

## 4 måder at få ledelsen til at tage ansvar for informationssikkerhed

af Frederik Helweg-Larsen, CISM

***Sikkerhedschefer i hele Danmark lider under topledelsens manglende interesse for informationssikkerhed og sidder ofte tilbage med en omfattende opgave uden egentlig indflydelse eller budget for implementering af sikkerhedspolitikken. Ansvar kan som bekendt ikke uddelegeres – kun opgaverne.***

Som sikkerhedsrådgiver er jeg dagligt i dialog med sikkerhedschefer over hele landet i såvel det private erhvervsliv som inden for stat og kommuner. Der er rigtig mange dygtige og kompetente sikkerhedsfolk i Danmark, men mange arbejder under en urimelig agenda.

Det forventes at de tager ansvaret for sikkerheden i organisationen og implementeringen af sikkerhedspolitik og beredskabsplan, men ofte uden et budget for omkostningerne og uden reel indflydelse i organisationen. På trods af at informationssikkerhed ikke er begrænset til IT men i høj grad handler om personale, adfærd og processer, så er der stadig mange sikkerhedsansvarlige der er placeret i IT afdelingen. Der er ikke noget at sige til, at det kan være svært at få indflydelse på hele forretningen når man er placeret i IT afdelingen og ikke har mandat til at ændre adfærden i andre afdelinger.

### Hvem er den sikkerhedsansvarlige?

Skal vi ikke lige slå fast hvem den sikkerhedsansvarlige egentlig er?

Direktionen har ansvaret. Det vil sige direktøren, kommunaldirektøren, departementschefen eller en tilsvarende topleder.

Der er kun én der har ansvaret, og på samme måde som man ikke kan afskrive sig ansvaret for virksomhedens økonomi ved at ansætte en økonomichef, så kan man sandelig heller ikke med sikkerhed. Et godt råd til de af jer der har titlen ”sikkerhedsansvarlig” er, at få rettet titlen til sikkerhedskoordinator, sikkerhedschef eller noget tilsvarende. Opgaven består nemlig ikke i at påtage sig ansvar, men at hjælpe ledelsen til at forstå deres ansvar og sikre, at de beslutninger der bliver truffet er velovervejede, og bliver fornuftigt implementeret.

Det er ikke let at få sikkerhed på agendaen hos topledelsen, men det er dog lykket os at gøre det en hel del gange med succes. De følgende fire punkter er baseret på egne erfaringer.

### PUNKT 1: Tal om relevante konsekvenser der er til at forstå

Sikkerhed bliver hurtigt diffust og kedeligt hvis du ikke kan relatere det til din hverdag. Det gælder også den travle direktør der er mere optaget af krise og bundlinje end websikkerhed og download af musik.

Det er vigtigt at ledelsen forstår at beskyttelse af virksomhedens image og aktiver er lige så afgørende for virksomhedens overlevelse som styring af økonomien.

Tegn derfor et billede af et muligt hændelsesforløb der er realistisk og relevant.

*For eksempel: "Hvis en af vores medarbejdere downloader musik og film ulovligt fra internettet, opbevarer det på vores servere og videredistribuerer det til vennerne, hvad er så de konkrete konsekvenser? Er virksomheden økonomisk ansvarlig for medarbejderens handlinger? Hvad gør vi hvis medierne skriver at vi opbevarer og distribuerer piratkopierede medier? Så er det helt sikkert direktøren de vil tale med. Vil det påvirke vores image hvis vi ikke har en klar politik der er kommunikeret til medarbejderen og en plan for de konsekvenser et brud på reglerne har?"*

Det her handler om at tage stilling inden problemerne opstår, og så lade IT, HR og Sikkerhed om i fællesskab at gennemføre ledelsens beslutninger.

Det er kun topledelsen der kan afgøre om medarbejderen i eksemplet skal politianmeldes eller afskediges, og klare regler er noget alle har glæde af.

### **PUNKT 2: Sørg for en klar fordeling af opgaver og ansvar**

Man kan bruge meget energi på at udarbejde en fin og dækkende sikkerhedspolitik, men hvis ordene ikke bliver omsat til handling, så mister den meget hurtigt sin værdi og bliver et eksempel på ledelsens manglende evne til at eksekvere beslutninger.

Sørg derfor altid for at det er helt klart hvem der har truffet de enkelte beslutninger og hvem der skal sikre at de bliver ført ud i livet. Hvis politikken ikke bliver omsat til konkrete opgaver knyttet til konkrete personer så skal I ikke forvente at den kommer til at leve.

### **PUNKT 3: Mål jeres indsats og resultater så ledelsen kan følge med**

Det er sikkert ikke alle dele af jeres sikkerhed der er lige vigtig for virksomheden. Det er nødvendigt at prioritere og udvælge de områder der udgør den største trussel, har den største konsekvens og samtidig er inden for vores indflydelse. Pluk de lavest hængende frugter først og gå dernæst videre til de højest prioriterede.

For alle indsatsområder skal det være tydeligt hvad der skal til for at efterleve politikken, og det skal være objektivt målbart. Det betyder at hvis der er en politik for brugeradministration, så skal det være klart, præcis hvilke processer og kontroller, der skal gennemføres for at vi er i mål.

Det giver ingen mening at træffe beslutninger uden at implementere dem og følge op på resultaterne.

#### **PUNKT 4: Sørg for en klar kommunikation til alle i organisationen**

I kan ikke regne med at medarbejderne følger reglerne hvis de ikke kender dem. Derfor skal sikkerhedspolitikken kommunikeres ud på modtagerens præmisser. Det er ikke godt nok at smide hele politikken på 55 sider efter dem. I sin helhed er politikken et opslagsværk.

Brug i stedet energien på at kommunikere de holdninger der ligger bag politikken, og lad det være klart at det er ledelsen der står bag. Lad medarbejderne følge med i arbejdet og del historier med dem om hvordan det *næsten* gik galt forleden dag. Det er vigtigt at alle forstår årsagen til at vi har en sikkerhedspolitik, nemlig at vi beskytter virksomheden og dermed arbejdspladserne.

Endelig er regler uden konsekvenser ikke ret meget værd. Det kender vi fra andre situationer i hverdagen. Ledelsen bliver derfor nød til at være klar til at tage konflikten med den medarbejder der ikke følger reglerne i virksomheden for at undgå at alt sikkerhedsarbejdet bliver undergravet.

#### **Lad være med at opfinde den dybe tallerken**

Det er muligvis første gang i skal samarbejde om informationssikkerhed i denne virksomhed, selvom alle kommer med erfaringer andre steder fra. Det tager lang tid til at finde en fælles referenceramme hvis det er noget der skal være enighed om, og det kan være svært at vide hvor meget man skal tage med og hvor detaljeret det skal være.

Brug de erfaringer der er tilgængelige og brug i stedet energien på implementeringen. Der findes konsulenter der har erfaringer fra hundredvis af virksomheder som jeres, og kan spare jer for alt det der ikke giver værdi eller er svært at gennemføre. Der er også et godt udvalg af erfa-grupper hvor man kan udveksle erfaringer med andre der har været processen igennem.

Det er billigere at lære af andres fejl end at forsøge sig på egen hånd. Det er vigtigt at arbejdet med informationssikkerheden bliver oplevet som noget der giver værdi, og det gør det kun hvis I kan vise fremdrift og succes med små konkrete tiltag.

God kamp...!

#### **Kontaktinformationer**

---

Frederik Helweg-Larsen

[fhl@policyenforcer.dk](mailto:fhl@policyenforcer.dk)

Telefon 70 20 88 18