VALGdirektoratet

Veileder for gjennomføring av valg

Teknisk veileder i bruk av EVA Skanning for kommuner og fylkeskommuner

Versjon 1.1
14. januar 2019

Innholdsfortegnelse

1 Innledning 2

2 Brukervilkår EVA Skanning 3

2.1 Tekniske krav til utstyr for å benytte EVA Skanning 3

2.1.1 Databaseserver 3

2.1.2 Dokumentskanner 4

2.1.3 PC til bruk med EVA Skanning 4

3 Sikkerhet ved maskinell telling av stemmesedler – EVA Skanning 5

3.1 Anbefalte sikkerhetstiltak ved bruk av EVA Skanning 5

3.1.1 Nye PCer 6

3.1.2 Windows 10 Enterprise 6

3.1.3 Fysisk sikring 6

3.1.4 Installasjon av EVA Skanning 6

3.1.5 Rutine for rullering av opptellingsstasjoner 6

3.1.6 Manuelle stikkprøver av skannede kasser med stemmesedler 7

3.1.7 Overvåkning 7

3.1.8 Nettverk 8

3.1.9 Kontrollert fjerntilgang 8

3.1.10 Maskiner skal låses når de forlates 8

3.1.11 Bruker er personlig og skal ikke lånes 8

3.1.12 Oppgrader program- og maskinvare 9

3.1.13 Installer sikkerhetsoppdateringer så fort som mulig 9

3.1.14 Ikke tildel administrator-rettigheter til sluttbrukere 9

3.1.15 Blokker kjøring av ikke-autoriserte programmer («hvitelisting») 9

3.1.16 Aktiver kodebeskyttelse mot ukjente sårbarheter 9

3.1.17 Herde applikasjoner 9

3.1.18 Bruk klientbrannmur 10

3.1.19 Bruk sikker oppstart og diskkryptering 10

3.1.20 Bruk antivirus/antiskadevare 10

3.1.21 Ikke installer unødvendig funksjonalitet 10

1 Innledning

Et av Valgdirektoratets hovedmål er å bidra til en korrekt og sikker valggjennomføring med tillit i befolkningen. Som et ledd i dette tilbyr Valgdirektoratet valgadministrasjonssystemet EVA til alle kommuner og fylkeskommuner. For at EVA skal benyttes på en korrekt og sikker måte, utgir direktoratet denne tekniske veilederen for bruk av EVA Skanning.

EVA Skanning er en lokalt installert applikasjon som driftes av kommuner og fylkeskommuner. Applikasjonen er utviklet av Valgdirektoratet. Installasjonsfilene gjøres tilgjengelig for kommuner eller fylkeskommuners.

Dette dokumentet er en teknisk veileder som inneholder brukervilkårene og anbefalte sikkerhetstiltak for bruk av Valgdirektoratets applikasjon EVA Skanning til bruk ved kommunenes og fylkeskommunenes valggjennomføring. Den tekniske veilederen retter seg mot IKT-personell i kommunene og fylkeskommunene for å sikre at applikasjonen benyttes på best mulig måte. Ved bruk av tredjepartsleverandører til støtte for EVA Skanning gjelder vilkårene i rammeavtalen.

I praksis betyr dette at brukervilkår og sikkerhetsanbefalinger gjelder kommuners og fylkeskommuners utstyr der EVA Skanning skal brukes. Brukervilkår gis for å sikre at applikasjonen gir optimal brukeropplevelse, sikkerhetsanbefalinger gis for å underbygge forsvarlig bruk av applikasjonen gjennom gode rutiner og kontroll.

2 Brukervilkår EVA Skanning

2.1 Tekniske krav til utstyr for å benytte EVA Skanning

2.1.1 Databaseserver

Maskinvare	Beskrivelse
Stor installasjon - skannsenter	
Database	Microsoft SQL Server 2016 eller nyere
Operativsystem	Windows Server 2016 eller nyere
LIten installasjon – enkelt PC med skanner tilkoblet	
Datasbase	Microsoft SQL LocalDB 2014 (12.0.2000.8) eller nyere som installeres på samme maskin som EVA Skanning og har derfor samme systemkrav som klientPC for EVA Skanning

2.1.2 Dokumentskanner

Tabell over anbefalte dokumentskannermodeller til bruk sammen med EVA Skanning ved valget i 2019.

Produsent	Modell	Leverandør
Fujitsu	fi5950c	Indra
	fi6400	Indra
Canon	DR-G1100	Idox / Evry
	DR-G1130	Idox / Evry
	DR-9050c	Idox
	DR-G2090	Evry
	DR-G2110	Evry
	DR-G2140	Evry

Andre modeller vil potensielt støttes, men Valgdirektoratet kan ikke garantere støtte utover modellene i tabellen over.

