Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Arien Hosseini
Asbjørn Loven
Thomas Selliseth

Informasjonssikkerhetsarbeid gjennom ledelsessystemer for informasjonssikkerhet

En casestudie for E.A. Smith

Bacheloroppgave i Digital Forretningsutvikling
Veileder: Torstein Elias Løland Hjelle
Mai 2021

NTNU
Kunnskap for en bedre verden

Arien Hosseini
Asbjørn Loven
Thomas Selliseth

Informasjonssikkerhetsarbeid gjennom ledelsessystemer for informasjonssikkerhet

En casestudie for E.A. Smith

Bacheloroppgave i Digital Forretningsutvikling
Veileder: Torstein Elias Løland Hjelle
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU

Kunnskap for en bedre verden

Forord

Denne bacheloroppgaven er skrevet ved Institutt for Datateknologi og Informatikk ved Norges teknisk-naturvitenskapelige universitet. Bacheloroppgaven er avsluttende del av det treårige studiet Digital forretningsutvikling, og er skrevet vårsemesteret 2021. Oppgaven er formet ut fra intervjuer av ansatte hos E.A. Smith i tillegg til selvstudie av relevant fagstoff. Bachelorgruppen har funnet det utrolig interessant å lære om informasjonssikkerhet fra mange vinkler og hvordan den påvirker organisasjoner. Etter flere møter med veileder og E.A. Smith ble det tydelig at informasjonssikkerhet er noe vi ønsker å se nærmere på, spesielt i henhold til sikring av informasjon og oppbygging av sikkerhetsrutiner i organisasjoner.

Vi ønsker å takke våre kontaktpersoner hos E.A. Smith samt andre ansatte vi hadde gleden av å intervjue for gode og informative samtaler og godt engasjement. I tillegg ønsker vi å gi en stor takk til våre informanter for at de ønsket å stille opp, og gi gode svar og refleksjoner rundt våre forskningsspørsmål og vår problemstilling. Vi setter svært stor pris på det samarbeidet vi har hatt gjennom disse månedene, og er svært takknemlige for all hjelpen som har latt oss produsere en god bacheloroppgave.

Til slutt vil vi takke vår veileder Torstein Elias Løland Hjelle for oppfølging, hjelp og gode råd gjennom forskningsprosessen. Vi setter pris på veiledningen hans, og sitter igjen med ny kunnskap etter dette prosjektet.

Tittel	Informasjonssikkerhetsarbeid gjennom ledelsessystemer for informasjonssikkerhet: En casestudie for E.A. Smith
Title	Information security work through an information security management system: A case study for E.A. Smith
Dato	20.05.2021
Deltakere	Arien Hosseini, Asbjørn J. Loven, Thomas Selliseth
Veileder	Torstein Elias Løland Hjelle
Oppdragsgiver	E.A. Smith AS, NTNU
Totalt antall sider	51
Antall vedlegg	10

Sammendrag

Informasjonssikkerhetsarbeid og prosesser rundt dette opplever stadig mer fokus i de fleste organisasjoner. Med økt digitalisering og informasjonsflyt øker også nødvendigheten for sikkerhet rundt denne informasjonen. Spesielt hos bedrifter er nødvendigheten for informasjonssikkerhet stor. Dette skyldes økt angrepsfrekvens og risiko i nyere tid, som gjør det enda viktigere å beskytte sensitive opplysninger både med hensyn til kunder og intern drift.

Denne oppgaven ser på risikoen tilknyttet mangelen på informasjonssikkerhet og hvor utsatt bedrifter kan være. Vi har undersøkt informasjonssikkerhetsarbeidet til E.A. Smith gjennom semi-strukturerte intervjuer. Basert på resultater herfra har vi gjennomgått en evaluering på i hvilken grad deres systemer måler seg mot standardiserte informasjonssikkerhetskrav. Samtidig ønsker vi å hjelpe dem med en hensiktsmessig innføring av et formelt styringssystem for informasjonssikkerhet. For å gjøre dette, tar vi hovedsakelig utgangspunkt i det internasjonale rammeverket for informasjonssikkerhet, ISO 27000-serien.

Abstract

Information security, with its associated risks and processes, is currently experiencing an increased focus in most organizations. With increased digitalisation and flow of information, the need for additional security measures consequently increases. This especially applies to companies, due to the higher attack frequencies and risks in modern times, which makes it even more important to protect sensitive data both in respect of customers and internal management.

This dissertation focuses on risk associated with the lack of proper information security and how vulnerable companies can be. We have researched E.A. Smith's work with information security through semi-structured interviews. Based on these results we have done an evaluation as to what degree their systems compare to standardised information security requirements. Simultaneously, we want to assist them in doing an appropriate implementation of a formal information security management system. To achieve this, we primarily focus on the international framework for information security, the ISO 27000-series.

Innholdsfortegnelse

Introduksjon

Med en stadig mer digitalisert verden vil trusselbildet konsekvent øke. Behovet for bedre informasjonssikkerhet øker, som artikkelen til E24 «Norges bankkjemper har avdekket flere Kina-angrep: - Trusselbildet er økende» formidler: *«Både DNB og Nordea opplyser og avdekker at et økende antall dataangrep rettes mot deres systemer – og at angriperne blir stadig mer profesjonelle. - Det generelle trusselbildet er økende. Antall dataangrep øker, kompleksiteten øker, og angriperne blir stadig mer profesjonelle»* (Wig, 2019). For å beskytte informasjonen en bedrift besitter, øker behovet for strategiske tiltak.

Konsekvensene av slike dataangrep kan i verste fall være katastrofalt for virksomheten. Et eksempel på dette er hentet fra den norske nettavisen Digi, som fokuserer på IT. I artikkelen forteller de om hvordan det danske høreapparatselskapet, Demant, ble hardt rammet av et virusangrep høsten 2019. Hendelsen skal ha tvunget Demant til å stenge ned alle IT-systemer på tvers av lokasjoner i mange uker, og hele kostnaden er regnet ut til å være på over 800 millioner kroner. Videre forteller Digi at: "*Hendelsen berørte kjernevirksomhet gjennom hele verdikjeden, inkludert forskning og utvikling, produksjon og distribusjon. Alle forretningsområder ble påvirket, men i ulik grad og med regionale forskjeller*" (Jørgenrud, 2019). Som vi ser er trusselen reell, og forebyggende informasjonssikkerhetsarbeid er derfor avgjørende for å møte dagens utfordringer.

Case-bedriften

Bedriften som denne casen baseres på, E.A. Smith AS, er en av landets ledende aktører innen salg av byggevarer, trelast, stål og armering. Bedriften er et familieselskap etablert i Trondheim i 1869, som eier og driver Bygger'n kjedekonsept på totalt 100 butikker, derav halvparten er egeneide og den andre halvdelen franchises. Samtidig eier og driver de virksomhetene Smith Stål, LSE Byggesystemer og HIBA Hus. Totalt er det 800 ansatte som jobber i bedriften, spredt rundt med en geografisk tilstedeværelse over hele landet.

Bedriften tilbyr også hjelp med planlegging og gjennomføring av byggeprosjekter. Dersom man ønsker å bygge et hus, en hytte eller en garasje, så tilbyr de å bygge det for kunden. De generer sine egne miljødeklarasjoner og benytter seg av en felles ERP-plattform, som er en

programvare for administrasjon av forretningsprosesser og bidrar til å forbedre arbeidsprosesser i bedriften.

Hverdagen til de ansatte i bedriften påvirkes av koronapandemien, som rammet hele verden i 2020. Dette har medført en rekke tiltak som bedriften har innført, blant annet hjemmekontor for alle som kan, digitale møter og økt nettkommunikasjon. En slik digitaliseringsprosess vil fort medføre nye og økte trusler for informasjonssikkerheten til bedriften, som går innpå formålet med denne bacheloroppgaven (E.A. Smith, 2020).

Informasjonssikkerhetsarbeidet i E.A. Smith foretas av IT-avdelingen deres. De har flere sikkerhetstiltak til stede i bedriften som bidrar til å ivareta informasjonssikkerheten deres, men informasjonssikkerhet er ikke et element de har innarbeidet i strategien deres. Bedriften er ikke ISO27001-sertifisert, men de har likevel noe virksomhet i Nordsjøen som er sertifisert ettersom det er et krav for å kunne operere i markedet der. Det er flere sikkerhetstiltak som bør implementeres, og det finnes rom for forbedringer til allerede eksisterende tiltak. Som er spesielt det denne oppgaven kommer til å utdype seg om.

Problemstilling

Denne bacheloroppgaven er gitt på oppdrag av E.A. Smith, og har til hensikt å styrke informasjonssikkerhetsarbeidet i organisasjonen. Dette skal gjøres gjennom å se på hvordan formalisert styringssystem for informasjonssikkerhet (ISMS) kan støtte arbeidet og bidra til et mer helhetlig og målrettet system innenfor informasjonssikkerhet. Dermed vil vi i denne oppgaven undersøke hvordan dagens informasjonssikkerhetssystem hos E. A. Smith måler seg mot standard ISMS og ISO 27001/02-rammeverket. ISO 27001 stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. ISO 27002 er en supplerende standard som gir god praksis for gjennomføring av dette (Standard Norge, u.d.). Dette vil bli undersøkt gjennom intervjuer med ansatte, gjennomgang av teori og forutsetninger for de aktuelle rammeverkene, samt hvordan dagens situasjon måler seg mot de anbefalinger og retningslinjer som er fastsatt under ISMS og ISO 27001/02-standarder.

På bakgrunn av dette arbeidet vil vi deretter komme med anbefalinger til tiltak for å kunne styrke informasjonssikkerheten og arbeidet rundt i organisasjonen. Videre vil det også bli

skissert en strategi/utgangspunkt for hvordan E. A. Smith kan implementere standard ISMS i henhold til ISO 27001/02-rammeverket.

Vår problemstilling blir dermed: *Hvordan kan innføring av et styringssystem for informasjonssikkerhet og ISO 27001-standarden styrke informasjonssikkerhetsarbeidet i organisasjonen E.A. Smith?*

Avgrensning av oppgaven

Gitt situasjonen til E.A. Smith og problemene de har samt områdene innen ISMS hvor de trenger veiledning, velger vi å avgrense oppgaven til bare to standarder i ISO 27000-serien. Ved å avgrense oppgaven til ISO 27001 og ISO 27002 er vi sikre på at vi holder oss relevant til utfordringene E.A. Smith opplever samt vår egen problemstilling. Videre kan resterende deler av ISO 27001 og ISO 27002 som vi finner å være relevante nok og/eller viktige på generell basis dekkes i mindre grad med fokus på å ikke skli vekk fra vår originale problemstilling.

Hvordan vi bestemmer hvilke deler av ISO 27001 og ISO 27002 standardene som skal beskrives i detalj kommer fra informasjon vi får direkte fra E.A. Smith. I utgangspunktet har vi fått en generell presentasjon av bedriften i tillegg til å ha gjennomført fire semi-strukturerte intervjuer. Disse intervjuene har produsert mye informasjon nødvendig for å svare på problemstillingen vår og assistere E.A. Smith i å forbedre sine ISMS systemer.

Spørsmålene vi bruker i disse intervjuene er konstruert for å spørre om spesifikke aspekter av IT-sikkerheten til E.A. Smith. Videre bruker vi svarene fra disse intervjuene til å sammenligne med ISO-standardene for å fastsette om implementering av ISO-standardene kommer til å produsere virkningsfulle resultater.

Oppgavens oppbygging

Oppgaven er strukturert som en tradisjonell case-studie. Med dette menes det at oppgaven starter med en forside, sammendrag, abstrakt og innholdsfortegnelse. Senere i oppgaven er det dedikerte kapitler som omhandler forskjellige aspekter som vi mener den bør inneholde for å produsere et tilfredsstillende svar på problemstillingen vår.

Den første av disse er introduksjon hvor vi klargjør våre motiver, relevansen av oppgaven i dagens miljø og introduserer casen vår og E.A. Smith som er selskapet vi jobber med. Neste kapittel handler om teori som er relevant for casen. Her introduserer og forklarer vi mange vitenskapelige begreper og teorier som er relevante for å svare på problemstillingen vår. Videre skal teorien beskrevet her gjenbrukes i senere kapitler for å dra konklusjoner. Det følgende kapitelet, casebeskrivelse, er dedikert til casen vår og hva vi tenker er best måte å løse problemstillingen vår på. Neste kapittel handler om metode og hvilke metoder vi har brukt til å samle inn data for å assistere E.A. Smith. Kapitelet inneholder også noen korte beskrivelser av forskjellige metoder samt vår begrunnelse for valg av metode vi har brukt.

Etter metode kapitelet følger fire kapitler som er mer selvstendige. Det første kapitelet etter metode er resultater, hvor vi går igjennom våre funn fra vår datainnsamling. Informasjonen vi har fått fra vår primærkilde, intervjuer, blir også grundig oppsummert. Videre har vi diskusjon hvor vi begynner å dra paralleller mellom problemene til E.A. Smith og manglene på ordentlige ISMS systemer og rutiner. Vi går også gjennom områder innen IT-sikkerhet hvor E.A. Smith ikke har hatt problemer, men er potensielt utsatt. Det følgende kapitelet er dedikert til å skissere diverse løsninger E.A Smith kan se fordeler av. Hovedsakelig peker alle disse løsningene mot å implementere ISO-standarder og sertifisere seg. Til slutt konkluderer vi oppgaven i det siste kapitelet kalt konklusjon. Her oppsummerer vi alt som er gjennomgått tidligere i oppgaven og produserer vår endelige konklusjon. Denne konklusjonen er i vår mening den beste måten å svare på problemstillingen vår og den beste måten å assistere E.A. Smith med sine problemer med IT-sikkerhet.

