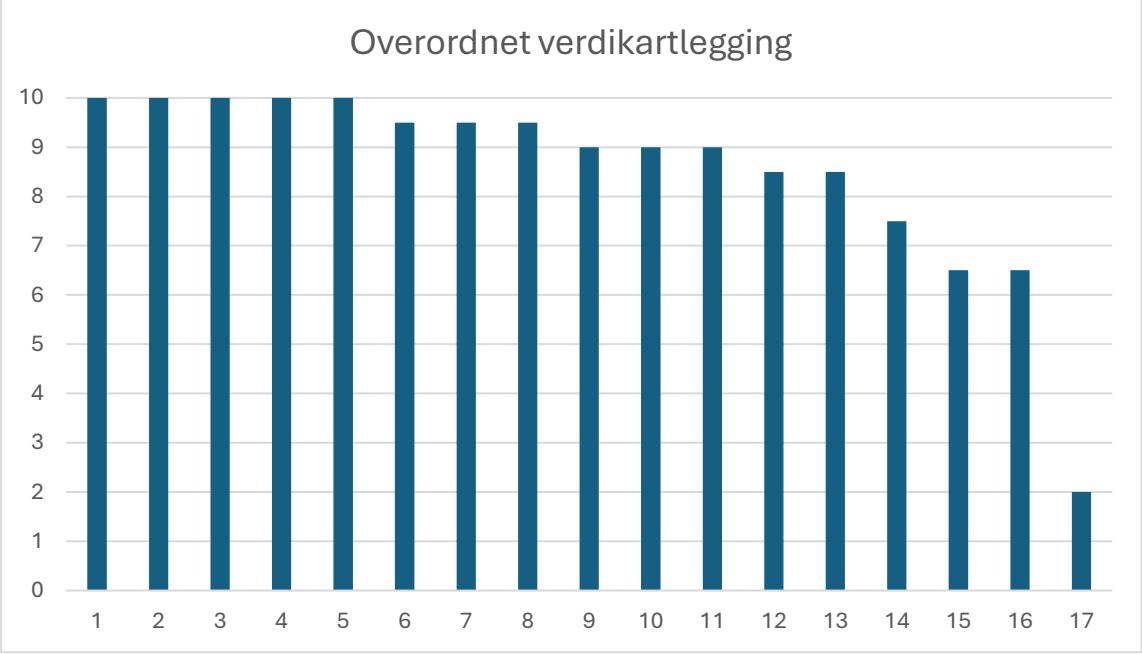
2.5 Overordnet verdikartlegging

Her blir datasenteroperatørene bedt om å vurdere i hvor stor grad de har oversikt over egne rammer.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.

[4] NSM artikler om sikkerhetskultur

[5] NSMs temarapport om innsiderisiko



Resultatet viser at datasenteroperatørene generelt i tilsynet rapporterer at de har en god oversikt over elementer som er med å bygge god digital sikkerhet.

2.5.1 Veiledning

For å kunne beskytte datasenterets funksjon er det viktig å vite hvilke interne prosesser som er nødvendige for å understøtte denne virksomheten, hvilke interne og eksterne IKT-systemer driften er avhengig av, og hvilke juridiske og kontraktsfestede rammer som gjelder. Over tid kan det skje endringer i alle disse innsatsfaktorene. Denne oversikten vil danne grunnlag for prioritering, beskyttelse og vedlikehold av datasenteret.

