NSM
SENTER FOR
ANVENDT KRYPTOLOGI

Kvantemigrasjon

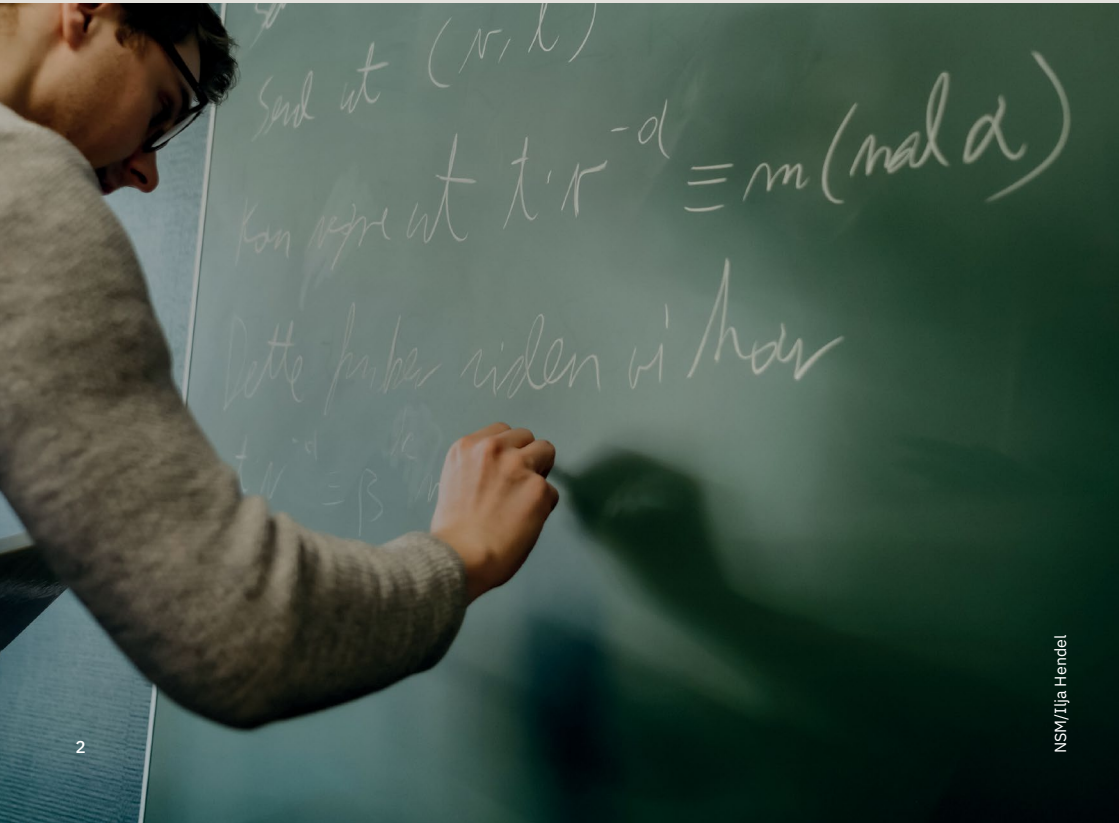
Veileder

Innledning

Utviklingen av nye kryptografiske standarder er i full gang internasjonalt. Disse erstatter de nåværende standardene. Dette er en omfattende prosess, som vil påvirke de aller fleste datasystemer som er i bruk. For noen vil dette arbeidet bunne ut i en enkel programoppdatering, for andre kan utskiftningen få store konsekvenser for daglig drift. For å gjøre endringsprosessen så smidig som mulig, er første bud at virksomhetene har oversikt over egne kryptoaktiva.

Denne veilederen gir en innføring i aktuelle problemstillinger og råd om hvordan virksomhetene kommer i gang. Veilederen retter seg spesielt mot systemeiere i offentlig som privat sektor som behandler sensitive opplysninger. Telekom, finans, helse, energi og olje er eksempler på områder som bør følge rådene.

Utfyllende informasjon og oppfølgere av denne veilederen vil fortløpende bli publisert på nsm.no/kvantemigrasjon.



NSM/Ilja Hendel

Kom i gang

NSM anbefaler å starte prosessen ved å gjennomføre en detaljert kartlegging av egen virksomhet. Kartleggingen skal gi svar på hvilke verdier virksomheten har og hvilken risiko som finnes. I tillegg må virksomheten skaffe oversikt over egen bruk av kryptografisk teknologi. Når denne kartleggingen er gjennomført, oppfordrer NSM virksomhetene til å starte dialogen om videre prosess med egne leverandører for å planlegge og budsjettere en overgang til nye standarder. Flyttingen av kryptografisk teknologi må skje trinnvis for å ivareta vanlig drift underveis.

