Risikovurdering for vandværker

#	Trussel	Sandsynlighed	Konsekvens	Samlet risikobillede	Forslag til yderligere sikkerhedstiltag for at imødegå de konstaterede trusler
1	Uautoriseret adgang til it-systemer	HØJ	HØJ	KRITISK	Undgå at bruge faste passwords. Indfør personlige passwords samt krav til sværhedsgrad og ændring af passwords
2	Vandværket rammes af et ransomware eller virusangreb	HØJ	HØJ	KRITISK	Implementer software, der blokerer trusler proaktivt (før der sker angreb).
3	Samme login og password bruges af flere	MIDDEL	MIDDEL	MIDDEL	Hvis det ikke kan undgås, må logning gøres mere effektiv
4	Datamedier, diske eller dokumenter med fortrolige data bliver stjålet/tabt/glemt, f.eks. under transport	HØJ	HØJ	KRITISK	Indfør værktøjer til at slette data på computeren, hvis den mistes. Efterlad aldrig fortroligt materiale i bil, når den forlades
5	Brugere skifter ikke adgangskode løbende	HØJ	MIDDEL	MIDDEL	Indfør passwordpolitik, med jævnlig ændring af passwords. Kontroller at den følges
6	Der er fejl på backup, så data ikke kan genskabes ved datatab eller nedbrud	LAV	HØJ	KRITISK	Test jævnligt om backup virker ved at udføre tests af genoprettelse
7	En medarbejder modtager og aktiverer virus eller trojansk hest via e-mail, browser eller usb-nøgle	MIDDEL	HØJ	KRITISK	Indfør sikkerhedsværktøjer, virusscanning af e-mail osv.
8	En ansat lokkes til at udlevere fortrolig/kritisk information til uvedkommende (social engineering)	LAV	MIDDEL	ACCEPTABEL	Informer medarbejdere, om hvad man skal passe på. Lad fortrolighedserklæringer indgå i ansættelsesaftaler/-kontrakter