Kjøreregler for hemmeligheter og kode

Grunntanker og prinsipper | Hemmeligheter | Beste praksis | Om uhellet er ute | Typer hemmeligheter | Versjonslogg

Grunntanker og prinsipper

Hemmeligheter

- Hemmeligheter skal ikke ligge i kildekode eller i kildekode-repositories.
- Passord, API-nøkler og sertifikater skal lagres kryptert "at-rest".
- Konfigurasjon som vil hjelpe en angriper å få tilgang til sensitive ressurser skal behandles som "hemmeligheter".

Beste praksis

For å gjøre koden lettere å vedlikeholde, og å bidra til å forhindre feilkonfigurering av et kjørende system, bør man skille kildekode og konfigurasjon. Konfigurasjon, som f.eks *vertsnavn*, som kan variere fra et miljø til et annet, skal trekkes ut av kildekode og legges i *konfigurasjonsfiler* der variablenes verdier injiseres run-time, om mulig.

Eksempler på konfigurasjonsfiler som benyttes slik er web.config, context.xml, application.properties, samt CaC-filer.

Selv om pasientdata og annen sensitiv informasjon ikke regnes under begrepet "hemmeligheter" i denne sammenhengen, er det en selvfølge at slik informasjon *ikke* egner seg for lagring i GitHub.

Om uhellet er ute

Om du, ved et uhell, har commitet en hemmelighet, må du utføre *alle* de neste stegene for å utbedre problemet:

1. **Rotere hemmeligheten** ⚠️
   Dette er det aller viktigste punktet, og det haster mest. Passord, tokens og andre typer hemmeligheter, *må* roteres der de benyttes, slik at ingen kan få utilsiktede tilganger om de har fanget opp hemmeligheten. I tillegg *må* alle aktive sesjoner tvangstermineres, slik at ingen kan henge igjen med gammel autentisering.

2. **Committe en ren versjon**
   Du må fjerne hemmeligheten fra koden og committe endringene, slik at HEAD blir ihht retningslinjene.

3. **Føre avviksmelding**
   For å sikre at alle kollegene dine i Helse Nord kan lære, og at vi, som foretak, er tilstrekkelig etterettelig, må det føres en avviksmelding i DocMap.

Slette repoet?

Det hjelper ikke å slette repoet. Git-historyen er fortsatt tilgjengelig for alltid. Det eneste som fungerer er å følge stegene over.

Typer hemmeligheter

Ressurs	Kryptert	Notat
Brukernavn		
Passord	At-rest	
API-nøkler	At-rest	
Sertifikater	At-rest	Sertifikater og private krypteringsnøkler.
Sertifikat-passord	At-rest	Passord/pin for å låse opp privatekey.
Sertifikat-fingerprint		Unik og automatisk generert hash som identifiserer det unike sertifikatet.

Sertifikat-navn		Logiske menneskeskapte sertifikatnavn som gjør det lettere å søke i sertifikat-filer/stores.
Sertifikat-filers filbane		Som et utgangspunkt også hemmelighet. Bjørn Einar Torsteinsen diskuterer gjerne dette.