Informasjonssikkerhet i Nettskjema

2023-07-03

Innholdsfortegnelse

1. Innledning

Nettskjema er en webapplikasjon som gjør det mulig å lage og gjennomføre spørreundersøkelser på nett.

Webapplikasjonen er utviklet og driftet av IT-avdelingen ved Universitetet i Oslo (USIT) og brukes av UH- og helse-sektoren etter avtale. Den er basert på Java, og har en arkitektur som gjør det mulig å oppnå svært høy oppetid og skalerbarhet.

Nettskjema tilbyr innlogging med tofaktorautentisering både via Feide, ID-portens innloggingsløsning for offentlige tjenester på internett og innlogging via TSD.

Skjemadesign og svar på vanlige skjema lagres i nettskjemas database. Ved krav om ekstra sikker lagring tilbyr Nettskjema integrasjon mot lagringssystemene Educloud (godkjent for «røde data») og TSD som oppfyller lovens strenge krav til behandling og lagring av sensitive forskningsdata (godkjent for «svarte data»).

2. Avgrensing

Dette dokumentet er avgrenset til sikkerhetsrelaterte forhold rundt Nettskjema og integrasjon mot TSD og Educloud. For dokumentasjon av sikring av servere, database og driftsinfrastruktur, se UiOs *Ledelsessystem for informasjonssikkerhet* (LSIS) kapittel 8: Grunnsikring av infrastruktur og tjenester
https://www.uio.no/tjenester/it/sikkerhet/lsis/8.html

3. Informasjonssikkerhet og personopplysninger

Nettskjema er underlagt UiOs *Ledelsessystem for informasjonssikkerhet* (LSIS):
https://www.uio.no/tjenester/it/sikkerhet/lsis

3.1 Klassifisering av data og godkjent lagring

«Lagringsguiden» er et tillegg til LSIS som beskriver hvor man kan behandle, lagre, og bearbeide ulike typer informasjon. Nettskjema er beskrevet under «Andre Tjenester», og er godkjent for innsamling av alle kategorier av data.
https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/lagringsguide.html

Skjemadesign, svar på vanlige skjema og utvalgte metadata lagres i nettskjemas database.

Nettskjema er spesielt tilpasset innsamling av sensitive data til TSD, som er godkjent for lagring av «svarte data». Dette tilsvarer graden **strengt fortrolig** i den offentlige Beskyttelsesinstruksen[1]. Ved UiO er det kun TSD som er godkjent for lagring og håndtering av direkte identifiserbare helseopplysninger.
https://www.uio.no/tjenester/it/forskning/sensitiv

Nettskjema tilbyr samme integrasjon mot Educloud, som er godkjent for «røde data».
https://www.uio.no/tjenester/it/forskning/plattformer/edu-research

LSIS beskriver klassifisering og fargekoder for data nærmere:
https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/lagring/infoklasser.html

3.2 Risiko- og sårbarhetsvurdering

Det gjennomføres en risiko- og sårbarhetsvurdering (ROS) av Nettskjema minst annethvert år, i henhold til LSIS Kapittel 7: Risiko- og sårbarhetsanalyser:
https://www.uio.no/tjenester/it/sikkerhet/lsis/7.html

Siste versjon av risiko- og sårbarhetsvurdering for Nettskjema er fra juni 2023.

LSIS kapittel 7 spesifiserer: «Tiltaksplaner og risikovurderinger som inneholder beskrivelser av sårbarheter som kan lette angrep skal behandles som konfidensielle dokumenter og skjermes for innsyn.»

Vi har derfor laget dette dokumentet for å redegjøre for sikkerhet i Nettskjema.

3.3 Kontinuerlig sikkerhetsarbeid

Målet med risiko- og sårbarhetsvurderingen er å lage en tiltaksplan for eventuelle risikoelementer fra ROS med moderat eller høy risiko.

Det er viktig med kontinuerlig sikkerhetsrelatert arbeid. Nettskjemas utviklings-team har som rutine å gjøre en trusselmodellering av all ny funksjonalitet eller endringer i Nettskjema som vi vurderer er sikkerhetsrelatert, eller hvis vi ikke har full oversikt over de sikkerhetsrelaterte effektene.

