Informasjonssikkerhet i IKT-systemer

Innlandet fylkeskommune

KU-møte

10.03.2022

Bakgrunn

- Bestilling av to forvaltningsrevisjoner med fokus på IKT-sikkerhet. Prosjektplaner behandlet 15.10.20.
  - Informasjonssikkerhet i IKT-systemer
  - Tilgangsstyring i IKT-systemer som behandler elevdokumentasjon

- Ramme 600 t eksl. foranalyse, leveres i løpet av 2021.

Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om å sikre at informasjonen som behandles i en virksomhet:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Hvorfor IKT-sikkerhet?

- Vigilo-saken i Bergen kommune (2019). Modul for kommunikasjon mellom hjem og skole, lagt ut opplysninger om hemmelig adresse. 3 mill i gebyr for ikke å ha gjennomført tiltak for å oppnå tilstrekkelig sikkerhetsnivå.

- Sikkerhetsbrudd i Conexus Engage (2020)– IT-system brukt i videregående skoler i Innlandet fylkeskommune som inneholder persondata om elever og lærere. Elev-videoer på Stream tilgjengelig for alle.

- Dataangrep i Østre Toten kommune (jan 2021) – Ilagt 4 mill i gebyr for mangler ved personopplysningssikkerheten og tilhørende internkontroll.

    - Ikke brukt to-faktor autentisering
    - Ikke tilfredsstillende back-up systemer
    - Ikke tilfredsstillende logging av viktige hendelser

++++

Hvorfor IKT-sikkerhet?

NSM advarer mot cyberoperasjoner i julen

Publisert: 13.12.2021

- Vi har sett en sterk økning av cyberoperasjoner i november og desember. Fra før vet vi at trusselaktørene utnytter fridager med lavere beredskap, og faren for angrep mot norske virksomheter i julen er derfor stor. Norske virksomheter må ta denne trusselen på største alvor, sier Sofie Nystrøm, direktør i Nasjonal sikkerhetsmyndighet (NSM).

I slutten av november advarte også amerikanske FBI om at høytiden vi nå står foran er en periode der det forventes at det blir gjennomført flere digitale angrep, blant annet i form av utpressing og sabotasje. Dette gjelder også i Norge.

- De som står bak vil utnytte enhver mulighet til å ramme norske virksomheter, og julen er ikke noe unntak. Selv om de fleste kan senke skuldrene og slappe av i julen, er det viktig at vi også har beredskap mot for eksempel digital utpressing gjennom høytiden, sier Nystrøm.

Innlandet fylkeskommune har ikke opplevd noe alvorlig dataangrep siden sikkerhetsbruddet på et skoleadministrativt system i 2020.

Det opplyser sikkerhets- og beredskapssjef Endre Hjelseth i Innlandet fylkeskommune.

Han ser svært alvorlig på at Nordland fylkeskommune ble utsatt for et datainnbrudd lille julaften. De fleste av fylkeskommunens systemer er fortsatt nede i arbeidet med å tette sikkerhetshullene.

Tetter sikkerhetshull

Fylkeskommuner og kommuner har ikke tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet, viste en rapport fra digitaliseringsdirektoratet høsten 2020. Spesielt gjelder dette små og mellomstore kommuner, het det i rapporten.

– Hva gjør Innlandet fylkeskommune for å sikre god styring og kontroll?

– Vi jobber iherdig for å styrke informasjonssikkerheten og tette eventuelle sikkerhetshull. Vi gjennomfører kontinuerlig risiko- og sårbarhetsanalyser av ulike IT-løsninger og kurser de ansatte. Vi har etablert et styringssystem for hvordan vi jobber med dette området og hvem som har ansvar for hva, svarer Hjelseth.

Fylkeskommunen er dessuten medlem av Kommune-CSIRT. Det er et ressurssenter som gir praktisk råd og støtte ved cyberhendelser.

