Bilaga 1

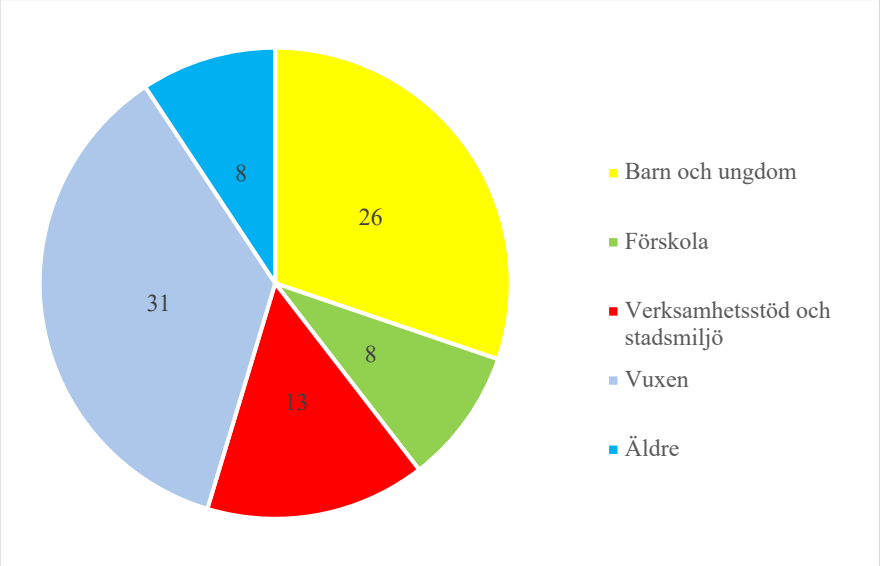
Sammanställning informationssäkerhets-incidenter Januari till Juli 2023

Detta är en sammanställning av IA-raporter under Januari till Augusti 2023, och följer med som bilaga till ledningsgruppens rapport. Sammanställningen tidigareläggs för att kunna utgöra underlag för ledningens rapport och sedan för verksamhetsplan 2024. Underlaget och sökningen på IA är utifrån rapporterade incidenter under perioden. Vissa incidenter kan ha skett tidigare, men ännu inte rapporterats. Detta för att få med samtliga rapporter som underlag.
Eftersom rapporten tidigareläggs går det inte att helt göra en jämförelse med förra årets. Detta då den utgår från annan tidsperiod. Dock var inrapporterade incidenter högre detta år med redan 86 rapporterade, än föregående som var för ett helår. Detta är en positiv utveckling då förvaltningen har ökat rapporteringsbenägenheten men inte allvarliga incidenter. Det är därmed inte troligt att antalet incidenter ökat, utan snarare har mörkertalet troligen minskat.
Utifrån läsning av de 86 incidenterna kan 38 anses kunnat hanteras helt utan att någon information läckt, förlorats eller integritet påverkats. Det innebär ändå att de föranlett andra åtgärder för att förhindra framtida oupptäckta incidenter. Överlag arbetar förvaltningen systematiskt med sin riskhantering.

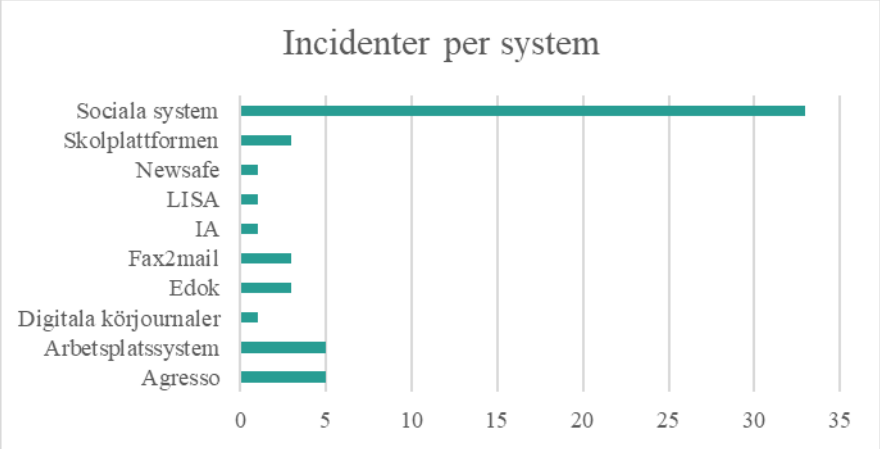
Hässelby-Vällingby stadsdelsförvaltning
Verksamhetsstöd och stadsmiljö

Hässelby torg 20-22
Box 3424
16564 Hässelby
Växel 08-50804000
Fax 08-508 04 099
hasselby-vallingby@stockholm.se
www.stockholm.se/hasselby-vallingby

Fördelning

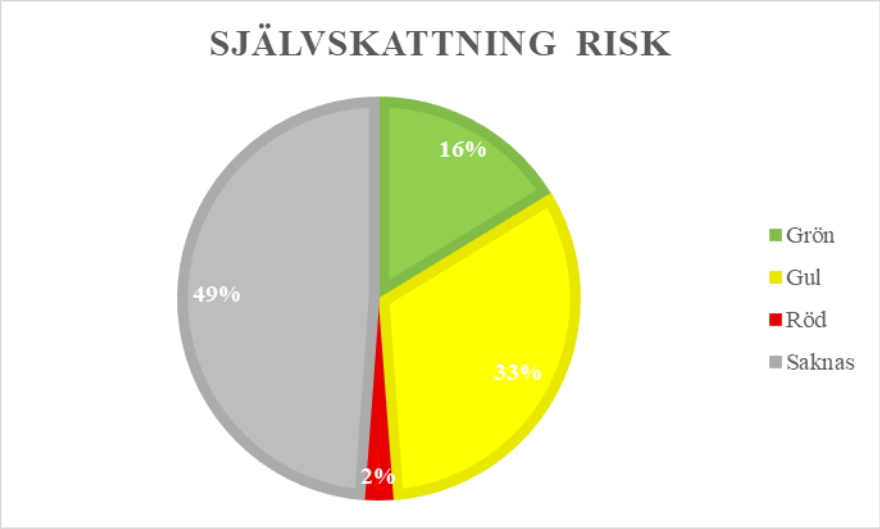


Incidentrapporterna är relativt jämt fördelade utifrån det flöde av ärenden och hantering av information som de olika avdelningarna hanterar. Det visar på att förståelsen för informationssäkerheten är på en grundläggande god nivå på de olika avdelningarna. Rapporter över incidenter fördelat per system är övervägande del för sociala system som står för nästan hälften av de inrapporterade incidenterna. Antalet användare till det systemet är dock också mycket större och innehåller mer känslig information. I incidenträkningen nedan har dock bluffmailen räknas bort då de inte bör ses som incidenter (se förklaring i nästa kapitel). Dessa utgjorde ytterligare 7 st för arbetsplatssystem (outlook, m.m.)



Av informationssäkerhetsincidenterna utgör 50 av de inrapporterade incidenterna personuppgiftsincidenter. Endast en av dessa gick vidare till IMY. I IA är denna incident dock inte utredd eller avslutad eller bedömd enligt risksummeringen nedan.

Hur allvarliga är incidenterna



Vissa incidenter har under längre tid inte hanterats och inte klarmarkerats. Andra inväntar uppföljning av åtgärder. Men nästan samtliga incidenter har hanterats inom IA och avslutats. En första bedömning av risken bör kunna göras nästan omgående, eller inom någon vecka.
De flesta riskerna har i IA-systemet av respektive enhetschef avgjorts som ha medelrisk, därefter lågrisk och slutligen bara 2 incidenter som nådde upp till röd nivå.
Avgörandet för riskens allvarlighet är hur ofta den anses inträffa tillsammans med allvaret i incidenten. IAs riskanalys är inte kompatibel med stadens övriga riskanalys utan följer den som oftast används inom arbetsmiljö.
Vid analys av riskbedömning kan man dock se att nästan hälften av riskbedömningar inte har getts någon nivå alls. Det har skett främst i början av året men kan finnas fler orsaker.
Delar av incidenterna har inte hamnat på rätt enhet, det är inte ovanligt att en risk uppmärksammas på en enhet men egentligen rör en annan. Det innebär att fel enhet klarmarkerar utan att göra en bedömning.
Det finns även en skillnad i uppföljningen mellan olika enheter och avdelningarna i att använda verktyget på ett bra sätt, och viss minskning i saknade bedömningar finns under senare halvan av perioden.
Vid analys av riskbedömningen kan man se att de risker som angetts som röda, främst rör en vanlig typ av felanvändning av paraplyet som rör skyddade personuppgifter. Dessa har inte hanterats korrekt av enskilda handläggare vilket till en början sågs som sällan-händelse men som riktigt senare bedömts som en händelse som sker ofta. Det sociala systemet förvaltas dock inte av staden utan sker i en objektorganisation där både den verksamhetsnära och den IT-nära finns på andra förvaltningar.

Förvaltningens paralyförvaltare har vidarbefordrat problematiken, men skulle kunna göras tydligare med grund i de IA-anmälningar som gjorts. Detta eftersom security by design inte tillräckligt bra arbetats in i systemet.
Endast en av incidenterna som har rapporterats har bedömts så allvarlig att den rapporterats in till IMY och nedlagd där. Den är dock inte hanterad i IA.
Incidenter som rör bluffmail finns fortfarande med, men bör nästan kunna tas bort. Endast incidenter där stadens funktioner för att undvika bluffmail är numera en incident. Vill säga först när länkar används eller på något annat sätt det leder till skada eller risk för skada ska dessa läggas in. Av de 7 bluffmailen som rapporterats in är enbart ett av dessa en incident.

Utredningar

Utredningarna och åtgärderna har en högre kvalité än föregående år. Men fortfarande har flera utredningar fortfarande inte påbörjats trots att tid har gått, eller där ingen notering har gjorts om varför det inte skett något. Det är inte ovanligt att en incident uppmärksammas på en enhet men behöver hanteras på en annan. T.ex. att den upptäcks inom ekonomi eller arkivfunktioner men incidenten har inträffat på barn och ungdom. Överflyttning av ärenden blir inte helt problemfri. IA har sina begränsningar vad gäller incidenter som kan ha skett över flera enheter, eller är oklara.
Utredningarna visar ofta på hur brister ska kunna förhindras i framtiden och ibland på hur den aktuella incidentens konsekvenser har hanterats. För förståelse skulle dokumentation behövas för hur båda dessa delar hanteras.

Orsaker till incident

I 69 av de 86 incidenterna har vid genomgången den mänskliga faktorn varit avgörande för att de kunnat ske. Det har då rört sig om felaktig användning av system mot rutiner, eller andra misstag i hanteringen. Det innebär att organisatoriska åtgärder men också åtgärder i system skulle kunna innebära en minskning av sannolikheten att de inträffar igen.
Men 10 poster innebär problem av teknisk karaktär som inte beror på förvaltningens handhavandefel. Här ligger ofta åtgärderna bortom förvaltningens kontroll då felet är i system som förvaltas av staden. Tyvärr visar utredningarna att incidentrapporten då avslutas med hänvisning till stadens ansvar. Det behöver finnas en kanal för insamlande av fel på centralt förvaltade system.

Brister i nuvarande system

Flera brister finns i nuvarande system och staden ser över införandet av ett nytt. Ett par noterade brister bör uppmärksammas:

- Automatiska påminnelser om IA-incidenter som inte hanterats
- En incident kan röra flera områden- en personuppgiftsincident kan även vara en NIS-incident, säkerhetsincident, brandincident os.v. Incidenter ska bara behöva rapporteras in en gång, och sedan anges i kryssrutor istället för vad som bedöms som tillämpligt. Detta bör vara enklare ifall systemet separeras från rent arbetsskade-relaterat. Valbara alternativ ska då vara få men tydliga.
- Inblandade system där förvaltningarna själva kan välja valbara system vore bra. Det är idag tidskrävande att ta fram statistik. Systemproblem bör automatiskt kunna gå vidare till objektägare och/eller objektledare för kännedom. Det skulle även underlätta arbetet med förnyade riskanalyser av objekten.
- Sannolikhet och sårbarhetsbedömningar som bättre stämmer överens med stadens framtagna i övriga risk och sårbarhetsanalyser eller bedömningsverktyg.
- Lex Sarah riskerar fortfarande tappas i den här hanteringen, när en sådan skulle kunna inneburit en personuppgiftsincident eller informationssäkerhetsincident. För en anställd behövs en ingång, och förslagsvis bör inledningen till en Lex Sarah-rapport dokumenteras i incidenthanteringssystemet och där sedan ge tillgång till en Lex Sarah-rapport för diarieföring.
- Tydligare uppdelning för användaren i dokumentering av hur den aktuella incidenten hanterats, och hur man undviker liknande incidenter i framtiden.
- Val av involverade borde kunna sättas upp i principer som följer den lokala förvaltningen. Det skulle tydliggöra vilken verksamhets berörda som faktiskt drabbas såsom klienter inom socialtjänst, allmänhet, anställd m.m. D.v.s. efter intressenter som identifieras av förvaltningen.