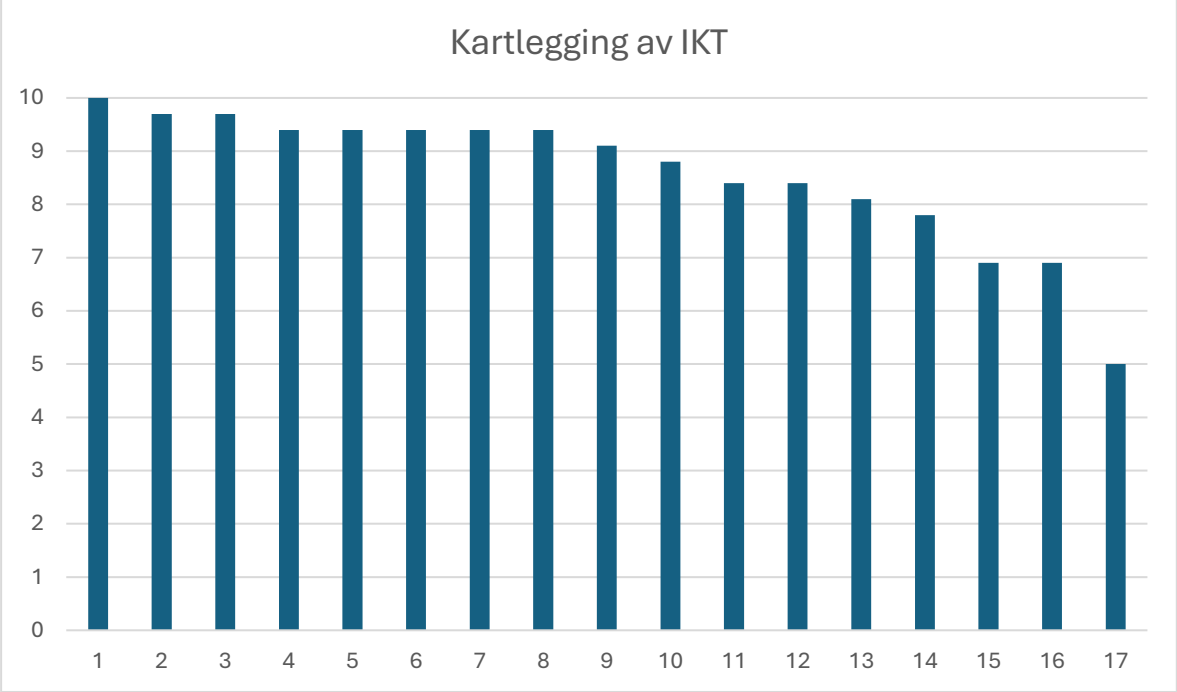
Les videre i NSMs grunnprinsipper for IKT-sikkerhet kapittel 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer[6].

2.5.2 IKT kartlegging

Et godt utgangspunkt for arbeidet med IKT-sikkerhet for en datasenteroperatør er å ha oversikt over servere, klienter, nettverk og programvare som er i bruk.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.

[6] Kartlegg styringsstrukturer, leveranser og understøttende systemer - Nasjonal sikkerhetsmyndighet



Resultatet viser at datasenteroperatørene rapporterer at de har god oversikt over sine IKT-elementer. Samtidig er det aktører som har et forbedringspotensial.

2.5.3 Veiledning

Det er vesentlig for en virksomhet å ha oversikt over servere, klienter, nettverk og programvare som er i bruk. Dette er nødvendig for å ha kontroll på potensielle sårbarheter og mulige angrep. Oversikt over hvilke versjoner som er i bruk er viktig, da sårbarheter oftest gjelder spesifikke versjoner. På den måten kan man sikre at tiltak som innføres blir gjennomført på alle relevante enheter og at datasenteroperatøren har kontroll på potensielle sårbarheter og mulige angrepsvektorer.

Det er anbefalt å bruke automatiserte og sentraliserte verktøy for å vedlikeholde nødvendig oversikt.

