3.5 Eksempel på scenarioer

Følgende liste er eksempelscenarioer som kan være til inspirasjon for arbeidet med risikovurderinger. Den er ikke uttømmende, og alle som skal gjennomføre en risikovurdering anbefales å idemyldre blant deltagerne og tilpasse scenarioene til egen virksomhet.

Se kapittel 2.3.6 Risiko for et eksempel på hvordan et scenario kan formuleres og beskrives når man skal vurdere sannsynlighet og konsekvens.

KIT	Eksempel på scenario
K	Snoking, f.eks. helsepersonell som ser i journaler uten tjenstlig behov
K	Uautorisert tilgang til systemer med helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
K	Uautorisert tilgang til systemer med helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
K	Fysisk innbrudd/tyveri av opplysninger (utstyr)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse/utnytte privatpersoner)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse myndighetspersoner for politiske formål)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
I	Helse- og personopplysninger knyttes til feil person i journal (feilføring)
I	Helse- og personopplysninger er ikke oppdaterte/feil i systemene
T	Tilsiktet og ikke-planlagte nedetider/utilgjengelighet på systemer (som følge av tjenestenektangrep, sabotasje, etc)
T	Utilsiktet nedetid på systemene (som følge av system- eller infrastrukturfeil, etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (utilsiktet, som følge av feil etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (tilsiktet, som følge av løsepengevirus eller andre typer angrep)
T	Brudd i kommunikasjon/funksjonalitet for sikker og rettidig deling av nødvendige helseopplysninger mellom samhandlende helsepersonell
T	Strømbrudd (fører til nedetid eller ødeleggelse)
T	Vannlekkasje (fører til nedetid eller ødeleggelse)
T	Naturkatastrofer og ekstremvær (fører til nedetid eller ødeleggelse)
KIT	Innsider benytter egne tilganger til andre formål (utro tjener)
KIT	Innsider benytter egne tilganger til andre formål som følge av press fra eksterne aktører (kriminelle, fremmede makter)
KIT	Innsider benytter egne tilganger til andre formål som følge av social engineering fra eksterne aktører (blir lurt, gjennom phishing eller andre teknikker)
KIT	Personell hos databehandler benytter tekniske tilganger til andre formål enn det som er regulert av databehandleravtalen
KIT	Menneskelig feil (utilsiktet)
	…