Vår oppfatning er at en slik oppbygning er mest gunstig for å være å så grundig som mulig samtidig som vi holder relevansen for oss og E.A. Smith høy. Alt som dekkes i denne oppgaven mener vi er nødvendig å dekke for å produsere et optimalt sluttprodukt.

Teori

Denne delen av oppgaven kommer først til å rette seg inn på begrepene "informasjon" og "informasjonssikkerhet", for å gi bedre forutsetninger til å forstå hva et ISMS er, før begrepet ISMS også forklares. Deretter gjennomgås begrepene "trusselbildet" og "risikoanalyse" og teorier som McCumbers sikkerhetskube og Demings prinsipper for kontinuerlig forbedring. Til slutt rettes oppgaven inn på de internasjonale standardene ISO 27001 og ISO 27002 og hvilken betydning de har for E.A. Smith.

ISMS

Informasjon og informasjonssikkerhet

Informasjon er et sentralt begrep med ulike betydninger avhengig av sammenhengen begrepet brukes om. Det kan være materiell data som ord, tall og bilder, eller andre menneskeorienterte ressurser som kunnskap, konsepter og ideer. Dersom vi tar utgangspunkt i NS-EN ISO/IEC 27000:2020 (ISO 27000), som omhandler informasjonsteknologi, sikringsteknikker og ledelsessystemer for informasjonsteknologi, så defineres informasjon som:

"Information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees." (Standard Norge, 2020).

NS-EN ISO/IEC 27002:2017 (ISO 27002), som omfatter tiltak for informasjonssikring, definerer informasjon som:

«Verdien av informasjonen går ut over de skrevne ordene, tallene og bildene: Kunnskap, konsepter, ideer og varemerker er eksempler på latente former for informasjon» (Standard Norge, 2017).

Videre formidler disse ISO-standardene hvordan informasjon kan overføres gjennom metoder som muntlig og elektronisk kommunikasjon, og hvordan informasjon er et viktig driftsmiddel. Informasjon er derfor en ressurs som ikke bare er viktig for bedriften å beskytte,

men det er essensielt for en organisasjons virksomhet. Konsekvent er det av stor interesse å beskytte denne informasjonen mot ulike sikkerhetsrisikoer og trusler som bedriften møter.

Ifølge Digdir, også kjent som digitaliseringsdirektoratet, som er regjeringens verktøy for raskere og mer samordna digitalisering av samfunnet, så er god informasjonssikkerhet en forutsetning for god virksomhetsstyring og en vellykket digitalisering. Det handler om å styre risikoene man møter. En offentlig virksomhet arbeider med informasjonssikkerhet for å utføre sine oppgaver og levere sine tjenester på en god måte, som dermed hjelper dem med å nå sine mål og ivareta lovpålagte forpliktelser (Digdir, 2021).

Informasjonssikkerhet handler derfor om å sikre informasjonssystemene som benyttes i virksomheten. Dette inkluderer digitale tjenester, IKT-systemer og komponenter som inngår disse systemene. Samtidig inngår dette tilretteleggelse av arbeidsoppgaver og kompetansesikring slik at mennesker kan ha gode forutsetninger for sikkerhetsarbeidet, og arbeidet for en kultur som understøtter dette arbeidet.

Informasjonssikkerhet omfatter dermed beskyttelse av:
Konfidensialitet - dette innebærer at informasjonen ikke blir kjent for uvedkommende
Integritet - at informasjonen ikke blir endret utilsiktet eller av uvedkommende
Tilgjengelighet - informasjonen er tilgjengelig ved behov

Figur 1: Bilde av «The CIA Triad of information security» (Comtact, 2019)

Dersom det skjer et brudd på ett eller flere av disse områdene, så regnes det som et brudd på informasjonssikkerheten (Digdir, 2021).

ISMS

ISMS er et styringssystem for informasjonssikkerhet som kan implementeres i bedrifter for å beskytte deres informasjonsressurser. Et ISMS bygger på å velge ulike strategier, policyer, prinsipper, retningslinjer, prosedyrer og standarder som er nødvendige for å bevare informasjonens konfidensialitet, integritet og tilgjengelighet fra ulike trusler og sårbarheter (Datatilsynet, 2018).

ISO 27000:2020 standarden definerer ISMS som:
"*An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives* (Standard Norge, 2020)".

Deretter går standarden mer i detalj og forklarer hvordan ISMS baserer seg på risikovurderinger og hvilket nivå av risiko bedriften kan akseptere. Det er viktig å kartlegge situasjonsbildet slik at bedriften kan iverksette sikkerhetstiltak for å kunne effektivt håndtere og forhindre trusler virksomheten møter. Å analysere behovene man mangler og deretter implementere velfungerende tiltak bidrar til en vellykket implementering av et ISMS.

Videre definerer standarden ni fundamentale prinsipper som kan bidra til en vellykket implementasjon av et ISMS for en virksomhet.

1. Bevisstgjøring rundt behovet for informasjonssikkerhet. Innebærer å forankre behovet for informasjonssikkerhet i bedriften, slik at alle aktører innser hvor viktig informasjonssikkerhet er.
2. Utdele ansvar for informasjonssikkerheten. Rollefordeling, slik at man har klare ansvarsområder de ansatte jobber med, og effektivt kan opprettholde sikkerheten.
3. Forankre ledelsen og interessenter inn i sikkerhetsarbeidet. Det er viktig å få med seg alle aktører i sikkerhetsarbeidet, hvis ikke er det fare for at implementasjonen ikke er vellykket.
4. Forbedre samfunnsmessige normer og verdier. At man behandler alle aktører i bedriften med respekt, uavhengig av rolle eller bakgrunn. Det etiske aspektet er viktig

for å skape en god kultur, som oppnås gjennom å forbedre verdier som ærlighet og rettferdighet.

5. Risikovurdering for å avgjøre hvordan ulike risikoer og trusler skal inngå under virksomhetens akseptkriterier. Gjennomgå risikovurderinger ofte for å kartlegge og analysere trusler bedriften møter.
6. At sikkerhet er innarbeidet som en nødvendig del av informasjonsnettverk- og systemer.
7. At virksomheten er proaktiv på å oppdage og forhindre sikkerhetsbrudd. En reaktiv tilnærming til sikkerhet er ikke nok til å forhindre fremtidige sikkerhetsbrudd. Det er viktig å forhindre sikkerhetsangrep før de skjer i så stor grad det er mulig.
8. Å sørge for en omfattende tilnærming til administrasjon av informasjonssikkerhet. Sikkerhet er et svært viktig aspekt og derfor er det nødvendig å sette inn nok arbeid for å skape en god standard for bedriften.
9. Regelmessig evaluering av informasjonssikkerheten og iverksette nødvendige tiltak ved behov. Det holder ikke å bare implementere et ISMS. Dette er en kontinuerlig prosess med jevnlige vurderinger og tiltak (Standard Norge, 2020).

For å ivareta informasjonssikkerheten er det nødvendig å implementere flere strategier og metoder for å kartlegge trusselbildet organisasjonen møter. Som ISO 27000:2020-standarden tilsier er gjennomføring av risikoanalyser en av dem, men før dette forklares, er forståelse av trusselbildet en nødvendig forutsetning.

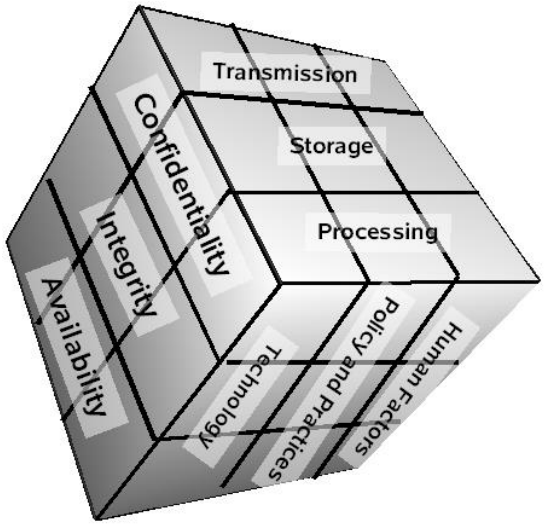
Trusselbildet

Å identifisere trusler bedriften kan rammes av og hvilke konsekvenser dette kan forårsake er svært viktig for informasjonssikkerheten til bedriften. Derfor vil det å kartlegge trusselbildet være en proaktiv metode for å dekke det behovet. Spesielt nå som NorSIS, norsk senter for informasjonssikring, som er en del av regjeringens innsats på informasjonssikkerhet i Norge, hevder i sin årlige "Trusler og trender" rapport at trusselbildet kommer til å utvikle seg fremover. For eksempel forteller de om hvordan løsepengeviruset, som er en foregående enorm trussel i Europa, rammet det aller meste av Østre Toten kommunes IT-systemer den 9. januar 2021. Ikke bare er offentlig sektor et offer for dette viruset, men NorSIS forteller videre: "*Vi vet at løsepengevirus og andre typer dataangrep rammer og ødelegger for store*

summer rundt om i Bedrifts-Norge hver eneste dag. Det skjer langt oftere og er mye vanligere enn mange tror (NorSIS, 2021).

En annen stor foregående trussel er kontokapring. Hele åtte av ti datainnbrudd i sky- og lagringstjenester er tilknyttet kompromitterte passord. Løsepengeviruset er også noe som kan spre seg til sky- og lagringstjenester, og angripere kan enkelt få tilgang til systemer gjennom lenker og vedlegg i e-post, Microsoft-filer, en Facebook-post eller gjennom sms. Alle disse risikoområdene gjør det svært viktig å kartlegge trusselbildet (NorSIS, 2021).

McCumbers sikkerhetskube er et rammeverk som John McCumber utarbeidet 1991. Rammeverket bidrar til å se på sikkerhetsutfordringer i lys av tre dimensjoner, som skal gjøre det lettere å etablere og evaluere sikkerhetsarbeid (National Institute of Standards and Technology, National Computer Science Center, 1991). De følgende dimensjonene er:



Figur 2: Bilde av sikkerhetskuben McCumber utarbeidet (Klefstad, Hjelle, & Haugset, 2018)

- *Ønskede mål*
    - *Konfidensialitet*
    - *Integritet*
    - *Tilgjengelighet*
- *Informasjonsstilstander*
    - *Data som er lagret*
    - *Data som blir overført*
    - *Data som kjøres eller prosesseres*
- *Ivaretakelsesmetoder*
    - *Retningslinjer (policies): regler om korrekt oppførsel*

- *Menneskefaktorer: ryggmargrefleksen, vil en ansatt instinktivt ha rett oppførsel når individet blir utsatt for en ny situasjon, fordi den ansatte kjenner til trusler, sin rolle og har opplæring i å være skeptisk.*
- *Teknologi: løse en sikkerhetsutfordring ved å hente inn en hardware- eller software løsning. Dette innebærer antivirus, brannmurer, back-up disker etc.*

Denne kuben bidrar til å se på sikkerhetsproblemer fra flere aspekter. Man har de overordnede målene man ønsker å oppfylle, tilstanden dataene befinner seg i og hvilke tiltak man må vurdere for å lykkes med dette. Det å øke sikkerhetsperspektivet fra det todimensjonale "konfidensialitet, integritet og tilgjengelighet" til et tredimensjonalt perspektiv, kan bidra til å ikke bare kartlegge trusler, men å redusere risikoen de utgjør gjennom bruk av ivaretakelsesmetodene. Bruk av denne kuben som et evalueringsverktøy vil gjøre det lettere å behandle trusler (National Institute of Standards and Technology, National Computer Science Center, 1991).

Risikoanalyse

Risiko er et sentralt begrep ved innføringen av et ISMS. Difi, nå en del av digitaliseringsdirektoratet, beskriver risiko som: "*Risiko handler om potensielle avvik fra det forventede eller potensielle avvik fra våre mål. Med det referansepunktet defineres risiko formelt som en kombinasjon av mulige konsekvenser (utfall eller resultat) og tilhørende usikkerhet* (Digitaliseringsdirektoratet, 2020)". Difi kvantifiserer denne usikkerheten gjennom sannsynlighet, som betyr at risiko utgjør en kombinasjon av sannsynligheten for at en uønsket hendelse inntreffer, og konsekvensene av det. Derfor er et av de viktigste stegene når man jobber med informasjonssikkerhet å gjennomføre risikoanalyser- og vurderinger, for å unngå uønskede hendelser.

Datatilsynet definerer risikovurdering som: «*En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. Som en del av internkontrollen skal virksomheten ha en oversikt over hvilke behandlinger av personopplysninger som inngår i disse. Denne oversikten skal brukes som underlag ved risikovurderinger*».
Videre tilfører Datatilsynet: «*Virksomheten skal gjennomføre en risikovurdering før personopplysninger behandles og før man tar i bruk et informasjonssystem. Virksomheten skal også gjennomføre risikovurdering ved endringer i forhold som kan påvirke*

informasjonssikkerheten, for eksempel endringer i behandlinger, endringer av informasjonssystem eller endringer i trusselbildet (Datatilsynet, 2019)». Derfor er ikke risikoanalyser bare en anbefaling for å opprettholde informasjonssikkerheten, men nærmere et krav. Spesielt for å beskytte sensitiv informasjon som personopplysninger og annen informasjon virksomheten ikke ønsker skal falle i feil hender.

