Riksrevisjonen

Presentasjon for pressen 17.01.2024

Informasjonssikkerhet i forskning innenfor kunnskapssektoren

I dag legger vi frem Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning.

Sikkerhetssituasjonen innenfor høyere utdannings- og forskningssektoren har blitt mer utfordrende de siste årene.

Informasjon og kunnskap fra forskning kan være av stor interesse både for etterretningsorganisasjoner og kommersielle virksomheter.

Det blir også samlet inn store mengder, til dels sensitive, forskningsdata om personer som mange aktører kan ha interesse av å forsøke å utnytte, blant annet i kriminell virksomhet.

Riksrevisjonen offentliggjør en oppsummering av undersøkelsen og en sladdet versjon av den underliggende rapporten. Stortinget har mottatt en fullstendig versjon av denne.

Noe informasjon i rapporten er unntatt offentlighet fordi innsyn ville lette gjennomføring av dataangrep, og enkelte opplysninger er i tillegg gradert *begrenset* etter sikkerhetsloven.

Vi strekker oss langt for å sikre åpenhet om våre rapporter. Samtidig må vi følge lovverket. Jeg vil understreke at det vi legger frem i dag gir et relativt fullstendig bilde av saken.

Vi har hatt en god dialog med Kunnskapsdepartementet og Nasjonal sikkerhetsmyndighet (NSM) om hva slags informasjon som kan offentliggjøres.

Vi har undersøkt hvordan universiteter, høyskoler og andre forskningsinstitusjoner under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep. Vi har også undersøkt hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdanning og forskning.

***

Vi har følgende konklusjoner:

- Forskningsdata er ikke i tilstrekkelig grad sikret mot dataangrep.
- Forskningsinstitusjoner har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen
- Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer.
- Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp

***

Forskningsdata skal i hovedsak bli tilrettelagt for åpen tilgang, men hensyn til sikkerhet, personvern, immaterielle rettigheter og forretningshemmeligheter tilsier i en del tilfeller at forskningsdata ikke kan gjøres helt åpent tilgjengelige.

En rekke lover og regler stiller krav til hvordan slike data skal sikres. Lovverket stiller også konkrete krav til virksomhetene om at de skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen. For å oppnå dette bør virksomhetene følge faglige standarder som angir god praksis.

Riksrevisjonen gjennomførte inntrengingstester mot tre forskningsinstitusjoner for å teste hvor godt dataene deres var beskyttet.

Målet var å få tilgang til sensitive forskningsdata, enten ved å få kontroll over IT-infrastruktur eller ved å utnytte tilgangsrettighetene den enkelte forsker har.

Inntrengingstestene ved to av forskningsinstitusjonene ga oss full kontroll over IT-infrastrukturen som blir brukt av ansatte og studenter i deres daglige arbeid. Ved en av dem oppnådde vi dette den første dagen av inntrengingstesten, og det ble funnet flere veier som kunne gi slik kontroll.

Oppnådd kontroll innebar at vi kunne administrere alle brukerkontoer, PC-er og servere. Med slik tilgang kunne vi tildele oss selv alle ønskede rettigheter og skaffe oss tilgang til all informasjon lagret i nettverket, inkludert sensitiv forskningsinformasjon.

Med disse rettighetene hadde det også vært mulig å endre, slette eller kryptere all informasjon dersom motivasjonen hadde vært økonomisk vinning eller sabotasje.

Ved den tredje forskningsinstitusjonen fikk vi kontroll med de fleste PC-er benyttet av ansatte. Det ga oss muligheter til å hente ut eller manipulere informasjon lagret lokalt på PC-er og på ansattes skylagringsløsning.

Tilgangen kan bli brukt til et målrettet angrep mot utvalgte forskere med kunnskap og tilgang til informasjon som angriperen ønsker tilgang til.

Vi fikk ikke kontroll med servere og datanettverk generelt ved den tredje forskningsinstitusjonen, fordi de sentrale delene av IT-infrastrukturen er bedre beskyttet.

Et av formålene med inntrengingstestene var å undersøke forskningsinstitusjonenes evne til å oppdage aktiviteter i et dataangrep. Vi gjorde ingen forsøk på å skjule våre simulerte angrep, men produserte mye nettverkstrafikk og kjente tegn på angrep.

Ved to av institusjonene ble få eller ingen av aktivitetene i inntrengningstestene oppdaget.

Ved den siste ble inntrengingstesten oppdaget den fjerde testdagen, og de fleste aktivitetene ga spor i logger som kunne gi dem et bilde av hvordan angrepet hadde blitt gjennomført og hvilke systemer som var berørte.

De tre forskningsinstitusjonene som ble testet har alle planlagt og til dels gjennomført en rekke tiltak som øker deres sikkerhet i etterkant av våre undersøkelser. De konkrete svakhetene som ble utnyttet i inntrengingstestene er utbedret.

Inntrengingstestene ga full kontroll hos de to forskningsinstitusjonene blant annet fordi de brukte svake passord, mange brukerkontoer var tildelt store rettigheter, og det var svakheter i beskyttelsen av nettverk. I tillegg ble lite av våre angrep oppdaget fordi overvåkningen var mangelfull.

