Interpellationssvar

Kommunstyrelsens ordförande
Richard Orgård

Till Kommunfullmäktige

Datum 2025-10-08
Dnr KS 2025/0021

Svar på interpellation nr 9/2025 - Hackningen av Miljödata och hur Österåkers kommun säkerställer skyddet av personuppgifter

Interpellationen från Sofia Almgren Johansson (S) rör det allvarliga dataintrånget mot systemleverantören Miljödata i augusti 2025. Frågorna som ställs är både befogade och angelägna, och jag vill tacka för att frågan lyfts till Kommunfullmäktige. Händelsen har berört många kommuner i landet och hanteras med stort allvar även hos oss i Österåker.

1. Vilken information har Österåkers kommun hittills fått från Miljödata om omfattningen av intrånget och vilka av kommunens anställda som kan vara drabbade?

När händelsen identifierats av Miljödata i slutet av augusti, informerade de kommunen att deras system blivit föremål för ett omfattande cyberangrepp. Miljödata har informerat om att deras forensiska utredning visat att angreppet har utförts av en extern, antagonistisk aktör som påstår sig tillhöra en s.k. ransomware-grupp (”Hotaktören”) som den 20 augusti 2025 beredde sig åtkomst till delar av Miljödatas IT-miljö. Initialt informerade Miljödata att hotaktören haft obehörig tillgång till delar av deras databaser.

Den 2 september meddelade Miljödata att det framkommit att hotaktören kunnat tillskansa sig viss information ur de påverkade systemen. Deras utredning hade då visat att Österåkers kommun var drabbade av detta och att hotaktören hade sammanställt information i form av CSV-filer – Comma Separated Value-listor - från det Miljödata kallar persontabeller. För Österåkers kommun avser den sammanställda informationen samtliga nuvarande och tidigare anställda sedan systemet togs i bruk 2017.

Miljödata har bekräftat att uppgifter som personnummer, adresser, telefonnummer och anställningsinformation har läckt. Miljödata uppger att de samarbetar med både Polisen och säkerhetsspecialister samt att de har anmält incidenten till Integritetsskyddsmyndigheten (IMY).

2. Vilka omedelbara åtgärder har kommunen vidtagit för att skydda de berörda, exempelvis genom information, stöd eller hjälp med att förebygga identitetsstöld och bedrägerier?

Kommunen har omedelbart efter händelsen:

- Informerat samtliga nuvarande medarbetare om dataintrånget via interna kanaler samt haft information på extern hemsida för tidigare anställda
- Nuvarande anställda med skyddade personuppgifter har kontaktats via närmsta chef för att informeras om vilka exakta uppgifter som varit med i det läckta materialet
- Informerat och påmint samtliga nuvarande anställda om IT-säkerhet med uppdaterad information och råd att tänka på för att förebygga att något skulle hända utifrån de uppgifter som hotaktören publicerat
- Erbjudit stöd genom HR och Dataskyddsombud för frågor och vägledning
- Kommunen har polisanmält händelsen och upprättat en anmälan till Integritetsskyddsmyndigheten (IMY)

3. Vilka krav ställer kommunen på Miljödata vad gäller ansvar, kompensation och transparens gentemot Österåkers anställda?

Vi har i kommunens kontakt med Miljödata ställt krav på följande punkter:

- Full transparens om vad som inträffat, omfattningen och vilka säkerhetsåtgärder som vidtagits.
- Specifik information om vilka anställda hos oss som är berörda.
- Att Miljödata tar sitt ansvar gentemot kunder och registrerade individer enligt GDPR.
- Att kompensation för eventuella skador eller merkostnader blir föremål för fortsatt diskussion, särskilt om det visar sig att försummelse förekommit.

4. Vilka långsiktiga åtgärder planerar kommunen för att stärka IT-säkerheten, särskilt vad gäller leverantörer som hanterar känsliga personuppgifter?

Vi har redan initierat ett förstärkt informationssäkerhetsarbete, vilket inkluderar:

- Det finns redan en tydlig struktur kopplat till framtagande av Personuppgiftsbiträdesavtal för att säkerställa att vi som kommun uppnår dataskyddskrav, detta arbete fortlöper och intensifieras för att säkerställa att alla aspekter tas om hand
- Att kommunen ser över skallkrav på upphandlade molntjänster
- Kommunen arbetar för att etablera ett ledningssystem för informationssäkerhet, ledningssystemet kommer att utgå från ISO27000 och innefattar bland annat klassning av samtliga informationstillgångar samt förbättra riskbedömningar av befintliga och nya system
- Att intensifiera interna utbildningar om informationssäkerhet för chefer och systemansvariga
- Kommunen bevakar att det centralt (SKR t.ex.) tas fram nationella regler för liknande tjänster

5. Hur avser kommunen att utveckla sin uppföljning och kontroll av externa leverantörer för att minska risken för liknande incidenter i framtiden?

Kommunen ser att det är mycket svårt att följa upp säkerheten hos enskilda leverantören, men att det finns ett tydligt behov av att stärka uppföljningen av leverantörer, särskilt de som hanterar personuppgifter. Därför kommer vi att:

- Se över och tydliggöra ansvarsfördelningen mellan kommunens Informationssäkerhetsansvarig, Digitaliseringsavdelning, Upphandlingsfunktion och verksamheterna när det gäller leverantörskontroll.
- Säkerställa att återkommande riskbedömningar av systemleverantörer sker
- Arbeta för att krav på incidentrapportering, redundans och säkerhet är skarpa och uppföljningsbara i avtal
- Utreda möjligheten att införa krav på externa säkerhetsrevisioner från oberoende part

Slutsats

Denna incident visar med all önskvärd tydlighet hur viktigt det är att ständigt arbeta med cybersäkerhet och dataskydd – inte bara internt, utan också i relation till våra externa leverantörer. Kommunen tar detta på största allvar och arbetar intensivt med att både hantera denna situation men även att ta med oss insikter och se hur processer kan bli än tydligare och uppdaterade.

Richard Orgård
Kommunstyrelsens ordförande