Utlåtande 2005: RI (Dnr 034-418/2005)

Revidering av policy och regler för informationssäkerhet i Stockholms stad

Kommunstyrelsen föreslår kommunfullmäktige besluta följande

1. Förslag till policy och riktlinjer för informationssäkerhet i Stockholms stad godkänns.
2. Stockholms Stadshus AB uppmanas anta policy och riktlinjer för informationssäkerhet inom koncernen.
3. Kommunstyrelsen ges i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad.

Kommunstyrelsen beslutar för egen del – under förutsättning att kommunfullmäktige beslutar enligt ovan – följande

Stadsdirektören ges i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet för Stockholms stad.

Föredragande borgarrådet Annika Billström anför följande.

Ärendet

Stadens nuvarande policy och underliggande regler för informationssäkerhet fastställdes av kommunfullmäktige den 3 september 2001 (utl. 2001:103). Mot bakgrund av en ökad och i viss mån förändrad hotbild, den tekniska utvecklingen och inte minst stadens ambition att vara en s.k. 24-timmarskommun har ett nytt förslag till policy och riktlinjer för informationssäkerhet för Stockholms stad utarbetats.

Ärendets beredning

Policyn och reglerna för informationssäkerhet har beretts av stadsledningskontoret. Förslaget har utsänts för sakgranskning till samtliga IT-säkerhetssamordnare vid Stockholms stads bolag och förvaltningar.

Stadsledningskontoret föreslår att nuvarande policy upphör till förmån för föreslagen policy och föreslagna riktlinjer. En ökad användning av Internet, ökat informationsutbyte mellan organisationer samt tjänster innehållande för medborgare integritetskänslig information leder ofrånkomligen till att stadens riskexponering förändras. Styrning av informationssäkerhet i en organisation genom tillämpning av ett ledningssystem för informationssäkerhet ökar förutsättningarna att etablera en nödvändig skyddsnivå.

Mina synpunkter

En väl fungerande informationshantering är en väsentlig förutsättning för Stockholms stads verksamhet. För att denna skall kunna bedrivas utan allvarligare störningar måste säkerheten beaktas. Jag anser att den reviderade och föreslagna policyn för ökad IT-säkerhet är en viktig förutsättning för att uppnå en tillräckligt hög grad av säkerhet i stadens IT-baserade system. Policyn och riktlinjerna syftar till att skydda stadens informationstillgångar mot alla hot – interna eller externa, avsiktliga eller oavsiktliga. I en tid då riskexponeringen förändras i snabb takt är det också viktigt att ständigt följa upp riktlinjerna för säkerhetsarbetet.

Utöver det renodlade hotet med intrång i IT-systemen m.m. är en viktig föresats i uppbyggnaden och vårdandet av systemen att tillförlitligheten förstärks. Staden kommer självfallet inte att kunna garantera sig helt mot avbrott, men ambitionen måste vara att minimera eventuella avbrott och dess längd.

Stadens strävan att ge god service genom elektroniska tjänster kan exemplifieras genom de Internettjänster som möjliggör för medborgarna att bl.a. söka bostad, daghemsplats och boendeparkering m.m. Ett annat exempel är möjligheten för anställda att läsa sin elektroniska post och komma åt dokument via Internet-uppkoppling från valfri plats i världen. Det gemensamma för dessa nya tjänster är att frågor om säkerhet alltid aktualiseras.

I takt med den tekniska utvecklingen, exempelvis mobilitet och trådlös kommunikation uppstår också krav på nya säkerhetslösningar. Vissa delar av stadens verksamheter är mer känsliga för intrång och avbrott än andra och även detta måste beaktas i utformandet av systemen. Även utifrån detta perspektiv måste ett regelverk för säkerhet omprövas oftare än tidigare.

Avslutningsvis vill jag lyfta fram att säkerhetsåtgärder och andra insatta åtgärder måste vara ekonomiskt försvarbara, dvs. kostnaden skall stå i rimlig proportion till säkerhetsbehovet.

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

Kommunstyrelsen delar borgarrådsberedningens uppfattning och föreslår kommunfullmäktige besluta följande

1. Förslag till policy och riktlinjer för informationssäkerhet i Stockholms stad godkänns.
2. Stockholms Stadshus AB uppmanas anta policy och riktlinjer för informationssäkerhet inom koncernen.
3. Kommunstyrelsen ges i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet i Stockholms stad.

Kommunstyrelsen beslutar för egen del – under förutsättning att kommunfullmäktige beslutar enligt ovan – följande

Stadsdirektören ges i uppdrag att utfärda tillämpningsanvisningar och instruktioner för informationssäkerhet för Stockholms stad.

