FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Nasdaq Oslo ASA
Postboks 443
0213 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
18/5919			11.11.2020

Tilsynsrapport

1. INNLEDNING

Finanstilsynet gjennomførte høsten 2018 - vinteren 2019 IT-tilsyn hos Nasdaq Oslo ASA (heretter omtalt som "Nasdaq Oslo" eller "Foretaket").

Foretaket har tillatelse som børs etter den tidligere børsloven (nå verdipapirhandelloven) og er underlagt et omfattende regelverk for å sikre sikker, ordnet og effektiv handel i finansielle instrumenter, jf. verdipapirhandelloven § 1-1.

Finanstilsynet varslet IT-tilsynet 14. juni 2018, og forespurt dokumentasjon ble mottatt 6. september 2018. Finanstilsynet ba om, og mottok, ytterligere informasjon senere under tilsynet.

Hensikten med tilsynet var å kartlegge Nasdaq Oslos evne til å motstå elektroniske angrep, samt Foretakets sårbarheter i kontinuitets- og beredskapsløsningene sett i lys av driftshendelsen som startet 18. april 2018. Mye av Foretakets informasjons- og kommunikasjonsteknologi er utkontraktert til andre foretak i Nasdaq-konsernet. Det er derfor lagt særlig vekt på Foretakets kontroll med kvaliteten til de utkontrakterte tjenestene.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 27. juni 2019 og styrets kommentarer til denne rapporten datert 19. september 2019.

2. Foretakets virksomhet

Foretaket inngår i et internasjonalt konsern med det amerikanske holdingselskapet Nasdaq Inc som konsernspiss. Foretak i konsernet driver blant annet handelsplasser, verdipapirregistre og virksomhet som sentral motpart, hovedsakelig i de nordiske landene og Baltikum. I tillegg er salg av IT-systemer, til foretak som driver nevnt virksomhet, et viktig område for konsernet. Handelsplassene er organisert som egne juridiske enheter, men det er et omfattende samarbeid mellom dem. Nasdaq Oslo er den eneste rene varederivatbørsen i Nasdaq-konsernet i Norden.

En rekke IT-systemer, funksjoner og tjenester er utkontraktert fra Foretaket til Nasdaq Stockholm. Utkontrakteringen er formalisert i egen avtale. Nasdaq Stockholm har i tillegg videreutkontraktert deler av IT-tjenestene til andre konsernforetak. Finanstilsynet forstår det slik at Foretaket har en

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Arild Tømmerås
Dir. tlf 22 93 98 00

struktur i konsernet der ulike forretningsområder som aksjer, obligasjoner, varederivater ("*commodities*") og IT-systemer er samlet globalt eller regionalt i egne grupper på tvers av de juridiske enhetene.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

3. Hendelse hos Foretaket 18. april 2018 og risikostyring, internkontroll og internrevisjon

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 12, Utkontraktering
- IKT-forskriften § 8, Drift
- Risikostyringsforskriften § 9, 1. og 2. Internrevisjon
- Risikostyringsforskriftens § 5, Utkontraktering
- Forskrift om utfyllende regler til MiFID 2 og MiFIR-forskriftene del 251 (RTS 7) artikkel 15 Business continuity arrangements.

18. april 2018 var handelsplassen hos Foretaket ute av drift fra børsstart og til 13:15 CET. Foretakets handelsplass var da reetablert på sekundært driftssted. Hendelsen førte til driftsstans for alle de nordiske handelsplassene i konsernet. Reetableringen tok vesentlig lenger tid enn kravene på to timer som følger av RTS 7 og de interne kravene Nasdaq Oslo selv har satt. Hendelsen avslørte en rekke svakheter i Nasdaq-konsernets systemer og IT-beredskap. I etterkant av hendelsen har Foretaket gjennomført tiltak for å redusere IT-risikoen og bedre IT-beredskapen.

Finanstilsynet påpekte i foreløpig rapport at nedetiden var betydelig over 2 timer, som foreskrevet i regelverket og i foretakets egne fastsatte grenser. Videre ble det påpekt at internrevisor før hendelsen beskrev at Nasdaq Oslo hadde en betydelig risiko for at nedetiden ville bli mer enn to timer dersom driften av Foretakets utkontrakterte systemer måtte flyttes til sekundært driftssted, og at Foretaket var gjort kjent med denne risikoen uten at Foretaket fulgte opp internrevisors anbefalinger i denne sammenheng.

Finanstilsynets vurdering i foreløpig rapport er at konsekvensene av hendelsen har mange likhetstrekk med virkningen av elektroniske angrep, og at tiltak for å bedre Foretakets IT-beredskap etter hendelsen også vil styrke Foretakets forsvar mot elektroniske angrep.

