NASJONAL SIKKERHETSMYNDIGHET

NSMs grunnprinsipper for IKT-sikkerhet

Hva skjer fremover og hvordan er knytningen mot ISO?

Mandag 30 okt 2023

Are Søndenaa

E-læringkurs NSM grunnprinsipper for IKT-sikkerhet

All time high deltagelse i oktober 2022

«En DDos av kurssertifikater på LinkedIn»

Fun facts:

- Ca **22 000** som har fullført kurset
- Mer enn **30.000** har startet (**1%** prosent av befolkningen - 18-70år)
- Flere firmaer har publisert at kurset er obligatorisk for alle ansatte
- Mange toppledere har tatt kurset
- Mange studenter ved ulike universiteter har tatt kurset

NSM grunnprinsipper-IKT E-læring

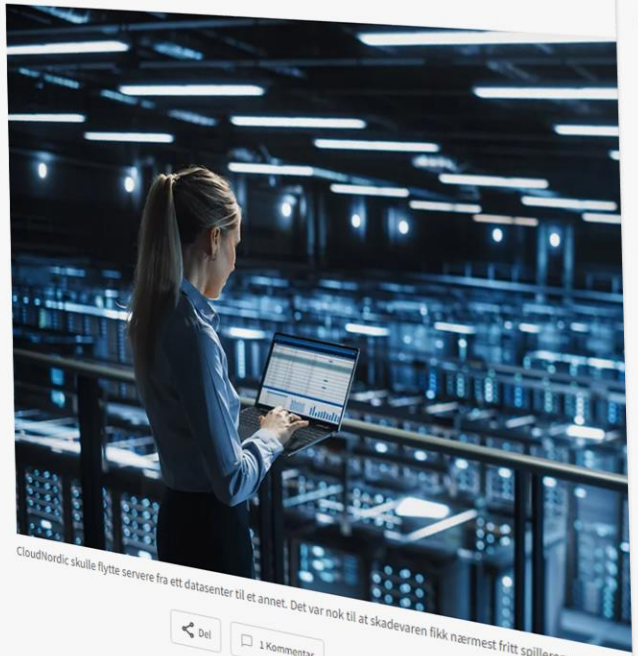
NSM

digi.no Ledige stillinger Nyhetsbrev Tips oss Abonner Logg inn Mer

SIKKERHET

Lammet av løsepengeangrep: Også backup av backupen er tapt

Selskapet verken kan eller vil betale kravet om løsepenger, og næ
data er tapt.



CloudNordic skulle flytte servere fra ett datasenter til et annet. Det var nok til at skadevaren fikk nærmest fritt spillerom. *Illustrasjo*

Del 1 Kommentar

Are Thunes Samsonsen Journalist

24. aug. 2023 - 05:00

nrk Nyheter Sport Kultur Humor Distrikt Mer Logg på

Norge Siste nytt Dokumentar Klima NRK Ytring

Tolv departementer utsatt for dataangrep

Det er foreløpig er usikkert hvem som står bak dataangrepet.

DATAANGREP: Direktør i DSS Erik Hope, kommunal- og distriktsminister Sigbjørn Gjelsvik (Sp) og Geir Arild Engh-Hellesvik i NSM orienterte i dag pressen om dataangrepene mot tolv departement.
FOTO: TERJE BENDIKSBY / NTB

