# Da millionene nesten forsvant …

Politioverbetjent
**Linn Breivik Erstad**
Avsnittsleder, Felles Enhet Forebygging Etterforsking (FEFE), Møre og Romsdal politidistrikt

«Hei. Jeg må be deg innstendig om raskt å overføre 2 MNOK til leverandør i Kina. Kan du raskt gjennomføre overførselen? Hilsen Tor, daglig leder.»

Transaksjonen gjennomføres av den nye økonomimedarbeideren ganske raskt etter at «Tor» oversender kontonummeret pengene skal overføres til. Den nye økonomimedarbeideren vet at Tor er på møte og regner med at det må være veldig viktig siden han sendte henne en slik e-post. Hun gjør det med en gang uten å snakke med noen. Ti dager senere går alarmen når Tor spør henne om hvorfor fakturaen på 500 000 kroner til leverandøren i Kina ikke er betalt på forfall. De forstår raskt at de har overført to millioner til en bankkonto i Nederland som ikke har noe med leverandøren å gjøre.

Pengene er tapt. Nå må de passe på omdømmet. Under ingen omstendighet må forbindelsene få vite at selskapet er lurt!

### Ikke alene

Sannsynligvis har mange av leserne opplevd ulike former for svindel-e-post. Det finnes utallige varianter som er sendt ut i stort omfang til tusenvis av bedrifter og privatpersoner i Norge og resten av verden. Det som for mange år siden startet som «katalogsvindel» og oppføringer i ulike «fiktive» telefonkataloger, har nå endt opp som en millionindustri for kriminelle nettverk. De tjener store penger på å utnytte samfunnets digitale strukturer og den økte effektiviseringen vi har fått i næringslivet.

NTAES (Nasjonalt tverretatlig analyse- og etterretningssenter) ga i februar 2019 ut en ny rapport som tok for seg ulike bedrageriformer mot næringslivet.[1] Rapporten viser at bedragerianmeldelser til politiet har økt med 36 % mot en nedgang i totale anmeldelser på 20 % for 2018. I 2018 ble det anmeldt vel 22 000 bedragerier, hvorav det i cirka 10 % av tilfellene dreide seg om foretak som var fornærmet.

Det er grunn til å tro at mørketallene er høye. Flere av foretakene (fornærmede) opplyser at de ikke anmelder forholdene fordi de har liten tro på at politiet vil oppklare forbrytelsen. I tillegg opplyser de at det er ressurskrevende å anmelde og/eller at de ikke ønsker å utsette sitt foretak for tap av omdømme ved å være åpne om slike forhold.

### Hvordan foregår egentlig internettbaserte bedragerier?

Det er flere former for bedragerier mot næringslivet i form av digital tilpasning. Her er to eksempler:

- *Phishing:* Dette er e-poster med formål å manipulere mottakeren til for eksempel å åpne e-post med vedlegg. Vedlegget er enten infisert med skadevare eller man klikker inn på en lenke til en kompromittert nettside. Slike datainnbrudd kan gi tilgang til sensitiv informasjon som senere kan brukes til et mer målrettet og sosialt manipulerende bedrageri.
- *Direktørsvindel*: Dette er e-poster som sendes til ansatte i betrodde økonomistillinger hvor e-postadressen er så lik direktørens at mottakeren tror han/hun mailer med sin sjef. Således utføres transaksjoner på direkte forespørsel fra «direktøren».


*NTAES (Nasjonalt tverretatlig analyse- og etterretningssenter) ga i februar 2019 ut en ny rapport som tok for seg ulike bedrageriformer mot næringslivet.*

*Bedragerier via e-post* defineres generelt som «Business e-mail compromise» (BEC-svindel). I flere tilfeller ser vi at kriminelle aktører har hacket en e-postkonto for å få ut informasjon fra en bedrift. De henter ut fakturaer og gjør endringer som de så sender videre

1 www.nsr-org.no/getfile.php/1312298-1554105326/Dokumenter/Eksterne%20publikasjoner/NTAES_2019-02-Bedrageri.pdf

til kunden. Kunden tror han får e-post med faktura fra rett person, men betaler altså til feil konto på grunn av endret fakturainformasjon. Det kan være umulig for mottaker å oppdage denne endringen fordi det er brukt avanserte metoder for å begå disse handlingene.

Det understrekes at endringer av kontonummer og annen informasjon ALLTID bør verifiseres muntlig.

Det er et utall av andre bedragerier-former og jeg anbefaler alle å lese rapporten fra NTAES for å få mer innblikk i temaet.

