Høgskulen på Vestlandet

Fakultet for teknologi, miljø- og samfunnsvitenskap

Institutt for datateknologi, elektroteknologi og realfag

IT sikkerhet og kultur, et samarbeid med Tysnes kommune

IT security and culture, a collaboration with Tysnes municipality

Visjonsdokument

Versjon. 1.3

REVISJONSHISTORIKK

Dato	Versjon	Beskrivelse	Forfatter
06.02.24	1.0	Førsteutkast: Innledende tanker, men flere mangler i kapitler, da dette må avklares sammen med veileder.	Martin N. Dyrstad
22.02.24	1.1	Oppdatert relevante kapitler og kommentarer på deler hvor malen ikke samsvarer med prosjektoppgaven	Martin N. Dyrstad og Siri K. Slyk
28.02.24	1.2	Oppdatert de fleste kapitlene og endret et par overskrifter for å bedre passe prosjektoppgaven.	Martin N. Dyrstad og Siri K. Slyk
01.03.24	1.3	Fullførte kap. 5 og 6	Siri K. Slyk
04.03.24	1.4	Visjonsdokumentet ferdigstilt, mindre endringer kommer senere.	Martin N. Dyrstad
08.03.24	2.0	Skrev litt om på innledningen, kap. 1	Martin N. Dyrstad

INNHOLDSFORTEGNELSE

1 INNLEDNING

Dette dokumentet har til hensikt å klargjøre formål, omfang og interessenter i prosjektet. Målet er å oppnå en gjensidig enighet mellom oppdragsgiver og prosjektgruppen om prosjektets visjon.

Prosjektet innebærer at prosjektgruppen utarbeider en rapport som vil stå igjen som et produkt. Rapporten har ingen direkte brukere, men vil inneholde forslag til forbedringer og tiltak mot eventuelle svakheter i IKT-sikkerheten som oppdages. Forslag til tiltak vil kunne iverksettes av Tysnes kommune.

Utover eventuelle tiltak har prosjektet ingen eksplisitte krav til innhold. Siden prosjektet ikke innebærer tradisjonell produktutvikling, forekommer det heller ingen eksplisitte ikke-funksjonelle krav. Det utføres imidlertid tester som tar for seg sikkerhetskulturen blant de ansatte i Tysnes kommune, og det følger implisitt at denne prosessen må ta høyde for spesifikke sikkerhetsaspekter som konfidensialitet, integritet og tilgjengelighet – ellers kjent som sikkerhetsegenskaper.

2 SAMMENDRAG PROBLEM OG RESULTAT

2.1 Problemsammendrag

Problem med	utilstrekkelig kunnskapsnivå om sikkerhetskulturen i Tysnes kommune. Dette inkluderer kunnskap om potensielle svakheter og resulterende implikasjoner.
Dette berører	kommunen som organisasjon, lederne, de ansatte, og ikke minst innbyggerne i kommunen.
Som resultat av dette	er sårbarhetsnivået ovenfor dataangrep potensielt høyere enn tidligere antatt og strekker seg dermed også eventuelt utover akseptabel risiko.
Et vellykket utfall vil	avdekke eventuelle forekomster/fravær av svakheter i sikkerhetskulturen blandt de ansatte.

2.2 Resultater og anbefalinger

For	Tysnes kommune
som	

	har behov for bedre innsikt i eget sikkerhetsnivå,
er resultatet navngitt	*IKT-sikkerhet og kultur, et samarbeid med Tysnes kommune* en leverbar rapport
som	viser resultatene av utførte tester, og som inneholder anbefalte tiltak for eventuelle svakheter som oppdages.
~~I motsetning til~~	: ikke anvendbar
~~Har vårt produkt~~	: ikke anvendbar

3 BESKRIVELSE AV INTERESSENTER OG BRUKERE

3.1 Oppsummering interessenter

(who is involved in the project)

Navn	Utdypende beskrivelse	Rolle under utvikling
Tysnes kommune	Anders Teigen er ekstern veileder og representant for kommunen (oppdragsgiver). Teigen er IT-leder i kommunen og ansvarlig for å implementere eventuelle tiltak og anbefalinger ut ifra prosjektets konklusjon.	Underveis i prosjektet stiller Teigen som kontaktperson og organisator for ressurser nødvendig for å gjennomføre prosjektet. Eksempler på dette kan være organisere møter med andre administratorer i Tysnes kommune, omvisning av lokaler, innkjøp av utstyr og ordne tilgang til interne servere.
Prosjektgruppen	Består av Martin N. Dyrstad, Stian Lødemel og Siri K. Slyk. Utfører prosjektet på oppdrag fra Tysnes kommune som del av bacheloroppgave ved Høgskulen på Vestlandet (HVL).	Ansvar for gjennomføring av prosjektet. Prosjektgruppen velger fritt hvordan best løse oppgaven ut ifra tid, kunnskap og andre tilgjengelige ressurser.
Høgskulen på Vestlandet	Tosin D. Oyetoyan representerer HVL som intern veileder for prosjektgruppen.	Gjennom prosjektets forløp stiller Oyetoyan med akademisk og faglig veiledning. Dette inkluderer ekspertise innen datasikkerhet, akademisk kompetanse, veiledning av beslutninger og konstruktive tilbakemeldinger.

Kommuneansatte	Prosjektet tar for seg sikkerhetskulturen blant de ansatte i Tysnes kommune. De ansatte er derfor involvert i prosjektet som testsubjekter.	De ansatte er uvitende ovenfor prosjektets forekomst og vil som en nødvendig del av prosjektet utsettes for tester som involverer sosial manipulasjon og observasjon. Testene kan sammenlignes med en uanmeldt brannøvelse og utformes på en slik måte til å unngå og fornærme eller på andre måter krenke de ansatte som individ.

3.2 Oppsummering brukere

(who will benefit from the result)

Navn	Utdypende beskrivelse	Rolle under utvikling	Representert av
	Forklar hvilken rolle denne brukeren spiller i dagens system. Eventuell annen viktig informasjon om denne brukeren.	*Hvilken rolle vil han/hun ha under utviklingen av systemet?*	*seg selv eller en annen bruker eller interessent?*
Innbyggere (bør denne raden være med?)	Innbyggerne er i ulik grad avhengig av kommunale tjenester og tilbud. IT-angrep kan true tilbudenes tilgjengelighet og integritet. Som brukere vil dårlig kommunal IT-sikkerhet også kunne føre til at sensitive personopplysninger kommer på avveie, og i verste fall utnyttes.	Ingen aktiv rolle.	Ikke representert.

Kommuneansatte	Kommunens personell kan fungere som en inngangsport for angripere som ønsker tilgang til kommunens interne systemer (referanse). Ansatte er av den grunn i høyere grad personlig eksponert for angrep gjennom jobben.	De ansatte tjener rollen som testsubjekter underveis i prosjektet.	Seg selv.
IT-leder / Oppdragsgiver	IT-lederen i Tysnes kommune er oppdragsgiver for prosjektet. Oppdraget samsvarer med IT-leder sitt ansvarsområde som sikter til å opprettholde et tilfredstillende kommunalt sikkerhetsnivå.	Oppdragsgiver stiller som ekstern veileder og kontaktperson, overser utførelse av tester samt stiller nødvendige ressurser til rådighet.	Anders Teigen

3.3 Brukermiljø

Brukermiljøet er i all hovedsak arbeidsplassen til de kommunalt ansatte i Tysnes. Dette vil variere alt etter hvilken kommunal seksjon en gitt ansatt tilhører, men en kontorsetting vil gjevnt over gå igjen som brukermiljø. Uavhengig av tilgang til eget kontor, er tilgang til PC, internett og kommunen sitt interne nettverk felles for alle ansatte.

3.4 Sammendrag av brukernes behov

Kommuneansatte har behov for:

- Tilgang til PC, mobil og internett. Det kan antas at dette er såpass generelle verktøy til å være relevant og nødvendig uavhengig av stilling.

- Egen kommunal brukerkonto. Brukerkontoen gir autorisasjon og tilgang til kommunen sitt IT-utstyr, system og interne nettverk (vedlegg 1). Hva en bruker har tilgang til i det interne nettverket er avgrenset ut ifra hva som er nødvendig for gitt stilling (vedlegg 1)

- Sikkerhet er som brukere av digitale system og verktøy et sentralt behov og innebærer:
  - Konfidensialitet: informasjon er kun tilgjengelig for de som har behov for det i jobben sin.
  - Integritet: informasjonen er fullstendig, nøyaktig og gyldig, og er ikke endret av uvedkommende.
  - Tilgjengelighet: informasjonen er tilgjengelig til rett tid for de som har behov for det.