Ingrid Uleberg
Journalist

Ola Mjaaland
Journalist

Sverre Holm-Nilsen
Journalist

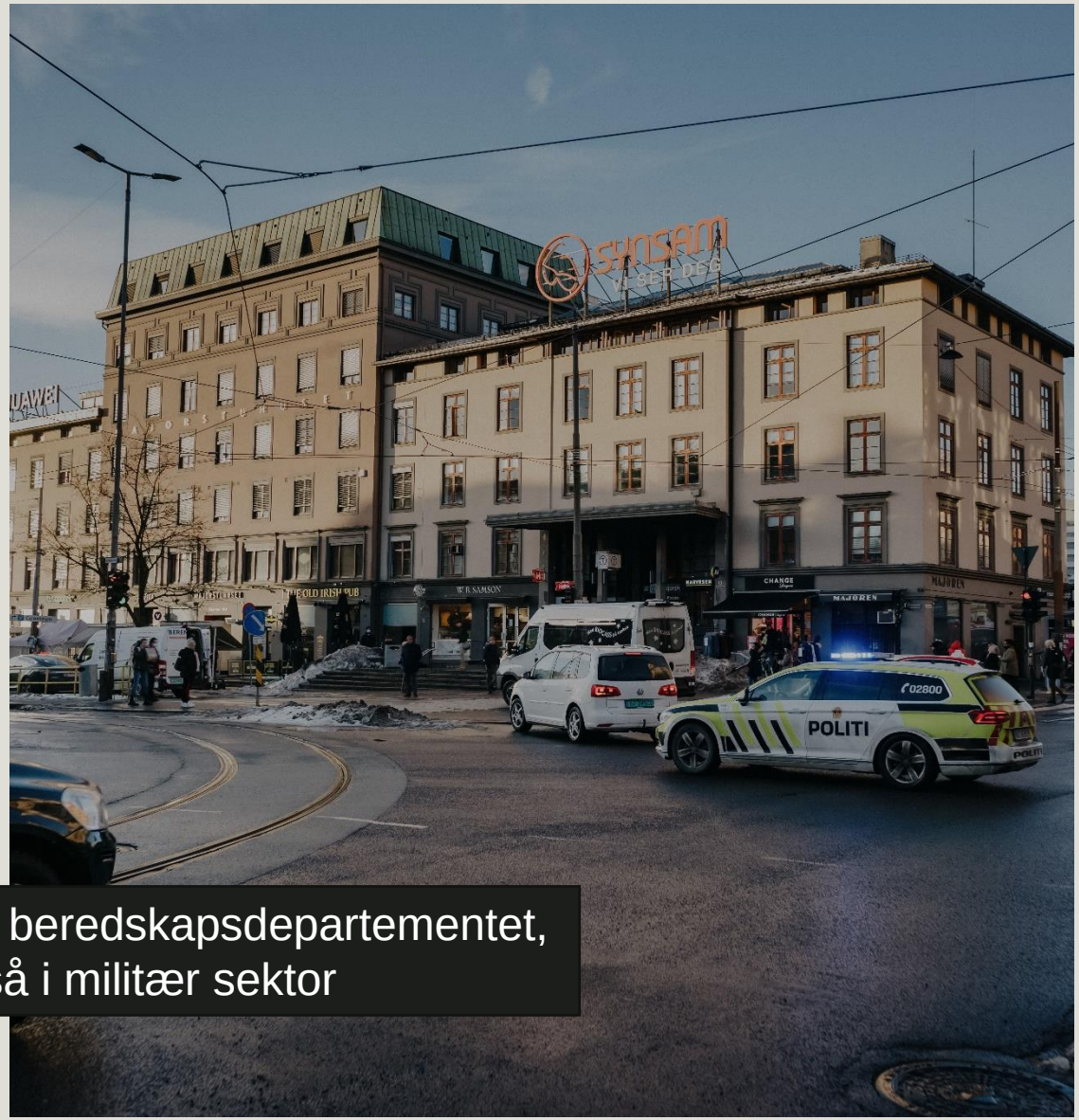
Publisert 24. juli kl. 08:41
Oppdatert 25. juli kl. 17:25

ANDY GREENBERG SECURITY JUL 12, 2023 4:34 PM

How a Cloud Flaw Gave Chinese Spies a Key to Microsoft's Kingdom

Microsoft says hackers somehow stole a cryptographic key, perhaps from its own network, that let them forge user identities and slip past cloud defenses.

