Høgskolen i Østfold

# Risiko og Sårbarhetsanalyse for Tilt.work

Vetle E, Gabriel W, Andrea S, Mathias J

Bacheloroppgave vår 2024

Avdeling for Informasjonsteknologi

Høgskolen i Østfold

# ABSTRAKT

Denne oppgaven inneholder en risiko og sårbarhets analyse for Tilt.work. ROS-analysen er gjennomført via anvendelse av flere ikt-sikkerhets prinsipper og oppfølging av flere faglige rutiner og normer for oppnåelse av ønsket resultat. Oppgaven består av en gransking av Nasjonal sikkerhetsmyndighet sine grunnprinsipper for IKT-sikkerhet samt forskjellige relevante verktøy som ble anvendt i gjennomføringen av en grundig analyse av Tilt.works plattform, dens funksjoner, oppsett samt deres egen opplevelse.
Dette studiet gir innsikt i hvordan Tilt.work kan optimalisere sitt forhold til IKT-sikkerhet og inneholder konkrete anbefalinger for fremtidig utvikling.

# ANNERKJENNELSER

Vi ønsker å utrykke vår takknemlighet til Ole Edvard Ørebæk for veiledning gjennom hele prosjektet, du fikk oss til å tenke kreativt og teknisk noe som var behjelpelig ved løsning av prosjektoppgaven. Vi ønsker å si tusen takk og vi er stolte over det vi har oppnådd sammen under din veiledning.

Vi ønsker også å takke Edgaras og Thomas fra Tilt.work for all kommunikasjon og veiledning under prosjektets varighet. Vi er utrolig takknemlig for godt samarbeid samt muligheten til å skrive denne oppgaven.

# FORKUNNSKAPER

Krav til forkunnskaper til oppgaven er grunnleggende ferdigheter i datanettverk, operativsystemer og sikkerhetsprinsipper som vil legge et solid grunnlag for full forståelse av helheten. Det er fordelaktig at leseren kan være kjent med sikkerhetsprinsipper, sikkerhetsprogrammer / OS og løsninger samt deres anvendelse.

# INNHOLDSFORTEGNELSE

**ABSTRAKT** ..... **I**

**ANNERKJENNELSER** ..... **II**

**FORKUNNSKAPER** ..... **III**

**INNHOLDSFORTEGNELSE** ..... **IV**

1.0 Introduksjon ..... 1
1.1 Prosjektgruppen ..... 1
1.2 Oppgaven ..... 3
1.3 Oppdragsgiver ..... 3
1.4 Mål ..... 4
1.4.1 Hovedmål ..... 4
1.4.2 Delmål 1 ..... 5
1.4.3 Delmål 2 ..... 5
1.4.4 Delmål 2.1 ..... 5
1.5 Metode ..... 6
1.6 ROS analyse for prosjektet ..... 6
1.7 Leveranser ..... 8
1.8 Arbeidsomfang ..... 9
1.9 Rapport Disposisjon ..... 10
2.0 Bakgrunn ..... 13
2.1 Forskningstema ..... 13
2.1.1 Penetrasjonstesting ..... 13
2.1.2 XSS cross site scripting ..... 16
2.1.3 IP adresser Hosts og protokoller ..... 17
2.1.4 Protokoller ..... 18
2.1.5 Sosial Manipulasjon ..... 20
2.1.6 GDPR ..... 21
2.1.7 Etisk Hacking ..... 22
2.1.8 Trusselmodellering ..... 22
2.1.9 OSINT ..... 23
2.1.10 Beredskapsplan ..... 24
2.1.11 Hendelseshåndtering ..... 24
2.1.12 ISO/IEC 27000 – Serien ..... 25
2.1.13 NSMs grunnprinsipper for IKT-sikkerhet ..... 31

2.2 Relatert arbeid ..... 35
2.2.1 Relatert ROS analyser ..... 36
2.2.2 Relatert artikkel om nettverksikkerhet ..... 36
2.3 Metoder ..... 37
2.4 Verktøy ..... 37
2.4.1 Kali ..... 38
2.4.3 Nmap ..... 39
2.4.4 ZAP ..... 40
2.4.5 SPIDERFOOT ..... 41
2.4.6 Burpsuite ..... 42
3.0 Planlegging ..... 44
3.1 Intervju med Tilt Work ..... 44
3.1.1 Styringsstrukturer ..... 44
3.1.2 Kartlegg enheter og programvare ..... 46
3.1.3 Kartlegg brukere og behov for tilgang ..... 46
3.1.4. Kontroller dataflyt ..... 46
3.1.5 Etabler evne til gjenoppretting av data ..... 47
3.1.6 Oppsummering av intervjuet ..... 47
3.2 Intervju med sikkerhetseksperter ..... 48
3.3 Oppsett og Installering av verktøy ..... 51
3.3.1 Kali linux - Operativ system ..... 51
3.3.2 Balena ..... 53
3.3.3 ZAP ..... 56
3.3.4 Nmap ..... 58
3.3.5 Burp Suite ..... 60
3.4 Risiko og sårbarhetsanalyse ..... 62
3.4.1 Mal for analyse ..... 62
3.5 Rapportene ..... 64
3.5.1 Detaljert/utdypet rapport (Excel-arket) ..... 64
3.5.2 Forenklet rapport (Tilt.work rapport) ..... 64
4.0 Gjennomføring ..... 66
4.1 Bruk av verktøy ..... 66
4.1.1 ZAP ..... 66
4.1.2 Burp Suite ..... 68
Forebygging ..... 70
4.1.3 WPScan ..... 71

4.1.4 Spiderfoot ..... 73
4.1.6 Nmap ..... 76
5.0 Resultater ..... 80
5.1 Endelig ROS analyse ..... 80
5.2 Risiko vurdering av IKT systemer ..... 84
6.0 Diskusjon ..... 87
6.1 Hovedmål ..... 87
6.2 Relatert arbeid ..... 90
6.2.1 Artikkel om cybersikkerhet ..... 90
6.2.2 Valdres ROS-analyse ..... 91
6.3 Refleksjon over delmålene ..... 93
Verktøyrefleksjon ..... 95
Valg av NSM sikkerhetsstandard vs. ISO standard ..... 96
Refleksjon om risikomatrisen ..... 101
7.0 Konklusjon ..... 103
8.0 Bibliografi ..... 110
9.0 Vedlegg ..... 115

# Figurer

1.0 ..... 4
1.1 ..... 8
2.0 ..... 15
2.1 ..... 31
2.2 ..... 42
3.0 ..... 52

3.1 ..... 53

3.2 ..... 54

3.3 ..... 55

3.4 ..... 56

3.5 ..... 56

3.6 ..... 57

3.7 ..... 58

3.8 ..... 59

3.10 ..... 60

3.11 ..... 61

4.0 ..... 66

4.1 ..... 67

4.2 ..... 68

4.3 ..... 69

4.4 ..... 71

4.5 ..... 72

4.6 ..... 73

4.7 ..... 74

4.8 ..... 74

4.9 ..... 75

4.10 ..... 75

4.11..... 76

4.12..... 76

4.13 ..... 77

4.14..... 77

4.15 ..... 78
4.16..... 78
5.0 ..... 84
5.1 ..... 85
5.2 ..... 86

# 1.0 Introduksjon

## 1.1 Prosjektgruppen

Gruppen består av 4 personer hvor alle har en stor interesse for IT-sikkerhet. Flere i prosjektgruppen har i løpet av bachelorstudiene deltatt i fag hvor de har jobbet sammen tidligere som informasjonssikkerhet, datasikkerhet, forretningssystemer og prosjektledelse. Gruppen har en sterk faglig interesse for sikkerhets-relaterte fag og ønsker å gå inn i en dypere studie om dette for å evaluere og utbedre ferdighetene sine. Gruppen består av:

Vetle, 23 år fra Lillestrøm. Studerer siste året på informasjonssystemer, med fordypning i datasikkerhet og web. Fritidsmessig Interesserer han seg for trening og friluftsliv.

Gabriel 23 år fra Lillestrøm. Studerer på Bachelor studium i Informasjonssystemer med fordypning i Datasikkerhet og Web. Interesserer seg innenfor trening, friluftsliv og fotball.

Andrea, 24 år fra Oslo. Har hatt en interesse for datasikkerhet siden videregående og har studert informasjonssystemer med fordypning i datasikkerhet og web siden høsten 2020. Hun interesserer seg av matlaging, tv-serier og sosiale medier.

Mathias, 25 år fra Oslo. Har alltid vært litt over middels interessert i datasikkerhet siden moren er advokat innenfor temaet. Har studert Informatikk med fordypning i datasikkerhet siden høsten 2019. På fritiden så går det mye i gaming, matlaging og modell-bygging.

## 1.2 Oppgaven

Vår prosjektgruppe har fått i oppdrag å generere to ulike rapporter som er basert på en risiko og sårbarhetsanalyse. Den ene rapporten skal være detaljert, og grundig, med forskjellige funn og utdypninger, mens den andre baseres på forslag til endringer som vil være lett forståelig for oppdragsgiver. Basert på system- og nettverks sikkerheten til Tilt.work vil vi som prosjektgruppe lage en ROS (Risiko og sårbarhets analyse) og finne eventuelle feil og sikkerhetsavvik i systemene deres. Det var også ønskelig for oppdragsgiver at vi implementer løsninger for disse feilene, om det er mulighet for dette.

Tilt.work ønsker å utbedre sikkerhetsstandardene i bedriften dermed vil rapportene bestå av innsikt i eventuelle sikkerhetsfeil og avvik i systemene deres slik at de kan få et klarere bilde av sikkerhetssituasjonen deres så de videre kan optimalisere systemene de bruker. Gruppen vil også gå i dybden av sikkerhetsevlaluerings-prossesser og fordype seg i temaer relevante for oppgaven. Risiko og sårbarhets analysen vil også være fungerende som en veiledning for hva ansatte i Tilt.work bør forholde seg til samt holde systemene og nettverket sitt sikkert og motstandsdyktig.

## 1.3 Oppdragsgiver

Oppdragsgiveren vår heter Tilt Work AS, de er en liten tre år gammel bedrift fra Oslo som fokuserer på IT løsninger og konsulent arbeid. Tilt.work er i hovedsak en cloud-basert bedrift, som vil si at de ikke har et fast kontor og baserer arbeidet sitt hovedsakelig på internett. Tilt.work får stadig forskjellige oppdrag innenfor utvikling, analyse og coaching av andre bedrifter.

Tilt.work sin daglige drift består av fire personer, to i lederstilling og to primære frilansere. De ansatte utfører ulike IT -tjenester på bakgrunn av forespørsler gitt av bedrifter og privatpersoner. Tilt.work er også et mediehus som publiserer ulike typer av artikler spesielt rettet mot ledelse, coaching, IT og bærekraft. Bedriften føler selv at de ikke har fullstendig oversikt over sikkerhetssituasjonen deres, de har ikke tilstrekkelig med sikkerhetsreguleringer og følger ikke alle sikkerhets-standarder i systemene sine dermed

ønsker en dypere, utbedret og detaljert rapport som spesifiserer hvilke avvik som kan utbedres.

tilt.work

**Figur: 1.0**

**Logo av oppdragsgiveren: Tilt.work**

## 1.4 Mål

Formålet med prosjektet vil være å få god innsikt til sikkerhetssituasjonen til Tilt.work sine systemer for å evaluere deres sikkerhet, gi de en oversikt og eventuelt utbedre eventuelle sikkerhetsfeil eller sårbarheter via testing og evaluering rundt systemene demmes som vi får tilgang til.

Målet vil også være å gå gjennom systemene til Tilt.work samt skrive en forebyggende og utdypet rapport opp mot sikkerhetsprinsipper etter gjeldende krav og reguleringer.

### 1.4.1 Hovedmål

Vårt hovedmål er å utforske og teste motstandsdyktigheten til systemene, samt oppdage feil.

Vi skal utføre en grundig gjennomgang av deres eksisterende systemer og identifisere mulige trusler, sårbarheter og risikofaktorer baserende på å samle inn data om systemets sikkerhetsstatus innenfor brukernes tilgangskontroll, sårbarheter, dataintegritet, konfidensialitet og tilgjengelighet.

### 1.4.2 Delmål 1

Vårt første delmål går ut på at vi skal identifisere og vurdere eksisterende risikofaktorer for å hjelpe Tilt.work unngå eventuelle fremtidige sikkerhetshendelser. Dette vil gå ut på at vi skal evaluere trusler, mulige konsekvenser av disse og eksisterende sårbarheter innad i systemet til Tilt.work.

### 1.4.3 Delmål 2

Vårt andre delmål omhandler at vi skal opprette en liste bestående av anbefalte tiltak Tilt.work kan implementere for å få en bedre IKT-sikkerhet. I dette delmålet må vi evaluere hvilke tiltak som er viktigst for Tilt.work å ta i bruk, basert på hvilke verdier de legger vekt på, samt prioritere disse tiltakene i en logisk rekkefølge avhengig av alvorlighetsgrad. Dette produktet vi lager skal da gi en teknisk oversikt til Tilt.work om deres nåværende sikkerhetssituasjon og tiltak de kan utføre for forbedringer av systemet deres.

Denne rapporten kommer til å bli et Excel-ark med relativt tekniske begreper og tiltak. Den blir lagt til som et vedlegg ved denne hovedrapporten. Det skal være mulig for dem å vise dette produktet til en tredjepart senere om de skulle ønske å ansette noen til å utføre tiltakene vi har spesifisert.

### 1.4.4 Delmål 2.1

Dette delmålet tar utgangspunkt i produktet vi beskriver at vi skal produsere i delmål 2. Her skal vi nemlig gi anbefalinger for hvordan Tilt.work kan sikre seg mot indentifiserte sårbarheter, konsekvensene som kan resultere i at disse sårbarhetene eksisterer, og dermed gi dem konkrete anbefalinger til hvordan å håndtere disse. Vi vil derfor påpeke, spesifisere og beskrive tiltakene de kan ta for å forbedre sikkerheten deres, samt redusere risikosituasjonen deres. Dette inkluderer revidering av systemkonfigurasjon, tilgangskontroller, implementering av sikkerhetsverktøy eller protokoller. Denne skal ikke være like detaljert slik som excel-vedlegget og har som hensikt å gi et overblikk til Tilt.work

og deres sikkerhetssituasjon. Den skal være lett forståelig slik at oppdragsgiveren kan fritt lese den uten å måtte skaffe seg en dypere forståelse av IT.

## 1.5 Metode

Til en god og innsiktsfull løsning av prosjektet har vi foretatt oss å starte først og fremst med nøye forberedelser og planlegging. En grundig plan som innebærer formålet med analysen og gjennomgang av sikkerhetsprinsipper, implementasjon samt rapportering av overnevnte. Vi planlegger først å evaluere rundt relevante sikkerhetsprinsipper som er hensiktsmessige for Tilt.work og hvordan disse skal implementeres samt eventuelt løses.

Når gruppen har opprettet en tilgang til systemet, planlegges det å identifisere sårbarheter og trusler som er relevante for Tilt.work.  Tilt.work er en cloud-basert bedrift derfor har prosjektgruppen tatt i betraktning og satt størst fokus på åpne porter, tjenester som kjører, eventuelle feil med konfigurasjon, tilgjengelighet samt mulig utsettelse for sosial manipulasjon.

Ved fastsettelse av trusler og sårbarheter vil gruppen foreta en sårbarhetsvurdering ved hjelp av ulike verktøy ment til penetrasjonstesting, evaluering og sårbarhetsvurdering.

## 1.6 ROS analyse for prosjektet

Risiko- og sårbarhetsanalyse er en tilnærmelse for å identifisere, evaluere og håndtere ulike risikoer som er tilknyttet et prosjekt, organisasjon eller system. En ROS analyse starter oftest med å identifisere kritiske ressurser som er både fysiske og digitale, dette kan være alt fra et system, applikasjon til enheter på et nettverk. Deretter går analysen over til trussel identifikasjon, der trusler blir identifisert og hvor det bestemmes hva som truer og om det kan være farlig eller utfordrende.

Etter at de overnevnte stegene er på plass vil analysen videreføres over til sårbarhetsidentifikasjon, spesifikt hvor det er sikkerhetshull og hvor eventuelle sårbarheter i systemene samt nettverket blir oppdaget. Sammenlagt danner dette ny innsikt og forståelse som lar oss gå videre til en risikovurdering. Risikovurderingen gir oss mulighet til å evaluere hvor sannsynlig det er at risikoen i disse sårbarhetene faktisk inntreffer og hva konsekvensene kan være om eller når hendelsen skulle oppstå.

Det første steget etter en foretatt risikovurdering vil være å danne og fastsette risikoreduserende tiltak. Dette innebærer å lage planer og danne ulike tiltak som hindrer for at hendelsene fører til skade eller i det hele tatt oppstår. Risikovurderingen gir også et klarere bilde på om risikoen og trusselen er såpass lav at den kan aksepteres og at den ikke kommer til å inntreffe eller gjøre skade. Planene kan variere fra en beredskapsplan til implementasjon av nye tiltak i systemet basert på hva risikovurderingen konkluderer og legger mest vekt på. Selve risikovurderingen gir et behandlingsgrunnlag for å iverksette nye tiltak samt implementere de nødvendige løsningene for å forhindre fremtidige hendelser og minimere skadene som kan utføres.

| Konsekvens | 1 | 2 | 3 |
|---|---|---|---|
| 5 | Brudd på taushetserklæring | Tap av arbeid | Får ikke fullført alle ønsket aspekter til oppgaven |
| 4 | Gruppemedlem velger å ikke fullføre studiet | Sårbar informasjon eller data som kommer på avveie | Kan være vanskelig å bruke bacheloroppgaven i fremtidig jobbsøk, grunnet konfidensiellt innhold |
| 3 | Skjevfordeling av arbeid mellom gruppemedlemmer | Kommunikasjonsfeil med veileder eller oppdragsgiver | Uenigheter innad i gruppen |
| 2 | Feil i innleveringsportal | Ikke oppdage viktige sikkerhetsfeil | Fordele tiden ujevnt mellom forskjellige oppgaver |
| 1 | Utestengt av epost og cloud-dokumenter grunnet midlertidig vedlikehold av skoletjenester | Gruppemedlemmer som ikke kan møte opp av uforutsigbare grunner | Sykdom |
| | 1 | 2 | 3 |
| | | Sannsynlighet | |

**Figur: 1.1 ROS analyse av prosjektoppgaven**

Ovenfor har vi en risiko og sårbarhets analyse tilsvarende dette prosjektet, med flere mulige risikoer og konsekvenser tilsvarende prosjektoppgaven. Boksene er markert med farger som strekker seg fra rød, gul til grønn. Basert på denne tabellen får vi en oversikt over potensielle konsekvenser og risikoer tilknyttet til selve prosjektet, samtidig som vi får mulighet til å forebygge disse.  Rød farge tilsvarer høy risiko og konsekvens, gul tilsvarer moderat risiko og konsekvens og grønn tilsvarer lav risiko og konsekvens.

## 1.7 Leveranser

Det skal leveres inn to separate rapporter, hvor den første rapporten vil fordype seg grundigere i analysens resultater samt fremgang, mens den andre skal opptre som en forenklet oppsummering av hovedrapporten. En slik struktur vil tilrettelegge for en lettere

forståelse for oppdragsgiver ved å gi en overordnet innsikt i arbeidet vi har gjort, funnene våre, og eventuelle råd vi har til å eliminere forskjellige trusler, mens den mer grundige og detaljerte rapporten vil gi mulighet for en dypere forståelse av sikkerhetsanalysen.

Hovedoppgaven vil være å få levert disse rapportene som skal inneholde en omfattende sikkerhetsanalyse av deres systemer i tillegg til eventuelle anbefalinger for nødvendige endringer. Dersom det oppdages åpenbare feil eller mangler i systemene vil rapporten også inkludere konkrete forslag til løsninger for disse feilene.

Etter nærmere avklaring med oppdragsgiver var det også et ønske om at det blir implementert løsninger for de eventuelle sikkerhetshullene som identifisert. Dette gjelder kun om tidsressurser i henhold til resten av oppgaven strekker til.

Videre vil den todelte rapportstrukturen skape effektiv kommunikasjon av funnene til oppdragsgiver. Den forenklede oppsummeringen vil gi en rask oversikt over hovedpunktene, mens den mer detaljerte rapporten vil gi en velbegrunnet og detaljert analyse. Dette vil tilrettelegge for optimal bruk av informasjon hvor oppdragsgiver kan ta i bruk den oppsummerte rapporten for en rask forståelse eller fordype seg i den omfattende rapporten for en dypere forståelse.

Begge rapportene vil nøye observere og identifisere sikkerhetsutfordringer i systemene til Tilt.work. Dette vil sørge for at rapportene ikke kun gir informasjon om funnene, men også vil være en praktisk veiledning for implementering av nødvendige sikkerhetstiltak innad i bedriften.

## 1.8 Arbeidsomfang

Etter tett kommunikasjon med Tilt.work har vi forstått at vi er nødt til å avgrense oppgaven slik at vi oppfyller ønskene deres. Nasjonal sikkerhetsmyndighet sin publikasjon ved navn *Risikoanalyse av IKT-systemer* presenterer de tre forskjellige fasene som inngår en komplett risiko og-sårbarhetsanalyse, hvorav stegene i den tredje og siste fasen blir beskrevet slik, "Lag en plan for oppfølging av risikoreduserende tiltak. Vurder effekten av sikkerhetstiltak ved bruk av styringsparameter (KPI). Vurder restrisikoaksept. Involver ledelsen i beslutninger og oppfølging av risikotiltak." (Nasjonal sikkerhetsmyndighet, 2021, s. 5). Oppdraget vårt går ut på at vi skal fullføre de to første fasene som inngår i en risiko-og sårbarhetsanalyse, samt det første steget i den tredje fasen som innebærer å opparbeide en

liste med risikoreduserende tiltak som må følges opp. Tilt.work er ikke interessert i at vi skal gjøre endringer i systemene deres eller at vi skal ta risikoreduserende beslutninger på deres vegne. De ønsker heller at vi skal gjøre alt grunnarbeidet, slik at de kan fullføre de resterende stegene i fase tre på deres egen tid og etter deres egen bedømmelse. Derfor ser vi oss nødt til å avgrense oppgaven til å inkludere de to første fasene, altså planleggingsfasen og risikovurderingsfasen samt alle stegene som inngår i disse, og første steget i den tredje fasen, risikohåndtering.

Nasjonal sikkerhetsmyndighet. (2021). *Risikovurdering av IKT-systemer*. (Første versjon). NSM. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

## 1.9 Rapport Disposisjon

De resterende kapitlene i rapporten vil inneholde følgende:

**Kapittel 2 Bakgrunn:**

I dette kapittelet vil vi foreta oss

- Forskningstema: Oversikt over relevante forskningstemaer, utdypet.
- Relatert arbeid: Relatert arbeid til vårt prosjekt. Dette gjelder hovedsakelig for våre verktøy som har blitt brukt for å finne svakheter i systemene til Tilt Work.
- Metoder: Metodene som skal benyttes i prosjektet.
- Verktøy: En oversikt over verktøyene vi benytter oss av i prosjektet, med forklaring for hvordan disse fungerer.

**Kapittel 3 Planlegging:**

I dette kapittelet vil det bli gått igjennom planleggingsprosessen for oppgaven. Hvordan vi tenker å benytte oss av de ulike verktøyene, plan for risiko analysen og en utdypning i

forhold til de to rapportene som skal leveres. Kapittelet vil inneholde følgende hovedpunkter:

- Intervjuet med Tiltwork
- Intervjuet med sikkerhetseksperter
- Oppsett og videre bruk av verktøy: Hva vi har gjort for å sette opp de ulike verktøyene, samt en planlegging for hva de ulike verktøyene skal brukes til.
- Risiko og sårbarhetsanalyse. Planlegging av vår hovedoppgave som er ROS analysen for Tilt Work.
- Rapportene: Utdypning av hva vi tenker videre for de to rapportene som skal gjøres i prosjektet.

**Kapittel 4 Implementering:**

I dette kapittelet blir det gått igjennom selve prossessen for bruk av de ulike verktøyene. Her vil resultater vi har funnet frem til ved bruk av disse også være med.

- Bruk av de ulike verktøyene.

**Kapittel 5 Resultater**:

Her er resultatene vi har funnet frem til.

- Endelig ROS analyse
- Risiko vurdering av IKT systemer
- Forenklet rapport vedlegg
- Hovedrapport vedlegg

**Kapittel 6 Diskusjon:**

Dette kapittelet inneholder diskusjon og refleksjon av oppdragsprosessen vår, hvordan vi gjennomførte prosjektmålene våre og hvilke valg vi tok underveis.

- Hovedmål
- Refleksjon over delmålene
- Verktøyrefleksjon
- Valg av NSM sikkerhetsstandard vs. ISO standarden
- Refleksjon om risikomatrisen
- Relatert arbeid
- Artikkel om cybersikkerhet
- Valdres ROS-analyse

**Kapittel 7 Konklusjon:**

Kapittel 7 vil inneholde en konklusjon av prosjektet, hva vi har funnet og oppnådd.

# 2.0 Bakgrunn

Bakgrunnen for dette prosjektet går ut ifra den økende digitalisering i dagens samfunn og stigningen i cybertrusler som mange bedrifter står ovenfor per dags dato. En ROS analyse har blitt et verktøy som blir brukt av stadig fler bedrifter for å identifisere, vurdere og minimere potensielle sikkerhetstrusler. I følge Symantec's 2019 Security Threat Report har antallet sikkerhetsbrudd økt med 11% fra 2018 til 2019, noe som bare understreker behovet for sikkerhetsanalyser i bedrifter (Symantec, 2019).

Dette prosjektet vil ha et mål om å utdype forståelse for en ROS analyse og hvor essensielt det er for en bedrift, med formål om å fremme en kultur av risikobevissthet blant bedrifter og deres ansatte.

I dette kapitelet skal vi gjøre rede for ulike forskningstema hvor vi vil gå i dybden innenfor it-sikkerhet samt deres anvendelse.

## 2.1 Forskningstema

For å kunne gi en god oversikt over fremgangsmåten vår må vi spesifisere og forklare en god del faguttrykk. I dette kapitelet skal vi forklare forskjellige metoder og verktøy vi kan ta i bruk i forskningen vår og hva disse kan gjøre for oss. Sammenlagt vil disse verktøyene være behjelpelig med å danne en innsiktsfull ROS analyse og gi et helhetsbilde på Tilt.work sine tjenester.

### 2.1.1 Penetrasjonstesting

Penetrasjonstesting er en form for sikkerhetstesting og brukes til å evaluere sikkerheten i et system, nettverk eller programvare. Penetrasjonstest identifiserer sårbarheter og avklarer

hvor det er avvik som muliggjør det å komme forbi sikkerhetshindre og få tilgang til informasjon.

Hovedformålet med penetrasjonstesting er å evaluere rundt sikkerheten i et IT-miljø ved å etterligne og gjøre angrep så ekte som en vanlig angriper hadde gjort dem. Slik blir det mulig å forebygge og samtidig forberede ett eventuelt angrep.

For å utføre en nøyaktig penetrasjonstest finnes det essensielle aspekter som gir et solid grunnlag, disse er som følger:

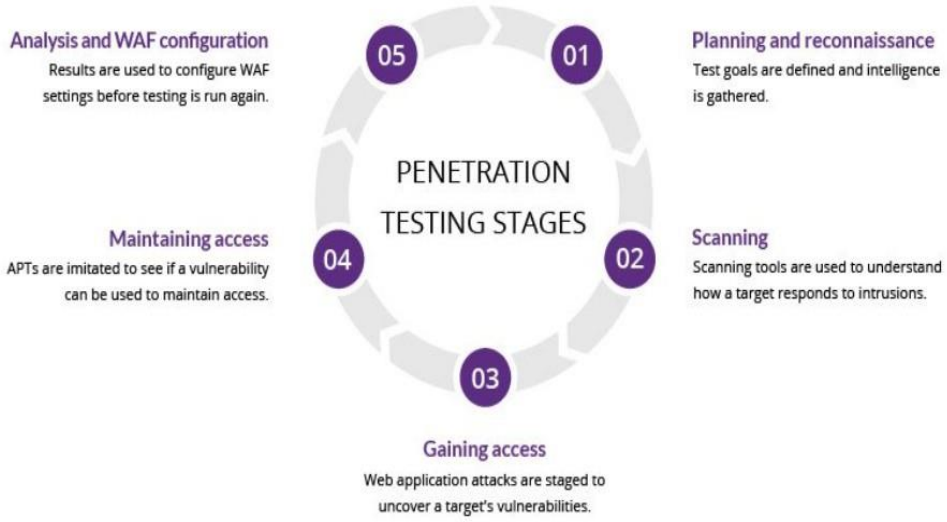
Rekognosering - Samle inn så mye informasjon som mulig på det vi ønsker å teste, dette innebærer blandt annet søking rundt i systemet etter nødvendig informasjon.

Scanning – Granske systemet vi ønsker å penetrere ved hjelp av verktøy egnet til det, verktøyet vil selv finne sikkerhetshull og gi tilbakemelding om dette, eksempelvis kan verktøyet være WPscan.

Få tilgang – Hovedmålet med penetrasjonstesting er å få tilgang til systemet, og finne eventuelle svakheter.

Opprettholde tilgang – Det å få tilgang er ikke nok, selv om en fikk muligheten til å komme inn, vil det ikke si at man kan være der lenge nok til å finne sårbarheter. Systemene kan nemlig detektere brukeren og lukke porten med tilgangen.

Analyse. - Analysere spesifikk data og sårbarheter vi har fått tilgang til samt samle og gå over data som ble samlet og loggføre hvor lang tid det tok før vi fikk tilgang.




**Figur: 2.0**

**På figuren ovenfor har vi en illustrasjon av hva en penetrasjonstest inneholder og hvordan penetrasjonen foregår steg etter steg.**

Ved vellykket penetrasjonstest vil man få tilgang til sensitiv informasjon som ligger lagret inn i systemene, potensielt utfall av en velutført penetrasjonstest er:

- **Tilgang til konfidensiell informasjon:** Alt fra sensitiv informasjon som brukernavn, passord og sensitive personopplysninger kan innhentes ved hjelp av penetrasjonstesting.
- **Tilgang til ressursene i systemet:** Tilgang til databaser, betalingsinformasjon eller oppsett av systemarkitektur, potensiell mulighet for å sette inn skadelig programvare inn i systemet ved uautorisert kode.
- **Ekstern tilgang:** En ekstern tilgang til systemet som allerede blir etablert ved første forsøk, det vil si at vi med lett måte har fått etablert en fast rute og får tilgang til systemet mer effektivt ved senere anledning. Dette omtales også som en “bakdør”.

Penetrasjonstesting kan på enkel måte gi tilgang til konfidensielle ressurser til en uautorisert bruker som kan utføre skade eller ta hånd om informasjon en ikke bør ha tilgang til, derfor er det særlig viktig for oss å forebygge mot at det kan forekomme.

### 2.1.2 XSS cross site scripting

XSS (Cross site scripting) Er en form for sikkerhetssårbarhet som gir angripere med ondsinnede hensikter muligheten til å sende inn skadelig programmer (skript) som vil bli vist til besøkende av en nettside. Om en besøkende på nettsiden trykker på dette eller bare går inn på en nettside, vil vedkommende sin maskin kunne bli injisert med skadevare. Ved mottakelse av skadevare kan det for eksempel gjøre at angripere får tilgang til sensitiv informasjon om vedkommende. XSS får ofte besøkende til å følge instruksjoner, uvitende om at dette ikke er noe som tilhører den originale nettsiden.

For Tilt.work er det viktig å være påpasselig med denne type angrep utenfra og ta hensyn til dette ved vedlikehold av sin nettside. Derfor er det viktig å oppdatere Tilt.work om potensielle farer for dette, og hvordan de kan forhindre det ved bruk av ulike sikkerhetsmessige retningslinjer for slike angrep.

Om dette rammer tiltwork sine abonnenter kan dette få store konsekvenser for deres tillit til Tilt.work og de kan med dette miste flere av sine abonnenter og inntekter. Akkurat derfor er det svært viktig for Tilt.work og forebygge at slike angrep forekommer på deres nettside.

Det er da avgjørende å følge retningslinjer for å forebygge slike angrep, nedenfor er de viktigste:

- **Regelmessig sikkerhetsrevisjon**: Jevnlig revidere koden til webapplikasjonen for å kunne oppdage potensielle trusler.
- **Inndatavalidering**: Forsikre seg om at inndata samsvarer med forventet format, samt avise data som kan tolkes som skript.

- **Innholdssikkerhetspolitikk**: Kontrollere hvilke ressurser som har lov til å laste på nettsiden ved å implementere CSP-hodene i nettsiden.

### 2.1.3 IP adresser Hosts og protokoller

En IP-adresse er en identifikator som tildeles hver enhet som blir produsert, dette kan være alt fra en datamaskin til en skriver. IP adressen fungerer som en unik adresse for å identifisere og lokalisere enheter på et nettverk eller enheter som er tilkoblet til et system. IP-adresse er særdeles nødvendig for at enheter skal kunne kommunisere med hverandre og for at nettverket skal kunne identifisere spesifikk enhet for å motta og overføre pakker til riktig host.

