Høgskulen på Vestlandet

MOØ300 Masteroppgave

MOØ300

Predefinert informasjon

Startdato:	07-05-2021 09:00	**Termin:**	2021 VÅR
Sluttdato:	21-05-2021 14:00	**Vurderingsform:**	Norsk 6-trinns skala (A-F)
Eksamensform:	Masteroppgave		
Flowkode:	203 MOØ300 1 O 2021 VÅR		
Intern sensor:	Torstein Nesheim		

Deltaker

Navn:	Ingelin Lygresten
Kandidatnr.:	221
HVL-id:	584401@hvl.no

Informasjon fra deltaker

Egenerklæring *:	Ja
Jeg bekrefter at jeg har registrert oppgavetittelen på norsk og engelsk i StudentWeb og vet at denne vil stå på vitnemålet mitt *:	Ja

Gruppe

Gruppenavn:	14
Gruppenummer:	
Andre medlemmer i gruppen:	Ingrid-Marie Lyster

Jeg godkjenner avtalen om publisering av masteroppgaven min *

Ja

Er masteroppgaven skrevet som del av et større forskningsprosjekt ved HVL? *

Nei

Er masteroppgaven skrevet ved bedrift/virksomhet i næringsliv eller offentlig sektor? *

Nei

Høgskulen på Vestlandet

MASTEROPPGAVE
MOØ300

"Hvordan påvirkes informasjonssikkerheten i Azets og Visma av teknologiutvikling?"

"How is information security in Azets and Visma affected by technology development?"

Ingrid-Marie Tromsdal Lyster & Ingelin Lygresten

Master i innovasjon og ledelse

Institutt for økonomi og administrasjon

Veileder: Carmen Olsen

Innleveringsdato: 21.05.2021

Jeg bekrefter at arbeidet er selvstendig utarbeidet, og at referanser/kildehenvisninger til alle

kilder som er brukt i arbeidet er oppgitt, *jf. Forskrift om studium og eksamen ved Høgskulen på Vestlandet, § 12-1.*

Sammendrag

Formålet med denne studien er å undersøke hvordan teknologiutvikling påvirker informasjonssikkerheten i Azets og Visma. For å belyse problemstillingen har vi tatt i bruk teori og forskning innenfor temaene teknologi, trusselbildet, forebygging og beskyttelse. Gjennom dybdeintervjuer fikk vi ledelsens og ansattes forståelse av hva informasjonssikkerhet er, og hva som påvirker den. Funnene viser at; Azets og Visma påvirkes av sine omgivelser som er kontinuerlig endring, og av nye kombinasjoner av eksisterende teknologi. Trusselbildet er for Azets og Visma preget av konstante angrep og deres største trussel er knyttet til den menneskelige faktoren i organisasjonene. Azets og Visma jobber kontinuerlig med forebygging av trusler gjennom opplæring av ansatte, bruk av beredskapsplaner og rammeverk.

Videre viser funnene at teknologi som AI og kvantedata vil i fremtiden brukes oftere til angrep. Videre lærte vi at organisasjonens omgivelser er stadig skiftende, noe som fører til at organisasjonene må være proaktive for å oppdage nye trusler. Da Azets og Visma er store organisasjoner strukturert som hierarki, kan implementering av rammeverk ta lengre tid, enn i mindre organisasjoner med mindre kompleks struktur Gjennom “latente feil- modellen” (David Woods) har vi lært at menneskelige feil påvirkes av teknologi, i like stor grad som at teknologien forårsaker menneskelige feil. Årsaken til menneskelige feil er derfor sammensatt, og kan sees i sammenheng med ledelsens fokus. Sikkerhetsekspertene mener at deres oppgave er å sørge for teknologien ikke skaper feil, ved å ikke ha for komplekse systemer. Ledelsens oppgave er å forhindre menneskelig feil ved å ha fokus kontinuerlig opplæring og oppfølging. Gjennom denne studien vil vi vise at dette samsvarer ikke alltid.

Abstract

The purpose of this study is to examine how technology development affects information security in Azets and Visma. To shed light on the problem, we have applied theory and research on the subjects of technology, the threat picture, prevention, and protection. Through in-depth interviews, we gained management's and employees' understanding of what information security is, and what affects it. The findings show that; Azets and Visma are affected by their environment which is constantly changing. They are also affected by new combinations of existing technology. The threat picture for Azets and Visma is characterized by constant attacks and their greatest threat is related to the human factor in the organization. Azets and Visma work continuously with threat prevention through employee training, the use of contingency plans, and frameworks.

The findings show that technology such as AI and quantum data will in the future be used more often for attacks. Furthermore, we learned that the organization's environment is constantly changing, which means that the organizations must be proactive to detect new threats. Azets and Visma are large organizations with a hierarchical structure and implementing frameworks can take longer than in smaller organizations with less complex structure. Through “latent error models” (David Woods) we have learned that human error is affected by technology, to the same extent as technology causes human error that technology causes human error. The cause of human error is therefore complex and can be seen in context with the management's focus. The security experts believe that their task is to make sure the technology does not create errors, by not having too complex systems. Management's task is to prevent human error by focusing on continuous training and follow-up. Through this study, we will show that this does not always correspond.

Forord

Denne studien er den avsluttende oppgaven ved masterstudiet innovasjon og ledelse ved Høgskulen på Vestlandet. Vår motivasjon for denne studien bygger vårt ønske om å skrive en oppgave som er relevant for samfunnet, samt relevant for vår karriere videre etter masterstudie. Vi har begge en bachelor i HR- og personalledelse. Da vi skulle bestemme oss for tema til masteroppgaven, ville vi bygge videre på vår kunnskap om mennesker og deres behov for opplæring, tilpasning og et arbeidsmiljø som tilrettelegger for dette. Innenfor masterløpet i innovasjon og ledelse er det spesielt den økte digitaliseringen i samfunnet som har fanget vår interesse. Derfor ville vi se på utfordringer som er knyttet til teknologi på arbeidsplassen. Da vi skulle velge hvilken bransje vi ønsket å studere nærmere falt valget på regnskapsbransjen. Vi anser regnskapsbransjen som noe som vil bli for alltid, da det vil alltid være et behov for å sette opp et regnskap uansett hvilken handelsvaluta fremtiden har å by på. Regnskapsbransjen må være tilpasningsdyktig både med tanke på politiske- og økonomiske endringer i samfunnet, som for eksempel større legale endringer fra politisk hold, men også endringer i praksis og kultur i enkelte bransjer og organisasjoner eller økonomiske svingninger i markedet

Vi vil her benytte anledningen til å takke våre intervjuobjekter fra Azets og Visma for godt samarbeid, verdifulle intervju og tilbakemeldinger.

Vi vil spesielt takke hverandre, for godt samarbeid gjennom fem år med bachelor- og masterstudier.

Innholdsfortegnelse

1.0 Innledning 7
1.1 Relevans og formål 8
1.2 Problemstilling og avgrensning 10
1.3 Oppgavens struktur 12
1.4 Azets og Visma 13
1.4.1 Azets 13
1.4.2 Visma 14
2.1 Teknologi 15
2.1.1. Digitalisering 16
2.1.2 Informasjonssystem 17
2.1.3 Implementering av teknologi 18
2.2 Trusselbildet 19
2.2.1 Sikkerhet 20
2.2.2.Informasjonssikkerhet ved bruk av skytjenester 22
2.2.3 Trusler og trender 23
Phishing 25
Menneskelige feil 27
2.3 Forebygging og beskyttelse 29
2.3.1 Rammeverk for internkontroll 30
2.3.2 Ledelse og ansvar 33
2.3.3 Opplæring og kompetanse 34
3.1 Forskningstilnærming og design 37
3.2 Populasjon og utvalg 38
3.4 Forberedelse og gjennomføring av dybdeintervjuer 39
3.5 Innholdsanalyse 41
3.6 Studiens validitet og reliabilitet 41
3.7 Etikk og personvern 42
4.1 Hvordan påvirker ny teknologi og digitalisering Azets og Visma? 44
4.2. Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning? 47
4.3 Hvordan forebygger Azets og Visma de største truslene? 55
5.1 59
5.2 61
5.3 65

6.1 Metodiske begrensninger 70
6.2 Implikasjoner 71
6.3 Videre forskning 71
7.0 Litteraturliste 73
8.0 Vedlegg 79
Vedlegg 1 79
Vedlegg 2 80
Vedlegg 3 82
Vedlegg 4 83
Vedlegg 5 84
Vedlegg 6 86

Figur- og tabelliste:

Figur 1.2.1 - Modell som illustrerer hvordan vi mener temaene i oppgaven vår påvirker hverandre.

Figur 1.3.1 - Oppgavens struktur og analytisk rammeverk.

Figur 1.4.1 - Organisasjonskart Azets.

Figur 1.4.2 - Organisasjonskart Visma.

Figur 2.3 - Risikoanalyse

Figur 2.3.1 - Rammeverk for internkontroll (av digitaliseringsdirektoratet)

Figur 3.2 - Framstilling av intervjuobjektene

Figur 4.1 - Oppsummering av funn “Hvordan påvirker ny teknologi og digitalisering Azets og Visma?”

Figur 4.2 - Oppsummering av funn “Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?”

Figur 4.3 - Oppsummering av funn - “Hvordan forebygger Azets og Visma de største truslene?”

Figur 6.0 - Presentasjon av hovedfunn, implikasjoner og videre forskning

1.0 Innledning

Informasjonssikkerhet[1] handler om at informasjonen ikke skal bli kjent for uvedkommende, endret utilsiktet, og at informasjonen er tilgjengelig ved behov. Lekkasje av informasjon påvirker ikke bare organisasjonen som oppbevarer informasjonen, men også privatpersoner og andre organisasjoner (Digdir-internkontroll/styringssystem). Informasjonssikkerhet er et sentralt tema på grunn av måten vi nå kan kombinere teknologi på. Dette kalles den fjerde industrielle revolusjon. Den består av robotikk, kunstig intelligens, nye teknologier, materialer, og produksjonsformer. Revolusjonen muliggjøres ved at ting begynner å kommunisere med hverandre over internett (Rolstadås m.fl. 2017.18). Denne utviklingen påvirker den generelle sikkerheten i organisasjonen, da kriminelle[2] har mer enn en måte å gjøre skade på. Organisasjoner må dermed se på sikkerhet på en annen måte, enn kun ved å ha en vekter i inngangsdøren.

Digitalisering[3] forenkler og effektiviserer mange av de prosessene vi har i dag, men digitaliseringen fører også med seg utfordringer (Rolstadås m.fl. 2017.18). En utfordring er knyttet til personvern[4] (Unit.no 2020). Privatpersoner utleverer i dag store mengder digital informasjon som kan knyttes direkte opp mot deres identitet, sensitive opplysninger[5] geografisk posisjon og interesser. Slik digital informasjon er sårbar for misbruk, som Identitets-tyveri. Både private og offentlige organisasjoner er lovpålagt å beskytte personopplysninger mot digitale sikkerhetstrusler. Dermed er sikkerheten rundt denne informasjonen viktig.
Det at digitalisering effektiviserer prosessene vi har i dag betyr også at endringene i omgivelsene og truslene er effektivisert. Digitalisering gjør at vi som privatpersoner og organisasjoner kan utføre arbeidsoppgavene mer effektivt, men parallelt med dette så effektiviseres også instrumentene til aktører som er ute etter å stjele og misbruke digital informasjon. Organisasjoner må derfor være i beredskap og være proaktive med å integrere

[1] *Informasjonssikkerhet inkluderer å sikre alle komponenter i informasjonssystemer (IKT-systemer, IKT-tjenester og IKT-komponenter. Ordet inkluderer IKT-sikkerhet, digital sikkerhet og cybersikkerhet). Begrepet "informasjonssikkerhet" (Digitaliseringsdirektoratet-begrepsliste).*
[2] *I denne oppgaven vil ordet kriminell alltid omhandle en person som gjør en kriminell handling via teknologiske løsninger.*
[3] *Digitalisering: Digitalisering handler om at informasjonen som blir lagret digitalt, blir brukt for å forenkle og fornye prosesser i organisasjonen.*
[4] *GDPR/Personvernloven*
[5] *Navn, adresse og telefonnummer som kan knyttes til enkeltpersoner (unit.no)*

nye teknologiske løsninger for å være et steg foran de kriminelle i trusselbildet. Organisasjoner må være dynamiske og respondere på endringer i omgivelsene, dette fører til kontinuerlig endring i arbeidsmetoder (Jones 2013.32).

Med bakgrunn i David Woods undersøkelser om menneskelige feil forstår vi at endringen i måten teknologi anvendes på arbeidsplassen også vil ha en effekt på menneskene som arbeider der (2010.153). Noen arbeidsoppgaver blir kanskje overflødige, mens andre bare blir endret. De ansatte får endrede arbeidsmetoder, og det stilles nye krav til dem som de kanskje ikke føler seg kompetente til å løse. Forskning antyder at lederen må ta en sentral rolle i kunnskapsdelingen i organisasjoner, slik at den ansatte utvikler seg. Ledelsen får andre utfordringer i form av opplæring og oppfølging av allerede ansatte i organisasjonen uten teknisk utdannelse (Nesheim & Olsen.2011).

I neste del skal vi presentere hvorfor vi har valgt å skrive om hvordan teknologi påvirker informasjonssikkerhet, og hvorfor vi valgte Azets og Visma til vår studie. Vi vil også presentere hvordan vi har valgt å svare på problemstillingen.

1.1 Relevans og formål

Med utgangspunkt i trusselbildet som stadig endres på grunn av økt bruk av nye teknologiske løsninger, ønsker vi å utforske hvordan dette påvirker informasjonssikkerheten i regnskapsbransjen.
Regnskapsbransjen er i stadig utvikling, og har endret seg mye de siste årene grunnet teknologiutvikling[6] og digitalisering. Regnskapsbransjen har tilgang til og oppbevarer store mengder sensitiv informasjon. Dersom deres datasystemer skulle bli utsatt for hacking, så kan det true sikkerheten og personvernet til både selve organisasjonen, men også enkeltindivider og samfunnet. Azets og Visma har opplevd at informasjonssikkerheten har blitt truet gjennom angrep[7]. Visma opplevde i 2018 et angrep knyttet til kinesisk etterretning, der målet var å få tak i Vismas kundeinformasjon. Hackerne fikk ved hjelp av phishing tak i brukernavn og passord som hjalp dem inn i Vismas systemer. Angrepet var ikke vellykket (Settevik.2019). Azets har opplevd at svindlere har brukt navn på sentrale personer i Azets for å få tak i kundeinformasjon. Svindlerne har tatt direkte kontakt med kunder over telefon, i tillegg til å

[6] *Teknologiutvikling: begrepet inneholder ikke bare utviklingen av ny teknologi, men nye måter å kombinere teknologi på*
[7] *Et cyberangrep kan defineres som et angrep som har til hensikt å skade eller overbelaste datasystemet (NHO.no.2018) I vår oppgave vil vi kun bruke ordet «angrep» for cyberangrep*.

bruke phishing metoden. Hva bakgrunnen med informasjonsuthentingen var er uklart, men svindlerne lyktes ikke å få tak i noe kritisk informasjon (Løvhøiden.2020). På bakgrunn av disse angrepene forstår vi det slik at kundedata er kritiske data for Azets og Visma. De har kunder som PSS Securitas og Norges fibromyalgi forbund, så det kan tenkes at bak deres regnskapstall ligger helseopplysninger[8]og opplysninger om hvilke steder som har vakthold. Dette er eksempel på kritisk data som ikke bør være tilgjengelig for alle.
På bakgrunn av eksemplene over, og at både Azets og Visma har dedikerte ansatte som jobber med sikkerhet, tenker vi informasjonssikkerhet er viktig for dem og dermed interessante kandidater for vår oppgave.

Formålet med studien er å undersøke hvordan informasjonssikkerheten til Azets og Visma blir påvirket av teknologiutvikling. For å svare på problemstillingen har vi valgt å svare på følgende underspørsmål:

1) *Hvordan påvirker ny teknologi og digitalisering Azets og Visma?*
2) *Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?*
3) *Hvordan forebygger Azets og Visma de største truslene?*

[8] *Reguleres av DPIA, vurdering av personvernkonsekvenser (Datatilsynet u.d)*

1.2 Problemstilling og avgrensning

I Innledning, relevans og formål har vi presentert utgangspunktet for vår oppgave. Da vi utformet problemstillingen, valgte vi en eksplorerende problemstilling som tilsier at vi ønsker å utforske **hvordan** en organisasjon påvirkes av en spesifikk faktor.
Problemstillingen vår er utformet som:

"Hvordan påvirkes informasjonssikkerheten i Azets og Visma av teknologiutvikling?"

Problemstillingen blir besvart gjennom følgende tema:

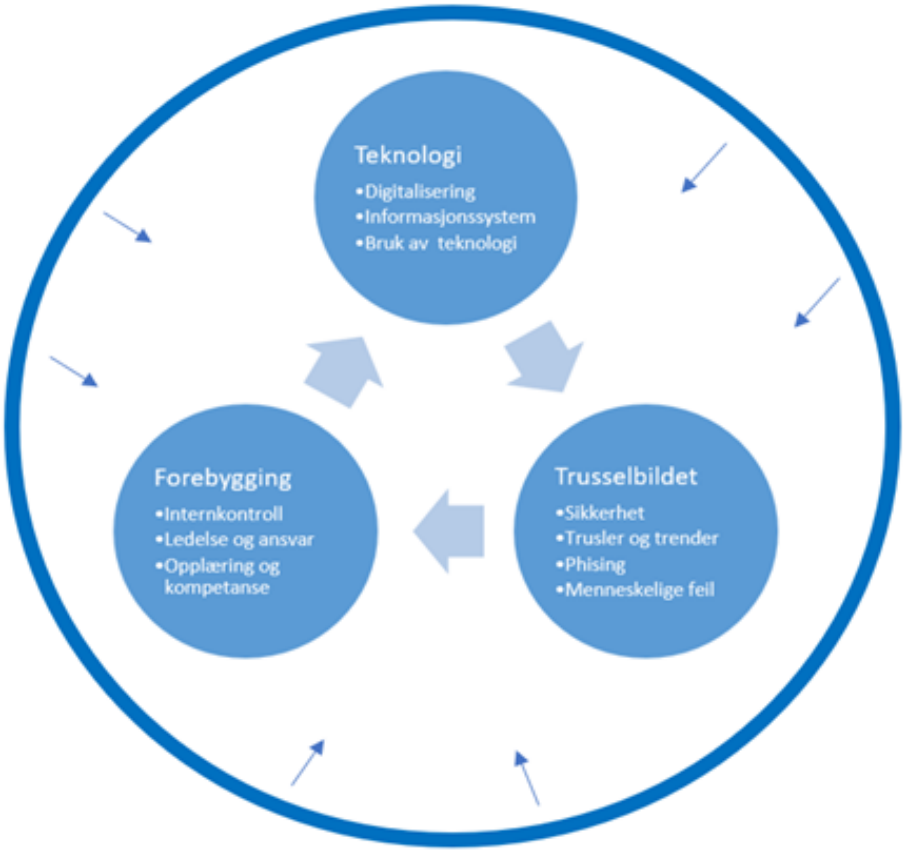
Teknologi - Herunder digitalisering, informasjonssystemer og hvordan integrering av ny teknologi fungerer i regnskapsbransjen.

Trusselbildet - Herunder informasjonssikkerhet, sikkerhet, trusler og trender. Vi har identifisert phishing og menneskelige feil som de to største truslene for informasjonssikkerhet, de har derfor egne underoverskrifter.

Forebygging og beskyttelse - Herunder internkontroll, ledelsen og dens ansvar for opplæring og kompetanse. Vi har valgt å fokusere på disse temaene, da vi ser de som mest aktuell for å forebygge og beskytte organisasjonene mot trusler.

Vi har avgrenset studien til én bransje, da fokuset på én bransje kan gi et mer konkret bilde på hvordan situasjonen er i dag. Valget falt på regnskapsbransjen, da det er en bransje som stadig påvirkes av teknologiske endringer, og som vi antar også i fremtiden – med en enda større hastighet – vil bli påvirket av endringene. Vi avgrenset studien til Azets og Visma grunnet tidsbegrensning da oppgaven skal ferdigstilles i mai 2021. Selv om vi har valgt å avgrense til to organisasjoner, føler vi at vi har fått en god innsikt i regnskapsbransjen, da Azets og Visma er store organisasjoner som leverer programvare og tjenester til offentlig og privat sektor nasjonalt og internasjonalt. Vi har i tillegg lange dybdeintervju med nøkkelpersoner for vår problemstilling. Deltakerne i vår studie er tre ansatte i Azets og tre ansatte i Visma og et intervjuobjekt fra en uavhengig organisasjon, som jobber med sikkerhetshåndtering. Vi skal utdype dette mer i 3.0 Kvalitativ metode.

Vi har på bakgrunn av teorien som anvendes i oppgaven utarbeidet en modell som illustrerer hvordan våre tre hovedtema henger sammen med - og påvirker hverandre. Teknologien påvirker trusselbildet til organisasjonene. For å minimere truslene må organisasjonene utføre ulike forebyggingstiltak. Den ytterste sirkelen i modellen illustrere omgivelsene rundt organisasjonen. Dette er en evigvarende prosess, da omgivelsene rundt organisasjonen stadig endres.



Figur 1.2.1 - Modell som illustrerer hvordan vi mener temaene i oppgaven vår påvirker hverandre.

1.3 Oppgavens struktur

Oppgavens struktur og analytiske rammeverk er presentert i modellen under; *1.3.1 oppgavens struktur og analytiske rammeverk.*

Studien starter med teoridelen som tar for seg relevante tema for vår studie. Videre blir det presentert metodedelen som gir grunnlag for hvilke metoder som brukes i studien, samt begrunnelse for valgene vi har tatt. Videre blir Azets og Visma presentert. I funn -og analysedelen vil funnene av vår undersøkelse analyseres og knyttes opp mot teoridelen. Videre vil dette diskuteres og drøftes opp mot hverandre. Avslutningsvis vil oppgaven oppsummeres i en konklusjon som besvarer problemstillingen og tar for seg utfordringer og veien videre.

2.0 Teori	Teoridelen består av relevante tema; Teknologi, Trusselbildet, Forebygging og beskyttelse. Med relevante modeller.
3.0 Metode	I metodedelen blir det redegjort for hvilke metoder som tas i bruk for å svare på problemstillingen og begrunnelse for hvorfor disse valgene tas. Her vil det også komme frem hvilke datainnsamlingsverktøy som skal brukes, håndtering av innsamlede data, og hvordan dataene analyseres.
4.0 Funn og analyse	Her presenteres funn gjort i innholdsanalysen av dybdeintervjuene.
5.0 Diskusjon	Her blir funnene fra innholdsanalysen diskutert opp mot teori og forskning.
6.0 Konklusjon	I konklusjonen vil det bli presentert et svar på problemstillingen. Det vil også komme frem begrensninger som er knyttet til oppgaven og forslag til videre forskning på temaet.

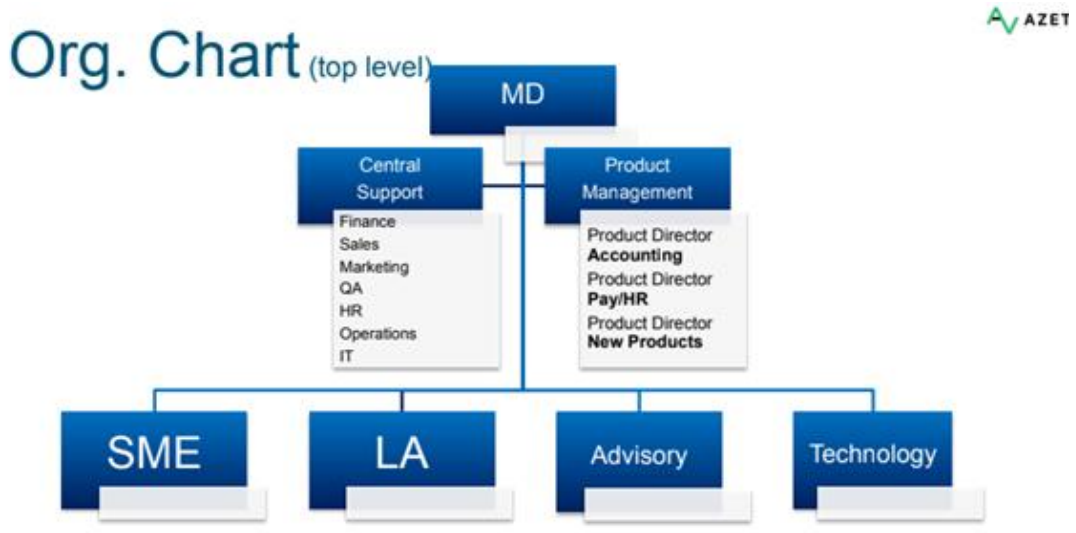
Figur - 1.3.1; Oppgavens struktur og analytiske rammeverk

1.4 Azets og Visma

Empirisk kontekst i vår oppgave består av innhentet informasjon fra Azets og Visma og én konsulent. Konsulenten som har bidratt ønsket å anonymisere sin arbeidsgiver og vil dermed ikke bli presentert her. Både Azets og Visma er store og komplekse organisasjoner, med hierarkisk oppbygning. Det betyr at endringer kan være tunge å gjennomføre, da det er mange linjer med linjeledere, eksperter og ansatte. Det har også preget vår oppgave, i den form av at når vi skriver om undertemaene i oppgaven, tar vi ikke hensyn til at det kan være annerledes i andre organisasjoner.

1.4.1 Azets

Azets er en organisasjon som tilbyr regnskap- og lønnstjenester, rådgivning og forretningstjenester. De er en internasjonal organisasjon med 6500 ansatte og over 120 000 kunder i Norden og Storbritannia. De tilbyr digital og personlig service. Azets ble etablert i 2016, men har eksistert siden 1971 under navnene Baldwins, Visma, Azets og CogitalGroup. (azets.no) I Norge har de et ekstra fokus på digitalisering og automatisering av økonomiske prosesser. Vi intervjuet tre personer i Azets; en sikkerhetsansvarlig, en økonomisk rådgiver og en rekrutteringsansvarlig.



Figur 4.1: Organisasjonskart Azets (personlig kommunikasjon i e-post med Azets. 30.04.21)

1.4.2 Visma

Visma leverer programvare og tjenester som skal gjøre forretningsprosesser forenklet og digitalisert. Visma ble opprettet i 1996, og etablerte seg internasjonalt i 1999. Visma er Europas ledende softwareselskap, de har 1 000 000 kunder som benytter deres produkter og 12 500 ansatte. Konsernet er i hele Norden, Benelux, Sentral og Øst-Europa. (visma.no)

Vi intervjuet tre personer i Visma; En sikkerhetsansvarlig, en HR-businesspartner og en programvare selger.

