FORUM FOR SAMARBEJDE OM GEODATA I KOMMUNERNE

Er jeres geodata sikret, hvis I bliver hacket?

Baggrund

Hackere er ikke længere skumle hætteklædte teenagere, der sidder i en kælder og forsøger at gætte dit password. Virkeligheden er i dag, at hacking udføres af professionelle firmaer i tæt samarbejde med staters efterretningstjenester, og at passwords kan købes på internettet.

Truslen for cybersikkerhed er meget høj[1], og hver fjerde kommune rammes dagligt af over 200 cyberangreb[2]. Der har desuden været flere eksempler på, at kommunernes systemleverandører også rammes af hacking. Erfaringer viser, at backup ikke kan indlæses korrekt efter en hacking i op til 60% af tilfældene[3].

FOSAKO anbefaler derfor kommunerne at undersøge jeres sikring af geodata, for at ruste jer bedst muligt før en eventuel hacking.

1) *Center for Cybersikkerhed rapport "Trusselsvurdering-Cybertruslen mod Danmark maj 2023"*
2) *KL pressemeddelelse "Danmark skal have ét samlet cyberforsvar" 21. juni 2023*
3) *Udtalelse fra Truesec på FOSAKO Sommermøde 2023*

Anbefaling

1. Tjek om dit password kan købes. Det kan f.eks. gøres på www.havelbeenPwned.com. Skift password, hvis det er til salg. Husk at to-faktor godkendelse er rigtig sikkert.

2. Overvej hvilke geodata der er vigtige for jer at have adgang til på kort og langt sigt.

3. Sørg for at have data i 3 kopier - på 2 forskellige medier, og 1 af dem offline. Så er I godt sikret.

4. Gå i dialog med IT-afdelingen: Hvilke geodata tages der backup af og hvor ofte? Har de en offline backup af data? Har de testet, om backup kan indlæses uden fejl?

5. Gå i dialog med jeres systemleverandører, hvis I har hostede løsninger. Spørg ind til, hvordan de tager backup, om de har testet at backuppen kan genindlæses, og om de har en offline backup af jeres data. Hvis ikke, så overvej selv at lave en backup.

6. Overvej fordele og ulemper ved hhv. primært at være baseret på webservice eller ved download af lokale kopidata.

Øvelse

Vi foreslår, at I laver en øvelse i GIS/geodatateamet sammen med jeres leder, hvor I tager udgangspunkt i følgende case:

- Kommunen bliver hacket. I bliver afskåret fra internettet, databaser og filservere i 1 uge. Hvilke data ville I ønske, I havde haft adgang til?

I får derefter at vide, at IT-afdelingen ikke kan genskabe indholdet på jeres filservere og database. Hvad ville I ønske, at I havde gjort på forhånd?

- Vil I sætte nogen nye initiativer i gang herefter?

Hvilke geodata er det relevant at sikre?

Vi anbefaler, at I overvejer 3 typer geodata:

1. De mest kritiske geodata
    - Hvilke data vil I have mest brug for i en krisesituation? Her kan det være nødvendigt at have en dialog med jeres krisestab.

2. De mest værdifulde geodata
    - Hvilke data har kostet mange mandetimer at skabe? Det kan f.eks. være jeres registrering af grønne områder.

3. De mest anvendte geodata
    - Overvej at logge, hvilke temaer, der er mest anvendte i jeres WebGIS. Brug det som udgangspunkt for hvilke temaer, I bør sikre en backup af.

Afrunding

Med dette initiativ ønsker FOSAKO at starte op på dialog om, hvordan vi kan sikre os bedre mod cyberkriminalitet. Hvad er de væsentligste datasæt og hvordan kan vi lave nogle gode rutiner for at sikre os bedre?

FOSAKO vil i 2024 starte op på dialogen med de store landsdækkende geodatabaser som GeoDanmark, Miljøportalen og Plandata, hvor kommunerne også har geodata.