



Projektplan

*Informationssäkerhet i system av
samhällsviktig karaktär*

Informationssäkerhet i system av samhällsviktig karaktär

Stora delar av stadens informationsflöde hanteras med hjälp av it-system och integrationer dem emellan. Informationssäkerhet innebär att upprätthålla informationens tillgänglighet, riktighet och konfidentialitet. Brister i informationssäkerheten kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas.

Stadens samhällsfunktioner är beroende av informationsteknologi för att kunna fungera. Olika tekniska system är dessutom beroende av varandra eller sammankopplade, vilket utgör en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som är svåra att förutse och hantera. It-baserade industriella styrsystem kan effektivisera verksamheterna men samtidigt innebära ökade säkerhetsrisker. Haveri eller intrång i it-systemen kan skapa stora problem och drabba både verksamhet och invånare.

Det är väsentligt att staden har ett ändamålsenligt informations-säkerhetsarbete med tillräcklig styrning, kontroll och uppföljning. Av särskild vikt är säkerheten i de system som förser befolkningen med samhällsviktiga tjänster som exempelvis dricksvatten, elektricitet och värme.

Digitaliseringen innebär möjligheter i arbetet med att utveckla stadens verksamheter. Av kommunfullmäktiges budget för 2019 framgår att: ”För att digitaliseringen ska kunna bidra till önskvärd utveckling krävs verksamhetskompetens, teknisk kompetens och omvärldsbevakning”. Det är väsentligt att kommunens verksamhetsutveckling med stöd av digitalisering och tillvaratagande av it sker på ett ändamålsenligt sätt. En ändamålsenlig it-säkerhet måste också säkerställas inom ramen för stadens digitaliseringsprocesser.

Stadsrevisionen har mot denna bakgrund fattat beslut i revisionsplanen för 2019 om att genomföra en förstudie om it-system av samhällsviktig

karaktär.¹ Informationen som sammanställts till förstudien visar att en fördjupad granskning bör genomföras av informationssäkerhetsarbetet i system av samhällsviktig karaktär.

NIS-direktivet, ny lagstiftning och regelverk avseende samhällsviktiga informationssystem

Informationssäkerhet i samhällsviktiga system aktualiseras även av ny lagstiftning. Europaparlamentet antog *direktivet för säkerhet i nätverk och informationssystem* (NIS-direktivet²) i juli 2016. Direktivet trädde i kraft 10 maj 2018 och införlivades i svensk lag genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174). Lagen kompletteras av förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lag och förordning trädde i kraft 1 augusti 2018.

NIS-direktivet innebär att särskilda krav ställs på säkerhet i nätverk och informationssystem avseende leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Med samhällsviktiga tjänster avses energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård samt leverans och distribution av dricksvatten. Kraven omfattar bland annat säkerhetsåtgärder, incidentrapportering och tillsyn. I och med den nya lagstiftningen stärks kraven på Göteborgs Stads informationssäkerhet ytterligare. Mycket av innehållet i den nya lagen har redan funnits i stadens riktlinjer men lagen medför även nya krav för stadens verksamheter.

NIS-direktivet, ovan nämnda lag och förordning samt Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter kommer att utgöra huvudkriterium i granskningen.

Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om de granskade nämnderna och styrelserna har säkerställt att informationssäkerhetsarbetet avseende samhällsviktiga system är ändamålsenligt.

¹ Ur revisionsplan för 2019

² The Directive on security of network and information systems.

Bedömningen tar sin utgångspunkt i följande revisionsfrågor:

- Bedriver nämnderna och bolagen ett systematiskt och riskbaserat informationssäkerhetsarbete avseende samhällsviktiga informationssystem i enlighet med lag, regelverk och riktlinjer?
- Har nämnderna och styrelserna vidtagit ändamålsenliga åtgärder för att säkerställa hanteringen av risker som hotar säkerheten i de samhällsviktiga informationssystemen?
- Har nämnderna och bolagen rutiner som säkerställer att styrningen, uppföljningen och kontrollen av informationssäkerhetsarbetet i de samhällsviktiga informationssystemen är tillräcklig?

Ansvarig nämnd/styrelse

I granskningen ingår Göteborg Energi AB med dotterbolagen Göteborg Energi Nät AB, Göteborg Energi Gasnät AB samt Gothnet AB, Göteborgs Hamn AB, Göteborgs kretslopp- och vattennämnd, Göteborgs trafiknämnd och kommunstyrelsen.

