Cybersecurity-trusler krever god internkontroll

I en virkelighet preget av digitalisering og stadig flere ukjente og komplekse risikoer, kreves tverrfaglig innsats og samarbeid mellom de som har innsikt i sikkerhet, compliance og internkontroll. Det er nødvendig for å være i forkant for å løse utfordringene effektivt.

Siviløkonom
Aase Lindahl
Partner i PwC
Hun leder et team som gir råd til virksomheter om etablering og forbedring av corporate governance, risikostyring, internkontroll.

Direktør
Eldar Lillevik
Tjenesteleder for Cybersecurity i PwC Norge

I fjor økte omfanget av såkalt «CEO-fraud» dramatisk i Norge. Dette er bedrageri der svindlere utgir seg for å være ledere i en virksomhet for så å instruere ansatte, via e-post, om å overføre penger til svindlernes kontoer. Fjorårets største enkeltbedrageri var på 400 millioner kroner. En regnskapsmedarbeider utførte transaksjonene basert på instrukser vedkommende trodde kom fra virksomhetens øverste leder. 100 av disse millionene er fortsatt på avveie, noe som gjør dette til norgeshistoriens hittil største «brekk» – større enn NOKAS-ranet i 2004.

Hvordan kunne dette skje? Kunne det vært forhindret? Finnes det en magisk formel som enkelt beskytter virksomheten mot slik kriminalitet?

La oss ta et skritt tilbake. Når vi snakker med norske virksomheter om digitalisering, er det tre viktige bekymringer som ofte kommer opp.

1. Regulering. Hvordan navigerer vi i det nye regulatoriske landskapet som kommer av digitalisering? For eksempel EUs nye personvernforordning, nye antihvitvaskregler og nye krav rundt betalingstjenester (PSD2).
2. Risiko. Hvordan håndterer vi nye risikoer som kommer av digitalisering og da for eksempel «CEO-fraud», interne misligheter, hacking som resulterer i tap av intellektuelle verdier eller tilstrekkelig sikkerhet hos IT-leverandøren?

3. Innovasjon og sikkerhet. Hvordan klarer vi å holde høy nok fart i utviklingen av teknologi, organisasjon og mennesker, samtidig som vi ivaretar sikkerheten?

Dessverre finnes det ingen enkle og raske løsninger for å lette bekymringene. Det å etterleve strengere eksterne krav og håndtere nye risikoer uten å tape fart, krever et velkjent og velprøvd botemiddel, nemlig målrettet arbeid med virksomhetens internkontroll.

Fem steg til en risikobasert internkontroll for cybersecurity-trusler

Bjørn Erik Thon i Datatilsynet har tidligere uttalt: «To ting har vært sentrale, og vil fortsette å være sentrale: Risikovurderinger og internkontroll!» Det har han helt rett i.

Hvordan kan man se for seg at et fungerende internkontrollsystem kunne forhindret at svindlerne i eksemplet vårt om CEO-svindel stakk av med 100 millioner NOK? Med fem steg kunne man bygget en effektiv beskyttelse:

1. Risikovurdering: I den årlige gjennomgangen av virksomhetens risikoer blir det oppdaget at «CEO-fraud» utgjør en ny stor økonomisk risiko, som også kan utløse bøter og pålegg (eks. varslingsplikt) fra myndigheter som virksomheten er underlagt.
2. Oppdatering av kontroller: Deretter blir eksisterende internkontrollrutiner gjennomgått og svakheter avdekket. Det blir derfor etablert nye regler om hvordan betalinger skal settes opp, med attestasjons- og godkjenningsfullmakter for ulike beløpsstørrelser og type utbetalinger og krav til dokumentasjon. Dokumentasjon kan være krav om intern eller ekstern faktura. Godkjenning av bankbetalinger blir også endret ved at dette alltid skal gjøres av flere enn én person med rette fullmakter.
3. Implementering av kontroller: En systematisk implementering av de nye kravene og rutinene skal gi trygghet for at reglene virker i praksis.
   a. Organisasjon: Fullmaktsmatrise, stillingsbeskrivelser, rutinebeskrivelser og lignende oppdateres.
   b. Operasjonelt: Alle som behandler inngående faktura, har attestasjonsfullmakter og fullmakt til å godkjenne utbetalinger fra bank, får opplæring i nye regler. Opplæringen må også forklare hvorfor disse innføres, da det å være bevisst og jobbe med god sikkerhetskultur er avgjørende for god sikkerhet. Alle ansatte i virksomheten får også løpende beskjed om dette og andre typer svindelforsøk da de skal lære å være på vakt og alltid melde fra om mistenkelig forhold.
   c. Teknologisk: Virksomheten oppdaterer fullmakter for godkjenning av inngående faktura i ERP-systemet og skrur på dobbel godkjenning i nettbanken og/eller betalingssystemet.
4. Overvåking av kontrollene: Det blir gjennomført kontroller av at nye rutiner fungerer ved å gjennomføre testing. Dette kan gjøres gjennom dialog med relevante ansatte, utvalg av utbetalinger for kontroll og/eller gjennom dataanalyser av alle utbetalinger fra en gitt periode for å kontrollere behandling i tråd med ny rutine. Eventuelle feil og avdekkede svakheter må følges opp, korrigeres og igjen kontrolleres.
5. Jevnlig evaluering: Vi setter opp i årshjulet at vi evaluerer hvordan fasene 1–4 fungerer om et halvt år, og foretar eventuelle justeringer.

