VALG

Bokmål

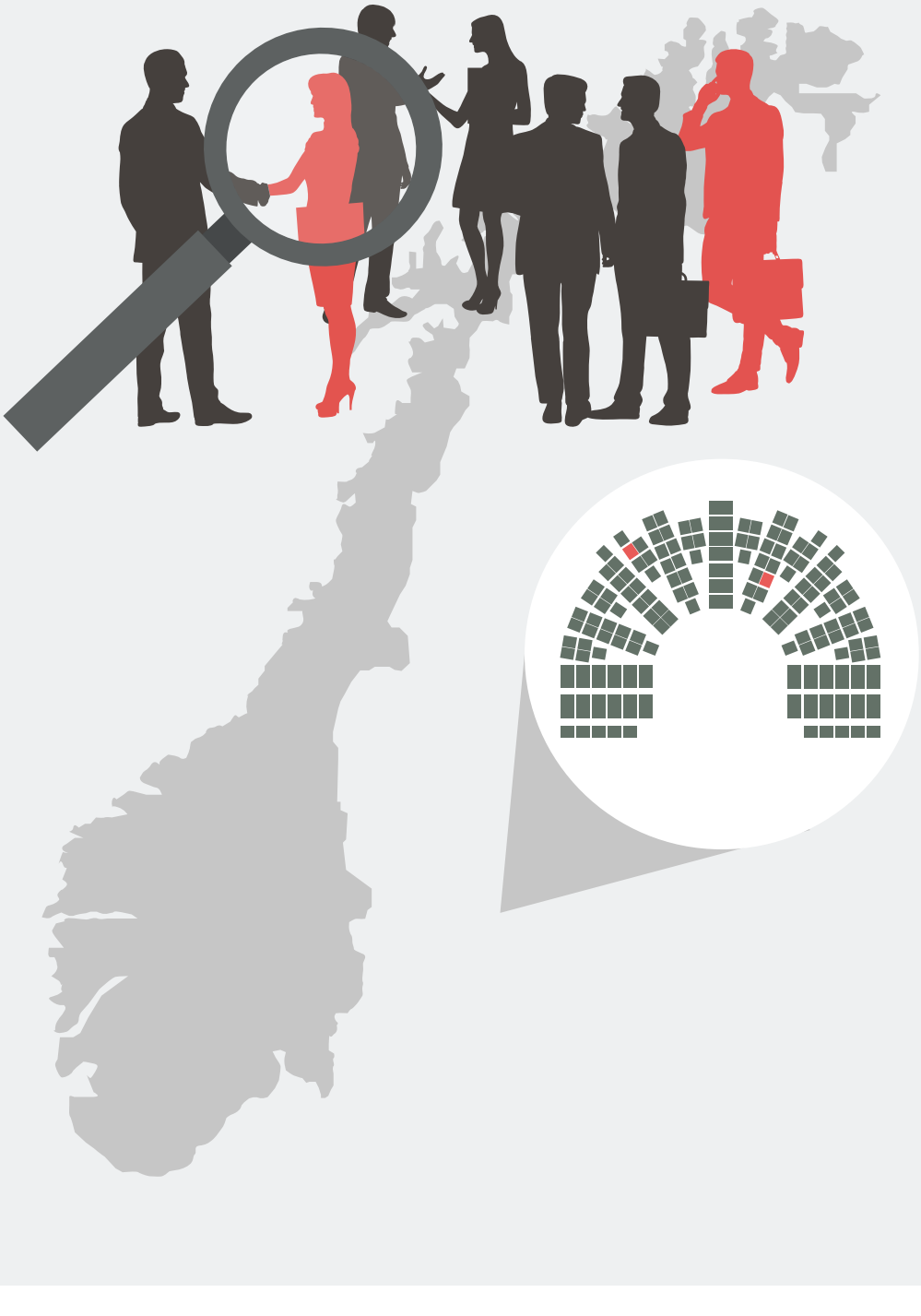
Du er av interesse –

Gode sikkerhetsråd til deg som stiller til valg

Utarbeidet av

- Etterretningstjenesten
- Nasjonal sikkerhetsmyndighet
- Politiets sikkerhetstjeneste

Innhold



Norge – et tillitsbasert samfunn

Det siste året har det vært økt oppmerksomhet rundt muligheten for at både fremmede stater og ikke-statlige aktører prøver å påvirke politiske prosesser i andre land. Påvirkning kan i denne konteksten defineres som en utenlandsk, statlig initiert (men gjerne gjennomført av ikke-statlig aktør), fordekt og tilsiktet aktivitet for å oppnå et mål som på kort eller lang sikt kan svekke norske interesser til fordel for en annen stat.

