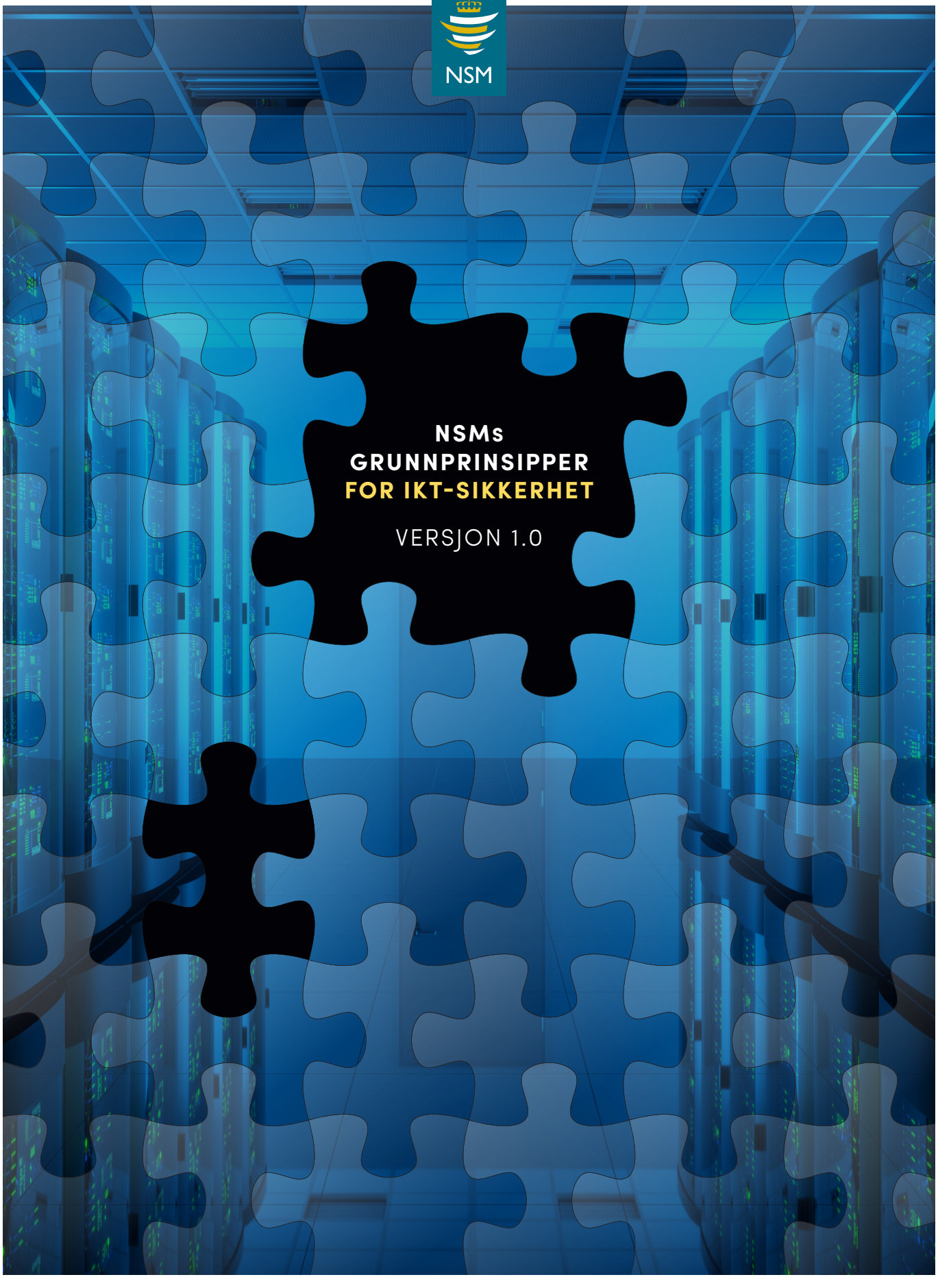

NSM
NSMs
GRUNNPRINSIPPER
FOR IKT-SIKKERHET
VERSJON 1.0

Sist revidert:
2017-08-25

Design:
REDINK

Trykk og distribusjon:
RK GRAFISK

Innhold

Introduksjon

DIGITALISERING AV samfunnet skaper kontinuerlig nye verdier og utviklingsmuligheter, men utvider også sårbarhetsflatene til det vi ønsker å beskytte. Vi ser stadige eksempler på tap av informasjon og at virksomheter ikke får levert tjenester de har behov for.

Det er ingen mangel på tilgjengelig informasjon om hvordan en virksomhet skal sikre sine IKT-systemer og infrastruktur. Mange virksomheter må i tillegg forholde seg til ulike regelverk med tilhørende forvaltere. All denne informasjonen kan fort bli en jungel av konkurrerende muligheter og krav som distraherer beslutningstakere fra å ta riktige valg.

Den stadig økende bruk av digitale tjenester, innebærer blant annet at brukere blir mer mobile og bruken av skybaserte tjenester øker. Denne situasjonen gir fordeler, men innebærer også økt kompleksitet ved at data og applikasjoner blir distribuert til flere enheter og lokasjoner. Konsekvenser av dette er økt avhengighet til tredjeparter og at sikringsbehovet for virksomheter og deres informasjonsverdier strekker seg ut over egen virksomhet. Med dette, følger også nye typer trusler som må adresseres.

Man må derfor spørre seg hvordan vi kan holde kunnskap og teknologi oppdatert og sikret i lys av hurtig utviklende IKT-miljøer med tilsynelatende uendelig antall mulige løsninger? Hva er de mest kritiske områdene vi bør adressere, og hvordan skal virksomheter ta første steg for å modne risikostyringen? Hvordan kan vi sikre at vi starter i riktig ende og med de mest grunnleggende stegene, og sørge for at vi får på plass fundamentale prinsipper for sikring, måling og forbedring som følges opp over tid?

Disse spørsmålene er bakgrunnen for utviklingen av grunnprinsippene. Basert på forslag fra NSM i Sikkerhetsfaglig råd[1], har vi fått et oppdrag å utforme et felles nasjonalt rammeverk for sikring av IKT-systemer. Dette vil hjelpe de ulike virksomhetene i utvelgelsen av sikringstiltak, og gi regelverksforvaltere et rammeverk de kan peke til i sin kravstilling og veiledning. Målet er at dette skal bli et levende og tidsaktuelt produkt som oppdateres jevnlig basert på innspill fra brukere og fagmiljøer fra offentlig og privat sektor.

Vi vil takke bidragsytere til denne første versjonen av grunnprinsippene. Gjennom 2017 har vi hatt møter med aktører fra offentlig og privat sektor som har gitt viktige innspill og bidrag. Vi vil rette en spesiell takk til Norges vassdrags- og energidirekorat (NVE), Nasjonal kommunikasjonsmyndighet (Nkom), Telenor, Statoil, Direktoratet for forvaltning og IKT (Difi) og Datatilsynet.

[1] https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

«Den fremvoksende informasjonen kan fort bli en «jungel» med konkurrerende muligheter og krav som distraherer beslutningstakere fra å ta riktige valg.»

HVA ER NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET?

NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser.

Grunnprinsippene beskriver **hva** en virksomhet bør gjøre for å sikre et IKT-system. De beskriver også **hvorfor** det bør gjøres, men ikke **hvordan**. Grunnprinsippene kompletterer, men erstatter ikke en virksomhets sikkerhetsstyringsarbeid. Viktige suksessfaktorer for å lykkes med implementasjon av grunn-prinsippene er at ledelsen involverer seg, at man har sikkerhetskompetanse i virksomheten og etablerte styrings- og risikosløyfer. Dette er videre adressert i NSMs veileder i sikkerhetsstyring[2]. Grunnprinsippene bør benyttes som en del av virksomhetsstyringen og gi retning for implementasjons- og driftsnivået i en virksomhet.

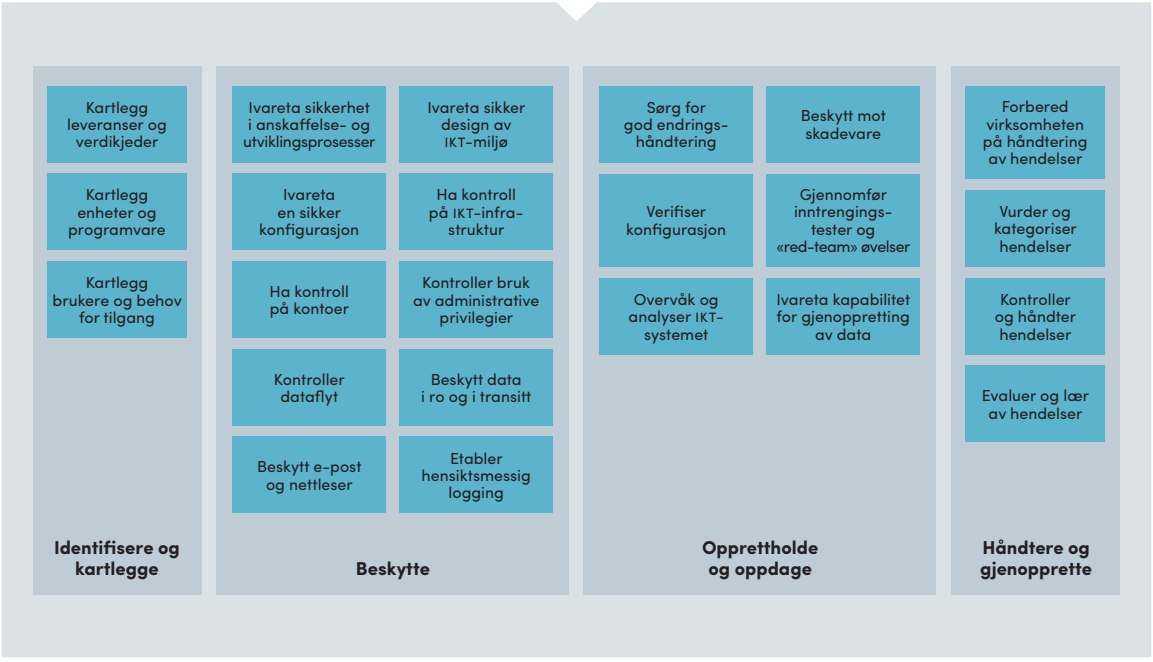
Utvelgelse av sikringstiltak bør baseres på det ordinære risikoarbeidet, men grunnprinsippene vil hjelpe virksomhetene med å velge ut riktige sikringstiltak. De kan også brukes for å identifisere risiko når anbefalte sikringstiltak utelates. En virksomhet som ikke implementerer et anbefalt sikringstiltak, vil i de aller fleste tilfeller ha økt risiko som må håndteres. Denne risikoen må vurderes opp i mot virksomhetens kommersielle risikotoleranse, i tillegg til krav i lovverk, bransjenormer og avtaler. Dersom risikoen ikke kan aksepteres, må kompenserende tiltak vurderes.

Utvikling av gode sikringstiltak er en kontinuerlig prosess, og NSM vil videreutvikle grunnprinsippene i tråd med trussel- og sårbarhetsbildet samt den teknologiske utviklingen i samfunnet.

Grunnprinsippene er strukturert i fire kategorier som vist i Figur 1 . Et grunnprinsipp er for eksempel «Beskytt data i ro og i transitt» som er en del av kategorien «Beskytte». Hvert grunnprinsipp har underliggende sikringstiltak som beskriver hva som bør gjøres. Hvert grunnprinsipp er en kontinuerlig aktivitet som må vurderes i hele systemets levetid, fra planlegging og etablering til avhending. Flere av grunnprinsippene bygger på hverandre, og enkelte er en forutsetning for at andre skal kunne implementeres effektivt. I sum inkluderer grunnprinsippene bredden av sikringstiltak som består av barrierer, deteksjon, verifikasjon og reaksjon for å etablere god sikkerhet i dybden. Tiltakene vil være gjeldende for både utilsiktede og tilsiktede handlinger, men hovedfokus har vært på tilsiktede handlinger.

Første versjon av grunnprinsippene handler om teknologiske og organisatoriske tiltak for å sikre IKT-systemer. Det menneskelige perspektivet og fysisk sikkerhet vil inkluderes i senere versjoner.

[2] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf



FIGUR 1 – oversikt over grunnprinsippene

DE FIRE KATEGORIENE

Identifisere og kartlegge – opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere.

Dette er grunnlaget for en effektiv implementering av de øvrige grunnprinsippene. 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. Dette gjør det mulig å fokusere og prioritere sikringstiltakene i tråd med risikostyringsstrategien og forretningsbehovene. Kategorien fokuserer også på å etablere prosesser for å forvalte kunnskapen over tid.

«Sikkerhet må være en integrert del av virksomhets-prosessene hvor både ansvar og oppgaver for å utøve sikkerhet ligger hos den enkelte medarbeider og leder.»

Beskytte – ivareta en forsvarlig sikring av IKT-miljøet.

Prinsippene som må til for å ivareta en sikker tilstand for IKT-miljøet for å motstå eller begrense skaden fra dataangrep. Det innebærer å sikre hvordan IKT-infrastrukturen anskaffes, designes og konfigureres slik at ønsket sikkerhet oppnås.

Opprettholde og oppdage – opprettholde den sikre tilstanden over tid og ved endringer, og oppdage sikkerhetstruende hendelser.

Prinsippene i denne kategorien ivaretar behovet for å håndtere endringer, både planlagte endringer, feilretting og sikkerhetsoppdateringer. Sentralt her er å overvåke IKT-miljøet opp imot ønsket, sikker tilstand og danne oppdatert situasjonsforståelse.

Håndtere og gjenopprette – håndtere sikkerhetstruende hendelser effektivt.

Her finner du prinsipper for å få på plass aktiviteter for å håndtere sikkerhetstruende hendelser. Dette innebærer prinsipper for å vurdere, kontrollere og håndtere, gjenopprette normaltilstand og forbedre sikkerheten basert på erfaringer fra hendelseshåndteringen.

MÅLGRUPPE

Grunnprinsippene er utarbeidet for å dekke et bredt spekter av virksomheter, både i form av størrelse og type leveranser. De er relevante for alle virksomheter, både offentlige og private, uavhengig om de behandler sikkerhetsgradert informasjon, eller ikke.

I den enkelte virksomhet er forretnings- og IT-ledelsen ofte bindeleddet mellom toppledelse og implementasjons- og driftsnivå, som vist i Figur 2. Dette inkluderer IT-ledelse og systemeiere, sikkerhetsledere og forretnings- og prosesseiere. Disse er hovedmålgruppen for NSMs grunnprinsipper.

Sikkerhet må være en integrert del av virksomhetsprosessene hvor både ansvar og oppgaver for å utøve sikkerhet ligger hos den enkelte medarbeider og leder. De fleste virksomheter har likevel nøkkelroller med stor påvirkning på virksomhetens informasjonssikkerhetsarbeid. Sikkerhetsleder eller informasjonssikkerhetsleder har ofte delegert det formelle ansvaret for informasjonssikkerheten. Sikkerheten i IKT-systemer vil ofte skapes i IT-driftsorganisasjonen slik at IT-ledelsen og systemeiere i praksis legger forutsetningene for informasjonssikkerheten i virksomheten. Tilsvarende er det forretnings- og IT-ledelse som kjenner virksomhetens

«Prosess- og systemeiere må kommunisere et korrekt risikobilde til toppledelsen og andre risikoeiere.»

leveranser og legger premissene for sikkerhetskrav.

Forretnings- og IT-ledelsen beslutter rammeverk og retningslinjer som angir hvilke sikringstiltak som skal implementeres. For å understøtte utvelgelsen beskriver grunnprinsippene hva en virksomhet bør gjøre. Prosess- og systemeiere må også kommunisere et korrekt risikobilde til toppledelsen og andre risikoeiere. Grunnprinsippene vil hjelpe målgruppen med å beskrive hvorfor de anbefalte tiltakene bør implementeres.

Toppledelsen har fokus på organisatorisk risiko og bruker IKT-sikkerhet som styringsparameter. Det er avgjørende at toppledelsen tar eierskap og driver sikkerhetsarbeidet i egen virksomhet gjennom styringsvirkemidler.

NSM vil i løpet av 2017 produsere en veileder i bruk av grunnprinsippene rettet mot toppledere.

GRUNNPRINSIPPENE SETT OPP MOT ANDRE REGELVERK, STANDARDER OG RAMMEVERK

NSMs grunnprinsipper er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet. Grunnprinsippene, som har et sektorovergripende fokus, uthever de viktigste sikringstiltakene i ISO/IEC 27002:2017 som vist i Figur 3. Grunnprinsippene er koblet mot relevante sikringstiltak i denne standarden.[3] Kategori-inndelingen i prinsippene er i stor grad sammenfallende med gjeldende inndeling i «Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)»[4] og «NIST Cyber Security Framework»[5]. Andre rammeverk som er benyttet som inspirasjon, og vil være gjenkjennbare i grunnprinsippene, er «Cyber Essentials»[6] og «CIS CSC Top 20[7]».

NSM har et sett med veiledninger som understøtter grunnprinsippene. Et eksempel er sjekklistene S-01 «Fire effektive tiltak mot dataangrep» og U-15 «Sikring av webtrafikk (HTTPS)». NSM vil koble disse veilederne mot grunnprinsippene i senere versjoner.

Der det finnes bransje-, teknologi- eller sektorspesifikke materiale bør dette benyttes i tillegg til de generiske standardene som ISO/IEC 27000-serien og NSMs grunnprinsipper. ⊙

[3] For mer informasjon, se vedlegg A.

