Universitetet i Stavanger

NORSK HOTELLHØGSKOLE

BACHELOROPPGAVE

STUDIUM: Hotelledelse	OPPGAVEN ER SKREVET INNEN FØLGENDE FAGOMRÅDE: Datasikkerhet ER OPPGAVEN KONFIDENSIELL? (**NB**! Bruk rødt skjema ved konfidensiell oppgave)
TITTEL: Moderne løsninger, skaper moderne utfordringer – Datasikkerhet i gjestfrihetsbransjen ENGELSK TITTEL: Modern solutions, create modern challenges – Cybersecurity in the hospitality industry	

FORFATTER(E)(**NB!** maks tre studenter pr oppgave):			VEILEDER:
Kandidatnummer:	Studentnummer:	Navn:	Lukasz Andrzej Derdowski
7067 ……..	255475 ……	Stine Soland …….	
7036 ……..	255435 ……	Birthe Arild …….	
……..	……	…….	

Datasikkerhet i gjestfrihetsbransjen:

MODERNE LØSNINGER, SKAPER MODERNE PROBLEMER

Birthe Arild
Stine Soland

20 studiepoeng

Norsk Hotellhøgskole
Hotelledelse
Mai 2022

Forord

Denne bacheloroppgaven er vår avsluttende oppgave ved Universitetet i Stavanger på studiet hotelledelse. Problemstillingen er noe vi begge har hatt og fått enda mer interesse for etter ferdig bacheloroppgave, og vi setter pris på kunnskapen vi har innhentet. Vi føler også tematikken er meget samfunnsaktuell og relevant for gjestfrihetsbransjen.

Vi ønsker å takke vår veileder Lukasz Andrzej Derdowski som har vært meget oppmuntrende og en gitt oss gode råd i prosessen. Vi setter pris på at du alltid har vært til god hjelp når vi har hatt behov for det. Det har alltid vært veldig motiverende å være på veiledninger og du har virkelig gitt oss en ekstra gnist under skrivingen av bacheloren. En ekstra takk til de som har tatt seg tid i en travel periode til å ta spørreundersøkelsen og gi oss et lite innsyn på hvordan gjestfrihetsbransjen, vi setter veldig pris på det.

Høydepunktet er de gode minnene vi har lagd sammen, og vi vil ta det med oss videre i livet. Tusen hjertelig takk.

Sammendrag

I denne oppgaven har vi sett på datasikkerhet i den norske gjestfrihetsbransjen, og hvordan den blir påvirket av dataangrep. Oppgaven viser til meget relevant forskning som belyser omfang av datasikkerhet i Norge. Hovedformålet er å besvare problemstillingen som lyder slik, "*Forekomst, svakheter og generelle effekter ved dataangrep i norsk gjestfrihetsbransje".*

For å besvare problemstillingen på best mulig måte tar vi i bruk kvantitativ metode, nærmere bestemt spørreundersøkelse. Spørreundersøkelsen er rettet mot ledere og mellomledere fra bransjen. Gjennom forskningen som vi har gjennomført har vi fått ett inntrykk av at datasikkerhet er noe som burde være på dagsorden, og dataangrep rettet mot norske bedrifter, innenfor gjesfrihetsbransjen, er en svært reell trussel.

Innholdsliste

1.0 Introduksjon

Utrykk som «det teknologiske samfunnet» er et begrep som ofte blir brukt til å beskrive tiden som har etterfulgt den industrielle revolusjon. Det moderne samfunnet bygger på, og er avhengig av avansert teknologi. (Gurslig-Berg og Rosvold, 2021). Siden 90-tallet har samfunnets produksjonsprosess av varer og tjenester vært avhengig av informasjonsinfrastruktur, og teknologisk innovasjon har vært en definerende faktor for økonomisk vekst. (Pettersen, 2018). «På slutten av 90-tallet flyttet informasjons- og kommunikasjonsteknologi for alvor inn i samfunnet, hvilket gjorde det mulig å organisere både arbeid og livene våre på fundamentale nye måter enn tidligere.» (Pettersen, 2018).

Den kraftige teknologiske utviklingen har hatt en stor innvirkning på det daglige liv, dette gjelder også i arbeidslivet. Reiselivsnæringen i Norge, som mange andre næringer og industrier, er avhengig av å følge den teknologiske utviklingen. Næringslivets hovedorganisasjon publiserte i 2018 en omfattende rapport kalt Verden og oss – Næringslivets perspektivmelding 2018. I all hovedsak handler rapporten om framtidsutsikter for næringslivet i Norge, og utvikling de neste tiår mot 2050. Rapporten er delt i ulike kapitler, det femte kapittelet handler om digitalisering. Kapittelet innledes slik, «Digitalisering vil endre samfunns -, nærings- og arbeidslivet på flere avgjørende måter i årene som kommer». (Næringsliv Hovedorganisasjon, 2018). Videre belyser de viktigheten av tillitt til IKT-systemer som digitaliseringen er avhengig av. Den teknologiske utviklingen de siste 20 årene har også ført til utfordringer. En konsekvens av at flere samfunnskritiske funksjoner blir avhengig av komplekse verdikjeder er sårbarhet i systemene. «En effekt av den digitale utviklingen er en kraftig endring i samfunnsrisiko- og sårbarhetsbilde» (NOU, 2015:13, s.15).

Nasjonal sikkerhetsmyndighet (NSM), er et sikkerhetsorgan som arbeider aktivt for å hjelpe norske bedrifter. I november 2019 opprettet NSM et nytt senter, som en del av NSM organet. Nasjonal cybersikkerhetssenter (NCSC) ivaretar og oppdaterer risikobildet i det digitale rom, i tillegg gir senteret råd og veiledning ved dataangrep. (Nasjonal Sikkerhetsmyndighet, 2020). NSM melder i sin årlige sikkerhets rapport fra 2021, om ett takt skifte innenfor digital risiko. Senteret har opplevd en markant vekst i aktivitetsnivå i det digitale rom. Videre har det vært en tredobling i antall alvorlige hendelser registrert i 2020, sammenlignet 2019. (Nasjonal Sikkerhetsmyndighet, 2021, s.7)

Gjestfrihetsbransjen i Norge har, som mange andre næringer, blitt påvirket av teknologisk innovasjon og digitalisering. Utviklingen fører til endring i dynamikken til forbrukeradferden, som også skaper muligheter for nye måter å samhandle med kunder. Teknologi er en av de viktigste megatrendene og drivkreftene som antas å forme fremtiden for gjestfrihetsbransjen. (Yallop & Seraphin, 2020) I all hovedsak er dette virkelighetsbildet som bachelor oppgaven tar utgangspunkt i.

1.1 Begrunnelse

Dataangrep er et svært samfunnsaktuelt tema, det gjenspeiles i rapportene til NSM, og deres nyopprettede organ Nasjonal cybersikkerhetssenter. Videre meddeler NSM at de opplever at de fleste norske bedrifter som blir utsatt for data hendelser har ikke nødvendige forebyggende tiltak på plass. NSM viser også til manglende kompetanse og kapasitet til å avdekke, håndtere eller begrense skadeomfang ved dataangrep (Nasjonal Sikkerhetsmyndighet, 2020). Datakriminalitet

er blant annet den tredje vanligste typen kriminalitet (Bjørshol, 2018). Dermed er det høyst aktuelt å sikre seg mot dagens trusselbilde i Norge.

Fremtidsutsiktene maler ett bilde om at den teknologiske utviklingen vil akselerere ytterligere. Utviklingen vil føre til økonomisk vekst, høyere konkurransekraft og verdiskapning, men en kan på mange måter omtale denne utviklingen som et tveegget sverd, det er også en massiv utfordring å imøtekomme (Næringsliv Hovedorganisasjon, 2018). Etiske dilemmaer om personvern og ikke minst sikkerhet vil være fremtredende. Dataangrep og datasikkerhet i gjestfrihetsbransjen er tema som er relevant i videre forskning.

1.2 Formålet med oppgaven

Formålet med denne oppgaven er å utforske hvorvidt norsk gjestfrihetsbransje tar for seg datasikkerhet, og hvilke trusler som truer bransjen i Norge. Vi ønsker gjennom denne oppgaven å gi bransjen innsikt om datasikkerhet i Norge, og hva som kan være forebyggende mot teknologiske trusler. Gjennom bruken av spørreundersøkelsen ønsker vi å kartlegge dataangrep i norsk gjestfrihetsbransje, for å se om det er noen faktorer som har mer påvirkning enn andre. Hovedproblemstilling for denne bachelor oppgaven er *"Forekomst, svakheter og generelle effekter ved dataangrep i norsk gjestfrihetsbransje".*

For å kunne besvare den overnevnte problemstillingen er det hensiktsmessig å ha noen underliggende forskningsspørsmål for å belyse de forskjellige aspektene i problemstillingen.

1. Har høy turnover effekt på dataangrep i norsk gjestfrihetsbransje?
2. Er datasikkerhet en prioritering i norsk gjestfrihetsbransje?

1.3 Bakgrunn for valg av problemstilling

Bakgrunnen for problemstillingen er basert på hvordan nyhetsbilde har utviklet seg de siste årene, og personlig interesse for datateknologi og teknologisk infrastruktur. Vi ønsker gjennom problemstillingen å se hvordan gjestfrihetsbransjen forholder seg til teknologi, og hvor klar de er for den teknologiske utviklingen i verden. Vi ønsker å studere om det er noen faktorer som utmerker seg i forhold til dataangrep og om det er noen forbedringsområder i gjestfrihetsbransjen.

1.4 Avgrensninger

Avgrensningen er satt etter at vi har utforsket flere ideer innen dataangrep og den teknologiske utviklingen i gjestfrihetsbransjen. Oppgaven er avgrenset til et nasjonalt utvalg av bedrifter i den norske gjestfrihetsbransjen. Videre har vi valgt å ta utgangspunkt i perspektivet til mellomledere og ledere i gjestfrihetsbransjen.

Underveis i prosessen vurderte vi blant annet å ta utgangspunkt i forbrukeren, da ville problemstillingen sannsynligvis blitt vinklet på en annen måte. Det ville vært interessant å undersøke hvordan dataangrep kan påvirke kjøpekraft og oppførsel til kunder, samt kartlegge hvordan forbrukeren opplever de store mengder av sensitiv data gjestfrihetsbransjen besitter.

Videre kunne det vært interessant å kartlegge et presist omfang av dataangrep i løpet av en gitt tidsperiode, for eksempel de siste 10 årene, og hvordan teknologien har endret seg. Vi kunne blant annet utforsket når gjestfrihetsbransjen begynte å benytte seg av ny teknologi, og gikk vekk ifra de mer tradisjonelle løsningene. Av flere ulike grunner kan det være vanskelig å innhente slik data, det er uklart om slike hendelser har blitt rapportert. I tillegg kan et annet problem være å finne de rette informantene til slik type data.

1.5 Oppgavestruktur

Oppgaven er strukturert inn i seks hovedkapitler som vist i figur 1. I kapittel 1 gjennomgår vi begrunnelse, formål med oppgave og avgrensninger. I kapittel 2 gjennomgår vi relevant teori for resten av oppgaven og problemstillingen. I kapittel 3 gjennomgår vi og redegjør for vårt valg av metode, her ser vi på forskningsstrategi, datainnsamlingsmetode og utforming av spørreskjema. I kapittel 4 presenterer vi funnene våre i analysedelen, etterfulgt av resultat. Til slutt ser vi på diskusjon og konklusjonen av oppgaven i kapittel 6.

Figur. 1: Oppgavestruktur

2.0 Begrepsforklaring

2.1 Turnover

Turnover er et begrep som blant annet blir brukt i gjestfrihetsbransjen, det blir beskrevet på norsk som «utskiftning av ansatte; gjennomtrekk» (Det Norske Akademis Ordbok, 2022). Turnover i gjestfrihetsbransjen er et utbredt problem, og det er ofte utskifting av ansatte, turnover kan også ha stor effekt på ansattes produktivitet og motivasjon. (Dwesini, 2019, s.1)

2.2 Point of Sales Systemer (POS)

Point Of Sales Systemer (POS systemer) blir definert i gjestfrihetsbransjen som et nettverk av system som samler kasse og server terminaler, disse systemene brukes til drift i gjestfrihetsbransjen. (Moon, Kim & Ham, 2014) POS systemer er svært gunstig for drift av virksomheter, systemet har bistått i å oppnå målet for å skape kundetilfredshet og har vært revolusjonerende for gjestfrihetsbransjen.

2.3 Virksomhet størrelse (micro, small, medium & large enterprise.)

Enterprise, også kjent som bedrift er en enhet som driver med økonomisk aktivitet. Det fins forskjellige størrelser på bedrifter og disse er innenfor satte rammer når det gjelder antall ansatte. Den europeiske unionen har laget en tabell og retningslinjer for hvordan disse bedriftene skal kategoriseres. (European Community Commission, 2003)

Kategori	Ansatte
Stor	>250
Medium	<250
Liten	<50
Micro	<10

Tabell 1: *Virksomhets størrelse*

2.4 Informasjons- og kommunikasjonsteknologi

Informasjons- og kommunikasjonsteknologi (IKT) er evnen til å forebygge, oppdage og håndtere følgende hendelser: brudd på konfidensialitet, som betyr innsyn på informasjon som ellers skal være beskyttet, brudd på integritet som betyr at data informasjon eller systemer blir endret på. Endringene kan være små, men det kan også bety at informasjonen blir flyttet eller slettet. Den siste hendelsen er brudd på tilgjengelighet, informasjon eller systemet blir tapt og er ikke tilgjengelig når det er behov for det. (Tømte, Næss & Røsdal, 2019)

3.0 Teori

Dette kapittelet gjør rede for teorien som skal brukes gjennom oppgaven, teoridelen er også et verktøy for hvordan vi ønsker å løse problemstillingen, og er hovedgrunnlaget for analyse og konklusjon. Teorien er også grunnlaget for oppbygning av spørreundersøkelsen, og vi har basert oss mye på rammeverket i teoridelen når vi har konstruert undersøkelsen i oppgaven. I dette kapittelet beskriver vi gjestfrihetsbransjen, risiko og krisehåndtering og A4 rammeverket.

