INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
M sum@sum.dk
W ism.dk

Til kommunernes valgansvarlige og KOMBIT

Dato: 07-11-2025
Enhed: Valgenheden
Sagsbeh.: Maria Pasmiyah Hansen Lolle
Koordineret med:
Sagsnr.: 2025 - 456
Dok. nr.: 4545414

Orientering om trusselsvurderingen ved kommunal- og regionalvalget tirsdag den 18. november 2025

SAMSIK, PET og FE har netop offentliggjort vedlagte trusselsvurdering vedrørende kommunal- og regionalvalget tirsdag den 18. november 2025.

Trusselsvurderingen indeholder følgende hovedvurdering:

- Truslen fra russisk påvirkning mod kommunal- og regionsrådsvalget gennem informationspåvirkning eller personlig påvirkning er LAV.
- Truslen fra russisk sabotage mod kommunal- og regionsrådsvalget er LAV.
- Cybertruslen mod kommunal- og regionsrådsvalget er HØJ.
- Det er sandsynligt, at pro-russiske hackergrupper vil udføre DDoS-angreb mod hjemmesider i forbindelse med valget.
- Det er muligt, at kriminelle hackere vil rette forsøg på ransomware-angreb mod it-systemer med forbindelse til valget.
- Det er mindre sandsynligt, at statslige hackere vil forsøge at forstyrre eller påvirke valget via cyberangreb.

Efter Indenrigs- og Sundhedsministeriets opfattelse giver trusselsvurderingen ikke anledning til nye beredskabs- og sikkerhedsinitiativer forud for kommunal- og regionalvalget.

Indenrigs- og Sundhedsministeriet henviser i den forbindelse til afsnit 7.16 om kommunernes beredskaber i ministeriets vejledning nr. 9565 af 26. juni 2025 om afholdelse af kommunale og regionale valg tirsdag den 18. november 2025.

Spørgsmål vedrørende dette brev kan rettes til Indenrigs- og Sundhedsministeriets Valgenhed på valg@im.dk eller telefon 72 26 90 00. Dette gælder også hele valgdagen.

Valgkonsulent Christine Boeskov kan i hastende tilfælde kontaktes på telefon 25 16 12 06.

Med venlig hilsen

Christine Boeskov
Valgkonsulent

Styrelsen for Samfundssikkerhed

PET

FORSVARETS EFTERRETNINGSTJENESTE

7. november 2025

Vurdering af truslen mod kommunal- og regionsrådsvalget den 18. november 2025

SAMSIK, PET og FE har udarbejdet en fælles trusselsvurdering for kommunal- og regionsrådsvalget i Danmark den 18. november 2025. Formålet er at orientere om relevante trusler, der kan påvirke eller forstyrre valget.

HOVEDVURDERING

- Truslen fra russisk påvirkning mod kommunal- og regionsrådsvalget gennem informationspåvirkning eller personlig påvirkning er **LAV**.
- Truslen fra russisk sabotage mod kommunal- og regionsrådsvalget er **LAV**.
- Cybertruslen mod kommunal- og regionsrådsvalget er **HØJ**.
- Det er sandsynligt, at pro-russiske hackergrupper vil udføre DDoS-angreb mod hjemmesider i forbindelse med valget.
- Det er muligt, at kriminelle hackere vil rette forsøg på ransomware-angreb mod it-systemer med forbindelse til valget.
- Det er mindre sandsynligt, at statslige hackere vil forsøge at forstyrre eller påvirke valget via cyberangreb.

Truslen fra påvirkning

Fremmede stater og deres efterretningstjenester forsøger løbende at påvirke politiske beslutninger og den offentlige debat i Europa, også i Danmark. Dette sker konstant og ikke kun i forbindelse med valg. Påvirkningstruslen fra fremmede stater udgår primært fra Rusland og Kina.

Truslen fra russisk påvirkning mod kommunal- og regionsrådsvalget gennem informationspåvirkning eller personlig påvirkning er **LAV**.

Det er mindre sandsynligt, at Rusland vil forsøge at påvirke kommunal- og regionsrådsvalget gennem informationspåvirkning eller personlig påvirkning. Kommunal- og regionsrådsvalg omhandler typisk velfærdsrelaterede politikområder og lokalpolitiske spørgsmål, der som udgangspunkt ikke vil være mål for russisk påvirkningsvirksomhed. Det er sandsynligt, at Danmark på nuværende tidspunkt ikke er et selvstændigt, prioriteret mål for Ruslands påvirkningsvirksomhed.

