6 Produksjonssetting

Sjekklisten er dynamisk, ikke uttømmende og skal oppdateres regelmessig. Dersom du har innspill til noen av punktene, vil vi gjerne høre fra deg.

Hvordan lage plan for hendelseshåndtering relatert til programvaren?

- Etabler en plan for hendelseshåndtering av programvaren som skal overleveres. Denne må omfatte konsekvensvurdering, tiltak og kontinuerlig forbedring av programvaren.
- Etabler et kontaktpunkt eller responssenter med egne kanaler for å varsle hendelser, ta høyde for interne og eksterne avviksrapporteringer. Eksempelvis vil det å oppmuntre og ha god dialog med «varslere» være avgjørende for om brukere vil fortelle eller ikke om sårbarheter, avvik og feil. At brukere rapporterer om sikkerhetshendelser kan bidra til økt robusthet i programvare dersom hendelsene håndteres.
- For å håndtere fremtidige trusler rundt programvaren, må planen omfatte:
  - Kontaktinformasjon og kanaler
    - ved personvern- og sikkerhetsbrudd
    - til teknisk support
  - Gode avtaler som sikrer krav til responstider med relevante leverandører.
- Etabler rutiner for hvordan håndtere risiko for de ulike scenarioer beskrevet under kravaktiviteten ved risikovurdering av personvern og sikkerhet. Hvor stor letthet eller sannsynlighet er det for at disse inntreffer, hva er konsekvensen, hvem skal informeres, skal systemet slås av umiddelbart, nødvendig logging og triggere for alarmering med mer.

  Eksempel:
  - Hva skjer hvis du er for proaktiv og slår av (shutdown) et system når en hendelse oppstår?
  - Kan bevis bli fjernet vedrørende triggere (treashholds) for alarmer ved forsøk på pålogging av samme bruker fra flere IP, masse brukernavn fra samme IP m.m.?
  - Hva skjer hvis noen oppdager at sensitive personopplysninger som lagres på feil plass? Hvem skal de kontakte.

- Definisjon av hva planen omfatter og hva en hendelse er.
- Definisjon av livssyklusen til et avvik, samt rutiner for å detektere, analysere, rapportere, håndtere og normalisere.
  - Detektere
    - Sikkerhetsovervåking av server, endepunkt og nettverk skal oppdage mistenkelig aktivitet, som kan utnytte sårbarheter i programvaren, som kan medføre personvern- og sikkerhetsavvik.
    - Sikkerhetsovervåking og alarmer som trigges ved avvikende mønstre bidrar til oversikt over trusler, sårbarheter og sikkerhetshendelser.
  - Verifisere
    - Verifiser om mistenkelig aktivitet er et faktisk sikkerhetsbrudd eller falsk positiv.
    - Følg virksomhetens prosedyre for granskning (forensics), omfatter hvem som leder granskning, når kobles politi eller andre eksperter inn for bistand, mm.
    - Analyser hendelsen, gjennomgå logger, få oversikt over hva har skjedd og omfang
  - Rapportere

        - Rapporter sikkerhetsbrudd slik interne retningslinjer for hendelseshåndtering tilsier. Merk at det å varsle om et avvik også kan varsle angripere, vær oppmerksom på hvordan man skal varsle.
        - Rapportere avvik som omfatter brudd på konfidensialitet, integritet og tilgjengelighet til personopplysninger innen 72 timer til Datatilsynet.
        - Informere den registrerte om avvik som omfatter brudd på konfidensialitet, integritet og tilgjengelighet til personopplysninger.
        - Skal hendelsen og erfaringer deles med bransjen? «Sharing is caring»
        - Skal andre myndigheter varsles, for eksempel politi, NSM, NorSIS, Finanstilsynet, Helsetilsynet mm.
    - Håndtere
        - Sikkerhetshendelser håndteres i henhold til virksomhetens kontinuitetsplan. Håndteres avvik ulikt om det har direkte konsekvens for kunde eller om de bare rammer internt i virksomheten. Vær oppmerksom på at en patch som ikke er planlagt kan fungere som et varsel til potensielle angripere om at en sårbarhet finnes.
        - Implementer sårbarhetsregulerende tiltak, eksempelvis patching, endre rutiner, utvide logging, regulere tilgang, stenge porter m.m.
        - Test at implementerende tiltak fungerer som tenkt, og at det ikke medfører nye sårbarheter.
    - Normalisere
        - Gjenopprette normaltilstand for forvaltning, drift og vedlikehold.
- Definisjon på konfigurering og håndtering av logger, inkludert føringer fra personvernregelverket.
- Evaluering av hendelseshåndtering og hvordan disse erfaringene kan få konsekvenser for utviklingsløpet, virksomheten og berørte.
- Identifisere personer som skal informeres, når og hvordan berørte skal kontaktes. Melding om brudd på personopplysningssikkerheten til Datatilsynet (72-timers regel) og underretning av den registrerte.
- Anbefalt rutine for oppdatering (patching) av den utviklede programvaren, som inkluderer relaterte programmer, også fra tredjeparter. Rutinen må inngå i virksomhetens helhetlige plan.
- Virksomhetens kontinuitetsplan oppdateres med ovennevnte krav. Triggere for oppdatering kan være nye tjenester, endret kritikalitet, endring i rutine for nødstenging, endring i kritikalitetsmatrise, endring i varslingslister med mer.