[4] Lov om forebyggende sikkerhetstjeneste, https://lovdata.no/dokument/NL/lov/1998-03-20-10

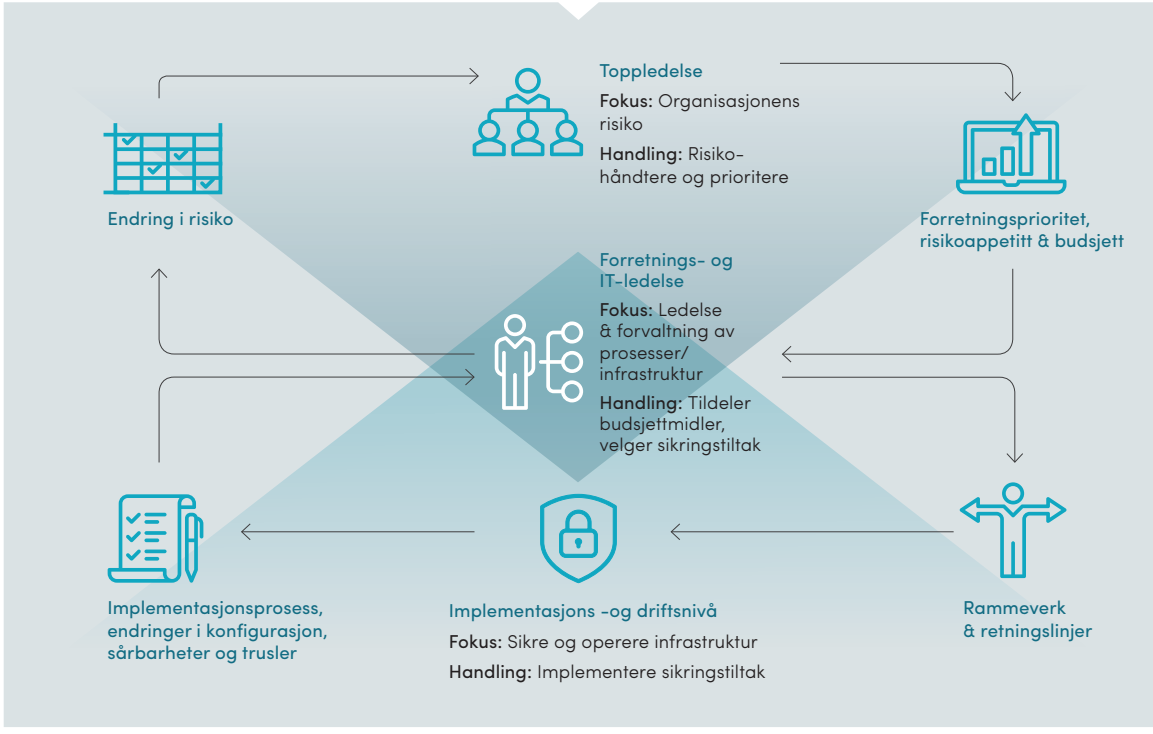
[5] NIST Cyber Security Framework, https://www.nist.gov/cyberframework

[6] Home Office Cyber essensials, https://www.cyberaware.gov.uk/cyberessentials/

[7] Center for internet security, https://www.cisecurity.org/controls/

Ofte har IT-avdelingen implementert gode og fornuftige sikringstiltak. Men tiltakene ikke er forankret i ledelsen. Ledelsen får dermed ikke prioritert sikkerhetsarbeidet på en hensiktsmessig måte som del av den løpende styringen av virksomheten. Vi har flere ganger sett at sikringstiltak er fokusert på feil verdier i en virksomhet. Viktige verdier er utelatt eller glemt fordi det ikke er lagt til grunn en helhetstankegang ved valg av tiltak. I verste fall kan sikringstiltakene virke mot sin hensikt.

«Sikringstiltakene er riktig implementert, men er det de riktige sikrings-tiltakene som er implementert på rett sted?»

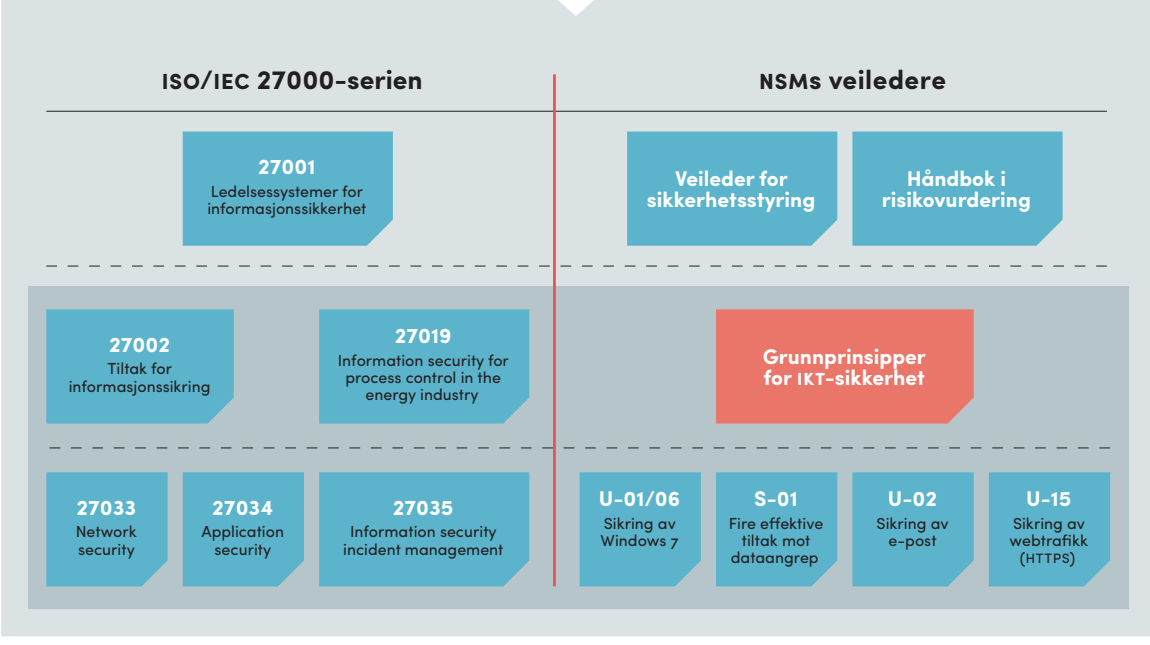


FIGUR 2 - Informasjons- og beslutningsflyt i en virksomhet

RELEVANTE RAMMEVERK, STANDARDER OG VEILEDNINGER VIRKSOMHETER KAN BENYTTE:

- NSM veileder i sikkerhetsstyring
- NSM håndbok i risikovurdering
- ISO/IEC 27001:2017
- ISO/IEC 27002:2017
- Cyber Essentials
- NIST Cyber Security Framework
- CIS CSC Top 20 Security controls

«NSMs grunnprinsipper er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet.»



FIGUR 3 – Deler av NSMs veiledningsmateriale sett opp mot utvalgte standarder i ISO/IEC 27000-serien

Gjennomgående vurderinger for god IKT-sikkerhet

BESLUTT TJENESTEMODELL

Offentlige og private virksomheter ser på IKT og bruken av IKT som en viktig del av virksomheten og realisering av dens strategi. Samtidig har de sett at kostnader, ressursbruk og den generelle avhengigheten til leveranse av IKT-tjenester er økende. Det er derfor et økende fokus på hvordan IKT-området utvikles og hvordan IKT-tjenestene kan leveres, og for mange er konklusjonen å kjøpe dette av en leverandør.
Med tjenesteutsetting menes her at virksomheten velger å anskaffe «varer eller tjenester» fra en ekstern leverandør i stedet for å levere den selv. Dette kan også gjelde kjøp av nye tjenester som skal integreres i IKT-infrastrukturen. Anskaffelse av skybaserte tjenester[8] inngår i denne definisjonen.

Økt behov for sikkerhet medfører også at mange virksomheter, spesielt de med små IT-miljøer, vil ha utfordringer med å implementere mange av sikringstiltakene. For disse aktørene kan ofte løsningen være å sette ut hele eller deler av driften. Dette gir en endring av leveransemodellen og dermed en endring av risikovurderingen for det som tjenesteutsettes.

Virksomheten må sørge for at sikkerhetsnivået opprettholdes eller forbedres i forbindelse med tjenesteutsetting. Kravene til sikring av tjenester satt ut til tredjepart vil i prinsippet ikke være annerledes enn når de leveres av virksomheten selv. De samme kravene må innfris og må reguleres i kontrakter, følges opp og kontrolleres, slik at de ivaretas av tjenesteleverandøren. De tjenester som settes ut må også inkluderes i den resterende porteføljen til virksomheten. Virksomheten må etablere en helhetlig arkitektur og må forstå hvilke funksjoner i det totale systemet som ivaretas hvor i arkitekturen og av hvem.

Når en virksomhet velger å sette ut leveranser er det viktig å kartlegge

Ved en tjenesteutsetting bør det som et minimum stilles krav til leverandøren om å ha:

- Et etablert styringssystem for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017
- Innsyn i sikkerhetsarkitekturen som benyttes for å levere tjenesten.
- Utvikling av sikkerheten i tjenesteproduksjonen og hos leverandøren, i tråd med utvikling i teknologi og trusselbildet over tid.
- En oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres samt grad av mekanismer for segregering fra andre kunder.
- Tilgangsstyring som inkluderer kryptering, aktivitetslogging, fysisk og logisk sikkerhet.
- Sikkerhetsovervåkning egnet til å avdekke hendelser og handlinger i tråd med virksomhetens trusselbilde og relevante trusselaktører.
- Rutiner for hendelseshåndtering, avviks- og sikkerhetsrapportering.
- Krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer.
- At bruk av underleverandører og deres bruk av underleverandører skal godkjennes før iverksetting.
- Hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon.

[8] Med skytjenester menes infrastructure as a service (IaaS), Platform as a service (PaaS) og Software as a service (Saas)

«Ofte er det bare timer fra en sikkerhetsoppdatering slippes fra en leverandør, til det første angrepet oppdages hos NSM NorCERT.»

hvilke lover, krav og regler som gjelder for egen virksomhet både nasjonalt og internasjonalt. Virksomheten bør kartlegge hvilke verdier som eksponeres ved tjenesteutsetting, og vurdere dette opp mot behovet for konfidensialitet, integritet og tilgjengelighet. Virksomheter bør utarbeide et detaljert kravdokument som dekker tjenesteleveransen og alle faser av tjenesteutsettingen det vil si anskaffelsen, forvaltning og driftsfasen samt ved terminering av kontrakten. Det er viktig å være klar over at utsetting av IKT-tjenester ikke bare har en merkantil dimensjon. Alle i virksomheten som påvirkes av utsettingen, må inkluderes både under anskaffelse, i driftsperioden og ved terminering. Det avgjørende er likevel at grunnprinsippene bør følges, uavhengig av om tjenesten leveres internt eller av en tjenesteleverandør.

SENTRALISER OG AUTOMATISER DRIFT OG FORVALTNING

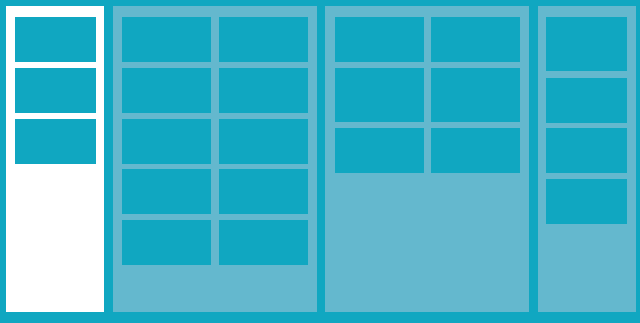
Kompleksiteten i IKT-systemer kombinert med et uoversiktlig trusselbilde, utfordrer forvaltningen av disse. Nye sårbarheter utvikles kontinuerlig, og tiden det tar fra en sårbarhet oppdages til den utnyttes reduseres. Ofte er det bare timer fra en sikkerhetsoppdatering slippes fra en leverandør, til det første angrepet oppdages hos NSM NorCERT. Samtidig må virksomheter holde tritt med den teknologiske utviklingen. Utstyr må byttes ut, nye leverandører må få tilgang og de ansatte ønsker å benytte den siste teknologien og knytte den mot virksomhetens nettverk og tjenester. En forsvarlig livsløpsforvaltning av IKT-porteføljen forutsetter at virksomheter må automatisere og sentralisere drift og forvaltning av IKT-systemer. En effektiv utøvelse av dette vil kreve konsistent, sentralisert og automatisert drift av virksomhetens IKT-systemer. Det holder ikke bare å anskaffe utstyret, det må også legges en plan for hvordan det skal håndteres gjennom levetiden, og hvordan og når det skal erstattes.

Helhetlig forvaltning av IKT og IKT-sikkerhet innebærer blant annet bruk av løsninger hvor man gjenbruker sikkerhetsmekanismer på tvers av ulike plattformer, tjenester og applikasjoner. Det kan ofte være et problem at budsjetter ikke tar høyde for at enheter må skiftes ut, at det trengs personell for å drifte et stadig mer automatisert og komplekst system og at man må følge med på hvilke sårbarheter som må håndteres.

I realiteten vil virksomheter møte kommersielt attraktive og til dels sterke dominerende tjenesteleverandører som i liten grad er villige til å gi tilstrekkelig transparens til å verifisere samsvar med regelverk og anbefalinger.

Der kravene ikke oppnås vil virksomheten ha en risiko og virksomheten må vurdere eventuelle kompenserende tiltak eller hvorvidt tjenesten faktisk skal settes ut.

1. Identifisere og kartlegge



1.1 KARTLEGG LEVERANSER OG VERDIKJEDER

Identifisere og kartlegge leveranser og tilhørende verdikjeder, funksjoner og ressurser som kan ha innvirkning på risiko og valg av sikringstiltak i forbindelse med beskyttelse av virksomhetens IKT-miljø og leveransen av tjenester.

HVORFOR ER DETTE VIKTIG?

Det å kjenne sin egen virksomhet er viktig for å drive effektivt og levere gode tjenester. For kommersielle virksomheter vil det ofte si å ha god inntjening, men for statlige virksomheter er det snakk om å få mest mulig ut av hver skattekrone. Dersom virksomheten ikke har identifisert, prioritert og satt fokus på å beskytte sine viktigste prosesser og funksjoner, kan mange av de viktigste verdiene og understøttende ressurser være eksponert for aktører med onde hensikter eller utilsiktede hendelser. Dersom en virksomhet ikke har oversikt over hele verdikjeden for sine viktigste leveranser kan enkelte deler være godt sikret, mens andre vitale deler kan være åpent eksponert og sårbare for tilfeldige og målrettede angrep. I tillegg til sikring av konfidensialitet og integritet, vil det for de fleste virksomheter være like viktig å ivareta behovet for tilgjengelighet av sine kritiske leveranser.

Kartlegging av leveranser og tjenester vil bidra til at viktige verdikjeder, informasjon og avhengigheter blir kartlagt og prioritert. Dette må tas hensyn til i forbindelse med riktig beskyttelse og vedlikehold av IKT-miljøet, eksempelvis i forbindelse med sikkerhetsdesign, soneinndeling, tilgangsstyring, sikker konfigurasjon, logging og sikkerhetsovervåkning. Det kan også vise seg at virksomheten er avhengig av leveranser og tjenester fra samarbeidspartnere, tjenesteleverandører eller underleverandører, og at disse inngår som en viktig del av virksomhetens verdikjede for å oppnå sikkerhetsmål og resultatmål. Hvis virksomheten ikke klarer å ha oversikt over hvilke data som lagres hvor, bør hele IKT-systemet sikres som en helhet basert på den informasjonen med høyest verdi.

Kunnskapen om leveranser og verdikjeder må forvaltes over tid, noe som kan være krevende i en dynamisk hverdag. Tiden der kunnskap lagres i permer er forbi, og det må fokuseres på digitalisering og automatisering av denne delen av virksomheten også.

NSM har erfart at det er utfordrende for virksomheter å ha kontroll på hvor informasjon befinner seg til en hver tid. Dette gjelder eksempelvis når virksomheter benytter skytjenester eller der informasjonen spres på enheter virksomheten ikke har kontroll på. Her følger to eksempler på utfordringer som kan være relevante for de fleste virksomheter.

SIKKERHETSKOPI AV MOBILE ENHETER

Flere virksomheter tillater at ansatte benytter egne enheter til å forvalte virksomhetens informasjon. Virksomheten må da også være klar over at den enkeltes brukers forvaltningsregime også kan påvirke hvor virksomhetens informasjon lagres. Eksempelvis kan en Apple bruker velge å ta en sikkerhetskopi av hele telefonen til iCloud eller til en lokal PC via iTunes slik at informasjonen da lagres utenfor virksomhetens kontroll.

SØKBARE PERSONDATA I SØKEMOTORER

Bruken av maskingenererte, «private» nettadresser har tidligere vært ansett som akseptabel sikkerhet og risiko, vurdert av den enkelte virksomhet og sektor. Slike direktelinker brukes ofte for å la brukere se for eksempel kvitteringer, fakturaer eller andre sensitive dokumenter, uten at brukeren må logge seg inn hos virksomheten det gjelder. Microsoft endret i 2017 hvilke kilder søkemotoren Bing bruker for sin indeksering. Dette medførte at innholdet på maskingenererte, personlige direktelinker endte opp søkbare i Bing og at virksomheten ikke har kontroll på informasjonen.

1.1 ANBEFALTE TILTAK

ID	BESKRIVELSE
1.1.1	Identifiser virksomhetens prioriterte mål og strategi, og hvilke regelverk, bransjenormer og avtaler som stiller krav til sikring av IKT-systemene. Dette er styrende for virksomhetens risikoprofil og derved hvilke sikkerhetsprioriteringer og sikringstiltak virksomheten gjennomfører.
1.1.2	Identifiser virksomhetens prioriterte leveranser og tilknyttede prosesser og aktiviteter basert på mål og strategi. Dette innebærer å se på hvilke verdikjeder som inngår i leveransene, hvem som eier leveransene og hvilke interne og eksterne avhengigheter virksomheten har. De interne eller eksterne aktiviteter virksomheten avhenger av for å sikre IKT-systemene, funksjoner eller organisasjonsledd bør kartlegges.
1.1.3	Kartlegg IKT-systemer, kritiske forretningsroller og informasjon, og gruppér i kritikalitetsnivåer. Kritikalitet er en vurdering av forretningsmessig påvirkning. Den bør beskrive krav til leveranser og konsekvenser dersom et system ikke fungerer eller informasjon kommer på avveie eller blir misbrukt. Kritikalitetsinndelingen skal benyttes for å forstå konsekvensen av en sikkerhetstruende hendelse mot systemet.
1.1.4	Kartlegg organisatorisk informasjonsforvaltning, kommunikasjon og dataflyt i virksomheten. Virksomheten må ha kontroll over hvor virksomhetskritisk informasjon befinner seg. Etabler oversikt over systemflyt (system flowcharts) og modeller som beskriver forholdet mellom entiteter for å illustrere hvordan informasjon flyter gjennom systemet. Dette vil være viktige for å kunne kontrollere dataflyt mellom ulike soner i virksomheten. Både dataflyt mellom komponenter (internt i systemer), mellom systemer og mellom soner bør beskrives.