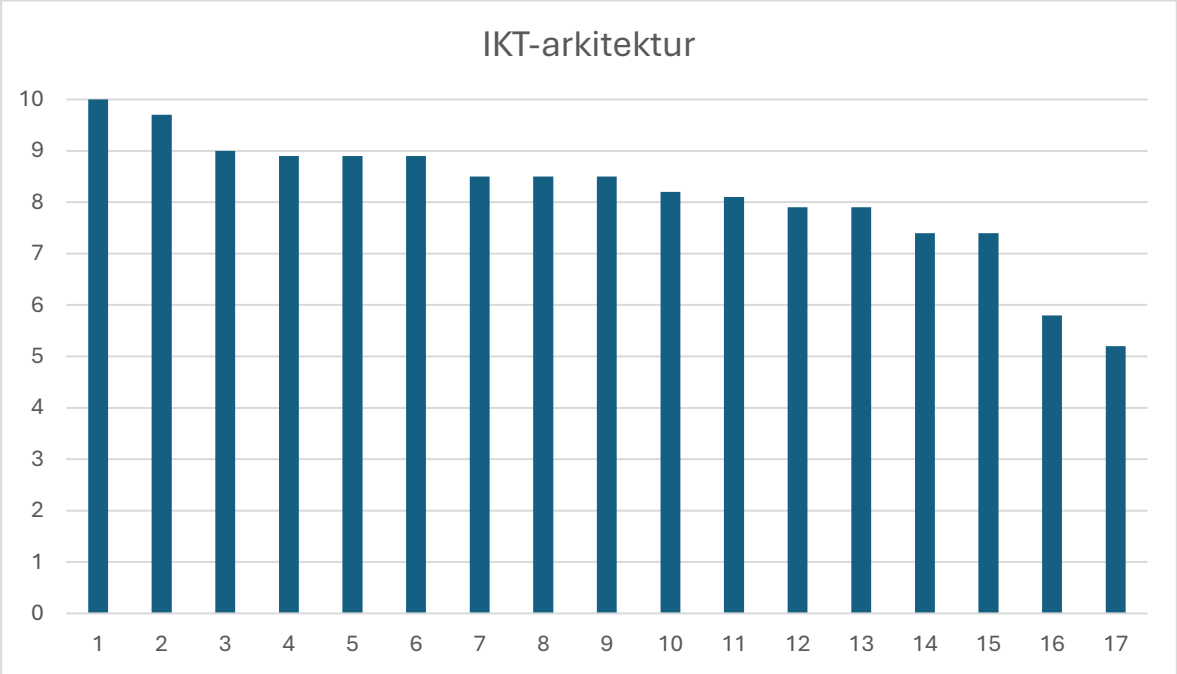
Les videre i NSMs grunnprinsipper for IKT-sikkerhet kapittel 1.2 Kartlegg enheter og programvare[7].

2.6 IKT arkitektur

Dette punktet handler om hvorvidt datasenteroperatøren har etablert en helhetlig IKT-arkitektur som ivaretar ønsket sikkerhetsnivå gjennom gode sikkerhetsfunksjoner og sikkerhetsstrukturer med mulighet for etterprøvbarhet.

[7] Kartlegg enheter og programvare - Nasjonal sikkerhetsmyndighet

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser at datasenteroperatørene rapporterer at de generelt sett har god oversikt over IKT-arkitekturen. Samtidig er det aktører som har et konkret forbedringspotensial.

2.6.1 Veiledning

Å inkludere sikkerhet allerede i planleggingen av IKT-systemene er den beste måten å sørge for at sikkerhet er en integrert del av systemet. Imidlertid inneholder ofte et IKT-system mange produkter og sikkerhetsfunksjoner som kobles sammen. For å sikre at disse fungerer godt sammen og ikke introduserer sikkerhetshull er det viktig at datasenteroperatøren har en overordnet plan for IKT-arkitekturen sin. En slik plan bør dekke så mange av områdene klienter, servere, nettverk, skytjenester og andre tjenesteutsatte tjenester som mulig. Videre må det være klare planer for grunnsikring, drift, vedlikehold og endringer, samt hvordan nettverket er delt opp og hvilke integrasjoner som finnes, samt hvilke deler av infrastrukturen som kan aksesseres utenfra og hvordan fjernaksess sikres.

Som et minimum bør brannmur være på plass for å styre trafikk mellom nettverk, som er delt opp på en hensiktsmessig måte. VPN eller tilsvarende bør være implementert for å sikre fjerntilgang, og sensitiv informasjon bør beskyttes ved transport og lagring.