  (vedlegg 1)
- Opplæring, oppdatering og oppfølging av regler og retningslinjer som angår IKT-sikkerhet er kritisk for at sikkerhetsegenskapene listet i forrige punkt skal være gjeldende.

- Fysisk tilgang. I noen etater har ansatte behov for fysiske nøkkelkort som gir behovsavgrenset tilgang til ulike bygg, avdelinger og andre ressurser (ref. Anders).

IT-leder:

- Som en delmengde av kommuneansatte er alle tidligere punkt også gjeldende for IT-leder. En merkverdig nyansering er at IT-leder har full tilgang og rådighet over kommunens interne datasystem og nettverk (referanse Anders).

- Som IT-leder har det oppstått behov for økt kunnskap om IKT-sikkerheten i kommunen (ref. Anders).

    - Som oppdragsgiver for prosjektet ønsker IT-leder derfor at det gjennomføres uanmeldte tester i reelle omgivelser.

    - Eventuelle svakheter som oppdages vil også avdekke behov for tiltak som kan bedre situasjonen.

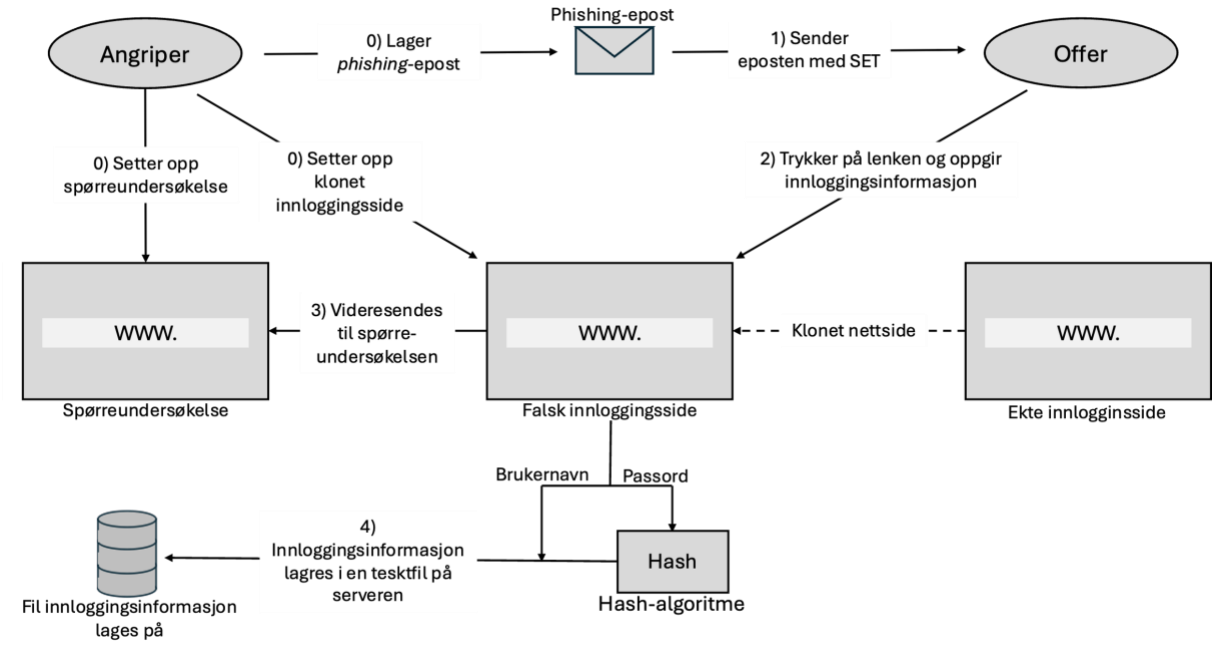
3.5 Alternativer til vårt produkt

Prosjektet tar for seg en problemstilling som utforskes fra et akademisk perspektiv. Som del av denne prosessen blir det gjennomført fysiske tester og andre oppgaver. Resultatet er teoretisk, men praktisk anvendbar kunnskap. Det utvikles derimot ikke et produkt, og det finnes derfor heller ingen alternativer.

Prosjektet gjennomføres på oppdrag for Tysnes kommune, og det kan for ordens skyld nevnes at det ikke er gjennomført liknende prosjekt for kommunen tidligere.

4 TESTOVERSIKT

4.1 Prosjektet i forhold til brukermiljøet



Figur 4-1 Viser phishing-angrepet sitt livsløp

Figuren viser hvordan phishing-angrepet skal utføres fra start til slutt Figur 4-1.

