

Sikkerhed er ledelsens ansvar – og ikke blot et IT projekt.

af Frederik Helweg-Larsen, CISM

Implementering af sikkerhedspolitikker baseret på kendte standarder er i fuld gang i virksomheder og organisationer landet over, men alt for ofte er det isolerede projekter, der ikke er forankret i ledelsen. Ved at følge nogle enkle grundregler kan det undgås, at projektet strander og ender i en fiasko.

I disse tider tales der rigtig meget om *compliance* og *governance*, dvs. efterlevelse af de politikker og regler der er besluttet – og ledelsens involvering og håndtering af alt, hvad der berører virksomhedens drift og troværdighed. Det er store ord der bruges her, men meget af dette omhandler den hverdag, vi har i vores daglige arbejde. Når vi taler om *governance* og *compliance* handler det mest af alt om at sætte denne hverdag i system og blive bedre til at styre efter de mål, der er sat af ledelsen.

Hvor er jeres sikkerhedspolitik i dag?

Der er næppe mange virksomheder, som ikke har en officiel IT sikkerhedspolitik i dag. Men der er sandelig mange forskellige variationer af dem. Jeg har efterhånden set temmelig mange sikkerhedspolitikker, og der er meget stor forskel på hvor omfattende de er, hvor detaljerede og i hvor høj grad de er implementerede. Endelig kan man dele politikkerne op i to hovedgrupper:

Dem der forankrede i virksomhedens ledelse.

Dem der er forankrede i IT afdelingen.

Prøv med denne uvidenskabelige inddeling at vurdere hvor langt jeres politik er nået:

1. er formaliseret og nedskrevet
2. er godkendt af ledelsen
3. er kommunikeret ud til alle medarbejdere (helt eller delvist)
4. bliver regelmæssigt fulgt op og kontrolleret
5. bliver regelmæssigt vurderet på møder i sikkerhedsudvalget
6. topledelsen modtager rapporter der beskriver risici og afvigelser som der reageres på

Fra politik til virkelighed – hvor langt er der?

Der er rigtig mange politikker, der kun eksisterer på papiret, og bestemt ikke er en afspejling af den hverdag, som medarbejderne oplever. De eksisterer kun på papir, fordi de er et sæt af beslutninger, der ikke er effektivt kommunikeret til medarbejderne, og fordi de ikke er underbygget af gode argumenter og konsekvenser ved ikke at følge reglerne. Det kan få den konsekvens, at medarbejderne ikke har respekt for de beslutninger der er truffet, da de jo ikke er helhjertet gennemført. Så er der kun en skuldertræk fra de medarbejdere, det hele handler om.

Compliance kan ses på bundlinjen

Uanset om sikkerhedspolitikken baseres på standarder som Cobit, ISO, Dansk Standard (DS484), Sarbanes-Oxley, EuroSOX eller andre, så er der ikke noget argument for at udlade at implementere politikken.

Der er gennemført adskillige internationale undersøgelser der alle viser, at virksomheder der er gode til at følge op på deres ledelsesbeslutninger og kan dokumentere efterlevelsen af de standarder der er besluttet, alle har en markant bedre indtjening end gennemsnittet.

Compliance er altså mere god ledelse og kvalitet, end noget der relaterer specifikt til IT sikkerhed.

Sikkerhed er ikke kun et anliggende for IT afdelingen

”Hvis det er så godt, hvorfor er det så ikke almindeligt udbredt?”, kunne man så spørge.

Når vi taler om IT sikkerhed, så ligger det store problem i de første to bogstaver – ”IT”. Det er nemlig medvirkende til, at projektet straks placeres i IT afdelingen, og ledelsen forventer at der nu er taget hånd om den opgave.

Hvis man har brugt tid på at bladre standarder som DS484 eller ISO27001 igennem, så bliver det hurtigt klart, at dette er meget mere end traditionel IT og teknik. Det vedrører frem for alt mennesker og processer, og involverer også personaleledelsen, økonomiledelsen og topledelsen. Alle virksomhedens funktioner er involverede, og netop derfor bør opgaven ikke isoleres i en enkelt afdeling.

Når ledelsen ikke er med får projektet ikke momentum

Som tidligere nævnt, så kan man dele politikkerne op i to hovedgrupper: Dem der er forankrede i virksomhedens ledelse, og dem der er forankrede i IT afdelingen. Det falder tit sammen med grupperne for succesfulde projekter og dem der blev knap så vellykkede.

Alle erfaringer viser, at hvis topledelsen ikke tager ansvar for opgaven med at beskytte virksomhedens værdier, så bliver det utroligt vanskeligt at få resten af organisationen med. Det betyder ikke, at topledelsen skal være dybt involverede i alt det praktiske arbejde med sikkerheden. Opgaverne kan sagtens uddelegeres – men ansvaret kan ikke!

Vejen frem – tjeklisten for et godt compliance projekt.

Der er nogle grundlæggende elementer, som altid er på plads hos de virksomheder, der får det fulde udbytte af deres sikkerhedspolitik. Det kan være en god idé at overveje, om organisationen er klar til at gennemføre projektet til fulde, inden det påbegyndes. Det kan have den modsatte effekt, hvis medarbejderne oplever, at ledelsen ikke bakker fuldt op om den politik, der bliver kommunikeret.

- Tag udgangspunkt i en kendt standard. Det giver en god ramme for politikken.
- Brug al den viden der i forvejen er opsamlet i de forskellige afdelingers retningslinjer.
- Sørg for at hele virksomhedsledelsen er involverede i projektet.
- Topleledelsen bør følge arbejdet, og bede om en status med passende intervaller.
- Sørg for at tage stilling til ALLE områder af standarden, også selv om de vælges fra.
- Lav en plan for hvordan politikken skal kommunikeres til medarbejderne.
- Vurder om en udefrakommende konsulent vil kunne bidrage til projektledelsen.
- Vurder om der skal bruges software til at understøtte arbejdet, så man ikke selv opfinder systemer til det hele – igen.

Sikkerhed er som bekendt ikke en statisk destination, men en vedvarende rejse. Og en rejse der er planlagt godt er som oftest den mest behagelige. Der er meget at blive klog på undervejs...