VALGdirektoratet

Veileder i sikkerhet

Hvordan gjennomføre sikre valg i kommuner og fylkeskommuner

Versjon 2.2
10. mars 2023

Endringslogg

#	Punkt	Dato	Versjon	Hvem
1	-	09.03.23	2.1.	John Andreas Johnsen
2	5.1.1	10.03.23	2.2	John Andreas Johnsen

1 Innholdsfortegnelse

2 Innledning

Ett av Valgdirektoratets hovedmål er å bidra til en korrekt og sikker valggjennomføring med tillit i befolkningen. Denne sikkerhetsveilederen er ett av våre bidrag til kommunene og fylkeskommunene for å nå dette målet.

I veilederen finner dere som valgansvarlige i kommuner og fylkeskommuner konkrete råd slik at dere kan få på plass gode tiltak og etablere rutiner knyttet til:

- Sikring av valgmateriell og IKT-utstyr som skal brukes i forbindelse med valggjennomføringen
- Sikring av lokaler og IKT-utstyr for maskinell opptelling av stemmesedler
- Sikkerhetstiltak for oppbevaring av IKT-utstyr som skal benyttes
- Sikring av opptellingslokaler der telling av stemmesedler skal foregå
- Sikring av valglokalet der stemmegivning utføres
- Sikker infrastruktur og bruk av EVA applikasjonene

Den tekniske delen av veilederen retter seg mot IKT-personell i kommunene og fylkeskommunene for å sikre at applikasjonene brukes på en sikker måte og i en sikker infrastruktur.

2.1 Sjekkliste for å gjennomføre sikkerhetstiltak

Gode sikringstiltak kjennetegnes ved at de er hensiktsmessige og praktisk utformet slik at tiltakene blir enkle å følge og oppleves som relevante. Videre må det legges vekt på å oppnå forståelse av tiltakene og at det er gevinster ved å følge veiledningen i form av tillit til valggjennomføringen. Det er derfor av stor betydning at valgansvarlig i kommunene og fylkeskommunene setter seg inn i sikringstiltak og prosedyrer som etableres i kommunen.

For å bidra til dette, følger det med en sjekkliste som dere kan bruke for å kontrollere at tiltak i denne veilederen innføres. Denne finner dere som vedlegg til denne veilederen.

2.2 Sikkerhetstiltak tar tid å implementere

Sikkerhetstiltak, være seg organisatoriske, menneskelige eller tekniske tar lang tid å implementere. Tiltakene kan også i noen tilfeller være kostbare. Valgdirektoratet anbefaler derfor at veilederen gjennomgås i god tid før valggjennomføringen og at tiltakene planlegges og iverksettes slik at de er effektive under *hele* valggjennomføringen og ikke bare under valgting og opptelling.

Vi anbefaler videre at de tekniske tiltakene som omhandler bruk av EVA leses og planlegges sammen med teknisk personell. Merk at hoveddelen av de tekniske tiltakene også gjelder IKT-utstyr brukt til EVA Admin, ikke bare EVA Skanning.

2.3 Risiko og sårbarhetsanalyse

ROS er et viktig verktøy for å kunne styre risikoen igjennom valggjennomføringen.

Det forutsettes at kommunene gjør en risiko og sårbarhetsanalyse i forkant av valggjennomføringen. En ROS har to formål:

1. Avdekke mulige hendelser, risiko for at disse oppstår og en vurdering av konsekvensen.
2. Belyse hvilke tiltak som kan iverksettes for å redusere enten *sannsynligheten* for, eller *konsekvensen* av hendelsene.

Når ROS er gjennomført skal valgstyret beslutte om risiko og tiltak er akseptable. Dersom de konkluderer med at risikoen ikke akseptabel, må ytterligere tiltak iverksettes.

Det finnes mange metoder for risiko- analyse og håndtering. Flere kommuner og fylkeskommuner har det allerede i sitt daglige virke. Vi anbefaler at kommunene og fylkeskommunene benytter prosess og metode som allerede er etablert.

For de som ikke har dette i sitt daglige virke, så kan vi anbefale Digitaliseringsdirektoratet sine veiledere publisert på https://www.digdir.no/informasjonssikkerhet/om-risiko-og-risikovurdering/3048. Mal for risikovurdering ligger under «Gjennomføre risikovurdering» og lenker til https://www.digdir.no/informasjonssikkerhet/malar-og-eksempel/3164.

2.4 Mer om sikkerhet

Veilederen er utarbeidet av Valgdirektoratet og er blant annet basert på NSM sine publiserte sikkerhetsveiledere og rapporter. For å lese mer om sikkerhet og få tilgang til ytterligere veiledning og informasjon kan man besøke https://nsm.stat.no

Tiltakene i denne veilederen er å tolkes som et *minimumsnivå*. Flere kommuner har ytterligere sikkerhetstiltak i sin portefølje. Disse bør i tillegg tas i bruk.

NSM publiserer også jevnlig rapporter og veiledere. Flere av disse gir verdi i valggjennomføringen, men kan være omfattende. Her er en liste over anbefalte

veiledere og rapporter publisert av NSM. Disse er relevant i valggjennomføring og sikkerhetsarbeid i kommunene og fylkeskommunene generelt:

- Grunnprinsipper for IKT-sikkerhet versjon 2.0
- Grunnprinsipper for fysisk sikkerhet
- Veileder i sikkerhetsstyring
- Temarapport: Innsiderisiko
- Rapport: Risiko 2022
- Rapport: Nasjonalt digitalt risikobilde 2022

I tillegg publiserer både e-tjenesten og PST årlige åpne trusselvurderinger. Vi anbefaler at kommuner og fylkeskommuner holder seg oppdatert med disse vurderingene.

- PST: Nasjonal trusselvurdering 2022
- Etterretningstjenesten: Fokus

PST sin årlige åpne trusselvurdering publiseres normalt i februar.

3 Fysisk sikring

Alle kommuner og fylkeskommuner som gjennomfører valg bør tilrettelegge for fysisk sikring av lokaler og utstyr som skal benyttes under valggjennomføringen. Det innebærer å ha gode rutiner for hvem som har tilgang til valgutstyret samt hvordan dette oppbevares og fraktes.

3.1 Soneinndeling

Lokalene som benyttes bør inndeles i områder og bli definert som henholdsvis grønn og rød sone med ulike krav til sikring.

En hensiktsmessig soneinndeling og kontroll med sonene bidrar til å redusere trusler ved å:

- Redusere antall personer med tilgang til lokaler, valgmateriell og maskinvare
- Føre kontroll med personer med tilgang til lokalene
- Bevisstgjøre personell og øke sikkerhetsfokus

Under følger en nærmere forklaring av hvilke prinsipper som ligger til grunn for sonemodellen.

3.1.1 Grønn sone

En grønn sone er et område som er åpent tilgjengelig for allmennheten. Dette vil eksempelvis være fellesarealer og servicesenter i kommunen og fylkeskommune. Under valggjennomføringen er dette området der valgavlukker vil stå og observasjon av opptelling vil foregå.

I grønn sone er det ikke behov for særskilt vakthold eller overvåking. Sonen er ikke begrenset utover generelt oppsyn og åpningstider. Utenom åpningstid skal området være avlåst.

Grønn sone er sikret med:

- Avlåsing utenom åpningstid

3.1.2 Rød sone

Rød sone er et område som kun er tilgjengelig for personell med tjenstlige behov, for eksempel valgansvarlig, valgfunksjonærer som tar imot stemmer, opptellingspersonell eller IT-ansvarlig.

Personellet skal være akkreditert til dette området. Tilgang til området skal

registreres med informasjon om hvem og når vedkommende har vært i området gjennom hele valggjennomføringen. Det kan også eksistere flere røde soner hvor forskjellig personell har tjenstlig behov. Som et eksempel er det ikke nødvendigvis sikkert at personell som tar imot stemmer også har behov for tilgang til opptelling. Akkreditering må derfor definere hvilke røde soner medarbeidere har tilgang til.

I en rød sone vil man eksempelvis oppbevare maskinvare og valgmateriell som skal benyttes under valggjennomføringen. Rød sone er også opptellingsområde under opptelling. Under hele valggjennomføringen skal tilgang til de røde sonene være kontrollert av personell foran inngangen som kontrollerer at personer som skal inn er riktig akkreditert.

Det er den sentrale valgorganisasjonen i kommunen som er ansvarlig for utlevering av akkreditering til medarbeidere som skal ha tilgang.