Disse svakhetene er vanlige ved forskningsinstitusjonene vi har undersøkt. Det gir grunn til å tro at inntrengingstester ved andre institusjoner kunne gitt lignende resultater.

Dette viser at mange av forskningsinstitusjonene ikke er godt nok beskyttet mot dataangrep.

***

Forskningsinstitusjonene skal gjennomføre tekniske sikkerhetstiltak for å oppnå en egnet sikring av sine IKT-systemer og informasjonen som er lagret. Sikkerhetstiltakene skal bidra til å forebygge at dataangrep lykkes. Det er også viktig å ha tiltak for å oppdage angrepene man ikke klarer å forebygge.

Vi har undersøkt tekniske sikkerhetstiltak ved ti forskningsinstitusjoner. Undersøkelsen viser at sentrale anbefalinger i Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* ikke blir fulgt av institusjonene. Vi fant:

- Mangelfull kontroll med brukerkontoer og tilgangsrettigheter
- Svake krav til passord
- Mangelfull sårbarhetsstyring av IT-utstyr og programvare
- Svakheter i nettverkssikkerheten
- Mangelfull logging og overvåkning

Nivået på sikkerhetstiltakene i forskningsinstitusjonene varierer imidlertid betydelig, og de har også ulike sikkerhetsmessige utfordringer.

Enkelte gjennomfører i stor grad systematiske sikkerhetstiltak og er mer robuste mot dataangrep, men har utfordringer med å sikre at tiltak blir gjennomført konsekvent i hele institusjonen.

Flere forskningsinstitusjoner har imidlertid kommet kortere, de har klare mangler i tekniske sikkerhetstiltak og begrenset evne til å oppdage dataangrep.

Undersøkelsen vår viser forbedringer i tekniske sikkerhetstiltak de seneste årene. For eksempel er to faktor-autentisering innført for mange tjenester, og ekstern sårbarhetsskanning er etablert av Sikt – Kunnskapssektorens tjenesteleverandør.

For flere av forskningsinstitusjonene er påviste svakheter i tekniske sikkerhetstiltak av en slik karakter at det vil ta tid å nå et tilfredsstillende sikkerhetsnivå.

Etter vår vurdering er det for store svakheter i grunnleggende tekniske sikkerhetstiltak i mange av forskningsinstitusjonene og dermed viktig med et systematisk arbeid for å oppnå en bedre beskyttelse mot dataangrep. Dette gjelder både små og store institusjoner.

***

For at en virksomhet skal oppnå et egnet sikkerhetsnivå må de tekniske sikkerhetstiltakene kombineres med sikkerhetstiltak i organisasjonen og rettet mot den enkelte bruker av IT-systemer.

For alle de ti forskningsinstitusjonene har vi derfor gjennomgått utvalgte sikkerhetstiltak som er ment å beskytte forskningsdata, og undersøkt om disse er i tråd med god praksis.

Undersøkelsen viser flere svakheter i gjennomføringen av tiltakene:

- Forskningsinstitusjonene har ikke god nok oversikt over forskningsdata. Det er **ikke tilfredsstillende**.
- De gir lite veiledning om sikker behandling av forskningsdata utover personopplysninger
- Opplæring og bevisstgjøring om informasjonssikkerhet og håndtering av forskningsdata er lite systematisk ved de fleste av institusjonene.
- IT-systemer som blir driftet lokalt i fakulteter, institutter og lignende omfattes ofte ikke av deres sentrale retningslinjer og rutiner
- De følger i liten grad opp sikkerheten hos leverandører av IT-løsninger.

Institusjonene har gjort forbedringer i gjennomføringen av disse organisatoriske sikkerhetstiltakene de siste årene. Spesielt har de arbeidet med å kartlegge og forbedre rutiner for behandling av personopplysninger.

Arbeidet med andre organisatoriske sikkerhetstiltak har de imidlertid kommet kortere med.

Vår vurdering er at det er et særlig behov for bedre sikkerhetstiltak for å identifisere og beskytte forretningssensitiv informasjon og informasjon som kan være av interesse for fremmede stater.

***

Gitt kravene i lovverket og de mulige konsekvensene av at sensitive data kommer på avveier, mener vi at det er **kritikkverdig** at forskningsdata i forskningsinstitusjoner ikke er tilstrekkelig sikret mot dataangrep.

***

Virksomhetene skal ha et ledelsessystem for informasjonssikkerhet. Systemet skal sikre at passende sikkerhetstiltak blir gjennomført og tilfredsstillende sikkerhet blir oppnådd.

Riksrevisjonens undersøkelse viser at det fortsatt er mangler i implementeringen av ledelsessystemene i forskningsinstitusjonene. De viktigste utfordringene gjelder:

- konkretisering av krav til gjennomføring av besluttede tiltak
- risikostyring
- evalueringer og etterkontroller av sikkerhetstilstanden
- avklaringer om roller og ansvar
- kompetanse og ressurser
- ledelsens informasjonsgrunnlag
- styrets rolle

Det er stor variasjon i forskningsinstitusjonenes arbeid med informasjonssikkerhet. Dette er til dels naturlig fordi de har svært ulik størrelse, ulikt omfang av forskningsdata og ulik kompleksitet i IT-infrastruktur. Hvordan disse utfordringene skal tas tak i, må være tilpasset den enkelte institusjon.