1.2 KARTLEGG ENHETER OG PROGRAMVARE

Aktivt spore og kartlegge alle maskinvareenheter, programvare og tjenester på nettverket for å skaffe oversikt over autoriserte (og uautoriserte enheter) og ha kontroll på gjeldende konfigurasjon.

HVORFOR ER DETTE VIKTIG?

Angripere er kontinuerlig på jakt etter nye og ubeskyttede systemer og sårbare versjoner av programvare som kan utnyttes. Angriperne ser også etter enheter (spesielt bærbare) som kobles til og fra virksomhetens nettverk og som mangler sikkerhetsoppdateringer og adekvat herding. Angripere kan dra nytte av ny maskinvare som er installert på nettverket en kveld, men ikke konfigurert og oppdatert med aktuelle sikkerhetsoppdateringer før neste dag. Selv enheter som ikke er synlige fra internett kan utnyttes av angripere som allerede har fått intern tilgang og er på jakt etter sårbare mål. Etter hvert som ny teknologi dukker opp har BYOD («Bring your own device») blitt svært vanlig der virksomheten tillater at ansatte anskaffer mobile enheter. Virksomheter har svært liten eller ingen kontroll på sikkerhetstilstanden til disse enhetene, og svake muligheter til sikkerhetsovervåkning. De kan bli, eller allerede være kompromittert og benyttes til å angripe interne ressurser.

Dårlig forvaltede maskiner vil ha større sannsynlighet for å kjøre unødvendig programvare (noe som kan introdusere potensielle sikkerhetshull) eller kjøre skadevare som er introdusert av en angriper etter et system har blitt kompromittert. Når en maskin først har blitt utnyttet, vil angripere ofte bruke den som et utgangspunkt for å samle sensitiv informasjon fra det kompromitterte systemet og fra andre systemer som den kan kommunisere med. Kompromitterte

maskiner blir i tillegg benyttet som et utgangspunkt for bevegelse rundt i hele nettverket samt i tilknyttede nettverk. På denne måten kan angripere raskt gjøre én kompromittert maskin om til mange. Virksomheter som ikke har en komplett oversikt over hvilke programvare som kjører og skal kjøre i nettverket evner ikke å finne ut om systemer kjører sårbar eller skadelig programvare. De klarer dermed ikke redusere skadepotensialet eller stenge angripere ute.

I praksis kan det være utfordrende for virksomheter å ha full kontroll på hele IKT-infrastrukturen. I valget mellom sikkerhet og behov for leveranser vil virksomheter ofte måtte godta enheter med lavere tillit enn ønsket og gi disse tilgang. Det avgjørende er at virksomheter er på bevisste de strategier som velges og vurderer de funksjonelle behovene opp mot risikobildet. I de tilfeller der virksomheten ikke har kontroll på en gitt type utstyr, eksempelvis der eksterne leverandører benyttes eller hvor utstyret endres hyppig (f. eks. BYOD), må virksomheten være bevisst de sikkerhetsutfordringer det medfører og vurdere kompenserende tiltak som for eksempel forsterket deteksjonsevne, segregering og lavere eksponering ovenfor verdifulle aktiva.

AKTIVABEHOLDNING:

Det bør som et minimum lagres informasjon om nettverksadresser, maskinnavn, formålet med hvert system, en ansvarlig aktiva-eier for hver enhet, og avdelingstilknytning for hver enhet. Beholdningen bør inkludere et hvert system som har en IP-adresse på nettverket, inkludert men ikke begrenset til stasjonære og bærbare datamaskiner, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, IP-telefoner, IoT-enheter, osv.

1.2 ANBEFALTE TILTAK

ID	BESKRIVELSE
1.2.1	Utarbeid en oversikt over maskin- og programvare som er godkjent for bruk i virksomheten ved hjelp av automatiske discovery-verktøy. Denne oversikten over gyldig konfigurasjon, bør overvåkes av verktøy for integritetssjekking for å validere at den ikke har blitt endret. Oversikten bør inkludere eierskap.
1.2.2	Opprettholde en aktivabeholdning av entiteter som er koblet til nettverket for å få en oversikt over virksomhetens gjeldende konfigurasjon.
1.2.3	Etabler verktøy for oversikt over all programvare i hele virksomheten som dekker hvert operativsystem i bruk. Inventarsystemet for programvare bør spore versjon av det underliggende operativsystemet samt programmer som er installert på det. Inventarsystemet for programvare bør knyttes opp til aktivabeholdning av nettverksenheter slik at alle enheter og tilhørende programvare spores fra ett sted.
1.2.4	Automatiser prosessen med å opprettholde en aktivabeholdning. Ta i bruk et automatisert verktøy for å oppdage og samle inn informasjon om enheter i virksomhetens nettverk. Virksomhetens logger kan brukes som støtte til å detektere ukjente systemer i virksomhetens nettverk ved å overvåke avvik fra normaltilstand.

1.3 KARTLEGG BRUKERE OG BEHOV FOR TILGANG

Kartlegge hvilke brukergrupper, brukere og tilgangsbehov som finnes i virksomheten og fastsett retningslinjer og regler for tilgangskontroll ved å etablere en prosess for tilgangsstyring.

HVORFOR ER DETTE VIKTIG?

Når en angriper får tilgang til et IKT-system er ofte det første målet å øke tilgangen. Dette gjøres i stor grad ved å ta over ulike kontoer for å eskalere rettigheter. Hvis alle brukere har tilgang til all informasjon vil kompromittering av én bruker kunne kompromittere hele IKT-systemet. Tilgangen til de ulike delene av IKT-systemet bør derfor deles opp for å redusere skaden av en kompromittering eller utro ansatt. En virksomhet må derfor ha kontroll på de ulike brukerne av virksomhetens IKT-systemer, de kontoene de disponerer og hvilke rettigheter en gitt konto har.

Manglende kontroll på brukerkategorier, brukere og tilgangsbehov vil gjøre det vanskelig å kontrollere og forvalte tilgang til kritiske tjenester og data. Mange brukere kan ha tilgang til systemer og tjenester de ikke har behov for, og med mer rettigheter og privilegier enn de trenger for å gjøre jobben sin. Dette kan føre til brudd på integritet, tilgjengelighet eller konfidensialitet til data og tjenester.

«Når en angriper får tilgang til et IKT-system er ofte det første målet å øke tilgangen.»

Utilsiktet tilgang til informasjon eller tjenester kan fås både gjennom bevisste og ubevisste handlinger. Dette kan påvirke verdikjeder og leveranser og påføre virksomheten økonomiske tap.

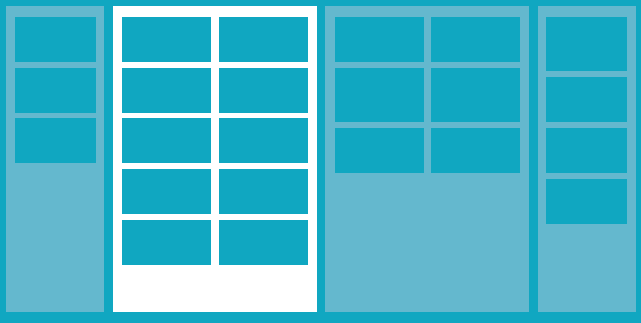
En bevisst handling kan være en ansatt som utnytter de utvidede rettighetene for egen eller andres vinning, for eksempel ved å lese dokumenter han vanligvis ikke har tilgang til. For vide tilganger og rettigheter vil også kunne utnyttes av en eventuell angriper dersom han klarer å ta over kontoen til en bruker, for eksempel ved eskalering av privilegier eller sideveis bevegelse i IKT-miljøet.

En ubevisst handling kan være en ansatt som endrer på innstillinger han ikke skal endre som et resultat av feiltrykk, også kalt «pølsefingre».

1.3 ANBEFALTE TILTAK

ID	BESKRIVELSE
1.3.1	Etabler prosess for vedlikehold av brukere, roller og tilganger slik at dette ivaretas gjennom hele livssyklusen til brukerne, fra opprettelse til avslutning av kontoer.
1.3.2	Kartlegg og fastsett retningslinjer og regler for aksesskontroll basert på minste privilegiums prinsipp.
1.3.3	Kartlegg og definer de ulike brukerkategorier som finnes i virksomheten for å definere tilgangsnivåer og behov for oppfølging og kontroll. Eksempler på brukerkategorier kan være: • «Vanlige brukere» med behov for tilgang til kontorstøttesystemer. • Brukere med behov for utvidede rettigheter eller privilegier • Administratorbrukere • Systembrukere • Leverandører og konsulenter
1.3.4	Kartlegg brukere, brukerkontoer (inkludert systemkontoer) og hvilke tjenester de ulike brukerne har behov for aksess til. Dette må forvaltes over tid og bør, i tillegg til de brukere som forvaltes i en katalogstruktur (eksempelvis AD eller LDAP), også inkludere system- og administratorkontoer som for eksempel administratorkontoer til databaser. Aksessbehov bør revideres jevnlig.
1.3.5	Kartlegg roller og ansvar knyttet til IKT-sikkerhet for hele organisasjonen samt tredjeparts interessenter (f. eks. leverandører, kunder, partnere) og etabler dette der det mangler.
1.3.6	Godkjenning av brukerrettigheter må kunne spores til en rolle og en ansvarlig person.

2. Beskytte



2.1 IVARETA SIKKERHET I ANSKAFFELSE- OG UTVIKLINGSPROSESSER

Etablere prosesser for anskaffelse og utvikling slik at varer og tjenester som innføres og integreres i virksomheten kan stoles på og ikke inneholder kjente sårbarheter og sikkerhetshull.

HVORFOR ER DETTE VIKTIG?

Dersom en virksomhet anskaffer eller utvikler komponenter og systemer som ikke tilfredsstiller kvalitetskrav eller ikke er godt integrert i virksomhetens øvrige sikkerhetsarkitektur, kan dette føre til innføring av sårbarheter og sikkerhetshull. En angriper benytter som oftest enkleste vei inn og hvis det finnes sikringstiltak som enkelt kan omgås vil en angriper lete etter, og utnytte, dette. Tilsvarende må tjenester som skal anskaffes og integreres i virksomhetens øvrige IKT-infrastruktur ivareta virksomhetens krav til sikkerhet, både når det gjelder selve tjenesten og integrasjonen.

Sårbarheter kan innføres på bakgrunn av at kvaliteten på fremskaffelsesprosessen ikke er god nok og virksomheten innfører komponenter eller tjenester med manglende sikkerhetsfunksjonalitet, manglende sikkerhetsrettinger eller konfigurerer komponenter feil. Disse sårbarhetene kan enten skyldes feil på produktet som en angriper kan utnytte, eller plantede sårbarheter fra en trusselaktør. Sårbarheter kan også innføres i etterkant av anskaffelsen gjennom oppdateringer eller vedlikehold.

Hvis virksomheten i tillegg mangler gode prosesser for test, verifisering og implementering av produkter eller tjenester, vil sannsynligheten være stor for at sårbarhetene ikke blir oppdaget eller at virksomhetsprosesser stopper opp. Kostnaden ved å rette opp i dette i etterkant er ofte høyre enn kostnaden ved å implementere gode prosedyrer for test og idriftsetting.

«En angriper benytter som oftest enkleste vei inn og hvis det finnes sikringstiltak som enkelt kan omgås vil en angriper lete etter, og utnytte, dette.»

Publiserte sårbarhetsvarsler viser at mange sårbarheter i programvare skyldes dårlig kvalitetskontroll av produktet. Dette kan skyldes mangel på forståelse og kunnskap om hvordan programvare kan misbrukes.

Standardinnstillinger som er designet for det godes hensikt kan i neste nu misbrukes av en angriper – dette er det ikke tenkt på. Problemene er ofte knyttet til mangel på autorisering, autentisering og integritetssikring.

2.1 ANBEFALTE TILTAK

ID	BESKRIVELSE
	Anskaffelse og utvikling:
2.1.1	Integrer sikkerhet i virksomhetens prosess for anskaffelse og utvikling, fra kravanalyse, prekvalifisering og design, til testing og idriftsetting. Fastsett krav til informasjonssikkerhet basert på anerkjente standarder og rammeverk slik at nødvendige aspekter relatert til konfidensialitet, integritet og tilgjengelighet adresseres i forbindelse med anskaffelse og utvikling. I tillegg til sikkerhetskrav for selve produktet eller tjenesten, bør det også stilles krav til funksjonalitet, analysekapasitet, overvåkbarhet, styring og integrasjon, herunder samsvar med virksomhetens sikkerhetsarkitektur. Kravene bør inkluderes i kontrakt for måling av etterlevelse.
2.1.2	Velg en leverandør av god kvalitet der virksomheten kan stole på leverandørkjeden og de tjenestene som leveres gjennom hele livsløpet til produktet eller tjenesten. Behovet for vedlikehold gjør at en vesentlig del av utfordringen vil ligge i livsløpet til komponenten. Leverandørens tilgang til IKT-systemet og oppgraderinger bør derfor reguleres og kontrolleres og ideelt sett unngås.
2.1.3	Kjøp moderne og oppdatert maskin- og programvare slik at den nyeste og mest tidsaktuelle sikkerhetsfunksjonaliteten følger med og nødvendige sikringstiltak kan benyttes
2.1.4	Planlegg livsløpet til materiellet ved anskaffelse og legg en plan for når materiell skal skiftes ut før det blir utdatert. Dette må derfor inkluderes i budsjettprosessen.
2.1.5	Foretrekk sertifiserte og evaluerte produkter gjennomført av en tiltrodd tredjepart. Dette øker sannsynligheten for at produktet oppfører seg som tiltenkt og ikke inneholder ukjente feil eller mangler. Et eksempel på et slikt regime er Common Criteria[9]. I tillegg bør produktene integreres i eksisterende IKT-miljø slik at kvalitet og tillit til sikkerhetskomponenter opprettholdes.
	Test og idriftsetting:
2.1.6	Benytt separate miljøer for utvikling, test og produksjon slik at operative virksomhetsprosesser og produksjonsdata ikke blir påvirket ved feil i utvikling- og testløp.
2.1.7	Beskytt integritet og konfidensialitet til testdata slik at sikkerhetstester blir gjennomført så reelt som mulig og sensitiv informasjon ikke kommer på avveie. For å redusere risiko kan konstruerte eller anonymiserte/ubrukelige datasett fra produksjon benyttes så sant det er innenfor rammene av en fortsatt valid test.
2.1.8	Gjennomfør tilstrekkelig med testing gjennom hele anskaffelses- og utviklingsløpet slik at feil og mangler rettes opp før idriftsetting. Dette inkluderer blant annet enhetstesting, integrasjonstesting, systemtest, akseptansetest, pilottest, inntrengingstest og stresstest.

Det kan for virksomheter være utfordrende å planlegge når materiell bør skiftes ut. Kostnader vil ofte påløpe, og mange virksomheter definerer utdatert som «at produktet ikke virker lenger» eller at det ikke kan løse det funksjonelle behovet.

Materiell bør vurderes skiftet ut når produktet ikke lenger understøtter adekvat og tidsmessig sikkerhet.

[9] Common Criteria er en internasjonal standard for evaluering av sikkerhetsegenskaper i IT-produkter og systemer. Den definerer et rammeverk for overvåking av evalueringer, syntaks for å spesifisere sikkerhetskravene som skal oppfylles, og en metode for å vurdere disse kravene, og er ofte definert som en forutsetning for innkjøp.

2.2 IVARETA SIKKER DESIGN AV IKT-MILJØ

Designe en helhetlig og enhetlig sikkerhetsarkitektur som ivaretar ønsket sikkerhetsnivå gjennom gode sikkerhetsfunksjoner, sikkerhetsstrukturer og behov for etterprøvbarhet.

HVORFOR ER DETTE VIKTIG?

En angriper vil til en hver tid gå minste motstands vei for å angripe et IKT-system. I hjemmet hjelper det lite med den tykkeste utgangsdøren med den beste låsen hvis vinduet i andre etasje står åpent. På samme måte som vi sikrer et hus må også et IKT-system designes og bygges på en sikker måte. Vindu- og dørlås, alarmsystem og vaktselskap er alle sikkerhetsfunksjoner man kan benytte for å sikre hjemmet tilstrekkelig. Et IKT-system er bygd opp av tilsvarende sikkerhetsfunksjoner, som kryptografiske moduler, katalogtjenester og brannmurer. Hver av disse funksjonene, som kan ses på som enkeltmoduler i systemet, må konfigureres på en sikker måte.

Gjenbruk av sikkerhetsfunksjoner, som brukerdatabaser, forvaltningsverktøy og systemovervåkning er viktig for å oppnå en helhetlig sikkerhetstilnærming. Den motsatte tilnærmingen, det vil si å utvikle hver node og server som en unik og skreddersydd løsning er både kostbar og arbeidskrevende, og reduserer ressursene fra viktige sikkerhetsproblemer. Målet må være å kunne gjenbruke mekanismer slik at de konfigureres færrest mulig steder og at sikkerhetsmekanismer ikke har mer funksjonalitet eller kompleksitet enn nødvendig. Ethvert produkt, uavhengig av sine overlegne individuelle kvaliteter, vil introdusere sårbarheter i et system hvis det ikke integreres på en

god måte. Samtidig bør systemet baseres på prinsippet «sikkerhet i dybden», der ulike sikkerhetsfunksjoner overlapper i funksjonalitet.

Sentrale elementer og funksjoner i et IKT-miljø som må implementeres og sikres, og fungere sammen.

- Operativsystem
- Database
- Nettverksenheter
- Konfigurasjonsstyringsverktøy
- Katalogtjenester
- Kryptografiske moduler
- Digitale sertifikater og Public Key Infrastructure(PKI)
- Brannmur
- Antivirus/anti-skadevare
- Verktøy for systemovervåkning
- Verktøy for sikkerhetskonfigurasjoner
- Intrusion detection(IDS) og protection(IPS) systems
- Funksjonalitet for sikkerhetskopiering og gjenoppretting

2.2 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.2.1	Etabler og vedlikehold en helhetlig sikkerhetsarkitektur som ivaretar en sikker og forsvarbar IKT-infrastruktur og gjenspeiler krav til leveranser. Påse at alle nødvendige og grunnleggende sikkerhetsteknologier omfattes med hensyn til valg av maskinvare, operativsystem, nettverksenheter, databaser og brannmurer.
2.2.2	Påse at systemkomponenter håndhever alle komponentspesifikke sikkerhetsfunksjoner som trengs av den aktuelle komponenten, for eksempel at komponentens pålogging, tilgangskontroll, logging, administrasjon, kodekontroll, ressursstyring og tilgjengelighetsfunksjoner ivaretas.
2.2.3	Bygg IKT-systemet fra systemkomponenter som er modulbaserte og standardiserte slik at de gjenbrukes når det er mulig, særlig når det gjelder nettverkssegregering og roller. Påse at sikkerhetsfunksjonaliteten til systemet integrerer og samarbeider godt, for eksempel ved at komponentene gjenbruker brukeridentifikasjonene som er definert av katalogtjenesten, i stedet for å implementere sine egne komponent- eller applikasjonsspesifikke brukeridentiteter (unngå multiple masterdatabaser for identiteter).
2.2.4	Del IKT-systemet i veldefinerte logiske ressursrom som primært er definert av katalogtjenesten for å binde sammen brukere og ressurser. Katalogtjenesten bør ta høyde for både prosessbaserte (prosjekt) og organisatoriske skiller.
2.2.5	Segreger IKT-infrastrukturen i sikkerhetssoner for å separere informasjon med ulik verdi og behov for brukertilgang, eksponerings- og kommunikasjonsbehov, funksjon og rolle, samt for å isolere utstyr med ulike sårbarheter og ulik tillit. Som et minimum bør det etableres egne soner for virksomhetens kontrollerte klienter, utstyr uten tillit og virksomhetens tjenester, eksempelvis egne servere. Tjenester eksponert på internett eller fra nettverk med lav tillit bør separeres fra øvrige tjenester. Eksempler på enheter med lav tillit er virksomhetens nettserver, BYOD-enheter og gjestebrukere. I tillegg bør systemadministrasjon utføres fra egne soner.
2.2.6	Reguler tilgang til tjenester basert på behovet for autentisering. Et eksempel er en bruker som logger seg på via en BYOD-enhet (virksomheten kjenner bare bruker og ikke enhet), vil gi tilgang til færre tjenester enn en bruker som logger seg på via en forvaltet enhet (virksomheten kjenner både klient og bruker).
2.2.7	Design et robust og motstandsdyktig IKT-miljø for å ivareta tilgjengelighet til kritiske funksjoner og leveranser.

2.3 IVARETA EN SIKKER KONFIGURASJON (AV MASKIN- OG PROGRAMVARE)

Konfigurer og tilpass maskin- og programvare slik at det tilfredsstiller virksomhetens behov for drift og sikkerhet.

HVORFOR ER DETTE VIKTIG?

De fleste systemkomponenter leveres med en standardkonfigurasjon utviklet av enten produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. Standardinnstillinger, åpne tjenester og porter, standardkontoer eller passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er tilstrekkelig konfigurert har større sannsynlighet for å introdusere sårbarheter som en angriper kan utnytte, for eksempel ved kjøring av utdaterte tjenester eller programmer som det ikke er funksjonelt behov for. Virksomheter må derfor herde systemkomponenter, eksempelvis ved å minimere funksjonalitet og fjerne standardinnstillinger og passord.

2.3 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.3.1	Installer og konfigurer systemet med kun nødvendig funksjonalitet for å understøtte virksomhetens forretningsprosesser. Kun autorisert programvare bør kjøre på virksomhetens enheter.
2.3.2	Etabler standard sikkerhetskonfigurasjoner av operativsystemer og programmer som kan installeres på virksomhetens enheter. Konfigurasjonen bør gjennomgås og oppdateres med jevne mellomrom for at den skal være oppdatert i forhold til de nyeste sårbarheter og angrepsvektorer. Konfigurasjonene bør kun kunne endres av autoriserte brukere.
2.3.3	Den sikre konfigurasjonen bør anses som en verdi og beskyttes deretter. Integriteten til konfigurasjonene bør sjekkes jevnlig og automatisk. Planlagte endringer bør følge virksomhetens prosess for endringshåndtering. Endringer i komponentens konfigurasjon avdekket gjennom automatiserte kontroll, og som ikke finnes å ha rot i en logget eller sentralstyrt endring, bør inngå som grunnlagsdata i sikkerhetsovervåkning og analyse.
2.3.4	Utfør all installasjon og fjernadministrasjon av servere, arbeidsstasjoner, nettverksenheter og lignende utstyr over tiltrodde kanaler.
2.3.5	Endre alle standardpassord på systemer før produksjonssetting. Dette inkluderer applikasjoner, operativsystemer, rutere, brannmurer og aksesspunkter.
2.3.6	Sørg for god konfigurasjonsstyring av den sikre konfigurasjonen slik at alle systemkomponenter, og nye systemer som produksjonsettes, innehar gyldige sikkerhetskonfigurasjon.
2.3.7	Implementer et verktøy for konfigurasjonsstyring som automatisk vil påtvinge og overskrive konfigurasjonsinnstillinger til systemer ved regelmessige intervaller. Verktøy bør melde fra dersom konfigurasjonen på enheter ikke samsvarer med gyldig konfigurasjon.
2.3.8	Blokker kjøring av ikke-autoriserte programmer («hvitelisting»). Bruk verktøy som Windows AppLocker for å kontrollere at sluttbrukere kun får kjøre godkjente applikasjoner. Blokker spesielt programmer utenfor godkjente mapper og på flyttbare media, som for eksempel på CD-er og minnepinner.
2.3.9	Bruk klientbrannmur regulerer innkommende trafikk og logger sikkerhetsrelevante hendelser. Inspiser loggfilene regelmessig.
2.3.10	Bruk antivirus/antiskadevare. Antivirus oppdager og blokkerer kjent skadevare som blant annet utnytter sårbarheter i e-postklienter og dokumentlesere. Fortrinnsvis bør man bruke et produkt som kan styres sentralt.
2.3.11	Aktiver kodebeskyttelse mot ukjente sårbarheter. Benytt kodebeskyttelsesfunksjoner som DEP (Data Execution Prevention), SEHOP (Structured Exception Handler Overwrite Protection), ASLR (Address Space Layout Randomization) og EMET (Enhanced Mitigation Experience Toolkit) som styrker systemet mot sårbarheter i applikasjoner og operativsystemet selv når det ikke finnes en oppdatering.

Manglende herding av systemkomponenter er ofte en viktig medvirkende årsak til at angripere får fotfeste i IKT-infrastrukturen, og er en viktig del av den totale informasjonssikkerheten. Operativsystemet på klientmaskinen, brukerdatabasen, brannmuren, skytjenesten, e-postklienten og nettverkssvitsjen er eksempler på systemkomponenter som må herdes. Disse komponentene må installeres og konfigureres på en sikker måte slik at ønsket funksjonalitet er aktivert og uønsket eller usikker funksjonalitet er deaktivert.

Selv om en sikker konfigurasjon er utviklet og installert, må den også

Utvikle og distribuere konfigurasjonsinnstillinger med god sikkerhetsfunksjonalitet er en kompleks oppgave, langt utenfor den enkelte brukers evne. For å ta gode valg må potensielt flere tusen innstillinger vurderes, bestemmes og implementeres på alle deler av IKT-infrastrukturen. Å etablere en sikker konfigurasjon vil kreve teknisk kompetanse på de komponentene som skal herdes, som vil medføre at mange virksomheter må støtte seg på eksterne aktører.

NSM utarbeider profiler for herding av enkelte sentrale systemkomponenter. Profiler er også tilgjengelige fra andre myndigheter og organisasjoner, eksempelvis Center for Internet Security. Benchmarks Division. Tilsvarende profiler distribueres også av enkelte programvare- og operativsystemleverandører.

Se mer på :

https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledninger-for-systemteknisk-sikkerhet

kontinuerlig forvaltes for å forhindre at sikkerheten svekkes over tid. Virksomheten må håndtere at maskin- og programvare oppgraderes eller oppdateres, nye sikkerhetsproblemer rapporteres, konfigurasjonen endres for å tillate nye komponenter eller systemet må understøtte nye operasjonelle krav.

2.4 HA KONTROLL PÅ IKT-INFRASTRUKTUR

Kontrollere og beskytte virksomhetens IKT-infrastruktur mot interne og eksterne trusler.

HVORFOR ER DETTE VIKTIG?

Tilkobling av virksomhetens IKT-infrastruktur til internett eller andre nettverk utenfor virksomhetens kontroll eksponerer systemene og teknologier for nye angrepsflater. Virksomhetens nettverk strekker seg ofte ut over kontorlokalet, og

«Er nettverkene feil konfigurert kan selv et nettverkspunkt i en usikker sone som kantinen være nok til å gi en angriper tilgang.»

gjør det utfordrende å definere den fysiske utbredelsen. En virksomhet kan ha flere lokasjoner, tjenester kan være satt ut til leverandører eller de ansatte har behov for mobile enheter eller å kunne arbeide hjemmefra eller på reise.

Virksomheter må planlegge for at klienter overtas av angripere. I tillegg til utro tjenere, kan leverandører med aksess til IKT-infrastrukturen eller manglende fysisk sikring medføre at en angriper får tilgang til IKT-systemet. Er nettverkene feil konfigurert kan selv et nettverkspunkt i en usikker sone som kantinen være nok til å gi en angriper tilgang.

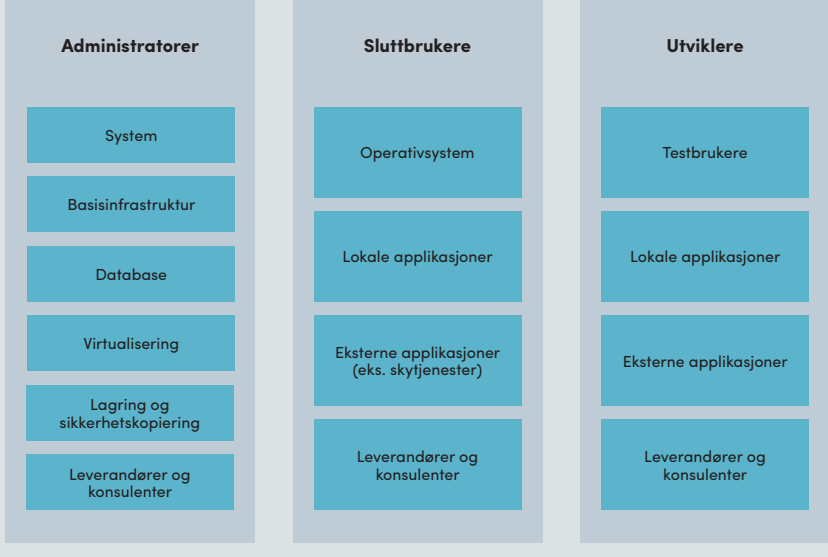
Virksomhetens IKT-infrastruktur må derfor sikres mot både interne og eksterne trusler. Hensikten med sikringen er å hindre en angriper tilgang og redusere skaden skulle en angriper få fotfeste i nettverket. En virksomhet må ha kontroll på nettverkenes utstrekning og IKT-infrastrukturen må beskyttes i henhold til eksponering og virksomhetens risikoprofil. Inndeling i sikkerhetssoner oppnås ved å segregere og/eller segmentere IKT-infrastrukturen. Med segregering menes fysisk adskillelse og segmentere menes logisk adskillelse.

FIGUR 4 – Eksempler på kontoer med ulike rettigheter som må forvaltes.

2.4 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.4.1	Segreger og segmenter virksomhetens IKT-infrastruktur inn i nettverk og soner som gjenspeiler virksomhetens risikoprofil og sikkerhetssoner. Trafikk for å administrere IKT-infrastrukturen bør skilles fra øvrig virksomhetsnettverk og autoriseres og autentiseres.
2.4.2	Kommunikasjon mellom segmenter bør reguleres ved å filtrere nettverkstrafikken slik at det representer virksomhetens sikkerhetssoner og behov for dataflyt.
2.4.3	Beskytt trådløse nettverk med sterke sikkerhetsmekanismer for å autentisere og autorisere brukere, samt beskytte informasjonen som bæres av nettverket.
2.4.4	Benyttes virksomhetsstyrte klienter bør disse segregeres til eget nett der også klienten autentiseres.
2.4.5	Minimer antall nettverkstilkoblinger ved å deaktivere og fysisk koble fra nettverkskabler fra ubrukte nettverksporter, nettverkskort, nettverksprotokoller eller nettverksapplikasjoner.
2.4.6	Benytt krypterte forbindelser, eksempelvis VPN, for kommunikasjon utenfor egne nettverk slik at virksomhetens sikkerhetsmekanismer kan utnyttes.
2.4.7	Ansatte som skal ha tilgang til virksomhetens tjenester fra en ekstern lokasjon bør benytte forvaltede enheter eller forvaltet programvare.

NSM erfarer ofte at virksomheter ikke har full kontroll på ulike kontoer i virksomheten. Selv i de tilfeller der Microsoft AD eller tilsvarende er implementert på en god måte, finnes det brukere som ikke forvaltes av katalogtjenesten og kan benyttes til angrep. Katalogtjenester ivaretar bare deler av de kontoene som eksisterer i en virksomhet. I flere tilfeller har NSM sett at administrator- eller testkontoer til enten databaser eller underliggende operativsystemer på databaseserveren kan utnyttes av angripere for å få tilgang til verdifull informasjon eller kritiske systemer.



2.5 HA KONTROLL PÅ KONTOER

Aktivt administrere livssyklusen til system- og applikasjonskontoer for å redusere muligheten for at angripere utnytter dem. Dette gjøres gjennom å ha kontroll på kontoers opprettelse, bruk, dvale og deaktivering/sletting.

HVORFOR ER DETTE VIKTIG?

Angripere har ofte som hensikt å få tilgang til en legitim bruker. Med denne ønsker angriperen å elevere rettigheter eller ta over andre kontoer med utvidede rettigheter.. Dette gjør det vanskelig for nettverksovervåkere å skille mellom legitime brukere og faktiske angripere basert på brukerens oppførsel i nettverket. Kontoer til terminerte leverandører og ansatte, hvor kontoen har blitt satt inaktiv og hvor rettigheter ikke har blitt fjernet, har ofte blitt utnyttet på denne måten. Enkelte ondsinnede innsidere eller tidligere ansatte har i tillegg aksessert etterlatte kontoer lenge etter utløp av kontrakter og fått uautorisert tilgang til virksomhetens IKT-systemer og sensitive data.

2.6 KONTROLLER BRUK AV ADMINISTRATIVE PRIVILEGIER

Kontrollere, korrigere, og spore tildeling, bruk og konfigurering av administrative rettigheter for å hindre misbruk av datamaskiner, nettverk og applikasjoner.

HVORFOR ER DETTE VIKTIG?

En av primærmetodene angripere benytter for å spre seg og få kontroll i

2.5 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.5.1	Sørg for at alle kontoer er personlige og har en utløpsdato. Opprettholden god dialog med bruker av konto med hva som overvåkes og logges relatert til kontoen.
2.5.2	Etabler og etterlev en prosess for å fjerne systemtilgang ved å deaktivere kontoer umiddelbart etter at en ansatt (fast eller midlertidig) slutter. Deaktiver fremfor å slette kontoer slik at revisjonsspor bevares. Dette må gjøres i henhold til gjeldende lover og regelverk.
2.5.3	Overvåk kontobruk for å detektere bruk av sovende kontoer, og varsle brukerens leder. Deaktiver slike kontoer hvis de ikke er nødvendige, eller dokumenter og overvåk unntak (f.eks. en leverandørs vedlikeholdskonto som brukes for å gjenopprette et system eller opprettholde kontinuitet). Eventuelt aktiver slike kontoer kun i det tidsrommet de er nødvendige. Koble aktive medarbeidere mot hver konto og deaktiver kontoer som ikke er tilordnet en gyldig ansatt.
2.5.4	Konfigurer tilgang for alle kontoer gjennom et sentralisert punkt for autentisering, for eksempel Active Directory eller LDAP. Virksomheter bør ha et spesielt fokus på de kontoer driftsmiljøet trenger for å forvalte IKT-infrastrukturen, slik at prinsippene for autentisering også gjelder for nettverks- og sikkerhetsenheter, databaser og servere.
2.5.5	Bruk multi-faktor autentisering for å autentisere brukere. Som et minimum bør det implementeres på brukerkontoer som har tilgang til sensitive data eller systemer, samt brukere med administrative rettigheter. Multi-faktor autentisering kan eksempelvis oppnås ved hjelp av smartkort, sertifikater eller engangspassord (OTP). Der multi-faktor autentisering ikke støttes, bør brukerkontoer bli pålagt å bruke lange, sterke passord på systemet.
2.5.6	Gjennomgå alle systemkontoer og deaktivere kontoer som ikke kan knyttes til en forretningsprosess og ikke har en eier.

en virksomhets nettverk er ved misbruk av administrative privilegier. To svært vanlige angrepsteknikker utnytter ukontrollert bruk av administrative privilegier. Den første metoden går ut på å lure en privilegert bruker til å åpne et e-postvedlegg, laste ned en fil fra en ondsinnet nettside eller gå inn på en nettside som inneholder skadevare som automatisk kan utnytte nettlesere. Filen eller utnyttelsen inneholder kjørbar kode som kjøres på offerets maskin, enten automatisk eller ved å lure brukeren til å godta kjøring av den. Hvis offerets klient innehar en sårbarhet som kan utnyttes for rettighetseskalering, eller dens brukerkonto har tilstrekkelige privilegier, kan angriperen ta fullstendig kontroll over maskinen og installere tastetrykklogging, sniffere og programvare for fjernaksess for å finne administrative passord og annen sensitiv data.

Den andre vanlige metoden brukt av angripere er eskalering av privilegier ved å gjette eller knekke passordet til en administratorbruker. Hvis administrative tilganger er distribuert ut løst og bredt i virksomheten, eller hvis administratorpassord er identiske til dem som benyttes på mindre kritiske systemer, vil det være enklere for en angriper å oppnå administrative privilegier. Det vil da være flere kontoer kan benyttes som inngangsport for en angriper som ønsker å få kontroll over et system.

2.6 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.6.1	Personer med administrative privilegier (operatører) bør bruke separate kontoer når de utfører systemadministrasjon.
2.6.2	Minimer bruken av administrative rettigheter og bruk administrative kontoer kun når det er påkrevet. Fokuser revisjon på bruk av administrative privilegerte funksjoner og monitorer systemene for avvikende atferd og eskalering av rettighetsnivå. I de tilfeller sluttbruker har behov for administrative privilegier, bør dette håndteres særskilt og kompenserende tiltak vurderes.
2.6.3	Administratorer bør påkreves å logge på systemer med en personlig, ikke-administrativ konto. Deretter bør transisjonen til administrative privilegier utføres.
2.6.4	Etabler ulike administratorkontoer til de ulike delene av IKT-infrastrukturen som skal forvaltes slik at kompromittering av en administratorkonto ikke gir fulle rettigheter til å endre hele infrastrukturen.
2.6.5	Administratorer bør benytte dedikerte maskiner for alle administrative oppgaver, eller oppgaver som krever forhøyede tilganger. Maskinen bør isoleres fra virksomhetens primære nettverk. Maskinen bør ikke benyttes til å lese privat e-post, utarbeide dokumenter eller ha mulighet til å surfe på internett.
2.6.6	Bruk multi-faktor autentisering for å autentisere administrative brukere.
2.6.7	Utfør all fjernadministrasjon av servere, arbeidsstasjoner, nettverksenheter, og lignende utstyr over sikre kanaler. Protokoller som telnet, VNC, RDP, eller andre som ikke aktivt støtter sterk kryptering bør bare brukes hvis de er utført over en sekundær, kryptert kanal, for eksempel TLS eller IPsec.

2.7 KONTROLLER DATAFLYT

Kontrollere informasjonsflyten inn til og ut av virksomhetens nettverk og mellom sikkerhetssoner slik at systemer ikke fritt kan kommunisere med hverandre.

HVORFOR ER DETTE VIKTIG?

Angripere fokuserer på å utnytte systemer de kan nå gjennom internett, ikke bare via eksponerte tjenester og servere, men også arbeidsstasjoner, bærbare og mobile enheter som ligger innenfor virksomhetens barrierer. De utnytter svakheter i konfigurasjon og sikkerhetsarkitektur funnet i systemer, nettverkskomponenter eller klienter med tilgang til internett for å få tilgang til virksomheten. Angripere søker etter nettverk tilgjengelige utenfra med sårbare eksponerte tjenester. Kjente eksempler er feilaktig konfigurerte nett- og e-postservere, fil- og printtjenester og andre tjenester konfigurert med standardinnstillinger. Aktører søker da etter disse tjenestene, benytter standard brukernavn og passord eller prøver kjente og ukjente sårbarheter. Deretter, med den tilgangen dette gir, beveger angriperen seg i virksomhetens nettverk for å etablere fotfeste og få tilgang til virksomhetens verdier. I tillegg treffer flere angrep virksomheten via nettverkene til samarbeidspartnere, ved at angripere hopper fra en virksomhet til en annen gjennom tillatte åpninger i en virksomhets perimetersikring.

Mange angrep gjennomføres gjennom nettverk som internett, mens andre er basert på tyveri eller kopiering av enheter som bærer informasjonen, eksempelvis klienter eller minnepinner. Felles for de fleste av disse, er at informasjonseieren ikke er kjent med at informasjonen kompromitteres siden virksomheter ikke overvåker dataflyten. En virksomhet bør ha kontroll på data som flyter gjennom virksomhetens perimetre og mellom sikkerhetssoner, både fysisk og elektronisk.

Virksomhetens sikring av ytre perimetre eksponert mot internett, og mellom sikkerhetssoner bør bygges etter prinsippet «sikkerhet i dybden» og baseres på brannmurer, proxyer, DMZ-

2.7 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.7.1	Benytt brannmurer med logging for å filtrere og kontrollere trafikken mellom de ulike sikkerhetssonene og mot internett ved kun å tillate ønsket trafikk mellom sonene. Brannmurregler bør ha en ansvarlig og beskrivelse av begrunnelse for åpning og bør revideres jevnlig.
2.7.2	Bruk applikasjonsbrannmurer foran alle kritiske servere for å validere trafikken som går til serverne. Uautorisert trafikk bør blokkeres og generere en alarm.
2.7.3	Vurder bruk av proxy-tjenester for å styre visse typer trafikk gjennom virksomhetens overvåkningsverktøy. Eksempelvis bør virksomhetens mobile tjenester rutes via virksomhetens nettverk for å kunne benytte de sikkerhetsmekanismene som eksisterer i de interne nettverkene.
2.7.4	Kommunikasjon til kjente, ondsinnede IP-adresser bør hindres eller begrenses (svartelisting), alternativt bør tilgang begrenses til nettsider man stoler på (hvitelisting).

soner og nettverksbaserte deteksjons- (IDS) og beskyttelsessystemer (IPS). Dette for å kontrollere trafikken gjennom nettverksperimetere og mellom sikkerhetssoner ved å kontrollere innholdet for angrep og se etter kompromitterte enheter.

2.8 BESKYTT DATA I RO OG I TRANSITT

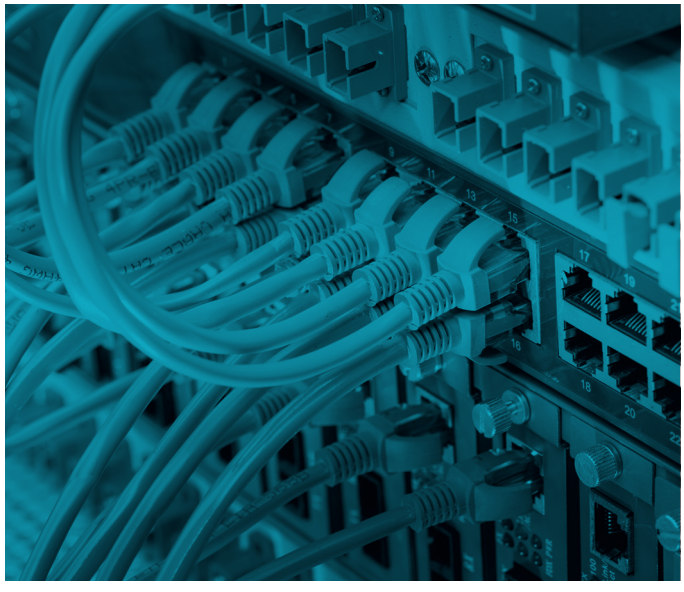
Beskytte virksomhetens data i ro på ulike lagringsmedium og når den formidles over ulike informasjonskanaler.

HVORFOR ER DETTE VIKTIG?

Kryptering er en forutsetning for sikring av dagens IKT-systemer. En virksomhet forvalter informasjon av ulik verdi som vil ha ulikt behov for beskyttelse. Denne informasjonen lagres på og overføres over ulike medium med ulik tillit, og på lokasjoner der virksomheten har varierende kontroll. Alle ansatte bør ha kjennskap til de regler som gjelder for informasjonsbeskyttelse i virksomheten. Den økte digitaliseringen og bruk av tredjepartsleverandører og mobile enheter gjør at informasjonen ofte flyter utenfor virksomhetens IKT-infrastruktur. Enkelte virksomheter opplever at ansatte benytter private tjenester til behandling av virksomhetsinformasjon av bekvemmelighetshensyn, eksempelvis private e-post eller skylagringstjenester. En virksomhet må derfor sikre at informasjonen til en hver tid behandles innenfor en akseptabel risiko.

Ved å benytte kryptografiske mekanismer, både i transitt og i ro, reduseres risikoen for kompromittering av sensitiv data. Kryptering av data medfører at virksomheten kan ha tillit til at informasjonen ikke kan avleses uten betydelige ressurser, selv om mediet som bærer informasjonen enten er avlyttet eller mistet. Dette er tilfelle hvis implementasjonen av de kryptografiske prosessene og de teknologiske mekanismene er implementert på en forsvarlig måte. Et eksempel er forvaltningen av kryptografiske nøkler som benyttes av ulike kryptografiske algoritmer for å beskytte data. En virksomhet må derfor utarbeide retningslinjer for hvordan informasjonen beskyttes. Informasjonen må beskyttes mot angrep på både konfidensialitet og integritet.

Når kryptering skal benyttes mellom virksomheter må de også ivareta behovet for å kunne oppdage «ondsinnet» trafikk som eventuelt går ut og inn av virksomheten. Tilliten som kryptering tilbyr må således opprettes mellom entitetene og ikke sluttbrukere. En egen tillit mellom brukere vil ofte måtte opprettes i tillegg.



2.8 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.8.1	Skru på kryptering i de tjenester som tilbyr slik funksjonalitet og sikre at kun anbefalte algoritmer og nøkkellengder benyttes.
2.8.2	Implementer kryptering av medier som holder sensitive data eller som lett kan mistes eller kompromitteres, eksempelvis mobile enheter. Definer hvordan ulike typer data skal krypteres, eksempelvis med kryptering av enkeltfiler, partisjoner eller hele disker.
2.8.3	Når sensitiv informasjon overføres, bør informasjonskanalen krypteres. Flyter informasjon fra virksomheten over informasjonskanaler med lav tillit, bør informasjonen krypteres. For de ulike kanalene må det bestemmes på hvilket nivå krypteringen gjennomføres, for eksempel i applikasjonen (TLS), på nettverkslaget (IPsec) eller på datalinklaget (MACsec).
2.8.4	Ende-til-endekryptering anbefales der det er mulig mellom entiteter som har behov for å sikre konfidensialitet og integritet ved overføring av data. Virksomheter bør definere hva som er deres entiteter, og de bør defineres så nært sluttbruker og tjeneste som mulig.
2.8.5	Utarbeid en håndteringsmatrise som viser hvilke sikringstiltak som gjelder for beskyttelse av informasjon med ulik sensitivitet når informasjon lagres på de ulike medier og overføres over de ulike informasjonskanalene. Det er den juridiske enhetens (virksomheten) behov for å sikre eget IKT-system som må gå foran den enkelte ansattes behov for integritet og konfidensialitet.
2.8.6	Utarbeid et konsept for hvordan kryptografi benyttes i virksomheten. Dette bør inneholde valg av kryptografiske mekanismer, håndtering av sertifikater, hvordan utøve sikker nøkkelgenerering, hvordan nøkler lagres i bruk, sikkerhetskopiering av nøkler, regenerering av nøkler (når) og hvordan håndtere tap av nøkkel. For nøkkelhåndtering bør det skilles på langtidsnøkler og sesjonsnøkler, der langtidsnøkler bør beskyttes særskilt, fortrinnsvis i maskinvare.

	INFORMASJONSKLASSIFIERING			
	Åpen	Intern	Sensitiv	Kritisk
I ro på virksomhetens datasentre	Ukryptert	Ukryptert	Ukryptert	Opp til informasjonseier
I ro utenfor virksomhetens datasentre	Ukryptert	Opp til informasjonseier	Opp til informasjonseier	Kryptert
I ro på forvaltede enheter	Ukryptert	Ukryptert	Ukryptert	Kryptert
I ro på uforvaltede enheter	Ukryptert	Kryptert	Ikke tillatt	Ikke tillatt

FIGUR 5 - Eksempel på en håndteringsmatrise av virksomhetens informasjon i ro på ulike plattformer.

2.9 BESKYTT E-POST OG NETTLESER

Minimere angrepsflaten og angriperes mulighet til å manipulere menneskelig oppførsel i forbindelse med bruk av e-postklienter og nettlesere.

HVORFOR ER DETTE VIKTIG?

Sikker konfigurasjon av tjenester, enheter og programvare er viktig for at angripere ikke skal få boltre seg fritt i en virksomhet og utnytte virksomhetens verdier og ressurser. Enkelte funksjoner og applikasjoner er likevel ekstra utsatt grunnet utstrakt kommunikasjon og interaksjon både internt i egen virksomhet og eksternt mot andre systemer. E-post og nettsider infisert med skadevare (virus, trojanere, osv.) er vanlige inngangsportaler for angrep, grunnet direkte interaksjon med brukere, andre systemer og nettsider. Innhold kan skreddersys for å lure brukere til å foreta handlinger som øker risiko for innføring av skadelig kode, tap av verdifulle data eller andre angrep. Hensikten er å hindre at skadevare blir levert sluttbruker eller får kjøre på maskinen den blir levert til.

E-post er en av de viktigste tjenestene som benyttes i dag på intranett og internett. Vedlegg i e-post er en av de vanligste inngangsveiene for å distribuere datavirus, ormer og annen type skadevare. Vedleggene utnytter ofte sårbarheter i andre applikasjoner, som Excel, eller at filtypen som vises i e-postklienter (.jpg, .exe, .zip, osv.) ikke alltid samsvarer med den faktiske filtypen. Vedlegg i innkommende e-post bør derfor alltid behandles med varsomhet, spesielt hvis de er uventet eller hvis avsender ikke er kjent. Virksomheten bør sikre e-post slik at ingen uvedkommende får tilgang til eller kan manipulere innholdet, at avsender verifiseres og at e-post ikke benyttes som leveranse av skadevare.

Nettleserteknologi har utviklet seg i et raskt tempo. Den har beveget seg fra den opprinnelige formen med å laste og vise tekst og bilder fra internett, til å bli et universelt «front-end» for nettverksbaserte applikasjoner. Nettlesere kan sees på som egne operativsystemer og kan håndtere et bredt spekter av forskjellige medieformater og fungerer også som en plattform for kjøring av fullverdige applikasjoner. Bruk av nettlesere kan føre til en rekke sikkerhetsproblemer grunnet feil bruk, feilkonfigurering eller programmeringsfeil. Mengden valg og funksjoner innebærer kompleks konfigurering og potensiale for sikkerhetsproblemer.

VIRKEMIDLER FOR Å REDUSERE FORFALSKET E-POST («SPOOFING»):

SPF (Sender Policy Framework) forteller omverdenen hvilke maskiner/systemer som har lov til å sende e-post fra ditt domene.

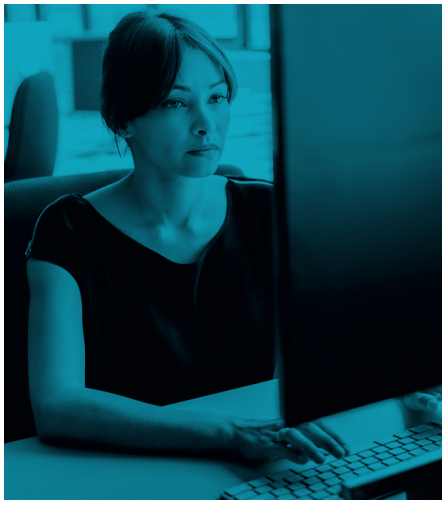
DKIM (DomainKeys Identified Mail) lar avsenders eposttjeneste signere en e-post kryptografisk. E-posttjenesten til mottaker kan verifisere at e-posten kommer fra noen som har kontroll over domenenavnet, og at innholdet i e-posten er uendret.

DMARC («Domain-based Message Authentication, Reporting and Conformance») bygger på både SPF og DKIM, og gir en anbefaling om hva mottakers e-postkonto bør gjøre dersom en e-post som har kommet inn feiler en av disse to sjekkene.

Både SPF, DKIM og DMARC baserer seg på at mottaker slår opp informasjon tilknyttet et domenenavn i DNS. Når et domene er sikret med **DNSSEC (Domain Name System Security Extensions)**, vil det være mulig å kontrollere både at svaret kommer fra riktig kilde og at det ikke er endret underveis.

2.9 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.9.1	Sørg for at kun fullt støttede e-postklienter og nettlesere tillates å kjøre i virksomheten. Kun siste versjon av nettlesere bør benyttes slik at de siste sikkerhetsrettingene og den nyeste sikkerhetsfunksjonaliteten tas i bruk.
2.9.2	Skann alle e-postvedlegg som ankommer virksomhetens e-posttjeneste og blokker vedleggene dersom de inneholder skadelig kode, mistenkelig innhold (spam eller mistenkelige URL-er) eller filtyper som ikke er godkjent for bruk i virksomheten. For å oppdage ondsinnet kode i vedlegg bør vedlegg kjøres og aktiveres i egne sandkasse-miljøer.
2.9.3	Konfigurer nettleser sikkert slik at skadelig kode i størst mulig grad hindres å kjøre. Dette kan blant annet gjøres ved å ta i bruk «Beskyttet modus» som standardinnstilling for nettsurfing. Dersom virksomheten har ulike behov i forhold til funksjonalitet i nettleser, eksempelvis for å kunne skille privat og virksomhetsspesifikk data, kan virksomheten benytte to ulike nettlesere med ulike sikkerhetsinnstillinger.
2.9.4	Verifiser at innkommende e-post er fra en legitim virksomhet for å forhindre «spoofing».
2.9.5	Avinstaller eller deaktiver unødvendig eller uautoriserte plugins eller tilleggsprogrammer til e-postklient eller nettleser. Hver plugin bør benytte applikasjons- og URL-hvitlisting og kun tillate kjøring av programmer fra forhåndsgodkjente domener.
2.9.6	Konfigurer klienter slik at de ikke kjører aktivt innhold når innkommende HTML-formaterte e-poster vises.
2.9.7	Begrens bruken av unødvendige skriptspråk i alle e-postklienter og nettlesere. Dette inkluderer bruk av språk som ActiveX og Javascript på alle systemer hvor det ikke er behov for støtte.
2.9.8	Sørg for at filer som lastes ned ikke automatisk kjører på maskinen siden disse kan inneholde skadevare.
2.9.9	E-post klienter eller nettlesere bør ikke tillates på annet enn sluttbrukerutstyr (eksempelvis bør det ikke benyttes på servere).