3.1 Gjestfrihetsbransjen

Ordet gjestfrihet er en direkte oversettelse av det engelske begrepet «Hospitality». «The hospitality industry" omfatter et bredt spekter av virksomheter, som dedikerer sitt arbeid til personer som er borte fra hjemmet sitt. (Chon & Maier, 2010, s.6) Gjestfrihetsbransjen har utviklet seg til en svært kompleks og omfattende industri som strekker seg på tvers av landegrenser. Økonomiske systemer påvirker hverandre og utfoldes i et samspill, hendelser i USA kan for eksempel påvirke industrien i Norge og omvendt. (Chon & Maier, 2010, s.6)

For rundt 10 år siden var gjestfrihetsbransjen primitiv i forhold til den teknologiske utviklingen som har vært de siste årene, for eksempel var interaktiv plasma-tv på hotellrom, sensor-basert lys og innsjekkings kiosker på blant annet flyplasser, teknologi som var relevant i datidens litteratur. (Chon & Maier, 2010. s.409) Per dags dato har gjestfrihetsbransjen tilgang til detaljert informasjon av forbrukeres behov og ønsker gjennom teknologi (Zsarnoczky, 2018). Gjestfrihetsbransje har endret seg med tiden, men også med den nye generasjonen av gjester som har vokst opp med teknologisk innovasjon. Dette markedssegmentet er også kjent som generasjon z, og har andre reisevaner en tidligere generasjoner. (Jamies, Erdem, Chen & Doyle, 2019)

«Teknologi som beriker opplevelser og leveranser, som utvidet virkelighet (augmented reality), er også på vei inn i reiselivet sammen med automatisering og robotifisering, som gir endringer i produksjon av tjenester og opplevelser.» (Innovasjon Norge, 2021, s.25) Det er flere hoteller i gjestfrihetsbransjen som allerede har begynt å eksperimentere med systemer som vil bli enda vanligere i fremtiden. Blant denne teknologien er for eksempel service-roboter, de benyttes i forskjellige bruksområder slik som bartendere, sosial underholdning og innsjekk, men denne

teknologien har enda ikke oppnådd sitt potensiale og er utilfredsstillende. (Drexler & Lapre, 2019)

I en undersøkelse gjort på gjestfrihetsbransjen i forhold til andre bransjer viser det til at gjestfrihetsbransjen er mer utsatt enn andre bransjer når det gjelder hacking og skadelig programvare. (Chen & Fiscus, 2018) Den samme undersøkelsen viser også til at gjestfrihetsbransjens store mengder av sensitiv data kan ha et stort negativt resultat ved dataangrep, og de fleste dataangrep var ikke alltid like lette å oppdage, før eventuelt regnskap eller bank ga beskjed om ondsinnete aktiviteter.

I 2018 opplevde den amerikanske hotellkjeden Mariott Hotels uautoriserte tilgang på sine server som inneholdt gjester sine personlige sensitive data. Det ble blant annet lekket navn, adresse og pass-nummer, Mariott var også usikker på om gjesters bankkort-nummer hadde blitt lekket. (Mariott International, 2018) Det er estimert at opp mot 300 millioner gjester ble påvirket av dataangrepet på Mariott Hotels, men det er høy sannsynlighet for at det var enda flere gjester som ble rammet. Hotellkjeden endte opp med å betale en bot på 215 millioner norske kroner. (BBC, 2020) I norsk gjestfrihetsbransje opplevde nylig Nordic Choice virusangrep på sine IT-systemer, viruset hadde stor effekt på operasjonene og slo ut flere systemer på hotellene. (Nordic Choice Hotels, 2021) Dataangrepet Nordic Choice opplevde resulterte i lekket sensitiv data om intern drift og ansattes informasjon (Gundersen, Lied & Thommessen, 2021).

For tiden produseres det betydelig mengder ustrukturert og strukturert data globalt, handlingen ved å behandle slik data kalles for «Big data». Big data kan videre defineres slik, en handling som foretas i stor skala, som ikke er mulig å gjennomføre på et mindre nivå, for å hente ut ny

innsikt (Yallop & Seraphin, 2020). Store mengder data i omløp er drevet frem av økt datakapasitet, regnekraft, skyløsninger, tingenes nett og kunstig intelligens. (Næringslivets Hovedorganisasjon, 2018) Gjestfrihetsbransjen har ett stort omløp av informasjon som brukes til å skreddersy opplevelser. «De digitale plattformselskapene sitter på en stor mengde informasjon om hver enkelt bruker. Da blir krav til transparens (for eksempel i søk), dataportabilitet og ansvarlighet (for eksempel i bruk av personopplysninger) viktige.» (Næringslivets Hovedorganisasjon, 2018) Datadrevet innovasjon gir uante muligheter for analyse av produksjonsprosesser, overvåkning og styring innenfor nesten alle næringer (Næringslivets Hovedorganisasjon, 2018).

3.2 Risiko og sårbarhet i gjestfrihetsbransjen

«Alle virksomheter skal kartlegge og vurdere alle farer og problemer, og vurdere risiko knyttet til arbeid.» Ansvaret ligger hos arbeidsgiver, som skal sørge for at dette blir gjennomført, vurdering skal sørge for at ingen blir skadet eller syk på grunn av arbeid. (Arbeidstilsynet, 2022) Det kommer frem i en undersøkelse gjort om norsk IKT-sikkerhets kompetanse, at det ikke er tilstrekkelig kompetanse innen fagfeltet. I undersøkelsen som er publisert i 2019 konkluderes det også at det vil være mangel på forståelse for IKT-sikkerhet og det er vanskelig å dekke etterspørselen som stadig stiger. (Mark, Tømte & Røsdal, 2019)

Den teknologiske utviklingen har ført til sårbarhet i gjestfrihets bransjen, sårbarhet fører til risiko for at en uønsket hendelse kan inntreffe. Innledningsvis ser vi at industrien er preget av flere uønskede hendelser. Bente Hoff meddeler i NSM rapport fra 2020 at digitale hendelser fra det siste året kunne vært avverget eller begrenset dersom virksomheter hadde fulgt rådene i NSMs grunnprinsipper for IKT-sikkerhet (Nasjonal Sikkerhetsmyndighet, 2020). Med andre ord norske

virksomheter har gode muligheter for å redusere risikobilde, dersom en iverksetter gode tiltak. “Det er viktig å være i forkant med risiko reduserende tiltak. Med bakgrunn i det utfordrende risikobilde vi nå står overfor, hvor konsekvensene av cyberangrep blir mer alvorlige, haster det mer enn tidligere å implementere tiltak» (Skaug, 2022)

Det har vært et behov for sikring av personinformasjon på grunn av den økte sårbarheten som følge av digitalisering. Informasjonsflyt av personlig data og virksomhetskritisk data står til fare for å bli utsatt for sikkerhetsbrudd. Andre forhold som er viktig å verne er informasjon som kan bli misbrukt til nye og uønskede formål. Derfor ble det i 2018 utarbeidet et nytt lovverk for EU landene, som heter General Data Protection Regulation (GDPR). Norge er ikke en del av EU, likevel ble forordningen vedtatt som norsk lov. (Einstabland, 2018)

Forskning innen dataangrep i gjestfrihetsbransjen foreslår at POS systemer er en svakhet som kan føre til dataangrep. (Gwebu & Barrows, 2020). Videre diskuterer artikkelen at størrelse på virksomhet påvirker hvor utsatt en kan være for dataangrep. Resultater av påvirkning ved dataangrep kan ha større konsekvenser for en mindre bedrift i forhold til store bedrifter, på grunn av hvor rustet de er for finansielle tap. Et annet viktig aspekt er at større bedrifter har bedre muligheter for økonomiske investering og utvikling, men dette gjør dem mer sårbare på grunn av at de er mer attraktive for utnyttelse. Med andre ord en stor bedrift kan eie ressurser som er attraktive å utnytte, og derfor være et større mål for kriminelle datagrupper.

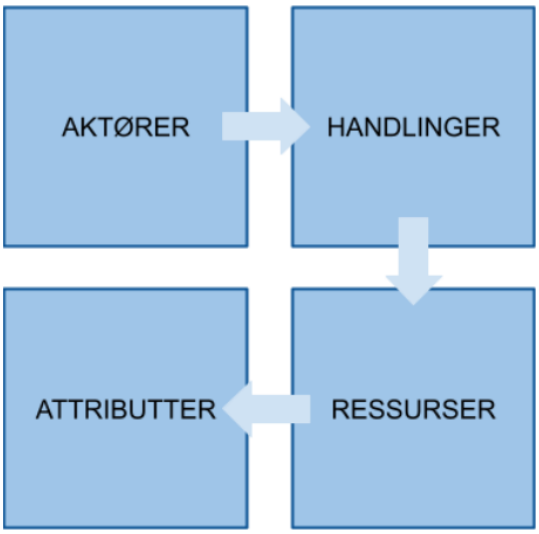
En forskningsartikkel gjennomført basert på data fra VERIS, viser til at turnover kan være en av årsakene for at gjestfrihetsbransjen er mer utsatt enn andre bransjer. (Gwebu & Barrows, 2020) Forskningsartikkelen sier også at gjestfrihetsbransjen har høy turnover, som kan bety dårlige

ferdigheter for nyansatte, hovedproblemet som blir nevnt ved høy turnover i gjestfrihetsbransjen er at dårlig datasikkerhetsopplæring og dataferdigheter kan i verste fall føre til høyere risiko for dataangrep.

3.2 The VERIS Community Rammeverk

"VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner." (VERIS Community, 2022). Rammeverket til VERIS Community har blitt brukt i flere forskningsartikler for å blant annet forstå karaktertrekk av hendelser ved dataangrep (Gwebu & Barrows, 2020). VERIS er en respons på utfordringer i datasikkerhets-industrien, hvor det lenge har vært mangler på et definerende språk for å beskrive og forstå dataangrep på en oversiktlig og anonym måte. Det overordnede målet for initiativet er å lære fra erfaring for å bedre måle og imøtekomme risiko innen datasikkerhet. (VERIS Community, 2022)

Rammeverket som er utviklet baseres på ulike komponenter under "the A4 Method", eller A4 metoden. Hensikten til rammeverket er å samle begreper og beregninger for å kartlegge virksomheters hendelsesrelatert informasjon innenfor datasikkerhet- og trusler. Begrepet er definert i en struktur av fire kategorier "actors, actions, assets og attributes" som vi direkte oversetter til "aktører, handlinger, ressurser og attributter." (VERIS Community, 2022) Videre gir denne strukturen et optimalt rammeverk for å måle frekvens, knytte kontroller, koblingseffekt og mange andre konsepter som kreves for risikostyring. (VERIS Community, 2022) Når en virksomhet skal kartlegge et eventuelt dataangrep kan de bruke de forskjellige kategoriene for å sette sammen hendelsesforløpet.



Figur.2: A4 Rammeverket

3.2.1 Aktører

VERIS Community har definert tre forskjellige aktører for trussel-aktører, trussel-aktører i dette tilfellet er hvem som har utført dataangrepet mot en eventuell virksomhet eller bedrift: *Eksterne aktører:* aktører som er utenfor organisasjonen, nettverk og partnere. Eksempler på eksterne aktører er; kriminelle grupper, tidligere ansatte, og statlige aktører (andre land). Eksterne aktører kan også være naturlige hendelser og ulykker. Det blir ikke gitt privilegier eller tillit til eksterne aktører. *Interne aktører:* aktører som er innenfor organisasjonen slik som ansatte. Interne aktører er aktører som blir gitt tillit og privilegier. *Tredjeparts aktører:* aktører som er tredjeparts aktører, og deler relasjoner med organisasjonen. Dette er leverandører, out-source IT support og lignende personell. Tredjeparts aktører har litt tillit og privilegier. (VERIS Community, 2022)

3.2.2 Handlinger

Handling definerer hva en eventuell aktør har gjort og beskriver de forskjellige truslene som kan oppstå under et eventuelt dataangrep.

Skadevare - Skadevare også kjent som "malware" eller skadelig programvare er software, eller kode som endrer enhetens status uten eiers samtykke. Eksempler av malware er; virus, spyware, keylogger, bakdører (VERIS Community, 2022)

1. *Hacking* - For Veris er hacking definert som å få tilgang uten autorisasjon.
2. *Sosial* - Sosial trussel er å skaffe informasjon eller tilgang gjennom manipulasjon, trussel, og generelt misbruk.
3. *Misbruk* - Misbruk er når organisasjonen eller virksomhetens ressurser blir brukt mot den hensikten den var ment for. Dette inkluderer administrativt misbruk, brudd på retningslinjer, bruk av ikke-godkjente eiendeler. Misbruk trenger ikke være ondsinnet, men det er reservert for de som har tillit og privilegier innad i organisasjonen.
4. *Fysisk* - Fysiske trusler er å skaffe informasjon gjennom tyveri, sabotasje og uautorisert tilgang. Fysiske handlinger er reservert til menneskelig innvikling, og gjelder ikke andre ting slik som ulykker og vær-katastrofer.
5. *Feil* - Feil handler om når ting har blitt gjort uriktig, eller ikke gjort i det hele tatt. Dette kan være feil i programmering, feil konfigurasjon på system, søl på elektronikk, ledninger som faller ut osv.
6. *Miljø* - Miljø handler om naturlige hendelser, slik som vær og flom, det kan også være farer på infrastruktur eller området rundt hvor ressursene befinner seg.