Hvis Rusland alligevel forsøger at påvirke valget, kan det ske ved at udnytte emner med stort potentiale til at skabe stærkt polariserede debatter og splittelse, som f.eks. situationen i Gaza. Udnyttelsen af sådanne emner vil kunne have en række konsekvenser for valget, såsom negativ opmærksomhed og chikane ift. kandidater eller valgmøder.

En sådan operation kan foregå ved at sprede vildledende information eller information, som ikke ønskes offentliggjort, via traditionelle og sociale medier. Dette kan eksempelvis gøres ved at anvende falske profiler på sociale medier til at påvirke synet på kandidater.

Det er usandsynligt, at kinesiske aktører vil forsøge at påvirke kommunal- og regionsrådsvalget gennem informationspåvirkning eller personlig påvirkning. Det gælder både selve afviklingen af valget og den politiske debat op til valget.

Formålet med påvirkning
Der er mange eksempler på, at lande forsøger at påvirke meningsdannelsen eller politiske beslutningsprocesser i andre lande eller internationale organisationer for at fremme deres egne interesser.

Påvirkningsvirksomhed er et af flere hybride virkemidler, som stater kan anvende til at påvirke den offentlige debat og politiske beslutningsprocesser, herunder ved at skabe splittelse og frygt for eskalation i det ramte samfund.

Påvirkningsvirksomhed omfatter **informationspåvirkning** og **personlig påvirkning** og foregår således både via platforme på internettet og gennem påvirkningsagenter. Påvirkningsagenter er personer, der arbejder sammen med fremmede efterretningstjenester for at påvirke beslutningsprocesser og meningsdannelse.

Påvirkningsvirksomhed er ofte rettet mod at udnytte eksisterende skillelinjer i en befolknings holdninger, hvor det er let at skabe konflikt og polarisering. Fremmede stater forsøger også mere målrettet at påvirke enkelte beslutningstagere i en mere favorabel retning. Aktiviteterne kan være målrettet konkrete begivenheder, f.eks. valghandlinger, men foregår i ligeså høj grad i det daglige.

Truslen fra sabotage
Truslen fra russisk sabotage mod kommunal- og regionsrådsvalget er **LAV**.

Rusland har siden 2023 stået bag en række sabotageaktioner mod mål i Europa. Det er sandsynligt, at der er tale om en regulær sabotagekampagne fra Rusland for at underminere den europæiske støtte til Ukraine.

Det primære formål med Ruslands sabotageaktioner er at svække de europæiske landes fortsatte politiske, militære og økonomiske støtte til Ukraine. Med sabotageaktionerne forsøger Rusland at skabe bekymring for yderligere eskalation blandt de europæiske befolkninger og samtidig sende et signal om, at der er mærkbare omkostninger forbundet med at yde støtte til Ukraine. Nogle typer af sabotage kan desuden forhindre specifikke leverancer af civilt og militært materiel i at nå frem til Ukraine.

Rusland har dog indtil videre afholdt sig fra at gennemføre sabotage mod politiske arrangementer, valgsteder og lignende lokaliteter i andre europæiske lande.

Cybertruslen
Cybertruslen mod kommunal- og regionsrådsvalget er **HØJ**.

Det skyldes hovedsageligt, at pro-russiske og kriminelle hackergrupper løbende udfører cyberangreb mod Danmark, som også kan få en forstyrrende effekt, hvis de rammer it-systemer med forbindelse til valget. Angrebene vil dog ikke kunne påvirke valgets gennemførsel eller resultat. Det er også mindre sandsynligt, at statslige hackere vil forsøge at påvirke valget gennem brug af cyberangreb.

Truslen fra pro-russiske hackere
Det er sandsynligt, at danske hjemmesider vil blive udsat for DDoS-angreb i forbindelse med kommunal- og regionsrådsvalget. Det skyldes, at pro-russiske hackergrupper løbende retter DDoS-angreb mod hjemmesider i forbindelse med europæiske valg. Angrebene understøtter Ruslands interesser, og det er sandsynligt, at nogle af disse hackergrupper har forbindelse til den russiske stat.

Eksempelvis blev Indenrigs- og Sundhedsministeriets valghjemmeside ramt af et DDoS-angreb fra en pro-russiskhackergruppe på dagen for europaparlamentsvalget i Danmark den 9. juni 2024. Angrebet var sandsynligvis en del af en større kampagne mod flere europæiske lande ved europaparlamentsvalget. Derudover har hjemmesider i Belgien også været mål for pro-russiske DDoS-angreb ved valg. Her blev hjemmesider hos valgmyndigheder, kommuner og nyhedsmedier ramt i forbindelse med landets kommunalvalg i oktober 2024.

