Digital Modenhet på Vestlandet

Delrapport 2: Datasikkerhet

Om undersøkelsen

Kartleggingen ble gjennomført via Questback fra 10.01.2022 til 15.02.2022. Totalt var det 372 respondenter, hvor 70% var fra Bergensregionen, 20% fra Stavangerregionen og resten fra Ålesund, Hardanger og Sunnhordland og Haugalandet. I tillegg har Norwegian Cognitive Center gjennomført 200 møter med ulike virksomheter siste to årene fra hele regionen.

Bransjer

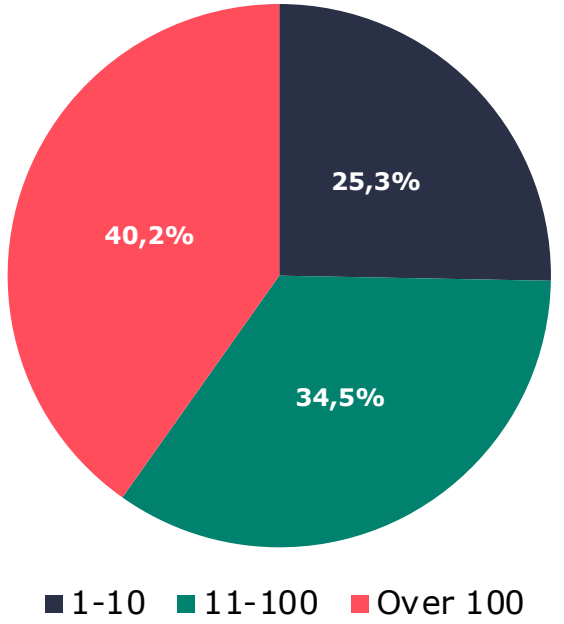
Samtlige bransjer fikk mulighet å delta på kartleggingen, men fordi vi ikke har store nok utvalg fra alle bransjer ble følgende femten bransjer vurdert som store nok til å kunne gi signifikante sammenlignbare resultater:

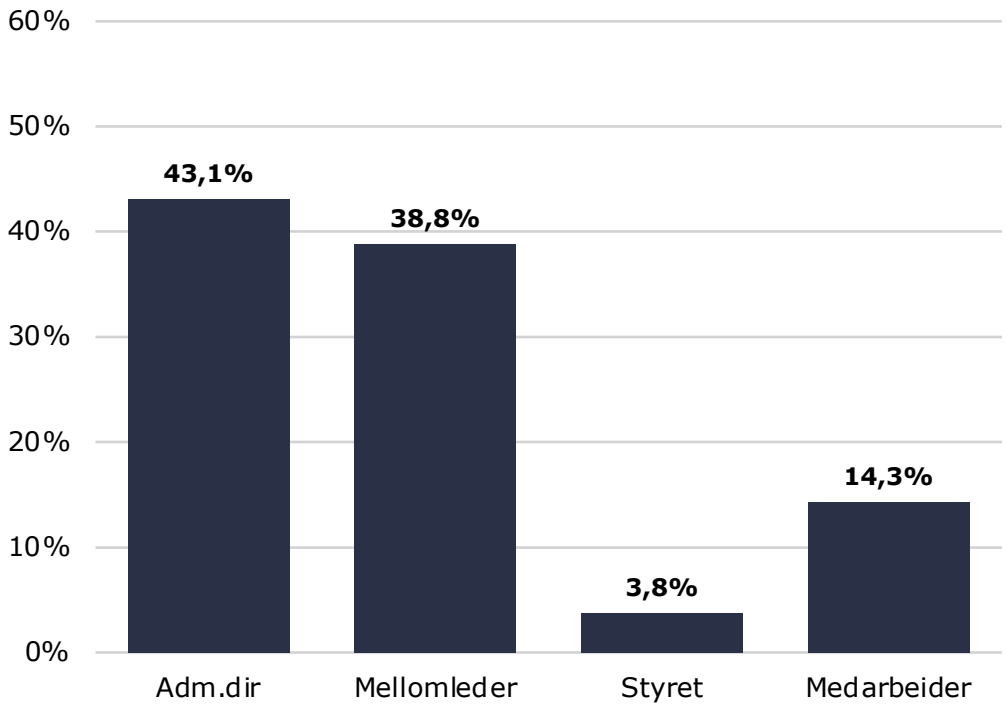
- **Bygg og anlegg**
- **Eiendom**
- **Energi**
- **Finans**
- **Utdanning**
- **Konsulent**
- **Offentlig sektor**
- **IKT**
- **Industri**
- **Maritim**
- **Varehandel**
- **Reiseliv**
- **Service**
- **Kultur**
- **Transport og logistikk**

372
respondenter

Størrelse på respondentene

For denne kartleggingen har vi kategorisert tre ulike størrelser på respondentene. Dette er små virksomheter (opptil 10 ansatte), mellomstore virksomheter (11-100 ansatte) og store virksomheter (over 100 ansatte). Det er store nok respondentutvalg i alle tre kategoriene, selv om fire av ti virksomheter er store virksomheter i utvalget.





Primærstillinger

Målet med kartleggingen har vært å nå bredt, slik at vi kan sammenligne svar mellom toppledere, mellomledere og ansatte. Vi har fått gode utvalg i alle tre kategoriene, som gjør det mulig å sammenligne svar og se hvilke type stillinger som bidrar mest til å øke den digitale modenhet i virksomhetene.

Definisjoner

Det finnes mange definisjoner av begrepet datasikkerhet. Denne kartleggingen har tatt utgangspunkt i følgende definisjoner:

Informasjonssikerhet:
har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke.

IKT-sikkerhet:
har med sikring av Informasjons- og kommunikasjonsteknologi å gjøre – altså maskinvare og programvare.

Cybersikkerhet:
dreier seg om sikring av alt som er sårbart ved bruk av IKT.

Cyberangrep:
ekstern trussel som har til hensikt å skade, forstyrre eller overbelaste datasystemet

Malware:
en fellesbetegnelse på ondsinnet programvare og kommer av de engelske ordene Malicious Software. Kalles ofte for «skadevare» eller «skadeprogrammer» på norsk.

Datasikkerhet

3 av 4 virksomheter har forbedringspotensial

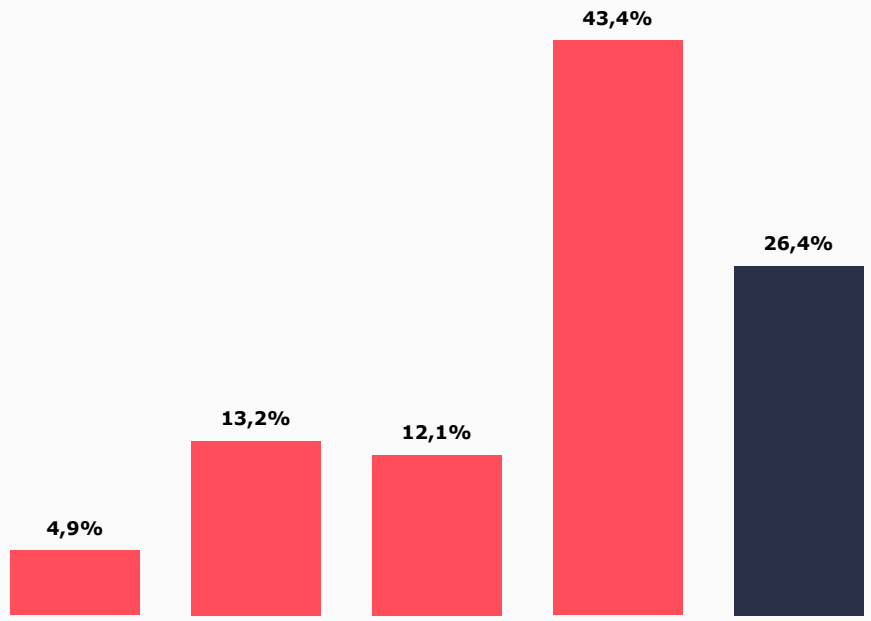
For å beskytte virksomheten er det helt avgjørende med en svært god organisatorisk og teknologisk sikkerhetskultur. Dessverre viser vår kartlegging at bare hver fjerde virksomhet sier selv at de har en god nok sikkerhetskultur. Hele **3 av 4 virksomheter** mener med andre ord at de har et forbedringspotensial, og **hver femte** virksomhet mener de må gjennomføre et større løft på datasikkerhet.

Likevel er vi bekymret for at det ligger mørke tall i bunn. Definisjonen på «god nok» kan variere fra virksomhet til virksomhet. Kompleksiteten av angrep er blitt så kompleks at man i mange tilfeller trenger mer enn bare «god nok» teknologisk- og organisatorisk sikkerhetskultur. Helst skulle vi sett samtlige respondere «helt enig» på dette spørsmålet. Vår analyse er derfor at næringslivet har en stor jobb foran seg, å sikre strukturen og dataene i egne virksomheter, og at dette er et område som må jobbes kontinuerlig med.