IP-adresse bruker per dags dato flere protokoller, protokoller legger til rette for kommunikasjon mellom en enhet og et gitt nettverk der IP protokollen muliggjør adresselokalisering mellom enheter tilkoblet til en server eller til et system og gir mulighet til å adressere disse spesifikt.

Protokollen(e) er ansvarlig for riktig pakkerouting der den bestemmer hvor data i form av pakker skal føres fra hovedsender til en destinasjon gjennom nettverk. Protokollene bestemmer også hvem som mottar informasjonen og hvor fort den overføres/sendes tilbake.

IP-adresser har i hovedsak to forskjellige typer protokoller som de blir identifisert med og bruker for å kunne kommunisere med enheter på et nettverk.

**IPv4** (Internet protocol version 4) – Ipv4 er den mest utbredte versjonen av IP- adresser i hele verden og består av fire tallseksjoner følgende med 3 rader. Eksempelvis kan en IPv4 se ut som *192.168.1.1 .*

**IPv6** (Internet protocol version 6) – Ipv6 er en nyere versjon av IP-adresser og har blitt introdusert på bakgrunn av økende antall enheter. Ipv6 adresser har åtte tallseksjoner og regnes som en mer sikker, men fortsatt en forholdsvis ny protokoll. Eksempelvis kan en IPv6 adresse se ut som *2001: 0db8: 0002: 4619.*

I en IP-adresse finnes det også porter som fungerer som virtuelle dører som tillater spesifikk trafikk å nå bestemte tjenester inne på et nettverk, eller en enhet. Porter er ofte nummerert og hver av de mottar og tillater informasjon å gå gjennom til hovedtjenesten for å så utføre handlinger.

Hver IP-adresse har tilgang til de samme portene, men det er selvbestemt på hvem av de portene som er åpne eller skjult som ofte er avhengig på hvilke tjenester som kjører inne på et nettverk, eller en enhet.

Per dags dato er de mest brukte portene:

- HTTP (port 80) som opprinnelig ble brukt for å betjene nettverkstrafikk, denne porten tillater enkel kommunikasjon mellom webservere og er lett tilgjengelig.
- HTTPS (port 443) Når behovet for sikker data og integritet begynte å bli større, ble det besluttet at port 443 skal være den mer sikre veien å gå for trafikk på nettverket, dette er på grunn kryptering denne porten tilbyr, noe som gjør det mer sikkert.

For prosjektoppgaven er det vesentlig at gruppen får tak i IP adressen til Tilt.work som kan brukes videre til penetreringstester og tilgang til systemer, IP adressen blir avslørt ved hjelp av verktøy som Nmap, ZAP og WpScan.

### 2.1.4 Protokoller

En protokoll innenfor nettverkspotologi er en rekke regler og prosedyrer som følges opp ved kommunikasjon mellom enheter på et nettverk. Protokoller definerer hvordan data som sendes og mottas skal formateres og tolkes både av sender og mottaker.

Det finnes i dag mange titalls protokoller, men på bakgrunn av denne oppgaven velger vi å vinkle studiet mot de mest kjente og omtalte protokollene innenfor nettverk og sikkerhet.

- **TCP –** Kjent som *Transmission Control Protocol* er en kommunikasjonsprotokoll på internett, som tillater ulike enheter å lage en kobling med hverandre og

kommunisere / sende data. Den sikrer at dataen blir overført til riktig mål og gir muligheten av å spore opp om dataen som ble sendt faktisk har blitt mottatt. TCP kommuniserer med tjenesten basert på TCP/IP pakke og får riktig port destinasjon derifra. TCP brukes i en rekke angrep hensiktsmessig mest opp mot DDOS angrep, der de mest utbredte angrep omhandler TCP-SYN-FLOOD. Dette angrepet handler om å sende mange (TCP)datapakker mot en destinasjon, uten å respondere på det serveren sender tilbake. SYN-FLOOD fører til overbelastning av destinasjonen på grunn av mengden av forespørsler og resulterer med at serveren blir utilgjengelig.

- **UDP-** Kjent som *User dataprogram protocol* er en koblingsprotokoll som ikke danner en kobling før kommunikasjonen oppstår. Den brukes som oftest av servere og applikasjoner som ikke trenger validering av data og som ikke loggfører sine overføringer. Det vil si at hvis en datapakke sendt over med UDP protokoll forsvinner, kan det bli vanskelig å spore den opp. UDP protokoller brukes i hovedsak av applikasjoner som opererer i nåtid som feks video tjenester.

- **HTTP og HTTPS –** *Hypertext transfer protocol* og *hypertext transfer secure protocol* er begge et hovedformål om å overføre data på internett ved å legge en kobling mellom webserver og en nettleser. Disse brukes vanligvis til å hente ut nettsider og lenker fra en servere på web.

- **SSH –** Kjent som *Secure Shell* er en kryptert protokoll som sørger for trygg og sikker kommunikasjon mellom enheter på internett. Protokollen brukes til å sikre dataen som blir sendt mot uautorisert tilgang og kan også brukes til å få fjernkontroll over andre datamaskiner eller servere.

- **DNS -** Kjent som *Domain Name System* er en protokoll med formål om å oversette domenenavn til IP adresser, noe som gjør det enklere for en datamaskin å forstå.

DNS sørger for at et domenenavn blir riktig distribuert og overfører brukere til nettsiden som blir oppsøkt.

### 2.1.5 Sosial Manipulasjon

Sosial manipulasjon også kjent som *social engineering*, er en praksis som baserer seg på å utnytte menneskelig atferd og psykologi med formål som gir utøveren en fortjeneste eller tilgang til å oppnå et ønsket mål. Sosial manipulasjon innebærer en rekke strategier som *Phishing*, *tailgating,* spoofing og *baiting,* hvor angriperen manipulerer menneskets atferd til å utføre en handling som kommer til å utføre skade eller gi en fortjeneste.

Phishing er den mest kjente og utbredte teknikken innenfor sosial manipulasjon, den går ut på at angriperen sender villedende meldinger i form av e-post, reklame eller fysisk post hvor hen utgir seg for å være andre aktører som kommer fra pålitelige kilder. Målet med phishing er å få brukeren til å oppgi viktig og sensitiv informasjon som eksempelvis brukernavn og passord.

Tailgating går ut på å utnytte andre sin generell ønske om sosial aksept, samarbeid og tilhørighet, kort fortalt vil det innebære å utnytte sosiale normer som å være alt for pålitelig med personen, bygge tillit og empati for å så oppnå informasjon man ønsker.

Baiting har i seg selv flere former den forekommer i, de mest omtalte formene vil være clickbaitng spesielt vanlig med koblinger som lenker og overskrifter der en blir flyttet til en annen nettside enn forventet. En vesentlig viktig del av baiting, er sikkerhetsbaiting som foregår i en teknologisk kontekst, der en person eksempelvis etterlater en USB-enhet insifert med virus som blir tatt opp av andre og plugget inn i datamaskinen med mål om å spre virus.

Spoofing – Er en teknikk hvor svindlere utgir seg for å være fra en pålitelig og sikker kilde, eksempelvis et norsk telefonnummer som de skjuler seg bak eller et kjent nettsted. Målet er å lure offeret til å tro at det er en bekjent eller en troverdig kilde for å gi fra seg informasjon eller gi tilgang til angriperen.

Sosial manipulasjon er ofte den mest utbredte formen for personer å få tilgang til informasjon på, det er mye enklere enn man tror og folk flest vet ikke hvor enkelt det kan være for en å utføre skade kun ved hjelp av mail eller en enkel forespørsel. Målrettet mot oppgavens formål vil vi utbedre en kort analyse til Tilt.work om forebygging mot sosial manipulasjon. (Kaspersky,2023).

Nedenfor er det en kort liste ovenfor sikkerhetstiltak:

1. Sikkerhetstiltak som implementerer hos bedriftens systemer og hos alle ansatte tilrettelagt for å gjenkjenne mistenkelige lenker, nettsteder og mailer.
2. To-faktor/Multi-faktor autentisering ved alle tjenester den ansatte benytter seg av for å unngå autorisert tilgang av personer med onde hensikter. To-faktor-autentisering ved pålogging til mail til tilgang i systemene.
3. Nettverkssikkerhetstiltak som brannmur som kan forebygge nedlastning av skadelig data gjennom internett. Målet er å tilby kontrollerte grensesnitt med ulike tillitsforhold på nettverket, slik at det finnes en sone på nettverket som er mellomliggende mellom bedriftens nettverk og nettverk tjenesten som blir besøkt av de ansatte. Det vil si at kun et utvalg av kilder har muligheten til å kommunisere og nedlaste på enhetene som Tilt.work benytter seg av.
4. Antivirus – regelmessig oppdatering av antivirus programvare.

Kontinuerlig evaluering og oppdatering av sikkerhetstiltakene er essensielt for å holde sikkerhetskulturen oppdatert og unngå uønskede hendelser.

### 2.1.6 GDPR

General data protection regulation / personvernordningen, er en forordning som skal styrke personvernet ved behandling av data innenfor EU. Selve ordningen er blitt implementert den 25. mai 2018, der den regulerte strengere rammeverk av personopplysninger hos privatpersoner og bedrifter, dette ble gjort ved hjelp av retningslinjer innenfor innsamling, deling og lagring av data.

En sentral bestemmelse innenfor GDPR er et krav om samtykke fra enkeltpersoner før behandling av personlig data noe som har tvunget organisasjoner til å ta personvern og datasikkerhet mer alvorlig. Dette har ført til økt investering i opplæring av ansatte og implementering av retningslinjer i bedrifter.

### 2.1.7 Etisk Hacking

Etisk hacking også kjent som Hvit-hatt hacking er en praksis hvor personer som ikke har noe formål om å utføre en skade selv, men heller identifiserer trusler og skader som kan gjøres i et system eller programvare, hacker seg inn i ett system. Dette gjøres hovedsakelig ved anvendelse av penetrasjonstesting, loadtesting og relaterte sikkerhetsmetoder.

Etisk hacking differerer seg fra hacking på bakgrunn av at personene har fått autorisert tilgang og tillatelse av oppdragsgiver å utføre slike tester inne på et nettverk eller et system, der hacking samsvarer også med retningslinjer gitt av eksempelvis NSM og andre aktører, dette innebærer skriftlig tillatelse av organisasjonen som eier systemet, overholdelse av retningslinjer, personvern samt etikk under utføring. I tillegg til å avsløre sårbarheter før de kan utnyttes av andre gir det også en innsikt i oppdragsgiverens sikkerhetspositur og finne potensielle forbedrelser som kan forebygge at angrep forekommer.

Etisk hacking har som hovedmål å finne sårbarheter samt å rapportere om disse til bedriften, slik at disse kan forebygges og utbedres. Baserende på formålet med å utbedre en risiko og sårbarhetsanalyse kommer prosjektgruppen til å utføre flere penetreringsangrep på Tilt.work sine systemer i henhold til retningslinjer med gitt tillatelse.

### 2.1.8 Trusselmodellering

Trusselmodellering er en prosess innenfor informasjonssikkerhet som utfører en tilnærming for organisasjoner i håndtering av potensielle trusler mot deres dataressurser og IT avdeling. Sentralt i denne prosessen ligger identifisering av resurser en bedrift innehaver, og som kan bli tilintetgjort, stjålet eller utsatt for angrep. Det er også essensielt at en bedrift tar tak i

deres sårbarheter og orienterer seg om eventuelle trusselaktører for å formulere eventuelle sikkerhetstiltak og danne en hendelseshåndterings plan. I en trusselmodelleringsplan ligger det som oftest interne og eksterne aktører som blir tatt til vurdering under dannelse av en slik prosess.

Dette strekker seg fra interne brukere, konkurrenter til eksterne trusler som hackere. Ved en trusselmodellering vil det anses som nødvendig å ta en analyse av bedriftens programvare, nettverkstopologi, og tilgang for å kunne modellere og finne frem til ulike trusler.

### 2.1.9 OSINT

OSINT (Open source intelligence) er en metode for datainnsamling for all data som er tilgjengelig om en kilde, dette er som regel ute på et nettverk, der informasjonen ikke er regulert av noen standarder. OSINT kan utføres med en webcrawl der den søker etter informasjon som kan anses som relevant eller likt med den søketerminologien som ble brukt da man startet denne webcrawleren.

Ting som en webcrawler kan finne er blandt annet: Data som er tilgjengelig i offentlig domene registeret som kan avsløre relevant informasjon som tilhører nettsiden man ønsker mer informasjon om.

OSINT kan inkludere informasjon som tabellinnhold, DNS-informasjon, sosiale medier, nyhetsartikler, navn, forum og mye mer for å identifisere trusler og finne frem relevant informasjon om Tilt.work.

OSINT er innhold som kan bli funnet på tvers av mange plattformer på internett, disse inkluderer: offentlige registre, nyhetsmedia, sosiale medier, bilder / video samt nettsider. Ved innsamling av slik data vil det være lettere å identifisere potensielle trusler og gi innblikk til en trusselvurdering av et spesifikt nettsted og samtidig finne informasjon som er på avveie eller få innsikt hvordan informasjonen er spredt rundt.

### 2.1.10 Beredskapsplan

En beredskapsplan er en overordnet plan som skal gjøre rede for hva som skal gjøres under en krisesituasjon i bedriften. En slik plan inneholder vanligvis retningslinjer, prosedyrer og resurser som skal iverksettes hvis en hendelse skulle oppstå. Planen skal etter retningslinjer være utformet slikt at bedriften skal være i stand til å respondere på hendelsen og at skadeomfanget skal minimeres eller tilintetgjøres.

Som regel vil hovedpunktene i en beredskapsplan bestå av:

- En risikovurdering for potensielle trusler som kan oppstå
- Beredskapsinstruksjoner som da vil si hva som skal gjøres ved situasjonen
- De ulike rollene og ansvaret
- Plan for kommunikasjon
- Gjennopprettingsplan: altså hvordan organisasjonen skal komme tilbake igjen til normal drift.

En beredskapsplan bør være fleksibel og laget for å kunne brukes under flere typer hendelser. Samtidig må planen være grundig for å kunne håndtere hver situasjon på en grundig og effektiv måte, samtidig som den konstant blir revidert og oppdatert med nye tiltak i henhold til retningslinjer. (FEMA, 2021)

### 2.1.11 Hendelseshåndtering

Hendelseshåndtering innenfor sikkerhetskontekst er prosessen av å oppdage, evaluere og reagere på sikkerhetshendelser som oppstår innad i bedriften. En slik prosess er essensiell for å minimere skader om de skulle oppstå og komme tilbake til normal drift så fort det lar seg gjøre.

En hendelseshåndterings-plan innad i bedriften er viktig når det gjelder å finne frem informasjon til hvordan hendelser behandles når bedriften først blir utsatt for et angrep eller en uønsket hendelse.

Vinklet mot oppgaven vil det utbedres en plan for hvordan Tilt.work bør håndtere en sikkerhetshendelse hvis det skulle oppstå gitt i en hierarkisk rekkefølge.

Det første steget ved å lage en hendelseshåndteringsplan er å identifisere risikoer og hendelser slik at man kan legge til grunn gode eksempler for mulige hendelser. Det er viktig å ha rikelig med opplæring og jevnlig evaluere kunnskapen slik at man kan stoppe hendelsen så fort det lar seg gjøre.

Andre steget i en slik plan er å analysere hendelsen som forekom i eksempelet, her bør både ledelsen og ansatte se nøye etter hva som kunne gå galt og hva som kunne vært gjort bedre, for å så i senere anledning være forberedt og eventuelt forebygge at dette skjer igjen.

Tredje steget vil være å løse hendelsen, etter en analyse vil man kunne komme til kjernen av problemet, for å så kunne løse den eksempelvis ved gjenoppretting av systemer eller iverksette nød prosedyrer.

Når hendelsen så inntreffer, er det særskilt viktig med kommunikasjon innad bedriften. Dette innebærer å informere ansatte, kunder og andre involverte aktører, slik at de også er forberedt.

### 2.1.12 ISO/IEC 27000 – Serien

ISO/IEC serien er en fastsatt informasjonssikkerhet standard utbredt og oppfølgt over hele verden. Standarden er publisert av International Organization of Standardization og International Electrotechnical Commision.

Iso serien har ulike protokoller og veiledninger, samt fastsatte prinsipper hver og en bruker bør forholde seg til, serien(e) har med overlag et bredt omfang i feltet og dekker data som personvern, konfidensialitet og IT / sikkerhetsproblemer. Alle organisasjoner oppfordres per dags dato til å behandle sine sikkerhetsprinsipper og evaluere rundt disse basert på denne serien.

Generelt

ISO 27000 serien er ett sett med ISO standarder som hjelper selskaper med å bygge opp ett Information Security Management System (ISMS).

Mens ISO 27001 er anerkjent som en verdifull standard for informasjonssikkerhet, er det likevel noen potensielle utfordringer og begrensninger som organisasjoner kan støte på ved

implementering. Det er viktig å merke seg at disse problemene ikke nødvendigvis gjør ISO 27001 uegnet, men de kan representere utfordringer avhengig av organisasjonens størrelse, bransje og spesifikke behov. Her er noen punkter vi vurderte:

**Kostnader og ressurser:**

ISO 27001-standarden innebærer betydelige kostnader og ressurskrav for organisasjoner som søker sertifisering. Opplæringskostnadene er ofte blant de første kostnadene en organisasjon møter. Opplæring av ansatte for å forstå kravene i ISO 27001 og hvordan implementere dem effektivt kan være tidkrevende og dyrt. Spesielt i mindre organisasjoner kan dette være en utfordring, da de kanskje ikke har de samme økonomiske ressursene eller infrastrukturen som større bedrifter har til rådighet.

Teknologiske kostnader er en annen viktig faktor. Implementering av tekniske sikkerhetsløsninger, som brannmurer, antivirusprogramvare, og sikkerhetskopiløsninger, kan være nødvendig for å oppfylle kravene i standarden. Dette krever ofte investering i ny teknologi eller oppgradering av eksisterende systemer, noe som kan være en betydelig økonomisk belastning.

Sertifiseringskostnadene er også viktige å vurdere. Organisasjoner som ønsker å bli sertifisert etter ISO 27001 må gjennomgå en omfattende vurderingsprosess av et uavhengig sertifiseringsorgan. Dette kan være en kostbar prosess, spesielt hvis organisasjonen må gjennomgå flere revisjoner eller implementere ytterligere tiltak for å oppfylle standardens krav.

**Kompleksitet:**

ISO 27001-standarden er omfattende og teknisk, og dens kompleksitet kan være en utfordring for organisasjoner som ikke har erfaring med informasjonssikkerhet.

Terminologien som brukes i standarden kan være vanskelig å forstå for de uten spesialisert kunnskap eller erfaring innenfor feltet. Dette kan føre til misforståelser eller feil tolkninger av kravene, noe som igjen kan resultere i manglende implementering eller ineffektive sikkerhetstiltak.

Implementeringsutfordringer kan også oppstå på grunn av standardens omfattende natur. Organisasjoner må identifisere og implementere et bredt spekter av kontroller og prosesser for å oppfylle kravene i ISO 27001. Dette kan være tidkrevende og kreve betydelige ressurser, spesielt hvis organisasjonen ikke har etablerte prosedyrer eller retningslinjer for informasjonssikkerhet på plass fra før av.

I tillegg kan kompleksiteten til ISO 27001 gjøre det vanskelig å opprettholde sertifiseringen over tid. Organisasjoner må kontinuerlig overvåke og vedlikeholde sitt informasjonssikkerhetssystem for å sikre at det forblir effektivt og i samsvar med standardens krav. Dette krever en betydelig innsats og ressursallokering fra organisasjonens side, noe som kan være en utfordring på lang sikt.

**Forankring i ledelsen:**

Ledelsens engasjement og støtte er avgjørende for suksessfull implementering og opprettholdelse av ISO 27001-sertifiseringen. Hvis toppledelsen ikke er sterkt engasjert i implementeringsprosessen, kan det være vanskelig å få støtte og ressurser som er nødvendige for å oppnå og opprettholde sertifiseringen.

Mangel på ledelsesengasjement kan føre til manglende prioritering av informasjonssikkerhetsspørsmål og resultere i underinvestering i nødvendige sikkerhetstiltak og prosesser. Dette kan igjen øke organisasjonens sårbarhet overfor trusler og angrep på informasjonssikkerhet, og svekke dens evne til å beskytte konfidensialiteten, integriteten og tilgjengeligheten til informasjonen.

Sterkt engasjement fra toppledelsen er derfor avgjørende for å etablere en kultur for informasjonssikkerhet og sikre at organisasjonen tar informasjonssikkerhet på alvor på alle nivåer.

**Stivhet i tilnærming:**

ISO 27001 gir et generelt rammeverk for implementering av informasjonssikkerhetstiltak, men noen organisasjoner kan oppleve standardens tilnærming som for stiv. Dette kan være spesielt utfordrende for organisasjoner som opererer i dynamiske eller innovative bransjer, hvor behovene og risikoene knyttet til informasjonssikkerhet kan endre seg raskt over tid.

Manglende fleksibilitet i standarden kan føre til at organisasjoner sliter med å tilpasse seg nye trusler eller teknologiske endringer som påvirker deres informasjonssikkerhet. Dette kan resultere i at organisasjonene ikke oppnår tilstrekkelig beskyttelse mot nye og fremvoksende trusler, og dermed settes i fare for sikkerhetsbrudd eller datalekkasjer.

For å håndtere denne utfordringen, kan organisasjoner vurdere å implementere et mer fleksibelt rammeverk for informasjonssikkerhet som lar dem tilpasse sine sikkerhetstiltak og prosesser etter behov og endringer i risikobildet.

**Overbetoning på dokumentasjon kontra faktisk sikkerhet:**

ISO 27001 legger til rette for omfattende dokumentasjon av informasjonssikkerhetssystemet (ISMS), inkludert utvikling av policyer, prosedyrer og registreringer. Mens dokumentasjon er viktig for å dokumentere organisasjonens informasjonssikkerhetsprosesser og kontroller, kan det være en risiko for at organisasjoner fokuserer for mye på papirarbeidet knyttet til sertifiseringen, på bekostning av faktisk sikkerhet.

Dette kan resultere i at organisasjonene oppfyller standardens krav på papiret, men likevel ikke oppnår reell forbedring eller styrking av sitt sikkerhetsklima. Det er derfor viktig at organisasjonene balanserer behovet for dokumentasjon med behovet for praktiske og effektive sikkerhetstiltak, og at de fokuserer på å oppnå reell sikkerhetsforbedring i tillegg til å oppfylle standardens krav.

For å oppsummere, selv om ISO 27001 er anerkjent som en verdifull standard for informasjonssikkerhet, er det viktig å være klar over de potensielle utfordringene og begrensningene som organisasjoner kan møte ved implementering. Ved å være oppmerksom på disse utfordringene og ta hensyn til dem i implementeringsprosessen, kan organisasjoner bedre posisjonere seg for å oppnå og opprettholde en effektiv informasjonssikkerhet praksis.

**Tidskrevende implementeringsprosess:**

Implementeringen av ISO 27001 kan være en langvarig prosess som krever betydelig tid og innsats fra organisasjonens side. En grundig gjennomgang av eksisterende prosesser og systemer må utføres for å identifisere potensielle svakheter og risikoer som må adresseres. Utvikling av nødvendig dokumentasjon, inkludert politikker, prosedyrer og registreringer, kan også være tidkrevende, spesielt hvis organisasjonen starter fra bunnen av. Opplæring av ansatte for å sikre at de forstår og kan implementere kravene i ISO 27001 er også en viktig, men ofte tidskrevende, del av prosessen. I tillegg kan organisasjonen møte utfordringer knyttet til koordinering av ulike avdelinger eller enheter, samt håndtering av eventuelle motstridende interesser eller prioriteringer som kan oppstå underveis. Alt dette kan føre til at implementeringsprosessen strekker seg over lang tid og krever betydelige ressurser.

**Behov for kontinuerlig oppdatering og vedlikehold:**

ISO 27001 krever kontinuerlig oppdatering og vedlikehold for å sikre at informasjonssikkerhetssystemet forblir relevant og effektivt over tid. Dette inkluderer regelmessig gjennomgang og revisjon av politikker, prosedyrer og kontroller for å sikre at de fortsatt er effektive og i samsvar med organisasjonens behov og mål. Det kan også være behov for å gjøre endringer i respons på nye trusler eller endringer i organisasjonens driftsmiljø. Dette kan være en omfattende prosess som krever betydelig tid og ressurser fra organisasjonen, spesielt hvis det oppstår større endringer som krever revisjon av eksisterende dokumentasjon eller implementering av nye sikkerhetstiltak.

**Begrenset fokus på menneskelige faktorer:**

ISO 27001 legger hovedsakelig vekt på tekniske og prosessmessige sikkerhetstiltak, og det kan ha begrenset fokus på menneskelige faktorer i informasjonssikkerhet. Dette kan være problematisk da menneskelige feil og atferd ofte er en av de største truslene mot informasjonssikkerhet i organisasjoner. For å håndtere denne utfordringen, må organisasjoner supplere tekniske og prosessmessige sikkerhetstiltak med opplæring og bevisstgjøring av ansatte om deres rolle og ansvar for informasjonssikkerhet. Dette kan omfatte opplæring i sikkerhetsbevissthet, retningslinjer og prosedyrer, samt implementering av retningslinjer for tilgangskontroll og overvåkning av ansattes atferd.

**Manglende tilpasning til nye teknologier og trender:**

ISO 27001 kan være utfordrende å tilpasse til nye teknologier og trender innen informasjonsteknologi. Med fremveksten av nye teknologier som skytjenester, IoT (tingenes internett) og kunstig intelligens, kan det være behov for tilpassinger eller tillegg til eksisterende kontroller og prosesser for å adressere nye sikkerhetsutfordringer. Dette kan være en utfordrende oppgave som krever kontinuerlig overvåking av teknologitrender og tilpasning av informasjonssikkerhetssystemet for å sikre at det forblir effektivt og relevant over tid.

**Begrenset krav til revisjoner og testing:**

ISO 27001 stiller krav til regelmessige revisjoner og tester av informasjonssikkerhetssystemet, men det gir ikke detaljerte retningslinjer for hvordan disse aktivitetene skal gjennomføres. Dette kan føre til manglende konsistens og sammenlignbarhet i revisjons- og testprosesser på tvers av organisasjoner. Organisasjoner må derfor utvikle sine egne tilnærminger til revisjon og testing, basert på deres spesifikke behov og risikoprofil. Dette kan inkludere utvikling av interne revisjons- og testprosedyrer, opplæring av revisjons- og testteam, og gjennomføring av regelmessige øvelser og simuleringer for å evaluere effektiviteten av sikkerhetstiltakene.

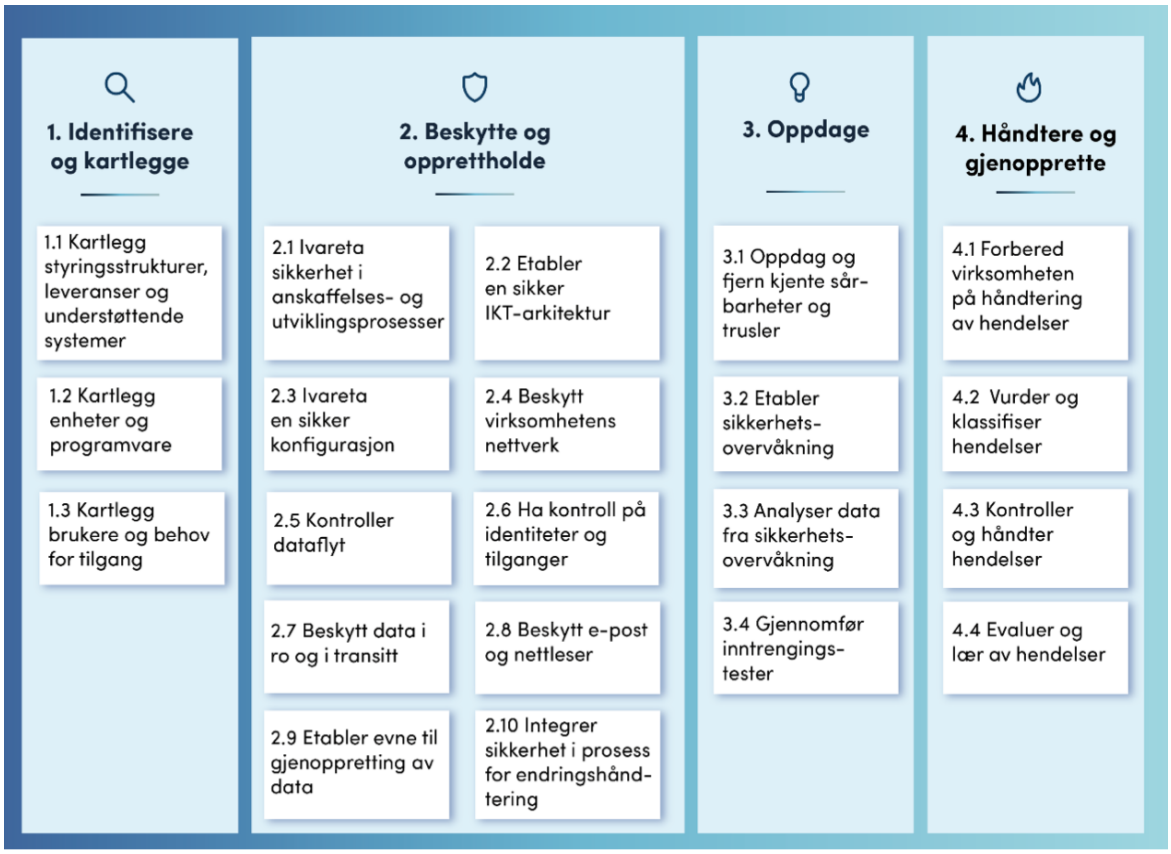
International Organization for Standardization. [Edition 3, 2022]. ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. https://www.iso.org/standard/27001

Mark1Systems. [29 November 2023]. Navigating the pros and cons of ISO 27001 Certification in the UK: A Mark1 Systems Perspective. https://mark1systems.com/navigating-the-pros-and-cons-of-iso-27001-certification-in-the-uk-a-mark1-systems-perspective/

Neumetric.[u.å]. ISO 27001 vs Other Security Standards. Hentet 8 mars 2024 fra: https://www.neumetric.com/iso-27001-vs-other-security-standards-a/

### 2.1.13 NSMs grunnprinsipper for IKT-sikkerhet

NSMs grunnprinsipper for IKT-sikkerhet er en publikasjon fra Nasjonal Sikkerhetsmyndighet som er til for å hjelpe norske virksomheter skape og opprettholde gode rammer og regler for IKT-sikkerheten deres. Dokumentet er delt i fire steg som representerer hoveddelene av prosessen i å styrke eller utvikle en god IKT-sikkerhet.




**Figur: 2.1** *Oversikt over NSMs grunnprinsipper for IKT-sikkerhet*, 2020, av Nasjonal sikkerhetsmyndighet
https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

**På figuren ovenfor har vi NSM sine grunnprinsipper innenfor IKT sikkerhet, laget for bedrifter, som følger ulike steg under hver kolonne.**

Steg 1: Identifisere og kartlegge

For å få en god oversikt over det eksisterende IKT-systemet poengterer NSM at man må kartlegge en mengde faktorer som er knyttet til virksomhetens daglige funksjoner. NSM sine grunnprinsipper beskriver det første steget slikt, "... opparbeide og forvalte forståelse om virksomheten herunder styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere" (Nasjonal sikkerhetsmyndighet, 2020, s.6). Dette inkluderer hva slags programmer virksomheten bruker i daglig drift, hvilke funksjoner i virksomheten er tjenesteutsatt og hvor sikre er disse tjenestene, hvilke enheter og hva slags programvare er i bruk, og hvem er brukerne og hva har de tilgang til.

Hensikten med dette steget er å få en god oversikt over hvordan virksomheten er driftet og hva slags daglige prosesser den tar i bruk. Dette kan hjelpe til å identifisere sikkerhetshull tidlig i sikkerhetsutbedringsprosessen, for eksempel at alle ansatte har sikkerhetsklarering til alle avdelinger i bedriften, selv om det ikke er behov for dette. NSM sine grunnprinsipper beskriver hensikten slik, "... å forstå virksomhetens leveranser og tjenester, få oversikt over hvilke teknologiske ressurser som må sikres og de roller og brukere virksomheten består av." (Nasjonal sikkerhetsmyndighet, 2020, s.6).

Ved å kartlegge programmene virksomheten tar i bruk kan man se hvilke programmer som ikke er nyttige for bedriften og som da kan elimineres, samt hvilke programmer som er livsviktige for virksomheten og må styrkes.

Steg 2: Beskytte og opprettholde

Etter man har fått en god oversikt over virksomhetens eksisterende IKT-system er det viktig å vite hvordan man skal beskytte og opprettholde virksomhetens prosesser, konfigurasjon og data.

NSM beskriver steget slikt, "[virksomheten] ivareta en forsvarlig sikring av IKT-systemet og opprettholde den sikre tilstanden over tid og ved endringer." (Nasjonal sikkerhetsmyndighet, 2020, s.6). Dette gjøres ved å få kjennskap til hvor dataene ligger, hvor dataen beveger seg og hvordan de best kan sikres, jevnlig kontrollere brukeres tilganger, identiteter og enheter, ha strenge protokoller for brukere i ansettelses og

oppsigelsesprosessen, etablere en protokoll til jevnlige sikkerhetskopieringer, samt skape en sikker og god IKT-arkitektur.

