## 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 | At en ansat får uretmæssig adgang til fortrolige data | **LAV** | **MIDDEL** | **ACCEPTABEL** | Lav løbende kontrol af, at brugerrettigheder er korrekte. Opsæt logning på adgang til filer med persondata, gennemse log. |
| 3 | Fyrede/fratrådte medarbejdere får ikke frataget adgangsrettigheder | **MIDDEL** | **MIDDEL** | **MIDDEL** | Implementer procedurer for nedlukning af tidligere medarbejderes it-adgange |
| 4 | Vandværket rammes af et ransomware eller virusangreb | **HØJ** | **HØJ** | **KRITISK** | Implementer software, der blokerer trusler proaktivt (før der sker angreb)  |
| 5 | Samme login og password bruges af flere | **MIDDEL** | **MIDDEL** | **MIDDEL** | Hvis det ikke kan undgås, må logning gøres mere effektiv |
| 6 | 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 |
| 7 | Misbrug af anden brugers adgang da der ikke logges ud efter brug af systemet | **MIDDEL** | **MIDDEL** | **MIDDEL** | Indfør automatisk logoff, når computeren har været inaktiv i 5 minutter (pauseskærm) |
| 8 | Brugere skifter ikke adgangskode løbende | **HØJ** | **MIDDEL** | **MIDDEL** | Indfør passwordpolitik, med jævnlig ændring af passwords. Kontroller at den følges |
| 9 | 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 |
| 10 | 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. |
| 11 | Brug af privat computer eller brug af firmacomputer til private formål åbner for misbrug eller hacker/virusangreb | **HØJ** | **HØJ** | **KRITISK** | Undlad at gøre brug af privat computer. Brug computer kun til firmaformål |
| 12 | En ansat lokkes til at udleverefortrolig/kritisk information tiluvedkommende (social engineering) | **LAV** | **MIDDEL** | **ACCEPTABEL** | Informer medarbejdere, om hvad man skal passe på. Lad fortrolighedserklæringer indgå i ansættelsesaftaler/-kontrakter |
|  |  |  |  |  |  |