(VERIS Community, 2022)

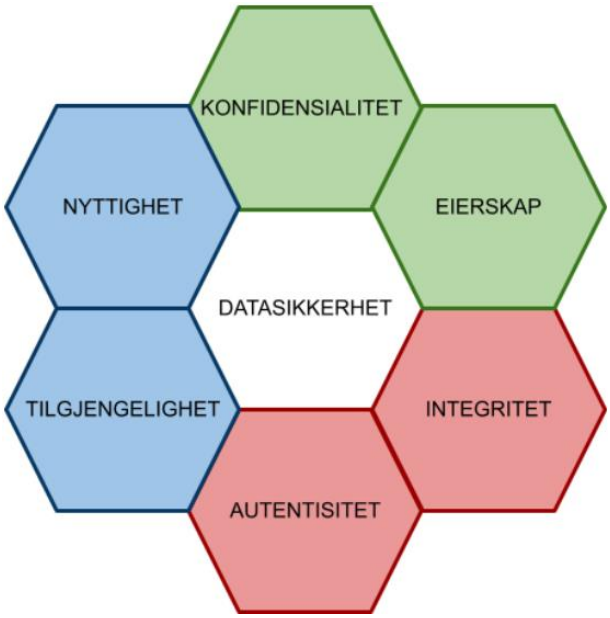
3.2.3 Ressurser

Ressurser handler om hvilken informasjon som ble tuklet med, det kan hende at informasjonen eller dataen gikk tapt, lekket eller at integriteten på et vis har blitt endret på. Ressurser kan være

fysisk eller basert på data, for eksempel en bærbar datamaskin eller viktige dokumenter på en server (VERIS Community, 2022).

3.2.4 Attributter

I det norske akademis ordbok blir attributt definert slik "vesentlig egenskap som noe må ha for å fortsette å være seg selv; grunnegenskap" (Den Norske Akademis Ordbok, 2022). Attributt er den siste definerte kategorien i VERIS Community sitt framework. Denne seksjonen er en utvidelse av retningslinje for informasjonssikkerhet i en organisasjon, som blir kalt for "Parkerian Hexad" som er en utvidelse av CIA triaden, den står for "confidentiality, integrity and availability" (VERIS Community, 2022). Utfra «Parkerian Hexad» er det laget seks attributter, de opprinnelige attributtene fra CIA triaden har blitt utvidet hvor de henger sammen som par, disse attributtene blir kalt for konfidensialitet & eierskap, integritet & autentisitet og nyttighet & tilgjengelighet. Attributter er egenskapene til ressursen som har blitt utsatt og endret på. (VERIS Community, 2022).



Figur. 2: Parkerian Hexad

Konfidensialitet – Referer til begrenset tilgang eller innsyn av ressurser eller data. Tap av konfidensialitet betyr at noen utenforstående har fått tilgang eller innsyn på ressurser som ellers var avgrenset. (VERIS Community, 2022)

Eierskap **–** Refererer til besittelse og kontroll over ressurser eller data. Tap av eierskap betyr at eier eller virksomhet ikke lenger har eksklusivt eierskap over ressursen eller dataen. (VERIS Community, 2022)

Integritet - Refererer til en ressurs som opprettholder sin originale form av tilstand, funksjon og innhold. Tap av integritet vil skje om ressursen blir modifisert, manipulert eller ved uautorisert tilgang. (VERIS Community, 2022)

Autentisitet – Refererer til samsvar med intensjoner, gyldighet og ærlige ressurser og data. Gyldigheten av dataen er ødelagt, det vil si urettmessig fremstillelse eller avvisning av ressurs. (VERIS Community, 2022)

Tilgjengelighet – Referer til en ressurs eller data som er klar til bruk, tilgjengelig eller til stede når det er behov for det. Tap av tilegnelig betyr at ressursen blir slettet, ødelagt, flyttet eller yter dårlig. (VERIS Community, 2022)

Nyttighet - Referer til hvor nyttig en ressurs eller data er for et formål. Tap av nyttighet er ved konvertering av data til en mindre brukelig form. Nyttighet kan også forstås ved at dataen fortsatt er til stede, men ikke brukbar lengre. For eksempel eksterne parter tukler med ressursen. (VERIS Community, 2022)

4.0 Metode

4.1 Valg av metode

«Et skille som raskt dukker opp i den samfunnsvitenskapelige metodelæren, er det mellom kvantitative og kvalitative metoder.» (Johannessen, Tufte & Christoffersen, 2016, s.27) Valg av metode bestemmer veien videre for forskningen som utrettes. Tidligere erfaringer og forskning innen samfunnsvitenskapelig metode brukes for å unngå fristelsen til å bruke fremgangsmåter som kan gi forutsatte resultater. (Johannessen et al., 2016, s.25). Med andre ord for å unngå at forskning skal gi de resultatene en ønsker. «Metode betraktes som et redskap til å skaffe seg innsikt, og man må være åpen og velge den eller de metodene som er best egnet til å besvare forskningsspørsmålene» (Johannessen et al., 2016, s.313). Denne oppgaven bruker kvantitativ metode for å løse problemstillingen som er satt. Metoden er best egent til formålet, altså redegjør dataangrep i norsk gjestfrihetsbransje.

4.1.1 Kvantitativ metode

Tallenes tale - kvantitativ metode anvender tall, i motsetning til kvalitativ metode som bruker tekst. Sentralt i kvantitativ metode er forståelsen av statistikken og talldata som er innhentet, derfor er det blitt utviklet formaliserte prosedyrer for statistikk. (Johannessen et al., 2016, s.239). Hvem som skal undersøkes defineres som enheter, enheter som svarer på en spørreundersøkelse betegnes som respondenter. (Johannessen et al., 2016, s.241)

4.2 Forskningsstrategi og design

«Når du velger problemstilling for din kvantitative bachelor eller masteroppgave, så velger du langt på vei designet for din studie samtidig» (Thrane, 2018, s.145). Forskningsdesign dreier seg om formgivning, hvor en tar utgangspunkt i forskningsspørsmålet, for å vurdere hvordan gjennomføre undersøkelse på best mulig måte fra start til slutt. (Johannessen et al., 2016, s.73).

Problemstillingen stiller spørsmål rettet mot «forekomst, svakheter og generelle effekter ved dataangrep i norsk gjestfrihetsbransje». Det er av den grunn tydelig retningen faller mot spørreundersøkelse i form av tversnittdesign. Ifølge Kvantitativ Metode, boken skrevet av Christer Thrane oppfattes survey i samfunnsfag som et eget design, men for å være mer konkret kan det kalles for en variant innen tverrsnittdesign. (Thrane, 2018, s.145) Tverrsnitts undersøkelse vil gi oss et innblikk i hvordan situasjonen er i nåtiden. «Ordet tverrsnitt kan bety flere ting, men i forbindelse med design tenker vi på flere fenomener kartlegges samtidig på tvers av en tidsakse – som et øyeblikksbilde» (Thrane, 2018, s.145).

4.2.1 Datainnsamling

«Nettbaserte spørreskjema gir forskeren stor frihet til å samle inn data fra respondenter fra hele landet (eller hele verden) uten at man trenger lokal organisering eller mange intervjuere til å gjennomføre datainnsamlingen» (Tjønndal & Fylling, 2021, s.40). Respondentene er hentet fra nettet i forhold til hva som er mest relevant, populasjonen er avgrenset til et utvalg av 187.

4.2.2 Utvalg

Undersøkelsens målgruppe, uavhengig av dens størrelse, blir ofte omtalt som populasjon i forskning. Ved noen tilfeller er det ikke nødvendig å inkludere hele populasjonen, en er derimot ute etter å undersøke et utvalg av populasjonen (Johannessen et al, 2016, s.241). Spørreundersøkelsen skal ta utgangspunkt i perspektivet til ledere og mellomledere i gjestfrihetsbransjen. Utvalgsstrategien er bekvemmelighetsutvelgelse, utvalgsstrategien går ut ifra hva som er den mest bekvemmelige formen for forskeren. (Johannessen et al, 2016, s.122.) Bekvemmelighets utvalg muliggjør tilgjengelighet. Oppgaven skal se på gjestfrihetsbransjen generelt og det er derfor ikke lagt vekt på en spesiell bransje innenfor gjestfrihetsbransjen, slik som for eksempel hotell eller flyselskap.

4.2.3 Datainnsamlingsteknikk

Denne oppgaven benytter seg av spørreundersøkelse som datainnsamlingsteknikk, teknikken blir brukt for å innhente relevant data knyttet opp til problemstillingen. Vi har valgt å bruke en internettbasert spørreundersøkelse tjeneste kalt SurveyXact. Dette er en plattform som kan brukes til å utarbeide spørreundersøkelser egnet til forskning. Forskningsverktøyet er tilrettelagt slik at det går an å legge inn respondentenes e-poster direkte. E-postene ble brukt til distribuering av invitasjon til spørreundersøkelsen. Nettsiden gir også mulighet til å laste ned datasettet som blir brukt til videre analyse.

5.0 Spørreundersøkelse

Det viktigste utgangspunktet i utformingen av spørreundersøkelsen er problemstillingen og forskningsspørsmålene. «Spørsmålene som blir framstilt er nøye utarbeidet for å innhente detaljert og konkret informasjon.» (Johannessen et al, 2016, s.262.) Spørreundersøkelsen er basert på A4 rammeverket for oppbygning av spørsmål og struktur, ettersom det er et verdifullt verktøy når det gjelder datainnsamling for dataangrep. «Det er ikke unormalt å bruke allerede eksisterende spørsmål fra spørreundersøkelser, så lenge de følger den forskningsmessige konvensjonen og kilde oppgis.» (Johannessen et al, 2016, s.262.)

Vi har systematisk samlet inn kontaktinfo til 187 potensielle respondenter fra norsk gjestfrihetsbransje, vi valgte denne mengden grunnet tid og kapasitet. Ideelt sett hadde det vært ønskelig å sende ut til alle aktører i gjestfrihetsbransjen for å få et fullstendig virkelighetsbilde. Respondentene er kategorisert slik: hotell, restaurant, utelivsbransjen, flyselskap, reisebyrå, ferje & båttransport og fornøyelsesparker. Vi opprettet en liste i Excel hvor vi samlet all kontaktinformasjon og holdt oversikt over alle de forskjellige respondentene.

Spørreundersøkelsen vil være et verktøy for oss når vi skal kartlegge data som er nødvendige for å svare på problemstillingen. Forkunnskaper og tanker rundt temaet kan være relevant for noen av spørsmålene, vi ønsker blant annet å se om det er lite investering blant virksomheter innen gjestfrihetsbransjen og om det stemmer at høy turnover og lite IKT kunnskaper kan føre til høyere sensitivitet for dataangrep i den norske bransjen, eller om bransjen i Norge er sikrere i forhold til den informasjonen vi sitter med fra forskningsartikler fra andre land. Det viktigste utgangspunktet i utformingen av spørreundersøkelsen er problemstillingen.

5.1 Oppbygning og utforming av spørreundersøkelsen

«Et spørreskjema kan være meget strukturert, det vil si ha oppgitte svaralternativer på alle spørsmålene. -Det betegnes da som et prekodet spørreskjema.» (Johannessen et al, 2016, s.263) «I tillegg kan man kombinere åpne og prekodede svar, noe som betegnes som semistrukturerte spørreskjemaer (semi betyr halv).» (Johannessen et al, 2016, s.263) Grunnlaget til spørreundersøkelsen er et semistrukturert spørreskjema. Semistrukturert spørreskjema er brukt fordi noen av spørsmålene som inngår i spørreundersøkelsen ber respondentene om å skrive ned svaret, men hovedsakelig er spørreundersøkelsen basert på prekodet spørreskjema.

Spørreundersøkelsen starter med en kort introduksjon om tema, problemstilling og et estimat på hvor lang tid respondenten sannsynligvis vil bruke på spørreundersøkelsen. Svarene til respondentene i spørreundersøkelsen er anonym, dette er oppnådd ved å ha en stor variasjon innen de forskjellige kategoriene, slik at det ikke skal være identifiserbare data, og at noen av de forskjellige virksomhetene deler noen like faktorer. I tillegg til variasjonen som er lagt inn i spørreundersøkelsen har nettsiden også et valg av å gjennomføre spørreundersøkelsen under

anonyme grunnlag. Spørsmålene i spørreundersøkelsen er bygget opp på en slik måte at de ikke skal være ledende og at de skal ha et tydelig budskap.

Spørreundersøkelsen er lagt opp på en slik måte at vi først kartlegger hvilken virksomhet det er, størrelse på virksomhet, turnover og POS system. POS og turnover er viktig å kartlegge basert på tidligere forskningsartikler innen dataangrep, og forskningsartikler som direkte oppfordrer til kartlegging av POS systemer innenfor gjestfrihetsbransjen, og for å svare på forskningsspørsmålet vi har satt som omhandler POS systemer. (Gwebu & Barrows, 2020). Videre kartlegger spørreundersøkelsen omfanget av investeringer virksomheten har gjort innen IKT og datasikkerhet. Vi ønsker med dette å finne ut om datasikkerhet er underprioritert i bransjen, og i hvilke kategorier det blir mer eller mindre investert i.

A4 Rammeverket blir brukt i spørreundersøkelsen når vi strukturerer og innhenter informasjon om dataangrep i virksomheten. Slik som hvilket dataangrep de er utsatt for, involverte aktører, effekt, og informasjon lekket. Vi ønsker også å kartlegge når dataangrepet var utført, for å se om det har blitt hyppigere i Norge.

Til slutt ønsker vi å kartlegge i hvilken grad virksomheten har satt i gang tiltak for å motvirke dataangrep, slik som datasystemer og IKT-personell. Vi ønsker å sammenligne hvor hyppig dataangrep kan være for de som har god datasikkerhet i forhold til de virksomhetene som ikke har like mange tiltak.

5.2 Prestudie

«Før skjemaet blir ferdigstilt og sendt ut, bør det gjøres en prestudie, Dette kan blant annet gjøres ved å samle en gruppe mennesker og diskutere hvilke begreper og formuleringer det er mest hensiktsmessig å bruke.» (Johannessen et al, 2016, s.276) Vi valgte å sende ut vår spørreundersøkelse til venner på studie og famille som kunne teste ut og se på hvordan spørreundersøkelsen vår var strukturert. Vi fikk flere gode tilbakemeldinger på hvordan vi burde endre spørreundersøkelsen for å gi oss best mulig flyt og sammenheng. Vi tok også tiden på oss selv, og venner for å se hvor langt tid som ble brukt på spørreundersøkelsen, slik at vi kunne gi et estimat til respondentene.

5.3 Distribusjon

«Hvis man har e-postadresser til respondentene, sendes skjemaet via e-post med en lenke som de kan klikke på slik at de får opp skjemaet. Dette betegnes som CAWI (Computer Aided Web Interviewing).» (Johannessen et al, 2016, s.277) Spørreundersøkelse er sendt direkte til ledere og mellomledere, samt generiske e-post for å nå ut til flest mulig respondenter. Disse generiske e-postene er for eksempel e-post adresse til hotellresepsjon, og de som ellers er ansvarlig for slike henvendelser. Det var flere tilfeller hvor vi ikke fant direkte e-post til ledere og mellomledere på nett og måtte utforske andre kanaler å nå frem på. De tilfellene hvor vi sendte lenken til de generiske e-postene, ba vi om at de skulle bli videresendt til nærmeste leder, eller mellomleder.

5.4 Begrensninger

Spørreundersøkelsen var ute i cirka tre uker, og ble avsluttet i slutten av april på grunn av tid og ressurser som må brukes for å analysere og se på eventuell data. Spørreundersøkelsen har hatt generelt lav respons, dette kan være av flere grunner.

Det vi opplevde når spørreundersøkelse var aktiv er blant annet respons e-post som markerte spørreundersøkelsen som søppelpost, mangel på tid eller ressurser i en travel hotell-sesong ettersom det er første sommer uten restriksjoner, og respons e-post hvor respondent ikke kan åpne lenker på grunn av datasikkerhet. Det kan også være at respondentene syntes at det var et sensitivt tema, og at flere kanskje ikke hadde et ønske om å delta. «En viktig grunn til at svarprosentene har gått drastisk ned de siste årene er ‘’overload’’, det vil si at folk utsettes for så mange spørreundersøkelser at de går lei, ønsker ikke å delta.» (Johannessen et al, 2016, s.248)

Det som kanskje var vår største utfordring, var å finne relevante e-post adresser for å finne relevante respondenter. Som nevnt tidligere måtte vi sende e-post til generiske e-post adresser for å få tak i ledere og mellomledere. Vi opplevde at når mellomledere og ledere fikk e-post direkte at det som regel var god respons. Vi valgte å ikke bruke Facebook eller LinkedIn til å innhente respondenter, fordi vi ønsket å ha noe kontroll på hvem som tok spørreundersøkelsen, selv om dette kanskje kunne betydd mer respons.

6.0 Analyse

På grunn av lite antall respondenter vil oppgaven bruke deskriptiv statistikk og krysstabeller for å se på den kvantitative dataen som er samlet. «Det som kjennetegner kvantitative metoder, er at dataen foreligger i en form som gjør at de kan telles.» For å se på dataen fra spørreundersøkelsen og forenkle det bruker vi SPSS for å analysere dataen som vi har hentet fra SurveyXact.

6.1 Respondenter

Som nevnt i tidligere i distribusjons kapittelet, distribuerte vi spørreundersøkelsen til SurveyXact gjennom en lenke ifra et utvalg av e-poster vi hadde samlet som bestod av ledere og mellomledere. Ut ifra utvalget fikk vi 9 svar totalt på vår spørreundersøkelse, vi anser dette som

lite respondenter etter gjennomført spørreundersøkelse. Grunnet lav respons er det ikke mulig å trekke noen konkrete konklusjoner. «Frafall kan føre til at resultantene du samler inn ikke avspeiler forholdene du ønsker å kartlegge, dermed blir det skjevheter i utvalget» (Eikemo & Clausen, 2007, s.21)

6.2 Univariant Analyse

Når det blir brukt spørreundersøkelse får du store mengder data som blir samlet inn i en matrise, disse tallmengdene må gjøres håndterbare og oversiktlig. Det må være mulig å forstå de forskjellige variablene, da må data forenkles. (Johannessen et al, 2016, s.279) For å forenkle dataen brukes univariant analyse, det handler om å se på hvordan enhetene fra datamatrisen fordeler seg på de forskjellige verdiene i forhold til hver enkelt variabel. (Johannessen et al, 2016, s.280)

6.2.1 Frekvenstabell

Om variabler er verdier som ikke kan rangeres, også kjent som nominalnivå, kan de presenteres i en frekvenstabell eller en grafisk figur. En grafisk figur kan eksempelvis være et stolpediagram, eller kakediagram. (Johannessen et al, 2016, s.280)

6.2.2 Sentralverdi

Det kan være relevant å finne den sentrale verdien i en fordeling, for å oppnå dette kan det brukes verktøy som gjennomsnitt, median og modus. (Johannessen et al, 2016, s.283) For å finne gjennomsnitte i dataen summeres enhetene og divideres med antall enheter, gjennomsnitt kan gi oss skjevheter i forhold til dataen. I dette tilfelle kan det brukes median for å finne det midtre. (Johannessen et al, 2016, s.284)

6.2.3 Standardavvik

Noen enheter i en datamatrise vil ha samme verdi som gjennomsnittet, men det finnes også verdier som ligger i nærheten eller lang vekk fra gjennomsnitt, dette er avvik. Det kan være interessant å finne ut hvor mye variasjon det er fra gjennomsnittet. (Johannessen et al, 2016, s.288-289) Hva er forholdsmessig standardavvik? På grunn av at standardisert avvik ikke kan bli tolket på samme måte som prosentnivå, det vil si verdier som varier fra 0-100, er det vanskeligere å definere hva som er et stort eller lite avvik fra gjennomsnittet. Det er dermed likevel nyttig å bruke når en skal sammenligne avvik fra gjennomsnittet. (Johannessen et al, 2016, s.291)

6.3 Bivariat Analyse

Når det brukes kvantitative data undersøkes sammenhengen mellom flere variabler, når det sammenlignes mellom to variabler blir det kalt for en bivariat analyse. De tre vanligste gjennomføringsmetodene når bivariat analyse blir brukt er krysstabeller, sammenlikning av gjennomsnitt og korrelasjonsanalyse. (Johannessen et al, 2016, s.295)

6.3.1 Krysstabell

Krysstabeller er sammensatt av avhengig og uavhengig variabel, også kalt for effekt og årsak. (Johannessen et al, 2016, s.298) Når variablene blir plassert i tabellen er det mulig å se den relative fordelingen, og regne frekvensene om til prosent, resultatet kan fortelle oss flere ting. Er det forskjeller, hvor stor er de eventuelle forskjellene i tabellen, har de en betydning og finner vi noen mønstre. (Johannessen et al, 2016, s.300)

6.4 Bortfallsanalyse

Usikkerhet ved bortfall i en spørreundersøkelse kan analyseres ved å gjennomføre en bortfallanalyse. Alle respondenter som er valgt ut til å delta kalles for bruttoutvalget. Derimot alle

respondenter som faktisk deltar kalles nettoutvalget, og svarrespons er nettoprosent av bruttoutvalget. (Johannessen et al, 2016, s.247)

Ifølge Tabell 1*: Brutto- & nettoutvalg* viser den at bruttoutvalget består av 187 respondenter totalt. Nettoutvalget består av 9 respondenter totalt. Det vil si at svarrespons utgjør 4,8 prosent. En svært høy svarespons vil være rundt 80-90 prosent, det er mer vanlig å få svarrespons på 30-40 prosent. Opprinnelig var ønsket svarrespons for spørreundersøkelsen rundt 40 prosent, det vil si litt under 100 respondenter. (Johannessen et al, 2016, s.247)

7.0 Resultat

I denne delen skal vi presentere resultatet av dataen vi har samlet ved bruk av analysemetodene som er nevnt ovenfor.

7.0.1 Univariat analyse av spørreundersøkelse

Vi har valgt å presentere de forskjellige spørsmålene vi mener er relevante på tross av lite antall respondenter. Dette skal presenteres i form av tabeller, spesifikt i form a stolpediagram. Det er fordi stolpediagram vil vise hvordan enhetene fordeler seg på de forskjellige variablene på en oversiktlig måte. Dataen som blir brukt for å skape stolpediagrammene har blitt hentet fra SPSS utskriftene vi har laget av dataen som er hentet fra spørreskjema. Vi har valg å kun bruke stolpediagram i vår univariate analyse. Vi har valgt å se bort ifra standardavvik og median på grunn av utregningen ikke vil gi oss verdifull data, vi har fortsatt med tabellene fra SPSS for å se på antall respondenter. Totalt sett er det 9 respondenter som har gjennomført spørreundersøkelsen, men det er 11 respondenter som har påbegynt spørreundersøkelsen. Vi tar utgangspunkt i de 9 respondentene.

7.0.1.1 Hvilken kategori ligger din virksomhet under?

Stolpediagram IV viser hvilke typer virksomheter som er med i vår spørreundersøkelse, disse blir vist i frekvens og ikke prosent, det er mer oversiktlig når det kun er 11 respondenter på spørsmålet. Selv om det er lite respondenter stemmer det overens med hvor mange hotellvirksomheter fikk spørreundersøkelsen i forhold til de andre virksomhetene i kategoriene.

7.0.1.2 Hva er størrelse på virksomheten din?

Tabell 2: Første del, viser antall som har svart på størrelse på virksomheten til respondenten, det er kun micro, liten og stor som er med og ingen av virksomhetene var av størrelse medium. Det er 45 prosent av respondentene som har svart at de tilhører en stor virksomhet med over 250 ansatte, mens det er likt fordelt på micro og liten.

7.0.1.3 Hva går virksomheten din under?

Dette spørsmålet handler om hvilken type virksomhet det er, og det er hovedsakelig virksomheter som er under et moderselskap.

7.0.1.4 Prosentvis turnover

Tabell 6 Turnover: Det er variasjon i besvarelsen på dette spørsmålet. Verdiene varier fra 8-40 prosent. I tillegg viser Stolpediagram V prosentvis gjennomtrekk.

7.0.1.5 Hvilket POS System benytter din virksomhet?

Spørsmålet kartlegger de forskjellige virksomhetenes POS System, dette spørsmålet ville vært mer relevant dersom vi hadde hatt et stort antall respondenter. Vi kan se at alle respondentene har svart forskjellig i forhold til hverandre.

7.0.1.6 Når var sist gang din virksomhet oppdaterte sin infrastruktur?

Spørsmålet kartlegger sist gang virksomheten oppdaterte sin teknologiske infrastruktur, vi kan se at 66 prosent av respondentene oppdaterte sin teknologiske infrastruktur innen de siste 5 månedene. 1 av respondentene visste ikke sist gang de oppdaterte.

7.0.1.7 Hvor mye har din bedrift investere i utvikling av teknologiske infrastruktur de siste 2 årene?

Dataen forteller oss hvor mye som ble investert av respondentens virksomhet de siste 2 årene, det samme gjelder her som i forrige spørsmål og 66 prosent svarte at de har investert over 150000 NOK i teknologisk infrastruktur. Det er 10 respondenter.

7.0.1.8 Dataangrep

Neste del av spørreundersøkelsen handlet om dataangrep, denne delen var kun tilgjengelig til respondenter som besvarte ja til at de har opplevd dataangrep. I spørreundersøkelsen var det kun to respondenter som har opplevd dataangrep i sin virksomhet (se Tabell 3: Andre del). Ut ifra besvarelsene kan vi se at dataangrepet har forekommet i løpet av de to siste årene. Det nyligste dataangrepet skjedde i 2022. Dataen viser også at det er stor spredning av effekten dagangrepet har hatt på virksomheten, fra distraherende for daglig drift til ingen effekt. Av de to respondentene, viser svaret at begge ble utsatt for eksterne krefter ved dataangrepet. Ingen av respondentene besvarer ja til at data var lekket. Videre viser dataen fra Stolpediagram III omfanget påvirkning fra dataangrep, altså liten påvirkning.

7.0.1.9 Omfang av IKT og fremtidig sikring

Dataen viser oss at respondentene er nøytrale eller sikret fra stor til svært stor grad, det er bare en respondent som ikke føler seg sikret mot fremtidige dataangrep. 7 av respondentene har dedikert IKT-personell i form av tredjepart eller eget, mens en av respondenter har daglig leder som IKT-

ansvarlig. Spørsmålet som kartlegger tiltak virksomheter har iverksatt har flervalgs muligheter. 55,5 prosent av respondentene har IKT-personell. 22,2 prosent har opplæring av ansatte som et tiltak. 44,4 prosent har gjennomført risikoanalyse av IT-systemer. 66,6 prosent sikrer lagring av data. 44,4 prosent har interne systemer. 22,2 prosent har fysisk sperre fra datarom og servere. Til slutt 33,3 prosent har digital sperre fra systemer for uvedkommende (passord m.m).

7.0.2 Bivariat analyse av spørreundersøkelse

Selv om vi har lavt antall respondenter ønsker vi å utforske forskningsspørsmål. For å gjøre dette bruker vi bivariat analyse i form av krysstabell. Forskningsspørsmålene vi tar utgangspunkt i er

1. Har høy turnover effekt på dataangrep i norsk gjestfrihets bransje
2. Er datasikkerhet en prioritering i din bedrift

7.0.2.1 Krysstabell 1

Krysstabell 1 Vedlegg III ser på forholdet mellom «Omfanget av IKT-personell i din virksomhet» og «I hvilken grad er din bedrift sikret mot fremtidig dataangrep?». I Krysstabell 1 fra Vedlegg II kan vi se i krysstabellen er at det er flest som har svart stor grad i forhold til omfang, og disse har tredjeparts IKT-personell.