Nasdaq Oslo har i sitt tilsvar beskrevet en rekke gjennomførte tiltak og Foretaket vurderer at risikoen ved tilsvarende hendelser nå er betydelig redusert.

Finanstilsynet tar Nasdaq Oslos opplysninger til etterretning.

[1] Tilsvarer RTS 7, http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

4. Intern risikorapportering og kontroll

Finanstilsynets merknader har følgende rettslige grunnlag:

- Risikostyringsforskriften § 6
- IKT-forskriftens § 3 Risikovurdering
- Risikoforskriftens § 8.

Finanstilsynet vurderte under tilsynet Foretakets risikorapportering og kontroll på IT-området. Finanstilsynet påpekte i foreløpig rapport at det er liten eller ingen samsvar mellom de risikofaktorene internrevisor har påpekt og de risikofaktorene som forefinnes i Foretakets risikogjennomgang. Internrevisjonens funn og oppfølgingen av disse bør være en naturlig del av administrasjonens oppfølging og dokumentasjon av risikoen i Foretaket. Det er Finanstilsynets vurdering at internrevisjonens gjennomganger dermed har begrenset innvirkning på Foretakets risikohåndtering og ikke bidrar slik den burde for å redusere Foretakets risiko. Det er særlig Foretakets håndtering av risiko med utkontrakterte tjenester som ikke synes å være tilstrekkelig håndtert.

Finanstilsynet har fra Nasdaq Oslos svar merket seg at Foretaket fremover vil innarbeide all risikoinformasjon fra internrevisors risikogjennomganger i Foretakets egne risikogjennomganger, slik at denne representerer Foretakets totale risikoprofil.

5. Foretakets egenvurdering

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 3 Risikovurdering
- RTS 7 artikkel 2 (1) Egenvurdering.

Finanstilsynet gikk under tilsynet gjennom Foretakets egenvurderingen etter RTS 7. Egenvurderingen er gjennomført i samarbeid med de øvrige nordiske handelsplassene i konsernet i desember 2018, et halvår etter den omtalte hendelsen 18. april 2018, men før tiltakene etter hendelsen er gjennomført. I egenvurderingen evaluerer Nasdaq Oslo eksempelvis sin oppfyllelse av RTS 7 artikkel 15 (2) om kravet til maksimum to timers nedetid ved handelsplassen etter en hendelse. Evalueringsresultatet viser "Compliant with no changes". Finanstilsynet påpekte i foreløpig rapport at resultatet av egenevalueringen i denne sammenheng ikke kunne være riktig, tatt i betraktning av at internrevisor før hendelsen anså at det var betydelig risiko for driftsavbrudd på mer enn to timer, at Foretaket faktisk opplevde en hendelse som viste dette og at Foretakets tiltak for å redusere risikoen ikke var gjennomført.

Finanstilsynet har fra Foretakets svar merket seg at Nasdaq Oslo anser at hendelsen 18. april 2018 viste svakheter i Foretakets beredskap med IT-virksomheten og elektroniske forsvar, og at Foretaket mener de nå har gjennomført tilstrekkelige tiltak mot svakhetene som ble avdekket ved den aktuelle hendelsen. Finanstilsynet har fra Foretakets svar også merket seg at Nasdaq Oslo planlegger flere forbedringer for framtidige egenvurderinger i denne sammenheng.

6. Nærmere om kontroll med utkontraktert virksomhet

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 8 Drift
- Risikostyringsforskriften § 3 Styret
- RTS 7 artikkel 15 Business continuity arrangements.

Finanstilsynet gikk under tilsynet gjennom Foretakets kontroll og oppfølging av utkontraktert virksomhet.

Finanstilsynet pekte i foreløpig rapport på at styret i Nasdaq Oslo har ansvar for en forsvarlig kontroll med all utkontraktert virksomhet, risikoen utkontrakteringen påfører Foretaket og at Foretaket har en klar organisasjonsstruktur, jf. risikostyringsforskriften § 3 første og annet ledd. Daglig leder i Nasdaq Oslo har et særlig ansvar for å følge opp Foretakets risiko, herunder den virksomheten som er utkontraktert til søsterselskapet Nasdaq Stockholm.

Finanstilsynet pekte også på viktigheten av at Nasdaq Oslo har integritet og får nødvendig gjennomslag overfor sitt søsterselskap, Nasdaq Stockholm, som oppdragstaker, slik at Foretaket kan utføre en forsvarlig løpende kontroll med de tjenester som er utkontraktert, herunder sikre lovmessige leveranser.

Videre pekte Finanstilsynet på at Foretaket må treffe særskilte tiltak for å identifisere og håndtere de interessekonflikter som kan følge av organiseringen der styreleder i Nasdaq Oslo er daglig leder i tjenesteleverandøren Nasdaq Stockholm, og dermed i praksis sitter på begge sider av bordet.

Finanstilsynet har fra svar til foreløpig rapport merket seg at styret for Nasdaq Oslo vil ha spesiell oppmerksomhet rettet mot eventuelle interessekonflikter mellom konsernforetakene. I svaret informeres det videre om at en omorganisering av konsernets risikostyringshåndtering har pågått en stund, og nå begynner å virke i ny form. Foretaket informerer videre om at et eksternt styremedlem i Nasdaq Oslos styre er planlagt og vil kunne bidra positivt også i denne sammenheng. Samlet sett anser Foretaket med dette at eventuelle interessekonflikter nå er adressert i Foretaket.

Finanstilsynet understreker styrets ansvar for å motvirke interessekonflikter.

7. Medlemmenes risiko ved manglende systemløsninger

Finanstilsynets merknader har følgende rettslige grunnlag:

- Vphl. § 12-4 (1) Medlemskap på regulert marked
- RTS 7 artikkel 15 Business continuity arrangements.

Finanstilsynet gikk under tilsynet gjennom hvordan medlemmene til Nasdaq Oslo blir påvirket av hendelser der Nasdaq Oslo må flytte driften til Foretakets sekundære driftssted.

En slik hendelse vil medføre at medlemmene til Nasdaq Oslo må foreta en omkobling mot sekundært driftssted. Det fremkom under tilsynet at mange av Nasdaq Oslos medlemmer ikke har løsninger som gjør slike omkoblinger automatisk, og at en manuell omkobling har vist seg å ta betydelig tid, sannsynligvis mer enn to timer slik RTS 7 krever. Nasdaq Oslo kan dermed oppleve

en situasjon med driftsavbrudd på mindre enn to timer for sine systemer, mens handelsplassen ikke kan være operativ i tide fordi medlemmer ikke har rukket å koble seg til innen fristen.

Finanstilsynets anså i foreløpig rapport at Nasdaq Oslo må vurdere tiltak for å sikre at handelen kan gjenopptas innen eller nær opptil to timer etter en forstyrrende hendelse, jf. RTS 7 artikkel 15 og IKT-forskriften §3 tredje ledd. Finanstilsynet anså også at Nasdaq Oslo bør vurdere om det er nødvendig å innføre mulige tiltak overfor medlemmene, eksempelvis å åpne handelsplassen uten at enkeltmedlemmer har mulighet til å handle fordi medlemmene selv har valgt å ikke ha tilstrekkelige tekniske løsninger. Medlemmene bør gjøres kjent med risikoen de er eksponert for dersom de ikke har tilstrekkelige systemløsning. Tiltakene kan for eksempel innføres gjennom børsens regelverk. Børsens egne regler skal samtidig være objektive og ikke-diskriminerende, jf. vphl. § 12-4 (1), for eksempel gjennom at børsens påloggingsløsninger ikke innebærer urimelig forskjellsbehandling.

Nasdaq Oslo informerer, i sitt tilsvar til foreløpig rapport, at handelsplassens regelverk Appendix 5 beskriver medlemmenes plikter til å teste sine systemer tilstrekkelig, slik at de kan handle på handelsplassen innen den foreskrevne tiden.

Finanstilsynets anser at Nasdaq Oslo ifølge RTS 7 artikkel 15, har et selvstendig ansvar for å sikre at handel på handelsplassen kan gjenopptas innen eller tett opptil to timer etter en forstyrrende hendelse. For at handel kan gjenopptas på en handelsplass må markedsbildet være representativt for markedet.

8. Særlig risiko forbundet med elektronisk angrep

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 3 Risikovurdering
- IKT-forskriften § 8 Drift
- RTS 7 Artikkel 15 Business continuity arrangements.

Nasdaq Oslo er en viktig del av norsk finansiell infrastruktur og handelsplassen har betydelige mengder informasjon og data som kan gi uønsket økonomisk påvirkning dersom denne kommer på avveie. Finanstilsynet gikk under tilsynet gjennom hvordan Nasdaq Oslo sikrer sine systemer og informasjon mot elektroniske angrep.

Finanstilsynet pekte i foreløpig rapport på at alvorlige hendelser i handelsplassens nære relasjoner, øker risikonivået for at slike hendelser også kan ramme Foretaket, jf. hendelsen hos Norsk Hydro ASA. Foretaket vil også lettere kunne bli kilde til spredning av skadevare til børsens samarbeidspartnere dersom ansatte i Nasdaq Oslo ikke utfører hensiktsmessige handlinger basert på vurderinger av Foretakets sikkerhetssituasjon.

Finanstilsynet har fra Foretakets svar merket seg at Foretaket har gjennomført tiltak etter hendelsen som rammet Norsk Hydro ASA og at Foretaket beklager at Finanstilsynet på tilsynsmøtet 20. mars 2019 mottok mangelfull informasjon vedrørende Foretakets gjennomførte tiltak ved nevnte hendelse. I motsetning til opplysningene som ble gitt på tilsynsmøtet ble det gjennomført flere tiltak i forbindelse med hendelsen.

9. Risikovurdering av Foretakets E-postteknologi

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 3.Risikoanalyse.

Foretakets sikring av E-postløsning ble gjennomgått på tilsynet. Nasdaq Oslo redegjorde for sin e-postløsning og bekreftet på tilsynsmøtet at kjent moderne sikkerhetsteknologi i forbindelse med bruk av E-post ikke var vurdert.

Finanstilsynets vurdering i foreløpig rapport var at Foretaket bør vurdere nye sikkerhetsløsninger og teknikker for å øke sikkerhetsnivået i sine E-postløsninger.

Nasdaq Oslo informerte i sitt svar om Foretakets tekniske oppsett vedrørende E-postsikkerhet. Foretaket orienterte videre om sine målsettinger for gjennomføring av konkrete forbedringstiltak på området.

Finanstilsynet tar Nasdaq Oslos orientering om konkrete forbedringstiltak til etterretning og ber om oppdatert status for gjennomføring av disse tiltakene.

10. Retningslinjer for bruk av eksterne sikkerhetstestere

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT-forskriften § 5. Sikkerhet.

Finanstilsynet så under tilsynet på hvordan Nasdaq Oslo gjennomfører sikkerhetstesting av egne systemer for å kontrollere og forbedre Foretakets elektroniske forsvar. Finanstilsynet så også på Foretakets bruk av ekstern bistand ifm. testingen. Det framkom under tilsynet at Foretaket ikke har utarbeidet policy eller retningslinjer for bruk av eksterne konsulenter ved slik sikkerhetstesting.

Finanstilsynets vurdering i foreløpig rapport er at Foretaket bør benytte kjente standarder og god praksis ved gjennomføring av tredjeparts testing av IT-sikkerhet.

Foretaket har i sitt svar beskrevet bruken av sikkerhetstesting og organisering av denne. Finanstilsynet savner omtale av Nasdaq Oslos rutiner og retningslinjer for valg av leverandører ved gjennomføring av sikkerhetstesting, samt hvordan og hvor ofte slike tester skal gjennomføres.

Finanstilsynet forventer at Foretaket oppdaterer sine rutiner på området og ber om å få oversendt kopi av rutiner for bruk av eksterne sikkerhetstestere når rutinene er oppdatert.

11. Kommunikasjon med handelsplassens medlemmer

Finanstilsynets merknader har følgende rettslige grunnlag:

- IKT forskriften § 11. Driftsavbrudd og kriseberedskap.

Finanstilsynet så under tilsynet på hvordan Nasdaq Oslo ivaretok den elektroniske kommunikasjonen med medlemmene ifm. hendelsen 18. april 2018. Ifølge Foretakets rapporter

sviktet Foretakets primære kommunikasjonsløsning når handelssystemet ble satt ut av drift på primært driftssted. Alternativ kommunikasjon ble da, ifølge Foretaket, både tilfeldig og preget av at løsningene ikke hadde tilstrekkelig kapasitet, og viste seg uegnet i en beredskapssituasjon. I Foretakets beskrivelse av tiltak etter hendelsen er alternativ kommunikasjon med kundene satt opp som et eget tiltak.

Kommunikasjon med medlemmene i en situasjon hvor systemene er ute av drift, er en viktig del av Foretakets beredskap. Finanstilsynet vurdering i foreløpig rapport er at Foretaket bør etablere tilstrekkelig sikrede og robuste kommunikasjonsløsninger, som også må fungere tilfredsstillende ved en driftsstans. Løsningene må i tillegg være tilstrekkelig uavhengige av Foretakets primærløsning, slik at de kan være operative selv om primærløsningen er ute av drift. Videre må Foretaket etablere rutiner slik at løsningen testes jevnlig, og at den ved behov enkelt kan tas i bruk av medlemmer.

Nasdaq Oslo informerte i svaret om de operasjonelle og systemmessige tiltak som handelsplassen har gjennomført etter hendelsen. Foretaket er av den oppfatning at handelsplassen nå har etablert kommunikasjonsløsninger som er tilstrekkelig robuste for å kunne håndtere tilsvarende hendelser i fremtiden.

Finanstilsynet tar Foretakets orientering til etterretning.

Kopi av merknadene bes sendt valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Arild Tømmerås
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.