Riskanalystillsyn NIS

PTS NIS-forum februari 2023

Bakgrund och syfte

- Nästa steg efter tidigare tillsyner som handlade om anmälan och incidentrapportering
- Denna tillsyn handlade om riskanalyser och utgick från PTS föreskrifter, PTSFS 2021:3
- Mer ingående tillsyn med bedömning av riskanalyser och vi valde därför endast tre aktörer till att börja med
  - Internetstiftelsen, ansvariga för toppdomänen .se
  - Loopia, webbhotell, e-post, inklusive registrar
  - GleSYS, moln, virtuella servrar, inplacering och DNS-tjänst
- Tillsynen inleddes i augusti förra året och avslutades i januari

Genomförande

- Inledande frågor
  - Beskrivning av hur man har identifierat de delar som ingår i NIS
  - Beskrivning av hur man arbetar med riskanalyser
  - Lista vilka riskanalyser har man tagit fram
- Begärde in riskanalyser och ställde kompletterande frågor
- Tog fram kontrollpunkter utifrån PTSFS 2021:3
- Gick igenom kontrollpunkterna för respektive aktör utifrån inskickat material
- Fysiska möten
  - Genomgång av arkitektur
  - Beskrivning av hur man arbetar med riskanalysprocessen
  - Detaljerade frågor från PTS utifrån riskanalyser och kontrollpunkterna

Kontrollpunkter från PTSFS 2021:3

- Identifiering av nätverk och informationssystem, 4 §
- Identifiering av samtliga relevanta hot, 4 §
  - Organisatoriska hot, personberoenden mm
  - Fysiska hot, stöld, brand, strömavbrott mm
  - Logiska hot, sårbarheter i mjukvara, DDoS, mm
- Unik beteckning och beskrivning av nät och informationssystem, 5 §
- Metoder och rutiner för riskanalys, 5 §
- Riskbedömning med sannolikhet och konsekvens, inklusive skäl, 5 §
- Åtgärder, elimineras, reduceras eller accepteras, 6 §
- Åtgärdsplan och att den ska bevaras i 5 år. 6 § och 7 §

Kontrollpunkter fortsättning

- Mer övergripande har vi också tittat på risker kring
  - Fysiska och logiska skydd, 8 §
  - Säker programvaruhantering, 9 §
  - Fysisk och logisk behörighets- och åtkomsthantering, 10 § och 11 §
  - Hantering av planerade tekniska och organisatoriska förändringar, 12 §
  - Säkerställande av kompetens och personella resurser, 13 §
  - Spårbarhet (loggning), 14 §
  - Åtgärder för att minimera verkningar av incidenter (larm), 14 §
- Vi har inte tittat på kontinuitetsplanering, 17 § - 19 §

Sammanfattning och slutsatser av resultaten

- ISO 27000-cerifiering spelar roll
- Det är ett ständigt förbättringsarbete och tar flera år
- Dokumentering viktigt
- Omorganisation, sammanslagning och uppköp påverkar
- Vissa risker hanteras redan i verksamheten
- Överväg om särskilt verktyg för riskanalyser behövs
- PTS har inte funnit några brister i sin tillsyn av riskanalyser och har därför avslutat tillsynen
- Nyhet publicerad 1 februari