7.0.2.2 Krysstabell 2

I Krysstabell 2 Vedlegg III ser på forholdet mellom «Hva er prosentvis turnover (gjennomtrekk) av ansatte i din virksomhet» og «I hvilken grad er din bedrift sikret mot fremtidig dataangrep?». Det vi ser er at det er stor spredning i turnover ut ifra besvarelsen til 7 respondenter totalt, og at det ikke er mulig å slå fast noen sammenheng mellom de to variablene.

8.0 Diskusjon

I diskusjonsdelen ønsker vi å sammenligne den eksisterende kunnskapen med resultatet vi fikk fra spørreundersøkelsen. Problemstillingen som oppgaven hadde som mål å utforske var: *"Forekomst, svakheter og generelle effekter ved dataangrep i norsk gjestfrihetsbransje".*

Første del av problemstillingen lyder slik, forekomst av dataangrep i gjestfrihets bransjen. Ut ifra spørreundersøkelsen finner vi ut at det er to respondenter som har opplevd dataangrep i nærmeste fortid. Resultat er interessant, på tross av få respondenter er det faktisk to som har blitt utsatt for dataangrep. Likevel, dette forteller oss ingenting om virkelighetens trusselbilde i Norge, mer spesifikt forekomst i norsk gjestfrihets bransje. Omfattende analyser, som årsrapport fra NSM og NHO perspektiv melding, viser tydelig hva som er virkeligheten for norske virksomheter i dag. En står ovenfor en massiv utvikling og digitalisering som har resultert i en tredobling av alvorlige digitale hendelser fra 2019 til 2020. Likevel forteller det oss ikke konkret hvordan det står til med forekomst av dataangrep i gjestfrihetsbransjen. Det kan tenkes at det er mange mulige grunner til at det er utfordrende å få et helhetlig bilde av forekomst. Blant annet viser tidligere forskning at det er mange dataangrep som går under radaren, virksomheten er ikke klar over at de har blitt utsatt for overtredelse i det digitale rom. (Chen & Fiscus, 2018)

Tidligere forskning viser at det kan være flere svakheter som er knyttet til teknologisk infrastruktur. Med teknologisk infrastruktur mener vi IKT, og andre digitale systemer som for eksempel POS. Ved tilstrekkelig utvalg ville en krysstabell blitt brukt for å utforske om turnover eller POS system påvirker datasikkerheten i en bedrift, men krysstabellene vi har foretatt i resultat var ikke tilstrekkelig grunnet lite representert utvalg. Gjestfrihetsbransjen har også som

svakhet at de kan falle offer for sosial utnyttelse, grunnet lite opplæring av ansatte. Ytterligere er gjestfrihetsbransjen preget av høy turnover. Teorien forteller oss at høy turnover kan føre til generell lav IKT kompetanse blant nyansatte. Under disse forholdene risikerer virksomheter å bli eksponert for uønskede hendelser.

Neste del av problemstillingen handler om generelle effekter ved dataangrep. Med effekter mener vi hvordan dataangrep påvirker en virksomhet. En virksomhet kan risikere at ressursene de har mister attributtene sine, det kan bli kostbart og gå ut over daglig drift. Først og fremst kan konfidensialitet og eierskap til informasjon og data bli kompromittert, som resulterer i at virksomheten ikke får tilgang til sine egne ressurser og data eller bli totalt utelukket. Direkte utestengelse er ofte brukt når kriminelle grupper stenger av informasjon og presser virksomheten til å «kjøpe» den tilbake. Eksempelvis var dette tilfelle når Nordic Choice ble utsatt for data angrep i desember 2021. For det andre kan integriteten og autentisitet til ressursene bli påvirket, av den forstand at ressursen blir manipulert eller gyldigheten av data blir ødelagt. Til slutt kan nyttigheten og tilgjengelighet bli påvirket. Med andre ord ressursen er ikke klar til bruk når det er behov for det eller at den ikke er brukbar.

Sikring av IKT omfanget som følge av digitalisering har over lengre tid ikke vært tilstrekkelig. Gjestfrihetsbransjen sitter på store mengder sensitiv informasjon og bruker den til å skreddersy opplevelser, spesialisere produkter og daglig drift. Bransjen har som følge av dette et stort ansvar for å opprettholde sikkerhet for forbrukerens data, og interne systemer. Direkte konsekvens av disse forholdene har sørget for at personvernlovverk GDPR har blitt opprettet, noe som er et steg i riktig retning. Likevel er det viktig å belyse nåværende og fremtidige etiske dilemmaer knyttet

til sensitiv informasjon. Det er helt essensielt for bedrifter i gjestfrihetsbransjen å håndtere ulike former for informasjon. Derfor er det viktig med gode lovverk og reguleringer.

1. Har høy turnover effekt på dataangrep i norsk gjestfrihetsbransjen?
2. Er datasikkerhet en prioritering i den norske gjestfrihetsbransjen?

Videre for å ta utgangspunkt og besvare forskningsspørsmålene ser vi først og fremst stor variasjon i besvarelsene fra spørreundersøkelsen. Denne informasjonen kan vi ikke trekke konklusjoner ut ifra. Derimot forteller litteratur at det finnes direkte korrelasjoner mellom høy turnover og forhøyet risiko for dataangrep. Viser til Gwebu & Barrows som sier at høy turnover fører til utilstrekkelig datakompetanse blant ansatte. Att på til viser besvarelser fra de fleste respondentene at de er klar for fremtidig dataangrep, og at det er relativt høy investering i teknologi. Det er vanskelig å lage et estimat på hva som er høy investering, på grunn av at det varier ut ifra størrelse og økonomi til bedriften en tar utgangspunkt i. Respondentene har et høyt antall forebyggende IKT løsninger mot et fremtidig dataangrep. Vi vil trekke frem at Nasjonal Sikkerhetsmyndighet meddeler at de fleste norske bedrifter er i økende grad mer sikkerhetsbevisste. Likevel er de som blir utsatt for digitale hendelser ikke godt nokk rustet. I den forstand at virksomheten hverken har tilstrekkelig forebyggende tiltak, kompetanse, kapasitet til å avdekke, håndtere eller begrense skadeomfang ved dataangrep. (Nasjonal Sikkerhetsmyndighet, 2020)

Som nevnt tidligere er det svært lite forskning rundt temaet i norsk gjestfrihetsbransje, ved hjelp av en større og mer omfattende undersøkelse kunne svarene gitt oss rikere informasjon, som for eksempel en bransjestandarder.

9.0 Konklusjon

Den teknologiske utvikling går raskere enn noen gang, og det er helt avgjørende for gjestfrihetsbransjen å delta for å kunne konkurrere. Medfølgende av denne utviklingen har gjestfrihetsbransjen et stort ansvar som de nå står ovenfor. Videre vil det være kritisk å ta vare på og sikre sensitiv informasjon, og etterretter lovverk og styringsrett. På grunn av bacheloroppgavens omfang og begrensning har vi ikke klart å samle inn ønsket data, likevel har vi undersøkt flere internasjonale forskningsartikler. Samtidig satt søkelyset på det digitale risikobilde i Norge i dag. Informasjonen som er belyst kan være svært nyttig for norsk gjestfrihetsbransje.

10.0 Kildekritikk

Når vi har forsket på dette temaet har vi funnet mye om det norske risikobilde innen datasikkerhet, men det har ikke vært noe som spesifikke forskningsartikler som omhandlet datasikkerhet innenfor gjestfrihetsbransjen i Norge. Det vi har funnet er en rekke norske nyhetsartikler som handler om temaet, men dette er ikke nok grunnlag til å danne et fullstendig bilde. På grunn av dette har det vært viktig for oss å være kritisk til de kildene vi har innhentet.

Vi har hatt et ønske om at de kildene vi innhenter som omhandler datasikkerhet og dataangrep i gjestfrihetsbransjen er troverdige, og vi har hovedsakelig forskningsartikler som er fagfellevurdert. Det er verdt å nevne at oppgaven mangler kilder som stiller seg kritisk til at digitalisering øker sårbarhet, på grunnlag av at vi ikke har kommet over slike artikler i vår forskning.

Litteraturliste

Arbeidstilsynet. (2022). Risikovurdering. Hentet fra Risikovurdering (arbeidstilsynet.no)

BBC. (2020, 30.oktober) Marriot Hotels fined £18.4m for data breach that hit millions. Hentet fra https://www.bbc.com/news/technology-54748843

Bjørshol, E. (2018, 06.februar). Undervurderer cyber-trusselen. *Horeca*. Hentet fra Undervurderer cyber-trusselen (hotellmagasinet.no)

Chen, & Fiscus, J. (2018). The inhospitable vulnerability. *Journal of Hospitality and Tourism Technology*, *9*(2), 223–234. https://doi.org/10.1108/JHTT-07-2017-0044

Chon, K., & Maier, T. (2010). Welcome to hospitality: ... an introduction (3rd ed.). Clifton Park, N.Y: Delmar.

Det Norske Akademis Ordbok (2022) Turnover. Hentet fra https://naob.no/ordbok/turnover

Det Norske Akademis Ordbok (2022) Atributt. Hentet fra attributt - Det Norske Akademis ordbok (naob.no)

Drexler, N., & Lapré, V. B. (2019). For better or for worse: Shaping the hospitality industry through robotics and artificial intelligence. Research in Hospitality Management, 9(2), 117-120. Hentet fra For better or for worse: Shaping the hospitality industry through robotics and artificial intelligence: Research in Hospitality Management: Vol 9, No 2 (tandfonline.com)

Dwesini, N. F. (2019). Causes and prevention of high employee turnover within the hospitality industry: A literature review. African Journal of Hospitality, Tourism and Leisure, 8(3), 1-15. Hentet fra article_38_vol_8_3__2019.pdf (ajhtl.com)

Eikemo, T., & Clausen, T. (2012). Kvantitativ analyse med SPSS: En praktisk innføring i kvantitative analyseteknikker (2. utg. ed.). Trondheim: Tapir akademisk forl.

Einstabland, N. K. (2018) Fra kaos til GDPR compliant - noen praktiske håndgrep. Praktisk økonomi Og Finans, (3), 214-225.Hentet fra https://www.idunn.no/doi/10.18261/issn.1504-2871-2018-03-05

European Community Commission. (2003). Recommendation concerning the definition of micro, small and medium-sized enterprises. Official Journal of the European Union, (l124/36). Hentet fra https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361&from=EN

Jaimes, J., Erdem, M., Chen, C., Doyle, B. (2019). An Assessment of Generation Z's Preferences for Guest-Facing Hotel Technologies. Journal of Hospitality, 1(3-4), 162-171. Hentet fra https://digitalscholarship.unlv.edu/hotel_fac_articles/446

Gundersen, M., Lied H., Thommessen K. J. (2021) Nordic Choice-Angrepet: hackere har lekket informasjon om ansatte. *NRK*. Hentet fra https://www.nrk.no/norge/nordic-choice-angrepet_-hackere-har-lekket-informasjon-om-ansatte-1.15773222

Gursli-Berg, G. & Rosvold, K. A. (2021) Teknologi. Store Norske Leksikon. Hentet fra https://snl.no/teknologi

Gwebu, K., & Barrows, C. (2020). Data breaches in hospitality: Is the industry different? *Journal of Hospitality and Tourism Technology*, *11*(3), 511-527. Hentet fra https://www.emerald.com/insight/content/doi/10.1108/JHTT-11-2019-0138/full/html

Innovasjon Norge (2021) *Nasjonal reiselivsstrategi 2023.* Hentet fra https://assets.simpleviewcms.com/simpleview/image/upload/v1/clients/norway/Nasjonal_Reiselivsstrategi_2021_1__2a784ce5-7b8f-438d-a40b-65a68707dff5.pdf?fbclid=IwAR11PVzZLPfqiYWufyrjMOJtLD_FeeVINkCCf3Mg776Wi0OBGyZF9t7oeu0

Jaimes, J., Erdem, M., Chen, C. C., & Doyle, B. (2019). An assessment of generation Z's preferences for guest-facing hotel technologies. Journal of Hospitality, 1(3-4), 162. Hentet fra https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1445&context=hotel_fac_articles

Mariott International. (2018). Marriott Announces Starwood Guest Reservation Database Security Incident. Hentet fra https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

Mark, M., Tømte, C., Næss, T., & Røsdal, T. (2019). Leaving the windows open - økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk Sosiologisk Tidsskrift, 3*(3), 173-190.. https://doi.org/10.18261/issn.2535-2512-2019-03-02

Moon, Y., Kim, W., & Ham, S. (2014). Users' intentions to employ a Point-Of-Sale system. *The Service Industries Journal, 34*(11), 901-921. Hentet fra Full article: Users' intentions to employ a Point-Of-Sale system (tandfonline.com)

Nasjonal Sikkerhetsmyndighet. (2020). *Nasjonalt cybersikkerhetssenter - en del av NSM.* Hentet fra https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/det-digitale-risikobildet/nasjonalt-cybersikkerhetssenter-en-del-av-nsm/

Nasjonal Sikkerhetsmyndighet. (2021) *Nasjonalt digitalt risikobilde 2021.* Hentet fra Nasjonalt digitalt risikobilde 2021 - Nasjonal sikkerhetsmyndighet (nsm.no)

Nordic Choice Hotels. (2021) Oppdatering 6. desember om virusangrepet på Nordic Choice Hotels' IT-systemer. Hentet fra https://www.nordicchoicehotels.no/presse/#/pressreleases/oppdatering-6-desember-om-virusangrepet-paa-nordic-choice-hotels-it-systemer-3149122

NOU 2015:13 (2015) Digital sårbarhet – sikkert samfunn, Justis- og beredskapsdepartementet. Hentet fra https://www.regjeringen.no

Næringsliv Hovedorganisasjon. (2018) Verden og oss. Næringslivets perspektivmelding 2018. Hentet fra https://www.nho.no/publikasjoner/p/naringslivets-perspektivmelding/digitalisering/?fbclid=IwAR2VSP-d-t8RD-BBeMcVDI1cT0ej4zB4zPg5349a0VGCg-zSeYq5Idd8_j0

Pettersen, L. (2018) Digitalisering. Norsk medietidsskrift, 25 (4), 1-17. doi: 10.18261/ISSN.0805-95352018-04-03. Hentet fra Digitalisering: Modernitetens flyttebyrå: NMT: Vol 25, No 4 (idunn.no)

Skaug, L. J. H. (2022, 23.mars) Risikobilde i den digitale verden. [Blogginnlegg]. Hentet fra Risikobildet i den digitale verden (habberstad.no)

Thrane, C. (2018). Kvantitativ metode: En praktisk tilnærming. Oslo: Cappelen Damm akademisk.