Rapporten stemmer godt overens med erfaringer og undersøkelser som vi har gjort i Danmark. Funnene at så mange bedrifter har forbedringspotensialer når det gjelder sikkerhetskultur er en utfordring. Og det er her det er viktig at vi klarer å få til et løft. Både å forstå risikobildet og at hver bedrift internt jobber aktivt med å forbedre interne rutiner.

- Ove Lennart Nes, leder for Underwritig i Tryg

Vår virksomhet har god nok organisatorisk og teknologisk sikkerhetskultur knyttet til å verne vår infrastruktur, systemer og data mot datakriminalitet.

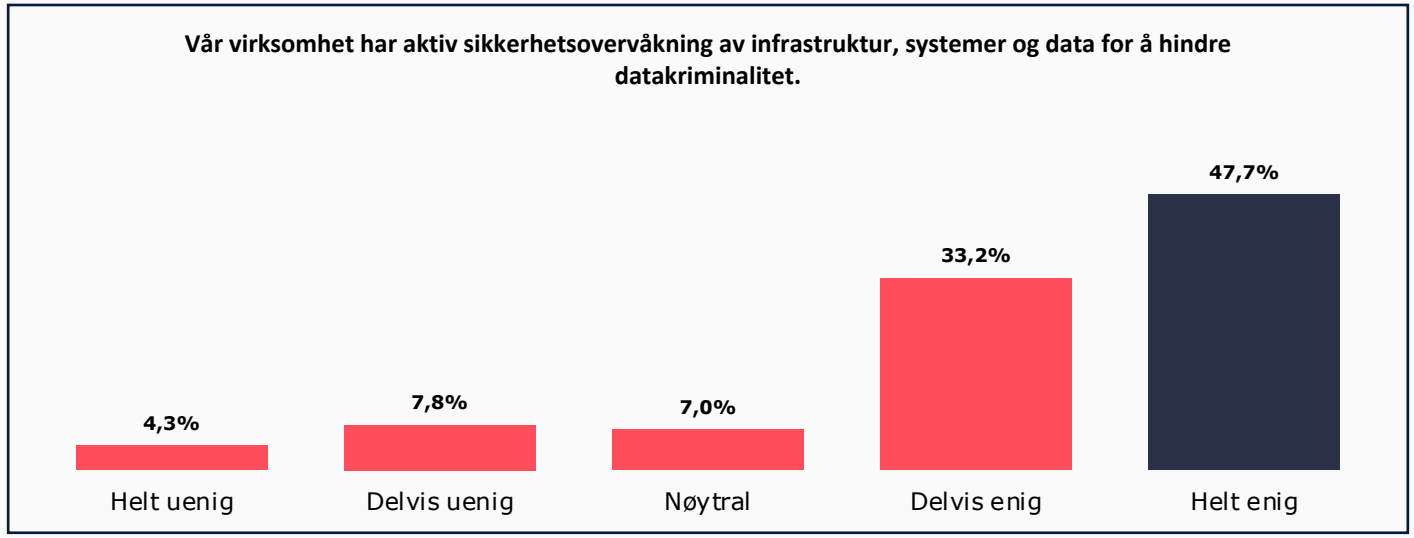


Mangel på sikkerhetsovervåking

En viktig del av arbeidet med å unngå dataangrep er aktiv sikkerhets-overvåking av kritisk infrastruktur, systemer og data. Selv om nærmere halvparten av respondentene mener de har en aktiv sikkerhets-overvåking av kritisk infrastruktur, svarer likevel over halvparten at de har et forbedringspotensial. Kun 12% av virksomhetene mener de ikke har et forbedringspotensial.

Det er alvorlig at så mange virksomheter ikke har en god nok sikkerhets-overvåking. Dette øker sannsynligheten for at angrep går igjennom. Noe av det viktigste en virksomhet kan gjøre er å bygge opp en kultur og struktur som gjør at man sikrer systemene sine og ikke minst dataen.

På neste side er det eksempler på virksomheter som ikke har hatt god nok struktur, og dermed endt opp med å måtte betale i dyre dommer.



