UniKunn (Universitetet for kunnskap) er et privat universitet med campuser i flere norske byer. Anta at du jobber i UKIT (UniKunns IT-avdeling) der du har fått i oppdrag å utføre en risikovurdering basert på følgende notat fra UniKunns sentraladministrasjon.

NOTAT fra sentraladministrasjonen i UniKunn
Hasteoppdrag for UKIT, høst 2026

Risikovurdering av eksamensplattformen Expera

Bakgrunn

UniKunn benytter eksamensplattformen Expera som er en SaaS skytjenese. Under forrige eksamensperiode ble det oppdaget uregelmessigheter ved eksamensplattformen Expera. Det mistenkes at følgende hendelser har inntruffet ved ulike eksamener:

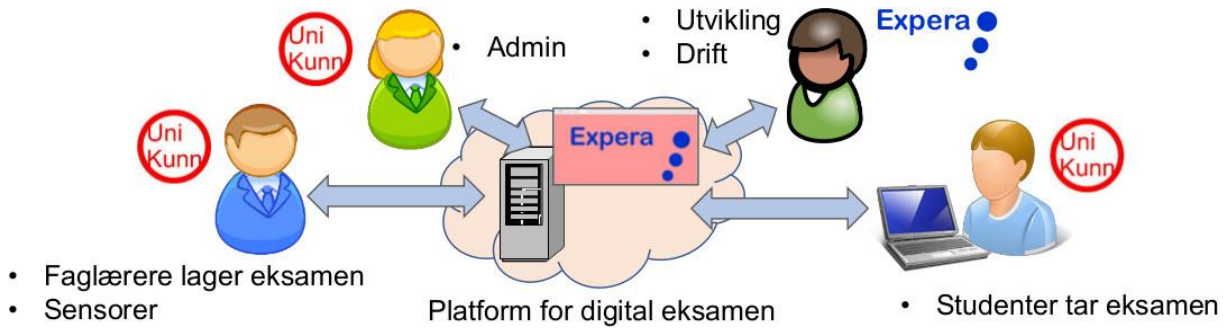
- Uautorisert uthenting av eksamensoppgaver før en eksamen.
- DDoS-angrep mot Experas server under eksamen.
- Uautorisert endring av sensur/karakter under sensureringsfasen.

UKIT har mottatt trusseletterretning om en cyberkriminell aktør kalt GradeAaaS som tilbyr tjenester på det mørke nettet. Blant tjenestene som GradeAaaS tilbyr er salg av ferske eksamensoppgaver før eksamen, DDoS-ing av eksamensplattformer, og endring av karakterer på ulike eksamensplattformer. Kunder av tjenestene antas å være studenter og deres familier som urettmessig betaler for å kunne få gode karakterer. GradeAaaS har en katalog over ulike eksamensplattformer og universiteter rundt i verden der disse tjenestene kan tilbys. Nylig har Expera og UniKunn blitt listet i katalogen.

UniKunns ledelse anser at denne situasjonen kan utvikle seg til å bli en eksistensiell trussel for universitetet. Det kan potensielt undergrave tilliten til UniKunns eksamener og vitnemål. I ytterste konsekvens kan UniKunn miste NOKUT-akkreditering hos Utdanningsdirektoratet for sine studieprogrammer, noe som kunne føre til nedstenging av hele universitetet og konkurs. På den bakgrunn ønsker UniKunns ledelse at UKIT gjennomfører en risikovurdering av Expera, og at UKIT foreslår sikkerhetstiltak. Dette prosjekter haster fordi anbefalte sikkerhetstiltak bør iverksettes før eksamensavvikling høsten 2026.

Situasjon for risikovurderingen

UniKunn benytter Experas eksamensplattform til å lage, gjennomføre og sensurere digitale eksamener, både hjemme-eksamen og i egne eksamenslokaler. Expera er en amerikansk SaaS skyløsning som driftes fra USA og utvikles i India. De viktigste brukergruppene for en Expera-installasjon hos et universitet er admin, faglærere/sensorer og studenter ved universitetet, og utviklere og drift hos Expera. Figur 1 nedenfor viser brukergruppene for UniKunns installasjon av Expera.



Figur 1. Brukere av Expera i UniKunns installasjon

Overordnet beskrivelse av UniKunns konfigurering av Exsperas eksamensplattform:

- Hvert universitet bestemmer hvordan innlogging til Expera skal skje, som f.eks. kan være med enkelt passord, med en internett-ID (f.eks. facebook eller google), med SMS-basert 2FA, eller andre nasjonale løsninger. UniKunn benytter kun enkelt passord for innlogging til sin Expera-løsning, uten noen spesifikk passordpolicy.
- Tilgangsautoriseringer
  - Faglærere har tilgang til å lese/redigere eksamensoppgaver i emner de underviser
  - Studenter har tilgang til å lese og besvare oppgaver under eksamen
  - Sensorer har tilgang til besvarelser og karaktersetting for eksamener de sensurerer
  - UniKunn admin spesifiserer tilgangsrettigheter for faglærere, sensorer og studenter
  - Expera drift har tilgang til å lese og redigere alle datapunkter i UniKunns Expera-plattform, inkludert oppgaver, besvarelser og sensurer/karakterer
  - Experas systemutviklere har tilgang til å konfigurere UniKunns eksamensplattform

Følgende ansvarsfordeling for sikkerhet gjelder

1. Expera er ansvarlig for nettverkssikkerhet (brannmur, IDS, logg og analyse av nettverkstrafikk) og hendelsesrespons for nettverkshendelser.
2. Expera har ansvar for å håndtere angrep mot selve sky-plattformen, men håndterer ikke angrep mot UniKunns egne applikasjoner.
3. UniKunn er ansvarlig for brukeridentiteter, autentiseringsordningen, og for tilgangsstyring for admin, faglærere, sensorer og studenter.