Det er anbefalt å avvente standardiserte løsninger fremfor å gjennomføre forhastede anskaffelser av kvantesikker kryptografi. Forhastede anskaffelser kan være en sikkerhetsrisiko for virksomheten. NSM oppdaterer oversikt over anbefalte kryptografiske algoritmer på nsm.no/kvantemigrasjon. **Fem steg for en vellykket kvantemigrasjon:**

1. **Avgjør** hvor kritisk det er å beskytte virksomheten mot kryptografisk relevante kvantedatamaskiner
2. **Kartlegg** nåværende bruk av kryptografi
3. **Identifiser** hvilke nye standarder som passer best til egne systemer
4. **Planlegg** utskiftingen av kryptografiske standarder
5. **Gjennomfør** selve migrasjonen

Kritiske virksomheter versus andre virksomheter

Hele samfunnet skal på sikt gå over til kvantesikker kryptografi. Noen må gå foran, og det må være virksomheter som forsyner andre med kritiske tjenester. NSM gir eksempler på hvem som bør begynne med å bytte ut de kryptografiske standardene nedenfor. **Seks faktorer kan benyttes til å vurdere hvorvidt det er kritisk at din virksomhet kommer snarlig i gang med prosessen med å bytte ut nåværende kryptografiløsninger:**

1. **Angrepsflate**
   Bruker eller forsyner virksomheten infrastruktur som kan være sårbar overfor en kryptografisk relevant kvantedatamaskin?

2. **Systemtyper**
   Hvilke systemer drifter virksomheten? Hvilke konsekvenser kan oppstå dersom disse får nedsatt funksjonalitet?

3. **Informasjonstyper**
   Hvilken informasjon behandler virksomheten? Hvilke skader kan oppstå ved kompromittering, eller uautorisert og uoppdaget modifikasjon?

4. **Tidskritisk**
   Hvor lenge vil informasjonen leve? Hvilke konsekvenser kan det få om informasjonen blir kompromittert om ti år?

5. **Næringskjeder**
   Hvilke avhengigheter har virksomheten til andre? Hvilke andre virksomheter forsynes med data?

6. **Trusselnivå**
   Husk at alle virksomheter kan bli utsatt for cyberangrep

Virksomheter i følgende kategorier bør spesielt anse seg selv som kritiske

Virksomheter som behandler personopplysninger med lang levetid

Dette kan være offentlige tjenester som i stor grad behandler personopplysninger over lang tid, som NAV og Skatteetaten, legekontorer og sykehus, eller banker og forsikringsselskaper. Krypterte personopplysninger er et utsatt mål fordi informasjonen kan lagres nå og dekrypteres på et senere tidspunkt ved bruk av en kryptografisk relevant kvantedatamaskin. Når nye standarder er klare, vil trolig GDPR-lovgivingen utvides med krav om beskyttelse mot kryptografisk relevante kvantedatamaskiner.

Virksomheter som behandler hemmelige opplysninger

Dette kan være både sikkerhetsgradert informasjon og skjermingsverdig, ugradert informasjon. Det kan også gjelde strategiske opplysninger om varer, tjenester og teknologi som er underlagt eksportkontroll.

Virksomheter som forsyner kritisk infrastruktur

Eksempler på dette er forsyning av vann og energi, samferdsel, telekommunikasjon og helsetjenester. Hvis disse tjenestene blir utsatt for funksjonsfeil, kan det føre til store helsemessige eller økonomiske tap. Virksomheter som drifter skjermingsverdige objekter og grunnleggende nasjonale funksjoner tilhører denne kategorien.

Virksomheter som forsyner langlevd infrastruktur

Utstyr som produseres i løpet av det neste tiåret, er sannsynligvis sårbart overfor en fremtidig kryptografisk relevant kvantedatamaskin. De nye kvantesikre standardene krever mer av maskinvaren enn nåværende standard. Virksomheter som drifter systemer med lang levetid, eksempelvis over 20 år, bør derfor være spesielt oppmerksomme på at utstyret vil være tilrettelagt for utskiftning av kryptografiske komponenter uten langvarig tap av funksjonalitet. Det vil si at utstyret må oppfylle krav til kryptosmidighet. Eksisterende utstyr som ikke kan erstattes, bør skjermes med et ytre lag med kvantesikker kryptografi, såkalt hybridisering.