NSM



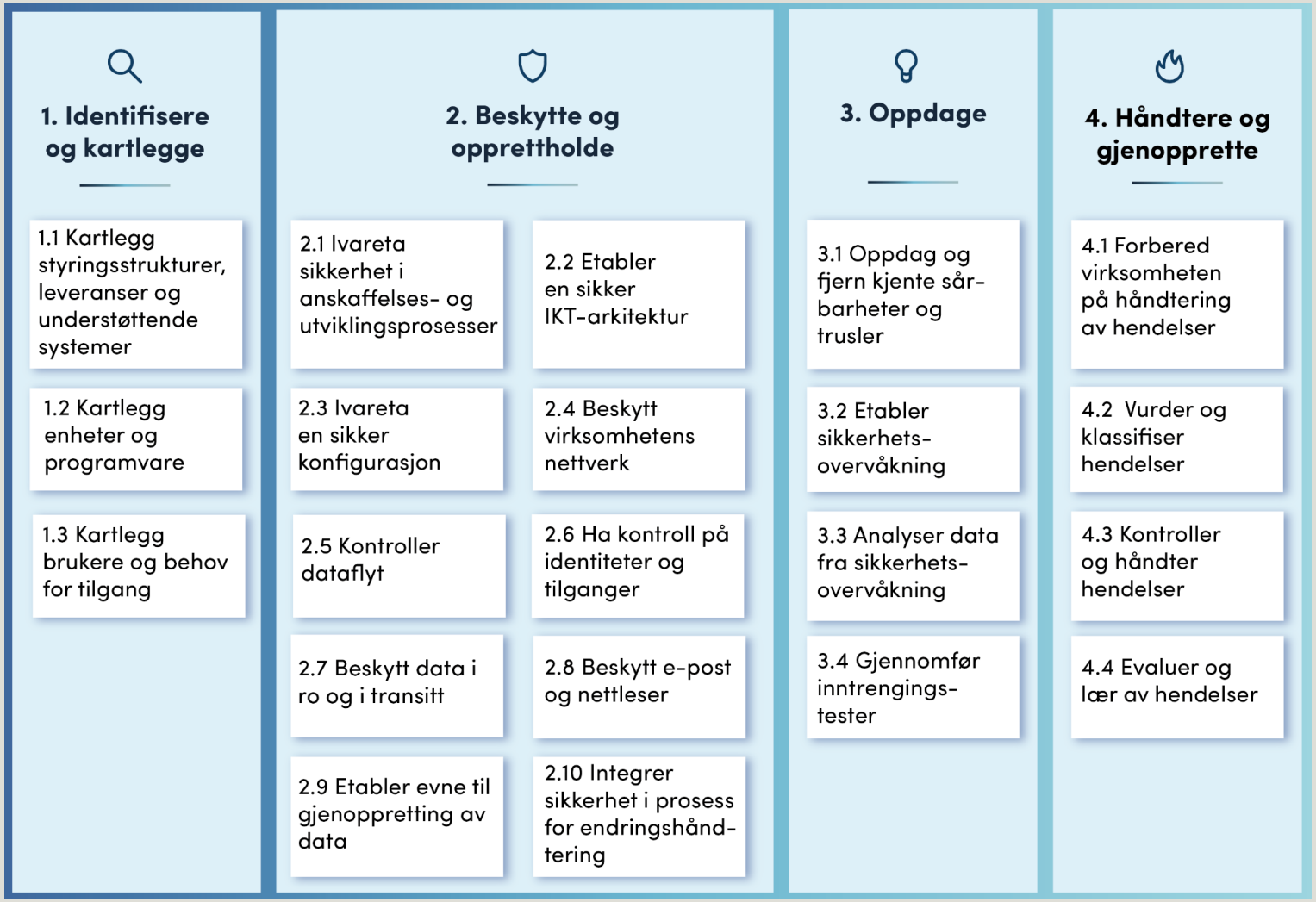
NSM er underlagt Justis- og beredskapsdepartementet, men opererer også i militær sektor


NSM
Risiko 2023
Økt uforutsigbarhet krever
høyere beredskap


NSM
Nasjonalt
digitalt
risikobilde
2023

NSM

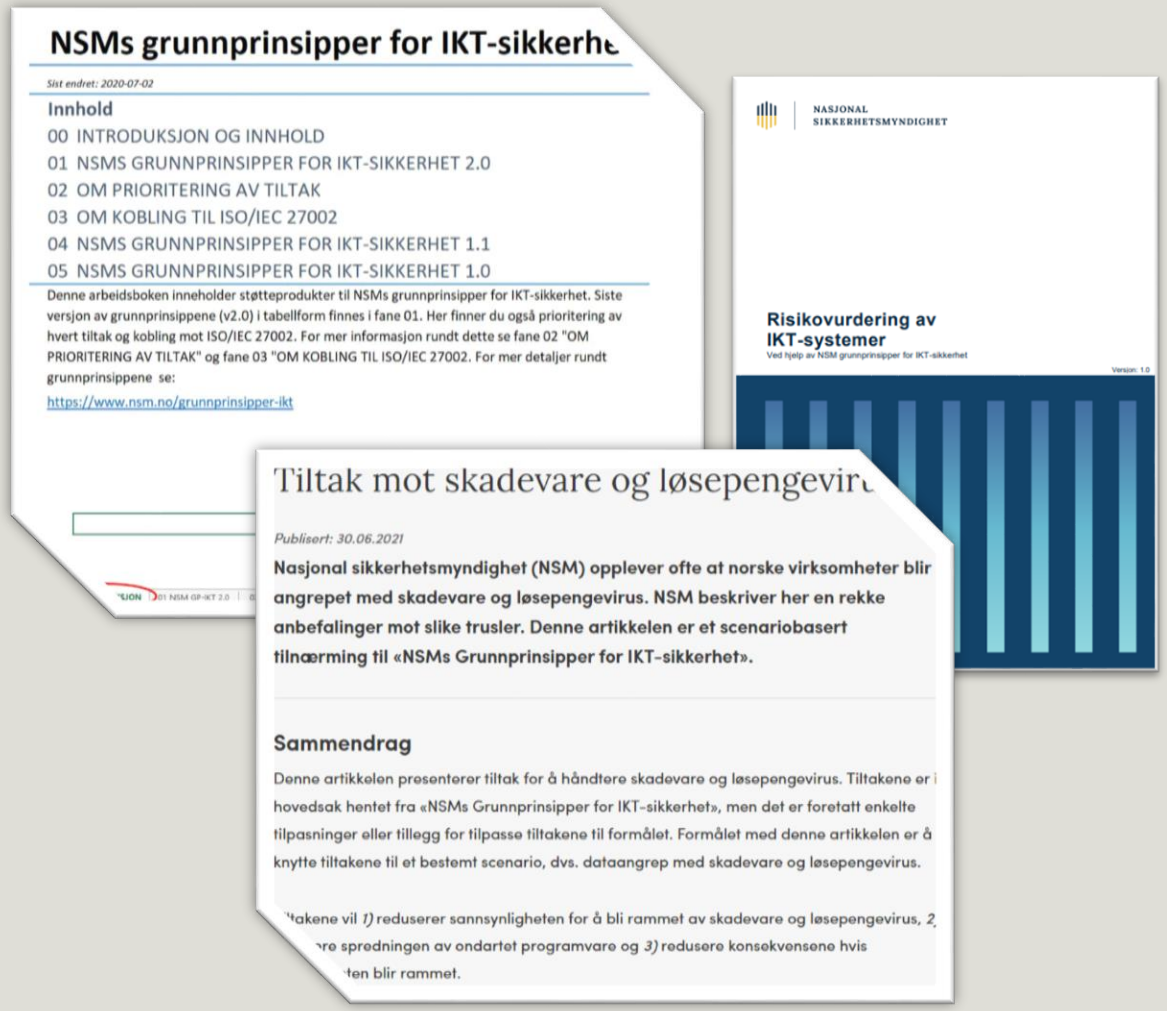
NSMs grunnprinsipper for IKT-sikkerhet (v 2.0)



