KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

DET KONGELIGE
KOMMUNAL- OG DISTRIKTSDEPARTEMENT

Til landets kommunedirektører og ordførere

Vår referanse:	22/00785-1
Arkivkode:	0
Saksbehandler:	Asbjørn Finstad
Deres referanse:	
Dato:	09.03.2022

Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina

Russlands invasjon av Ukraina har gitt økt usikkerhet rundt trusselnivået i det digitale rom. Det er derfor nødvendig at alle kommuner nå vurderer sin egen sikkerhets- og sårbarhetssituasjon på bakgrunn av den pågående konflikten. I dette brevet, som er sendt til alle norske kommuner, kommer Kommunal- og distriktsdepartementet og KS med konkrete råd og anbefalinger til kommunene som følge av situasjonen, om hvordan kommune kan sikre sine kritiske funksjoner og tjenester.

Bakgrunn
Både Politiets Sikkerhetstjeneste og Etterretningstjenesten har advart mot statlige etterretningsoperasjoner i sine åpne trusselvurderinger. De nasjonale trusselvurderingene som kom 11. februar 2022, pekte på at Russland er en kjent trussel-aktør for Norge, og at den generelle trusselen om cyberoperasjoner fortsatt står ved lag.

Nasjonal Sikkerhetsmyndighet (NSM) har også kommet med klare råd til virksomheter om å forebygge og avverge cyberangrep.

Nasjonale anbefalinger
Per i dag vurderer ikke norske myndigheter at trusselnivået mot virksomheter er økt på bakgrunn av denne konflikten. Samtidig må det presiseres at situasjonsbildet kan endre seg raskt. I tiden fremover forventer norske sikkerhetsmyndigheter økt aktivitet med svindel, nettfisking og sosial manipulering. Derfor bør kommunene i tiden fremover prioritere å innarbeide en god sikkerhetskultur.

Nasjonal sikkerhetsmyndighet har utarbeidet en liste over prioriterte tiltak virksomheter kan iverksette i en skjerpet sikkerhetssituasjon[i], og som kommunene nå bør innarbeide i sitt pågående sikkerhetsarbeid.

Kommunal- og distriktsdepartementet og KS foreslår iverksetting av flere tiltak
Det er nødvendig at alle kommuner nå vurderer sin egen sikkerhets- og sårbarhetssituasjon. Kommunal- og distriktsdepartementet og KS anbefaler at alle kommuner iverksetter følgende undersøkelser og vurderer iverksetting av tiltak på følgende områder:

1) Sikkerhetsovervåkning
   a) Verifiser om kommunen har nødvendig sikkerhetsovervåkning av IKT-systemer for å kunne oppdage dataangrep og datainnbrudd, og at kommunen har nødvendig bredredskap for å kunne håndtere dette.
   b) Hvis kommunen selv ikke har driftsansvaret for IKT-systemer, må driftsleverandør(er) kontaktes for å verifisere om de har nødvendig sikkerhetsovervåkning av IKT-systemer, og i en forlengelse av dette, nødvendig beredskap for å håndtere et dataangrep og datainnbrudd.

c) Kommunen bør etterspørre og verifisere hos leverandøren hvilke tiltak som er gjennomført for sikkerhetsovervåkning og beredskap for å håndtere dataangrep og datainnbrudd.

2) Sikring av kritiske funksjoner og tjenester
   a) Verifiser om det er kartlagt hvilke funksjoner/tjenester i kommunen som anses som kritiske. Sjekk også hvilke konsekvenser det vil ha for kommunens funksjonsevne hvis IKT-systemene blir utilgjengelige, eller mister tillitt fordi data er manipulert eller på avveie.
   b) Verifiser om kommunen har oppdaterte beredskap- og kontinuitetsplaner for bortfall av tjenester. Vurder videre om kommunen har nødvendig kapasitet til å opprettholde sin funksjonsevne, spesielt på kritiske tjenester, hvis IKT-systemer faller ut over lengere tid.
   c) Verifiser om det finnes gjenopprettelsesrutiner, og om backup er plassert slik at denne ikke kan bli manipulert eller ødelagt.
   d) Flere leverandører av programvare har utviklings- og supportavdelinger i landene som nå er involvert i konflikten. Verifiser med leverandør om hvordan leverandøren håndterer situasjonen hvis de har utviklings- eller supportavdeling i de aktuelle landene.

3) Beskytte tjenester som er tilgjengelig på Internett.
   - Undersøk om to-faktor autentisering er implementert. Dette gjelder spesielt for digitale tjenester som er tilgjengelig over internett.
   - Hvis ikke, undersøk hvor fort dette kan implementeres, og hvilke risikoreduserende tiltak som er gjennomført for å beskytte slike tjenester.

4) Årvåkenhet og teknologi.
   - Det bør sendes ut varsel til organisasjonen at alle bør være ekstra årvåkne når de mottar e-post
   - Kommunen bør vurdere å kartlegge om det finnes konkrete interne eller eksterne trusler som kan utgjøre en risiko for kommunens funksjonsevne.
   - Se anbefalinger og tiltak publisert av JustisCERT[ii] og HelseCERT[iii], og følg opp der det er relevant.

Dersom man har ytterligere spørsmål om anbefalingene ovenfor, kan KS kontaktes på følgende e-post: fagradip@ks.no.

Kommunal- og distriktsdepartementet og KS følger situasjonen tett, og vil eventuelt komme tilbake med anbefalinger til kommunene om ytterligere tiltak.

Med vennlig hilsen

Kommunal- og distriktsminister

KS Styreleder

Kopi: Justis- og beredskapsdepartementet

[i] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/digital-beredskap-i-en-skjerpet-situasjon/
[ii] https://justiscert.no/[justiscert-varsel]-[018-2022]-[tlphvit]-krigen-i-ukraina-berorer-norske-virksomheter-sorg-for-tilstrekkelig-sikkerhet-mot-cyberoperasjoner
[iii] https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak