Utfordringer og muligheter:

Cybersikkerhet og arbeidsdeling

I artikkelen ser vi på hvorfor selskaper har utfordringer i forhold til arbeidsdeling (Segregation of Duties) og hva de kan gjøre for å løse mulige problemstillinger. Vi går gjennom noen eksempler på «best practice» og ser på de viktigste årsakene til at *det går bra* når risiko behandles på riktig vis.

Manglende kontroll med arbeidsdeling gjør at en hacker som har greid å komme inn i et system, vil møte færre hindringer for å få tilgang til og kontroll over konfidensielle data eller til og med hele selskapets ERP-system.

KPMG
Manager revisjon/data og analyse
Dylan Clark
KPMG

Partner revisjon/leder data og analyse
Jo Sigurd Pedersen
KPMG

I et næringsliv der overskriftene mange ganger handler om økonomisk svindel og risiko knyttet til cybersikkerhet, er det én utfordring som stadig går igjen både hos IT-konsulenter og den øverste ansvarlige for IT-sikkerhet i et selskap: Hvordan er det mulig å få bedriften til å fungere så effektivt som mulig samtidig som det skaper minimalt med utfordringer relatert til arbeidsdeling (Segregation of Duties conflicts)?

En typisk utfordring når det gjelder arbeidsdeling, vil være å gi tilgang til både å opprette en leverandør i systemet, inkludert bankkontoopplysninger, sammen med muligheten til å betale leverandøren.

Et annet eksempel er muligheten til å justere lønnen til en ansatt og deretter godkjenne lønningslisten.

Til tross for stadig mer sofistikerte løsninger innen IT og dataanalyse, er utfordringer relatert til noe så enkelt som arbeidsdeling, en utfordring selv for de største selskapene internasjonalt.

Hva som kan gå galt

Først ser vi på hva som kan gå galt, og det er ganske mye hvis virksomheten ikke tar hensyn til at det er utfordringer knyttet til arbeidsdeling.

Manglende kontroll med arbeidsdeling betyr at en eventuell hacker som har greid å komme inn i systemet, vil møte færre hindringer for å få tilgang til og kontroll over konfidensielle data eller til og med hele selskapets ERP-system.

Arbeidsdeling – et viktig forsvar mot cyberangrep

Fordi ERP-systemene kan sies å være selskapenes kronjuveler – deres mest verdifulle eiendeler – blir disse syste-

mene attraktive mål og i økende grad utsatt for angrep. Med tanke på hva som finnes av informasjon i ERP-systemene, blir derfor arbeidsdeling en viktig del av forsvaret mot cyberangrep.

Selv uten hackere vil svake rutiner i forhold til arbeidsdeling øke et selskaps risiko.

Feil skjer

Feil kan og vil skje og det samme gjelder svindel. Noen ganger blir det veldig kostbart.

Det dukker stadig opp saker der høyt betrodde ansatte har begått underslag gjennom mange år, eller historier der innkjøpsansvarlige enten har underslått produkter eller mottatt bestikkelser. Det mest overraskende med mange av disse historiene som dukker opp i pressen, er hvor enkelt det har vært å gjøre disse underslagene eller å motta disse bestikkelsene.

Størrelse teller

Hvis man vet at risikoen finnes og samtidig er så åpenbar, hvordan kan da til og med verdens største og mest teknologikompetente organisasjoner fortsatt ha utfordringer når det gjelder arbeidsdeling?

Å se på størrelse og kompleksitet er et godt utgangspunkt for å forklare dette.

Mens utfordringen for mindre organisasjoner når det gjelder arbeidsdeling ofte handler om at det er for få mennesker å fordele de forskjellige oppgavene på, er utfordringen for de største selskapene at de har tusenvis av brukere og veldig komplekse forretningssystemer. Svært verdifull informasjon ligger i ERP-systemene deres samtidig som organisasjonen er i stadig endring. Det er derfor nærmest umulig å ha en design/et opplegg for arbeidsdeling som er 100 prosent perfekt. Alt for mange selskaper gir derfor opp i forsøket på å rydde opp på dette området.

Utfordringer med selve ERP-systemet

Noen ganger ligger det utfordringer i selve ERP-systemet. I et veldig mye brukt system som for eksempel SAP er det så mye valgfrihet at det i seg selv kan bli en utfordring. Systemet er nemlig laget slik at brukerne kan gjøre akkurat samme type oppgave på mange forskjellige måter, noe som gjør utfordringen med arbeidsdeling enda vanskeligere.

Fordeling av ansvar

Den neste utfordringen handler om fordeling av ansvar. Større selskaper har ofte flere viktige miljøer med overlappende ansvarsområder, noe som kan gjøre at et tema som arbeidsdeling faller mellom to stoler. Et typisk eksempel kan være at de som jobber med virksomhetens forretningsdel vil tro at rolledesign er et rent teknisk spørsmål, mens IT-delen på sin side tenker på dette som et rent forretningsmessig spørsmål. Rolledesign handler om å gi brukere nødvendige tillatelser i et

system (access rights) slik at de blir i stand til å utføre sine oppgaver.

Må bruke eksterne konsulenter
En tilleggsutfordring er at selv de største selskapene har behov for eksterne IT-konsulenter for å implementere systemer som er like komplekse som SAP. Det kan føre til at det blir skyldt på andre når det stilles spørsmål om hvem som egentlig er ansvarlig for arbeidsdelingen. Er det for eksempel selskapet selv som er ansvarlig for å definere hvilke regler som skal gjelde? Ofte har konsulentene bare teknisk kunnskap og har lite fokus på forretningssiden.

