Styringsmodel for Uniloginføderationen

Version 1 20.12.2019

Baggrund

Nærværende dokument beskriver de formelle krav, som myndigheder skal leve op til for at kunne blive tilkoblet Unilogin Broker med henblik på, at brugere kan anvende egen IdP i Unilogins sikkerhedsføderation.

Formelle krav til ansvarlige for IdP'er på sigt

Unilogin Føderationen vil på sigt anvende rammeværket i National Standard for Identiteters Sikringsniveauer (NSIS), Version 2.0.1. Styrelsen for It og Læring sørger for anmeldelsen af Unilogin Broker til Digitaliseringsstyrelsen.

Hvis en organisation på dette tidspunkt ønsker at få tilkoblet organisationens egen IdP til Unilogin Broker, skal IdP'en ligeledes på sigt anmeldes til Digitaliseringsstyrelsen på det sikringsniveau, som IdP'en kan opfylde.

Skemaer til NSIS anmeldelse, vejledninger mv. findes her:
https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/

Når en IdP er NSIS-anmeldt til Digitaliseringsstyrelsen, vil NSIS rammeværket udgøre den styringsmodel, som Unilogin føderationen vil bygge på. Lokale IdP'er, der ønsker at blive koblet på Unilogin Broker vil dog fortsat skulle anmelde sig til STIL, da dette er den formelle meddelelse til STIL om, at man ønsker at få tilkoblet en IdP på brokeren. Denne anmeldelse vil dog begrænse sig til et supplement til NSIS anmeldelse, hvor anmelderen skal forpligte sig til at dele sikkerhedshændelser og tilsvarende nødvendige oplysninger med STIL.

Formelle krav til ansvarlige for IdP'er frem mod NSIS implementeringen

Fra idriftsættelse af det nye Unilogin og den nye Unilogin Broker i februar 2020 vil Unilogin føderationen ikke understøtte NSIS. Frem mod implementeringen af NSIS sikringsniveauerne skal autentificering med lokale IdP'er være korrekt, men med en lokal vurdering af, hvad dette indebærer. Den lokale vurdering skal dog tage udgangspunkt i kravene til NSIS sikringsniveauerne. Anmeldere af IdP'er har ansvaret for hele livscyklus for Id-midlet og vurderer i den forbindelse, hvad der giver et tilstrækkeligt sikkerhedsniveau. Id-midlets livscyklus er nærmere defineret i NSIS, og NSIS indeholder en række krav til IdP'er, som kan inspirere anmelderen af en IdP til, hvad der kan give et tilstrækkeligt sikkerhedsniveau. NSIS er en god retningslinje for et godt 1-faktor login, og en bevidsthed omkring kravene i NSIS kan desuden mindske forandringen ved en NSIS-anmeldelse.

IdP'er, der omfatter børn, vil ikke være omfattet af NSIS, men NSIS kan også i disse tilfælde anvendes som rettesnor for IdP'en i kombination med den tekniske løsning for Unilogin IdP'en, sådan at lokale IdP'er for børn på sigt lægger sig så tæt op af NSIS som muligt. Ved lanceringen af det nye Unilogin i uge 8 skal lokale IdP'er for børn således også tage udgangspunkt i kravene for NSIS sikringsniveauerne. En IdP for børn skal ikke anmeldes til Digitaliseringsstyrelsen, før der evt. er fundet tekniske løsninger, der gør, at kravene til NSIS også kan opfyldes for børn. Indtil da skal IdP'er for børn alene anmeldes til STIL.

Herudover skal den ansvarlige for en IdP, der ønskes koblet til Unilogin Broker, også indgå en aftale med Styrelsen for It og Læring om tilkoblingen. I denne aftale skal kommunen eller institutionen forpligte sig til af egen drift straks at meddele Styrelsen for It og Læring, hvis sikringsniveauet ønskes ændret, eller hvis der er en sikkerhedshændelse i forhold til den lokale IdP. Kommunen eller institutionen skal ligeledes være til rådighed for en opfølgende dialog samt afklaring af evt. spørgsmål fra Styrelsen for It og Læring.

Hvis en sikkerhedshændelse påvirker brugere, er det kommunens eller institutionens ansvar at informere brugerne om dette, og relevante modforanstaltninger skal træffes som f.eks. spærring af IdP'en mv. I tilfælde af en sikkerhedshændelse i en lokal IdP, hvor Styrelsen for It og Læring vurderer, at det er nødvendigt at afkoble den lokale IdP fra Unilogin Broker for at dæmme op for sikkerhedshændelsen, kan Styrelsen for It og Læring gøre dette. Styrelsen for It og Læring kan desuden i den forbindelse sætte IdP'ens sikringsniveau til et lavere sikringsniveau, hvis Styrelsen for It og Læring vurderer, at dette er mere retvisende. Styrelsen for It og Læring vil dog kun gøre dette, hvis dette er proportionalt med den risiko, der er forbundet med ikke at gøre det. Hvis en lokal IdP afkobles brokeren, vil brugerne kunne anvende Unilogin indtil den lokale IdP evt. kan kobles på brokeren igen.

Endelig skal kommunen eller institutionen erklære, at kommunen eller institutionen er opmærksom på, at der på sigt vil blive stillet krav om NSIS-anmeldelse, og at et sådant krav vil medføre, at den lokale IdP enten skal være NSIS anmeldt eller vil blive afkoblet Unilogin Broker. Kravene til NSIS anmeldelsen vil følge implementeringen af NemLog-in og MitID, som forventes lanceret henholdsvis november 2020 og sommer 2021. Hvis denne implementering bliver forsinket, forsinkes kravet om NSIS-anmeldelse tilsvarende.

Proces for tilkobling af lokal IdP

Processen for at få koblet en lokal IdP på brokeren vil således overordnet være følgende:

- Kontakt Styrelsen for It og Lærings Support med henblik på at blive tilkoblet STILs eksterne testmiljø, herunder fremsendelse af relevante metadata
- IdP'en tilkobles STILs eksterne testmiljø og anmelderen af IdP'en sørger for, at den lokale IdP testes på testbrugere i brugerorganisationen
- Indsend underskreven anmeldelse af lokal ID-tjeneste til Styrelsen for It og Lærings Support
- IdP'en kobles på Unilogin Broker

Som ansvarlig for en IdP tilkoblet Unilogin Broker, skal man tage hånd om alle dele af livscyklussen for Id-midlet. Dette er nærmere beskrevet i NSIS standarden, der kan give inspiration til, hvad der er tilstrækkeligt.

Uanset om der er tale om en NSIS anmeldt IdP eller ej, er den der anmelder en IdP til Styrelsen for It og Læring ansvarlig over for evt. fejl og svigt over for dem, der anvender IdP'en.

Brokere for IdP'er med flere ansvarlige, kan ikke kobles på Unilogin Broker, så længe føderationen ikke har implementeret NSIS. Det er således kun den ansvarlige myndighed, der kan få koblet en IdP på Unilogin Broker. Det er STIL uvedkommende, om den ansvarlige myndighed selv udvikler sin IdP-løsning eller indgår en aftale med en privat leverandør. STIL har dog brug for et minimum af indblik i den løsning, der er valgt for den lokale IdP af hensyn til de tjenester, der er tilkoblet Unilogin Broker og for at kunne håndtere sikkerhedshændelser så effektivt som muligt. Private leverandører kan få koblet test-IdP'er på STILs eksterne testmiljø, hvis leverandøren har mindst ét etableret kundeforhold til en ansvarlige myndighed.

Ud over Unilogin IdP og lokale IdP'er vil NemID også være tilkoblet brokeren.

Oversigt over formelle krav

Beskrivelse af plan for idriftsættelse og evt. NSIS anmeldelse
Overordnet beskrivelse af den lokale ID-tjeneste
Overordnet beskrivelse af det organisatoriske setup, parter, underleverandører mv.
Underskrevet ledelseserklæring ift.

- at ID-tjenestens samlede data-, system- og driftssikkerhed er betryggede
- at ledelsen er opmærksom på, at der på sigt vil blive stillet krav om NSIS-anmeldelse, og at det medfører, at ID-tjeneste skal være NSIS-anmeldt for ikke at blive afkoblet Unilogin Broker
- at medsendte dokumentation er retvisende
- at ledelsen er opmærksom på, at man som ansvarlig myndighed er ansvarlig for fejl og svigt over for anvenderne af ID-tjenesten
- forpligtelsen til af egen drift straks at meddele Styrelsen for It og Læring, hvis sikringsniveauet ønskes ændret, eller ved fejl eller svigt i ID-tjenesten
- at være til rådighed for en opfølgende dialog ved fejl eller svigt
- at informere brugerne om ændringer i sikringsniveau eller fejl eller svigt samt at træffe relevante modforanstaltninger som f.eks. spærring af ID-tjenesten i relevant omfang mv.
- at Styrelsen for It og Læring i tilfælde af en sikkerhedshændelse kan afkoble ID-tjenesten fra Unilogin Broker, hvis Styrelsen for It og Læring vurderer, at dette er en nødvendig modforanstaltning
- at Styrelsen for It og Læring kan sætte ID-tjenestens sikringsniveau til et lavere sikringsniveau, hvis Styrelsen for It og Læring vurderer, at dette er mere retvisende

Anmeldelse af lokal ID-tjeneste til Unilogin Broker

Ansvarlig for den lokale ID-tjeneste

Institutions-nr:_____