Risikovurdering av tjenester

Både vertsorganisasjoner og tjenesteleverandører er pålagt å gjennomføre risikovurderinger av informasjonssikkerheten til data og personopplysninger, for eksempel informasjon om ansatte og studenter eller elever, ved bruk av (i) Dataporten og (ii) tjenester som tilbys via Dataporten.

Nedenfor gis først en kort oversikt over hvilke krav som stilles til risikovurderinger i personopplysningsloven med forskrift. Deretter gis noen eksempler på uønskede hendelser som risikovurderinger av tjenester i Dataporten kan avdekke.

Hva, når og hvor ofte?

Risikovurderingene skal omfatte all behandling av data og personopplysninger som skjer i forbindelse med (i) bruk av Dataporten og (ii) tilgjengeliggjøring og bruk av andre eksterne tjenester i Dataporten. Slike vurderinger skal gjennomføres

- før vertsorganisasjoner tar i bruk Dataporten og øvrige eksterne tjenester som tilbys via Dataporten,
- før tjenesteleverandører tilbyr sine tjenester til vertsorganisasjoner via Dataporten,
- ved vesentlige endringer i tjenestene eller bruken av dem (gjelder både vertsorganisasjoner og tjenesteleverandører).

Uønskede hendelser og risiko

Målet med risikovurderingene er at data og personopplysninger som behandles i tjenestene skal være tilfredsstillende sikret mot tre typer uønskede hendelser:

1. brudd på konfidensialiteten, det vil at data eller personopplysninger kommer uvedkommende i hende,
2. brudd på integriteten, det vil si at data eller personopplysninger urettmessig endres, slettes, redigeres eller manipuleres på andre måter,

3. brudd på tilgjengeligheten, det vil si at data eller personopplysninger ikke er tilgjengelige for personer som har rettmessig behov for tilgang til dem.

Om data og personopplysningene er tilfredsstillende sikret mot disse tre typene uønskede hendelser eller ikke, avgjøres på følgende måte

- først identifiseres mulige uønskede hendelser som kan oppstå i forbindelse med en aktuell tjeneste,
- dernest foretas en vurdering av risikoen (sannsynlighet/konsekvens) knyttet til hver enkelt uønsket hendelse.

Resultater og tiltak

Dersom resultatet av vurderingen er at risikoen for uønskede hendelser - brudd på opplysningenes konfidensialitet, integritet eller tilgjengelighet – er uakseptabel høy, skal det iverksettes tiltak for å øke sikkerheten til et tilfredsstillende nivå. Kravet om iverksetting av tiltak (dersom det er nødvendig) gjelder både for vertsorganisasjoner og tjenesteleverandører.

Viser det seg at det ikke er mulig å iverksette visse typer nødvendige tiltak, for eksempel fordi tjenesteleverandøren motsetter seg dette, eller at informasjonssikkerheten er utilfredsstillende også etter at tiltak er iverksatt, skal man unngå å benytte/tilby den aktuelle tjenesten.

Eksempler på uønskede hendelser

Nedenfor følger noen eksempler på uønskede hendelser som kan oppstå i forbindelse med bruk av (i) Dataporten og (ii) tjenester som benytter Dataporten.

Vertsorganisasjoner og tjenesteleverandører kan benytte eksemplene som utgangspunkt for sine egne risikovurderinger.

Dataporten

- Brudd på tilgjengeligheten til personopplysninger fordi Dataporten utsettes for tjenestenektangrep (DDOS).

- Brudd på konfidensialiteten til personopplysninger fordi sluttbrukere som har reservert seg mot personsøk likevel er søkbare i Dataporten.
- Brudd på konfidensialiteten til personopplysninger fordi API-er som vertsorganisasjonen gjør tilgjengelig via Dataporten gir tilgang til flere opplysninger enn planlagt/nødvendig.
- Brudd på integriteten til personopplysninger på grunn av at innbrudd i Dataporten («hacking») fører til uautorisert endring eller sletting av sluttbrukeropplysninger.
- Brudd på konfidensialiteten og tilgjengeligheten til personopplysninger fordi innbrudd i Dataporten («hacking») fører til at uvedkommende får tilgang til og setter autorisasjonsserveren ut av spill.

Tjenester som benytter Dataporten

- Brudd på integriteten fordi tjenesten utsettes for skadelig programvare som fører til uautorisert endring eller sletting av vertsorganisasjonens data eller personopplysninger.
- Brudd på tilgjengeligheten til data eller personopplysninger fordi tjenesten utsettes for tjenestenektangrep (DDOS).
- Brudd på konfidensialiteten på grunn av at leverandøren utleverer data eller personopplysninger til tredjeparter, for eksempel markedsføringsfirma, uten først å ha innhentet godkjenning til dette av vertsorganisasjonen.
- Brudd på konfidensialiteten fordi konfigurasjonsfeil hos tjenesteleverandøren fører til at vertsorganisasjonens data eller personopplysninger eksponeres mot andre kunder hos samme leverandør som deler på å bruke de samme dataressursene (mangelfull segmentering av data/personopplysninger).
- Brudd konfidensialiteten fordi utro tjener hos leverandøren selger eller utleverer vertsorganisasjonens data eller personopplysninger til konkurrerende virksomheter.

- Brudd på tilgjengeligheten fordi vesentlige endringer i forutsetningene for bruk av tjenesten, for eksempel av tjenesteleverandøren går konkurs, fører til at vertsorganisasjonens ikke lenger har tilgang til egne data eller personopplysninger.