Tjønndal, A., & Fylling, I. (2021). Digitale forskningsmetoder (1. utgave. ed., Forskningsmetoder). Oslo: Cappelen Damm akademisk.

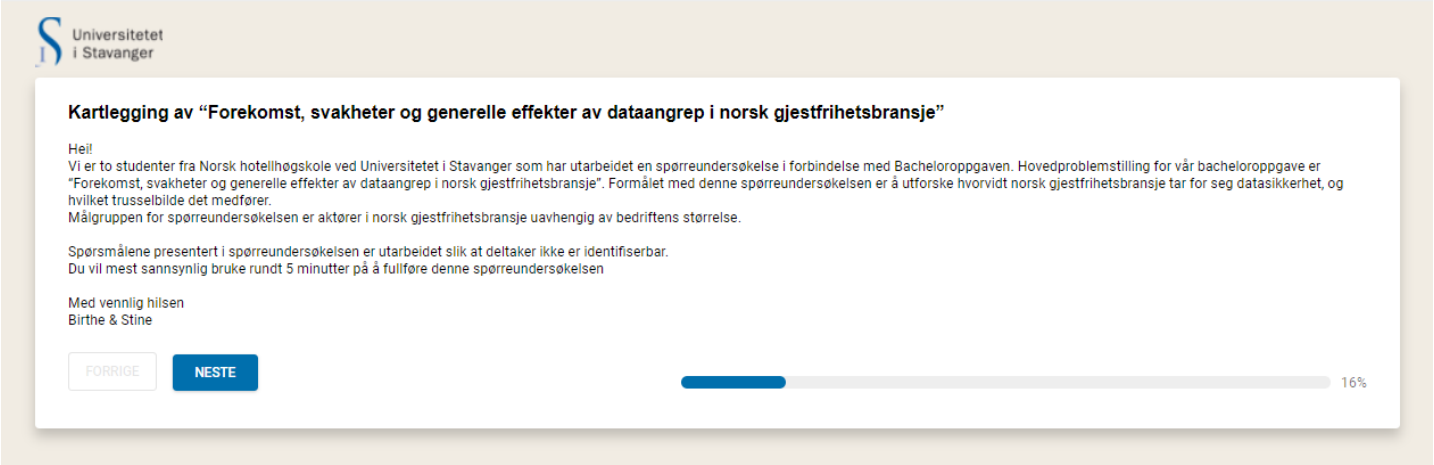
VERIS Community (2022) Veris. Hentet fra http://veriscommunity.net/index.html

Yallop, A., & Seraphin. H. (2020) Big data and analytics in tourism and hospitality: Opportunities and risks. *Journal of Tourism Futures, 6*(3), 257-262. Hentet fra Big data and analytics in tourism and hospitality: opportunities and risks | Emerald Insight

Zsarnoczky, M. (2018). The Digital Future of the Tourism & Hospitality Industry. Boston Hospitality Review. 6. Hentet fra https://www.researchgate.net/profile/Martin-Zsarnoczky/publication/325989297_The_Digital_Future_of_the_Tourism_Hospitality_Industry/links/5b32220f0f7e9b0df5cbf032/The-Digital-Future-of-the-Tourism-Hospitality-Industry.pdf

Vedlegg

Vedlegg I, side 1: Spørreundersøkelse



Universitetet i Stavanger

Kartlegging av "Forekomst, svakheter og generelle effekter av dataangrep i norsk gjestfrihetsbransje"

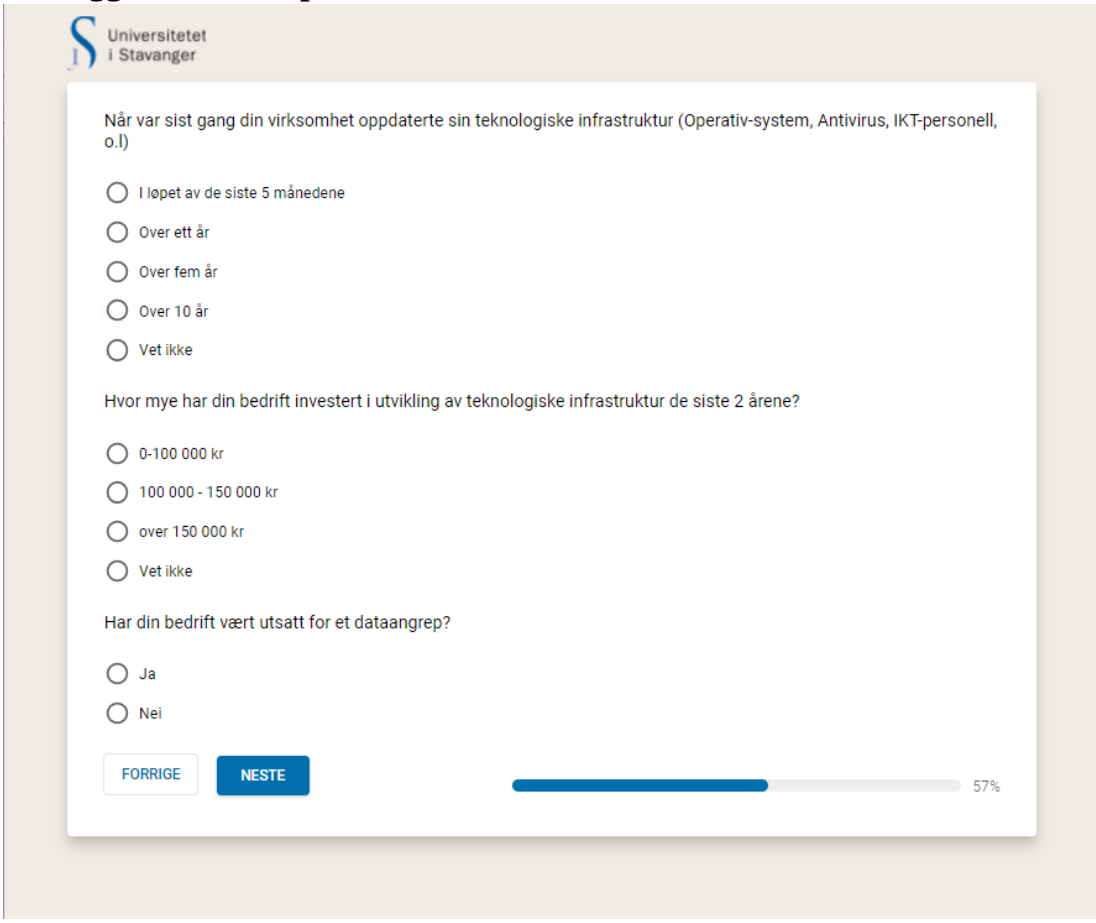
Hei!
Vi er to studenter fra Norsk hotellhøgskole ved Universitetet i Stavanger som har utarbeidet en spørreundersøkelse i forbindelse med Bacheloroppgaven. Hovedproblemstilling for vår bacheloroppgave er "Forekomst, svakheter og generelle effekter av dataangrep i norsk gjestfrihetsbransje". Formålet med denne spørreundersøkelsen er å utforske hvorvidt norsk gjestfrihetsbransje tar for seg datasikkerhet, og hvilket trusselbilde det medfører.
Målgruppen for spørreundersøkelsen er aktører i norsk gjestfrihetsbransje uavhengig av bedriftens størrelse.

Spørsmålene presentert i spørreundersøkelsen er utarbeidet slik at deltaker ikke er identifiserbar.
Du vil mest sannsynlig bruke rundt 5 minutter på å fullføre denne spørreundersøkelsen

Med vennlig hilsen
Birthe & Stine

FORRIGE NESTE 16%

Vedlegg II, side 2: Spørreundersøkelse



Universitetet i Stavanger

Når var sist gang din virksomhet oppdaterte sin teknologiske infrastruktur (Operativ-system, Antivirus, IKT-personell, o.l)

- I løpet av de siste 5 månedene
- Over ett år
- Over fem år
- Over 10 år
- Vet ikke

Hvor mye har din bedrift investert i utvikling av teknologiske infrastruktur de siste 2 årene?

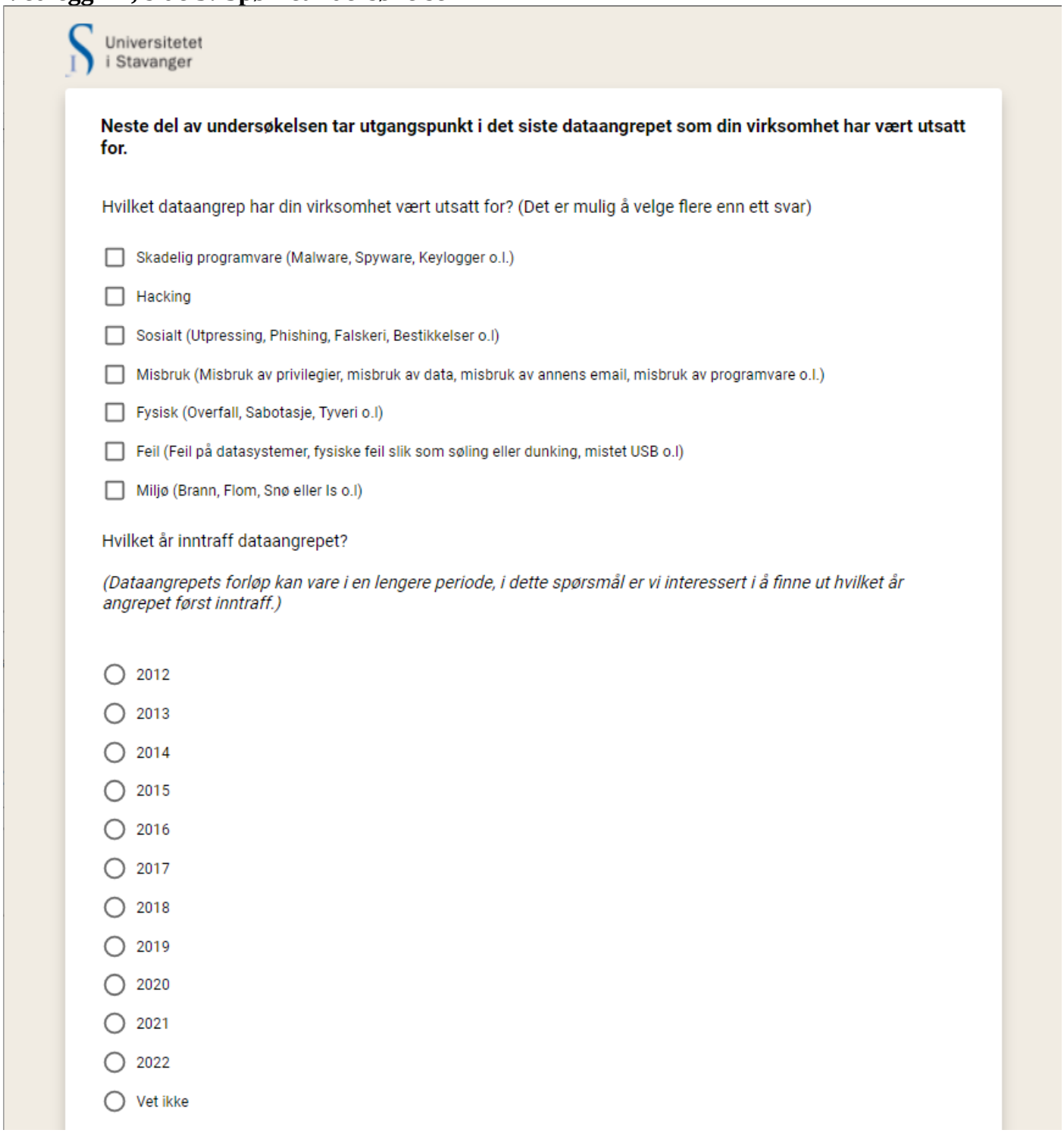
- 0-100 000 kr
- 100 000 - 150 000 kr
- over 150 000 kr
- Vet ikke

Har din bedrift vært utsatt for et dataangrep?

- Ja
- Nei

FORRIGE NESTE 57%

Vedlegg III, side 3: Spørreundersøkelse



Universitetet i Stavanger

Neste del av undersøkelsen tar utgangspunkt i det siste dataangrepet som din virksomhet har vært utsatt for.

Hvilket dataangrep har din virksomhet vært utsatt for? (Det er mulig å velge flere enn ett svar)

- [ ] Skadelig programvare (Malware, Spyware, Keylogger o.l.)
- [ ] Hacking
- [ ] Sosialt (Utpressing, Phishing, Falskeri, Bestikkelser o.l)
- [ ] Misbruk (Misbruk av privilegier, misbruk av data, misbruk av annens email, misbruk av programvare o.l.)
- [ ] Fysisk (Overfall, Sabotasje, Tyveri o.l)
- [ ] Feil (Feil på datasystemer, fysiske feil slik som søling eller dunking, mistet USB o.l)
- [ ] Miljø (Brann, Flom, Snø eller Is o.l)

Hvilket år inntraff dataangrepet?