Figur 4.2: Organisasjonskart Visma (Personlig kommunikasjon med Visma i e-post 03.05.21)

I dette kapittelet har vi presentert Azets og Visma, som er grunnlaget for vårt empiriske innhold. I neste kapittel vil vi knytte teorien fra kapittel 2 opp mot funnene fra intervjuene.

2.0 Teori

I teoridelen av denne oppgaven vil vi presentere teori og forskning ut ifra følgende spørsmål;

1. Hvordan påvirker ny teknologi og digitalisering Azets og Visma?

2. Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?

3. Hvordan forebygger Azets og Visma de største truslene?

Temaene vi presenterer her er 2.1 Teknologi, 2.2 Trusselbildet, 2.3 Forebygging og beskyttelse. Hovedvekten av teorien og forskningen vi har brukt handler om phishing, menneskelige feil og sikkerhet, fordi det er de mest sentrale temaene våre.

2.1 Teknologi

Teknologi kan defineres som kombinasjonen av kunnskaper, teknikker, materialer og maskiner som brukes for å lage produkter og tjenester (Jones 2013.252). Videre deler Jones organisasjonens teknologi inn i tre nivåer; individuelt nivå, funksjonelt nivå og organisasjonsnivå. Det individuelle nivået handler om kompetansen som hver enkelt person innehar. På det funksjonelle nivået handler det om hvordan avdelingen/gruppen bruker sin kompetanse og teknikker for å lage produkter. Rolstadås mener at ny teknologi oppstår når samfunnet har behov for den, eller når samfunnet er modent til å ta i bruk den nye teknologien (Rolstadås 2017.13). Teknologi har gjennom tidene påvirket samfunnet, alt i fra hvor folk bosatte seg for mange tusen år siden og frem til i dag, der den eksempelvis bestemmer hvordan arbeidsoppgaver organiseres (Rolstadås 2017.14). Utviklingen i teknologien handler ikke bare om nye oppfinnelser, men også nye måter å anvende teknologien vi allerede har. Big data[9] er en ny teknologi som gjør det mulig å analysere større og mer komplekse data hurtigere enn før. Big data kan forklares ved ordene volum, variety og velocity. I tillegg har dataene stor variasjon, noe som betyr tilgang til ulik type data gjennom ulike kilder.

[9] *Big data defineres ut ifra de tre ordene volum, variation og velocity. Big data kan forstås som store mengder data, med mye variasjon i dataene og som stadig endres (Nordlie.2019).*

I dette delkapittelet har vi definert hva teknologi er og hvordan det påvirker organisasjoner, i neste del vil vi skrive om prosessen med å ta nye teknologier i bruk; digitalisering.

2.1.1. Digitalisering

Digitalisering handler om at informasjonen som blir lagret digitalt, blir brukt for å forenkle og fornye prosesser i organisasjonen. Eksempel på digitalisering kan være utvikling av elektronisk identifikasjon og elektronisk signering (Scrive u.d.). Haraldseth skriver i sin artikkel at digitalisering handler om å ta i bruk digitale løsninger for å videreutvikle organisasjonen og hvordan implementering av disse endrer organisasjonen (Haraldseth u.d.). Et eksempel er virtuelt privat nettverk (VPN). De fleste organisasjoner har et internt kryptert nettverk som de ansatte jobber fra. Ved å ta i bruk VPN kan ansatte bruke beskyttelsen fra arbeidsgiver, uansett hvor de befinner seg.

Digital transformasjon handler om at organisasjonen forbedrer prosesser og oppgaveløsningen innad, forbedrer produkter og tjenester, eller skaper nye tjenester som følge av å ta i bruk ny teknologi (Difi.no.2019). Det å ta i bruk teknologi istedenfor analoge løsninger kalles digitalisering. Artikkelen til Myhrvold (u.d) viser til tre ulike årsaker til den økte digitaliseringen i samfunnet. Dette handler om at det stadig utvikles nye teknologier raskere enn før. Videre trekkes det fram at ulike teknologier gir organisasjoner muligheter til å få tilgang til store mengder informasjon, og at robotisering og automatisering blir mer vanlig (Myhrvold u.d). Videre har det også blitt utviklet programmer som Sender Policy Framework (SPF)[10] og Domain Keys Identified Mail (DKIM) som skal forhindre spoofing[11] og garantere mottaker at e-post kommer fra en sikker kilde. (Google.21)

[10] *SPF brukes i e-postserveren for å kontrollere om avsenderen har lov til å sende deg e-post fra et gitt domene. Det skal hindre og mottar e-post fra falske e-post adresser. DKIM er en signatur som legges til e-posten, den bekrefter at den er sendt på riktig måte og at e-posten ikke har blitt endret (Nettvett.2021)*

[11] *Forfalskning av avsenders identitet via digital kommunikasjon*

2.1.2 Informasjonssystem

I denne studien bruker vi digitaliseringsdirektoratets definisjon av et informasjonssystem[12]; *"Et informasjonssystem er et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon"*

Eksempler på informasjonssystemer er e-postservere, regnskaps- og lønnstjenester som Electronic data interchange (EDI)[13]. Utviklingen av teknologi som kunstig intelligens (AI)[14], big data og blockchain[15] gir muligheten for nye innovasjoner, verdiskapning og effektivisering. Utviklingen kommer også med nye usikkerhetsmomenter, sårbarheter og trusler. Norsk sikkerhetsmyndighet rapporterer at det kommer flere og mer avanserte digitale angrep mot norske organisasjoner. (mediaplanet u.d). Utviklingen setter krav til både informasjonssystemene og brukerne av dem. Som et tiltak for å minske sårbarhet kan organisasjoner bruke monitorering. Ved bruk av monitorering kan et fåtall utvalgte ansatte overvåke at de ansattes pc-er i sanntid, for å forsikre seg om at de ikke laster ned malware[16].

I følge Rolstadås m.fl. vil fremtidens teknologi være raffinering av tradisjonell datateknologi. I tillegg må maskinene kunne samarbeide med mennesker utenfor kontrollerte miljøer (2017.46). Samfunnet må kunne stole på at løsningene som informasjonssystemene gir er sikre. Hvis ikke systemene er sikre kan det redusere viljen til å investere i teknologien med påfølgende konsekvens av at ingen bruker dem (mediaplanet. u.d). Et eksempel på raffinering av tradisjonell datateknologi, er skyløsning. Det å ta i bruk skyløsninger som lagringsplass er blitt veldig vanlig. I skyløsningene krypteres informasjonen slik den ikke er tilgjengelig for uvedkommende. Som en konsekvens av at flere velger skybasert lagring, må algoritmene[17] og krypteringene[18] som gjøres være gode nok til å holde flere år fremover.

---

[12] Informasjonssystem: "Et informasjonssystem er et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon" - Digitaliseringsdirektoratet.
[13] Elektronisk overføring av papirer som faktura, ordre og varekataloger (Azets - Teknologi. 2021)
[14] er informasjonsteknologi som "tenker selv" fordi den har blitt lært opp av et menneske hvordan den skal reagere i gitte tilfeller (Tidemann.2020)
[15] Blockchain: Er en teknologi som gjør det mulig å overføre penger, dokumenter og avtaler. Teknologien gjør det mulig å overføre verdier uten bruk av et mellomledd som for eksempel en bank. Teknologien reguleres ved at partene ikke kan endre historikken og ved bruk av smarte kontrakter. (Viglo u.d.)
[16] Malware kan defineres som programvare som har ødeleggende hensikter. For eksempel kan det være ulike typer virus (Netsecurity 2021)
[17] Algoritmer kan defineres som en oppskrift bestående av ulike skritt, og rekkefølgen på skrittene Algoritmer brukes ofte i søkemotorer og sosiale medier, for at personene skal få opp relevante innlegg ut ifra søkehistorikken til personen (Grønmo 2020).
[18] Kryptering kan defineres som en metode som gjør at informasjon blir låst, slik at ingen uvedkommende ikke kan få tilgang til informasjonen. For å få tilgang til informasjonen må vedkommende bruke en nøkkel (Datatilsynet 2017).

Fordi kvantedatamaskiner[19] blir mer tilgjengelig og nå utgjøre en trussel.
Kvantedatamaskiner er en trussel mot vanlig algoritmer og krypteringer. En kvantedatamaskin kan dekryptere mange krypteringer som brukes i dag. Hvis vi skal kunne stole på informasjonssystemene som brukes, må det brukes krypteringer som kan tåle angrep fra en kvantedatamaskin (Grimstad.2020).
Kvantedatasikkerhet tilbys av tjenester som Amazon og Google, i disse tjenestene kan organisasjonene lagre informasjonen trygt. Teknologiutviklingen kan benyttes både instrumentelt som forsvarsmekanisme, men også i digitale angrep. En digital angrepssituasjon blir i denne sammenhengen «maskin mot maskin», i kontrast til «menneske mot maskin», som er den tradisjonelle oppfatningen av eksempelvis en hacking situasjon. Konsekvensen av at teknologien feiler kan være stor. Dersom noen klarer å komme seg inn i organisasjonens systemer og lekker opplysninger slik at det er brudd på personvernforordningen, kan dette føre til bot fra datatilsynet (Datatilsynet.2018). Organisasjonen forsikre seg mot angrep ved å ha en cyberforsikring[20]. En cyberforsikring kan forhindre denne økonomiske belastningen dersom organisasjonen skulle bli utsatt for kriminalitet, men det forsikrer ikke mot potensielle negative effekter på organisasjonens goodwill eller andre kulturelle aspekter (Vismas hjemmeside - goodwill).

2.1.3 Implementering av teknologi

Implementering kan forstås som å iverksette, utføre eller realisere ulike tiltak i organisasjonen (Nilstun 2020). I vår studie handler implementering om hvordan ny teknologi blir realisert blant de ansatte i organisasjonen.

Rindasu har forsket på hvordan regnskapsførere blir påvirket av nye teknologier. I likhet med teorien om teknologi, tar hun også opp samarbeidet mellom teknologien og mennesket. Regnskapsbransjen opplever nå økt mengde data og må nå å ta i bruk ny teknologi for å håndtere dataen. Ny teknologi er designet for å dekke et bredt spekter av krav, slik som big data, dataanalyse, mobilteknologi og skybaserte plattformer. Bruk av ny teknologi er ment for å skape fleksibilitet, stordriftsfordeler, mobilitet og mer nøyaktighet (Rindasu 2017.582).

---

[19] Kvantedatamaskiner: En kvantedatamaskin er en maskin som bruker informasjonsenheten qubit/kvantebit (en vanlig maskin bruker bits). Dette gjør at kvantemaskiner kan jobbe raskere enn en vanlig datamaskin. Kvantemaskiner kan oppnå kvanteoverlegenhet, noe som betyr at de kan løse problemer som ikke vanlige maskiner hadde kunnet løst innen rimelig tid. Dette antyder at de snart kan utføre oppgaver som hittil har vært umulige. (Linder, Skaar og Hansen.2019)
[20] Cyberforsikring er en forsikring som hjelper bedriftene dersom de har blitt utsatt for datakriminalitet. Hensikten med forsikringen er at skadeomfanget skal bli så lite som mulig (Gjensidige u.d.)

Kunstig intelligens og prosessautomatisering blir overtatt av robotikk. Robotikken tar nå repeterende oppgaver, tidligere utført av fagfolk. Dette frigir tid til mer komplekse arbeidsoppgaver som analyse og forretningsrådgivning. Kunstig intelligens og prosessautomatisering kan skape merverdi for regnskapsfirma (Rindasu.2017.582).
Big data er også blitt en del av regnskapsbransjen fordi det er relatert til sanntidsrapporteringsprosessen, eller monitoreringen.

I følge Rindasu krever bruk av ny teknologi, fagfolk som vil kunne utnytte ressursene effektivt (Rindasu 2017.587). Regnskapsførere bør fungere som et mellomledd mellom IT-avdelingen og lederne. IT-avdelingen kan bistå med råd om tekniske løsninger (Rindasu 2017. 587). Det har også kommet frem at læreplaner på studiesteder ikke fokuserer nok på teknologier, som skal sørge for å dekke kompetansekravet i arbeidslivet. Det har derimot vist seg at regnskapsførere har interesse av å ta i bruk den nye teknologien, på grunn av fordelene det gir (Rindasu 2017.588).
Det er ulike årsaker til sikkerhetsbrudd i digitale systemer. Den primære kilden er eksterne angrep, etterfulgt av feil systemkonfigurasjon, kompetansemangel hos ansatte, for vide tilganger, utilsiktet eksponering av sensitive data, svake passord og mangel på effektiv forebygging og kontroll (Rindasu 2017.589). Det er organisasjonene som er ansvarlige for å beskytte mot datalekkasjer, det kan gjøres ved å sikre at de ansatte er klar over risikoen forbundet med teknologien. Videre kan det hjelpe med en kontinuerlig styring av sikkerhetssystemene, som må vokse i takt med de nyeste informasjonsteknologiene. (Rindasu 2017.592)

I delkapitlene over har vi presentert hva teknologi er, hva digitalisering er og hvordan teknologien implementeres i informasjonssystemene. I neste del skal vi presentere hvordan ulike krefter rundt organisasjonene og ulike trusler, danner organisasjonenes trusselbilde.

2.2 Trusselbildet

Trusselbildet er en del av en organisasjons omgivelser. Organisasjonens omgivelser kan defineres som krefter som kan påvirke hvordan en organisasjon drives og dens tilgang til ressurser. Generelt blir organisasjoner påvirket av kulturelle, internasjonale, politiske, miljø, økonomiske og teknologiske endringer i omgivelsene, både på nasjonalt og internasjonalt nivå. Videre blir hver enkelt organisasjon påvirket av spesifikke omgivelser som leverandører, kunder og konkurrenter (Jones 2013.83) I hvilken grad en organisasjon blir påvirket av

omgivelsene rundt seg avhenger av tre faktorer; hvor dynamiske, hvor komplekse og hvor rike kreftene er (Jones 2013.88). Omgivelsens kompleksitet handler om antall spesifikke og generelle krefter som kan påvirke organisasjonen, samt hvor sterk påvirkningskraft disse har. Hvor dynamisk omgivelsene er, handler om hvor raskt de spesifikke og generelle omgivelsene endrer seg over tid. Hvor rike omgivelsene er handler om hvilke, og hvor stor tilgang organisasjonen har til ressurser som de avhenger av (Jones 2013.89).

Organisasjonsendring handler om at organisasjonen endrer sin struktur og kultur, for å kunne nå et mål de har satt for organisasjonen i fremtiden (Jones 2013.32). Vårt inntrykk er at en organisasjons omgivelser stadig blir mer komplekse. Organisasjonen vil derfor ha behov for å gå fra å endres seg gradvis, til å endre seg i takt med omgivelsene.

I denne delen har vi presentert hva organisasjonens omgivelser er, og hvordan disse omgivelsene kan påvirke en organisasjon. I neste del vil presentere hva sikkerhet og risiko er.

2.2.1 Sikkerhet

Sikkerhet kan ifølge Roar Thon (mediaplanet u.d) forklares som et fravær av uønskede hendelser. Begrepet sikkerhet brukes også til å beskrive tiltakene en organisasjon har mot truslene, eksempelvis antivirusprogrammer. I vår oppgave ser vi spesielt på informasjonssikkerhet knyttet til behandling[21] av informasjonsdata, og hvordan sikkerheten påvirkes av ulike trusler.

Risiko uttrykkes ved sannsynligheten for og konsekvensene av en hendelse. For å snakke om sikkerheten rundt informasjonssystemer, må vi først forklare begrepet; risiko. Risikobegrepet har utviklet seg til å inneholde tilsiktede gjerninger gjort av aktører med forsett. **Risiko er da definert som forholdet mellom faktorene; trussel, verdi og sårbarhet.** Dette forstås som at det er intensjon, kapasitet og motiv for den tilsiktede handlingen. Denne handlingen utføres enten fordi den har som mål å skade, ødelegge eller vinne. **Aktøren ønsker å utnytte sårbarheten i teknologien for å oppnå sitt mål**. Hvem som er trusselen, må ifølge Rolstadås m.fl. (2017.212) sees i sammenheng med bransjen og kunnskapen aktøren trenger.

Informasjonsverdier kan ifølge Rolstadås m.fl. være personopplysninger som avslører vår identitet eller helse. Sikring av informasjonsverdier deles opp i tre prinsipper, som beskriver

[21] *lagring og oppbevaring*

teknologiens evne til å ivareta informasjonens; **konfidensialitet, integritet og tilgjengelighet.** Konfidensialitet er å sikre at ingen uvedkommende har tilgang til, eller kjennskap om systemer. Integritet er å sikre at informasjon ikke kan endres. Tilgjengelighet er å sikre at informasjon og teknologi er til stede for eier og brukere.

Organisasjoner må vurdere om de skal ha alt ansvaret for teknologien internt, eller om de vil dele risikoen, ved å kjøpe digitale tjenester som driftes av andre (2017.213). Rolstadås m.fl. skriver at det har vært tilfeller der sensitive opplysninger om ansatte i Norge har blitt tilgjengelig for andre fordi det er kjøpt inn digitale tjenester fra andre land (2017.216). Ifølge SSB har 4,6 prosent av norske kommuner vært utsatt for virusangrep og annet som har ført til tap av data. I 2020 opplevde 20,1 prosent av statlige organisasjoner uautorisert tilgang til systemer eller data.

Organisasjoners sårbarhet øker når det innføres ny teknologi, fordi det blir større og mer omfattende. Det å skulle holde kontroll på alle systemene som samhandler blir en omfattende jobb. Eksempelvis har ansatte en IP-adresse[22] koblet til sitt adgangskort, som ofte har flere tilganger enn nødvendig for å utføre jobben. Dermed kan det føre til at personalet har tilgang til sensitive områder som datarom og arkiver. Videre poengterer Rolstadås m.fl. at den **største sikkerhetssvikten** en organisasjon har, er **mennesket selv**. Alle som jobber med digitale systemer, må derfor ha et bevisst forhold til informasjonssikkerhet og konsekvensene av sikkerhetsbrudd. Dette krever utvikling av hver og ens kompetanse. Det må være **fokus på risikobevissthet, risikoreduserende tiltak og digital atferd** (2017.218).

John A Pendley skriver at god sikkerhetspraksis skal falle naturlig. Ansatte skal behandle selskapets informasjon på lik linje med sin egen personlige informasjon. Han sammenligner ubeskyttet data med ubeskyttet husnøkkel. Pendley mener at hvis god sikkerhetspraksis blir en vane, så vil ikke ansatte like lett falle for phishing forsøk. I artikkelen presenterer Pendley måter finansbransjen kan forbedre informasjonssikkerheten, ved å gå fra passiv bevissthet til aktiv involvering i informasjonssikkerhet. Han legger vekt på at tiltakene er måter organisasjonene kan forbedre informasjonssikkerheten på, uten å legge mer arbeidsoppgaver på IT- avdelingen, da de allerede har tidkrevende oppgaver. Organisasjonen kan forbedre informasjonssikkerheten ved å **identifisere kritiske data og kryptere dem, systematisere reguleringer, etablere rutiner for bruk av mobile enheter og definere grunnleggende**

[22] *IP-adresse: Internet Protocol-adresse (IP-adresse) kan defineres som adressen til en enhet som er tilkoblet internett, for eksempel en pc eller en mobil. Hver enhet har sin unike identitet (Jensen 2018)*

rutiner for sikkerhet (Pendley 2018.53-55). Kritiske data er data som vil true organisasjonens eksistens eller rykte om det gikk tapt. Et eksempel på kritiske data kan være kundedata.

Alle ansatte må være klar over organisasjonens regler for mobile enheter og hvorfor reglene er satt. De ansatte må også være klar over sitt ansvar ved tap eller tyveri (Pendley 2018.57). Bruk av mobile enheter kan øke produktiviteten samtidig utgjør det en sikkerhetsrisiko, da mobile enheter blir lett stjålet eller mistet. Organisasjonen må vurdere om ansatte skal kunne knytte private mobile enheter opp mot arbeidsplassens nettverk (Pendley 2018.56.). Organisasjonene må sørge for at programvare er oppdatert, ansatte bør ikke bruke offentlige nettverk og bruke krypterte enheter slik at dataen blir ubrukelig i uvedkommende hender.

Alle organisasjoner bør ha et dokument med retningslinjer for IT-sikkerhet. Retningslinjer kan forbedre bevisstheten på informasjonssikkerhet og personvern. De ansatte må få informasjon om vanlige fallgruver ved passord, hvor ofte de må byttes og hva som er forskjellen på et svakt og et sterkt passord. Ansatte bør bruke to-faktor autentisering, da det er veldig vanskelig for hackere å ha tilgang til både primær og sekundærkilden til passord (Pendley 2018.57).

I denne delen har vi presentert hva sikkerhet og risiko er, og hvilke tiltak organisasjoner kan ta i bruk for å bedre informasjonssikkerheten. I neste del vil vi presentere hvordan informasjonssikkerheten er ved bruk av skytjenester.

2.2.2.Informasjonssikkerhet ved bruk av skytjenester

Skytjenester finnes i ulike former og gir kunden ulik tilgang og kontroll over applikasjoner, nettverk, operasjonssystemer og lagringsmuligheter. Datatilsynet deler skytjenestene inn i tre kategorier:

1. **Saas-programvare** går ut på at kunden bruker leverandørens programvare på en nettsky.
2. **Paas-plattform** der kunden bruker applikasjoner utviklet av leverandør.
3. **Iaas-infrastruktur** er levering av datastruktur som en tjeneste over et nettverk (Datatilsynet 2019).

En utfordring knyttet til bruk av skyløsninger, er hvem som har ansvaret for sikkerheten. I en undersøkelse utført av IBM kom det frem at det var stor variasjon i oppfatningen av hvem som hadde ansvaret for sikkerheten. En annen utfordring er knyttet til risiko-opplæring for de ansatte. Dersom ansatte installerer programvare på egenhånd utenfor godkjente prosedyrer, øker risikoen for angrep (Grini 2020).

I delkapittel 2.2.1 og 2.2.2 har vi presentert sikkerhet, ulike tiltak for å bedre sikkerheten generelt og sikkerhet knyttet til skytjenester. I neste delen vil vi presentere trusler og trender, som sier noe om de ulike truslene som kan påvirke informasjonssikkerheten og hvilke trusler som er størst i dag.

2.2.3 Trusler og trender

Trusler og trender er en årlig rapport fra Norsk senter for informasjonssikring (NorSIS), som presenterer de største digitale truslene. NorSIS har som mål å bidra til økt fokus på informasjonssikkerhet i Norske organisasjoner. I rapporten presenteres de fire største digitale truslene for 2021; løsepengevirus, kontokapring, verdikjedeangrep og svindel (NorSIS 2021)

Løsepengevirus har i løpet av det siste året blitt en av de største truslene for organisasjoner i Europa. Dette er en stor trussel da bare et klikk på feil link, kan føre til at all organisasjonens informasjon blir kryptert. Organisasjonen får ofte beskjed om at de kun får tilbake sin informasjon, mot å betale en sum med løsepenger til de som har utført angrepet. Et slikt angrep kan ligge lenge i systemet før det slår til, og kan på den tiden spre seg videre til skytjenester og andre tilknyttede IT-systemer (NorSIS 2021.4).

Kontokapring innebærer at kriminelle har fått tak i påloggingsinformasjon som ofte er fra lurt offeret med phishing. Denne informasjonen bruker de til å logge seg på kontoer som Facebook eller e-post. Dette kan føre til omdømmetap for organisasjoner hvis de kriminelle finner informasjon som de sprer videre (NorSIS 2021.6).

Verdikjedeangrep er angrep mot en usikret kilde i verdikjeden. De kriminelle angriper den usikrede kilden istedenfor å angripe målet direkte. På denne måten kommer de seg inn i systemet og kan enklere nå målet. Den usikrede kilden kan være hva som helst som er koblet mot internett, uten sikring; eksempelvis privat pc (NorSIS 2021.8).

Svindel - Svindlere spiller ofte på tillit, frykt eller fristelser. Svindel kan være phishing, direktørsvindel[23], falske nettbutikker og falske nettprofiler (NorSIS 2021.10).

Trend Micro Inc er et sikkerhetsselskap som i over 30 år har ønsket å gjøre utveksling av digital informasjon trygg, verden rundt. De samarbeider med organisasjonene; AWS, Microsoft, Google, IBM og vmware (Trend Micro u.d) De utarbeider hvert år en sikkerhetsrapport, i 2019 ble Norge rangert på femteplass i verden over land som var attraktiv for direktørsvindel (Knudsen.2019). I rapporten for 2020 har Trend Micro Inc fokusert mye på covid-19 pandemien. Bakgrunnen for det økte fokuset er den økte bruken av hjemmekontor under pandemien, og utvidet mulighetene for kriminalitet. Fra januar til juni 2020 ble det oppdaget nærmere 9 millioner sikkerhetstrusler som var relatert til pandemien. Sikkerhetstruslene er ikke knyttet til selve infeksjonen Covid-19, men de kriminelle sender eksempelvis mail om at postlevering er utsatt på grunn av pandemien og får offeret til å trykke på en link for å godkjenne at de har mottatt beskjeden. Dette kan sees i sammenheng med hvorfor organisasjoner har sikrede nettverk på arbeidsplassen som vi tok opp i delkapittel *2.1.1 Digitalisering.* Er de ansatte sikret med VPN[24] nettverk utenfor arbeidsplassen vil være mindre mottakelige for slike trusler. Ifølge Trend Micros rapport for 2020 var staten, helsetjenester, bank og regnskapsbransjen, teknologibransjen, olje og gass, og telekommunikasjon de som var mest utsatt for phishing.

Trend Micro anbefaler én sikkerhetsløsning som har flere lag, i motsetning til sikkerhetsløsninger som bare beskytter et program eller for en type virus. Dette mener de at vil gi flere indikatorer og vil hjelpe IT-ansatte med å kunne se et mer helhetlig bilde uten å bruke ekstra tid og ressurser på det. Trend Micro mener også at siden hjemmekontor er blitt en større del av de ansattes liv, er det ekstra viktig å lære opp de ansatte i informasjonssikkerhet. Trend Micro mener at ved å ta i bruk et program for all sikkerhet, vil det gjøre det lettere å oppgradere programmet. Oppdateringen vil også gjelde for ansatte på hjemmekontor, og det vil kreve lite nedetid[25].

I denne delen har vi presentert ulike trusler som kan påvirke informasjonssikkerheten. I neste del vil vi ta for oss to av de største truslene, nemlig phishing og menneskelige feil.