Revisionskriterier

- NIS-direktivet
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Kommunallag (2017:725)
- Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga system 2018:7
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8
- Myndigheten för samhällsskydd och beredskapsföreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9
- Riktlinje för informationssäkerhet – Göteborgs Stad
- Policy och riktlinjer för användning av informationsteknik inom Göteborgs Stad
- Regler gällande driftsdokumentation för it-baserade informationssystem, Göteborgs Stad

- Regler gällande informationssäkerhetsansvar för chefer i Göteborgs Stad.
- Riktlinje för hantering av säkerhetsrisker, Göteborgs Stad
- Förvaltnings/bolagsspecifika styrdokument och riktlinjer
- Grundläggande it-säkerhetsåtgärder – en vägledning, MSB
- Metodstöd systematiskt informationssäkerhetsarbete, MSB.

Metod

Granskningen kommer att genomföras genom dokumentanalys av regelverk och riktlinjer. Strukturerade intervjuer kommer att genomföras med nyckelpersoner inom nämndernas och bolagens it-avdelningar och säkerhetsorganisationer samt vid stadsledningskontoret. Systemansvariga tjänstepersoner kommer intervjuas för ett till tre system som kan anses vara samhällsviktiga inom respektive nämnd och bolag. Intervjuerna och dokumentanalysen kommer att beröra det systematiska informationssäkerhetsarbetet samt följsamhet mot NIS-direktivet.

Avgränsningar

MSB har ställt upp kriterier som leverantörer ska använda sig av för att identifiera om de anses vara leverantörer av samhällsviktiga tjänster och därmed omfattas av NIS. Dessa kriterier har utgjort grund för urval av vilken verksamhet som ska omfattas av granskningen.

Urvalet har kompletterats med verksamhet som inte omfattas av NIS-direktivet, men som ändå har bedömts ha ansvar för informationssystem av samhällsviktig karaktär. När det gäller bedömningen av dessa verksamheter utifrån regelverk kommer dock inte NIS-direktivet i sin helhet tillämpas. Det avser Göteborgs kretslopp- och vattennämnd avseende distribution av dricksvatten, som bedömts lyda under säkerhetsskyddslagstiftning, Göteborg Energi AB avseende distribution av fjärrvärme samt Gothnet AB avseende stadsnät. De båda senare omfattas inte av NIS-direktivet.

Avstämning har genomförts med de myndigheter som ska bedriva tillsyn enligt NIS-direktivet. Vid avstämningen framgick att Inspektionen för vård och omsorg (IVO) kommer att bedriva tillsyn vid en av Göteborgs Stads stadsdelsnämnder. Därför kommer granskningen inte omfatta stadsdelsnämnder eller Göteborgs nämnd för Intraservice. Stadsdelsnämnderna omfattas av NIS avseende system för hälso- och sjukvård, för dessa system ansvarar nämnden för Intraservice för driften.

Granskningen kommer i mindre utsträckning beröra systemens fysiska säkerhet.

Säkerhet och sekretess

Avrapportering kan komma att ske i särskild och i begränsad form då information i rapporten kan sekretessbeläggas på grund av säkerhetsskäl. Likaså kommer systemen som granskas att avidentifieras.

Oberoende och integritet

De sakkunnigas oberoende och integritet har prövats enligt stadsrevisionens oberoendedeklaration vilken baseras på Sveriges kommunala yrkesrevisorers modell. Inga omständigheter har framkommit som kan ifrågasätta förtroendet för de sakkunnigas oberoende och integritet som granskare.

Projektorganisation

Granskningen kommer att genomföras av Cecilia Ribeiro Goncalves (projektledare), Susanne Grandin och Lisa Nöjd.

Avrapportering

Avrapportering till revisorsgruppen planeras att ske hösten 2019.

Kvalitetssäkring

Rapportens innehåll kommer att stämmas av med de granskade verksamheterna. Kvalitetssäkringen genomförs av kvalitetsansvarig för fördjupade granskningar.



Stadsrevisionen

Postadress: Box 2141, 403 13 Göteborg

Besöksadress: Stora Badhusgatan 6

Göteborgs Stads kontaktcenter: 031-365 00 00, kansli: 031-368 07 00

stadsrevisionen@stadsrevisionen.goteborg.se

www.goteborg.se/stadsrevisionen