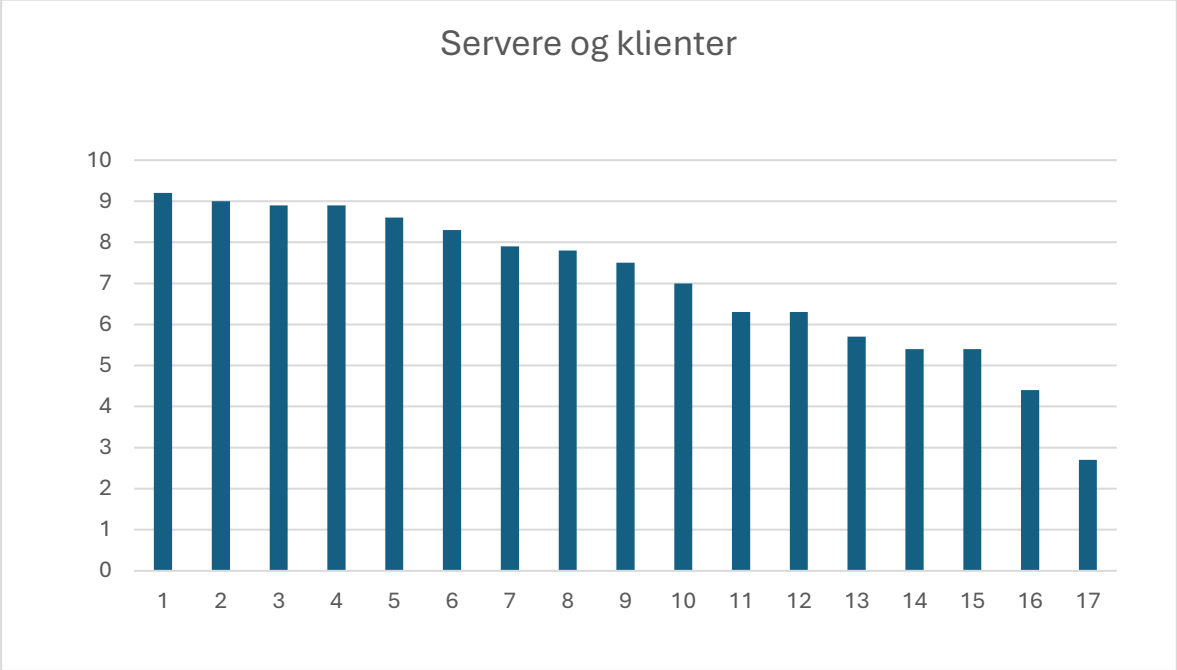
NSM grunnprinsipper for IKT-sikkerhet kapittel 2.2 Etabler en sikker IKT-infrastruktur omhandler dette temaet.[8]

[8] Etabler en sikker IKT-arkitektur - Nasjonal sikkerhetsmyndighet

2.7 Servere og klienter

Dette punktet handler om sikkerhetsoppdatering av programvare på servere og klienter blir utført regelmessig og tidsnok. Dersom sikkerhetsoppdateringer ikke installeres, vil angripere kunne utnytte offentlig kjente sårbarheter.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser en spredning på sikkerhetsnivået med flere datasenteroperatører med lavere poengscore.

2.7.1 Veiledning

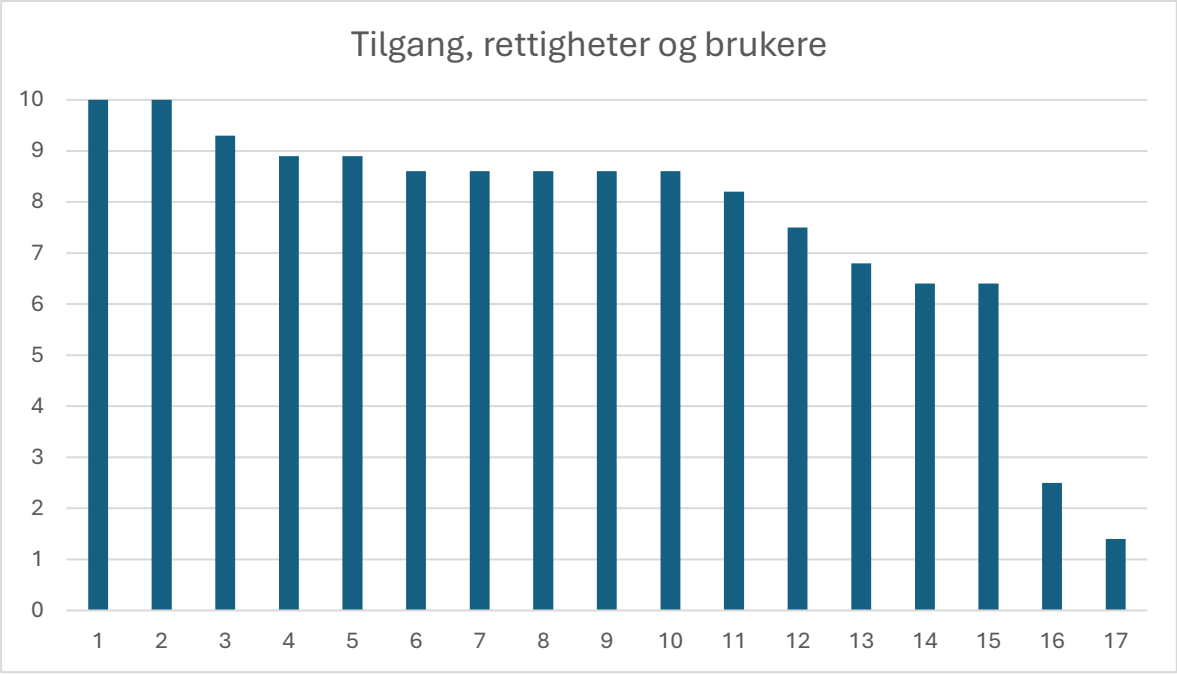
For å sikre servere og klienter er det sentralt at datasenteroperatøren har rutiner for sikkerhetsoppdatering av servere og klienter, sikkerhetskopiering, lagring og gjenoppretting av data, samt inn- og utfasing av nytt og gammelt utstyr. Dette for å redusere sårbarhetsflaten så langt det lar seg gjøre, samt kunne gjenopprette normal drift dersom uhellet allikevel er ute.