---

[23] Direktørsvindel er svindel der kriminelle utgir seg for å være ledelsen i organisasjonen Nettvett 16.10.19
[24] VPN: Virtuelt privat nettverk. Oppretter en tunell, som krypterer og sender all datatrafikken din gjennom en utgang. Data som kommer inn til deg via sider du besøker må gjennom VPN-tunellen før den kommer inn deg. Dette kan hindre avlytning og gi trygg tilgang til internett (Nettvett.26.10.20)
[25] Nedetid er den tiden organisasjonens systemer er utilgjengelig, under og etter et angrep.

Phishing

Phishing[26] er ifølge Europol en av kjernetruslene mot informasjonssikkerhet. Denne typen kriminalitet er ofte utgangspunktet for andre former for kriminalitet (NorSIS 2021.21).
I artikkelen "Cyber attacks for sale" av Meland og Sindre, kommer det frem at personer enkelt kan kjøpe ulike tjenester for å gjennomføre et angrep, via det "darkweb"[27]. Blant de mest populære tjenestene var "hackers for hire", account/password crackers» og "phishing kit" Hackers for hire er en tjeneste der kjøperen betaler for at noen andre skal utføre et angrep for dem. Account/password crackers er en tjeneste som gjør at kjøperen klarer å få tilgang til passordene i ulike tjenester. Phishing kit består av falske nettsider, som er klargjort for svindling. Ved at personer får tilgang til å kjøpe slike tjenester, tilrettelegger det for at flere kan utføre angrep uten å inneha stor grad av teknisk kunnskap (Meland og Sindre 2020).

Ifølge SSB ble 67,1 prosent av statlige organisasjoner og 52,9 prosent av kommuner i Norge utsatt for phishing i 2020 (SSB.2020). I en undersøkelse gjort av buypass viser det seg at tre av fem nordmenn har vært utsatt for phishing (Buypass.2020). Utgangspunktet og årsaken bak truslene som nevnt i 2.2.3 Trusler og trender, er ofte phishing eller menneskelige feil.

Datatilsynet skriver på sin nettside (17.07.20) at phishing er en effektiv måte kriminelle kan utnytte mennesker på, for å oppnå sine mål. Datatilsynet har laget en veiledning for hvordan organisasjoner kan beskytte seg mot phishing på. Phishing kan komme i form av lenker tilsendt av kjente og ukjente avsendere. Hvis avsender er noen mottaker, kjenner er sannsynligheten større for å bli lurt. Automatiserte forsøk på phishing er ofte mail som er standardiserte. Disse angrepene er ofte ute etter brukernavn og passord for å selge dem videre. Manuelle angrep er når den kriminelle "skreddersyr" mailen til mottaker som ved direktørsvindel, disse kan være vanskelig å oppdage. Kriminelle prøver å manipulere ansatte til å enten åpne eller klikke på en lenke. De kriminelle kan også prøve å lure de ansatte til å betale en falsk regning. Når mottaker klikker på lenken installeres malware som

[26] Phishing kan defineres som manipulering der den kriminelle prøver å lure noen til for eksempel å trykke på en lenke. Dersom personen trykker på lenken, installeres skadevare på personens enhet (Datatilsynet 2020)
[27] Det mørke nettet eller darkweb har oppstått på grunn av misbruk av anonymitet i kommunikasjonskanaler realisert ved hjelp av en anonym ruting. Dette latt seg ikke spore enkelt. Dette misbrukes for å gjøre ulovlige handlinger. (Knapskog 13.03.18)

ransomware[28], slik at kriminelle får tak i brukernavn og passord. Brukernavn og passord kan brukes for å få tak i informasjon fra organisasjonens interne systemer.

Datatilsynet kaller phishing for det innledende angrepet, dersom phishingen er vellykket vil det følge et etter-angrep. Det vil si at de kriminelle nå har tilgang på organisasjonens systemer og informasjon som den kan bruke (17.07.20). Målet for en organisasjon er å få stoppet alle angrep slik at det ikke påvirker driften. Om den kriminelle har lykkes med innledende angrep, vil det være hensiktsmessig å minimere skaden slik at minst mulig informasjon lekkes. Organisasjonen må prøve å redusere risiko og gjenopprette normaltilstand. Dette kan gjøres ved å endre passord og fjerne alle tilganger på den utsatte kontoen. Det er også viktig at organisasjonen har rutiner for sikkerhetskopiering og gjenoppretting av data, slik at de raskt kan gjenopprette driften (Datatilsynet 17.07.20). Organisasjonen må skaffe seg oversikt over hendelsesforløpet og hvem den kriminelle aktøren er. Eksempelvis, mottaker og avsender av skadelig e-post, sporing av IP-adresser og kartlegging av hvilke data de kan ha hentet ut. For å få tak i denne informasjonen er det viktig at organisasjonen har et loggsystem. Loggsystemet er viktig for å kunne lage forebyggende tiltak (Datatilsynet 17.07.20). I etterkant av et angrep må organisasjonen melde avvik og informere de berørte.
Brudd på personopplysningssikkerheten skal meldes til Datatilsynet (Personvernforordningen artikkel 33). Organisasjonen må også vurdere om de registrerte skal få informasjon om bruddet (Personvernforordningen artikkel 34). Organisasjonen må også beskytte seg mot etterfølgende angrep, eksempelvis ved å oppdatere datasystemene ofte og ha tofaktorautentisering [29] (Datatilsynet 17.07.20).

Datatilsynet mener at for å beskytte seg mot phishing må **organisasjonen ha tekniske og organisatoriske tiltak**. Organisatoriske tiltak som opplæring og bevisstgjøring av de ansatte slik at de mindre sannsynlig blir lurt av falske e-poster, ved å e teste de ansatte slik at de kan se hvor godt en ansatt hadde kjent igjen et phishing forsøk. Organisasjonen kan også opprette en egen kanal hvor de ansatte kan få hjelp til å identifisere e-post eller telefonnummer de er usikre på. Tekniske tiltak kan være oppdatert antivirus-/antimalwareløsning og automatisk filtrering av e-post, som filtrerer bort e-post fra kjente kriminelle (Datatilsynet 17.07.20).

[28] *Ransomware er en form for malware. Ransomware blokkerer informasjonen, slik at personen ikke har tilgang til informasjonen lenger. Kriminelle bruker ofte dette for å presse ut penger av personer, mot at de ikke publiserer innholdet (Netsecurity 2021)*
[29] *Tofaktorautentisering: er et ekstra sikkerhetsnivå for innlogging på kontoen, som gjør at det kreves noe i tillegg til brukernavn og passord. Eksempel kan være å få tilsendt en kode på SMS, som må brukes i tillegg (Datatilsynet 2020).*

Menneskelige feil

Menneskelige feil er som ordene beskriver, feil gjort av mennesker. Mørketallsundersøkelsen fra 2018, viser at over halvparten av sikkerhetsbrudd i norske organisasjoner skyldes menneskelige feil (NorSIS 2019-2020.25). Derfor er menneskelige feil en del av trusselbildet som organisasjonene bør forholde seg til. Mennesker gjør feil og enn så lenge er de fleste organisasjoner bestående av mennesker, dermed bør organisasjoner regne med den eksisterende risikoen knyttet til menneskelige feil. Bakgrunnen til feilene vi belyser i denne studien kan variere, men sees i sammenheng med at systemene er komplekse og krever at de som bruker systemene har riktig kompetanse.

Teknologien har utviklet seg fort og blitt implementert i arbeidslivet. Tidligere skolegang har ikke fokusert like mye på teknologiutvikling. Resultatet av den raske implementeringen er at mange ansatte sannsynligvis har hatt en praktisk og gradvis teknologisk opplæring.
Disse ansatte kvalifiserer ikke for å gjennomskue den stadig mer "menneskelige-tilnærmingen" de kriminelle bruker. AI og stordata brukes i stor grad av kriminelle, det gir dem bedre innsikt i personene de skal svindle. De kriminelle kan derfor være mer målrettet og det fører til at de er vanskeligere å avsløre. AI og stordata gir de kriminelle tilgang til opplysninger som arbeidssted, arbeidstittel, personlige interesser og kommende arrangementer. Dette inkluderer de i e-postene og gjør budskapet mer troverdig (NorSIS 2019-2020.33).

Studien av Banker og Feng 2019 deler inn brudd på sikkerheten i tre deler; **systemfeil, kriminell svindel og menneskelige feil.** Systemfeil handler om hendelser forårsaket av både prosessfeil og ondsinnede hacking. En prosessfeil er ofte et resultat av dårlig designet IT-system. Kriminell svindel inkluderer ikke-systemrelaterte bruddhendelser, på grunn av svindel begått av ansatte, entreprenører eller tredjeparter. Menneskelige feil omhandler bruddhendelser forårsaket av feil, uaktsomhet eller uforsiktighet. Ifølge Microsoft Norge skyldes 80 prosent av datainnbrudd i skyløsninger på grunn av tap av påloggingsinformasjon (NorSIS 2019-2020.34). Big Data gjør organisasjoner mindre rustet for å håndtere de nye måtene kriminelle arbeider for å svekke organisasjonene. NorSIS poengterer at trusselbildet nå henger sammen med at stadig flere enheter er koblet på nett og i skyen. Hvis noen får påloggingsinformasjonen vår på nett, kan det sammenlignes til at vi gir dem nøkkelen til livet vårt (NorSIS 2019-2020.34). Når organisasjoner er tilkoblet nett i en verdikjede, er det flere svakheter for de kriminelle å angripe. Det betyr at vi må tenke sikkerhet på en ny måte.

Skallsikringen skjer innenfra like mye som utenfra. Med bakgrunn i trusselbildet er det blitt enda viktigere at ledere har fokus på digital kompetanse og sikkerhetskultur (NorSIS 2019-2020.35). For å kunne beskytte organisasjonen mot kriminalitet må ansatte også ha oversikt over verdiene og verdikjedene som er i organisasjonen (NorSIS 2019-2020.35).

Hvis en forestiller seg at det er kun én måte å feile på, blir mennesket ofte sett på som den som har skylden. Studier viser at det er mer komplekst enn som så. Det som vi ser på som en menneskelig feil, er egentlig en feil som har skjedd på grunn av flere kognitive, samarbeidene og organisasjonelle faktorer. Dette synliggjøres ved å se forbi merkelappen «menneskelige feil», da synes de systematiske faktorene til den menneskelige oppførselen (David Woods et al 2010.35).

David Woods et al beskriver en «latente feil modell» (2010.51). Feilene som skjer, er på bakgrunn av hull i komplekse system. Modellen består av flere lag med triggere som: dårlig kultur i organisasjonen, arbeidspress, teknologi, dårlig opplæring og individuell distraksjon som fører til at mennesket feiler. (2010.55) Modellen kan bidra til å forstå at mennesket ikke er årsaken til feilen, men at det er et eller flere hull i systemet som skaper feilen.

En annen årsak er bruk av ny teknologi (2010.143.). Når organisasjoner tar inn ny teknologi på arbeidsplassen, så må organisasjonene tenke over at det gjerne endrer en hel aktivitet. Den gamle arbeidsmetoden endres, ved at teknologien endrer måten arbeidsoppgavene gjøres på (2010.146). Forskning viser at det å presentere teknologi som skal redusere arbeidspress blant de ansatte, ikke nødvendigvis gjør det.
Ny teknologi gir de ansatte nye oppgaver, som gjør at de må tenke på en annen måte.
De ansatte må kanskje ha en annen kunnskap eller kommunisere på en ny måte, som skaper muligheter for menneskelige feil (2010.147). Når den nye teknologien gjør noe så flyttes fokus hos den ansatte fra hva den selv gjør, til hva teknologien gjør (2010.148). Ny teknologi som skyløsninger og mobilteknologier kan være kostnadseffektive.
Studier viser at ansatte ikke vet hva som er riktig oppførsel når de bruker disse teknologiene (Rindasu 2017.584). Dette viser at det er en miskommunikasjon mellom teknologien og mennesket. Det er først når denne overraskende situasjonen er over at den ansatte kan reagere på situasjonen. Studien utført av Banker og Feng 2019 sier at IT-ansvarlig er ansvarlig for å etablere et IT-system som skal minimere risikoen for systemfeil.
David Woods et al foreslår at istedenfor å redusere menneskelige feil, inneholder teknologien feil som skjer i samhandlingen med mennesker. Så istedenfor at teknologien tar over for

mennesker og dermed reduserer kompetansebehovet til den ansatte, bare endrer den kompetansebehovet (2010.153).
Årsaken til sikkerhetshendelser er forskjellige, og den primære kilden er eksterne angrep, etterfulgt av feil konfigurasjon av systemene, mangel på passende ferdigheter hos ansatte, overdrevne tilgangsrettigheter og utilsiktet eksponering av sensitive data. (Rindasu 2017.589).

Vi har i denne delen presentert ulike trusler og trender som påvirker en organisasjon, med fokus på de største truslene som er phishing og menneskelige feil. I neste del skal vi presentere hvordan organisasjonene kan forebygge og beskytte seg mot de nevnte truslene.

2.3 Forebygging og beskyttelse

Forebygging innebærer hvordan organisasjonen kan forebygge at trusler fører til stor skade for organisasjonene. Organisasjonene kan forebygge ved ulike tiltak som risikoanalyse og internkontroll. Beskyttelse handler om hvordan organisasjonene skal beskytte seg mot kjente trusler. Dette kan gjøres ved ulike tiltak som fokus på ledelse, lovverk og opplæring blant ansatte.

En **risiko- og sårbarhetsanalyse (ROS)** er en kjent måte å håndtere risiko på.
Risikovurdering er metode som brukes for å finne ut hvor godt organisasjons verdier er beskyttet mot uønskede hendelser og trusler. Denne metoden sier noe om det er en type risiko organisasjonen kan akseptere, reduseres via sikkerhetstiltak, overføres til andre eller om trusselen kan unnvikes (NHO 2019.39). Arbeidsmiljøloven, personopplysningsloven, arbeidsplassforskriften og internkontrollforskriften inneholder alle **krav til gjennomføring av risikovurdering** (NHO 2019.39) Helhetsvurdering av risikoen er en vurdering av verdier, trusler, sårbarhet og tidsregnskapet[30] (NHO 2019.46). Konklusjonen av ROS-analysen skal være, **hvor farlig er de uønskede hendelsene når sikkerhetstiltakene er trukket fra.**
Her prøves det så godt det lar seg gjøre å ha en balanse mellom verdier, trusler og tiltak (NHO 2019.47).

[30] *Tidsregnskapet er tiden fra en trussel er oppdaget til den er avverget eller overført til andre.*

Konsekvens og sannsynlighet	1. Ubetydelig	2. Mindre alvorlig	3. Betydelig	4. Alvorlig	5. Svært alvorlig
1. Lite sannsynlig	1	2	3	4	5
2. Noe sannsynlig	2	4	6	8	10
3. Sannsynlig	3	6	9	12	15
4. Meget sannsynlig	4	8	12	16	20

Figur 2.3 Risikoanalyse (Utarbeidet etter NHOs modell)

Hendelser i **røde** felt: Tiltak nødvendig, i utgangspunktet ikke akseptabelt

Hendelser i **gule** felt: Tiltak må vurderes

Hendelser i **grønne** felt: Ikke stor risiko, tiltak kan vurderes

En risiko- og sikkerhetsanalyse er aldri endelig. Sikkerhetsutfordringer endrer seg hele tiden og er dermed en kontinuerlig prosess. Risikovurdering må dermed gjentas jevnlig (NHO 2019.48).

I neste del skal vi presentere rammeverk for internkontroll.

2.3.1 Rammeverk for internkontroll

Rammeverk for internkontroll som er utarbeidet av digitaliseringsdirektoratet, kan brukes av organisasjoner for å vedlikeholde informasjonssikkerheten internt. Rammeverket består av etableringsaktiviteter og systematiske aktiviteter (Digdir1). Etableringsaktiviteter består av aktiviteter som bør gjøres i forkant og i forberedelsesfasen av internkontrollen (Digdir1).

Først må organisasjonen avklare behov og lage en plan. Det gjøres ved å analysere statusen den er i. Resultatet av analysen kan samles i en business continuity plan. En business continuity plan er en plan som beskriver hvordan organisasjonen skal opprettholde driften når uplanlagte hendelser skjer. Planen inneholder ofte en sjekkliste over rekvisita og ressurser, sikkerhetskopiering av data og hvor disse lagres. Den inneholder også ofte kontaktinformasjonen til beredskapspersonell og nøkkelpersoner. I tillegg en detaljert strategi for hvordan driften skal kunne opprettholdes videre (IBM.2020). Organisasjonen må analysere om arbeidet rundt informasjonssikkerhet er godt nok. Analysen bør utføres av ansatte som kjenner organisasjonen godt. I analysen bør det komme frem hvilke punkter som

bør forbedres og hva som er målet. Organisasjonen bør velge en person som skal følge opp arbeidet rundt internkontrollen.

Etablering i organisasjonen handler om å utarbeide dokumenter og opplæring av ansatte. Hensikten med det er å ha retningslinjer for uplanlagte hendelser i de etablerte rutinene. En slik plan bør derfor være langsiktig og det er viktig at planene følges opp av ledelsen (Digdir1.). Deretter må organisasjonen få på plass de viktigste aktivitetene. Styrende dokumenter avklarer hvem som har ansvaret for hva, og hva som skal gjøres. De styrende dokumentene er derfor viktig for å sørge for at internkontrollen blir gjennomført som ønsket. Dette kan eksemplifiseres med **ISO sertifiseringer**. ISO sertifiseringer er standarder som er utarbeidet av den internasjonale standardiseringsorganisasjonen. Innenfor informasjonssikkerhet er **ISO 27001** relevant. For å få en ISO 27001 sertifisering stilles det krav til etablering, implementering, vedlikehold og forbedring av ledelsessystem (Standard Norge.2021). **ISO 27017** handler om informasjonssikkerhet knyttet til levering og bruk av skytjenester (Standard Norge 27017:2015).

Ledelsen i organisasjonen bør ha hovedansvaret med internkontrollen. Hvem som har ansvar for de ulike oppgavene, bør være tydelig og utarbeidet i et dokument. Organisasjonen bør utforme informasjonsmateriell knyttet til internkontrollarbeidet. Det bør videre vurderes hvordan opplæring og informasjon bør gis til de ulike aktørene i internkontrollarbeidet. Organisasjonen bør etablere et system for å registrere hendelser og avvik. Det bør være klart hvem som skal rapportere, hvordan håndtere hendelsen og hvem som skal informeres om hva (Digdir1.)

Tredje aktivitet er å **skape en god plattform for internkontrollen.**
Sikkerhetstiltakene som blir etablert bør være rettet mot behovet i organisasjonen. Rammeverket skal brukes til dokumentasjon av internkontrollen. Den bør inneholde formål, bruksområde og tydeliggjøre hva som skal loggføres og hva som skal være tilgjengelig på organisasjonens intranett (Digdir1.)

Siste aktivitet er å lage et **godt grunnlag for sentrale systematiske aktiviteter.**
Organisasjonen kan ta utgangspunkt i typiske oppgave- og informasjonstyper som blir behandlet i organisasjonen, og identifisere risikofaktorer knyttet til disse. Sikkerhetstiltak og regelverk knyttet til de ulike arbeidsoppgavene bør identifiseres i organisasjonen. (Digdir1). **Ledelsens styring og oppfølging** er grunnlaget for overordnede styrende dokumentene.

Ledelsen har ansvar for oppfølging av arbeidet gjennom organisasjonsstyring. (Digir2). Som figur 2.3.1 viser, påvirker ledelsen alle punktene i internkontrollen.

Risikovurdering er kjernen i internkontrollen. Risikoen må identifiseres, analyseres og evalueres. Det kan gjelde hele organisasjonen, enkelte prosesser eller helt spesifikke oppgaver. Her er det leder som sørger for at de riktige risikovurderingene tas.

Risikohåndtering handler om hvordan håndtere risikoen og iverksette tiltak. Dette skal gjøres i samsvar med fastlagte kriterier for akseptert risiko.

Akseptert risiko er noe organisasjonen har bestemt seg for at den kan leve med (Digir2). Digitaliseringsdirektoratet beskriver at ISO- 27002 har som hensikt å redusere ulike sårbarheter til et akseptabelt nivå, sørge for at lover og forskrifter blir fulgt og at interne og eksterne krav blir ivaretatt (Digdir. ISO/IEC 27002).

Overvåking og hendelseshåndtering er rutiner som avdekker avvik, slik at de kan følges opp. Hendelseshåndteringen er viktig for læring da det er erfaring som tas med videre (Digir2). **Måling, evaluering og revisjon** er når organisasjonen kontrollerer om tiltakene fungerer. Målingene må gjennomføres både ved etableringen og når tiltakene er i bruk. Disse utgjør et viktig beslutningsgrunnlag for lederne (Digir2). ISO 27005 handler om hvordan sørge for informasjonssikkerhet på bakgrunn av risiko som er kartlagt i organisasjonen (Standard Norge).

En god sikkerhetskultur i organisasjonen er viktig for at internkontrollen skal fungere og ansatte skal lære. God **kommunikasjon** legger til rette for læring, kompetanse- og kulturutvikling. Dette er viktig for hendelseshåndtering og er det som gjør en organisasjon i stand til å jobbe samlet med informasjonssikkerhet (Digir2).

Figur 2.3.1: Rammeverk for internkontroll (bilde tatt fra digitaliseringsdirektoratet - systematiske aktiviteter (Digir2)

2.3.2 Ledelse og ansvar

Ledelsen har ansvar for å etablere rammeverk for internkontroll i organisasjonen. Ledelsen bør sørge for god styring og kontroll av informasjonssikkerheten, for å sørge for at organisasjonen er drevet på en god måte (Digitaliseringsdirektoratet u.d). I 1984 påpekte konsulentselskapet EY at datasikkerhet ***ikke burde overlates til teknologer, men at det burde være et viktig tema for leder***e" - (Roar Thon Mediaplanet. ud.) Dette begrunnes med at det krever systematisk fokus på samspillet mellom mennesker og teknologi, prosesser, organisasjonskultur og ledelse. Vi anser det som at hvis hele organisasjonen samarbeider om informasjonssikkerheten, med lederne i spissen vil det gi et bedre resultat enn hvis IT-avdelingen skal være alene om det.

I komplekse organisasjoner som Azets og Visma må de ansatte forholde seg til personopplysningsloven, lov om god regnskapsførerskikk og egne databehandleravtaler. Alle disse lovene har påvirkning på informasjonssikkerheten og hvordan det skal håndteres. Lederne må legge opp til kunnskapsdeling i organisasjonen, for å sørge for at de ansatte kjenner til innholdet i disse lovene (Nesheim & Olsen 2011). Et kunnskapsnettverk for de ansatte, er en måte ansatte kan utveksle erfaringer og spre beste praksis på. Nesheim og Olsen undersøkte i 2011 hvordan dette kan gjøres i komplekse organisasjoner. I deres undersøkelser ble nettverkene ledet av en fagleder som ikke var en linjeleder. Kunnskapsnettverket ble fulgt opp av linjeledere. Nettverkene inneholdt forelesninger, diskusjoner og relasjonsbygging fysisk og digitalt. De ansatte i undersøkelsen svarte at kunnskapsnettverkene ga dem erfaring og læring, forbedring i ytelse og høyere etterlevelse av styrende dokumenter. Ansatte opplevde også egenutvikling og større personlige nettverk som følge av kunnskapsnettverket.

Datatilsynet informerer om organisasjonens plikter i forbindelse med **GDPR.** En viktig plikt alle organisasjoner har, er å ha oversikt over hvordan den samler inn og behandler personvernopplysninger. Videre må organisasjonen ha klare mål om hvorfor de samler inn personinformasjon og hva den skal brukes til. Det er også viktig å vite hvilken type informasjon som samles inn, da det er egne regler organisasjonen må forholde seg til når det gjelder spesielt sensitiv informasjon[31](Datatilsynet u.d.).

[31] *Sensitiv informasjon som helseopplysninger reguleres av DPIA.*

Standarden for god regnskapsføringsskikk skal gi regnskapsbransjen retningslinjer for god regnskapsføringsskikk (Regnskap Norge u.d.). Organisasjonen bør sørge for at alle medarbeiderne har skrevet under på taushetserklæring. I tillegg bør andre som har tilgang til regnskapsmaterialet eller annen dokumentasjon, også signere en taushetserklæring. Taushetsplikten er varig, og gjelder selv etter ansatte har sluttet i organisasjonen (Regnskap Norge u.d.). Kapittel 2.8.5 i standarden omhandler IT-sikkerhet. Organisasjonen skal sørge for god sikring av programvaren slik at ingen uvedkommende får tilgang, kan gjøre endringer, slette eller ødelegge data (Regnskap Norge u.d.).

Kapittel 2.8.6 handler om ekstern drift av informasjons- og kommunikasjonsteknologi (IKT). Her kommer det fram at en avtale med en ekstern leverandør bør etterleve kravene som finnes i en databehandleravtale. En databehandleravtale skal sikre at personopplysninger blir behandlet i henhold til personopplysningsloven. Organisasjoner som tar i bruk underleverandører, er pliktet til å utarbeide en databehandleravtale (Datatilsynet 2018). Selv om organisasjonen tar i bruk eksterne leverandører til drift av IKT systemene så er det fortsatt organisasjonen som har det formelle ansvaret når det gjelder informasjonsbehandling, dokumentasjon og oppbevaring av data (Regnskap Norge u.d.).

I neste del skal vi presentere hvordan fokus på opplæring og kompetanse blant de ansatte, kan forhindre menneskelige feil.

2.3.3 Opplæring og kompetanse

Opplæring og kompetanse er viktig for å forhindre menneskelige feil. Det kommer tydelig frem i undersøkelsen gjort av NorSIS. En måte å øke fokus på opplæring innenfor informasjonssikkerhet er Norsk senter for informasjonssikkerhets sikkerhetsmåned, som er en kampanje som skal gi økt kunnskap og bevissthet om informasjonssikkerhet (mediaplanet u.d).

NorSIS publiserte i 2020 en undersøkelse om nordmenn og digital sikkerhetskultur. I undersøkelsen svarte kun 22 prosent av intervjuobjektene at de hadde fått organisert opplæring i digital sikkerhet. Av de som hadde fått organisert opplæring, svarte 46 prosent at de opplevde at de hadde fått bedre ferdigheter innenfor sikkerhet i etterkant av opplæringen (NorSIS 2020.37). Videre viste studiene at 88 prosent av intervjuobjektene vet hva digital sikkerhet er, likevel er det 70 prosent som mener at de utsetter seg for risiko på tross av dette.