Noen nyttige råd på veien

Sveitserostmodellen til James Reason er verdenskjent for å vise at alle barrierer mot en uønsket hendelse har hull, og at man derfor må bygge flere lag med barrierer for å stanse en uønsket kraft. Disse barrierene, eller osteskivene om du vil, må imidlertid systematiseres, vedlikeholdes og utvikles i tråd med virksomhetens risikobilde og kontinuerlig vurderes med tanke på effektivitet og verdiskaping. For mange osteskiver blir kostbare og tungvinte for virksomheten, mens for få gjør at virksomheten kjører med høyere risiko enn ledelsen kanskje er klar over.

Erfaringsmessig kan følgende råd være nyttige å ta med seg når man skal forbedre sin internkontroll:

I. Bruk etablerte standarder og hold deg oppdatert.

COSO-rammeverket for internkontroll er verdens mest anerkjente og anvendte og gir gode råd om hvordan et internkontrollsystem bør bygges opp. For informasjonssikkerhet er ISO 27 001 kanskje den mest kjente. COSO og ISO 27 001 har vesentlige fellestrekk, særlig knyttet til å gjøre risikovurderinger, det å forstå og prioritere riktige tiltak til riktige problemer, overvåking og kommunikasjon. Videre finnes offentlige veiledere om disse temaene som

også private virksomheter kan hente mye god inspirasjon fra.

Et spørsmål mange stiller seg er: «Hva gjør andre som vi kan sammenlignes oss med?». Det finnes en rekke nettverk tilbudt av ulike aktører der man kan møtes og utveksle erfaringer. I tillegg publiseres det stadig artikler og studier om temaer innenfor styring og kontroll. Det gjelder å holde seg oppdatert om regelverk, trender og praksis.

II. Få kontrollfunksjonene i andrelinjeforsvaret til å samarbeide[1]

I de fleste virksomheter har linjeledelsen ansvaret for å påse at risikoer styres gjennom en velfungerende internkontroll (såkalt førstelinjeforsvar). For større virksomheter og andre som har dette som et regulatorisk krav, er en uavhengig internrevisjonsfunksjon gitt ansvaret for å kontrollere etterlevelse på vegne av styret (tredjelinjeforsvaret). Derimot har funksjonene som ivaretar andrelinjeforsvaret ofte en mye mer udefinert rolle.

Eksempler på andrelinjeforsvar er gjerne avdelinger for risikostyring og internkontroll, compliance og sikkerhet. God praksis er at andrelinjeforsvaret har ansvaret for å utforme og implementere retningslinjer, rutiner og kontroller, støtte linjeledelsen og å overvåke at internkontrollen fungerer i virksomheten. En vanlig utfordring med denne modellen, er at disse funksjonene, som har ansvaret for ulike deler av virksomhetens risikostyring og internkontroll, fokuserer på eget område og ikke samarbeider om en helhetlig risikostyring på tvers av virksomheten og fagområder. Dette kan være farlig når digitaliseringsalderen bringer med seg komplekse risikoer som det ofte kreves en tverrfaglig tilnærming for å løse. Dette gjør det også vanskelig for toppledelsen og styret å få et godt totalbilde på virksomhetens risikoer og hvor effektivt disse kontrolleres. Det kan også være utfordrende å sikre god koordinering av andrelinjefunksjonenes aktiviteter og oppfølging av organisasjonen. En dag kommer for eksempel noen og sjekker etterlevelse av personvernregler fra et juridisk perspektiv, og neste dag kommer noen og spør om akkurat de samme tingene, men med en cybersecurityhatt på.