Kostnadsaspektet av et dataangrep kan i verste fall sette virksomheten i stor gjeld

2017

MAERSK

Kostnad $300m

TNT

Kostnad $400m

MERCK

Kostnad $1.3bn

2019

Hydro

Kostnad $80m

2020

HONDA

Kostnad $80m

2021->

AKVA GROUP

tieto EVRY

STORTINGET

Nylige nasjonale dataangrep

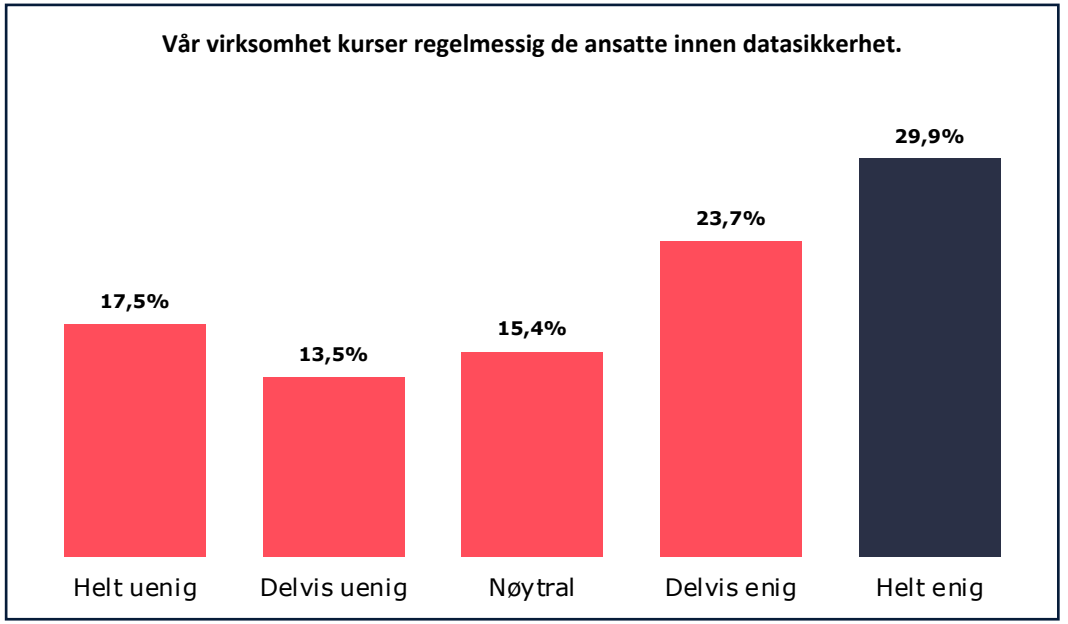
TNT og Merck ble begge angrepet på lik måte, og resultatet ble at TNT ikke kunne levere hundretusenvis av varer. Manuelle prosesser måtte igangsettes som var betydelig mindre effektive enn de automatiske prosessene de var avhengige av. Gjenopprettingen ble til slutt stoppet, og operasjoner overført til morselskapet sine systemer.
Aerospace Company: Skadevare gikk inn via en dårlig konfigurert server og angriperne fikk tilgang til en superbruker i klienten. De infiserte mange servere og tok ned hele produksjonen. Selskapet klarte ikke å prosessere bestillinger for varelagrene siden systemet var helt nede.
Hydro fikk mest sannsynlig skadevare gjennom en e-post som tok ned store deler av Hydro sine fabrikker og kontorer i over 40 land. De fleste fabrikker måtte gå over til saktegående, mindre effektive manuelle prosesser, mens noen prosesser ble stoppet helt. Skadevaren prøvde også å slette backup, skiftet passord fra brukere for å stenge dem ute fra systemet og skadeliggjorde 22 000 datamaskiner og tusenvis av servere.
Maersk: Skadevaren kom inn som følge av en standard oppdatering av et regnskapssystem som ble brukt i et av landene som Maersk opererer i. I det skadevaren ble installert, spredde den seg gjennom nettverket som førte til umiddelbar stopp for virksomheten på et globalt nivå. Innen 90 minutter ble hver eneste server infisert, back-office operasjoner og kommunikasjon mellom kollegaer stoppet helt opp.

Kilde: Deloitte

Det hele begynner med å bygge kompetanse på datasikkerhet

Økt kompetanse er nøkkelen for å lykkes med datasikkerhet. Det er derfor bekymringsverdig at vår kartlegging viser at det er en stor mangel på kompetanseutvikling i næringslivet. Hele **7 av 10 virksomheter** kurser ikke sine ansatte regelmessig på datasikkerhet, noe som er overraskende. Nærmere **hver femte virksomhet** kurser ikke i det hele tatt.

Datasikkerhet er ikke bare et topplederansvar eller IT-ansvarlig sitt ansvar. Det er et ansvar hver og en i organisasjonen må ta. Derfor er det viktig at det finnes gode rutiner for å kurse alle ansatte, regelmessig, slik at man ikke gjør feil som kunne blitt unngått. Dette er spesielt viktig når vi ser at angrepene blir mer komplekse og realistiske enn vi noen gang tidligere har sett, og ofte er det menneskelige feil som er årsaken til at angrepene lykkes.



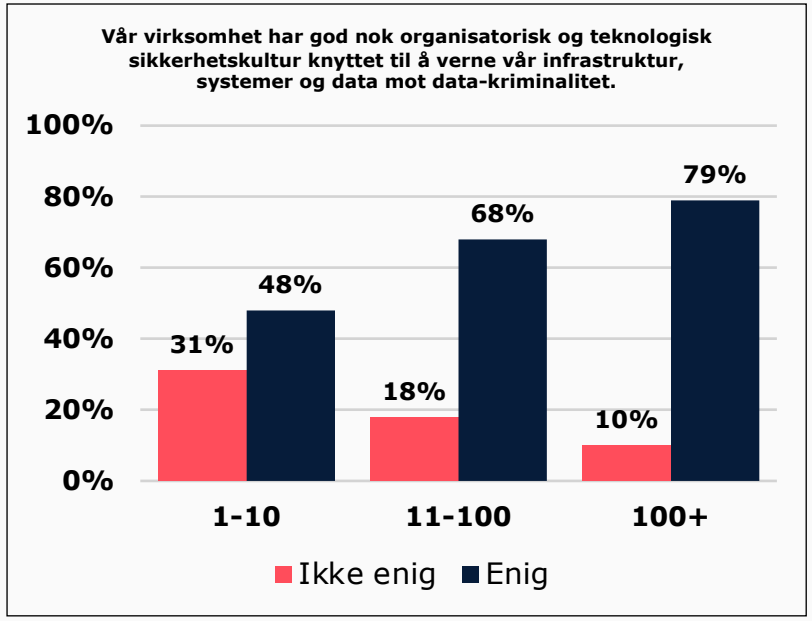
Våre analyser viser at følgende bransjer har størst forbedringspotensial på datasikkerhet:

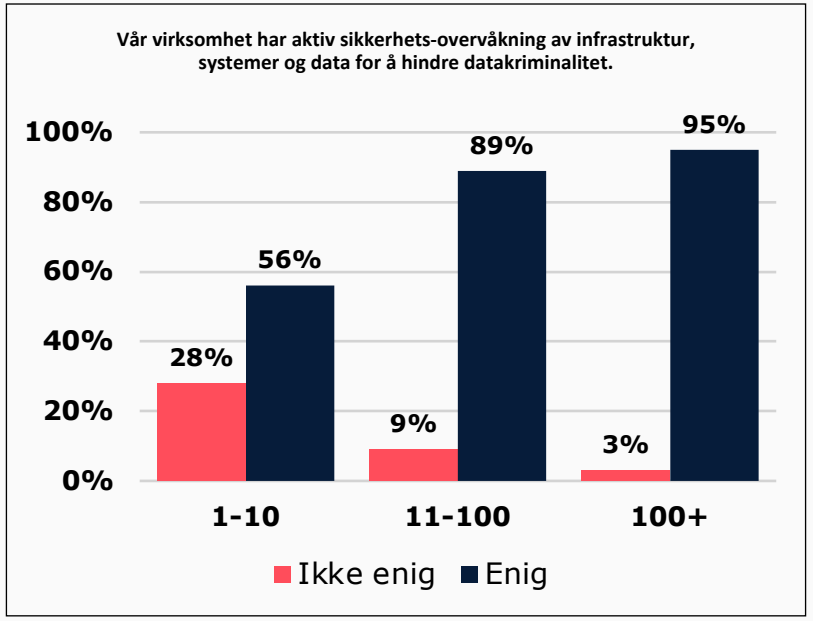
Maritim
Reiseliv
Varehandel
Offentlig
Transport

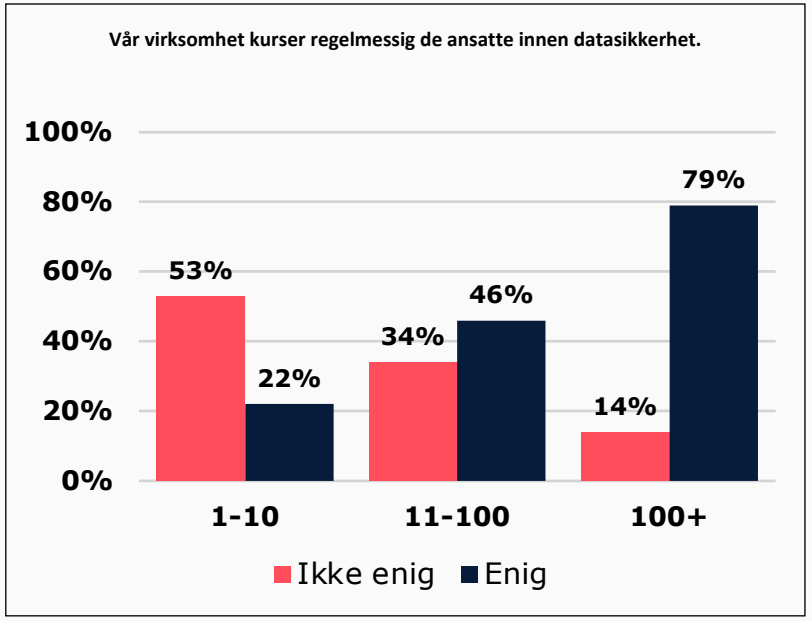
Større virksomheter er kommet betydelig lengre enn små og mellomstore virksomheter når det gjelder datasikkerhet

Dessverre, men ikke overraskende, ser vi at det er en tydelig korrelasjon mellom størrelse på virksomheten og hvor «gode» man er på datasikkerhet i egen virksomhet. Jo større virksomhet, jo «bedre» er man. Dette kjenner vi igjen fra at større virksomheter kan være mer utsatt, og kan ha egne avdelinger som jobber med datasikkerhet i daglig drift. Derimot så kan vi ikke lengre si at mindre virksomheter ikke kan bli utsatt. Alle kan bli utsatt for alvorlige dataangrep som i verste fall kan bety kroken på døren. Derfor er det viktig å begynne tidlig med å øke kompetansen blant små- og mellomstore virksomheter på datasikkerhet. Grunnleggende spørsmål som «Hva, hvorfor og hvordan?» er avgjørende å starte med.

Det er også viktig å påpeke at dette ikke gjelder bare små- og mellomstore virksomheter. Hver femte virksomhet over 100 ansatte sier at de har forbedringspotensial på både det organisatoriske og teknologiske sikkerhetskulturen, og at de heller ikke kurser regelmessig sine ansatte. Dette er faresignaler som må tas på alvor.







Fakta om kartleggingen

Dette er første gang Bergen Næringsråd og Norwegian Cognitive Center gjennomfører en kartlegging på digital modenhet på Vestlandet. Bergen Næringsråd har derimot en lang tradisjon for å gjøre kartlegginger på både bransjer og tematikker i regionen. Noen av disse finner dere her.

Kartleggingen er gjennomført av Bergen Næringsråd og Norwegian Cognitive Center i samarbeid med Næringsforeningen i Stavanger og Næringsalliansen. Det er brukt en kvantitativ undersøkelse med 372 respondenter, og det er gjennomført et fåtalls intervjuer med et utvalg virksomheter i regionen. I tillegg bygger kartleggingen på over 200 intervjuer som Norwegian Cognitive Center har gjort.

Undersøkelsen er utarbeidet av Anri Håvard Hebib, Odd Gurvin og Anne Jacobsen. Analyse og rapport er utarbeidet av Anri Håvard Hebib med bistand fra Nicoline Wiederstrøm.

Tusen takk til medlemmene fra Bergen Næringsråd, Næringsforeningen i Stavanger og Næringsalliansen som har bidratt med å ta en relativt omfattende undersøkelse.

Tusen takk til Agenda Vestland som har finansiert kartleggingen.

Spørsmål til kartleggingen:

Anri Håvard Hebib
Næringspolitisk rådgiver
Bergen Næringsråd

anri@bergen-chamber.no
+47 47259740

BERGEN NÆRINGSRÅD
Bergen Chamber of Commerce and Industry

Norwegian Cognitive Center

næringsalliansen

NÆRINGS FORENINGEN
Gir kraft til vekst

AGENDA VESTLANDET


næringsalliansen
NÆRINGS FORENINGEN
Gir kraft til vekst
BERGEN NÆRINGSRÅD
Bergen Chamber of Commerce and Industry
Norwegian Cognitive Center
AGENDA VESTLANDET