Workshop 4: Eksterne Aktører

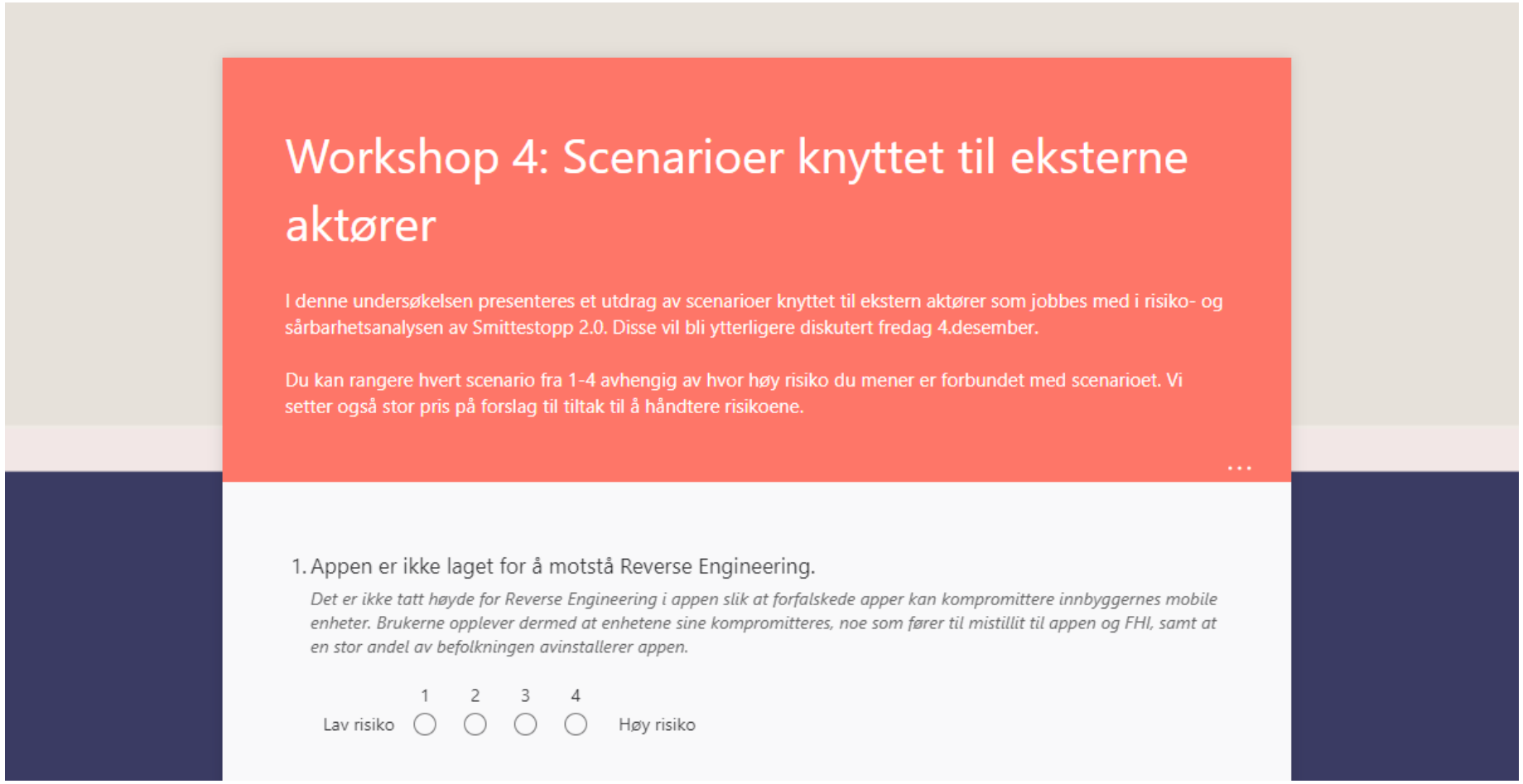
Gjennomgang av scenarioer

FHI 04.12.2020

Agenda

- Introduksjon
- Dashboard
- Scenarier og tiltak
- Åpen diskusjon

Introduksjon



Workshop 4: Scenarioer knyttet til eksterne aktører

I denne undersøkelsen presenteres et utdrag av scenarioer knyttet til ekstern aktører som jobbes med i risiko- og sårbarhetsanalysen av Smittestopp 2.0. Disse vil bli ytterligere diskutert fredag 4.desember.

