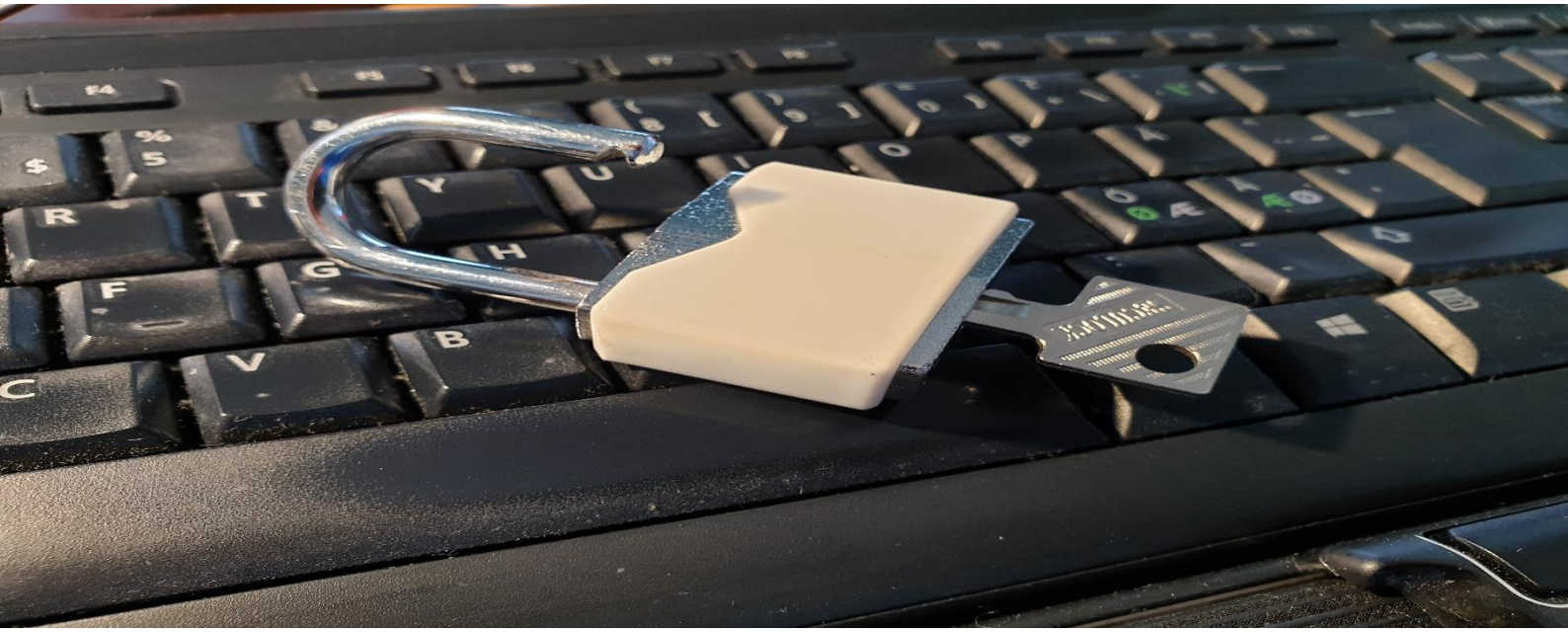
Riksrevisjonen

Riksrevisjonens undersøkelse av informasjonssikkerhet i Norfund

Rapportvedlegg til Dokument 3:2 (2020–2021)



Revisjonen er gjennomført i henhold til lov om Riksrevisjonen § 9, andre ledd, og instruks om Riksrevisjonens virksomhet § 5 første ledd. Revisjonen er gjennomført i samsvar med Riksrevisjonens faglige retningslinjer for selskapskontroll og INTOSAIs standard for etterlevelsesrevisjon (ISSAI 4000)

Forsidebilde: Riksrevisjonen

ISBN-978-82-8229-494-2

Innhold

Figuroversikt

Faktaboksoversikt

1 Bakgrunn

Våren 2020 ble Statens investeringsfond for næringsvirksomhet i utviklingsland (Norfund) svindlet for om lag 100 millioner kroner etter et målrettet dataangrep.

Norfund er et sentralt virkemiddel i norsk utviklingspolitikk. Gjennom sitt mandat skal selskapet kombinere hensynet til lønnsomhet med det overordnede målet om å fremme bærekraftig utvikling.

Norfund er et heleid statlig særlovsselskap som har mottatt årlige bevilgninger over statsbudsjettet siden etableringen i 1997.

I 2019 ble antall ansatte økt fra 75 til 87, og i budsjettforslaget for 2020 er det foreslått en økning i antall ansatte, slik at selskapet mot slutten av året vil ha om lag 100 ansatte. Norfunds ansatte er fordelt på hovedkontoret i Oslo og fem regionkontorer.[1] Selskapet benytter eksterne leverandører av en del tjenester som for eksempel IKT.

I 2019 utgjorde de statlige bevilgningene til Norfund 1 905 millioner kroner. I tillegg mottok selskapet 105 millioner kroner som ble øremerket en ny ordning for prosjektutvikling og risikoavlastning. Norfunds bokførte egenkapital var 23 milliarder kroner ved utgangen av 2019. Norfund investerte for totalt 4 milliarder kroner i 2019. De siste ti årene har Norfund fått tilført betydelig kapital fra staten. Dette gjør at Norfund kan gjennomføre flere nye investeringer.

Siden begynnelsen av 2018 har Norfund gjennomført rundt 2 100 utbetalinger. I snitt gjennomfører selskapet to utbetalinger og mottar fire innbetalinger per dag.

Mange norske virksomheter utsettes hvert år for dataangrep, både med mål om å skade virksomhetens aktivitet og å svindle til seg penger. Svindel gjennom sosial manipulering, det vil si at svindleren manipulerer betaleren til å gjennomføre en transaksjon, har økt betydelig de siste årene. Statistikk viser at det på verdensbasis i perioden 2016–2019 har vært om lag 166 000 tilfeller av svindel med en kostnad på 26 milliarder dollar.[2] I Norge indikerer rapporterte tall til Finanstilsynet at det i 2019 ble tapt over 500 millioner kroner i slik svindel. I om lag en femtedel av sakene ble mottakerkonto endret.[3] Det antas at mørketallene er store, og at mange virksomheter ikke rapporterer om at de har blitt svindlet. Risikoen datakriminalitet utgjør, stiller økte krav til informasjonssikkerhet i virksomheter som er utsatt, både når det gjelder tekniske sikkerhetsløsninger og interne rutiner.

1.1 Mål og problemstillinger

Målet med undersøkelsen er å vurdere Norfunds arbeid med risikostyring på informasjonssikkerhetsområdet med utgangspunkt i svindelen selskapet ble utsatt for våren 2020.

Målet belyses gjennom følgende problemstillinger:

1. Hva skjedde da Norfund ble svindlet?
2. Hvordan har Norfund arbeidet med styringen av informasjonssikkerheten?
3. Hvordan har Norfund fulgt opp leverandøren av IKT-tjenester?
4. Hvordan har Utenriksdepartementet fulgt opp risikostyringen og informasjonssikkerheten i Norfund?

[1] Regionkontorene er lokalisert i Ghana, Kenya, Sør-Afrika, Costa Rica og Thailand.
[2] Federal Bureau of Investigation, «Business Email Compromise the $26 billion scam». https://www.ic3.gov/media/2019/190910.aspx [hentedato: 24. september 2020].
[3] Finanstilsynet: Risiko- og sårbarhetsanalyse (ROS) 2020, punkt 4.4.

2 Metodisk tilnærming og gjennomføring

Undersøkelsen omhandler internkontroll og risiko på informasjonssikkerhetsområdet. Det er ikke foretatt en fullstendig gjennomgang av Norfunds internkontroll eller av Utenriksdepartementets eierstyring av Norfund.

I denne undersøkelsen brukes både begrepene informasjonssikkerhet og IKT-sikkerhet. Begrepene overlapper i stor grad, og brukes ofte som synonymer både i dagligtale og i virksomheters styring av området.[4]

For å belyse arbeidet med risikostyring på informasjonssikkerhetsområdet er det gjennomført dokumentanalyse og intervjuer. Undersøkelsesperioden er fra 2017 til august 2020.

Det er gjennomført utvalgte kontroller av sikkerhetstiltak i Norfunds IKT-systemer gjennom uttrekk foretatt i august 2020.

Datainnsamlingen ble gjennomført i perioden fra juni til september 2020.

2.1 Dokumentanalyse

Det er gjennomført dokumentanalyse av:

- protokoller med underlagsdokumentasjon fra styremøter i Norfund (fra 2017 til 2020)
- referater fra kontaktmøter mellom Norfund og Utenriksdepartementet (fra 2017 til 2020)
- Norfunds interne rutiner og retningslinjer som beskriver selskapets IKT-miljø og -sikkerhet
- avtalen mellom Norfund og leverandøren av IKT-tjenester (2010) og endringer i denne (vedlegg)
- referat fra møter mellom Norfund og leverandør av IKT-tjenester

Videre er dokumenter utarbeidet i forbindelse med svindelen mot selskapet i 2020 gjennomgått. Dokumentene er utarbeidet av Norfund eller på oppdrag fra Norfund, og beskriver hendelsesforløpet, årsakene til svindelen og tiltakene selskapet har iverksatt som følge av hendelsen.

Styringsdokumenter for selskapet (strategier og vedtekter) er også gjennomgått.

2.2 Møter

Det har vært gjennomført tre møter med Norfund i løpet av undersøkelsen. Temaene for møtene har vært:

- årsaker til svindelsaken og selskapets håndtering av den, herunder iverksatte tiltak
- arbeid med internkontroll og risikostyring med spesiell vekt på informasjonssikkerhetsområdet
- synspunkter og vurderinger på konklusjoner og anbefalinger i PwCs rapport
- dialog med eierdepartementet og styret
- IKT-sikkerhet i Norfund, herunder systemer, rolle- og ansvarsdeling, tilgangsstyring og håndtering av brukere og rettigheter, prosesser for sikkerhetsoppdateringer og oversikt over kontroll med autorisert programvare.

Det er også gjennomført et møte med styreleder i Norfund. Temaene i møtet var:

- styrets arbeid med internkontrollen i Norfund
- eierdialogen med Utenriksdepartementet.

Det har vært avholdt to møter med Utenriksdepartementet (UD), som er ansvarlig for eierstyringen av Norfund. Det første var et oppstartsmøte hvor departementet fikk presentert undersøkelsen og forelagt revisjonskriterier. I det andre møtet var temaene:

- svindelhendelsen
- eierstyringen av Norfund
- Utenriksdepartementets arbeid med styresammensetning i Norfund.

