Personvernforordningen i praksis for Open Source

Bergen Open Source

30.10.2025, Bergen

- Fredrik Christensen – Seniorrådgiver, Teknolog
- Seksjon for Teknologi, Sikkerhet og tilsyn (TST)
- Bakgrunn fra informasjonssikkerhet i spesialisthelsetjenesten

Datatilsynet

- Opprettet 1980, lokalisert i Oslo
- Ca 60 medarbeidere + 9 studenter
- Uavhengig forvaltningsorgan
  Regelverk:
  - Forordningen og personopplysningsloven
  - Helseregisterloven
  - Helseforskningsloven
  - Kredittopplysningsloven
  - Politiregisterloven
  - Lov om Schengen informasjonssystem
  - mv.
- Personvernnemnda er klageorgan for våre vedtak

GDPR + Open source = interessant kollisjon…

Open Source bygger på deling og transparens

GDPR bygger på kontroll og ansvar

GDPR hindrer innovasjon og legger opp hindringer?

Fra personregisterloven til i dag….


Datatilsynet

Konsesjon
for opprettelse av personregister

Personregisterloven
1978

Personopplysningsloven
2000

Personvernforordning og personoppl.lov
2018

EUs personverndirektiv
1995

EUs personvernforordning
2016

De registrertes rettigheter og friheter, jf. EMK

De registrertes friheter:

- Retten til privatliv
- Kommunikasjonsvern
- Ytringsfrihet
- Tankefrihet
- Bevegelsesfrihet
- Forbud mot diskriminering
- Samvittighets- og religionsfrihet

Kontekst

- Personvernforordningen – Hva er det egentlig?
  - Internkontroll
  - Personopplysningssikkerhet

- Behandlingsansvar – er det så viktig da?
  - Virksomhetens plikter og de registrertes rettigheter

Prinsipper – informasjonssikkerhet og ansvarlighet

- «Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet») (art. 5 nr. 1 bokstav f)

- Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene overholdes (ansvarlighetsprinsippet).

Art. 5 nr. 1 f
Art. 5 nr. 2

Internkontroll etter personvernregelverket

- Sikre forsvarlig behandling av personopplysninger
  - Sikre den registrertes rettigheter og friheter
  - Ivareta virksomhetens mål med behandlingen
- Ledelsens verktøy for å ivareta sitt ansvar etter lover og regler, og demonstrere etterlevelse
- De ansattes verktøy for å utføre oppgaver på forsvarlig og sikker måte

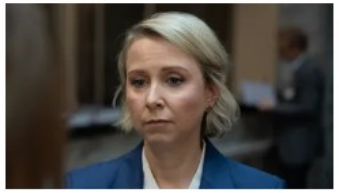
Hvorfor er dette relevant for Open Source?

- Som en behandlingsansvarlig virksomhet har du plikter
  - Proprietær kode
  - Open Source kode
- Personvernforordningen gjelder for alle som behandler personopplysninger utenfor rent personlig bruk
- Er det ikke kodeutviklers ansvar at koden er sikker?
  - NEI (i kontekst av brudd på personopplysningssikkerheten)
  - Virksomheten plikter å påse at all kode og programvare som benyttes for behandling av personopplysninger er sikker.

Et levende risikobilde

Kritisk sårbarhet i Cisco-utstyr under angrep

18. okt. 2023

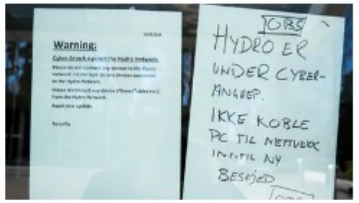


Nulldagssårbarhet ble benyttet til å utføre dataangrepet mot departementene

25. juli 2023

Brukte ett år på å oppdage at de var hacket: – Det skal jo ikke skje

6. feb. 2023



Hydro rammet av hackerangrep

19. mars 2019

NSM: – Trusselaktører bruker i mye større grad underleverandører for å komme seg inn

5. nov. 2021

Snart kommer det falsk e-post du trolig blir lurt av

19. feb. 2023

Nito: – Unge er dårligst på IKT-sikkerhet

3. feb. 2023

Verdensomfattende dataangrep rammet leverandører av viktig infrastruktur

13. mai 2017

(Saker hentet fra Digi.no)

Når funksjonalitet blir personvernbrudd i Open Source

- Log4Shell (Log4j) – 2021
  - Fjernkodeeksekvering-> web shell -> dataeksfiltrering
- Hearthbleed (OpenSSL) – 2014
  - Eksponerte kryptonøkler
- XZ utils backdoor (2024)
  - Potensiell total kompromittering
- npm event-stream sårbarhet (2018)
  - datatyveri

Log4j (Log4Shell)

- Javabasert rammeverk brukt for applikasjonslogging
- Utviklet av Apache Software Foundation
- Log4j er ekstremt utbredt
  - Fortune 500
  - Stat
  - SMB
  - Privat

«Veracode samlet inn data over 90 dager fra 3 866 organisasjoner som bruker 38 278 applikasjoner avhengige av Log4j, med versjoner mellom 1.1 og 3.0.0-alpha1. Av disse applikasjonene bruker 2,8 % Log4j-varianter fra 2.0-beta9 til 2.15.0, som er direkte sårbare for Log4Shell.»

Utnyttelse i Norge

Beskriv hva som har skjedd. Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.

[redacted] ble Palo Alto Cortex XDR installert på klienter og noen servere i vårt domene. Dette for

Har dere undersøkt den opprinnelige årsak til at angrepet kunne finne sted?

Rotårsak er utnyttelse av Apache Log4J sikkerhetshull i VMware Horizon-løsningen. Dette ble muliggjort gjennom at løsningen ble skrudd av for å sikre miljøet når sårbarheten ble identifisert [redacted] og dermed ikke ble oppdatert med øvrige systmer når sårbarheter ble tettet på disse VMware Horizon ble så skrudd på igjen etter sluttbruker (ekstern bruker med tilgang til en VM) tok kontakt med IT-support den [redacted] og rapporterte at de ikke hadde kontakt med sin løsning/skrivebord. Under feilsøking av denne saken ble VMware Horizon påskrudd uten at nødvendig patching ble foretatt. Systemet ble derfor eksponert for sårbarheten som videre kunne utnyttes fra denne datoen.

Beskriv hva slags type personopplysninger som ble berørt av avviket

Brukerdatabasen (AD)

Oppsummering

- Som virksomhet/organisasjon har du et selvstendig ansvar
- Hvordan etterleve regelverket:
  - Gjennomføre vurderinger og analyser (ROS & DPIA)
  - Dokumentere
  - Internkontroll
    - Styrende rutiner – overordnet policy
    - Gjennomførende rutiner – System og patch-styring, Tilgangsstyring, hendelseshåndtering sikkerhetskopiering og gjenoppretting, logging og overvåking mv.
- Ha en «sikkerhetsnørd» med riktig kompetanse
- GDPR/Personvernforordningen setter klare rammer for hvordan en virksomhet kan behandle personopplysninger… selv for virksomheter som bruker Open Source programvare eller biblioteker

Takk for oppmerksomheten

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no