Det finnes flere måter å gjennomføre en risikoanalyse på, og dette er noen svært relevante trinn for å gjøre det.

- Avdekke mulige uønskede hendelser som vi må beskytte oss mot. Første steget i å kartlegge trusselbildet.
- Bedømme sannsynligheten for at hendelsen skal inntreffe
- Vurdere hvilke konsekvenser det vil skape dersom hendelsen inntreffer
- Vurdere tiltak som kan hindre at hendelsen inntreffer eller som kan minske konsekvensene dersom det skjer (Digitaliseringsdirektoratet, 2020).

Ved å gjennomføre disse trinnene, vil man ha kartlagt trusselbildet bedriften står overfor, og fått vurdert tiltak for å forhindre eller redusere risikoen av disse uønskede hendelsene. Når man skal vurdere tiltak, så er det fire aktuelle strategier for å håndtere en risiko.

- Unngå risiko: Innebærer å eliminere eller redusere risikoen ved å redusere sårbarheten eller utnyttelsen av den. Eventuelt ved å fjerne all risiko tilknyttet en informasjonsressurs. For eksempel kan man la være å gjennomføre et prosjekt hvis det er risikoer tilknyttet prosjektet, eller la en annen ansatt gjennomføre viktig arbeid dersom kompetanseforskjellen utgjør en risiko. En annen måte å terminere risiko på er ved å utvikle nye løsninger for å erstatte tidligere løsninger. For eksempel ved å gå over til skybasert lagring, så termineres den fysiske risikoen forbundet med lokal lagring.
- Dele risiko: Handler om å overføre risikoen til andre ressurser, prosesser eller organisasjoner. Dette kan være ting som taushetserklæringer, som forsikrer seg om at motparten må kompensere dersom den brytes, og andre lignende kontrakter eller forsikringer.
- Redusere risiko: Redusere konsekvensene av et angrep. Dette kan være alt fra beredskapsplaner, kontinuitetsplaner og andre strategier som forbereder virksomheter mot et angrep, til tiltak som 2-stegs autorisering, som kan forhindre

eller redusere konsekvensene av at passord og brukernavn utgis til uautoriserte parter.

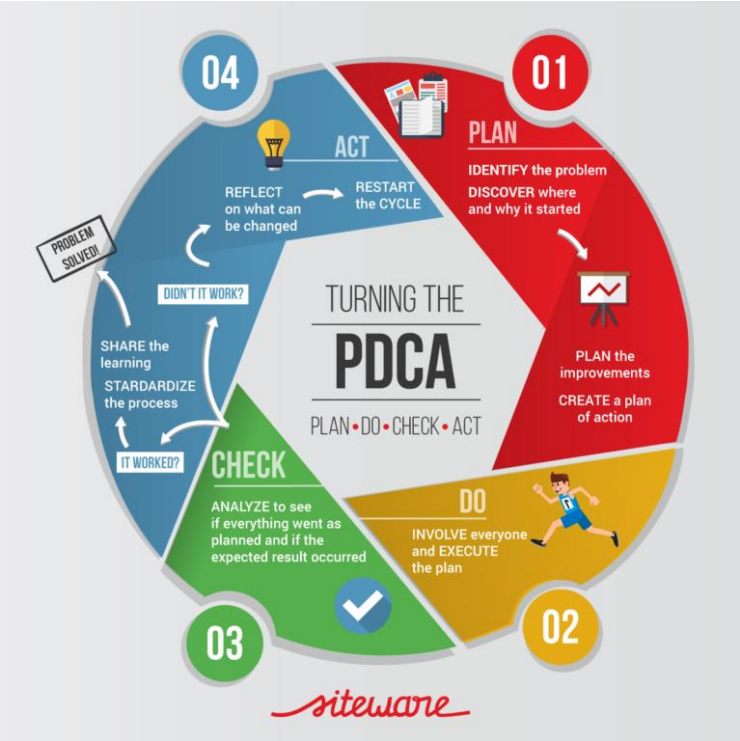
- Akseptere risiko: At man aksepterer at det kommer til å være en risiko forbundet med det man gjør, men å iverksette tiltak for å redusere eller kontrollere risikoen til et akseptabelt nivå (Digitaliseringsdirektoratet, 2020).

Figur 3: Figur for stegene i en risikoanalyse (One Comodo, 2021)

Som figuren over viser, så innebærer risikostyring de tidligere forklarte stegene; identifisering, analyser og tiltak. Deretter er det to steg til; overvåkning og kontroll. I overvåkningsfasen holder man øye med risikoene mens man iverksetter planlagte tiltak. Til slutt kommer kontrollfasen der man måler effektiviteten til tiltakene og prøver å kontrollere risikoene. Dette kan medføre at man identifiserer nye risikoer, eller oppdager et behov for å gjennomføre nye risikoanalyser, som starter en ny risikostyringsprosess.

Demings prinsipper for kontinuerlig forbedring

Demings sirkel, også kjent som PDCA (plan – do – check – act) er en iterativ metode som gjennomgående brukes i bedriftssammenhenger for kontinuerlig forbedring av prosesser og produkter. Demings sirkel har blitt endret og videreutviklet gjennom årene med flere ulike versjoner, men alle deler det samme målet om kontinuerlig forbedring, og de fire fasene i sirkelen; planlegge, utføre, følge opp og iverksette skaper forutsetninger for dette (Moen & Norman, 2009).



Figur 4: PDCA sirkelen (Siteware, 2019)

I sammenheng med oppgaven, vil første fase innebære planlegging av sikkerhetstiltak. Her gjennomføres tiltak som forankring av arbeidet, fastsette mål for tiltaket, risikoanalyser og valg av tiltak for å håndtere risiko. Neste fase, som er å utføre tiltaket, innebærer å gjennomføre alle de planlagte tiltakene i forrige fase. Blant annet å forankre sikkerhetsarbeidet gjennom å utarbeide policyer og retningslinjer, gjennomføre motivasjon-, opplæring- og kulturprogram. Samt å dokumentere arbeidet som gjennomføres for å forberede seg til neste fase. I oppfølgingsfasen analyseres og evalueres iverksettelsen av sikkerhetstiltaket for å vurdere hvordan det gikk, og for å sammenlikne det med planen for arbeidet. Etter evalueringen bærer man på resultatene videre til fjerde fase. Siste fase, som er å iverksette, så gjennomfører man korrigerende tiltak basert på evalueringer fra forrige fase, dersom det er nødvendig. Dette er fasen der fokuset er på å rette opp i feil og lære av dem, slik at man kan forbedre prosessen til neste gang. Etter fjerde fase er over, går man tilbake over til første fase og planlegger det neste prosjektet eller sikkerhetstiltaket (Moen & Norman, 2009).

ISO 27001

ISO 27001 er det sentrale rammeverket i ISO 27000-serien. ISO 27001 er en internasjonal standard som inneholder generelle krav på områdene etablering, implementering, vedlikehold og kontinuerlig forbedring av ledelsessystem for informasjonssikkerhet. Videre inneholder den krav til vurdering og håndtering av sikkerhetsrisikoer i organisasjonen. Dermed er ISO 27001 en standard som er ment å være anvendelig for alle typer organisasjoner, uavhengig av størrelse og omfang.

Bakgrunn

Standarden NS-EN ISO/IEC 27001:2017, (ISO 27001), er den offisielle versjonen av ISO-standarden i Norge, og det er dermed denne som organisasjonen må forholde seg til for å kunne bli ISO-sertifisert. Når en bedrift er ISO-sertifisert vil det kort forklart si at man følger de kravene som er fastsatt i ISO 27000-standarden på en tilfredsstillende måte og har bestått evaluering som bekrefter dette. Mer informasjon om nøyaktig hvordan en slik prosess fungerer kommer under diskusjonsdelen i denne oppgaven (Standard Norge, 2017).

Denne standarden gir organisasjonen spesifiserte krav til hvordan et ledelsessystem for informasjonssikkerhet kan opprettes i en organisasjon og tar for seg prosessene etablering, implementering, vedlikehold og videre kontinuerlig forbedring.

Definisjon

ISO 27001 definerer standarden som: «*Denne internasjonale standarden spesifiserer kravene til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet innenfor konteksten til en organisasjon. Denne internasjonale standarden inneholder også krav til vurdering og håndtering av informasjonssikkerhetsrisikoer, tilpasset behovene i organisasjonen.*» (Standard Norge, 2017).

Tilnærming til etablering

PDCA-trinnene (også kalt Demings sirkel for kontinuerlig forbedring) som ble nevnt tidligere er sentrale i forbindelse med etableringen av ISMS for organisasjonen. Det bør likevel understrekes at disse fra 2013-versjonen av ISO 27001 ikke lenger er obligatoriske for at organisasjonen skal kunne bli ISO-sertifisert. Grunnen til at vi likevel nevner disse som en viktig hjelp i tilnærmingen til informasjonssikkerhet er at etablering, vedlikehold og forbedring av ISMS i organisasjonen er et kontinuerlig arbeid, og denne standarden ble utarbeidet nettopp for å stille krav til disse områdene (Disterer, 2013). Ved å ta i bruk en slik modell vil derfor kunne være til stor hjelp for å sørge for at bedriften opererer i henhold til de nødvendige kravene.

Videre skal det utvikles nødvendige opplæringsprogram for å kunne implementere ISMS i henhold til ISO-standarden. På denne måten får man gjennomslag for, og opparbeidet den nødvendige kunnskap, samtidig som man skaper en forståelse av betydningen disse har i organisasjonen. Kravene skal være fastsatt og grundig dokumentert, og disse kravene er beskrevet i standarden gjennom bestemmelser av viktig innhold, nødvendige dokumenter, samt spesifikasjoner og overvåkningsstrukturer (Disterer, 2013).

Hovedkrav

I ISO 27001 standarden står det spesifikt at "Det er ikke akseptabelt å ekskludere noen av kravene i punkt 4 til 10 dersom en organisasjon vil hevde at den er i samsvar med denne standarden" (Standard Norge, 2017, s. 5). For å kunne bli ISO-sertifisert i henhold til standardene vil man derfor måtte ha regler og retningslinjer på plass for alle disse punktene dersom informasjonssikkerhetsarbeidet skal være tilstrekkelig. Disse punktene omfatter:

- Punkt 4: Omhandler ledelsessystem for informasjonssikkerhet, og her kommer det frem at organisasjonen skal etablere, implementere, vedlikeholde og foreta kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Dette ledelsessystemet må stå i samsvar med ISO 27001-standarden (Standard Norge, 2017, s. 5).
- Punkt 5: Øverste ledelse i organisasjonen er ansvarlig for ledelsessystemet. Dette skal gjøres gjennom tildeling av ressurser, roller, ansvar, sørge for bidrag gjennom prosessen og fremme kontinuerlig forbedring. I tillegg skal det under dette punktet

fremlegges policy, retningslinjer og myndighet i organisasjonen (Standard Norge, 2017, s. 6).

- Punkt 6: Omhandler planlegging av ledelsessystemet. Under dette punktet skal man foreta risikovurdering samt opprette en prosess for hvordan organisasjonen skal håndtere risikoene innenfor informasjonssikkerhet. Videre skal det utarbeides tiltak for håndtering av disse risikoene ut ifra resultatene som kommer frem i risikovurderingene slik at disse kan implementeres i systemet. De videre virkningene av disse tiltakene skal også evalueres (Standard Norge, 2017, s. 7).
- Punkt 7: Dette punktet handler om støtte i systemet. Her kommer det frem at man behøver nødvendig tilgang på ressurser, kompetanse, bevisstgjøring og kommunikasjon. Videre kreves det dokumentert informasjon i form av generell info i henhold til standarden, systemer for oppretting og oppdatering, og for å være i henhold til ISO-standarden må denne dokumentasjonen styres (Standard Norge, 2017, s. 9).
- Punkt 8: Drift av systemet. Organisasjonen skal i dette punktet planlegge, iverksette og styre de prosesser som er nødvendige for å oppfylle informasjonssikkerhetskravene. Med hensyn til kravene som allerede skal være fastsatt i punkt 6.1.2 a), skal det også utføres risikovurderinger av informasjonssikkerheten både med planlagte intervaller og ved betydelige endringer. Man skal også implementere plan for håndtering av de informasjonssikkerhetsrisikoene som kommer frem, og dokumentert informasjon rundt resultatene av denne håndteringen skal oppbevares av organisasjonen (Standard Norge, 2017, s. 10).
- Punkt 9: Prestasjonsevaluering. Her skal informasjonssikkerhetsprestasjonen og virkningen av ledelsessystemet for informasjonssikkerhet måles. Mer spesifikt vil man her beslutte hva som skal overvåkes og måles, hvem som skal utføre og når det skal utføres, og det skal bestemmes metoder for overvåking, måling, analyse og evaluering for å sikre gyldige resultater. Videre skal det utføres interne revisjoner for å gi organisasjonen informasjon om ledelsessystemet for informasjonssikkerhet, samt sørge for at resultatene er i samsvar med organisasjonens egne krav for systemet, samt at det er i henhold til ISO 27001-standarden. Den øverste ledelsen i organisasjonen skal også gjennomgå ledelsessystemet for informasjonssikkerhet for å fortløpende kunne gjøre vurderinger av systemet og avgjøre om det er virkningsfullt, velegnet og tilstrekkelig (Standard Norge, 2017, s. 11).