[4] Jf. NOU 2018:14 *IKT-sikkerhet i alle ledd*.

Det er videre gjennomført et møte med PwC om konklusjoner og anbefalinger i rapporten *Independent Assessment of the LOLC incident*, *Report developed for Norfund* som ble utarbeidet på oppdrag fra Norfund i etterkant av svindelen.

2.3 Kontroll av sikkerhetstiltak

For å få et mer helhetlig bilde av informasjonssikkerheten i Norfund er det foretatt et utvalg kontroller av tekniske sikkerhetstiltak. Sikkerhetstiltakene har ikke direkte sammenheng med svindelhendelsen i Norfund, men er viktige tiltak for å sikre Norfunds informasjonsverdier. Utgangspunktet for kontrollen har vært uttrekk av data fra Norfunds systemer i august 2020. Uttrekkene har blitt analysert og evaluert opp mot beste praksis for sikkerhetstiltak (jf. omtale i kapittel 3.2). Det er hentet ut uttrekk som gir oversikt over:

- sikkerhetsoppdateringer av programvare
- brukerkontoer og deres rettigheter
- programvare benyttet av Norfund.

Resultatene av analysene er presentert for Norfund i møte 8. september 2020.

3 Revisjonskriterier

3.1 Krav til risikostyring og internkontroll

I Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping* (eierskapsmeldingen) uttrykker staten tydelige forventninger til selskaper med direkte statlig eierskap. [5] Staten stiller forventninger til selskapene på en rekke områder. Felles for alle forventningene er at de støtter opp under statens mål som eier om høyest mulig avkastning over tid eller effektiv oppnåelse av sektorpolitiske mål.

Det forventes blant annet at selskapene:

- har effektiv risikostyring som er tilpasset selskapets virksomhet, mål og strategi
- følger Norsk anbefaling om eierstyring og selskapsledelse (NUES), der den er relevant og tilpasset selskapets virksomhet

Ifølge eierskapsmeldingen er risikostyring og internkontroll verktøy for styret for å føre tilsyn med ledelsen og for å bidra til høyere måloppnåelse og verdiskaping. Mange av selskapene opererer i komplekse omgivelser der risikobildet og forretningsmodeller kan endres raskt. Det går fram av meldingen at det er vesentlig å identifisere relevant risiko, inkludert risiko som ikke er enkel å tallfeste.

I eierskapsmeldingen står det at effektiv risikostyring forutsetter at risikovurderinger er integrert i selskapets strategi, kjernevirksomhet og beslutningsprosesser. Et godt risikostyringssystem bidrar til å identifisere, evaluere og rapportere risiko og legger til rette for at selskapet kan respondere strategisk, operasjonelt og finansielt. Det inkluderer også beredskap for krisehåndtering. Formålet med risikostyring er å håndtere, ikke eliminere, risiko.

Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping* viderefører i stor grad omtalen og kravene til risikostyring som også var beskrevet i den forrige eierskapsmeldingen Meld St. 27 (2013–2014) *Et mangfoldig og verdiskapende eierskap*. [6]

I eierskapsmeldingen fra 2014 står det blant annet at styret bør sørge for at selskapet har styringssystemer og kultur for risikohåndtering som er forenelig med hvordan selskapet ønsker å forholde seg til risiko. Videre framgår det av meldingen at organisering av risikoarbeidet bør inngå som en del av styrets vurderinger. Ifølge meldingen innebærer dette vurdering av om det bør utnevnes eller etableres roller med et særskilt ansvar innenfor etterlevelse av lover, regler og interne retningslinjer (compliance) og risikostyring med direkte rapporteringslinjer til styret, for eksempel compliance officer, chief risk officer og intern revisjon.

I NUES kapittel 10 omtales risikostyring og intern kontroll.[7] Der står det at styret skal påse at selskapet har god intern kontroll og hensiktsmessige systemer for risikostyring i forhold til omfanget og arten av selskapets virksomhet. Internkontrollen og systemene bør også omfatte selskapets retningslinjer mv. for hvordan det integrerer hensyn til omverdenen i verdiskapingen.

Det framgår også av NUES at styret årlig bør foreta en gjennomgang av selskapets viktigste risikoområder og den interne kontroll, og at denne bør ta for seg:

- endringer i forhold til forrige års gjennomgang knyttet til art og omfang av risikoer av betydning, og selskapets evne til å tilpasse seg virksomhetsendringer og eksterne endringer;
- omfanget av og kvaliteten på ledelsens løpende oppfølging av risikoer og internkontrollsystem, og dersom det er relevant, internrevisjonens arbeid;
- omfang og hyppighet av ledelsens rapportering til styret om resultatene av denne oppfølgingen, som gjør det mulig for styret å foreta en samlet vurdering av kontrolltilstanden i selskapet og hvordan risikoene håndteres;
- tilfeller av betydelig kontrollsvikt eller svakheter som er avdekket i løpet av året, og om de har hatt, kunne ha hatt eller vil kunne ha betydelig innvirkning på selskapets økonomiske resultat eller stilling, og hvordan selskapets eksterne rapporteringsprosess fungerer.

[5] Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping,* jf. Innst. 225 S (2019–2020).
[6] Meld St. 27 (2013–2014) *Et mangfoldig og verdiskapende eierskap*, jf. Innst.140 S (2014–2015).
[7] Eierstyring og selskapsledelse, Norsk anbefaling, 17. oktober 2018.

Internkontroll utgjør en del av en virksomhets helhetlige risikostyring. Internkontrollen i Norfund er basert på COSOs rammeverk for internkontroll. COSO-modellen tar utgangspunkt i beste praksis for et integrert internkontroll- og compliancesystem og inneholder fem innbyrdes sammenhengende komponenter som regelmessig skal gjennomgås. De fem komponentene er kontrollmiljø, risikovurdering, kontrollaktiviteter, informasjon og kommunikasjon, og overvåkning.

3.2 Krav til informasjonssikkerhet

Informasjonssikkerhet handler om å sikre at informasjon i en virksomhet

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

God informasjonssikkerhet betyr at informasjonssystemene som benyttes for å behandle informasjon, er sikret, og inkluderer sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene.[8]

Alle virksomheter bør ha en egeninteresse i et systematisk arbeid med informasjonssikkerhet. Ifølge Digitaliseringsdirektoratet er innebygd informasjonssikkerhet et overordnet prinsipp i arbeidet med informasjonssikkerhet.[9] Innebygd informasjonssikkerhet betyr at informasjonssikkerhet er innarbeidet i virksomhetsstyringen og understøtter virksomhetens mål.[10]

Et styringssystem for informasjonssikkerhet skal sikre nødvendig konfidensialitet, integritet og tilgjengelighet av virksomhetens informasjon.[11] Kjernen i styringssystemet er en risikostyringsprosess som skal gi virksomhetens interessenter tillit til at informasjonssikkerhetsrisikoer håndteres på en adekvat måte.[12]

ISO 27001 er en standard for et styringssystem for informasjonssikkerhet. Det er ikke et krav om at Norfund skal følge ISO 27001, men standarden er anerkjent som beste praksis.

I ISO 27001 framgår det blant annet at virksomheten bør planlegge og iverksette sikkerhetstiltak for å håndtere risikoene. Ledelsen i virksomheten bør sikre at ansvar og myndighet for roller som er relevante for informasjonssikkerhet, er tildelt og kommunisert. Videre bør det sikres at nødvendig kompetanse og ressurser er tilgjengelig, og ledelsen bør sikre veiledning om og støtte til styringssystemet og informasjonssikkerhet. Virksomheten bør også sørge for at utkontraherte prosesser styres.

Nasjonal sikkerhetsmyndighet (NSM) har laget noen grunnprinsipper for IKT-sikkerhet. Grunnprinsippene er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.[13]

Virksomheter må gjøre vurderinger av informasjonssikkerhet selv om IKT-infrastruktur og -tjenester er satt ut til eksterne leverandører. NSM har gitt ut sikkerhetsfaglige anbefalinger ved tjenesteutsetting (outsourcing). For å ivareta IKT-sikkerheten ved tjenesteutsetting anbefaler NSM at virksomheten er bevisst behovet for:

- oversikt og kontroll på hele livsløpet
- god bestillerkompetanse
- gode risikovurderinger for å kunne ta riktig beslutning
- riktige og gode krav til IKT-tjenesten og til leverandør
- riktig beslutning på riktig nivå

[8] https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet.
[9] https://www.difi.no/nyhet/2016/09/innebygd-informasjonssikkerhet.
[10] Direktoratet viser til at innebygd informasjonssikkerhet oppnås når informasjonssikkerhet er: Innarbeidet i virksomhetsstyringen og understøtter virksomhetens mål, innarbeidet i virksomhetens prosesser og prosjekter fra starten av, tatt hensyn til i hele livssyklusen til IKT-løsninger, og er et tema alle ansatte kjenner til og vet hva innebærer for sine arbeidsoppgaver.
[11] https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001.
[12] Jf. NS-ISO/IEC 27001;2017 punkt 6 og https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001.
[13] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

3.3 Krav til Utenriksdepartementets oppfølging av Norfund

I Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping* (eierskapsmeldingen) uttrykker staten en tydelig forventning til at selskaper med direkte statlig eierskap skal ha effektiv risikostyring som er tilpasset selskapets virksomhet, mål og strategi.[14] I eierskapsmeldingen er det videre satt krav om at styrene i selskapene med direkte statlig eierskap skal levere på statens mål som eier og ta eierskap til områdene der staten har forventninger. Ved svak måloppnåelse over tid eller vesentlige avvik fra statens forventninger, vurderer staten hvordan dette kan følges opp. Dette skjer først og fremst gjennom eierdialogen og ved behov gjennom beslutninger på generalforsamling.

Meld St. 27 (2013–2014) *Et mangfoldig og verdiskapende eierskap* inneholder en tilsvarende beskrivelse av eiers oppfølging av statlig eide selskaper.[15] Det framgår av stortingsmeldingen at staten som eier kan øve innflytelse på selskapets virksomhet gjennom deltakelse i nominasjonsprosesser og valg til styrende organer, fastlegging av selskapets formål og øvrige vedtektsbestemmelser, og gjennom å trekke opp rammer for virksomheten på generalforsamlingen.

I reglement for økonomistyring i staten er det satt krav til departementer som har overordnet ansvar for selskaper.[16] Der framgår det blant annet at staten skal, innenfor gjeldende lover og regler, forvalte sine eierinteresser i samsvar med overordnede prinsipper for god eierstyring, blant annet med vekt på at den valgte selskapsform, selskapets vedtekter, finansiering og styresammensetning er hensiktsmessig i forhold til selskapets formål og eierskap og at styret fungerer tilfredsstillende. Styring, oppfølging og kontroll samt tilhørende retningslinjer skal tilpasses statens eierandel, selskapets egenart og risiko og vesentlighet.

[14] Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping,* jf. Innst. 225 S (2019–2020).
[15] Meld St. 27 (2013–2014) *Et mangfoldig og verdiskapende eierskap*, jf. Innst.140 S (2014–2015).
[16] Reglement for økonomistyring i staten, § 10.

4 Hva skjedde da Norfund ble svindlet?

4.1 En kort redegjørelse for svindelhendelsen

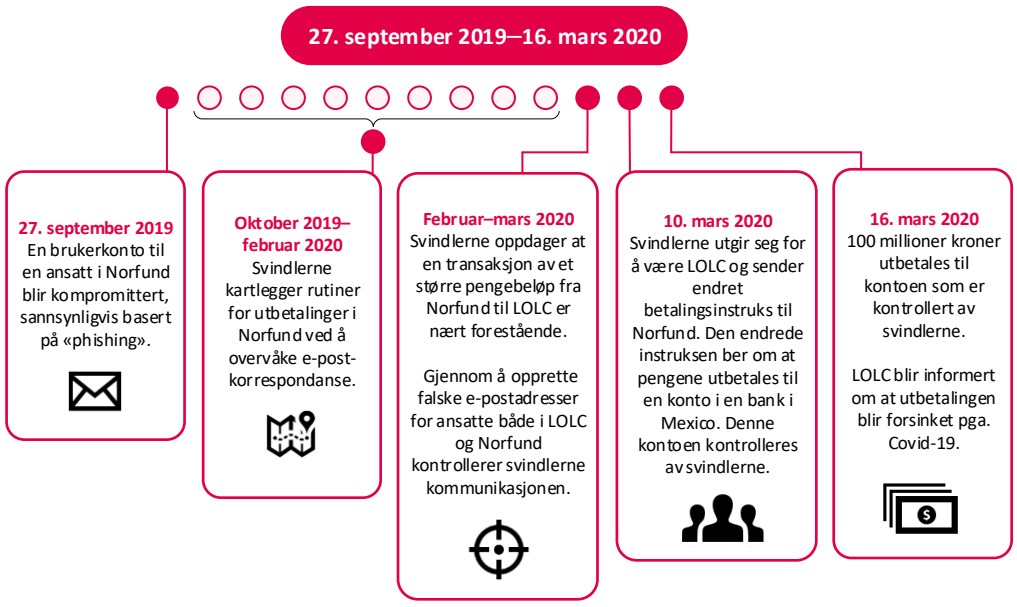
I slutten av september 2019 ble en e-postkonto tilhørende en ansatt ved regionkontoret til Norfund i Bangkok kompromittert. Dette skjedde trolig gjennom nettfiske («phishing»)[17] og uten bruk av skadelig programvare. Etter at e-postkontoen ble kompromittert, ble den i flere måneder overvåket av svindlere som kartla Norfunds rutiner og kommunikasjon. Gjennom overvåkningen fikk svindlerne i begynnelsen av mars 2020 informasjon om en transaksjon på 100 millioner kroner som skulle skje samme måned mellom Norfund og finansinstitusjonen LOLC Plc. (heretter LOLC) i Kambodsja.

Svindlerne opprettet da falske e-postkontoer og utga seg for å være henholdsvis Norfund og LOLC. På den måten infiltrerte de e-postkommunikasjonen, og fikk endret betalingsdetaljene slik at pengene ble overført til svindlernes bankkonto i Mexico 16. mars 2020. Etter 16. mars fortsatte svindlerne å sende falske e-poster til begge parter for å utsette at svindelen ble oppdaget. Til LOLC skrev de at utbetalingen var forsinket grunnet Covid 19, mens de til Norfund skrev at LOLC hadde mottatt utbetalingen. Etter henvendelse fra LOLC om at de ikke hadde mottatt utbetalingen, får Norfund en bekreftelse på overføringen fra DnB. I en e-post 30. april opplyser LOLC at kontoen i Mexico ikke tilhører dem. Omtrent samtidig blir betalingsdetaljene i en transaksjon som skal gå fra Norfund til en annen mottaker i Kambodsja forsøkt endret til samme bank i Mexico. En ansatt i Norfund stiller imidlertid spørsmål ved dette, og får bekreftet av rettmessig mottaker at bankkontoen i Mexico ikke tilhører dem.

Ifølge Norfund er det ikke uvanlig at utbetalinger går til eller via andre land enn det landet mottakeren er fra. Dette er aktuelt i land som mangler gode finansinstitusjoner, men det gjøres også rutinemessig utbetalinger via korresponderende banker i tredjeland. Ifølge Norfund er det i seg selv ikke uvanlig at det gjøres utbetalinger til banker i Mexico, men det er ifølge selskapet uvanlig at utbetalinger til Kambodsja går via en bank i Mexico.

Betalingsrutinene til Norfund ble fulgt da utbetalingen til kontoen i Mexico ble gjennomført.

Figur 1 Hvordan skjedde svindelen?



[17] Nettfiske/phishing er forsøk på svindel eller manipulasjon der bakmennene, ofte ved å sende en e-post, forsøker å lure brukeren til å oppgi sensitive opplysninger (f.eks. passord) eller klikke på lenker som laster ned skadevare.

4.2 Håndteringen av hendelsen så langt

Pengene ble overført til svindlernes bankkonto i Mexico 16. mars 2020, mens svindelen ble oppdaget først 30. april.

Styret i Norfund og Utenriksdepartementet[18] ble orientert umiddelbart etter at Norfund oppdaget svindelen. Norfunds bankforbindelse, DNB, ble varslet og kontaktet involverte banker for å søke å spore og tilbakekalle betalingen. DNB varslet også om svindelen gjennom sitt internasjonale meldingssystem. Norfund kontaktet politiet for å anmelde forholdet, samt anmode om bistand til å forfølge pågående bedrageriforsøk. Alle utbetalinger ble stoppet inntil videre, og undersøkelser av interne rutiner og kontrolltiltak ble iverksatt.

Norfunds leverandør av IKT-tjenester ble raskt involvert for å undersøke eventuell infiltrering av Norfunds e-post/nettverk. Norfund engasjerte den 5. mai 2020 PwCs cybersikkerhetsteam for å bistå med håndtering av hendelsen. Det ble også innført diverse strakstiltak, blant annet for å styrke IT-sikkerheten.

PwC ble også engasjert av Norfunds styre den 6. mai 2020 for å gjøre en uavhengig gjennomgang av hendelsen for å identifisere årsaker og mulige tiltak. Gjennomgangen skulle primært fokusere på håndtering av finansiell kontroll, betalingsrutiner og IKT-infrastruktur, samt styring og styringsverktøy relatert til disse prosessene.

Endelig rapport fra PwC ble avgitt til Norfunds styre 3. juli 2020. Rapporten og et brev fra styret der det blir redegjort for rapportens hovedfunn, igangsatte tiltak og forslag til videre oppfølging fra Norfund, ble sendt til utviklingsministeren 9. juli 2020. I brevets oppsummering står det at styret og administrasjonen systematisk vil gjennomgå og følge opp funnene og tiltakene som er anbefalt i rapporten.

Utenriksdepartementet mener Norfund har vist en stor grad av åpenhet om svindelen de ble utsatt for. Departementet mener at Norfund har vist handlekraft i situasjonen og raskt igangsatt tiltak. Utenriksdepartementet har gjennomgått rapporten og registrerer at hendelsen og nødvendige tiltak ser ut til å bli godt ivaretatt av selskapet. Utenriksdepartementet uttaler at de ikke fant det nødvendig å gi ytterligere føringer til Norfund om videre håndtering av hendelsen. Dette begrunner departementet med informasjon mottatt gjennom styreleders møter med utviklingsministeren, departementets gjennomgang av PwC-rapporten og styreleders redegjørelse om oppfølging av rapporten. Utenriksdepartementet opplyser at orientering om videre oppfølging av hendelsen er inntatt i eierstyringsdialogen.

Av hensyn til etterforskningen og i samråd med politiet gikk Norfund ikke offentlig ut med saken før 13. mai 2020. Det ble da gjennomført en pressekonferanse. Norfund har uttalt at det er viktig for selskapet å være åpne om hendelsen, ikke minst for å redusere risikoen for at andre blir utsatt for noe lignende.

Så langt er det ikke avdekket hvem som står bak svindelen. Politiets etterforskning er ikke avsluttet, og både politiet og Norfund har igangsatt separate prosesser mot banken i Mexico som mottok utbetalingen.[19]

[18] Sentral kontrollenhet i Utenriksdepartementet ble også orientert.
[19] Gjennomgangen i kapittel 4 baserer seg på følgende dokumenter:
- Verifisert referat fra møte mellom Riksrevisjonen og Norfund 18. juni 2020.
- Brev fra styreleder i Norfund til Utenriksdepartementet *Orientering fra styret i Norfund,* 5. juni 2020
- Rapport, *Independent Assessment of the LOLC incident*, Report developed for Norfund, PwC 30. juni 2020.
- Brev fra styreleder i Norfund til Utenriksdepartementet *Orientering fra styret i Norfund,* 9. juli 2020.
- Verifisert referat fra møte mellom Utenriksdepartementet og Riksrevisjonen 4. september 2020.
- Brev fra Utenriksdepartementet til Riksrevisjonen 22. oktober 2020.

5 Norfunds styring av informasjonssikkerhet

Informasjonssikkerhet innebærer at informasjon i en virksomhet ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet).

Relevante føringer[20]

- Norfund skal ha effektiv risikostyring som er tilpasset selskapets virksomhet, mål og strategi:
  - Effektiv risikostyring forutsetter at risikovurderinger er integrert i selskapets strategi, kjernevirksomhet og beslutningsprosesser.
  - Det er vesentlig å identifisere relevant risiko.
- Norfund har ansvar for informasjonssikkerhet selv om IKT-infrastruktur og -tjenester er satt ut til eksterne leverandører.
- En vellykket utsetting av IKT-tjenester fordrer at virksomheten har god bestillerkompetanse.
- I et styringssystem for informasjonssikkerhet bør
  - sikkerhetstiltak gjennomføres for å håndtere identifiserte risikoer
  - ansvar for informasjonssikkerhet være tydelig plassert
  - nødvendig kompetanse og ressurser være tilgjengelig
- Norfund bør gjennomføre sikkerhetstiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.

Oppsummering
Undersøkelsen av Norfunds styring av informasjonssikkerhet viser at selskapet:

- har hatt mest oppmerksomhet rettet mot risiko i sine investeringer og på investeringsprosessen
- har undervurdert informasjonssikkerhet som risiko
- ikke har hatt et styringssystem for informasjonssikkerhet
- ikke har hatt tilstrekkelig kompetanse eller ressurser til å følge opp tjenesteleverandørene av IKT-tjenester
- ikke hadde avklart roller og ansvar for håndtering av sikkerhetshendelser
- manglet skriftlige rutiner for håndtering av varsler som kan være tegn på dataangrep
- ikke har gjennomført sikkerhetstiltak tidsnok til å kunne forhindre svindelhendelsen
- fortsatt har svakheter i informasjonssikkerheten per august 2020

5.1 Risikostyring

5.1.1 Informasjonssikkerhet har vært undervurdert som en risiko i Norfund

Norfund har hatt mest oppmerksomhet rettet mot risiko i sine investeringer og på investeringsprosessen

Ifølge Norfund er selskapet eksponert for risikoer på flere ulike områder. Det skyldes at selskapet investerer i utviklingsland og innenfor risikoutsatte sektorer, i tråd med mandatet. Selskapet skal blant annet prioritere investeringer som ellers ikke ville blitt igangsatt på grunn av høyt risikonivå.

Norfund gjør hvert år en analyse av selskapets overordnede risiko. Analysen oppsummeres i en egen rapport til styret. I analysene som er gjennomført for årene 2017–2019, er temaene hovedsakelig finansiell risiko i porteføljen, landrisiko, sektorfordeling og selskapsrisiko. Dette er områder som er knyttet opp til selskapets kjernevirksomhet og de sektorpolitiske målene som er satt for selskapet.

Norfund peker på at fordi den identifiserte risikoen er knyttet til virksomhetsmålene og relatert til investeringsprosessen og porteføljen, har selskapets arbeid med risikostyring i hovedsak vært rettet mot:

- krav til undersøkelser og dokumentasjon i investeringsprosesser
- risiko i enkeltinvesteringer og land
- korrupsjon
- sikkerhet for ansatte på reise

[20] Se kapittel 3 Revisjonskriterier.

- intern svindel og misligheter.

5.1.2 Informasjonssikkerhet har vært undervurdert som en risiko

Informasjonssikkerhet har ikke vært et tema i de overordnede risikovurderingene i årene 2017–2019. Det er heller ikke tema i selskapets kvartals- eller årsrapporter.

Norfund bekrefter i intervju at oppmerksomheten ikke har vært rettet mot informasjonssikkerhet. I forbindelse med at reglene om GDPR trådte i kraft i Norge 1. juli 2018, har selskapet imidlertid foretatt en risikovurdering av håndtering av alle personopplysninger.

Ifølge Norfund har risikoen for interne misligheter medført at kontrollaktiviteter og -rutiner har vært innrettet mot å avverge intern svindel. Norfund har ment at omdømmerisikoen kan være større ved intern svindel enn ved ekstern svindel. Ifølge selskapet har trussel fra eksterne svindlere ikke fått like stor oppmerksomhet, og dette forklarer hvorfor risikostyringen i liten grad har vært rettet mot IKT-sikkerhet og annen operasjonell og intern risiko.

Ifølge styreleder i Norfund har ikke selskapet hatt et styringsrammeverk for helhetlig risikostyring som tydelig nok beskriver roller og ansvar. Høsten 2020 skal styret vedta et slikt rammeverk som skal gi en mer helhetlig tilnærming til risikovurderinger. Som et ledd i arbeidet med et helhetlig styringsrammeverk ble det i juni 2020 opprettet et risiko- og revisjonsutvalg under selskapets styre. Selskapet er for tiden også i prosess med å kjøpe inn internrevisortjenester som skal følge opp selskapets rutiner og kontrollfunksjoner. Norfund mener at begge tiltakene vil bidra til å styrke internkontrollen i selskapet.

COSOs rammeverk for internkontroll ligger til grunn for internkontrollen i Norfund. Selskapet har satt systemet for internkontroll opp i en matrise etter COSO-modellen. Modellens beskrivelse av kontrollmiljø og risikovurdering gir hovedføringene for arbeidet som gjennomføres. Informasjonssikkerhet er ikke en del av modellen.

Styret får i juni hvert år en redegjørelse for arbeidet med internkontroll og etterlevelse. Redegjørelsen omfatter en generell statusrapportering, en redegjørelse for arbeidet som har blitt gjort siden forrige rapportering til styret, og en plan for internkontroll og etterlevelse for det påfølgende året. I rapportene til styret for årene 2017–2019, har temaene blant annet omhandlet:

- hvordan risiko rapporteres på overordnet nivå
- håndtering av personopplysninger – status på personvernområdet
- oppdatering av investeringsmanualen
- IKT-systemer
- kontroll med midler
- HR-relaterte spørsmål
- opplæring og kommunikasjon
- gap-analyse – forskrift om risikostyring og internkontroll
- organisatoriske endringer

I sin rapport om svindelsaken skriver PwC at håndtering av risiko relatert til selskapets investeringer har hatt høy prioritet. Selskapet har imidlertid ikke hatt en systematisk tilnærming til intern risiko, og tilnærmingen til denne type risiko har til en viss grad vært hendelsesstyrt.[21]

Norfund uttaler i intervju at de mener det i etterkant av svindelsaken ikke er vanskelig å være enig i at oppmerksomheten mot IKT-sikkerhet burde vært større, og at IKT-sikkerhet burde vært tatt inn som en del av selskapets overordnede risikovurderinger – og fulgt opp gjennom internkontrollen.

5.1.3 Norfund har ikke et styringssystem for informasjonssikkerhet

Et styringssystem for informasjonssikkerhet skal sikre nødvendig konfidensialitet, integritet og tilgjengelighet av virksomhetens informasjon. Kjernen i styringssystemet er en risikostyringsprosess som skal gi virksomhetens interessenter tillit til at informasjonssikkerhetsrisikoer håndteres på en adekvat måte.

[21] Jf. verifisert referat med PwC datert 2. september 2020.

Norfund har ikke hatt mål eller strategier for informasjonssikkerhet. Selskapet uttaler i intervju at de ikke har gjennomført en systematisk vurdering av hvilken informasjon selskapet bør prioritere å beskytte.

Når det gjelder policyer og prosedyrer, har selskapet hatt dokumentet «IT User Policy» og generelle bestemmelser om konfidensialitet i «Code of Conduct». Ifølge selskapet inneholder disse to dokumentene krav til ansattes bruk av Norfunds IKT-systemer.

Ifølge Norfund håndterer selskapet verken kritisk infrastruktur/tjenester eller store mengder sensitive eller kritiske data utover de opplysninger som normalt innhentes fra ansatte og forretningsforbindelser. Norfund har derfor ikke ansett det nødvendig å innføre et styringssystem for informasjonssikkerhet. Ifølge selskapet er elementer fra et slikt styringssystem likevel ivaretatt hva gjelder f.eks. rutiner for arkivering, tilgangsstyring til dokumenter, dokumentasjon av prosedyrer, policyer etc.

Norfund viser til at hovedregelen har vært at mest mulig informasjon skal være tilgjengelig for alle ansatte. Norfund mener det meste av informasjonen håndteres på en tilfredsstillende måte. Ifølge selskapet er konfidensiell eller sensitiv informasjon begrenset til personalinformasjon forvaltet av HR, informasjon i enkelte sensitive prosjekter, bankdetaljer, KYC-dokumenter[22], styredokumenter og grunnlagsdokumentasjon for ledermøter.

Ifølge Norfund har LOLC-hendelsen vist at informasjon i forbindelse med overføringer av penger (betalingsdata/cash- management) er vesentlig informasjon som må beskyttes bedre enn den har vært. Å kun benytte e-post i forbindelse med utbetalinger, har vist seg å ikke være tilstrekkelig for å beskytte denne informasjonen.

Norfund opplyser at arbeidet med å endre fokus på risiko og å kartlegge sårbarheten selskapet står overfor, har begynt.

5.2 IKT–organisering

5.2.1 Lite kapasitet til håndtering av IKT

Norfunds IKT-infrastruktur og brukerstøtte leveres i det vesentlige fra eksterne leverandører.

Ifølge ledelsen i Norfund har selskapet et mål om å være mest mulig effektive og å holde administrasjonskostnadene på et moderat nivå. Foruten det å sikre tilgang til kompetanse og et profesjonelt driftsmiljø, har dette ifølge selskapet også vært bakgrunnen for å sette ut IKT-tjenester til tredjepart.

Ansvaret for overordnet oppfølging av IKT lå per desember 2019 i Org og HR-avdelingen. Org og HR-avdelingen hadde ansvaret for oppfølging av support og oppsett for kontorer i Oslo og ute. Finansavdelingen hadde ansvar for oppfølging av enkeltsystemer.

To ansatte sto for den løpende oppfølgingen i form av dialog med leverandører, support og diverse bistand. I et notat til ledergruppen i desember 2019 kom det fram at disse også hadde andre oppgaver, og at det førte til at de ikke i stor nok grad hadde mulighet til å fokusere på de strategiske valgene innenfor IKT.

Som en del av strategiprosessen i 2019 evaluerte Norfund ansvaret for IKT i selskapet. Selskapet peker i evalueringen på at kompleksiteten i deres systemmiljø er økende, og at manglende sentralisert kontroll på sikt kan føre til en kompleks, mindre sikker og uoversiktlig IKT-løsning. I denne prosessen ble det identifisert et behov for å styrke IKT-funksjonen. Det ble også vist til at Norfund har behov for å etablere et mer robust rammeverk for videre IKT-anskaffelser, drift, sikkerhet og utvikling. Videre blir det pekt på at det er en forutsetning at den som skal håndtere en slik prosess har nødvendig kompetanse, og kapasitet, til å gjennomføre dialog med de som leverer ekstern bistand.

På denne bakgrunn vedtok selskapet i desember 2019 å ansatte en person for å ivareta ansvaret for IKT. En person ble ansatt i slutten april 2020.

Ifølge PwCs granskning av svindelhendelsen hadde ikke Norfund tilstrekkelig ressurser eller kompetanse til å følge opp leverandøren av IKT-tjenester.

[22] KYC-dokumenter: KYC står for «Know Your Customer». Dokumenter som utarbeides med det formål å forebygge og avdekke om det finansielle systemet brukes til hvitvasking eller terrorfinansiering.

5.2.2 Ingen formell stillingsinstruks for brukerstøttefunksjonen

De siste ni årene har det vært betydelig grad av utskifting i Norfunds brukerstøttefunksjon.

