NORGES HANDELSHØYSKOLE

Bergen, 20. juni 2008

Informasjonssikkerhet i et ledelsesperspektiv

Heine Didriksen

Veileder: Tore B. Holmesland

Utredning i fordypningsområdet Strategi og ledelse

NORGES HANDELSHØYSKOLE

INNHOLDSFORTEGNELSE

FIGURLISTE:

1. Innledning

Den ekstremt hurtige utviklingen internett har hatt det siste tiåret, har hatt meget stor innvirking på moderne økonomi. Internett har vokst fra å være et lukket forskningsnettverk med bare et par tusen brukere midt på 80-tallet, til å bli et verdensomspennende nettverk med over 1,2 milliarder brukere i dag. Bruken av internett som tjenesteleverandør og kommunikasjonsbærer har langt på vei erstattet tradisjonelle forretningsmetoder, og tvunget virksomheter til å ta i bruk digitale informasjonssystemer.

Ved å ta i bruk slike systemer eksponerer virksomheten også sine systemer mot en rekke nye trusselfaktorer. Ikke bare fra eksterne aktører, men også internt i virksomheten.

Siden avhengigheten av informasjonssystemer i dag er så stor, kan et potensielt sikkerhetsbrudd på slike systemer få store negative konsekvenser for virksomhetens omsetning, kundemasse og omdømme. Dette dilemmaet mellom sikkerhet og effektivitet gjør informasjonssikkerhet til en meget viktig komponent i virksomheters forretningsstrategi. Etablering av effektive prosesser rundt informasjonssikkerhet, som tar for seg de risikoene som virksomheten til enhver tid står overfor og hvordan disse risikofaktorene skal behandles, bør ha høy prioritet.

Organiseringen av slike sikkerhetstjenester har tradisjonelt vært bottom-up, hvor administrative avdelinger har hatt avsvar for å planlegge og ivareta informasjonssikkerheten. Dette er problematisk, da slike avdelinger ikke nødvendigvis har kjennskap til virksomhetens kjerneprosesser. Jeg vil i denne oppgaven forsøke å belyse denne problemstillingen. Det vesentlige her er å få vist at denne type sikkerhetsarbeid ikke er begrenset til teknisk utstyr som ivaretas av en administrativ enhet som f.eks. en it-avdeling. Informasjonssikkerhet er et arbeid som må involvere hele virksomheten, med forankring i toppledelsen. Jeg vil også ta for meg hvilke prosesser en organisasjon bør etablere og vedlikeholde for å sikre velfungerende informasjonssikkerhet på lang sikt.

Jeg har valgt å dele prosessen rundt informasjonssikkerhet inn i tre faser, hvor jeg i hver fase tar for meg hvilke utfordringer bedriften står overfor, hvilke problemstillinger som bør avklares og hvor i bedriften ansvaret bør ligge.

De tre fasene er:

1. **Planleggingsfase** – I denne fasen identifiserer man bedriftens aktiva, og tar for seg trusler og sårbarheter, før man analyser av trusselbildet og anslår risiko.

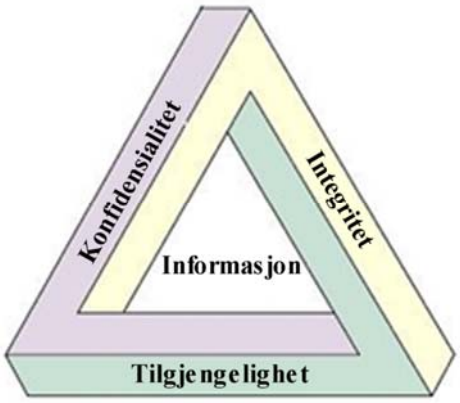
2. **Strategifase** – Her utarbeider man konkrete handlingsplaner og sikkerhetspolicyer på bakgrunn av analysene som ble gjennomført i første fase.

3. **Implementeringsfase** – Dette er selve gjennomføringsfasen. Her settes de planlagte tiltak i verk, både teknisk og organisatorisk.

Før jeg går videre til de tre fasene, er det viktig å klargjøre hva som menes med informasjonssikkerhet. Informasjonssikkerhet er ikke det samme som it-sikkerhet. Der it-sikkerhet i stor grad fokuserer på teknologi, tar informasjonssikkerhet for seg alle deler av en virksomhet som kan ha skadelig innvirkning på organisasjonens ulike informasjonsaktiva. It-sikkerhet er en meget viktig del av dette, men altfor ofte er det bare dette som blir vektlagt når man skal beskytte sine informasjonssystemer og -prosesser. Ved å tillegge dette arbeidet en ensidig teknologisk vinkling, får man ofte en situasjon hvor man delegerer dette arbeidet til en it-avdeling fremfor å behandle utfordringene sammen med representanter fra toppledelsen.

Informasjonssikkerhet har tre grunnleggende faktorer:

- ***Konfidensialitet***. Kravet til konfidensialitet skal sikre at informasjonen ikke blir gjort tilgjengelig for uvedkommende.
- ***Intergritet***. Kravet til integritet innebærer at informasjonen ikke skal kunne endres utilsiktet eller av uvedkommende.
- ***Tilgjengelighet***. Kravet til tilgjengelighet skal sikre at informasjonen er tilgjengelig for brukere når de har behov for denne.



Figur 1.1 KIT-modell

Hver av disse tre faktorene har egne utfordringer knyttet til seg, og sammen utgjør de et rammeverk for det sikkerhetsarbeidet som virksomheten står overfor. Ved å ha fokus på disse tre faktorene har man et godt utgangspunkt for det videre arbeidet med informasjonssikkerhet.

2. Undersøkelsesfasen

Den første fasen i sikkerhetsarbeidet har jeg valgt å kalle undersøkelsesfasen. Her er målet å få en oversikt over hvilke sikkerhetsrisikoer virksomheten står overfor. Risiko består her av tre komponenter, påvirkningsgrad, sårbarhet og trusler. Dersom en av disse komponentene ikke er til stede, har man heller ikke noen risiko. Utfordringen i denne fasen blir da å innhente så mye informasjon som mulig om disse tre komponentene, og på bakgrunn av disse vurdere risiko. Dette danner så grunnlag for det videre sikkerhetsarbeidet.
Risiko i forbindelse med informasjonssikkerhet kan dermed defineres ved følgende formel:

Risiko = Trussel * sårbarhet * påvirkningsgrad

Risiko er muligheten for at en trussel skal utnytte en sårbarhet og dermed forårsake skade på et aktivum, eller for å si det på en annen måte – kombinasjonen av sannsynlighet og konsekvens.
Man skiller ofte mellom to typer risikovurderinger – kvantitativ og kvalitativ. Ved kvantitativ risikovurdering er målet å anslå objektive numeriske verdier for hver risikofaktor, for så å gjøre en kostnad/nytte-analyse. Man benytter seg av empiriske data for å anslå en så nøyaktig sannsynlighetsgrad som mulig, og beskriver dette med numeriske verdier. Deretter forsøker man å beskrive påvirkningsgraden et så nøyaktig tall som mulig i forhold til hva bedriften vil tape dersom en hendelse setter systemet ut av drift. På bakgrunn av dette har man en risikokoeffisient som i teorien skal være nøyaktig. En slik kvantitativ metode er velegnet ved beregning av risiko ved investeringsanalyser og andre prosesser hvor bakgrunnsmaterialet er tallfokusert, mens man ved analyse av informasjonssystemer fort oppdager at de ulike komponentene er meget vanskelig å anslå nøyaktig.
Ved kvantitativ analyse forsøker man ikke å tillegge de ulike risikofaktorene numeriske verdier, men man bruker i stedet mer generelle og subjektive variabler, som for eksempel *høy, medium, lav*, for å beskrive de ulike leddene i risikoformelen. Fremgangsmåten er altså lik, forskjellen ligger i detaljene. Fordelen med den kvalitative analyseformen er man unngår den meget tidkrevende og detaljfokuserte utfordringen som ligger i å anslå nøyaktige verdier for

de ulike verdiene, og man kan i stedet se resultater fra risikoprosessen etter kort tid. Derfor mener jeg det er riktig å fokusere på kvalitative metoder i undersøkelsesfasen.

2.1 Påvirkningsgrad

Man starter datainnsamlingen med å identifisere virksomhetens aktiva, for så klassifisere disse ut fra hvor virksomhetskritiske og verdifulle de er. Dette er viktig, da man ikke kan identifisere trusler og sårbarheter før man har en komplett oversikt over virksomhetens egen informasjon og systemer. Dette er med andre ord en oversikt og verdisetting av systemer og komponenter som skal inngå i sikkerhetsarbeidet.

Det kan være hensiktsmessig å identifisere og klassifisere aktiva etter følgende kriterier:

- Informasjonsaktiva. Dette er all type lagret informasjon. Dette kan være dokumenter, databaser, logger og arkiver. M.a.o., all informasjon som har blitt generert av bedriftens virksomhet.
- Programvare. Dette omfatter kommersiell programvare og egenproduserte applikasjoner.
- Fysiske Aktiva. Dette begrenser seg ikke til informasjonssystemer som maskinvare, nettverksutstyr og lagringsmedia, men omfatter også bygninger og andre aktiva som ikke-teknologiske aktiva.
- Kunnskapsaktiva. Dette er mer abstrakte aktiva, som menneskelige egenskaper og interne prosesser.
- Tjenester. Tjenester som virksomheten er avhengig av kan være tjenester som er outsourcet, eksterne kommunikasjonstjenester og strømnett.

For fysiske aktiva er det forholdsvis lett å anslå verdi, mens dette er mer komplisert for informasjonsaktiva. Før man kan verdsette informasjonsaktiva, må man fastslå hvem som har eierskap til de forskjellige kategoriene. Det er systemeier som best kan vurdere hvor virksomhetskritisk og verdifull denne informasjonen er. Programvare verdsettes som regel best av it-avdelingen, kundedatabaser av salgsavdelingen, osv.

Når man har foretatt en verdivurdering, kan man starte klassifiseringen av de ulike aktiva etter hvor stor påvirkning et eventuelt sikkerhetsbrudd eller tap vil ha, både på aktivumet spesielt og på virksomheten generelt. Påvirkningsgraden vil da utgjøre en variabel i risikoformelen som ble nevnt innledningsvis i dette kapittelet.

2.2 Trusselvurdering

Neste steg blir å identifisere trusselbildet. Det er essensielt for en virksomhet å ha et detaljert bilde av de truslene man står overfor, og hvilke effekt disse truslene kan forårsake.

Truslene kan deles inn i to grupper, naturgitte trusler og ondsinnede trusler.

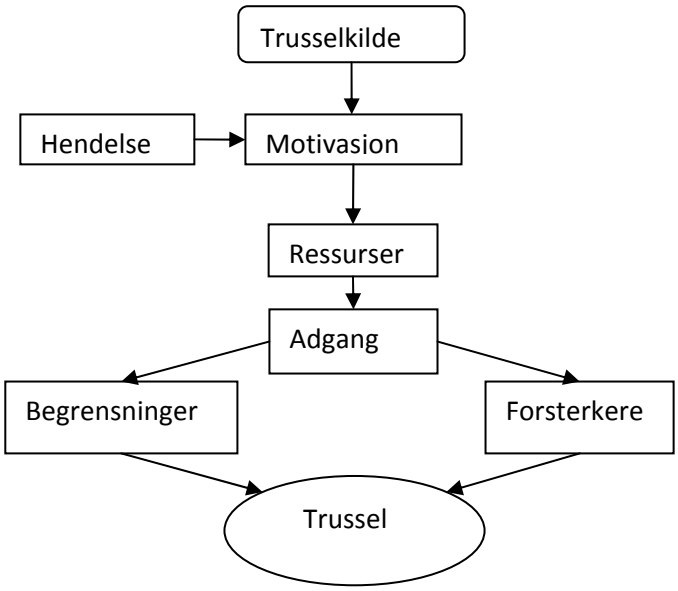
Naturgitte trusler

Naturgitte trusler inkluderer alle typer naturkatastrofer, som f. eks flom, jordskjelv, etc. Dette er trusler som ikke er direkte rettet mot virksomheten, men som likevel kan forårsake stor skade dersom men ikke har tatt nødvendige forhåndsregler. Dette er som oftest et statisk trusselbilde som på forhånd er veldokumentert, og arbeidet med å få et tilstrekkelig overblikk over situasjonen er overkommelig.
Skade som blir forårsaket av menneskelige feil og uhell passer også best inn i denne gruppen. Det som skiller denne gruppen fra ondsinnede trusler, er at motivasjonen for skade ikke er tilstede. I likhet med naturgitte trusler er også slike typer trusler statiske og veldokumenterte.

Ondsinnede trusler

Denne gruppen menneskeskapte trusler er den som bringer de største utfordringene, da virksomheten vil stå overfor et vidt trusselbilde som er i stadig forandring. Etter min mening er det mest hensiktsmessig å ta utgangspunkt i de identifiserte aktiva fra kap 2.1, og så vurdere trusselbildet for hvert enkelt aktivum. Dette fordi jeg mener at de forskjellige elementene i en virksomhet har sitt eget trusselbilde, og må vurderes individuelt. Dette betyr ikke at man ikke skal se på hele virksomheten under ett. For eksempel vil en amerikansk bedrift i Midtøsten naturlig nok ha et helt annet trusselbilde enn en lokal bedrift med de samme systemene, men det er etter min mening likevel viktigere å se for seg hvilken trusselfare hvert enkelt system og hver enkel avdeling står overfor.

En trussel er bygget på en rekke ulike komponenter, beskrevet i figuren under.



Figur 2.1 Trusselkomponenter

Som det går frem av figuren må det finnes en trusselkilde, en såkalt threat agent, som står bak trusselen. Dette kan være kriminelle, konkurrenter, ansatte, etc. Det finnes etter hvert flere standardiserte oversikter over slike trusselkilder, bl.a. Intels Threat Agent Library**.** Dette er oversikter som lister opp og beskriver de mest kjente trusselkildene og deres motiver, fremgangsmåter, styrker og svakheter. Slike oversikter kan være svært nyttige i denne type sikkerhetsarbeid.

En trusselkilde må ha motivasjon, ressurser og adgang for å kunne utgjøre en fare. I tillegg vil hver enkel trusselkilde bli møtt ulike faktorer som vil begrense eller forsterke trusselfaren. Ved å vurdere ulike typer trusselkilder opp mot de forskjellige komponentene, kan man anslå hvor stor fare trusselen utgjør for virksomheten eller det spesifikke informasjonssystemet.

Motivasjon

Det finnes en rekke ulike typer motivasjon bak en trussel. Dette er den viktigste faktoren som må vurderes når man tar for seg de ulike trusselkildene. Uten motivasjon utgjør man heller ingen trussel. Eksempler på motivasjonsfaktorer kan være politiske og religiøse motiver, profitt, hevn eller noe så banalt som anerkjennelse. Da Estland i fjor bestemte seg for å flytte et militært monument fra Sovjettiden, møtte de store protester fra Russland og fra etniske russere i Estland. I tiden som fulgte ble Estlandske informasjonssystemer lammet av massive Denial Of Service-angrep. Dette førte til store problemer, særlig fordi Estland har vært en pioner på bruk av IT i sitt offentlige byråkrati. Her ser vi at man har en hendelse som skaper motivasjon, slik det er beskrevet i figuren over.

Ressurser

Neste faktor er ressurser. Her forsøker man å anslå trusselkildens evne til å utnytte de sårbarhetene som man vet er tilstede. Dette er selvsagt en komplisert oppgave, men man har hjelp i en rekke standardiserte og til enhver tid oppdaterte trusselmatriser, som opererer på samme måte som det overnevnte Threat Agent Library. Slike hjelpemidler blir utarbeidet av internasjonale sikkerhetsorganisasjoner som overvåker de ulike truslene som IT-bransjen til enhver tid står overfor. Mange virksomheter har også sine egne konkrete trusselkilder som de overvåker og kartlegger.

Mulighet

For at man skal kunne gjøre skade på et system, må man ha adgang til dette. Denne adgangen kan være fysisk eller elektronisk. Hvor stor faren for at en trusselkilde kan få tilgang til et system, avdekker man ved hjelp av sårbarhetsundersøkelser, som jeg vil omtale i neste avsnitt.

2.3 Sårbarhetsvurdering

Neste steg i denne fasen er å vurdere hvor virksomhetens sårbarheter befinner seg. Sårbarhet og trusler henger tett sammen, og det viktige her er å vurdere hvor sårbar bedriftens systemer er i forhold til det kartlagte trusselbildet.

Teknologi.

At informasjonssystemer har sårbarheter er verken en nyhet eller en hemmelighet. Sikkerhetshull i operativsystemer og programvare er veldokumentert, og selv om det finnes en rekke kilder med informasjon som forklarer og foreslår løsninger på slike problemer, er det ofte her det syndes mest. Til tross for at leverandører i dag er raske med å tilgjengeliggjøre oppdateringer som lukker sikkerhetshull og stenger eventuelle bakdører i systemet, er dette en del av sikkerhetsarbeidet som mange it-organisasjoner nedprioriterer. Et eksempel på dette så man ved den ekstremt hurtige utbredelsen Sapphire/Slammer-ormen fikk i januar 2003. Denne utnyttet en svakhet i Microsofts SQL-databaseserver, og smittet over 75.000 systemer over hele verden. Over 90% disse systemene ble infisert løpet av de ti første minuttene av utbruddet, og i de tidlige fasene ble antall smittede systemer doblet hvert 8,5 sekund. En patch for det hullet ormen benyttet seg av hadde vært tilgjengelig i over et halvt år da utbruddet fant sted, og illustrerer godt hvor viktig det er å alltid ha utstyr oppdatert. Andre lignende angrep utnytter sårbarheter som enda ikke er oppdaget av systemleverandøren selv. Dette understreker bare at slike tilsynelatende små sårbarheter kan få store konsekvenser, og synliggjør behovet for en kontinuerlig oppfølging av slike hendelser. Selv om denne type sårbarheter i stor grad blir fikset fortløpende, vil man alltid ha et tidsrom hvor sårbarheten er allment kjent uten at en løsning foreligger. Slike sårbarheter kan man vanskelig beskytte seg mot, men må uansett tas høyde for under sikkerhetsarbeidet. Det er ikke bare i software man finner sikkerhetshull og sårbarheter, de finnes også i hardware, altså fysiske løsninger. Et eksempel på dette er uroen rundt 2000-overgangen, og de potensielle konsekvensene dette kunne få på eldre it-systemer som ikke taklet firesifrede årstall.

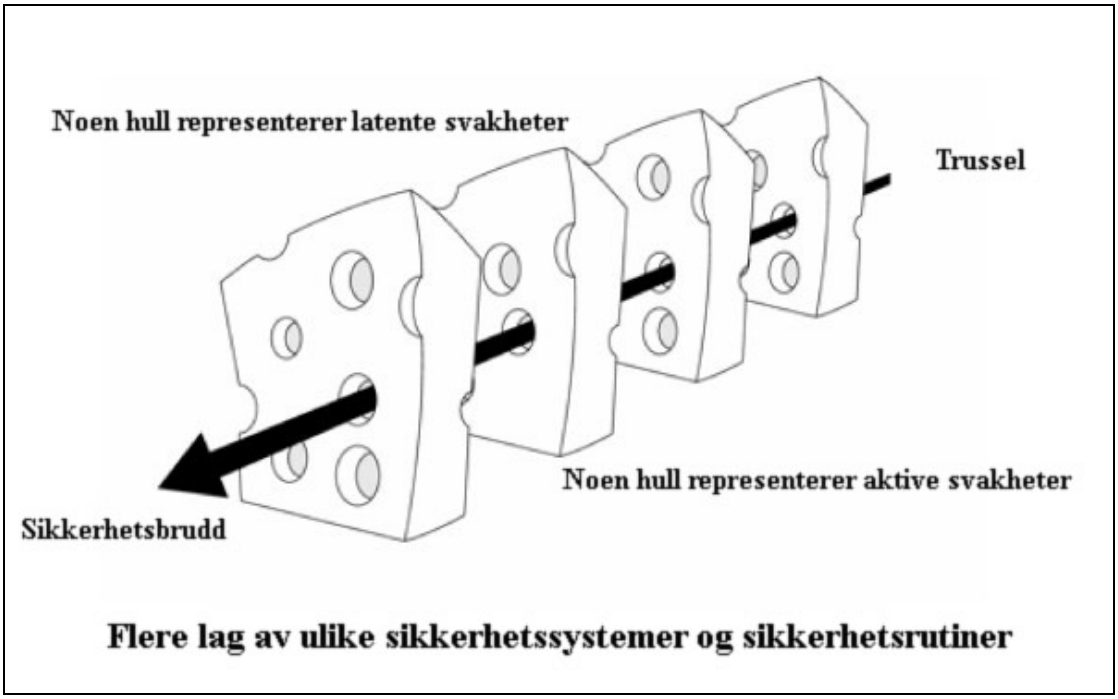
Når man gjennomfører slike sårbarhetsanalyser av informasjonssystemer tar man ofte i bruk såkalt penetration-testing, altså et slags angrep på egne systemer. Slike tester blir som regel utført av et eksternt sikkerhetsfirma, og har som mål å avdekke sikkerhetshull både eksternt og internt i virksomhetens systemer.