## Finansinstitusjonenes rolle

Mange av bedrageriene stanses på forsøksstadiet ved at enten truende e-poster stanses av datasikkerhetsrutiner eller ved at bankene oppdager unormale transaksjoner. Bankene har ulike verktøy og samarbeidsrutiner innenfor finanssektoren som gjør at flere transaksjoner stanses og kontrolleres før de går ut av banken.

Karl Otto Hessen, Leder for Internasjonal Betaling og Finansiering i Sparebanken Møre forteller følgende om deres arbeidsmetodikk for å avdekke svindelforsøk:

– Svindlerne blir stadig mer sofistikerte, og både vi og andre banker jobber målrettet for å forhindre svindeltransaksjoner. Målet er både å beskytte egne kunder mot tap, samt stoppe pengestrømmer til kriminell virksomhet.

Som finansinstitusjon har vi flere verktøy som kan hjelpe oss i dette arbeidet.

*Karl Otto Hessen, Leder for Internasjonal Betaling og Finansiering i Sparebanken Møre.*

Vi overvåker alle transaksjoner i realtid og basert på egenskaper ved den enkelte betalingen undersøker vi nærmere enkelte betalinger før de sendes fra banken. Etter at betalingen er sendt, må som regel mottakerbank få kontoeiers tillatelse for å kunne returnere betalingen. Kunden som mener seg svindlet, bør alltid involvere lokalt politi. Et samarbeid mellom kunde, bank og politi kan bidra til at de utenlandske bankene reagerer raskere på forespørsel om retur av betaling.

Enkelte jurisdiksjoner krever at avsenderbanken må avlegge en «indemnity statement» (erstatningsuttalelse) for å holde mottakerbanken skadesløs, dersom den angitte svindelbetalingen skulle være en korrekt betaling. I de tilfellene dette kreves, er det naturlig at selskapet som mener seg svindlet, signerer på tilsvarende erklæring overfor sin bank.

I Norden samarbeider finansinstitusjonene godt for å bekjempe cybercrime gjennom Nordic Financial CERT, der de enkelte institusjonene blant annet bidrar med å melde inn kjente svindel-/muldyrskonti.

Vi vil også presisere viktigheten av å være bevisst på hvilke opplysninger man deler, både som privatperson og i arbeidslivet. Oppgi aldri personopplysninger, kontoopplysninger, kortinformasjon, kodebrikke, kundenummer og koder basert på en e-post eller telefon du har fått, eller på nettsider som du opplever som tvilsomme. Et annet godt råd er å verifisere alle endringer på leverandørenes betalingsopplysninger, og ikke godta slike endringer på e-post/faktura. Ta alltid en telefon til kjente kontaktpersoner hos leverandøren for å få bekreftet slike endringer.

## 3,1 millioner holdt på å forsvinne

På Sunnmøre hadde vi en svindelsak i slutten av 2018 som nettopp startet med at et norsk firma ringte sin kunde i et nord-europeisk land og spurte hvorfor fakturaen på 3,1 millioner kroner ikke var betalt på forfall. Svaret han fikk var at «*joda, fakturaen var betalt samme dag til den nye kontoen de hadde fått oppgitt i e-post dagen i forveien*». Alarmen gikk. Det norske firmaet hadde ikke endret noe kontonummer og heller ikke sendt noen e-post!

Beløpet var vesentlig for firmaet og et slikt tap ville ha store konsekvenser.

Bedriften ringte heldigvis raskt til oss på øko-avsnittet i Møre og Romsdal politidistrikt og vi ga råd om hva som måtte gjøres med en gang. Bedriften ble bedt om å varsle sin bank umiddelbart om sårbarhet for angrep og mulighet for å varsle andre banker om transaksjonen. Vi tok kontakt med kunden i det andre landet og ba ham varsle sin bank om å stanse transaksjonen hvis det lot seg gjøre.

I tillegg kontaktet vi Kripos og Økokrim for å få tak i internasjonale kontaktpersoner for å starte en etterforskning og sikre verdier.

Firmaene ble også rådet til å kontakte sine IT-leverandører umiddelbart, for å undersøke hvor datainnbruddet hadde skjedd og hvem som var sårbare for nye angrep.

## Innbrudd i e-postsystemet, men transaksjon stoppes

Det viste seg raskt at det var kunden som var utsatt for et datainnbrudd. Gjerningsmenn hadde kommet seg inn via e-postsystemet. Deretter var firmaet sannsynligvis overvåket digitalt over lengre tid. Fakturaen fra det norske firmaet var hentet ut og endret med nytt kontonummer. Så var e-post med ny faktura sendt kunden uten at han kunne oppdage at e-posten var endret underveis.