Utsetter problemene til senere
Bedriftene forsømmer seg ofte når det gjelder spørsmål om arbeidsdeling. De har press på seg for å levere løsningene raskt og det er enkelt å overbevise andre om at spørsmål som har med arbeidsdeling å gjøre, kan løses senere. Rotete prosesser implementeres rett i det nye ERP-systemet med en forventning om at «alt» vil bli bedre i et nytt system. I virkeligheten vil det samme «rotet» ganske enkelt ha et annet grensesnitt og i slutten av prosjektet er problemstillingene relatert til arbeidsdeling akkurat de samme som da prosjektet ble startet opp.

Det er nettopp derfor det er så viktig at virksomheten prioriterer spørsmål om arbeidsdeling.

Ta ansvar
Det sies ofte at du må gjør jobben selv hvis du vil at den skal bli gjort riktig – og på dette området stemmer det veldig bra. Med mindre det er ansatt en konsulent som spesielt skal ta seg av spørsmål om arbeidsdeling, må nemlig virksomheten ta ansvar.

Førstelinjeansvar
Et godt utgangspunkt er å starte med jobbdesign/rolledesign og ansvarsfordeling som et førstelinjeforsvar mot uønsket eller manglende arbeidsdeling. Utfordringen vil være å justere forretningsprosesser og ansvar på en slik måte at ansatte kan holde seg til et regelverk, men samtidig være i stand til å utføre sine arbeidsoppgaver på en tilfredsstillende måte. Ingen skal for eksempel kunne godkjenne sine egne fakturaer eller kunne justere sin egen lønn. Å starte implementeringen med å prioritere jobbdesign/rolledesign, er et godt utgangspunkt for å få til en god arbeidsdeling.

Mye hjelp i standard programvare
Heldigvis finnes det god hjelp både i standard programvare og i et stort utvalg av tilnærminger til data og analyse. SAP GRC er et standardverktøy som har en del fordeler når det gjelder integrering av den ERP-løsningen som brukes, noe som gjør jobben med å endre rolledesign betydelig lettere.

Det finnes også en rekke GRC-verktøy på markedet. Dette er verktøy for internrevisjon samt risikostyring og compliance (GRC=Governance, Risk, Compliance). Med slike verktøy kan man lett se hvilke valgmuligheter som eksisterer og velge noe som passer i forhold til organisasjonens budsjett.

Både store og små virksomheter kan også gjøre en rekke tilnærminger ved hjelp av data og analyse for å redusere risiko og gjøre endringer når det er problemstillinger innenfor arbeidsdeling.

Can-Do og Did-Do
En tradisjonell Can-Do-skanning er et naturlig utgangspunkt. Dette er en analyse som viser mulige problemstillinger som kan dukke opp når det gjelder de ansattes roller og hva som kan gjøres for å forhindre dårlige løsninger. En slik analyse gjør det lettere å avdekke, prioritere og løse de viktigste problemområdene.

Spesielt i store og komplekse organisasjoner kan en Can-Do-scan resultere i en del støy i form av uviktige funn. Et alternativ for slike virksomheter er å bruke en annen, litt mer resurskrevende, type analyse – Did-Do-scan – som viser hvor ansatte faktisk har utført handlinger som er uheldige i forhold til arbeidsdeling. På det viset avdekkes de mest problematiske områdene som det bør prioriteres å gjøre noe med. En Did-Do-scan fungerer også utmerket som en mislighetsanalyse.

Hva som kan bli riktig
Etter mye om hva som kan gå galt i forhold til arbeidsdeling, kan det være greit å si litt om hva som kan bli riktig dersom arbeidsdeling blir gjort på rett vis.

Fordi børsnoterte selskaper må tilfredsstille strenge krav gitt i revisjons- og regnskapsstandarder, er det også disse selskapene som har mest å tape på uheldig arbeidsdeling. Dette ikke minst fordi regulerende myndigheter, som Finanstilsynet, forventer at børsnoterte selskaper holder en høyere standard enn andre selskaper. Å prioritere gode rutiner for roller og fullmakter i tillegg til en sterk internkontroll, er derfor avgjørende både for selskapene og deres revisorer.

I tillegg til at virksomheten unngår misligheter, viser den også at den er på samme side som revisor når det gjelder å avdekke og redusere mislighetsrisiko. Det vil også være mye enklere å dokumentere at det i virksomheten ikke ligger opplagte muligheter for svindel som utro tjenere eller andre kan benytte seg av.

Prisen for slurv
Virksomheter må sørge for å unngå problemer knyttet til arbeidsdeling fordi det unødig øker risikoen på viktige områder i virksomheten. Å prioritere slike spørsmål bidrar til å redusere risiko der det er viktigst – i virksomhetens ERP-system.

Noen ganger kan risikoen synes lav, men prisen for slurv kan gjøre at ondsinnede aktører får tilgang til virksomhetens finansielle kronjuveler. Dårlig PR kan også gjøre ubotelig skade.

Ingen grunn til å vente
Risiko relatert til arbeidsdeling kan heldigvis reduseres ved å vise ansvarlighet, ha på plass en god rolledesign og investere i ekspertise innen dataanalyse.

Det er ingen grunn til å vente med å be revisor og øverste ansvarlig for IT å gi dette topp prioritet!