Prosjekthåndbok

Trussel deteksjon i Microsoft Azure Cloud

Bachelorprosjekt Vår 2019

Naren Yogarajah

Innholdsfortegnelse

1.Arbeidskontrakt 3
2. Framdriftsplan 4
3. Møteinnkallinger med referat 5
3.1 10 januar 19 5
3.1.1 Møteinnkalling 5
3.1.2 Møtereferat 6
3.2 24 januar 19 8
3.2.1 Møteinnkalling 8
3.2.2 Møtereferat 9
3.3 7 februar 19 10
3.3.1 Møteinnkalling 10
3.3.2 Møtereferat 11
3.4 20 februar 19 12
3.4.1 Møteinnkalling 12
3.4.2 Møtereferat 13
3.5 14 mars 19 14
3.5.1 Møteinnkalling 14
3.5.2 Møtereferat 15
3.6 28 mars 19 16
3.6.1 Møteinnkalling 16
3.6.2 Møtereferat 16
3.7 Møte 26 april 19 17
3.7.1 Møteinnkalling 17
3.7.2 Møtereferat 18
3.8 Møte 9 mai 19 19
3.8.1 Møteinnkalling 19
3.8.2 Møtereferat 20
4. Timeliste med statusrapporter 21

1.Arbeidskontrakt

Avtale mellom partene

Bedrift/virksomhet: DNB OSLO

Student(ene): NAREN YOGARAJAH

og

NTNU, IDI AIT

Studentprosjekt SIKKERHET I AZURE

Gjennomføring
Studenten skal gjennomføre et studentprosjekt i samarbeid med bedriften/virksomheten. IDI AIT veileder arbeidet faglig. Det er utarbeidet retningslinjer for gjennomføring av studentprosjekt som beskriver oppgavefordeling og hvordan studentprosjekter gjennomføres. Retningslinjene tar også opp ansvarsfraskrivelse, opphavsrettigheter og tilgjengelighet med muligheter for individuelle avtaler.

Ansvarsfraskrivelse
Instituttet er ikke ansvarlig for eventuelle ødeleggelser som studenten måtte påføre oppgavestillers utstyr direkte eller som følge av programvare studenten lager og/eller bruker, eller som studenten på annen måte medvirker til.

Opphavsrett og tilgjengelighet
Når ikke annet er avtalt, eier studenter selv den IPR (immaterielle rettigheter) de skaper som en del av studier/studieopphold ved IDI AIT. Alle resultater er åpent tilgjengelig. Opphavsretten reguleres av Åndsverksloven. Avtaler som inngås mellom IDI AIT og studenter skal som minimum sikre instituttet rett til å bruke generert IPR til utdannings- og forskningsformål. IDI AIT skal også motta en vurderingskopi av arbeidet inkludert eventuell kildekode.

Marker med kryss det som gjelder denne oppgaven:

☒ Normalsituasjonen: Studentene har selv alle rettigheter knyttet til resultatet fra bacheloroppgaven, med de unntak som er beskrevet over.

☒ Oppdragsgiveren har rettighetene og kan utnytte produktet kommersielt og videreutvikle produktet/metoden. Instituttet vil ikke utnytte produktet kommersielt, men vil kunne arbeide videre med den grunnlagskompetansen som er vunnet gjennom prosjektet, som beskrevet over.

☒ Resultatene fra arbeidet legges ut som OpenSource iht lisens _____ (Se http://creativecommons.no/lisenser).

☒ Bacheloroppgaven (det skriftlige arbeidet) skal være undergitt utsatt offentliggjøring i 3 (maks 3) år.

Oppdragsgiver er selv ansvarlig for å avtale håndtering av eventuelle konfidensielle opplysninger med veileder/sensor og studenten(e).

Denne avtalen er underskrevet i 3 – tre - eksemplarer hvor partene skal ha hver sin.