4.2 Forutsetninger og antakelser

Testing av sikkerhetskulturen krever visse forutsetninger ovenfor de ansatte.

For en vilkårlig ansatt antas gitte forutsetninger tilfredsstilt:

- Kan lese, snakke og forstå norsk (bokmål/nynorsk).
- Har tilgang til PC, mobil og internett.
- Har egen kommunal brukerkonto som gir tilgang til det interne nettverket.
- Er uviten ovenfor prosjektets natur og/eller forekomst.

5 TESTKRAV

Hvor sikkerhetsbevisste er de ansatte ovenfor phishing-angrep?

Hva kreves av prosjektgruppen for å utføre testene:

- PC som er tilkoblet internett.
- Nyttige verktøy/toolkit for å utføre phishing-angrep.
- Server som kan motta resultater fra testene.
- Server med en falsk Microsoft-innloggingsside.
- Spørreundersøkelse.

Krav til ansatte som utsettes for angrep:

- PC med tilgang til internett.
- Ansattkonto med tilhørende kommunal epostadresse som kan motta phishing-epost.

Evaluering av testene:

- Et rammeverk for å evaluere resultatene fra en gitt test. Et slikt rammeverk kan være *handbok i informasjonstrygglik for Tysnes kommune*, GDPR eller retningslinjer fra Datatilsynet.
-

Hvor sikkerhetsbevisste er de ansatte i det hverdagslige arbeidsmiljøet?

Hva kreves av prosjektgruppen for å utføre testene:

- Telefon med kamera for dokumentasjon av resultater.
- Minnepinner som inneholder et program som gir en tilbakemelding til en server dersom filen blir forsøkt åpnet.

Krav til ansatte som utsettes for angrep:

- PC med tilgang til internett og USB-inngang som gjør det mulig å benytte "infisert" minnepinne.
- Tilgang til lokasjon hvor testen finner sted.

Evaluering av testene:

- USB-aktivitet evalueres kvantitativt.
- Teste låsing av skjerm (resepsjonist), evalueres også primært sett kvantitativt, men med en kort beskrivelse av atferd
-

Hvordan kan sikkerhetskulturen eventuelt forbedres ut ifra resultatene fra de andre forskningsspørsmålene?

Hva kreves for å kunne utarbeide tiltak:

- Informasjon om god sikkerhetskultur (gode praksiser).
- Innsikt i dagens rutinger og regler.
- Hvordan disse rutinene blir implementert og fulgt opp i dag.
- Kunnskap om sikkerhetskulturen (resultater).
- Samarbeid med IT-leder.

6 IKKE-FUNKSJONELLE EGENSKAPER OG ANDRE KRAV

Da resultatet av prosjektet ikke er et produkt er det ikke behov for ikke-funksjonelle krav, men heller krav til den eksisterende sikkerhetskulturen i kommunen. Sikkerhetskulturen til Tysnes kommune skal måles basert på ulike tester som skal utføres. Det vil derfor være behov for å resonnere innvirkningen denne kulturen har på visse sikkerhetskrav som konfidensialitet, integritet og tilgjengelighet.

Konfidensialitet vil si at ansatte ikke skal ha tilgang på nettverket eller på tjenester i kommunen som ikke er nødvendig for at en ansatt skal kunne utføre jobben sin. Et brudd på konfidensialiteten vil være om en ansatt har tilgang til ressurser som den ansatte ikke er autorisert til å ha med tanke på jobbeskrivelse. [1]

Tilgjengelighet innen sikkerhet vil si at tjenester ansatte har behov for å betjene er tilgjengelig til enhver tid det er behov for å betjene denne. Hvis en uvedkommen kommer seg inn i systemet og gjør en tjeneste utilgjengelig for ansatte vil dette være et brudd på sikkerheten. [1]

Integritet eller pålitelighet omhandler om dataen på systemet og på nettverket er troverdig, og ikke manipulert av uvedkommende. Hvis en ansatt sitt passord kommer på avveie betyr det at integriteten til denne brukeren er brutt, da det ikke er mulig å vite om det er den ansatte som er pålogget eller om det er en uvedkommen som utgir seg får å være offeret. [1]

7 REFERANSER

[1] «Hvorfor styring av informasjonssikkerhet? | Digdir». Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://www.digdir.no/informasjonssikkerhet/hvorfor-styring-av-informasjonssikkerhet/3145