Workshop 3: Sikkerhet

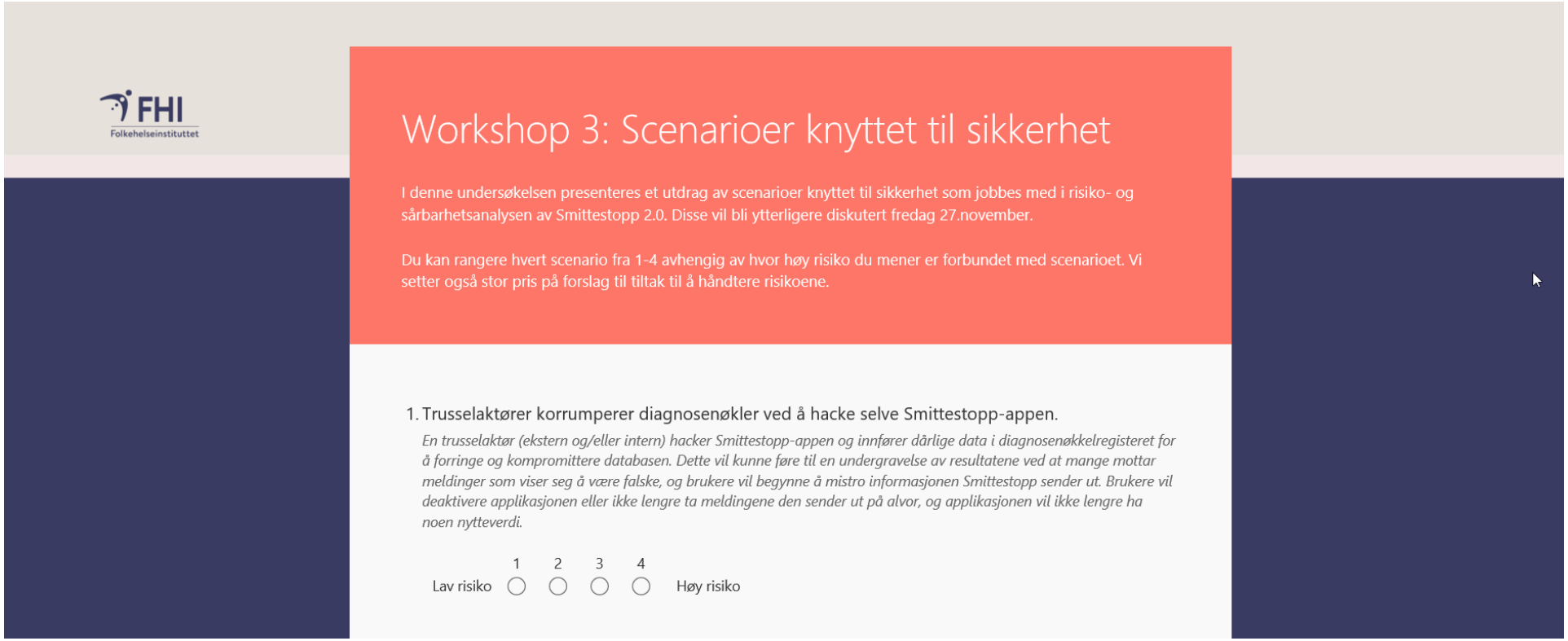
Gjennomgang av scenarioer

FHI 27.11.2020

Agenda

- Introduksjon
- Oppdatering siden sist v/ Pål Solerød
- Scenarier og tiltak
- Åpen diskusjon om sikkerhet

Introduksjon



Scenarier og tiltak

Scenario 1

Trusselaktører korrumperer diagnosenøkler ved å hacke selve Smittestopp-appen

En trusselaktør (ekstern og/eller intern) hacker Smittestopp-appen og innfører dårlige data i diagnosenøkkelregisteret for å forringe og kompromittere databasen. Dette vil kunne føre til en undergravelse av resultatene ved at mange mottar meldinger som viser seg å være falske, og brukere vil begynne å mistro informasjonen Smittestopp sender ut. Brukere vil deaktivere applikasjonen eller ikke lengre ta meldingene den sender ut på alvor, og applikasjonen vil ikke lengre ha noen nytteverdi

Tiltak scenario 1

Trusselaktører korrumperer diagnosenøkler ved å hacke selve Smittestopp-appen

A. Autentisering av innbygger før diagnosedata lastes inn i appen. Dermed skal all data som sendes fra appen og til databasen være autentisert.
B. Innbygger signerer med nøkkel for å autentisere diagnosedata før det legges inn i appen og dermed sendes til backend.
C. Sørge for at nettverks- og WAF-sikkerhetstiltak er på plass for å hindre storskalaangrep.
D. Det er lagt inn begrensning slik at kun én app kan sende data til backend.
E. Mulighet til å ta ned hele Smittestopp-løsningen dersom man oppdager at appen er hacket.