Stockholm den

På kommunstyrelsens vägnar:
A N N I K A B I L L S T R Ö M

Anette Otteborn

ÄRENDET

Mot bakgrund av en ökad och i viss mån förändrad hotbild, den tekniska utvecklingen och inte minst stadens ambition att vara en s.k. 24-timmarskommun har ett nytt förslag till policy och riktlinjer för informationssäkerhet för Stockholms stad utarbetats.

Bakgrund

Stadens nuvarande policy och underliggande regler för informationssäkerhet fastställdes av kommunfullmäktige den 3 september 2001 (KS utl. 2001:103).

Motivet för och avsikten med denna typ av dokument är att kommunkoncernen skall hantera säkerhetsfrågor kring informationshantering på ett enhetligt sätt och att staden skall verka för en homogen och trygg hantering av såväl integritetskänslig information som annan ur verksamhetssynpunkt väsentlig information.

I enlighet med målet för stadens e-strategi produceras idag nya elektroniska tjänster till medborgare, nya funktioner för samarbetspartners och kunder till staden samt givetvis också för stadens anställda. I takt med den tekniska utvecklingen, exempelvis mobilitet och trådlös kommunikation uppstår också krav på nya säkerhetslösningar. Ett regelverk för säkerhet måste därför idag omprövas oftare än tidigare.

Ärendets beredning

Ärendet har beretts av stadsledningskontoret. Förslaget har utsänts för sakgranskning till samtliga IT-säkerhetssamordnare vid Stockholms stads bolag och förvaltningar. Deras synpunkter har i allt väsentligt inarbetats i materialet.

Stadsledningskontorets tjänsteutlåtande daterat den 4 februari 2005 har i huvudsak följande lydelse.

Informationssäkerhet som begrepp omfattar skydd av information både när den hanteras manuellt av människor och när den behandlas och kommuniceras med hjälp av informations- och kommunikationsteknik.

Utveckling av IT-användningen, inte minst den som följer av satsningen på 24-timmarsmyndigheter, innebär stora möjligheter men ger också en dramatiskt ökad sårbarhet. En ökad användning av Internet, ökat informationsutbyte mellan organisa-

tioner samt tjänster innehållande för medborgare integritetskänslig information leder ofrånkomligen till att stadens riskexponering förändras.

Medborgare och företag ska på elektronisk väg kunna få information, lämna uppgifter, framföra synpunkter och uträtta andra ärenden på ett snabbt och enkelt sätt oberoende av tid och plats. Målet är bättre service, ökade möjligheter till insyn och delaktighet samt ett mer effektivt resursutnyttjande.

Nya tekniker såsom mobila tjänster via telefon eller handdatorer och trådlös kommunikation skapar också behov av nya säkerhetslösningar.

Styrning av informationssäkerhet i en organisation genom tillämpning av ett ledningssystem för informationssäkerhet ökar förutsättningarna till att etablera en nödvändig skyddsnivå.

En viktig ingrediens i ett sådant ledningssystem är en heltäckande och kraftfull policy samt riktlinjer och anvisningar för arbetet.

Stadens nuvarande policy och regler för informationssäkerhet fastställdes av Kommunfullmäktige 2001. Ovanstående problembild var vid det laget inte lika tydlig som idag.

Mot bakgrund av den ökade satsningen på elektroniska tjänster till medborgare, samarbetspartners och anställda samt i beaktande av den nya hotbild som växt fram har ett nytt förslag till Policy och Riktlinjer utarbetats.

Stadsledningskontoret föreslår att Kommunstyrelsen dels antar policy och riktlinjer att gälla för egen del, dels föreslår Kommunfullmäktige godkänna bilagda dokument. Därmed upphör nuvarande Policy och Riktlinjer att gälla.

Vidare föreslår Stadsledningskontoret att KS beslutar att ge stadsdirektören i uppdrag att utfärda anvisningar och instruktioner för tillämpning av policy och riktlinjer.

Sådana anvisningar, benämnda Appendix A i policydokumentet, avser områden som kommer att preciseras under våren.

Bilaga

1. Sammanfattning av innehåll i policy och riktlinjer för informationssäkerhet.
2. Policy och riktlinjer för informationssäkerhet

Bilaga 1

Sammanfattning av policy och riktlinjer för informationssäkerhet

En väl fungerande informationshantering är en väsentlig förutsättning för Stockholms stads verksamhet. För att denna skall kunna bedrivas utan allvarligare störningar måste säkerheten beaktas. Regelverket bidrar till att skydda stadens informationstillgångar mot alla hot – interna eller externa, avsiktliga eller oavsiktliga.