Slik påvirkning kan rettes mot gjennomføringen av valget, mot politiske aktører eller mot velgerne og holdninger i befolkningen. Vi har et velfungerende og stabilt demokratisk system og et samfunn preget av åpenhet. Det bidrar til robusthet både i institusjonene og hos enkeltpersoner med politiske verv. Norge har dermed et godt utgangspunkt for å stå imot forsøk på slik påvirkning av innenrikspolitiske prosesser.

Samtidig skal vi ikke være naive. Fremmede stater vil kunne søke informasjon om og påvirke norske politikere, politiske prosesser eller forhold. Her kan hver og en av oss bidra til å sikre sensitiv informasjon om oss selv og politiske prosesser, samt å håndtere eventuell slik påvirkning.

Din informasjon – ditt ansvar

Du må selv bidra til å beskytte egen informasjon og de verktøyene du bruker for å kommunisere. Hva du selv gjør, har betydning for din sikkerhet og evne til å kommunisere trygt og sikkert. Det er viktig at du har kunnskap om hvordan du kan håndtere situasjoner som kan innebære risiko. Dette kan være situasjoner knyttet til menneskelige relasjoner og bruk av digitale verktøy.

Du er av interesse

Fremmede staters etterretningstjenester driver målrettede operasjoner i Norge. Særlig der man har motstridende eller konkurrerende interesser. Når du stiller til valg, betyr det at du må regne med at fremmede staters etterretningstjenester kan være interessert i deg som et ledd i sin virksomhet. For å nå sine mål bruker de både åpne og skjulte metoder. Detaljert kunnskap om deg, både som privatperson og politiker, kan ha høy verdi. Etterretningstjenestene er dyktige til å skape relasjoner mellom mennesker, blant annet gjennom hyggelige og naturlige møter. Noe så tilsynelatende enkelt som din kontaktliste på telefonen kan være av interesse.

FALSK E-POST

Det sendes stadig ut e-poster som utgir seg for å være noe de ikke er. Avsenderne spiller på tillit, frykt eller fristelser. For eksempel kan det være at noen utgir seg for å være banken din og skal ha deg til å logge inn for å løse et problem. Idet du klikker på en lenke eller åpner vedlegget, øker risikoen for at enheten din kan overtas av andre, eller de får tak i påloggingsinformasjon eller annen viktig informasjon som kan utnyttes videre.

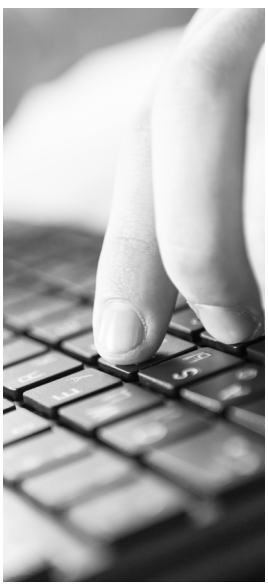
MENNESKELIG TILNÆRMING

En norsk lokalpolitiker kommer i snakk med et delegasjonsmedlem eller en næringsdrivende. Senere inviteres politikeren på lunsj. Lunsjen følges opp med flere møter over en lengre periode. Politikeren bes om informasjon om andre i partiet eller et konkurrerende parti. Det kan være av personlig karakter eller jobbrelatert. Vedkommende ber også politikeren legge til rette for møter med ledelsen i partiet eller andre interessante parter. Utenlandske aktører som nevnt i eksemplet kan være tilknyttet eller utnyttet av landets etterretningstjeneste. Dette er en vanlig måte å operere på i Norge.

Sårbarheter utnyttes

Fremmede stater og andre aktører forsøker kontinuerlig å ta seg inn i datasystemer for å hente ut informasjon eller ta kontroll over systemer. Sentralt i slike virkemidler står ofte såkalte innsidere. Med dette menes personer som har eller har hatt en lovlig tilgang til informasjonen og systemene, og som misbruker denne kunnskapen og tilgangen på en måte som påfører andre skade eller tap. Det å lure mennesker til å skaffe seg slik tilgang er noe som skjer daglig.

