# Bilag 2: Eksempel på trusselskatalog – bør justeres til organisations kontekst før brug

**Trusselskatalog**

Ejer af procedure/metode: [kontor/enhed]

Dato for ikrafttrældelse: [dato]

Godkendt af: [Informationssikkerhedsudvalg]

Næste planlagte revision: [dato]

J.nr.. 2019 - 4421

| **Trussel** |
| --- |
| Trusler mod de fysiske omstændigheder |
| Brandskade, brand i tilstødende omgivelser, brand forårsaget af forsømmelse |
| Vandskade, skybrud der fører til oversvømmelse, sprinklersystemfejl, rørskade |
| Elektromagnetisk beskadigelse, lynnedslag, solstorm, statisk elektricitet |
| Skade ved naturhændelse, kraftig storm, jordskælv, frost, tørke, |
| Skade ved katastrofal ulykke. Fly-, tog- eller køretøjsulykke, eksplosion |
| Forurening af faciliteter, radioaktivt udslip fra atomulykke, biologisk eller kemisk udslip, gasudslip, luftbårne partikler, vulkansk nedfald |
| Fejl i fysisk miljøstyring |
| Kølingsfejl, luftfiltreringsfejl, opvarmningsfejl |
| Vandforsyningssvigt |
| El-forsyningsfejl |
| Strømsvigt, el-forsyningslinjebrud |
| Strømfluktuation, sag, surge, spike, brownout |
| Forsyningsudstyrssvigt, UPS-fejl, generatorfejl |
| Elforsyningsoverbelastning |
| Brugerfejl |
| Uforsætlige brugerhandlinger, fejlbehandling af medier, mangel på brugeruddannelse |
| Drifts- eller vedligeholdelsesfejl |
| Fejl i forbindelse med drifts-, support- eller vedligeholdelsesprocesser. |
| Angreb med skadelig kode |
| Virus, malware, ransomware, rootkits, ondsindende links og trojanske heste |
| Cyberangreb |
| Destruktiv hacking, hacktivisme |
| DDoS- eller SPAM-angreb |
| Statsfinansierede angreb (State-sponsored attacks = APT) |
| Forfalskning af informationer, ødelæggelse af websites |
| Hacking, industrispionage, aflytning, opsnapning af information |
| Kapacitetsfejl |
| Kapacitetsmangel for systemer eller storage |
| Softwarefejl |
| Softwarenedbrud, bugs, databasekorruption |
| Uautoriseret eller ikke-testet kode |
| Hardwarefejl |
| Kommunikationslinjenedbrud |
| Udstyrsnedbrud eller -defekt, slid, korrosion, henfald af lagringsmedier |
| Misbrug |
| Forfalskning, svindel, underslæb |
| Uautoriseret brug, misbrug af rettigheder |
| Brud på ophavsrettigheder |
| Tilsigtet informationslæk eller -tyveri |
| Hacking, industrispionage, aflytning, opsnapning af information |
| Tyveri af datamedier eller fysiske dokumenter |
| Politisk eller økonomisk motiveret informationslæk |
| Utilsigtet informationslæk |
| For vidtgående brugerrettigheder/adgangsprivilegier |
| Forkert konfigureret adgangskontrol |
| Fejlagtig publicering af data, der indeholder følsomme oplysninger |
| Tab af datamedier eller fysiske dokumenter |
| Bevidst ødelæggelse af aktiver |
| Brandstiftelse, hærværk |
| Terrorbombning |
| Sabotage begået af hævngerrige medarbejdere |
| Tyveri af fysiske aktiver |
| Indbrud, røveri |
| Tyveri, tricktyveri |
| Tyveri begået af ansatte |
| Manglende overholdelse af lovkrav og aftaler |
| Brud på ophavsrettigheder |
| Virksomheden opfylder ikke de gældende compliance-krav |
| Forkert offentliggørelse af personlige oplysninger |
| Videnstab |
| Afskedigelse, opsigelse, rekruttering fra konkurrenter |
| Manglende vidensoverførsel |
| Personafhængighed |
| Tab af personale (ressourcetab) |
| Vold, bortførelse, mord |
| Dødsulykke eller alvorlige skader |
| Sygdom, epidemi, pandemi |
| Arbejdsafbrydelse |
| Lokale arbejdskonflikter, strejke, lockout |
| Leverancesvigt |
| Konkurs, nedlæggelse |
| Serviceleverandørfejl, hostingleverandørfejl |
| Afvigelse fra aftalt serviceniveau/leverede ydelser |
| Ændringer af servicen, en ny strategi fra leverandøren |
| Fejl hos underleverandører, dårlig håndtering af underleverandører |
| Sikkerhedsbrud fra leverandørens side |
|  |
| Utilstrækkelig sikkerhed fra leverandørens side |
| Leverandørafhængighed |
| Ikke-standardløsninger, afhængighed af leverandørs infrastruktur, dårlige muligheder for dataeksport |
| Lange kontraktsperioder, høj pris for at afbryde samarbejdet |
| Leverandør mangler compliance- eller  governance-procedurer |
| Leverandøren opfylder ikke egen sikkerhedspolitik og -regler |
| Leverandøren opfylder ikke compliance-krav jf. kontrakten |
| Nye og ubehandlede sikkerhedstrusler |
| Nye angrebsformer |
| Nye former for misbrug af it-systemer |