En oversiktlig IKT-arkitektur og en rekke protokoller til forskjellige prosesser innad i virksomheten er avgjørende for å få styrke bedriftens sikkerhet og gjør det mer lesbart å spore hvor eventuelle sårbarheter eller trusler oppstår. Ved å snevre inn på tilgangen ansatte har til forskjellig informasjon, vil det være vanskeligere for trusler å trenge seg inn til alle systemene ved hjelp av en ansatt-innlogging alene.

Steg 3: Oppdage

Ved å gjøre seg kjent med IKT-arkitekturen og rydde den slik at den blir mer oversiktlig blir det lettere for virksomheten å kartlegge hvor det er sårbarheter eller eksisterende trusler. NSM beskriver prinsippene under steg 3 slikt, "Prinsippene i denne kategorien fokuserer på å oppdage og fjerne kjente sårbarheter og trusler gjennom sårbarhetskartlegging og overvåking av IKT-systemet" (Nasjonal sikkerhetsmyndighet, 2020, s.6). Ved å oppdage disse sårbarhetene kan man klassifisere de i forskjellige kategorier i hvor farlige de er, om de bør styrkes, overvåkes eller bli der.

Overvåkning spesifiserer NSM at er et viktig punkt i dette steget. Etter å ha implementert en sikkerhetsovervåkning er det viktig å etablere en jevnlig analyse av data og funn som blir produsert. Ved å analysere disse kan man enkelt se hvor trusler har prøvd å trenge seg inn.

For å sjekke om IKT-systemet til virksomheten tilstrekkelig og for å videre kartlegge sårbarheter forteller NSM oss at det er viktig å utføre inntrengingstester. Dette er også kjent som etisk hacking, hvor noen prøver å trenge seg inn i et system for å se hvor det er svakheter.

Steg 4: Håndtere og gjenopprette

Dette steget går ut på hvordan virksomheten skal utføre hendelseshåndtering om en trussel har brutt seg inn i systemet. Det vil si at virksomheten må sette visse protokoller til hva som vil skje om visse hendelser finner sted. NSM spesifiserer oppgavene under steg 4 slikt, "...

dette innebærer å forberede seg på, vurdere, kontrollere og håndtere hendelser, gjenopprette normaltilstand, samt forbedre sikkerheten basert på erfaringer fra hendelseshåndteringen." (Nasjonal sikkerhetsmyndighet, 2020, s.7). Om hendelsen ikke er fullt så alvorlig, men er fortsatt kritisk trussel vil det være nyttig å kontinuerlig overvåke den, uten at man gjør det åpenbart for selve trusselaktøren at de har blitt oppdaget. Denne overvåkingen bør vare helt til man vet nok om hendelsen til å kunne ta tilstrekkelige grep i hendelseshåndteringen. Om hendelsen er svært alvorlig og skadelig for systemet vil det være nyttig å gjøre alt man kan for å stoppe trusselen, uansett om det så blir åpenbart for trusselaktøren at de har blitt oppdaget.

Det siste punktet i dette steget er å evaluere og lære av hendelsen som fant sted. En hendelse kan synliggjøre en eksisterende sårbarhet i systemet som virksomheten ikke har vært klar over tidligere, som videre kan bidra til å styrke bedriftens systemer.

NSMs oppsett

NSMs grunnprinsipper for IKT-sikkerhet er et dokument på 55 sider, hvor relevansen til alle delstegene i de fire kategoriene, vist i figur 2.1 blir beskrevet i detalj, samt en tabell-oversikt over anbefalte tiltak og en avsluttende paragraf med utdypende informasjon. Et slikt oppsett gjør dokumentet svært oversiktlig og lett å finne seg frem.

NSM eller ISO?

For å velge riktig standard å følge, så må vi stille oss selv flere spørsmål. Er det viktig for oppdragsgiver at de kan selv forstå standarden vi tar i bruk? Er det en standard som er mer egnet til denne spesifikke virksomheten, Tilt.Work, enn en annen?

Er det viktig for oppdragsgiver at de selv kan forstå standarden vi tar i bruk? Vi kan se tilbake på selve oppdraget vi har fått, som er at vi skal produsere to forskjellige produkter, ett lettleselig et som ledelsen kan forstå, og ett mer avansert et som de kan eventuelt gi videre til en spesialist om de ønsker dette. Det at de vil ha et spesifikt produkt som er lettleselig kan støtte argumentet hvor valget er NSM sine grunnprinsipper. Grunnlaget for denne tanken er at det kan være ønskelig at oppdragsgiver har mulighet for å forstå eller i det

minste få en oversikt over standarden vi velger for å analysere IKT-systemene deres. NSMs grunnprinsipper er gratis, oversiktlig og lett tilgjengelig ved et søk, mens ISO standarden gjemmer seg bak en betalingsmur, samt kan være vanskeligere å forstå siden den er tungvinn på fagord.

Dette bringer oss til vårt neste punkt, om det er en standard som er mer åpenbar egnet i dette tilfellet enn en annen. ISO er en universell standard som kan bli tatt i bruk hvor som helst, som gjør den både nyttig, relevant og ikke minst troverdig samtidig som at den er detaljert og gjennomført, NSMs grunnprinsipper derimot, er mer oversiktlig. NSM sin standard refererer til ISO innenfor flere forskjellige prinsipp, mens de vinkler informasjonen de forklarer til å bedre egne seg for norske virksomheter, "NSMs grunnprinsipper for IKT-sikkerhet er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet og er inspirert av mange av disse... Eksempler på styringsrammeverk og veiledninger er: ISO/IEC 27001 – Internasjonal standard som beskriver et ledelsessystemer for informasjonssikkerhet."(Nasjonal sikkerhetsmyndighet, 2020, s.7).

ISO er en svært relevant standard, og selv om vi har stor interesse for å bruke denne til å utføre risiko-analysen vår, er det i vårt tilfelle best å forholde seg til NSM sine grunnprinsipper. Dette er på grunn av at NSM egner seg bedre til norske virksomheter, samt de punktene som hadde vært relevante for oss i ISO standarden i stor grad allerede refereres til hos flere grunnprinsipper. I tillegg til dette er ISO-standarden såpass tungvinn at ikke en person med et standard nivå av IT-kjennskap vil kunne lese gjennom den på strak arm.

Nasjonal sikkerhetsmyndighet. [15.4.2020]. Grunnprinsipper for IKT-sikkerhet. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

## 2.2 Relatert arbeid

Da det er begrensninger for hva som finnes av relatert arbeid innenfor en type sikkerhetsoppgave som dette har vi i hovedsak holdt oss til et begrenset antall relevante

kilder. To relevante ROS analyser, samt en artikkel om generelle kunnskaper for sikkerhet som legger grunnlaget for et slikt arbeid.

### 2.2.1 Relatert ROS analyser

**ROS (risiko- og sårbarhetsanalyse)**

- Nasjonal sikkerhetsmyndighet. [21 Juni 2021]. Risikovurdering av IKT-systemer. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

Dette er risiko og sårbarhetsanalysen til NSM. Denne er relevant da vi har valgt å benytte oss av disse punktene som mal i vår ROS analyse. Vi har valgt denne malen da den gir en god oversikt over punkter man bør ha med i en slik analyse for å gi Tilt.work en så god og oversiktlig risiko og sårbarhetsanalyse som mulig.

**Valdres risiko og sårbarhetsanalyse**

- IKTvaldres,[oktober,2020].https://www.iktvaldres.no/wp-content/uploads/2021/10/ikt-valdres-iks-ros-mal.xlsx

Dette er forholdsvis simpel versjon av en ROS analyse som ikke gir en utdypet og god oversikt over trusselbildet. Vi refererer til Valdres sin risiko og sårbarhetsanalyse i diskusjonskapittelet.

### 2.2.2 Relatert artikkel om nettverksikkerhet

- PwC[2023]. Hva er cybersikkerhet. Hentet fra: https://www.pwc.no/no/teknologi-omstilling/hva-er-cybersikkerhet.html

Denne artikkelen om cybersikkerhet dekker godt over generell informasjon om hva dette innebærer og går igjennom de fleste kjente type dataangrep man må være påpasselig for, samt generell informasjon om ulike type hackere. Videre er gode eksempler på kjente cyberarngrep og det avsluttes med råd til it-sikkerhet for bedrifter. Det denne artikkelen har til felles med vår oppgave er at den formidler god informasjon om mange av de store dataangrepene Tilt.work må være påpasselig på og den formidlere også gode råd for it-sikkerheten i en bedrift. Dette er mange gode råd som for mange bedrifter kan lønne seg å ta med seg videre for å opprettholde et godt sikkerhetsnivå og bidra til en tryggere arbeidsplass. Vi diskutere artikkelen videre i diskusjons kapitelet.

## 2.3 Metoder

Metodikken vil utføres på bakgrunn av ulike steg i stigende rekkefølge som vil basere seg på forarbeid og research. Metoden for å løse dette sikkerhetsoppdraget vil starte med Identifikasjon av trusler, altså hva som potensielt kan utføre skade og hva slags konsekvens dette vil gi. Truslene kan potensielt være uaktsomhet, misbruk av gitt informasjon eller skadelig programvare.

Fastsettelse av trusler vil muliggjøre og evaluere rundt sårbarheter i systemet og gi innsikt på hvordan man kan vurdere sårbarhetene i et system eller nettverk, dette innebærer hvordan en sårbarhet kan være en innvei for trussel.

Ved fastsettelse av potensielle sårbarheter og trusler vil det være mulig å foreta en risikovurdering, altså hvor sannsynlig det er for at disse faktisk inntreffer og danner en trussel.

## 2.4 Verktøy

Tilt.work har gitt spesifikk tilgang til systemene sine til hele prosjektgruppen hvor all informasjon skal holdes konfidensielt og er kun til bruk i rapporten. Gruppen planlegger å benytte seg av verktøy som programmer, operativsystemer og applikasjoner som vil være til

hjelp under løsning av oppdraget. Disse er undernevnte programmer som prosjektgruppen skal benytte seg under oppdraget til Tilt.work. I omfang vil alle verktøyene bli brukt og testet opp mot Tilt.work sine systemer for å utføre en analyse og evaluere rundt sikkerheten.

### 2.4.1 Kali

Kali er et operativt system som gir et sett med verktøy for sikkerhetstester, penetetrasjonstester og for sårbarhetsanalyse av systemer og nettsider. Kali i seg selv er et operativsystem som vil gi oss verktøyene som tester hvor sikkert et system egentlig er og kjøres. Den kan brukes til å finne og løse sårbarheter i systemet og nettverket og etter at Kali er ferdig oppsatt vil vi kunne bla gjennom ulike applikasjoner allerede forhåndsinstallert som eksempelvis penetrasjonstesting der det mest brukte applikasjonen er metasploit.

Kali Linux kan brukes til:

- **Simulering av angrep**: Ved penetrasjonstesting kan det simuleres et reelt angrepsscenario. På denne måten kan man evaluere hvordan systemet reagere på ulike trusler.
- **Sikkerhetssjekk før lansering av nye applikasjoner:** Ved å gjennomføre en penetrasjonstest før det lanseres nye applikasjoner eller tjenester kan man på forhånd oppdage om det finnes mulige sikkerhetshull eller sårbarheter.
- **Testing av sikkerhet for tredjeparts leverandør**: Ved utførelse av penetrasjonstesting kan man teste systemer eller tjenester til tredjeparts leverandører for å forsikre seg om at disse også opprettholder sikkerhetsstandarder.
- **Sikkerhetsvurdering av IT-infrastrukturen til en bedrift:** Gjennomføring av penetrasjonstesting for å mulig kunne oppdage sårbarheter i bedriftens nettverk, sårbarheter i servere og andre digitale ressurser.

For prosjektoppgaven vil Kali hovedsakelig brukes til simulering av ulike angrepsscenarior og sikkerhetsvurdering av IT-infrastrukturen til Tilt.work. Ved å gi innsikt til Tilt.work sine systemer vil vi kunne danne en rapport med sikkerhetsfeil, ulike aspekter av systemet som avviker fra normer og kunne informere om dette.

### 2.4.3 Nmap

Nmap er et verktøy som primært brukes for å skanne portene i ett nettverk for å finne hvilke av portene som er åpne. Nmap er en forkortelse for "Network mapper" og brukes ofte av nettverks administratorer for å sjekke at det ikke er noen åpne porter på maskinene på deres nettverk som burde være lukket. Men det kan også brukes av potensielle TA i informasjonssamlingsfasen av ett angrep for å finne ut hva slags type angrep en maskin/et nettverk kan være sårbart for.

Nmap starter ofte med å utføre en portskanning for å finne ut hvilke porter som er åpne på målmaskinen. Den kan bruke forskjellige teknikker som TCP SYN-skanning, TCP Connect-skanning, UDP-skanning osv. For eksempel, med TCP SYN-skanning, sender Nmap en SYN-pakke til hver port, og hvis en port er åpen, svarer målmaskinen med en SYN/ACK-pakke. Hvis porten er lukket, svarer den med en RST-pakke.

Etter å ha funnet åpne porter, kan Nmap prøve å fastslå hvilket operativsystem som kjører på målmaskinen. Det gjør dette ved å analysere forskjellige nettverksprotokollsvar, for eksempel TCP/IP-stakkfingeravtrykk, ICMP-respons og andre karakteristiske egenskaper.

Nmap kan deretter identifisere hvilke tjenester som kjører på de åpne portene. Dette gjøres ved å sende spesifikke forespørsler til tjenestene og analysere svarene for å fastslå hvilken programvare som kjører, og hvilken versjon av programvaren det er.

Etter å ha identifisert tjenestene, kan Nmap prøve å fastslå den eksakte versjonen av programvaren som kjører. Dette gjøres ved å sammenligne responsen fra tjenesten med en database over kjente programvareversjoner og deres karakteristiske trekk.

Til slutt analyserer Nmap alle innsamlede data og genererer en rapport som kan inneholde informasjon om åpne porter, kjørende tjenester, versjonsdetaljer, operativsystemdeteksjon og mer.

Etter endt installasjon av Nmap vil vi kunne starte programmet, deretter vil vi få en konsoll som vil ta imot ulike kommandoer om hva vi ønsker å utføre. Koden vi brukte var omfattende kun for å finne ut av hvem porter på tjenestene til Tilt.work som var åpne.

- Nmap kan bland annet brukes til: **Portscanning**: Identifisere hvilke porter som er åpne på målmaskiner. På denne måten kan det evalueres mulige angrepspunkter.
- **Penetrasjonstesting**: Identifisere svakheter i nettverket.
- **Sikkerhetsskanning**: Utføre sikkerhetsskanning for å oppdage mulige sårbarheter i nettverket.
- **Ressursoptimalisering**: Nmap kan bidra til å identifisere ressurskrevende tjenester og/eller prosesser på en datamaskin, som kan hjelpe maskinen å arbeide med optimal effekt.

### 2.4.4 ZAP

ZAP er en forkortelse for zed attack proxy, det er et populært åpen-kildekode verktøy for sikkerhetstesting av nettsider og cloud baserte applikasjoner. Zap er et verktøy utviklet med formål om å evaluere rundt sikkerheten til nettsteder, med mål som innebærer:

- **Sikkerhetstesting**: ZAP hjelper med å identifisere sårbarheter og sikkerhetsfeil i source koden til nettsiden.
- **Sikkerhetsbevissthet:** Zap gir bedre forståelse for potensielle sikkerhetstrusler, ved å gi tilbakemelding på hva som er feil og hva konsekvensen av dette kan være. ZAP vil samtidig gi tips om hva som må endres og har innebygd database med kjente sårbarheter hvor den sammenligner koden og oppsettet av nettsiden hvor den finner relevant sammenligning.
- **Sårbarhetsanalyse:** ZAP tilbyr omfattende en sårbarhetsanalyse som viser sårbarhetene den finner frem og gir en sikkerhetsrangering på disse samt deres alvorlighetsgrad, dette gir omfang av sikkerhetsrisikoer og hva som må gjøres for å

løse dem. ZAP leveres også med en rekke funksjoner forhåndsinstallert når man starter programvaren.

- **Spidering:** Kartlegging av nettsiden ved oppfølging av lenker, og identifisering av resurser som sendes inn og ut av serveren inkludert API ende punkter.
- **Passiv skanning:** ZAP overvåker trafikken mellom nettsiden og andre servere uten å generere trafikk, det vil si at den selv ikke sender forespørsler og data, men kun avlytter trafikken som blir sendt inn og ut av serverne og mellom tjenester. På denne måten kan vi se hvem datapakker nettsiden tillater og hva som blir sendt inn og ut av nettsiden.
- **Fuzzing** – Er en måte for å se om nettsiden responderer på ugyldig kode og tom data som blir sendt, dette er ment for å identifisere svakheter i datainntasting og behandling. ZAP vil generere en rapport som vil gi innsikt på oppsammlet informasjon. Denne rapporten vil inkludere identifiserte sårbarheter, deres alvorlighetsgrad samt forslag til løsning av disse.

Konkluderende vil Zap bli brukt til å se etter svakheter på nettsiden til Tilt.work og gi gruppen innblikk på eventuelle sårbarheter og hva som må gjøres for å utbedre disse.

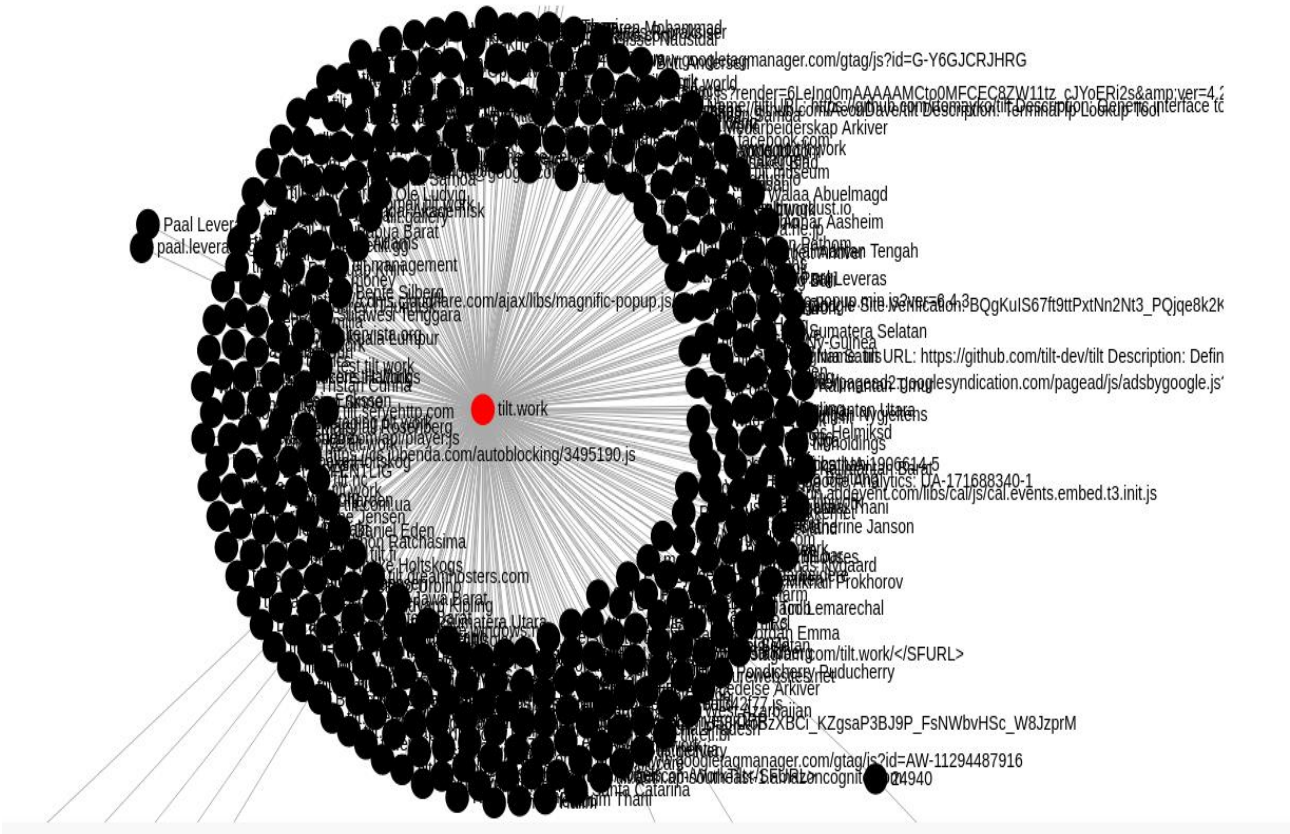
### 2.4.5 SPIDERFOOT

Spiderfoot er et rekogniseringsverktøy som sender ut forespørsel til flere hundre forskjellige datakilder (OSINT), for å samle inn og ettersøke etter IP-adresser, e-post, navn, domener og tilgjengelig informasjon om en nettside eller tjeneste.

Spiderfoot bygger en forståelse og viser mulige koblinger mellom all data som går inn og ut av serveren, samt informasjon som er forholdsvis lik den vi leter etter for å kunne finne likheter og stikkord samtidig som den analyserer dataen som flyter gjennom og kan filtrere blant de mest kjente sårbarhetene.

Verktøyet vil også selv analysere all data den samler opp og gjennomgå det, spiderfoot vil sette opp dataen den samler opp mot sammenhenger mellom datakilder, mønstre og koblinger som kan ha en påvirkning mot Tilt.work sine systemer. Spiderfoot kan også brukes til å overvåke trusselaktører ved å samle opp data fra ulike hackerforum, mistenkelige IP

adresser og datapakker noe som gir en helhetlig trusselmodellering og en tilnærming på trusler som kan forekomme.




**FIGUR: 2.2**

**På bilde ovenfor har vi foretatt en scan etter Tilt.work sin nettside som viste oss alle mulige koblinger, der innhold finnes på andre nettsteder. Dette lar oss evaluere og danne et trusselbilde, samt gir oss innsikt på hvor informasjon om Tilt er tilgjengelig.**

## 2.4.6 Burpsuite

Burp suite er et verktøy innenfor nettverkssikkerhet som utfører tester og evaluerer sikkerheten til nettsider, der den lar brukere oppdage sårbarheter som kan potensielt utnyttes.

Innebygd i Burpsuite er sårbarhetsscanning, håndtering av sesjoner og mulighet til å manipulere HTTP-trafikk til nettsiden for å danne en analyse.

# 3.0 Planlegging

Vår hovedoppgave vil være å lage en detaljert ROS analyse i form av to rapporter. Det er da viktig å vite hvordan vi tenker å gå frem for å gjennomføre dette, ved hjelp av verktøy som tillater oss å gjennomføre en grundig sårbarhetsanalyse og finne trusler.

I dette kapittelet går vi gjennom vår planlegging frem til analysen og kapittelet vil inneholde følgende: et intervju med Tilt.work for å få en bedre forståelse for rutinene og verdiene deres, et intervju med sikkerhetseksperter som vi gjennomførte får å få en bedre forståelse av IKT-sikkerhet i praksis.

Installasjons-og bruksguide til forskjellige relevante verktøy vi vurderer å bruke i oppgaven, fremgangsmåte på hvordan vi skal utføre risiko-og sårbarhetsanalysen vår, og til slutt en produktbeskrivelse av de to forskjellige leveransene vi skal produsere for Tilt.work.

## 3.1 Intervju med Tilt Work

Før eventuell implementasjon har gruppen valgt å gjennomføre et intervju med Tilt.work og stille dem noen spørsmål som gir innsikt til deres stilling til sikkerhet og hvordan det fungerer internt i bedriften.

Vi intervjuet Thomas Nygaard den 08.03.2024 og stilte han spørsmål som var relevante for at gruppen kunne få framgang i planlegging.

### 3.1.1 Styringsstrukturer

**Hva er verdiene deres, og er det noe spesifikt dere ønsker sikret?**

**Svar:** Det er i hovedsak tekstene som ligger i databasen, artiklene tekstene og selve medlemsregisteret. Tap av artikler er en frykt fordi det er informasjon bygd opp over mange år. Kort fortalt er det Innholdet, medlemsbasen og kundeforhold. Vi ønsker en sikret og stabil nettside som minimerer tap av innhold og som laster inn raskt.

**Hvem er admin?**

**Svar:** Det finnes ingen superadmin, alle de ansatte er egentlig admin(Paul, Eddy, Thomas og Jeanette) har tilgang.

**Hvordan er ansvaret fordelt?**

**Svar:** Det er ganske klare roller, og hvem som gjør hva i bedriften. Paul har hovedansvaret for innhold, sjefdirektør og har aktivt forretningsutvikling. Han bestemmer bland annet på hvem kurs vi skal lage og hva foredragene skal handle om.

Thomas Nygaard er daglig leder og har ansvaret for økonomistyring og administrerer butikken.

Jeanette er egentlig ikke ansatt, men til rollen som desker. Hun lager headlines og overskrifter samt som hun skriver ingresser og jobber med tekstene og artiklene. Jeanette jobber også med markedsføring og har hovedansvaret for Facebook og LinkedIn sidene.

Eddy er tekniker og IT medarbeider, som hovedsakelig jobber med backend

**Hvem er de forskjellige ansatte?**

**Svar:** Vi er totalt 4 ansatte som fakturer Tilt. Det er meg (Thomas Nygaard), Paul, Jeanette og Eddy.

**Hvilke spesifiserte roller eller stilling har de?**

**Svar:** Det finnes ingen stillingsbeskrivelser, formelt sett så har ikke dette firmaet noen ansatte. En ansatt er noen som får lønn, men det er ingen som får lønn fra Tilt. Alle fire ansatte har egne firmaer som fakturerer tilt og er desverre ikke beskyttet av arbeidsmiljøloven.

**Hvem publiserer artikler?**

**Svar**: Janette publiserer artiklene. Alle som har, forfatter status (skribenter som har blitt gitt det) kan gå inn skrive direkte inn i wordpress. Forfattere kan legge inn artiklene i wordpress men en admin må godkjenne artiklene for at de skal kunne publiseres.

**Hva er deres understøttende system i tillegg til Wordpress, Stripe, Cloudflare og Fiken?**

**Svar:** Ja det vi bruker flere av dem, blant annet en Linux-server, storage-box, AVS og Google Workspace.

### 3.1.2 Kartlegg enheter og programvare

**Hva har dere av enheter og hvor mange har dere av hver?**

**Svar:** Alle ansatte har PCer, nettbrett og en mobiltelefon, der alle enhetene er private.

**Hvordan nettverk bruker dere på arbeidsplassen?**

**Svar:** Kontoret ligger i et bygg sammen med andre bedrifter, alle i bygget bruker samme nettverk og har samme passord til å få tilgang.

### 3.1.3 Kartlegg brukere og behov for tilgang

**Hvor mange har en ansattbruker?**

**Svar**: Forfattere som har tilgang til Wordpress, samt alle de ansatte i bedriften

**Hva har artikkel skribenter av tilgang og kontoer og hvor stort behov er det for disse tilgangene?**

Svar: Forfattere har kun tilgang til artikler når de skal skrives, artiklene må godkjennes av admin / e, før de eventuelt publiseres. Det er stort sett ikke noe behov for at disse skal ha tilgang til Wordpress.

### 3.1.4. Kontroller dataflyt

**Hvorfor valgte dere fiken?**

**Svar:** Det var ikke et bevisst valg, vi valgte fiken fordi Paul brukte det fra før i et annet firma og han hadde gode erfaringer med det. Vi tittet også på brukergrensesnitt og det ser klart og fint ut.

**Hva slags data er det dere sender til fiken/hva slags data er det fiken får?**

**Svar:** Alle våre økonomiske transaksjoner, registreres i fiken. Fiken er integrert med banken vår (DNB). En gang i måneden gjøres det også en bankavstemning og det kommer en kontoutskrift. Der passer man på at alt er registrert og hører eventuelt med fiken om det er noe som ikke er på plass.

Det er også mye kunde data i fiken, alt fra adresse, navn til betalingshistorikk og kontoinformasjon står opp registrert. Mye av kundedataen er hentet fra brønnøysundregisteret noe som er offentlig informasjon.

### 3.1.5 Etabler evne til gjenoppretting av data

**Har dere en sikkerhetskopiering eller back-up?**

**Svar:** Backup av databasen, wordpress filer blir gjort hver 24t og blir gjort automatisk av cloudways. De backupene varer i 30 dager før de rulleres. Restore på cloudways kan gjenopprette enten  wordpress, databasen eller begge. Vi har også en backup server i linux og kjører et program som heter backup pc som er koblet opp til vår cloudways med SSH.

### 3.1.6 Oppsummering av intervjuet

Oppsummerende har gruppen funnet flere brudd på sikkerhet som strider med NSM sine grunnprinsipper og retningslinjer. Eksempelvis vil “Bring your own device” eller ta med privat maskin på jobb være en potensiell fare for Tilt Work, hensiktsmessig vil det forekomme potensielle trusler ved bruk av privat verktøy på jobb grunnet flere faktorer.

Manglende oppdateringer av programvare, altså dårlig vedlikehold av datamaskinen sin vil føre til at den er mer utsatt for potensielt angrep. Privat verktøy kan også bli utsatt for CSRF angrep og angriperen får tilgang til systemene til Tilt.

Manglende antivirusprogrammer på datamaskinene til de ansatte kan føre til at det er større sjanse for infisert programvare som fører til deling av bedriftsdata når maskinen er innlogget på Tilt Work sine systemer.

## 3.2 Intervju med sikkerhetseksperter

For å få en bedre forståelse av hvordan vi skal gå fremover med risikoanalysen vår, har vi hatt et intervju med to sikkerhetseksperter som er ansatt i en stor og anerkjent internasjonal bank.

Før vi begynte intervjuet viste sikkerhetsdirektøren oss litt rundt i bedriften, og videre tok oss med til hans avdeling. For at vi skulle komme inn til kontoret hans måtte han bruke et ID kort for å låse oss inn og videre forklarte han at kun han og to andre ansatte har adgang til denne avdelingen. Kontoret består av et lite, adskilt møterom, som brukes til videomøter, et større rom med en åpen-landskap løsning hvor det var to store pulter, med fire monitorer på hver side, et større, adskilt kontor der de to sikkerhetsekspertene sitter hovedsakelig og jobber, og til slutt et stengt rom, med en tung dør. Dette sistnevnte rommet fikk vi ikke innsyn til, men de beskrev det som et fysisk kontrollrom, der de har forskjellige maskiner og verktøy. Vi satt oss ned ved pultene i avdelingen som hadde et åpent landskap, og startet intervjuet.

For å starte intervjuet og bli litt mer kjent med ekspertene så spurte vi hva de jobber med og hva slags oppgaver de løser på en daglig basis.

**Hvordan ser en vanlig dag ut for dere?**

**“**Vi driver først og fremst med etterforskning. Dette kan være oppgaver vi får fra det tekniske sikkerhetsdepartementet hos oss, hvor de ber oss sjekke ut ting som de kanskje ikke har tilgang til. I tillegg til dette har vi ofte foredrag og møter hvor vi informerer om sikkerhet. Dette kan være enten for politiet, andre på arbeidsplassen eller skoleelever.”
Videre forklarte de enkelt hvordan en hendelsesetterforskning hos dem foregår.
“Etter den tekniske avdelingen har stoppet en hendelse, er det vår oppgave å grave. I denne prosessen av hendelsesetterforskningen så er det mest utfordrende å loggføre.” For å parafrasere forklarer de videre hvordan de kommuniserer med den tekniske avdelingen, og hvordan de kommuniserer med hverandre i løpet av etterforskningen.

For å få en bedre forståelse om hvordan vi som elever kunne starte en risikoanalyse valgte vi å spørre dem om de kunne gi oss noen enkle skritt vi kunne begynt med.

**Hvilke tips hadde dere gitt oss i hvordan vi skal gå frem i en risikoanalyse?**
“Det er vanskelig å si hvor man skal begynne, siden vi ikke vet noe om selve nettsiden dere skal analysere, men en start er å vurdere hvordan nettsiden ser ut. Videre er det lurt å sette seg inn i nettsidens logginger, krypteringer, oppdateringsrutiner og tilganger.”

Siden vi vil ta i bruk en sikkerhetsstandard i risikoanalysen vår, og har bestemt oss for å ta i bruk NSM, ville vi likevel få deres mening om hvilken standard av ISO eller NSM som de mener er best å bruke i vårt tilfelle.

**Hvordan vil dere evaluere ISO versus NSM i forhold til en risikoanalyse?**
"ISO er en standardiseringsprosess og ikke en direkte sikkerhetsdannende prosess. Problemet med ISO er at det går ut på om du har bra dokumentasjon, som vil si at man kan dokumentere at man har god sikkerhet i *prinsipp* fordi man kan dokumentere for det, men det betyr ikke nødvendigvis at man har god sikkerhet i praksis”. Sier den ene sikkerhetseksperten. Han jobber med det mer tekniske innenfor cybersikkerhet. Videre forteller han, “NSM er litt mer faglig orientert, de har mer kunnskap om det de prater om, de har en grei standard, den er bra. Lur å bruke.”