Mennesker.

Til tross for at det finnes en rekke mangler og sårbarheter i selve systemene, skyldes de aller fleste store sikkerhetstabber menneskelige feil. Som tidligere nevnt utgjør bedriftens ansatte en av de største sikkerhetstrusler, og sikkerhetstiltak som ikke tar hensyn til mennesker som sårbarhetsfaktor er dømt til å mislykkes. Når man snakker om sårbarheter på det menneskelige plan, kan man skille mellom sårbarheter som oppstår på systemsiden, hvor man har rene feil i konfigurering og bruk av systemer som er i produksjon, og sårbarheter som oppstår på brukersiden grunnet uvitenhet. Såkalt Social Engineering er et typisk eksempel på det siste. Her utnytter trusselkildeen ikke en feil i systemet, men forsøker i stedet å få adgang til lukkede systemer gjennom bevisst manipulering av uvitende brukere. Høyskolen i Bergen ble nylig utsatt for slik manipulasjon. En eller flere studenter ble lurt til å gi bort passordet sitt til nigerianske svindlere, som deretter brukte denne informasjonen for å forsøke å svindle til seg penger. Et annet eksempel som viser hvor lett dette kan være er et forsøk som ble gjort på Londons undergrunnsbane. Her stilte man tre-fire spørsmål til forretningsfolk, hvorav et av spørsmålene var hva passordet deres var. 90% av de spurte oppga passordet sitt i løpet av den korte tiden undersøkelsen tok.

Sårbarhetsvurdering er en kompleks oppgave, da man ofte opplever at potensielle svakheter i systemer som under normale omstendigheter ikke er alvorlige, kan vise seg å utgjøre store sikkerhetshull i kombinasjon med andre sårbarheter.

Reason’s Swiss Cheese Model (Reason, 1990), illustrerer dette. Modellen var opprinnelig ment som en illustrasjon på psykologiske prosesser, men har senere blitt benyttet hyppig i ulike typer sikkerhetsarbeid.



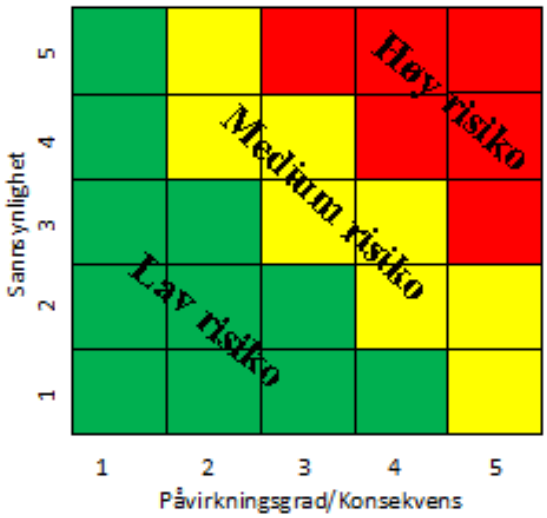
Figur 2.4 Swiss Cheese Model

I denne modellen blir en virksomhets systemer satt ved siden av hverandre som stykker av ost. Hullene i ostestykkene illustrerer sårbarhetene i de ulike deler av sikkerhetssystemene. Modellen skiller mellom aktive og latente svakheter, representert med hullene i osteskivene. Latente svakheter er sårbarheter har vært gjeldende over lang tid i form av feilkonfigurering, prosedyrefeil, eller lignende, uten å forårsake skade. Aktive svakheter er sårbarheter som direkte kan knyttes til enkelthendelser, og som når de inntreffer kan aktivere de latente sårbarhetene. Det er denne kombinasjonen som blir illustrert i modellen, ved at hull i alle stykkene blir eksponert på en slik måte at en trussel vil kunne passere gjennom alle hindrene og forårsake skade. Modellen viser at selv om sårbarheter ikke utgjør stor risiko på egenhånd, kan det i sære tilfeller forekomme kombinasjoner av disse som kan få store konsekvenser.

Ved å belyse ulike typer trusler og tilhørende sårbarheter for så å gi dem verdier i forhold til hvor alvorlig disse er, vil man kunne anslå sannsynligheten for et vellykket angrep på de ulike systemene.

2.4 Risikovurdering og håndtering

Etter å ha vært gjennom de tre fasene, må man analysere det materialet man har samlet inn. Figuren under viser risiko med bakgrunn i forholdet mellom sannsynlighet og påvirkningsgrad:



Figur 2.3 Risikomatrise

Ved å kombinere sårbarhet, trusselbilde og påvirkningsgrad får man altså risiko. Ut fra denne risikooversikten kan virksomheten starte sitt videre sikkerhetsarbeid. Målet er ikke å eliminere all risiko, men å finne en balansegang hvor man reduserer effektene av de ulike truslene til et akseptabelt nivå. Dette blir som nevnt innledningsvis en kostnad/nytte-analyse, hvor man anslår hva det vil koste å utbedre risikoen, i forhold til den skade man kan forvente dersom velger å ikke innføre risikotiltak. Etter å ha funnet de ulike risikoene, har man ulike måter å håndtere disse på:

Aksept av risiko.

Dette er vanlig ved hendelser som har lav risikograd, og ved hendelser hvor man anser kostnaden for å utbedre risikoen som større enn alternativet. Dette er som regel den billigste utveien på kort sikt, men dyrest på lang sikt.

Overføring av risiko.

Dette innebærer at man overfører risiko til en tredjepart. Et typisk eksempel på dette er forsikringsavtaler, selv om dette ofte kan være vanskelig med tanke på informasjonssikkerhet. Mer vanlig er det med ulike typer outsourcing. Dette skal jeg gå mer inn på i kapittel 4.2.

Risikoreduksjon.

Dette er den vanligste risikohåndteringsstrategien, og det er dette jeg skal konsentrere meg om videre i denne oppgaven. Her innfører man nødvendige tiltak for å redusere risikoen mot de ulike aktiva. Dette er altså bedriftens egne sikkerhetstiltak.

2.5 Ansvar og organisering

Organiseringen og ansvarsfordelingen er vesentlig for å sikre en effektiv fremdrift og gode resultater av sikkerhetsarbeidet. De fleste bedrifter av en viss størrelse har en eller flere personer ansatt med ansvar for risikohåndtering. Dette ansvaret har tradisjonelt sett vært knyttet til bedriftens kjernefunksjoner, med fokus på bl.a. finansiell og strategisk risiko. I slike virksomheter hvor risikofunksjonen allerede er etablert, kan det oppstå forvirring når risikoarbeidet i forhold til informasjonssikkerhet også blir løftet opp på toppnivå, og skal inngå i den samlede risikohåndteringen. Det er først den siste tiden at risikovurdering med tanke på informasjonssikkerhet har blitt et tema, og mange organisasjoner ser fremdeles ikke forskjell på IT- og informasjonssikkerhet. Tradisjonelt har dette arbeidet vært teknisk preget, og gjennomført av avdelinger med teknisk fokus, som oftest IT-avdelingen. Dersom man på toppnivå ikke ser denne forskjellen på it og informasjon, vil man fortsatt ha et fokus utelukkende på teknisk risiko, og man vil mangle et fullstendig perspektiv på hele bedriftens funksjon.

For at man skal få en effektiv drift av risikoarbeidet med tanke på informasjonssikkerhet, er det min mening at det bør ansettes en person som utelukkende har ansvar for dette. Som nevnt innledningsvis mener jeg at alt it-sikkerhetsarbeid må ha forankring i toppledelsen, og en slik stilling bør ideelt sett bør være etablert i eller like under toppledelsen for å kunne ha nødvendig myndighet og oversikt. Risikoarbeid er et nitidig arbeid som mange vil se på som et mer eller mindre nødvendig onde, og da er det viktig at den som sitter med ansvaret har nødvendig autoritet.

For å kunne få et vidt nok nedslagsfelt, bør det dannes en gruppe som skal ta for seg denne type risiko. Denne gruppen bør bestå av ansatte fra ulike deler av virksomheten, og er illustrert i figur 2.4.

Figur 2.4 Organisering av planleggingsfasen

IT-avdelingen bør naturlig nok være representert, da informasjonssikkerhet er direkte, men ikke utelukkende, knyttet til IT-drift. Informasjonssikkerhet og IT-drift kan ofte være i en slags konfliktsituasjon, da en IT-avdeling lett kan se på dette som et hinder for tekniske nyvinninger og ideell funksjonalitet. For å unngå en slik konflikt, er det viktig at lederen for en slik gruppe klarer å synliggjøre den nytteverdien bedriften har ved å fokusere på denne type sikkerhet, og ikke bare på tekniske løsninger. På denne måten kan man minimere en del av de grensene som ofte eksisterer mellom it-avdelingen og bedriften ellers.

En annen avdeling som bør involveres i dette arbeidet er personalavdelingen. Denne avdelingen håndterer en rekke sensitive dokumenter, og er samtidig den delen av organisasjonen som har best oversikt over hvordan ansatte utøver sine oppgaver. Som sagt utgjør den menneskelige faktor en meget stor del av trusselbildet mot virksomhetens aktiva, og dermed er det naturlig at personalavdelingen er med på et slikt risikoarbeid.

Teknisk avdeling, som er avdelingen med ansvar for fysisk sikkerhet, bør også være representert i en slik arbeidsgruppe. Dette er personer med inngående kjennskap til virksomhetens fysiske infrastruktur, alarmsystemer, brannsikkerhet og andre mer tradisjonelle sikkerhetstiltak. Denne type informasjon er nødvendig for å få et fullstendig bilde av risikoen

I tillegg til disse tre, som etter min mening er de vesentlige komponentene i en slik gruppe, har jeg også tatt markedsavdelingen som en mulig bidragsyter i en slik prosess. Markedsavdelingen er sannsynligvis den avdelingen som har best oversikt over virksomhetens eksterne omgivelser, hvilket omdømme bedriften har og om hvorvidt det

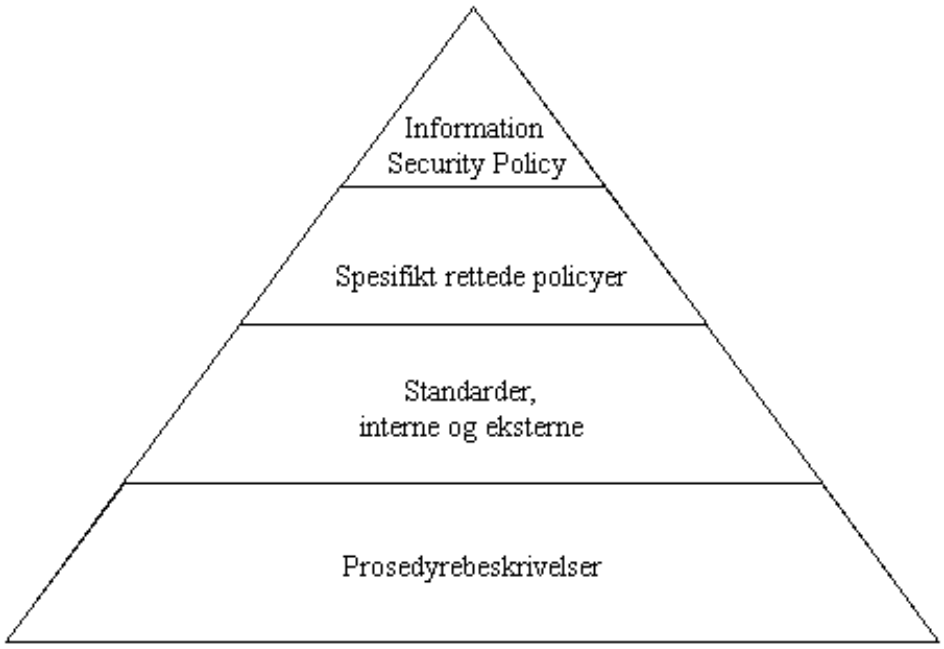
finnes interessegrupper som kan ha motivasjon til å utgjøre en trussel. I slike tilfeller kan en god markedsavdeling ha nyttig informasjon om trusselbildet, og kan fungere som en slags intern etterretningsorganisasjon.

Fordelene ved å involvere ressurser på tvers av avdelingene i en organisasjon er mange. Man får spredt budskapet om at dette er et viktig arbeid til alle avdelinger, og kan i så måte også sees på som første ledd i en prosess for å skape et sikkerhetsfokus i organisasjonen. Dessuten blir det lettere å få gjennomslag for tiltak og endringer dersom store deler av organisasjonen ser hvordan dette kan skape verdi. Dersom et slikt arbeid blir gjennomført på en god måte, får man samlet alle elementer i informasjonssikkerhetsarbeidet, satt dem i riktig kontekst og kommunisert dette til hele organisasjonen.

3. Strategifasen.

3.1 Sikkerhetspolicy og dokumentasjonsarbeid

Etter å ha gjennomført en risikovurdering, har virksomheten en god oversikt over hva som bør beskyttes og hvor tiltak bør settes i verk for å oppnå tilfredsstillende sikkerhet. Dette er den fasen som oftest blir ignorert, da man som regel hopper direkte til implementeringsfasen etter å ha oppdaget svakheter. Selv om åpenbare sikkerhetshull kan kreve umiddelbare tiltak, er det viktig å bruke tid og ressurser på å planlegge hvordan slike tiltak skal iverksettes og ivaretas over tid. For å sikre kontinuitet i sikkerhetsarbeidet, må prosessene rundt dette formaliseres. En formalisering vil redusere kompleksiteten rundt design og implementering av de tiltakene som har vist seg nødvendig gjennom undersøkelsesfasen. Slik formalisering tar form gjennom utarbeidelsen av et hierarkisk sett av dokumentasjon, som på hvert nivå gir en spesifikk type dokumentasjon. Figur 3.1 illustrerer dette dokumentasjonshierarkiet:



Figur 3.1 Dokumentasjonshierarki

3.1.1 Overordnet Information Security policy

Det øverste nivået i dette dokumentasjonshierarkiet er en såkalt Information Security Policy. Dette er et dokument som er en overordnet, generell retningslinje som reflekterer virksomhetens syn på informasjonssikkerhet. En slik policy skal definere hvorfor sikkerhetstiltak er nødvendig, hvilke aktiva som er verdifulle i denne sammenheng, og bør også i generelle termer gjøre rede for virksomhetens målsetninger i forhold til informasjonssikkerhet. Dette er med andre ord en kortfattet strategisk plan for implementering og videreføring av tiltak som skal sikre informasjonsaktiva.

3.1.2 Spesifikt rettede policyer

Neste nivå er de mer spesifikt rettede policyer. Mens den overordnede policyen ser på hele virksomheten under ett, tar disse policyene for seg grupperinger internt i virksomheten. Dette kan være blant annet være for ulike avdelinger, ulike prosesser eller policyer som retter seg mot ulike brukergrupper. Slike policyer er mer detaljerte enn den i øverste nivå, men er likevel generelle i sin formulering. Et eksempel på en slik er *Policy for akseptabel bruk*, som jeg har beskrevet i kapittel 3.3.

3.1.3 Standarder

På neste nivå blir dokumentasjonen mer konkret og fokuset på teknologi er dominerende. Formålet med å etablere standarder er å redusere kompleksiteten ved å stadfeste helt spesifikt hva som skal oppnås og hva som forventes i forhold til de målene som er nedfestet i sikkerhetspolicyen. For egenutviklede systemer og prosesser bør slike standarder kan være opprettet internt i virksomheten, men det er også vanlig å benytte seg av allerede etablerte standarder som er tilgjengelige fra en rekke kilder. Dette er internasjonale standarder som beskriver best-practice løsinger for ulike systemer og IT-relaterte prosesser, og som kan spare bedrifter for tidkrevende dokumentasjonsarbeid så lenge de blir fullt ut forstått av dem som skal implementere disse.

3.1.4 Prosedyrer

Prosedyrene er det siste leddet i formaliseringen av virksomhetens informasjonssikkerhet. Dette er dokumentasjon som skal beskrive nøyaktig hvordan de ulike tiltakene skal settes i verk, eller nøyaktig hvordan ulike prosesser skal utføres. Ved å ha detaljrike prosedyrebeskrivelser, kan man forhindre at brukere skaper egne rutiner som kan være i strid med de målene man ønsker å oppnå.

3.2 Hva bør en sikkerhetspolicy inneholde?

I dette avsnittet vil jeg beskrive hva en policy bør inneholde i forhold til de ulike truslene en virksomhet står overfor, og i tillegg gi en kort beskrivelse av hvorfor jeg mener de ulike punktene er viktig for informasjonssikkerheten i en virksomhet. Jeg har dessuten beskrevet en Policy for akseptabel bruk, siden dette er en viktig del av arbeidet med å heve brukernes forståelse for sikkerhetsarbeidet.

Fysisk sikring:

Her tar man for seg fysisk sikring av både infrastruktur og informasjon. Dette er en viktig del av dokumentasjonsarbeidet, siden man her skal beskrive hvordan viktige aktiva skal beskyttes mot naturgitte og andre fysiske trusler. Dette kan tilsynelatende være en enkel dokumentasjon å skrive, men det finnes en rekke viktige hensyn som må tas på dette området. Det bør tas med informasjon om hvordan datarom skal beskyttes, hvilke miljøhensyn som skal tas og hvordan man regulerer fysisk tilgang til de ulike lokalene

Nettverk

Den delen av sikkerhetspolicyen som omhandler nettverkssikkerhet bør beskrive hvordan man ser for seg at sikkerheten bør være mot internett, og hvordan man vil organisere nettverkssikkerheten internt.

Fokus er ofte på eksterne trusler, men fokus på å sikre nettverket internt er vel så viktig. Det er vanlig å dele opp det interne nettet mellom ulike avdelinger, slik at man ikke har tilgang til nettverksressurser på tvers avavdelinger og enheter. En slik inndeling har også ofte med et fellesnett som alle har tilgang til, samt en såkalt DMZ, hvor man plasserer enheter som er eksponert mot internett. I denne delen av polycien bør man også beskrive hvilke regler som

gjelder for oppkobling mot bedriftsnettet dersom man befinner seg utenfor bedriftens fysiske nett, samt regler rundt trådløsnett

Autentisering

En policy bør definere hvordan virksomheten ser for seg at brukere autentiserer seg til nettverket.

Dette kan blant annet være passordregler, annet utstyr for bruk av autentisering, gjesteadgang og rettighetsfordeling. Man bør også informere om hvilken informasjon som blir logget når brukeren er tilknyttet virksomhetens nettverk.

Internett

Siden bruk av internett nå er vanlig på de fleste arbeidsplasser, er virksomheter eksponert mot et utall eksterne elektroniske trusler. En sikkerhetspolicy bør beskrive hvordan man ser for seg at det interne nettverket blir beskyttet mot trusler fra internett, og bør også regulere de ansattes bruksmønster når de bruker internett fra virksomhetens it-ressurser.

E-post

En sikkerhetspolicy bør beskrive hvordan virksomheten ser for seg at e-post blir håndtert, både med tanke på teknisk håndtering og brukerhåndtering.

E-post er en av de største sårbarhetene i en organisasjon, og kan fungere som inngangsport for en rekke trusler. Dessuten er e-post i utgangspunktet ikke en kryptert kommunikasjonsform, så den kan i teorien leses i alle ledd mellom avsender- og mottakernettverk.

Hvert døgn mottar Norges Handelshøyskoles e-postsystem i underkant av 500.000 e-post, hvorav ca 98,5% blir forkastet før de rekker mottaker. Dette illustrerer hvor viktig det er å ha god kontroll på innkommende og utgående e-post.

Backup og arkivering av data

Policyen bør også inneholde en beskrivelse av hvordan man ser for seg at backup og arkivering av data skal foretas i virksomheten. Dette gjelder for filer, databaser og ikke minst for arkivering av e-post. Det har i det siste vært stort fokus på arkivering av e-post i virksomheter, siden man her opererer uten papir som kan arkiveres på tradisjonell måte. Dermed kan det oppstå problemer i tvister hvor viktig kommunikasjon må dokumenteres.

Det bør også dokumenteres hvor ofte man tar backup, hvor lenge man tar vare på roterende backupmedia og hvor ofte man tar ut backupsett til permanent arkivering.

Kryptering

En policy bør utdype om kryptering skal benyttes i elektronisk kommunikasjon, og hvilke typer kommunikasjon som skal krypteres.

Som nevnt er mesteparten av nettverkstrafikken på internett ukryptert. Det samme gjelder trafikk på det interne nettet. Kryptering av nettverkstrafikk forhindrer slik avlytting, og blir stadig mer vanlig i forretningssammenheng på internett. De nyeste versjonene av programvare for navigering på internett gir mulighet for meget god kryptering, og det har i dag blitt langt enklere for bedrifter å innføre slik sikker kommunikasjon enn for bare få år siden.