I avtalen om innleie av konsulent til brukerstøtte i 2020 er ikke oppgavene spesifisert utover at konsulenten under Norfunds ledelse skulle yte bistand til support og brukerstøtte hos selskapet. Det har ikke vært noen formell stillingsinstruks eller arbeidsbeskrivelser for brukerstøttefunksjonen i Norfund.

5.2.3 Ingen systematisk opplæring i IKT-sikkerhet

Etter svindelsaken i 2018 (Alios-hendelsen jf. punkt 5.3.4) så Norfund et generelt behov for å øke oppmerksomheten rundt IKT-sikkerhet i selskapet og bevisstheten om denne type kriminalitet. Under Norfund-dagene[23] høsten 2018 ble det derfor holdt en presentasjon for alle ansatte der svindelen og metodene som kan brukes i denne type saker, ble gjennomgått. Opplæringen som ble gjennomført i 2018, ble ikke gjentatt før etter at svindelhendelsen ble oppdaget i april 2020.

Norfunds opplæringsprogram for nyansatte har fram til svindelhendelsen i 2020 inkludert en gjennomgang av retningslinjer for bruk av Norfunds IKT-systemer («IT-user policy»), men ikke inkludert opplæring i informasjonssikkerhet generelt. For å styrke informasjonssikkerheten i selskapet mener Norfund at det blant annet er viktig å øke ansattes bevissthet om IKT-sikkerhet og trusselbildet gjennom gjentagende trening og opplæring.

5.3 Oppfølging av leverandøren

5.3.1 Avtalen samsvarer ikke lenger med selskapets IKT-miljø

Avtalen med Norfunds tjenesteleverandør av selskapets IKT-løsninger og -tjenester er basert på statens standardavtale og ble inngått i 2010. Leverandøren har ansvar for å levere brorparten av alle tjenester knyttet til drift og forvaltning av Norfunds IT-plattform herunder klienter, servere, nettverk, sikkerhet og applikasjoner.

Avtalen gjaldt i utgangspunktet i fire år, men blir automatisk fornyet årlig dersom ikke en av partene sier opp avtalen. Avtalen har blitt forlenget fram til 2020. Endringer siden opprinnelig inngåelse er tatt inn som nummererte vedlegg i avtalen. Det er totalt 23 vedlegg til avtalen per juli 2020.

Det har skjedd vesentlige endringer i selskapets IKT-miljø fra inngåelsen av avtalen i 2010 og til nå. Norfund har vokst betydelig som organisasjon og har nå en egenkapital på 23 milliarder kroner mot 3,5 milliarder kroner i 2010. Norfund anvender i dag andre systemer enn i 2010, blant annet for porteføljestyring og for arkiv, og har tatt i bruk skyløsningen Microsoft Office 365. Dette innebærer at den tekniske infrastrukturen beskrevet i kravspesifikasjonen og løsningsbeskrivelsene som inngår i avtalen, er vesentlig forskjellig fra den som benyttes i dag. Videre er det i kravspesifikasjonen i avtalen lagt vekt på løsninger for å møte trusselbildet i 2010, noe som innebar at drift av brannmurer og antivirusløsninger var sentrale punkter.

I avtalen legges ifølge Norfund ansvaret for IKT-sikkerhet til tjenesteleverandøren, noe som har ligget til grunn for selskapets forventninger til hva leverandøren skal levere. Etter selskapets oppfatning var IKT-sikkerheten godt ivaretatt fordi tjenesteområdet hadde blitt satt ut til en ekstern og kompetent leverandør. Norfund opplyser at selskapet bevisst valgte en stor leverandør for at sikkerheten skulle ivaretas best mulig. Selskapet opplyser at LOLC-hendelsen har vist at det har vært et gap mellom Norfunds forventninger til hva tjenesteleverandøren skulle levere, og hva som er levert med hensyn til IKT-sikkerhet.

I en intern strategiprosess identifiserer Norfund i desember 2019 at kravene til IKT i selskapet har økt og blitt mer komplekse, og at det var behov for systemer som ivaretar sikkerhet og sikrer kontroll og oversikt. Norfund hadde planlagt en evaluering av tjenesteutsettelsen i 2019, men denne ble utsatt til ny IKT-ansvarlig var på plass.

[23] Norfund-uken gjennomføres årlig. Samlingen er for alle ansatte i selskapet. En vesentlig del av uken settes av til intern opplæring og konkret trening og gjennomgang av prosedyrer.

5.3.2 Lite oppfølging av krav til IKT-sikkerhet i avtalen

Avtalen mellom Norfund og tjenesteleverandøren inneholder flere generelle krav til IKT-sikkerhet, blant annet at drift og forvaltning skal følge beste praksis innen informasjonssikkerhet ut fra ISO 27001 eller tilsvarende. Den gir også Norfund flere muligheter til å følge opp leverandøren med hensyn til sikkerhet:

- Kunden skal ha rett til å utføre årlige kvalitetsgjennomganger hos leverandør.
- Leverandøren skal gjennomføre årlige sikkerhetsrevisjoner, som skal dokumenteres og forelegges kunden.
- Kunden har rett til å gjennomføre sikkerhetsrevisjoner.
- Kunden skal godkjenne sikkerhetspolicy og regelsett for brannmurer.
- Leverandøren skal innen den 15. hver måned rapportere skriftlig om bl.a. oversikt over alvorlige og kritiske hendelser, oppfyllelse av sikkerhetskrav og forslag til forbedringsområder.

Norfund uttaler i intervju at de ikke har gjennomført kvalitetsgjennomganger eller sikkerhetsrevisjoner hos leverandøren. Leverandøren har ikke rapportert om etterlevelse av kravene til sikkerhet eller gjennomførte sikkerhetsrevisjoner, og Norfund har heller ikke etterspurt dette.

Leverandøren rapporterer jevnlig til Norfund om leverte tjenester i henhold til tjenestenivåavtale. Rapportering er i stor grad knyttet til håndtering av henvendelser fra Norfund (antall, ventetid etc.) og saker som er typiske servicedesk-saker. Det er ikke rapportering opp mot krav til sikkerhet i avtalen, og Norfund har ingen systematisk oppfølging av etterlevelse av kravene i avtalen på dette området. Ifølge Norfund har selskapet forutsatt at leverandøren har kompetanse til å sørge for tilfredsstillende sikkerhet.

I avtalen legges grunnlag for samhandling mellom Norfund og tjenesteleverandøren ut fra ulike møter. Det framgår av bilag til avtalen at koordineringsgruppen mellom kunde og leverandør skal møtes hver tredje måned, hvor leverandør innkaller og skriver referat. Driftsmøter skal avholdes etter avtale. I avtalen framgår også at minimum en gang i året skal det gjøres en kvalitetsgjennomgang av leverandørens driftsspesifikasjon, hvor kunden skal skrive referat.

Mottatt dokumentasjon viser at det er avholdt møter mellom Norfund og leverandøren. Referater viser at disse har blitt avholdt hver tredje måned i 2020, men at det over tid er avholdt sjeldnere, for eksempel kun to ganger i 2019. Ifølge Norfund omhandler møtene hovedsakelig tjenestenivårapportering, sånn som hvor mange henvendelser leverandøren har fått fra Norfund, ventetid for bistand mv.

Det framgår i PwCs rapport om svindelen at ledelsen i Norfund har forventet at deres IKT-leverandør er proaktive med hensyn til å gi råd og veiledning om Norfunds IKT-tjenester. Leverandøren på sin side har forventet at Norfund har en klar forståelse av egne behov og kan angi blant annet forventet sikkerhetsnivå.

Norfund mener at LOLC-hendelsen viser at forventningene til hvordan en ekstern IKT-leverandør skal følges opp, er større enn hva Norfund har lagt til grunn. Ifølge Norfund har ikke selskapet hatt tilstrekkelig og dedikert kompetanse til å kunne sette strenge nok krav til tjenesteleverandøren, eller til å stille de riktige spørsmålene til IKT-sikkerhet.[24]

5.3.3 Uklare roller og ansvar for håndtering av sikkerhetshendelser (varsler)

I avtalen mellom Norfund og tjenesteleverandøren er det flere krav til håndtering av uønskede hendelser:

- Det skal foreligge en prosedyre for å melde om uønskede hendelser som en del av driftsspesifikasjon utarbeidet av leverandør.
- Norfund skal klassifisere og melde hendelser til leverandøren uten ugrunnet opphold.
- Leverandøren skal ha effektive varslingsrutiner for sikkerhetsbrudd som gjør at leverandøren raskt kan identifisere, rette og rapportere uønskede hendelser. Kontakt med kunden skal inngå i disse planene.

Ved overgang til bruk av skytjenesten Microsoft Office 365 ble muligheten til å oppdage sikkerhetshendelser rundt innlogging og e-post flyttet til Microsoft. Da skytjenesten ble tatt i bruk, rapporterte Microsoft om hendelser til Norfund, mens rutinen etter hvert ble justert slik at varsler også ble sendt til Norfunds brukerstøtte. PwC har i sin undersøkelse av svindelhendelsen pekt på at Norfunds brukerstøtte ikke har hatt en konsistent praksis for håndtering av varsler. Ifølge Norfund har ikke selskapet hatt skriftlige rutiner for håndtering av slike sikkerhetshendelser.

[24] Jf. Brev fra Norfund til Riksrevisjonens med kommentarer til utkast til rapport, 21. oktober 2020.

I løpet av 2019 og fram til hendelsen i 2020 mottok Norfund flere varsler om unormal aktivitet i flere e-postkontoer. Tre varsler gjaldt brukerkontoen som senere ble benyttet i svindelen, der Microsoft i forbindelse med det siste varselet 3. januar 2020 anså det som så høy risiko for at brukerkontoen var kompromittert at den ble stengt. Det siste varselet ble sendt videre til Norfunds tjenesteleverandør for undersøkelse, mens de to første ikke ble sendt til leverandøren. Brukerkontoen ble gjenåpnet raskt, men det kan ikke dokumenteres hvem som gjenåpnet kontoen. Det kan heller ikke dokumenteres om leverandøren foretok undersøkelser med henblikk på å finne den bakenforliggende årsaken til hendelsene som gjorde at Microsoft stengte kontoen.

Norfund mener leverandøren på selvstendig grunnlag burde ha iverksatt nødvendige undersøkelser etter å ha mottatt henvendelsen om at en brukerkonto var stengt på grunn unormal aktivitet, selv om det ikke eksplisitt var angitt at Norfund ønsket at leverandøren skulle finne den bakenforliggende årsaken til hendelsen. Norfund uttaler i intervju at da svindelen ble oppdaget, ble leverandøren spurt om det fantes tegn til at e-postkontoen var kompromittert. Etter kort tid kom det svar om at leverandøren så tegn til dette.

Som en del av dataangrepet aktiverte svindlerne videresendingsregler for e-post. Dette gjorde at de i lang tid kunne følge med på, og etterhvert infiltrere, kommunikasjonen mellom Norfund og låntakeren. Norfund mener det bør kunne forventes at en tjenesteleverandør med ansvar for IKT-sikkerhet gjennomfører regelmessige kontroller og undersøkelser av unormale videresendingsregler til eksterne adresser.

5.3.4 Tiltak besluttet etter tidligere svindelhendelse tok lang tid å implementere

Alios-hendelsen

I juni 2018 ble det oppdaget at en av Norfunds samarbeidspartnere, Alios Tanzania og Alios Zambia, hadde blitt utsatt for svindel. Norfund kunne ikke se at Alios hadde betalt en faktura med avdrag innen forfall, og selskapet ble derfor purret opp. Da Alios kunne legge fram dokumentasjon på at beløpet var betalt, ble det oppdaget at avdraget på 800 000 dollar var manipulert og utbetalt til feil konto.

De påfølgende undersøkelsene viste at svindlere hadde sendt en e-post til Alios der de utga seg for å være Norfund med en kopi av fakturaen fra Norfund. På den forfalskede fakturaen var kontonummeret til Norfund byttet ut med kontonummeret til et annet norsk selskap med konto i DnB. I e-posten til Alios stod det at Norfund hadde fått en ny aktiv konto for innbetaling av avdrag og renter. Undersøkelsene tydet ikke på at svindelen hadde skjedd som følge av dataangrep eller sikkerhetsbrudd hos Norfund.

Besluttede tiltak som følge av Alios-hendelsen

Saken førte til at Norfund økte sin oppmerksomhet rundt IT-sikkerhet. Norfund mente at bedrageriet var en påminnelse om at de måtte være på vakt, og at det var behov for å øke bevisstheten om denne type kriminalitet i selskapet. I august 2018 ble det derfor iverksatt tiltak som hadde som mål å forbedre interne rutiner. Norfund vurderte det hensiktsmessig med en fullstendig gjennomgang av IKT-sikkerhet generelt og sending av e-post spesielt. Diskusjoner med en innleid konsulent og leverandøren av IKT-tjenester førte til at det i slutten av august 2018 ble laget en endring i driftsavtalen med leverandøren av IKT-tjenester der besluttede sikkerhetstiltak ble bestilt. Implementering av tiltakene var anslått til 60 timer. Norfund bestemte å innføre skytjenesten Microsoft Office 365 i dette tidsrommet, og innføring av multifaktor-autentisering var et viktig sikkerhetstiltak i den forbindelse.

Faktaboks 1 Multifaktor-autentisering for sikker identifisering ved bruk av skytjenester

Angripere forsøker ofte å få kontroll over en legitim brukerkonto. Autentisering er prosessen for å identifisere brukeren. Multifaktor-autentisering (MFA) innebærer at en bruker må oppgi en kode fra for eksempel et smartkort eller en applikasjon på mobiltelefon ved siden av passord, slik at det gir en sikrere identifisering av bruker. Dette avhjelper sårbarheter ved at svake passord kan gjettes, passord kan gjenbrukes på forskjellige tjenester eller brukere lures til å oppgi passord ved sosial manipulasjon. NSM har observert mange tilfeller der angripere forsøker å logge seg på skytjenester som Microsoft Office 365 uten MFA, og anbefaler derfor bruk av MFA ved bruk av disse tjenestene.

Kilde: NSM: Hvordan sikre Exchange og Office 365 og NSM: Grunnprinsipper for IKT-sikkerhet, versjon 2.0

Gjennomføringen av besluttede tiltak tok lang tid

I juni 2019 blir styret i Norfund orientert om at alle brukere de siste 12 månedene er oppgradert til Office 365 og hadde e-post «i skyen». Styret ble i samme møte også orientert om at det ble jobbet med innføring av to-trinns autentisering (MFA) for å gjøre pålogging sikrere.

Innføringen av multifaktor-autentisering (MFA) stoppet opp hos leverandøren. Det er ikke dokumentert at Norfund fulgte opp leveransen før i januar 2020. MFA ble gjennomført 7. april 2020. Dataangrepet hvor svindelaktøren fikk kontroll over en brukers e-postkonto i Norfund, skjedde i september 2019.

Norfund uttaler i intervju at bruk av e-post er en viktig del av investeringsprosessen. Overgang til skytjenesten Microsoft Office 365 eksponerte Norfunds e-post for økt risiko fordi innlogging skjer fra Internett. PwC mener at overgang til Microsoft Office 365 uten at viktige sikkerhetstiltak var på plass, betød at Norfunds IKT-sikkerhet ikke var tilpasset nye trusler. Etter PwCs syn ble disse svakhetene utnyttet når angriperen fikk kontroll over e-postkontoen som ble brukt ved svindelhendelsen.

Ifølge Norfund er det flere årsaker til at implementeringen av tiltak for å øke IKT-sikkerheten ikke ble prioritert og gjennomført:

- stor arbeidsbelastning i Norfund, herunder håndtering av enkelthendelser som for eksempel terrorangrepet mot selskapets kontor i Nairobi
- utskifting av prosjektleder hos leverandøren av IKT-tjenester etter nyttår 2018/19
- utfordringer med nettverkskapasiteten på flere av utekontorene

Ifølge Norfund er det ikke åpenbare tekniske årsaker til at implementeringen av tiltakene tok tid, utover utfordringene med nettverkskapasiteten på regionskontorene. Norfund mener at en kombinasjon av manglende dedikerte ressurser og behov for en stegvis implementering av tiltak, forklarer hvorfor implementeringen tok tid.

PwC mener at det i tillegg til ovennevnte punkter er en årsak til manglende oppfølging fra Norfunds side at selskapet generelt manglet ressurser med nødvendig kompetanse for å være ansvarlig motpart ved en IKT-leveranse. PwC mener at det ikke er noen tekniske årsaker til at implementeringen av de besluttede tiltakene for å styrke IKT-sikkerheten tok tid.[25]

PwC mener at det ble vist handlekraft i Norfund etter Alios-saken. Tiltak for å styrke sikkerheten ble utredet og besluttet, men det sviktet da tiltakene skulle gjennomføres. Leverandøren av IKT-tjenester gjennomførte ikke tiltakene, og det er ikke dokumentert at Norfund fulgte opp saken før i januar 2020.

Ifølge ledelsen i Norfund ble oppfølgingen av tiltakene håndtert på saksbehandlernivå. Ledelsen og styret fikk en kort statusrapport om arbeidet med å overføre brukerne til skybaserte løsninger og innføring av to-trinns autentisering, men ble ikke løpende orientert om videre oppfølging av tiltakene. Ledelsen viser til at den manglende oppfølgingen av tiltakene ikke var et bevisst valg fra ledelsen.

PwC mener det ikke kan utelukkes at selskapet hadde blitt utsatt for svindel selv om tiltakene etter Alios hadde blitt iverksatt umiddelbart.[26] PwC mener imidlertid at det er grunnlag for å si at innbrudd i den aktuelle e-postkontoen ville vært vanskeligere for svindlerne om tiltakene hadde blitt gjennomført.

[25] Jf. verifisert referat fra møte mellom PwC og Riksrevisjonen, 2. september 2020.
[26] Jf. verifisert referat fra møte mellom PwC og Riksrevisjonen, 2. september 2020.

5.4 Norfund har fortsatt svakheter i informasjonssikkerheten per august 2020

For å få et mer helhetlig bilde av informasjonssikkerheten i Norfund er det foretatt noen kontroller av tekniske sikkerhetstiltak. Sikkerhetstiltakene vi har vurdert, har ikke direkte sammenheng med svindelhendelsen i Norfund, men er andre viktige tiltak for å sikre Norfunds verdier. Utgangspunktet har vært anbefalte sikkerhetstiltak i NSMs Grunnprinsipper for IKT-sikkerhet, hvor NSMs anbefalinger av fire effektive sikkerhetstiltak for å stoppe dataangrep har vært viktige for valg av hvilke tiltak som undersøkelsen omfatter.

Faktaboks 2 Fire effektive tiltak mot dataangrep

NSM mener de fleste dataangrep teknisk sett er relativt enkle å stoppe og har lagt fram fire tekniske tiltak som kan stoppe 80–90 prosent av angrepene:

- oppgrader program- og maskinvare.
- installer sikkerhetsoppdateringer så fort som mulig.
- ikke tildel administratorrettigheter til sluttbrukere.
- blokker kjøring av ikke-autoriserte programmer («hvitelisting»).

Kilde: NSM: Sjekkliste: Fire effektive tiltak mot dataangrep

Analyse av uttrekk fra Norfunds systemer i august 2020 viser at selskapet ikke følger anbefalingene om sikkerhetstiltak:

- Det benyttes i noen grad programvare som ikke lenger støttes av leverandør, og som det dermed ikke lenger mottas sikkerhetsoppdateringer for. Gammel programvare har dårligere sikkerhetsfunksjoner og har kjente sårbarheter som kan utnyttes ved dataangrep.
- Det er svakheter i sikkerhetsoppdateringer ved at noen typer programvare ikke blir oppdatert, eller at programvare på enkelte maskiner ikke blir oppdatert. For noen svakheter finnes ferdiglagde programmer tilgjengelige på Internett som kan utnytte sårbarhetene i et dataangrep.
- Langt flere brukerkontoer har mer rettigheter i Norfunds systemer enn det som følger av beste praksis. De fleste av disse kontoene er hos selskapets tjenesteleverandør. Beste praksis tilsier at tilgangsrettigheter begrenses til tjenstlig behov. Kontoer med mange rettigheter er ofte et mål i et dataangrep for å få full kontroll over IKT-systemer.
- Norfund har mangelfulle tiltak for å sikre at kun godkjent programvare kjøres i virksomhetens nettverk. Dette gjør det vanskeligere for selskapet å sørge for at programvare blir oppdatert, i tillegg til at det gjør det enklere å kjøre skadelig programvare i selskapets nettverk.

Sikkerhetsoppdateringer er en oppgave som Norfund har satt ut til tjenesteleverandør, og brukerkontoer med høye rettigheter er også i stor grad knyttet til tjenesteleverandørs oppgaveløsning. Ifølge Norfund mottar de ikke rapportering om sikkerhetsoppdateringer, og følger heller ikke opp i etterkant at sikkerhetsoppdateringer er gjennomført. Selskapet mener tjenesteleverandørens tilganger i Norfunds systemer er regulert av avtalen. Norfund har derfor ingen oppfølging av dette.

Norfund har satt krav om at brukere skal sikre at deres passord ikke blir kjent, og at de ikke skal skrive ned passord.[27] Analyse av oversendt dokumentasjon viser enkelte dokumenter der flere passord for administrasjon av IKT-tjenester er skrevet ned i klartekst, og er tilgjengelig for flere personer.

Vår undersøkelse av tekniske sikkerhetstiltak er nærmere omtalt i vedlegg til rapporten. Vedlegget er unntatt offentlighet.

[27] Norfund, *IT User Policy*.

6 Utenriksdepartementets eierstyring av Norfund med utgangspunkt i svindelhendelsen

Relevante føringer[28]

- Utenriksdepartementets eierstyring, oppfølging og kontroll samt tilhørende retningslinjer skal tilpasses statens eierandel, selskapets egenart og risiko og vesentlighet.
- Styret skal påse at selskapet har god intern kontroll og hensiktsmessige systemer for risikostyring, mens svak måloppnåelse over tid må følges opp av Utenriksdepartementet.

Oppsummering

Undersøkelsen av Utenriksdepartementets eierstyring med utgangspunkt i svindelhendelsen, viser at:

- Utenriksdepartementet er opptatt av Norfunds måloppnåelse som instrument i norsk utviklingspolitikk.
- Informasjonssikkerhet og IT-risiko har ikke vært tema i kontaktmøtene mellom Norfund og Utenriksdepartementet.

6.1 Utenriksdepartementets styring er knyttet til Norfund som virkemiddel i utviklingspolitikken

Ifølge Utenriksdepartementet er Norfund et viktig instrument i norsk utviklingspolitikk. Selskapet er regjeringens virkemiddel i satsingen på næringsutvikling i utviklingsland. Det er en forventning til at statlig eide selskaper har effektiv risikostyring som er tilpasset selskapets virksomhet, mål og strategi.

Utenriksdepartementet uttaler at departementet ikke har gitt konkrete føringer knyttet til Norfunds operasjonelle virksomhet ut over det som er nedfelt i Norfunds mandat (Lov om Norfund) og vedtekter, og i budsjettproposisjoner. Informasjonsssikkerhet og Norfunds håndtering av IKT-sikkerhet har dermed ikke vært et eget tema i dialogen mellom Utenriksdepartementet og Norfund.

Faktaboks 3 Hovedtrekk i Norfunds vedtekter

Norfund skal prioritere å investere i alle ODA-godkjente land, jf. OECD/DACs retningslinjer, samt i de land der Stortinget vedtar at næringsutviklingskapittelet på bistandsbudsjettet skal gjelde. Prioritet skal gis til Afrika sør for Sahara og de minst utviklede landene. Norfund skal prioritere investeringer i fornybar energi, som over tid bør utgjøre om lag halvparten av tilført kapital. Norfund forventes å foreta investeringer i risikoutsatte sektorer der utviklingseffektene er særlig høye, herunder i verdikjedene knyttet til landbruk og fiskeoppdrett.

Kilde: Vedtekter for statens investeringsfond for næringsvirksomhet i utviklingsland (Norfund). Fastsatt av ordinær generalforsamling i Norfund 18. juni 2018 med hjemmel i lov av 9. mai 1997 nr. 26 om statens investeringsfond for næringsvirksomhet i utviklingsland (NORFUND) § 8.

6.1.1 Dialogen mellom Utenriksdepartementet og Norfund

Det avholdes fem kontaktmøter mellom Utenriksdepartementet og Norfund i året. Kontaktmøtene har form av tematiske gjennomganger om utviklingseffekter av investeringene, resultater knyttet til viktige nøkkeltall (KPI'er), risikovurderinger, rapportering, ansvarlighet og utviklingspolitikk. Ifølge Utenriksdepartementet er formålet med møtene i eierstyringsdialogen informasjonsutveksling som danner grunnlag for videre oppfølging, forberedelser og generalforsamlingsvedtak.

Utenriksdepartementet uttaler at de er opptatt av utviklingseffekter og hvordan disse måles. Ifølge departementet diskuteres også andre temaer med Norfund, for eksempel hva som pågår innfor næringsutvikling i andre fora som EDFI (den europeiske organisasjonen for investeringsfond i utviklingsland) og i andre utviklingsfinansieringsinstitusjoner i andre land og i OECD, særlig knyttet til standardutvikling for måling og rapportering.

Utenriksdepartementet uttaler i intervju at de har hatt dialog med Norfund om blant annet anbefalinger gitt i uavhengige evalueringsrapporter om Norfund. Norfund har utviklet policy på likestilling, og styret har nylig

[28] Se kapittel 3 Revisjonskriterier.

vedtatt en klimastrategi. Norfund har også jobbet med å revidere dokumentasjon/policy knyttet til menneskerettigheter og arbeidsrettigheter. Retningslinjene er retningsgivende for selskapets investeringsvirksomhet. Utenriksdepartementet mener det er viktig at disse dokumentene er tilgjengelige på selskapets hjemmeside og at de revideres jevnlig.

Utenriksdepartementet har årlige møter med hvert medlem av styret og med administrerende direktør i Norfund. Møtene handler om Norfunds ledelse og drift, basert på veiledning fra Nærings- og fiskeridepartementet. Ifølge departementet blir innholdet i møtene oppsummert i notat til statsråden og utgjør et grunnlag for valg av styre.

Den formelle eierstyringen av Norfund utøves på generalforsamlingen. Det er vanlig at utviklingsministeren deltar på disse. Når den formelle delen av generalforsamlingen er avsluttet, får utviklingsministeren normalt en grundig orientering om utviklingen av fondet.

6.1.2 Dialog mellom Utenriksdepartementet og styret i Norfund om risikostyring og internkontroll i Norfund

Ved valg av styre er Utenriksdepartementet opptatt av å finne styremedlemmer med riktig kompetanse, og vektlegger kompetansebehov og ivaretakelse av mangfold. Utenriksdepartementet ønsker styremedlemmer som har kunnskap om investeringsaktivitet i utviklingsland, bistand eller lignende i landene Norfund opererer i, og at de forstår risikoen forbundet med å investere i utviklingsland.

Ifølge departementet utarbeides det en kompetansevurdering av styret, som blant annet redegjør for eventuelle behov styret har for økt kompetanse. Denne legges til grunn for endringer i styret.

Ifølge Utenriksdepartementet har risikostyring vært et tema i de årlige møtene med hvert styremedlem. I intervju uttaler departementet at de i samtalene med styrets medlemmer har innhentet informasjon om hvordan styret forholder seg til det sammensatte risikobildet Norfund skal håndtere. Ifølge Utenriksdepartementet har styret i samtalene vært bevisste på og opptatte av risikostyring og internkontroll. Departementet mener at det derfor ikke har vært grunnlag for å gi styret ytterligere føringer for eller forventninger til Norfunds risikostyring og internkontroll.

Utenriksdepartementet opplyser at de har blitt orientert om Norfunds arbeid med å styrke risikostyring og internkontroll, blant annet gjennom endringer i ledergruppen i selskapet. Det er departementets forståelse at risikostyring og risikoforståelse i bredt har vært et tema i styret.

Tidligere mottok Utenriksdepartementet alle styreprotokollene fra Norfund. I 2016 ble praksisen endret fordi Utenriksdepartementet ikke anså det som nødvendig for å ivareta eierskapsutøvelsen. Fram til 2017 rapporterte også Norfund alle mislighetssaker til sentral kontrollenhet[29] i Utenriksdepartementet. Fra 2017 har det vært styret som avgjør om hendelsen er av en slik avlorligshetsgrad at Utenriksdepartementet skal varsles. Varslet sendes til eierstyrer med kopi til sentral kontrollenhet i departementet.

Ifølge Utenriksdepartementet ble de ikke varslet om Alios-saken i 2018. Departementet opplyser at det ikke har vært dialog om denne saken mellom Utenriksdepartementet og Norfund.

Utenriksdepartementet opplyser at de som følge av svindelhendelsen våren 2020 har blitt mer oppmerksom på utfordringer og risiko knyttet til driften av Norfund, og vil ønske å bli holdt orientert om eventuelle ytterligere utfordringer selskapet har knyttet til driften. Departementet vil følge dette opp i kontaktmøtene i tiden fremover.

[29] Sentral kontrollenhet er en egen avdeling i Utenriksdepartementet, og den behandler saker som gjelder mistanke om brudd på gjeldende regelverk i utenrikstjenesten med mindre ansvaret for oppfølging er lagt til en annen enhet. Fire ganger i året legger sentral kontrollenhet fram en oversikt over saker der det er varslet mistanke om økonomiske misligheter, tiltak og status for oppfølging.

7 Vurderinger

7.1 Svindelen av Norfund for 100 millioner var mulig fordi selskapet har hatt manglende bevissthet om og forståelse for informasjonssikkerhet

7.1.1 Norfund har undervurdert informasjonssikkerhet som en risiko

Norfund skal ha effektiv risikostyring som er tilpasset selskapets virksomhet, mål og strategi. Det påligger Norfund å identifisere relevant risiko.

Undersøkelsen viser at Norfund i sine risikovurderinger har hatt mest oppmerksomhet rettet mot risiko ved selskapets kjernevirksomhet og de sektorpolitiske målene. Selskapet har i liten grad vurdert informasjonssikkerhet som en relevant risiko eller etablert et styringssystem for informasjonssikkerhet. De har heller ikke hatt mål eller strategier for informasjonssikkerhet. Selskapet har ikke gjennomført en systematisk vurdering av hvilken informasjon selskapet bør prioritere å beskytte.

I etterkant av svindelsaken mener Norfund at det ikke er vanskelig å være enig i at oppmerksomheten om IKT-sikkerhet burde vært større, og at IKT-sikkerhet burde vært tatt inn som en del av selskapets overordnede risikovurderinger – og fulgt opp gjennom internkontrollen.

I 2018 ble Norfund berørt av en liknende svindelsak, Alios-hendelsen, der en av deres låntakere etter et dataangrep ble lurt til å betale avdrag på lånet de hadde i Norfund til svindleres bankkonto. Norfund mente at denne hendelsen var en påminnelse om at de måtte være på vakt, og at det var behov for å øke bevisstheten om denne type kriminalitet i selskapet.