Oppgave

I denne oppgaven skal en kombinasjon av kvalitativ og kvantitativ beregning av risiko benyttes. Her uttrykkes kvalitativ sannsynlighet og konsekvens på skalaen [0, 5], og den beregnede kvalitative risikoen på skalaen [0, 10]. Risikovurderinger gjøres med regnearket som kan lastes ned fra: https://www.mn.uio.no/ifi/forskning/grupper/sec/laeringsressurser/uio-risikovurdering.xlsx

Besvarelsen skal bestå av ett pdf-dokument, strukturert etter romertall I – IV nedenfor.

I. Følgende skal defineres (10 p):
   - Kvalitativt terskelnivå for akseptabel risiko. Terskelnivået må velges i intervallet [4, 7]. Valg av terskelnivå skal begrunnes ut ifra UniKunns risikoappetitt.

II. Følgende skal kalibreres i regnearket (20 p)
   - «Snarest» antatt hendelsesfrekvens *S* som sannsynlig antall hendelser per år, som dermed representerer kvalitativt sannsynlighetsnivå 5 (høyest).

- «Verst» tenkelig konsekvens *V* som et kvantitativt tap, som dermed representerer kvalitativt konsekvensnivå 5 (høyest).

III. Bruk regnearket til å utføre risikovurderinger (50 p.).

For risikovurderingene anses en eksamen å være en prosess med tre faser:
1) Redigering: Faglærere redigerer eksamensoppgavene
2) Besvaring: Studentene besvarer oppgavene under eksamen
3) Sensurering: Sensorene gir karakter på eksamensbesvarelsene

Kategorier av digitale verdier (eng. assets) som skal tas med i vurderingene er:
- DATA: Eksamensoppgaver
- DATA: Sensurer/karakterer
- APP: Expera-plattformen

Konsekvens av brudd på sikkerhetsmålsettingene KIT (konfidensialitet, integritet, og tilgjengelighet) er forskjellig for de ulike verdikategoriene, og vil dessuten endre seg gjennom de tre fasene i eksamensprosessen. Risikovurdering skal gjøres for tre risikoer:

A. For eksamensoppgaver skal risiko for brudd på konfidensialitet før eksamen vurderes.
B. For sensurer/karakterer skal risiko for brudd på integritet vurderes.
C. For eksamensgjennomføring skal risiko for brudd på Experas tilgjengelighet vurderes.

Dette gjøres ved å beskrive hver av de tre risikoene og analysere deres risikonivåer. I regnearket skal risiko A, B og C beskrives henholdsvis på radene 8, 9 og 10. Hvis en risiko er uakseptabel skal det foreslås relevante sikkerhetstiltak som vil redusere risikoen til et akseptabelt nivå. Hver risiko og foreslåtte sikkerhetstiltak beskrives ved følgende:

- Beskriv en trussel som anses mest relevant
- Beskriv sårbarhet(er) og hendelse (brudd på sikkerhetsmål).
- Beskriv konsekvensaspekter ved hendelsen.
- Estimer kvalitativ sannsynlighet for at hendelsen inntreffer, dvs. for at en eksamen blir kompromittert på henholdsvis en av de tre nevnte måtene.
- Estimer kvalitativt konsekvensnivå i tilfelle en eksamen blir kompromittert.
- Automatisk beregne kvalitativt risikonivå før nye sikkerhetstiltak
- Automatisk beregne kvantitativ risiko, som funksjon av kvalitativ sannsynlighet og konsekvens, S og V.
- Hvis risikoen er uakseptabel, foreslå sikkerhetstiltak for å redusere risikoen.
- Revurder kvalitativt risikonivå etter innføring av sikkerhetstiltak(ene)
- Automatisk beregne kvantitativ risikoreduksjon etter håndtering med sikkerhetstiltak.

Det som forventes i besvarelsen av oppgave III er følgende:

- En beskrivelse av risikoene A, B og C basert på tekst fra regnearket.
- Kopi/screenshot av rader 2 – 10 og kolonner K – Y fra regnearket.

Selve regnearket skal **ikke** være en del av besvarelsen.

IV. Skriv et sammendrag av vurderingene for risiko A, B og C for UniKunns toppledelse (executive summary) (20 p).

Sammendraget skal inneholde:

- Grafisk samlet visualisering av de tre risikoene før og etter risikohåndtering. Visualiseringen skal ligne på lysbilde s.41 fra presentasjon 7b om risikostyring, der hver risiko A, B, C vises to ganger, dvs. både før og etter innføring av sikkerhetstiltak, med pil fra risiko før til risiko etter.
- Maks en halv side med tekst med kort oppsummering av vurderingene og anbefalte tiltak for hver risiko. Sammendraget skal forklare hvorfor risikoene håndteres på en god måte slik at sikkerhetsnivået blir forsvarlig. Sammendraget skal være på et språk som toppledelsen kan forstå, med antagelse om at toppledelsen har en ikke-teknisk utdanning og erfaring.