Antivirus- og programvareoppdateringer

En sikkerhetspolicy bør inneholde informasjon om hvordan man ser for seg et forsvar mot virus og annen skadelig programvare. Denne delen bør også understreke hvor viktig det er å til enhver tid ha oppdatert software og operativsystem.

Outsourcing

For å sikre at komponentene i KIT-modellen blir ivaretatt ved en eventuell outsourcing, bør en sikkerhetspolicy inneholde informasjon om hvilke krav som blir stilt til tredjepart, og om hvordan dette budskapet skal formidles og formaliseres.

Katastrofehåndtering og beredskapsplaner

En sikkerhetspolicy bør slå fast hva som er forventet av katastrofehåndtering, samt et krav om regelmessige revisjoner av slike disse.

Katastrofehåndtering er en meget vesentlig del av sikkerhetsplanleggingen, og krever mye arbeid på alle nivåer i dokumentasjonshierarkiet. Slike planer inneholder elementer fra alle de overnevnte punktene, og må fokusere på hvordan virksomheten skal videreføre sine virksomhetskritiske prosesser dersom de skulle bli rammet av en hendelse som setter store deler av virksomheten ut av spill.

3.3 Policy for akseptabel bruk av IT-verktøy

En policy for akseptabel bruk er et dokument som tar for seg de delene av sikkerhetspolicyen som går direkte på bruk av systemene, og som vil fungere som en brukermanual i forhold til informasjonssikkerhet. I mindre bedrifter er dette ofte den eneste gjeldende sikkerhetsdokumentasjonen. Ideelt sett er dette et dokument som alle ansatte må signere. En slik sluttbrukerpolicy bør være kort og konsis, og skal fortelle hva sluttbrukeren kan og ikke kan foreta seg ved bruk av virksomhetens it-ressurser. De viktigste punktene i en slik policy er:

- *Regler rundt autentisering.*
  Her beskriver man hvilke regler som gjelder rundt autentisering på nettverket. Dette kan være regler rundt passordbytte, passordoppbevaring og presisering av viktigheten ved å holde passord hemmelig. Dersom disse reglene blir fulgt, har man langt på vei klart å forhindre sikkerhetsbrudd basert på Social Engineering.

- *Bruk av selve datautstyret*
  Her beskriver man hva brukeren har lov til å foreta seg med det utstyret man har til disposisjon. Dette kan gjelde installasjon av tredjeparts programvare og bruk av egen hardware. Man har i dag muligheten til å lagre store mengder data på små eksterne enheter, som for eksempel mobiltelefoner, mp3-spillere og minnepenner. Bruken av slike enheter bør reguleres. Nylig kunne man lese om en ansatt ved et PPT-kontor i en av Bergens nabokommuner, som hadde mistet en minnepenn hvor det blant annet var lagret store mengder konfidensielle pasientopplysninger. Dette illustrerer tapspotensialet ved bruk av slike enheter, og hvorfor dette må reguleres.

- *Bruk av e-post og internett.*

  Her bør man på en enkel måte beskrive hva som er akseptable bruk av Internett. Utfordringen her blir å beskrive forskjellen mellom internett som ressurs og internett som en trussel. En kort beskrivelse av hvilken type nettsteder som er forbudt bør også være med her. Man bør også bli påminnet om at dersom man benytter virksomhetens ressurser på internett, vil man automatisk bli linket til virksomheten. Det man foretar seg gjør man altså i virksomhetens navn.

  Denne delen av policyen bør også beskrive hvilken informasjon brukere har lov til å sende elektronisk over internett, og i så tilfelle hvordan dette skal gjøres.

- *Sanksjoner*

  En slik policy bør også inneholde et avsnitt som tar for seg de ulike sanksjonsalternativene virksomheten kan ta i bruk ved brudd på sikkerhetsreglementet.

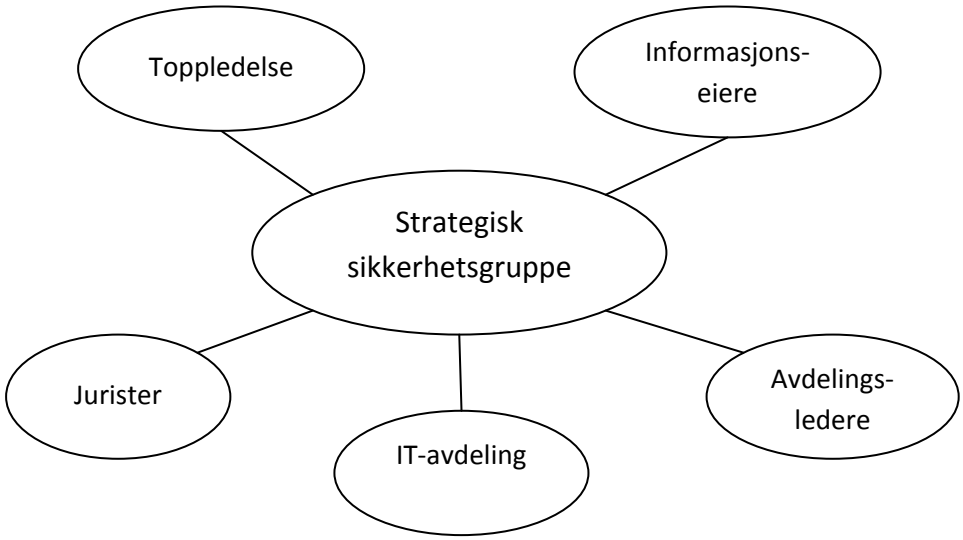
3.4 Ansvar og organisering

Før man starter dokumentasjonsarbeidet, er det viktig å ha klare ansvarsfordelinger og en etablert sikkerhetsgruppe. Man kan gjerne ta utgangspunkt i ansvarsfordelingen fra risikoarbeidet som ble gjennomført i den foregående fasen. Som nevnt er støtte fra toppledelsen viktig for å etablere en velfungerende sikkerhetsorganisasjon. Ved etablering av sikkerhetspolicyer strekker toppledelsens ansvar seg lengre enn bare støtte, den må også være en del av prosessen. Involvering fra toppledelsen er det ofte vanskelig å få gjennomslag for. Dokumentasjonsarbeid, på lik linje med annet sikkerhetsarbeid, fokuserer mye på detaljer, mens toppledelsen har fokus på det store bildet. Dessuten vil et slikt sikkerhetsarbeid kreve betydelig finansiell støtte, uten at man kan forvente håndfaste finansielle resultater. En god risikovurdering vil synliggjøre dette behovet, men det kan likevel være vanskelig å oppnå uten at toppledelsen er involvert i selve prosessen. Det at toppledelsen deltar aktivt i utformingen av en sikkerhetspolicy, sender også et signal til resten av organisasjonen om at dette er en viktig prosess, og skaper dermed en form for anerkjennelse internt i organisasjonen. Dette vil gjøre implementeringsfasen til en mer overkommelig oppgave. Videre vil man ha bedre ryggdekning for de sanksjonsalternativene man vurderer som aktuelle i en slik policy, og man vil ha bedre innsikt i eventuelle juridiske problemstillinger som kan oppstå som følge av slike sanksjoner.

Siden ledelsen ofte mangler teknisk forståelse i forhold til mange av de tiltakene som er aktuelle, er det viktig å formidle at ikke alle involverte trenger å vite hvordan teknologien fungerer, men man trenger å vite hvilken effekt de ulike tiltakene har på virksomhetens forretningsprosesser. En sikkerhetspolicy blir definert ikke bare ut fra resultatene fra undersøkelsesfasen, men også fra virksomhetens langsiktige strategiske planer. Dersom sikkerhetstiltak blir overlatt til teknologer, kan man fort oppleve at de går på bekostning av andre forretningskritiske prosesser, og på den måte vil virke mot sin hensikt. Det eksisterer som tidligere nevnt ofte et markant skille mellom de som ivaretar virksomhetens forretningsprosesser og de som drifter de tekniske løsningene. Dette må også tas hensyn til i dokumentasjonsarbeidet. Ved å etablere en gruppe som inneholder parter fra begge leire, hvor man tar for seg de ulike risikoene som ble avdekket i undersøkelsesfasen, kan man sammen vurdere hvordan en sikkerhetspolicy kan underbygge de forandringene som kreves. I tillegg bør en slik gruppe inneholde ledere fra samtlige av virksomhetens avdelinger, siden hele

bedriften vil bli berørt ved innføring av en sikkerhetspolicy. En slik gruppe vil være en ressurs, ikke bare under utarbeidelsen av en slik sikkerhetspolicy, men også for å opprettholde bedriftens kunnskap om dette arbeidet. Siden sikkerhet er en kontinuerlig prosess, vil en sikkerhetspolicy være avhengig av stadige revisjoner, og da vil etableringen av en slik gruppe ha stor verdi.

En slik gruppe bør altså inneholde representanter fra toppledelse, mellomledelse og fra it-avdelingen. Man bør også ta utgangspunkt i arbeidet som ble gjort da man kartla virksomhetens informasjonsaktiva i undersøkelsesfasen. En del av det arbeidet som ble gjort der var å finne ut hvem som hadde eierskap til de ulike aktivaene, siden det var disse som best kunne anslå den interne verdien av disse. Disse informasjonseierne vil det være naturlig å ta med i en slik gruppe, siden de vil være best egnet til å anslå hvordan foreslåtte tiltak vil påvirke de ulike informasjonsaktiva. Figur 3.2 viser hvordan en slik gruppe bør være sammensatt.



Figur 3.2 Organisering av strategifasen

Når man så har samlet en slik gruppe, starter man arbeidet på den overordnede sikkerhetspolicyen. Denne skal bare inneholde de målsetningene som skal synliggjøre bedriftens filosofi i forhold til informasjonssikkerhet, og danne grunnlaget for det videre arbeidet. Som tidligere nevnt, har man ofte en overordnet sikkerhetspolicy, og mange

underordnete som tar for seg informasjonssikkerheten på de ulike nivåer og avdelinger i en virksomhet. Disse er ofte mer spesifikke, og tar for seg hvordan man ser for seg sikkerhetsnivået i forhold til bestemte systemer og rutiner. Når man har fullført policyene fra de to øverste nivåene i dokumentasjonshierarkiet, overtar avdelingslederne og informasjonseierne arbeidet med utarbeidelsen av prosedyrer og standarder. Dette er detaljarbeid, og krever eksperthjelp fra de som er systemeksperter. Ekspertene her er ikke nødvendigvis teknologer, mye av prosedyrearbeidet går på hvordan mennesker skal forholde seg til ulike trusselbilder, og krever like mye innsats fra en personalavdeling som fra en it-avdeling.