Du kan rangere hvert scenario fra 1-4 avhengig av hvor høy risiko du mener er forbundet med scenarioet. Vi setter også stor pris på forslag til tiltak til å håndtere risikoene.

...

1. Appen er ikke laget for å motstå Reverse Engineering.

Det er ikke tatt høyde for Reverse Engineering i appen slik at forfalskede apper kan kompromittere innbyggernes mobile enheter. Brukerne opplever dermed at enhetene sine kompromitteres, noe som fører til mistillit til appen og FHI, samt at en stor andel av befolkningen avinstallerer appen.

	1	2	3	4	
Lav risiko	◯	◯	◯	◯	Høy risiko

FHI
Folkehelseinstituttet

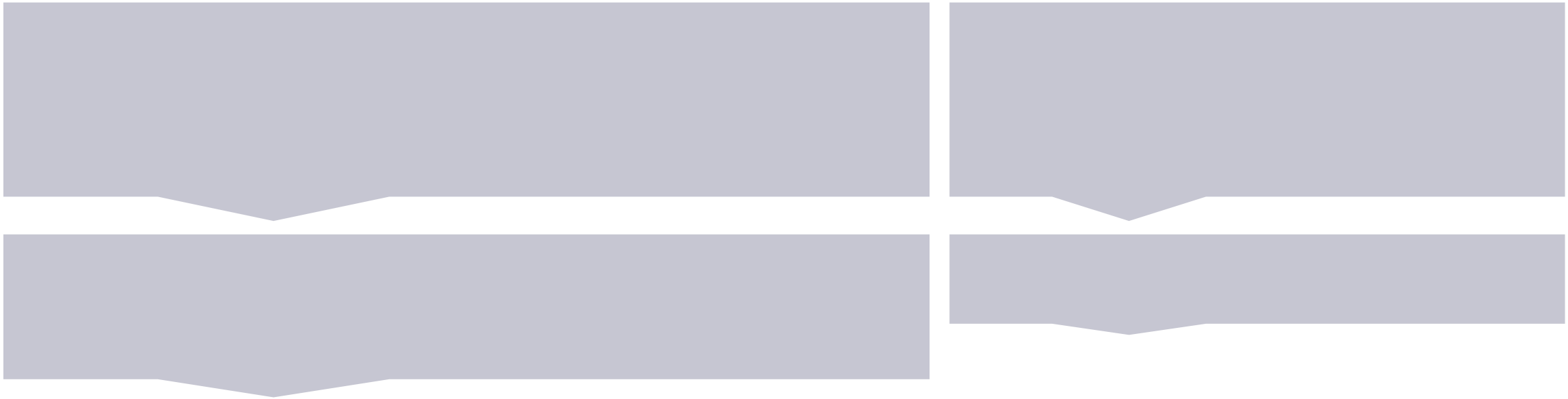
Dashboard

Scenarier og tiltak

Scenario 1

Appen er ikke laget for å motstå Reverse Engineering.

Det er ikke tatt høyde for Reverse Engineering i appen slik at forfalskede apper kan kompromittere innbyggernes mobile enheter. Brukerne opplever dermed at enhetene sine kompromitteres, noe som fører til mistillit til appen og FHI, samt at en stor andel av befolkningen avinstallerer appen.



Tiltak scenario 1

Appen er ikke laget for å motstå Reverse Engineering.

A. Vurdere sårbarheter i henhold til anbefalinger under Resilience against Reverse Engineering – Android fra standarden OWASP Mobile Application Security.

Scenario 2

Angrep mot MSIS for å korrumpere smittedata.