Hvad er DDoS-angreb?
DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at skabe usædvanligt store mængder data-trafik mod en hjemmeside (webserver) eller netværk. Målet er at gøre hjemmesiden eller netværket utilgængelig, mens angrebet står på. Hvis hjemmesiden eller netværket, der angribes, f.eks. hoster brugervendte tjenester, kan et DDoS-angreb gøre disse utilgængelige for brugere.

Såfremt pro-russiske hackere vælger at rette DDoS-angreb mod Danmark i forbindelse med valget, kan angrebene blive rettet mod

mange forskellige hjemmesider. Det gælder både hjemmesider med direkte forbindelse til valget, som f.eks. dem der bruges til at formidle valgresultatet, men også andre hjemmesider tilhørende f.eks. kommuner eller trafikselskaber.

Det er usandsynligt, at eventuelle DDoS-angreb direkte kan forstyrre valgets gennemførelse eller resultat. Det skyldes, at DDoS-angreb generelt ikke påvirker fortroligheden og integriteten af hjemmesidernes data, samt at effekten af angrebet typisk ophører efter kort tid, når angrebet standses. DDoS-angreb kan dog få en forstyrrende effekt, hvis f.eks. hjemmesider ikke kan tilgås. Samtidig kan succesfulde angreb skabe usikkerhed i forbindelse med valget og føre til mistillid til, at myndighederne kan håndtere situationen.

Truslen fra kriminelle hackere
Det er muligt, at it-systemer med forbindelse til valget vil blive ramt af forsøg på ransomware-angreb fra kriminelle hackere. Det skyldes, at de kriminelle hackergrupper, som udfører angrebene, generelt er opportunistiske og retter angreb mod it-systemer på tværs af samfundet.

Hvis it-systemer, der er kritiske for forberedelsen og gennemførslen af valget, bliver ramt eller påvirket af et ransomware-angreb, kan det potentielt forstyrre valget. Det skyldes, at succesfulde ransomware-angreb typisk kræver omfattende genoprettelse af data. Dette kan tage dage eller uger og kan i nogle tilfælde også lede til tab af data.

Ransomware-angreb vil således kunne forsinke opgørelsen og udmeldingen af valgresultatet, hvis eksempelvis it-systemer, der bruges til at kontrollere stemmeafgivelsen og -opgørelsen, bliver ramt. Desuden vil angrebene også kunne føre til usikkerhed om sikkerheden i forbindelse med valget. Angrebene vil dog som udgangspunkt ikke påvirke resultatet af valget, idet stemmerne afgives analogt og derfor vil kunne optælles manuelt igen.

Hvad er ransomware-angreb?
Ransomware-angreb er cyberangreb, hvor kriminelle forsøger at gøre ofrenes data og systemer utilgængelige, ofte ved at kryptere data. De kriminelle kræver derefter en løsesum, typisk i form af kryptovaluta, for at gøre data og systemer tilgængelige igen. I nogle tilfælde truer de kriminelle også med at offentliggøre stjålne informationer, hvis ikke ofrene betaler løsesummen. Ransomware-angreb er typisk rettet mod systemer med adgang til internettet. Systemer eller enheder, der ikke er forbundet til internettet, kan dog også kompromitteres, hvis data overføres til og fra systemer med internetadgang.

Truslen fra statslige hackere
Flere stater, herunder Rusland, har kapacitet til at udføre cyberangreb mod it-systemer, der understøtter eller har forbindelse til valget. Dette understreges af flere eksempler på, at stater har udført cyberangreb, der

har haft til formål at understøtte påvirkningsaktiviteter i forbindelse med andre landes valg.

Samtidig forsøger statslige hackere løbende at udføre cyberspionage mod mål i Danmark og andre NATO-lande. De oplysninger og adgange, som hackerne måtte indsamle i den forbindelse, vil også kunne bruges i forbindelse med eventuel påvirkningsaktivitet mod valg.

På trods af dette er det mindre sandsynligt, at statslige hackere vil forsøge at forstyrre eller påvirke valget via cyberangreb.

Trusselsniveauer

FE, PET og SAMSIK bruger i denne trusselsvurdering følgende trusselsniveauer.

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's, PET's og SAMSIK's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.

Sandsynlighedsgrader

FE, PET og SAMSIK bruger denne skala for sandsynlighedsgrader i analyser:

En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed. FE, PET eller SAMSIK "vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.