2.10 ETABLER HENSIKTSMESSIG LOGGING

Samle og administrere logger for hendelser som kan bidra til å oppdage, forstå, eller gjenopprette etter et angrep.

HVORFOR ER DETTE VIKTIG?

Hendelser bør registreres slik at sikkerhetsbrudd kan detekteres så tidlig som mulig, om ikke forhindres. Ved sikkerhetsbrudd kan logger bidra til at skadens karakter og omfang kan identifiseres og skaden utbedres. Manglende eller feilaktig konfigurering av logger og logganalyse vil kunne medføre at angripere uoppdaget kan skjule sin

tilstedeværelse, skadevare og aktiviteter i virksomhetens IKT-systemer. Logger vil også bidra til å kartlegge skadeomfanget av et angrep, tidslinje for angrepet, og vil danne grunnlag for eventuelle rettslige forfølgelser.

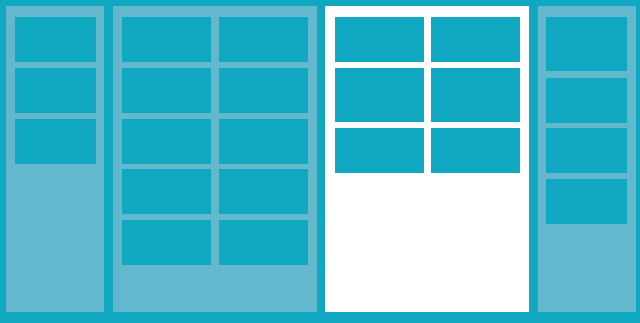
Uønsket aktivitet i eget nettverk vil være utfordrende å oppdage, og dersom en angriper får fotfeste i virksomheten vil det meste av trafikken internt i eget nettverk maskeres som legitim trafikk. Logger må derfor benyttes for å etablere en oversikt over normaltilstand, slik at avvik kan oppdages. Dette, kombinert med mer bruk av ende-til-ende-kryptering, gjør at logging på endepunkter og mellom sikkerhetssoner bør prioriteres fremfor logging av generell nettverkstrafikk.

Logger er viktige for hendelseshåndtering og rasjonell drift av IKT-systemer, men de må også benyttes med varsomhet og således beskyttes godt. Logger kan inneholde sensitiv informasjon om den enkelte medarbeider og behovet for lagring av slik informasjon må til enhver tid veies opp mot behovet for personvern.

2.10 ANBEFALTE TILTAK

ID	BESKRIVELSE
2.10.1	Logging må gjennomføres på en måte som sikrer ansvarlighet, tilgjengelighet og integritet. Logger må innsamles og håndteres på en måte som inngir tillit til det som står i loggen, at det som skal logges blir logget og at loggingen ikke er blitt stoppet, innholdet endret eller slettet. Logger skal kun benyttes til å ivareta sikkerheten i IKT-systemer og bør lagres i lang nok tid til at man kan oppdage og kartlegge uønsket aktivitet og bevegelse i etterkant av en hendelse.
2.10.2	Behovet for logging av metadata og/eller innhold bør veies mot brukerens og virksomhetens behov for konfidensialitets-beskyttelse og bør beskrives.
2.10.3	Gjennomfør en intern vurdering for å avgjøre hvilke systemer og komponenter det er viktigst å generere logger for. Ta hensyn til følgende i vurderingen: • Hvor ligger virksomhetens mest sensitive data? • Hvilke systemer er virksomheten avhengig av for å understøtte leveranser og forretningsprosesser? • Hvilke brukere har størst privilegier i virksomheten? • Gjennom hvilke nøkkelpunkt flyter data? • Hvilke «gateway-er» finnes mellom interne og eksterne systemer?
2.10.4	Logging bør slås på i den konfigurasjonen som gir det beste datagrunnlaget for hendelseshåndtering. Generer logger for alle relevante systemer og komponenter med hovedfokus på endepunkter og trafikk mellom sikkerhetssoner.
2.10.5	Verifiser at loggingen fungerer etter hensikt og beskyttes mot manipulering. • Synkroniser logger mot minste to referansetidskilder slik at aktiviteter er tilordnet et korrekt tidsstempel og kan leses av kronologisk. • Valider at logginnstillinger fungerer og at det som skal logges blir logget. Sørg for at alle systemer som jevnlig lagrer logger har tilstrekkelig lagringsplass slik at loggfiler ikke fylles opp mellom rotasjonsintervallene. • Arkiver og signer loggene digitalt med jevne mellomrom for å sikre loggintegritet. • Samle logger i et sentralt lager slik at loggen er tilgjengelig når det er behov for dem. Benytt et standardisert format for logger slik at de enkelt kan leses av tredjeparts logganalyseverktøy. • Sørg for tilstrekkelig tilgangsstyring på logger og implementer funksjonalitet som oppdager forsøk på manipulering eller sletting av logger.

3. Opprettholde og oppdage



3.1 SØRG FOR GOD ENDRINGSHÅNDTERING

Opprettholde den sikre tilstanden over tid når virksomheten utsettes for planlagte eller ikke-planlagte endringer.

HVORFOR ER DETTE VIKTIG?

Over tid vil en virksomhet utsettes for både planlagte og ikke-planlagte endringer av virksomhetsprosesser, organisasjon eller teknologi. Planlagte endringer kan initieres av en rekke rutinemessige hendelser, for eksempel feilretting, maskin- og programvareoppdateringer, kontoadministrasjon eller ytelsesjusteringer. Disse endringene kan kreve en gjennomgang og omdefinering av de implementerte sikringstiltakene, eksempelvis etter installasjon av ny programvare. Ikke-planlagte endringer kan initieres av en rekke dramatiske hendelser, for eksempel angrep, ulykker eller funksjonsfeil. Det er avgjørende for en virksomhet at disse endringene håndteres på en god måte, slik at virksomheten forstår konsekvensen av endringen og implementerer kompenserende tiltak for de eventuelle sårbarhetene selve endringen eller behovet for endring vil medføre. Først da vil IKT-systemet kunne holdes sikkert gjennom hele dets levetid.

Eksempler på endringer som bør vurderes som fast-track:

- Tiden fra patch til skadevare blir kortere og kortere (ned mot en uke). Virksomheter må automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer..
- Opprettelsen av en ny bruker

Alle endringer bør gå til implementasjons-vurdering der også test må vurderes og sporbarheten må ivaretas.

3.1 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.1.1	Etabler en formell prosess for å håndtere og dokumentere alle forslag til endringer i virksomheten. Endringer som bør behandles i en felles prosess inkluderer, men er ikke begrenset til, endrede forretningsprosesser, nye oppdateringer, utskifting av utstyr, endring av organisasjon (brukere eller roller), endring av konfigurasjonen til systemkomponenter, og så videre.
3.1.2	Prosessen for endringshåndtering bør som et minimum inkludere følgende tre faser: • Teknisk gjennomgang av forslag til endring som resulterer i en teknisk anbefaling. • Vurdere de forretningsmessige konsekvenser av foreslåtte endringer og beslutte endring. • Planlegg implementering av godkjente endringer. Evaluering av konsekvenser av endringen og risiko må vurderes helhetlig. Dette kan eksempelvis være nedetid på IKT-systemer, behov for opplæring eller håndtering av økt risiko ved at endringen ikke er gjennomført.
3.1.3	Sørg for formelt å godkjenne og dokumenter alle endringer, og ikke bare et utvalg. Virksomheten bør etablere forhånds-godkjenninger (fast track) av de fleste typer endringer slik at beslutningsleddene i virksomheten fokuserer på de viktigste endringene. Sporbarhet må ivaretas for alle endringer.
3.1.4	Benytt verktøy som automatisk oppdaterer og ruller ut godkjente endringer til virksomhetens systemer med gitte tidsinter-valler, eller manuelt ved hendelser. Dette vil gjøre implementeringen enklere for virksomheten, og påse at kritiske endringer rulles ut hurtig nok.

3.2 BESKYTT MOT SKADEVARE

Kontrollere installasjon, spredning og kjøring av skadelig kode i virksomhetens IKT-miljø og benytt automatiserte verktøy for sårbarhetsovervåkning og oppdatering sikringstiltak.

HVORFOR ER DETTE VIKTIG?

Skadelig kode er en integrert og farlig del av cybertrusler og kan utformes for å påvirke systemer, enheter og data. Det kan bevege seg hurtig, endre seg etter behov og komme seg inn gjennom en rekke punkter som sluttbrukerutstyr, e-postvedlegg, nettsider, skytjenester, ved brukerhandlinger og flyttbare medier. Moderne skadevare kan utvikles for å unngå forsvar, eller for å angripe eller deaktivere dem.

En virksomhet må ha oversikt over og beskyttes mot kjente skadevarer og angrepsmetoder. Forsvar mot skadevare må være i stand til å operere i dynamiske miljøer, gjennom storskala automatisering, hurtige oppdateringer, og integrert med prosesser som hendelseshåndtering. Det må også distribueres til et antall mulige angrepspunkter for å detektere, hindre bevegelse eller kontrollere kjøring av skadelig kode.

NSM NorCERT publiserer viktige oppdateringer på NSMs nettsider, se https://nsm.stat.no/norcert/norcertvarsler/

Tilsvarende varsler distribueres også fra kommersielle aktører og leverandører av programvare.

3.2 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.2.1	Installer sikkerhetsoppdateringer så fort som mulig. Selv de beste produktene har feil og sårbarheter som kan utnyttes av angripere. Etabler et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware (f. eks. BIOS-kode).
3.2.2	Benytt automatiserte verktøy for kontinuerlig overvåkning av antivirus, antiskadevare, klient-brannmurer og verts-baserte IPS-funksjonalitet installert på arbeidsstasjoner, serverer og mobile enheter. Alle hendelser relatert til oppdagelse av skadevare bør sendes til virksomhetens verktøy for administrasjon av antiskadevare og loggservere for hendelser.
3.2.3	Kjør automatiserte sårbarhetsskanningsverktøy mot alle systemer på nettverket, ukentlig eller hyppigere, prioriter og håndter de mest kritiske sårbarhetene og verifiser at sårbarhetene blir lukket. Benytt skanningsverktøy som både leter etter kodebaserte sårbarheter (CVE) og konfigurasjonsbaserte sårbarheter (CCE).
3.2.4	Abonner på tjenester relatert til sårbarhetsetterretning for å være oppdatert på nye og kommende sårbarheter og benytt denne informasjonen som input til verktøyene for sårbarhetsskanning. Alternativt sørg for at verktøy benyttet til sårbar-hetsskanning jevnlig blir oppdatert med alle relevante sikkerhetssårbarheter.
3.2.5	Etabler en prosess for å risikovurdere sårbarheter basert på utnyttelsesmulighet og potensiell konsekvens. Tildel sikkerhets-rettinger for de mest risikoutsatte sårbarhetene først.

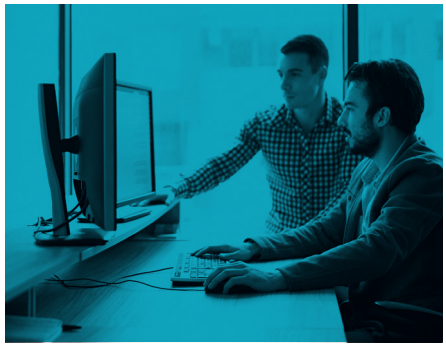
3.3 VERIFISER KONFIGURASJON

Spore, rapportere og korrigere sikkerhetskonfigurasjon av enheter, programvare og tjenester for å hindre angripere i å utnytte sårbare tjenester og innstillinger.

HVORFOR ER DETTE VIKTIG?

IKT-miljøet er under kontinuerlig justering og endring når løsninger først er idriftsatt. Det kan være små og store endringer på enheter, programvare og tjenester, brukere som har behov for tilpasninger i forbindelse med bruk av tjenester, eller endringer i trusler, sårbarheter eller beskyttelsesbehov som gjør at konfigurasjonen må justeres.

Angripere utnytter ofte at sikkerhets-konfigurasjonen på komponenter i nettverket over tid svekkes. Angripere søker etter sårbare standardinnstillinger



som ikke har blitt endret og logiske hull i sikkerhetskomponenter som brannmurer, rutere og svitsjer og utnytter dette for å omgå eller komme gjennom sikkerhetsbarrierer. Det er derfor viktig at konfigurasjonen sjekkes ved jevne mellomrom og at avvik registreres, rapporteres og håndteres på en effektiv måte.

3.3 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.3.1	Implementer og test et automatisert system for overvåkning av konfigurasjon som verifiserer alle eksternt testbare elementer for sikkerhetskonfigurasjon, og varsler når uautoriserte endringer forekommer. Dette inkluderer funksjonalitet for å oppdage endringer i brannmurkonfigurasjon (f.eks. åpning av nye porter), nye administrative brukere og nye tjenester som kjører på et system.
3.3.2	Sammenlign konfigurasjonen på systemkomponenter som nettverksutstyr og klienter (gjeldende konfigurasjon) mot en sikker, standard konfigurasjon (gyldig konfigurasjon) som er definert for hver enhet i virksomheten. Sikkerhetskonfigurasjonen for slike enheter bør dokumenteres, gjennomgås og godkjennes av virksomhetens endringskontrollregime. Alle avvik fra standardkonfigurasjon eller oppdateringer til denne skal dokumenteres og godkjennes av endringskontrollsystemet.
3.3.3	Kontroller at kun porter, protokoller og tjenester med godkjent forretningsbehov kjører på hvert system.
3.3.4	Utfør automatiserte portskanner regelmessig mot alle nøkkelservere og sammenlikne resultatet mot godkjent konfigurasjon. Hvis det oppdages en endring som ikke er en del av virksomhetens godkjente konfigurasjon bør det logges, automatisk rapporteres og gjennomgås av relevant personell.
3.3.5	Benytt verktøy for integritetssjekking for å sikre at kritiske systemfiler ikke har blitt endret. Integritetskontrollene bør identifisere mistenkelige systemendringer som endring av eier og tillatelser for filer eller kataloger, bruk av alternative datastrømmer som kan brukes til å skjule ondsinnede aktiviteter; og innføring av ekstra filer til viktige systemområder. Dette kan indikere skadelig nyttelast lagt igjen av angripere eller flere filer feilaktig lagt under batch distribusjon prosesser.

3.4 GJENNOMFØR INNTRENGINGS-TESTER OG «RED-TEAM»-ØVELSER.
Teste den totale styrken i virksomhetens forsvarsmekanismer (teknologi, prosesser og personell) ved å simulere mål og handlinger til en angriper.

HVORFOR ER DETTE VIKTIG?

I et komplekst miljø hvor teknologien konstant utvikler seg og nye angrepsmetoder stadig dukker opp, bør virksomheter jevnlig teste egen forsvarsevne for å identifisere gap og vurdere egen beredskap. Angripere utnytter ofte gapet mellom god design og funksjonalitet og gjeldende implementasjon og vedlikehold.

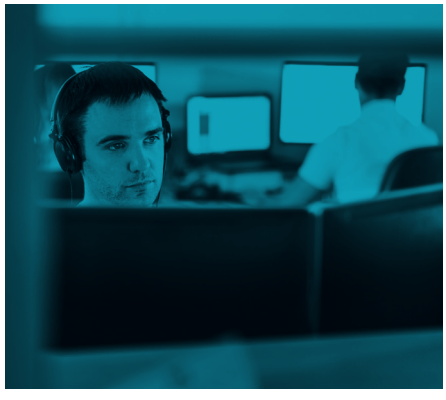
Eksempler inkluderer:

- For langt tidsvindu fra annonsering av en sårbarhet og tilgjengeliggjøring av retting fra leverandør, til faktisk installasjon på hver enkelt komponent.
- Velmenende retningslinjer, for eksempel relatert til passordkvalitet, men manglende mekanismer for å påtvinge dette til brukere.
- Mangelfull etablering av sikker konfigurasjon av komponenter i IKT-miljøet eller maskiner som jevnlig kobler seg til og fra nettverket.
- Manglende evne til å forstå verdikjeder og avhengigheter mellom systemer.

Et vellykket forsvar krever et omfattende program av tekniske forsvar, god styring, gode retningslinjer og riktige handlinger fra personell.

Inntrengingstesting er et kontrollert dataangrep som prøver ut motstandskraften i IKT-systemer gjennom målrettede søk og analyser, og forsøksvis utnyttelse av sårbarheter, feil og mangler som identifiseres. Selv om angrepene tilstreber å simulere en trusselaktør, må virksomheter være bevisst at en inntrengingstest foregår i en begrenset tidsperiode og omfatter ofte kun enkelte, spesifikke mål. Resultatet av en slik test vil gi dypere innsikt, gjennom en faktisk demonstrasjon i hva slags virksomhetsrisiko sårbarheter kan utgjøre. Målet med en slik test vil være å finne de viktigste feilene slik at disse kan utbedres. En inntrengingstest kan demonstrere hvordan man kan få tilgang til virksomhetssensitive data, administrativ kontroll over deler av IKT-infrastrukturen eller kontroll over spesifikke tjenester. Samtidig kan tester benyttes før tjenester går i produksjon eller ved større endringer.

«Red Team»-øvelser tester virksomhetens beredskap for dataangrep gjennom simulering av faktiske angrep. Dette vil være en mer helhetlig tilnærming og vil utfordre virksomhetens retningslinjer, prosesser og sikringstiltak. Uavhengige «Red Team» kan bidra med verdifull og objektive testing av effektiviteten av beredskapsprosesser og personell tilknyttet dette.