For å redusere sannsynligheten for og konsekvensene av cyberangrep er det mange tiltak man kan innføre på servere og klienter.
Dette kan være sentraliserte løsninger for å oppdage og deaktivere skadevare, passordkontroll på IKT-utstyr, flåtestyringsverktøy for styring og kontroll av klienter og mobile enheter for å nevne noe.

2.8 Tilgang, rettigheter og brukere

Tilgangsstyring er sentralt i arbeidet med digital sikkerhet. Dette punktet handler om i hvor stor grad datasenteroperatørene prioriterer dette i sin virksomhet.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser at flere datasenteroperatører rapporterer at de prioriterer arbeidet med tilgangsstyring i organisasjonen, mens noen har et forbedringspotensialet.

2.8.1 Veiledning

Effektiv tilgangs- og rettighetsstyring er en grunnpilar i moderne IKT-sikkerhet. Ved å sikre at brukerne kun har tilgang til de systemene og dataene de faktisk har behov for, reduseres risikoen for både menneskelige feil og utilsiktet feilbruk, og mer ondsinnede handlinger som sabotasje eller bevisst misbruk.

Like viktig som gode rutiner for tildeling av roller, er løpende verifisering av identiteter og tilgangsnivåer, slik at endringer i roller, arbeidsoppgaver eller sikkerhetskrav fanges opp og håndteres korrekt. På den måten kan en bruker få tildelt nye rettigheter som er nødvendig for å ivareta endring i oppgaver, men også fjerne eventuelle tilganger som ikke lenger er nødvendige, eller som utgjør en uakseptabel risiko i kombinasjon med noen av de nye tilgangene. God styring av roller, rettigheter og autentiseringsmekanismer bidrar til å begrense muligheter for og potensialet for skadeomfang ved misbruk, samtidig som at sporbarhet og mulighet for kontroll økes.

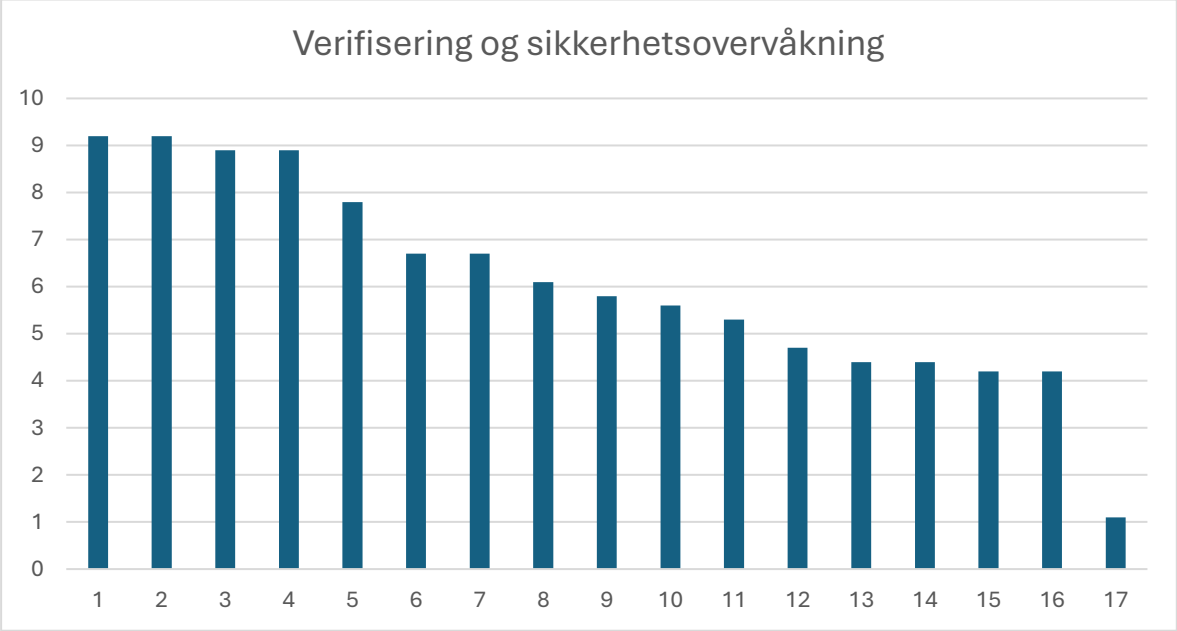
En vanlig angrepsmetode mot et IKT-system er å forsøke å få tilgang til en eller flere brukerkontoer på styrings- eller administrasjonssystemer. Det er derfor viktig å innføre tiltak som beskytter kontoer, samt å holde orden på kontoer og hvilke rettigheter de gir brukeren.

Vi viser til NSMs grunnprinsipp 2.6. Ha kontroll på identiteter og tilganger for videre veiledning[9].

2.9 Verifisering og sikkerhetsovervåkning

IKT-systemer må overvåkes og relevante data samles inn for å redusere sannsynlighet og konsekvensene av et angrep på virksomhetens IKT-systemer.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser en spredning mellom datasenteroperatørenes rapporterte arbeid med å etablere sikkerhetsovervåkning av IKT-systemene, og verifisere sikkerhetsmekanismene. Flere av virksomhetene har et forbedringspotensiale på dette området.

2.9.1 Veiledning

For å avdekke angrep og hendelser i IKT-systemer er det viktig at de er tilstrekkelig overvåket og at det er etablert logging og kapasitet til å analysere loggene. Logging er en automatisk og systematisk registrering av hendelser, transaksjoner og aktiviteter i systemet.

[9] Ha kontroll på identiteter og tilganger - Nasjonal sikkerhetsmyndighet

Det er viktig at man vurderer forskjellige former for beskyttelsessystemer. Noen med utplasserte agenter og andre som passivt logger og overvåker trafikk i nettverkene. Felles for veldig mange av de store angrepene som har vært, er at man har kunne oppdaget inntrenger i eksisterende logger. Hvis man hadde hatt ressurser, kunnskap og tid til å oppdage avvikene.

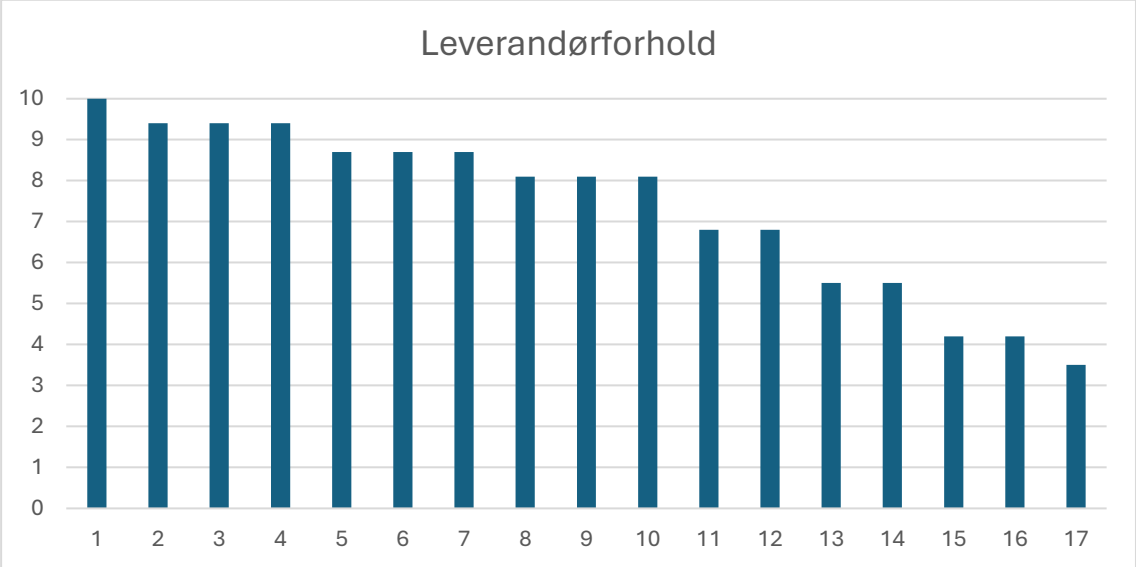
Når man overvåker virksomhetens systemer, vil man ofte lagre og overvåke forskjellige typer for data. Det er viktig å sette seg inn i gjeldende og relevante lover, regler og reguleringer. Data som overvåkes og lagres kan være persondata tilhørende ansatte, kunder og brukere. Hvor lenge slike data skal lagres og hvilke samtykker og hva slags informasjon som skal være gjort tilgjengelig i forkant er også viktig å avklare.

Mer detaljert veiledning finnes i NSMs grunnprinsipper for IKT-sikkerhet 3.2 Etabler sikkerhetsovervåkning.[10]

2.10 Leverandørforhold

I dette punktet er leverandørforhold avgrenset til om IKT-sikkerhet er en del av vurderingene ved innkjøp av IKT-produkter og IKT-tjenester.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.



Resultatet viser en viss spredning i datasenteroperatørenes rapporterte arbeid med å inkludere IKT-sikkerhet i arbeidet med IKT-anskaffelser.

[10] Etabler sikkerhetsovervåkning - Nasjonal sikkerhetsmyndighet

2.10.1Veiledning

IKT-sikkerhet er viktig i alle IKT-produkter og IKT-tjenester, ikke bare ved anskaffelse av rene sikkerhetsprodukter som en brannmur. Dersom en virksomhet anskaffer IKT-produkter og IKT-tjenester som har svak sikkerhet eller som ikke integrerer godt med virksomhetens øvrige sikkerhetsarkitektur og eksisterende IKT-produkter kan dette øke sårbarheten og redusere sikkerhetsnivået i virksomheten (NSM).

Leverandørforhold kan være bygget opp av kompliserte verdikjeder, anskaffelser av nye IKT-produkter og -tjenester kan medføre ny eller økt risiko. Før slike prosesser igangsettes er det viktig å skaffe seg oversikt over hvilke nye sårbarheter og avhengigheter som kan introduseres, og å kvalitetssikre hele prosessen sikkerhetsmessig fra planlegging, innkjøp, driftsfase, til avvikling.
Det er viktig å utarbeide tydelige avtaler med leverandøren som ivaretar sikkerheten knyttet til anskaffelser.