Siden vi har som oppdrag å utføre en ROS-analyse for Tilt.work, valgte vi å spørre ekspertene hva de oppfatter som "dårlig praksis" i forhold til nettside design, som isteden for å interessere brukere, heller skremmer dem vekk fra å bruke nettsiden.

**Finnes det noen "synder" eller "No-No" handlinger som dere prøver å styre unna når det kommer til sikkerhet?**

"Ja, det er jo det. Det første man bør se på er om nettsiden har kryptert kommunikasjon eller HTTPS med gyldig dokumentasjon. Mistenkelige sider eller *phishing*-sider inneholder mange *buzz-words,* som *Vi er Agile!* For å få nettsiden til å se profesjonell ut er det viktig å unngå intetsigende tekst, samtidig som at nettsiden ikke spør om alt mulig rart for å få tillatelse for å samle inn data, derfor er det viktig å ikke samle inn data man ikke har behov for."

For å få en bedre forståelse av hvordan IT-sikkerhet oppfattes i praksis hos bedrifter, så ba vi dem beskrive deres erfaring med det.

**Hvordan har dere opplevd hvordan IT-sikkerhet blir sett på hos bedrifter? Er det hovedsakelig DevOps eller DevSecOps for eksempel?**

**"**Utviklingen går som regel veldig fort, og cybersikkerhet blir først tatt med inn i bilde etterpå." Videre beskriver de et kjent tilfelle for dem der de ofte blir dratt inn "kvart på tolv". De forklarer at ved flere anledninger blir sikkerhetsavdelingen kalt inn i kort tid, eller i deres beskrivelse "et kvarter" før utviklingsavdelingen skal presentere det de har produsert til ledelsen. "I slike tilfeller der de drar oss inn i siste liten for å godkjenne sikkerheten i produktet deres så hender det at vi må gripe inn og si ifra om at et program ikke er sikkert nok. Utfordringen med cyber security er at det er vanskelig å beregne tap og hvor mye man eventuelt har *tjent* på sikkerhet".

Videre forteller de om en hendelse som fant sted for et par år siden, og for å forholde oss til personvernsreglementet velger vi å videre-fortelle hendelsen deres vagt.

Sikkerhetsekspertene beskriver at de satt i et møte med ledelsen og hadde valget mellom å godkjenne eller avvise et forslag om en ny og revolusjonerende form for betaling. Flere andre konkurrenter hadde godkjent dette forslaget, og det var av stor interesse hos ledelsen å gjøre det samme. Likevel, viste intervjuobjektene våre skepsis til forslaget, mente det ikke

var sikkert nok enda å ta et slikt grep, avviste det, og satte en rekke krav til hva som skulle til for at forslaget kunne blitt godkjent ved senere anledning. Etter et par måneder med denne nye teknologien som andre konkurrenter valgte å ta i bruk var det store mengder av svindelangrep som ble rapportert, og sikkerhetsekspertene fikk i dette tilfelle virkelig kjenne på at de gjorde et positivt og riktig valg for bedriften, selv om at det var upopulært der og da.

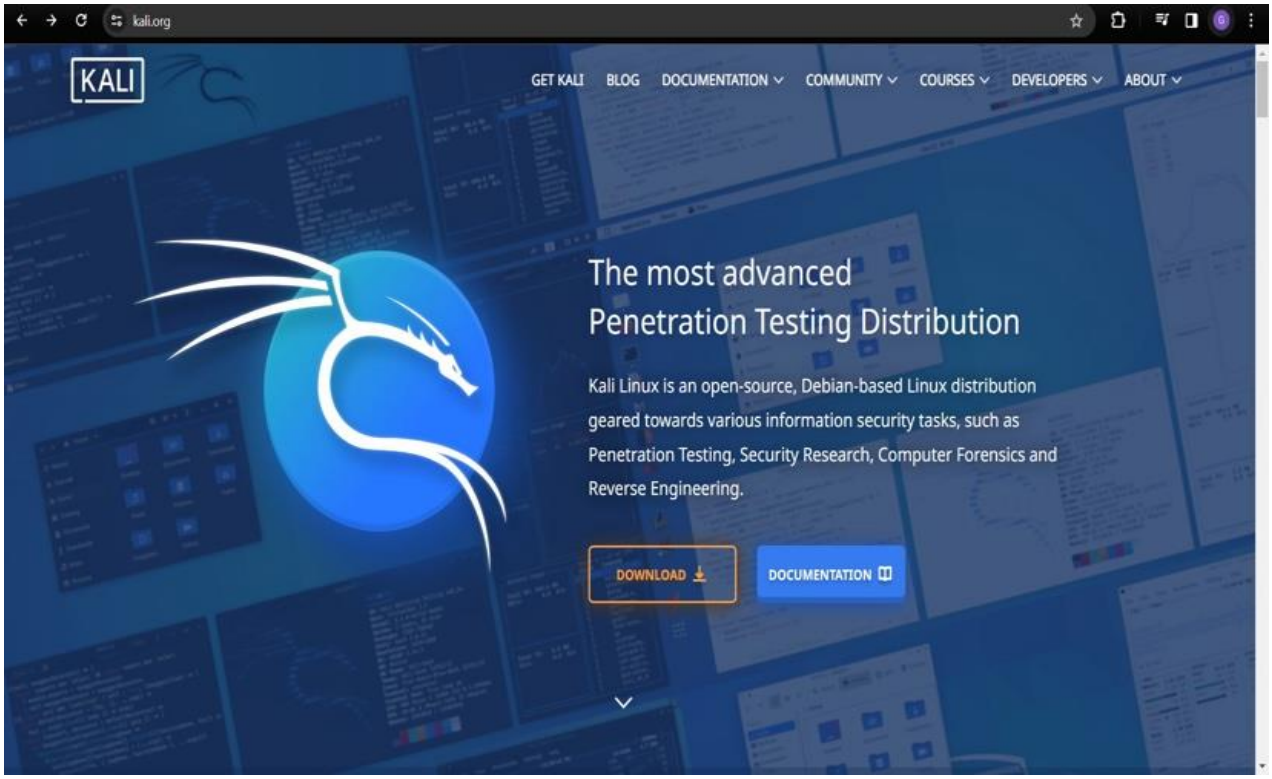
## 3.3 Oppsett og Installering av verktøy

Vi vil ta i bruk ulike verktøy for å gjennomføre ROS analyse på Tilt.work sine systemer. Verktøyet vil være behjelpelig med oppgaver som pentesting, sårbarhetsscanning og nettverksovervåkning, noe som vil være nyttig med å danne et helhetsbilde når det gjelder innsikt i systemene til Tilt.work sitt tekniske rammeverk og gi et eventuelt grunnlag til endringer.

### 3.3.1 Kali linux - Operativ system

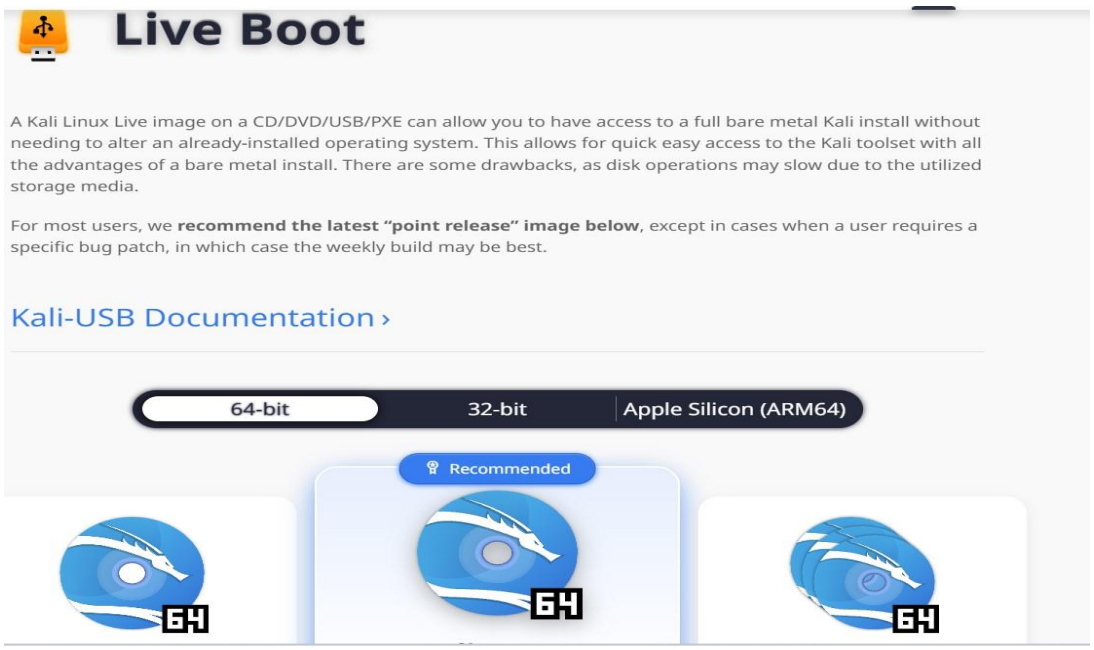
Ved installasjon av Kali Linux har vi fulgt flere steg: brukte en minnepenn som vi flashet en kali iso(operativsystem) for å kjøre en live boot på maskinen ved hjelp av et program som heter Balena.

Ved besøk av hovedsiden til www.kali.org fikk vi lastet ned versjonen vi trengte.




**Figur: 3.0 Kali landingsside**

På figuren ovenfor har vi et bilde av hovedsiden til Kali.org, det er her man laster ned operativsystemet og legger det over på en flashet minnepenn. På nettsiden har vi mulighet til å velge flere versjoner av systemet basert på formål og antall bit på operativsystemet maskinen vår er ment for. I gruppen sitt tilfelle har vi valgt å gå for "security" versjon på 64bit.




**Figur: 3.1 Kali nedlastningsside**

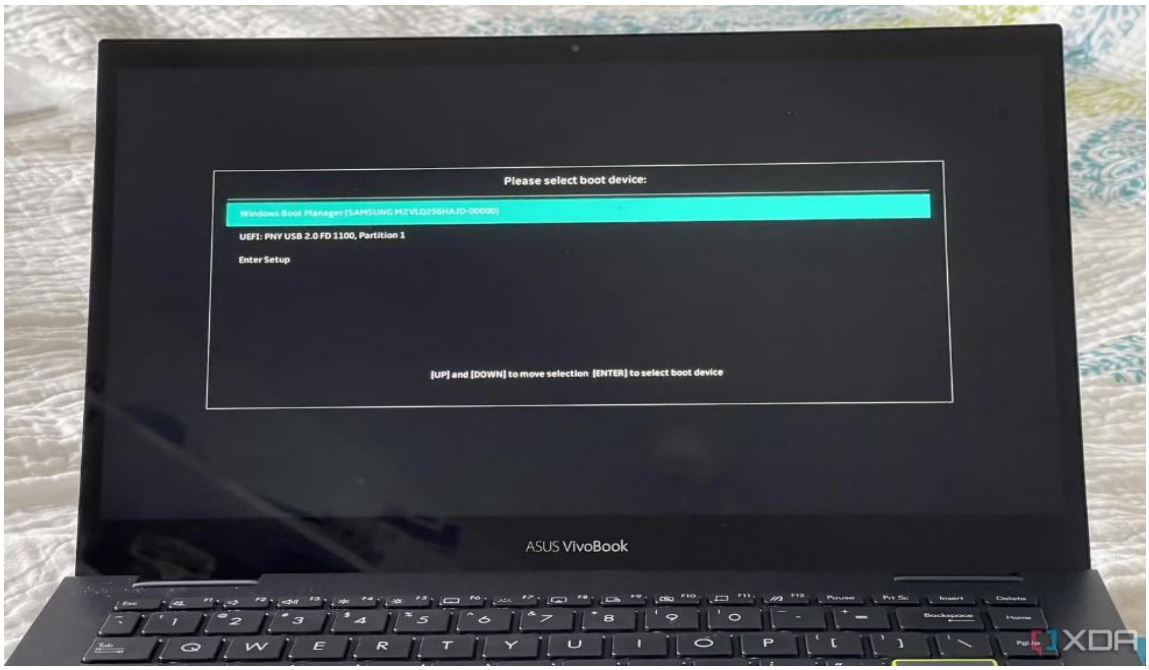
Ved installasjonen av kali, valgte vi å gå for liveboot delen, der vi først lastet det ned på en flashet USB minnepenn og bootet den i bios på datamaskinen. Kali linux er fast lagret på en USB-minnepenn som kan bootes på alle datamaskiner innad gruppen, dette vil være behjelpelig med å kjøre flere tester samtidig.

### 3.3.2 Balena

Balena brukes til å administrere programvare både på datamaskinen og på USB minnepenn. Programmet brukes til å formatere USB minnepennen til en boot device, altså at programvaren som installeres på den kan kjøres i bios på datamaskinen.

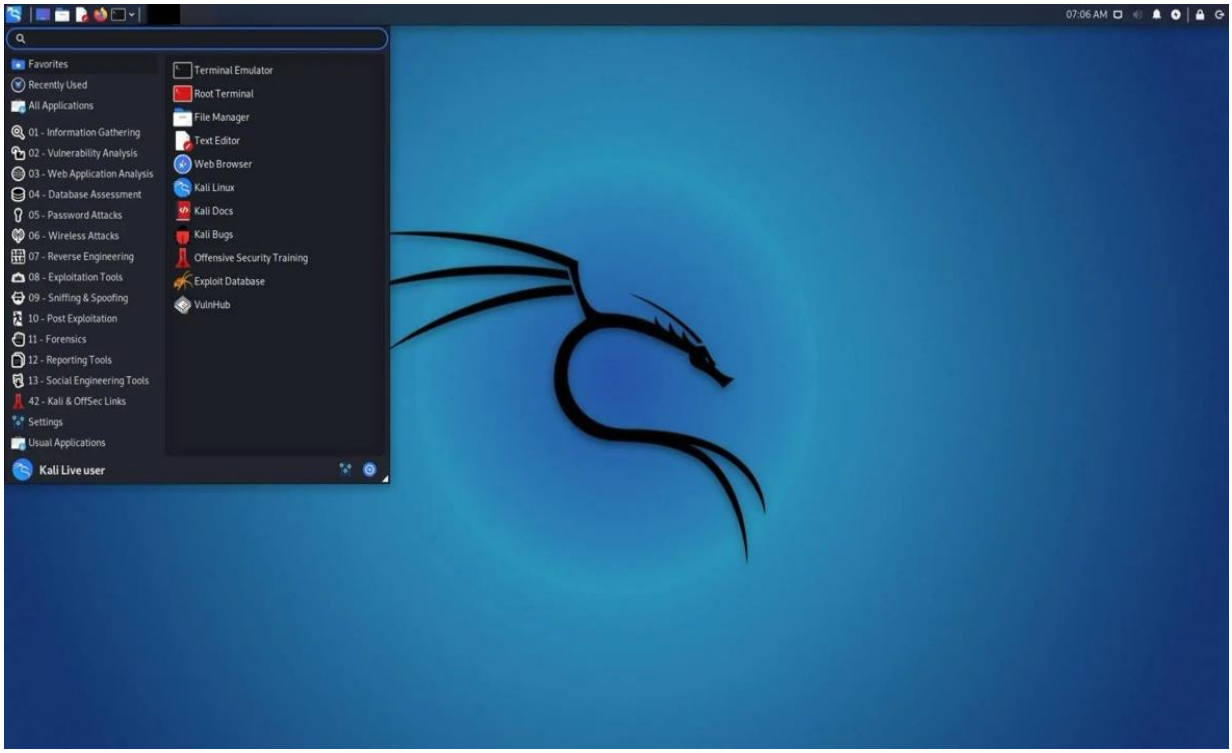
Ved videre fremgang

SKRU AV SECURE BOOT – for at kali skal kunne bootes som et operativsystem må vi først skru av secure boot i bios inne på datamaskinen.Secure boot er en sikkerhetsstandard i lagt i Windows datamaskiner for å sikre at det kun kjøres systemer som følger en sikkerhetsstandard og at ingen uautoriserte systemer skal få muligheten til å boote på datamaskinen. Ved fjerning av denne tjenesten vil det muliggjøres å boote flere operativsystemer på samme datamaskin.




**Figur: 3.2 Boot meny**

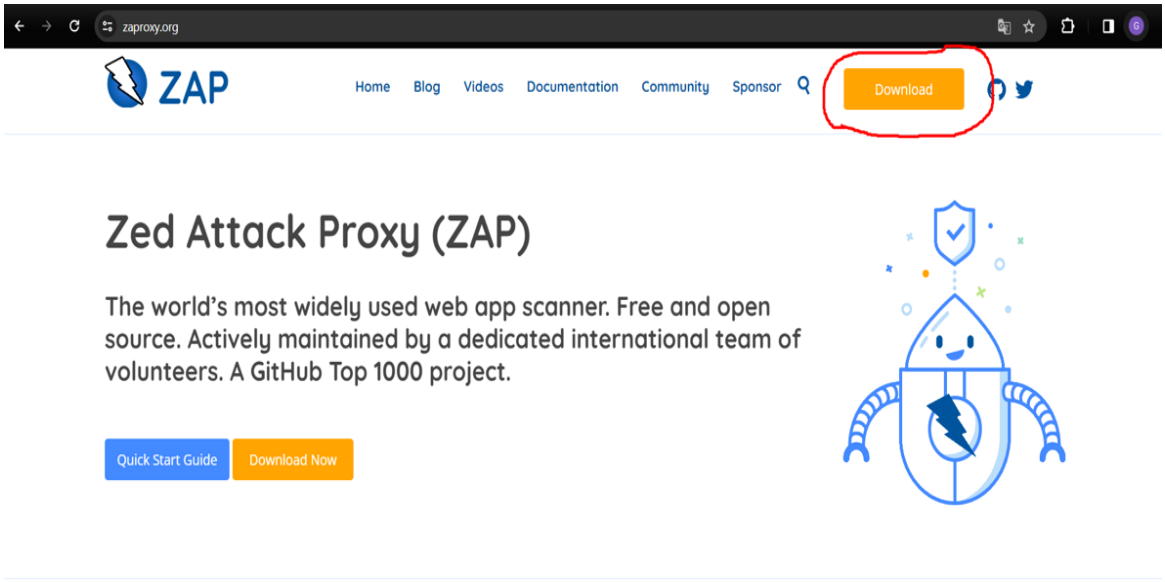
Ved oppstart av datamaskinen holder man F2 tasten for å komme inn i bios og velge operativsystemet en datamaskin skal kjøre på. I dette tilfellet velger vi Kali linux som skal starte opp og begynner med installasjon og oppsett, der vi får tilgang til oppsett av systemet med verktøy som trengs, etter at alt er ferdig installert kan vi begynne å bruke Kali.




**Figur: 3.3 Start meny Kali-linux**

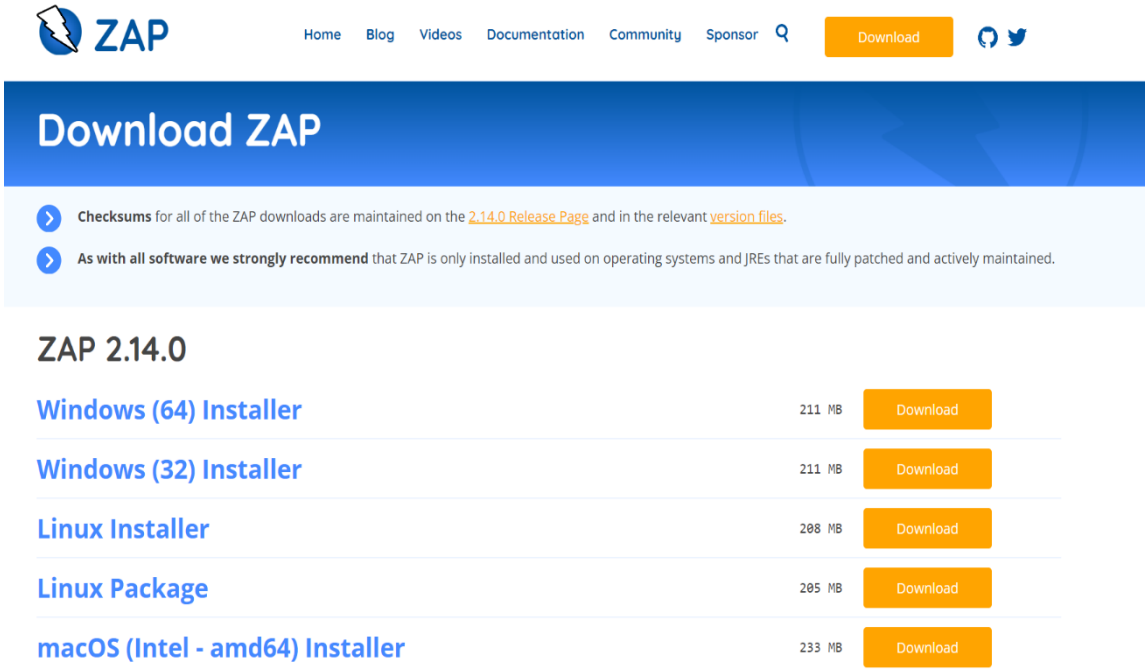
På figuren ovenfor ser vi ferdig oppsett og ferdig installering av operativsystemet samt alle pakkene som fulgte med Kali er klar til bruk til sikkerhetstesting av et gitt nettverk eller system. Til sikkerhetstesting vil vi bruke forhåndsinstallerte programmer som er ferdig installert på kali, dette involverer nmap, wpscan og metasploit.

### 3.3.3 ZAP




**Figur: 3.4 ZAP landingsside**

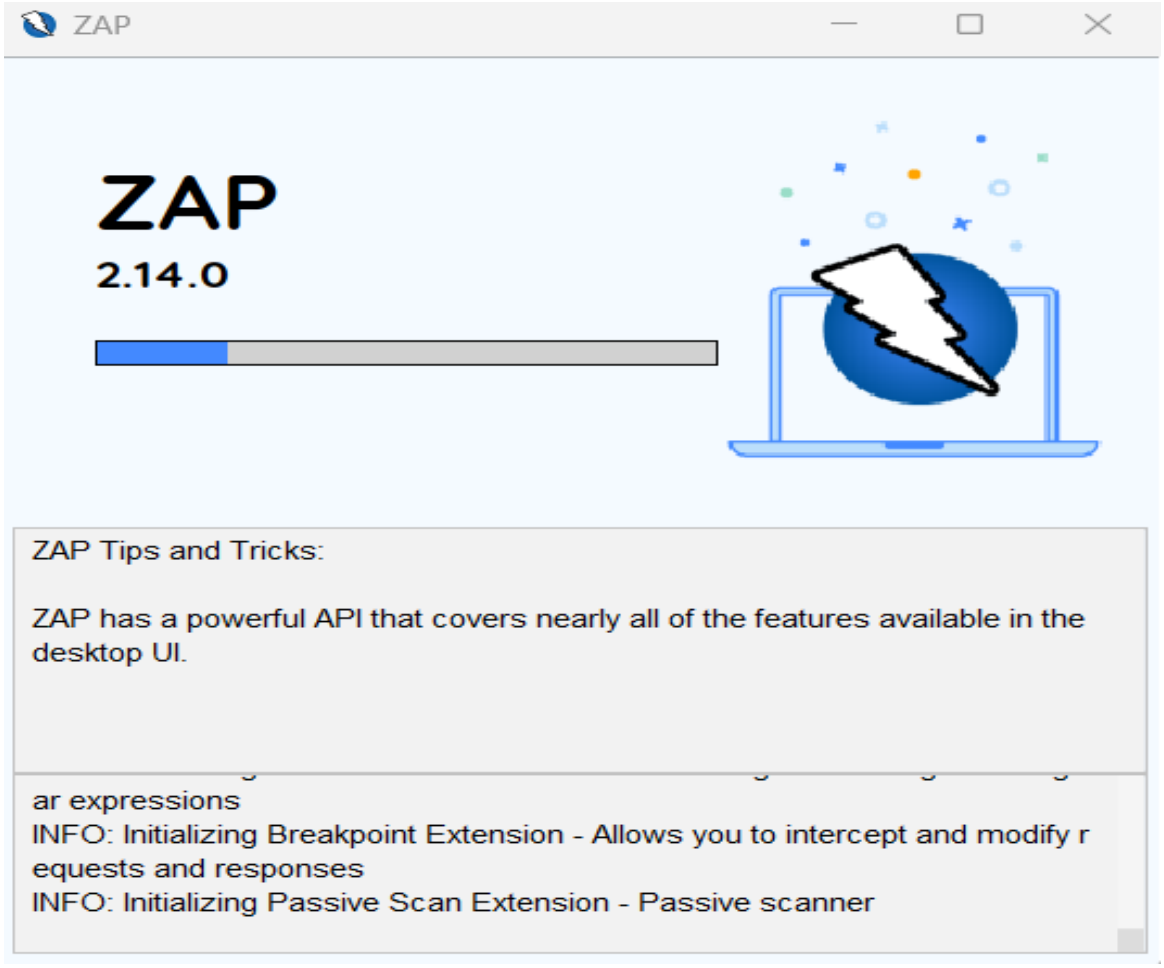
Under installasjon av Zap besøker vi først den offisielle nettsiden til ZAP og trykker på download. Vi får valg mulighet til å laste ned til ulike typer av programvaren avhengig av operativsystem og bit.




**Figur: 3.5 ZAP nedlastingsside**

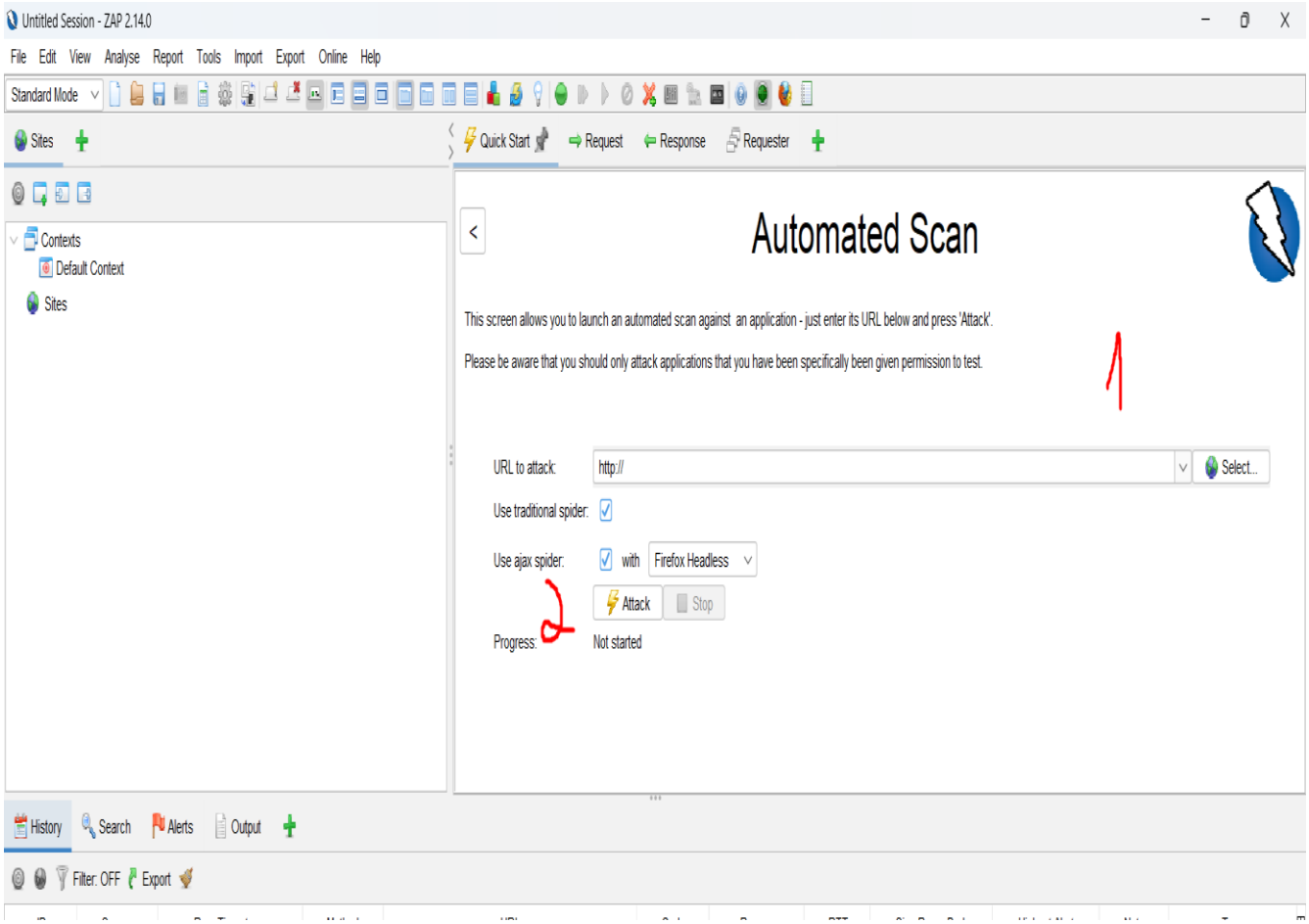
I vårt tilfelle laster vi ned Windows sin 64 bit versjon av programvaren, det er dog viktig å bemerke at maskinen trenger et Javamiljø (Java sitt offisielle programvare), forhåndsinstallert på datamaskinen.

På grunnlag av at ZAP er skrevet i Java og trenger det for å kjøre fordi den er komprimert til Java bytekode.




**Figur: 3.6 ZAP installasjonsvindu**

Når nedlastningen er ferdig vil programvaren sette i gang med installasjon på datamaskinen, der alle nødvendige pakker blir installert for å bruke datamaskinen sitt miljø.




**Figur: 3.7: Figuren ovenfor illustrerer fremgangsmåten for å utføre en scan i Zap.**

Nå holder det bare å lime inn lenken (URL) til nettsiden vi ønsker å utføre sikkerhetstest på og sette i gang.

### 3.3.4 Nmap

Nmap kommer forhåndsinstallert på Kali, men kan også lastes ned som en separat installasjon på Windows eller andre OS. Vi ser på det som at det er enklere å bruke det den nmap versjonen som er integrert i Kali for brukervennlighet. Integrert versjon av nmap lar oss forflytte IP-adresser direkte til penetreringsverktøy og samarbeider også med andre applikasjoner i sanntid.