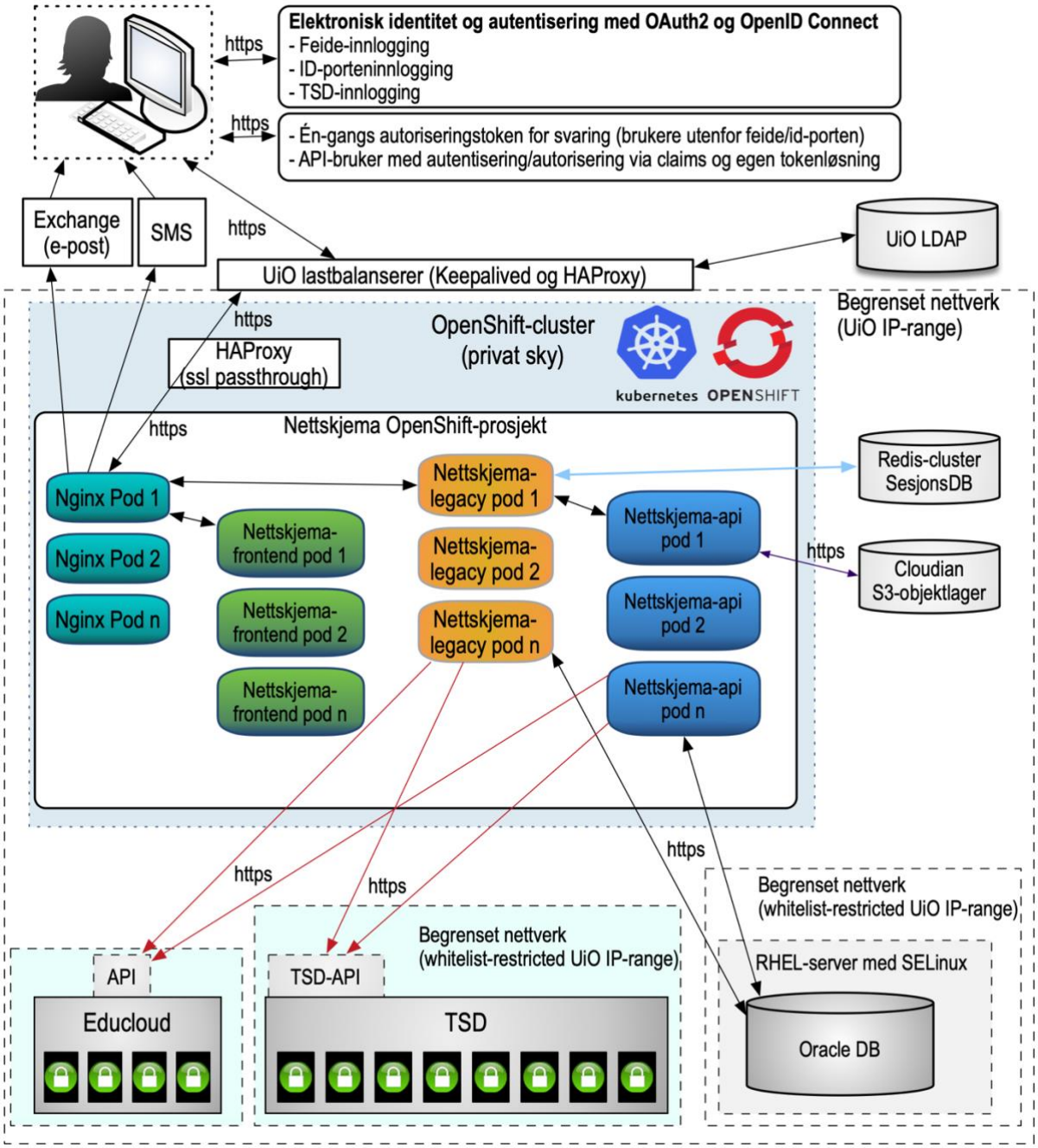
[1] https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352

Utviklingsarbeidet skal alltid skal være i henhold til «best practice» og forholde seg til «OWASP topp 10»: *Top 10 Most Critical Web Application Security Risks*
https://owasp.org/www-project-top-ten/

3.4 Sikkerhetstesting

Som et tiltak for å motvirke OWASP **A06:2021-Vulnerable and Outdated Components** bruker vi «*OWASP dependency check*» til daglig automatisk sikkerhetstesting av sårbarheter i alle programvarekomponenter vi bruker. Å fikse eventuelle alvorlige sårbarheter i komponenter prioriteres foran annet utviklingsarbeid.

4. Teknisk systembeskrivelse



4.1 Digital identitet og tilgangsstyring

For administrering av skjema tilbyr Nettskjema elektronisk identitet og autentisering med protokollene OpenID Connect/OAuth2 fra identitetstilbyderne Feide, ID-porten og TSD.

Feide (*Felles Elektronisk IDEntitet*) utvikles av Sikt, og er Kunnskapsdepartementets valgte løsning for sikker identifisering i utdanningssektoren. Tofaktorautentisering (2FA) kreves av de fleste feideinstitusjonene.

ID-porten er felles innloggingsløsning for offentlige tjenester på internett, og blir driftet av Digitaliseringsdirektoratet. Innlogging krever tofaktorautentisering.

TSD tilbyr også egen elektronisk ID og innlogging med tofaktorautentisering.

Feidebrukere ved institusjoner som har avtale med Nettskjema har tilgang til å bruke Nettskjema til å lage egne skjema. Det er også mulig å gi tilgang til enkeltbrukere som autentiserer seg via Feide, ID-porten eller TSD.

Det er mulig å gi grupper ved UiO rettigheter til et skjema. Grupperettigheter er ikke implementert for andre institusjoner.

Hvert enkelt skjema må spesifisere en respondentgruppe som kan svare på skjemaet:

- Innloggede Feide-brukere
- ID-porten nivå 3 eller nivå 4 (og eventuell signering)
- Kun inviterte - invitasjon via e-post eller SMS
  - Autentisering via Feide for Feide-brukere
  - Autentisering via éngangstoken for andre brukere
- Uautentisert, dvs. uten innlogging, bl.a. for anonyme svar

4.2 Kryptering

All trafikk til og fra Nettskjema foregår over krypterte forbindelser, men data lagres i de fleste tilfeller ikke kryptert.

Nettskjema har frem til 2023 støttet PGP-kryptering av svar lagret i nettskjemas database, men holder på å fase ut denne tjenesten, og anbefaler i stedet lagring i TSD.

Svar på skjema knyttet til TSD og Educloud lagres i utgangspunktet kun i henholdsvis TSD eller Educloud. Hvis det oppstår en feil i kommunikasjon med TSD/Educloud, f.eks. hvis lagringstjenesten har driftsproblemer, mellomlagres svaret kryptert i objektlagringssystemet Cloudian.

4.3 Driftsmiljø, utviklingsinfrastruktur og overvåking

Nettskjema driftes i henhold til vanlig strengt driftsregime ved IT-avdelingen.

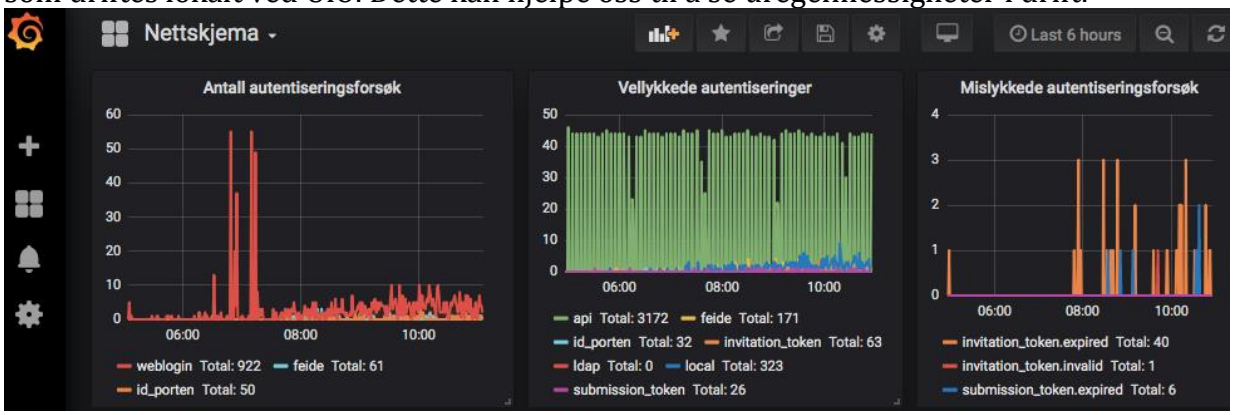
Driftsmiljøet er en lokalt driftet instans av okd (privat sky).