En avansert statlig aktør ønsker å påvirke Norges økonomi. Gjennom langsiktige påvirkningsoperasjoner på flere nivå ønsker en statlig aktør å hindre økonomisk vekst i Norge for å svekke Norges posisjon i verdenssamfunnet og samtidig skape interne uroligheter. En av disse påvirkningsoperasjonen har som mål å angripe MSIS for å korrumpere data slik at smittetallet i Norge blir kritisk høyt og tvinger fram full lockdown. Norske myndigheter har siden første lockdown ikke vist motivasjon til å føre landet inn i en ny lockdown periode. Dette grunnet de store sosioøkonomiske utfordringene det skapte. Norge håndterer de utbruddene som oppstår på en god måte og smittetrykket er stabilt lavt. Aktøren får tak i den private nøkkelen til grensesnittet og igangsetter målrettede angrep mot det eksponerte MSIS API-grensesnittet ved å benytte metoder for kodeinjisering.

Dette resulterer i at aktøren klarer å hente ut data fra grensesnittet igjennom returmeldingen til grensesnittet. Etter at aktøren har tilegnet seg tilgang sørger den for at smittetrykket gradvis øker slik at det ikke fattes mistanke til utviklingen. Tiden går og norske myndigheter foreslår stadig kraftigere og mer inngripende tiltak, men nekter å sette landet i lockdown. Ved å øke smittetrykket eksponentielt etter lang tid med moderat oppgang, tvinges myndighetene til å gjeninnføre lockdown i en tidsbegrenset periode. Aktøren sørger for at smittetallet synker, men at det til enhver tid holder seg rett over og under nivået norske myndigheter setter som grense for å oppheve lockdown. Dette fører til at Norge over en lang periode stenger ned landet og de sosioøkonomiske konsekvensene er fatale for norsk økonomi. Norge opplever en kraftig resesjon over lengre tid.

Tiltak scenario 2

Angrep mot MSIS for å korrumpere smittedata.

A. Sikker håndtering av nøkler til grensesnittet gjennom beste praksis på området, eksempelvis ISFs Crypto Key Management. Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges.

B. Herding av integrasjonsgrensesnitt (MSIS API).

C. Gjennomføre penetrasjonstester av eksponerte grensesnitt for å kartlegge sårbarheter og mulige angrepsmønstre fra trusselaktører.

Scenario 3

Lav kodekvalitet på grunn av mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse

Mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse fører til lav kodekvalitet. Dette fører til at kvaliteten på Smittestopp blir dårligere. Brukere blir misfornøyde og Smittestopp blir mindre virkningsfull i forhold til sitt formål. Lav kodekvalitet gjør det også vanskeligere tilføre nye oppdateringer i Smittestopp.

Tiltak scenario 3

Lav kodekvalitet på grunn av mangelfull kontinuerlig forbedring av sikker utviklingsmetodikk, styring og kompetanse

A. Fokus på kontinuerlig utvikling og implementering av kodemetodikk for å styrke applikasjonen.

B. Dra nytte av samarbeid med andre lands oppdateringer i tilsvarende applikasjoner, eksempelvis Danmark.

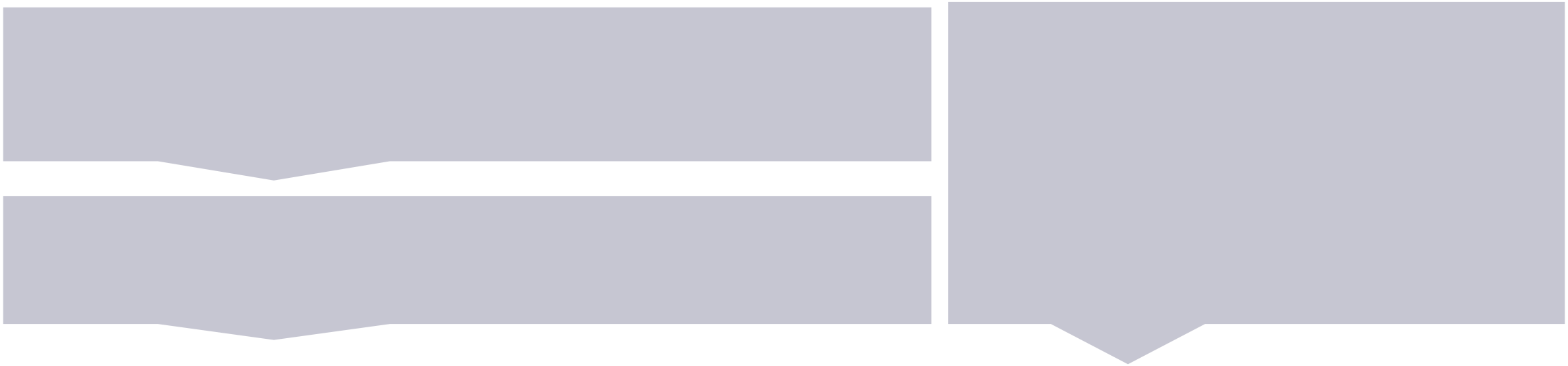
C. Dra nytte av Google og Apples kompetanse og informasjon på området.

D. Ivareta personvern og sikker utvikling.

Scenario 4

Mangelfull forståelse av sikker koding fører til ustabile applikasjoner og datalekkasje.

Mangelfull institusjonell forståelse av sikker koding benyttet til overgripende sikkerhetsaktiviteter integrert inn i utviklingsprosessene. Eksempler på dette er angrepsmodeller, sikker design og standardiseringsarbeid. Dette fører til ustabile applikasjoner eller datalekkasje, som gjør at FHI opplever en mediestorm uten sidestykke. Resultatet er at FHI blir tvunget til å gjennomføre en ekstern revisjon/evaluering av hele utviklingsløpet. Evalueringen konkluderer med at det ikke er gjennomført en vurdering av NetCompany og deres metodikk for sikker utvikling, samt at flere feil er begått i utviklingsløpet. Dette blir både kostbart og tidkrevende, samtidig som det svekker omdømme og tilliten den norske befolkning har til både FHI og Smittestopp. Mediene går ut med en anbefaling til befolkningen om å slette applikasjonen og FHI/norske myndigheter har nå spolert alle muligheter for å benytte digitale verktøy i forbindelse med smittesporing og pandemihåndtering.



Tiltak scenario 4

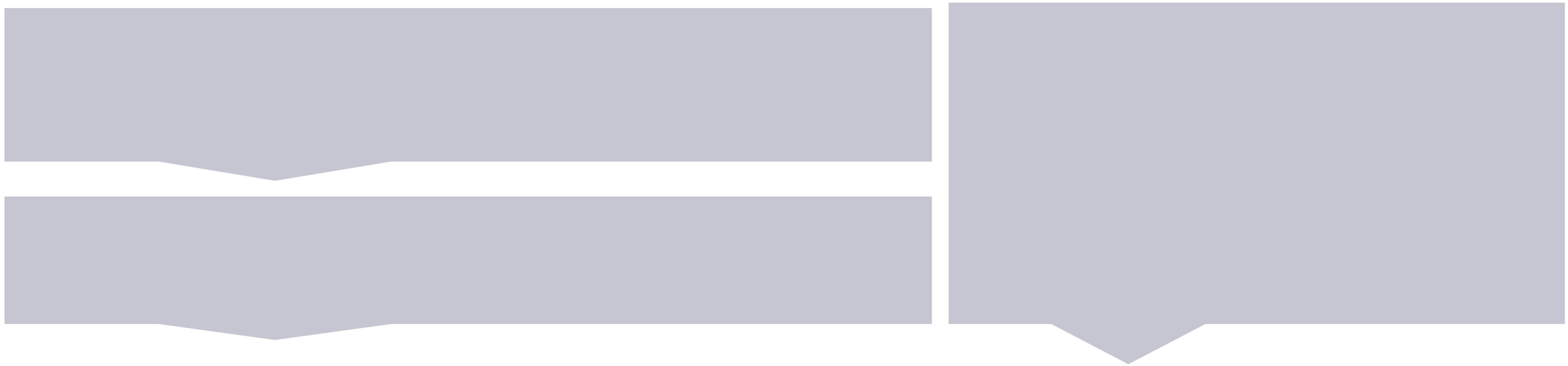
Mangelfull forståelse av sikker koding fører til ustabile applikasjoner og datalekkasje.

A. Gjennomføre trening og øvelser på viktige sikkerhetsområder som omfatter sikker koding.
B. Bruke sikkerhetseksperter til å sørge for at sikkerhetsaktiviteter blir integrert i utviklingsprosessen.
C. Kontinuerlig vurdere sikkerhetsarbeidet og diskutere mulige angrepsmodeller underveis i utviklingsarbeidet.
D. Kontinuerlig monitorere og vurdere utviklingsprosessen for å detektere mangler knyttet til sikker koding.

Scenario 5

Sårbarheter i kildekode på grunn av manglende analysemetoder for avdekking.

Risiko for mangel på analysemetoder for å avdekke sårbarheter i kildekode; herunder arkitekturanalyse, koderevisjon og sikkerhetstesting. Dette fører til at sårbarheter eksisterer uten at utviklingsteamet og FHI er klar over det, og kan utnyttes av trusselaktører. Sårbarheter kan gi hackere tilgang på personlig data og sette FHI i en svært uheldig situasjon der data er korrumpert, fjernet eller på avveie.



Tiltak scenario 5

Sårbarheter i kildekode på grunn av manglende analysemetoder for avdekking.

A. Implementere standardiserte prosesser for arkitekturanalyse, koderevisjon og sikkerhetstesting.

B. Utnevne ansvarlige i utviklingsteamet til å overse at sårbarheter i kildekode avdekkes.

C. Gjennomføre rutinemessige automatiske og manuelle koderevisjoner og sikkerhetsetestinger gjennom hele utviklingsløpet.

D. Benytte åpne kildekode og oppfordre innbyggere til å finne feil.

E. Utarbeide en responsplan som dekker prosesser rundt gjennomføring av tiltak og kommunikasjon utad dersom sårbarheter i kildekoden avdekkes.

Scenario 6

En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Danmark som lagrer backendløsningen og/eller datasenteret i Norge som lagrer verifiseringsløsningen.

Rekognoseringen gjennomføres over lengre tid og i flere steg for å unngå oppmerksomhet. Aktøren kjører forbi datasenteret på ulike tider av døgnet og bruker for å kartlegge bemanning og få en god oversikt over området og rutiner. Aktøren tar samtidig bilde av ansatte som har tilgang til datasentrene og gjennom å kjøre reverserte bildesøk på google/eller ved å overvåke den enkelte finner de fram til identiteten deres. Aktøren benytter sosial manipulering til å komme seg på innsiden av datasenteret. Aktøren ønsker først å teste beredskapen og responstiden til politi, nødetater og vektertjeneste og gjennomfører et enkelt innbrudd mot en av inngangene til datasenteret. Aktøren avbryter innbruddet etter at alarmen er satt av og trekker seg tilbake i posisjon til å observere responstid.

Etter å ha dokumentert responstid legger aktøren en omfattende plan der det skisseres flere mulige framgangsmåter. Aktøren kan nå fritt ta seg inn eller true ansatte på bakgrunn av informasjon man har om vedkommende til å igangsette flere mulige utfall;

1. Aktør får tilgang direkte inn i NHN eller NetCompanys systemer og laster ned en større mengde sensitiv data og forlater stedet uberørt. Potensielt tap av enorme mengder data med diagnosenøkler eller annen persondata.

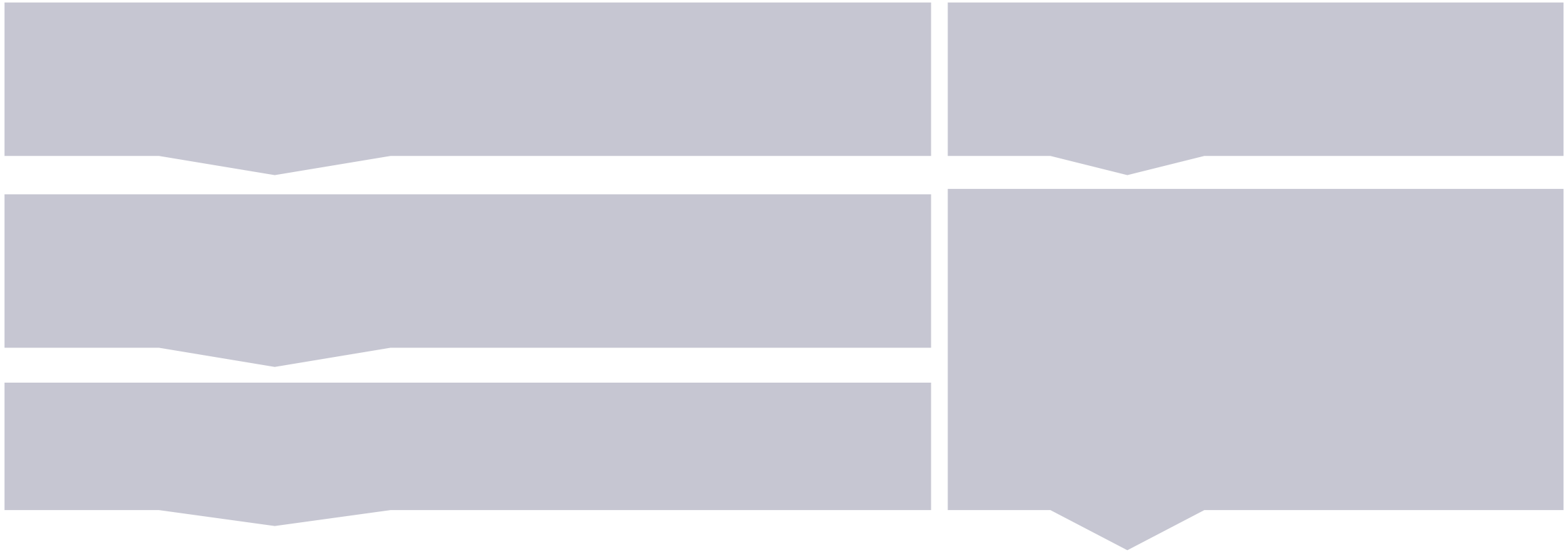
2. Aktøren plasserer ondsinnet skadevare i backendløsningen eller verifseringsløsningen og forlater stedet uberørt. Omdømme, tap av data og driftskonsekvenser er konsekvensen for Smittestopp.

4. Aktøren saboterer serverfarmen ved hjelp av brann, eksplosjon eller liknende. Omdømme, tap av data og driftskonsekvenser for Smittestopp og FHI.

5. Aktøren gjennomfører ingen ondsinnede handlinger, men legger igjen bevis på inntrengning, legger ut hele operasjonen på nett og forårsaker enorm skade i form av at befolkningen mister tillit til FHI og Smittestopp sin evne til å håndtere sensitive helse- og personopplysninger.

Scenario 6

En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Danmark som lagrer backendløsningen og/eller datasenteret i Norge som lagrer verifiseringsløsningen.



Tiltak scenario 6

En ukjent trusselaktør gjennomfører en ondsinnet villet handling mot datasenteret i Danmark som lagrer backendløsningen og/eller datasenteret i Norge som lagrer verifiseringsløsningen.

A. Gjennomføre risikovurdering av datasenteret som lagrer verifiseringsløsningen og datasenteret.

B. Utarbeidelse, kontinuerlig gjennomføre scenariotrening og forbedring av respons- og beredskapsplaner for å sikre effektiv håndtering av hendelser på datasenteret.

Takk for din deltakelse.