3.4 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.4.1	Gjennomfør jevnlige eksterne og interne inntrengingstester for å identifisere sårbarheter og angrepsvektorer som kan bli brukt for å utnytte virksomhetens systemer og ressurser. Inntrengingstestingen bør gjennomføres fra utsiden av virksomhetens nettverksbarrierer (eksempelvis fra internett eller trådløse frekvenser i nærheten av virksomhetens lokaler) samt fra innsiden av barrierer (eksempelvis på det interne nettverket) for å simulere eksterne og interne angrep.
3.4.2	Still krav til at rapporteringen fra en inntrengingstest dekker behovene til hele virksomheten. En inntrengingstest bør dokumenteres med en oppsummering (ledelsesoppsummering), oversikt over detaljerte funn og eventuelt forslag til tiltak og en prioritering av funn.
3.4.3	Brukere eller kontoer som brukes til å utføre inntrengingstesting bør kontrolleres og overvåkes for å sikre at de bare brukes til lovlige formål, og fjernes eller gjenopprettes til normal funksjon etter at testingen er over.
3.4.4	Sørg for å informere relevante aktører i forkant av en inntrengingstest. Graden av informasjon og til hvilke parter avhenger av hva slags type test som skal gjennomføres. Identifiser samtidig miljøer, systemer eller komponenter som skal unntas fra testingen. Dette kan være deler av IKT-infrastrukturen som er kritisk i forhold til opprettholdelse av ulike tjenester eller som i løpet av testperioden ikke er tilstrekkelig konfigurert til å tåle en inntrengingstest.
3.4.5	Utføre periodiske «Red Team»-øvelser for å teste virksomhetens beredskap i forhold til å identifisere, stoppe og respondere hurtig og effektivt på dataangrep.
3.4.6	Planlegg inntrengingstestene med tydelige mål og omfang, gjerne med flere angrepsmåter for å simulere kompleksiteten ved APT-er (Advanced Persistent Threats), eksempelvis med en blanding av sosial manipulering og internett- eller nettverksutnyttelse. Bruk av flere ulike angrepsvektorer og verktøy vil gi et mer realistisk bilde i forhold til et faktisk angrep og vil gi en mer korrekt evaluering av de implementerte sikkerhetsbarrierene og forsvarssystemene i virksomheten.
3.4.7	Benytt verktøy for sårbarhetsskanning i kombinasjon med utnyttelses- og inntrengningsverktøy. Sårbarhetsskanningen kan benyttes som et utgangspunkt for å rettlede og fokusere inntrengingstestingen.

3.5 OVERVÅK OG ANALYSER IKT-SYSTEMET

Generere, samle, konsolidere, analysere og varsle på tilstrekkelig monitoreringsdata for å bygge en oppdatert situasjonsforståelse av handlinger og aktiviteter i virksomhetens nettverk.

HVORFOR ER DETTE VIKTIG?

Manglende sikkerhetslogging, sammenstilling og analyse av loggdata gjør at angripere kan skjule tilstedeværelse, handlinger og aktiviteter i virksomhetens nettverk og på maskiner som utnyttes. Selv om en virksomhet vet at systemer og maskiner har blitt infiltrert, vil de være blinde for detaljene i angrepet dersom de ikke har tilstrekkelig loggdata og god nok beskyttelse og analyse av disse. For at loggdata skal kunne brukes effektivt må de samles til et sentralt punkt og konsolideres for å kunne oppdages, forstås og gjøre det mulig å reagere riktig på hendelser. Sammenstilling og analyse av loggdata er vesentlig for å kunne oppdage og forstå hendelser på tvers av strukturer og komponenter i nettverket. Loggdataene vil også kunne benyttes i forbindelse med granskning for å finne rotårsaken til hvorfor hendelsen oppsto, og i forbindelse med kriminaletterforskning.

Tidlig oppdagelse av uregelmessigheter og hendelser er vesentlig for å kunne oppdage og håndtere dataangrep. For å få til en hurtig og effektiv prosess rundt analyse og varsling basert på de samlede overvåkningsdataene, må virksomheten ha automatiserte analyseverktøy som kontinuerlig kalibreres basert på satte terskelverdier og kunnskap om «normalnivået» i virksomheten. «Normalnivået» beskriver hva som er et «rent nettverk» og hvilke innstillinger

For å overvåke og analysere IKT-systemet må en virksomhet vite hva som er «normaltilstand». Virksomheten må ha en egenevne til å oppdage unormal oppførsel og hendelser, hvor kun personell som forvalter systemene i det daglige har kompetanse til å se avvik fra normalbildet. For å få nok data til å oppdage og analysere unormaliteter og dataangrep er det viktig å ha informasjon fra flere kilder. Mange av kildene vil naturlig inngå i andre deler av dette dokumentet, inkludert:

- Kartlegg enheter og programvare
- Ivareta sikker design av IKT-miljø
- Ivareta en sikker konfigurasjon
- Ha kontroll på kontoer
- Kontroller bruk av administrative privilegier
- Kontroller dataflyt
- Beskytt e-post og nettleser
- Etabler hensiktsmessig logging
- Sørg for god endringshåndtering
- Beskytt mot skadevare
- Verifiser konfigurasjon

3.5 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.5.1	Utarbeid en strategi for logging og fastsett hvor lenge logger skal oppbevares. Gjennomfør en vurdering i hele virksomheten på hvilke behov som finnes for overvåkningsdata. Denne vurderingen bør gjøres jevnlig (minst en gang i året) og ved spesielle behov (f. eks etter et en større hendelse eller ved et vellykket dataangrep).
3.5.2	Aktiver logging på relevante komponenter og punkter i IKT-infrastrukturen. Samle relevante overvåkningsdata og konsolider dette til en stor eller flere sammenkoblede databaser. Eksempler på dette kan være loggdata fra klienter og nettverksenheter.
3.5.3	Automatiser prosessen med å analysere innsamlede data ved benyttelse av analyseverktøy som kalibreres og vedlikeholdes.
3.5.4	Gjennomgå og trim den sentrale loggdatabasen jevnlig i tråd med strategien slik at den kun tar vare på verdifulle loggdata. Dette innebærer å • Fjerne innsamlede loggdata som ikke lenger har noen operasjonell eller sikkerhetsmessig relevans • Ta vare på loggdata som potensielt kan benyttes i forbindelse med etterforskning, skadevurdering, trendanalyser og kapasitetsplanlegging. • Kombinere flere lav-nivå hendelser til en eller flere systematiske hendelser som viser et høyere tjenestenivå perspektiv, og samtidig fjern lav-nivå hendelser. • Overføre loggdata for trendanalyser og kapasitetsplanlegging til mer kompakte presentasjoner som oppsummeringer eller statistikker.
3.5.5	Etabler og vedlikehold en profil for «normaltilstand» i virksomhetens IKT-systemer og opparbeid kompetanse og kapabilitet til å oppdage anomaliteter i systemene ved at systemenes logger sentraliseres, sees i sammenheng og gjennomgås. Fastsett og vedlikehold terskelverdier og generer automatiske alarmer med varsling til en bemannet tjeneste i virksomheten hvor alarmer håndteres. Normaltilstanden bør forvaltes over tid slik at den ivaretar endringer i bruksmønster i forbindelse med omstillinger og omorganiseringer, oppkjøp, sammenslåing, nedbemanning og endring av driftskonsept.
3.5.6	Konfigurer overvåkningssystemer for å undersøke både inngående og utgående trafikk samt trafikken i utsatte soner mot kjente sårbarheter og angrepsmetoder. Overvåkningssystemene som benyttes på nettverkenes perimeter og de som benyttes for å beskytte interne nettverk bør være ulike for å ivareta sikkerhet i dybden.

og dataflyt som er vanlig i nettverket under daglig drift. Hvilke enheter skal normalt få lov til å snakke med hverandre, og hvordan? Hvilke data skal flyte mellom hvilke sikkerhetssoner? Hva slags type trafikk kjører normalt i nettverket og til hvilke tider? Dette er spørsmål virksomheten må finne ut av når overvåknings- og analyseverktøy kalibreres.

Som med lokale logger må også sentraliserte loggdatabaser trimmes jevnlig. Dette for å unngå at man benytter unødig mye lagringsplass til loggdata man ikke har bruk for, både med hensyn til plass og personvern. Dette må veies opp mot behovet for å ta vare på data som man potensielt kan få bruk for i fremtidig etterforskning, skadevurdering, trendanalyser og kapasitetsplanlegging.

3.6 ETABLER KAPABILITET FOR GJENOPPRETTING AV DATA

Etabler en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap.

HVORFOR ER DETTE VIKTIG?

Virksomheten må etablere kapasitet for å gjenopprette tapte eller endrede data eller systemkonfigurasjoner. Enkelte dataangrep medfører at kritiske konfigurasjoner, programvare eller informasjon endres eller gjøres utilgjengelig. Dette kan påvirke virksomhetskritiske prosesser. Et eksempel på et slikt angrep er kryptovirus, der informasjon eller hele systemer krypters slik at de blir utilgjengelige for en virksomhet.

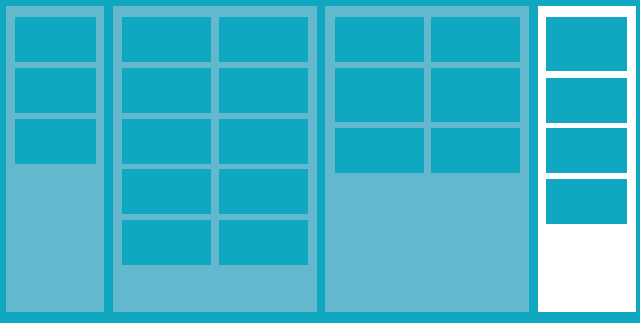
En plan for sikkerhetskopiering bør som et minimum beskrive:

- Hvilke data som skal sikkerhetskopieres
- Hvilke data som skal ekskluderes fra sikkerhetskopier
- Regelmessighet for sikkerhetskopiering. Ukentlig sikkerhetskopiering anbefales, hyppigere for virksomhetskritiske systemer eller systemer hvor data endres ofte.
- Hvilke forretningsenheter som er ansvarlig for sikkerhetskopieringen
- Prosedyrer for feilrapporter
- Oppbevaringsperiode
- Gjenopprettingsevne og krav til denne
- Beskyttelse av sikkerhetskopieringsdata

3.6 ANBEFALTE TILTAK

ID	BESKRIVELSE
3.6.1	Sikkerhetskopiering av data bør gjennomføres regelmessig av alle relevant data, basert på en sikkerhetskopieringsplan. En slik plan bør stille krav til gjenopprettingstid fra sikkerhetskopi for virksomhetens ulike systemer basert på en verdivurdering eller behov for tjenestekvalitet. Planen bør også beskrive målet for hva slags data som hentes tilbake (fra hvilket punkt hentes data fra).
3.6.2	Planen for sikkerhetskopiering bør godkjennes av prosesseiere som bruker dataene og ansvarlige for applikasjonen som forvalter de data som skal sikkerhetskopieres.
3.6.3	For å sikre rask gjenoppretting, bør både operativsystemet, programvaren og dataene på en maskin være inkludert i den generelle sikkerhetskopieringsprosedyren. Disse tre komponentene i et system må ikke nødvendigvis inkluderes i den samme sikkerhetskopifilen eller bruke samme sikkerhetskopieringsprogramvare.
3.6.4	Det bør være flere sikkerhetskopieringer over tid, slik at systemet kan gjenopprettes selv om systemet er sikkerhetskopiert etter at en feil eller infeksjon oppstod.
3.6.5	Sikkerhetskopier bør lagres på en alternativ lokasjon enn produksjonsservere. Denne lokasjonen bør tilfredsstille de samme kravene som ellers i virksomheten for å forvalte informasjonen som sikkerhetskopieres.
3.6.6	Test sikkerhetskopier regelmessig ved å utføre en gjenopprettingsprosess for å sikre at sikkerhetskopieringen fungerer tilstrekkelig.
3.6.7	Kontroller at sikkerhetskopier er riktig beskyttet via fysisk sikkerhet eller kryptering når de lagres, samt når de flyttes over nettverket. Dette inkluderer ekstern sikkerhetskopiering og skytjenester.
3.6.8	Som et minimum bør virksomhetskritiske systemer ha minst en sikkerhetskopidestinasjon som ikke kan adresseres kontinuerlig gjennom operativsystemanrop. Dette vil redusere risikoen for angrep som krypteringsvirus. Dissesøker å kryptere eller ødelegge data på alle adresserbare filområder, inkludert lokasjoner for sikkerhetskopier.

4. Håndtere og gjenopprette



4.1 FORBERED VIRKSOMHETEN PÅ HÅNDTERING AV HENDELSER

Beskytte virksomhetens tjenester, informasjon, ressurser og omdømme ved å utvikle og implementere effektive prosesser for hendelseshåndtering for hurtig å kunne oppdage hendelser og effektivt kontrollere og fjerne hendelsesårsaken og gjenopprette integriteten til systemer og nettverk. Dette inkluderer planverk, definerte roller, øving, kommunikasjon og ledelsesoversikt.

HVORFOR ER DETTE VIKTIG?

Angrep i cyberdomenet er nå så vanlig at det har blitt en del av dagliglivet. Selv store, teknisk sofistikerte virksomheter

HVA GJØRE MAN HVIS ET DATA-ANGREP BLIR OPPDAGET KL 18:00 PÅ EN FREDAG, LIKE FØR EN FERIEPERIODE?

- Har man mekanismer for å oppdage angrepet hurtig?
- Er telefonlisten oppdatert?
- Har man betalt for at underleverandører og støttepersonell kan trå til på kort varsel?
- Hva skal man gjøre hvis nøkkelpersoner er på ferie i utlandet?

Ved oppdagelse og spredning av skadevare som Wannacry 1.0/2.0 må man reagere hurtig for å hindre omfattende skadefølger. Virksomheten har ofte bare en time eller to på seg fra skadevaren oppdages til de må ta en avgjørelse på situasjonen skal håndteres.

- Skal brannmurer stenges?
- Skal strømmen trekkes ut fra sentrale servere?
- Har man tjenester som må isoleres fra øvrig IKT-infrastruktur?
- Fungerer sikkerhetskopier hvis man må resette alle servere?

God planlegging, et oppdatert og veltestet planverk og tilknytning til en døgnkontinuerlig vaktordning kan bety vinn eller forsvinn for virksomheter når dataangrep inntreffer. Er din virksomhet beredt?

4.1 ANBEFALTE TILTAK

ID	BESKRIVELSE
4.1.1	Etabler et planverk for hendelseshåndtering som ivaretar behovet for virksomhetskontinuitet i krise- og beredskapssituasjoner. Planverket bør inkludere personellroller for håndtering av hendelser og definere de ulike fasene innen hendelseshåndtering.
4.1.2	Tildel jobbtitler og plikter for håndtering av maskinvare og nettverk til spesifikke roller i virksomheten. Dersom dette må gjøres ad-hoc når en hendelse inntreffer kan det allerede være for sent.
4.1.3	Utarbeid avtaler med underleverandører slik at de kan reagere hurtig og inngår som en del av hendelsesteamet der dette er hensiktsmessig.
4.1.4	Utarbeid og distribuer kontaktinformasjon for interne og eksterne nøkkelpersoner. Alternative kommunikasjonskanaler bør også vurderes.
4.1.5	Definer ledelsespersonell som vil supportere hendelseshåndteringsprosessen ved å fungere som beslutningstakere i nøkkelroller.
4.1.6	Utarbeid retningslinjer som omfatter hva som forventes av hele virksomheten fra hendelsen oppdages til den avsluttes, mekanismer for rapportering og hva slags informasjon som skal inkluderes i hendelsesvarslingen. Rapporteringen bør også inkludere varsling til korrekt sektor-CERT i henhold til juridiske og regulatoriske krav for informasjon til andre virksomheter og eventuelt støtte til håndtering av hendelsen.
4.1.7	Test og øv planverk jevnlig slik at denne er godt innøvd for involvert personell. Slike tester bør også inkludere relevante underleverandører og bør kombineres med «Red Team»-øvelser.
4.1.8	Revider og oppdater planverket jevnlig, og i etterkant av øvelser, større hendelser eller angrep. Revisjonen bør gjøres minst en gang i året.

med mye ressurser har utfordringer med å holde følge med frekvensen og kompleksiteten på dataangrep. Spørsmålet er ikke «om» en virksomhet blir offer for et vellykket dataangrep, men «når». Det er for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier når hendelsen inntreffer. Disse må utarbeides og øves i god tid i forveien for å gjøre virksomheten i stand til å forstå, håndtere og gjenopprette normaltilstanden. Uten en plan og en virksomhetsprosess for hendelseshåndtering er det ikke sikkert at virksomheten vil oppdage at et angrep er i gang, og hvis angrepet først oppdages, er det stor sannsynlighet for at virksomheten ikke følger gode prosedyrer for begrense skaden, fjerne angriperens tilstedeværelse og gjenopprette normaltilstand på en effektiv og sikker måte. Angrep vil da kunne få et større omfang og påføre virksomheten større skade, infisere flere systemer og hente ut mer sensitive data enn hvis effektive prosesser for hendelseshåndtering var på plass. I enkelte tilfeller kan det være nødvendig å la en aktør være aktiv i virksomhetens IKT-infrastruktur for å forstå omfanget av kompromitteringen.

4.2 VURDER OG KATEGORISER HENDELSER

Rettidig og korrekt vurdere og kategorisere hendelser slik at de blir håndtert effektivt, med riktig prioritet og involverer nødvendige ressurser og personell.

HVORFOR ER DETTE VIKTIG?

Kategorisering av hendelser er viktig for å kunne håndtere hendelser med riktig prioritet, ressursbruk og innen nødvendig tid. Hvis det tar lang tid fra en hendelse blir oppdaget til den blir varslet, prioritert og håndtert kan skadeomfang, ressursbruk og gjenopprettingstid bli betydelig større enn hvis hendelsen hadde blitt håndtert tidlig. Feilaktig kategorisering kan føre til at en virksomhet bruker mye tid og krefter på uvesentlige hendelser, mens viktigere hendelser går under radaren. Manglende involvering av interne og eksterne beslutningstagere kan føre til at hendelsen eskalerer og aktiviteter sprer seg til andre systemer og virksomheter fordi det ikke hurtig nok settes inn reaktive tiltak. Ved skadevare av en viss kompleksitet vil de færreste klare å se reelt skadeomfang før i etterkant av hendelsen. For mange virksomheter vil det være nødvendig å hente kompetanse utenfor egen virksomhet for riktig vurdering og kategorisering av hendelser.

Når en hendelse oppstår vil det alltid være en diskusjon på om man skal stenge ned tjenester, sette inn tiltak eller sitte stille og bygge kompetanse om hva som skjer. Dette er en svært vanskelig vurdering som krever kompetente observatører, og dersom man velger feil sti kan skadene bli store. Dersom man eksempelvis stenger ned for tidlig kan det være vanskelig å rydde opp i etterkant. Det å stenge ned en tjeneste vil også kunne medføre konsekvenser for virksomhetens leveranser. Virksomheter må derfor tilstrebe at alle relevante ressurser sitter rundt bordet når beslutningen skal tas.