Støtteprodukter og veien videre

- Regneark med sikkerhetstiltak
  - 15 tiltak – Prioritetsgruppe 1
  - 20 tiltak – prioriteringsgruppe 2
  - 83 tiltak – prioriteringsgruppe 3
  - **Kobling mot ISO 27002** (oppdatering på gang)
- Verktøy for risikovurdering
- Scenariobasert tilnærming
  - skadevare og løsepengevirus
- Ofte stilte spørsmål
- E-læringskurs
- Engelsk versjon (kommer)
- Versjon 3 (under planlegging)

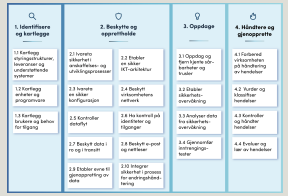
nsm.no/grunnprinsipper-ikt



Kobling mot ISO

Anbefalt rekkefølge ved implementering av tiltakene:

1. Prioritetsgruppe 1 (15 tiltak)
   - Inkludert 5 effektive tiltak
2. Prioritetsgruppe 2 (20 tiltak)
3. Prioritetsgruppe 3 (83 tiltak)



Totalt 118 tiltak

NSM GP-IKT

Prioritet 1

15 viktige tiltak
(5 effektive tiltak)

Prioritet 2

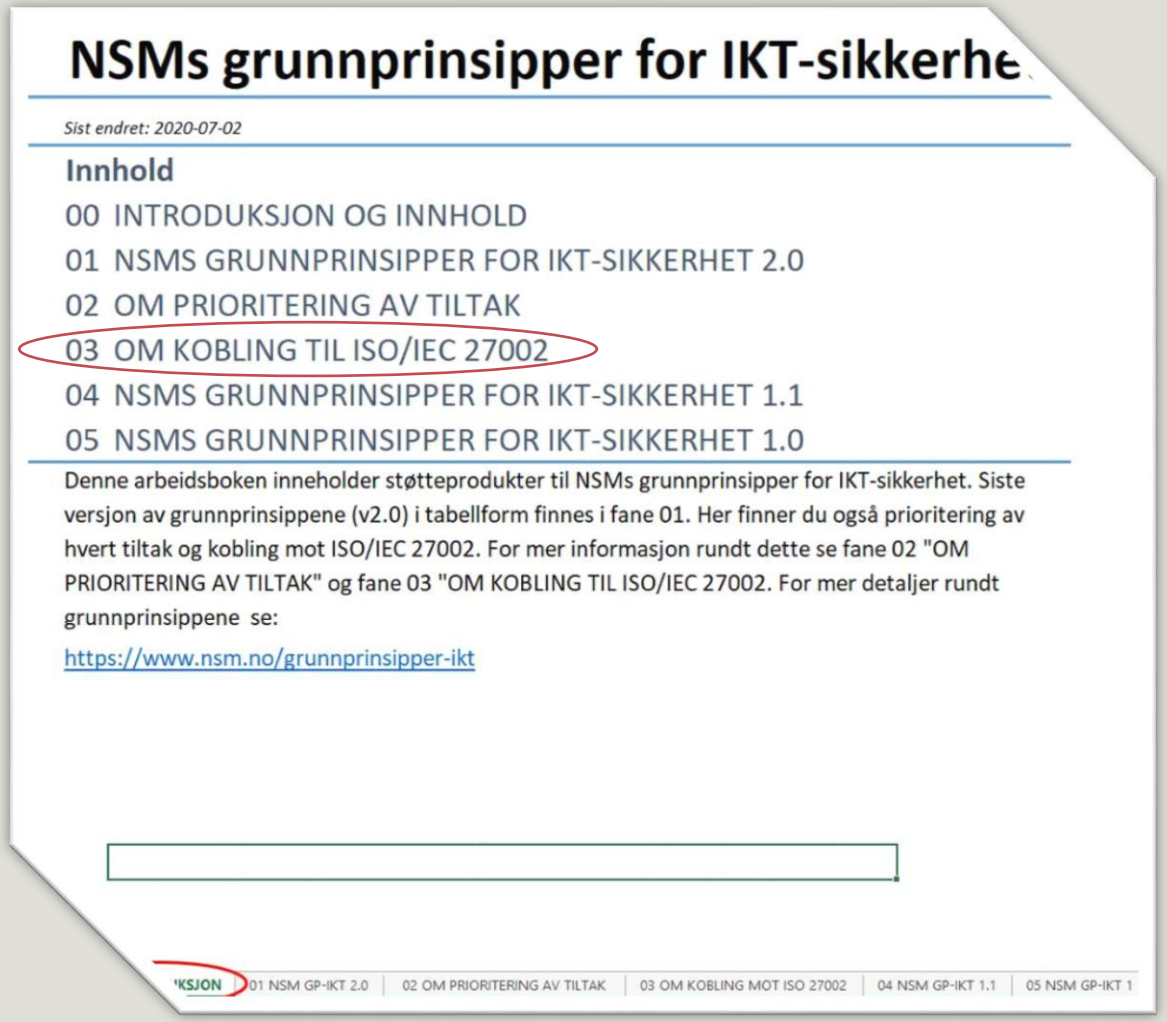
***20 tiltak* for videre-kommende**

Prioritet 3

***83 tiltak* som gir forsvar i dybden.**

ISO 27002

- Organisatorisk
- Personell
- Fysisk
- Teknologisk



NSMs grunnprinsipper for IKT-sikkerhe

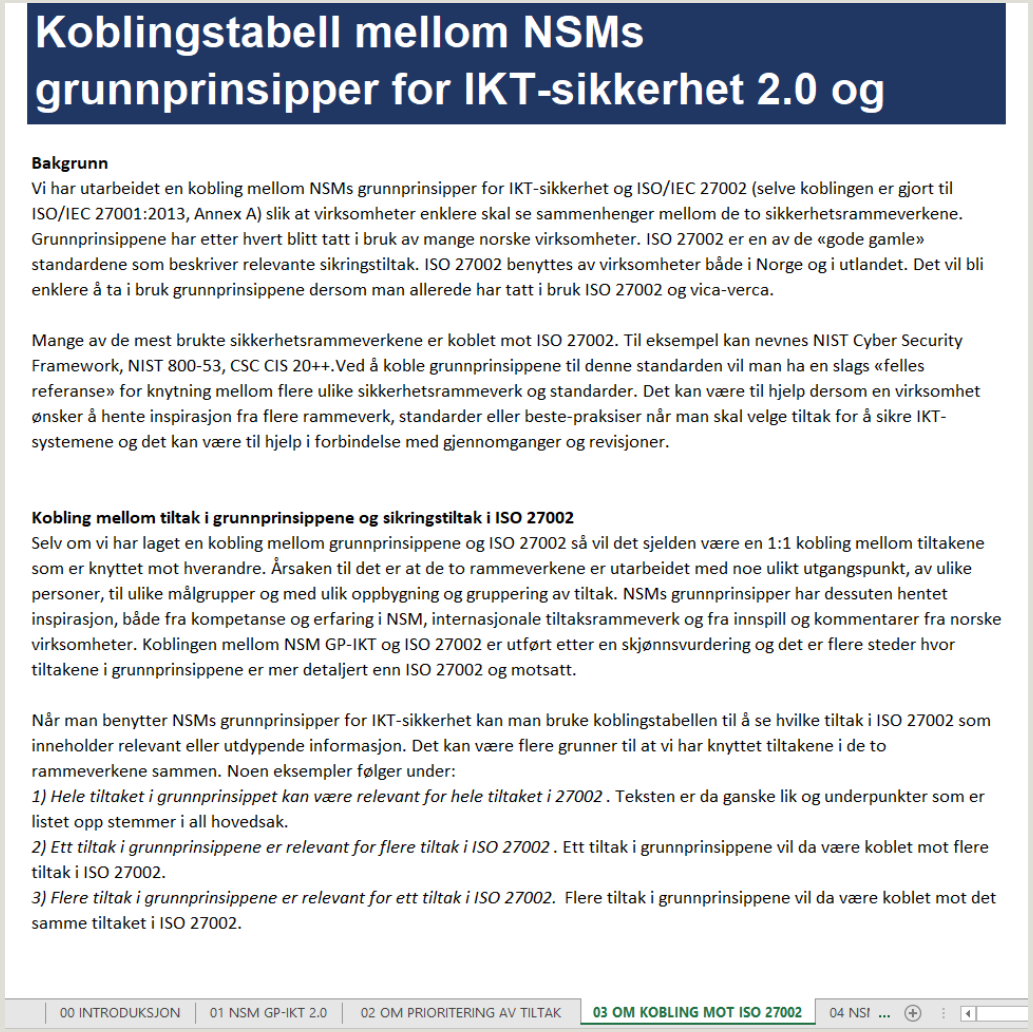
Sist endret: 2020-07-02

Innhold

Denne arbeidsboken inneholder støtteprodukter til NSMs grunnprinsipper for IKT-sikkerhet. Siste versjon av grunnprinsippene (v2.0) i tabellform finnes i fane 01. Her finner du også prioritering av hvert tiltak og kobling mot ISO/IEC 27002. For mer informasjon rundt dette se fane 02 "OM PRIORITERING AV TILTAK" og fane 03 "OM KOBLING TIL ISO/IEC 27002. For mer detaljer rundt grunnprinsippene se:

https://www.nsm.no/grunnprinsipper-ikt

'KSJON | 01 NSM GP-IKT 2.0 | 02 OM PRIORITERING AV TILTAK | 03 OM KOBLING MOT ISO 27002 | 04 NSM GP-IKT 1.1 | 05 NSM GP-IKT 1



Koblingstabell mellom NSMs grunnprinsipper for IKT-sikkerhet 2.0 og

Bakgrunn

Vi har utarbeidet en kobling mellom NSMs grunnprinsipper for IKT-sikkerhet og ISO/IEC 27002 (selve koblingen er gjort til ISO/IEC 27001:2013, Annex A) slik at virksomheter enklere skal se sammenhenger mellom de to sikkerhetsrammeverkene. Grunnprinsippene har etter hvert blitt tatt i bruk av mange norske virksomheter. ISO 27002 er en av de «gode gamle» standardene som beskriver relevante sikringstiltak. ISO 27002 benyttes av virksomheter både i Norge og i utlandet. Det vil bli enklere å ta i bruk grunnprinsippene dersom man allerede har tatt i bruk ISO 27002 og vica-verca.

Mange av de mest brukte sikkerhetsrammeverkene er koblet mot ISO 27002. Til eksempel kan nevnes NIST Cyber Security Framework, NIST 800-53, CSC CIS 20++.Ved å koble grunnprinsippene til denne standarden vil man ha en slags «felles referanse» for knytning mellom flere ulike sikkerhetsrammeverk og standarder. Det kan være til hjelp dersom en virksomhet ønsker å hente inspirasjon fra flere rammeverk, standarder eller beste-praksiser når man skal velge tiltak for å sikre IKT-systemene og det kan være til hjelp i forbindelse med gjennomganger og revisjoner.

Kobling mellom tiltak i grunnprinsippene og sikringstiltak i ISO 27002