Ved bruk av nmap får vi frem ulike datapakker sendt mellom host og nettverket, det vil også gi oss innblikk i trafikken / hvor de forskjellige pakkene lander og blir lagret hos målmaskinen.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap tilt.work
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 03:55 E
ST
Nmap scan report for tilt.work (172.67.176.24)
Host is up (0.0072s latency).
Other addresses for tilt.work (not scanned): 104.21.56.27 2606:4
700:3033::6815:381b 2606:4700:3032::ac43:b018
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds

┌──(kali㉿kali)-[~]
└─$ nmap tilt.work -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 03:56 E
ST
Nmap scan report for tilt.work (172.67.176.24)
Host is up (0.0072s latency).
Other addresses for tilt.work (not scanned): 104.21.56.27 2606:4700:3033::6815:381b 2606:4700:3032::ac43:b018
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.99 seconds
```

**Figur: 3.8 Terminal med nmap kommandoer**

For å finne IP adressen brukte vi Nmap – tilt.work.no der nmap utførte en scan og ga informasjon basert på det. Nmap scan report (172.67.176.24) altså

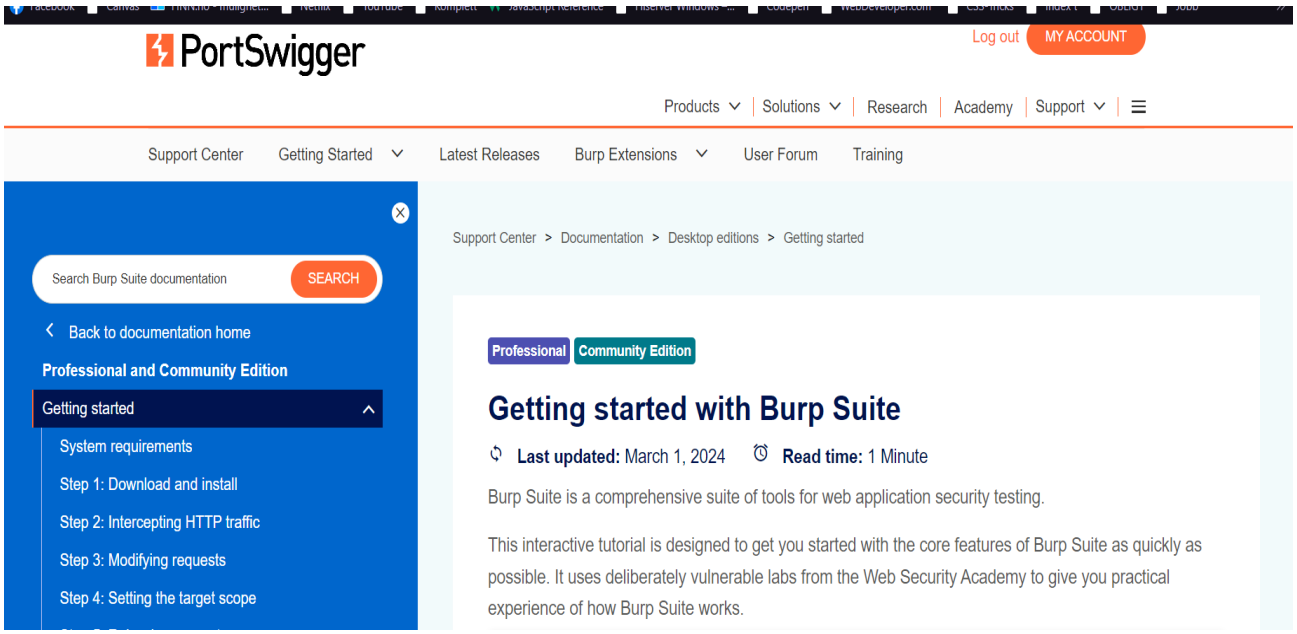
På bilde ovenfor har vi kjørt to nmap kommandoer som utførte en kort og et langt scann mot Tilt.work en for å se hvem porter som er åpen og en versjonssjekk.

På SV flagget ser man at de kjører cloudframe som versjon og at det er en HTTP Proxy.

### 3.3.5 Burp Suite

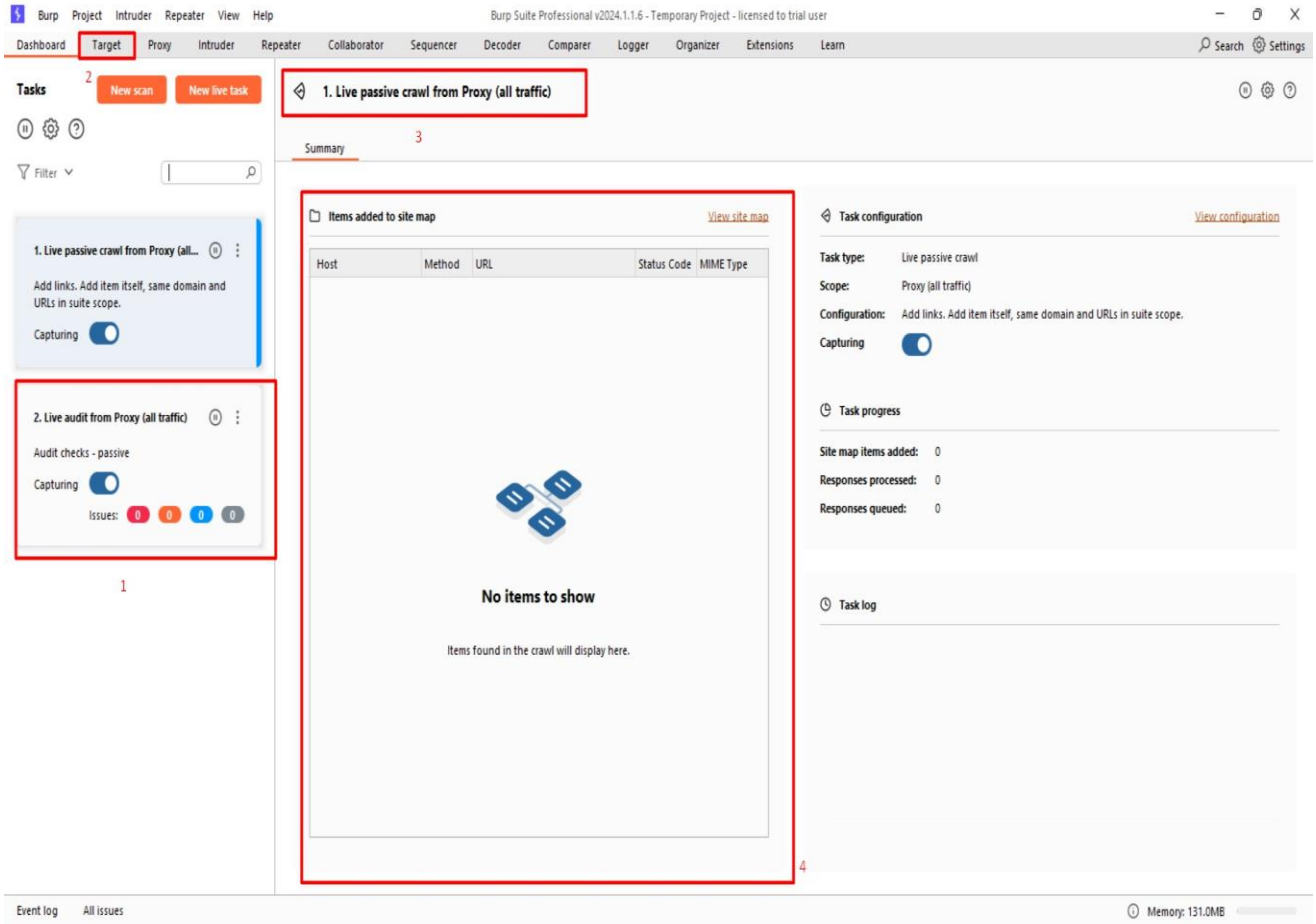
Den primære funksjonen til burp suite er å fungere som en Proxy-server til den nettsiden som blir sikkeretstestet, det vil si at den fanger opp, inspiserer og evaluerer rundt HTTPS trafikken mellom serverne og en spesifikk destinasjon. Samtidig vil den se etter hvordan target nettsiden vår (tilt.work.no) vil behandle slike forespørsler og hvordan den håndterer disse. Ved innblikk i hvordan en nettside håndterer forespørsler gir det fundament på risikoanalyse.

Burp suite tilbyr også en automatisk skanner, som ser etter relevante sikkerhetsutfordringer i nettsider, inkludert XSS, injeksjonssårbareter, feil i kildekode og generere en rapport basert på den informasjonen som den har fanget opp.




**Figur: 3.10 Port Swigger Burp Suite informasjonsside**

Ved førstegangsnedlastning av burp suite besøker vi portswigger.net og lager en bruker, etter en sendt forespørsel, vil vi få godkjenning og tilsendt innhold til nedlastning av burp suite. Det vil lastes ned og kjøres automatisk på datamaskinen, uten noen nødvendige forhåndsinstalleringer.




**Figur: 3.11 Burp Suite panelet**

Ovenfor har vi oppsett etter endt installasjon av Burp suite. Figuren er markert med røde bokser som er nummerert fra 1-4, dette er ment som en enklere forklaring for hva man kan utføre i verktøyet.

1. Live audit samler opp alle feil som den fanger opp under en scan, disse er rangert ut ifra risikograd og blir telt opp slik at det lettere kan holdes orden på antall feil det forekommer samt alvorlighetsgraden.
2. Target er det området hvor det limes inn URL til nettsiden man ønsker å teste.
3. I denne boksen velger man ut type crawl man ønsker å utføre, dette varierer mellom ulike kategorier og tidsbegrensninger. I vårt tilfelle har vi valgt å iverksette en passiv crawl.
4. I denne delen får vi opp all informasjonen som verktøyet fanger opp, med informasjon som plassering, type og risikograd. Det finnes også nøyaktig beskrivelse

av hver hendelse og en veiledning om hva som bør gjøres, noe som muliggjør en måte som er mer effektiv med tanke på danning av ROS analyse.

## 3.4 Risiko og sårbarhetsanalyse

### 3.4.1 Mal for analyse

Vi tar utgangspunkt i NSM sin risikoanalyse. Vi siterer Nasjonal sikkerhetsmyndighet under:

1. PLANLEGGING

- Sørg for å få ledelsesaksept
- Avgrens og sett et mål for arbeidet
- Identifiser hvilke relevante ressurser som er nødvendig
- Lag en plan for risikovurderingen med estimater og datoer

2. RISIKOVURDERING

- Identifisere hvilke IKT-systemer som skal vurderes
- Identifisere sårbarheter og eventuelle trusler
- Identifisere eksisterende sikkerhetsmekanismer
- Identifisere konsekvenser ved brudd på tilgjengelighet, integritet og konfidensialitet

3. RISIKOHÅNDTERING

- Lag en plan for oppfølging av risikoreduserende tiltak
- Vurdere effekten av sikkerhetstiltak ved bruk av styringsparameter (KPI).
- Vurder restrisikoaksept
- Involver ledelsen i beslutninger og oppfølging av risikotiltak

(Nasjonal sikkerhetsmyndighet, 2021, s.5).

Siden vi gjør en risikoanalyse med vekt på risikovurdering, dette fordi ordlyden til oppgaven fra Tilt.work gjør en helhetlig risikohåndteringsplan ikke like relevant, slik som beskrevet i siste punktet over. Vi skal derfor heller fokusere på planlegging og risikovurdering, samt fullføre det første punktet under risikohåndterings seksjonen som er å lage en plan for oppfølging av risikoreduserende tiltak.

For planlegging av selve analysen har vi kommet frem til følgende:

Med analysen ønsker vi å gi Tilt.work en oversikt over potensielle trusler for å gjøre de oppmerksomme på deres risikobilde, samt foreslå tiltak for å kunne øke deres robusthet. Målet er å identifisere de potensielle truslene for bedriften, og hva slags innvirkning disse potensielt kan ha.

Analysen vil bli gjennomført ved testing av ulike verktøy og virkemidler på deres systemer, og også gjennom intervjuer med ansatte og andre fagrelaterte personer. For å samle inn data vil vi fokusere på testing ved bruk av verktøy som Kali linux, intervjuer med ansatte og relaterte, samt bruk av generell informasjon om nettverkssikkerhet.

I analysen vil trusler og potensielle sårbarheter basere seg på informasjonen som har blitt samlet inn gjennom tester og annen datainnsamling. Resultatene vi kommer frem til vil brukes for å komme med risikoene og tiltakene for disse. Tiltakene vil inneholde anbefalinger om hva som bør gjøres med de ulike risikoene. Hvilken grad de ulike truslene vil falle under, med tanke på sannsynlighet for at truslene kan skje og for skaden truslene kan forårsake.

Gjennom denne planleggingsprosessen har vi bygget et godt fundament for videre arbeid med ROS-analysen i oppgaven og ved å følge planen forventer vi å oppnå gode resultater i vår analyse.

Nasjonal sikkerhetsmyndighet. (2021). *Risikovurdering av IKT-systemer*. (Første versjon). NSM. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

## 3.5 Rapportene

Vi skal i alt levere to rapporter til Tilt.work, der den første vil være en detaljert rapport, og den andre vil være en forenklet og lett forståelig versjon av den første rapporten. Nedenfor står det beskrevet om planleggingen av de to rapportene:

Generelt for begge rapportene har vi planlagt å lage den detaljerte rapporten først. Dette vil gi oss et godt utgangspunkt til å videre kunne skrive den forenklede rapporten.

### 3.5.1 Detaljert/utdypet rapport (Excel-arket)

Dette velger vi å referere til som *Excel-arket,* eller *Excel-malen*. Her skal alt vi finner være forklart på en detaljert og fagorientert måte. Sårbarhetene og avvikene i Tilt.work sine systemer vil bli listet nedover i forhold til alvorlighet, med spesifiserte tiltak til hvert avvik fra NSM sine grunnprinsipper for IKT-sikkerhet, og den nåværende sikkerhetssituasjonen hos Tilt.work vil bli forklart.  Da oppdragsgiver leser den forenklede utgaven vil de kunne få en mer komplisert og mer definitiv forklaring av punktene ved å slå opp i dette Excel-arket. Kort oppsummert skal dette være en fagorientert ROS analyse av Tilt.work sine systemer.

### 3.5.2 Forenklet rapport (Tilt.work rapport)

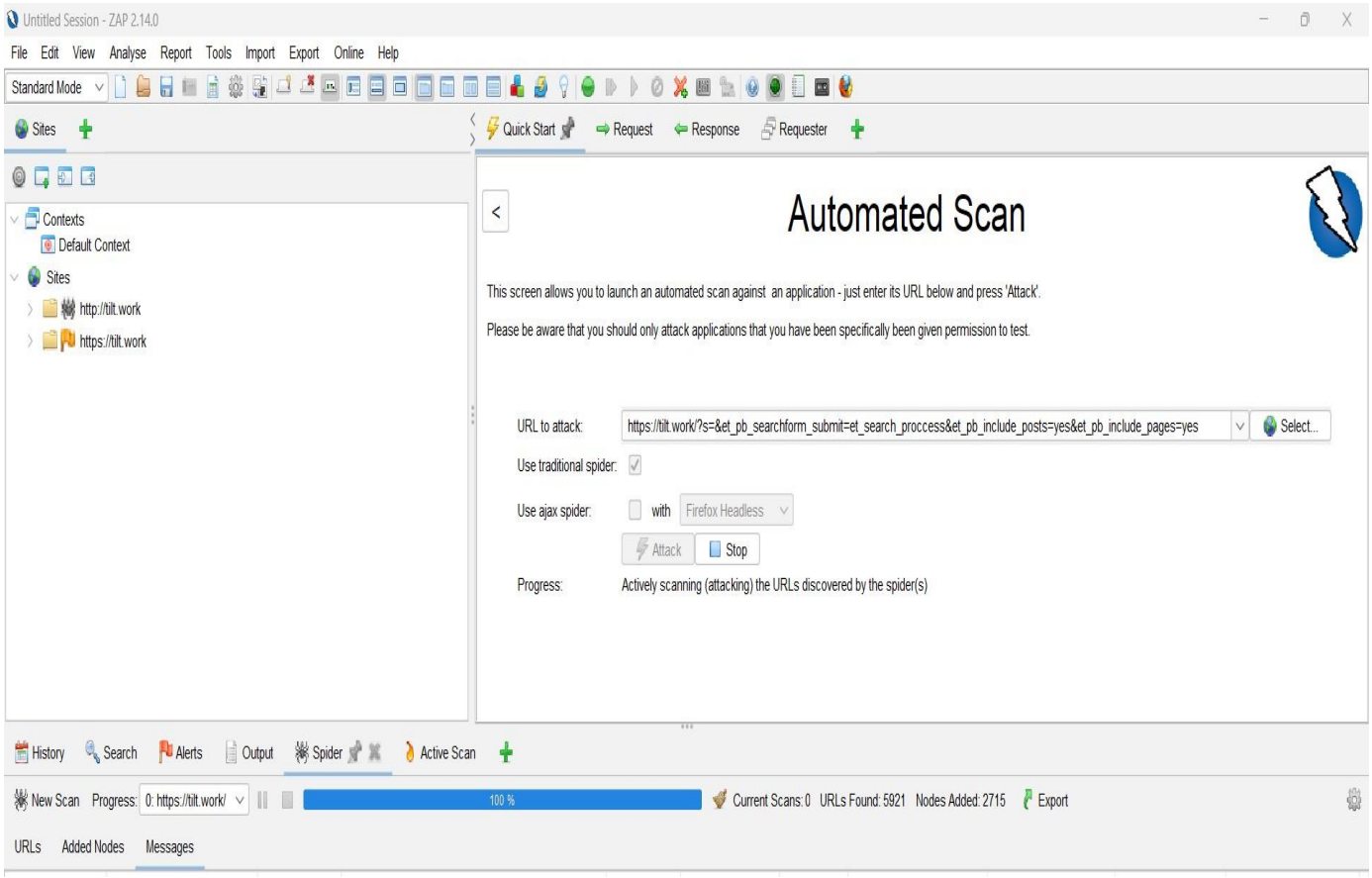
Denne rapporten vil være en forenklet versjon av Excel-arket. Hensikten med den forenklede rapporten vil være å gi en lettere forståelse samt oversikt over de potensielle problemene vi finner. Dette produktet vil ta utgangspunkt i at en person uten IT-utdanning skal klare å forstå funnene våre, tiltaksbeskrivelsene våre og konsekvensene som kan følge av forskjellige sårbarheter eller avvik. Denne rapporten vil kunne opptre som et hjelpemiddel for Tilt.work slik at de kan kunne ta for seg Excel-versjonen med den forenklede rapporten ved siden av, for å få en bedre forståelse av deres nåværende sikkerhetssituasjon. Rapporten vil hovedsakelig bestå av en punktliste av alle avvik og sårbarheter som er listet i Excel-arket, samt ha en mer detaljert og folkelig forklaring på konsekvensene som kan forekomme av disse. I tillegg er det også tiltak som er beskrevet på en ytterligere lettlest måte enn i Excel-arket.

# 4.0 Gjennomføring

I dette kapittelet vil selve hensikten til de forskjellige verktøyene som vi skal ta i bruk gjennom oppdraget vårt forklares. Altså hvordan vi skal gjennomføre oppgaven vår, finne og utforske sårbarheter og trusler, ved hjelp av verktøy.

## 4.1 Bruk av verktøy

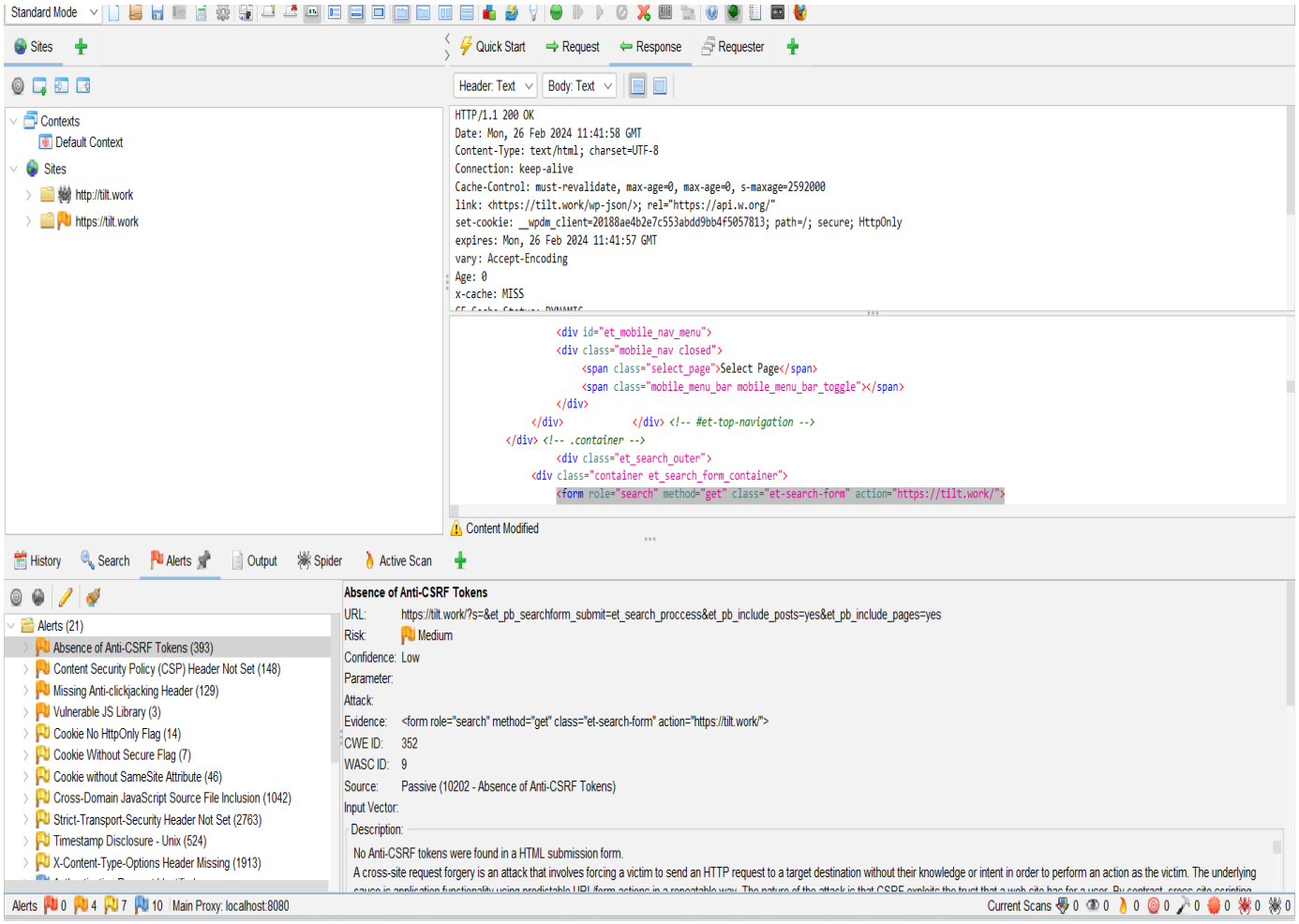
### 4.1.1 ZAP




**Figur: 4.0 ZAP panelet**

Når oppsettet til ZAP er ferdig og den har dannet et miljø på maskinen kan vi starte med å lime in URL-en til nettsiden vi ønsker en scann på, i dette tilfeller brukte vi Tilt.work sin hjemmeside og startet en web crawl. Dette førte i hovedsak til at ZAP avlyttet kommunikasjonen mellom Tilt.work og eksterne servere.

ZAP fikk også tilgang til source koden på Tilt.work sin hovedside og genererte en rapport på hva av kildekoden som har eventuell sårbarhet.




**Figur: 4.1 Fullført ZAP scann**

Etter fullført scann ser vi en konsoll samt “alerts” som ZAP klarte å fange opp fra hovedsiden til Tilt.work. Tilbakemeldingene har en alvorlighetsgrad som strekker seg fra grønn til rød. På bilde ovenfor ser vi at ZAP har fire oransje varsler og påtegnelser angående nettsiden og som den mener er noe mer alvorlig.

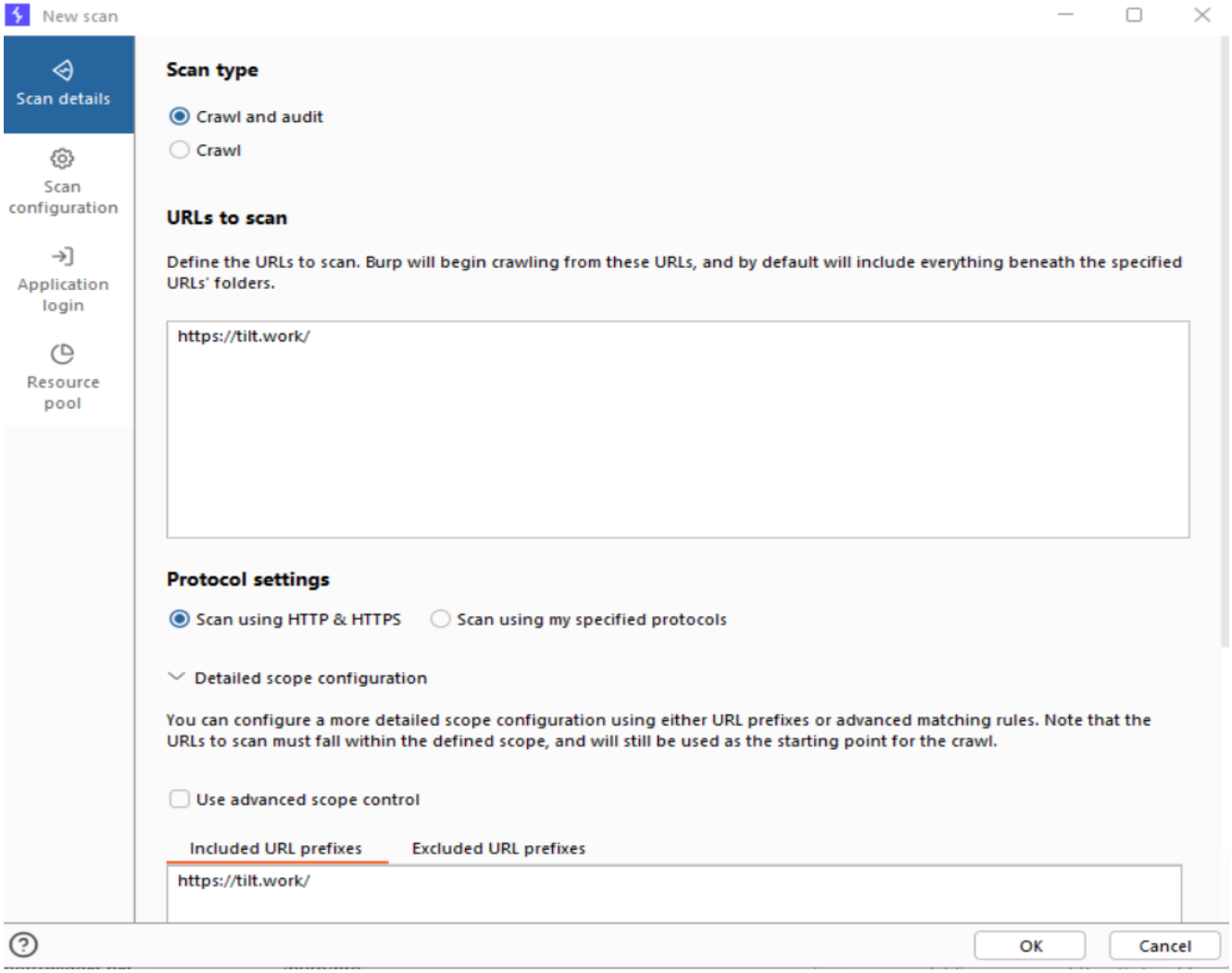
Øverste tilbakemeldingen påpeker at kildekoden til nettsiden ikke har en anti CSRF(Cross-site-request-forgery) tokens i HTML skjemaet sitt.

CSRF (Cross Site Request Forgery) er en type angrep som går ut på at angriper får offer-maskinen til å utføre handlinger på et nettsted der offeret har tilgang eller er logget inn på. Dette kan eksempelvis skje med en link som blir tilsendt offeret, mens hen er logget inn på en applikasjon. Ved åpning av linken vil angriperen kunne få tilgang til konfidensielt eller

personlig innhold og kunne kapre økten samtidig som angriperen tar over kontroll og kan utføre handlinger som brukeren ikke er klar over.

For å beskytte seg mot CSRF-angrep, er det nødvendig med en CSRF-token. En slik token vil sørge for at det legges til et unikt skjema til alle forespørsler og skjemaer på serveren en bruker benytter seg av.  En CSRF-token vil sammenligne informasjonen med tjenesten og serveren for å sørge for at all data som flyter gjennom er autentisk gitt av brukeren, og at ingen andre har mulighet til eller allerede har fått tilgang.

### 4.1.2 Burp Suite




**Figur: 4.2 Burp Suite panel**

På figuren ovenfor begynner vi å foreta en sikkeretsscan av Tilt.work sine nettsider det vil si hovedsiden samt alle artikler og koblinger som er relevant.  Burp Suite vil dermed starte en crawl som vil gå gjennom kildekode, sende forespørsler og vil generere en rapport på funn som ble oppdaget.

| Time | Source | Issue type | Host | Path | Insertion point | Severity | Confidence | Comme |
|---|---|---|---|---|---|---|---|---|
| 14:07:36 18 Mar 2024 | Task 5 | TLS certificate | https://tilt.work | / | | Information | Certain | |
| 14:07:36 18 Mar 2024 | Task 5 | Robots.txt file | https://tilt.work | /robots.txt | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Frameable response (potential Clickjacking) | https://tilt.work | / | | Information | Firm | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | / | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | / | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | /blog/2024/03/12/darwin-dating-og-damer-o... | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | /blog/2024/03/05/snyltekapitalismen/ | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | /blog/2024/02/26/farvel-til-alderismen-eldre-s... | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cross-domain script include | https://tilt.work | /project/rewired-to-relate-2/ | | Information | Certain | |
| 14:07:30 18 Mar 2024 | Task 5 | Cacheable HTTPS response | https://tilt.work | / | | Information | Certain | |
| 14:11:38 18 Mar 2024 | Task 5 | Backup file | https://tilt.work | /category-sitemap.xml | | Information | Certain | |
| 14:12:57 18 Mar 2024 | Task 5 | Backup file | https://tilt.work | /et_code_snippet_type-sitemap.xml | | Information | Certain | |
| 14:15:57 18 Mar 2024 | Task 5 | Backup file | https://tilt.work | /kompetanse-sitemap.xml | | Information | Certain | |

Advisory | Request 1 | Response 1 | Request 2 | Response 2 | Request 3 | Response 3 | Path to issue

**Frameable response (potential Clickjacking)**

Issue: **Frameable response (potential Clickjacking)**
Severity: **Information**
Confidence: **Firm**
Host: **https://tilt.work**
Path: **/**

**Issue detail**

This issue was found in multiple locations under the reported path.

**Issue background**

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking

**Figur: 4.3 Fullført webcrawl**

Etter en utført webcrawl ble det generert en rapport i Burp Suite, på bilde ovenfor var en av funnene en "*Frameable response (potential Clickjacking)*". Det betyr at nettsiden til Tilt. work ikke har tilstrekkelig med Content-Security-Policy (CSP). Det kan være en mulighet at en angriper vil legge over sitt eget grensesnitt ovenfor grensesnittet til nettsiden. Det tilsier at det opprinnelige grensesnittet til nettsiden blir overlappet og ser ekte ut, men angriperen

vil ha tilgang og se hvor brukeren trykker og hva de skriver inn. En slik hendelse fører til mulig avlytting av data og potensiell mulighet for å stjele informasjon.

Også omtalt som *click-jacking* er et slikt angrep ment til å få tilgang til sensitiv informasjon og avlytte brukerne, med en slik metode vil angriperen ha mulighet til å finne påloggingsinformasjon til ofrene, få tilgang til sensitiv informasjon og utføre handlinger som brukeren selv ikke ville gjort.

### *Forebygging*:

For å effektivt kunne forebygge angrep med *clickjacking* vil det være nødvendig at applikasjonen returnerer en respons header med navnet *X-frame* og verdien DENY for at innrammingen ikke skal være mulig. Dette tilintetgjør muligheten for at angriperen kan legge over sitt rammeverk over til nettsiden sin og få mulighet til å gjøre noen endringer.

Hver eneste nettside har et *iframe*-element i kildekoden sin, som er ansvarlig for innhold som vises til brukeren. X-frame header er en HTTP-respons header med formål om å oppdage om innholdet er eller kan bli innrammet av andre, det er i hovedsak to ulike verdier som settes i en slik header for å forebygge *clickjacking.*

**DENY:** Denne verdien vil sørge for at ingen del av nettsiden kan innrammes av andre og bli overlappet med et usynlig vindu som kan loggføre mus og tastaturklikk. Ved å sette "X-frame-options: "DENY" vil den returnere kun den sanne protokollen uten en mulighet for redigering.

**SAMEORIGIN:** Vil sørge for at *iframe*-elementet kun kan tilhøre den opprinnelige siden sin URL, med andre ord er det kun sider fra det samme domenet som kan bli innrammet, dette forebygger mot at eksterne nettsteder kan ha mulighet til å gjøre endringer.

Det er forventet at alle nettsider har en implementert *X-frame* i koden sin for å forebygge mot slike angrep.

### 4.1.3 WPScan

WPScan er et verktøy utviklet spesifikt for å teste sikkerheten til nettsider utviklet i wordpress. Verktøyet er designet til å oppdage sårbarheter ved å sammenligne disse opp mot offentlige databaser og finne avvik. WPScan vil gå inn i kildekoden og utvidelser for å identifisere potensielle trusler, dette inkluderer *brute-force* angrep for å evaluere sikkerheten rundt innloggingsinformasjon.

Wpscan vil også generere rapporter som gir detaljert informasjon med sårbarheter som ble oppdaget og potensielle trusler, samtidig som den vil gi en veiledning på hvordan man kan gå videre under løsning av disse.

```
___________________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___    ___  __ _ _ __   Â®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
___________________________________________________________________

[+] URL: https://tilt.work/ [172.67.176.24]
[+] Started: Thu Apr  4 16:03:40 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - cache-provider: CLOUDWAYS-CACHE-DE
 |  - cf-cache-status: DYNAMIC
 |  - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=k98RoWAx6Mk%2BddXbXETcy
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: cloudflare
 |  - cf-ray: 86f3e08edf6ab52d-OSL
 |  - alt-svc: h3=":443"; ma=86400
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://tilt.work/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://tilt.work/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 30%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
```

**Figur: 4.4 Terminal der WPScan har blitt kjørt**

På bilde ovenfor er det blitt utført et scann på hovedsiden til Tilt.work med potensielle sårbarheter som verktøyet har oppdaget.