Det er enkelt å konkludere med at samordning og samarbeid er essensielt for å få det fulle bildet på virksomhetens risikoer og sikre effektiv kontroll. Men det kreves mer enn et ønske om samarbeid. Toppledelsen bør pålegge disse funksjonene å samarbeide om sine risikovurderinger og oppfølging av virksomheten. Dette vil tvinge frem felles diskusjoner av utfordringer, erfaringsutveksling, nettverksbygging og kompetanseheving. Over tid vil dette gå mer av seg selv, når andrelinjen og virksomheten opplever gevinstene ved samarbeid.

III. Bruk teknologi. Gjør automatiske kontroller.

Økende digitalisering gjør at flere internkontrolltiltak kan automatiseres, noe som øker en virksomhets evne til å oppdage og forebygge avvik og unormal aktivitet. Bakgrunnen er at vi «endelig» har fått teknologi som evner å lære mønstre (maskinlæring) og gir oss muligheten til å analysere store mengder data kostnadseffektivt.

Innen sikkerhet gjør dette at man kan oppdage og stanse dataangrep og innsidetrusler mer effektivt. For internkontrollen gir det uvurderlige data som kan brukes til overvåking av datastrømmer, måling av aktiviteter og varsling av avvik. Vi har i dag teknologi for å alarmere om det meste av uønsket atferd, eksempelvis feilsending av dokumenter med viktig informasjon, ikke-autoriserte overføringer, tyveri av informasjon over minnepinne, eller snoking av informasjon. Spørsmålet er hvordan vi implementerer dette og bruker informasjonen på en måte som både er i henhold til lovverk og samtidig gir relevans både til de som jobber med sikkerhet og internkontroll. I dag er det nemlig ofte bare noen få på sikkerhet som sitter på mye av disse dataene.

Det anbefales at de som jobber med å utforme og forbedre internkontrollen i virksomheten, andrelinjeforsvaret, utforsker hvordan automatiserte kontroller og dataanalyser kan integreres i virksomhetens internkontroll og overvåkingen av denne. Ett eksempel er ikke-autoriserte overføringer. Programvare kan identifisere uønskede utbetalinger og anvendes for å avdekke og avverge disse, samt identifisere hvor i virksomheten internkontrollen har sviktet og må forbedres.

IV. Ikke glem kulturen

Vi ser ofte at de virksomhetene som har god internkontroll på andre områder, som finansiell rapportering, ofte også har god kontroll på sikkerheten. Det kan forklares ved at virksomheten har en kultur hvor det stilles tydelige krav, det er rom for feiling, læring og forbedring og at etterlevelse følges opp. Mange virksomheter er mer uformelle, med lite nedfelte rutiner, uklare roller og ansvar og hvor sikring av etterlevelse av lover og regler er basert på tillit. Slike virksomheter har ofte ikke oversikt over sine sikkerhetsrisikoer og da evner de heller ikke å identifisere og lukke gapet mellom hva de gjør og hva de bør gjøre.

I slike virksomheter er det viktig å ta den rådende kulturen på alvor når internkontrollen skal forbedres og utvikles. Dette for å sikre at den etablerte kulturen ikke blir en kraft som motarbeider det virksomheten ønsker å oppnå. Mer formalisering og systematisering vil blant annet innebære mer transparens, tydelighet i retningslinjer og ofte endringer i rutiner, noe som igjen kan endre maktbalanser og måten man jobber på. I tillegg til god opplæring og veiledning, er det derfor avgjørende med tydelig kommunikasjon fra ledelsen på alle nivåer i organisasjonen om formålet med endringsarbeidet, forventninger til den enkelte og oppfølging av etterlevelse.

Oppsummering

Ledelsen og styret har behov for verktøy som gir et godt og fullstendig bilde av viktige risikoer virksomheten står overfor og som effektivt og systematisk håndterer disse. Å etablerer interne kontroller og følge opp at de virker er i så måte et kraftfullt verktøy å bruke.

1 Ref. ECIIA/FERMAs 3 Lines of Defense model.

Jeg er regnskapsfører.
What's your superpower?

Vi støtter superheltene i regnskapsbedriftene som ser nye muligheter i en stadig mer digital hverdag.

Les mer om våre løsninger på Visma.no/byralosninger

VISMA