- Punkt 10: Siste hovedkrav omhandler forbedring av ledelsessystemet for informasjonssikkerhet. Her kommer det frem at under avvik skal organisasjonen kunne reagere, og dersom det er nødvendig komme med korrigerende tiltak eller håndtere eventuelle konsekvenser. Videre skal behovet for tiltak med hensikt å eliminere årsakene til avvik undersøkes og dersom nødvendig skal det dermed implementere disse tiltakene, gjennomgå virkingen av dem og om nødvendig foreta endringer i ledelsessystemet for informasjonssikkerhet. Organisasjonen skal også foreta kontinuerlig forbedring av ledelsessystemet for informasjonssikkerhet, for på denne måten kunne utbedre systemets egnethet, tjenlighet og virkning (Standard Norge, 2017, s. 12).

ISO 27002

Bakgrunn og definisjon

Versjonen av ISO/IEC som ser mest bruk er 27001-standarden. Som nevnt tidligere er ISO 27001 det sentrale rammeverket i ISO 27000-serien, som er en serie dokumenter som gjelder ulike deler av informasjonssikkerhetsadministrasjon og inneholder kravene for implementering av et ISMS (Irwin, 2019).

ISO 27002 er en supplerende standard som fokuserer på informasjonssikkerhetskontrollene som organisasjoner kan velge å implementere. Disse kontrollene er oppført i vedlegg A i ISO/IEC 27001, som du ofte ser informasjonssikkerhetseksperter refererer til når de diskuterer informasjonssikkerhetskontroller. Imidlertid, mens vedlegg A bare skisserer hver kontroll i en eller to setninger, dedikerer ISO 27002 i gjennomsnitt en side per kontroll. Dette er fordi standarden forklarer hvordan hver kontroll fungerer, hva dens mål er, og hvordan du kan implementere den (Irwin, 2019).

«Den engelskspråklige versjonen av europeisk standard EN ISO/IEC 27002:2017 ble fastsatt som Norsk Standard NS-EN ISO/IEC 27002:2017 i mai 2017. Den norske versjonen ble utgitt i mai 2017. Rettelsesblad Cor 1:2014 og Cor 2:2015 ble innarbeidet i den norske versjonen i mai 2017. Denne standarden erstatter NS-ISO/IEC 27002:2013» (Standard Norge, 2017).

Forskjeller mellom ISO 27001 og ISO 27002

Som nevnt tidligere er ISO 27002 en utdypning av ISO 27001 dedikert til informasjonssikkerhetskontroller beskrevet i Vedlegg A. Årsaken til denne oppbygningen er for å unngå at ISO 27001 standarden blir unødvendig lang og komplisert. ISO 27001 er i stedet en oversikt over hvert aspekt av et ISMS, mens mer utfyllende informasjon detaljeres i egne supplerende standarder. I tillegg til ISO 27002 som fokuserer på informasjonssikkerhetskontroller finner vi blant annet ISO 27005 og ISO 27014 som henholdsvis fokuserer på Informasjonssikkerhetsrisikostyring og informasjonssikkerhetsstyring. Den betydelige forskjellen i detalj er en merkbar forskjell mellom ISO 27001 og de resterende standardene (Irwin, 2019).

Bedrifter kan bli sertifisert i ISO 27001, men ikke i ISO 27002. Grunnen til dette er at ISO 27001 er en ledelsesstandard som gir en fullstendig liste over samsvarskrav, mens de resterende tilleggsstandardene som blant annet ISO 27002 adresserer er et spesifikt aspekt av et ISMS (Irwin, 2019).

ISO 27000 serien er en massiv samling av informasjon og bedrifter er kompliserte samlinger av styrker, svakheter, kunnskap og trusler. Dette betyr at det er tilfeller hvor ikke all informasjonen som ISO 27000 serien tilbyr er anvendelig for enhver bedrift når de skal implementere et ISMS. Det er bedriftens ansvar å gjennomføre alle nødvendige risikovurderinger for å identifisere hvilke standarder i ISO 27000 serien som kommer til å effektivt beskytte bedrifter fra trusler. ISO 27001 er på generell basis mer anvendelig i den forstand at den spesifiserer akkurat dette, hvorimot de resterende standardene er eksklusivt utdypninger av informasjon funnet i ISO 27001 (Kosutic, u.d.).

Innhold i NS-EN ISO/IEC 27002:2017

ISO 27002 består av 18 punkter hvorav 14 går i høy detalj om diverse temaer innen informasjonssikkerhet. I ulikhet med ISO 27001 er disse ikke krav til bedrifter, men heller forslag til implementeringer. En bedrift har eget ansvar for å fastslå hvilke områder innen bedriften som har fordel av implementering av denne standarden.

Nummereringen av punktene på listen under gjenspeiler rekkefølgen på punktene i innholdsfortegnelsen i ISO 27002 standarden. De 14 punktene som bedrifter kan ta i bruk er:

5. Informasjonssikkerhetspolicyer

5.1. «*Ledelsens føringer for informasjonssikkerhet*, har mål om å formidle ledelsens føringer og støtte til informasjonssikkerhet i samsvar med forretningsmessige krav og relevante lover og forskrifter» (Standard Norge, 2017, s. 10).

6. Organisering av Informasjonssikkerhet

6.1. «*Intern organisering*, ønsker å etablere et styringsrammeverk for å initiere og kontrollere implementering og forvaltning av informasjonssikkerhet i organisasjonen» (Standard Norge, 2017, s. 11).

6.2. «*Mobilt utstyr og fjernarbeid*, jobber mot å ivareta sikkerheten ved fjernarbeid og bruk av mobilt utstyr» (Standard Norge, 2017, s. 13).

7. Personellsikkerhet

7.1. «*Før ansettelse*, bør det være et mål å sikre at ansatte og kontraktører forstår sitt ansvar og er egnet for de rollene som de vurderes for» (Standard Norge, 2017, s. 15).

7.2. «*Under ansettelsesforholdet*, bør det være et mål å sikre at ansatte og kontraktører er klar over og oppfyller sitt ansvar for informasjonssikkerhet» (Standard Norge, 2017, s. 17).

7.3. «*Opphør og endring av ansettelsesforhold*, har i mål å beskytte organisasjonens interesser som en del av prosessen med endring eller opphør av ansettelsesforhold» (Standard Norge, 2017, s. 19).

8. Forvaltning av Aktiva

8.1. «*Ansvar for aktiva*, er et mål om å identifisere organisasjonens aktiva og definere ansvar for tilstrekkelig beskyttelse» (Standard Norge, 2017, s. 19).

8.2. «*Klassifisering av informasjon*, er et mål om å sikre at informasjonen har et tilstrekkelig beskyttelsesnivå i samsvar med dens betydning for organisasjonen» (Standard Norge, 2017, s. 21).

8.3. «*Håndtering av medier*, har i mål å forhindre uautorisert utlevering, modifisering, fjerning eller ødeleggelse av informasjon lagret på medier» (Standard Norge, 2017, s. 23).

9. Aksesskontroll

9.1. «*Virksomhetskrav til aksesskontroll*, har i mål å begrense aksess til informasjon og systemer for informasjonsbehandling» (Standard Norge, 2017, s. 24).

9.2. «*Styring av brukeraksess*, jobber mot å sikre autoriserte brukere aksess og å forhindre uautorisert aksess til systemer og tjenester» (Standard Norge, 2017, s. 26).

9.3. «*Brukeransvar*, er der for å ansvarliggjøre brukerne for å sikre sin autentiseringsinformasjon» (Standard Norge, 2017, s. 29).

9.4. «*Kontroll av aksess til systemer og applikasjoner*, forhindrer uautorisert aksess til systemer og applikasjoner» (Standard Norge, 2017, s. 30).

10. Kryptografi

10.1. «*Kryptografiske kontroller*, hjelper å sikre korrekt og effektiv bruk av kryptografi for å beskytte konfidensialiteten, ektheten og/eller integriteten til informasjon» (Standard Norge, 2017, s. 32).

11. Fysisk og Miljømessig Sikkerhet

11.1. «*Sikre områder*, bidrar til å forhindre uautorisert adgang til, skade på og forstyrrelser i organisasjonens informasjon og systemer for informasjonsbehandling» (Standard Norge, 2017, s. 34).

11.2. «*Utstyr*, er et mål om å forhindre tap, skade, tyveri eller kompromittering av aktiva samt avbrudd i organisasjonens drift» (Standard Norge, 2017, s. 37).

12. Driftssikkerhet

12.1. «*Driftsprosedyrer og ansvar*, hjelper å sikre korrekt og sikker drift av systemer for informasjonsbehandling» (Standard Norge, 2017, s. 41).

12.2. «*Beskyttelse mot ødeleggende programvare*, forsikrer at informasjon og systemer for informasjonsbehandling er beskyttet mot ødeleggende programvare» (Standard Norge, 2017, s. 43).

12.3. «*Sikkerhetskopiering*, beskytter mot tap av data» (Standard Norge, 2017, s. 45).

12.4. «*Logging og overvåking*, registrerer hendelser og genererer bevis» (Standard Norge, 2017, s. 45).

12.5. «*Kontroll av operativ programvare*, sikrer integriteten til operative systemer» (Standard Norge, 2017, s. 47).

12.6. «*Styring av tekniske sårbarheter*, forhindrer utnyttelsen av tekniske sårbarheter» (Standard Norge, 2017, s. 48).

12.7. «*Hensyn ved revisjon av informasjonssystemer*, minimerer virkningen av revisjonsaktiviteter i operative systemer» (Standard Norge, 2017, s. 50).

13. Kommunikasjonssikkerhet

13.1. «*Styring av nettverkssikkerhet,* forsikrer beskyttelse av informasjon i nettverk og understøttende systemer for informasjonsbehandling» (Standard Norge, 2017, s. 50).

13.2. «*Informasjonsoverføring*, opprettholder sikkerheten til informasjon som overføres innenfor en organisasjon og med eksterne enheter» (Standard Norge, 2017, s. 52).

14. Anskaffelse, Utvikling og Vedlikehold av Systemer

14.1. «*Sikkerhetskrav til informasjonssystemer*, bidrar til å påse at informasjonssikkerhet er en integrert del av informasjonssystemer gjennom hele livsløpet. Dette omfatter også kravene til informasjonssystemer som tilbyr tjenester over offentlige nettverk» (Standard Norge, 2017, s. 54).

14.2. «*Sikkerhet i utviklings- og støtteprosesser*, har i mål å påse at informasjonssikkerhet er utformet og iverksatt i hele utviklingsprosessen til informasjonssystemer» (Standard Norge, 2017, s. 57).

14.3. «*Testdata*, har i mål å sikre beskyttelse av data som brukes for testing» (Standard Norge, 2017, s. 61).

15. Leverandørforhold

15.1. «*Informasjonssikkerhet i leverandørforhold*, bidrar med å sikre beskyttelse av virksomhetsaktiva som er tilgjengelige for leverandører» (Standard Norge, 2017, s. 62).

15.2. «*Styring av leverandørens tjenesteleveranser*, har i mål å opprettholde et avtalt nivå for informasjonssikkerhet og tjenesteleveranser i tråd med leverandøravtaler» (Standard Norge, 2017, s. 64).

16. Styring av Informasjonssikkerhetsbrudd

16.1. «*Styring av informasjonssikkerhetsbrudd og forbedringer*, sikrer en enhetlig og virkningsfull tilnærming til styring av informasjonssikkerhetsbrudd, herunder kommunikasjon av sikkerhetshendelser og svakheter» (Standard Norge, 2017, s. 66).

17. Informasjonssikkerhetsaspekter ved styring av Virksomhetskontinuitet

17.1. «*Informasjonssikkerhetskontinuitet*, bør være forankret i organisasjonens ledelsessystemer for virksomhetskontinuitet» (Standard Norge, 2017, s. 69).

17.2. «*Redundans*, vil sikre tilgjengeligheten til systemer som skal behandle informasjon» (Standard Norge, 2017, s. 71).

18. Samsvar

18.1. *«Samsvar med juridiske og kontraktmessige krav*, har i mål å unngå brudd på juridiske, lovfestede, regulatoriske eller kontraktsmessige forpliktelser knyttet til informasjonssikkerhet og på ethvert sikkerhetskrav» (Standard Norge, 2017, s. 72).

18.2. *«Gjennomganger av informasjonssikkerhet*, forsikrer at informasjonssikkerhet er iverksatt og forvaltes i samsvar med organisasjonens policyer og prosedyrer» (Standard Norge, 2017, s. 74).

Alle punktene nevnt over er valgfrie for bedrifter og ikke nødvendig for ISO sertifisering. De er laget med det formål å være til hjelp for alle bedrifter som føler det nødvendig. Disse punktene er høyst relevante for tilnærmet alle bedrifter i dagens IT baserte miljø og samfunn og bør vurderes av alle virksomheter (Standard Norge, 2017).