Rød sone er sikret med:

- Avlåsing
    - Avlåsing kan erstattes med vakthold
- Registrering av alle som entrer og forlater sonen
    - Elektroniske dørlåser kan brukes for automatisk inn- og ut-registrering
    - Videoovervåking av inn- og ut-registrering kan også benyttes
- Innbrudds- og brannalarm

Personell som har tjenstlig behov for tilgang til disse områdene under valggjennomføringen, er i hovedsak:

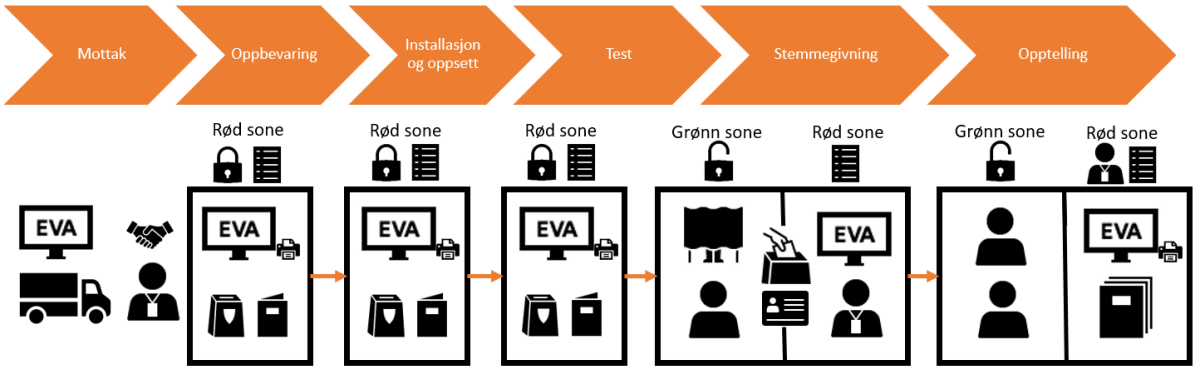
- Valgansvarlig i kommunen
- IT-ansvarlig under valggjennomføringen
- Valgfunksjonær med akkreditering og tildelt rolle i valggjennomføringen, eksempelvis:
    - Personell som jobber med opptelling
    - Personell som tar imot stemmer

Kommuner og fylkeskommuner som benytter seg av en skanning-leverandør anskaffet via Valgdirektoratets rammeavtale kan også gi personell fra leverandør tilgang til nødvendige røde soner.

3.2 Sikring av valgmateriell og IKT-utstyr

Anbefalingene til fysisk sikkerhet er til stede for å sikre maskinvaren og annet valgmateriell. Tiltakene er knyttet til å sikre lokaler der dette materiellet befinner seg. To eksempler på slikt utstyr er PCer som brukes med EVA Admin og stemmesedler.

Skissen under illustrerer soneinndeling under valggjennomføringen.



Denne kjeden har primært to kritiske hovedelementer:

- Tilgangskontroll for lokaler der materiell oppbevares
- Flytting eller overgang fra et ledd i leveransekjeden til et annet.

Valgmateriell og maskinvare som skal sikres med rød sone kan ikke bli stående i en sone med lavere nivå uten tilsyn. For eksempel vil man ikke lenger kunne sies å ha kontroll dersom en pall med PCer, eller annet valgmateriell blir stående i kommunens servicesenter eller varemottak over tid og således eksponeres for personell som ikke skal ha tilgang til dette materiellet.

I veilederen definerer vi «maskinvare» som IKT-utstyr som skal benyttes i valggjennomføringen. Dette omfatter blant annet:

- PCer der EVA-applikasjonene skal brukes
- Buypass smartkortlesere som skal brukes av EVA-applikasjonene
- Strekkodeskannere som skal brukes av EVA-applikasjonene
- Dokumentskannere som skal brukes av EVA Skanning
- Nettverksutstyr

3.2.1 Sikring før valggjennomføring

For å begrense hvem som har tilgang til materiellet og maskinvaren i forkant av valget, oppbevares dette til enhver tid i rød sone. Dette begrenser muligheter for sabotasje eller andre uønskede hendelser.

Kommuner og fylkeskommuner som benytter maskinvare fra eksisterende maskinvarepark til valggjennomføringen, må påse at disse til enhver tid av sin livssyklus har vært oppbevart innenfor det som kan betraktes som rød sone, eller under tilsyn av brukeren som har fått utlevert utstyret.

Valgmateriell og maskinvare til bruk i valggjennomføringen oppbevares i rød sone fra materiellet ankommer kommunen eller fylkeskommunen til valget er gjennomført og

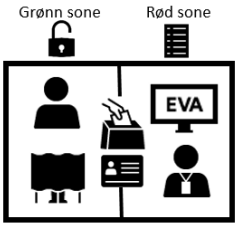
godkjent. Kun autorisert personell med særskilt tjenstlig behov skal ha tilgang. Eksempelvis valgansvarlig i kommunen og fylkeskommunen og IKT- ansvarlig i valggjennomføringen.

Ansatte/valgmedarbeidere som har med utstyr ut av rød sone, for eksempel med hjem til bruk i forbindelse med hjemmekontor, skal påse at utstyret er nedlåst i skap/skuff eller i forseglingspose når det ikke er i bruk. Nøkkel og utstyr kan ikke deles med andre (eksempelvis familiemedlemmer) som ikke har tjenstlig behov for tilgang til utstyret.

Denne sikringen gjelder for følgende lokaler:

- Oppbevaringsrom/lager for materiellet
- Lokaler for installasjon og oppsett
- Lokaler for test av maskinvare og valgmateriell

3.2.2 Lokaler for stemmegivning under valggjennomføringen



Mottak av forhånds- og valgtingsstemmesedler skal foregå i grønn sone, registrering av stemmegivninger i manntallet skal foregå i rød sone.

Av den grunn må man dele inn i to soner:

- Et grønt for publikum med stemmeavlukker
- En rød for maskinvare og manntall – tydelig adskilt fra publikum for å sikre valgets integritet og ivareta tilgangsbegrensning til maskinvaren og manntallet

I praksis betyr dette at stemmegivere aldri skal ha tilgang til PCer eller avkrysningsmanntall der stemmegivning registreres.

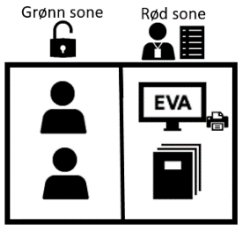
3.2.3 Transport av stemmesedler mellom stemmegivning og opptelling

Transporten av stemmesedler fra stemmegivning til opptelling er en kritisk del av verdikjeden og har følgende krav:

- Kjøretøyet som benyttes er å anse som rød sone fra transport starter til den avsluttes. Dersom det benyttes kollektiv eller kommersielle transportører er det kommunen eller fylkeskommunens ansvar å sikre at transportør oppfyller kravene til rød sone ved transport.
- Transporten skal skje i forseglede beholdere og på en slik måte at transporten er rask men sikker.

- Forsegling av beholdere skal gjøres før beholderne overleveres til transportør, og transportør skal ikke ha tilgang til forseglingsutstyr.
- Overlevering ved transportstart og -slutt skal alltid være bemannet og overlevering skal dokumenteres og kontrolleres av mottaker
- Ved overlevering til transportør skal det kvitteres ut:
    - Hvem som avleverer
    - Hvem som er transportør
    - Hva som overleveres
    - Hvor mange kolli, og hvilke kolli som overleveres
    - Tid for overlevering
    - Sted for overlevering
- Ved transportørs overlevering til opptellingssted skal det kvitteres ut:
    - Hvem som avleverer
    - Hvem som er mottaker
    - Hva som overleveres
    - Hvor mange kolli, og hvilke kolli som overleveres
    - Tid for overlevering
    - Sted for overlevering

3.2.4 Lokaler for opptelling under valggjennomføringen



Opptelling av stemmesedler skal være åpent tilgjengelig for publikum. Samtidig er det viktig at tilgang til maskinvare og valgmateriell begrenses for å minimere mulighetene for sabotasje eller andre uønskede tilsiktede eller utilsiktede hendelser.

Av den grunn må man dele inn i to soner:

- En grønn sone for publikum – for å tilfredsstille kravet om allmenn tilgjengelighet
- En rød sone for maskinvare og valgmateriell – tydelig adskilt fra publikum for å sikre valgopptellingens integritet og ivareta tilgangsbegrensning til materiell og maskinvare

Publikum og besøkende som ønsker å overvære opptellingen skal oppholde seg i grønn sone. Den røde sonen skal være et avgrenset område innenfor den grønne.

Maskinvare og valgmateriell som skal benyttes til opptellingen skal plasseres og oppbevares trygt innenfor rød sone. Kun autorisert personell skal ha tilgang til sonen. Sonen kan for eksempel avgrenses med sperrebånd. Vakthold besørges av eget personell eller av funksjonærer med tilgang til rød sone. Det er viktig at vakten har kontroll på at ingen uten akkreditering passerer avgrensningen mellom grønn og rød sone.

4 Organisasjon og mennesker

4.1 Anbefalte organisatoriske og menneskelige sikkerhetstiltak

I NSM sine veiledere er organisatoriske og menneskelige sikkerhetstiltak 2 forskjellige kapitler. Vi har valgt å slå disse sammen for å samle *minimumsnivået* av tiltakene under ett kapittel.

Hensikten med disse sikkerhetstiltakene er å sette opp menneskelige og organisatoriske barrierer mot tilsiktede uønskede handlinger.

Barrierene er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, adferd og/eller anvendelser av sikkerhetstiltak. Sikkerhetstiltakene kan blant annet etableres i form av skilting, opplæring og bruk av adgangskort.

4.1.1 Kompetanse

I opplæringen av valgmedarbeidere bør kommunene og fylkeskommunene påse at medarbeiderne også læres opp i sikkerhet. Opplæringen bør i hovedsak bygge på denne veilederen og kommunens planverk (se 4.1.3).

4.1.2 Personellsikkerhet

Det vies stor tillit til medarbeidere som jobber med valggjennomføringen. Valgmedarbeidere har bred tilgang i valgsystemene og utgjør således en risiko. Det er derfor viktig at kommunene og fylkeskommunene sikrer at valgmedarbeidere er til å stole på. Det er også viktig at personellet er klar over at de ufrivillig kan benyttes som en brikke i en større sikkerhetshendelse både uten at personellet vet om det, men også at man kan bli truet til å gjøre en handling.

Det er ikke nødvendig med sikkerhetsklarering på personell som jobber med valget med mindre personellet skal ha tilgang til gradert informasjon som trusselvurderinger og sårbarhetsrapporter. Valgstyret må likevel påse at alle som jobber med valggjennomføringen har hatt en sikkerhetssamtale om trusler, sikkerhetstiltak og rutiner med sikkerhetsansvarlig i valggjennomføringen.

4.1.3 Planverk

Kommunene og fylkeskommunenes planverk må inneholde relevante rutiner knyttet til sikkerhet. Disse må inneholde regler for hvordan valgmedarbeidere skal gjøre

jobben sin sikkert og hvordan andre organisatoriske tiltak skal utføres. Viktigst av disse er:

- Rutine for sikkert mottak av stemmesedler
- Rutine for transport av stemmesedler fra valglokale til opptellingslokale
- Regler for bruk av IKT utstyret
- Varslingsrutine for hendelser
- Tydelige kommunikasjonslinjer ved sikkerhetshendelser
- Sikkerhetsledelse
- Skilting
- Avlåsingsregime

Kommunene og fylkeskommunene bør også etablere et planverk for hendelseshåndtering som ivaretar behovet for kontinuiteten i valggjennomføringen ved beredskap og krise. Dette bør inkludere en oversikt over krav til gjenopprettelse av IKT- funksjoner, IKT-tjenester og IKT-systemer basert på en analyse av konsekvenser for virksomheten, rolle- og ansvarsbeskrivelser for relevant personell, krav til opplæring for relevant personell, klassifiseringsregime for hendelser og grenseverdier for å aktivere krisestab, krav til testing og øving av planverk og personell.

Det er viktig å revidere og oppdatere planverket jevnlig, minst en gang pr. valg og i etterkant av øvelser og større hendelser eller angrep.

4.1.4 Sikker tjenesteutsetting

Kommunene og fylkeskommunene er ansvarlig for sikkerheten ved tjenesteutsetting av IKT-leveranser.

Dette inkluderer å ha oversikt og kontroll på hele livsløpet til tjenesten(e) som skal settes ut, ivareta behovet for bestiller kompetanse (f.eks. forvaltning-, administrasjon- og IT- arkitekturkompetanse) gjennom hele livsløpet til tjenesteutsettingen, gjennomføre gode risikovurderinger som inkluderer hele livsløpet, utarbeide et kravdokument for alle faser av tjenesteutsettingen hvor krav kan verifiseres, avtaler om tjenesteutsetting av IKT-tjenester.

5 Informasjonssikkerhet ved bruk av EVA

5.1 Anbefalte sikkerhetstiltak ved bruk av EVA-applikasjonene

Under følger en oversikt over hvilke tiltak Valgdirektoratet anbefaler at kommuner og fylkeskommuner innfører dersom de skal benytte EVA applikasjonene. Anbefalingene i dette kapittelet omhandler bruk av alle EVA-applikasjonene og gjelder i alle fasene av valget, ikke bare under opptelling. For de som benytter EVA Skanning er det ytterligere noen anbefalinger beskrevet i et eget kapittel.

Samtlige anbefalinger gjelder også for kommuner og fylkeskommuner som benytter seg av teknisk bistand fra en tredjepart - avhengig av avtale vil disse dekke deler av rollen IKT-ansvarlig vanligvis har. Dette må avklares mellom den enkelte kommune eller fylkeskommune og leverandør av teknisk bistand.

Anbefalte sikkerhetstiltak vil bidra til å fjerne sårbarheter og redusere risiko på flere områder:

- Forebygge omdømmetap
  - For kommunen og/eller fylkeskommunen
  - For valggjennomføringen
- Opprettholde tilliten
  - Til valggjennomføringen
  - Til valgresultatet
- Forebygge forsinkelser
  - Forsinkelser i tilgjengeliggjøring av valgresultat
  - Omtelling av stemmesedler
- Forebygge manipulering
  - Av stemmegivning
  - Av valgresultat

De fleste kommuner benytter seg av Windows ved gjennomføringen av valget. Vi tar derfor dette som utgangspunkt i de tekniske anbefalingene. Benytter kommunen et annet operativsystem slik som iOS/Android på nettbrett, eller Linux/MacOS på PC må kommunen sette seg inn i innskrenkningsmekanismene som gjelder for nevnte operativsystem. Uavhengig av valg av operativsystem bør *prinsippene* i dette kapittelet følges.

5.1.1 Nye PCer

PCene som brukes til EVA bør være nye, eller være i et kontrollregime som ivaretar kravene til sikkerhet. Gamle maskiner som brukes må ha vært sikret iht. punkt 3.2 i veilederen gjennom hele sitt livsløp.

Disse kravene stilles for å sikre kommunene mot at uvedkommende får uautorisert tilgang til EVA, eller på andre måter angriper maskinene.

Disse tiltakene minimerer risikoen for at valggjennomføringen i kommunen hindres, eller at det sås tvil om at valgresultatet i kommunen er riktig.

Anbefalingene knyttet til PCer stilles for å i større grad skape sikkerhet rundt opphav og oppbevaring av PCene som brukes i valggjennomføringen.

Maskiner som har blitt brukt i valggjennomføringen bør tømmes og settes opp på nytt når valget er over og før maskinene blir brukt til andre ting. Dette for å sikre at sensitiv valgdata ikke kommer på avveie.

5.1.2 Windows 10 Enterprise

Windows-PCer hvor EVA benyttes skal kjøre operativsystemet Windows 10 Enterprise.

Kravet om bruk av Windows 10 Enterprise stilles for å begrense internett- og applikasjonstilgang fra PCene ved hjelp av innskrenkningsmekanismer som kun finnes i denne versjonen av Windows. Ved hjelp av disse mekanismene vil det kun være mulig å bruke applikasjoner og internett-tjenester som er nødvendige for å bruke EVA. Alle andre tilganger og applikasjoner kan blokkeres.
Ved å begrense applikasjons- og internett- tilgangen på PCer der EVA brukes, begrenses også angrepsflaten og mulighetene for kompromittering.

5.1.3 Kontrollert fjerntilgang

Fjerntilgang for leverandører av teknisk støtte til kommunene må skje i kontrollerte former og under overvåkning av autorisert personell hos kommunen/fylkeskommunen.

Vedvarende fjerntilgang må derfor deaktiveres på maskiner som skal benyttes til EVA. Skulle det være nødvendig med fjerntilgang for å utføre støtte, skal denne initieres av autorisert personell fra EVA maskinen i det den skal benyttes.

Det er den enkelte kommune eller fylkeskommune som bestemmer om man vil benytte seg av fjernaksess, og når dette skal skje. I så fall må kommunen eller fylkeskommunen åpne for dette i henhold til en avtalt prosedyre med utveksling av nødvendige koder for å kunne logge seg inn.

5.1.4 Maskiner skal låses når de forlates

I rød sone

Operativsystemet skal låses når maskinen forlates slik at uvedkommende ikke får tilgang til det den innloggede brukeren har tilgang til.

I grønn sone

Forlates maskinen i en grønn sone skal maskinen også låses ned i skuff, skap eller liknende, eventuelt kan maskinen legges i en forseglingspose. Se kapittel om fysisk sikring. Hjemmekontor er definert som «grønn sone».

5.1.5 Bruker er personlig og skal ikke benyttes av andre

Alle som jobber i EVA-applikasjonene får tildelt personlige brukere og det er derfor aldri behov for å låne bort sin personlige bruker. Lånes brukeren bort kan det føre til at du selv blir ansvarlig for feil andre måtte gjøre.

5.1.6 Standardpassord

Endre alle standardpassord på all maskinvare før produksjonssetting. Dette inkluderer applikasjoner, operativsystemer, rutere, brannmurer, skrivere, og skannere. I den grad maskinvaren støtter det, bør man benytte sertifikatbasert autentisering og redusere mulighet for passordbasert autentisering over nettverket.

5.1.7 Oppgrader program- og maskinvare og installer sikkerhetsoppdateringer

Nyere produktversjoner inneholder funksjonelle og sikkerhetsrelaterte forbedringer, og de har ofte flere og bedre sikkerhetsfunksjoner.

Sørg for å kun benytte IKT-produkter som støttes og mottar sikkerhetsoppdateringer fra leverandøren. Eldre IKT-produkter må fases ut. Der det er hensiktsmessig, for eksempel ved tjeneste-leverandør bør man be leverandøren (som kjenner IKT-produktet best) i å informere om risikoer og sårbarheter produktet kan utsettes for og spesifisere nærmere hvordan IKT-produktet kan sikkerhets-herdes og beskyttes.

Selv de beste produktene har feil og sårbarheter som kan utnyttes av angripere. Systemeiere må etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og fastvare. For Windows 10 oppdateringer bør serveren

wsus.valg.no benyttes. Oppdateringer som hentes fra denne serveren er testet til å fungere sammen med EVA applikasjonene.

5.1.8 Ikke tildel administrator-rettigheter til sluttbrukere

De fleste valgmedarbeidere har ikke behov for administrator-rettigheter. I et sentralt administrert system kan valgmedarbeidere få den programvaren de trenger fra et felles distribusjonspunkt. Det er heller ikke behov for administrator-rettigheter for å kunne bruke EVA-applikasjonene.

5.1.9 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.

Ved installasjon av EVA Skanning blir en AppLocker policy også satt opp på maskinen. Til EVA Admin anbefales det å bruke AppLocker konfigurasjonen som ligger tilgjengelig i vedlegg 3.

5.1.10 Deaktiver enheter og funksjonalitet som ikke brukes

Deaktiver enheter og funksjonalitet, som ikke skal brukes under valget, i klientene. Som et minimum bør wifi og bluetooth deaktiveres, men enheter som kamera, infrarød, pcmcia, firewire og com/lpt porter bør også deaktiveres. Den sikreste måten å deaktivere dette på er i maskinens fastvare, eksempelvis BIOS. Se leverandørens dokumentasjon på hvordan dette gjøres.

5.1.11 Herde applikasjoner

Protected Mode/View for nettleseren, Microsoft Office og Adobe Reader begrenser skadeomfanget ved kompromittering. Deaktiver unødvendig mobil kode og makroer. For å herde f.eks. Windows og Microsoft Office kan Microsoft Security Compliance Toolkit[1] benyttes.

Enhver ny applikasjon og funksjon øker mulighetene for angrep. Valgmedarbeidere har for eksempel ikke behov for Java Runtime eller JavaScript i Adobe Reader. Unødvendig programvare bør fjernes. Som minste krav må de herdes og holdes oppdatert, noe som øker administrasjonsbyrden på systemet.

[1] https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

5.1.12 Bruk klientbrannmur

Windows Brannmur støtter kun filtrering basert på applikasjon og/eller lag 3 (IP, Port) og baserer seg eksempelvis ikke på domenenavn. Windows Brannmur bør settes opp slik at den blokkerer all trafikk initiert utenfra og kun åpner for nettleseren som skal benyttes og annen nødvendige trafikk, som DNS, WSUS og DHCP ut fra klienten.

Vi anbefaler bruk av nettleseren Chrome. Via GPO bør man så konfigurere Chrome til å kun tillate tilgang til en liste med domener/URL-er. Valgdirektoratet vedlikeholder en slik liste nødvendig for EVA i vedlegg 2.

Brannmuren bør også settes opp slik at den logger sikkerhetsrelevante hendelser. Disse loggene bør inspiseres regelmessig.

5.1.13 Bruk sikker oppstart og diskkryptering

Sikker oppstart (Secure Boot) og Windows BitLocker bruker maskinvare og harddiskkryptering for å oppdage manipulering av oppstartsprosessen og forhindre tap av data fra stjålne/tapte PC'er.

5.1.14 Bruk antivirus/antiskadevare

Antivirus oppdager og blokkerer kjent skadevare som bl.a. utnytter sårbarheter i epost-programmer og dokumentlesere. Fortrinnsvis bør man bruke et produkt som kan styres sentralt og som virker bra sammen med operativsystemet.

5.1.15 Monitorering

Valgdirektoratets verktøy for monitorering av operativsystemet bør også installeres. Verktøyet vil monitorere aktivitet som utføres på klienten den er installert på og vil gjøre det mulig for Valgdirektoratet å bruke loggene ved en eventuell hendelseshåndtering.

6 Ekstra tiltak ved bruk av EVA Skanning

6.1 Anbefalte sikkerhetstiltak ved bruk av EVA Skanning

For å telle stemmer maskinelt ved å benytte EVA Skanning har vi utarbeidet en liste med ekstra tiltak for denne maskinvaren. Det er viktig at alle tiltakene i kapittel 5 også er gjennomført. Denne listen er ytterligere tiltak spesielt rettet mot maskinell telling.

6.1.1 Installasjon av EVA Skanning

Installasjon og oppsett av EVA Skanning skal følge installasjonsveiledningen som distribueres med EVA Skanning. Installasjonsprosessen er utformet for å gi en mest mulig kontrollert og sikker installasjon av EVA Skanning.

6.1.2 Tilstandsrapportering

Av sikkerhetshensyn ønsker Valgdirektoratet å kjenne tilstanden for PCer der EVA Skanning er installert for maskinell telling av stemmesedler. PCer der EVA Skanning er installert og som brukes til maskinell telling av stemmesedler vil derfor kontinuerlig rapportere sin tilstand til Valgdirektoratet.

Dette gjøres for å kunne avdekke avvik i oppsett og konfigurasjon som kan utgjøre en sikkerhetsrisiko, samt innhente statistikk om hvor mange PCer som er i bruk ved maskinell telling av stemmesedler ved en valggjennomføring for på den måten å forbedre tjenesten for maskinell telling av stemmesedler.

6.1.3 Nettverk

Nettverket der EVA Skanning benyttes må sikres. Det fysiske nettverket (kabling, switcher, brannmurer, etc) må sikres i henhold til rød sone.

Anbefalte tiltak:

- Sett opp et dedikert kablet nettverk til bruk for EVA Skanning
    - Trådløst nettverk bør ikke benyttes
- Beskytt nettverket med perimetersikring mot omverden som kun tillater absolutt nødvendig trafikk ut (se egen liste) og blokkerer all trafikk inn
- Autoriser kun enheter som skal ha tilgang til nettverket

- Trafikk mellom enheter krypteres
- Sikre nettverket fysisk slik at man har kontroll på antall nettverkskontakter, kontaktenes plassering og tilkoblede enheter
- Benytt portsikkerhet, eksempelvis IEEE 802.1X

6.1.4 Perimetersikring

Perimetersikring i dette tilfellet handler om konfigurering av brannmur og/eller annen beskyttelse av det lokale nettverket der EVA Skanning er installert. For at EVA Skanning applikasjonen skal fungere må det legges inn åpninger i perimetersikringen. Dette kan for eksempel være brannmurer og andre mellomtjenere. Valgdirektoratets IP adresser er 62.92.129.0/24 og vi anbefaler at det åpnes for alle protokoller mot vårt nettverk. Valgdirektoratet vedlikeholder også en liste med domener ut over våre egne IPer i vedlegg 2.

Noen av domenene i listen vi vedlikeholder står bak CDN-nettverk hvor IP adresser kan endre seg. Det anbefales derfor å benytte perimetersikring som kan basere seg på domenenavn istedenfor bare IP:port.

7 Vedlegg

- Vedlegg 1: Sjekkliste
- Vedlegg 2: Lister med domener og URL-er
- Vedlegg 3: AppLocker konfigurasjonsfil