Fikk tak i passord

Sikkerhets- og beredskapssjefen i Innlandet har hatt mye kontakt med sin kollega i Nordland fylkeskommune etter at de oppdaget dataangrepet der lille julaften. Det synes klart at inntrengerne har klart å få tak i et admin-passord og kommet seg bak brannmuren på den måten.

– De foreløpige analysene av datainnbruddet i Nordland fylkeskommune tyder på at aktøren har vært ute etter konkret informasjon, sier Hjelseth.

– Hva slags informasjon kan hackerne være interessert i?

– Det er det umulig å si, men fylkeskommunen kan sitte på mye informasjon som kan være interessant for ulike aktører. Hvis det er snakk om etterretningsvirksomhet, kan det for eksempel være interessant å få informasjon om fylkesvegnettet. Men det er bare et hypotetisk eksempel, understreker Hjelseth.

Problemstillinger

1. *Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?*
2. *I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?*

Kilder til revisjonskriterier

- Personopplysningsloven – gjelder all behandling av personopplysninger
- eForvaltningsforskriften – gjelder for forvaltningsorgan som benytter IKT-systemer til elektronisk saksbehandling og kommunikasjon
- Digitaliseringsdirektoratets (Digdir) veiledningsmateriell

- ISO/IEC 27001, Standard for styringssystem for informasjonssikkerhet
- Nasjonal Sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet

Metode

- Knyttet til oss ekstern ekspertise - Diri AS (NTNU). Kvalitetssikring av revisjonskriterier, vurderinger og konklusjoner.
- Valg av IKT-systemer
  - Kriterier: behandle sensitive personopplysninger, ikke system som brukes i skolen
  - Elements: sak- og arkivsystem, nytt, behandler store mengder personopplysninger, stort antall brukere.
  - Skyssweb: saksbehandlingssystem for skoleskyss, Innlandstrafikk. 23 000 elever hadde skoleskyss i 20/21, 430 aktive brukere.
- Dokumentanalyse
- Intervju med sentrale personer - mailkorrespondanse

Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?

Revisjonskriterier:

- Policy for informasjonssikkerhet – med visse krav til innhold Bestått -
- Hensiktsmessig intern organisering av arbeidet med informasjonssikkerhet Bestått -
- Overordnet retningslinje for gjennomføring av risikovurderinger Ikke bestått
- Nødvendige rutiner og prosedyrer Bestått - -
- Rutine for kontinuerlig evaluering og forbedring av internkontrollsystemet med underliggende dokumenter Ikke bestått
- Rutine for regelmessig statusrapportering til ledelsen – politisk og administrativ

Delvis bestått

Styrende retningslinjer

- Retningslinje og prosedyre for klassifisering av informasjon.
- Retningslinje for behandling av personopplysninger.
- Retningslinje for informasjonssikkerhet i leverandørforhold.
- Retningslinje for avviks- og hendelseshåndtering.

Er det etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet i Innlandet fylkeskommune?

Konklusjon

Innlandet fylkeskommune har ikke etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet.

- Sårbar arbeidsfordeling, stort ansvar på få ressurser
- Flere styrende dokumenter ikke på plass, blant annet overordnet retningslinje for risikostyring, beredskapsplan for hendelser knyttet til informasjonssikkerhet.
- Ikke systematisert arbeid med evaluering og forbedring av styringssystem
- Svak sammenheng mellom mål og strategi

I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Identifisere og kartlegge:

- Fylkeskommunen skal ha gjennomført risikovurdering av systemet.
- Foreslåtte tiltak knyttet til risikovurderingen bør ha blitt gjennomført i henhold til en fastsatt plan, med fastsatt tiltakseier og tidsfrist.
- Fylkeskommunen bør oppdatere risikovurderingen i faste intervaller og ved betydelige endringer.

Beskytte og opprettholde:

- Fylkeskommunen skal ha gjennomført sikkerhetsopplæring av systemets brukere.
- Det bør være etablert et regime for sikkerhetsoppdatering av systemet.
- Fylkeskommunen bør ha gjennomgått IT-systemets funksjonaliteter og unødvendig funksjonalitet bør ha blitt slått av.
- Systemets standardpassord bør ha blitt byttet.
- Fylkeskommunen bør beskytte data i IT-systemet under oppbevaring i samsvar med gjennomført klassifisering av systemets informasjonsverdier.
- Fylkeskommunen bør beskytte data i systemet under overføring (dataflyt) i samsvar med gjennomført klassifisering av systemets informasjonsverdier.
- Informasjonsverdier lagret på medier bør være tilstrekkelig sikret i samsvar med gjennomført informasjonsklassifisering, ved:
    - - Bruk
    - - Flytting/transport
    - - Avhending/Arkivering
- Fylkeskommunen bør ha sikret muligheten til å gjenopprette systemets data.
- Det bør ha blitt gjennomført regelmessige tester for å verifisere at sikkerhetskopien fungerer.

I hvilken grad har Innlandet fylkeskommune ivaretatt informasjonssikkerheten i utvalgte IKT-systemer?

Oppdage:

- Fylkeskommunen bør ha opprettet en hendelseslogg for hvert system.
- Loggføring bør inneholde informasjon om systemadministrators og systemoperatørers aktiviteter.
- Systemets logger bør være tilstrekkelig sikret.
- Det bør være etablert sikkerhetsovervåking av systemet.
- Det bør være gjennomført penetrasjonstest av systemet.

Håndtere og gjenopprette:

- Fylkeskommunen bør ha utarbeidet en hendelseshåndteringsplan for systemet.
- Fylkeskommunen bør ha vurdert redundansmuligheter som sikrer tilgjengelighetskrav.

Elements Cloud

Konklusjon

Innlandet fylkeskommune ivaretar i høy grad informasjonssikkerheten i sak- og arkivsystemet Elements Cloud.

Revisjonen mener at fylkeskommunen i stor grad har sikret at informasjonen i systemet er beskyttet i samsvar med risikovurderingen av informasjonsverdiene.

- Ikke gjennomført penetrasjonstest
- Mangler systematisk oppfølging av risikovurdering

Skyssweb

Konklusjon

Basert på den informasjonen som foreligger konkluderer revisjonen med at Innlandet fylkeskommune ikke i tilstrekkelig grad ivaretar informasjonssikkerheten i skoleskyss-systemet Skyssweb. Revisjonen finner flere mangler ved informasjonssikkerheten.

- Tiltak ikke basert på risikovurderinger
- Rutine for sikkerhetsoppdateringer medfører risiko for at kritiske sårbarheter forblir i systemet over tid.
- Den tekniske sikringen av data under oppbevaring og i transitt (dataflyt) er vanskelig å vurdere basert på den informasjonen som foreligger. Data under oppbevaring og intern datatrafikk er ikke kryptert, men det foreligger ingen vurdering som sier at dette er i samsvar med risiko. Dersom den fysiske sikringen av serverne har sårbarheter, vil dette kunne medføre at inntrengere kan få tilgang til ukrypterte data.
- Det er etablert evne til å gjenopprette data. Det oppbevares to separate sikkerhetskopier, men det er ikke etablert offline back-up. Dersom det ikke foreligger sikkerhetskopier utenfor det interne nettverket, vil eventuelle inntrengere kunne kryptere/låse all back-up.
- Det er opprettet en hendelseslogg for systemet, men revisjonen stiller spørsmålstegn ved om loggene er tilstrekkelig sikret. Det er uheldig at det finnes muligheter til å endre logger og at loggene slettes etter relativt kort tid.
- Det er ikke etablert en tilfredsstillende sikkerhetsovervåking av systemet. Dette kan medføre risiko for at hendelser ikke oppdages i tide.