Gjennomgang av verdier og kryptoaktiva

Alle systemeiere i kritiske virksomheter bør gjennomføre en grundig gjennomgang av egne systemer. NSM anbefaler å utarbeide en oversikt over systemer som faller inn i minst én av følgende kategorier:

- Systemer som understøtter kritisk eller langlevd infrastruktur, grunnleggende nasjonale funksjoner eller skjermingsverdige objekter, jf. Sikkerhetsloven kapittel 7.
- Systemer som behandler minst én av følgende: Sikkerhetsgradert informasjon eller skjermingsverdig ugradert informasjon, strategiske varer, tjenester eller teknologi som er underlagt eksportkontroll.
- Sensitive personopplysninger.
- Systemer som benytter kryptografiske løsninger som forventes å være sårbare i møte med kryptografisk relevante kvantedatamaskiner. Dette inkluderer systemer som behandler data med levetid til tidligst 2030 eller benytter seg av logisk adgangskontroll basert på asymmetriske algoritmer. Se oppdatert liste over sårbare algoritmer på nsm.no/kvantemigrasjon.

Innledningsvis anbefalte NSM virksomheter å ta flytteprosessen trinnvis, i tillegg til å kartlegge nåværende bruk av kryptografi. Det er viktig med et fullstendig situasjonsbilde av virksomheten, derfor bør virksomheten gjennomføre en egen risikovurdering. På den måten kan man fremskaffe oversikt over flere områder som blir viktige i kvantemigrasjonen. **For å få best mulig oversikt over virksomhetens nåværende situasjon, anbefaler NSM at man går gjennom disse fire områdene:**

Risikovurdering

Kritiske virksomheter utfører allerede interne risikovurderinger. Disse bør ta utgangspunkt i at en potensiell trusselaktør er fleksibel og har tilgang på kryptografisk relevante kvantedatamaskiner. Det er nødvendig å anta at en trusselaktør vil unytte ny teknologi til å angripe hittil utilgjengelige svakheter i eksisterende teknologi. Dermed må virksomheten revurdere risikoen den står overfor.

Oversikt over egen bruk av kryptografi

Hver virksomhet må ha fullstendig oversikt over egne kryptografiske systemer og ressurser for at overgangen skal kunne gjennomføres på en sikker måte. Dette gjelder både program- og maskinvare, i tillegg til nye anskaffelser. Dersom en usikker kryptografisk komponent forblir i virksomheten, kan det fungere som en inngangsport til hele systemet.

Oversikten bør være så detaljert som mulig. Som et minimum bør den inneholde informasjon om hvorvidt hver enkelt ressurs er sårbar ovenfor kryptografisk relevante datamaskiner. I tillegg bør den beskrive hvilket kvantesikkert alternativ som er den beste erstatningen. Dersom ressursen er anskaffet av en ekstern leverandør må dette fremkomme i rapporten.

Oversikt over informasjon, systemer og verdier som forvaltes av virksomheten

Virksomheten må opprettholde en detaljert oversikt over hvilke verdier og data den forvalter for å avgjøre hvilke komponenter og systemer som skal ha høyest prioritet i flyttingen. **Listen bør inneholde følgende informasjon:**

- **Hvilken datatype** dette gjelder. Er den lagret, i bruk eller i transitt?
- **Hvor** dataen befinner seg.
- **Dataens verdi.** Er det krav til konfidensialitet?
- **Eventuell sikkerhetsgradering.**
- **Individuell risikovurdering** for hver gruppe av data.
- **Hvilke personer** som har tilgang på verdiene.

Oversikt over leverandører av kryptografiske tjenester og utstyr

Mesteparten av kryptografiske komponenter og systemer i norske virksomheter er anskaffet fra eksterne leverandører. Det er vesentlig at virksomheten har tett dialog med leverandør i overgangsprosessen, og sørger for at leverandør tilbyr mulighet for overgang til nye standarder.

Kritiske virksomheter må ha oversikt over egen kryptografiske verdikjede og alle leverandører involvert, inkludert leverandører av digitale sertifikater. Oversikten bør inneholde informasjon om alle produkter som er anskaffet, alle avtaler inngått og kontaktinformasjon til hver enkelt leverandører. Virksomheter bør kartlegge egne interne kommunikasjonssystemer, inkludert hjemmekontorløsninger og såkalt «skygge-IT».

Virksomheter som forsyner andre med kryptografiske løsninger, må begynne forberedelsene til å flytte egne kunder til kvantesikker kryptografi tidlig.

Senter for anvendt kryptologi utarbeider fortløpende veiledere og notater for å belyse kvantemigrasjonen.

For oppdaterte veiledere og mer informasjon, se nsm.no/kvantemigrasjon.

NSM skal bidra til å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler.

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00