Incidentrapport - Miljödata

Kort beskrivning

Den 26 augusti 2025 kl 16.54 informerades Arbetsmarknadsnämnden av Stadsledningskontoret (SLK) att systemleverantören Miljödata utsatts för ett cyberangrepp som innebar att hotaktören troligtvis fått tillgång till personuppgifter som Arbetsmarknadsnämnden är personuppgiftsansvariga för (obehörig åtkomst). Den 14 september publicerades personuppgifterna av hotaktören på Darknet. Attacken innebar även att en del information som fanns i systemet inte var tillgänglig i systemet.

1100-1500 medarbetare och tidigare anställda omfattas av incidenten. Incidenten har bedömts vara mycket allvarlig och har anmälts till IMY.

Bakgrund och beskrivning av incident

Miljödata i Karlskrona (Miljödata) informerade Kommunstyrelsen i Stockholm stad den 25 augusti att de utsatts för ett cyberangrepp. Angreppet ska ha skett mellan den 20-23 augusti 2025, men sårbarheten i systemet som hotaktören nyttjade för att komma åt uppgifterna har funnits längre. Incidenten detekterades av larmsättning i den tekniska miljön.

Den 26 augusti 2025 kl 16.54 informerade SLK samtliga nämnder om incidenten genom ett mailutskick. Det fanns vid tidpunkten inga bevis på stöld av Stockholms stads data. De registrerade som berörs av incidenten uppges vara nuvarande anställda.

Den 29 augusti skickade Arbetsmarknadsnämnden in en anmälan till tillsynsmyndigheten IMY med anledning av att incidenten inte osannolikt leder till en hög risk för fysiska personers (de registrerades) fri- och rättigheter.

Allvarlighetsgraden av incidenten bedömdes till en början vara betydande, men ändrades till mycket allvarlig efter att stölden av personuppgifter bekräftats den 3 september 2025. Den 14 september 2025 publicerades personuppgifterna på Darknet av hotaktören.

Den 17 september informerar SLK att skyddade personuppgifter läckt ut och att incidenten även omfattar registrerade som haft en anställning inom staden från 2024 och framåt. Hos Arbetsmarknadsnämnden identifierades fem personer med skyddad identitet som fått sina personuppgifter läckta.

Arbetsmarknadsförvaltningen
Staben för strategi och samordning

Box 10014
12126 Stockholm-Globen
linda.johansson.3@stockholm.se
start.stockholm

Personuppgifter som omfattas av incidenten
Incidenten berör personuppgifter om medarbetare som är eller har varit anställda under perioden 2024 till augusti 2025. Antalet personer som berörs av incidenten är 1100-1500. Personuppgifterna behandlas med allmänt intresse som rättslig grund.

Personuppgifter som berörs av incidenten:

- personnummer
- förnamn och efternamn
- telefon och mobiltelefon (hem och/eller till arbete)
- e-postadress (hem och/eller till arbete)
- utdelningsadress (hem)
- organisationskopplingar (Webb-ID strukturen i LISA självservice)
- anställningsidentitet/AD-konto
- anställningsperiod
- anställningsform
- yrke/befattning (yrkeskod).

Varför Arbetsmarknadsnämnden hade personuppgifter i Stella
Staden som helhet har haft för avsikt att införa ett systemstöd för rapportering och uppföljning av arbetsmiljöincidenter (Stella). Staden hade vid tiden för incidenten ännu inte driftsatt systemet, varför inga uppgifter om arbetsmiljöincidenter behandlats hos Miljödata. Inför kommande driftsättning har staden från april 2025 haft en produktionsmiljö hos Miljödata i syfte att bl.a. verifiera att organisatoriska strukturer och roller är korrekt konfigurerade i systemet och för att kunna identifiera problem eller brister i flödet för incidentrapportering, så att systemet ska fungera på ett korrekt och säkert sätt vid driftsättning. Behandlingen har bestått i en integration från stadens löneadministrativa system Lisa från vilket det har överförts bl.a. anställningsuppgifter, namn, adress och personnummer.

Inom ramen för införandeprojektet har det bedömts att det fanns ett behov att inkludera uppgifter om anställda från ungefär ett år bak i tiden i syfte att verifiera den fullständiga organisationsstrukturen. Staden har i e-postkorrespondens med Miljödata strax före sommaren framfört instruktioner om gallring av tidigare laddningar och testladdningar i Miljödatas system. Uppgifter om tidigare anställda inaktiverades av Miljödata, vilket gjorde att de inte längre syntes i stadens produktionsmiljö. Staden har därför varit av uppfattningen att endast uppgifter om nuvarande anställda behandlats hos Miljödata. Det är i samband med incidenten som staden fått information om att uppgifterna endast inaktiverats hos Miljödata, men inte gallrats.

Skyddade personuppgifter
Fem personer med skyddade personuppgifter, varav två ungdomar, har fått sina personuppgifter läckta. Samtliga har kontaktats av ansvarig chef och en flaggning i Lisa har nu åtgärdats.

De fem personer som berörs av incidenter har inte flaggats i Lisa och därför har deras personuppgifter läckt. För att en flaggning ska ske krävs en i dagsläget en manuell hantering.

Riskbedömning
Händelsen bedöms som mycket allvarlig utifrån omfattningen av personuppgifter, volymen av registrerade, känsligheten i de personuppgifter som läckt ut och att även personer med skyddade personuppgifter omfattas av incidenten.

Konsekvenser

- Den registrerade förlorar kontrollen över sina personuppgifter.
- Identitetsstöld och bedrägeri.
- Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt.

Information till de registrerade
Den 4 september publicerades en nyhet på externa hemsidan av SLK och av Arbetsmarknadsförvaltningen på intranätet med information om incidenten, vilka personuppgifter som berörs, vidtagna åtgärder, sannolika konsekvenser av incidenten, hur de registrerade kan begränsa eventuell skadeverkan och kontaktuppgifter till dataskyddsombud samt IT-chef.

Valet att gå ut med information på hemsidan grundade sig i att det var det snabbaste sättet att nå ut till så många som möjligt.

Den 15 september publicerades en nyhet på intranätet av SLK med information om att skyddade personuppgifter förekommer i läckan. Information om att berörda medarbetare kommer att kontaktas av närmsta chef samt att en utredning kring varför dessa personuppgifter hamnat i systemet påbörjas.

Den 17 september publiceras ytterligare en nyhet av SLK nu med mer utförlig information om vad som hänt, att uppgifterna publicerats på Darknet, en uppdaterad lista över vilka personuppgifter som omfattas av incidenten och information om att även tidigare anställda berörs. Vilka åtgärder som staden vidtagits och en mer utförlig beskrivning av sannolika konsekvenser av incidenten samt en uppmaning till de registrerade att vidta extra försiktighet. Nyheten publicerades både externt och internt.

Den 25 september går digital post ut genom Kivra till stadens medarbetare, samt tidigare anställda, med information om incidenten enligt den information som publicerats på intranätet samt kontaktvägar. För de medarbetare som inte är anslutna till Kivra går fysisk post ut.

Att gå ut med information digitalt och fysiskt är ett omfattande arbete vilket bidragit till att information den här vägen, genom fysiska och digitala utskick, inte gått ut tidigare.

Åtgärder

Följande åtgärder har vidtagits:

- Kontinuerliga avstämningar internt och med SLK.
- Anmälan till IMY.
- Polisanmälan har upprättats av SLK.
- Information till de registrerade.
- Särskild information (direktkontakt) till registrerade med skyddade personuppgifter.
- Ny rutin för hantering av personer med skyddad identitet.

- Införandet av Stella har pausats i avvaktan på en utredning kring om kravställda säkerhetsåtgärder uppfylls och integrationen till EPS:en är införd.

Följande åtgärder kräver fortsatt utredning eller åtgärd:

- Säkerställa dokumentation (PUB-avtal, konsekvensbedömningar, personuppgiftsansvarsförhållanden), ansvar och roller gentemot SLK för de gemensamma systemen.
- Roller, ansvar och kommunikationsvägar i händelse av en personuppgiftsincident behöver dokumenteras och förankras.
- Alla medarbetare ska känna till vad en incident är och hur den rapporteras.
- En utredning kring hanteringen av skyddade personuppgifter har påbörjats. Integration är på gång (SLK).
- Gallring av personuppgifter behöver säkerställas att det sker och att det sker hela vägen.
- Säkerställa att information till de registrerade går ut i tid.
- Säkerställa kunskap kring hantering i händelse av en krissituation kopplat till informations- och cybersäkerhetsområdet.
- Säkerställa att all information som hanteras digitalt går genom digitaliserings- och informationssäkerhetsprocessen.

Återkoppling till SLK

- Kommunikationsvägar och rutiner för hantering av informationssäkerhetsincidenter behöver formaliseras oavsett hur personuppgiftsansvarsförhållandet ser ut. För de gemensamma systemen är SLK kontaktvägen in för leverantörerna.
- Tydliggöra kommunikationsvägarna när ny information ska nå ut: Förvaltningschefer, systemansvariga chefer, ISAM och DSO. Under den här incidenten var upplevelsen att den var spretig till en början, men blev bättre allt eftersom.
- Bra att SLK:s anmälningar till IMY skickades ut. Det underlättade hanteringen internt då SLK var den som satt på all information och ensam hade kontakt med leverantören.
- Det tog för lång tid innan SLK, som är leverantörernas kontaktväg in, informerade personuppgiftsansvariga nämnder. Ett exempel är när SLK informerades om incidenten (25/8 på morgonen) och när nämnderna fick information om incidenten (26/8 16.54).
- Fiktiva inloggningsuppgifter (användarnamn och lösenord) till Stella som tilldelats nämnderna har skickats ut i ett samlat dokument. Förvaltningarna har visserligen fått en specifik inloggningsuppgift tilldelad till sig, men eftersom att alla förvaltningars inloggningsuppgifter skickades i ett dokument till alla har det funnits möjlighet att logga in med andra förvaltningars inloggningsuppgifter och fått ta del av personuppgifter som man inte har rätt att ta del av.
- Det saknas information på externa hemsidan om hur anställdas personuppgifter hanteras inom staden.
- Överlag bra hanterat!

Slutsatser

- Informationsutbytet mellan SLK och nämnderna kan effektiviseras.
- Dataskyddsarbetet kopplat till Stella och personuppgiftsansvarsförhållandet var inte klarlagt. Arbetsmarknadsnämnden står inte uttryckligen med som personuppgiftsansvariga i befintligt PUB-avtal.
- Konsekvensbedömning (DPIA) är inte genomförd inför införandet av Stella. Det har inte heller genomförts någon informationsklassning på arbetsmarknadsförvaltningen. Registerförteckningen är inte uppdaterad. ISAM och IT kände inte till systemet.
- Samtliga medarbetare inom staden behöver känna till vad en personuppgiftsincident är och veta hur man rapporterar. Bättre att rapportera en gång för mycket än en gång för lite.
- Vi behöver höja cybersäkerhetskompetensen inom verksamheten hos nyckelpersoner ute i verksamheten. Där inkluderat informationssäkerhet och dataskydd.
- Ansvar och roller kring personuppgiftsincidenter när det är ett gemensamt personuppgiftsansvar behöver redas ut, dokumenteras och fastställas.
- Säkerställa att vi har tydliga processer för upphandling av tjänster och system samt att de är förankrade.

Kontaktuppgifter

Karina Uddén
Förvaltningschef
Karina.udden@stockholm.se

Personuppgiftsansvarig
Arbetsmarknadsnämnden, Stockholms stad

Dataskyddsombud
Peter Sundström
peter.sundstrom@stockholm.se
Nils-Erik Lundborg
nils.lundborg@stockholm.se