NorSIS mener at årsaken kan skyldes fokuset på opplæringen, at opplæringen ikke bidrar til nok atferdsendring. NorSIS legger vekt på at opplæringen ikke nødvendig handler om kunnskapen, men handler om en atferdsendring som skal gjøre de ansatte i stand til å ta valg som ikke utsetter dem for sikkerhetsrisiko. Opplæringen bør skje jevnlig, slik at de ansatte ikke glemme hva de skal gjøre (NorSIS 2020.63). NorSIS presenterer Banduras teori på at en god sikkerhetsopplæring bør fokusere på mottakerens mestringsforventning. Bandura sin teori om mestringsforventning sier at mestringsforventning vil påvirke presentasjon, ambisjon og motivasjon (NorSIS 2020.65). I undersøkelsen legger de vekt på følgende tiltak som kan øke mestringsforventningen til mottakeren:

Egen tidligere erfaring for å mestre aktiviteten: En god sikkerhetsopplæring bør derfor inneholde progresjon i vanskelighetsgrad. Opplæringen bør bygge på det som er lært tidligere, og med økende vanskelighetsgrad. Mestringsforventningen som den ansatte opplever blir assosiert med deres tidligere suksess.

Vikarierende erfaring i form av modellering: Dersom en selv ikke har erfaring med opplæringen, kan den ved å observere andre som utfører aktiviteten øke mestringsfølelsen. Eksempelvis opplæring via videosnutter.

Verbal overtalelse: En måte å øke mestringsfølelsen til de ansatte på, er at lederne oppmuntrer de ansatte til at de kommer til å klare opplæringen.

Fysiologisk aktivering: Opplæringen innenfor informasjonssikkerheten bør ikke gjennomføres i omgivelsene som stresser de ansatte (NorSIS 2020.71).

I et felteksperiment ble effekten av hvordan opplæring knyttet til sikkerhet påvirker sjansen for å bli utsatt for phishing angrep undersøkt. (Bora, Lee og Kim 2019, 1157-1158) Undersøkelsen viste at 7.7 prosent av opplært ansatte gikk på phishing angrepet og av de som ikke hadde fått opplæring var det 12,8 prosent som gikk på phishing angrepet. (Bora, Lee og Kim 2019, 1164-1165)

I Romania har problemene med nye teknologier innen regnskapsfeltet vært forsket på de siste årene, fokuset i forskningen har vært ferdighetene til brukerne. Å jobbe i skyen har blitt vurdert som et viktig tema, da det fører til nedgang i antall feil ved å raskere identifisere dupliserte dokumenter og transaksjoner (Rindasu 586.2017). En annen studie av Rindasu som omhandler regnskapsføreres vilje til å akseptere skyløsninger, har lagt vekt på at det er stor

interesse for fordelene med skyløsninger. Som nevnt tidligere i studie er det også kommet frem til at læreplaner på studiesteder ikke fokuserer nok på teknologier for å skape et tilstrekkelig grunnlag til å effektivt kunne dekke kompetansenivået (Rindasu 588.2017).

Security Awareness Improvement Tool in the Workplace (SAWIT) er et nytt web-basert verktøy som har som formål å øke bevisstheten tilknyttet sikkerhet blant ansatte i organisasjonen. Ansatte som ikke har nok kunnskap om phishing eller andre sikkerhetstrusler er den største årsaken til angrep i organisasjonene. Det er derfor viktig å investere i og lære opp ansatte innenfor sikkerhet, da IT-ansvarlig ikke kan ha alt ansvaret selv (Kovacevic, og Radenkovi´c 2020, 2). SAWIT- verktøyet foregår gjennom fire ulike faser; sosialisering, eksternalisering, kombinasjon og internalisering. For å få et samlet bilde av sikkerhetsnivået blant de ansatte, utføres det en forhåndstesting (sosialisering) Her blir den tause kunnskapen til den ansatte målt, og det vil bli foreslått passende opplæring ut ifra dens nivå. Videre vil de ansatte få opplæring i de områdene som de hadde lite kunnskap i (eksternalisering).
Den tredje fasen består av at ansatte utfører en kort test for å måle i hvilken grad de ansatte har tilegnet seg kunnskapen. Til slutt måles den faktiske atferden til de ansatte for å undersøke om deres sikkerhetsatferd har endret etter bruk av SAWIT-verktøyet (Kovacevic, og Radenkovi´c 2020, 7). SAWIT- programmet ble testet ut av 22 studenter, og i spørreundersøkelsen i etterkant kom det fram at 86 prosent av intervjuobjektene synes at programmet er nyttig. 82 prosent svarte at det ga et godt grunnlag for bevissthet knyttet til informasjonssikkerhet (Kovacevic, og Radenkovi´c 2020,9).

I neste del skal vi presentere hvordan vi har brukt kvalitativ metode for å undersøke om teori og forskning vi samlet inn, samsvarte med praksis. Vi vil vise hvordan vi har analysert intervjuene for å lære mest mulig, finne likheter og ulikheter.

3.0 Kvalitativ metode

I dette kapittelet vil vi beskrive hvordan vi valgte forskningstilnærming, design og hvilken strategi vi brukte. Når vi bruker metode, så følger vi en bestemt vei mot målet. Vi samler inn data, tolker og analyserer disse. Den hjelper oss å finne ut om konklusjonene våre stemmer med virkeligheten eller ikke. (Johannessen, Christoffersen og Tufte 2011.33) For å få klarhet i hvordan problemstillingen blir håndtert i praksis vil vi bruke kvantitativ metode, i form av flere semistrukturerte dybdeintervju. Gjennom arbeidet med metode og analyse har vi fulgt samme underspørsmål og kategorier som oppgaven er strukturert etter *jf. 1.3.1 oppgavens struktur*.

3.1 Forskningstilnærming og design

Vi har tatt i bruk et **deskriptivt design**. Et deskriptivt design skal beskrive en situasjon på et gitt område, og kan brukes til å se sammenhengen mellom flere variabler (Gripsrud 2016, 50). Ved bruk av et deskriptivt design kan vi ikke undersøke om det er en kausal sammenheng, men bare undersøke om det er **samvariasjon mellom variablene** (Gripsrud 2016, 50). Vår problemstilling er

"Hvordan påvirkes informasjonssikkerheten i Azets og Visma av teknologiutvikling?"

For å svare på problemstillingen har vi delt den inn i tre underspørsmål;

1. Hvordan påvirker ny teknologi og digitalisering Azets og Visma?
2. Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?
3. Hvordan forebygger Azets og Visma de største truslene?

Vi ønsker derfor å finne ut om det er samvariasjon mellom teknologi, trusselbildet, forebygging og beskyttelse, ledelse og ansvar, opplæring og kompetanse.

Vi samlet inn kvalitative primær og sekundærdata, i form av semistrukturerte **dybdeintervjuer**. Easterby-Smith et al definerer primærdata som ny informasjon som forsker skal samle inn. Primærdata kan være informasjon fra sikkerhetseksperter, om hvordan de oppfatter sammenhengen mellom teknologiutvikling og risiko. Det kan også være direkte

informasjon fra de ansatte om hvilken opplæring de har innenfor informasjonssikkerhet (2018.173).

Sekundærdata, er eksempelvis nettsiden til Azets og Visma, rapporter fra SSB og tidligere forskning som er gjort på lignende tema. Easterby-Smith et al definerer sekundærdata som data som allerede eksisterer (2018.173). Sekundære tekstdata som eksemplene over, er skriftlige informasjonskilder som er produsert for en annen grunn enn forskningen, men er relevant til hvilket som helst forskningsprosjekt. De blir ofte kalt for ikke-responsive data (Easterby-Smith et al. 2018.174). Sekundærdata sparer forskeren for tid, de er ofte av høy kvalitet om det er produsert av organisasjonen selv. Forskere skal også være kritisk til denne informasjonen fordi den prøver kanskje å fremstille organisasjonen på en god måte, altså at det kan foreligge et bias.

Vår forskningstilnærming startet med å samle inn sekundærdata i form av teori og forskning, for så gjøre teori om til temaer for intervjuguide. Intervjuguiden fungerte som vårt verktøy til å samle inn primærdata. I neste delkapittel skal vi gå nærmere inn på hvordan vi samlet inn primærdata.

3.2 Populasjon og utvalg

Populasjonen i denne studien er ansatte i Azets, Visma og én uavhengig kilde. Vi valgte å kontakte Azets og Visma fordi de er store organisasjoner som kunne gi oss mye data til våre intervju. Organisasjonene har også egne sikkerhetseksperter som kunne gi oss informasjon om hvordan endring i bruk av teknologi påvirker informasjonssikkerheten.
Begge organisasjonene ligger også lokalt plassert. Dersom samfunnet hadde tillatt det, hadde vi hatt muligheten til å møte intervjuobjektene og snakke med dem ansikt til ansikt.

Vår uavhengige kilde valgte vi å intervjue fordi vi ville ha innslag av hvordan en sikkerhetsekspert jobber som konsulent. Som konsulent er sikkerhetseksperten i arbeid for mange aktører både statlig, kommunalt og privat. Vi tenkte konsulenten kunne være et godt bidrag til vår oppgave, da vi hadde to store private organisasjoner som hovedfokus.

Videre deles populasjonen inn i et utvalg. Vi har tatt i bruk et vurderingsutvalg som er en blanding av sannsynlighet og ikke-sannsynlighetsutvalg. Azets og Visma ble valgt fordi de har bestemte egenskaper, men vi hadde ikke bestemt hvilken sannsynlighet det var for at de ble valgt. Vår uavhengige kilde ble valgt ut spesifikt på grunn av sin arbeidsstilling (Gripsrud

2016.169). Vi har vist utvalget vårt i en figurfremstilling *figur 3.2*, denne viser hvor informantene jobber og hva vi vil kalle dem i analysedelen.

Vi valgte først å intervjue sikkerhetsekspertene i de tre organisasjonene. Vi ønsket å få deres perspektiv som eksperter, slik at vi kunne stille mer konkrete spørsmål til de ansatte som jobber i lavere linjer. Vi spurte ekspertene om de anbefalte oss å snakke med noen andre spesifikke personer i organisasjonen, og kontaktet dem. Videre valgte vi å intervjue ansatte i organisasjonen, som ikke jobbet med sikkerhet for å se om noe av det ekspertene hadde uttalt, ble gjenspeilet av dem. Vi intervjuet fire personer innenfor HR, salg, rekruttering og økonomi for å dekke flest mulig roller.

	Azets	Visma	Uavhengig	Intervju-tid
Sikkerhetsekspert	Ekspert 1	Ekspert 2	Ekspert 3	6 timer
HR		HR		1 time
Salg		Ansatt 1		1 time
Rekruttering	Ansatt 2			1 time
Økonomi	Ansatt 3			1 time

Figur 3.2 Fremstilling av intervjuobjektene.

I neste del vil vi forklare hvordan vi forberedte oss til intervjuene med tanke på spørsmålsutforming, samtykke og tid til gjennomføring av intervju.

3.4 Forberedelse og gjennomføring av dybdeintervjuer

For å forberede oss til dybdeintervju begynte vi å utarbeide en intervju mal med faste spørsmål og oppfølgingsspørsmål. Gjennom spørsmålene våre ønsket vi å avdekke dybdeinformasjon som holdninger, meninger og erfaringer. Et semistrukturert dybdeintervju er en fleksibel form for intervju da det gir oss rom for å stille faste spørsmål og oppfølgingsspørsmål som er tilpasset svaret til intervjuobjektene (Easterby-Smith et al. 2018.184). Da vi ikke er eksperter på teknologi eller programvare, så vi på denne intervjuformen som en fordel. Vi kunne la ekspertene svare på spørsmålene våre, samtidig som vi kunne be den utdype der vi trengte mer informasjon for å forstå helheten. Da vi intervjuet de andre ansatte, gjorde denne metoden at vi lettere kunne sette oss inn i hvert intervjuobjekts personlige opplevelse. Easterby-Smith et al. 2018.185 anbefaler at intervjuguide for semistrukturerte dybdeintervju bør basere seg på overordnede tema,

og istedenfor å stille spesifikke spørsmål bør fokuset være på å få dekket alle temaene. Derfor utformet vi intervjuguiden basert på temaene og underspørsmålene som er presentert tidligere. Alle spørsmålene er teoretisk forankret, men skrevet i dagligtale slik at det skulle være enkelt å forstå uten å ha lest teorien, for å styrke reliabiliteten i intervjuet (Krumsvik 2015.127). Fordi vi har brukt samme tema og underspørsmål gjennom hele oppgaven, har det gjort det lettere for oss å strukturere intervju og analysene. Vi testet ut spørsmålene i forkant av intervjuene for å sjekke om de var forståelige og svarer på de temaene vi ønsker, ved å stille dem til en tidligere medstudent.

Vi utformet intervjuguidene slik at de tre ekspertene svarte på de samme spørsmålene. De tre som jobber innenfor rekruttering, økonomi og salg svarte på samme spørsmål. HR avdelingen fikk noen andre spørsmål med tanke på opplæring. Intervjuguidene ligger som vedlegg nr. 2, 3 og 4. Før intervjuet sendte vi intervjuobjektene intervjuguiden, med informasjon om oss, hva som var formålet med intervjuet og hva det ville bli brukt til. Vi informerte intervjuobjektene om at de kunne være anonyme og hadde mulighet til å ta vekk spørsmål de eventuelt ikke hadde lov å svare på.

Selve intervjutiden ble satt til to klokketimer med ekspertene, og 45 min til 1 time med de ansatte. Vi har hatt totalt 10 timer intervju. Alle intervjuene ble gjennomført over zoom og teams da fysiske intervju ikke lot seg gjennomføre på grunn av restriksjoner knyttet til COVID-19. Vi gjennomførte intervjuene slik at en av oss holdt intervjuet og kunne fokusere på samtalen og stille relevante oppfølgingsspørsmål og den andre kunne ta gode notater til transkriberingen. Vi prøvde også å følge med på kroppsspråk, da det ofte sier mer enn ord. Dette ble noe utfordrende på grunn av intervjuene måtte holdes digitalt. Alle våre intervjuobjekt hadde hjemmekontor, så i alle utenom to intervju ble det forstyrrelser på grunn av andre personer som var hjemme samtidig. Vi antar at det at en annen person har vært til stede under intervjuet kan ha påvirket svar fra informantene i noen grad. Spesielt spørsmål om egen kompetanse, fordi det kan være vanskelig å være ærlig om egne feil foran andre (Krumsvik 2015.131). Alle informantene våre stilte godt forberedt og hadde satt av tid til å snakke med oss. Vi lærte mye av hver enkelt og sa oss dermed fornøyd etter syv intervjuer. Vi hadde planlagt å få snakket med HR i begge organisasjonene, da vi hadde fått muligheten til å se nærmere på opplæringen i begge organisasjonene. Det lot seg ikke gjøre. Videre hadde vi i utgangspunktet bestemt oss for å ha en anonym kvantitativ spørreundersøkelse til de ansatte i begge organisasjonene for å avdekke flere sider ved kompetanse knyttet til

informasjonssikkerhet. Fordi det kan være lettere å svare ærlig når intervjuobjektet har mulighet til å være anonym. På grunn av tidsbegrensning lot ikke det seg gjøre.

For å avdekke hva som er det viktigste i alle intervjuene, samt hva som er likheter og forskjeller mellom intervjuobjektenes utsagn brukte vi transkribering av intervjuene og en innholdsanalyse.

3.5 Innholdsanalyse

Vi transkriberte intervjuene for at vi lettere kunne analysere intervjuene i etterkant. Vi ba om tillatelse, da vi ønsket å være transparente i vår forskningsprosess og intervjuobjektene har rett på å vite hva de bidrar til (Easterby-Smith et al. 2018.157).
Som analysemetode valgte vi innholdsanalyse, fordi det er en analysemetode vi føler oss komfortabel med da vi gjorde det i vår bacheloroppgave. Vi syns også at det gir oss en god oversikt over hva som er likt og ulikt mellom de forskjellige intervjuobjektene og hva som blir sagt flere ganger, og er spesielt viktig.
Innholdsanalyse går ut på at vi i forkant har utarbeidet koder som vi leter etter i de transkriberte intervjuene, for å se hvor ofte kodene kommer igjen; **Trusselbildet, ansvar og opplæring, kompetanse, menneskelige feil, sikkerhet, teknologi, og ledelse** (Easterby-Smith et al. 2018.239). Vi har laget sammendrag for hvert tema/kode som kan leses i kapittel 5.0 Funn og analyse. Vi analyserte ekspertintervjuene sammen, ansatt intervjuene sammen og HR sitt alene. HR sitt intervju satt vi til slutt sammen med både ekspertintervjuene og ansattintervjuene, fordi HR fungerer som bindeleddet mellom ledelsen og de ansatte.
Kodeskjema ligger som vedlegg nr. 6

Prosessen fra å samle inn teori og forskning, lage en intervjuguide, gjennomføre intervjuene og sette dem opp i en analyse er med på å bestemme studiens kvalitet.

3.6 Studiens validitet og reliabilitet

Studiens kvalitet bestemmes av studiens **validitet og reliabilitet.** Validitet handler om gyldigheten til resultatene, og kan deles inn indre og ytre validitet. **Indre validitet** handler om resultatene av studiene er gyldige for det utvalget som er inkludert i studiene. Hvis den indre validiteten er sterk kan den påvise sammenheng mellom variablene, eksempelvis om det er sammenheng mellom brudd på informasjonssikkerheten og menneskelige feil (Johannessen,

Tufte og Christoffersen 2011.365). Er det svak indre validitet så påstås det ikke si at det ene påvirker det andre. **Ytre validitet** handler om i hvilken grad studienes resultater kan overføres til andre populasjoner, eksempelvis PWC (Johannessen, Tufte og Christoffersen 2011.367).

Reliabiliteten sier noe om hvor pålitelig svarene er, altså om studien gjennomføres en gang til og får samme svar er studien reliabel.

For å sikre validitet og reliabilitet i vår oppgave har brukt flere virkemidler. Under intervjuet unngikk vi å bruke **flertydige spørsmål** fordi reliabiliteten i et intervju blir redusert ved bruk av flertydige spørsmål, da intervjuobjektet kan misforstå hva de skal svare på (Krumsvik 2015.127). Vi testet og sikret reliabiliteten ved at vi valgte en del av hvert intervju, der begge transkriberte, så **sammenlignet vi teksten** (Krumsvik 2015.133). God reliabilitet øker validiteten. Det er lett å få sympati med informanten og dermed er det viktig å transkribere ord for ord, slik at det ikke blir empatisk fortolkning. Dette henger også sammen med **intervjuetikk**, der hensikten er at personen må kunne kjenne seg igjen i transkriberingen (Krumsvik 2015.136). Vi utformet vår **egen problemstilling**, med **egenvalgte organisasjoner** og brukt **nyere teori og forskning**, slik at det skulle være relevant og ikke en kopi av andres oppgave. Vi har prøvd å **beskrive** forskningen og prosessen godt både i oppgaven og til intervjuobjekter for at forskningsprosessen skal være **gjennomsiktig og reflekterende** (Easterby-Smith et al. 2018.270).

En del av å sikre studiens kvalitet er å ha fokus på etikk og personvern. Som nevnt tidligere har vi hatt fokus på at informantene skal vite så mye som mulig om vår forskningsprosess. I denne forskningsprosessen har vi også måttet ta hensyn til deres personvern og sørget for at vi har hatt en etisk forskningsprosess.

3.7 Etikk og personvern

I følge Easterby-Smith et al. 2018.156 forventes det at forskere ikke skader noen med forskningen sin. I vårt tilfelle kan skade skje hvis vi lyver om funnene gjort i intervjuene våre slik at det setter Azets og Visma i et dårlig lys. Videre presenterer Easterby-Smith et al. 2018.157 en tabell med ti prinsipper for etisk forskning. Disse prinsippene er utarbeidet av Bell og Bryman i 2007. De første seks prinsippene handler om å beskytte det eller dem som undersøkes, altså Azets, Visma og informantene derfra. De siste fire prinsippene handler om å beskytte integriteten til forskningsprosessen, at det en fri for bias, altså at den ikke er påvirket

av egne personlige meninger. Dette henger sammen med validiteten og reliabiliteten av forskningen. I tillegg har vi som forklart tidligere, vært åpen om hva vi skal intervjue om, hva det skal brukes til og hvordan det vil håndtert. Da vi valgte å bruke intervju som metode, søkte vi om godkjennelse hos Norsk senter for forskningsdata (NSD) via et meldeskjema for personopplysninger. Vedlegg nr. 5

4.0 Funn og analyse

Funn og analyse består av funnene vi har fra intervjuene, knyttet opp mot teorien vi har presentert i 2.0 teori.

Denne delen vil følge de tre spørsmålene;

1. **Hvordan påvirker ny teknologi og digitalisering Azets og Visma?**
2. **Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?**
3. **Hvordan forebygger Azets og Visma de største truslene?**

De ulike intervjuobjektene vil bli referert til i denne delen, etter navnene i tabell *3.2. Fremstilling av intervjuobjekter.*

4.1 Hvordan påvirker ny teknologi og digitalisering Azets og Visma?

I denne delen vil vi knytte funn fra intervjuene opp mot teori *2.1 Teknologi* med undertemaene 2.*1 digitalisering*, 2.2 *informasjonssystem* og *2.3 implementering av teknologi*

Teknologi

Teori viser at vi mennesker tar i bruk teknologi oftere og på nyere måter, her er regnskapsbransjen ikke et unntak. Teknologi har endret måten å jobbe på, fra fysiske papirer til at alt kan gjøres fra egen pc eller mobile enheter. Teknologien har dermed blitt en del av trusselbildet og sikkerhetsløsningene. Teorien viser hvordan arbeidsprosesser går gjennom en digital transformasjon, digitaliseres. Det gir oss informasjonssystemer og standardiseringer som skal gjøre arbeidsdagen lettere. Samtidig fører det med seg nye krav til ansattes teknologiske kompetanse og læring, ledelsens oppfølging og et krav til at IT ikke bare er den klassiske IT-avdelingen lenger, men nå har ansatte som er gode på teknologi, og hvordan teknologien påvirker organisasjonen. Forskning viser til at brukerne som tar i bruk ny teknologi i arbeidslivet er positive til det, men de har ikke nødvendigvis utdanningen eller erfaringen til å gjøre det på en sikker måte. Det faktum at organisasjoner inkluderer Big Data, mobilteknologi og skybaserte løsninger kan gi stordriftsfordeler fordi det frigjør tid for de ansatte. Dersom regnskapsfører ikke er trygg på egen kompetanse når den skal ta i bruk de nye verktøyene, flyttes den frigitte arbeidsmengden over på sikkerhetsavdelingen og IT-

avdelingen. Her er forskningen klar; opplæring via utdanning eller erfaring må være en del av digitaliseringen.

Ekspert 1 sa at phishing angrep er blitt automatiserte, og kriminelle er blitt mer proff. Derfor har de investert i teknologi som skal stå som motpart. Ransomware har vært lenge og de som har drevet med dette aktivt har tjent gode penger på det, de har nå råd til dyrere teknologier for å angripe. *«Det er automatiserte angrep som stoppes av våre automatiserte mekanismer, Etter hvert som AI og maskinlæring blir brukt til angrep, så må man bruke det tilsvarende til forsvaret, så når en kvantedatamaskin klarer å utføre en million avanserte angrep på noen få minutter, så må du ha noen på andre siden som klarer å forstå hva som skjer og tilsvarende stoppe det."*

Ekspert 1 mente at kvantedatamaskiner er noe vi må være oppmerksom på i fremtiden, da denne teknologien har blitt mer tilgjengelig for allmennheten. Et annet alternativ er å ha en tredje backup et sted som er helt utilgjengelig, til og med for administrator. De løser selv det ved å bruke skyplattform som er kvantesikker og har datasenter på hemmelig lokasjon. På arbeidsplassen har de to-faktorautensiering, kryptering av data og pc-er, brannmur, VPN og monitorering. I tillegg har de investert i SPF og DKIM som skal hjelpe mottaker av e-post å være trygg på avsender. **Ekspert 1s** tanker om fremtiden *"Arbeidsmetoden endrer seg nok ikke så mye, det som endrer seg er teknologien. Nå som man begynner å få AI og maskinlæring som begynner å bli bra og fungere. I store grader allerede nå så er det maskiner vs. maskiner»*

Videre kunne **Ekspert 1** fortelle oss at bak hver teknologi er det et menneske, for det er enda ikke noe som tenker selv. AI reagerer slik et menneske har fortalt at det er riktig å reagere. Så hvis teknologien feiler så er det også et eller flere av menneskene bak som har feilet. Det kan være for komplekse systemer, opplæring, feilbruk eller for få ansatte i avdelingen. Hvis en skulle brukt teknologi til å gjøre pc-er helt sikre måtte alle administrative rettigheter fjernes slik at ingen programmer kan snakke med hverandre. Det er mulig, men det gjør det til et veldig lukket system som er vanskelig å jobbe i. Intervjuobjektet anbefaler bruk av dette i en viss grad, men ikke i en helt lukket grad.
Det **Ekspert 1** sier er utfordrende er monitorering. *"Digitaliseringen er på god vei, men det er mange år igjen for å få den på plass"*

Ekspert 2 fortalte at det alltid er hull i teknologien, som det er det ikke er mulig å beskytte seg helt mot. Visma selv bruker filtre og monitorering aktivt, i tillegg til programvare som skal fange opp phishing. For å teste om teknologien de har nå er god nok tar de jevnlige penetrasjonstester der de kvalitetssikrer at en hacker ikke skal klare å komme seg inn i deres systemer. På spørsmål om hvordan intervjuobjektet så for seg fremtiden, svarte intervjuobjektet: *"Vi får håpe at vi ved bruk av riktig teknologi, klarer å holde stand"*

Ekspert 2 var kjent med at *"kvaliteten på skytjenester er avhengig av leverandør og hva slags program man snakker om"*

"Hvis de riktige typene utviklingsrammeverkene er på plass vil jeg påstå at skytjenester er tryggere enn annen type lokalt installert programvare"

For å forklare hvor god teknologien er uttalte **Ekspert 3** *"I mitt hode handler det mye om samhandlingen mellom teknologien du bruker og menneskene"* Videre mente intervjuobjektet at det var viktig å ha gode programmer som kunne ta backup, og varsle om phishing i e-post. Med tanke på fremtiden var synspunktet at *"Organisasjoner med fokus på teknologi er nok godt rustet til fremtiden, mens organisasjoner med lite fokus på teknologi. eks. dagligvare er ikke godt nok rustet for fremtiden"*

1) Hvordan påvirker ny teknologi og digitalisering Azets og Visma?
Angrep er automatiserte.
Kvantedatamaskiner, AI og maskinlæring blir tilgjengelig for allmenheten.
Arbeidsmetoden endrer seg nok ikke så mye i fremtiden, men teknologien endrer seg.
Bak hver teknologi er et menneske
Teknologien er dum, alltid hull i teknologien.
Digitalisering er på god vei, men tar mange år for å få den på plass.
Om fremtiden: vi får håpe at vi ved bruk av riktig teknologi klarer å holde stand.
Fokus på sammenheng mellom mennesker og teknologi.
Organisasjoner med lite fokus på teknologi, er mindre rustet til fremtiden.