Nedan följer en sammanfattning av de säkerhetsföreskrifter som alla nämnder och bolagsstyrelser skall iaktta. Det ankommer på förvaltningsledningarna att se till att dessa regler följs. Säkerhetsåtgärder skall vara ekonomiskt försvarbara. Det innebär att kostnaden skall stå i rimlig proportion till säkerhetsbehovet.

Informationssäkerhetspolicy Stockholms stad

- **Stadens styrande dokument skall vara kända**

Alla skall vara medvetna om det regelverk, med eventuella lokala anpassningar, som styr informationssäkerhetsarbetet inom staden.

- **Stadens säkerhetsorganisation skall vara känd**

Det är av yttersta vikt att de roller med tillhörande ansvar som är knutna till IT-system och därtill hörande säkerhet är identifierade, tillsatta och kommunicerade.

Vid störning/avbrott skall det vara känt vem som ansvarar för vad så att IT-systemen snarast möjligt åter fungerar enligt av verksamheten ställda krav.

- **Grundnivån för säkerheten skall fastställas genom informationsklassificering**

För stadens IT-system skall alltid en av staden fastställd grundsäkerhetsnivå gälla.

För ett antal system ställs dessutom utökade säkerhetskrav utifrån legala och verksamhetsmässiga aspekter.

Informationsklassificering skall genomföras för respektive IT-system enligt en av staden fastställd metod.

- **Berörd personal skall ha nödvändiga kunskaper om aktuella IT-system samt gällande säkerhetsregler**

Personalen skall ha en sådan kunskapsnivå att misstag/felaktigt agerande vid användande av IT-system undviks.

Verksamhetschef ansvarar för att nödvändig utbildning genomförs. Det är viktigt att utbildning tillhandahålls kontinuerligt.

- ✍ **Fysiskt skalskydd skall anpassas efter genomförd riskanalys**

Åtgärder skall vidtas för att förhindra obehörigt tillträde till utrymmen där dessa informationstillgångar finns. Vilket skalskydd, dvs fysiskt skydd, som skall gälla fastställs med hjälp av riskanalys.

- ✍ **Skriftligt godkänt SLA/motsvarande skall finnas före driftsättning**

SLA (Service Level Agreement) är ett avtal om den servicenivå som IT-driften skall leverera till verksamheten. Avtalet beskriver vad som reglerats mellan parterna i form av tillgänglighet, ändringsintervall, säkerhetskopiering etc.

SLA/motsvarande upprättas mellan systemägare och IT-ansvarig.

- ✍ **Åtkomst/behörighet skall tilldelas formellt och endast efter behov samt följas upp regelbundet**

Den som, för att kunna utföra sina arbetsuppgifter, har behov av åtkomst till IT-system skall tilldelas aktuell behörighet. Inga andra skäl finns för behörighetstilldelning.

Systemägarrepresentant fastställer behörighetsnivåer för systemet. Tilldelning av användarkonto sker enligt gällande anvisningar.

- ✍ **Säkerhetsaspekter skall beaktas vid utveckling och anskaffning av IT-system**

Vid systemutveckling/-anskaffning skall särskild vikt läggas vid att tidigt ange säkerhetskraven. Detta uppnås genom att informationsklassificera systemen, kompletterat med riskanalyser.

- ✍ **Uppfyllnad av rättsliga krav skall tillgodoses i alla IT-system**

Stadens informationshantering styrs av ett antal lagar och förordningar såsom Tryckfrihetsförordningen (offentlighetsprincipen) Personuppgiftslagen, Sekretesslagen, m.fl.

Huvudregeln i de flesta verksamheter är att informationen skall vara tillgänglig för allmänheten. I samband med informationsklassificering undersöks vilka lagar som är tillämpliga och hur säkerhetskraven uppfylls.

- ✍ **En kontinuitetsplan och en avbrottsplan skall finnas för verksamheter med starkt beroende av IT-system**

En kontinuitetsplan skall dokumentera verksamhetens åtgärder vid allvarliga störningar i datorstödet.

En avbrottsplan skall dokumentera IT-driftens åtgärder för att återställa IT-stödet till normalt driftläge enligt gällande SLA. Det är viktigt att dessa planer årligen testas och följs upp.

- ✍ **Alla incidenter skall rapporteras och kontinuerlig uppföljning skall ske mot fastställda regler**

Alla användare skall snarast möjligt rapportera incidenter och säkerhetsmässiga svagheter (försök till dataintrång, manipulering av information etc) så att nödvändiga åtgärder kan vidtas för att minimera skada i IT-miljön.

Rapportering skall ske till säkerhetssamordnaren i egen organisation och stadens system för incidentrapportering skall användas.