(Dataangrepets forløp kan vare i en lengere periode, i dette spørsmål er vi interessert i å finne ut hvilket år angrepet først inntraff.)

- ○ 2012
- ○ 2013
- ○ 2014
- ○ 2015
- ○ 2016
- ○ 2017
- ○ 2018
- ○ 2019
- ○ 2020
- ○ 2021
- ○ 2022
- ○ Vet ikke

Vedlegg IIII, side 3: Spørreundersøkelse

Hvilke aktører var involvert?

- ○ Interne aktører (Ansatte)
- ○ Eksterne aktører (Tidligere ansatte, gjester, kriminelle grupper o.l)
- ○ Tredjeparts aktører (Leverandører, out-sourcing o.l)
- ○ Vet ikke

Hva var effekten av dataangrepet?

- ○ Ingen effekt
- ○ Distraherende for daglig drift
- ○ Gikk hardt utover daglig drift
- ○ Skadelig for virksomhet (inntekt m.m.)
- ○ Vet ikke

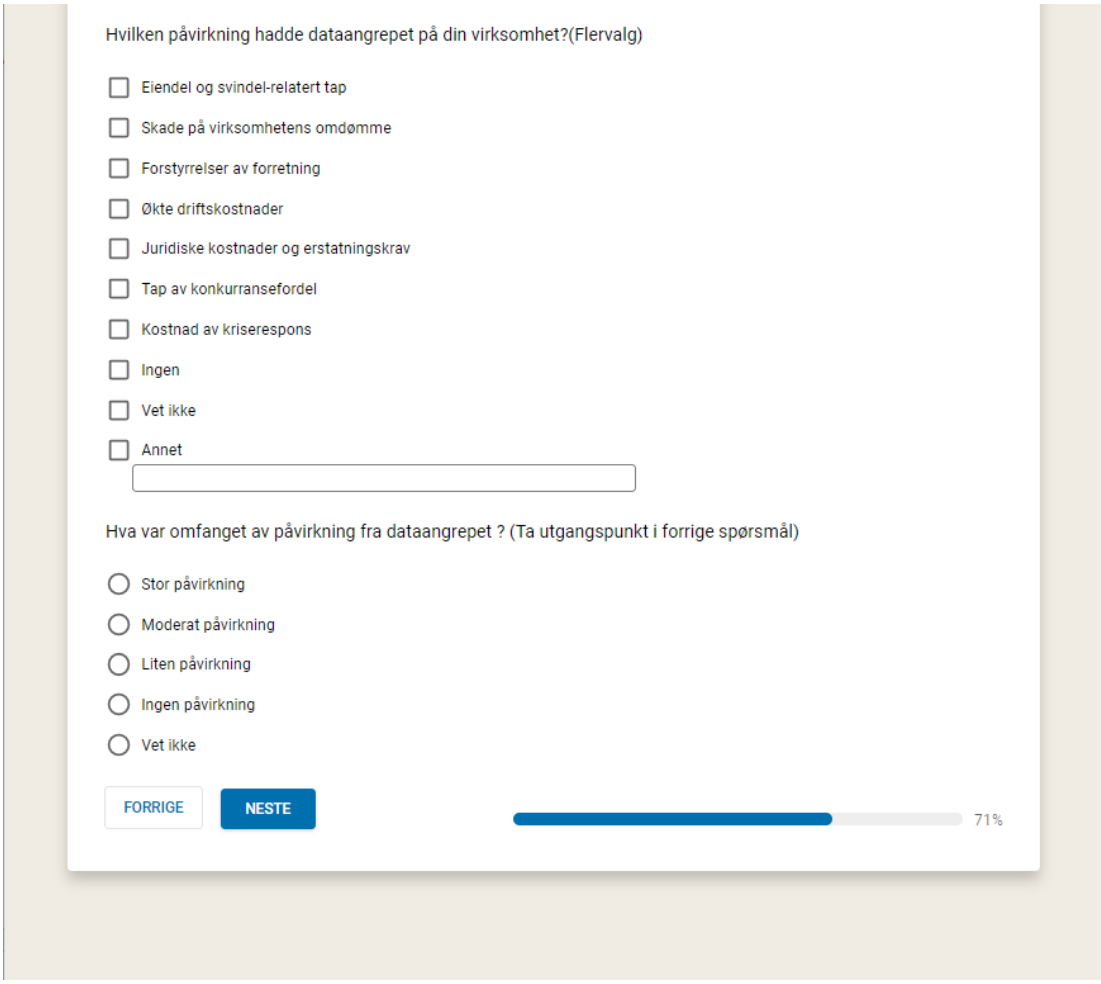
Ble informasjon lekket under dataangrepet?

- ○ Ja
- ○ Nei
- ○ Vet ikke

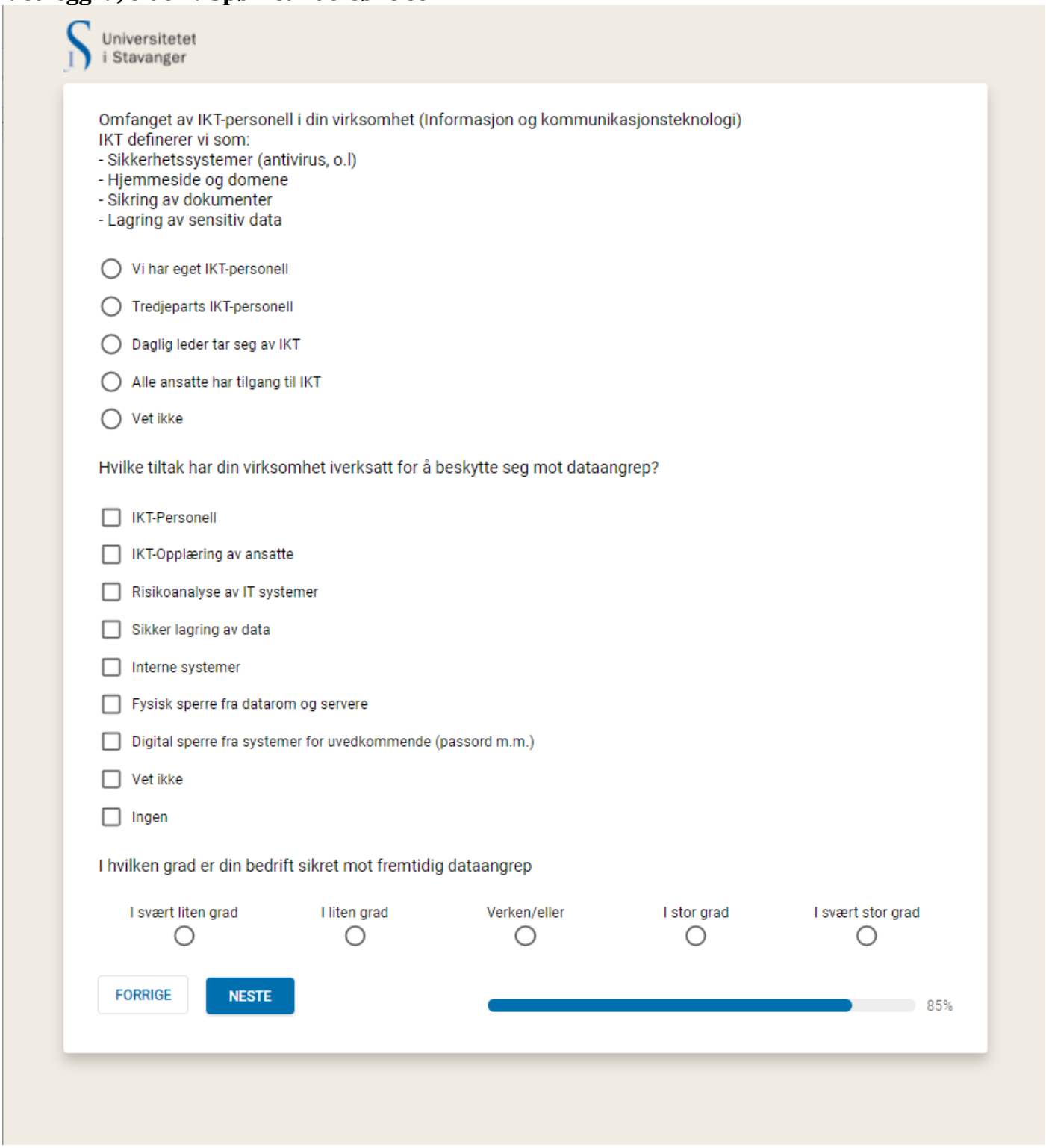
Hvilken informasjon ble lekket? (Flervalg)

- ☐ Sensitiv informasjon
- ☐ Ikke sensitiv informasjon
- ☐ Informasjon om ansatte
- ☐ Informasjon om gjester
- ☐ Økonomisk informasjon
- ☐ Ingen informasjon
- ☐ Vet ikke

Vedlegg IV, side 3: Spørreundersøkelse



Vedlegg V, side 4: Spørreundersøkelse



Universitetet i Stavanger

Omfanget av IKT-personell i din virksomhet (Informasjon og kommunikasjonsteknologi)
IKT definerer vi som:
- Sikkerhetssystemer (antivirus, o.l)
- Hjemmeside og domene
- Sikring av dokumenter
- Lagring av sensitiv data

- ○ Vi har eget IKT-personell
- ○ Tredjeparts IKT-personell
- ○ Daglig leder tar seg av IKT
- ○ Alle ansatte har tilgang til IKT
- ○ Vet ikke

Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep?

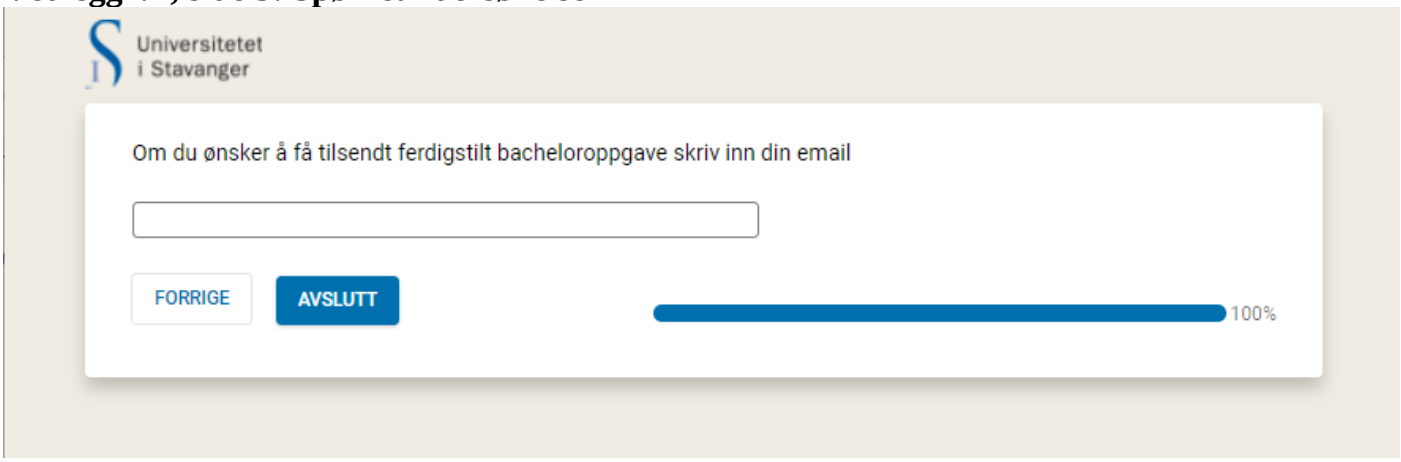
- ☐ IKT-Personell
- ☐ IKT-Opplæring av ansatte
- ☐ Risikoanalyse av IT systemer
- ☐ Sikker lagring av data
- ☐ Interne systemer
- ☐ Fysisk sperre fra datarom og servere
- ☐ Digital sperre fra systemer for uvedkommende (passord m.m.)
- ☐ Vet ikke
- ☐ Ingen

I hvilken grad er din bedrift sikret mot fremtidig dataangrep

I svært liten grad	I liten grad	Verken/eller	I stor grad	I svært stor grad
○	○	○	○	○