Figur 4.1: Oppsummering av funn "Hvordan påvirker ny teknologi og digitalisering Azets og Visma?"

4.2. Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?

I denne delen vil vi knytte funn fra intervjuene opp mot teori 2.2 Trusselbildet med undertemaene *2.2.1 sikkerhet, 2.2.2 informasjonssikkerhet ved bruk av skytjenester* og *2.2.3 trusler og trender*

Trusselbildet

Jones forklarer en organisasjons omgivelser som hvordan en organisasjon drives, og deres tilgang til ressurser. I hvor stor grad en organisasjon påvirkes av omgivelsene rundt seg, avhenger av faktorer som hvor komplekse de er og antall generelle og spesielle omgivelser som påvirker organisasjonen. Endring av organisasjonen handler om at organisasjonen endrer strukturen og kulturen sin, for å nå et framtidig mål. I NorSIS sin rapport fra 2020 var de største truslene løsepengevirus, kontokapring, verdikjedeangrep og svindel. Alle disse fire truslene kan komme av phishing og menneskelig feil i organisasjonene.

På spørsmål om hva som er de største truslene for organisasjonen i dag, svarer alle tre sikkerhets ekspertene at de anser phishing angrep og menneskelige feil som den største trusselen knyttet til informasjonssikkerhet. **Ekspert 1** sier at det er mer komplisert og sammensatt av kun bestående av bare en ren trussel. De ansatte svarte at de trodde hacking og uthenting av informasjon er den største trusselen for informasjonssikkerheten. De tre ekspertene fikk videre spørsmål om de hadde opplevd noen kjente angrep i det siste. **Ekspert 1** svarte at de ikke hadde opplevd noen større angrep i det siste, men at organisasjonen var stadig under angrep. **Ekspert 2** sier også at de opplever ca. 30 000 angrep i løpet av året. **Ekspert 3** er enig med de andre og at årsaken til alle angrepene i løpet av et år, kan spores tilbake til phishing og menneskelige feil.

For å minske trusselbildet til organisasjonen, sier teorien at organisasjoner burde ha en plan for å forebygge og beskytte seg mot disse feilene. En måte å starte forebyggingsarbeidet på er ved å utarbeide en risikoanalyse, som kartlegger hvilke risiko organisasjonen står overfor, og hva konsekvensen av risikoen kan være. Basert på denne analysen, kan organisasjonen utarbeide rammeverk for internkontroll og ulike planer de skal ta i bruk dersom de opplever angrep.

Ekspert 1 sier at de har utarbeidet et rammeverk i en business continuity plan. Målet med planen er at de kan fortsette å levere, på tross av angrepet de har opplevd. Der er det informasjon om hvem som skal gjøre hva ved et eventuelt angrep. **Ekspert 2** sier at de har utarbeidet en beredskapsplan med utgangspunkt i ulike trusler, som igjen er basert på ISO-sertifiseringer. **Ekspert 3** sier at de har selv utarbeidet en beredskapsplan for intern bruk i organisasjonen. De utarbeider også egne rammeverk og beredskapsplaner for de organisasjonene de selger sikkerhetsløsninger til. Intervjuobjektet sier at de fokuserer på opplæring og ledelseskunnskap i de eksterne organisasjonene.

Når det gjelder hvordan informasjonssikkerheten blir påvirket av økt bruk av hjemmekontor, svarer ekspertene ulikt. **Ekspert 2** svarer at de ikke har opplevd noen økt trussel på grunn av hjemmekontor, og at de har hatt tiltak og regelverk knyttet til hjemmekontor. **Ekspert 1** svarer at hjemmekontor har hatt negativ effekt på trusselbildet, men usikker på hvor mye det har påvirket. **Ekspert 3** svarer at mange organisasjoner har utarbeidet gode tekniske løsninger for det, som kanskje gjør at det ikke påvirker trusselbildet så mye.

Sikkerhet

Rolstadås `beskrivelse av sikkerhet er at det et er et fravær av uønskede hendelser. For å kunne jobbe med sikkerhet i organisasjonen, må risikoen vurderes. Risikoen sier noe om hva sannsynligheten er for at noe skjer og konsekvensen av det. Sårbarheten til en organisasjon øker i takt med endring av teknologi, fordi det er mange faktorer som spiller inn når en skal ta i bruk ny teknologi. Sikring av informasjonsverdier innebærer sikkerhet knyttet til; konfidensialitet, integritet og tilgjengelighet. I John Pendleys forskningsartikkel fremkommer det at informasjonssikkerhet bør falle alle organisasjoner naturlig. Pendley sammenligner ubeskyttet data med en ubeskyttet husnøkkel. Han sier at IT-avdelingen i organisasjonen ofte sitter med mye ansvar, og at det ikke kan legges mer ansvar på dem.

Ekspert 1 forklarte at det var tre hovedkategorier de jobbet etter for å beskytte i organisasjonen: *"Det vi forsøker å beskytte er de tre store; CIA. Konfidensialitet, integritet og tilgjengelighet. Det er det tre faktorene innenfor IT-sikkerhet man prøver å beskytte"* Videre sier intervjuobjektet at sikkerhet har blitt en viktigere del av regnskapsbransjen de siste årene, men at regnskapsbransjen ikke er den bransjen som er den som er mest utsatt for trusler. For å være i forkant av ulike hendelser som kan påvirke sikkerheten har de utarbeidet en business continuity plan. Den tar for seg ulike scenarioer som kan skje organisasjonen, og har som mål

å ha en plan for de ulike hendelsene slik at organisasjonen kan opprettholde driften så godt som mulig. Intervjuobjektet legger vekt på at opplæring av ansatte er viktig for informasjonssikkerheten i organisasjonen. **Azets** tar blant annet i bruk et eget sikkerhets opplæringsprogram som gjennomføres minst hvert kvartal. Videre legger intervjuobjektet vekt på at awareness trening er viktig, og at det gir dem en god oversikt over sikkerhetsnivået i organisasjonen. Intervjuobjektet påpeker videre at *«Du kan ha så mye sikkerhet du bare vil, men mottar du en phishing e post som er skrevet godt, den trenger ikke være veldig avansert engang. Er du en god svindler så trenger du ikke så mye ressurser"*

Ekspert 1 forklarer videre hvilke ulike sikkerhetstiltak de har tatt i bruk. Blant annet så kan ingen ansatte installere programmer på sine pc-er. All informasjon blir kryptert og alle pc-er er kryptert. Videre tar de i bruk to-faktor systemer. Når det gjelder bruk av pc på hjemmekontor er det krav til bruk av eget nettverk, passord og oppbevaring av dokumenter.

En svakhet **Ekspert 1** mener organisasjonen har, er fokus på fysisk sikkerhet; *"Fysisk sikkerhet er noe vi er veldig dårlig på. Det er sånne ting man anser som mindre sannsynlig at skal komme denne veien her»*

I intervjuet hadde vi spørsmål knyttet til hvem som burde ha ansvar for informasjonssikkerheten i organisasjonen. Er det kun IT-avdelingen sitt ansvar, eller er det andre som bør ha ansvar? *"Det er legacy tankegang som tilhører fortiden. Før i tiden var det IT-avdelingen som tenkte sikkerhet for da var det nok at IT satt opp en brannmur, men sånn er det ikke lengre. Likevel er det mange som tenker at sikkerhet er IT-problem. Det jobber vi mye med, for å sørge for at alle er klar over at sikkerhet er alle sitt ansvar, uansett."*

Videre stilte vi spørsmål rundt forskjell rundt sikkerheten ved bruk av skybaserte tjenester eller ved bruk av program. **Ekspert 1** nevner ulike fordeler og ulemper med både skybaserte tjenester og program. Dersom du har et eget datasenter har du mye ansvar, med tanke på datasikkerhet og fysisk sikkerhet. Tar organisasjonen i bruk skytjenester derimot, er den sikret ved at leverandøren har datasentre på hemmelige lokasjoner. Intervjuobjektet konkluderer med at hva som er mest sikkert, kommer an på kompetansen en selv sitter på eller selskapet du kjøper det fra har.

Hvordan anser intervjuobjektene sikkerheten nå i forhold til fremtiden?

Her peker **Ekspert 1** på at teknologier som kvantedatamaskiner, AI og maskinlæring kommer til å bli brukt til ulike angrep. Det er derfor viktig at organisasjoner har kunnskap om disse teknologiene, og vet hvordan de skal bruke det for å sikre seg mot angrepene.

«.. . Det er det en del ser, at de må tenke annerledes og tenke sikkerhet på en annen måte. Ha flere lag med sikkerhet og gjemme ting mye bedre."

"At man har god nok innsikt i hva som skjer. Det er det man må bruke, for man kan ikke bare ha masse ting som tar trusselen i det den treffer, eller etter at den har truffet. Vi må ha et eller annet som ser at dette skjer nå, så vi må gjøre tiltak med en eneste gang, være proaktive, sånn at vi ikke finner ut av det i ettertid»

Ansatt 3 svarte at når det gjaldt opplæring innenfor informasjonssikkerhet så hadde de tatt i bruk en egen kursportal som heter Smart Learn. Det hadde i tillegg vært en del Webinar.
I kursportalen får de ansatte oversikt over de ulike kursene de har gjennomført.
Intervjuobjektet føler seg trygg på sine egen kompetanse innenfor informasjonssikkerhet, og føler at dersom intervjuobjektet er usikker, så kan den alltids få hjelp fra IT-avdelingen. På spørsmål om hva som kunne vært bedre med opplæringen innenfor informasjonssikkerhet, svarer intervjuobjektet at det burde vært flere gjennomganger. Spesielt med fokus på hvordan hver enkelt skal sikre seg når det er mye bruk av hjemmekontor.

Intervjuobjektet fra **HR** har gjennomgått forskjellig opplæring i forbindelse med informasjonssikkerhet. Blant annet ulike kurs innenfor informasjonssikkerhet, Code of conduct, compliance og GDPR. Intervjuobjektet legger vekt på viktigheten ved at de ansatte har opplæring og kunnskap innenfor informasjonssikkerhet *"Vi har mye kundedata og hvis vi noen gang ikke skulle oppbevare det på et sikkert sted så er det helt key at vi har kontroll for å håndtere sikkerhet og kundenes data."*

På spørsmål om hvordan bedre ansattes kompetanse innenfor informasjonssikkerhet, sier intervjuobjektet at opplysning er vesentlig. Viktig å bli holdt oppdatert når det skjer endringer i ulike rutiner og prosesser. I tillegg legger intervjuobjektet vekt på at de har kollegaer som jobber innenfor IT-sikkerhet som de kan lene seg på om det trengs.

Ekspert 2 sier at deres sikkerhetsprogram handler om tre kategorier; *"delt inn i forskjellige tekniske kategorier som går på intern IT, hvordan sikrer de ansatte, konfidensialitet og personvern"* intervjuobjektet sier at de jobber med å ivareta kundenes data, som de lagrer i Visma sine løsninger. Det er ulike ansatte som jobber med sikkerhet i Visma, blant annet en såkalt «sikkerhetsingeniør» «*det er den som er ansvarlig på det teamet, for å ivareta alle de prosessene vi har relatert til sikkerhet, i forhold til utvikling, testing og drift av skytjenester"*

Ekspert 2 sine arbeidsoppgaver handler i hovedsak om å svare kunder som ønsker å kjøpe Visma sine produkter. Det er ofte spørsmål knyttet til hvordan sikre sine ansatte, konfidensialitet, og ulike tester de utfører for å unngå sårbarheter.
Intervjuobjektet nevner flere tiltak Visma har tatt i bruk for å bedre informasjonssikkerheten. Blant annet nevner intervjuobjektet at de ikke lenger krever jevnlig endring av passord, men alle må ha et godt passord og i tillegg benytte seg av tofaktorautentisering. Et annet viktig tiltak er opplæring av ansatte. Blant annet månedlige kurs med ulike fokusområde hver måned. Videre har ansatte taushetsplikt og ulike retningslinjer de må følge for bruk av interne systemer.
Visma har i likhet med Azets, fokus på å kunne opprettholde driften uavhengig av trusler og hendelser som skjer. De har utviklet en business continuity plan, og har i tillegg et team som skal respondere dersom de ulike scenarioene oppstår;*"Vi har det som kalles en cyber security incident respons team forkortes til CSIRT. Et team som tester software og står klart til å respondere på forskjellige type trusler»*
Intervjuobjektet sier også; *"security is a shared responsibility»* og at det ikke bare bør være IT-avdelingen sitt ansvar.

Ekspert 1 sier videre at en regnskapsfører har allerede i dag et ansvar for informasjonssikkerheten med tanke på kundenes data. På spørsmål om hva som er minst risiko med av skytjenester og programvare, legger intervjuobjektet vekt på kvalitetssikring. **Ekspert 1** sier at dersom det tas i bruk et program så vil alle kundene håndtere sikkerheten på forskjellige måter. Dersom en organisasjon selger og leverer en skytjeneste er det de som har ansvaret, og det er derfor lettere å kvalitetssikre enn programmene. Dette stemmer overens med teorien i 2.2.2 som sier at risikoen er større dersom ansatte laster ned programvare lokalt, uten tilstrekkelig opplæring. **Ansatt 1** sier at kundene er opptatt av sikkerhet. De har ofte spørsmål knyttet til hvordan dataene lagres, hvordan Visma oppbevarer den og hvordan de jobber mot potensielle brudd.

Innenfor informasjonssikkerhet har intervjuobjektet fått intern opplæring via et system som heter extra mile. Intervjuobjektet sier at for at organisasjonen skal kunne bli bedre rustet innenfor informasjonssikkerhet, bør det være en person som har ekstra eierskap til opplæring innenfor sikkerhet. Det er i tillegg viktig at opplæringen skjer kontinuerlig, og ikke bare en gang. Intervjuobjektet sier videre at Visma er veldig opptatt av å være transparente, og at de derfor dokumenterer alt de gjør av sikkerhetsarbeid, og at dette er tilgjengelig for alle. På spørsmål om hva som er mest sikkert av programvare og skytjeneste, svarer intervjuobjektet at det er skytjeneste som totalt sett er tryggest, men det avhenger av leverandør og program.

Ekspert 3 sier at en stor trussel innenfor informasjonssikkerhet er knyttet til e-post sikkerhet, da mye av fokuset blant organisasjonene har vært knyttet til sikkerhet i andre deler av organisasjonen. For å bedre informasjonssikkerheten sier intervjuobjektet at rutiner som å slette tilganger når ansatte slutter, er viktig. Det er viktig å ha gode e-post filter som gjør at dersom noen trykker på en feil link så sprer den seg minst mulig. *«I mitt hode handler det veldig mye om samhandlingen mellom teknologien du bruker og menneskene"*.
Ekspert 3 sier videre at det er viktig å ha en person i organisasjonen som har ansvar for dataloss prevention og informasjonssikkerhet i organisasjonen.

På spørsmål om hvordan sikkerheten er nå i forhold til i fremtiden, sier **Ekspert 3** at organisasjoner som har hatt lite fokus på sikkerhet fram til nå kan lett bli hengende etter når teknologien utvikler seg så raskt og at disse blir lett mere sårbare. *«De vil ha nytte av å endre strategien sin selv og ha et fokus på det. Selv om det sannsynligvis vil koste de mer penger"*
På spørsmålet om hva som er størst risiko av skytjeneste eller program, svarer intervjuobjektet at de i utgangspunktet har samme risiko. Intervjuobjektet mener forskjellen handler mer om du kjøper eller bygger programvaren selv.

Menneskelige feil

Ut ifra teori og forskning hadde vi inntrykket av at bak hver teknologi er det et menneske som påvirker, og derfor er menneskelige feil en stor del av sikkerhetsbrudd. Tallene fra NorSIS bekreftet dette. Når mennesket møter teknologi kan skyldspørsmålet bli delt, hvem har egentlig skylden hvis noe blir feil i en automatisert prosess? Hvor ligger feilen? Og kan den enkelte ansatte straffes for det? Opplæring og oppfølging er det teorien og forskning sier må til for å minske mengden menneskelige feil. Feilene som menneskene gjør, er også muligens er et resultat av komplekse systemer i organisasjonen.

Vi stilte ekspertene et spørsmål om hva de tenkte om påstanden om at menneskelige ofte er grunnlaget for brudd på sikkerheten. **Ekspert 1** var litt enig i denne påstanden. Intervjuobjektet mente at brudd alltid kan spores tilbake til menneskelige feil. Det er gjerne uflaks som fører til feilen, fordi det er fortsatt en del manuelle prosesser. Er det en automatisert prosess, så er det feil i kjeden. Teknologien får beskjed av mennesker hvordan den skal oppføre seg. **Ekspert 2** var enig i denne påstanden. **Ekspert 3** var enig i påstanden, men ikke i skylddelingen. Ansatte burde i utgangspunktet ikke klare å gjøre feil, og at problemet ligger i at rutinene ikke er gode nok.

Neste spørsmål handlet om hvilke konsekvenser ansatte kunne få dersom en slik feil skjedde. **Ekspert 1** svarte at den ansatte ikke fikk en direkte konsekvens, men kunne få sparken dersom feilen ble gjort med vilje. Videre sier **Ekspert 1** at dersom det er mulig å gjøre feil, så er det feil i organisasjonens rutiner eller systemer. Som et resultat av feilen kan det være at ansatte må få bedre opplæring, eller at organisasjonen må revurdere interne rutiner. **Ekspert 2** sier at en ansatt kan få advarsler, dersom den slurver over tid og feilene gjentar seg. **Ekspert 3** fokuserer mer på hvordan løse problemet det dersom en feil har oppstått. Ekspert 3 nevner også at den ansatte må gi fra seg passord og brukernavn slik at en kan begynne å se hvilke skader feilen har forårsaket. **HR** sier at de bruker kursing for å øke de ansattes kompetanse og dermed unngå menneskelige feil. De tre ansatte har ikke gjort noen tabber som de vet om, men har blitt utsatt for phishing.

Phishing

Forskning viser til at phishing er en av kjernetruslene innenfor kriminalitet, og er en inngangsportal for andre typer av trusler som løsepengesvindel og direktørsvindel. For å beskytte seg mot phishing mener forskningen at organisasjonen må både ha tekniske tiltak gjennom ulike filter, og organisatoriske tiltak gjennom opplæring og kursing av ansatte.

Ekspertene fikk spørsmål om de tenkte at phishing var største trusselen for informasjonssikkerheten. Det var alle ekspertene enige i. **Ekspert 1** sa at det er den vanligste og enkleste måten å angripe på. **Ekspert 2** svarte at det er den enkleste metoden, og at den i dag blir mer og mer overbevisende. De kriminelle tar ofte i bruk kjente fakta, som gjør at det er lett å lure ansatte til å trykke på en feil link. Av tiltak mot phishing angrep hadde organisasjonene flere ulike tiltak. **Ekspert 1** nevnte at de har jevnlig kurs. De tar i bruk to-faktor autentisering. I tillegg har de ulike filter i e-post systemet som skal utelukke phishing.

Ekspert 2 sier at de bruker forskjellige typer programvare fra ulike leverandører, blant annet tar de i bruk Google sin plattform. De har også e-post filter og monitorerer enhetene til de ansatte. Eksperten mente at det viktigste tiltaket var opplæring av de ansatte. De har et kurs hver måned, med ulike tema relatert til sikkerhet. **Ekspert 3** mente at ulike filter i e-post systemene er viktig. Blant annet at e-postene blir vasket, og at de ansatte får beskjed dersom det er mail fra en usikker kilde. I tillegg bør det være en hjelpeknapp, der de ansatte kan melde fra dersom de er usikre. Eksperten legger vekt på at infrastrukturen må være på plass, og at et kurs for de ansatte ikke er nok. Intervjuobjektet mener at organisasjoner har lagt ansvaret over på brukerne.

Vi spurte videre om hvor mange ansatte de tror hadde trykket på en link, dersom den ble sendt ut. Alle ekspertene mente at det alltids var noen som kom til å trykke på linkene, og **Ekspert 1** mente at det kunne være 10-20 prosent av de ansatte som trykket. Vi spurte også de ansatte om phishing. Alle ansatte visste hva phishing var. **Ansatt 2 og 3** nevnte at de hadde blitt utsatt for det, men at de hadde gode rutiner i organisasjonen for å melde fra om det.

2) Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?
Sikkerhet er blitt en viktigere del av regnskapsbransjen
Opplæring av ansatte er viktig for sikkerhet, må være trygg på egen kompetanse.
En svakhet er lite fokus på fysisk sikkerhet.
Skytjenester lagrer informasjonen på hemmelig lokasjon.
Alle har et ansvar for sikkerhet, ikke bare IT-avdelingen.
Tenke sikkerhet på en annen måte, ha flere lag med sikkerhet.
Sikkerhetstiltak; taushetsplikt, retningslinjer og business continuity plan.
Transparente.
Sikkerhet handler om samhandling mellom teknologi og mennesker.
Phishing og menneskelige feil er den største trusselen.
Alle angrep i løpet av et år, kan spores tilbake til menneskelige feil.
Tiltak mot trusler: rammeverk.
Hjemmekontor har ikke stor påvirkning på trusselbildet.
Ved å øke ansattes kompetanse igjennom kursing, kan man unngå menneskelige feil.

Figur 4.2: Oppsummering av funn "Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning?

4.3 Hvordan forebygger Azets og Visma de største truslene?

I denne delen vil vi knytte funn fra intervjuene opp mot teori 2.3 Forebygging og beskyttelse med undertemaene *2.3.1 rammeverk for internkontroll, 2.3.2 ledelse og ansvar* og *2.3.3 opplæring og kompetanse.*

Forebygging og beskyttelse

Arbeidsmiljøloven, personopplysningsloven, arbeidsplassforskriften og internkontrollforskriften **krever risikovurdering**. Denne må gjentas flere ganger og er aldri helt ferdig, fordi omgivelsene stadig endrer seg. Det finnes etablerte rammeverk organisasjoner kan følge for å sørge for at dette gjøres på en god måte.

Gjennom intervjuene ble vi kjent med at våre tre eksperter hadde gode rutiner for risikovurdering, hvor målet er å kartlegge de største truslene og svakhetene for sin organisasjon. Det var også likhet i hvem som var med på dem.
3 av 3 eksperter svarte at det er helst ledelsen som er med å teste og utforme rutinene.
Det var likevel noen forskjeller; **Ekspert 1** sa de hadde rammeverk som var basert på forskjellige typer standarder, han kunne informere om at rammeverkene er ganske like, så det gjelder å finne et som passer organisasjonen og holde seg til det. **Ekspert 2** jobber i en organisasjon som er ISO sertifisert, så de holder seg til disse rammeverkene.
Ekspert 3 er konsulent som hjelper organisasjoner med å bli ISO sertifiserte. Informanten hjelper ledelsen med å etablere gode rammeverk og integrere disse i organisasjonen.

Ledelse og ansvar

Lederne er med å utforme beredskapsplanene til organisasjonen og må dermed også vise de ansatte hvordan aktivt bruke dem i sin arbeidshverdag.
Teori og forskning viste oss at lederne må ta en aktiv del i kunnskapsdeling, tilrettelegge for kunnskapsdeling og støtte de ansatte slik at de tar del av nettverk som kan hjelpe dem i arbeidshverdagen sin.

Ekspert 1 fortalte at lederne er med å teste beredskapsplanene i praksis. Der lederen skal forklare hvordan den hadde reagert i den skapte situasjonen. De får da kunnskap om hvordan

bruke business continuity plan i praksis. Videre forklarte **Ekspert 1** at tankegangen om at det er IT-avdelingen som skal ha ansvar for alt som har med sikkerhet å gjøre, er kun ledelsen som kan hjelpe med å endre. Det at hver enkelt ansatt har sitt eget ansvar for å opprettholde sikkerheten, er det ledelsen som må ta ansvar for å formidle.
Ekspert 2 påpekte at det de ofte ser er at ledere er redde for å fortelle de ansatte at de må bruke de sikkerhetstiltakene som Visma tilrettelegger for dem, som tofaktorautentisering.

På spørsmål om hvem som burde ha ansvar for informasjonssikkerheten i organisasjonen, sier både **Ekspert 1 og Ekspert 2** det samme. Begge sier at informasjonssikkerheten bør være et felles ansvar i organisasjonene.
Ekspert 1 sier at det er alle sitt ansvar, og en er ikke sterkere enn det svakeste leddet. Det at IT-avdelingen skal ha ansvar alene for informasjonssikkerheten, er en tankegang fra fortiden.
Ekspert 3 sier at det bør være en IT-sikkerhetssjef som har ansvaret for informasjonssikkerheten, men ledelsen har et felles ansvar når det kommer til implementering og å sette opp systemene i organisasjonene.
Videre sier både **Ekspert 1 og Ekspert 2** at regnskapsførere i dag har i stor grad ansvar for informasjonssikkerheten. De har ansvar for data de behandler for kundene og kundens systemer de får tilgang til. Av lovverk de må forholde seg til, sier begge at de må forholde seg til Norsk lov, arbeidsmiljøloven og spesielt GDPR og bokførings og regnskapsføringsloven.

Opplæring og kompetanse

I NorSIS sin undersøkelse kom det fram at 88 prosent av respondentene visste hva digital sikkerhet går ut på, men at 70 prosent fortsatt mener at de utgjør en risiko for informasjonssikkerheten.
Her tenker vi at det er dårlig opplæring av ansatte som fører til dette problemet.
Ulik forskning innenfor feltet, har vist at konkret opplæring innenfor ulike risikoer som for eksempel phishing og phishing angrep, gjør at de ansatte er bedre rustet til å stå imot slike angrep.

Ekspert 1 og Ekspert 2 sier at alle i organisasjonen får opplæring innenfor informasjonssikkerhet, men at opplæringen er ulik for ulike roller i organisasjonen.
Ekspert 3 sier at de sørger for å lære opp ledelsen og styremedlemmene i de organisasjonene

de jobber for.
I opplæringen fokuserer organisasjonene på implementering av sikkerhetsverktøy. **Azets** har et eget opplæringsprogram som består av tester og trening. Der har de ulike tester og oppgaver som ansatte må gjennom i løpet av året. **Visma** har eget onboardingsprogram som organisasjoner de kjøper opp, må gjennom.
Videre sier **intervjuobjektet fra HR** a**t** de tar i bruk et eget opplæringssystem som heter My Development. Intervjuobjektet sier at alle ansatte får i utgangspunkt lik opplæring, men med noen tilleggskurs. Det er også obligatorisk Cyber Security month som alle ansatte må være med på.