Selv om vi har laget en kobling mellom grunnprinsippene og ISO 27002 så vil det sjelden være en 1:1 kobling mellom tiltakene som er knyttet mot hverandre. Årsaken til det er at de to rammeverkene er utarbeidet med noe ulikt utgangspunkt, av ulike personer, til ulike målgrupper og med ulik oppbygning og gruppering av tiltak. NSMs grunnprinsipper har dessuten hentet inspirasjon, både fra kompetanse og erfaring i NSM, internasjonale tiltaksrammeverk og fra innspill og kommentarer fra norske virksomheter. Koblingen mellom NSM GP-IKT og ISO 27002 er utført etter en skjønnsvurdering og det er flere steder hvor tiltakene i grunnprinsippene er mer detaljert enn ISO 27002 og motsatt.

Når man benytter NSMs grunnprinsipper for IKT-sikkerhet kan man bruke koblingstabellen til å se hvilke tiltak i ISO 27002 som inneholder relevant eller utdypende informasjon. Det kan være flere grunner til at vi har knyttet tiltakene i de to rammeverkene sammen. Noen eksempler følger under:

1) Hele tiltaket i grunnprinsippet kan være relevant for hele tiltaket i 27002 . Teksten er da ganske lik og underpunkter som er listet opp stemmer i all hovedsak.

2) Ett tiltak i grunnprinsippene er relevant for flere tiltak i ISO 27002 . Ett tiltak i grunnprinsippene vil da være koblet mot flere tiltak i ISO 27002.

3) Flere tiltak i grunnprinsippene er relevant for ett tiltak i ISO 27002. Flere tiltak i grunnprinsippene vil da være koblet mot det samme tiltaket i ISO 27002.