2.1.3 PC til bruk med EVA Skanning

Maskinvare	Beskrivelse
Operativsystem	Windows 10 Enterprise (64-bit)
Nødvendig tilbehør	Innebygget smartkortleser for signering av opptellinger ved overføring til EVA Admin eller USB smartkortleser for signering av opptellinger ved overføring til EVA Admin Håndholdt USB strekkodeskanner

Nødvendig programvare	EVA Skanning Internet explorer 11
Bærbare PC med internettilgang	minimum 8 GB internminne Intel Core i5 prosessor eller bedre 250 GB SSD disk 15" tommers skjerm – minimum oppløsning 1280x1024 pixler. 4 USB porter
Anbefalt tilbehør	USB-mus Ekstern skjerm

3 Sikkerhet ved maskinell telling av stemmesedler – EVA Skanning

3.1 Anbefalte sikkerhetstiltak ved bruk av EVA Skanning

Under følger en oversikt over hvilke tiltak Valgdirektoratet anbefaler at kommuner og fylkeskommuner innfører dersom de skal benytte EVA Skanning til maskinell opptelling av stemmesedler.

Samtlige anbefalinger gjelder også for kommuner og fylkeskommuner som benytter seg av teknisk bistand til EVA Skanning - 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
- Forebygge omdømmetap for valggjennomføringen
- Opprettholde tilliten til valggjennomføringen og valgresultatet
- Forebygge situasjoner som gir grunnlag for tap av tillit og omdømme ○ Forsinkelser i tilgjengeliggjøring av valgresultat ○ Omtelling av stemmesedler

Mange av de påfølgende sikkerhetstiltakene vil bli utført av installasjonsfilene som følger med EVA Skanning installasjonspakken. Disse tiltakene er merket med «inkludert i installasjonspakken».

3.1.1 Nye PCer

PCer hvor EVA Skanning skal installeres skal være nye og aldri tidligere brukt.

Anbefalingen om nye PCer stilles for å i større grad skape sikkerhet rundt opphav og oppbevaring av PCene som brukes til maskinell telling av stemmesedler (ved hjelp av EVA Skanning). En ny PC er en enkel og god forsikring om at PCen ikke er kompromittert. I tillegg er det enkelt å etablere en sikker rutine for oppbevaring og kontroll av nye PCer fra mottak til bruk med EVA Skanning.

3.1.2 Windows 10 Enterprise

PCer hvor EVA Skanning skal installeres 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 Windowsversjonen. Ved hjelp av disse mekanismene vil det kun være mulig å kjøre applikasjoner, og bruke internett-tjenester som er nødvendige for å kjøre EVA Skanning. Alle andre tilganger og applikasjoner blokkeres.
Ved å begrense applikasjons- og internett-tilgangen på PCer der EVA Skanning installeres og brukes, begrenses også angrepsflatene og mulighetene for kompromittering.

3.1.3 Fysisk sikring

Valgdirektoratet har laget en veileder som omhandler fysisk sikring av teknisk utstyr under valggjennomføringen. Denne gjelder blant annet for teknisk utstyr til bruk av EVA Skanning og sikring av lokaler for maskinell telling.

3.1.4 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.

3.1.5 Rutine for rullering av opptellingsstasjoner

Kommuner og fylkeskommuner må innføre en rutine som gjør at alle tellinger ikke utføres av samme PC der EVA Skanning er installert.

Dette sikrer variasjon av utstyr som brukes til å tolke stemmesedler og øker mulighetene for å avdekke eventuelle systematiske feil eller avvik.

For «liten installasjon» (kun 1 dokumentskanner med 1 PC) må det veksles mellom 2 PCer der EVA Skanning er installert.

3.1.6 Manuelle stikkprøver av skannede kasser med stemmesedler

For å kunne avdekke systematiske avvik som et resultat av kompromittering eller feil i programvaren, er det nødvendig med manuelle stikkprøver mens tellinger pågår. Ved å gjennomføre og dokumentere stikkprøver underveis i telleprosessen, skapes det i tillegg etterprøvbar dokumentasjon på den maskinelle telleprosessens integritet.

Stikkprøver skal gjøres for:

- Partifordeling ved maskinell *omtelling* opp mot tidligere maskinell *opptelling*
- Personstemmer ved endelig telling

På den måten sikres det at det ikke foregår kun maskinell vurdering av stemmesedler.

Typisk vil en kasse med stemmesedler utgjøre en stikkprøve. Hver stikkprøve (kasse) bør inneholde minimum 70 stemmesedler.

Stikkprøvene skal gjøres på tilfeldig valgte tidspunkt i opptellingen, og på tilfeldige valgte opptellingsstasjoner.

Den manuelle tellingen av stikkprøven (kassen) kontrolleres opp mot tilsvarende utsnitt (kasse) i telleresultat i EVA Skanning. Systemstøtte for dette vil bli utviklet.