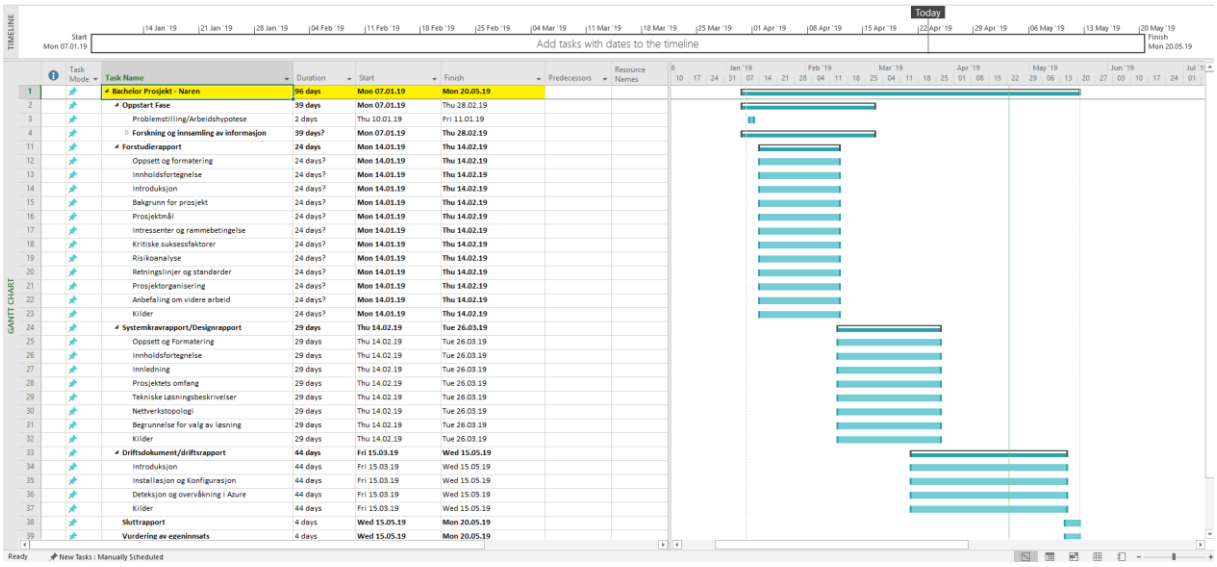
14.01.19, OSLO
(dato, sted)

Bedrift/virksomhet

Sturla Meisingseth
Veileder ved IDI AIT

Y. Naren
Student(ene)

2. Framdriftsplan



Ovenfor er framdriftsplanen for bachelorprosjektet vedlagt. Dette er en framdriftsplan som er utviklet i Microsoft Project. Jeg har fulgt denne planen fra 7 januar 2019 til og med 20 mai 2019 som er siste frist for innlevering.

3. Møteinnkallinger med referat

3.1 10 januar 19

3.1.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure

Tidspunkt/Sted: Torsdag 10.01.2019 kl. 11.00 - 11.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Agenda:

- Problemstilling forslag/Diskutere arbeidshypotese
- Invitasjon til SharePoint side/ Spørre om alle har fått tilgang til denne siden
- Avtale møter for resten av året - ønsker en fast dag hver uke fremover med veiledning

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte. I og med at dette er årets første møte trenger vi ikke dette.

Sak 3: Godkjenning av agenda.

Sak 4: Eventuelt

Mvh
Naren

3.1.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 1

10.01.2019

Tidspunkt/Sted: Torsdag 10.01.2019 kl. 11.00 - 11.30, Elektronisk nettmøte

Til stede:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Naren Yogarajah

Sak 1:

Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2:

Godkjenning av referat fra siste møte

Vi brukte ikke referat fra siste møte siden dette var årets første veiledningsmøte.

Sak 3:

Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4:

Arbeidshypotesen som ble gitt ut til forslag for bachelorprosjektet ble godkjent.

Arbeidshypotesen ligger vedlagt under:

Hvilke muligheter finnes det for trussel deteksjon i Azure ved bruk av tjenester som Azure Active Directory (Azure AD), Azure Log Analytics og Azure Security Center?

Det ble også gitt forslag om at dersom det blir tid til overs kan man også fokusere på muligheter som ligger utenfor disse tjenestene.

Sak 5:

Alle har fått tilgang til SharePoint siden.

Sak 6:

Ordning av fast dag i uken med veiledninger er greit, og det kommer til å bli planlagt fremover fra neste møte som er 24.01.19 kl.11.00 - 11.30.

Sak 4:

DNB har mulighet til å gi ut en Azure Standalone konto for bruk til bachelorprosjektet.

Sak 5:

Etter samtale med DNB, ble det gitt beskjed om at det mest sannsynlig ikke trengs en taushetserklæring som må skrives under i bachelorprosjektet.

Sak 6:

DNB skal introdusere en kollega som også kommer til å være med i veiledninger fremover.

Sak 7:

Ønske om å jobbe hos DNB med bachelorprosjektet var mulig i noen perioder men hovedsakelig er det lite plass hos DNB.

Referent:

Naren Yogarajah 10.01.2019

3.2 24 januar 19

3.2.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure

Tidspunkt/Sted: Torsdag 24.01.2019 kl. 11.00 - 11.30, Elektronisk nettmøte (Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Agenda:

- Avtale signering
- Tilbakemelding – forstudierapport (vedlegger forstudierapporten 23.01.19 på SharePoint)
- Oppbygging av oppgaven – gjennomgang av tenkt struktur
- Gjennomgang av prosjektplan og timeliste

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Eventuelt

Mvh
Naren

3.2.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 2

24.01.2019

Tidspunkt/Sted: Torsdag 24.01.2019 kl. 11.00 - 11.30, Elektronisk nettmøte (Skype)

Til stede:

Lars Arne Sand
Johan Fredrik Juell

Stein Meisingseth

Naren Yogarajah

Sak 1:

Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2:

Godkjenning av referat fra siste møte

Referat fra siste møte ble godkjent.

Sak 3:

Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4:
Ønsket om å få en standard tier konto Subscription i Azure ble godkjent. Dersom man mangler noen funksjoner kan det sendes en epost til DNB med en beskrivelse av de manglende komponentene som igjen kan legges inn på Azure kontoen. Det blir gitt ut en "Pay as you go" Subscription i Azure. Azure brukerkonto detaljer blir gitt ut 25.01.2019 til studenten.

Sak 5:

Forstudierapporten krever noen endringer:
Risikoanalyse må omgjøres. Risikoelementer som sykdom og naturkatastrofer må endre plassering på risiko grafen. Oppgaven skal struktureres slik som at man starter med å beskrive generelle trusler og sikkerhet i Azure og droppe den generelle beskrivelsen av Cloud Computing. Effektmålet som er satt angående forbedre sikkerheten i Azure kan bli satt som et indirekte mål i forstudierapporten. "Dagens systemer og finansiering av videreutvikling og forvaltning" delen kan droppes å tas med i forstudierapporten. Å skrive at Azure skal ha en oppetid på 100 % blir feil å si og å si at Azure skal ha en oppetid på 99 % er anbefalt av veileder.

3.3 7 februar 19

3.3.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure veiledning #3

Tidspunkt/Sted: Torsdag 07.02.2019 kl.12.00 – 12.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Johan Fredrik Juell

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Lovlige metoder som kan tas i bruk for sikkerhetstesting i Azure, noen tips til verktøy.

Sak 5: Tilbakemeldinger - forstudierapport (Vedlegges 06.02.19 på SharePoint)

Sak 6: Timeliste revisjon (Vedlegges 06.02.19 på SharePoint)

Sak 7: Prosjektplan revisjon (Vedlegges 06.02.19 på SharePoint)

Sak 8: Eventuelt.

3.3.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 3 - 07.02.2019

Tidspunkt/Sted: Torsdag 07.02.2019 kl. 12.00-12.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken
Stein Meisingseth
Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Lovlige metoder som kan tas i bruk for sikkerhetstesting i Azure, noen tips til verktøy.
Vi ble enig om at hovedfokuset i oppgaven skulle være å fokusere på metoder for å oppdage angrep som foregår i Azure og ulike tiltak som kan settes i gang for å bli kvitt disse truslene. DNB jobber opp mot noen typiske Use case ut i fra trusselsituasjoner og de kunne deles ut om rundt 3 uker for studenten. Ut i fra dette kan studenten jobbe mot et eller flere Use case og hvordan man håndterer dem i Azure. Oppsummert så blir det viktig å jobbe ut ifra disse punktene: varsler, deteksjon, hvordan angrep foregår og hvordan man finner det i Azure.

Sak 5: Tilbakemeldinger - forstudierapport.
Noen små endringer som må gjøres på forstudierapporten, ellers godkjent.

Sak 6: Timeliste revisjon.
Timeliste godkjent.

Sak 7: Prosjektplan revisjon.

Prosjektplan godkjent.

Referent: 07.02.2019
Naren Yogarajah

3.4 20 februar 19

3.4.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure veiledning #4

Tidspunkt/Sted: Onsdag 20.02.2019 kl.13.00 – 13.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Johan Fredrik Juell

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Use Case fra DNB

Sak 5: Avtale tidspunkt for presentasjon av bachelorprosjekt hos DNB

Sak 6: Timeliste revisjon (Vedlegges 20.02.19 på SharePoint)

Sak 7: Prosjektplan revisjon (Vedlegges 20.02.19 på SharePoint)

Sak 8: Eventuelt.

3.4.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 4 - 20.02.2019

Tidspunkt/Sted: Onsdag 20.02.2019 kl. 13.00-13.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken
Lars Arne Sand
Stein Meisingseth
Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Use Case fra DNB
DNB skal utarbeide noen forslag til Use Case studenten kan jobbe med fremover. DNB har også gitt forslag for å ta i bruk websiden: https://attack.mitre.org/matrices/enterprise/ i tillegg til Use Case som blir delt ut som forslag. Fra denne websiden finner man en liste over kjente teknikker angripere pleier å ta i bruk. Det ble avtalt at studenten kan starte med å sette seg inn i 3-4 Use Case og disse casene vil kreve en del god tid. I den sammenheng blir også neste veiledningsmøte flyttet til 14 mars 2019. DNB ønsker et møte med studenten og de kontakter studenten nærmere for å avtale tidspunkt for møte.

Sak 5: Avtale tidspunkt for presentasjon av bachelorprosjekt hos DNB
Tidspunkt for presentasjon av bachelorprosjekt hos DNB holdes tirsdag 21.05.2019, kl.12.00 - 13.00.

Sak 6: Timeliste revisjon.

Timeliste godkjent.

Sak 7: Prosjektplan revisjon.

Prosjektplan godkjent.

3.5 14 mars 19

3.5.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure veiledning #5

Tidspunkt/Sted: Torsdag 14.03.2019 kl.11.00 – 11.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Systemkrav Rapport - tilbakemelding, forslag til endringer og tips til innhold som kan legges til.

Sak 5: Eventuelt.

3.5.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 5 - 14.03.2019

Tidspunkt/Sted: Torsdag 14.03.2019 kl. 11.00-11.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken
Lars Arne Sand
Stein Meisingseth
Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Systemkrav Rapport - tilbakemelding, forslag til endringer og tips til innhold som kan legges til.
Det ble gitt en del tilbakemeldinger på systemkravrapporten. Å ha en tydeligere struktur på rapporten blir viktig å fokusere på fremover. Under punkt 3.4 trusler og sikkerhet i skyen ble det anbefalt å sette opp noen trussel scenarioer og en beskrivelse av disse. I tillegg bør fagspråket være på engelsk. Videre ble det anbefalt å få inn flere referanser og henvise direkte i rapporten er også en god ide.

Referent: 14.03.2019
Naren Yogarajah

3.6 28 mars 19

3.6.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure veiledning #6

Tidspunkt/Sted: Torsdag 28.03.2019 kl.12.00 – 12.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Systemkrav Rapport 2. utkast - tilbakemelding, forslag til endringer og tips til innhold som kan legges til.

Sak 5: Eventuelt.

3.6.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime nr 6 - 28.03.19

Tidspunkt/Sted: Torsdag 28.03.2019 kl. 12.00-12.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken
Lars Arne Sand
Stein Meisingseth
Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Systemkrav Rapport 2. utkast - tilbakemelding, forslag til endringer og tips til innhold som kan legges til.
Systemkrav Rapport 2. utkast er godkjent. Det ble anbefalt å starte videre på driftsdokument.
Neste veiledningsmøte er satt til 25 april fra kl. 11.00 - 11.30.

Referent: 28.03.2019
Naren Yogarajah

3.7 Møte 26 april 19

3.7.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure veiledning #7

Tidspunkt/Sted: Torsdag 26.04.2019 kl.11.00 – 11.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Driftsdokument - 1.utkast

Sak 5: Eventuelt.

Mvh
Naren Yogarajah

3.7.2 Møtereferat

Møtereferat Bacheloroppgave Veiledningstime - 26.04.19

Tidspunkt/Sted: Fredag 26.04.19 kl. 11.00-11.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Driftsdokument - 1.utkast

Stein er fornøyd med driftsdokumentet, noen små endringer som bør legges til. Det ble anbefalt om å gi en kort beskrivelse av de viktigste tjenestene før man starter på selve installasjonen i driftsdokumentet. Det er også anbefalt å ha en border på bildene i driftsdokumentet. DNB vil gi en tilbakemelding på driftsdokumentet på mail.

Siste veiledningsmøte er satt til 9 mai 2019 fra kl. 11.00 - 11.30. Veiledningsmøte som er satt opp 13 mai 2019 blir avlyst.

Mvh
Naren Yogarajah

3.8 Møte 10 mai 19

3.8.1 Møteinnkalling

Innkalling til møte: Bacheloroppgave – Sikkerhet i Azure – Siste møte før innlevering

Tidspunkt/Sted: Torsdag 10.05.19 kl.11.00 – 11.30, Elektronisk nettmøte(Skype)

Følgende personer innkalles:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Sak 1: Godkjenning av møteinnkalling.

Sak 2: Godkjenning av referat fra siste møte.

Sak 3: Godkjenning av agenda.

Sak 4: Driftsdokument - 2.utkast

Sak 5: Eventuelt.

Mvh
Naren Yogarajah

3.8.2 Møtereferat

Møtereferat Bacheloroppgave Siste Veiledningstime før innlevering – 10.05.19

Tidspunkt/Sted: Fredag 10.05.19 kl. 11.00-11.30, Elektronisk nettmøte (Skype)

Til stede:

Roger Schage Storløkken

Lars Arne Sand

Stein Meisingseth

Naren Yogarajah

Sak 1: Godkjenning av møteinnkalling.

Innkalling av møtet godkjent.

Sak 2: Godkjenning av referat fra siste møte.

Referat fra siste møte ble godkjent.

Sak 3: Godkjenning av saksliste.

Sakslisten ble godkjent.

Sak 4: Driftsdokument - 2.utkast

Det ble anbefalt å kutte ned til 4 versjonsendringer i driftsdokumentet. Videre ble det anbefalt at det bør skrives en litt mer konkret beskrivelse på hva man ser av resultater under deteksjon og overvåkningskapitlet i driftsdokumentet: f.eks hvordan ser man at man har blir angrepet og hva er den faktiske besvarelsen og henvisningen til et påpekt angrep fra Microsoft sin side, noe mer om geolokasjon og hvilke ip-adresser angrepene stammer fra kan også tas med i dokumentet.

Mvh

Naren Yogarajah

4. Timeliste med statusrapporter

Timeliste med statusrapporter blir vedlagt i et Excel dokument i ZIP filen som leveres.