Bilaga 7 till kommunfullmäktiges protokoll 2004-10-18 **§ 19**

Svar på interpellation 2004:31 av Fredrik Wallén (kd) om stadens IT-säkerhet

Interpellanten har ställt ett antal frågor som berör stadens IT-säkerhet. Det handlar bl.a. om vilka åtgärder som staden har vidtagit för att förhindra att framtida t.ex. datavirus och maskar inte ska kunna få lika stor spridning i stadens datorer. Interpellanten undrar också om staden följer kommunfullmäktiges fastställda IT-säkerhetspolicy.

Det är ett antal viktiga frågeställningar interpellanten lyfter fram och därför har jag valt att mer utförligt besvara frågorna samt redogöra för händelseförloppet. Det är av värde att denna information kommer så många som möjligt till del inom stadens verksamheter.

Bakgrund

Tisdagen den 5 maj 2004 mellan klockan 12.30 – 12.45 drabbades Stockholms stad av Sasser. Den omedelbara effekten var att trafiken blev långsam, speciellt Internet-accessen, och att ett stort antal datorer slogs ut. Utslagningen innebar att datorerna startade om, gick ned och startades om automatiskt.

Det visade sig att Sasser angrep ett av Microsoft känt publicerat säkerhetshål för operativsystemen Windows 2000 och Windows XP. Publiceringen av detta och av anvisade motmedel, s.k. säkerhetspatchar, skedde den 13 april 2004. Virusdefinitioner för att stoppa Sasser fanns tillgängliga, men de kunde inte fungera i efterhand utan måste vara förinstallerade för att motverka Sasser.

Stadens policy är att inte lägga på säkerhetspatchar innan de testats för eventuell negativ påverkan av IT-miljön. Staden var således fortfarande sårbar för de brister som påtalats innan denna genomgång och test genomfördes. Av stadens datorer blev ca. 3-4000 påverkade av viruset.

IT-avdelningens personal påbörjade felsökning och produktion av rensningsverktyg så snart diagnosen var fastställd. Virusdefinitioner uppdaterades i takt med att rensningsarbetet pågick. Ett bekymmer som upptäcktes tidigt var att (i de flesta fall) rensningen måste utföras på plats i varje enskild dator och således fick man bränna CD-skivor med verktygen för distribution.

Information till stadens förvaltningar skedde via Ementors helpdesk med hjälp av telefon då datoråtkomsten var oklar i första skedet. En krisledningsgrupp formerades bestående av IT-chefen, kommunikationsansvarig, tekniker och informationssäkerhetschefen, samtliga vid stadsledningskontorets IT-avdelning. Till gruppen fördes också resurser från Stokab och Ementor samt representant för Information Stadshuset. Information som insamlades vid mötestillfällena spreds såväl internt som externt via kanalerna webb, intranät, fax och mail. Informationsansvaret var fördelat på flera personer inom gruppen.

I anslutning till ovan beskrivna incident upptäcktes ett nytt allvarligt mjukvarufel i stadens kommunikationstjänst. Mjukvarufelet i denna tjänst komplicerade och försvårade ett snabbt och relevant beslutsfattande. Den inrättade krisgruppen tvingades till att analysera och prioritera dessa två allvarliga incidenter samtidigt för att säkerställa stadens IT-stöd för verksamheten.

Påverkan för stadens kärnverksamhet

Inledningsvis fanns farhågor för att socialtjänstens verksamhetssystem Paraplyet och dess utbetalningsrutin skulle påverkas, men dessbättre visade det sig inte vara fallet i någon större omfattning. Inga indikationer på att någon kärnverksamhet blivit allvarligt lidande har funnits. I viss utsträckning störddes emellertid socialtjänstens jourförbindelser i samband med det utdragna ADSL-problemen. Det var uppdatering och informationssökning i journalsystem som inte fungerade, men några stora konsekvenser har inte meddelats.

Åtkomst till vissa av ID-portalens tjänster var inte heller möjlig under en tid vilket påverkade access till bland annat Bostadsförmedlingens webtjänst. Detta avbrott var dock av kortare karaktär och inga större konsekvenser har rapporterats. Driften av de centralt avtalade servrarna påverkades ej men åtkomsten till dessa blev begränsad på grund av ökad belastning av kommunikationstjänsten.

De främsta störningar som inträffat verkar således ha drabbat det administrativa arbetet (normalt kontorsarbete) som bedrivs inom staden.

Identifierade problem och åtgärder

Ett antal problem har identifierats i samband med denna händelse. Det kan dock konstateras att ingen enskild person har brustit i ansvar eller aktion, utan generellt kan bristerna i stor utsträckning hänföras till systematiska oklarheter. Bristerna som orsakade virusintrånget är av olika karaktärer, men inte på något vis omöjliga att åtgärda. Det rör sig främst om följande.

a) organisatoriska brister,
b) rutinmässiga brister,
c) tekniska brister.

För att utreda ovanstående problematik och för att vidtaga åtgärder som stärker stadens säkerhet inför framtiden har en grupp bestående av representanter från stadsdelsförvaltningar, fackförvaltningar och bolag tillsatts. Sammankallande för gruppen är stadens IT-säkerhetschef. Gruppen skall redovisa förslag till ytterligare åtgärder under september 2004.

En krisledningsorganisation har etablerats inom IT-avdelning dels för att förebygga att nya virusangrepp kan åstadkomma motsvarande problem, dels för att i en akut situation snabbt kunna sammankallas för att samordna insatser och snabbt ge korrekt information om vad som inträffat och vilka åtgärder som skall vidtas. Gruppen består av företrädare för IT-avdelning, Stokab, Information Stadshuset samt företrädare för berörda IT-företag och i förekommande fall de förvaltningar som är särskilt berörda.

Krisledningsorganisationens rapporterar till kommunledningen och lämnar information till förvaltningar och bolag, medborgare/näringslivet och massmedia. I samband med etableringen av krisledningsgruppen har en översyn inletts som beaktar eventuella behov av samordning med stadens övergripande krisledningsorganisation. IT-avdelningen kommer också att strama upp rutinerna för hur och när och av vem information om nya patchar skall lämnas.

En betydande risk för att få in virus i systemet är när anställda kopplar in sina bärbara datorer i näten om dessa inte skyddats tillräckligt genom virusprogram eller brandväggar när de används utanför det fasta nätet. Det behövs därför ökade kunskaper i grundläggande datorhandhavande. Var och en som använder en dator som används både i och utanför nätet måste försäkra sig om att han eller hon har tillräckliga kunskaper om vilka skyddsåtgärder som skall vidtas.

Alla förvaltningar och bolag har IT-säkerhetsansvariga. De säkerhetsansvariga har en viktig betydelse för skyddet lokalt och att tillräckliga säkerhetsåtgärder vidtas inom de olika förvaltningarna. De har också ett ansvar vad gäller att informera och utbilda berörda anställda inom respektive förvaltning i grundläggande datorsäkerhet.

Den nya tekniken gör stadens och många andras verksamheter sårbara. Vi kan vara förvissade och säkra på att nya virusattacker kommer att komma även i framtiden. Min bedömning utifrån den senaste attacken är att de åtgärder som stadsledningskontoret vidtagit är tillräckliga för att förbättra beredskapen inför nya datavirushot.

2004-06-11

Annika Billström
Finansborgarråd