Programvareutvikling med innebygd personvern

Krav

Etabler oversikt over type personopplysninger, behandlingsgrunnlag, formål og ansvarlighet, samt hvem som er behandlingsansvarlig, databehandler og underleverandører. Ivareta personvernprinsipper og de registrertes rettigheter. Sørg for å:

- ✓ avklare bruk av samtykke eller lovhjemmel for behandlingen
- ✓ avklare hvilke personopplysninger som er nødvendig for formålet, hvor detaljerte opplysningene må være, om historikk er nødvendig, lagringssted og lagringstid, hvem skal ha tilgang og fra hvor, samt krav til informasjonssikkerhet (bruk for eksempel OWASP ASVS)
- ✓ vise åpenhet om behandlingen - gi god informasjon om bruk av personopplysninger og hvordan de registrerte kan utøve sine rettigheter
- ✓ definere toleransenivå
- ✓ gjennomføre risikovurderinger og vurdering av personvernkonsekvenser

Design

Definer krav til design, analyser angrepsflaten og gjør trusselmodellering. Sørg for:

- ✓ at den registrertes rettigheter gjenspeiles i programvarens design som er knyttet til personopplysninger og funksjoner, ved å for eksempel begrense og minimere mengden opplysninger, anonymisere eller pseudonymisere, aggregere og sette personvern som standardinnstilling
- ✓ å analysere hvordan programvaren kan misbrukes ved ulike scenarier og hvordan designet kan forbedres for å unngå identifiserte trusler

Koding

Sørg for sikker koding ved å:

- ✓ beskrive tillatte verktøy, prosesser og rammeverk for programvareutvikling samt å risikovurdere og godkjenne disse internt i virksomheten
- ✓ analysere funksjoner, API, tredjepartsbibliotek og moduler - forby de av disse som er utrygge og oppdater de som er utdaterte eller inneholder kjente sårbarheter
- ✓ regelmessig gjøre statisk kodeanalyse og kodegjennomgang – gjør en automatisk gjennomgang, supplert av manuell for å fange opp svakheter som kan gi feil bruk eller lekkasje av personopplysninger
- ✓ kontrollere dataflyt, lagring og mellomlagring av personopplysninger
- ✓ deaktivere unødig sporing, logging og innsamling av personopplysninger

Test

Sikkerhetstesting er en del av testingen. Sørg for å:

- ✓ teste om personvernkrav og sikkerhetskrav er implementert og riktig implementert
- ✓ gjennomføre dynamisk testing, fuzz testing og penetrasjonstesting/sårbarhetsanalyse - undersøk om det er kjente sikkerhetsfeil som Cross-site scripting og SQL injection, og test alle input-felt og grensesnitt (bruk for eksempel OWASP Testing Project)
- ✓ verifisere at angrepsvektorer avdekket i designfasen er håndtert, og at nye angrepsvektorer introdusert under koding er identifisert og håndtert
- ✓ gjennomgå analysene for trusselmodellering, angrepsflaten, personvernkonsekvenser og sikkerhetsrisiko på nytt for å se at sårbarhetsregulerende tiltak er implementert
- ✓ bruke fiktive/syntetiske testdata

Produksjonssetting

Programvaren gjøres klar for produksjonssetting ved å:

- ✓ utarbeide plan for hendelseshåndtering som omfatter håndtering av oppgaver, hendelser, myndighet og roller etter produksjonssetting
- ✓ gjøre en full sikkerhetsgjennomgang av programvaren, der personvernombud og sikkerhetsrådgiver verifiserer at personvern- og sikkerhetskrav er implementert og fungerer etter hensikten
- ✓ sørge for at noen med myndighet godkjenner produksjonssetting
- ✓ arkivere alle vurderinger, analyser, tester, dokumentasjon og kode

Forvaltning

Sørg for å være forberedt på god forvaltning av programvaren ved å:

- ✓ håndtere hendelser og avvik etter planen
- ✓ implementere styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold, samt rutiner for logging, testing og måling av effekt på organisatoriske og tekniske tiltak

Opplæring

Sørg for god kunnskap til regelverk og metodikk tilknyttet programvarens bruksområde ved å:

- ✓ lage en differensiert opplæringsplan tilpasset ulike profesjoner i utviklingsløpet
- ✓ forankre opplæringen i ledelsen

Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 25 i EUs personvernforordning (GDPR)

Datatilsynet