Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2024-05-24
Diarienummer 0473/23

Handläggare
Elias Örjefelt
Telefon: 031-368 65 55
E-post: elias.orjefelt@intraservice.goteborg.se

Nämnden för Intraservices anvisning för informationsklassning

Förslag till beslut

I nämnden för Intraservice:

Intraservices anvisning för informationsklassning fastställs.

Sammanfattning

Kommunfullmäktige fastställde i maj 2023 stadens riktlinjer för informationssäkerhet. I riktlinjens kravställning framgår bland annat att nämnder och styrelser ska informationsklassa sin information. Metodiken för genomförande av informationsklassning behöver utarbetas av den enskilda myndigheten.

Informationsklassning utgör tillsammans med riskanalyser kravställningen för de organisatoriska och tekniska säkerhetsåtgärder som ska tillämpas på Intraservices information. Syftet är att förstå värdet på Intraservices information och i förlängningen införa tillräckliga säkerhetsåtgärder. Bristfällig efterlevnad av kravställning på informationsklassning kan resultera i att informationen får ett otillräckligt skydd alternativt att dyra och omständliga säkerhetsåtgärder införs som inte motsvarar värdet på informationen som hanteras.

Förvaltningen bedömer därför att nämnden för Intraservice bör fastställa Anvisning för informationsklassning för att säkerställa att informationsklassningsarbetet utförs kvalitativt och med en standardiserad metodik. Rutin, process och processbeskrivning har bilagts tjänsteutlåtandet i syfte att ge kontext till anvisningen.

Bedömning ur ekonomisk dimension

I Göteborgs Stads riktlinjer för informationssäkerhet framgår att information ska informationsklassas. Förvaltningen bedömer att arbetet med att informationsklassa nämndens information initialt kommer belasta nämndens personella resurser avsevärt. Därför kommer arbetet behöva bedrivas på samtliga nivåer, tjänster och personalkategorier i syfte att kunna uppfylla kravställningen i Stadens riktlinjer.

I förlängningen är förvaltningens bedömning att värderingen av informationen kommer leda till ökade kostnader kopplade till införande och förvaltning av säkerhetsåtgärder. Den ökade kostnaden är inte ett direkt resultat av själva informationsklassningsarbetet utan kommer följa av den kravställning på säkerhetsåtgärder som i framtiden kommer kopplas till säkerhetsnivåerna i Göteborgs Stads informationsklassningsmodell.

Åtgärderna förväntas stärka säkerheten för Intraservices och Stadens information avsevärt vilket sannolikt kommer leda till betydande kostnadsbesparingar över tid. Informationsklassning är en viktig komponent i proaktivt och riskbaserat informationssäkerhetsarbete, vilket kommer vara en kravställning vid införandet av den nya cybersäkerhetslagen (den svenska implementeringen av NIS2). Förvaltningen bedömer att en av åtgärderna för att undvika att påföras en administrativ avgift i samband med tillsyn är att införa en standardiserad metodik för informationsklassning.

Informationsklassning hjälper förvaltningen att bedöma vilka informationsmängder som är i behov av ett ökad skydd och omvänt vilka informationsmängder som inte har höga skyddsbehov. Vissa kostnadsbesparingar kommer troligtvis realiseras genom att skyddet för viss information kan göras mindre kostsamt efter genomförd informationsklassning.

Kontrafaktiska kostnadsbesparingar är svårbedömda, men med en ökad informationssäkerhet minskar risken för kostsamma säkerhetsrelaterade händelser så som ransomeware.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

En standardiserad modell för informationsklassning hjälper förvaltningen i bedömningen av vilken information som är särskild värd att skydda. För den enskilde innebär det sannolikt ett förhöjd skydd för känsliga personuppgifter och den personliga integriteten.

Särskilt utsatta grupper inom exempelvis socialförvaltningarnas eller Äldre samt vård- och omsorgsförvaltningens verksamheter kommer sannolikt omfattas av ett utökad skydd som ett resultat av informationsklassningsarbetet.

En central aspekt i informationsklassningsarbetet är att bedöma krav på tillgänglighet för informationsmängder. Förvaltningen bedömer därför att åtgärden kommer stärka arbetet med Agenda 2030 kopplat till mål 16.10 *Säkerställa allmän tillgång till information och skydda grundläggande friheter.* Förvaltningen bedömer att informationsklassningsarbetet kommer stärka skyddet för den information som behövs för att upprätthålla kritiska samhällstjänster som bedrivs i kommunal regi och kommer därför även stärka mål 11B *Utveckla strategier för inkludering, resurseffektivitet och katastrofriskreducering.*

Samverkan

Samverkan har skett 2024-06-19.

Bilagor

1. Anvisning för informationsklassning
2. Rutin för informationsklassning (med bilagor)
3. Processbeskrivning – informationsklassning
4. Process - informationsklassning

Ärendet

Föreslagen anvisning ska utifrån Göteborgs Stads riktlinje för informationssäkerhet ange hur Intraservice ska arbeta med informationsklassning. Anvisningen ska säkerställa att Intraservice informationsklassning sker med en förutsägbar, standardiserad och kvalitetssäkrad metodologi.

Beskrivning av ärendet

Bakgrund

Kommunfullmäktige fastställde i maj 2023 stadens riktlinjer för informationssäkerhet. I riktlinjens kravställning framgår bland annat att *"Nämnder och styrelser ansvarar för att säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet och det är Göteborgs Stads klassificeringsmodell som ska användas"*.

Informationsklassning innebär att nämndens information delas upp i lämpliga informationsmängder och värderas utifrån Göteborgs Stads fastställda informationsklassningsmodell. Informationsmängderna värderas ur aspekterna konfidentialitet, riktighet och tillgänglighet. Göteborgs Stad har valt att definiera dessa aspekter enligt följande:

- Konfidentialitet - att information inte tillgängliggörs eller avslöjas för obehöriga.
- Riktighet - att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- Tillgänglighet - att information är tillgänglig och användbar när den behövs.

Informationsmängderna blir tilldelad ett värde mellan 0–4 för aspekterna konfidentialitet, riktighet och tillgänglighet. En given informationsmängd kan ha högt värde för konfidentialitet men inte för riktighet och tillgänglighet och tilldelas då konfidentialitet 3, riktighet 1 och tillgänglighet 1.

För att riktlinjen ska kunna efterlevas i praktiken krävs det ytterligare styrning från nämnden i syfte att konkretisera hur informationsklassning ska genomföras.

Nuvarande modell

Intraservice ska enligt Göteborgs stads riktlinje för informationssäkerhet informationsklassa den information som myndigheten äger. Förvaltningen har i dagsläget ingen fastställd modell för informationsklassning. Nuvarande modell bygger på best-practice och ad-hoc lösningar som tillämpas sporadiskt och med olika metodik beroende på vem som leder arbetet.

Gemensamt för nuvarande tillvägagångssätt för informationsklassning är att fokus ligger på den information som hanteras i Intraservices tekniska system, vilket resulterar i att det har varit svårt att särskilja den information som Intraservice är informationsägare för och den information som kunderna är informationsägare för. Metodiken resulterar i att tjänsterna många gånger tvingats gissa värdet på information som tillhör Intraservices kunder i syfte att kunna färdigställa en informationsklassning. I bästa fall har tjänsterna involverat ett urval av kunder vid informationsklassningen. Detta tillvägagångssätt kommer med sina egna utmaningar, främst att urvalet i kundkretsen är svårdefinierat.

Syftet med en informationsklassning är att i slutändan omgärda informationen med tillräcklig säkerhet i förhållande till informationens värde. När informationsklassning endast genomförs för information i ett enskilt tekniskt system omhändertas inte det faktum att informationshantering nästan alltid är en kedja av händelser och informationsbärare.

Nuvarande metodiken försvårar bedömning om vart säkerhetskrav ska riktas eftersom det ofta finns bakomliggande infrastrukturkomponenter eller applikationer som är en förutsättning för att informationen i systemet ska säkras. Eftersom informationsklassningen i nuvarande utformning endast tar hänsyn till systemet eller applikationen som är föremål för informationsklassningen vid det givna tillfället uppstår svårigheter att rikta krav mot tjänster, infrastrukturkomponenter eller applikationer som för tillfället inte är föremål för informationsklassning, även om dessa är en förutsättning för systemet eller applikationen. Metodiken riskerar därför att resultera i att ett antal kravställningar på understödjande komponenter i praktiken inte förmedlas till ansvarig för komponenten.

Föreslagen modell

Modellen består av två styrdokument med tillhörande bilagor:

- Nämnden för Intraservices anvisning för informationsklassning. Anvisningen fördelar ansvar, mandat, begreppsapparat och grundläggande krav på informationsklassning. Förvaltningens bedömning är att anvisningen behöver fastställas av nämnden eftersom den utpekar ansvar för genomförande av informationsklassning. Det ansvaret är sedan tidigare fördelat till nämnder och styrelser genom Göteborgs stads riktlinjer för informationssäkerhet. Anvisningen fördelar mandat till Intraservices CISO att fastställa rutiner och instruktioner tillhörande anvisningen
- Intraservices rutin för informationsklassning. Rutinen är en detaljerad steg-för-steg-guide som ska användas av informationsägaren eller den person informationsägaren har pekat ut som genomförandeansvarig. Rutinen ska fastställas av Intraservices CISO.

Ambitionen har varit att upprätta en begreppsapparat som hjälper Intraservices förvaltning och kunderna att på ett tydligt sätt kunna särskilja på Intraservices information och kundernas information. I modellen delas information upp i:

- Innehållsinformation, som är den information som uppstår när användare nyttjar tjänsten. Det kan handla om dokument, meddelanden, bilder etc. som skapas i samband med att staden genomför sitt dagliga arbete. Detta är kundernas eller Intraservices som tjänstekonsuments information.
- Gemensam innehållsinformation, som är information som tillhandahålls av tjänsten och nyttjas av flera användare eller tjänster men som inte skapats av användarna. Informationen är så att säga en del av tjänsten. Det kan handla om användardatabaser, metadatastrukturer, sammansättningar av stora mängder information som presenteras i olika vyer etc. Detta är tjänsternas information.
- Funktions- och säkerhetsinformation, som är den information som tekniskt eller praktiskt upprättas i samband med tjänsteleveransen. Det kan handa om loggar, certifikat, kryptonycklar, listor över komponenter eller applikationer etc. Detta är tjänsterna eller Intraservice som egen systemägares information.

En ytterligare målsättning i arbetet med den ny informationsklassningsmodellen har varit att särskilja bedömningen av informationens värde från det eller de tekniska system informationen behandlas med hjälp av. Det är förvaltningens bedömning att det kommer underlätta i arbetet eftersom värdet på information sällan förändras medan eventuella systemstöd som informationen hanteras i förändras oftare. Förhoppningen är att den förändrade metodiken resulterar i att färre informationsklassningar kommer behöva genomföras eftersom kopplingen mellan tekniskt system och informationens värde bryts, informationsklassningar kommer därmed inte med nödvändighet behöva genomföras vid exempelvis upphandling eller förändring av tekniska system. Vidare behåller varje informationsmängd sitt värde oavsett till vilket system informationen flyttas. Detta är framför allt viktigt om information någon gång hanteras i stora, ostrukturerade tjänster eller tillämpningar som e-post eller fillagring.

Processbaserad informationsklassning

Nu föreslagen modell bygger på att underlaget för informationsklassningarna är förvaltningens processer. Det innebär att verksamheten måste gå igenom sina etablerade processer eller vid avsaknad av etablerad process överskådligt visualisera verksamhetsprocesserna i syfte att kunna identifiera och informationsklassa den information som uppstår i processen. Kunder till tjänster ska informationsklassa den innehållsinformation som behandlas i Intraservices tjänster. Summan av kundernas informationsklassningar ska ligga till grund för vilka säkerhetsåtgärder som behöver vidtas i tjänsterna. Intraservice som förvaltning räknas i det här sammanhanget som kund till Intraservice som tjänsteleverantör och ska därför informationsklassa som kund.

Förhoppningen är att det även ska bli enklare att genomföra informationsklassning eftersom processer man arbetar är visualiserad, det blir då enklare att identifiera vilka informationsmängder som uppstår i en viss process.

Intraservice som tjänsteleverantör ska informationsklassa den information som ingen annan kan ta ansvar för. Främst handlar det om information som Intraservice som tjänsteleverantör tar fram i gemensamma databaser vid leverans av tjänsterna. Tjänsterna ska även informationsklassa den information som uppstår i samband med leverans av tjänst, det vi kallar funktions- och säkerhetsinformation.

Reglerad kravställning

Kravställning på informationssäkerhet har inte endast sitt ursprung i verksamhetens bedömning av värdet utan kan i många fall vara uttryckt i lagstiftning eller styrdokument. Det är därför viktigt att man vid en informationsklassning identifierar vilka reglerande dokument informationen eller processen omfattas av. Detta kommer vara av vikt vid bedömning av informationens värde i en informationsklassning. I många fall finns dessutom uttryckliga krav på hur verksamheten får hantera sin information, det är därför viktigt att kraven identifieras för att senare kunna omhändertas med hjälp av en eller flera säkerhetsåtgärder.

Offentlighets- och sekretesslagen (OSL) intar en särställning inom informationsklassningen eftersom merparten av konfidentialitetsaspekten inom offentlig förvaltning regleras här. Det framstår som orimligt att bedöma information till höga värden av konfidentialitet om det inte finns någon sekretessreglering för uppgifterna i OSL. Förvaltningen har därför gjort bedömningen att verksamheterna behöver identifiera om informationsmängderna omfattas av sekretessbestämmelse i OSL och i så fall vilken

reglering. Förförandet kan framstå som krångligt men kommer hjälpa verksamheterna att inte sätta höga värden för konfidentialitet på information som är offentliga allmänna handlingar och ändå kan komma att lämnas ut vid begäran. Omvänt är det viktigt att verksamheten identifierar de informationsmängder som omfattas av sekretessbestämmelser i OSL för att i förlängningen kunna vidta tillräckliga säkerhetsåtgärder för informationen.

Liknande OSL intar även GDPR en särställning för informationsklassningen. Hantering av personuppgifter sker i nästan samtliga informationsmängder. Personuppgifternas typ och dess tillämpning kommer styra skyddsvärdet för informationen. Identifieringen kommer dessutom vara till hjälp vid både tröskelanalys, konsekvensbedömning och personuppgiftsregistersvård. Det är därför förvaltningens bedömning att bedömning av vilka personuppgifter som hanteras i informationsmängderna ska anges vid informationsklassning.

Delegering av mandat att fastställa rutin

Förvaltningen bedömer att tidigare metodik för informationsklassning har haft en låg efterlevnadsnivå delvis på grund av att metodiken varit allmänt hållen och svår att omsätta i praktiken. Följaktligen är rutinen kopplat till nu föreslagen anvisning framtagen med en hög detaljeringsgrad. Till rutinen finns även ett antal bilagor som är tänkta att vara till hjälp vid identifiering av lagkrav, särskilt då sekretessregleringar.

Med detaljeringsnivån följer ett behov av återkommande aktualisering av rutinen, det framstår som onödigt betungande för både förvaltningen och nämnden att återkommande lyfta mindre förändringar i rutinen för beslut i nämnd. Förvaltningen föreslår därför att Nämnden för Intraservices CISO delegeras att fastställa förändringar i rutinen kopplat till anvisningen.

Förvaltningens bedömning

Informationsklassning utgör tillsammans med riskanalyser kravställningen för de organisatoriska och tekniska säkerhetsåtgärder som ska tillämpas på Intraservices information. Syftet är att förstå värdet på Stadens information och i förlängningen införa tillräckliga säkerhetsåtgärder. Bristfällig efterlevnad av kravställning på informationsklassning kan resultera i att informationen får ett bristfälligt skydd alternativt att dyra och omständliga säkerhetsåtgärder införs som inte motsvarar värdet på informationen som hanteras.

Intraservice är Stadens centrala leverantör av digital infrastruktur och digitala tjänster och hanterar därmed information som är av stor vikt inte bara för myndigheten själv utan för Staden som helhet. Det är förvaltningens bedömning att en systematisk och robust metodik för informationsklassning gynnar både Intraservice och Staden i informationssäkerhetsarbetet och i förlängningen Stadens möjlighet att leverera trygga och säkra tjänster till medborgarna.

Utan en standardiserad metodologi för informationsklassning riskerar Intraservice att ha svårt att uppfylla kraven i stadens styrande dokument samt kommande cybersäkerhetslagstiftning (NIS2-direktivet).

Behovet av styrning och förtydligande på nämndnivå är angelägen med tanke på Intraservices särställning som tjänsteleverantör till övriga Staden. Det blir därför viktigt att kunna särskilja på den information som Intraservice hanterar åt andra och därför inte är informationsägare av och den information som Intraservice innehar informationsägarskap för.

För att säkerställa att informationsklassning sker på ett likartat sätt inom förvaltningen är det nödvändigt att utarbeta detaljerade rutiner för hur informationsklassning ska genomföras. En hög detaljeringsgrad i rutiner för genomförandet leder till att bestämmelserna periodvis behöver förändras i syfte att vara uppdaterade med systemstöd, lagar, styrdokument etc.

Förvaltningen bedömer därför att nämnden bör fördela mandat att fastställa detaljerade rutiner för informationsklassningens genomförande till Intraservices CISO.

Stina Hall Hellqvist	Peter Söderström
Avdelningschef	Förvaltningsdirektör