Det var et krevende døgn for firmaene å vente på en avklaring om enten bank eller politi klarte å stanse transaksjonen. Men det gjorde vi altså denne gangen. Samarbeidet mellom bank og politi var meget godt i denne saken og førte til at pengene ble tilbakeført til kunden 48 timer senere.


*Det finnes utallige varianter av svindel-e-post som er sendt ut i stort omfang til tusenvis av bedrifter og privatpersoner i Norge og resten av verden.*

Vi har i flere saker på Sunnmøre sett at der bank og politi har samarbeidet ved å utveksle tidskritisk informasjon, så har vi lykkes med å beslaglegge eller sikre verdier i inn- og utland som kan tilbakeføres til fornærmede i Norge.

## Suksesshistorie til tross .... Bedriftene må være årvåkne!

Næringslivet kan ikke basere seg på at politiet vil oppklare og gjenfinne tapte verdier relatert til slik svindel i alle saker. Vi er sammen helt avhengig av at slike forsøk stanses og ikke ender opp i tap.

Med andre ord så mener vi at næringslivet sammen med politiet og bankene har en stor rolle i å forebygge og implementere sikkerhetstiltak for å redusere risikoen for slike «angrep». Politiet har som sin fremste strategi å forebygge kriminalitet og har de senere årene utviklet et mye tettere samarbeid med næringslivet i form av «Næringslivskontakter» i alle politidistrikter og ulike «Arbeidslivskriminalitetsamarbeid». Dette er tiltak som står sentralt for oss slik at vi kan se trusler og løsninger i en større sammenheng.

Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019 (KRISINO) har vist at tre av ti virksomheter har en skriftlig risikovurdering. Det er de store virksomhetene med mer enn hundre ansatte som i størst grad har slik risikovurdering.

**Hva med de mindre bedriftene?**
Hva med de små og mellomstore bedriftene? De som ikke har egne sikkerhetsrådgivere eller systemer som kan fange opp for eksempel svindel-e-post?

Er det ikke vel så viktig at alle bedrifter uavhengig av størrelse foretar en sikkerhetsgjennomgang og risikovurdering årlig for å forebygge at uønskede hendelser skjer?

Der kommer revisjons- og regnskapsbransjen inn som en viktig støttespiller for å belyse dette for næringslivet. Alle som arbeider tett opp mot bedrifter i næringslivet har mulighet til å sette søkelys på viktigheten av sikkerhetsrutiner når det gjelder for eksempel utbetalinger av penger.

## Hva med rollen til revisor og regnskapsfører?

Revisor og regnskapsfører er i en særstilling når det gjelder kontakt med bedrifter. Gjennom året gjennomføres det samtaler om drift, rutiner, økonomistyring og en rekke andre problemstillinger.

Dette er en bransje som har en unik mulighet til å løfte inn temaet om digital sikkerhet og sikkerhetsrutiner i bedriftene. Temaet kan tas opp for å redusere sårbarheten til bedriftene og for å sette søkelyset på enkle grep som kan gjøres for å unngå tap eller andre uønskede hendelser.

Revisorer og regnskapsførere bør jevnlig tilegne seg oppdatert fenomenkunnskap om ulike former for økonomisk kriminalitet slik at de kan gi råd dersom en bedrift står i en vanskelig posisjon.

Vi i politiet samarbeider godt med regnskapsførere og revisorer. Likevel opplever vi at det oftest er politiet som tar kontakt i konkrete saker med forespørsel om informasjon innenfor lovens rammer.

Vi er svært opptatt av å få vite om fenomener, trusler og hva som rører seg i næringslivet. Først når vi har en slik oppdatert kunnskap, kan vi komme i forkant for å forebygge og tette de hullene som måtte finnes for å unngå at kriminalitet kan skje. Vi har stor tro på at samarbeid mellom næringsliv, revisjon- og regnskapsbransje og politiet kan gi gode ringvirkninger for å forhindre kriminalitet.

Det er viktig å presisere at all kriminalitet bør anmeldes til politiet. Det er først når bedriftene anmelder/varsler oss at vi får kunnskapen vi må ha for å iverksette tiltak. Anmeldelser gir oss kunnskap om kriminalitet som gjør at vi kan se eventuelle nettverk som vi må jobbe opp mot. Vi håper at dere i bransjen oppfordrer næringslivet til å anmelde slike saker til politiet.

Det er viktig å minne om at en henlagt sak kan gjenopptas når det kommer nye opplysninger.

Lykke til med det viktige arbeidet dere gjør og ha et «godt årsoppgjør»!