Møte **Arkitektmøte eksternt fagråd Smittestopp (ny)**

Dato, sted **101120, Skypemøte**

Til stede

- Roger Schäffer
- Pål Jakob Solerød
- Barbro Kvaal
- Sindre Møgster Braaten
- Christine Lunde
- Terje Granum
- Terje Sandstrøm
- Tor Gaute Indstøy
- Trond Arve Wasskog
- Johannes Brodwall
- Harald Wesenberg
- Lise Lyngsnes Randeberg
- Henrik Vincent Vassal
- Christian Thon
- Hege Torrissen
- Patrick Romstad
- Duy Nguyen
- Dan Bakmand-Mikalski
- Morten Lerudjordet
- Sindre Solem
- Martin Røpcke
- Pavel Shramau
- Siri Oldervik
- Tor-Martin Holen

Agenda:

- Gjennomgang utkast Azure-infrastruktur m/diskusjon i etterkant
- Q&A hvor deltakere kan komme med spørsmål rundt hva de lurer på og forslag til hva vi skal dekke på de neste møtene

Gjennomgang utkast Azure-infrastruktur m/diskusjon i etterkant

https://github.com/folkehelseinstituttet/Fhi.Smittestopp.Documentation/blob/main/HLD/D

Q&A hvor deltakere kan komme med spørsmål rundt hva de lurer på og forslag til hva vi skal dekke på de neste møtene

Spørsmål fra Harald Wesenberg:

Spørsmål 1) Jeg antar at dette bygger på eksisterende beste praksis i enten FHI eller NHN. Er det mulig å si noe om dette, også offentlig etterhvert? Begrunnelse: Velprøvde løsninger er alltid mer tillitsvekkende enn "dette har vi aldri gjort før"-initiativ, og hvis man kan vise til at dette er noe FHI og NHN har kompetanse på fra tidligere, så vil det øke tilliten til bruken av Azure.

Svar: Ja.

Spørsmål 2) Hvor mye av dette settes opp som kode (Infrastructure as code)? Begrunnelse: Jeg er veldig tilhenger av å bygge komponenter (spesielt tilstandsløse/stateless komponenter) fra sikker tilstand (hver time) for å beskytte bakenforliggende komponenter som er mer sårbare (databaser etc). Dette krever scriptede konfigurasjoner. Er det mulig å si noe om dette?

Svar: Forsøker på høy grad av IaC for verifiseringsløsningen, lite/ingen IaC for backend (med unntak av felleskomponenter).

Spørsmål 3) Har det vært gjennomført eller planlagt gjennomført pen-test mot tilsvarende arkitektur i regi av FHI tidligere?

Svar: Ja, det ble gjennomført både pentest av app (Transcendent Group) og API-er (Mnemonic) for Smittestopp v1. Det ble planlagt nye pentester for hver sprint (etter vurdering om endringer medførte ny risiko), men Smittestopp v1 ble stoppet før vi kom i gang med det. Pentest av ny løsning planlegges gjennomført før release.

Question Johannes Brodwall: In the OWASP ASVS standard, there are defined level 1, 2 and 3 verification levels. Have you considered an appropriate level of verification effort

Answer Tor Gaute Indstøy: Yes, we are following all OWASP ASVS levels as part of the risk assessment. In addition BSIMM and Normen v. 6.0

Question Johannes Brodwall: I understand the answer as that you are aiming to fulfill OWASP ASVS level *3* (plus BSIMM and Normen). Correct?

Answer Tor Gaute Indstøy: Yes, for Normen there will be selected relevant areas for this solution. e.g. access management

Question Harald Wesenberg: Kan vi få en beskrivelse av drift, overvåkning og også hvordan flytte data fra forskjellige miljøer? Prod data i test, hvordan sikre at dette foregår på riktig måte, beskrive dette?

Svar Sindre S: Kan ikke beskrive enda. Bortsett fra MSIS er det ikke så mye data.

Kommentar Johannes Brodwall: We also want to follow up on the pull request for the anonymization of the token. This would take care of must of the privacy uncertainties that we're thinking about now

Kommentar Lise Randeberg: Har spørsmål, legger disse i Slack-kanalen. Enighet om å fortsette spørsmål/svar der.

Neste arkitektmøte: 171120