På spørsmål om hvilken opplæring de ansatte fikk innenfor informasjonssikkerhet, var det litt ulike svar. De **ansatte i Azets** hadde en del opplæring via kursportal og Webinar.
Ansatt 2 svarte at den hadde mye ansvar for egen opplæring, gjennom «Learning by doing».
Ansatt 1 har hatt fått opplæring via et internt system, og i tillegg lært mye om informasjonssikkerhet på egenhånd. **HR** hadde fått opplæring i form av ulike kurs innenfor IT-sikkerhet, Code of conduct, compliance og GDPR.
Alle intervjuobjektene er enig i at opplæringen de har mottatt har vært relevant.
Ansatt 2 svarer at den samtidig har vært kritikkverdig, da det ikke ble fulgt opp i etterkant av opplæringen. Alle intervjuobjektene enige i at organisasjonene har fått frem budskapet, om hvorfor kurs om informasjonssikkerhet er viktig.

Intervjuobjektene ble stilt spørsmålet om hva de tenker om sin egen kompetanse innenfor informasjonssikkerhet. **Ansatt 2 og 3** svarer at de er ganske trygge på egen kompetanse, og **Ansatt 2** påpeker at kompetansen innenfor informasjonssikkerhet er god, da den i tillegg har fått opplæring fra en annen arbeidsgiver.
Ansatt 1 anser sin kompetanse over gjennomsnitt, på bakgrunn av de casene den har jobbet med. Videre ble det stilt spørsmål om hva som skal til for at ansatte i organisasjoner skal være godt rustet innenfor informasjonssikkerhet. Det er gjennomgående svar fra alle intervjuobjektene at jevnlig opplæring og oppdatering er viktig.
Ansatt 1 sier også at organisasjonene burde ha en egen person som har ansvar for opplæringen, og som kan fokusere på kontinuerlig opplæring av ansatte.

HR ansatt fikk spørsmål om HR-avdelingen hadde fått tilbakemelding fra ansatte om deres opplæring. Intervjuobjektet svarte at ansatte hadde gitt uttrykk for at de skjønte viktigheten av opplæring, men at noen syns opplæringen kunne være kjedelig. For at opplæringen skal bli

bedre, mener **HR ansatt** at de bør fokusere på den pedagogiske delen av opplæringen, og hvordan kursene er lagt opp. HR-avdelingen spør ikke i medarbeiderundersøkelsen, om hvordan den enkelte ansattes kompetanse eller trygghet innenfor informasjonssikkerhet. HR sier at så lenge de ansatte svarer at du vil anbefale organisasjonens produkter, så gjenspeiler det at den ansatte føler seg trygg.

3) Hvordan forebygger Azets og Visma de største truslene?
Lederne er med å teste å teste ut beredskapsplaner i praksis.
Ledelsen må hjelpe med å endre tankegangen om at IT alene har sikkerhetsansvar.
Ledere er redde for å mase på sine ansatte.
Informasjonssikkerhet er et felles ansvar i organisasjonen.
Alle ansatte får opplæring, men opplæringen er ulik.
Fokus på opplæring av ledelse og styremedlemmer.
Alle tar i bruk intern kursing.
Organisasjonene har fått fram budskap om hvorfor kurs er viktig.
Alle ansatte er trygg på egen kompetanse.
HR spør ikke om kompetanse innenfor informasjonssikkerhet.

Figur 4.3: Oppsummering av funn "Hvordan forebygger Azets og Visma de største truslene?

5.0 Diskusjon

I denne delen vil vi diskutere funnene som er presentert i 4.0 Funn-og-analysedel, opp mot teori og forskning presentert i *2.0 Teori.*

5.1

Gjennom teorien vår i *delkapittel 2.1 Teknologi* viser Rolstadås til at ny teknologi oppstår når samfunnet har behov for det, og er modent nok til å ta det i bruk. Gjennom informantene våre i Azets og Visma lærte vi at det ikke alltid er tilfellet. Ekspert 1 viste til at de kriminelle har gjennom lang tid tjent penger via phishing, så nå har de råd til å ta skrittet videre. Kvantedatamaskiner og teknologien bak er i ferd med å bli mer tilgjengelig for allmennheten, men kanskje er ikke alle organisasjoner forberedt på det. Videre sier vi i *delkapittel 2.1* at teknologi ikke bare handler bare om oppfinnelser, men også nye måter å ta bruk den teknologien vi har. Eksempel på det er Ekspert1 sin uttalelse om at dagens phishing angrep har blitt mer automatiserte. Derfor må organisasjonene ta i bruk lignende teknologi for å kunne stå imot angrepene. Ekspert1 nevner at kvantedatamaskiner er noe vi bør anse som en trussel i fremtiden, og derfor bør organisasjoner hele tiden jobbe for å sikre seg mot den nyeste teknologien. Det støttes også av forskning jf. *2.1.2 Informasjonssystem.* Azets og Visma løser det på et organisasjonsnivå, ved å bruke skytjenester som har kvantesikre krypteringer og cyberforsikring. Da vi spurte dem om hvordan de trodde fremtiden så ut var det likevel tvil i svarene deres om vi kom til å klare å henge med i teknologiutviklingen.

Tvilen bak svarene deres tenker vi henger sammen med Rolstadås funksjonelle og individuelle nivå. Det forstår vi som hvordan de forskjellige avdelingene bruker teknologien de har tilgang til og kompetansen på gruppe- og individnivå. For det er sammenheng mellom mennesket og teknologi, i den form av at det er ikke enda teknologi som tenker helt selvstendig. Alle ekspertene vi intervjuet var enige om at det er mennesker bak enhver

teknologi og dermed må det sees på som en sammenheng og ikke to separate enheter. Begge påvirker hverandre, er det feil i teknologien, er denne feilen laget av et menneske, og kan igjen få et annet menneske til å feile. Det kan forstås som at det er viktig med fokus på **sammenhengen mellom teknologien i seg selv og menneskene som skal ta i bruk teknologien.**

I *2.1.1 Digitalisering* skriver vi om at det handler om å ta i bruk digitale løsninger for å videreutvikle organisasjonen, som er det Azets og Visma jobber med. De selger løsninger og rådgivningstjenester. Ekspert 2 la vekt på at når de selger sikkerhets software til kundene sine så legger alt til rette for at kunden skal kunne ha en trygg opplevelse, men de opplever at kunden ikke bruker alle integrasjonene. Vi tenker det kan henge sammen med at de ansatte enten ikke kan teknologien godt nok så de er redde for å bruke den, eller informasjonen fra Visma ikke blir videreformidlet til de ansatte. Dette skal vi ta opp igjen i diskusjonen under integrering av teknologi.

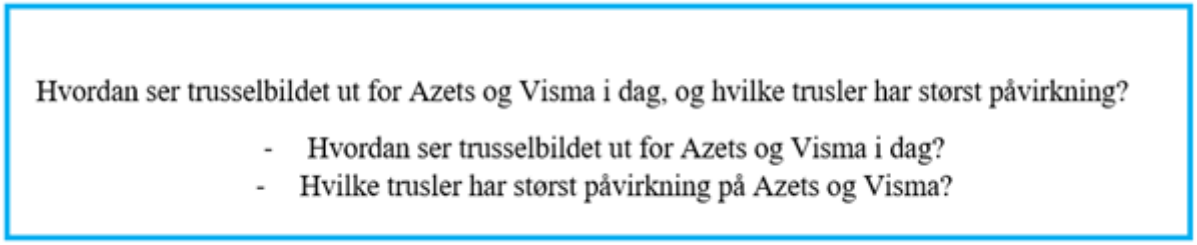
Ekspert 1 sier at arbeidsmetodene ikke vil endre seg så mye i fremtiden, men teknologien vil endres. Intervjuobjektet sier videre at det i stor grad nå blir maskin mot maskin.
Både ekspertene i Azets og Visma sier at de må ta i bruk nyere teknologi for å kunne stå imot angrep. Ekspert 1 fortalte at digitalisering har ført til at phishing angrep er blitt automatiserte og sofistikerte, og dermed må beskyttelsen også være automatisert. Begge organisasjonene har programmer som varsler de ansatte om at e-post kan være phishing. De har tatt i bruk to-faktor, brannmur, kryptering, VPN, SPF og DKIM, men likevel blir de utsatt for phishing daglig. Dette kan støttes av Norsk sikkerhetsmyndighet, jamfør *2.1.2 informasjonssystem*, de mener at økningen og avanseringen av angrepene som skjer mot organisasjoner, setter større krav til informasjonssystemer og menneskene bak dem. Både ekspert 1 og 2, påpeker at monitorering er vanskelig, fordi det krever at den ansatte bruker enheter som er satt opp av organisasjonen, og ikke private enheter. Noe som latt seg regulere av styrende dokumenter, men de kan ikke vite at alle forholder seg til de styrende dokumentene til enhver tid.

Når en skal *integrere teknologi i en arbeidshverdag 2.1.3* så gjør ofte organisasjoner det for å kutte kostnader og effektivisere prosesser. For at det skal være tilfellet må de ansatte kunne bruke teknologien på en god måte. I studien gjort av Rindasu viste det seg at det var mangel på opplæring i teknologi på utdanningsnivå, men det var interesse fra de ansatte for å ta i bruk ny teknologi. Her tenker vi at det er opp til organisasjonen å fylle gapet med kompetansekartlegging, kurs og oppfølging. Fylles ikke gapet så er det rom for å feile, et rom

for brudd for informasjonssikkerheten. Azets og Visma kurser alle sine ansatte i informasjonssikkerhet, og tilpasser kursene etter hvilken stilling de ansatte har.

Gjennom teori og intervju har vi kommet til delkonklusjonen om at ny teknologi og digitalisering påvirker Azets og Visma i form av at de må tenke sikkerhet på en ny måte enn før. Fordi gjennom digitalisering blir teknologien mer tilgjengelig og skadelig, den blir kjappere og det blir vanskeligere å gjennomskue hva som er trusler. Den påvirker de også i form av at integrering av ny teknologi koster penger. De er begge store organisasjoner, der mange ledd skal overtales og mange ledd skal opplæres.

5.2



Vi velger å dele opp hovedspørsmålet i to deler, illustrert i figuren under. Spørsmålet dekker flere viktige tema, som vi anser som relevant for å besvare vår problemstilling. Vi har derfor delt spørsmålet opp for å kunne beskrive temaene godt nok. Del 1 *"hvordan ser trusselbildet ut for Azets og Visma i dag?"* besvares av delkapittel 2.2 - 2.2.2. Del 2 *"Hvilke trusler har størst påvirkning på Azets og Visma?"* besvares av delkapittel 2.2.3.

I delkapittel 2.2 Trusselbildet, har vi beskrevet hvilke krefter og omgivelser som påvirker en organisasjon, og i hvilken grad den blir påvirket. Truslene knyttet til informasjonssikkerhet kan sies å være påvirket av flere ulike krefter. Ekspert1 sier at trusselbildet er mer sammensatt enn kun bestående av en trussel. Videre sier Ekspert1 at sikkerhet har blitt en større del av regnskapsbransjen. Ut av dette kan vi tolke at den økte bruken av teknologien, gjør at regnskapsbransjen må i større grad ta hensyn til informasjonssikkerheten. Noe som viser organisasjonenes trusselbilde godt, er at både Ekspert 1 og Ekspert 2 nevner hyppige angrep i løpet av et år. Ekspert1 sier at organisasjonen er under konstant angrep.

Både Azets og Visma er store, internasjonale organisasjoner bygget som hierarki. De er ressursrike og velkjente, med et godt rykte i samfunnet. Vi mener dermed at de er godt rustet for endringer. En negativ side ved Azets og Vismas størrelse, tenker vi er at det er langt

mellom linjene i organisasjonen. Størrelsen på organisasjonene kan påvirke kommunikasjon og kompetansebygging. Som ekspertene selv påpekte i intervjuene, så kjenner de ikke til hva sine kollegaer arbeider med. Vi antar at dette kan være med å påvirke trusselbildet for Azets og Visma, da det kan gjøre det vanskeligere for dem å gjennomføre en endring. Som vi diskuterte i forrige del, skjer endringene nå hurtigere enn før.

I 2.2.2 Defineres sikkerhet som fravær av uønskede hendelser, det forstår vi som at hvis vi kan utelukke at noe uønsket skjer, er vi sikre. For å være sikre mot brudd på informasjonssikkerheten har Azets og Visma mange tiltak, som vi nevnte i del 1 av diskusjonen. Risiko er sannsynligheten for og konsekvensen av den uønskede hendelsen. Selv om begge organisasjonene har iverksatt teknologiske tiltak for at det ikke skal være brudd på informasjonssikkerheten, så finnes det likevel en risiko for at det skjer. Risiko er forholdet mellom trussel, verdi og sårbarhet. I regnestykket er informasjonssikkerhet verdien, trusselen er kriminelle som vil ha tilgang, og sårbarheten er mennesket. Den kriminelle bruker sårbarheten til å oppnå verdien. Både Rolstadås og Ekspert1 bruker samme ordene for å beskrive hva som er målet med å bruke teknologi for å beskytte verdiene; Konfidensialitet, integritet og tilgjengelighet. Azets og Visma har tilgang til verdier i form av personopplysninger som lønn, helsepapirer og personnummer. Opplysningene kan være interessant for mange kriminelle aktører, og skadelig for privatpersoner om det kommer ut. I intervjuene la begge ekspertene vekt på at det er informasjonen bak tallene de har som er skadelig. En risiko for Azets og Visma er utviklingen av kvantedatamaskiner, AI og maskinlæring. Det er ansatte som lener seg på at IT-avdelingen håndterer sikkerheten og at de kriminelle har blitt vanskeligere å gjennomskue.

Da trusselbildet blir mer og mer sammensatt, tenker vi at organisasjonene også må sørge for at sikkerheten er like kompleks. Det gjelder ikke bare å ha god sikring knyttet til teknologien. Ekspert 1 sier at en svakhet hos dem er fysisk sikring. Her tenker vi at fysisk sikring bør være minst like viktig som sikring av teknologien, for å kunne beskytte informasjonen best mulig. Ekspert 3 sier at e-post sikkerhet ofte blir glemt, da andre deler av organisasjonen har blir fokuser mer på. Dette sier noe om at ikke alle deler av sikkerhetsarbeidet er like godt gjennomført. Organisasjonene burde utarbeide risikoanalyser for alle truslene, for å kunne vite hva som skal til av ressurser for å redusere truslene. Videre er det viktig at sikkerheten blir et fokus for hele organisasjonen. Det underbygger Ekspert 1 ved å si at IT-avdelingen alene har ansvar for alt knyttet til informasjonssikkerhet, er gammeldags tankegang. Det samme sier Ekspert2 som mener at sikkerhet skal være et delt ansvar. Ekspert1 legger vekt på at

opplæring av ansatte er viktig for å ivareta informasjonssikkerheten. Pendley påpeker at det er ikke kun IT-avdelingen som har et ansvar for informasjonssikkerhet. Alle ansatte må ta ansvar for å utgjøre så liten risiko som mulig. Azets og Visma legger opp til at sine ansatte skal utgjøre minst mulig risiko ved at de gir dem kompetanse og verktøy i form av sikrede enheter. Azets og Visma har retningslinjer for bruk av egne enheter, jobb enheter, lagring av filer og nettverk. Det er vanskelig er å følge opp at alle de ansatte følger retningslinjene til enhver tid. Det kan være fristende å bruke egen pc eller mobiltelefon fordi den er mer tilgjengelig i øyeblikket, eller koble seg på nettverket på flyet å sende e-post fordi det sparer tid på reisen. Ut ifra disse funnene virker det som om organisasjonene har et fokus på at alle ansatte er godt nok opplært og at alle har et ansvar for sikkerheten. Et funn som kan tale imot er ansatt 3 som er trygg på egen kompetanse, men samtidig påpeker at de alltids kan få hjelp fra IT-avdelingen. Det kan tolkes som at de ansatte alltid har noen å lene seg på, og kanskje ikke er så opptatt av å være fult opplært innenfor informasjonssikkerhet. Ekspert1 sier at organisasjonene må være proaktive og sørge for å ha flere lag med sikkerhet for å kunne stå imot fremtidige angrep. For at de ansatte skal øke sin kompetanse innenfor informasjonssikkerhet, svarer intervjuobjektet at jevnlig opplæring er viktig. De ansattes behov for jevnlig opplæring, kan være et tegn på at de ansatte får for lite eller for sjelden opplæring.

Gjennom arbeidet med studien har vi lært mye om informasjonssikkerhet, og en av funnene våre som har vært veldig interessant er sikkerhet ved bruk av skytjenester 2.2.1. Da vi startet studien vår hadde vi inntrykket av at det var en vesentlig forskjell i SaaS og PaaS tjenester. Gjennom intervjuer med ekspertene lærte vi at hovedforskjellen på disse to er brukers kompetanse. Har du god kompetanse innenfor informasjonssikkerhet kan du bruke Paas tjenester. Ved bruk av SaaS tjenester får du derimot en annens ekspertise på kjøpet, i tillegg til at lagringsplassen er hemmelig og du er forsikret om noe skulle skje med den informasjonen du har lagret hos leverandøren.

I 2.2.3 Trusler og trender presenteres de fire største digitale truslene. Alle fire har samme inngangsportal: phishing av mennesker. Gjennom intervjuene ble det klart at phishing og menneskelige feil er de største truslene for Azets og Visma, og at disse to har en klar sammenheng med hverandre. Statistikken på hvor mange organisasjoner og privatpersoner som har blitt utsatt for phishing stemmer godt overens med informantenes opplevelser. Ekspert 1 mente at brudd på sikkerheten alltid kan spores tilbake til menneskelige feil.

Teorien sier at målet må være å få stoppet slike angrep slik at den kriminelle ikke kommer inn i organisasjonens systemer.
Både Azets og Visma kunne fortelle at de ikke hadde opplevd at kriminelle hadde kommet seg inn i deres system den siste tiden. Det kan forstås som at begge organisasjonene har gode rutiner på hva som skal gjøres hvis de først utsettes for phishing. Dette skal vi komme tilbake til i neste del. Ekspertene sier at de må være proaktive, lære opp de ansatte og ha flere lag med sikkerhet.
Videre i 2.2.3 viste forskning til at Covid 19 hadde ført til nærmere 9 millioner sikkerhetstrusler. Informantene mente at var den perfekte testen for å se hvor godt forberedt de var på pandemi, organisasjonene var godt forberedt ved at de allerede hadde tiltak som VPN, sikrede enheter til de ansatte og retningslinjer. Da vi snakket med de ansatte fikk vi et annet bilde, der nevnte en av dem at den i forbindelse med hjemmekontor følte at den burde ha fått mer informasjon om hvordan den skulle forholde seg til retningslinjene. Den visste blant annet ikke at organisasjonen hadde VPN den kunne bruke hjemmefra. Dette ser vi kan være i sammenheng med kommunikasjonsflyten i et hierarki. Ekspertene hadde ikke inntrykk av at økt bruk av hjemmekontor økte trusselen. Ekspert 3 mente at mange organisasjoner hadde gode rutiner for hjemmekontor, som gjorde at trusselen ikke var så stor. Ekspert 3 sier at menneskelige feil er årsaken til mange av truslene, men at problemet ligger i at rutinene ikke er gode nok. Er rutinene gode nok, så skal det ikke være mulig for den ansatte å gjøre feil. Det samme sier Ekspert 1, som mener at dersom en ansatt kan gjøre feil så er det også feil i organisasjonens rutiner.
Intervjuobjektet fra HR-avdelingen sier at de fokuserer på opplæring for å redusere menneskelige feil i organisasjonen. Ekspert 2 sier også at utenom opplæring, så må alle ansatte skrive under på taushetsplikt og de har utarbeidet rutiner for bruk av interne systemer. Ut ifra disse utsagnene kan vi tolke det som at organisasjonene har forståelse for at teknologien og menneskene henger sammen, og for å redusere menneskelige feil må fokuset rettes mot rutiner og opplæring. Disse utsagnene kan underbygger teorien om latente feil, som nevnes i 2.2.3.

Latente feil modellen til David Woods forklarer godt hvordan en programfeil kan få et menneske til å feile, og dermed kategoriseres det som en menneskelig feil. Denne sammenhengen har vi blitt veldig synlig i arbeidet med denne studien og i intervjuene vi har hatt. Skillet mellom en teknologisk feil som påvirker mennesket og mennesket som påvirker teknologien til å feile er nesten umulig å finne. Gjennom intervjuene ser vi at det er

mennesker som styrer programmer som oppdager trusler, menneskene reagerer da med å iverksette andre programmer som skal ta redusere eller eliminere trusselen. Hvis en feil skjer her, så tenker vi at det er vanskelig å forklare på en god måte hva eller hvem som var opprinnelsen.

Teknologien som blir integrert i arbeidshverdagen til den ansatte endrer den ansattes hverdag. Som vi ser i teorien, kan dette endre fokusområdet til den ansatte. Da vi intervjuet ansatte om hvordan de oppfattet egen kompetanse, syns alle at de var kompetent nok til å oppdage trusler, og de hadde fått opplæring i hvordan de skal håndtere og rapportere trusselen. Men flere av dem hadde glemt mye av innholdet på kurset og kunne ønske det ble repetert oftere. I tillegg kunne et par av dem fortelle at de hadde lært seg det meste om informasjonssikkerhet og riktig oppførsel i sammenheng med dette selv. Da vi spurte ekspertene om de trodde mange av de ansatte hadde gått på en phishing scam så svarte de at de trodde mange hadde nok gjort det, og at det holder med at kun en prosent gir fra seg informasjon, så kan det gjøre mye skade.

Som en delkonklusjon kan vi si at Azets og Visma står ganske stødig i endrede omgivelser og trusler fordi de er store organisasjoner med høy ekspertise på hva som skjer i omgivelsene. De har likevel sårbarheter knyttet til de største truslene, phishing og menneskelige feil. Det som er interessant er at de på høyere nivå virker å ha god oversikt over hva som må gjøres for å unngå truslene, men at det ikke blir kommunisert godt nok til lavere nivå i organisasjonen. I neste drøftingsdel skal vi se nærmere på hvilke tiltak Azets og Visma bruker for å forebygge og redusere de største truslene.

5.3

Hvordan forebygger Azets og Visma de største truslene?

I delkapittel *2.4 forebygging og beskyttelse* fremheves det at organisasjoner må ha en plan for å forebygge og beskytte seg selv for trusler. Som skrevet i forrige del har vi identifisert de største truslene til å være, phishing og menneskelige feil.

Azets og Visma har begge beredskapsplaner for hva som skal gjøres hvis feil først skjer. De gjennomfører jevnlige øvelser med lederne. De har da hatt en risikovurdering basert på en helhetsvurdering, som konkluderer med hvor farlig de uønskede hendelsene er når sikkerhetstiltakene er trukket fra. For å se hvor godt organisasjonens verdier er beskyttet. De lager et falskt scenario om at en uønsket hendelse likevel kommer gjennom, så skal ledergruppen løse denne. Det er da opp til ledelsen å videre implementere disse beredskapsplanene nedover i organisasjonen.

Verktøyet ledergruppen får til å løse scenarioet er en business continuity plan. Det passer perfekt overens med modellen til digitaliseringsdirektoratet, presentert i *2.4.2 rammeverk for internkontroll.* Visma har i tillegg ulike ISO-sertifiseringer som gjør at det stilles krav til implementering, vedlikehold og forbedring av internkontroll. Ut ifra dette virker det som om begge organisasjonene har et godt grunnlag for arbeidet med informasjonssikkerheten, og har lagt gode planer for hva de skal gjøre dersom de blir rammet. Rammeverket beskriver videre at lederne bør være inkludert i arbeidet med forebygging og beskyttelse, for så å etablere rutiner og opplæring som skal tas med inn i organisasjonen. Det må være fokus på kompetanse og kulturutvikling, og god kommunikasjon. Ledelsen skal stå for styring og oppfølging. Hvordan lederne kan legge opp til kompetanse og kulturutvikling, og god kommunikasjon skal vi diskutere i neste avsnitt.

I delkapittelet 2.4.2 Ledelse og ansvar presenterer vi at ledere må legge opp til og ta en aktiv rolle i kunnskapsdeling, spesielt i komplekse organisasjoner. IT-avdelingen er avhengig av lederne i andre avdelinger for å bli kvitt tankegangen om at det er kun IT som skal ha ansvar for informasjonssikkerheten. Informasjonssikkerheten er et felles ansvar, ekspertene sier videre at det er ledelsens ansvar å sørge for at tankegangen rundt dette endres i organisasjonen.

Gjennom intervju fikk vi vite at det er HR-avdelingen som normalt planlegger og sender ut kurs. Da vi kun fikk intervju med én person som jobber i HR så har vi ikke et godt totalbilde, men et interessant funn var at den HR-avdelingen har aldri spurt sine ansatte om egen kompetanse rundt informasjonssikkerhet. Dette syns vi var interessant fordi organisasjonen bruker mye ressurser på sikkerhet og har et stort fokus på teknologi og sikkerhet. I tillegg til funnene fra de ansatte som sier at de har hatt mye egenlæring og kunne ønske seg oftere repetisjon av kurs som går på informasjonssikkerhet.

I delkapittelet *2.4.3 Opplæring og kompetanse* beskrives at økt mestringsforventning vil motivere de ansatte til å ta sikkerhetsopplæring. NorSIS legger vekt på at opplæringen bør handle om atferdsendring blant de ansatte, og ikke nødvendig kunnskap. Videre bør opplæringens bygge på hva du har lært tidligere, og ha en økende vanskelighetsgrad ut fra eget nivå**. Dersom den ansatte ikke får grundig nok opplæring tilpasset sitt eget nivå, kan det være vanskelig å oppnå denne atferdsendringen.** Dette tenker vi at kan løses av SAWIT verktøyet, da det måler hva de ansatte allerede kan og hva de trenger mer opplæring i. I tillegg til at verktøyet måler om atferden etter kurset har endret seg.

Gjennom intervjuene med de ansatte var tilbakemeldingen at Azets og Visma hadde klart å få frem budskapet om hvorfor kurs på informasjonssikkerhet var viktig, og at de hadde innslag av forskjellige læringsteknikker i kursene, som de ansatte satt pris på. I Azets har det blant annet eget opplæringsprogram med tester og trening, som de må igjennom i løpet av et år. **Ut ifra disse funnene virker det som om alle ansatte får god opplæring.** Det som kan tale imot at alle har fått god opplæring, er at to ansatte sier at hovedvekten av sin kompetanse har de fått gjennom egen opplæring.

Vi mener at en god måte for lederne i Azets og Visma å jobbe på hadde vært å utnytte seg av kunnskapsnettverk beskrevet av Nesheim og Olsen. På grunn av organisasjonsstrukturen deres. Med kunnskapsnettverk fysisk og digitalt er det lettere å dele kunnskap og erfaringer mellom linjene. Det hadde også tatt presset av lederne, som det nå virker som ikke klarer å gi informasjon ut i hele linjen. I det ene intervjuet med en ansatt ble det foreslått noe lignende. Den ansatte savnet en person som var kun dedikert til rollen som oppfølging av kurs og kompetanse. En slik person hadde kunnet ha ansvar for kunnskapsnettverk.