Den enkleste metoden for å ta seg inn i datasystemer er å få mottakere av e-poster til å åpne vedlegg eller lenker som starter det teknologiske angrepet. Kunnskap om f.eks. sensitiv og privat informasjon eller politiske standpunkt kan utnyttes.



Kjenn dine verdier

Vit hva som er verdifull informasjon for deg og ditt parti

- Hvilken informasjon har størst verdi eller alvorligst konsekvens for deg og ditt parti hvis andre fikk tilgang til den?
- Hvem kan du dele slik informasjon med, og hvem skal den ikke deles med?

Behandle verdifull informasjon med forsiktighet

- Tenk over hva du skriver/sier hvor og hvem som leser/lytter – både på telefon og i det offentlige rom.
- Forsikre deg om identiteten til de du kommuniserer med.
- Enkelte temaer eller saker bør ikke diskuteres på telefon eller sendes via vanlig e-post eller SMS.
- Når noe er sensitivt, bør møter gjennomføres uten PC, mobil og smartklokker til stede.
- Bruk krypteringsløsninger for elektronisk kommunikasjon.

Beskytt ditt digitale utstyr og dine digitale tjenester

- Ikke lån bort dine digitale enheter til andre.
- Aktiver skjermlås, og bruk gjerne fingeravtrykk eller ansiktsgjenkjenning for å unngå at andre ser PIN-kode når du låser opp enheten.
- Hold digitale enheter oppdatert med siste versjon av apper/programvare.
- Bruk flerfaktorautentisering (bruk av passord i kombinasjon autentiseringsapp, kodebrikke eller lignende) der hvor det tilbys.
- Bruk forskjellige passord for hver tjeneste.

E-post

- Vær kritisk til lenker og vedlegg i e-post som du mottar.
- Er du usikker på om du bør åpne et vedlegg eller en lenke – vurder om det er strengt nødvendig.
- Ta kontakt med avsender via telefon/annet om du er i tvil.
- Gjør gjerne et internettsøk på informasjonen uten å åpne lenken/vedlegget.
- Rapporter mistenkelige e-poster til egen partiorganisasjon, tillitsvalgt for din liste eller arbeidsgiveren din.

Sosiale medier, apper og digitale tjenester

- Vær kritisk til hvilke apper og tjenester du installerer på dine digitale enheter.
- Bruk personverninnstillingene til å beskytte tilgang og synlighet etter ditt behov.
- Vær bevisst på hva du legger ut om deg selv og andre.
- Vær kritisk til det som kan være falske nyheter – unngå å spre videre.
- Slå av informasjon om hvor du befinner deg, om ikke du absolutt trenger å bruke det.
- Benytt et unikt, sterkt passord og slå på flerfaktorautentisering.

På reise

- Unngå å koble deg opp til offentlige trådløse nett. Bruk mobildata eller mobilt bredbånd.
- Unngå å lade digitale enheter via andres USB-ladepunkter/ USB-tilkoblinger.
- Dersom du reiser til utsatte land, bør du ikke ta med din vanlige mobiltelefon, PC eller nettbrett. Dette gjelder for eksempel land som Norge ikke har et nært sikkerhetspolitisk samarbeid med.

Når bør du be om rådgivning?

Ta kontakt med din partiorganisasjon, tillitsvalgt eller din arbeidsgiver om du skulle oppleve hendelser som

- mottak av e-poster som er spesielt mistenkelige
- tekniske uregelmessigheter i digitalt utstyr
- tap av digitalt utstyr som mobiltelefon, PC og nettbrett
- tap av verdifull informasjon
- målrettet tilnærming
- misbruk av dine profiler i sosiale medier
- spredning av falsk informasjon

Dersom du tror du er utsatt for et digitalt angrep, påvirkning eller uønsket tilnærming, bør du så raskt som mulig informere og diskutere saken med din nærmeste leder.

Er du fortsatt bekymret? Ta kontakt med relevante myndigheter som Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) eller lokalt politi.

For mer informasjon om digital sikkerhet, besøk nettvett.no.

For mer informasjon om kritisk medieforståelse, besøk medietilsynet.no.

Denne brosjyren er utarbeidet av Etterretningstjenesten, Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste på oppdrag fra Forsvarsdepartementet og Justis- og beredskapsdepartementet, koordinert og finansiert av Kommunal- og distriktsdepartementet.