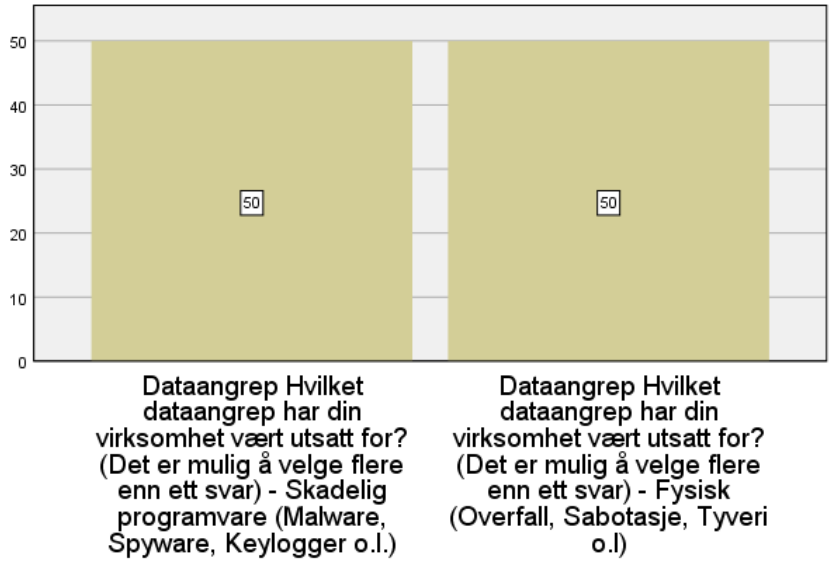
FORRIGE NESTE 85%

Vedlegg VI, side 5: Spørreundersøkelse

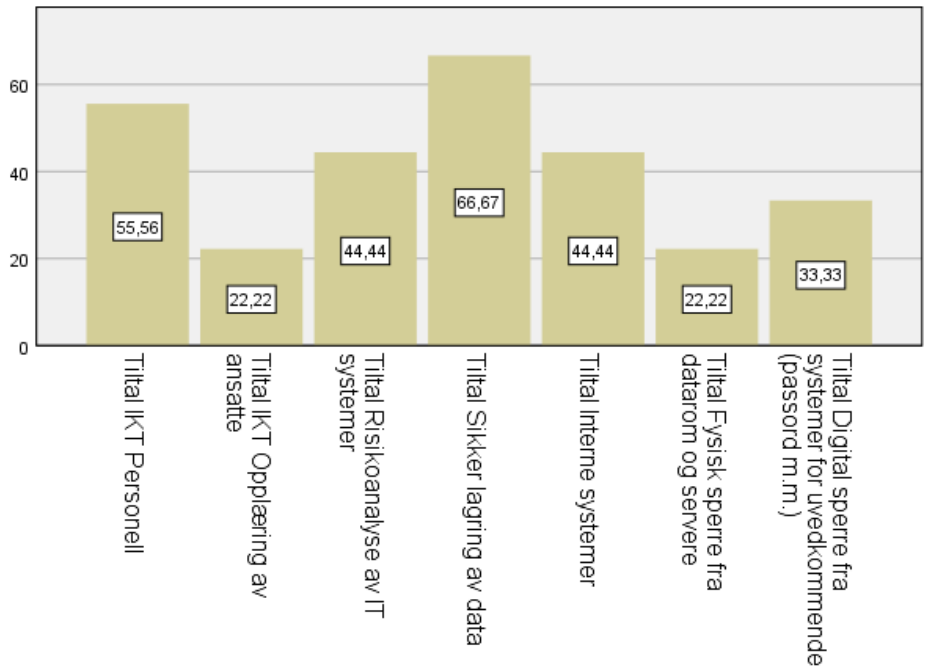


Stolpediagram

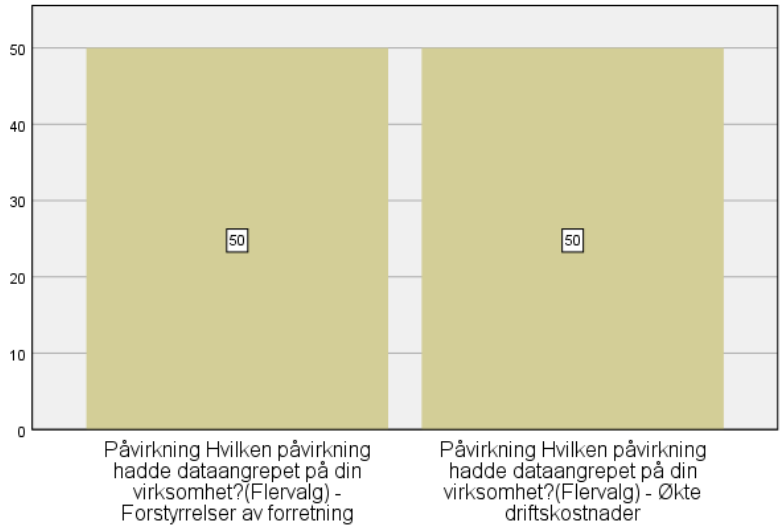
Stolpediagram I: Hvilket dataangrep har din virksomhet vært utsatt for? (Det er mulig å velge flere enn ett svar)



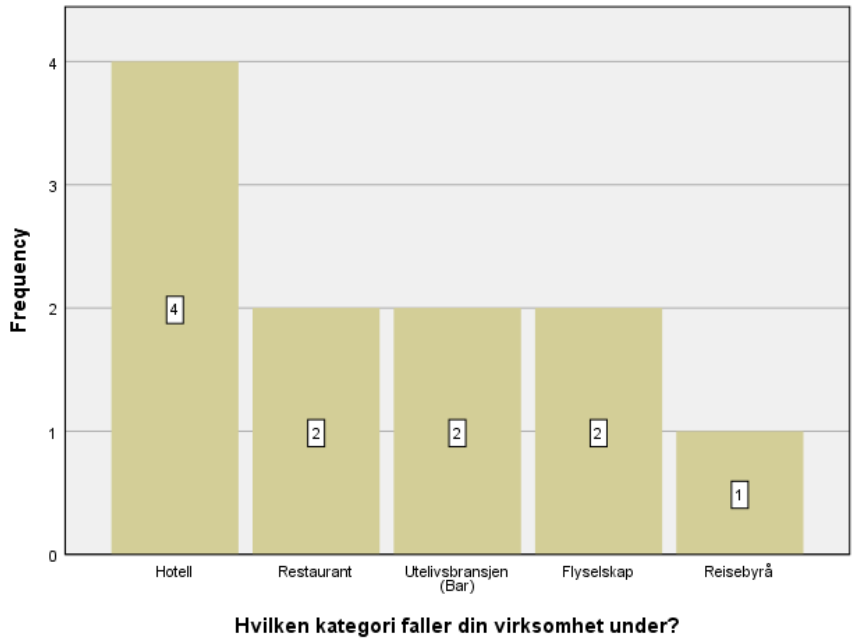
Stolpediagram II: Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep?



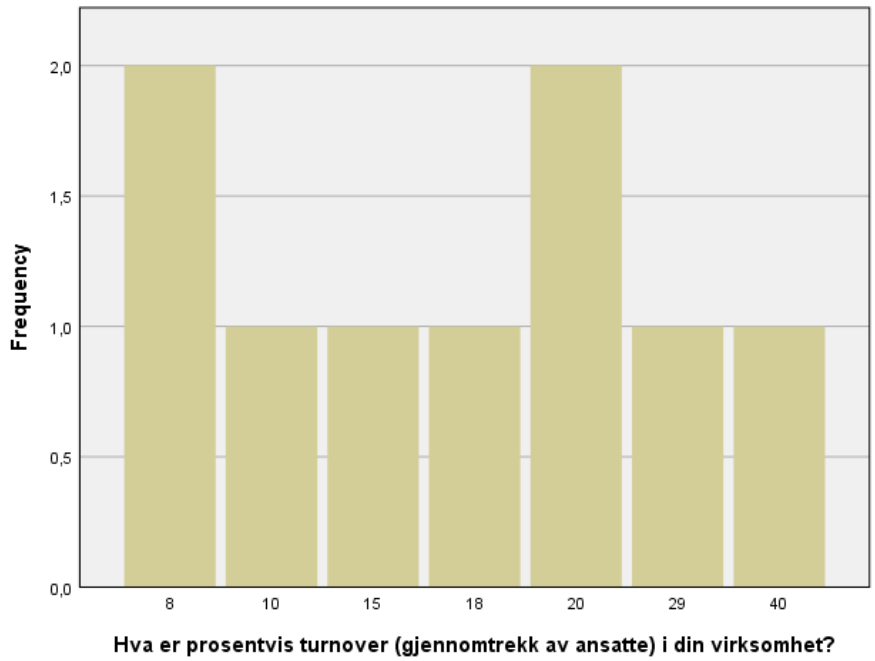
Stolpediagram III: Hvilken påvirkning hadde dataangrepet på din virksomhet?



Stolpediagram IV: Hvilken kategori faller din virksomhet under?



Stolpediagram V: Hva er prosentvis gjennomtrekk i din virksomhet?



Tabell

Tabell 1: Brutto- & nettoutvalg

Samlet status - Gjennomført

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ikke valgt	178	95,2	95,2	95,2
	Valgt	9	4,8	4,8	100,0
	Total	187	100,0	100,0	

Tabell 2: Første del

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Hvilken kategori faller din virksomhet under?	11	1	5	2,45	1,440
Hva er størrelsen på virksomheten din?	11	1	4	2,64	1,362
Hva går virksomheten din under?	11	1	3	1,82	,603
Hva er prosentvis turnover (gjennomtrekk av ansatte) i din virksomhet?	9	8	40	18,67	10,500
Når var sist gang din virksomhet oppdaterte sin teknologiske infrastruktur (Operativ-system, Antivirus, IKT-personell, o.l)	10	1	5	1,80	1,317
Hvor mye har din bedrift investert i utvikling av teknologiske infrastruktur de siste 2 årene?	10	1	4	2,80	1,033
Har din bedrift vært utsatt for et dataangrep?	10	1	2	1,70	,483
Valid N (listwise)	8				

Tabell 3: Andre del (Dataangrep)

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Hvilket år inntraff dataangrepet? (Dataangrepets forløp kan vare i en lengere periode, i dette spørsmål er vi interessert i å finne ut hvilket år angrepet først inntraff.)	2	9	11	10,00	1,414
Hvilke aktører var involvert?	2	2	2	2,00	,000
Hva var effekten av dataangrepet?	2	1	3	2,00	1,414
Hva var omfanget av påvirkning fra dataangrepet ? (Ta utgangspunkt i forrige spørsmål)	2	3	3	3,00	,000
Ble informasjon lekket under dataangrepet?	2	2	2	2,00	,000
Valid N (listwise)	2				

Tabell 4: Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep?

$Tiltak Frequencies

		Responses		Percent of Cases
		N	Percent	
Tiltak[a]	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - IKT-Personell	5	19,2%	55,6%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - IKT-Opplæring av ansatte	2	7,7%	22,2%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - Risikoanalyse av IT systemer	4	15,4%	44,4%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - Sikker lagring av data	6	23,1%	66,7%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - Interne systemer	4	15,4%	44,4%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - Fysisk sperre fra datarom og servere	2	7,7%	22,2%
	Hvilke tiltak har din virksomhet iverksatt for å beskytte seg mot dataangrep? - Digital sperre fra systemer for uvedkommende (passord m.m.)	3	11,5%	33,3%
Total		26	100,0%	288,9%

Tabell 5: Tredje del

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Omfanget av IKT-personell i din virksomhet (Informasjon og kommunikasjonsteknologi)□ IKT definerer vi som: - Sikkerhetssystemer (antivirus, o.l) - Hjemmeside og domene - Sikring av dokumenter - Lagring av sensitiv data	9	1	5	2,11	1,269
I hvilken grad er din bedrift sikret mot fremtidig dataangrep	9	1	7	4,33	2,236
Valid N (listwise)	9				

Tabell 6: Turnover

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Hva er prosentvis turnover (gjennomtrekk av ansatte) i din virksomhet?	9	8	40	18,67	10,500
Valid N (listwise)	9				

Krysstabell 1

Omfanget av IKT-personell i din virksomhet (Informasjon og kommunikasjonsteknologi)IKT definerer vi som: - Sikkerhetssystemer (antivirus, o.l) - Hjemmeside og domene - Sikring av dokumenter - Lagring av sensitiv data * I hvilken grad er din bedrift sikret mot fremtidig dataangrep Crosstabulation

Count

		I hvilken grad er din bedrift sikret mot fremtidig dataangrep				
		I svrt stor grad	I stor grad	I liten grad	Verken/eller	Total
Omfanget av IKT-personell i din virksomhet (Informasjon og kommunikasjonsteknologi)IKT definerer vi som: - Sikkerhetssystemer (antivirus, o.l) - Hjemmeside og domene - Sikring av dokumenter - Lagring av sensitiv data	Vi har eget IKT-personell	1	1	1	0	3
	Tredjeparts IKT-personell	0	3	0	1	4
	Daglig leder tar seg av IKT	0	0	0	1	1
	Vet ikke	0	0	0	1	1
Total		1	4	1	3	9

Krysstabell 2

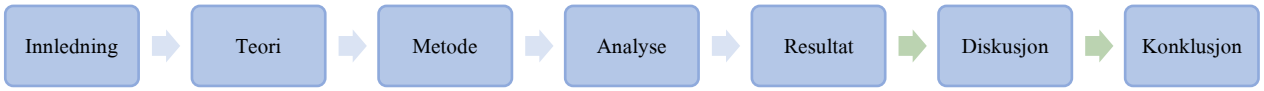
Hva er prosentvis turnover (gjennomtrekk av ansatte) i din virksomhet? * I hvilken grad er din bedrift sikret mot fremtidig dataangrep Crosstabulation

Count

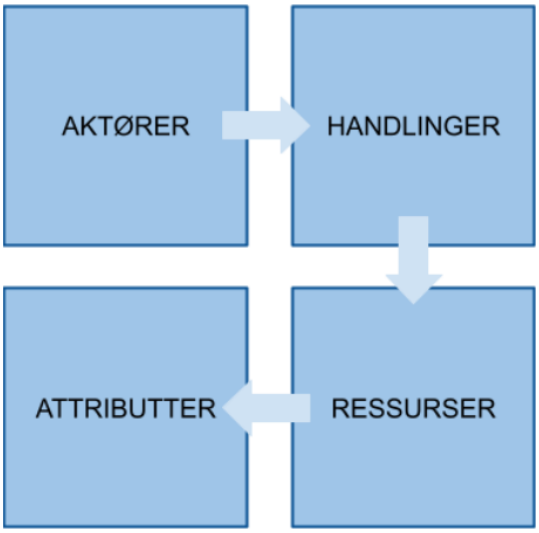
		I hvilken grad er din bedrift sikret mot fremtidig dataangrep			
		I stor grad	I liten grad	Verken/eller	Total
Hva er prosentvis turnover (gjennomtrekk av ansatte) i din virksomhet?	8	0	0	1	1
	15	1	0	0	1
	18	0	1	0	1
	20	1	0	1	2
	29	1	0	0	1
	40	0	0	1	1
Total		3	1	3	7

Figur

Figur 1



Figur 2



Figur 3