VALGdirektoratet

Veileder for gjennomføring av valg

Teknisk veileder i bruk av EVA Admin for kommuner og fylkeskommuner

Versjon 1.1
14. januar 2019

Innholdsfortegnelse

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 tekniske veilederene for bruk av EVA.

EVA Admin applikasjonen er en standard webapplikasjon som driftes og forvaltes sentralt av Valgdirektoratet. Applikasjonen gjøres tilgjengelig gjennom nettleser på kommuner eller fylkeskommuners PCer.

Dette dokumentet er en teknisk veileder som består av to hoveddeler: brukervilkår og anbefalte sikkerhetstiltak for bruk av Valgdirektoratets applikasjon EVA Admin ved kommunenes og fylkeskommunenes valggjennomføring. Den tekniske veilederen retter seg mot alle brukere av EVA Admin i kommunene og fylkeskommunene for å sikre at applikasjonen benyttes på best mulig måte.

I praksis betyr dette at brukervilkår og sikkerhetsanbefalinger gjelder kommuners og fylkeskommuners PCer der EVA Admin 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.

Valgdirektoratet anbefaler at du tar kontakt med egen IT-ansvarlig for spørsmål rundt anbefalingene.

2 Brukervilkår EVA Admin

2.1 Tekniske krav til utstyr for å benytte EVA Admin

Maskinvare	Beskrivelse
PC med internettilgang	Minimum 4 GB internminne Minimum skjermoppløsning på 1280x1024 pixler Støtte for utskrivning i lokalet – for utskrift av duplikatvalgkort, møtebøker og rapporter
Nødvendig programvare	Operativsystem: Windows 10 Enterprise Nettleser: Chrome (siste versjon) eller Nettleser: Internet Explorer (versjon 11) eller Nettleser: Microsoft Edge (siste versjon) For nettlesere: Javascript må være tillatt

2.2 Anbefalt og valgfritt utstyr

Anbefalt tilbehør	Ekstra strømadapter pr. 5. PC Håndholdt USB strekkodeskanner – HID kompatibel – dersom elektronisk manntall er valgt
Valgfritt tilbehør	Innebygget, eller USB basert smartkortleser dersom smartkort skal brukes for pålogging via ID-porten.

2.3 Forklaringer

HID: Human Interface Device – strekkodeleseren skal fungere som forlengelse av tastaturet slik at strekkoden leser inn tall i felt for manntallsnummer. HID produkter er merket med forkortelsen HID eller Human interface Device.

Javascript: EVA bruker JavaScript. JavaScript er et skriptspråk som kjører i brukerens nettleser for å gi bedre funksjonalitet. EVA krever at JavaScript er aktivert. Hvis JavaScript er deaktivert vil ikke EVA fungere.

3 Sikkerhet ved bruk av EVA Admin

3.1 Anbefalte sikkerhetstiltak

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

3.1.1 Fysisk sikring

Valgdirektoratet har laget en veileder som omhandler fysisk sikring av teknisk utstyr under valggjennomføringen. Denne gjelder også for teknisk utstyr til bruk av EVA Admin.

3.1.2 Deaktiver fjerntilgang

Fjerntilgang på maskiner gjør at andre kan få tilgang til maskinen. Dette bør derfor deaktiveres på maskiner som skal brukes opp mot EVA Admin.

3.1.3 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.

3.1.4 Bruker er personlig og skal ikke lånes

Alle som jobber i EVA Admin 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.

3.1.5 Oppgrader program- og maskinvare

Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner.

3.1.6 Installer sikkerhetsoppdateringer så fort som mulig

Selv de beste produktene har feil og sårbarheter som kan utnyttes av angripere. Systemeiere bør etablere et sentralt styrt regime for oppdatering av applikasjoner, operativsystemer og firmware.

3.1.7 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 Admin.

3.1.8 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.

3.1.9 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.

3.1.10 Herde applikasjoner

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

3.1.11 Bruk klientbrannmur

Windows Firewall blokkerer all ubedt innkommende trafikk og logger sikkerhetsrelevante hendelser. Inspiser loggfilene regelmessig.

3.1.12 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.

3.1.13 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.

3.1.14 Ikke installer mer funksjonalitet enn nødvendig

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.