**Hjelpeskjema for vurdering av trusler innenfor informasjonssikkerhet**

### God oversikt over relevante trusler er nødvendig for å gjøre en god risikovurdering

For å beskrive relevante og aktuelle risikoer er det nødvendig å ha oversikt over hvilket trusselbilde virksomheten står overfor. Derfor er det nyttig å skaffe seg oversikt over hva som kan representere relevante trusler *før* man setter i gang og beskriver konkrete risikoer. En oversikt over relevante trusler fungerer som et nyttig hjelpemiddel for å sikre at virksomheten gjør en helhetlig og tilstrekkelig grundig vurdering.

Listen nedenfor gir en slik generell oversikt. I tillegg kan andre faktorer være relevante for virksomheten. Listen brukes på enkleste måte ved at man leser gjennom den og bruker den som bakgrunnsmateriale og hjelp når man skal beskrive konkrete risikoer.

Noen virksomheter kan ha nytte av å gjøre mer omfattende trusselvurderinger og rangere de kartlagte trusselfaktorene i forhold til hverandre ved hjelp av verktøy som er spesielt beregnet på dette. Dette hjelpeskjemaet er avgrenset til å gi en generell oversikt over trusler og en kort oversikt over hva man bør vurdere for å finne ut hvor alvorlig den aktuelle trusselen er.

### Generelt om trusler innenfor informasjonssikkerhet

Truslene kan deles i to hovedkategorier; de som innebærer fare for uønskede hendelser og de som innebærer risiko for uønskede villede hendelser. Den førstnevnte kategorien er hendelser som kan oppstå helt uavhengig av om noen har satt i gang hendelsen med vilje (eks en brann eller en menneskelig feil). Den sistnevnte kategorien er de tilfellene hvor det ligger vilje/ønske om å skade til grunn for hendelsen (eksempel cyberangrep).

Eksemplene i listen gir en generell oversikt. I den enkelte virksomhet kan det være andre typer trusler som kan være relevante i tillegg. Eksemplene nedenfor er satt opp alfabetisk. Listen ikke er ment som noen «fasit». Vær imidlertid obs på at trusselen «menneskelige feil» normalt kommer høyt opp på listen over trusler som er relevante og aktuelle for enhver virksomhet.

### Trusselvurdering

Her nevnes bare helt kort momenter man kan tenke på når man skal vurdere hvor alvorlig og relevant trusselen kan være for virksomheten. Det er ikke meningen at man skal være nødt til å gjøre en fullstendig trusselvurdering med definisjon av trusselnivå for de enkelte truslene. For enkelte virksomheter kan dette være nyttig, men dette dokumentet gir ikke en mal for en slik fullstendig vurdering.

Følgende momenter kan ha betydning når man skal vurdere hvor relevant og alvorlig en trussel er i seg selv:

* Har det skjedd før?
* Må vi gå ut fra med at denne trusselen eksisterer / er til stede rundt oss?
* Har denne typen trussel kapasitet eller potensial til å ramme oss?
* Er denne typen trussel særlig aktuell for oss; må vi anta at noen kan ønske å ramme oss, eller er det omstendigheter som gjør oss spesielt utsatt for trusselen?

### Eksempler

|  |  |
| --- | --- |
| **Eksempler på hva eller hvem som kan representere en trussel mot informasjonssikkerhet** | **Nærmere beskrivelse** |
| Aktivister og andre som jobber mot politiske mål eller andre konkrete formål | Her er det grupperinger som jobber mot bestemte – ofte politiske – mål som kan representere trusler mot informasjonssikkerheten. Det kan bety at det er personer eller grupperinger som gjennomfører en form for aksjon som innebærer trusler for informasjonssikkerheten, for eksempel ved å tilegne seg – for deretter evt å publisere - informasjon de ikke har rett til.  Metoder kan være mange av de samme som for vinningskriminelle. |
| Brann | Brann er en generell trussel for en virksomhet og relevant i flere sammenhenger, blant annet i generelt beredskapsarbeid. Brannvern er også et selvstendig sikringsområde. I informasjonssikkerhetsmessig sammenhengen er brann relevant som en trussel mot tilgjengelighet til informasjon, og som i verste fall kan føre til at informasjon går tapt for alltid. |
| Egne ansatte | Med *egne ansatte* menes ansatte i Oslo kommune som av en eller annen grunn velger å misbruke sin tilgang til informasjon. Dette kan være heltids- eller deltids ansatte, fast ansatte eller ansatte i vikariater. |
| Ekstremvær, kvikkleire, solstorm, pandemi | Alle disse er eksempler på mer sjeldne, men alvorlige trusler som i svært varierende grad kan være relevante for en virksomhet. Alle disse truslene er trusler som har en glidende overgang til ren beredskapshåndtering der ikke bare informasjon er en verdi som er truet, men liv og helse i vid forstand. |
| Menneskelige feil | Med menneskelig feil menes at uønskede hendelser forårsakes av individer uten intensjon om å skade virksomhetens verdier. Dette kan for eksempel skyldes feilvurderinger, inkompetanse eller regelrette uhell. |
| Strømbrudd | Strømbrudd kan lamme tilgangen til elektronisk informasjon. Langvarige strømbrudd lammer etter hvert også muligheten til å bruke virksomhetens lokaler, og dermed tilgangen til papirdokumentasjon. |
| Systemfeil | Med *systemfeil* menes svikt i programvare eller maskinvare knyttet til Oslo kommunes IKT-systemer. |
| Terrorister | Med *terrorister* menes individer eller grupperinger som står bak ulovlig bruk av, eller trussel om bruk av, makt eller vold for å oppnå politiske, religiøse eller ideologiske mål. Denne gruppen skiller seg fra andre grupper ved at de skadelige konsekvensene av handlingene er store / omfattende. |
| Vann | Her tenker man på vannskader som oppstår relativt plutselig som følge av feil ved infrastruktur som bærer vann, for eksempel rørsystemer for vann og kloakk. |
| Vinningskriminelle / kriminelle | Her er det først og fremst økonomisk gevinst som er motivet. I denne kategorien regnes tradisjonell vinningskriminalitet, men utstrakt bruk av elektroniske hjelpemidler og Internett innebærer en stadig økt risiko for at vinningskriminelle kan få tilgang til informasjon, infrastruktur og systemer i vinnings formål eller i ren skadehensikt.  Eksempler   * Tyveri av utstyr som mobiler, pc’er, nettbrett osv * Bruk av ransomware som «kidnapper» informasjonen på en enhet, gjerne med krav om «løsesum». * Tapping av informasjon som har salgsverdi eller kan utnyttes på andre måter. |