00 INTRODUKSJON | 01 NSM GP-IKT 2.0 | 02 OM PRIORITERING AV TILTAK | 03 OM KOBLING MOT ISO 27002 | 04 NSI ...

NSM

				Prioritet	Kobling mellom NSM GP-IKT 2.0 og ISO/IEC 27002:2013										
2															
3	Tiltak ID	Tiltaksoverskrift	Tiltaksbeskrivelse		A	B	C	D	E	F	G	H	I	J	K
56	2.6.1	Etabler retningslinjer for tilgangskontroll	**Etabler retningslinjer for tilgangskontroll. a)** Retningslinjene bør dekke flest mulig av ressursene i virksomheten: brukere, klienter, felles-mapper, server-applikasjoner, servere, nettverksenheter, sikkerhetsenheter og databaser. **b)** Retningslinjene bør følge minste privilegiums prinsipp; ikke gi sluttbrukere, service-kontoer, utviklere eller driftsbrukere flere privilegier enn nødvendig. Alle trenger ikke tilgang til alt. Og hvis man trenger tilgang så holder det ofte med lese-rettigheter, alle trenger ikke rett til å skrive, slette og kjøre. **c)** Alle kontoer bør kunne spores til en ansvarlig bruker (også upersonlige kontoer uten personnavn). **d)** Alle kontoer, tilganger og rettigheter bør spores til en ansvarlig rolle og person som godkjente dette. **e)** Kontoer, tilganger og rettigheter bør revideres jevnlig. Dette er spesielt kritisk mht. kontoer, tilganger og rettigheter for drift og spesialbrukere. **f)** Gjenbruk identiteter mest mulig på tvers av systemer, delsystemer og applikasjoner (ideelt «Single sign on»). **g)** Ansvarliggjør brukere mht. at passord er personlige og hemmelige og aldri skal deles med noen, selv ikke med nære kollegaer eller overordnede. Klienter bør i tillegg låses når de forlates av bruker.	2	A.9.1.1	A.9.1.2	A.9.2.3	A.9.2.4	A.9.2.5	A.9.3.1	A.9.4.2	A.11.2.8	A.11.2.9	A.12.6.2	
57	2.6.2	Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter	**Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter. a)** Prosessen bør omhandle **i)** *kontoer* til brukere, enheter og systemprosesser, **ii)** *tilganger* til systemer og applikasjoner, **iii)** samt *rettigheter* mht. operativsystemer (f.eks. admin-rettigheter) og virksomhetens felles brukerdatabase. **b)** Prosessen bør omfatte hele livssyklusen og omfatte opprettelse, vedlikehold og deaktivering. Deaktiver fremfor å slette kontoer og tilganger slik at revisjonsspor bevares, i henhold til gjeldende lover og regelverk. **c)** Retningslinjer for tilgangskontroll (2.6.1) og prosess for administrasjon av kontoer, tilganger og rettigheter (2.6.2.a) bør dokumenteres og være kjent i virksomheten.	2	A.9.2.1	A.9.2.2	A.9.2.5	A.9.2.6	A.9.4.1	A.12.6.2					
58	2.6.3	Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter	**Benytt et sentralisert og automatiserbart verktøy for å styre kontoer, tilganger og rettigheter. a)** Styr kontoer, tilganger og rettigheter til flest mulig av ressurser (ref. 2.6.2.a) i virksomheten med helst *ett* verktøy for hele virksomheten. **b)** Bruk verktøyet til å holde oversikt over alle kontoer, tilganger og rettigheter. Verktøyet bør kunne utføre mest mulig av retningslinjene i 2.6.1, **c)** Ved opprettelse av enkelte kontoer (f.eks. innleide) bør man sette foreløpige utløpsdatoer for deaktivering. **d)** Detekter og følg opp kontoer som ikke har blitt brukt på lenge dersom de ikke er nødvendige (overvåk unntak som f.eks. en leverandørs vedlikeholdskonto). **e)** Bruk et sentralt verktøy til å kontrollere passord-kvaliteten opp mot virksomhetens sikkerhetskrav, som et minimum bør man hindre bruk av vanlige ord og navn på norsk og engelsk, samt årstall og årstider.	2	A.9.4.1	A.9.4.3									
59	2.6.4	Minimer rettigheter til sluttbrukere og spesialbrukere	**Minimer rettigheter til sluttbrukere og spesialbrukere. a)** Ikke tildel administrator-rettigheter til sluttbrukere. **b)** Håndter spesialbrukere (f.eks. utviklere) som unntaksvis kan ha et faktisk behov for utvidede systemrettigheter, inkl. administrative rettigheter. Oppgavene bør skilles i to kontoer. En for vanlig kontorbruk som e-post og internett-søk og en annen for oppgaver som krever forhøyet («elevated») rettigheter. Disse kontoene bør ha tilstrekkelig sikkerhetsskille og som absolutt minimum ikke ha samme passord.	1	A.9.2.3	A.12.6.2									
	2.6.5	Minimer rettigheter på drifts-	**Minimer rettigheter på drifts-kontoer. a)** Etabler ulike kontoer til de ulike drifts-operasjonene (selv om det kanskje er samme person som reelt sett utfører oppgavene), slik at kompromittering av en konto ikke gir fulle rettigheter til hele systemet. Dvs. forskjellige drifts-kontoer for backup, brukeradministrasjon, klientdrift, serverdrift, mm. **b)** Begrens bruken av kontoer med domene-admin rettigheter til kun et minimum av virksomhetens drifts-operasjoner. Spesielt bør kontoer med domene-	1	A.9.2.3	A.9.4.4	A.13.1.1								