```
[+] Headers
 | Interesting Entries:
 |  - cache-provider: CLOUDWAYS-CACHE-DE
 |  - cf-cache-status: DYNAMIC
 |  - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=BGtOIdQlvafKutflpY5KECU
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: cloudflare
 |  - cf-ray: 86f8a7ee1aebb518-OSL
 |  - alt-svc: h3=":443"; ma=86400
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://tilt.work/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://tilt.work/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 30%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://tilt.work/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] This site has 'Must Use Plugins': https://tilt.work/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] Registration is enabled: https://tilt.work/wp-login.php?action=register
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://tilt.work/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
```

**FIGUR: 4.5 Resultat av en aggressiv scann mot Tilt.work**

På bilde ovenfor har vi utført et aggressivt scann på URL-en til Tilt.work sine nettsteder. Her har det blitt printet generell informasjon samt sårbarheter som har blitt identifisert og som potensielt kan utnyttes.

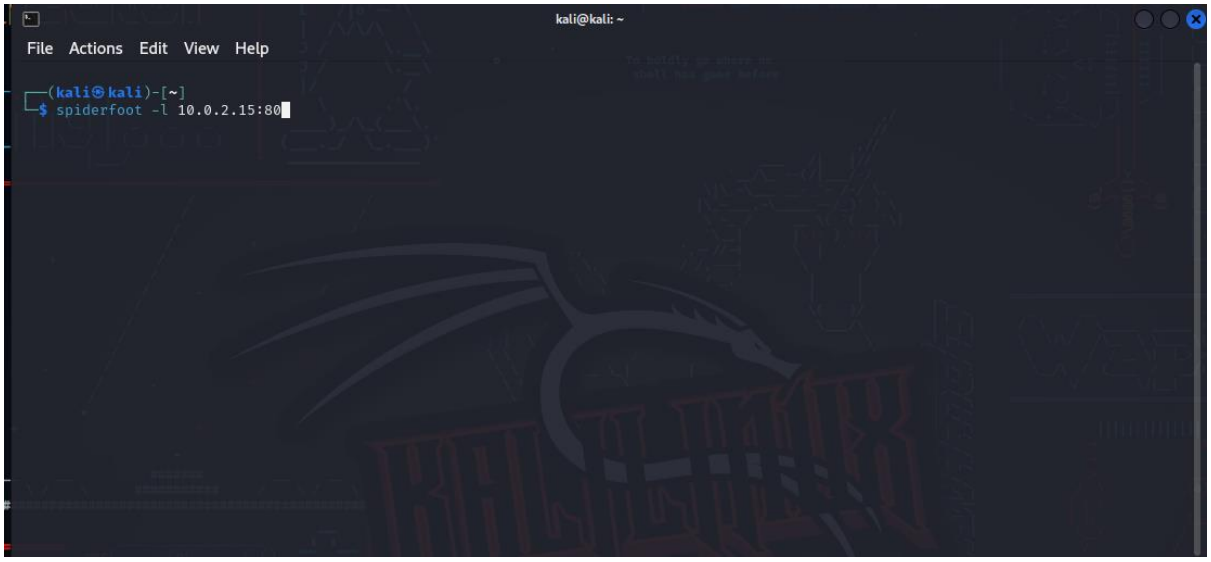
1. Cache og Cloudflare: Tilt.work bruker cloudflare for caching, noe som gir indikasjon på bruk av en tredjepartstjeneste.
2. Aktiverte funksjoner: Scanning avdekket av XML-RPC og registrering er aktivert, noe som kan bære potensielle risikoer.

**XML-RPC –** er en protokoll som tillater eksterne tjenester å sende forespørsler til wordpress-nettsteder. Denne protokollen brukes til flere oppgaver inkludert publisering av artikler og administrering av nettstedet. XML-RPC i seg selv er svært viktig for integrasjon med tredjeparts nettsteder, men bør deaktiveres for å redusere sjansen for angrep hvis denne funksjonen ikke brukes.

## Identifiserte sårbarheter

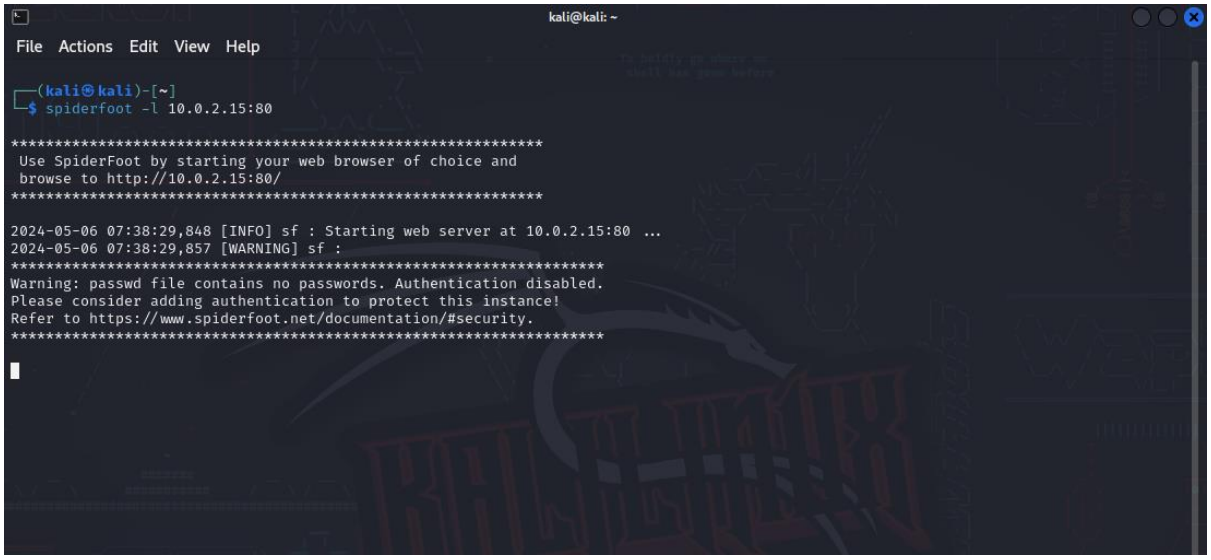
1. *Event ticket plugin*: En utdatert versjon av *event ticket plugi*n (versjon: 5.8.2), noe som kan muliggjøre stjeling av informasjon.
2. *Starbox Plugin*: Denne plugin'en ble funnet til å ha flere kjente sårbarheter inkludert, en mulighet for å lagre XSS og ha tilgang til uautoriserte brukerinnstillinger.
3. *Memberpress Download Plugin*: En utdatert versjon av *Memberpress plugi*n (versjon: 1.2.6) har blitt identifisert og omtalt med en kjent sårbarhet (CVE2024-0256). På grunn av utilstrekkelig filtrering av data åpner den en mulighet for XSS som gjør det mulig for personer med abonnement å legge inn filer, eller kode inn på nettsiden.

### 4.1.4 Spiderfoot



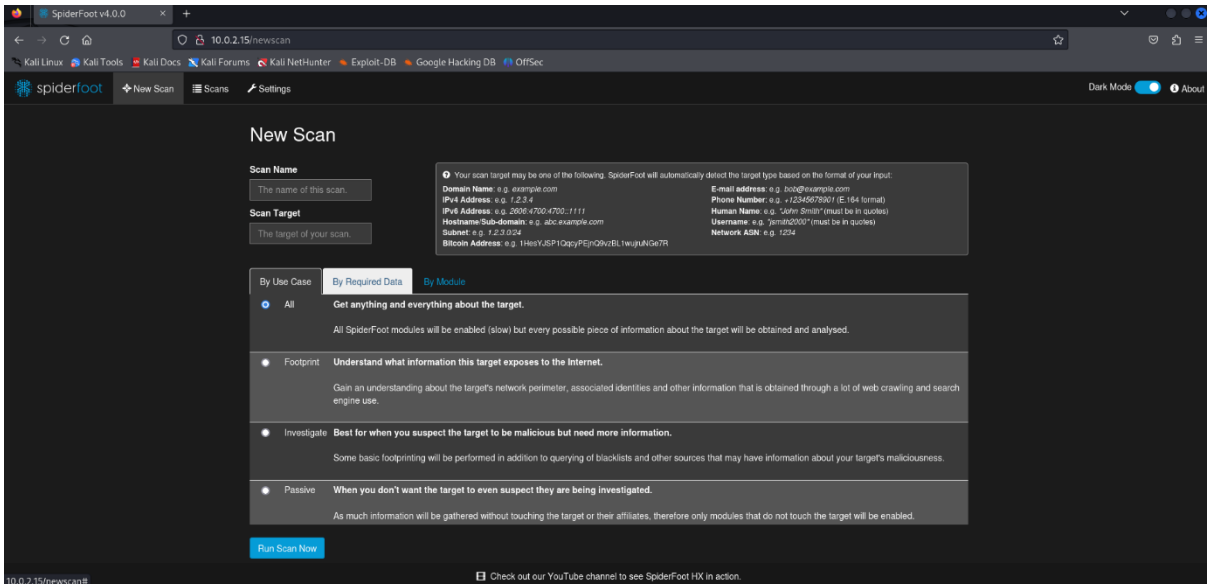

**FIGUR: 4.6 Terminal med kommando for å starte spiderfoot**

På bildet over så har vi skrevet inn kommandoen som starter opp spiderfoot med flagget "-l" som står for "listening". Dette gjør at spiderfoot nå kjører og lytter på en lokal IP adresse, 10.0.2.15 i dette tilfellet, på port 80.



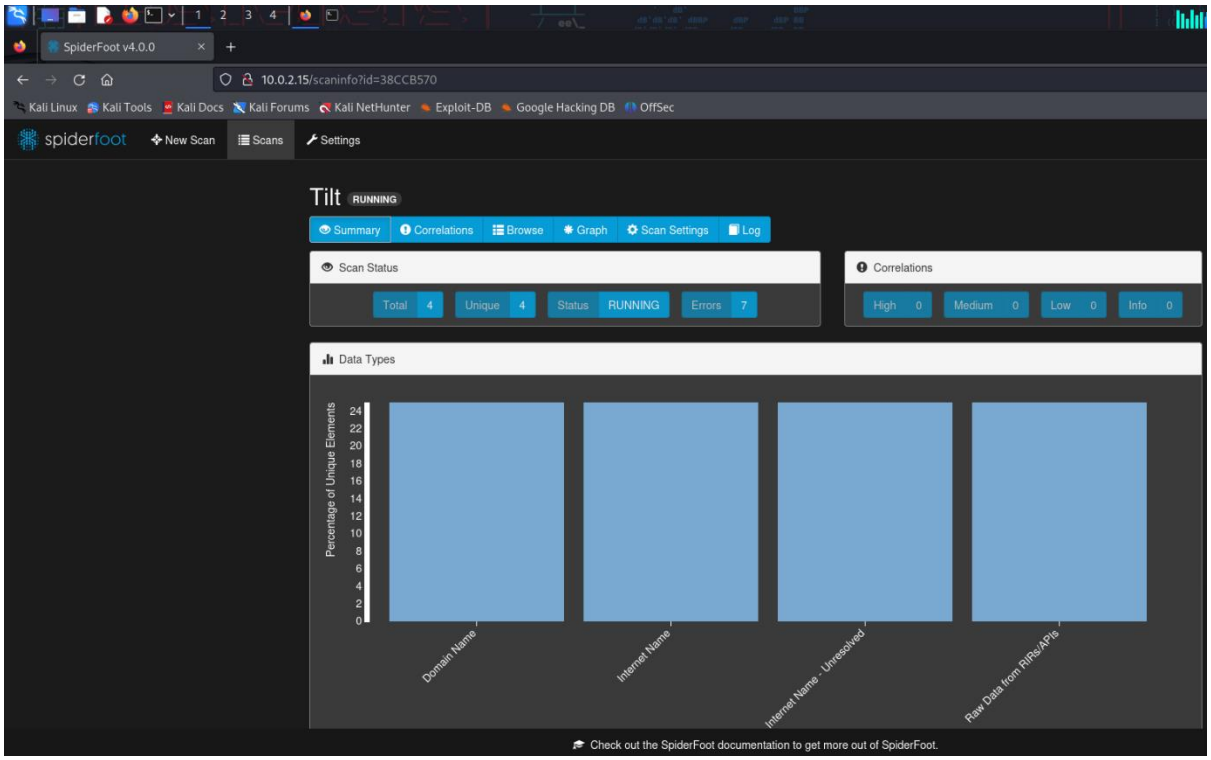

**Figur 4.7 Resultatet av å starte spiderfoot i terminalen**

På bildet over så ser vi resultatet av kommandoen spiderfoot –l 10.0.2.15:80. Her ser vi at programmet har startet uten problemer og at webserveren ligger på den tidligere nevnte adressen. Hvis vi ønsker å gå inn på denne så kan vi skrive inn denne adressen i en nettleser eller klikke på adressen i terminalen.



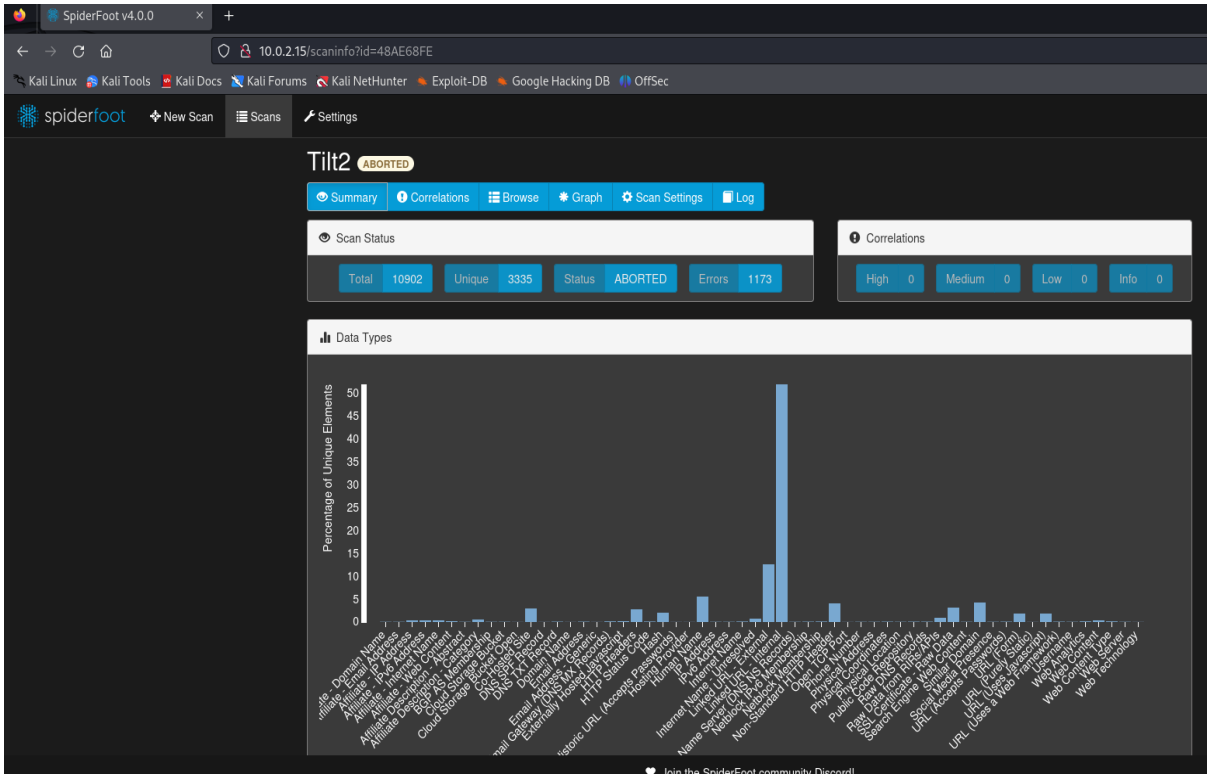

**Figur 4.8 Webgrensesnittet for Spiderfoot**

På bildet her så ser vi hvordan webgrensesnittet for Spiderfoot ser ut. Ved å gi en scann ett navn og så gi spiderfoot noe å søke etter, Tilt.work i dette tilfellet, og å bestemme hva slags scann vi vil gjøre, "All" i dette tilfellet, så kan vi klikke på "*Run Scan Now*" for å starte scannen.



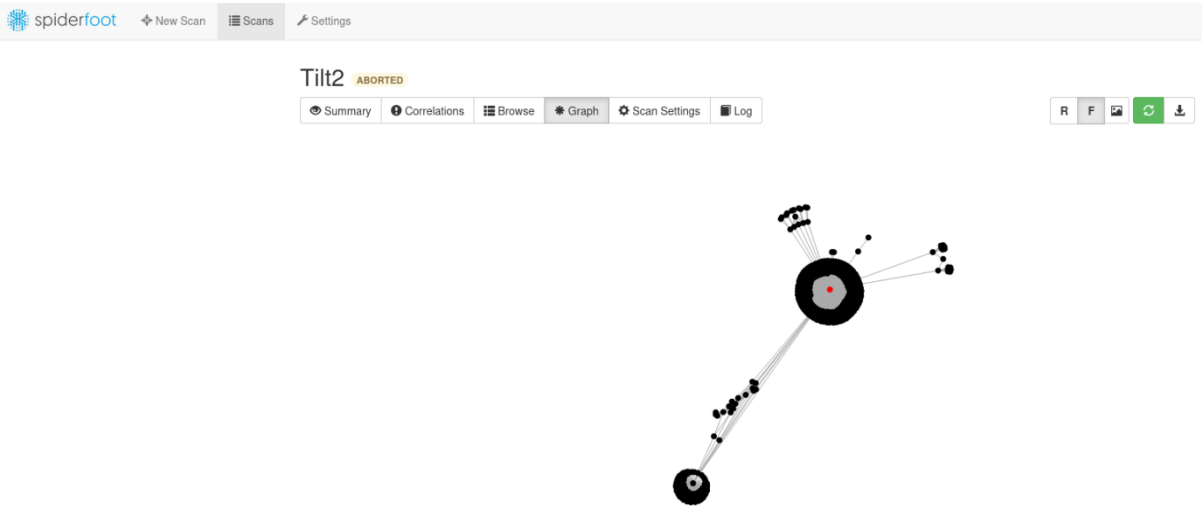

**Figur 4.9 Webgrensesnittet for et scann som er underveis**

Her ser vi hva som skjer når man har startet en scan, resultater triller inn og fyller opp dette stolpe diagrammet etter hvert som de blir funnet.



**Figur 4.10 Webgrensesnitt for et scann som er fullført**

Her ser vi resultatet av et scann som har gått over mange timer. Vi kan se at den har fått over 10000 treff og at alle disse datapunktene har blitt samlet inn i diagrammet over. Vi kan også bruke knappene over diagrammet for å endre visningen av disse datapunktene.




**Figur 4.11 Node-graf-representasjon av stolpediagrammet fra figur 4.10**

Her ser vi resultatet fra figur 4.10 representert i en in node-graf.

### 4.1.6 Nmap

**Figur 4.12 Resultat av ”nmap tilt.work”**

På bildet over så ser vi resultatet av å kjøre nmap verktøyet mot Tilt.work, her får vi tilbake at webserveren har 4 åpne porter: 80, 443, 8080 & 8443.

```
kali@kali: ~
File  Actions  Edit  View  Help
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds

┌──(kali㉿kali)-[~]
└─$ nmap tilt.work -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 08:05 EDT
Nmap scan report for tilt.work (104.21.56.27)
Host is up (0.012s latency).
Other addresses for tilt.work (not scanned): 172.67.176.24 2606:4700:3033::6815:381b 2606:4700:3032::ac43:b018
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.34 seconds

┌──(kali㉿kali)-[~]
└─$
```

**Figur 4.13 resultat av ”nmap Tilt.work -sV”**

På dette bildet ser vi resultatet av å kjøre nmap mot Tilt.work med “–sV” flagget som står for “*Service Version*” dette gir oss mer informasjon om tjenesteversjoner som kjøres på serveren. I bildet så finner vi slik ut at Tilt.work bruker “*cloudflare https proxy*”, noe som er nyttig å vite hvis man planlegger ett eventuelt angrep mot tjenesten.

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap tilt.work -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 07:23 EDT
Nmap scan report for tilt.work (104.21.56.27)
Host is up (0.0072s latency).
Other addresses for tilt.work (not scanned): 172.67.176.24 2606:4700:3033::6815:381b 2606:4700:3032::ac43:b018
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://tilt.work/
443/tcp  open  ssl/http Cloudflare http proxy
|_http-generator: WordPress 6.5.3
| ssl-cert: Subject: commonName=tilt.work
| Subject Alternative Name: DNS:tilt.work, DNS:*.tilt.work
| Not valid before: 2024-04-25T12:15:52
|_Not valid after:  2024-07-24T12:15:51
|_http-title: tilt.work - tilt.work
|_http-server-header: cloudflare
8080/tcp open  http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://tilt.work/
8443/tcp open  ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=tilt.work
| Subject Alternative Name: DNS:tilt.work, DNS:*.tilt.work
| Not valid before: 2024-04-25T12:15:52
|_Not valid after:  2024-07-24T12:15:51

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.66 seconds
```

**Figur 4.14 Resultat av ”nmap Tilt.work -A”**

På figuren over så ser vi resultatet av en aggressiv scann som gir oss enda mer informasjon som kan komme godt med for eventuelle angrep. Dette gjøres med flagget “–A".

```
┌──(kali㉿kali)-[~]
└─$ nmap 65.21.4.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 08:12 EDT
Nmap scan report for static.5.4.21.65.clients.your-server.de (65.21.4.5)
Host is up (0.022s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```

**Figur 4.15 Resultat av ”nmap 65.21.4.5”**

Her ser vi en nmap scann av backup-serveren til Tilt.work, her kan vi se at port 22 er åpen. Port 22 er verdt å merke seg siden den ofte blir brukt som inngangsport for skadevare hvis den ikke er sikret tilstrekkelig.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap 65.21.4.5 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 08:27 EDT
Nmap scan report for static.5.4.21.65.clients.your-server.de (65.21.4.5)
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 cb:a4:6a:a6:6b:66:d6:91:86:6b:9f:06:63:80:b7:4e (ECDSA)
|_  256 bc:3b:73:06:32:5d:51:16:61:77:c3:07:4d:16:83:4f (ED25519)
80/tcp  open  http     Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
443/tcp open  ssl/http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| ssl-cert: Subject: commonName=TRAEFIK DEFAULT CERT
| Subject Alternative Name: DNS:28bd3cd1847c064559d1daf1a875e1cb.359e4cbd4fd7f4de33c9b7575e0b7336.traefik.default
| Not valid before: 2024-03-26T20:42:28
|_Not valid after:  2025-03-26T20:42:28
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.71 seconds
```

**Figur 4.16 Resultat av ”nmap 65.21.4.5 -A”**

Figuren ovenfor viser et aggressivt scann av backup serveren, her ser vi videre att vi finner¨¨ noe mer informasjon på port 22 som for eksempel *SSH-host* nøkkelen og hvilken Debian-versjon som serveren kjører, begge deler er informasjon som kan være veldig nyttig for å planlegge et angrep mot tjenesten.

# 5.0 Resultater

Dette kapittelet inneholder resultatene vi har fått etter gjennomføringen av ROS-analysen vår og risikovurdering av IKT-systemene til Tilt.work.

## 5.1 Endelig ROS analyse

Vedlagt med denne hovedrapporten så ligger et Excel-dokument med tittelen "NSM Risikovurdering av IKT-systemer for Tilt.work". I dette Excel-dokumentet så har vi gått gjennom NSM sin anbefalte metode for gjennomføring av risikovurderinger for mindre bedrifter, steg for steg.

NSM sin Excel-mal for risikovurdering inneholder 118 sikkerhetstiltak for vurdering. Siden Tilt.work er en mindre virksomhet ser vi oss nødt til å avgrense dette etter NSM sin anbefaling som er skrevet som følger, "Samtlige 118 sikkerhetstiltak er med i regnearkverktøyet. For mindre IKT-systemer og/eller anlegg kan listen med *prioritet 1* og *prioritet 2* sikkerhetstiltak anvendes. Dette vil medføre at risikovurdering gjøres mot 35 tiltak i stedet for alle 118." Dette vil gi oss mulighet for å fokusere på de absolutt viktigste temaene innenfor risikovurdering av Tilt.work sine systemer, samt gi oss mer tid til å fokusere på disse.

I denne hovedrapporten vil vi gå gjennom noen av hovedpoengene som vi fant da vi gjennomførte risikovurderingsdelen av denne prosessen.

Av de 35 tiltakene som NSM anbefaler at man tester for mindre bedrifter så oppfyller i dag Tilt.work 5 av dem i høy grad, 8 av dem i moderat grad og 19 av dem i liten grad. 3 av tiltakene fant vi til å ikke være relevante for Tilt.work sin nåværende situasjon.

Tiltakene som Tilt.work oppfylte i høy grad var tiltak **2.1.2**, **2.3.7**, **2.2.2**, **2.7.2** og **2.10.2**. **2.1.2** Omhandler *"kjøp av moderne og oppdatert maskin- og programvare."* (Nasjonal sikkerhetsmyndighet, 2020 s.18). Dette var et relativt enkelt tiltak å sjekke ettersom

dokumentasjonen som har blitt laget av Tilt.work ga oss en god oversikt over de programmene de har kjøpt og bruker i Tilt.work.

**2.3.7** Omhandler *"endring av alle standardpassord på IKT-produktene før produksjonssetting."* (Nasjonal sikkerhetsmyndighet, 2020 s.25). Igjen så ser vi av dokumentasjonen at alle passord som vi har tilgang til er endret og etter å ha sendt en epost til Eddy (Edgaras) så fikk vi dette bekreftet. Passordene som brukes av selskapet er både endret og meget sikre. Vi gjorde også noen bruteforce angrep med hjelp av rockyou ordlisten ved hjelp av WPScan verktøyet noe som ikke ga noe resultat.

**2.2.2** Omhandler *"bygging av IKT-systemer med IKT-produkter som fungerer godt sammen sikkerhetsmessig."* (Nasjonal sikkerhetsmyndighet, 2020 s.22). Med de tilgangene vi har fått så har vi tilgang til admin panelet i Tilt.work. Her ser vi at det som kjøres av plugins på nettstedet fungere fint sammen og det ikke ser ut til å være noen store hull som må plugges her. Vi ser også av dokumentasjonen vi har fått at de tredjepartstjenestene som de bruker fungerer godt sammen.

**2.7.2** Omhandler *"aktivering kryptering i de tjenestene som tilbyr slik funksjonalitet."* (Nasjonal sikkerhetsmyndighet, 2020 s.32). Gjennom kommunikasjon med Eddy og dokumentasjonen han har skrevet så er det klart at det som kan krypteres er kryptert i Tilt.work.

**2.10.2** Omhandler *"Involver nødvendig IKT-sikkerhetspersonell i forbindelse med endringer."* (Nasjonal sikkerhetsmyndighet, 2020 s.36). Edy har vært en aktiv deltaker i arbeidet der hvor det har vært relevant, derfor er dette tiltaket oppfylt i høy grad.

Tiltakene som Tilt.work oppfylte til moderat grad var tiltak **1.2.4**, **2.3.3**, **2.9.1**, **1.3.3**, **2.1.1**, **2.2.1**, **2.6.2** og **2.6.3**.

**1.2.4** Omhandler *"kartlegging av programvare i bruk i virksomheten."* (Nasjonal sikkerhetsmyndighet, 2020 s.15). Dette tiltaket oppfyller Tilt.work relativt godt på ett av

underpunktene, men veldig lite på de andre punktene. De har i dag relativt god kontroll over alt av programmer som kjøres på Tilt.work sin nettside og de serverne som de leier, men det er ingen kontroll over de enhetene som brukes for å få tilgang til de sensitive dataene og områdene knyttet til Tilt.work siden Tilt i dag har et BYOD(Bring Your Own Device) system.

**2.3.3** Omhandler *"deaktivering av unødvendig funksjonalitet."* (Nasjonal sikkerhetsmyndighet, 2020 s.24). Vi fant flere inaktive men fremdeles sårbare plugins i admin panelet til WP siden til Tilt.work. Ved hjelp av WPScan så fant vi fram til 2 konkrete svakheter som var knyttet til disse plugins'ene som kan brukes av en TA ved et eventuelt angrep. Derimot så fant vi veldig lite overflødig programvare de andre stedene i systemene deres som vi har fått tilgang til.

**2.9.1** Omhandler *"at man skal legge en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata."* (Nasjonal sikkerhetsmyndighet, 2020 s.35). Tilt.work har i dag det vi vil betegne som en særdeles god sikkerhetskopieringsordning for en bedrift på deres størrelse. De har gode systemer og rutiner for sikkerhetskopier som lagres i ett år per dags dato, med mulighet for å utvide disse til enda lengre hvis de ønsker dette, noe vi anbefaler at de ser på å gjøre ettersom noe skadevare kan ha lengre inkubasjonstid enn ett år.

**1.3.3** Omhandler *"kartlegging av ansvar og roller spesielt knyttet til IKT-sikkerhet."* (Nasjonal sikkerhetsmyndighet, 2020 s.16). Selv om dette ikke er skrevet ned fast noe sted så er arbeidsfordelingen i Tilt.work slik at det egentlig kun er Edy som er teknikeren deres og derfor er det mest logisk at han sitter med mesteparten av ansvaret og rollene i henhold til IKT-sikkerhet.

**2.1.1** Omhandler "*Integrering av sikkerhet i virksomhetens prosess for anskaffelser."* (Nasjonal sikkerhetsmyndighet, 2020 s.18). Vi ser at Tilt.work har brukt det som kan ansees som "bransjestandarder" og "de vanligste" tjenestene der de har måttet hente inn tjenester og kode utenifra. Ettersom mange av disse er så allestedsnærværende blandt kunder som setter opp nettsider som Tilt.work har gjort så er det i grunn ganske gode sikkerhets rutiner innebakt i disse løsningene. Men vi har funnet ett par hull som kan fikses på selv om disse løsningene er såpass vanlige.

Tiltakene som Tilt.work oppfylte til liten grad var tiltak **1.2.3**, **2.1.9**, **2.2.3**, **2.3.1**, **2.3.2**, **2.6.4**, **2.6.5**, **3.2.3**, **3.2.4**, **4.1.1**, **2.6.1**, **2.6.6**, **2.6.7**, **2.8.4**, **2.9.3**, **3.1.1**, **3.1.3**, **3.2.5** og **4.1.3**.

**1.2.3** Omhandler *"kartlegging av enheter i bruk i virksomheten."* (Nasjonal sikkerhetsmyndighet, 2020 s.14). I dagens BYOD system så er det ingen kontroll over hvilke enheter som blir gitt tilgang (login info) til Tilt.work sin WP-side. Dette åpner opp mulige angrepsvektorer for utenforstående inntrengere via ellers pålitelige enheter.

**2.1.9** Omhandler *"å ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting."* (Nasjonal sikkerhetsmyndighet, 2020 s.19). Grunnet størrelsen til selskapet så har de relativt små muligheter for å utvikle effektive og sikre løsninger internt, noe som gjør at de henter alle sine tjenester fra andre leverandører som blant annet WordPress, Stripe, Fiken og Cloudflare. Vi ser ikke noen tegn på at det er blitt gjort noen umiddelbare tanker om sikkerheten til de tjenestene de har valgt å bruke. Noen ideer om hvilke sikkerhetsløsninger som er viktige for Tilt.work burde noteres så alle involverte er innforstått med disse.

**2.2.3** Omhandler "*oppdeling av virksomhetens nettverk etter virksomhetens risikoprofil."* (Nasjonal sikkerhetsmyndighet, 2020 s.22). På kontoret så sitter Tilt.work på ett delt nettverk med alle andre leietakere av kontorlokaler på SoCentral. Der er det ingen segmentering som kan diskuteres. Alle 4 hovedansatte på WP har alle de samme administrasjonstilgangene, noe som antagelig ikke er nødvendig. Men på en annen side så ser vi at brukerne av tjenesten deres får ikke administrasjonstilgang, noe som følger bransjestandard.

**2.3.1** Omhandler "*etablering et sentralt styrt regime for sikkerhetsoppdatering."* (Nasjonal sikkerhetsmyndighet, 2020 s.24). Det er ingen overordnet regime for dette, selskapet har flere forskjellige regimer for hvor og når ting oppdateres. Det vil være lurt å samkjøre disse for å lettere holde oversikt over hva som oppdateres og når.

**2.3.2** Omhandler "*konfigurering av klienter slik at kun kjent programvare kjører på dem."* (Nasjonal sikkerhetsmyndighet, 2020 s.24). I dagens BYOD system så er dette tiltaket ikke oppfylt på noen av underpunktene til tiltaket ettersom det ikke er gjennomført noe som helst kontroll over hvilke programvarer som kjøres på klientene som får tilgang til Tilt.work sin backend.

Nasjonal sikkerhetsmyndighet. [15.4.2020]. Grunnprinsipper for IKT-sikkerhet. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

## 5.2 Risiko vurdering av IKT systemer

Ved oppsett av risikovurdering av systemene til Tilt.work har gruppen benyttet seg av en mal som er satt opp av NSM. Risikovurderingen baserer seg på flere steg som innebærer grundig planlegging og gjennomføring.

| Risikovurdering av IKT-system<br>Planlegging | | |
|---|---|---|
| Virksomhet | Tilt Work AS | |
| IKT-system | tilt.work | |
| Dato | 26.02.2024 | |

| ID | Beskrivelse av aktiviteter og milepæler | Tidsestimat | Oppgaveeier | Steg 1-2-3 |
|---|---|---|---|---|
| | | | | |
| A1 | Møte med tilt.work | 2 | Bachelor Gruppe | Steg 1 Planlegging |
| A1-1 | Lag aktivitetsplan og milepæler for gjennomføring av risikovurdering. Eier av risikovurderingsgjennomgang | 1 | Andrea Sunde | Steg 1 Planlegging |
| A1-2 | Innkall til oppstartsmøte og involver aktuelle ressurser til oppstartsmøte | 2 | Bachelor Gruppe | Steg 1 Planlegging |
| M1 | Gjennomført oppstartsmøte risikovurdering IKT-system ABCD | 0 | Bachelor Gruppe | Steg 1 Planlegging |
| | | | | |
| A2-1 | Innkall til risikovurdering | 1 | Bachelor Gruppe | Steg 2 Risikovurdering |
| A2-2 | Utfør risikovurdering, identifiser og beskriv risikoområder | 14 | Mathias Jarbekk | Steg 2 Risikovurdering |
| A2.2 | Beskriv forslag på sikkerhetstiltak på avdekt risikoer | 4 | Bachelor Gruppe | Steg 2 Risikovurdering |
| A2.3 | | | | |
| M2 | Gjennomført risikovurdering IKT-system XYZ | 0 | Bachelor Gruppe | |
| | | | | |
| A3 | Utfør risikhåndtering av de avdekte risikoer | 4 | Edgaras Slezas | Steg 3 Risikohåndtering |
| A3-1 | Ledelsens vurdering og effektmål. KPI oppfølging | 4 | Thomas Nygaard | Steg 3 Risikohåndtering |
| A3-2 | Registrert utførte risikovurderinger og planlegg for nye gjennomganger. Kontinuerlig prosess | 3 | Thomas Nygaard | Steg 3 Risikohåndtering |
| M3 | Gjennomført risikovurdering med ledelsesinvolvering | 0 | Thomas Nygaard | Steg 3 Risikohåndtering |
| | | | | |

**FIGUR: 5.0 Planleggingsarket i NSM Risikovurdering av IKT-systemer for Tilt.work**

I planleggingsfasen har gruppen begynt så tidlig som mulig for å kunne danne et helhetsbilde av Tilt.work og deres systemer samt holdning til sikkerhet. Oppsettet starter

med et intervju med Tilt.work hvor det blir etablert en innsikt i hvordan Tilt.work sin holdning til sikkerhet ser ut. Videre i risikohåndteringsstegene har vi utnevnt hvem i bedriften som vi mener er oppgaveeieren videre i ROS-analysen som er utenfor vårt arbeidsomfang.