Vi bruker sentral overvåking med lokalt driftet Zabbix og logging til lokalt driftet ELK.

Nettskjema logger applikasjonens driftsdata («helsedata») i overvåkingssystemet Zabbix som utgangspunkt for alarmer. Utviklerteam og hjemmevakt varsles om eventuelle

driftsforstyrrelser via e-post og chat. Vi bruker lokalt driftet instans av Mattermost til chat.

Viktige måltall for applikasjonen aggregeres i en Graphite database. Målinger, tidsserier og trendanalyser kan visualiseres via ulike dashboards i en Grafana-instans som driftes lokalt ved UiO. Dette kan hjelpe oss til å se uregelmessigheter i drift.



4.4 Backup

Det tas kontinuerlig backup av data i Nettskjemas database som beholdes 90 dager. Se informasjon fra TSD og Educloud for data som lagres i disse systemene.

4.5 Utvikling og kildekode

Nettskjema utvikles i *Seksjon for Webutvikling* i *Underavdeling for IT i forskning, formidling og utdanning*, som er en del av IT-avdelingen ved Universitetet i Oslo.

Nettskjema-teamene jobber etter prinsippene for smidig programvareutvikling og DevOps. Et av hovedmålene er kort vei (tid) fra behov for ny funksjonalitet, eller behov for endring/retting, til produksjonssetting.

For å klare dette, og ha kontroll på risiko og sårbarhet, utvikler vi applikasjonen og tilhørende støttesystemer i små inkrementelle steg, og har fokus på automatisert testing og kontinuerlig kvalitetsforbedring i utviklingsstøttesystemene.

Med små endringer fra forrige versjon er det mindre som kan gå feil. Mer isolerte endringer påvirker vanligvis mindre del av applikasjonen. Dette gjør det enklere å oppdage feil og enklere å fikse eller rulle tilbake feil.

Kortere tid mellom utvikling/kodeskriving og prodsetting gjør at det er mindre sjanse for at miljøendringer rundt systemet gir feil. Utvikleren er inne i problemstillingen (i kontekst) og kan raskere/enklere oppdage og rette opp eventuelle feil. Utvikleren er ikke ferdig før utviklet funksjonalitet er i produksjon og virker som planlagt.

Utviklerne må bruke sin personlige driftsbruker-konto med obligatorisk tofaktorautentisering ved utvikling og administrasjon av driftstøttesystemer.

Kodekontroll

Alle prioriterte ønsker og behov for utvikling spesifiseres som brukerhistorier eller oppgaver.

Vi praktiserer streng kodekontroll. For all ny funksjonalitet skal det opprettes en egen kodegren (feature branch) i versjonskontrollsystemet som knyttes til en oppgave. Vi bruker GitHub Enterprise server som driftes lokalt ved UiO.

Tilordning av oppgaver til de enkelte utviklere og status for arbeidsflyt registreres i *Jira* eller *GitHub Issues*.

All kode som skal flettes inn må gjennom en kodegjennomgang (code review) i form av en «pull request», der andre utviklere må lese gjennom og godkjenne endringene. Det er dermed minst «4 øyne» på all ny kode som går ut i produksjon.

CI-server, testing og automatisering

Vi bruker CI/CD-server med automatisert bygging, enhetstester, funksjonelle tester og integrasjonstesting. (Per juni 2023 brukes Jenkins med planlagt overgang til GitHub Actions ca 2024.)

Som nevnt i kapittel 3.3 har vi en CI/CD pipeline som automatisk kjører «*OWASP dependency check*» hver dag. Denne søker etter nye publiserte sårbarheter i alle programvarekomponenter vi bruker, for å avdekke om noe må oppdateres.

I tillegg til full kjøring av automatiserte tester ved kodeendringer i produksjon, har vi integrert automatisert testing så tidlig i prosessen som mulig, dvs. automatisert testing ved alle commit av kode.