00 INTRODUKSJON | 01 NSM GP-IKT 2.0 | 02 OM PRIORITERING AV TILTAK | 03 OM KOBLING MOT ISO 27002 | 04 NSM GP-IKT 1.1 | 05 NSM GP-IKT 1.0

NASJONAL
SIKKERHETSMYNDIGHET

Takk for oppmerksomheten

www.nsm.no/grunnprinsipper-ikt

NSM

Fem effektive tiltak mot dataangrep

1. Installer sikkerhetsoppdateringer så fort som mulig, og mest mulig automatisk.
2. Ikke tildel administrator-rettigheter til sluttbrukere.
3. Ikke tillat bruk av svake passord, og bruk multifaktorautentisering der det er mulig.
4. Fas ut eldre IKT-produkter.
5. Tillat kun programvare som er godkjent av virksomheten eller enhetsleverandøren.

nsm.no/5tiltak

Tiltakene i prioritetsgruppe 1

15 viktige tiltak:

1. 1.2.3 Kartlegg enheter i bruk i virksomheten.
2. 1.2.4 Kartlegg programvare i bruk i virksomheten.
3. 2.1.2 Kjøp moderne og oppdatert maskin- og programvare.
4. 2.1.9 Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
5. 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
6. 2.3.1 Etabler et sentralt styrt regime for sikkerhetsoppdatering.
7. 2.3.2 Konfigurer klienter slik at kun kjent programvare kjører på dem.
8. 2.3.3 Deaktiver unødvendig funksjonalitet.
9. 2.3.7 Endre alle standardpassord på IKT-produktene før produksjonssetting.
10. 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere.
11. 2.6.5 Minimer rettigheter på drifts-kontoer.
12. 2.9.1 Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.
13. 3.2.3 Avgjør hvilke deler av IKT-systemet som skal overvåkes.
14. 3.2.4 Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
15. 4.1.1 Etabler et planverk for hendelseshåndtering.

Merknader: alt henger sammen med alt …

- Merknad til 1.2.3: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 1.2.4: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 2.1.2: Fokuser i første omgang på klientene.
- Merknad til 2.2.3: Bør sees i sammenheng med 2.5.1.
- Merknad til 2.3.2: Dette må tilpasses klient-operativsystem og applikasjoner.
- Merknad til 2.3.3: Fokuser i første omgang på klientene.
- Merknad til 2.3.7: Og vurder generelt passordkvaliteten i virksomheten, se 2.6.3.e.
- Merknad til 2.3.7: Og vurder å ta i bruk multi-faktor autentisering, se 2.6.7.
- Merknad til 2.9.1: Test sikkerhetskopier regelmessig ref. 2.9.3.
- Merknad til 3.2.3: Se tiltaket i sammenheng med bl.a. 3.2.4, 3.3.1 og 3.3.3.
- Merknad til 3.2.4: Se tiltaket i sammenheng med bl.a. 3.2.3, 3.3.1 og 3.3.3.
- Merknad til 4.1.1: Som minimum planlegg roller og ansvar ref 4.1.3. Og øv på dette, ref. 4.1.6.

NSM

Oppbygning av hvert prinsipp

Grunnprinsippet (overskriften)
- et anbefalt prinsipp som virksomheter bør følge

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og 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 eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf

NSM

Målet med prinsippet

- beskriver hva man skal oppnå ved å innføre grunnprinsippet

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og 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 eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk_sikkerhet/U-09_Sikring_av_NTP.pdf

Hvorfor er dette viktig?

- beskriver hvorfor grunnprinsippet er viktig og mulige konsekvenser dersom grunnprinsippet ikke blir implementert

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og 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 eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk_sikkerhet/U-09_Sikring_av_NTP.pdf

NSM

Anbefalte tiltak

- beskriver sikkerhetstiltak en virksomhet bør gjøre for å følge grunnprinsippet

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og 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 eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf

NSM

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og 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 eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

- beskriver «kjekt-å-vite-informasjon» om prinsippet og lenker hvor man kan finne utdypende informasjon

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf