Andri Fannar Arnarson

Universitetet I Sørøst Norge
Bø I Telemark
Vår 2020

Det svakeste leddet I alle Systemer Du!

Analyse av sikkerhet innenfor IT i Norge

Februar 4 , 2020

Innhold

1. Inledning

Jeg har valgt å skrive en teoretisk bacheloroppgave. De vil si at resultatet av denne oppgaven blir en vitenskapelig rapport som

reflekterer på problemstillingen som jeg har utformet. Hovedfokus blir på objektiv analyse av hendelser innenfor IT-Sikkerhet.

2. Bakgrunn

Jeg har alltid vært fokusert på sikkerhet når det kommer til teknologi. Først var det fascinasjon med teknologi og hvordan jeg kunne få ting til å gjøre hva jeg ville. Men å vokse opp i tidlig 2000 tallet gjør deg oppmerksom på ufattelige mengden av informasjon som er der ute og hvor lett tilgjengelig den er, noen ganger også for de som spesifikt ikke skal ha tilgang til den. Derfor har sikkerhet alltid vært i fokus hos meg. Når teknologi har utviklet seg har jeg fulgt med på hva det er som skjer i samfunnet rundt meg. Og det som skjer rundt meg er massevis av sikkerhetsbrudd. Store og små alle lekker dataen din ut til det vide internettet. Sykehus, aksjemeglere, banker og politikere alle har det til sammens at de kan bli hacket som alle andre.

Dette har blitt mer og mer prevalent i tekniske industrier i de siste årene. Det har dannet seg en katt og mus lek som spilles på alle tekniske arenaer. Dette er noe som jeg er ekstrem interessert i og håper at jeg kan komme med noen hensiktsmessige observasjoner eller nyttig informasjon innenfor IT-sikkerhet.

Det er derfor jeg har valgt min problemstilling innenfor IT-sikkerhet. Nemlig; Svakeste leddet i alle systemer. Du! Hvor stort er menneske problemet i IT-systemer. Hvordan kan vi lage systemer som unngår menneske feil eller forventer de og justerer seg med dem. Hvordan kan

kloke prosedyrer og standarder gjøre det mindre sannsynlig at menneske feil lager store problemer innenfor IT.

3. Problemstilling

Hvordan kan vi design systemer som unngår at menneske feil kan ha store konsekvenser. Systemer som unngår å la enkeltmennesker ta store valg innenfor sikkerhet av seg selv.

Jeg skal ta for meg noen få eksempler av sikkerhetsbrudd som jeg dokumenterer, analyser og drøfter løsninger som kunne potensielt stoppet eller minsket konsekvensene for den hendelsen.

Videre ser jeg på hvordan aktører i disse hendelsene har endret på prosedyrer, teknologi eller hvordan virksomhetene fungerer på grunn av denne hendelsen.

4. Forutsetninger og Rammer

I en sånn type oppgave blir rammeverket rundt oppgaven veldig viktig. Rammene innenfor denne oppgaven er at jeg skal holde men innenfor Norge. Beskrivelse, rapporter og dokumenter jeg samler inn kommer fra Norske aktører eller handler om et sikkerhetsbrudd som skjedde innenfor norge.

Jeg skal prøve å holde meg til mellomstore bedrifter som har blitt utsatt for sikkerhetsbrudd i de siste 3 - 5 årene. Dette sikkerhetsbruddet skal ha hatt konsekvenser for bedriften selv, økonomisk eller juridisk eller konsekvenser for brukerdata eller anden sensitiv data.

Oppgaven kommer til å ha et utvalg av 2 representative hendelser som jeg vurderer kvalitativt og i dybde.

4.1 Premisser

Premissene her er det som styrer innholdet i oppgaven. I dette tilfellet er det selvpålagte rammebetingelser som skal hjelpe med siktet til oppgaven. De betingelsene vil påvirke det endelige resultatet av prosjektet. Det er viktig at oppgaven holder seg innenfor disse rammene og holder siktet mot det som ble satt her i beskrivelsen.

Premissene mine er at det er et datasikkerhets problem som øker stadig mens samtidig er fokus på dette problemet ekstremt svak, spesielt hos mellomstore bedrifter i norge. Med å analysere brudd som har skjedd tidligere kan vi lage retningslinjer og standarder for sikkerhet ikke bare for bedriftene men dens kunder og arbeidstakere.

4.1.1 Krav

Kravene til hver hendelse er at den skjer innenfor norske grenser eller rammer Norske brukere. Det skal være målbar skade eller tap som konsekvens av hendelsen.

5. Mål

5.1 Effektmål

Effektmålet er en analyse av få utvalg av sikkerhetsbrudd som kan være representativ for hvordan sikkerhet er i IT sektoren i dag og hvordan den kan forbedres i fremtiden.

5.2 Resultatmål

Resultatmålet med denne oppgaven er en teoretisk rapport om sikkerhet i IT-sektoren og hvordan prosedyrer, standarder og systemer kan forbedres. En kvalitativ analyse av sikkerhet i dag.

6. Faser

Første fase av prosjektet er datainnsamling. Jeg skal samle inn så mye data om 2 sikkerhetsbrudd fra de siste 3 - 5 årene som kan være gode representanter for mellomstore bedrifter i Norge. Incident Reports er ikke alltid tilgjengelig men målet er å få tak i de for hver sak så den kan kartlegges grundig. Ikke bare hva skjedde men også hva ble gjort. Viktig er også å undersøke hver sak fra andre synspunkter enn den som bruddet skjedde hos, siden det er i dems interesse å skjule informasjon som sette skylden på de. Mitt mål er å få så objektiv syn på hver sak som mulig. Når jeg har funnet hendelser som håpentlig representerer et bredt spekter av IT-sektoren i Norge kan jeg gå videre til neste fase.

Analyse av valgte hendelser er en meget viktig del av prosessen. Hvis jeg skal kunne dokumentere og drøfte løsninger må det sørges for at så mye informasjon om saken som mulig har blitt funnet, dokumentert og kategorisert. Det som jeg skal bestemme til best mulig grad er

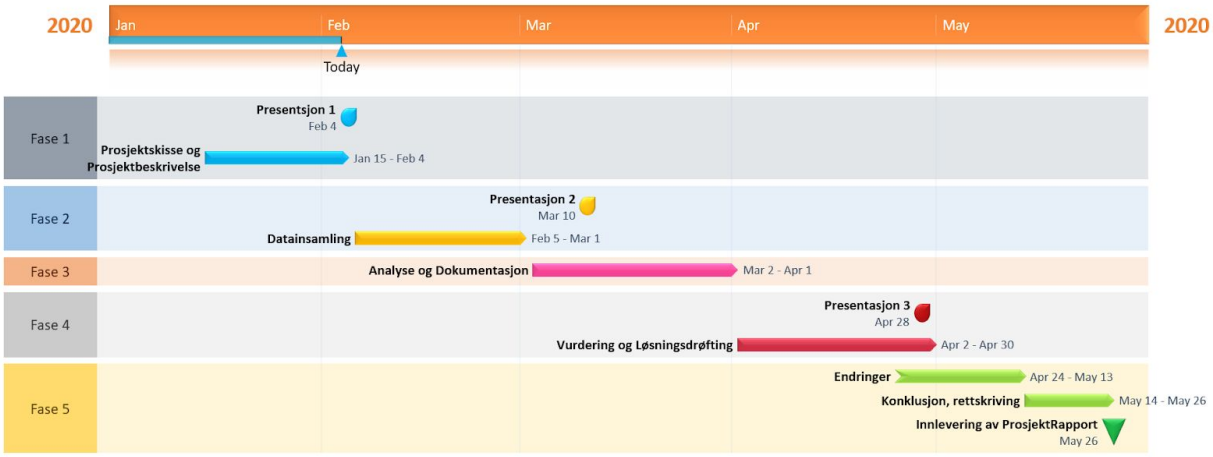
- Hva skjedde?
    - En generell beskrivelse av hva skjedde. Hvor, når og hvordan
- Hva er konsekvensene av denne hendelsen?

    - Hva er skadene. Monetære? Fysiske? Personlig data?
- Hvorfor skjedde dette?
    - Hvilken valg feil eller teknologi var det som førte til denne hendelsen.
- Stopper?
    - Hva kunne ha stoppet denne hendelsen fra å skje.
- Hva skjedde videre?
    - Hvordan justerer den som ble utsatt for hendelsen seg og hva er de synlige resultatene fra den justeringen.

Neste fase handler om idee drøfting på teknologiske og menneskelige forebyggende faktorer. Som leder inn i neste fase.

Løsningsdrøftingen skal være basert på allerede eksisterende standarder og teknologi. Her skal løsninger vurderes og foreslås. Dette skal skje i en fix-up rapport for hver hendelse for seg. Her blir hendelsene også sammenlignet hvis det er aktuelt.

7. Fremdriftsplan



8. Kritiske Faktorer

Datainnsamling og metodikk til datainnsamling er veldig kritiske i denne oppgaven. Siden resten av oppgaven er definert av hvilken data om hendelsene jeg klarer å samle inn blir det ekstremt viktig at jeg samler inn relevant data om relevante hendelser.

Det er også viktig at utvalgene er vurdert nøye så at de kan representere mellomstore bedrifter i Norge. Prosjektet skal representer sikkerhet innenfor mellomstore bedrifter i norge så godt som mulig.

9. Literatur

Det er viktig at jeg velger nøytrale kilder i denne oppgaven for å representere utvalget godt. All informasjon må stilles kritiske spørsmål til og data grundig undersøkt for å ikke komme med påstander eller vurderinger som er feil. Hvis ikke dataen er riktig blir all drøfting vurdering og potensieller løsninger poengsløs.

https://www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf

https://www.ssb.no/