**Risikovurdering av IKT-system**

Vurdering ved hjelp av NSM grunnprisipper for IKT-sikkerhet

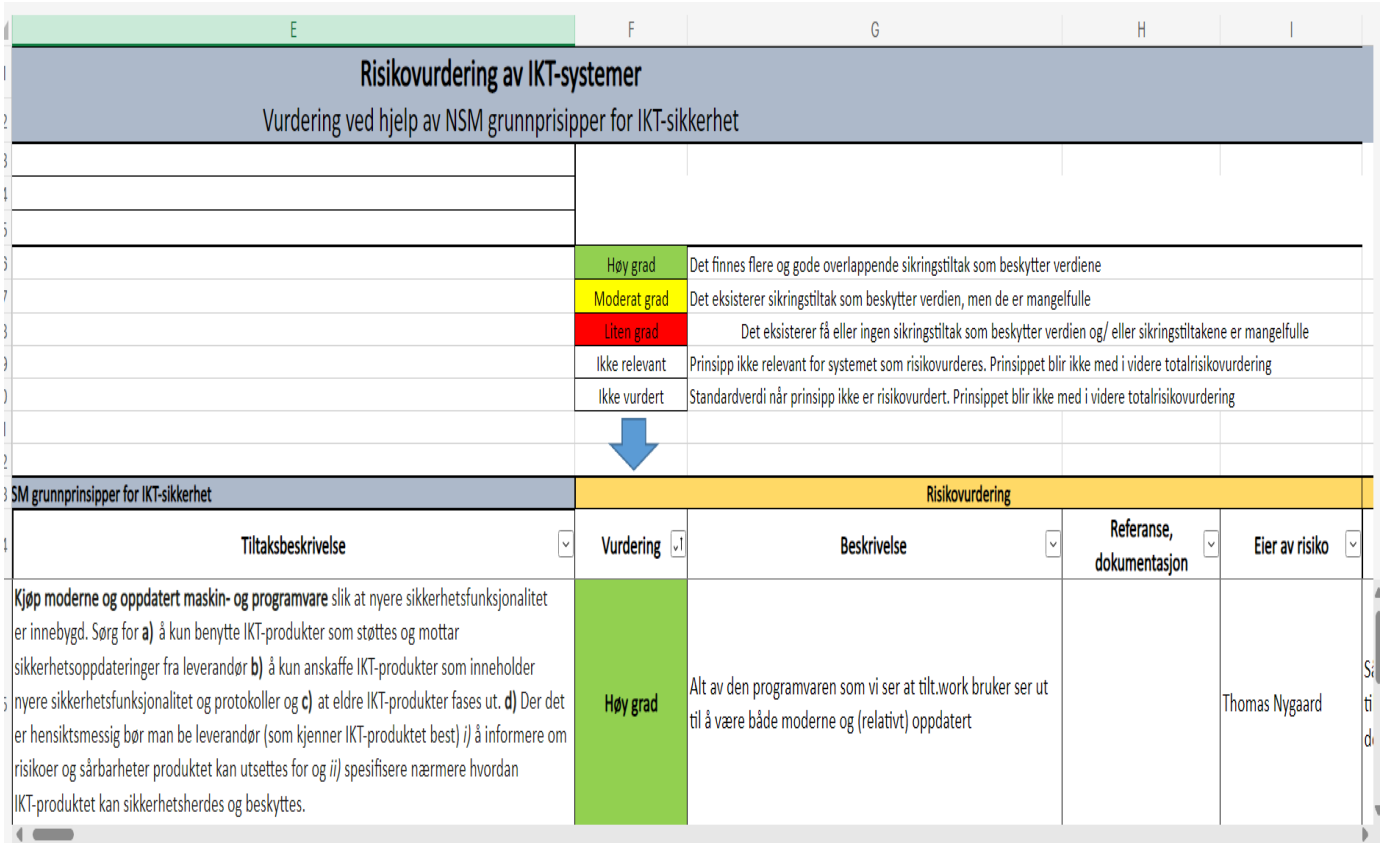
**Deltagerliste**

| | |
|---|---|
| **Virksomhet** | Tilt Work AS |
| **IKT-system** | tilt.work |
| **Dato** | 26.02.2024 |

| Stilling | Navn | Ansvarsområde | Kommentar | Aktivitet | Dato deltagelse |
|---|---|---|---|---|---|
| *Daglig Leder* | *Thomas Nygaard* | *Sikkerhetsstyring og planlegging* | | *Steg 1 ,2, 3* | *01.01.2024* |
| *IT Tekniker* | *Edgaras Slezas (også kjent som Edy)* | *Teknisk ansvarlig for tilt.work* | | *Steg 3* | *01.01.2024* |
| Bachelor Gruppe Medlem | Andrea Sunde | Gjennomføring av risikoanalysen | | Steg 1 ,2, 3 | *01.01.2024* |
| Bachelor Gruppe Medlem | Vetle Enberg | Gjennomføring av risikoanalysen | | Steg 1 ,2, 3 | *01.01.2024* |
| Bachelor Gruppe Medlem | Gabriel Wieczorek | Gjennomføring av risikoanalysen | | Steg 1 ,2, 3 | *01.01.2024* |
| Bachelor Gruppe Medlem | Mathias Jarbekk | Gjennomføring av risikoanalysen | | Steg 1 ,2, 3 | *01.01.2024* |
| | Bachelor Gruppe | | | | |
| | | | | | |

**FIGUR: 5.1 Deltagerark fra NSM Risikovurdering av IKT-systemer for Tilt.work**

Videre i prosessen er det en deltagerliste som inkluderer alle gruppemedlemmer samt, kontaktpersonene fra Tilt.work.



**Risikovurdering av IKT-systemer**

Vurdering ved hjelp av NSM grunnprisipper for IKT-sikkerhet

| | |
|---|---|
| Høy grad | Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene |
| Moderat grad | Det eksisterer sikringstiltak som beskytter verdien, men de er mangelfulle |
| Liten grad | Det eksisterer få eller ingen sikringstiltak som beskytter verdien og/ eller sikringstiltakene er mangelfulle |
| Ikke relevant | Prinsipp ikke relevant for systemet som risikovurderes. Prinsippet blir ikke med i videre totalrisikovurdering |
| Ikke vurdert | Standardverdi når prinsipp ikke er risikovurdert. Prinsippet blir ikke med i videre totalrisikovurdering |

| SM grunnprinsipper for IKT-sikkerhet | Risikovurdering | | | |
|---|---|---|---|---|
| Tiltaksbeskrivelse | Vurdering | Beskrivelse | Referanse, dokumentasjon | Eier av risiko |
| **Kjøp moderne og oppdatert maskin- og programvare** slik at nyere sikkerhetsfunksjonalitet er innebygd. Sørg for **a)** å kun benytte IKT-produkter som støttes og mottar sikkerhetsoppdateringer fra leverandør **b)** å kun anskaffe IKT-produkter som inneholder nyere sikkerhetsfunksjonalitet og protokoller og **c)** at eldre IKT-produkter fases ut. **d)** Der det er hensiktsmessig bør man be leverandør (som kjenner IKT-produktet best) *i)* å informere om risikoer og sårbarheter produktet kan utsettes for og *ii)* spesifisere nærmere hvordan IKT-produktet kan sikkerhetsherdes og beskyttes. | Høy grad | Alt av den programvaren som vi ser at tilt.work bruker ser ut til å være både moderne og (relativt) oppdatert | | Thomas Nygaard |

**Figur: 5.2 Risikovurderings ark fra NSM Risikovurdering av IKT-systemer for Tilt.work**

Ved risikovurdering av Tilt.work sine systemer har vi basert det på alle risikoer og sårbarheter som vi har oppdaget i systemene og fysiske rammeverkene til virksomheten.

Risikoene er fargebasert og strekker seg fra grønn (høy-grad), til gul (moderat grad) og videre til rød (liten-grad).

# 6.0 Diskusjon

I diskusjonskapittelet vil vi diskutere prosessene som fant sted under prosjektet og diskutere de forskjellige valgene og beslutningene vi måtte ta underveis i prosjektet. Vi skal reflektere over målene vi satte oss i begynnelsen av oppgaven og hvordan vi har nådd disse. Vi vil også referere til andre eksterne og relaterte verk som kan ligne på vår egen oppgave.

## 6.1 Hovedmål

Denne oppgaven ble startet med at vi satte oss mål for hva vi ønsket å oppnå gjennom prosjektet. Disse målene delte vi opp i ett hovedmål og 3 delmål. Hovedmålet vårt gikk ut på at vi ønsket å få en god innsikt i sikkerhetssituasjonen til Tilt.work sine systemer for å best kunne evaluere deres sikkerhet. Vi ønsket å bruke denne informasjonen til å kunne gi Tilt.work en god oversikt over eventuelle sikkerhetsfeil eller sårbarheter. Vi ville gjøre dette slik at Tilt.work kunne enklest mulig ta til seg de resultatene vi fant og bruke dem til å bedre sikre seg mot de svakhetene som vi sannsynligvis kom til å finne.

Det første delmålet vårt omhandlet at vi skulle identifisere og vurdere eksisterende risikofaktorer for å unngå at Tilt.work ville bli utsatt for fremtidige sikkerhetshendelser. For å gjøre dette så måtte vi evaluere trusler, mulige konsekvenser for en eventuell sikkerhetshendelse og eksisterende sårbarheter som vi fant i systemene til Tilt.work.

Det andre delmålet vårt gikk ut på at vi skulle lage en liste over anbefalte tiltak som Tilt.work kunne implementere for å bedre IKT sikkerheten deres.  Denne listen skulle bli presentert som ett Excel-ark og være basert på NSM sin mal for ROS analyser for IKT systemer slik at dette enkelt kunne bli presentert framfor en tredjepart ved senere anledning hvis Tilt.work ønsket å ansette eller tjenesteutsette denne oppgaven til noen andre.

Vi hadde ett siste delmål som egentlig faller litt under delmål to, men vi tenkte det var ryddigst å skrive det på denne måten. Dette delmålet omhandler en annen del av det som blir selve produktet vi lager for Tilt.work. Her snakker vi om et mer dagligdags dokument som skal gå over funnene våre og eventuelle konsekvenser som kan forekomme om Tilt.work ikke følger tiltakene til disse. Dette produktet skal være i et liste-format og skal

være såpass lettleselig at det ikke skal være nødvendig å ha noen ekstra IT-forståelse enn det "folk flest" har i dag for å forstå dette. Dette dokumentet er spesielt rettet mot ledelsen i Tilt.work til forskjell fra Excel-arket som er mer rettet mot IT avdelingen hos selskapet.

For å gjennomføre disse målene våre så gikk vi metodisk til verks med forskjellige teknikker. Ved å kombinere en åpen kommunikasjon med ledelsen og IT avdelingen hos Tilt.work, og å gjøre noen litt mer tekniske penetrasjonstester mot Tilt.work-nettsiden så mener vi at vi har fått en god oversikt over selskapet sine styrker og svakheter. Vi har gjennom hele prosjektet hatt en åpen kommunikasjonslinje til ledelsen til Tilt.work gjennom eposter til Thomas samt at vi har hatt en åpen linje av kommunikasjon til IT avdelingen gjennom eposter til Edgaras. Vi har også hatt møter med Thomas ved 2 anledninger når vi har hatt større spørsmål som har trengt mer diskusjon enn det et enkelt svar i en epost kunne gi.

Vi fastsatte oss at vi ikke så for oss at Tilt.work var noe stort mål for eventuelle TA-er. Men at det istedenfor var mer sannsynlig at risikoene lå hos de potensielle kundene til selskapet. Ved fastsettelsen av trusler hadde vi noen utfordringer med feilmeldinger som stadig dukket ved bruk av enkelte verktøy, et viktig eksempel var ved sikkerhetsscan utført av ZAP, der hadde ZAP rapportert om at det er sensitiv personlig informasjon som ligger ute på Tilt.Work sine nettsider og klarerte med å si at det er kredittkort informasjon. Dette viste deg å være tallkombinasjon i en URL streng på nettsiden som var den samme tallkombinasjonen som MasterCard bruker for å identifisere kortnummer. Noe som forvirret ZAP til å tro at det lå kredittkort informasjon ute offentlig på Tilt.work sine nettsider.

Som vi skrev om i kapittel 4.1 så brukte noen penetrasjonstestingsverktøy som f.eks WPScan og Nmap for å finne flere potensielle svakheter ved Tilt.work sine systemer, samtidig som vi også fant at de er sikret mot flere av det som kan sees på som "enkle" angrep som vi prøvde oss på. Det vi fant ut at ikke fungerte mot Tilt.work var blant annet *SQL injections*, XSS og *Bruteforce* angrep mot admin-brukeren på Tilt.work-nettsiden. Derimot så fant vi enkelte sårbarheter i form av en del utdatert og ubrukt kode i form av plugins og temaer som er installert på serveren, disse kan utvikle sårbarheter som så kan bli brukt av en eventuell TA. Dette er fordi at det er fort gjort at man glemmer eller velger å ikke oppdatere det som ikke brukes til daglig siden det sees på som "ikke så farlig". Men hvis en sikkerhetsoppdatering blir publisert fordi en svakhet i en *plugin* har kommet til dage, men selskapet ikke oppdaterer *pluginnen* så vil den sårbarheten vedvare på selskapets maskiner. Vi fant også

en åpen *SSH*-port på backup serveren deres, dette burde undersøkes nærmere av Tilt.work for å være sikre på at tilgangene til denne porten er sikret på best mulig måte ettersom at *SSH* er en typisk angrepsvektor. Vi fant også at tilt.work-nettsiden har XML-RPC skrudd på. XML-RPC er en *"legacy"* protokoll som fungerer som et *"interface"* for et utdatert API som WP har erstattet med det mer moderne REST-API-et. XML-RPC brukes for at tredjeparts applikasjoner skal kunne kommunisere med innholdet i en WP-side. XML-RPC er noe som vi vil anbefale på det sterkeste at Tilt.work stenger ettersom dette er *"legacy"* kode som ikke lenger blir oppdatert noe særlig og som det finnes flere sårbarheter som lett kan brukes for å bruke XML-RPC til å angripe et nettsted som bruker dette.

Når dette er sagt, så er det ikke slik at vi ser for oss at Tilt.work er særlig utsatt for noe angrep. Selskapet er ikke en enorm aktør som tiltrekker seg masse oppmerksomhet og de har en relativt liten nisje som de supplerer tjenester for. Derimot så bør det også nevnes at noen av kundene til Tilt.work er relativt store navn i business verden, noe som kan av seg selv trekke med seg potensielle trusselaktører som kan være ute etter å hente inn informasjon om den enkelte personen, men som ved et eventuelt slikt angrep også vil få tilgang til brukerinformasjonen til de andre brukerne til Tilt.work-nettsiden. Det er primært dette vi ser for oss som det største trusselbildet som Tilt.work står ovenfor, ikke nødvendigvis vinklet mot selskapet selv, men eventuelt mot kundene deres.

Vi gjorde også litt rekognosering på noen av større hacking-forumer som blant annet *Breachforums* og *Maultalk*, og diverse Telegram kanaler som finnes der ute for å se om Tilt.work hadde blitt nevnt, men vi fant ikke noen steder der Tilt.work, eller noen av navnene til de som er involvert i ledelsen til selskapet ble nevnt. Nå er det ganske dårlig logikk å se mangel på bevis til å bety at noe ikke skjer. Men vi velger likevel å tolke dette som ett godt tegn om at Tilt.work antagelig ikke er i siktet til noen TA per dags dato.

Det er forsåvidt viktig å huske at det er kun ved å gjennomføre de anbefalte tiltakene som vi har gitt i dette prosjektet og ved å sørge for at dette opprettholdes at man kan fortsette å holde seg sikret.

Som vi har snakket om tidligere så er det viktig at Tilt.work opprettholder den sikkerhets-tankegangen som vi håper vi klarer å formidle til dem gjennom dette prosjektet. Særlig framover i tid ettersom det desverre er slik at IT er ett emne som er i rask og stadig utvikling

at det er høyt sannsynlig at om 8-12 måneder så vil sikkerhets bildet rundt de punktene som vi har fremmet her være helt annerledes. Kanskje vil det være en stor ny svakhet som har kommet til dags i mellomtiden og derfor vil hovedfokuset ved en eventuell ROS analyse da omhandle denne eventuelle svakheten.

Til slutt i denne diskusjonen så er det viktig å gå over hvordan trusselbildet til Tilt.work ser ut i dag. Som vi har sagt tidligere så ser vi ikke for oss at Tilt.work i seg selv som selskap er noe stort mål for en potensiell TA grunnet størrelsen på selskapet og bransjen de jobber i. Det som derimot er med på å gjøre trusselbildet til Tilt.work mer reelt er kundene deres, Tilt.work markedsfører veldig mot business Norge og de har en del kunder som er relativt store navn i denne verdenen. Dette er individer som bringer med seg en utvidet sannsynlighet for en IT-sikkerhetshendelse ettersom disse individene kan ansees som særdeles utsatt når man snakker om sannsynligheten for en IT-sikkerhetshendelse.

## 6.2 Relatert arbeid

Vi fant det vanskelig i starten av oppgaven å finne gode kilder for relatert arbeid da de lignende oppgavene innenfor sikkerhetsfeltet som oftest holdes konfidensielt for allmenheten. Ved funn av Valdres kommune sin ROS analyse valgte vi å fjerne det meste av relatert arbeid vi allerede hadde funnet, da det ikke i samme grad var relevant i forhold til vår nye kilde. Akkurat grunnet dette er det kun to kilder for vårt relaterte arbeid, hvor vi mener alle relaterer godt oppgaven.

### 6.2.1 Artikkel om cybersikkerhet

Basert på vårt relaterte arbeid gir artikkelen angående cybersikkerhet en oversikt over trusselen bedrifter og privatpersoner i dagens samfunn står ovenfor. I artikkelen blir det introdusert flere typer kjente angrep som DoS eller DDoS, *ransomware* eller løsepengevirus, *phising* og *spearphising, man-in-the-middle*-angrep, *drive-by* angrep, passord angrep, *SQL-injection*-angrep, avlyttingsangrep, og direktørsvindel. Alle disse nevnte er kjente angrep som generelt sett alle bedrifter bør være obs på. Disse angrepene kan forårsake bedrifter alvorlige konsekvenser, spesielt i form av økonomiske tap eller tillitsbrudd fra faste kunder. Dette viser til viktigheten av en god ROS-analyse slik at bedrifter som Tilt.work er klar over disse sikkerhetstruslene.

Artikkelen går også generelt over hva cybersikkerhet går ut på. I tillegg nevner den ulike typer hackere og hvorfor faren for angrep har økt i moderne tid. Artikkelen fremstiller flere forslag til tiltak for å øke sikkerheten i en bedrift. Dette inkluderer blant annet:

- "Sørg for at alle ansatte bruker tofaktoratentisering på firma e-posten" (PwC, 2023).
- "Gjør en risikovurdering. Dette vil gi deg bedre oversikt og mulighet til å prioritere tiltak" (PwC, 2023).
- "Test eksisterende infrastruktur for eventuelle sårbarheter" (PwC, 2023).
- "Kartlegg dine viktigste digitale verdier og inkluder disse i en risikovurdering. Dette gjør det enklere å prioritere dersom angrepet blir et faktum" (PwC, 2023).

Enkle tiltak som dette vil styrke bedriftens digitale sikkerhet og kan også skape bevissthet angående sikkerhet blandt de ansatte i bedriften.

Informasjonen som forekommer i denne artikkelen, viser store farene ved nettverkskriminalitet i dagens samfunn. Det er akkurat derfor det er essensielt for en bedrift som Tilt.work å få utarbeidet en ROS-analyse for å få en oversikt over de potensielle farene som kan forekomme, samt konsekvensene disse kan ha. Ved å ta i bruk informasjonen og innsiktene gitt i denne artikkelen har vi fått et viktig innblikk for videre forståelse gjennom vår analyse slik at Tilt.work skal kunne opprettholde god sikkerhet.

- PwC.[2023]. Hva er cybersikkerhet. Hentet fra: https://www.pwc.no/no/teknologi-omstilling/hva-er-cybersikkerhet.html

### 6.2.2 Valdres ROS-analyse

Under relatert arbeid er det vedlagt en ROS analyse fra IKT Valdres. Dette Excel-arket var det eneste vi fant som lignet på vår oppgave, da det er meget begrenset hva som er ute på internett av relaterte ROS analyser. Dette er da en ROS analyse utført av IKT Valdres for Valdres kommune.

Valdres sin ROS analyse ser forholdsvis godt organisert ut, hvor det er gode seksjoner for de ulike punktene. I analysen blir det også vektlagt at minst to personer skal utføre vurdering,

som kan føre til en bedre helhetlig vurdering av situasjonen. Videre gir analysen konkrete eksempler på konfidensialitet, integritet og tilgjengelighet som tydeliggjør standarder som må opprettholdes. Det beskrives hvordan sannsynlighet og konsekvenser skal vurderes med ulike eksempler. Dette skaper gode rammer for videre evaluering for brukere. I analysen blir det også referert til en relevant matrise utarbeidet av Bergen kommune som skaper troverdighet til analysen.

På den andre siden mangler det tekniske detaljer, spesielt for en type analyse som dette fører dette til at analysen blir ufullstendig. Denne analysen er utdatert og om ikke det er utarbeidet en ny analyse kan det forekomme store mangler da det kontinuerlig vil oppstå nye trusler og sårbarheter. I tillegg til dette er det mangel på tiltak for å håndtere de identifiserte sikkerhetstruslene. Det forekommer en generell forklaring av eksempler og beskrivelser noe som kan føre til at risikoer og sårbarheter i denne analysen kan undervurderes eller bli sett bort ifra, noe som videre kan gi store konsekvenser.

Hovedpunktene som skiller Valdres sin ROS-analyse fra vår egen er mangel på detaljerte beskrivelser, tekniske detaljer, samt tiltak for trusler. Dette gjør Valdres sin analyse svakere fremstilt enn vår egen og tilrettelegger for et dårligere utgangspunkt for å oppdage, forebygge, samt løse de potensielle sikkerhetstruslene som kan oppstå. Det er også viktig å poengtere at denne ROS-analysen var gjort offentlig, noe som også kan bidra til store konsekvenser.

Vår oppgave tildelt fra Tilt.work som inngår i våre andre delmål var å lage en ROS analyse av deres systemer, hvor leveransen skulle inneholde to rapporter. En detaljert, utdypet rapport og en forenklet rapport.

Det var mange måter å løse oppdraget på og vi har i hovedsak tatt i bruk erfaring fra relevante undervisningsfag fra studiet, samtidig som at vi har basert oss på de mest kjente prinsippene som omhandler IT-sikkerhet.

Ved oppstart av prosjektet har vi evaluert hvilke metoder som kan være mest relevante for løsning av oppdraget, samt diskutert relevante løsninger og hensiktsmessige tiltak underveis.

IKTvaldres. [oktober,2020].https://www.iktvaldres.no/wp-content/uploads/2021/10/ikt-valdres-iks-ros-mal.xlsx

## 6.3 Refleksjon over delmålene

For å kunne utføre vårt første delmål, *identifisere og vurdere eksisterende risikofaktorer for å hjelpe Tilt.work unngå eventuelle fremtidige sikkerhetshendelser,* måtte vi ha en grundig forståelse for hva som Tilt.work ser på som sine verdier. For å oppnå dette hadde vi et langt møte med Thomas Nygaard som er daglig leder hos Tilt.work, og etter dette fikk vi et mye klarere perspektiv på hvilke verdier som må sikres og hva selve oppdraget vårt skulle omhandle videre. Vi fikk en klar oversikt over backup-rutinene deres, hvor mange administrative brukere de har, hvilke tilganger forskjellige skribenter av nettsiden har og hvordan nettsiden har blitt utviklet til slik den er i dag. Verdiene deres består av artiklene som er publisert på nettsiden deres, og at de ikke skal forsvinne da nettsiden opptrer som et bibliotek for disse verkene som har blitt samlet opp over 10 år.

Mens vi var i møtet med Tilt.work identifiserte vi to risikofaktorer som vi umiddelbart varslet om, antall skribenter med tilgang til forskjellige interne sider på nettsiden var overflødig og unødvendig, og grunnleggeren av virksomheten sitt private telefonnummer er oppført på hjemmesiden som et kundeservicenummer. Disse sårbarhetene, andre risikofaktorer og tiltak til disse er listet i et eget dokument ved navn Tilt.work rapport som er vedlagt denne hovedrapporten.

I praksis har identifikasjonen og vurdering av eksisterende risikofaktorer blitt gjort ved å undersøke selve nettsiden og de interne sidene til Tilt.work i Wordpress ved bruk av forskjellige verktøy og ren teoretisk analyse av deres rutiner.

For å kunne utføre vårt andre delmål fokuserte vi på å utarbeide en liste med tiltak som Tilt.work kan implementere. Der evaluerte vi hvem tiltak som var viktigst basert på verdiene til Tilt.work og prioriterte dem etter alvorlighetsgrad. Målet var å gi en teknisk oversikt i form av Excel-ark som beskrev Tilt.works nåværende sikkerhetssituasjon og foreslåtte handlinger.

Inkludert i dette er andre grenen av delmålet å gi konkrete anbefalinger for hvordan Tilt.work kan sikre seg mot identifiserte sårbarheter og redusere risikoen. Vi beskriver potensielle konsekvenser og eksisterende sårbarheter, med gitte tiltak for utbedring som revisjon av systemkonfigurasjon, forbedring av tilgangskontroller og implementering av sikkerhetsverktøy. Denne delen er utformet for å gi enkel oversikt uten behov for dyp IT-kunnskap.

For vårt andre delmål, *opprette en liste bestående av anbefalte tiltak Tilt.work kan implementere for å få en bedre IKT-sikkerhet,* som omhandlet å utarbeide denne i form av et excel-ark hvor tiltak Tilt.work kunne implementere skulle inkluderes. Her var det essensielt å sette seg inn i Tilt.work sin sikkerhetssituasjon for å kunne lage en liste som kan bidra til økt robusthet og en bedre sikkerhetsbevissthet for bedriften og de ansatte. Tiltak for bedre sikkerhet er viktig for både store og små bedrifter, hvor hovedpoenget vil være å skape en type kultur innad i selskapet om å fremme god sikkerhet ved hjelp av bevissthet. Med gode tiltak, samt opplæring i bedriften vil dette trolig føre til færre menneskelige feil som igjen ofte er en stor inngangsnøkkel for TA til en bedrift.

Vårt siste delmål (som også faller under delmål to), *gi anbefalinger for hvordan Tilt.work kan sikre seg mot indentifiserte sårbarheter, konsekvensene som kan resultere i at disse sårbarhetene eksisterer, og dermed gi dem konkrete anbefalinger til hvordan å håndtere disse.* Som forklart tidligere i diskusjonen er dette et delmål som inngår i den ene delen av selve produktet vi har produsert til Tilt.work i form av en forenklet og lettleselig liste som inneholder våre funn, og konsekvensene som potensielt kan forekomme ved å ikke følge tiltakene til disse.

For å kunne skreddersy disse målene for å gi de produktene som vil passe deres situasjon best mulig var det nødvendig å holde kontakten med selskapet. Vi har gjennom hele prosjektet holdt en kontinuerlig kommunikasjon hvor spørsmål har blitt besvart uten noen komplikasjoner, dette bidro til å styrke vår evne til å løse disse målene best mulig for Tilt.work. Som tillegg til dette har verktøyene vi har tatt i bruk i denne oppgaven gitt oss muligheten for å finne bedriftens styrker og svakheter, som videre har bidratt til noe vi selv mener har blitt et bra slutt produkt.

### *Verktøyrefleksjon*

Når vi ser tilbake på selve prosjektprosessen vår, så merker vi at vi brukte lenger tid på denne granskingen enn nødvendig da vi endte opp med å hovedsakelig bruke WPScan, nmap, spiderfoot, kali og zap.

Underveis i prosjektet oppdaget vi at Parrot og Wireshark ikke var verktøy som var veldig relevante for oss, selv om vi var temmelig sikre i begynnelsen av prosjektet at vi hovedsakelig skulle ta i bruk disse to verktøyene.

Vi startet med å bruke Parrot linux, noe som i senere tid falt av og vi brukte Kali linux isteden. Selve grunnen til at vi ikke brukte Parrot er fordi Kali var mer kjent for oss fra tidligere, har en større krets, og er mer brukt i praksis enn Parrot samtidig som vi anså Kali som mer egnet og hadde mer forhåndsinstallert programvare, integrert Nmap og metasploit, noe som muliggjorde en mer effektiv måte å jobbe med oppgaven. Vi har dog ikke noe vondt å si om Parrot, men det er rett og slett et for nytt operativsystem til at vi kunne satse på å bruke det gjennom hele prosjektet, spesielt siden vi var usikre på hvordan oppdraget skulle utvikle seg og om det var noe vits å sette seg inn i et slik OS uten å vite hvor mye vi egentlig skulle a det i bruk. Derfor ble Kali et mye mer naturlig valg, siden det også finnes utallige mengder av ressurser og hjelpemidler til dette OS-et.

Parrot var ikke det eneste verktøyet vi valgte å gå bort ifra midtveis i oppgaveløsningen og Wireshark var også et program som vi ekskluderte etter hvert. Grunnen til at vi ikke brukte Wireshark er fordi at vi da måtte vi ha vært til stede i Tilt.work sitt kontor og hatt tilgang til nettverket de tar i bruk, et nettverk som er åpent og brukes av flere andre bedrifter som oppholder seg i samme kontorbygg. Med dette kan vi anta at det er mye trafikk på dette nettverket, noe som hadde vært spennende å undersøke, men vi så for oss en tidskrevende prosess ved å be om tillatelser for å gjøre et slik inngrep og dermed valgte å fokusere på selve nettsiden til Tilt.work isteden. Selv om vi ikke undersøkte nettverket på kontoret til oppdragsgiveren vår så kunne vi likevel gi dem anbefalinger for å bedre sikre seg fra sårbarhetene som vanligvis kommer med et åpent nettverk, og videre anbefalte dem å anskaffe seg sitt eget nettverk. Vi kom frem til dette tiltaket da vi på et teoretisk plan undersøkte kjente sårbarheter som ofte kommer ved bruk av et felles og åpent nettverk på tvers av forskjellige bedrifter. Likevel vil vi konstatere at wireshark absolutt er et relevant

verktøy og hadde kunnet gitt oss et interessant og viktig innsyn i nettverkstrafikken til Tilt.work.

### *Valg av NSM sikkerhetsstandard vs. ISO standard*

En av de første fasene i oppdragsløsningen vår var å vurdere sikkerhetsstandarder, sammenlikne dem med hverandre, og til slutt velge en som igjen ville formet formatet og fremgangsmåten til prosjektet vårt. Tidligere i rapporten har vi diskutert NSM og ISO med en vinkling fra Tilt.works beste interesse med fremtidig bruk, men vi må også gjøre rede for valget vårt basert på oppdraget vi skal fullføre. Prosessen vi opplevde der vi måtte ta et valg mellom hvilken sikkerhetsstandard vi skulle basere risiko-og sårbarhetsanalysen vår var krevende siden ISO og NSM er begge betraktet som gode standarder. Derfor måtte vi gjøre en grundig vurdering av hvilken standard som egnet seg best i vårt tilfelle.

RISMA, en organisasjon som jobber med å gi andre bedrifter verktøy og oversikt over deres egen risikostyring, beskriver ISO som, "den internasjonale organisasjonen for standardisering, og lager internasjonale regler for kvalitetssikring av produkter og tjenester" (RISMA, id.). I følge *Store norske leksikon* har ISO en rådgiverstatus i FN, samtidig som den har som hensikt å produsere internasjonale standarder og består av flere nasjonale standardiseringsorganer (Holtebekk, 2021). Siden ISO er internasjonal, har rådgiverstatus i FN, samtidig som at den er en uavhengig og ikke-statlig organisasjon bidrar til at ISO oppleves som en troverdig og grundig kilde med gode standarder. I tillegg til dette har ISO en overveldende mengde av sikkerhetseksperter som bidrar til utarbeidelsen og produksjonen av standardene deres, "Arbeidet utføres av faggrupper som får innspill fra eksperter og interessenter. Det finnes rundt 3000 tekniske grupper og cirka 50 000 eksperter bidrar årlig til organisasjonen" (Holtebekk, 2021).