Hvert punkt nevnt over har også et dedikert mål oppført. Videre består hvert punkt av flere underpunkter som beskriver forskjellige aspekter av hovedpunktene, sikringstiltak, implementeringsveiledning og annen informasjon med intensjonen om å oppnå målet beskrevet i starten av hvert hovedpunkt (Standard Norge, 2017).

Casebeskrivelse

Denne casen ble gitt i oppdrag av E.A. Smith på bakgrunn av et ønske om å forbedre informasjonssikkerhetsarbeidet sitt, og finne ut hvordan dagens systemer måler seg opp mot ISO 27001-standarden og standardiserte ledelsessystem for informasjonssikkerhet. E.A. Smith ønsker konkrete anbefalinger for forbedringer og/eller komplett hensiktsmessig innføring av ISMS-standard for organisasjonen. Dette er et tema som blir stadig viktigere, ettersom arbeidslivet og arbeidsmiljø stadig blir mer digitaliserte og derfor møter økte utfordringer på dette området.

Samtidig var dette en oppgave som engasjerte gruppemedlemmene. Arbeid med informasjonssikkerhet i en bedrift er svært relevant for studiet Digital Forretningsutvikling og funnene vi kommer fram til er noe både vi og E.A. Smith kan benytte oss av. Utfordringer innen informasjonssikkerhet er viktig å kunne overkomme, og arbeidet med dette casestudiet kan forhåpentligvis skape bedre forutsetninger for begge parter til å kunne håndtere dette fremover.

Metode

Fremgangsmåten en bruker for å oppnå resultater kalles metode. I en mer akademisk setting har begrepet metode mer til seg enn bare det. En akademisk fremgangsmåte eller forskningsmetode hjelper oss samle inn relevant data for å svare på problemstillingen vår. Innsamling av ikke relevant data kan være problematisk, så det er også viktig å velge riktig metode fra starten av for å unngå å kaste bort tid på å behandle irrelevant informasjon.

Utvikling av problemstillingen

Som nevnt i introduksjonen var oppgaven som ble gitt oss fra E.A. Smith å se på hvordan formalisert ISMS kan støtte arbeidet og bidra til et mer helhetlig og målrettet system innenfor informasjonssikkerhet. I oppgaven ble det også lagt vekt på et ønske om å undersøke hvordan dagens informasjonssikkerhetsarbeid i organisasjonen måler seg opp mot ISMS og ISO 27001/02-standarder. For å kunne svare best mulig på begge disse utfordringene kom vi dermed fram til forskningsspørsmålet "*Hvordan kan innføring av et ISMS og ISO 27001-standarden styrke informasjonssikkerhetsarbeidet i organisasjonen E.A. Smith?"* som utgangspunkt for problemstillingen.

Kvalitativ og kvantitativ forskningsmetode

Når man gjennomfører en vitenskapelig undersøkelse, skiller man mellom to forskningsmetoder for datainnsamling. Kvalitativ og kvantitativ forskningsmetode. For å besvare problemstillingen til en slik undesøkelse, bruker man enten én av forskningsmetodene, eller en kombinasjon av dem begge.

Den kvalitative forskningsmetoden brukes vanligvis om data som foreligger i form av tekst, og anskaffes som oftest ved bruk av metoder som deltakende observasjon, intervjuer, fokusgrupper eller kvalitativ innholdsanalyse. Denne metoden fokuserer på å oppnå en dybdekunnskap eller forståelse om et valgt tema, og brukes til å formulere hypoteser og teorier for å besvare problemstillinger. Denne metoden er godt egnet til å skaffe god innsikt i et tema, siden intervjuobjektene ofte får utdypet sine meninger, og man får gransket nyanser av tema man ikke enkelt kan gjøre ellers (Grønmo, Store norske leksikon, 2020).

Derimot, så omfatter kvantitativ forskningsmetode gjerne mange flere enheter enn ved en kvalitativ forskningsmetode. Noe som gjør det svært utfordrende å kartlegge all dataen i form av tekst. Derfor benytter kvantitativ metode seg heller av datainnsamling i form av tall eller andre mengdetermologier, for å lettere kunne analysere og kontekstualisere den potensielt enorme mengden dataen som innhentes fra enhetene (Grønmo, Store norske leksikon, 2020).

Valg av metode

På grunn av oppgaven samt problemstillingens art er det mest naturlig å behandle oppgaven som en typisk casestudie. Casestudier har ingen forhåndsbestemt forskningsmetode som er ansett som korrekt (Walsham, 1995). Etter våre vurderinger basert på problemstillingen vi har formulert er det mest gunstig for oss å samle informasjon i høy kvalitet for å best besvare problemstillingen vår. En kvalitativ forskningsmetode er altså mer effektiv for å besvare forskningsspørsmålet fremfor en kvantitativ metode.

To kvalitative metoder ble utnyttet for å samle informasjon. Før alt annet ble det utført en grundig litteraturgjennomgang av relevant fagstoff av alle gruppemedlemmer med den hensikt å være utdannet og forberedt for den resterende oppgaveskrivingen. Senere utførte vi intervjuer av fire ansatte hos E.A. Smith, siden intervjuer er en kvalitativ forskningsmetode som henter inn relevant og detaljert informasjon. Intervjuer har også den ekstra fordelen at spørsmål kan justeres samt at man kan legge til flere hvis det oppstår noe som er verdt å merke seg.

Hva slags type undersøkelser / Utvalg

Vi har gjennomført intervjuer med fire personer hvorav tre av dem har like roller i E.A. Smith. De tre første, som vi kaller informant 1, 2 og 3 var IT-konsulenter på drift og supportavdelingen, og informant 4 var leder for prosess-støtte. Disse intervjuobjektene hadde relevante roller i bedriften med varierende erfaring, og satt på god kunnskap og kompetanse. Å intervjue tre ansatte fra IT-avdelingen ga oss også flere synsvinkler på de samme problemene rundt IT, som gjorde det lettere for oss å fastslå hvilke problemer som var åpenbare og hvilke som var vanskeligere å rette. Dette hjalp oss bygge bedre innsikt i bedriftens nåværende situasjon.

Vi har også hatt fortløpende kontakt med IT-direktør, Avd. Leder Teknisk IT/senior IT-Konsulent og en IT-konsulent som var vår hovedkontaktperson. Det var også planlagt å basere oss på intervju fra alle disse personene, men det ble bestemt basert på mengden kvalitativ data at de fire intervjuobjektene vi hadde gav god nok innsikt til å besvare problemstillingen.

Påvirkninger av Covid-19

På grunn av Covid-19 situasjonen ble stort sett all møte- og intervjuvirksomhet gjort digitalt gjennom møtetjenestene til Microsoft Teams og Zoom. Det ble heller ikke mulighet for fysiske møter gjennom f.eks. omvisning hos bedriften eller lignende. Dermed var det naturlig at oppgaven måtte basere seg på den informasjonen som ble lagt fram gjennom digitale møter. Vår oppfatning er at dette likevel har fungert bra ettersom Microsoft Teams har gode forutsetninger for samskriving og samarbeid for øvrig. I tillegg var de ansatte i E.A. Smith og veileder veldig behjelpelige både med å stille opp til digitale intervjuer og med å svare på spørsmål som oppsto underveis.

Datainnsamling

Tillatelse for gjennomføring

Informasjons- og datainnsamling ble som nevnt gjort gjennom intervjuer med ansatte som jobbet med områder tett knyttet mot vår problemstilling og dermed satt på viktig innsikt for oppgaven. Alle intervjuobjektene sa seg villig til å delta på frivillig grunnlag og tidspunktene for intervjuene ble avtalt gjennom e-post og Microsoft Teams på forhånd. I etterkant ble det også sendt ut samtykkeskjemaer til intervjuobjektene for å sikre at alle var klar over hvilke rettigheter og plikter de ulike aktørene hadde.

Etiske vurderinger

Ettersom oppgaven omhandler informasjonssikkerhet og dermed potensielt sensitiv informasjon ble det besluttet at intervjuobjektene skulle anonymiseres og heller refereres til som informanter eller gjennom deres generelle stillingsbeskrivelse. Dette ble gjort for å sikre

nødvendig personvern (De nasjonale forskningsetiske komiteene, 2019, ss. 7, punkt 11) og sikre at oppgaven kunne offentliggjøres etter ferdigstillelse og innlevering.

Intervjugjennomføring

Intervjuene som ble gjennomført med de ansatte i E.A. Smith ble gjennomført som Individuelle semi-strukturerte intervjuer. På denne måten fikk vi svar på våre spørsmål sett fra de ulike ansattes eget perspektiv, samt at man unngikk eventuell påvirkning fra andre aktører. I tillegg gav dette oss de ansattes egne meninger og erfaringer som var til stor hjelp for å gi oss et godt helhetlig bilde av informasjonssikkerhetsarbeidet i organisasjonen.

Analyse og behandling av data

Data som ble samlet gjennom intervjuene ble tatt opp som opptak etter samtykke fra intervjuobjektene til bruk i oppgaveskrivingen. I tillegg ble det skrevet referat underveis i intervjuene for å gi oss informasjon både muntlig og skriftlig. I henhold til NTNUs regler (NSD, Norsk senter for forskningsdata, 2021) vil/ble opptakene og annen sensitiv informasjon slettes etter at bacheloroppgaven ble ferdigstilt.

Begrensinger og svakheter

Oppgaven baserer seg på informasjon gitt av et begrenset utvalg av ansatte hos E.A. Smith og gir dermed ikke nødvendigvis en fullstendig beskrivelse av situasjonen på alle områder eller synet til E.A. Smith som helhet. Dette er heller ikke noen fasit på hvordan informasjonssikkerhetsarbeidet gjennomføres i E.A. Smith.

På noen områder var det også vanskelig å få konkrete svar på ulike spørsmål angående situasjoner innenfor E.A. Smith, siden ikke alle intervjuobjektene hadde den samme oversikten eller oppfatningen. Dette gjorde at det også ble lagt fram ulike syn som kunne motsi hverandre eller at det ble trukket frem andre aspekter som hovedårsak til problemer eller utfordringer.

All informasjon og data er hentet inn digitalt og presise tall på ulike utfordringer, feil, mangler eller lignende i informasjonssikkerhetsarbeidet er ikke gjort tilgjengelig for oss.

Denne bacheloroppgaven bør derfor benyttes som et verktøy for anbefalinger og syn fra en tredjepart, og ikke som en fullstendig informasjonssikkerhetsguide som gir svar på alle situasjoner som kan oppstå.

Primærdata og Sekundærdata

Det som skiller primærdata fra sekundærdata, er hvorvidt informasjonen er hentet fra eksterne kilder eller om informasjonen er original og produsert av oss i hensikt å svare på problemstillingen vår. I henhold til vår oppgave vil all informasjon hentet direkte fra E.A. Smith av oss være ansett som primærdata. All resterende informasjon brukt til å danne konklusjoner i oppgaven faller da under definisjonen sekundærdata.

Den åpenbare fordelen med primærdata er at det kommer rett fra kilden og samles inn av oss for vår problemstilling. Det er dermed naturlig å bruke en kvalitativ forskningsmetode for å samle inn så mye fordelaktig informasjon som mulig. Våre intervjuer med E.A. Smith ble utført med dette i bakhodet.

Sekundærdata er data samlet inn av andre forfattere for å løse en annen problemstilling enn vår egen. Vi er dermed nødt til å filtrere denne informasjonen for å finne informasjonen som er relevant til spesifikt oss og vår problemstilling. I den situasjonen ser vi på diverse kriterier som for eksempel hvem som samlet inn informasjonen, aktualitet, datainnsamlingsmetode, relevans, målgruppe og formål. Ved å dømme sekundærdata etter blant annet disse kriteriene har vi tilnærmet garantert sekundærdata i høy kvalitet.

Resultater

I dette kapittelet presenteres de kvalitative resultatene fra datainnsamlingen vår. Denne datainnsamlingen baserer seg på fire semi-strukturerte intervjuer med informanter fra E.A. Smith. Resultatene nedenfor er en oppsummering av opplysningene vi mottok under intervjuene, etter at vi gjennomførte en analyse av hvert intervju. Av konfidensielle årsaker har vi valgt å utelukke navn på sikkerhetssystemer E.A. Smith benytter seg av.

Bevissthet rundt sikkerhetsarbeid

Gjennom intervjuene fikk vi litt forskjellige syn på bruken av policyer og retningslinjer, noe som er ganske naturlig ettersom personene hadde ulike roller og ansvarsområder innenfor E.A. Smith. Personene som jobbet innenfor IT-avdelingen som konsulenter hadde en oppfatning av at dette er et område med forbedringspotensialet og at dagens ordning på området er noe mangelfull, spesielt for personer med mindre teknisk kompetanse. Personen med en mer operativ lederrolle la mer vekt på at taushetsplikt og retningslinjer var noe som ble utgitt og gått gjennom ved for eksempel nyansettelser.
Informantene var alle enige om at det ikke er en nedskrevet sikkerhetspolicy i bedriften, men at mye av sikkerhetsarbeidet baseres på tillit og opparbeidede rutiner. Det er altså ikke noen formell evalueringsprosess for å måle i hvor stor grad de ansatte følger disse kravene. Flere av informantene meddelte et ønske om større fokus rundt strategi og formelle rutiner i bedriften, for å ivareta informasjonssikkerheten i bedriften.