Som en delkonklusjon kan vi si at Azets og Visma har gode beredskapsplaner for phishing og menneskelige feil, men, at de mangler en skikkelig plan er i hvordan de skal få denne informasjonen ut til de ansatte på en god måte. Kommunikasjonen fra lederne og nedover i hierarkiet er ikke god nok. Opplæring og kompetanse er noe de begge tar på alvor i organisasjonen, men igjen er det bunnlinjen som ikke får nok oppmerksomhet. Vi antar at kunnskapsnettverk med dedikert leder for nettverket hadde vært perfekt i et tungt hierarki.

6.0 Konklusjon

I denne studien har vi undersøkt hvordan informasjonssikkerheten i Azets og Visma påvirkes av teknologiutvikling. For å besvare problemstillingen har vi i denne delen konkludert ut fra underspørsmålene *1) Hvordan påvirker digitalisering i informasjonssikkerheten i Azets og Visma? 2) Hvordan ser trusselbildet ut for Azets og Visma i dag, og hvilke trusler har størst påvirkning? 3)Hvordan forebygger Azets og Visma de største truslene?*
Våre hovedfunn, implikasjoner og videre forskning er samlet i tabell 6.0 på siste siden.

Hvordan påvirker ny teknologi og digitalisering Azets og Visma i dag?

Azets og Visma blir påvirket av ny teknologi og digitalisering ved at ny teknologi stadig blir raskere, og angrep blir vanskeligere å gjennomskue. Det fører til at organisasjonene må tenke sikkerhet på en annen måte enn tidligere.
For å beskytte informasjonssikkerheten innfører Azets og Visma økt bruk av teknologiske løsninger, der målet er at alle ansatte skal være med å forebygge brudd på informasjonssikkerheten. De benytter teknologiske løsninger som monitorering av ansattes enheter, e-post filter og skylagring med cyberforsikring.
Ny teknologi og digitalisering påvirker også samspillet mellom teknologien og menneskene i Azets og Visma. De ansatte får kurs i informasjonssikkerhet og hva som påvirker den. Organisasjonen har implementert løsninger i deres programvare der ansatte kan melde om trusler. På den måten kan ansatte bidra til å redusere antall angrep som kan true informasjonssikkerheten.

Hvordan ser trusselbildet ut for Azets og Visma i dag?

Organisasjonene har et høyt og komplekst trusselbilde, ved at de anser seg som stadig under angrep fra ulike trusler. Angrepene er hyppige, men blir fanget opp av systemene de bruker for å beskytte seg selv. Per i dag håndterer Azets og Visma trusselbildet. Endringene i omgivelsene gjør at trusselbildet i fremtiden er usikkert. Azets og Visma innehar høy ekspertise innenfor informasjonssikkerhet. Dette gjør at de er godt forberedt på endringer i omgivelsene. Bakdelen er at det er kostbart for organisasjonene å være proaktive i form av investering i de nyeste sikkerhetsløsningene. Det kan være fordi de er store og komplekse organisasjoner med mange ledd, der viktigheten av sikkerhetsløsningene må kommuniseres før investering. Det at ikke alle beslutningstakerne har forståelse for hvordan teknologi kan

påvirke informasjonssikkerheten, i tillegg til kostnaden for opplæring av ansatte i nye programmer, kan gjøre det vanskelig å overtale dem.

Hvilke trusler har størst påvirkning?

I intervjuene med Azets og Visma kom det frem at det er phishing og menneskelige feil de anser som sine største trusler. Det begrunnes i at alle feil som skjer, kan spores tilbake til et menneske, enten ved at det er en feil i et system, eller en ansatt gjør en teknisk feil.
Disse truslene er de vanligste og enkleste truslene som kan føre til lekkasje av informasjon. Phishing en stor trussel da angrepene blir stadig vanskeligere å gjennomskue.
Både phishing og menneskelig feil anser vi som et resultat av manglende opplæring innen informasjonssikkerhet, eller lite fokus på kompetanse og kunnskapsdeling blant lederne.

Hvordan forebygger Azets og Visma de største truslene?

Azets og Visma har i tillegg til nevnte teknologiske løsninger, utarbeidet gode rutiner og beredskapsplaner for hvordan de skal beskytte seg mot de største truslene.
Begge organisasjonene fokuserer på opplæring av ansatte innenfor informasjonssikkerhet. Det virker for oss som at lederne i organisasjonene ikke har et høyt fokus på ansattes kompetansenivå. De ulike rammeverkene og beredskapsplanene som sikkerhetsavdelingen har tilrettelagt, blir testet ut på ledergruppen. I begge organisasjonene fikk vi inntrykk av at denne kunnskapen stopper hos ledelsen, og ikke blir kommunisert godt nok nedover i organisasjonen til de ansatte. Dette inntrykket fikk vi fordi de linjeansatte forklarte at de gjennomførte pålagte kurs, men fikk ingen oppfølging som forsikret at de har lært innholdet i kurset. Dette kan underbygges av at flere av de linjeansatte hadde glemt hva de lærte på kursene. Rammeverket for internkontroll viser at ledelsen skal implementere det de lærer på gjennomføringene nedover i organisasjonen. Det virker for oss som at dette ikke blir etterfulgt.

Vi kan ut ifra dette konkludere med at informasjonssikkerheten til Azets og Visma blir påvirket av teknologiutvikling ved at det stadig kommer nye kombinasjoner av teknologi som kvantedatamaskiner. Ny kombinasjon av teknologi fungerer både som en trussel og som et mulig forsvar. Denne teknologiutviklingen resulterer i et økt trusselbilde, fordi det gir de kriminelle flere inngangsportaler til verdiene i Azets og Visma via phishing eller adgangskort. I tillegg er manglende kompetanse og oppfølging blant de ansatte i linjene en stor trussel, da de mangler teknisk kompetanse til å bruke hjelpemidlene som finnes i organisasjonen.

Endelig konklusjon på hvordan informasjonssikkerheten i Azets og Visma blir påvirket av teknologiutvikling er sammensatt. **Nye kombinasjoner av teknologi** fører til at organisasjonene kan **angripes** på nye måter, samtidig som det gir dem mulighet for nye måter å **beskytte** seg mot truslene på. Videre er det fremtidige fokuset på **kompetansen blant ansatte** viktig, for å redusere den **menneskelige faktoren**. Da er ikke bare opplæring av ansatte viktig, men **ledelsen** bør også fokusere på **oppfølging av ansatte**, for å avdekke de ansattes manglende kunnskap og egen oppfattelse av kompetanse innenfor **informasjonssikkerhet**. Basert på dette vil vi si at det er en samvariasjon mellom variablene; teknologi, trusselbildet, forebygging og beskyttelse, opplæring og kompetanse.

6.1 Metodiske begrensninger

Vår studie ble utført i en begrenset tidsperiode på fem måneder. Videre er studien begrenset til å omfatte to organisasjoner, og ikke regnskapsbransjen som helhet. Vi valgte å utføre studien ved bruk av kvalitativ metode, gjennom dybdeintervjuer. Det kan tenkes at vi hadde funnet andre resultater dersom vi hadde inkludert flere organisasjoner, og organisasjoner av ulik størrelse i vår studie. Videre kunne bruk av metodetriangulering, ved for eksempel å ta i bruk spørreundersøkelser, kunne gitt oss flere svar fra hvordan ansatte i organisasjoner opplever informasjonssikkerheten.

Vi kan vi konkludere med at reliabiliteten i studien er tilfredsstillende, dersom noen andre utførte lik studie med samme forutsetninger ville fått samme resultat. Samtidig er vår studie basert på syv informanter[32] og deres personlige erfaringer til temaene. Informasjonen vi har innhentet stemmer for vårt utvalg, da populasjonen er mye større er ikke utvalgets meninger representativt for hele populasjonen. Vi mener at vi har indre validitet da vi har vist gjennom analyse og diskusjon at det er samvariasjon mellom variablene teknologi, trusselbildet, forebygging og beskyttelse, ledelse og ansvar, opplæring og kompetanse. Vi mener også at studiene kan overføres til andre organisasjon, da den ikke hensyntar spesifikke programmer eller tjenester brukt av Azets og Visma. Studien kan derfor overføres til alle organisasjoner som benytter teknologiske løsninger, og dermed kan rammes av phishing og menneskelige feil.

[32] *Av 19.000 ansatte*

6.2 Implikasjoner

Som nevnt vil teknologiutviklingen føre til nye kombinasjoner av teknologi. Azets og Visma har i dag ansatte som jobber med informasjonssikkerhet i organisasjonene. For å holde tritt med utviklingen anser vi det som viktig å fokusere på økt kunnskap om teknologiutvikling, For å stå imot det stadig endrede trusselbildet, er både Azets og Visma proaktive for å kunne forutse hvilke trusler som kan komme. Ut ifra intervjuene kan det oppleves som at de ansatte er lite selvstendig, og lener seg for mye på IT-avdelingen. Dette kan løses ved økt fokus på kompetanse. I tillegg er det viktig at alle ansatte forstår hvordan de kan påvirke informasjonssikkerheten i organisasjonen. For at ansatte skal forstå sin rolle, er det viktig med jevnlig fokus på opplæring av ansatte, og ikke minst oppfølging i etterkant. Til slutt er det viktig at ledelsen kommuniserer godt med de ansatte, for å sørge for at informasjonssikkerheten blir et delt ansvar.

6.3 Videre forskning

I figuren under har vi kommer med forslag til hva som kan være relevant for videre forskning. Vi tenker at forslagene vi har presentert kan bidra til en bedre forståelse av hva informasjonssikkerhet innebærer, og hvordan organisasjoner kan jobbe for å sørge for god informasjonssikkerhet.

Figur 6.0: Presentasjon av hovedfunn, implikasjoner og videre forskning.

Spørsmål	Hovedfunn	Implikasjon	Videre forskning
Spørsmål 1: Hvordan påvirker ny teknologi og digitalisering Azets og Visma?	• Ny kombinasjoner av teknologier: Kvantedatamaskiner, AI – maskinlæring. • Digitalisering påvirker/endrer gammel teknologi. • Arbeidsmetoder og kompetansekrav endres. • Samspillet mellom teknologi og mennesket påvirker risiko.	• Kombinasjon av ny teknologi – som trussel og forsvar. • Kunnskap om teknologi/teknologiutvikling må økes i takt med teknologien. • Fokus på teknologiutvikling for å ivareta informasjonssikkerheten.	• Hvordan skal organisasjoner jobbe målrettet med å øke kunnskap og fokus på ny teknologi i fremtiden? Kompetansebygging Kunnskapsnettverk SAWIT Kommunikasjon
Spørsmål 2.1: Trusselbildet og sikkerhet	• Konstante angrep av sammensatte trusler. • Oppdatert kunnskap om trusselbildet – hva er de største truslene. • Trusselbildet er kompleks gjør at man må ha flere lag med sikkerhet.	• Alle må være ansvarlig for informasjonssikkerheten. • Rammeverk for beredskap og risiko gjør organisasjonen mindre sårbar. • Proaktiv holdning til sikkerhet.	• Hvordan sørge for at alle ansatte har eierskap til informasjonssikkerheten i organisasjonen? • Hvordan implementere rutinene i hele organisasjonen?
Spørsmål 2.2: Trusler og trender	• Phishing og menneskelige feil er største trussel. • Ansattes manglende kompetanse knyttet til informasjonssikkerhet.	• Opplæring og oppfølging av ansatte.	• Hvordan sette fokus på oppfølging for å redusere den menneskelige feilen?
Spørsmål 3: Hvordan forebygger Azets og Visma de største truslene?	• Fokus på opplæring • Sikkerhetsavdeling med fokus på informasjonssikkerhet. • Rammeverk for risiko og beredskap. • Fokus på ledergruppen.	• Ledelsens kommunikasjon med ansatte.	• Hva er årsaken til at ledergruppen ikke alltid fører videre viktigheten rundt informasjonssikkerhet?

7.0 Litteraturliste

Azets hjemmeside. *"Om oss".* Hentet fra: https://www.azets.no/om-oss/ lesedato 22.04.21

Azets hjemmeside. *"EDI".* hentet fra: https://www.azets.no/teknologi/edi/ Publisert: 2021. Lesedato 08.05.2021.

Berriman, John. PwC. «cyber security challenge» ACCA think ahead – artikkel. Hentet fra: https://www.accaglobal.com/vn/en/student/sa/features/cyber.html?fbclid=IwAR3qXl5hm1BBkM4fAX12Y9wCQNP0a3laS524XQKOjML-wtaBVfuqx3Z2Src Uten dato. Lesedato 23.11.20

Bora Kim, Do-Yeon Lee & Beomsoo Kim. «Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks.» *Behaviour & Information Technology*, 19 august 2019: 1157-1175.

Buypass. *Rapport: tre av fem nordmenn utsatt for phishing* NTB Kommunikasjon. Hentet fra: https://kommunikasjon.ntb.no/pressemelding/rapport-tre-av-fem-nordmenn-utsatt-for-phishing?publisherId=14703121&releaseId=17896076 Publisert 23.11.2020. Lesedato 01.02.21

Datatilsynet. *Databehandleravtale.* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/ Publisert: 06.06.18. Lesedato 16.04.21

Datatilsynet *"Ha behandlingsgrunnlag"* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/ Publisert. 28.05.18 Endret. 20.06.18 Lesedato 15.04.21

Datatilsynet. «Datatilsynet.» "*Kryptering"* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/ Publisert 07.03.17. Lesedato: 09.05.21.

Datatilsynet *Når må man inngå en databehandleravtale?* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/databehandleravtale/naar-maa-man-inngaa-databehandleravtale/ Publisert: 20.12.2019. Lesedato 16.04.21

Datatilsynet. "*Virksomhetens plikter"* uten dato. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/ Lesedato 28.11.20

Datatilsynet. "*Personvern på ulike områder"* Hentet fra: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/ Publisert: 23 08 2019. Lesedato 15.02.21.

Datatilsynet. "*Phishing - hvordan beskytte virksomheten"*. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten/ sist endret 17.07.20 Lesedato 15.02.21.

Datatilsynet. "*Risikovurdering".* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/risikovurdering/ uten dato. Lesedato 02.12.20

Datatilsynet. "*Vurdering av personvernkonsekvenser".* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/ Uten dato. Lesedato 02.12.20.

«Difi.no.» 03 mai 2019. *"Digital transformasjon" Hentet* fra: https://www.digdir.no/digitalisering-og-samordning/digital-transformasjon/1589 Uten dato. Lesedato 30.11.2020.

Digitaliseringsdirektoratet. *"Begrepsliste". https://internkontroll-infosikkerhet.difi.no/begrepsliste#Informasjonssystem* Uten dato. Lesedato 08.05.21

Digitaliseringsdirektoratet. "*Internkontroll- etableringsaktiviteter."* (Digdir 1) Hentet fra: https://internkontroll-infosikkerhet.difi.no/etableringsaktiviteter. Uten dato. Lesedato 02.12.20

Digitaliseringsdirektoratet. *Interkontroll/styringssystemer.* Hentet fra: https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet Uten dato. Lesedato 23.04.21

Digitaliseringsdirektoratet. "*Internkontroll"*. Hentet fra: https://internkontroll-infosikkerhet.difi.no/. Uten dato. Lesedato 02.12.20

Digitaliseringsdirektoratet. "*internkontroll/styringssystem (versjon 1.5)"* (Digdir2) Hentet fra: https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter Uten dato. Lesedato 02.12.20

Digitaliseringsdirektoratet. "*ISO/IEC 27002".* Hentet fra: https://www.digdir.no/digitale-felleslosninger/isoiec-27002/1696 uten dato. Lesedato 16.April 2021.

Digitaliseringsdirektoratet. "*Ledelsens styring og oppfølging".* Hentet fra: https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging. Uten dato. Lesedato 08.05.21

Gjensidige. "*Cyberforsikring".* Hentet fra: https://www.gjensidige.no/naringsliv/forsikring/datakriminalitet. Uten dato. Lesedato 09.05.21.

Google. *"Ensure mail delivery & prevent spoofing (SPF)"* Hentet fra: https://support.google.com/a/answer/33786?hl=en Uten dato 2021. Lesedato 14. April 2021.

Grini, Mari. *Computerworld.*. Hentet fra: https://www.cw.no/artikkel/debatt/de-tre-storste-truslene-skyen. Publisert 15.06.2020. Lesedato 15.02.21

Gripsrud, Geir, Ulf Henning Olsson og Silkoset. *Metode og Dataanalyse.* Oslo: Cappelen Damm, 2016.

Grimstad, Grunde. *"Kvantedatamaskinene kommer"* Finansavisen. Hentet fra: https://finansavisen.no/nyheter/teknologi/2020/05/17/7528452/vil-kvantedatamaskiner-bli-en-velsignelse-eller-forbannelse lesedato 15.04.21. Publisert 17.05.20.

Grønmo, Sigmund. *"algoritme"*. Hentet fra: https://snl.no/algoritme. Publisert 02.11.20. Lesedato 09.05.21

Haraldseth, Bjørn. *«Visolit.»* Hentet fra: https://www.visolit.no/artikler/hva-er-egentlig-digitalisering. Uten dato. Lesedato 30.11.20

IBM Services. *«Adapt and respond to risks with a business continuity plan (BCP).* Hentet fra https://www.ibm.com/services/business-continuity/plan Publisert 25.11.20. Lesedato 16.04.21.

«IKT Norge.» *Industri 4.0 – digitalisering av tradisjonell industri.* Hentet fra: https://www.ikt-norge.no/tema/industri-4-0-digitalisering-av-tradisjonell-industri/. Uten dato. Lesedato 23.1120.

Jensen, Peter Skovbjerg. *Hva er en IP-adresse?* Hentet fra: https://komputer.no/internett/nettverk/hva-er-en-ip-adresse. Publisert 13.04.18. Lesedato 09.05.21

Johannessen, Asbjørn, Per Arne Tufte og Line Christoffersen. 2011. *Introduksjon til samfunnsvitenskapelig metode.* Oslo: abstrakt forlag.

John A *«Pendley Finance and Accounting professionals and cybersecurity awareness».* ER the journal of corporate accounting & finance. Editoral review. 2018. Wiley periodical, Inc. Published online in wiley online libery

Jones, Gareth. *Organizational Theory, Design, and Change.* 7.utgave. Pearson Education Limited, 2013.

Knapskog, Svein Johan. "*Det mørke nettet".* Store norske leksikon. Hentet fra: https://snl.no/Det_m%C3%B8rke_nettet Oppdatert 13.03.18. Lesedato 09.05.18

Knudsen, Egil *Ny rapport om IT angrep: Norge er et av de mest utsatte målene i verden.* 2019. digi.no. Hentet fra: https://www.digi.no/artikler/ny-rapport-om-it-angrep-norge-er-et-av-de-mest-utsatte-landene-i-hele-verden/459390 Publisert 02.03.19 Lesedato 11.02.21

Kovacevic, Ana, og Sonja D. Radenkovi´c «SAWIT—Security Awareness Improvement Tool in the Workplace.» *Applied Sciences*, 28 april 2020: 1-13.

Krumsvik, Rune Johan, *forskningsdesign og kvalitativ metode – ei innføring.* 2015 Fagbokforlaget Vigmostad & Bjørke AS. 2. opplag

Leveraas, Paal. *«Dataforeningen.»* Hentet fra: https://www.dataforeningen.no/fra-digitisering-til-digitalisering/. Uten dato. Lesedato 02.03.21.

Linder, Jacob, Johannes Skaar, Jan-Petter Hansen. *"Kvantemaskiner".* Store norske leksikon. Hentet fra: https://snl.no/kvantedatamaskin Oppdatert 11.12.19. Lesedato 09.05.21

Lønneid, Marie Rykkje. *«Regnskapsbransjen er i et paradigmeskifte.» Visma.no*, 9 juni 2020.

Løvhøiden, Anders. *"Telefonen - svindlerens favoritt".* Hentet fra: https://www.azets.no/blogg/telefonsvindel/ Publisert 19.06.20. Lesedato 08.05.21.

Meland, Per Håkon, og Guttorm Sindre. «Cyber Attacks for Sale.» *IEEE Xplore*, 20 april 2020: 1-6.

Myhrvold, Bjørn. *"Automatiserte, men ikke borte".* Regnskap Norge. Hentet fra: https://www.regnskapnorge.no/faget/artikler/teknologi2/automatisert-men-ikke-borte/. Uten dato. Lesedato 29.11.20

Nesheim, Torstein, Karen M. Olsen *"Kunnskapsdeling i en kompleks organisasjon"* Magma.no. Hentet fra: https://www.magma.no/kunnskapsdeling-i-en-kompleks-organisasjon Publisert 03.2011. Lesedato 30.04.2021

Netsecurity. «Netsecurity.» *Hva er egentlig malware?* Hentet fra: https://www.netsecurity.no/fagblogg/hva-er-egentlig-malware. Publisert: 05.05 2021. Lesedato 09.05.21

Netsecurity. "*Disse dataangrepene bør du kjenne til i 2021*" Hentet fra: https://www.netsecurity.no/fagblogg/disse-dataangrepene-b%C3%B8r-du-kjenne-til-i-2021. Publisert 26.04.21. Lesedato 09.05.21.

Nettvett.no. *Aktiver totrinnsbekreftelse!* Hentet fra: https://nettvett.no/2-trinns-bekreftelse/. Publisert 14.10.19 Lesedato 09.05.21

Nettvett.no. *"Direktørsvindel (CEO-fraud)".* Hentet fra: https://nettvett.no/direktor-svindel/ Oppdatert 16.10.19. Lesedato 08.05.21

Nettvett.no. *"DMARC"*. Hentet fra: https://nettvett.no/dmarc/ Oppdatert 04.02.21. Lesedato 08.05.21.

Nettvett.no *"VPN: Virtuelt privat nettverk"* Hentet fra: https://nettvett.no/vpn-virtuelt-privat-nettverk/ Oppdatert 26.02.20. Lesedato 09.05.21.

NHO.no. *Hva er et cyberangrep?* https://arbinn.nho.no/Medlemsfordeler/medlemsfordeler-nho/nho-forsikring/sporsmal-og-svar/hva-er-et-cyberangrep/. Publisert 30.04.18. Lesedato 09.05.21.

NHO Service og handel og Norsk arbeidsmandforbund. *"vekterfaget, lovpålagt nasjonal vekteropplæring"* 2017. Fagbokforlaget. Vigmostad & Bjørke AS. 2.utgave. 2. opplag 2019

Nilstun, Carina. *Implementere.* Hentet fra: https://snl.no/implementere. Publisert 18.07.20. Lesedato 08.05.21

Nordlie, Erik Amit. *"Hva er egentlig Big Data?"* Visma blogg. https://www.visma.no/blogg/hva-er-big-data/ Publisert 29.05.19. Lesedato 08.05.21

Norsk senter for informasjonssikring *"Trusler og trender 2019-2020"*https://norsis.no/trusler-og-trender-2019-2020/ PDF. Publisert 04.02.20. lastet ned 23.11.20

Norsk senter for informasjonssikring *"Trusler og trender 2021 https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf* Publisert 24.03.21. lastet ned 16.04.21

Norsk senter for informasjonssikring *"Nordmenn og digital sikkerhetskultur 2020"* Publisert 2020. lastet ned 16.04.21

PWC. *«Hva er Big Data og hva betyr det for deg.» PWC.* Hentet fra: https://www.pwc.no/no/publikasjoner/information-management/big-data.pdf. Publisert 2015 Lesedato 30.11.20

Rowe, Jason. *Tre ting du må vite om kunstig intelligens (AI)*. Hentet fra: https://www2.deloitte.com/no/no/pages/technology/articles/tre-ting-vite-kunstig-intelligens-ai.html. Uten dato. Lesedato 09.05.21

«Scrive.» *Digitalisering.* Hentet fra: https://www.scrive.com/no/digitalisering/ Uten dato. Lesedato 23.11.20.

Settevik, Aase. Vismas hjemmeside. *"Intelligence report recognises Vismas contribution to illuminate threats and protect organisations from cyberspionage" Hentet* fra: https://www.visma.com/press-releases/intelligence-report-visma Publisert 06.02.19. Lesedato 08.05.21

Smith, Easterby Mark, Richard Thorpe, Paul.R Jackson, Lena J. Jaspersen *«Management & Business research»* 6. Edition. SAGE publications Ltd. 2018

Standard Norge. *«NS-EN ISO/IEC 27001 ledelsessystemer for informasjonssikkerhet – krav»* https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/?gclid=Cj0KCQjw1PSDBhDbARIsAPeTqrcSBMUJgLPEOwhs6t8eSOIA7HopVqZGTA7BPBy1ZGhNi0Ox_wH0hvQaAqgjEALw_wcB Sist oppdatert 11.03.2021. Lesedato 19.April 2021.

Standard Norge. *ISO/IEC 27005:2018.* Hentet fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=983942 Uten dato. Lesedato 19.04.16

Standard Norge. *«NS-ISO/IEC 27017:2015)* Hentet fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=800605. Uten dato. Lesedato 16.04.21

Statistisk Sentralbyråd *Bruk av IKT i offentlig sektor*. Hentet fra: https://www.ssb.no/teknologi-og-innovasjon/statistikker/iktbruks Oppdatert 04.05.20 Lesedato 15.02.21

Stoksvik, Marthe. NRK. *"Russisk etterretningsekspert: uinteressant og meningsløst å grave i stortingets e-post"* Hentet fra: https://www.nrk.no/norge/russland_-_det-er-uinteressant-og-meningslost-1.15199297 Oppdatert 14.10.20. kl. 05:34. Lesedato 23.11.2020

Rajiv D. Banker, Feng Cecilia (Qian). *"The impact of information security breach incidents on CIO turnover"* Journal of information systems. Vol 33. No.3. pp. 309-329. 2019.

Regnskap Norge. *God regnskapsføringsskikk.* Hentet fra: https://www.regnskapnorge.no/faget/grfs/grfs/#2.1_Rutiner_og_intern_kontroll. Uten dato. Lesedato 22.04.21.

Rindasu, Sinziana-Marie. *«Emerging information technologies in accounting and related security risks – what is the impact on the Romanian accounting profession»* Accounting and Mangement information systems. Vol. 16, No, pp.581-609,2017.

Rolstadås, Asbjørn., Arne Krokan, Lars Thomas Dyrhaug (red.) *«Teknologien endrer samfunnet»*. 2017. Fagbokforlaget. Vigmostad & Bjørke AS.