FIGUR 6 – Eksempel på klassifiseringsregime for hendelser

«Spørsmålet er ikke «om» en virksomhet blir offer for et vellykket dataangrep, men «når».»

Uautorisert tilgang til informasjon	7							
Kompromittering	6							
Forsøk på komprimittering	5							
Tjenestenekt	4							
Svindel	3							
Rekognosering/ informasjonsinnsamling	2							
Støtende innhold	1							
Beskrivelse	Vekt	1 Individ	2 Virksomhet	3 Sektor	4 Nasjonalt	5 Virksomhet	6 Sektor	7 Nasjonalt
						Med kritisk infrastruktur og/eller kritiske samfunnssituasjon		

4.2 ANBEFALTE TILTAK

ID	BESKRIVELSE
4.2.1	Gjennomgå loggdata og samle inn andre relevante data om hendelsen for å oppnå et godt beslutningsgrunnlag. Dette kan innebære innhenting og sammenstilling av data fra flere kilder, gjennomføre tester eller måling for å verifisere eller avkrefte en hendelse. Metode og omfang vil avhenge av type sikkerhetshendelse som har oppstått.
4.2.2	Gjennomfør en vurdering for å avgjøre om hendelsen er en mulig eller bekreftet sikkerhetshendelse eller om det er falsk alarm.
4.2.3	Kategoriser hendelsen i henhold til klassifiseringsregime og varsle nødvendige roller og interessenter i henhold til gjeldende varslingsprosedyrer.
4.2.4	Sørg for at alle involverte enheter loggfører alle aktiviteter, resultater og relevante avgjørelser for senere analyser. Personell som håndterer hendelsen bør etablere en tidslinje for egne og trusselaktørens aktiviteter.

4.3 KONTROLLER OG HÅNDTER HENDELSER (EFFEKTIVT)

Håndtere hendelser korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og slik at normaltilstand opprettholdes eller gjenopprettes effektivt.

HVORFOR ER DETTE VIKTIG?

Når en hendelse inntreffer er det fort gjort å slå alarm og sette himmel og jord i bevegelse. Det er da viktig å beholde roen, men samtidig varsle og involvere de riktige personene hurtig. Dersom virksomheten ikke forstår omfanget av et dataangrep, hvilke deler av IKT-infrastrukturen som er rammet og håndterer dette riktig, kan konsekvensene bli katastrofale.

Oppskriften er å følge fastsatte prosedyrer basert på klassifisering av hendelsen og involvere personell med spesialkompetanse på IKT-miljøet og den daglige driften. Uansett type hendelse vil det være en del felles prinsipper som sil gjelde. Hendelsen må undersøkes i form av utbredelse og skadepotensiale og hendelsesdata og situasjonsbildet bør holdes så oppdatert som mulig gjennom hele håndteringen av hendelsen. Man må være forberedt på eventuell eskalering og nye, samtidige hendelser og sørge for god kommunikasjonsflyt mellom involverte parter.

Reaktive tiltak må settes i gang så snart man har nok informasjon til å iverksette dette. En tommelfingerregel er at man har 2 timer fra «noe» skjer i Europa til man har tatt en beslutning i egen virksomhet på hvordan man skal agere. Alle aktiviteter og avgjørelser bør logges slik at man i etterkant kan følge utviklingen. Interne og eksterne som er berørt av hendelsen bør, så langt det lar seg gjøre, holdes oppdatert om situasjonen.

> «Det er viktig å beholde roen, men samtidig varsle og involvere de riktige personene hurtig.»

Når en hendelse har oppstått vil tillit til tjenester, systemer og IKT-infrastruktur naturlig nok svekkes. Effektiv hendelseshåndtering vil bidra til å gjenopprette dette slik at man igjen oppnår en tiltrodd og sikker tilstand i IKT-miljøet og tilhørende tjenester.

Handlingsmønster vil avhenge av hva slags type hendelse som har oppstått. Det er for eksempel forskjell på om en hendelse akkurat har oppstått og eskalerer i omfang eller om en hendelse har pågått over lengre tid, og er i en «stabil» fase. Under er eksempler på anbefalte handlinger ved ulike scenarier.

SCENARIO 1

Ved omfattende spredning av skadevare som selvspredende kryptovirus – **kast deg rundt og stopp angrepet!**

SCENARIO 2

Dersom «noen» har fått fotfeste i virksomheten og man ser at tilgangen har vært der i en lengre periode – **vent, observer, forstå, handle**. Er virksomheten utsatt for en avansert aktør med godt fotfeste, kan feil handling føre stil at aktøren går i dvale eller benytte mindre synlige angrepsmetoder. Dette vil gjøre det vanskeligere å avklare skadeomfang, sikre bevis og fjerne aktøren fra virksomheten.

4.3 ANBEFALTE TILTAK

ID	BESKRIVELSE
4.3.1	Undersøk hendelsen(e) som definert i henhold til klassifiseringsregime og kartlegg omfang og påvirkning på forretnings-prosesser.
4.3.2	Undersøk om hendelsen er under kontroll og gjennomfør nødvendige reaktive tiltak. Dersom hendelsens omfang øker og ser ut til å få alvorlige konsekvenser på virksomhetens forretningsprosesser bør kriseresponsaktiviteter iverksettes ved å eskalere til krisehåndteringsfunksjonen. Eksempler på reaktive tiltak er: • Allokering av interne og eksterne menneskelige ressurser for å håndtere hendelsen. • Innkapsling og blokkering av offensive handlinger for å hindre spredning. • Terminering av truende eller kompromitterende aktiviteter i systemer, for eksempel stenge ned kompromitterte, interne servere som kan benyttes av angripere for videre angrep på systemer og IKT-infrastruktur.
4.3.3	Oppdater hendelsesdata og situasjonsbilde underveis for best mulig datagrunnlag til håndtering av hendelsen.
4.3.4	Iverksett gjenopprettingsplan i løpet av, eller i etterkant av hendelsen. Tiltakene vil variere avhengig av type hendelse, men kan inkludere: • Reaktivere redundante ressurser som ble tapt eller skadet under hendelsesforløpet. • Reinstallere maskin- og programvare på rammede komponenter. • Gjenopprette konfigurasjonsinnstillinger, med eventuelle tilpasninger. • Gjenopprette tjenester som ble stoppet under hendelsesforløpet.
4.3.5	Koordiner og kommuniser med interne og eksterne interessenter underveis i hendelseshåndteringen. Dette kan være intern drift, ledelsen, interne eller eksterne avdelinger som blir påvirket av hendelsen.
4.3.6	Loggfør alle aktiviteter underveis i hendelseshåndteringen og sikre elektroniske bevis.
4.3.7	Gjennomfør aktiviteter etter hendelsen, herunder: • Etterforskning for å finne rotårsak til hendelsen, inkludert: – Type skadevare – Trusselaktør – Angrepsvektor – Verktøy – Operasjonsmåte, hvordan hendelsesforløpet utviklet seg og hvilke bevegelser og aksjoner trusselaktøren gjennomførte • Oppsummerende rapport som ledelsen kan forstå og ta stilling til. • Kommunikasjon til relevante parter, inkludert sektorvise responsmiljøer og/eller NSM NorCERT.

4.4 EVALUER OG LÆR AV HENDELSER

Lære av hendelser og gi forbedringsinnspill til sikringstiltak, hendelsesprosesser, opplæring av personell og oppdatering av gjeldende prosedyrer.

HVORFOR ER DETTE VIKTIG?

Når en hendelse er ferdig håndtert og lukket er det viktig at virksomheten hurtig identifiserer og lærer fra gjennomførte aktiviteter og handlinger og sørger for at konklusjoner blir gjennomgått og tatt tak i. Dersom dette ikke gjøres vil mye av kunnskapen og erfaringen fra håndterte hendelser forsvinne, og man vil ofte gjøre de samme feilene om igjen neste gang en hendelse oppstår. Det kan i tillegg være at det oppdages nye sårbarheter, eller behov for nye, eller forbedrede sikringstiltak underveis i håndteringen av hendelser, som kan forhindre at fremtidige situasjoner oppstår. Man ender ofte opp med en rekke potensielle forbedringer og tiltak, men det deles ofte inn i tre hovedområder:

1. Nye eller endrede krav til sikringstiltak av teknisk eller ikke-teknisk art. Dette kan inkludere oppdatering av bevisstgjøringsmateriell til brukere og oppdatering av sikkerhetsretningslinjer.
2. Ny eller endret trussel- og sårbarhetsinformasjon som kan føre til endring av virksomhetens metodikk for risikovurdering.
3. Endringer i planverk for hendelseshåndtering, prosesser, prosedyrer, rapporteringsformat, organisasjonsstrukturer, og så videre.

4.4 ANBEFALTE TILTAK

ID	BESKRIVELSE
4.4.1	Identifiser erfaringer og læringspunkter («lessons learned») fra sikkerhetshendelsen slik at både de momenter som virket videreføres og de som ikke virket optimalt kan forbedres.
4.4.2	Kartlegg og gjennomgå identifiserte, kompromitterte sikringstiltak og oppdater eller forny disse for å hindre at en tilsvarende hendelse gjenoppstår.
4.4.3	Gjennomgå, identifiser og forbered virksomhetens risikovurderinger der det er oppdaget verdier, sårbarheter, trusler eller tiltak som ikke er adressert i eksisterende risikobilde.
4.4.4	Gjennomgå effektiviteten på prosesser, prosedyrer, rapporteringsformater og organisatoriske strukturer i forhold til å respondere på hendelser. Oppdater prosesser og planer for hendelseshåndtering basert på læringspunktene.
4.4.5	Kommuniser og del erfaringsresultatene med relevante interessenter og bruk reelle historier fra hendelseshåndtering i opplæring og bevisstgjøring av ansatte.
4.4.6	Gjennomfør evalueringer av prosesser og personell tilknyttet hendelseshåndtering ved jevne mellomrom.

Vedlegg A – Kobling mellom Grunnprinsippene og tiltak ISO/IEC 27002:2017

KATEGORI	ID	GRUNNPRINSIPP	KONTROLL ISO 27002
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.8.1.1
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.8.1.2
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.8.2.1
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.13.1.2
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.17.1.1
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.17.1.2
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.18.1.1
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.18.1.2
Identifisere og kartlegge	1.1	Kartlegg leveranser og verdikjeder	A.18.1.4
Identifisere og kartlegge	1.2	Kartlegg enheter og programvare	A.8.1.1
Identifisere og kartlegge	1.2	Kartlegg enheter og programvare	A.8.1.2
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.6.1.1
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.1.1
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.1.2
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.2.1
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.2.2
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.4.1
Identifisere og kartlegge	1.3	Kartlegg brukere og behov for tilgang	A.9.4.4
Beskytte	2.1	Sikre anskaffelser	A.6.1.5
Beskytte	2.1	Sikre anskaffelser	A.7.1.2
Beskytte	2.1	Sikre anskaffelser	A.7.2.1
Beskytte	2.1	Sikre anskaffelser	A.13.1.2
Beskytte	2.1	Sikre anskaffelser	A.13.2.2
Beskytte	2.1	Sikre anskaffelser	A.14.1.1
Beskytte	2.1	Sikre anskaffelser	A.14.2.1
Beskytte	2.1	Sikre anskaffelser	A.14.2.3
Beskytte	2.1	Sikre anskaffelser	A.14.2.5
Beskytte	2.1	Sikre anskaffelser	A.14.2.6
Beskytte	2.1	Sikre anskaffelser	A.14.2.8
Beskytte	2.1	Sikre anskaffelser	A.14.2.9
Beskytte	2.1	Sikre anskaffelser	A.14.3.1
Beskytte	2.1	Sikre anskaffelser	A.15.1.1
Beskytte	2.1	Sikre anskaffelser	A.15.1.2
Beskytte	2.1	Sikre anskaffelser	A.15.1.3
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.6.2.1
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.9.4.2
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.9.4.4
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.12.1.4

KATEGORI	ID	GRUNNPRINSIPP	KONTROLL ISO 27002
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.13.1.1
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.13.1.2
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.13.1.3
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.14.2.5
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.17.1.1
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.17.1.2
Beskytte	2.2	Ivareta sikker design av IKT-miljø	A.17.2.1
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.12.5.1
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.12.6.2
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.14.2.2
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.14.2.6
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.14.2.7
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.14.2.8
Beskytte	2.3	Ivareta en sikker konfigurasjon	A.14.2.9
Beskytte	2.4	Ha kontroll på IKT-infrastruktur	A.6.2.1
Beskytte	2.4	Ha kontroll på IKT-infrastruktur	A.6.2.2
Beskytte	2.4	Ha kontroll på IKT-infrastruktur	A.13.1.1
Beskytte	2.4	Ha kontroll på IKT-infrastruktur	A.13.1.3
Beskytte	2.5	Ha kontroll på kontoer	A.7.3.1
Beskytte	2.5	Ha kontroll på kontoer	A.9.1.1
Beskytte	2.5	Ha kontroll på kontoer	A.9.1.2
Beskytte	2.5	Ha kontroll på kontoer	A.9.2.1
Beskytte	2.5	Ha kontroll på kontoer	A.9.2.2
Beskytte	2.5	Ha kontroll på kontoer	A.9.2.5
Beskytte	2.5	Ha kontroll på kontoer	A.9.2.6
Beskytte	2.5	Ha kontroll på kontoer	A.9.4.2
Beskytte	2.5	Ha kontroll på kontoer	A.9.4.3
Beskytte	2.6	Kontroller bruk av administrative privilegier	A.9.2.3
Beskytte	2.6	Kontroller bruk av administrative privilegier	A.9.4.2
Beskytte	2.6	Kontroller bruk av administrative privilegier	A.12.4.3
Beskytte	2.7	Kontroller dataflyt	A.13.1.2
Beskytte	2.8	Beskytt data i ro og i transit	A.6.2.1
Beskytte	2.8	Beskytt data i ro og i transit	A.6.2.2
Beskytte	2.8	Beskytt data i ro og i transit	A.8.2.2
Beskytte	2.8	Beskytt data i ro og i transit	A.8.2.3
Beskytte	2.8	Beskytt data i ro og i transit	A.8.3.1
Beskytte	2.8	Beskytt data i ro og i transit	A.8.3.3
Beskytte	2.8	Beskytt data i ro og i transit	A.10.1.1

KATEGORI	ID	GRUNNPRINSIPP	KONTROLL ISO 27002
Beskytte	2.8	Beskytt data i ro og i transit	A.10.1.2
Beskytte	2.8	Beskytt data i ro og i transit	A.13.2.1
Beskytte	2.8	Beskytt data i ro og i transit	A.13.2.2
Beskytte	2.8	Beskytt data i ro og i transit	A.13.2.3
Beskytte	2.8	Beskytt data i ro og i transit	A.14.1.2
Beskytte	2.8	Beskytt data i ro og i transit	A.14.1.2
Beskytte	2.8	Beskytt data i ro og i transit	A.14.1.3
Beskytte	2.9	Beskytt e-post og nettleser	A.13.2.3
Beskytte	2.10	Etabler hensiktsmessige logger	A.12.4.1
Beskytte	2.10	Etabler hensiktsmessige logger	A.12.4.2
Beskytte	2.10	Etabler hensiktsmessige logger	A.12.4.3
Beskytte	2.10	Etabler hensiktsmessige logger	A.12.4.4
Opprettholde og oppdage	3.1	Sørg for god endringshåndtering	A.12.1.2
Opprettholde og oppdage	3.1	Sørg for god endringshåndtering	A.12.5.1
Opprettholde og oppdage	3.1	Sørg for god endringshåndtering	A.14.2.2
Opprettholde og oppdage	3.1	Sørg for god endringshåndtering	A.14.2.3
Opprettholde og oppdage	3.1	Sørg for god endringshåndtering	A.14.2.4
Opprettholde og oppdage	3.2	Beskytt mot skadevare	A.6.1.3
Opprettholde og oppdage	3.2	Beskytt mot skadevare	A.6.1.4
Opprettholde og oppdage	3.2	Beskytt mot skadevare	A.12.2.1
Opprettholde og oppdage	3.2	Beskytt mot skadevare	A.12.6.1
Opprettholde og oppdage	3.3	Verifiser konfigurasjon	A.12.5.1
Opprettholde og oppdage	3.4	Gjennomfør penetrasjonstester og "red-team" øvelser	A.14.2.9
Opprettholde og oppdage	3.5	Overvåk og analyser informasjonssystemet	A.12.1.3
Opprettholde og oppdage	3.5	Overvåk og analyser informasjonssystemet	A.12.5.1
Opprettholde og oppdage	3.5	Overvåk og analyser informasjonssystemet	A.12.6.1
Opprettholde og oppdage	3.6	Etabler kapabilitet for gjenoppretting av data	A.12.3.1
Opprettholde og oppdage	4.1	Forbered virksomheten på håndtering av hendelser	A.6.1.3
Opprettholde og oppdage	4.1	Forbered virksomheten på håndtering av hendelser	A.6.1.4
Opprettholde og oppdage	4.1	Forbered virksomheten på håndtering av hendelser	A.7.1.2
Opprettholde og oppdage	4.1	Forbered virksomheten på håndtering av hendelser	A.17.1.1
Håndtere og gjenopprette	4.2	Vurder og kategoriser hendelser	A.6.1.3
Håndtere og gjenopprette	4.2	Vurder og kategoriser hendelser	A.6.1.3
Håndtere og gjenopprette	4.2	Vurder og kategoriser hendelser	A.16.1.2
Håndtere og gjenopprette	4.3	Kontroller og håndter hendelser	A.16.1.2
Håndtere og gjenopprette	4.3	Kontroller og håndter hendelser	A.16.1.4
Håndtere og gjenopprette	4.3	Kontroller og håndter hendelser	A.16.1.5
Håndtere og gjenopprette	4.3	Kontroller og håndter hendelser	A.16.1.7
Håndtere og gjenopprette	4.4	Evaluer og lær fra hendelser	A.7.2.2

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no