Et eksempel på denne prosessen er som følger:

- Et antall kasser merkes fysisk som kandidater for stikkprøver under forberedelsen av opptellingen. Kassene som merkes som kandidater for stikkprøver må minimum inneholde 70 stemmesedler
- Når markert kasse er skannet telles denne manuelt
- Partifordeling og personstemmer fra stikkprøvetelling sammenliknes med partifordelingen og personstemmer fra den maskinelle tellingen av den gitte kassen og dokumenteres med tidspunkt gjennomført, samt eventuelle avvik
- Det er ingen grunn til å avbryte opptelling og overføring i påvente av at stikkprøver gjennomføres – de kan gjennomføres i parallell med pågående opptellingsprosess og kvitteres ut etterskuddsvis

3.1.7 Overvåkning

Valgdirektoratet ønsker å kjenne tilstanden for PCer der EVA Skanning er installert og som brukes til maskinell telling av stemmesedler. PCer der EVA Skanning er installert og som brukes til maskinell telling av stemmesedler vil derfor 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.

Valgdirektoratets flåtestyringsverktøy bør også installeres. Dette verktøyet vil bli beskrevet i installasjonsveiledning.

Inkludert i installasjonspakken.

3.1.8 Nettverk

Nettverket der EVA Skanning benyttes må sikres.

Anbefalte tiltak:

- Sett opp et dedikert nettverk til bruk for EVA Skanning
- Beskytte nettverket med brannmur mot omverden som kun tillater absolutt nødvendig trafikk ut og blokkerer trafikk initiert utenfra
- Autorisere enheter som skal ha tilgang til nettverket
- Trafikk mellom enheter er kryptert
- Sikre nettverket fysisk slik at man har kontroll på antall nettverkskontakter, kontaktenes plassering og tilkoblede enheter
- Trådløst nettverk skal ikke benyttes

3.1.9 Kontrollert fjerntilgang

Fjerntilgang for leverandører av teknisk støtte til EVA Skanning må skje i kontrollerte former og under overvåkning av autorisert personell hos kommunen/fylkeskommunen. Fjerntilgang bør derfor deaktiveres på maskiner som skal benyttes til EVA Skanning. Skulle det være nødvendig med fjerntilgang for å utføre støtte, skal denne initieres av autorisert personell fra EVA Skanning maskinen. 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.

Deaktivering inkludert i installasjonspakken.

3.1.10 Maskiner skal låses når de forlates

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

3.1.11 Bruker er personlig og skal ikke lånes

Alle som jobber i EVA Skanning 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.

3.1.12 Oppgrader program- og maskinvare

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

Valgdirektoratets oppdateringsserver for Windows 10 Enterprise er inkludert i installasjonspakken, men kommunene og fylkeskommunene er selv ansvarlig for å oppdatere.

3.1.13 Installer sikkerhetsoppdateringer så fort som mulig

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 firmware.

Valgdirektoratets oppdateringsserver er inkludert i installasjonspakken, men kommunene og fylkeskommunene er selv ansvarlig for å oppdatere.

3.1.14 Ikke tildel administrator-rettigheter til sluttbrukere

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

Valgdirektoratets installasjonspakke inneholder en kioskmodus, men kommunene og fylkeskommunene er selv ansvarlig for å ikke tildele brukeren administrator rettigheter.

3.1.15 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.

Inkludert i installasjonspakken.

3.1.16 Aktiver kodebeskyttelse mot ukjente sårbarheter

DEP, SEHOP, ASLR og EMET styrker systemet mot sårbarheter i applikasjoner og operativsystemet selv når det ikke finnes en oppdatering.

Inkludert i installasjonspakken.

3.1.17 Herde applikasjoner

Protected Mode/View for Internet Explorer, Microsoft Office og Adobe Reader begrenser skadeomfanget ved kompromittering. Deaktiver unødvendig mobil kode og makroer.

Ved bruk av installasjonspakken blir maskinen nedlåst i kioskmodus og bare tillatte applikasjoner vil være tilgjengelig. I kioskmodus vil ikke fjernaksess være tilgjengelig. Prosedyre for bruk av fjernaksess er beskrevet i kontrakten med leverandørene av teknisk støtte til EVA Skanning.

3.1.18 Bruk klientbrannmur

Windows Firewall blokkerer all trafikk initiert utenfra og logger sikkerhetsrelevante hendelser. Man bør inspisere loggfilene regelmessig.

Inkludert i installasjonspakken.

3.1.19 Bruk sikker oppstart og diskkryptering

Windows Secure Startup og Windows BitLocker bruker TPM-målinger og harddiskkryptering for å oppdage manipulering av oppstartsprosessen og forhindre tap av data fra stjålne/tapte PC'er.

3.1.20 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.

Inkludert i installasjonspakken.

3.1.21 Ikke installer unødvendig funksjonalitet

Enhver ny applikasjon og funksjon øker mulighetene for angrep. Få brukere har for eksempel behov for Java Runtime eller JavaScript i Adobe Reader. Også unødvendig programvare må herdes og oppdateres, noe som øker administrasjonsbyrden på systemet.

Inkludert i installasjonspakken.