Styret har det øverste ansvaret for å håndtere risikoen for informasjonssikkerheten og for at virksomheten har systemer som hindrer at sensitive forskningsdata i virksomheten kommer på avveier.

Etter vår vurdering mottar de fleste styrene for lite informasjon om informasjonssikkerhetsrisikoen til å kunne ta stilling til sikkerhetsnivået.

Trusselsituasjonen i sektoren er betydelig skjerpet de siste årene, og det er viktig at styrene tar sitt ansvar for å påse at institusjonene har god nok informasjonssikkerhet.

Så, til tross for forbedringer i undersøkelsesperioden, arbeider mange forskningsinstitusjonene i for liten grad systematisk med informasjonssikkerhet, og styrene deres fyller ikke i stor nok grad rollen de skal ha. Dette er **ikke tilfredsstillende**.

***

Kunnskapsdepartementet har ansvar for å avklare sentrale roller og ansvarsområder på informasjonssikkerhetsområdet og sørge for at den

overordnede organiseringen og virkemiddelbruken på området er ressurseffektiv.

I 2019 satte Kunnskapsdepartementet i gang et fireårig informasjonssikkerhetsprogram i universitets- og høyskolesektoren.

Departementet etablerte en styringsmodell for informasjonssikkerhet, hvor ansvaret ble gitt til Direktoratet for høyere utdanning og kompetanse. De etablerte også et Cybersikkerhetssenter for høyere utdanning og forskning. Ansvaret for senteret er gitt til Sikt – Kunnskapssektorens tjenesteleverandør.

Undersøkelsen vår viser at styringsmodellen har gjort at den enkelte forskningsinstitusjon har fått tettere oppfølging. Det er positivt.

Samtidig ser vi at Kunnskapsdepartementet i begrenset grad har lyktes med å nå målet med informasjonssikkerhetssatsingen.

Flere institusjoner har blant annet svak evne til å oppdage dataangrep. Opprettelsen av Cybersikkerhetssenteret ser foreløpig ikke ut til å ha avhjulpet dette problemet.

Riksrevisjonens vurdering er at senterets tjenestetilbud i dag styres i for stor grad av den enkelte virksomhets etterspørsel og betalingsvilje, og i for liten grad av behovene til sektoren som helhet. Vi ser også at virkemidlene i for liten grad treffer de små forskningsinstitusjonene som har størst behov for støtte. Dette er **ikke tilfredsstillende**.

***

Kunnskapsdepartementet skal sørge for å ha et tilstrekkelig informasjonsgrunnlag for styringen.

Vår undersøkelse viser at Direktoratet for høyere utdanning og kompetanse baserer sine risiko- og tilstandsvurderinger til departementet på forskningsinstitusjonenes egenrapportering.

Flere av forskningsinstitusjonene i undersøkelsen har kjøpt inntrengingstester fra private konsulentselskaper eller revisjonsfirmaer, men Kunnskapsdepartementet får ikke informasjon om resultatene fra disse testene.

Cybersikkerhetssenteret kan også gjennomføre for eksempel inntrengingstester, men dette har senteret hittil ikke kapasitet til.

Kunnskapsdepartementet har gitt Nasjonalt organ for kvalitet i utdanningen, NOKUT, ansvar for å føre uavhengig kontroll med

informasjonssikkerheten i sektoren, men de gjennomfører ikke noen slike kontroller.

Kunnskapsdepartementet mottar med andre ord lite systematisk informasjon om de tekniske sikkerhetstiltakene som er iverksatt ute i virksomhetene, og om virkningen av tekniske og organisatoriske sikkerhetstiltak. Kunnskap om den faktiske sikkerhetstilstanden og verdiene i sektoren er viktig for at departementet skal kunne målrette krav og tiltak slik at sektoren er bedre i stand til å forbedre sikkerheten.

Undersøkelsen vår viser også at risikoreduserende tiltak på sektornivå som er identifisert, og som Kunnskapsdepartementet er orientert om, ikke blir gjennomført.

Dette gjelder tiltak som inntrengingstesting, revisjoner av den enkelte virksomhets arbeid med informasjonssikkerhet og personvern og kompetanseheving overfor virksomhetene.

En del av tiltakene har ikke blitt gjennomført, og har heller ikke vært realistiske å gjennomføre, da de i praksis har forutsatt både at Cybersikkerhetssenteret etablerer nye tjenester og at forskningsinstitusjonene betaler for gjennomføringen.

Det er **ikke tilfredsstillende** at Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og at risikoreduserende tiltak ikke blir fulgt opp.

***

Så vil jeg benytte muligheten til å nevne at vi tidligere i dag offentliggjorde en undersøkelse om sømløse kollektivreiser. Den viser at det fortsatt er for komplisert å reise kollektivt og at den nasjonale reiseappen Entur er lite kjent og lite brukt. Du finner den også på riksrevisjonen.no.

***

Takk for oppmerksomheten!