NSMs Grunnprinsipper for IKT-sikkerhet er det andre sikkerhetsstandard-alternativet vårt. NSM sin virksomhetshensikt beskriver de som følger, "Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler" (Nasjonal Sikkerhetsmyndighet, u.å.). Grunnprinsippene deres er inspirert av andre nasjonale og internasjonale regelverk, standarder og rammeverk samtidig som at

grunnprinsippene skal opptre som et supplement til disse (Nasjonal sikkerhetsmyndighet, 7). De fastslår også at de er relevante for alle norske virksomheter.

ISO er internasjonal, mens NSM er nasjonal og egnet for norske virksomheter, og det er vanskelig å glemme ISO sin ekstreme erfaring og ekspertise og med såpass mange gode kvaliteter, hvorfor skulle vi ikke valgt ISO som sikkerhetsstandard i oppdraget vårt?

Dog det ikke er noe tvil om at ISO er en god standard, så er det flere grunner til at vi stusset på om den var den riktige standarden å velge. ISO standarden bidrar ikke bare til sikkerhet, men hjelper virksomheter å holde seg relevante og oppdaterte i dagens tider. Dette er da best egnet for store virksomheter med flere konkurrenter der det å holde seg mest relevant i forhold til andre er en stor interesse. Tilt.work er en nokså liten bedrift med få ansatte, hvor hensikten med virksomheten er å hjelpe en svært spesifikk målgruppe. Grunnet størrelsen deres er interessen for å konkurrere med andre liknende og større bedrifter liten, og målet deres ved at vi utfører en risiko-og sårbarhetsanalyse er ikke for å bedre konkurranseevnen deres, men heller for å gi dem en bedre oversikt over sikkerhetssituasjonen deres i dag. NSM sine grunnprinsipper, derimot, har som hovedmål å hjelpe virksomheter i deres sikkerhetsimplementasjonsreise, ved å hjelpe dem vurdere hva som skal sikres, hvilke løsninger som egner seg for hvilke bedrifter, og ved å forsikre at sikkerhetsreisen starter i riktig ende (Nasjonal sikkerhetsmyndighet, 2020, s.3). Siden NSM har som hovedmål å sikre virksomheter for at det skal være oppdaterte i dagens sikkerhetssituasjon, og utelater verktøy og retningslinjer som bidrar til virksomheters konkurransedyktighet, som ISO derimot har et fokus på, er NSM helt klart et bedre alternativ ved dette tilfellet.

ISO standardene er ikke kun ekstremt omfattende, men veldig komplekse, og Tilt.work med en såpass liten ledelse har begrensende ressurser og tid til å kunne sette seg inn i standardene og videre implementere forskjellige krav. ISO standarden er også veldig dyr, og for en såpass liten bedrift gir det rett og slett ikke mening å ta i bruk standarden i dette tilfelle. NSM sine grunnprinsipper derimot, dog deres egentlige hovedmålgruppe er virksomheter som driver med kritiske samfunnsfunksjoner, fastslår de at de er relevante for alle virksomheter, inkludert private virksomheter, slik som Tilt.work (Nasjonal sikkerhetsmyndighet, 2021, s. 4).

Etter å ha gjort en slik drøfting er det likevel vanskelig å lande på et spesifikt valg. ISO er åpenbart et soleklart valg når det kommer til ekspertise og troverdighet, men den er svært omfattende, samtidig som at den er dyr. NSM sine grunnprinsipper er egnet for norske bedrifter, og kan beskrives som en litt mer simplifisert versjon av ISO. Ja, grunnprinsippene er gratis og lett tilgjengelig, men dette kan også bidra til problemstillingen om at en trussel aktør kan finne ut akkurat hvilke retningslinjer en virksomhet har brukt til å styrke sikkerheten sin med offentlige fremgangsmåter, mens ISO standardene derimot ikke er publisert offentlig.

I vårt valg av sikkerhetsstandard har vi vektlagt tilgjengelighet, pris, forståelsesgrad og relevans. NSM er lett tilgjengelig, er enklere å forstå siden den er på norsk, samtidig som at den er gratis og relevant for private virksomheter. Ved å velge NSM sine grunnprinsipper for IKT-sikkerhet i vårt oppdrag, så velger vi heller ikke bort ISO-standardene. En stor fordel ved NSM sine grunnprinsipper er nettopp det at den er såpass inspirert av ISO sine standarder, som vil indirekte gi oss både pose og sekk.

I planleggingsfasen var vi så heldige at vi fikk et intervju med to sikkerhetseksperter, som er dokumentert i kapittel 3.2. Vi hadde allerede fastslått at vi skulle bruke NSM sine grunnprinsipper for denne oppgaven, men vi ville likevel spørre ekspertene hva de tenkte om ISO versus NSM. De forklarte at ISO er en god standard, men er hovedsakelig basert på at man skal kunne *dokumentere* for at virksomheten har god sikkerhet, noe de mener man kan dokumentere for uten å egentlig ha det. De beskrev også NSM som en grei standard, at den er lur å bruke samtidig som at den er mer faglig orientert. Ekspertene sa likevel ikke noe vondt om ISO, men belyste heller en kjent problemstilling som kan forekomme ved å ta i bruk deres standarder.

RISMA Systems AS. [u.å]. Hvorfor er ISO-standarder så viktige? Hentet 25 februar, 2024 fra: https://www.rismasystems.com/no/ressurser/artikler/hva-er-fordelene-med-en-iso-standard

Nasjonal sikkerhetsmyndighet. [15.4.2020]. Grunnprinsipper for IKT-sikkerhet. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

Nasjonal sikkerhetsmyndighet. [6.6.2021]. *Risikovurdering av IKT-systemer*. (Første versjon). NSM. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

Nasjonal sikkerhetsmyndighet. [u.å.] *Dette er NSM*. NSM. https://nsm.no/om-oss/ledige-stillinger/dette-gjor-nsm/

Holtebekk, Trygve: *ISO* i *Store norske leksikon* på snl.no. Hentet 1. april 2024 fra https://snl.no/ISO

## Refleksjon over NSM sine grunnprinsipper for IKT-sikkerhet i praksis

Vår opplevelse med NSM gjennom oppdraget har vært fantastisk. For å gjøre oss godt kjent med prinsippene satte vi av to uker hvor vi studerte alle prinsippene for å få en helhetlig forståelse av dem, samt finne de grunnprinsippene som er mest relevante i oppdraget vårt. En slik gransking av prinsippene gjorde oss godt orientert på sikkerhet gjennom resten av oppgaven da vi etablerte oss en linse med sikkerhet i fokus.

I løpet av dette dypdykket innenfor NSM kom vi over deres publiserte verk av fremgangsmåte for ROS-analyse ved navn *Risikovurdering av IKT-systemer,* samt en konkret Excel mal for dette, som tegner opp hele prosessen som inngår i en risikoanalyse, med felter der man selv kan fylle inn oppdagede sårbarheter og eventuelle tiltak for å bearbeide disse.

*Risikovurdering av IKT-systemer*-publikasjonen var til god hjelp for oss da vi skulle forme funnene våre og tiltak til disse i vår enkle rapport til Tilt.work, mens Excel-malen hjalp oss avgrense relevante prinsipper, samt strukturere den spesifiserte rapporten vår og vi har videre brukt denne malen i vår leveranse i oppdraget vårt. Når vi ser tilbake på dette valget av hjelpemidler hadde det gavnet oss om vi hadde laget vår egen mal og konstruert funnene våre rundt den kompliserte rapporten på egenhånd.

Excel-malen til NSM er et stort hjelpemiddel å ta i bruk i et slikt oppdrag og forenkler prosessen ved en risikoanalyse i stor grad, dog uten den hadde det vært utfordrende å skape en så raffinert rapport, med en slik oversiktlig struktur. Dette er fordi vi ikke har mye praktisk erfaring innenfor risikoanalyse, men heller en større teoretisk forståelse av informasjonssikkerhet. Hypotetisk sett om vi skulle lagd vår egen mal hadde dette tatt mye tid, ressurser og ført til diskusjoner innad i gruppa om hvordan det best kunne blitt utført og strukturert. Ved at vi valgte å bruke NSM sin mal har vi spart tid og krefter som vi heller har brukt til å utføre selve ROS-analysen i praksis.

Vi har opplevd NSMs grunnprinsipper for IKT-sikkerhet som svært oversiktlige, utdypende og tydelige og har opptrådd som et kompass for oss gjennom oppdraget vårt og har hjulpet oss med det siste punktet i vårt første delmål, *evaluere trusler, mulige konsekvenser av disse og eksisterende sårbarheter innad i systemet til Tilt.work.* Denne evalueringen av sårbarhetene og konsekvensene av disse er utført og beskrevet i Excel-malen, mens i Tilt.work rapporten er disse enklere forklart, men ytterligere utdypet. For at Tilt.work skal få en bedre forståelse av konsekvensene til visse sårbarheter har vi trukket frem teoretiske hendelsesforløp som kan forekomme ved at disse ikke blir bearbeidet.

### *Refleksjon om risikomatrisen*

| Konsekvens | 1 | 2 | 3 |
|---|---|---|---|
| 5 | Brudd på taushetserklæring | Tap av arbeid | Får ikke fullført alle ønsket aspekter til oppgaven |
| 4 | Gruppemedlem velger å ikke fullføre studiet | Sårbar informasjon eller data som kommer på avveie | Kan være vanskelig å bruke bacheloroppgaven i fremtidig jobbsøk, grunnet konfidensiellt innhold |
| 3 | Skjevfordeling av arbeid mellom gruppemedlemmer | Kommunikasjonsfeil med veileder eller oppdragsgiver | Uenigheter innad i gruppen |
| 2 | Feil i innleveringsportal | Ikke oppdage viktige sikkerhetsfeil | Fordele tiden ujevnt mellom forskjellige oppgaver |
| 1 | Utestengt av epost og cloud-dokumenter grunnet midlertidig vedlikehold av skoletjenester | Gruppemedlemmer som ikke kan møte opp av uforutsigbare grunner | Sykdom |
| | 1 | 2 | 3 |
| | | Sannsynlighet | |

Før vi gikk i gang med prosjektoppdraget valgte vi å utføre en risiko og sårbarhetsanalyse gjennom en risikomatrise for selve oppgaven vi skulle gjennomføre. I dag kan vi referere tilbake til denne og sjekke hvilke risikoer som ble til virkelighet for oss i utførelsen av prosjektet vårt. Av 15 risikoer vi identifiserte, var det tre identifiserte risikoer som faktisk fant sted underveis.

To risikoer som vi identifiserte under fargen gul som vi opplevde var *sykdom* og f*ordele tiden ujevnt mellom forskjellige oppgaver*. Sykdom hadde vi merket som veldig sannsynlig, med relativ lav konsekvens dersom sykdommen ikke var langvarig for noen av gruppemedlemmene. Flere gruppemedlemmer opplevde dette som et hinder i løpet av semesteret og stoppet dem fra å kunne delta i diverse møter og arbeidsøkter. Sykdomssituasjonen var heldigvis ikke alvorlig eller langvarig for noen av oss, og fant sted en sjelden gang og med sporadiske mellomrom.

Ujevn tidsfordeling mellom forskjellige oppgaver opplevde vi i en liten grad tidlig i prosjektet da vi valgte å fokusere mye av tiden vår på å undersøke forskjellige verktøy som vi vurderte å ta i bruk underveis. Denne risikoen hadde også en relativt lav konsekvens siden den ikke påvirket prosjektet i så stor grad som vi fryktet, men tiden kunne blitt jevnere fordelt da vi heller kunne ha fokusert kreftene våre på produksjonen av produktene våre tidligere.

Den siste risikoen vi opplevde var markert som rød og omhandlet *tap av arbeid*. Dette var noe vi opplevde en sjelden gang, men var likevel frustrerende. I Excel-produktet vårt mistet vi en del fremgang tidlig i prosjektet da en tidligere arbeidsøkt ikke hadde blitt lagret, noe som var vanskelig å forstå siden vi brukte OneDrive, en tjeneste som automatisk lagrer arbeid gjennom utførelse. Vi opplevde dette også i hovedrapporten mot slutten av prosjektet som bremset prosjektutviklingen vår på et relativt ubeleilig tidspunkt.

De to gule risikoene var forståelige og lite hindrende da de ikke hadde noen store konsekvenser. Risikoen med tidsdisposisjon var veldig sannsynlig da alle gruppemedlemmene gjorde en risiko-og sårbarhetsanalyse for en bedrift for første gang, og tar konsekvensene av dette som en rik lærdom videre. Den siste røde risikoen var upopulær og lite motiverende å oppleve, da den ikke var konstruktiv i vår utførelse av prosjektet, men den var heldigvis ikke destruktiv heller.

# 7.0 Konklusjon

Gjennom dette prosjektet har vi utviklet en omfattende risiko-og sårbarhetsanalyse for Tilt.work, ved oppfølging av gitte prinsipper og regler produsert av Nasjonal Sikkerhetsmyndighet (NSM). Oppgaven var i det hele å evaluere Tilt.work sin sikkerhet i form av en risiko og sårbarhetsanalyse, utarbeidet i to eksempler med ulik dybdeinnsikt. Vårt mål med oppgaven var å få en oversikt over Tilt.work sin IT-sikkerhet, og derfra kunne utarbeide en ROS analyse som skildrer deres utfordringer samt opprette en liste med forebyggende tiltak for potensielle sikkerhetsproblemer som kan oppstå.

Ved å anvende en kombinasjon av penetrasjonstesting, gjennomgang av systemkonfigurasjon, intervjuer med personell og metodikker innenfor informasjonssikkerhet har arbeidet vårt funnet flere kritiske sårbarheter hos Tilt.work som utdatert kode, åpne porter i backup serveren og rom for å optimalisere nettstedet. Basert på disse funnene har vi foreslått praktiske og tekniske tiltak for å forbedre deres sikkerhetssituasjon.

Prosjektet har vist at selv i små bedrifter, er det en viktig egenskap å prioritere informasjonssikkerhet for å beskytte deres data og informasjon samt hvor viktig det er for disse å dedikere ressurser til å bevare sin motstandsdyktighet. Gitt at Tilt.work implementerer anbefalte sikkerhetstiltak kan de ikke bare redusere risikoen for sikkerhetsbrudd, men også styrke seg selv som en pålitelig bedrift innenfor IT-bransjen.

Etter vår undersøkelse av Tilt.work sine systemer gjennom dette prosjektet konstaterer vi at per i dag er de ikke særdeles utsatt for sikkerhetstrusler eller konkrete trusselaktører, men det har blitt oppdaget såpass store sårbarheter at disse må bearbeides, spesielt hvis de ønsker å skalere opp virksomheten sin.

En av de viktigste lærdommene fra dette prosjektet er den kritiske rollen menneskelig faktor spiller i informasjonssikkerhet. Opplæring, bevisstgjøring og oppdatering blandt de ansatte er avgjørende for at de implementerte sikkerhetstiltakene er effektive og forblir.  I tillegg til dette er det er viktig å anerkjenne at sikkerhet innenfor IT er veldig dynamisk og krever kontinuerlig oppdatering. For fremtiden anbefaler vi at Tilt.work fortsetter å regelmessig vurdere sin sikkerhetsstatus gjennom overnevnte ROS analyser og orientering av sikkerhets

rutiner, samt revisjon av selskapets nåværende tilgangskontroll for å holde seg oppdatert med utviklingen av cybertrusler.

Dette prosjektet har møtt de mest essensielle målene, men også etablert et viktig fundament for fremtidig sikkerhetsarbeid hos Tilt.Work. Ved å fokusere både på de tekniske og menneskelige aspektene av sikkerhet, vil det gi Tilt.Work et grunnlagg til å fortsette sitt arbeid opp mot robusthet og håndtering av både nåværende og fremtidige sikkerhetstrusler.

# Ordliste

| | |
|---|---|
| **Open VAS** | Verktøy for sårbarhetsanalyse en del av kali / linux |
| **TOR browser** | Nettleser med fokus på personvern og anonymitet på internett ved å skjule IP adresse. |
| **Brute force angrep** | Angrep hvor det prøves alle kombinasjoner for å finne påloggingsinformasjon eller data |
| **NSM** | Nasjonal Sikkerhets Myndighet |
| **Bytekode** | Kode som er mellomledd mellom kildekode og maskinkode |
| **Avlytte** | Fange opp data som sendes mellom enheter |
| **Malware** | Skadelig programvare |
| **Pakkerouting** | Prosess av å sende informasjon mellom servere og tjenester. |
| **Protokoll** | Et sett med regler og standarder for kommunikasjon på et nettverk og mellom enheter. |
| **Nettverkstopologi** | Strukturen av enheter inne på et nettverk |
| **Admin** | En person som styrer nettverk og systemeier. |
| **SSH** | Secure Shell – nettverksprotokoll som brukes for ekstern tilgang til systemer og overføring av data. |
| **HTTPS** | HTTPS er en kommunikasjonsprotokoll som støtter sikker kommunikasjon over internett. Protokollen sikrer at man kan verifisere identiteten til nett-tjenesten man kommuniserer med, samt at informasjonen som overføres ikke kan avlyttes. **https://snl.no/HTTPS** |
| **HTTP** | Hypertext Transfer Protokoll, er en kommunikasjonsprotokoll som i hovedsak brukes til å overføre HTML-dokumenter mellom tjenere og klienter ved hjelp av en transportprotokoll, vanligvis Transfer Control Protocol (TCP). https://snl.no/HTTP |
| **White-hat-hacker** | White-hat-hackere er motsatsen til svarte hatter. De utnytter datasystemer eller nettverk for å identifisere sikkerhetsfeil, slik at de kan gi anbefalinger for forbedringer. https://no.kaspersky.com/resource-center/definitions/hacker-hat-types |
| **Grey-hat-hacker** | Mellomtingen mellom white hat-og black hat hackere. Grey hat-hackere leter ofte etter sårbarheter i et system uten eierens tillatelse eller kunnskap. Hvis problemer blir funnet, rapporterer de |

| | |
|---|---|
| | dem til eieren, og noen ganger ber de om en liten godtgjørelse for å løse problemet. https://no.kaspersky.com/resource-center/definitions/hacker-hat-types |
| **Black-hat-hacker** | Black hat-hackere er kriminelle som bryter seg inn i datanettverk med ondsinnet hensikt. https://no.kaspersky.com/resource-center/definitions/hacker-hat-types |
| **IP-adresse** | En IP-adresse er en unik adresse som identifiserer en enhet på internett eller et lokalt nettverk. https://no.kaspersky.com/resource-center/definitions/what-is-an-ip-address |
| **Penetrasjonstesting** | Penetrasjonstesting er en metodikk for sikkerhetstesting der et system eller et nettverk med tillatelse blir utsatt for dataangrep. https://snl.no/penetrasjonstesting |
| **Sikkerhetsrevisjon** | En sikkerhetsrevisjon omfatter kontroll og verifikasjon av nødvendige sikkerhetstiltak i virksomheten, og skal gjennomføres jevnlig. https://www.ehelse.no/normen/normen-dokumenter/sikkerhetsrevisjon-faktaark-06 |
| **CSRF** | Cross-Site-Request-Forgery er en type angrep som utnytter påloggingsinformasjon for å få tilgang å utføre handlinger uten brukerens samtykke. |
| **Rekognosering** | Å fremskaffe data eller informasjon om en aktør, aktiviteter eller fysiske karakteristikker i et definert fysisk område eller domene ved et gjennomsøk. https://www.etterretningstjenesten.no/om-etterretning/begreper-og-definisjoner |
| **Routing** | Nettverksrouting er en prosess med å velge en bane på tvers av ett eller flere nettverk. https://www.cloudflare.com/learning/network-layer/what-is-routing/ |
| **Phising** | Er en betegnelse på snoking etter sensitiv informasjon som passord eller kredittnummer. https://no.wikipedia.org/wiki/Phishing |

| | |
|---|---|
| **Tailgating** | Innebærer å snike seg inn på et forbudt sted bak en person som er autorisert til å gå inn. https://www.fortinet.com/resources/cyberglossary/tailgating-attack |
| **Spoofing** | Spoofing er en bred betegnelse for den typen atferd som innebærer at en nettkriminell later som om de er en pålitelig aktør eller enhet for å få deg til å gjøre noe som er til fordel for hackeren, og skadelig for deg. https://no.kaspersky.com/resource-center/definitions/spoofing |
| **Baiting** | En type angrep hvor en hacker vil bruke falske belønninger eller løfter for å stjele sensitiv informasjon av ofre ved å infisere systemene deres med skadelig programvare. https://www.privacysense.net/terms/baiting/ |
| **Brannmur** | Brannmur er en programvare som skal avvise uønsket kommunikasjon til et program, en datamaskin eller et nettverk. https://snl.no/brannmur |
| **Antivirus** | En betegnelse for programvare som har til hensikt å oppdage og fjerne ulike former for skadevare. https://snl.no/antivirus |
| **GDPR** | GDPR står for General Data Protection Refulation, oversatt til norsk heter det personvernforordningen. Dette er en lov som ble innført i 2018 og gir en enhetlig og streng regulering for personvern i Europa. https://gdprcontrol.no/hva_er_gdpr/ |
| **Fuzzing** | En automatisert programvaretestingsteknikk som innebærer å gi ugyldige, uventede eller tilfeldige data som input til et dataprogram. https://en.wikipedia.org/wiki/Fuzzing |
| **ROS analyse** | Risiko og sårbarhetsanalyse er en analyse som ofte brukes til å finne sårbarheter i et system. |
| **Sensitiv informasjon** | Er informasjon som skal holdes hemmelig for utenforstående. Dette kan for eksempel være personnummer eller bankkortdetaljer. |

| | |
|---|---|
| **Ekstern tilgang** | Muligheten for en autorisert person til å få tilgang til en datamaskin eller et nettverk fra en geografisk avstand via en nettverkstilkobling. https://ncpeaprofessor.org/ekstern-tilgang/ |
| **XSS (Cross Site Scripting)** | XSS er et sikkerhetsproblem på nettet som lar en angriper kompromittere interaksjonene brukere har med en sårbar applikasjon. https://portswigger.net/web-security/cross-site-scripting |
| **IPv4** | Et sett med protokoller for adressering og sending av datapakker over nettverk og internett. https://ndla.no/subject:1:81b3892a-78e7-4e43-bc31-fd5f8a5090e7/topic:1:35b4877b-4c94-479f-af07-98951659d5d2/topic:1:eefa49f5-025d-49d4-b436-7a8e00e25e14/resource:8efe036c-716d-40a2-90f6-3081c6832f76 |
| **IPv6** | Versjon 6 av internett-protokollen og er etterfølgeren til IPv4. Den ble utviklet for å håndtere mangelen på mulige IP-adresser som oppstod med IPv4 versjonen. https://no.wikipedia.org/wiki/IPv6 |
| **Sosial minipulasjon** | Det å benytte psykologiske virkemidler for å gjøre angrep mot brukere av IT-systemer. https://snl.no/sosial_manipulering_-_datasikkerhet |
| **Virus** | Virus er innen IT en type skadevare som kopierer seg inn i andre filer på en datamaskin og tilkoblede lagringsenheter. https://snl.no/datavirus |
| **To faktor autorisering** | Tofaktorautorisering er en form for autentisering der man benytter to autentiseringsmetdoer i kombinasjon. Dette gir høyere sikkerhet. https://snl.no/tofaktorautentisering |
| **Trusselmodellering** | Trusselmodellering er en prosess som går igjennom sikkerheten til et system, identifiserer problemområder, og evaluerer risikoen assosiert med hvert område. https://infosec.sintef.no/informasjonssikkerhet/2018/06/trusselmodellering/ |

| | |
|---|---|
| **Trusselaktør (TA)** | Trusselaktør er en person eller organisasjon som har gjennomført eller kan tenkes å gjennomføre et dataangrep. https://snl.no/trusselakt%C3%B8r |
| **Hendelseshåndtering** | Hendelseshåndtering er et samlebegrep for systemer og rutiner som kan iverksettes som en respons på sikkerhetshendelser. https://snl.no/hendelsesh%C3%A5ndtering_-_informasjonssikkerhet |
| **Brute-force angrep** | Et prøv-og-feil forsøk på å gjette en brukers påloggings informasjon. Dette vil si brukernavn og passord. Algoritmen vil prøve forskjellige varianter til den finner en vellykket pålogging. https://vpnoverview.com/no/nettsikkerhet/nettkriminalitet/brute-force-angrep/ |
| **Metasploit** | Penetrasjonsverktøy med rammeverk til sikkerhetstesting. |
| **Burp-suit** | Testing av webapplikasjon sikkerhet. |
| **Nikto** | Webserver sårbarhetsverktøy som skanner etter sårbarheter. |
| **Sikkerhetsskanning** | Prosess for å finne sikkerhetssvakheter i programvare og systemer. Kilde: https://www.splunk.com/en_us/blog/learn/vulnerability-scanning.html |
| **Ressursoptimalisering** | Oppdatere og planlegging av resurser for å få mest mulig utkast kilde: https://www.runn.io/blog/resource-optimization |
| **Spidering** | Den automatiserte prosessen med å gå gjennom et nettsteds struktur og samle informasjon om sidene og innholdet. https://eitca.org/cybersecurity/eitc-is-wapt-web-applications-penetration-testing/spidering/spidering-and-dvwa/examination-review-spidering-and-dvwa/what-is-spidering-in-the-context-of-web-application-penetration-testing-and-why-is-it-important/ |
| **OSINT** | Innsamling og analyse av informasjon som ligger offentlig. (https://www.sans.org/blog/what-is-open-source-intelligence/) |
| **TA** | Forkortelse for trusselaktør. |
| **WP** | Forkortelse for wordpress. |

# 8.0 Bibliografi

[1] International Organization for Standardization. [Edition 3, 2022]. ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. https://www.iso.org/standard/27001

[2] Mark1Systems. [29 November 2023]. Navigating the pros and cons of ISO 27001 Certification in the UK: A Mark1 Systems Perspective. https://mark1systems.com/navigating-the-pros-and-cons-of-iso-27001-certification-in-the-uk-a-mark1-systems-perspective/

[3] Neumetric.[u.å]. ISO 27001 vs Other Security Standards. Hentet 8 mars 2024 fra: https://www.neumetric.com/iso-27001-vs-other-security-standards-a/

[4] Nasjonal sikkerhetsmyndighet. [15.4.2020]. Grunnprinsipper for IKT-sikkerhet. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

[5] Kali.org. [u.å]. Kali Linux. Hentet 5 februar 2024 fra: https://www.kali.org/

[6] Parrotsecorg. [u.å]. Parrot Security. Hentet 5 februar 2024 fra: https://parrotsec.org/

[7] Imperva. [u.å]. Penetration Testing. Hentet 5 februar 2024 fra: https://www.imperva.com/learn/application-security/penetration-testing/

[8] CompTIA. [u.å]. What Is a Network Protocol? Hentet 1 mars 2024 fra: https://www.comptia.org/content/guides/what-is-a-network-protocol#:~:text=A%20network%20protocol%20is%20an,internal%20processes%2C%20structure%20or%20design.

[9] Zaproxy. [u.å]. OWASP ZAP. https://www.zaproxy.org/

[10] PortSwigger Ltd. [u.å]. Burp Suite. https://portswigger.net/burp

[11] Shivanadhan, M. [2 oktober, 2020]. What is Nmap and How to Use It: A Tutorial for the Greatest Scanning Tool of All Time. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

[12] OSINT Framework. [u.å]. OSINT Framework. Hentet 5 februar 2024 fra: https://osintframework.com/

[13] Balena. [u.å]. Balena hjemmeside. Hentet 5 februar 2024 fra: https://www.balena.io/

[14] Tilt.Work. [u.å]. Tilt. Hentet 8 januar 2024 fra: https://tilt.work/

[15] IBM. [u.å]. What is Social Engineering? Hentet 10 mars 2024 fra: https://www.ibm.com/topics/social-engineering

[16] NetworkChuck,[9 juli 2020] Nmap Tutorial to find Network Vulnerabilities. https://www.youtube.com/watch?v=4t4kBkMsDbQ

[17] RISMA Systems AS. [u.å]. Hvorfor er ISO-standarder så viktige? Hentet 25 Februar 2024 fra: https://www.rismasystems.com/no/ressurser/artikler/hva-er-fordelene-med-en-iso-standard

[18] Holtebekk, Trygve: *ISO* i *Store norske leksikon* på snl.no. Hentet 1. april 2024 fra https://snl.no/ISO

[19] Synopsys. [u.å.]. What is ethical hacking? Hentet 20. februar 2024 fra: https://www.synopsys.com/glossary/what-is-ethical-hacking.html#:~:text=Ethical%20hacking%20involves%20an%20authorized,and%20actions%20of%20malicious%20attackers.

[20] Nasjonal sikkerhetsmyndighet. [21 Juni 2021]. Risikovurdering av IKT-systemer. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

[21] Wikipedia. [3 mai, 2024]. General data protection regulation. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[22] IKT Valdres.[Oktober, 2020]. Risikovurdering for Valdres Kommune. Hentet 29 april 2024 fra: Blir lagt til som vedlegg.

[23] Ncpea Proffesor.[3 januar 2022]. Hva er ekstern tilgang? https://ncpeaprofessor.org/ekstern-tilgang/

[24] PortSwigger.[u.å]. What is Cross-site-Scripting (XSS). Hentet 12 februar 2024 fra: https://portswigger.net/web-security/cross-site-scripting

[25] Nist. [25 april 2024]. National vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2024-0256

[26] Sonkusare, R. [29 mars, 2023]. What is BurpSuite|How to use BurpSuite| BurpSuite Tutorial for Beginners. https://techofide.com/blogs/what-is-burp-suite-how-to-use-burp-suite-burp-suite-tutorial-for-beginners/

[27] Figur3.1[Bios/Asus/Tuf]. Hentet den 11 mars 2024 fra: tps://static1.xdaimages.com/wordpress/wp-content/uploads/wm/2023/12/20231204_164731850_ios.jpg?q=50&fit=crop&w=1500&dpr=1.5)

[28] Figur3.3[OS/Kali Linux] Hentet den 11 mars 2024 fra:https://b1490832.smushcdn.com/1490832/wp-content/uploads/2021/04/Kali-Linux.jpg?lossy=2&strip=1&webp=1)

[29] Augustene, A. [25mars,2023].Sosial manipulering forklart: Angrepsteknikker og forebygging. https://nordvpn.com/no/blog/sosial-manipulering/

[30] Heine Natt, T. [25 januar, 2024]. Hendeleshåndtering (informasjonssikkerhet). https://snl.no/hendelsesh%C3%A5ndtering_-_informasjonssikkerhet

[31] Wikipedia.[u.å]. Ip-adresse:https://no.wikipedia.org/wiki/IP-adresse

[32] PWC. [2023]. Artikkel om Cybersikkerhet.:https://www.pwc.no/no/teknologi-omstilling/hva-er-cybersikkerhet.html

[33]Kaspersky.[2023].Hva er sosia¨¨l manipulasjon https://no.kaspersky.com/resource-center/definitions/what-is-social-engineering

[34]Fema.[2021].Developing and maintaining Emergency Operation Plans.

https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf

[35] Nasjonal sikkerhetsmyndighet. [u.å.] *Dette er NSM*. NSM. https://nsm.no/om-oss/ledige-stillinger/dette-gjor-nsm/

[36] Nasjonal sikkerhetsmyndighet.(2021). *Mal for risikovurdring av IKT-systemer* [Excel-fil]. Hentet fra https://nsm.no/getfile.php/136606-1625054194/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Vedlegg-%20Mal%20for%20risikovurdring%20IKT-systemer.xlsx

# 9.0 Vedlegg

Denne hovedrapporten blir levert inn i en komprimert .zip fil. Når denne filen er dekoprimert så vil det være en mappe som heter “Vedlegg” ved siden av denne PDF-filen. Innad i “Vedlegg” mappen vil følgende vedlegg ligge:

NSM Risikovurdering av IKT-systemer for Tilt.work: Dette er NSM malen vi har brukt til å fullføre den tekniske risiko-og sårbarhetsanalysen og inkluderer alle relevante avvik og sårbarheter som vi har funnet i Tilt.work sine systemer, samt NSM sine tiltak for disse.

Risikoanalyse for Tilt.work (Tilt rapport): Dette er dokumentet som tidligere nevnt skulle være lett forståelig for noen uten ytterligere IT-erfaring. Her er prosessen til risiko og-sårbarhetsanalysen beskrevet og dokumentert i større grad, samtidig som at vi har utarbeidet en spesifikk liste over avvikene som er nevnt i Excel-malen. Ytterligere forklart i dette dokumentet er mulige konsekvenser av de forskjellige avvikene og sårbarhetene, samt tiltak de kan ta i bruk for å bearbeide disse.

IKTvaldres: Dette er en kilde som vi har vedlagt fordi den i senere tid har blitt fjernet fra nettet.