Holdninger rundt informasjonssikkerhet

Informantene hadde ulike syn om hvorvidt holdningene rundt informasjonssikkerhet var tilfredsstillende eller ikke. Enkelte mente holdningene generelt var gode i bedriften, mens andre savnet bedre rutiner, opplæring og kompetanse. Alle var imidlertid relativt enige om at tekniske kompetansen på området ikke nødvendigvis er tilstrekkelig. Det har spesielt vært en del tilfeller med sikkerhetsglipp på e-post. Personer i bedriften har for eksempel trykket på viruslinker eller spam på e-post, eller har gitt bort sensitiv informasjon slik som personlige passord.

Nyansatte i bedriften får kurs i hvordan de skal utfylle de tekniske kravene for å kunne gjøre jobben sin, men det mangler opplæringsprogrammer med fokus på nettvett og informasjonssikkerhet. Derfor har ikke informasjonssikkerhet nødvendigvis vært i hovedfokus for ansatte når de jobber med prosjektarbeid og lignende. Med tanke på at mange ansatte har ulike bakgrunner så har de ikke samme forutsetninger for å opprettholde et tilfredsstillende nivå av informasjonssikkerhet. Dette kan spesielt være en risiko når de jobber og/eller sitter på sensitiv informasjon, ettersom det er fort gjort å glemme eller å ikke være oppmerksom på alle truslene som bedriften møter.

Selv om det ikke akkurat er formelle retningslinjer og sikkerhetspolicyer som de ansatte følger, så er rutiner og holdninger noe nyansatte opparbeider seg. Mye av dette skjer ved hjelp av mer erfarne ansatte i bedriften som lærer bort rutiner og holdninger til nye ansatte.

Nye ansatte

Nye ansatte får begrenset opplæring når de starter arbeid hos E.A. Smith. Det er ingen formell opplæringsprosess og heller ingen offisielle retningslinjer som alle forholder seg til. Dette betyr at opplæringsprosessen hos E.A. Smith er på det beste en verbal overføring av kunnskap fra en allerede ansatt til en ny ansatt. Mangelen på både en ordentlig opplæringsprosess og konkrete retningslinjer resulterer i en mangel på konsistens. Dette videreutvikler seg videre til en mangel på standarder som igjen videreutvikler seg til latskap og unnasluntring som kan bidra til risiko for bedriften på flere fronter.

Adgangskontroll

E.A. Smith benytter seg av hierarkisk fordeling av tillatelser, der ansatte er klassifisert i grupper som får tilgang dersom de oppfyller visse kriterier. Adgangskontroll i bedriften kan kategoriseres etter fysisk og digital adgang. Fysisk adgangskontroll omfatter lokalene og hvilke ansatte som har tilgang til ulike lokasjoner. For eksempel har daglig leder, regionssjefer og øvre del av hierarkiet tilgang til lokalene døgnet rundt, mens ansatte i faste stillinger stort sett har tilgang til lokalene rett før og etter åpningstid. Midlertidig ansatte, leverandører og eksterne konsulenter har ikke egen adgang, så de har kun adgang via andre eller når lokalet er åpent. Stort sett er det kun IT-avdelingen som har tilgang til serverrommene.

Når det gjelder digital adgangskontroll, så brukes det også en hierarkisk rollefordeling for å begrense systemtilgang utover det som er nødvendig. Man trenger visse roller for ulike systemtilganger, og dersom man trenger ytterligere systemtilgang, så skjer det dersom visse kriterier oppfylles. Mye av systemtilgangen kontrolleres og skreddersys for ulike roller gjennom selskapets informasjonssikkerhetsteknologi, som blir beskrevet nedenfor. De har også gjestenett som kunder og andre aktører kan benytte seg av, for å hindre uønsket tilgang til intranettet deres.

Når det gjelder evaluering av roller og systemtilganger, så meddelte informanter om at det kan være et behov for å gjennomføre evalueringer oftere for å kontrollere hvilke aktører som har tilgang til hva.

Reisevirksomhet i bedriften

Reisevirksomheten i E.A. Smith sine lokaler samt systemer har som de fleste andre bedrifter blitt hardt påvirket av Covid-19 situasjonen og har dermed blitt redusert kraftig. Generelt er det likevel slik at direktører og ledere har mye adgang under kontorets åpningstider. Utenom disse er det stort sett IT-avdelingen eller annet relevant personale som har tilgang til kritiske funksjoner slik som serverrom. Eksterne konsulenter og annet personale vil kun få tilgang dersom det er spesifikt behov for det, og som sikkerhet er det tatt i bruk et besøkslogg-system.

Motivasjon for arbeidet

Ønsket av å forsterke informasjonssikkerheten kommer av at det er identifisert mange problemer med IT sikkerhet og at flere ansatte opplever et behov for å forsterke sikkerheten i organisasjonen. Det nåværende sikkerhetsarbeidet har stort sett vært reaktivt og ikke proaktivt, som i seg selv utgjør en sikkerhetsrisiko. Det er mange registrerte tilfeller av at ansatte gir opp passord til upålitelige sider og personer. Mangelen på to stegs verifikasjon utgjør en stor risiko mener flere av intervjuobjektene.

Videre tar E.A. Smith i bruk et informasjonssikkerhetssystem som filtrerer ut mye potensielt farlig og gir IT avdelingen tilnærmet full kontroll, men som også kanskje har for mye restriksjoner. E.A. Smith er også utsatt for en økende angrepsfrekvens og er i stor fare for å

miste mye vesentlig data. De er for øyeblikket også i en overgangsfase i henhold til å flytte dataen sin til skybaserte tjenester, som kan plassere dem i en posisjon med stor risiko.

Utenfor IT avdelingen er spennet i IT kompetanse stort. Derfor er det behov for opplæring av ansatte for på best mulig måte kunne sikre at kompetansen er god nok, og dermed kunne forebygge uønskede hendelser og risikosituasjoner i firmaet. Dette behovet er der allerede i dag, men flere av informantene mener at dette vil bli enda viktigere fremover. Man ser at det oppstår problemer knyttet til informasjonssikkerhet omtrent daglig, og det er en økende angrepsfrekvens i selskapet. Det legges vekt på at det foreløpig ikke har oppstått virkelig kritiske episoder, de har blant annet aldri blitt tatt av utpressingsvirus eller andre brudd på bakgrunn av angrep eller daglig spam. Dette tror de er takket være en sta og kompetent IT-avdeling, samt gode systemer hos sikkerhetssystemleverandørene.

Eksisterende sikkerhetssystemer

E.A. Smith benytter seg av et informasjonssikkerhetssystem levert av spesialisert tredjepart. Ifølge intervjuobjektene som jobber på IT-avdelingen er dette et system som har mange restriksjoner og lar IT-avdelingen ha kontroll på hva ansatte laster ned og kjører på PC-en sin, og stopper uvedkommende filer fra å kjøre. Dette sikkerhetssystemet har også en avansert antivirus-løsning, dette er et system som styres av kunstig intelligens (AI). Denne skal altså over tid bli smart av seg selv og lære systemet for på den måten å kunne gi nødvendige varsler og oversikt over aktivitet. Denne sikkerhetsløsningen er fortsatt relativt ny og reagerer derfor på mer enn det som er nødvendig, men man regner med at dette forbedrer seg etter hvert som systemet utvikler seg.

Videre har Microsoft og tilhørende Office 365 egne filter for å stoppe svindelforsøk og phishing. Dette gir bedriften et ekstra sikkerhetstiltak spesielt knyttet mot e-post til ansatte. Som nevnt er dette et av områdene med størst risiko og flest tilfeller av sikkerhetsbrudd og uheldige hendelser.

Det ble også nevnt i intervjuene at det er enkelte PCer som ikke benytter seg av selskapets innkjøpte informasjonssikkerhetssystem, men baserer seg på andre sikkerhetstiltak. Disse mangler dermed den samme graden av sikkerhet, men skal fortsatt være sikre nok til at IT-avdelingen stoler på dem.

Et annet sikkerhetsaspekt for E.A. Smith er selvsagt de ansatte selv. Man stoler på at de ansattes kompetanse er god nok til å opprettholde informasjonssikkerhetsarbeidet i bedriften. Dette gjelder spesielt på områder som dårlige/usikre linker, svindelforsøk og phishing. Dette er et område hvor bedriften har opplevd utfordringer og uheldige episoder tidligere, men er likevel en risiko man må leve med til en viss grad for at aktiviteten i bedriften kan gå sin gang. Et sikkerhetstiltak som benyttes her er opplæring av ansatte ved for eksempel nyansettelser.

Lagring av data

For øyeblikket benytter deg seg av lokal lagring, men de er i prosessen av å konvertere til skybaserte tjenester. Mesteparten av dataene lagres lokalt og oppbevares i et gammelt bomberom som er fysisk utilgjengelig for andre enn IT avdelingen, samt ansatte i høyere stillinger gitt at de ber om tilgang. E.A. Smith planlegger å benytte seg av de skybaserte tjenestene til Amazon og regner med å være ferdigstilt og skybasert innen slutten av 2021. Unntaket til dette er selvfølgelig back-up filer samt enkelte filer som er mest egnet for å kjøre lokalt, men intensjonen til E.A. Smith er å være hovedsakelig skybasert.

Hittil har det oppstått noen komplikasjoner med overgangsprosessen. Servere har gått ned, og enkelte prosjekter som bedriften gjennomfører støtter ikke opp mot skytjenestene de prøver å benytte seg av, som medfører at de må bruke lokal lagring for disse prosjektene. Dette er situasjoner som kan forsinke overgangsprosessen, og viser også at heller ikke en skybasert løsning vil kunne løse alle sikkerhetsutfordringer hos E.A. Smith.

Diskusjon

Trusselbilde basert på resultater

I denne delen vil vi analysere den informasjonen vi har tilegnet oss gjennom intervjuer av de ansatte i E.A. Smith. Vi vil her komme med vårt syn på dagens situasjon i bedriften og kartlegge mangler og behov som har kommet frem. I tillegg vil vi komme med våre anbefalinger til tiltak og tilnærminger for å kunne svare på oppgavens problemstilling.

Under intervjuene med de ansatte i E.A. Smith kom det frem at bedriften har et relativt avansert sikkerhetssystem på sine PCer og IT-verktøy. De benytter seg av sikkerhetssystemet til en spesialisert tredjepart på de aller fleste av disse, og disse systemene gjør ifølge IT-avdelingen en meget god jobb for å sikre deres systemer mot utenforstående trusler slik som angrep, phishing og svindel. I tillegg har de tatt i bruk et ai-basert system som bruker maskinlæring for å styrke informasjonssikkerheten. Dette systemet er imidlertid fortsatt relativt nytt og er derfor ifølge informantene i overkant sensitiv slik at den reagerer på langt mer enn nødvendig.

Relativt klart trusselbilde

Videre har bedriften et relativt klart kartlagt trusselbilde. Det kommer frem at phishing, spam og svindelforsøk på e-post er den største utfordringen å håndtere, samt at det er på dette området man tidligere har opplevd flest uønskede hendelser. Dette tror man kommer av for dårlig kunnskap og svake IT-ferdigheter blant enkelte ansatte som dermed utgjør en risiko for angrep og uønskede hendelser herfra. Bedriften har også Microsoft 365 sine egne sikkerhetssystemer på dette området, men det er ikke alltid nok for å kunne forhindre at slike hendelser inntreffer.

Ønske om forbedringer

Blant de informantene vi har snakket med i bedriften er det også et stort ønske om forbedringer på områder rundt informasjonssikkerhet. Vi har fått inntrykk at man er veldig godt klar over hvilke mangler som bedriften for øyeblikket har på området og at man har et

genuint ønske om å utbedre disse, noe som er en stor styrke og solid start. I tillegg har E.A. Smith en kompetent IT-avdeling med god innsikt i trusler og utfordringer i bedriften.

De ansattes ønsker om forbedringer ga oss dermed flere konkrete eksempler på områder der bedriften opplever mangler, for dårlige systemer eller fraværende rutiner og retningslinjer. For å kunne komme i gang med en implementeringsprosess for ISMS og ISO-sertifisering hos E.A. Smith er det derfor viktig å kartlegge disse. Deretter kan man gå videre med konkrete tiltak og tilnærminger for å få på plass et komplett informasjonssikkerhetssystem.

Ikke ISO-sertifisert

En av de mest åpenbare manglene hos bedriften er selvsagt at de ikke har ISO-sertifisering for øyeblikket. Mangel på ISO-sertifisering er ikke nødvendigvis negativt, dersom bedriften har gode rutiner og sikkerhetsstrategier, men dette ser ikke ut til å gjelde for E.A. Smith. Med økende angrepsfrekvens og flere tilfeller hvor ansatte har gitt bort innloggingsinformasjonen sin til tvilsomme kilder, er innføring av ISO standarden noe som kan skape større trygghet og evne til håndtering av slike hendelser. Innføring av ISO standarden kan også eliminere mange eksisterende problemer hos E.A. Smith. Blant annet kan det heve den overordnede sikkerhetsstandarden til virksomheten. Ved å forankre sikkerhetsarbeidet i bedriften og øke fokuset på strategi tilknyttet dette, vil dette beskytte bedriften bedre mot risikoer som tidligere ville ha rammet dem. Et formelt styringssystem for informasjonssikkerhet vil skape retning i bedriften, ettersom alle ansatte dermed får noe å forholde seg til.

Mangel på formelle retningslinjer eller policyer tilknyttet informasjonssikkerhet

E.A. Smith har, som vi har oppdaget under våre intervjuer, ingen nedskrevne retningslinjer eller policyer. Uten retningslinjer og policyer befinner E.A. Smith seg i en svak posisjon sikkerhetsmessig og er veldig sårbare for angrep på IT. Som oppdaget i våre intervjuer har E.A. Smith allerede en økende angrepsfrekvens. Den mest vanlige hendelsen som ble nevnt i intervjuene var at ansatte gir fra seg eposten sin til tvilsomme kilder. Dette er igjen noe som kan unngås med klare og tydelige retningslinjer og policyer. Introduksjon av slike grep kan også drastisk redusere arbeidsmengden til IT avdelingen som videre kan redusere både forventede og uforventede kostnader i fremtiden.

Liten eller ingen opplæring

I våre intervjuer ble det også oppdaget at ansatte får liten eller ingen opplæring innen generell IT. Dette ser ut til å være en av de større kildene til IT problemene nevnt i intervjuene, hovedsakelig ved at ansatte gir bort eposten sin. Det er E.A. Smith sitt ansvar som et selskap at folk de ansetter enten allerede har nettvett eller at E.A. Smith lærer dem hva som er akseptabelt og ikke på jobben. Nye ansatte burde absolutt få opplæring for å ikke eksponere E.A. Smith sine systemer og IT avdeling for nye trusler. I likhet med punktet om retningslinjer og policyer kan unngåelse av et problem i utgangspunktet være mer effektivt enn å løse et problem når det først oppstår. Opplæring av ansatte kan dermed også bidra til å redusere arbeidsmengden til IT avdelingen og videre påløpende kostnader.

Stort spenn i IT-kompetanse

Det er urimelig å anta at alle har god forståelse for IT. Hos E.A. Smith har vi oppdaget at det er stort spenn i IT kompetanse hos de ansatte. Generell opplæring burde innføres for å få alle ansatte opp til et akseptabelt nivå for E.A. Smith. En annen synsvinkel er at klare og tydelig retningslinjer og policyer som mindre teknologisk tilbøyelige ansatte kan anvende seg til i tilfeller det føler seg usikre kan redusere mengden opplæring som er nødvendig.

Lagring av data

All data lagres for øyeblikket lokalt i et gammelt bomberom som har blitt tatt i bruk som et serverrom. Dette er en mindre trussel med tanke på at fysisk tilgang er praktisk talt umulig, men trusselen av ondsinnet og skadelig programvare er fortsatt til stede. Samtidig er E.A. Smith i prosessen med å flytte alt over til skybaserte tjenester. Dette betyr at all informasjonen deres kan sikres betydelig sterkere mot slik programvare og igjen blir fysisk tilgang tilnærmet umulig.

Adgangskontroll

Tilgang til diverse funksjoner og lokasjoner hos E.A. Smith avhenger sterkt på stillingen din innen selskapet. Stort sett er det kun IT-avdelingen som har adgang til kritiske funksjoner på

eksempelvis serverrom. Ledelsen derimot må be om tilgang dersom de ønsker det, men er fullstendig i stand til å få tilgang skulle de ønske det. Eksterne konsulenter får som nevnt tidligere i oppgaven eksklusiv tilgang til det de er leid inn til å gjøre.

E.A. Smith er veldig strenge på hvem som har tilgang til diverse funksjoner og kritiske områder. Dette er dermed et område der E.A. Smith ikke har opplevd alvorlige hendelser. Samtidig er dette strenge systemet svakt i den forstand at det ikke er basert i et system. Dette gjør at adgangskontroll kan anses som et risikoområde der det kan være hensiktsmessig å innføre policyer og retningslinjer som letter på begrensningene samtidig som det beholder strengheten. Videre kan dette være et av flere tiltak E.A. Smith bør vurdere som del av implementering av ISO 27001 siden dette hjelper bedriften være i samsvar med ISO sine tiltak for klassifisering av informasjon og aksesskontroll beskrevet i punkt A.8.2 og A.9.

Skisse for innføring

Som del av oppgaven vår har vi identifisert mange mangler hos E.A. Smith. Vi har brukt disse manglene til å bygge et helhetsbilde over situasjonen til virksomheten. Som et resultat av vårt arbeid med disse manglene har vi kartlagt disse sammen med risikoen de representerer for bedriften. Vi tilbyr dermed også en skisse for innføring av diverse tiltak E.A. Smith bør vurdere uavhengig om de velger å innføre ISMS basert på ISO-standardene.

Risikoanalyse

Uønsket hendelse	Årsak	Mulig konsekvens	S	K	R
Ansatte utgir brukernavn og passord (A)	Mangel på IT kunnskaper og nettvett.	Hackere kan logge inn på E.A. Smiths sine systemer og gjøre skade og/eller stjele informasjon.	4	3	12
Cyberangrep (B)	Installasjon av ondsinnet programvare, virus via epost eller lenker	Datasystemer slutter å fungere som de skal.	1-5	1-5	1-25
		Kan føre til tap eller spredning av kundedata.	2	5	10
	Manglende sikkerhetssystemer og rutiner	Avbrudd i daglig drift, økonomiske konsekvenser.	2	4	8
		Kan ramme bedriftens omdømme.	2	3	6
Brudd på kommunikasjonslinjer (C)	Serverproblemer	Feilkommunikasjon	2	2-4	4-8
	Tekniske feil	Mangel på kommunikasjon	3	2	6
Brudd på sikkerhetsklarering (D)	Uautoriserte personer får tilgang til sensitiv informasjon eller materiale Mistet/deling adgangskort	Kan gjøre at konkurrenter, tredjeparter eller andre får tilgang på informasjon/materiale som skader bedriften	2	1-5	2-10

Tabell 1: Oversikt over uønskede hendelser samt risikoen de representerer.

Som tredjepart er det vanskelig for oss å fullstendig forstå alle truslene E.A. Smith står ovenfor. Videre er det også vanskelig å vite hvilke aktiva de verdsetter mest og dermed hvor stor risiko diverse trusler representerer for bedriften. I et forsøk på å beskrive alvorligheten bak disse diverse truslene har vi konstruert risikoanalysen i *tabell 1*. Her analyserer vi risikoen diverse hendelser representerer for E.A. Smith samt hvilke måter disse kan fremstå på. Enkelte hendelser slikt som hendelse D, Brudd på sikkerhetsklarering, kan oppstå på flere måter og er dermed vanskelig å angi et eksakt tall på etter vår vurdering.

Det bør noteres at tallkodene funnet i *tabell 2* under, representerer hendelsene beskrevet i *tabell 1* funnet over.

E.A. Smith		1	2	3	4	5
		Ubetydelig	Mindre	Moderat	Betydelig	Alvorlig
5	Veldig sannsynlig					
4	Sannsynlig			A		
3	Mulig		C2	B1		
2	Usannsynlig			B4, C1	B3, D	B2
1	Veldig usannsynlig					

Tabell 2: Visuell representasjon av risiko for E.A. Smith

I *tabell 2* over, presenterer vi risikoen E.A. Smith er utsatt for visuelt. Vi har brukt risikoene vi kom frem til i *tabell 1* til å visualisere hvor skadelig de kan være for bedriften. Den mest truende risikoen er faren for cyberangrep som fører til tap eller spredning av kundedata, som vi kan se ved at punkt B1 fra *tabell 1* ligger under oransje område i *tabell 2*. Videre i *tabell 1* kan vi se at mange punkter har varierende risiko. Dette er et resultat av at vi har begrenset klarhet over hvor mye diverse aspekter av E.A. Smith sine aktiva er verdt etter

Fargekode	Tilsvarende Risiko
	Lav risiko
	Lav til middels risiko
	Middels risiko
	Middels til høy risiko
	Høy risiko

Tabell 3: Forklaring av fargeindeks i tabell 2

deres synspunkt. Vi har dermed vurdert de risikoene vi har nedskrevet basert på den informasjonen vi har tilgjengelig.

Tiltaksanalyse

Uønsket hendelse	Eksisterende tiltak	Nye tiltak
Cyberangrep	Brannmur Informasjonssikkerhetssystemer Sikkerhetsløsning styrt av maskinlæring og kunstig intelligens	Videreutvikling av eksisterende systemer Kontinuerlig forbedring
Serverproblemer/tekniske feil	Håndtering av IT-avdeling eller annet personale med ferdigheter og kunnskap om situasjonen	Proaktive retningslinjer med klare roller og ansvarsområder for effektiv feilretting og forebyggende arbeid
Brudd på sikkerhetsklarering	Håndtering av vaktpersonale og/eller ledelsen avhengig av situasjon og omfang	Opparbeiding av rutiner og retningslinjer i henhold til ISO-standard Sikkerhetspolicy
Utgivelse av brukernavn/passord	Håndtering av IT-avdeling og eksisterende sikkerhetssystemer	It-opplæring Standardisering av rutiner og retningslinjer Sikkerhetspolicy

Tabell 4: Oversikt over eksisterende tiltak samt forslag til nye tiltak i tilfelle uønskede hendelser.

Å lage en fullstendig guide til hvordan E.A. Smith kan implementere ISMS med ISO 27001-sertifisering er en svært omfattende oppgave og vil i seg selv være nok stoff til enda en bacheloroppgave. Vi ønsker likevel å lage en kortfattet plan på hvordan en slik implementeringsprosess kan foregå basert på informasjonen hos Standard Norge som har ansvaret for ISO-sertifisering i Norge, samt med hjelp av relevant fagstoff.

Selve ISO-sertifiseringen foretas av godkjent sertifiseringsorgan og gjennomføres som en undersøkelse med dem som overvåkende part. Her kan E.A. Smith sammen med sertifiseringsorganet fastslå i hvilken grad man allerede opererer i samsvar med standarden og hvilke tiltak som må utrettes før en vellykket standardisering kan skje. I tillegg bør det på forhånd bli gjort kjent hvilke tiltak som behøves og hvordan dagens ordninger samsvarer med standarden gjennom et forberedelsesprosjekt. Her kan det også være nødvendig å hente inn utenforstående eksperthjelp for å danne et fullstendig bilde av hva om behøves.

Etter at sertifiseringsorganet har sjekket all dokumentasjon av ISMS i organisasjonen i forkant vil de foreta undersøkelser til stede hos bedriften. Her vil det gjennomføres intervjuer og tester med alle involverte parter for å videre undersøke hvordan informasjonssikkerhetsarbeidet foregår i praksis. Deretter vil det lages en rapport basert på de resultatene man har fått gjennom sine undersøkelser, og det vil opparbeides en rapport der man gjennomgår resultater og presiserer eventuelle tiltak eller endringer som må foretas. Dersom resultatene er tilfredsstillende og dekker nødvendige krav vil man dermed få ISO-sertifisering.

Sertifiseringen kan ta fra noen måneder til et par år avhengig av situasjonen i bedriften. Det er generelt en enklere prosess å bli sertifisert dersom bedriften fra før har implementert tiltak og systemer slik som f.eks. standardiserte retningslinjer/policyer, eller mer avanserte rammeverk slik som COBIT, ISO 2000 eller ITIL. Derfor er det flere tiltak vi vil anbefale E.A. Smith å igangsette så snart som mulig og få på plass for en mer effektiv implementering og sertifisering av ISO-standarden i fremtiden.

Forslag til umiddelbare tiltak

Først vil vi anbefale å utarbeide formelle retningslinjer knyttet til informasjonssikkerhetsarbeidet i bedriften. Dette vil kunne være med på å redusere usikkerheten i bedriften rundt nødvendige handlinger og tiltak når en hendelse oppstår, samt at det vil kunne være med på å hindre at uønskede hendelser oppstår generelt. Disse retningslinjene bør knyttes opp mot alle kritiske informasjonssikkerhetsområder i E.A. Smith, slik som f.eks. bruk av e-post, pålogging, tilgang, sikkerhetsinnstillinger og mer.

Alle retningslinjer og policyer som utarbeides bør videre basere seg på kravene i ISO-standarden. Dette vil innebære å basere seg på ISO 27001-standarden for konkrete

retningslinjer og policyer, med ISO 27002-standarden som supplerende evaluering. Ved å benytte standardene herfra som bakgrunn vil E.A. Smith på denne måten opparbeide seg de rutinene og kravene til informasjonssikkerhet som er nødvendig for å senere bli sertifisert. Dermed vil denne prosessen bli mindre omfattende, og man kan få en mer smidig gjennomføring av sertifiseringen og videre informasjonssikkerhetsarbeid.

Basert på informasjonen som er gitt tidligere rundt det store spennet i IT-kompetanse i bedriften kan det også være fordelaktig å opprette et program for IT-opplæring i bedriften. Dette kan for eksempel styres av IT-avdelingen for å sikre at kunnskapen som opparbeides her er tilstrekkelig for bedriftens behov. Hva nøyaktig disse behovene er vil det naturlig nok være IT-avdelingen som har størst kunnskap om, så å involvere dem i denne prosessen vil ha størst potensiale for gode resultater.

Alle tiltak som gjennomføres bør også baseres på Demings sirkel for kontinuerlig forbedring med fasene planlegging, utførelse, oppfølging og iverksettelse. Dette vil altså si at informasjonssikkerhetsarbeidet aldri blir ferdig, men er et kontinuerlig arbeid der man stadig må vurdere og forbedre de tiltakene som er innført. På denne måten styrker man sjansene for et effektivt informasjonssikkerhetsarbeid i organisasjonen og at de rutiner, retningslinjer og tiltak som innføres også tilpasses nye situasjoner, samt følger utviklingen og situasjonsbildet generelt.

Konklusjon

I våre undersøkelser var forskningsspørsmålet vi hadde valgt ut som nevnt «*Hvordan kan innføring av et styringssystem for informasjonssikkerhet og ISO 27001-standarden styrke informasjonssikkerhetsarbeidet i organisasjonen E.A. Smith?*». Dette ble bakgrunnen for hvordan oppgaven ble satt opp og hvordan vi arbeidet med fagstoffet fra teori-delen til diskusjon og vår skisse til innføring. Som følge av dette arbeidet har vi kommet frem til at innføring av et formelt ISMS og ISO 27001-standarden kan være med å styrke informasjonssikkerhetsarbeidet i E.A. Smith på flere områder.

Først og fremst vil de kunne bidra til å forbedre og forankre holdningene de ansatte i bedriften har, ettersom de har formelle retningslinjer og policyer å støtte seg på. Dette vil skape mer klarhet under uforutsette hendelser og vil være med på å gi en mer effektiv daglig drift av informasjonssikkerhetsarbeidet med klare roller og ansvarsområder.

Samtidig kan det å kartlegge trusselbildet og jevnlig utføre risikoanalyser bidra til å forbedre innsikten de ansatte har rundt truslene bedriften møter, og gi dem bedre forutsetninger til å håndtere dem. Gode evalueringsrutiner gjennom kontinuerlig forbedring vil bidra til å holde bedriften oppdatert mot nye risikoer som oppstår og eventuelle forbedringer som burde implementeres.

Innføring av ISMS og ISO-sertifisering vil videre kunne skape en større trygghet for eventuelle kunder og utenforstående. Det å være sertifisert og ha klare sikkerhetsprosedyrer på plass skaper et inntrykk av en bedrift som tar dagens utfordringer på alvor og vil være i stand til å forhindre sikkerhetsbrudd og uønskede hendelser.

Innføring av et ordentlig ISMS vil også ha finansielle positive effekter. ISO-standarden har mange retningslinjer som omhandler verdi i bedrifter og implementering av ISO-standardene kan dermed hjelpe E.A. Smith opprettholde bedre kontroll på sin egen finans. Videre hjelper ISO-standardene bedrifter se og ta nytte av verdien av informasjon E.A. Smith sitter på, særlig nå som informasjon behandles som aktiva i den nyeste versjonen.

En annen måte å se på finansielle gevinster er å se på hvilke gevinster du ikke mister, fremfor hvilke du får. Ved implementering av ISO-standarder og ISMS kan E.A. Smith forebygge og hindre betydelig tap i form av bl.a. sikkerhetsbrudd. Disse kombinerte finansielle fordelene er i stand til å produsere nok verdi for E.A. Smith til å gjøre seg selv til en positiv investering før man tar i betraktning alle de andre fordelene nevnt utover oppgaven.

Svakheter og begrensinger i arbeidet vårt

På grunn av korona pandemien var det ingen fysisk kontakt med de ansatte hos E.A. Smith og det var dermed ingen besøk av deres lokaler heller. Oppgaven ble skrevet uten noen praktisk erfaring med den interne driften til virksomheten, som begrenser vår innsikt i bedriftens aktiviteter og fysiske situasjon. Av de samme årsakene var det begrenset fysisk kontakt mellom gruppemedlemmene under arbeidet med bacheloroppgaven, så nesten alt arbeidet skjedde gjennom digitale møter, samhandlings- og samarbeidsverktøy.

Pandemien begrenset også tilgangen vår til NTNUs ressurser, ettersom flere av disse bare kan benyttes dersom man er tilkoblet NTNU sitt wifi nettverk. Dette var noe vi overkom gjennom bruk av VPN, men det gjorde innhenting av litteratur, som blant annet fra Standard.no mer tungvint. I sin helhet er resultatene våre basert på de digitale intervjuene som ble gjennomført med representanter fra E.A. Smith.

Videre arbeid

Denne bacheloroppgaven inneholder en evaluering av E.A. Smith sitt informasjonssikkerhetsarbeid og veiledning/tiltak til hvordan de kan forsterke informasjonssikkerheten. Uheldigvis, på grunn av begrensinger tilknyttet oppgavens størrelse og omfang, så fokuserer den ikke like mye på selve prosessen E.A. Smith må gjennomgå for å forbedre informasjonssikkerheten sin. Her kunne det vært nødvendig med en til bachelor- eller masteroppgave som bygger videre på arbeidet vårt, og som fokuserer på å hjelpe E.A. Smith gjennom denne informasjonssikkerhetsprosessen. En oppgave som kommer med mer konkrete tiltak til forbedringer av informasjonssikkerheten, som gjennomfører risiko- og tiltaksanalyser i samarbeid med bedriften, og som i tettere samarbeid kan hjelpe med implementering av et formelt ISMS og ISO-sertifisering.

Referanser

Comtact. (2019, Februar 7). *What is the CIA Triad: Comtact*. Retrieved from https://comtact.co.uk/blog/what-is-the-cia-triad/

Datatilsynet. (2018, Oktober 10). *Iverksette styringssystem for informasjonssikkerhet: Datatilsynet.* Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Datatilsynet. (2019, Juli 16). *Datatilsynet: Risikovurdering*. Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/

De nasjonale forskningsetiske komiteene. (2019, februar 8). *Forskningsetiske retningslinjer for naturvitenskap og teknologi*. Retrieved from https://www.forskningsetikk.no/retningslinjer/nat-tek/forskningsetiske-retningslinjer-for-naturvitenskap-og-teknologi/

Digdir. (2021, April 30). *Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål*. Retrieved from https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123

Digitaliseringsdirektoratet. (2020, Mai). *Hva er risiko: Difi*. Retrieved from https://internkontroll-infosikkerhet.difi.no/risikostyring/hva-er-risiko

Digitaliseringsdirektoratet. (2020, Mai). *Hva er risikohåndtering*. Retrieved from https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/hva-er-risikohandtering

Disterer, G. (2013, April 16). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*.

E.A. Smith. (2020, Mai). *Om oss: E.A. Smith*. Retrieved from https://www.smith.no/om-oss/

Grønmo, S. (2020, November 3). *Store norske leksikon.* Retrieved from Kvalitativ metode: https://snl.no/kvalitativ_metode

Grønmo, S. (2020, Juni 4). *Store norske leksikon.* Retrieved from Kvantitativ metode: https://snl.no/kvantitativ_metode

Irwin, L. (2019, April 2). *IT Governance UK Blog*. Retrieved from IT Governance UK: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002

Jørgenrud, M. B. (2019, Oktober 1). *Digi.no*. Retrieved from https://www.digi.no/artikler/cyberangrep-koster-dansk-horeapparatselskap-minst-800-millioner/475385

Klefstad, B., Hjelle, T., & Haugset, B. (2018, Januar). *Blackboard.* Retrieved from https://ntnu.blackboard.com/webapps/blackboard/execute/content/file?cmd=view&content_id=_889758_1&course_id=_19097_1

Kosutic, D. (n.d.). *27001 Academy: Advisera*. Retrieved from Advisera: https://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

Moen, R., & Norman, C. (2009, September 19). *Evolution of the PDCA cycle*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.5465&rep=rep1&type=pdf

National Institute of Standards and Technology, National Computer Science Center. (1991, Oktober). *Google Books, side 328.* Retrieved from https://books.google.no/books?id=fgwSAQAAMAAJ&printsec=frontcover#v=onepage&q&f=false

NorSIS. (2021). *NorSIS, Norsk senter for informasjonssikring.* Retrieved from https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

NSD, Norsk senter for forskningsdata. (2021, Februar 12). *Meldeskjema for behandling av personopplysninger.* Retrieved from https://learn-eu-central-1-prod-fleet01-xythos.learn.cloudflare.blackboardcdn.com/5def77a38a2f7/8740159?X-Blackboard-Expiration=1621447200000&X-Blackboard-Signature=q3agn7ANynsNsJrSysBlxZPYD%2ByuKPjPKm19A%2FTE7ZA%3D&X-Blackboard-Client-Id=303508&response-

One Comodo. (2021, Mai 5). *IT Risk Management*. Retrieved from https://one.comodo.com/risk-management/

Siteware. (2019, Februar 19). *Siteware*. Retrieved from https://www.siteware.co/en/methodologies/what-is-the-pdca-cycle/

Standard Norge. (2017, Mai 1). *NS-EN ISO/IEC 27001:2017.* Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900

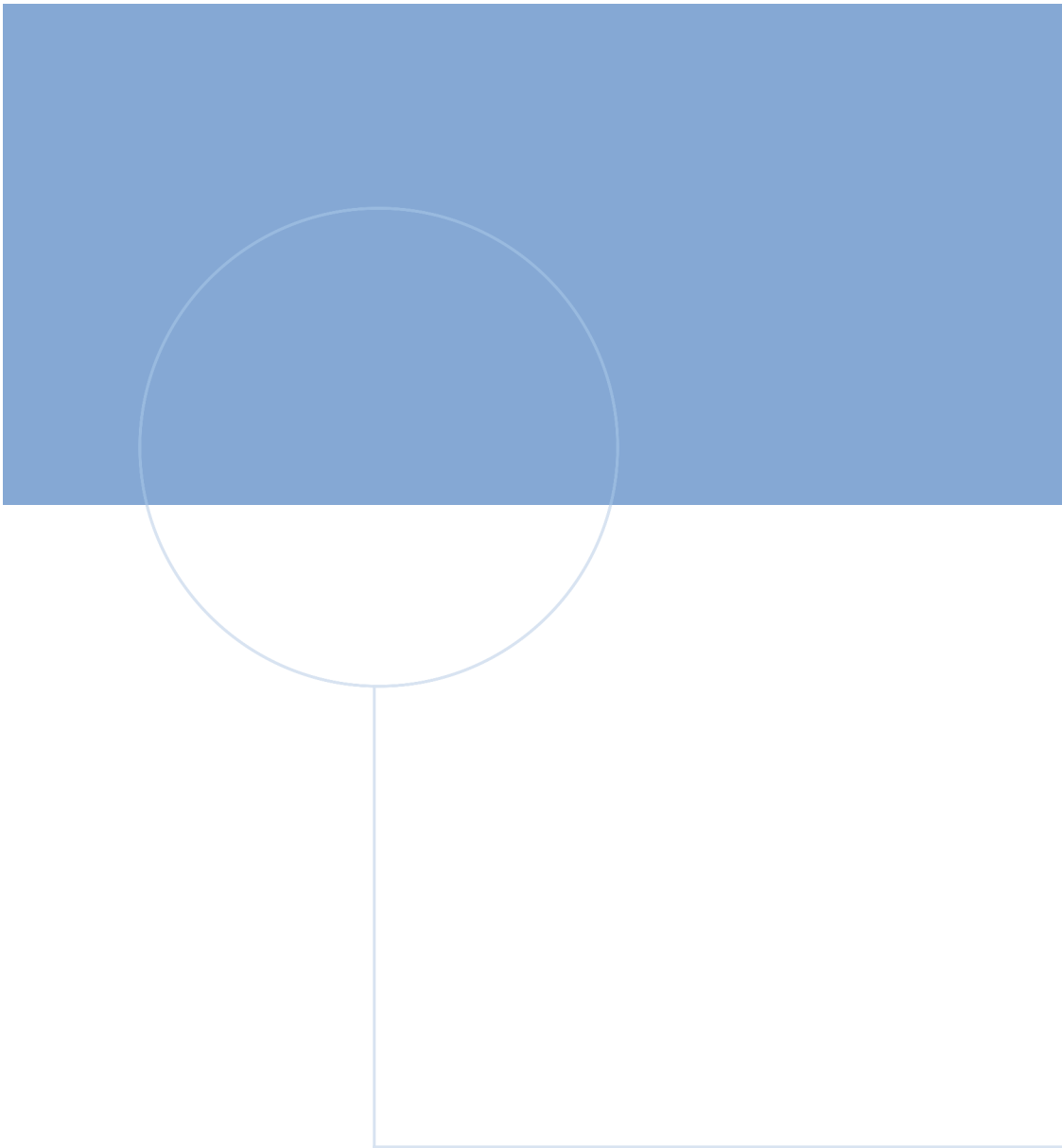
Standard Norge. (2017, Mai 1). *NS-EN ISO/IEC 27002:2017.* Retrieved from standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925901

Standard Norge. (2020, April 1). *NS-EN ISO/IEC 27000:2020.* Retrieved from standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1128720

Standard Norge. (n.d.). *IT-sikkerhet - ISO/IEC 27000*. Retrieved from Standard Norge: https://www.standard.no/fagomrader/ikt/it-sikkerhet/

Walsham, G. (1995, Mai 1). *Interpretive case studies in IS research: nature and method. SpringerLink.* Retrieved from https://link.springer.com/article/10.1057/ejis.1995.9

Wig, K. (2019, Februar 10). Norges bankkjemper har avdekket flere Kina-angrep: – Trusselbildet er økende. pp. https://e24.no/teknologi/i/qLynzO/norges-bankkjemper-har-avdekket-flere-kina-angrep-trusselbildet-er-oekende.



NTNU

Kunnskap for en bedre verden