Selv om Alios-hendelsen rammet Norfund indirekte, ble Norfund gjort oppmerksomme på hendelsen, og det ble vurdert som nødvendig å iverksette tiltak i etterkant av denne. Etter vår vurdering burde Alios-hendelsen gjort selskapet bevisst på at det var en risiko for at de kunne bli utsatt for datakriminalitet og ført til at denne risikoen ble tatt inn i de overordnede risikovurderingene.

7.1.2 Norfund har ikke hatt tilstrekkelig oppfølging av leverandøren av IKT-tjenester

Norfund har ansvaret for informasjonssikkerhet selv om IKT-infrastruktur og -tjenester er satt ut til eksterne leverandører. For å ivareta IKT-sikkerheten ved tjenesteutsetting er det anbefalt å ha god bestillerkompetanse og god kompetanse til å følge opp gjennom hele kontraktsperioden.

Norfunds IKT-tjenesteleverandører har vært fulgt opp av personer som ikke hadde dette som sin hovedoppgave. Selskapet har ikke hatt tilstrekkelig og dedikert kompetanse til å kunne stille spørsmål og sette krav til tjenesteleverandøren når det gjelder IKT-sikkerhet.

Avtalen mellom Norfund og tjenesteleverandøren inneholder flere generelle krav til IKT-sikkerhet, og gir Norfund flere muligheter til å følge opp leverandøren med hensyn til sikkerhet. Undersøkelsen viser at Norfund ikke har utnyttet disse mulighetene, for eksempel ved å gjennomføre kvalitetsgjennomganger eller sikkerhetsrevisjoner. Videre har leverandøren ikke rapportert om etterlevelse av kravene til sikkerhet eller gjennomførte sikkerhetsrevisjoner, og Norfund har heller ikke etterspurt dette.

Det var Norfunds oppfatning at IKT-sikkerheten var godt ivaretatt fordi tjenesteområdet hadde blitt satt ut til en ekstern og kompetent leverandør.

Etter vår vurdering har Norfund i for stor grad basert seg på at leverandøren skal ivareta sikkerheten.

7.1.3 Enkle tiltak kunne gjort det langt vanskeligere å gjennomføre svindelen

Særlig to sikkerhetstiltak kunne gjort det langt vanskeligere å gjennomføre svindelen:

- innføring av multifaktor-autentisering (MFA) for sikker identifisering av brukere
- gode rutiner for behandling av varsler om sikkerhetshendelser

Norfund besluttet å innføre MFA i august 2018 etter Alios-hendelsen, på samme tid som skytjenesten Microsoft Office 365 ble besluttet innført. Microsoft Office 365 var fullt implementert i løpet av våren 2019.

Manglende oppfølging fra både Norfund og tjenesteleverandør innebar imidlertid at MFA ikke ble innført før i april 2020. Ifølge Norfund er det flere årsaker til at implementeringen av MFA ikke ble prioritert:

- stor arbeidsbelastning blant annet på grunn av terrorhendelsen mot Norfunds kontor i Nairobi
- utskifting av prosjektleder hos tjenesteleverandøren
- utfordringer med nettverkskapasiteten på flere av utekontorene

Etter vår vurdering var det ikke tekniske årsaker til at implementeringen av MFA tok lang tid.

Innføring av skytjenester som Microsoft Office 365 gjør en virksomhet utsatt for datainnbrudd dersom det ikke samtidig blir innført MFA. Det ville vært langt vanskeligere for svindlerne å få kontroll over en e-postkonto i Norfund dersom MFA hadde vært innført.

Norfund har satt krav om håndtering av sikkerhetshendelser i avtalen med tjenesteleverandør, men har ingen skriftlige rutiner eller konsistent praksis for håndtering av varsler om sikkerhetsbrudd. Norfund mottok fra høsten 2019 og fram til svindelhendelsen flere varsler om mistenkelig aktivitet og om at e-postkontoer sannsynligvis var kompromittert. Tre av disse varslene gjaldt kontoen brukt i svindelhendelsen. En forsvarlig behandling av varslene kunne ha stoppet svindelen.

Etter vår vurdering har det vært mulig å gjennomføre svindelen fordi Norfund:

- har hatt manglende bevissthet om og forståelse for risiko knyttet til informasjonssikkerhet
- ikke har etterspurt informasjon om sikkerheten i egne systemer
- ikke har fulgt opp implementeringen av viktige sikkerhetstiltak
- ikke har sørget for at selskapet har hatt tilstrekkelig kompetanse til å følge opp tjenesteleverandøren

7.2 Norfund har fortsatt svakheter i informasjonssikkerheten

For å få et mer helhetlig bilde av informasjonssikkerheten i Norfund har vi foretatt noen kontroller av viktige tekniske sikkerhetstiltak per august 2020. Tiltakene ble valgt ut fra NSMs anbefalinger om fire effektive sikkerhetstiltak for å stoppe dataangrep. NSM mener disse tiltakene kan stoppe 80−90 prosent av dataangrep.

Undersøkelsen viser svakheter i de kontrollerte sikkerhetstiltakene i Norfunds systemer. Riksrevisjonens utvalgte kontroller viser at svakhetene per august 2020 er at Norfund:

- i noen grad benytter systemer som ikke lenger støttes av leverandører
- ikke oppdaterer all programvare fortløpende
- ikke har kontroll på hvilke programmer som kan kjøres i deres nettverk
- har svært mange brukere med rettigheter som gir tilgang til og kontroll over selskapets IKT-systemer, hovedsakelig hos tjenesteleverandøren.

Flere av svakhetene er knyttet til tjenesteleverandørens oppgaveløsning, men Norfund har ingen oppfølging som kan gi selskapet styring med informasjonssikkerheten.

Etter vår vurdering betyr dette at Norfund fortsatt har svakheter i informasjonssikkerheten. Selv om selskapet har gjennomført tiltak som kan hindre en tilsvarende svindelhendelse som de ble utsatt for våren 2020, gjør svakhetene selskapet fortsatt sårbart for dataangrep.

7.3 Utenriksdepartementets eierstyring

Utenriksdepartementets eierstyring av Norfund skal tilpasses statens eierandel, selskapets egenart og risiko og vesentlighet. Svak måloppnåelse over tid må følges opp av Utenriksdepartementet.

Den formelle eierstyringen av Norfund utøves på generalforsamlingen. I tillegg avholdes det fem kontaktmøter med Norfund hvert år og ett møte med hvert medlem av styret.

Informasjonssikkerhet og Norfunds håndtering av IKT-sikkerhet har ikke vært eget tema i dialogen mellom Utenriksdepartementet og Norfund. Kontaktmøtene har form av tematiske gjennomganger om utviklingseffekter av investeringene, resultater knyttet til viktige nøkkeltall (KPI-er), risikovurderinger, rapportering, ansvarlighet og utviklingspolitikk. Utenriksdepartementet har ikke gitt konkrete føringer knyttet

til Norfunds operasjonelle risiko eller operasjonelle virksomhet ut over det som er nedfelt i Norfunds mandat (Lov om Norfund) og vedtekter, og i budsjettproposisjoner.

Utenriksdepartementet mener at styremedlemmene i de årlige samtalene har vært opptatt av og bevisste på risikostyring og internkontroll. Departementet mener det ikke har vært grunnlag for å gi styret ytterligere føringer eller forventninger knyttet til Norfunds risikostyring og internkontroll. Det er styrets ansvar å påse at et selskap har god internkontroll og hensiktsmessige systemer for risikostyring.

Vi registrerer at Utenriksdepartementet ikke har funnet grunn til å følge opp informasjonssikkerheten i selskapet i dialogen med Norfund.

7.4 Norfund har vært åpne om svindelhendelsen

Selskapet har vært åpne om svindelhendelsen de har vært utsatt for, og igangsatt en granskning av hendelsen som omhandler hvordan den kunne skje. Videre jobber Norfund med å gjennomføre tiltak for å styrke selskapets informasjonssikkerhet. Dette er en tilnærming som gjør at andre selskaper og virksomheter kan lære hvordan slike hendelser kan unngås i framtiden.

Etter vår vurdering er det positivt at Norfund legger til rette for at de selv og andre skal lære av svindelhendelsen.

8 Referanseliste

Lover og forskrifter

- *Lov om Statens investeringsfond for næringsvirksomhet i utviklingsland (Norfundloven).*

Stortingsdokumenter

- Meld St. 27 (2013–2014) *Et mangfoldig og verdiskapende eierskap*, jf. Innst.140 S (2014–2015)
- Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping* side 7*,* jf. Innst. 225 S (2019–2020)

Instrukser, vedtekter og reglementer

- *Reglement for økonomistyring i staten*
- Vedtekter for statens investeringsfond for næringsvirksomhet i utviklingsland (Norfund). Fastsatt av ordinær generalforsamling i Norfund 18. juni 2018.
- Utenriksdepartementets instruks for eierskapsutøvelse av Norfund fastsatt 2013.

Rapporter, analyser, anbefalinger og prinsipper

- *Independent Assessment of the LOLC incident*, Report developed for Norfund, PwC, 30. juni 2020
- *Eierstyring og selskapsledelse*, Norsk anbefaling, 17. oktober 2018 (NUES)
- *Ledelsessystemer for informasjonssikkerhet*, NS-ISO/IEC 27001:2017
- *Risiko- og sårbarhetsanalyse (ROS) 2020*, Finanstilsynet.
- *Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester*, NSM.
- *Grunnprinsipper for IKT-sikkerhet*, versjon 2, NSM.
- NOU 2018:14 IKT-sikkerhet i alle ledd

Internettsider- og artikler

- Regjeringen: *Norfund* https://www.regjeringen.no/no/tema/utenrikssaker/utviklingssamarbeid/norfund/id707148/ [hentedato: 31. august 2020].
- Federal Bureau of Investigation: *Business Email Compromise the $26 billion scam*. https://www.ic3.gov/media/2019/190910.aspx [hentedato: 24. september 2020]
- https://dfo.no/filer/Fagomr%C3%A5der/Internkontroll/Veileder-internkontroll.pdf
- https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet
- https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet
- https://internkontroll-infosikkerhet.difi.no/regelverkskrav
- https://www.difi.no/nyhet/2016/09/innebygd-informasjonssikkerhet
- https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001
- https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/
- https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/introduksjon/
- https://www.norfund.no/our-impact/ [hentedato: 17. september 2020].
- NSM: Sjekkliste: Fire effektive tiltak mot dataangrep. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sjekkliste-fire-effektive-tiltak-mot-dataangrep/
- Microsoft: Best practices for securing Active Directory (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface
- Sean Metcalf: There's Something About Service Accounts (https://adsecurity.org/?p=4115)
- NSM: Passordanbefalinger fra Nasjonal sikkerhetsmyndighet (https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet