Eksempler

**Ledelsens udmelding om de overordnede mål og principper**

*Eksempel 1*

En accepteret størrelse kan for eksempel være en tidskrævende genetablering af data i form af indkøring af backup og tab af få og på anden måde tilgængelige data. Det er normalt aldrig acceptabelt, hvis vandværket mister store datamængder uden mulighed for umiddelbart at kunne reetablere dem.

Det er også uacceptabelt, hvis forbrugere, medarbejdere eller samarbejdspartneres fortrolige data kan kompromitteres.

**Vigtige grundprincipper for sikkerhedsarbejdet**

## Funktionsadskillelse

*Eksempel 1*

Programmer og dokumenter er i denne sammenhæng vandværkers ressourcer. Kun driftspersonale og enkelte nøglepersoner skal normalt have adgang til vandværkets SRO-system og programmer til ledningsregistrering. Det er også kun regnskabsføreren og/eller kassereren, der skal have adgang til forbrugerafregning, indkomne mails fra forbrugerne samt løn og ansættelsesforhold.

*Eksempel 2*

Adgang til mapper og programmer tildeles eller begrænses til hver enkelt medarbejder eller bestyrelsesmedlem. Det er en forudsætning, at hver enkelt bruger har sit eget login. En it-konsulent kan eventuelt hjælpe med denne opsætning, men planen for systemadgang skal fastlægges af driftslederen eller bestyrelsen.

*Styring af sikkerhedshændelser*

Eksempel 3

Vurdering sker ved at følge meddelelser og opdateringer fra systemleverandøren f.eks. Microsoft, Rambøll eller lignende. Sikkerheden kan trues, hvis en hacker har fundet et ”hul” i adgangen til leverandørens system, så han/hun kan tilgå data og foretage ændringer, steder hvor f.eks. regnskabsføreren kun har adgang via sin adgangskode.

Eksempel 4

Risikobilledet udtrykker den generelle bekymring for, om en uautoriseret adgang til vandværkets it-system kan finde sted. En ændring i vandværkets skema til risikovurdering kan være konsekvensen af et midlertidigt eller permanent ændret risikobillede.

*Dokumentation*

Eksempel 5

En væsentlig sikkerhedsaktivitet er at skifte adgangskoder jævnligt. Opdatering og opgradering af it-programmer som eksempelvis Windows eller Rambøll Fas er også en væsentlig sikkerhedsaktivitet. I beskrivelsen af proceduren nævnes de enkelte aktiviteter, tidsplan for udførelsen, og hvem, der er ansvarlig for opgaven. Tidsplan for revidering af proceduren beskrives også.

Sikkerhed i forbindelse med outsourcing.

Eksempel 6

Brug Danske Vandværkers skabelon til en databehandleraftale.

**Hovedpunkterne i regelsættet/retningslinjerne er:**

*Punkt 4: Styring af aktiver*

Eksempel 7

For at undgå at data falder i de forkerte hænder, kan det være nødvendigt at ødelægge it-udstyr eller dele af dette. Eksempelvis harddisken inden den bortskaffes. USB-nøgler og CD’er skal også ødelægges inden de bortskaffes. Hvis I blot sletter indholdet på en harddisk eller en USB-nøgle, kan det reetableres.

Punkt 5: Adgangsstyring

Eksempel 8

System- og dataejer er programleverandøren (f.eks. Rambøll) og vandværket.

Punkt 8: Driftssikkerhed

Eksempel 9

En sikkerhedsforanstaltning kan eksempelvis være installation af et whitelist-program, der sikrer, at pirat-programmer ikke kan gøre skade. Kombineres dette med et antivirusprogram, eksempelvis fra Microsoft, kan farlige programmer også slettes. Hvis programmerne indstilles til automatisk opdatering, vil ovenstående foregå uden, at it-brugeren bemærker det i dagligdagen.

Eksempel 10

En teknisk sårbarhed kan eksempelvis være anvendelse af trådløst netværk på vandværket, fjernkommunikation med en privat medarbejder pc, eller fjernstyring af drift og administration i forbindelse med support. De sårbare punkter og forholdsreglerne, der træffes, skal beskrives og med jævne mellemrum revideres.

Punkt 11: Leverandørforhold

Eksempel 11

Ved fjernbetjening anvender medarbejderen hos leverandøren en pc, der kan udgøre en sikkerhedsrisiko, hvis den ikke som minimum overholder vandværkets egne regler for it-sikkerhedspolitik.

Punkt 12: Styring af brud på informationssikkerhed

Eksempel 12

Kommunikation om sikkerhedstruende hændelser og svagheder indebærer eksempelvis, at medarbejdere giver besked til ledelsen, hvis de modtager potentielt farlige e-mails, også selvom det ikke har medført et sikkerhedsbrud. Der skal også kommunikeres til ledelsen, hvis uvedkommende har uhindret adgang til software på vandværket.

Punkt 13: Beredskabsstyring m.m.

Eksempel 13

Hvordan kan eksempelvis forbrugerdata, som blandt andet indeholder oplysninger om måleraflæsning til brug for årsafregning, genskabes eller tilvejebringes inden udsendelse af årsopgørelsen.