Etter at dokumentasjonsarbeidet er gjennomført, bør man sende forslaget til høring i virksomheten. Det er spesielt viktig at den blir vurdert av jurister, slik at man får avklart om det foreligger eventuelle brudd på lover og regler forbundet med personsikkerhet og lignende. Nylige eksempler fra Vinmonopolet og Redningsselskapet viser hvilke problemer en virksomhet kan havne i dersom man griper for mye inn i ansattes private sfære. Dessuten må man få avklart at de sanksjonene man opererer med er i tråd med gjeldende lover og regler.

4. Implementeringsfasen

Implementeringsfasen har jeg valgt å dele inn i to deler. Første del tar for seg hvordan virksomheten bør gå frem ved implementering av sikkerhetspolicy og andre tiltak som går på brukeratferd. Dette er holdningsskapende arbeid, hvor mye av implementeringsprosessen er fokusert på hvordan ledelsen skal formidle de nye rutinene og tiltakene som har blitt dokumentert i strategifasen.

Den tekniske implementeringsfasen tar for seg hvordan virksomheten bør gå frem for å sikre at de tiltakene som bygger på informasjonsteknologi blir gjennomført på en forsvarlig måte. Her har jeg fokusert mye på outsourcing, siden jeg mener dette ofte er et fornuftig valg for de fleste virksomheter.

4.1 Implementering av sikkerhetspolicy

En sikkerhetspolicy fører ikke i seg selv til god sikkerhet, den definerer sikkerheten organisasjonen trenger, og oppmuntrer til iverksettelse av tiltak. Det viser seg imidlertid ofte at ansatte ikke følger de prosedyrer de har signert på og sagt seg villige til å følge. Utfordringene blir dermed å sikre at gjeldende retningslinjer faktisk blir fulgt.

Utviklingsarbeidet har størst mulighet for å lykkes dersom det styres av en sterk, handlekraftig og engasjert ledelse, men alle ansatte som blir berørt bør involveres. For at en omstillingsprosess skal lykkes er det viktig at alle berørte parter er enige i og erkjenner at det er behov for en endring. De ansatte bør, som nevnt i strategifasen, involveres sammen med ledelsen for å komme frem til en felles diagnose av problemet. Dette vil medføre sterkere forpliktelse når behandlingen av problemet skal gjennomføres. Det er svært viktig at medarbeiderne raskt orienteres om hvilke omstillinger som planlegges. Å motivere til ny praksis innebærer imidlertid alltid en utfordring, da slike tiltak ofte medfører merkbare endringer i de ansattes arbeidshverdag, og slike endringer blir ofte mottatt med skepsis. Ansatte i de lavere lag av virksomheten, som gjerne kan betegnes som det svakeste leddet i en sikkerhetsorganisasjon, har ofte en langt mindre følelse av personlig ansvar overfor de oppgavene man er satt til å utføre, og nye sikkerhetstiltak kan lett bli ignorert til fordel for

tradisjonelle og etablerte arbeidsrutiner. Her er det viktig for ledelsen å stå frem som sterk og handlekraftig i forhold til de nye visjonene som blir synliggjort gjennom sikkerhetspolicyer og tilhørende sikkerhetsdokumentasjon.

Dersom sluttbrukerne ikke forstår hvilken merverdi som ligger i de nye tiltakene og de risikoene som er knyttet til de systemer og prosesser som angår dem, blir det vanskelig å innføre nye rutiner. For å sikre at alle berørte parter forholder seg til og følger de omstillinger som er påkrevd, må informasjonen om endring være saklig og tilpasset hver enkelt målgruppe. De ansatte bør også få mulighet til å komme med innspill og ha opplevelse av et samarbeid med ledelsen i forhold til hvordan de ulike problemene kan løses. Dette styrker teamopplevelsen og følelsen av å ha påvirkningskraft i forhold til egen arbeidssituasjon, noe som igjen øker sjansene for at de ansatte faktisk innretter seg etter påkrevde endringer.
De forventninger man har til de ansatte må formidles tydelig. Det er en fordel om forventningene kan formuleres i sikkerhetspolicyene som konkrete regler for atferd som de ansatte må følge.

I en omstillingsprosess bør man videre sikre at de ansatte opplever at de har tilstrekkelig med ressurser, både materielt og menneskelig, til å gjennomføre de endringer som blir pålagt.
Noen av de tiltak som kan settes i verk for å fremme bevisstheten rundt informasjonssikkerhet blant sluttbrukere er:

Brukeropplæring
Ved å innføre opplæringskampanjer, hvor man informerer om risiko, tiltak og verdien av selskapets informasjonsaktiva, øker man bevisstheten hos de ansatte. Obligatorisk kursing, med fokus både på bedriftens generelle policy og på risiko som berører den ansattes arbeidsoppgaver spesielt, er en effektiv måte å holde de ansatte oppdatert på. Egne sikkerhetsprogrammer for nyansatte er også en effektiv måte å opprettholde virksomhetens sikkerhetskultur.

Sikkerhetsinformasjon må tilgjengeliggjøres

Informasjonen må være lett tilgjengelig, og informasjonen må være tilrettelagt for de enkelte avdelingers oppgaver.

Signering av policy

Man bør gjøre det obligatorisk å lese og signere sikkerhetspolicyen, hvor de ansatte bekrefter at de er klar over hva som blir forventet av dem og hvilke sanksjoner som kan bli iverksatt ved brudd på disse reglene.

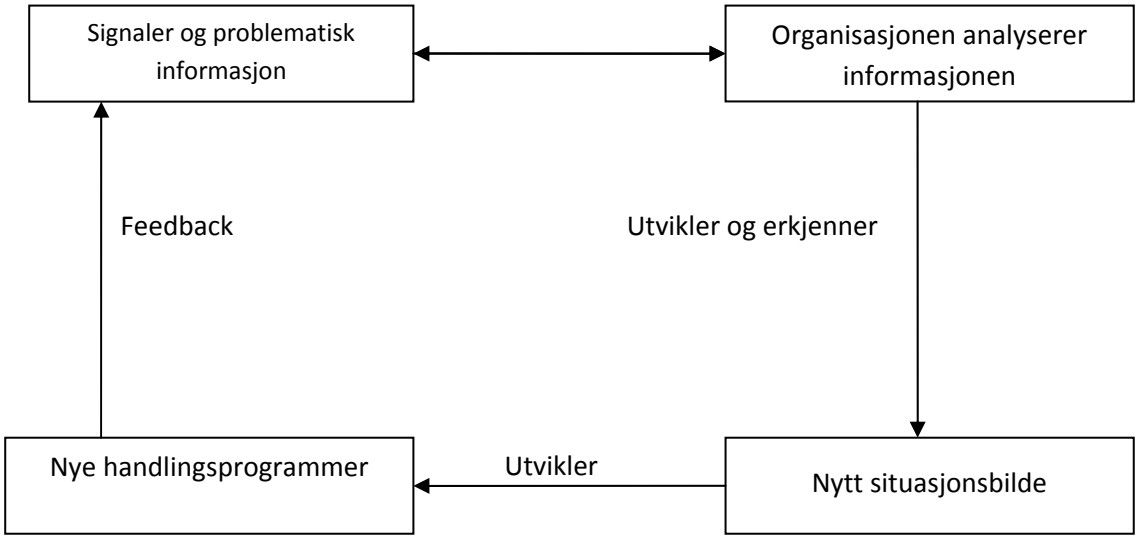
Fokus på supportapparat

Nye rutiner skaper usikkerhet, og et godt supportapparat vil gjøre overgangen lettere for uerfarne og usikre brukere.

Motiveringsarbeid

Det kan videre være aktuelt å utarbeide oversikt over aktuelle negative konsekvenser eller korrektive tiltak som vil inntreffe dersom man som arbeidstaker ikke retter seg etter de nye retningslinjene som er innført. Det er viktig å forberede arbeidstakerne på eventuelle negative konsekvenser som vil komme i kjølvannet av uønsket praksis. Dette skaper forutsigbarhet og gir bilde av en tydelig ledelse for bedriftens ansatte. Det er imidlertid verdt å merke seg at innlæring av ny atferd hos en gruppe ansatte fremmes best gjennom positivt motiverende tiltak. Som nevnt tidligere forutsetter et slikt fokus at forventet atferd fra de ansatte er tydelig og konkret definert i gjeldende regelverk, slik at det ikke er tvil om hva ønsket praksis faktisk er. Videre innebærer det at ledelsen på alle nivåer i bedriften må være aktive i det å fremheve ønsket praksis. Eksempler på at de nye retningslinjene blir fulgt bør løftes opp og belyses, sammen med informasjon om hvilken betydning dette har hatt for bedriften. Det kan være hensiktsmessig å se både på individuelle prestasjoner, den enkelte avdelings virksomhet, og bedriften som helhet. Positive tilbakemeldinger vil virke motiverende på de ansatte og bidra til at de i økt grad følger opp i forhold til sikkerhetspolicyen. Det å rose de ansatte for å følge gjeldende regelverk vil virke mer læringsfremmende og medføre at den nye policyen integreres som en del av bedriftens rutiner langt raskere, enn dersom ledelsen avventer og ikke gir tilbakemelding til de ansatte før det er en eller flere som har brutt med gjeldende retningslinjer.

Implementering av nye sikkerhetspolicyer bør ideelt sett iverksettes i perioder hvor organisasjonen er velfungerende og stabil. Arbeidsklimaet vil da være preget av tillit mellom ansatte og ledelse, og de ansatte vil dermed vise mindre motstand mot endring. Utfordringen er imidlertid at når en organisasjon fungerer godt er det vanlig å gjøre mer av det man alltid har gjort for å bedre kvalitet og effektivitet, fremfor å forandre rutinene. Endring og styrking av sikkerhetspolicyer vil ofte tvinges frem av en krise. Samarbeidet mellom ansatte og ledelse vil da ofte preges av mistenksomhet og mistillit, noe som vanskeliggjør endringsarbeidet. Det er derfor viktig at organisasjoner etablerer et slikt utviklingsarbeid som en del av de interne rutinene, og at forbedringsfokuset manifesteres som en viktig del av organisasjonskulturen.



Figur 4.1 Implementering av sikkerhetspolicy

Figuren viser hvordan dette kontinuerlige samspillet mellom ledelse og ansatte bør fungere for at informasjonen rundt nye sikkerhetstiltak og rutiner skal få effekt i form av endret atferd.

4.2 Teknisk implementering

I den tekniske implementeringsfasen står virksomheten overfor to valg. Man kan velge å implementere og drifte de tekniske sikkerhetsløsningene internt, eller man kan gi ansvaret for disse til eksterne eksperter, såkalt outsourcing.

Velger man å drifte de tekniske løsningene internt, må man vite at de ansatte som er satt til å gjøre jobben behersker de utfordringene som er knyttet til dette arbeidet. Sikkerhetsløsninger er som regel komplekse, og utfordringene er mange. Et stadig tilbakevendende problem er mangelen på kvalifisert arbeidskraft innenfor denne sektoren. Spesielt små og mellomstore bedrifter kan oppleve problemer med å tilfredsstille de kunnskapskrav som kreves innenfor disse segmentene, og man vil ofte oppleve at søkermassen til ledige it-stillinger er underkvalifisert. It-avdelinger, som ofte har ansvar for store deler av implementeringsfasen, er utsatt for et konstant press hvor man forventer at man gjør mye med begrensede midler. I slike situasjoner vil det ofte være aktuelt å outsource hele eller deler av sikkerhetsarbeidet til eksterne sikkerhetseksperter.

Det mest tilbakevendende argumentet for outsourcing er kostnadsreduksjon. Ved å flytte ansvaret for sikkerhet ut av bedriften, vil man redusere kostnader i forhold til bemanning, drift og investeringer i utstyr og annen type infrastruktur knyttet til informasjonssystemer. Blant disse er reduksjon i bemanning ofte den største kostnadsbesparelsen, spesielt for større virksomheter som krever 24-timers oppetid året rundt. Da slipper man ressurskrevende sikkerhetsarbeid, og kan i stedet fokusere på bedriftens kjernevirksomhet. Outsourcing gir et oversiktlig kostnadsbilde, med faste kostnader og få, om noen, uventede tillegg. Man slipper å bruke ressurser på sykelønn, overtid, reise- og kurskostnader og andre typer personalkostnader som kommer på toppen av de faste lønnsutgiftene. Man slipper også store deler av investerings- og driftskostnadene som er knyttet til hardware, software, lokaler, etc., som man trenger for å tilfredsstille sikkerhetskravene. Dette ansvaret blir her skjøvet over på det eksterne sikkerhetsfirmaet.

En annen grunn til å velge å drifte slike systemer eksternt vil være at man er på jakt etter økt servicegrad. Firma som tilbyr slike tjenester vil i stor grad være spesialister innenfor sikkerhetsfeltet, og vil som regel ha langt høyere samlet kompetanse enn det man kan oppnå hos sine interne ansatte. Mindre organisasjoner har ofte ikke tilstrekkelig mengde arbeidsoppgaver til å tiltrekke høyt kvalifisert arbeidskraft. Er man ekspert på et område vil man sjelden være fornøyd med de ensformige arbeidsoppgaver og den rutinemessige jobbtilværelsen som ofte er hverdagen hos virksomheter hvor IT bare er en hjelpefunksjon. Sikkerhetsfirma kan tilby bedre betingelser, varierende arbeidsoppgaver og ikke minst et miljø hvor man til stadighet blir utsatt for sikkerhetsmessige utfordringer. Sikkerhetsfirma med tilstrekkelig stor kundebase vil være kontinuerlig utsatt for angrep, noe som gir ekspertene uvurderlig erfaring. Eksperter har også tid og mulighet til å teste, utvikle og implementere de verktøyene som til enhver tid er best egnet, og med en vid kundekrets vil de kunne dra nytte av den erfaringen som man tilegner seg hos andre kunder. Dessuten kan man sammen med andre firma oppnå stordriftsfordeler, siden slike store sikkerhetsfirma ofte vil ha kraftige systemer som en enkel virksomhet ikke vil ha midler til å anskaffe. Dette er systemer som kan håndtere flere kunders sikkerhet samtidig, og som dermed lettere kan gjenkjenne trusler og angrepsmønstre når slike oppstår, problemer som mindre systemer ikke ville ha fanget opp før problemet var omfattende. Det er med andre ord meget vanskelig for vanlige virksomheter å matche den kompetansen slike sikkerhetsfirma sitter inne med.

Outsourcing har også negative sider. Den vanligste bekymringen ved outsourcing er at virksomheten mister kontrollen over sikkerhetsprosessen siden de ikke lenger har kontroll over den daglige driften. Man kan lett mistenke en tredjepart for ikke å ha samme fokus og interesse av å beskytte virksomheten som det man ville oppnådd ved å drifte tjenestene intern. For mindre organisasjoner kan man i tillegg oppleve at man ikke får det samme fokus fra sin tjenesteleverandør som større virksomheter, både med tanke på tjenester, pris og kompetanse. Selv om et sikkerhetsfirma har eksperter med høy kompetanse, er det langt fra sikkert at disse blir benyttet nettopp for din organisasjon, og dette vil særlig gjelde for mindre kunder. Man kan også oppleve at man mister muligheten for egne tilpasninger og konfigurasjoner ved outsourcing. Eksterne firma tilbyr gjerne standardpakker, med et tjenesteinnhold som dekker de fleste behov, men som ikke tar hensyn til bedriftsspesifikke behov.

Ved outsourcing begrenser man også muligheten til å videreføre kunnskap om de ulike sikkerhetsprosessene. Selv om den daglige driften blir satt ut til en tredjepart, må man ha en mulighet for å flytte denne driften tilbake dersom noe skulle skje med firmaet man setter ut driften til. Sikkerhetsfirmaet kan gå konkurs, det kan bli oppkjøpt eller det kan fase ut ulike typer av sin virksomhet. Det er da meget viktig at kunden har kunnskap nok om sin egen sikkerhetsprosess til å kunne ivareta denne i en overgangsperiode. Dette er en balansegang som kan være vanskelig å håndtere, siden et av argumentene for outsourcing er å redusere intern arbeidskraft innenfor dette området.

Outsourcing er også et spørsmål om tillit. Ved å outsource informasjonssikkerheten, gir man i praksis en tredjepart innsyn i virksomhetens konfidensielle informasjon, og dette kan sitte langt inne hos ledelsen. Siden sikkerhetsfirma opererer med flere kunder, vil ulike kunders sensitive informasjon i prinsippet bli behandlet av de samme systemene.

Kostnadsreduksjon og ekspertise er dermed nøkkelordene for outsourcing, mens mangel på kontroll og tillit, samt spørsmål rundt leverandørens kompetanse, er de mest brukte motargumentene. Hvordan håndterer man da denne usikkerheten, slik at man kan oppnå de åpenbare besparelser som effektiv outsourcing medfører, og hvordan velger man den tilbyderen som gir det beste tilbudet for virksomheten?

Valget av riktig outsourcing-partner er en vanskelig prosess dersom man ikke kjenner markedet. De fleste slike bedrifter fremstår som ganske like, mens kompetansen i markedet er meget variabel. Derfor er kjennskap til bransjen viktig for bedrifter som er på jakt etter slik hjelp. Tjenesteleverandørens økonomiske situasjon er også viktig, da man fort kan risikere å stå på bar bakke dersom leverandøren ikke lenger klarer å opprettholde sitt tilbud.

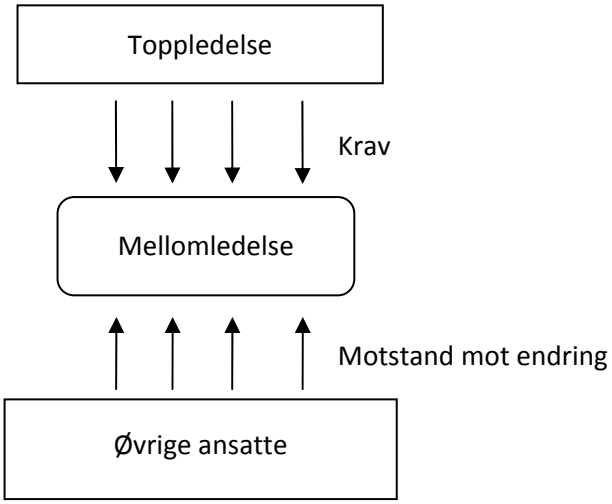
Når man har valgt leverandør, vil neste steg være å opprette gode Service Level Agreements (SLA) med sikkerhetsfirmaet man velger. Dette er avtaler som regulerer forholdet mellom kunden og tjenesteleverandør, og beskriver de forventningene kunden har til tjenestenivået. Dette kan være funksjonelle krav til bl.a. oppetid, responstid og logging, men også krav om kvalifisert personell og beskrivelser av prioriteringer. Utformingen av slike avtaler er en viktig, men ressurskrevende prosess, avhengig av kompleksiteten i tjenestene man ønsker å

outsource. Ved å fokusere på disse kan man unngå ubehagelige overraskelser og skjulte kostnader, samtidig som man får formalisert samarbeidet med sikkerhetsleverandøren på en måte som er vanskelig å få til på tvers av interne avdelinger.

4.3 Ansvar og organisering.

4.3.1 Implementering av sikkerhetspolicy - endringsledelse

Implementering av sikkerhetspolicyer og nye prosedyrer i en virksomhet krever en tydelig top-down basert kommunikasjonsform, hvor ledelsen påpeker viktigheten av de tiltakene som skal settes i verk. Burke Litwin-modellen (Bruke, 2008) understreker viktigheten av å analysere hvilke former for organisasjonsendringer man ønsker, for slik å klargjøre hvordan implementering skal gjennomføres. I denne modellen skilles det mellom transaksjonsledelse, som rettes mot endring i ledelsespraksis, struktur og systemer, og transformasjonsledelse, hvor omstillingen omhandler organisasjonsmedlemmenes måte å tenke på, og hvor leders oppgave blir å motivere sine underordnede og på den måten fokusere på å heve deres bevissthetsnivå. Med utgangspunkt i denne modellen, er det naturlig å tenke at organisasjonen i denne sammenheng har behov for en transformasjonsledelse, siden målet er å endre organisasjonens måte å tenke på i forhold til sikkerhet. I en slik endringsprosess må man ha en ledelse som står frem som en rollemodell for resten av organisasjonen, og som klarer å formidle budskapet om informasjonssikkerhet på en måte som inspirerer og motiverer. Ledelsen må også ha særlig fokus på mellomledere og avdelingsledere, og sørge for at disse er kontinuerlig orientert og oppdatert i forhold til de tiltakene som blir satt i verk i forbindelse med sikkerhetspolicyene. Dette fordi ledere på dette nivået er i en presset situasjon mellom toppledelsen og de øvrige ansatte i virksomheten, som vist i figur 4.2.



Figur 4.2 Fokus på mellomledelse

Ofte kjennetegnes omstillingsprosesser i en organisasjon ved at det er mangel på struktur, opplevd uvisshet og lav egenkontroll blant de ansatte. Arbeidsklimaet kan endres og bli preget av stress i en overgangsperiode. Omstillinger hvor ledelsen er tydelig og engasjert og har en klar plan for hvordan omstillingsarbeidet skal gjennomføres kan imidlertid styrke organisasjonen, i form av bedre samhold hvor hele organisasjonen jobber mot et felles mål. Dermed vil man lettere få aksept for sikkerhetstiltak som i utgangspunktet kan fremstå som unødvendige og hemmende.

4.3.2 Teknisk implementering – håndtering av outsourcing

Når man planlegger outsourcing av informasjonssikkerhet bør man uansett opprettholde et sikkerhetsfokus hos den gjenværende it-staben. Dette for å beholde kontinuitet rundt kunnskapen om bedriftens sikkerhetsprosesser, og for å kunne beholde nok it-kunnskap til å kunne stille kritiske spørsmål rundt de tekniske løsningene som blir tilbudt fra den eksterne partneren. For at outsourcing av informasjonssikkerhet skal være vellykket, må det være en felles forståelse mellom virksomheten og tredjepart rundt omfanget av prosessen. Virksomheten må definere klare retningslinjer for hvilke mål som skal oppnås og hvilket ansvar som skal legges til en tredjepart. Siden de delene av informasjonssikkerheten som kan outsources i denne fasen utelukkende er teknisk, er det naturlig at en teknolog, helst it-sjefen, eller har ansvar for denne delen. Likevel bør man også her ha representanter fra ledelsen med for å kunne sikre at et slikt arbeid ikke risikerer negativ påvirkning på virksomhetens kjerneprosesser.

Når en slik avtale om outsourcing er på plass, er det viktig med god kommunikasjon mellom de to partene. Slik kommunikasjon fortoner seg annerledes enn det man vanligvis har internt i organisasjonen, og dette kan være vanskelig i en overgangsperiode. En økt formalisering av kommunikasjonsprosessen krever planlegging og nøyaktighet, men kan på sikt føre til økt effektivitet da man ideelt sett ikke lenger er påvirket av interne mellommenneskelige faktorer.

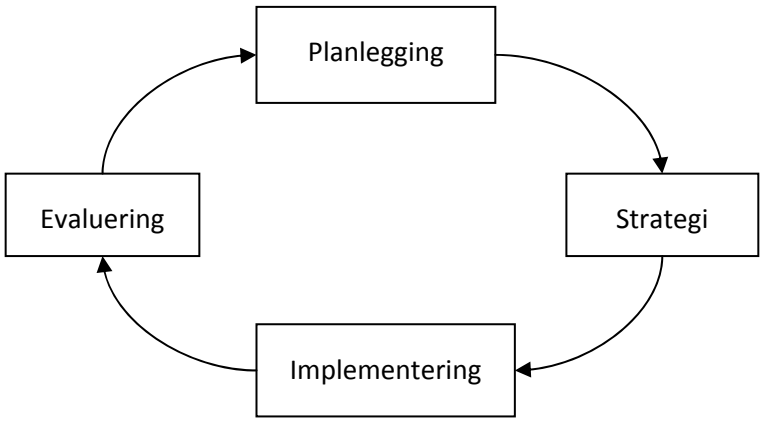
5. Konklusjon

I et informasjonssikkerhetsperspektiv, kan man si at det finnes to typer ansatte i en virksomhet – it-ansatte og brukere. De to gruppene har ofte divergerende oppfatning av informasjonssikkerhet. Teknologer har ofte vanskelig for å se for seg viktigheten av virksomhetens kjerneprosesser i forhold til det trusselbildet som systemene står overfor, mens brukere ofte ser på it-ansatte som en hemsko som reduserer effektiviteten i arbeidsdagen ved å pålegge dem tilsynelatende unødvendige sikkerhetstiltak. Dette gapet mellom brukere og it-avdeling er lite effektivt og kan fort bli kostbart, og det reflekterer toppledelsens manglende vilje til å involvere seg i sikkerhetsarbeid. Altfor ofte opplever man at sikkerhetsarbeid i en virksomhet utvikler seg ved at it-avdelingen oppdager behov for tiltak, for så å måtte kjempe for både midler og aksept før de får støtte til dette. En slik fremgangsmåte vil muligens løse spesifikke problemer på kort sikt, men bidrar svært lite til langsiktig kontinuitet i sikkerhetsarbeidet. Som jeg har påpekt gjennom alle de tre fasene, er involvering fra toppledelsen meget viktig for å oppnå tilfredsstillende sikkerhet. Ved å vise interesse og involvering i slike saker, sender dette et signal til resten av virksomheten om viktigheten av å beskytte og sikre organisasjonens informasjonsaktiva. Dessuten må man ha representanter fra ledelsen med i et slikt arbeid for å kunne sikre at det ikke settes i verk tiltak som reduserer effektiviteten i virksomhetens kjerneprosesser.

Som jeg har forsøkt å vise i denne oppgaven, skaper ikke teknologiske løsninger sikkerhet i seg selv. Tekniske løsninger uten tilstrekkelig bakgrunnsundersøkelser, dokumentasjon og kompetanse, skaper falsk trygghet og kan for vise seg å være et pengesluk uten tilsiktet effekt. Det som etter min mening må til, er en grundig og strukturert gjennomgang av de risikoene virksomheten står overfor, og en veloverveid plan for hvordan denne risikoen skal håndteres. Dette får man ikke til uten at toppledelsen er involvert. Informasjonssikkerhet har like mye med prosesser og menneskelig adferd å gjøre, som det har med teknologi. Ved å ta et slikt initiativ, vil toppledelsen ikke bare bidra til å skape bedre sikkerhetsrutiner, de vil også redusere avstanden mellom it-avdelingen og resten av de ansatte.

Alle de ulike fasene har ulik organisering, men felles for dem alle er at toppledelsen har en viktig rolle. Disse gruppene utgjør sammen et internt sikkerhetsforum i forhold til virksomhetens informasjonssikkerhet. Gruppene vil naturlig nok overlappe hverandre i sammensetning, men det viktige her er at informasjonen flyter godt mellom de ulike fasene, og at man klarer å utnytte de synergieffekter som en slik konstellasjon kan oppnå.

Det er viktig å påpeke at det arbeidet som jeg har beskrevet ikke er et prosjektarbeid hvor man har en prosjektstart og -slutt, men at det er et kontinuerlig arbeid som krever stadig oppfølging og oppdatering. Dette er beskrevet i figur 5.1.



Figur 5.1 Sikkerhetssyklus

Som en del av et slikt oppfølgningsarbeidet bør det også gjennomføres it-revisjoner, spesielt for større virksomheter. En it-revisjon er en kontroll gjennomført av eksternt konsulentselskap. Her man tar for seg de av virksomhetens it- og sikkerhetsprosesser som allerede er implementert, og vurderer disse opp mot de målsetninger virksomheten har satt seg. Formålet med slike kontroller er å få belyst sider av sikkerhetsprosessene som man gjerne ikke får avdekket ved intern kontroll, og for å få bekreftet at de etablerte tiltakene er i henhold til gjeldende lover og regler.

Ved å ha en slik kontinuerlig oppfølging, med jevnlige møter i sikkerhetsgruppene, oppdatering av nyttig dokumentasjon og opplæring av ansatte, vil man langt på vei kunne opprettholde et tilfredsstillende sikkerhetsnivå.

Informasjonssikkerhet er ikke et produkt, det er en prosess. Man kan ikke bare kjøpe en sikkerhetspakke og forvente at man har fjernet risikoen fullstendig. God planlegging, veldokumenterte systemer og prosesser, og en kontinuerlig oppfølging av de implementerte tiltakene skaper en sikrere hverdag for alle ansatte. Målsettingen er ikke å implementere perfekte sikkerhetstiltak, målsetningen er tilfredsstillende sikkerhet i forhold til den risikoen man har sagt seg villig til å akseptere. Vi vil fortsatt måtte godta at det finnes usikre nettverk, usikre applikasjoner og uoppdagede sårbarheter. Samtidig har mennesker alltid tatt risikofylte avgjørelser ellers i samfunnet, uten at samfunnet har brutt sammen av den grunn. Dette vil nok heller ikke informasjonssystemer gjøre, så lenge man har fokus på prosesser og ikke bare på teknologi.

Litteraturliste

BBC News (2007): *The cyber raiders hitting Estonia*. BBC News 17.05.2007 <http://news.bbc.co.uk/2/hi/europe/6665195.stm>

Burke, W. Warner (2008): *Organization Change, Theory and Practice*. 2. utg. Sage Publications, California

CAIDA (2003): *The Spread of the Sapphire/Slammer Worm*. Cooperative Association for Internet Data Analysis, 2003 <http://www.caida.org/publications/papers/2003/sapphire/sapphire.html>

Hausland, Anne Marie (2005): *Hvordan integrere IT-revisjon?* Riksrevisjonen, 2005. <http://www.riksrevisjonen.no/Aktuelt/Fagartikler/Fagartikkel_Hvordan_integrere_ITrevisjon.htm>

Intel Information Technology (2007): *Threat Agent Library Helps Identify Information Security Risks*. Intel White Paper, sep. 2007 <www.intel.com/it/pdf/threat-agent-library.pdf>

Landoll, Douglas J. (2006): *The security Risk Assessment Handbook,* Auerbach Publications, USA

Langeland Haugen, Erlend (2008): *HiB forsøkt svindlet*. Bergens Tidende, 2. apr. 2008 <http://www.bt.no/lokalt/bergen/article536123.ece>

Leyden, John (2003): *Office workers give away passwords for a cheap pen*. The Register, 18. apr. 2003 <http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords>

Panko, Raymond R. (2004): *Corporate Computer and Network Security*, Prentice Hall, New Jersey

Peltier, Thomas R. (2002): *Information Security Policies, Procedures and Standards*. Auerbach Publications, USA

Reason, James (1990): *Human Error*. Cambridge University Press, Cambridge

Schneider, Bruce (2004): *Secrets & Lies – Digital Security in a Networked World*. Wiley Publishing, Indiana

Skåra, Ove (2005): *Datatilsynet melder Redningsselskapet til politiet*. Datatilsynet, 3. okt. 2005 <http://www.datatilsynet.no/templates/Page____1208.aspx>

Skåra, Ove (2005): *Vinmonopolet politianmeldes*. Datatilsynet, 10. okt. 2005 <http://www.datatilsynet.no/templates/Page____1229.aspx>

Storvik, Anne Grete (2008): *Mistet taushetsbelagt informasjon på parkeringsplass*. Dagens Medisin, 11. mar. 2008 <http://www.dagensmedisin.no/nyheter/2008/03/11/mistet-taushetsbelagt-info>