Scenario 2

Trusselaktører korrumperer diagnosenøkler ved å hacke backendløsningen til Smittestopp-appen.

En trusselaktør (intern og/eller ekstern) innfører dårlige data i diagnosenøkkelregisteret direkte i backendløsningen for å forringe og kompromittere databasen. Dette fører til en undergravelse av resultatene ved at mange brukere mottar meldinger som viser seg å være falske. Brukerne begynner derfor å mistro informasjonen Smittestopp sender ut, og ender opp med å deaktivere applikasjonen eller ikke lengre ta meldingene den genererer på alvor. Statistikken applikasjonen genererer er falske, og Smittestopp har ikke lengre har samme nytteverdi.

Tiltak scenario 2

Trusselaktører korrumperer diagnosenøkler ved å hacke backendløsningen til Smittestopp-appen.

A. Integritetssjekk av enheter gjøres av applikasjonen i løpet av «onboardingen» av enheten. Det må sørges for at all trafikk til backenden til Smittestopp er beskyttet via dette.
B. Autentisering av innbygger før diagnosedata lastes inn i backendløsningen fra appen.
C. Signering av diagnosedata med nøkkel av innbygger før de legges inn.
D. Sørge for at nettverks- og WAF-sikkerhetstiltak er på plass for å hindre storskalaangrep.
E. Etablere kontinuerlig monitorering av backend.

Scenario 3

Utro tjener utnytter sin rolle og korrumperer data i backend eller selger sensitiv data til ukjente aktører.

Ansatt i NetCompany utnytter sin rolle og tilgang til backendløsningen til Smittestopp til å korrumpere data eller selge sensitiv data til ukjente aktører. Den ansatte gjør dette ved å overstyre tilgangskontrollen og godkjenne økt tilgang til seg selv slik at vedkommende får tilgang til deler av backend han/hun i utgangspunktet ikke hadde. Konsekvensen er at sensitiv data om den norske befolkningen er på avveie til høystbydende eller at smittesporingen er forgjeves fordi dataen i backend er ødelagt.

Tiltak scenario 3

Utro tjener utnytter sin rolle og korrumperer data i backend eller selger sensitiv data til ukjente aktører.

A. Sikre gode prosesser for tilgangsstyring og jevnlig gjennomgang av tilganger.
B. Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges.
C. Logge hendelser og innlogginger for å detektere mulig abnormal oppførsel.
D. Mulighet til å ta ned hele Smittestopp-løsningen dersom man oppdager at appen er hacket.

Scenario 4

Dataoverføring gjøres gjennom usikrede metoder, som åpner tilgang til data idet den sendes mellom brukeren og FHI, eksempelvis symptomer.

Dataoverføringen fra Smittestopp til FHI gjøres gjennom utilstrekkelig sikrede metoder som gjør at trusselaktører får tak i informasjonen. Hver gang applikasjonen brukes sendes data fra applikasjonen til FHI og denne dataen omfatter eksempelvis symptomer som er personlig informasjon som dermed risikeres å kompromitteres. Konsekvensen av dette er data på avveie eller upålitelig data fra Smittestopp dersom trusselaktøren gjør endringer i symptomdata på vei til FHI.

Tiltak scenario 4

Dataoverføring gjøres gjennom usikrede metoder, som åpner tilgang til data idet den sendes mellom brukeren og FHI, eksempelvis symptomer.

A. Kryptere all data i ro og i transitt mellom innbyggerne og FHI.
B. Sørge for hashing av data slik at det ikke er mulig for trusselaktører å koble hvilke enkeltindivider som har blitt smittet og hvilke symptomer de har hatt.
C. Etablere en responsplan med mitigerende tiltak for hendelser som blant annet datalekkasje, for å hindre økning i negative ringvirkninger etter denne type hendelser.

Takk for din deltakelse.