Full sikkerhetsgjennomgang av utviklet programvare

- Baser sikkerhetsgjennomgangen på tidligere gjennomganger gjort i utviklingsløpet.
- Bruk ulike ekspertgrupper i gjennomgangen, diskutere forskjellige scenarioer og vurdere konsekvens, eventuelt tiltak.
- Gjennomgå med direkte involverte roller/personer i aktivitetene (hva har fungert bra, og hva har ikke fungert bra – kontinuerlig forbedring).
- Full sikkerhetsgjennomgang skal inngå i de kontrollpunkter (control gates) som gjøres før produksjonssetting. Alle aktiviteter gjennomgås for å avdekke eventuelle avvik og inkluderer
    - personvernkrav
    - sikkerhetskrav
    - toleransegrenser
    - vurdering av personvernkonsekvenser (DPIA)

- risikovurdering
- angrepsflater
- output fra verktøy
- designanalyse (Er det avvik i forhold planlagte og gjeldende designkrav?)
- kodeanalyse (Er manuell og statisk analyse i.h.t. avdekkede fokusområder, er funn i henhold til toleransenivå?)
- verktøy og tredjepartskomponenter (Er det kun benyttet godkjente verktøy og tredjepartskomponenter i utviklingsløpet?)
- dynamiske tester, penetrasjonstester eller sårbarhetsanalyser (Er funn i henhold til definert toleransenivå?)
- resultater fra penetrasjonstester og sårbarhetsanalyser
- å revidere ferdig programvare opp mot opprinnelig trusselvurdering for å avdekke implementasjonsavvik og eventuelt iverksette tiltak mot implementasjonsavvik

Godkjenne produksjonssetting og arkivering

- Programvaren skal godkjennes forut for produksjonssetting for å sikre at personvern- og sikkerhetskrav er ivaretatt.
- Godkjenning skal gjøres av en leder som har ansvar/myndighet til dette.
- All relevant data i hele utviklingsløpet skal arkiveres, dette inkluderer alle spesifikasjoner, kildekode, binærkode, private symbols, vurdering av personvernkonsekvenser (DPIA), risikovurderinger, dokumentasjon, beredskapsplaner, lisenser og tjenestevilkår for tredjeparts programvare. Slik arkivering er viktig for å utføre supportoppgaver, bistår med å redusere langsiktige kostnader knyttet til forvaltning og vedlikehold, muliggjør tilbakerulling til tidligere versjon. Eksempelvis kan arkivering gjøres i Escrow.
- Basert på resultatene etter full sikkerhetsgjennomgang beslutter leder (med slik ansvar/myndighet) at programvaren kan settes i produksjon. (Personer som ikke har ansvar kan gi anbefaling om produksjonssetting).

Hvorfor stille krav til produksjonssetting?

- Det stilles krav til hendelseshåndtering og kontinuitet. En plan for hendelseshåndtering kan bidra til at alvorlige hendelser håndteres og beskyttes mot negative konsekvenser ved feil eller uhell, jf. artikkel 32, 33 og 34.
- Endelig sikkerhetsgjennomgang av programvaren skal forankres ved/i internkontroll, jf. artikkel 30 og 32.
- Produksjonssettingen skal godkjennes, og arkivering av aktivitetene gjort i utviklingsløpet, jf. artikkel 30 og 32.