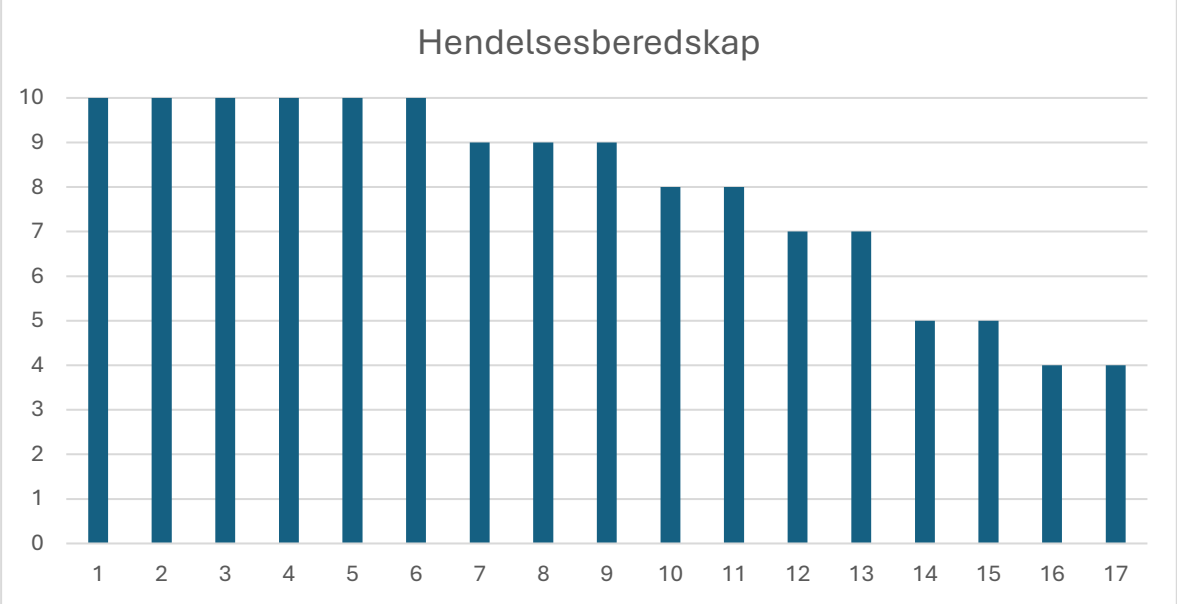
Ved anskaffelser av produkter, tjenester og tjenesteutsetting er det viktig å ta med sikkerhet i alle fasene av anskaffelsen. Dette handler både om å stille riktige krav til leverandøren, men også å ha riktig kompetanse i virksomheten, gjøre de riktige vurderingene og følge opp leverandøren på en god måte. Det er også viktig å ha planer klare for avslutning av anskaffelsen, spesielt i fall dette skjer ufrivillig eller brått. Dette kan komme av årsaker knyttet til geopolitikk, energi, linjebrudd, cyberangrep og annet.
VI viser til NSM grunnprinsipper for IKT-sikkerhet kapittel 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser, som utdyper dette emnet.[11]

2.11 Hendelsesberedskap

Både målrettede og tilfeldige uønskede hendelser bør oppdages og håndteres hurtig. Dette punktet handler om hvor forberedt datasenteroperatørene er på dette.

Tabellen nedenfor viser fordelingen av poengscoren på de 17 tilsynsobjektene. Data er sortert synkende.

[11] Ivareta sikkerhet i anskaffelses- og utviklingsprosesser - Nasjonal sikkerhetsmyndighet



Resultatet viser en spredning i datasenteroperatørenes rapporterte arbeid med hendelsesberedskap. Datasenteroperatørene må forsikre seg om at krav i lov og forskrift om beredskapsplanlegging for å ivareta forsvarlig sikkerhet og beredskap i datasenter blir ivaretatt.

2.11.1Veiledning

Det er viktig at datasenteroperatørene har planer for å håndtere uønskede hendelser, både for å begrense omfanget, men også for å raskt kunne gjenopprette kritiske systemer og data dersom uhellet er ute. Et godt utviklet beredskapssystem som er oppdatert, kjent for de som har aktive roller, og øvet er essensielt for å effektivt gjenopprette informasjon og tjenester dersom datasenteroperatøren har vært rammet av alvorlige hendelser.

Dataangrep kan ramme alle datasenteroperatører, også de som har brukt mye ressurser på å heve IKT-sikkerheten. Konsekvensen av et eventuelt angrep vil variere for de ulike datasenteroperatørene.

Vi anbefaler datasenteraktørene å etablere relevante tiltak som er beskrevet i NSMs grunnprinsipper for IKT-sikkerhet kapittel 4.1 Forbered virksomheten på håndtering av hendelser[12], kapittel 4.3 Kontroller og håndter hendelser[13], og kapittel 4.4 Evaluer og lær av hendelser[14].

[12] Forbered virksomheten på håndtering av hendelser - Nasjonal sikkerhetsmyndighet

[13] Kontroller og håndter hendelser - Nasjonal sikkerhetsmyndighet

[14] Evaluer og lær av hendelser - Nasjonal sikkerhetsmyndighet

3 Virksomhetens dokumentasjon

Nkom har i forbindelse med tilsynet innhentet dokumentasjon fra tilsynsobjektene.

Dokumentasjonen oppbevares hos Nkom