Tidemann, Axel. *"Kunstig intelligens".* Store norske leksikon. Hentet fra: https://snl.no/kunstig_intelligens Oppdatert 08.01.2020. Lesedato 08.05.2021

Thon, Roar. Mediaplanet. *"Uten digital sikkerhet stanser Norge!"* Mediaplanet.Hentet fra: https://www.altomsamfunnssikkerhet.no/digital-sikkerhet/uten-digital-sikkerhet-stanser-norge/ Uten dato. Lesedato 29.11.20

Trend Micro Research "*Securing the pandemic-disrupted workplace. Trend Micro 2020 midyear cybersecurity report"* Hentet fra: https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf.Uten dato. Lesedato 15.02.21

«Unit.no.» *Informasjonssikkerhet og personvernforordningen (GDPR).* Hentet fra: https://www.unit.no/informasjonssikkerhet-og-personvernforordningen-gdpr. Publisert 24.04.20. Lesedato 23.11.20.

Viglo, Geir Arne. *Tre spørsmål og svar om blockchain.* Hentet fra: https://www2.deloitte.com/no/no/pages/technology/articles/tre-sporsmal-svar-blockchain.html. Uten dato. Lesedato 09.05.21

Vismas hjemmeside. *"Hva er goodwill".* Hentet fra: https://www.visma.no/eaccounting/regnskapsordbok/g/goodwill/. Uten dato. Lesedato 08.05.21.

Vismas hjemmeside. *"om oss"* Hentet fra: https://www.visma.no/om-visma/ Uten dato. lesedato 22.04.21

Woods D. David, Sidney Dekker, Richard Cook, Leila Johannesen, Nadine Sarter. *«Behind the human error»* 2. edition. Taylor & Francis Group. Print pub date 28.09.2010

8.0 Vedlegg

Vedlegg 1

INFORMASJONSSKRIV TIL INTERVJUOBJEKTER

Vår mastergruppe består av Ingrid-Marie og Ingelin. Vi studerer master i innovasjon og ledelse ved Høgskulen på Vestlandet. Dette intervjuet vil brukes som et supplement til teori og forskning i vår masteroppgave. Vi ønsker å intervjue deg om hvordan informasjonssikkerhet praktiseres hos dere.

Problemstillingen vår er *«Hvordan påvirkes informasjonssikkerheten av teknologiutvikling?»*

Endringer kan forekomme, hvis endringene er av vesentlig grad vil vi informere deg om dette på forhånd.

Vi ber deg lese gjennom spørsmålene før intervjuet slik at hvis det er et eller flere av spørsmålene du ikke har mulighet til å svare på, så kan vi endre ordlyd og innhold.

Du har rett til å være anonym i intervjuet, men vi ber om tillatelse til å bruke firmanavn, stillingstittel og arbeidsoppgaver.

Intervjutiden vil bli satt til omtrentlig 2 klokketimer.

Takk for at du tar deg tid til å snakke med oss og bidra til vår masteroppgave. Hvis du skulle ha noen spørsmål må du gjerne henvende deg til oss.

Kontaktinfo:

Ingelin Lygresten. Ingelin4444@hotmail.com – 90940008

Ingrid-Marie Tromsdal Lyster. Ingrid-marielyster@hotmail.com – 98874870

Vedlegg 2

EKSPERTINTERVJU

Hva er din tittel?

Hvor lenge har du jobbet i organisasjonen?

Hva er dine arbeidsoppgaver?

Har du erfaring innen samme arbeidsområdet fra tidligere?

Trusselbildet.

Hva anser du som største trussel (innenfor informasjonssikkerhet)?

- *Kan du forklare oss litt rundt hvorfor det.*

Har dere en beredskapsplan eller tiltaksplan knyttet til trussel scenarioer?

- *Hvorfor/Hvorfor ikke?*

- *Kan du fortelle oss litt om denne? Hvem er med?*

Vet du om organisasjonen har opplevd noen angrep i det siste?

- *Kan du fortelle litt rundt dette? (Omfang, type, konsekvens)*

Hva tenker du om sikkerheten nå vs. I fremtiden? Eks. Tror du teknologien utvikler seg fortere enn vi klarer å henge med, eller er vi forberedt?

Tror du det er større risiko ved bruk program eller skytjenester?

- *Hvorfor tror det det er størst risiko ved det?*

- *Hva tenker du er den viktigste forskjellen?*

Phishing

Hva er din mening om det?

Hvilke tiltak har dere for å beskytte dere mot phishing?

Hvis vi hadde sendt ut en e-post med en ondartet link til alle ansatte i organisasjonen hvor mange tror du hadde trykket på den?

Menneskelige feil

Vårt inntrykk er at menneskelige feil er ofte grunnlaget for brudd på informasjonssikkerheten. Hva syns du om påstanden?

Forklar oss gjerne litt om hvorfor du tenker den er riktig eller feil?

Dersom det er en menneskelig feil, hvilken konsekvens får det for den eventuelle ansatte?

Ansvar og opplæring

I mange organisasjoner har IT avdelingen ansvar for informasjonssikkerheten, tenker du det er riktig?

Hvem tenker du burde ha ansvaret for informasjonssikkerheten?

Syns du linjeansatte bør ha et ansvar for informasjonssikkerheten? Gjerne forklar litt rundt hvordan eller hvorfor.

Hvordan er ansvaret fordelt hos dere?

Hvem for opplæring i informasjonssikkerhet i hos dere?

- *Får alle like omfattende opplæring?*

- *Hvordan foregår opplæringen? Har dere et program for opplæring?*

Har dere rammeverk for internkontroll?

Hvilke lover og regler må organisasjonen forholde seg til?

Hvilke konsekvenser kan organisasjonen få av et angrep? Med tanke på GDPR og regnskapsføringsloven?

I hjemmekontor tider, har alle egne pc og logger på egne nettverk. Hvordan påvirker dette sikkerheten?

Annet

Er det noe du tenker er relevant vi kan ta med?

Er det andre vi kan/burde snakke med for å få et bedre totalt bilde?

Kan vi ta kontakt med deg på et senere tidspunkt hvis vi skulle ha spørsmål?

Vedlegg 3

Intervjuguide ansatt

1. Hvilken stilling har du?

2. Hvilken opplæring fikk du med tanke på it og it-sikkerhet? Husker du system?

3. Hvordan opplevde du den opplæringen? Var den relevant? Nyttig?

4. Har de fått frem budskapet om hvorfor de må ta kurs?

5. Hva tenker du om egen kompetanse med tanke på sikkerhet?

6. Hva kunne vært bedre? Og Hvilken opplæring og oppfølging kunne du eventuelt trengt?

7. Har du annen type kurs/ opplæring / utdanning innenfor informasjonssikkerhet fra andre steder? Hvilken type?

8. Vet du hva de største truslene innenfor informasjonssikkerhet er?

9. Tror du det er større risiko ved bruk av skytjenester eller ved bruk av programvare?

10. Har du hørt om phishing? Har du blitt utsatt for det?

11. Kan vi kontakte deg dersom vi har flere spørsmål?

Vedlegg 4

Intervju HR

Hvilken stilling har du?

Hvilken opplæring fikk du med tanke på it og informasjonssikkerhet?

Hvilke rutiner har dere for opplæring av deres ansatte innenfor IT og informasjonssikkerhet?

Bruker dere noe spesielt system for opplæring innenfor it og informasjonssikkerhet?

Hvilket og hvordan fungerer det?

Har du fått tilbakemeldinger fra ansatte på opplæring innenfor informasjonssikkerhet?

Hvordan syns du opplæringen innenfor informasjonssikkerhet fungerer i dag?

Hva burde eventuelt vært bedre?

For at ansatte skal være godt rustet innenfor informasjonssikkerhet, hva mener du skal til?

Har du fått tilbakemelding på hvordan de ansatte føler sin egen kompetanse er i forhold til informasjonssikkerhet? Føler de at de kan det godt nok i forhold til jobben sin?

Det blir ikke spurt de ansatte direkte i noen trivselsundersøkelser om kompetansen på sikkerhet?

Kan vi kontakte deg igjen dersom vi har flere spørsmål?

Vedlegg 5

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Hvordan påvirkes IT-sikkerheten i regnskapsbransjen av teknologiutvikling?

Referansenummer

387029

Registrert

05.02.2021 av Ingrid-Marie Lyster - 584420@stud.hvl.no

Behandlingsansvarlig institusjon

Høgskulen på Vestlandet / Fakultet for økonomi og samfunnsvitskap / Institutt for økonomi og administrasjon

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Carmen Olsen, carmen.olsen@hvl.no, tlf: 92018157

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Ingrid-Marie Lyster, ingrid-marielyster@hotmail.com, tlf: 98874870

Prosjektperiode

01.01.2021 - 30.06.2021

Status

02.03.2021 - Vurdert

Vurdering (1)

02.03.2021 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjema med vedlegg 2.3.2021. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 30.6.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres og som kan trekkes tilbake.

Lovlig grunnlag for behandlingen vil dermed være de registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:
- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18) og dataportabilitet (art. 20).

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Easyquest er databehandler i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Lasse Raa
Tlf. personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 6

Kodeskjema - HR

Opplæring	Hvilken opplæring fikk du med tanke på informasjonssikkerhet?	Kurs i IT-sikkerhet, cyber security, code of conduct, compliance og GDPR
Opplæring	Hvilke rutiner har Visma for opplæring av sine ansatte innenfor informasjonssikkerhet?	Alle får samme, noen får tilleggskurs. Obligatorisk cyber security month
Opplæring	Bruker visma noe spesielt system for opplæring innenfor informasjonssikkerhet?	My developement, det fungerer helt utmerket
Opplæring	Har du fått tilbakemeldinger fra ansatte på opplæring innenfor informasjonssikkerhet?	kjedelig, viktig og skjønner hvorfor de har det. Ansatte har forskjellige preferanser på hvordan kursene skal være.
Opplæring	Hvordan syns du opplæringen fungerer og hva kunne eventuelt vært bedre?	Det fungerer bra. De kan jobbe litt med det pedagogiske, utforming av kurs.
Kompetanse	For at ansatte skal være godt rustet innenfor informasjonssikkerhet, hva mener du skal til?	opplysning/oppdatering
Kompetanse/ledelse	Har du fått tilbakemeldinger på hvordan de ansatte føler sin egen kompetanse er innenfor informasjonssikkerhet?	Ja.
ledelse	Spør dere om dette i medarbeiderundersøkelse?	Nei

Kodeskjema – ansatte

		Rekrutteringskonsulent	Advisor	cloud sales executive	likheter	forskjeller
Opplæring	Hvilken opplæring fikk du (nåværende jobb) i informasjonssikkerhet?	Vi hadde en kursportal, men var i utgangspunktet learning by doing, pga få ansatte.	Kursportal som heter smart learn. Webinarer. En del i starten får vi innføring i hvordan vi skal forholde oss til det meste.	Visma Trust Center. Egen læring, der vi ansatte skal lese oss opp. Intern opplæring via extra mile knyttet til phishing og det digitale landskapet.	3 av 3 har hatt opplæring i informasjonssikkerhet på arbeidsplassen.	1 av 3 hadde learning by doing 1 av 3 har tatt kurs som kreves 1 av 3 har tatt interne kurs og i tillegg brukt selskapets sider.
Opplæring	Hvordan opplevde du opplæringen? Var den relevant? Nyttig?	Relevant men kritikkverdig fordi det ble ikke fulgt opp. Mange ansatte brukte ikke systemet.	Ja. Spesielt det med phishing	Absolutt. Så jeg vil si opplæringen var god.	3 av 3 mener den var relevant	1 av 3 mener den ikke var bra nok.
Opplæring	Fikk de frem budskapet om hvorfor du måtte ha kurs?	Ja, men ble kastet litt ut i det.	"Si det, ikke bortsett fra det åpenbare"	Absolutt. Vi skal ikke slippe inn noen som helst type trusler i våre systemer. Det er godt begrunnet.	2 av 3 mener de fikk frem budskapet	1 av 3 er usikker.
Kompetanse	Hva tenker du om egen kompetanse innenfor informasjonsssikkerhet?	Ganske høy, fordi jeg har hatt lik opplæring hos annen arbeidsgiver der jeg har fått godkjennelser.	Føler seg i stor grad trygg på egen kompetanse	Har fått ekstra kompetanse gjennom casene jeg har jobbet med. Kompetansen er ikke perfekt, men over gjennomsnittet.	3 av 3 er fornøyd med egen kompetanse	
Opplæring	Hva kunne vært bedre?	En helt konkret plan, kurs i GDPR og hvitvasking.	Det kunne vært live, oftere, spesielt nå når det er mye hjemmekontor.	Tidspunkt for utlevering av kursene. De kommer som regel når det er travlest. Får lite fokus på kursene.	3 av 3 mener gjennomføringen kunne vært annerledes. 3 av 3 mener det kunne vært oftere.	Alle har ulike punkt de mener er viktig eller kunne vært bedre, men i all hovedsak innenfor samme kategori
Kompetanse	Har du annen type kurs/utdanning/opplæring innenfor informasjonssikkerhet?	Ja, jeg har GOS, GDPR, AFR gjennom annen arbeidsgiver	Nei.	Nei	2 av 3 har ikke annen kurs/utdanning/opplæring	1 av 3 har kursing gjennom annen arbeidsgiver.
Kompetanse	For at ansatte skal være godt rustet innenfor informasjonssikkerhet, hva skal til?	Faddersystem og gjennomganger med tester.	Kunne vært oftere kursing.	En dedikert person internt i organisasjonen, som kan fokusere på kontinuerlig læring, minne ansatte om viktigheten, gjennomføring av kurs og sertifiseringer.	3 av 3 sier det handler om kontinuerlig læring, testing og gjennomføring av kurs	1 av 3 har et forslag om en dedikert person som kan håndtere denne rollen.

Trusselbildet	Tror du det er større risiko ved bruk av sky- eller programvare?	Vet ikke	Vet ikke	Totalt sett, skytjeneste er tryggest, kommer an på program og leverandør. Har de Riktig type sertifisering og riktig type utviklingsramme verk så er skytjenester tryggest, tror jeg.	2 av 3 vet ikke.	1 av 3 mener skytjeneste har minst risiko hvis man velger riktig leverandør.
Trussebildet	Vet du hva de største truslene innenfor informasjonssikkerhet er?	Det er hacking av systemer og uthenting av informasjon av kundebaser, tror det.	"eh nei, egentlig ikke. Men regner med det er datafangst eller, hacking. Informasjon som kommer på avveie."	Phishing og spoofing. Og at ansatte ikke vet nok, og er ukritiske.	3 av 3 mener det handler om uthenting av informasjon.	1 av 3 nevner spoofing. 1 av 3 nevner menneskelig feil.
Trusselbildet	Har du hørt om phishing?	Ja	Ja	Ja	3 av 3 sier ja	ingen ulikhet
Trusselbildet	Har du blitt utsatt for phishing?	Ofte, men det er ganske gjenkjenbart for meg. Så da er det å rapportere på en bestemt måte.	både privat og hos tidligere arbeidsgiver.	Nei, ikke så vidt jeg vet.	2 av 3 har blitt utsatt for phishing	1 av 3 har ikke blitt utsatt for phishing.
Produkt	Hvilke sikkerhetsløsninger selger dere mest av?	(ikke relevant)	lønnssystemer	(Ikke relevant)		
Produkt	Hva er firmaer dere selger til, mest opptatt av å sikre seg mot?	(ikke relevant)	Sensitive informasjon som ligger i lønn/personinformasjon. De vil vite hvordan det er lagret og beskyttet. Skytjeneste.	(Ikke relevant)		

Kodeskjema – Eksperter

		Azets	Visma	Uavhengig	Likheter	Ulikheter
Trusselbilde	Største trussel	ikke spesifikk trussel i dag - mer komplisert enn det. Phishing er mest plausibelt/jobber mest med å unngå/ ene rene trusselen. Den menneskelige faktoren	mennesker/menneskelig svikt	Phishing - Fordi fokus har vært på andre ting, epost sikkerhet har vært glemt.	2 av 3 - Phishing. av 3 - Menneskelig faktor	2 1 av 3 nevner ikke mennesker
Trusselbilde	Beredskapsplan/tiltaksplan	Ja, for mange scenarioer, samlet i en business continuity plan. Alle har det tilgjengelig på sin PC. Målet med beredskapsplanen er å kunne fortsette å levere. Vi tester ut planene med table-top test. Sikkerhetsavdelingen lager planene. Sikkerhet har blitt en stor del av regnskapsbransjen.	Ja. Tilpasset forskjellige type trusler. ISO sertifisering (27001)	Ja, internt og leverer til kunder. Eget team som er opplært i IRT.Internt hos oss har vi gode løsninger for back up og tilgangskontroll. Gode systemer for epost. Diskutere med ledelsen forløp og hendelseshåndtering. Få rutiner på plass. Teknisk og ledelseskompetanse hos nøkkelpersoner	3 av 3 har tiltaks og beredskapsplan. av 3 har tilpassede planer til ulike trusler.	3 Kun 1 har nevnt hvordan dette fungerer/er samlet. Kun 1 har nevnt hva det er bygget opp på.
Trusselbilde	Rammeverk	Business contunity plan.	Ja. Dannet selv (VCDM). Basert på forskjellige internasjonale standarder.		2 av 3 har et spesisikt rammeverk.	1 av 3 nevner ikke noe navn
Trusselbilde	Kjente nylige angrep.	Ingen direkte store angrep. Under angrep hele tiden (åpne brannmur, gjette passord). Hele tiden phishing angrep, mye automatisert og målrettet. Fakturasvindel er en reell ting i regnskapsbransjen	Ja. 30.000 i året. 1 alvorlig til interne systemer. Basert på phishing og menneskelig svikt.	Ja,fryktelig mye. Gjennom phishing. Man må ha et aktivt forhold og plan for det. Samhandling mellom teknologien og menneskene.	3 av 3 under angrep, men ikke et spesifikt stort. av 3 sier det er pga. phishing. 2 av 3 sier det pga mennesker	3 1 av 3 nevner fakturasvindel.

Trusselbilde	Sikkerheten nå vs. I fremtiden	Kvantedatamaskiner, AI, maskin vs. Maskin gjør fremtiden usikker. Data du strømmer i dag, kan være like sensitiv om 5 år. Regnskapsbransjen ikke mest utsatt. Digitalisering/Teknologien er på god vei, men det er mange år igjen for å få den på plass. Prosessen i fremtiden er nok ganske lik, bare med andre produkter. Må tenke sikkerhet på andre måter.	Nei, evig kamp. Håper å holde stand ved bruk av riktig teknologi. Menneskelige faktoren. Ledere. Passord. Tofaktor.	De bedriftene som ikke har IT som fokus eller kjerneområdet vil ha nytte av å endre strategi og fokus. De vil være mer sårbar ettersom teknologien endrer seg fort.	2 av 3 nevner endring av strategi og fokus. 3 av 3 nevner teknologiutvikling. 3 av 3 mener vi ikke er forberedt på fremtiden.	1 av 3 fokuserer mest på at t eknologien utvikler seg og blir mer tilgjengelig. 1 av 3 fokuserer på å forbedre eksisterende tiltak.
Trusselbilde	Størst risiko ved progam eller skytjenester?	Kommer an på kompetansen du selv har eller selskapet du kjøper det av har. Delt ansvar, automatisk backup, tryggere å lagre hvis man bruker skytjenester. Eget datasenter krever mye. Det er like risikabelt, kommer an på hvordan du bruker det. Menneskelige feil. Tofaktor	Skytjenester er mer eksponert, men vil alltid være bedre pga. det er lettere å kvalitetssikre. Program/software er mer på lykke og fromme	Samme risiko. Vil heller skille på om du kjøper eller bygger selv. Server er en server, kjøper du software så har du ikke innsikt i sikkerheten som ligger i forkant.	2 av 3 sier det er like risikabelt. 3 av 3 nevner kompetanse/bruk av tjenesten. 3 av 3 nevner flest fordeler ved skytjenester.	1 av 3 nevner usikkerhetsaspektet i kjøpt ferdig programvare.
Phishing	Phishing er største trussel nå?	Helt klart, vanligste og enkleste måten. Krever mye å stoppe det.	Ja. Enklest. Blir mer sofistikert og overbevisende. Tilpasser basert på kjente fakta.	Ja	3 av 3 sier ja. 2 av 3 sier dette er enkleste måte.	Ingen ulikheter
Phishing	Tiltak mot phishing	Opplæring (x3) Nyansatte må på kurs, kurs kjøres jevnlig hele året. Tofaktor. Epostfunksjonalitet mot phishing (privat sertifikat/nøkkel, digitalt signerer epost for å verifisere)	Google plattform. Filtrer og monitorering. Forskjellige type programvarer fra kjente leverandører. Viktigst er opplæring av ansatte (x2). Et team som jobber med nytt IT tema måned til måned. Kurs hver måned relatert til IT-sikkerhet.	Epost filter, vasker epost, integrasjoner som gjør det mulig å varsle, hjelpeknapp, beskjed om usikker kilde og fake domene. Hjelpemidler og infrastruktur må være på plass, eposten skal ikke havne i innboksen. Bedrifter har lagt ansvaret over på brukeren. To timers kurs hjelper ikke.	3 av 3 nevner opplæring 3 av 3 nevner epost filter og funksjonaliteter knyttet til dette.	1 av 3 nevner at ansvaret fortsatt ikke ligger på brukeren.
Phishing	Hvor mange hadde trykket på ondartet link?	10-15% aka. Godt over 100 kontoer.	Noen.	Alltid noen som trykker.	3 av 3 mener noen ville trykket på linken.	Ingen ulikheter
Menneskelige feil	Menneskelige feil er ofte grunnlaget for brudd på informasjonssikkerhet?	Litt enig, kan alltids spores tilbake til menneskelig feil. Gjerne uflaks som gjør det, fordi det fortsatt er en del manuelle prosesser. Er det automatisert prosess, så er det feil i kjeden. Teknologien får beskjed av mennesker, hvordan den skal oppføre seg.	Ja.	Det er jeg helt enig i. Men ikke enig i skylddelingen, brukeren skulle aldri fått den muligheten.	3 av 3 er enige.	1 av 3 påpeker at det er mennesker bak automatiserte prosesser. 1 av 3 påpeker at bruker ikke skal ha mulighet for brudd på informasjonssikkerhet.
Menneskelige feil	Konsekvens for ansatt - om utfører menenskelig feil.	Ingen konsekvens for den enkelte. Kan få sparken om det gjøres med vilje. Er det mulig å gjøre feil så er det feil i rutiner eller kompliserte systemer, dårlig tilrettelegging. Kanskje personen må ta opplæring og kursing og se på interne ting.	Advarsel, konsekvenser hvis man slurver over tid.	De må gi fra seg brukernavn og passord.	3 av 3 sier ingen personkonsekvens for den ansatte.	1 av 3 nevner feil gjort med forsett. 1 av 3 nevner feil pga. slurv 1 av 3 nevner kun praktiske konsekvenser.
Ansvar og opplæring	IT avdelingen alene har ansvar for informasjonssikkerhet?	Nei, delt/felles ansvar (x4). Tankegang som tilhører fortiden. Ikke sterkere enn svakeste ledd.	Nei, delt/felles ansvar (x3). IT skal drive det. Jurister - den juridiske siden. GDPR og holdninger - HR	Nei, det bør være en CISO. Gjerne ha en ansvarlig internt i bedriften når det kommer til DLP og informasjonssikkerhet. Felles ansvar å implementere, handle inn og sette opp systemene.	3 av 3 mener det er et felles ansvar. 2 av 3 nevner andre nøkkelroller med ansvar.	1 av 3 nevner at IT skal drifte informasjonssikkerheten.
Ansvar og opplæring	Skal regnskapsførere ha ansvar for informasjonssikkerheten?	Ja, de har like mye ansvar som meg. De har ansvar for dokument og data de behandler. Ansvarsfordelingen hos oss er kompleks. Vi har veldig mange roller, med forskjellig ansvar. Men er til syvende og sist, alles ansvar.	I høyeste grad. Kunders data. Kundens systemer. Databehandleravtale	(ikke relevant)	2 av 2 sier ja. 2 av 2 nevner at det er kunders data de er ansvarlig for.	Ingen ulikheter
Ansvar og opplæring	Hvem får opplæring i informasjonssikkerhet?	Alle får i stor grad like mye opplæring. Egne kurs med forskjellige vinklinger for spesifikke roller. HR har ansvaret for opplæring som har med sikkerhet å gjøre. GDPR, regnskapsloven osv.	Alle, på forskjellig nivå. Spesialister og utviklere får en annen type.	CEO, CFO, styremedlemmer skal ha oversikt og være med på risikovurdering. Ned på ingeniørnivå med implentasjon av sikkerhetsverktøy.	3 av 3 sier alle får opplæring. 3 av 3 sier det er tilpasset rollen.	Ingen ulikheter
Ansvar og opplæring	Program for opplæring	Eget IT-sikkerhetsopplæringsprogram. Tester, tilbyr trening, rapporering. Hvert kvartal . 2-3 video/oppgaver de skal gjøre. Kjører phishing tester og oppgaver jevnlig hele året. Problemet er at det koster penger.	onboardingsprogram til VCDM	Vi har maler, men det må sys til de forskjellige organisasjonene.	3 av 3 har eget opplæringsprogram.	3 av 3 har forskjellig program
Trusselbilde	Rammeverk for internkontroll	Ja, basert på NIST og CIS. Et CMS verktøy som inneholder alle risikoer og internkontroller, linket mot hverandre. Vi har hentet litt fra datatilsynet og nasjonal sikkerhetsmyndighet. Har foreløpig ikke sertifiseringer.	Ja, vanlig kvalitetssystem basert på ISO Sertifisering.	ISO 27001 - det er når de ønsker sertifisering at de kontakter oss.	2 av 3 er ISO sertifisert. 3 av 3 bruker kjente rammeverk.	1 av 3 er ikke sertifisert.
Ansvar og opplæring	Lover og regler dere må forholde dere til?	AML, Norsk lov, GDPR, internajonale lover pga internasjonale kunder.	Norsk lov. Spesielt GDPR, bokførings og regnskapsføringsloven.	(ikke relevant)	2 av 3 helt like lover og regler	1 av 3 ikke spurt, fordi det ikke er regnskapsbedrift.
Ansvar og opplæring/menneskelige feil	Konsekvens av angrep (lov)	Verste er å miste ansikt (miste kunder, ikke få nye kunder). GDPR brudd, 10% av total omsetning eller 20 mill euro. Mindre erstatningsansvar. Andre ting: Ødelegge folks liv pga personopplysninger, dette er med i risikovurdering. Advokater hjelper der.	Dårlig omdømme, Persondata på avveie, bot av datatilsynet (4% av omsetning, omsetter for 23 milliarder)	(ikke relevant)	2 av 2 nevner omdømme, bot og persondata på avveie.	
Trusselbilde	Hvordan påvirker hjemmekontor informasjonssikkerheten?	Ikke opplevd problemer med det, men har hatt tiltak og regelverk.	Negativt, men vet ikke i hvilken grad.	Teknisk, tror jeg mange organisasjoner har løst det godt.	3 av 3 har ikke et konkret svar	1 av 3 tror det har påvirket negativt.