SAFE for beslutningstakere

Formål

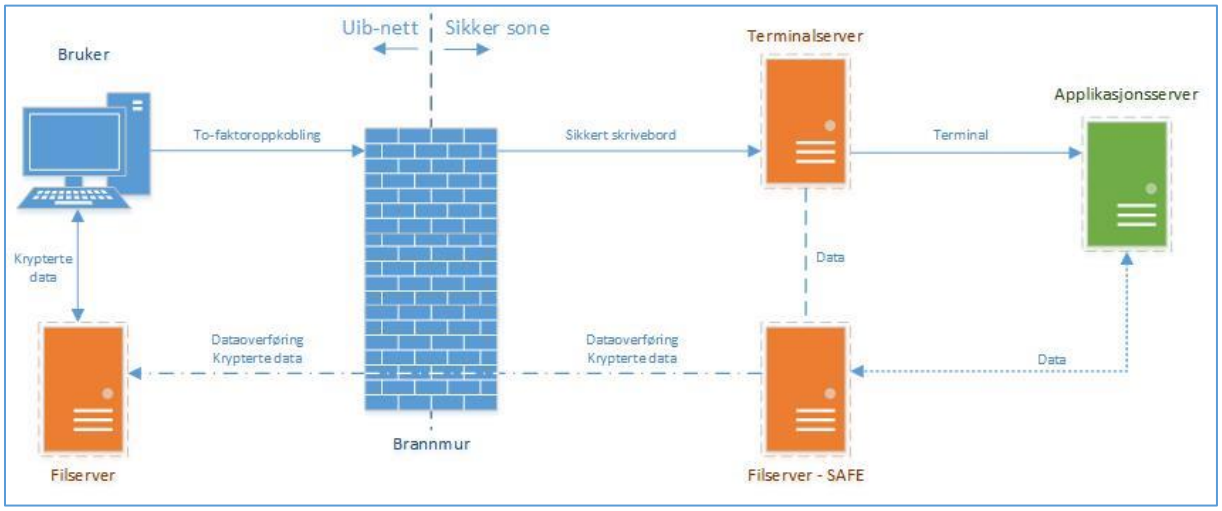
På IT-avdelingen ved Universitetet i Bergen har vi utviklet en løsning for sikker behandling av sensitive personopplysninger i forskning. Løsningen kaller vi SAFE (Sikker Adgang til Forskningsdata og E-infrastruktur).

SAFE bygger på Norm for informasjonssikkerhet i helse- og omsorgstjenestene (Normen) og sikrer at informasjonssikkerheten med hensyn til konfidensialitet, integritet og tilgjengelighet blir ivaretatt ved behandling av sensitive personopplysninger.

Gjennom SAFE tilbyr IT-avdelingen en løsning der ansatte, studenter og eksterne får tilgang til dedikerte ressurser for behandling av sensitive personopplysninger.

Prinsipp

Tilgang til SAFE kan beskrives med følgende figur:



Tilgang til SAFE

Brukeren når sitt *sikre skrivebord* fra sin egen datamaskin ved å bruke en VPN-klient som støtter to-faktor autentisering. I praksis betyr det at bruker må oppgi en engangskode i tillegg til brukernavn og passord. Brukeren mottar engangspassord på mobiltelefonen, enten som en tekstmelding eller i en app. Etter vellykket VPN-oppkobling mot SAFE, kan bruker koble seg mot sitt sikre skrivebord med «Remote Desktop» programvare.

Det sikre skrivebordet er en sesjon på en Windows terminalserver som er herdet i tråd med Datatilsynets, temaark 1, «Bruk av terminalserver». Fra det sikre skrivebordet er det ikke mulig å klippe/lime, skrive ut eller koble seg mot filområder.

Brukere i samme prosjekt deler terminalserver. Data ligger på en filserver, men er tilgjengelig som et filområde fra det sikre skrivebordet. Tilgang til filene er styrt av prosjektleder i et tilgangsdokument.

Noen prosjekter kan få tilgang til en dedikert Linux applikasjonsserver om det er behov for det. Brukerne når applikasjonsserveren over ssh-protokollen via programvaren Putty eller X-win.

Overføring av filer til og fra SAFE gjøres ved hjelp av en filsluse.

Opprette prosjekt i SAFE

Prosjektleder kan be om å få opprettet prosjekt i SAFE i *problemdatabasen* (https://bs.uib.no/). En dedikert terminalserver blir satt opp av IT-avdelingen i samråd med prosjektleder. Relevant programvare installeres og prosjektleder får tilgang. En filstruktur med relevant tilgangsstyring blir satt opp slik at prosjektleder kan overføre data inn i SAFE.

For å gi andre brukere tilgang til prosjektet må tilgangsdokumentet oppdateres. Tilgangsdokumentet er kun tilgjengelig for prosjektleder og inneholder autoritativ informasjon om alle brukere i prosjektet, deres brukernavn, navn, mobilnummer og hvilken tilgang de skal ha. For å initiere endring basert på tilgangsdokumentet, oppretter prosjektleder sak i problemdatabasen.

Tilgang til SAFE krever per i dag konto ved UiB, men for eksterne brukere kan en slik konto opprettes ved avdelingen/instituttet der prosjektet hører hjemme.

Overføring av data

Data til og fra SAFE overføres via en filsluse. I praksis er filslusen to filstrukturer; en i SAFE og en i UiB-nett, samt en samling skript som overfører data mellom disse filstrukturene i faste intervaller. Prosjektleder styrer hvilke brukere som har tilgang til filslusen for sitt prosjekt.

Når data overføres ut av SAFE, blir det i tillegg laget an kopi av filen samt en loggoppføring som beskriver overføringen som prosjektleder har tilgang til. Før data overføres ut av SAFE, blir de også kryptert med AES-256. Passordet for å åpne filen ligger i en mappe som brukeren har tilgang til i SAFE.

Infrastruktur

SAFE er bygget på en virtualiseringsplattform basert på VMware. Sikkerhetskopi av filserverne og applikasjonsserverne blir kryptert før data forlater SAFE. Sikkerhetskopi av Terminalserverne inneholder ingen persondata og blir ikke kryptert. Hardware i SAFE er i størst mulig grad redundant.

Drift av SAFE

For å kunne drifte løsningen har IT-avdelingens driftspersonell tilgang til driftssonen. Herfra er det mulig å utføre vedlikehold på den fysiske plattformen SAFE er bygget på.

SAFE benytter seg av noen grunnleggende nettverkstjenester i UiB-nett som DNS, DHCP, AD og Puppet. SAFE følger også IT-avdelingens oppgraderingsregime med fast endringtidspunkt 3. lørdag hver måned.

Drift av klienter

IT-avdelingen ved UiB tilbyr drift av klienter både for Windows, Mac og Linux. For brukere som ikke har datamaskin driftet av UiBs IT-avdeling, forventes det at brukeren forholder seg til kravene som er skissert i dokumentet, «SAFE N - Kontrakt med eksterne brukere.docx» (vedlegg 1).

Opplæring

Det er laget et kurs på *Mitt UiB* (https://mitt.uib.no) som gir potensielle brukere av SAFE en forståelse av hva løsningen kan tilby, samt detaljerte beskrivelser av hvordan man kommer i gang med å bruke SAFE. Kurset krever konto ved UiB.

Vedlegg 1:

UNIVERSITETET I BERGEN
IT-avdelingen

Avtale mellom Universitetet i Bergen og <navn på partner> ved <navn på institusjon>

Sikker Adgang til Forskningsdata og E-infrastruktur (SAFE)

Minimumskrav til utstyr som skal koble seg opp mot SAFE:

For å koble seg opp mot SAFE med utstyr som ikke er driftet av IT-avdelingen ved UiB forventes det at følgende krav er oppfylt:

1. Maskinen er personlig (ikke delt)
2. Operativsystemet er supportert og oppdatert
3. Antivirusprogramvare er installert og oppdatert
4. Personlig brannmur er påslått
5. Pålogging er gjort med konto uten hevede rettigheter
6. Låsing av skjerm ved inaktivitet er aktivert
7. Passordet er komplekst
8. Autentisering kun foregår kryptert
9. Ingen unødvendige tjenester kjøres lokalt

I tillegg forventes følgende oppførsel:

1. SAFE skal kun brukes til det formål det er tiltenkt
2. I den grad sensitive personopplysninger hentes ut fra SAFE oppbevares disse kryptert så lenge maskinen er tilknyttet internett
3. Alle sikkerhetshendelser rapporteres til UiBs sikkerhetsansvarlige

Universitetet i Bergen forbeholder seg retten til å til å blokkere tilgang til SAFE fra maskiner som ikke tilfredsstiller nevnte krav.

signatur partner