IT-kommissionen

Anne-Marie Eklund Löwinder
tel 08-405 33 67

Dnr 2001/39
2001-04-03

Till Justitiedepartementet

Grundskydd i datorer och programvaror

I spåren av den snabba tillväxten av mängden hushåll som har dator och tillgång till fast Internetanslutning krävs åtgärder när det gäller att möta de säkerhetsrisker som sådana anslutningar för med sig. Genomtänkta metoder för att skapa ett ökat medvetande om risker och kunskaper om skydd behövs om vi inte mycket snart ska få problem när det gäller tillit till IT.

IT-kommissionen har givit Observatoriet för informationssäkerhet uppgiften att specificera funktioner för att åstadkomma ett grundskydd i persondatorer. Bifogade PM innehåller beskrivning av sådana funktioner och förslag till åtgärder enligt följande:

Förslag till åtgärder

IT-kommissionen anser att det i alla nya avtal för personaldatorer är rimligt att öka medvetandet om säkerhetsfrågornas betydelse och om behovet av en högre säkerhetsnivå genom att ställa krav på att varje persondator som levereras under avtalen ska levereras med:

- **samtliga nättjänster avstängda;** dvs. datorn ska inte erbjuda aktiva nätverkstjänster (t.ex. utskrift, fildelning, m.m.) som grundinställning. Det innebär att inte heller någon annan kan dra nytta av tjänster som användaren inte vet om att de finns eller medvetet har slagit på. Konsekvensen av att sådana tjänster redan är påslagna vid leverans är t.ex. att informationen i datorn görs tillgänglig för andra som den inte är avsedd för utanför användarens kontroll.

- **nättjänster som är robusta och motståndskraftiga mot attacker;** de tjänster som aktiveras ska inte kunna missbrukas eller manipuleras från nätet. Om det inte görs så kan andra nätanvändare sabotera en dator utifrån, från nätet.

- **enkla funktioner för att aktivera nättjänster och konfigurera behörighet för de som har rätt att använda dessa;** om det inte görs så är det stor risk för att användaren antingen inte kan använda de tjänster denne vill eller att man öppnar

okontrollerat och gör datorn tillgänglig för andra utanför användarens kontroll.

- **möjlighet att separera olika användare;** säkerhetsfunktioner måste ställas i relation till vilka applikationer och tjänster som används. Om åtkomstbegränsningar inte kan vara grundade på individ, dvs. lämpade för att tillåta en användare att skydda personlig information, är risken uppenbar att olika familjemedlemmar kan läsa eller förstöra varandras information.

- **anti-virusprogram med möjlighet till automatiska uppdateringar;** annars löper man stor risk att datorn blir virusinfekterad. Nya virus utvecklas hela tiden, och anti-virusprogrammen kan bara ligga i hälarna på den utvecklingen, men knappast före. Virusangrepp kan ha en rad negativa konsekvenser från att datorn blir helt förstörd, till att man i och med avsaknaden av skydd medverkar till att andra får sin information eller sin dator förstörd.

- **applikationer som inte automatiskt och utan föregående varning exekverar program som kommit in via nätet;** på det sättet går det exempelvis att undvika att ett program som dolts i ett e-postmeddelande skickar sig själv till alla mottagare i den egna adressboken.

- **funktioner för säkerhetskopiering;** trots skyddsåtgärder kan man drabbas av förlust av all information och programvara på datorn, t.ex. vid hårdvarufel, virusangrepp m.m. Då är det viktigt att kunna återställa datorn och återskapa informationen.

- **beskrivning (och hänvisningar) så att en användare via datorn enkelt kan ta del av information om relevanta IT-säkerhetsproblem;** en sådan åtgärd bidrar till att skapa ett ökat medvetande om risker och kunskaper om skydd.

Uppdrag till Statskontoret

IT-kommissionen anser att regeringen bör ge Statskontoret i uppdrag att formulera och föra fram krav till leverantörer på förinstallerade säkerhetsfunktioner enligt ovan. Samtidigt bör man fästa uppmärksamheten på behovet av sådana funktioner hos samtliga som har ett ansvar för upphandling av personaldatorer inom både näringsliv och offentlig förvaltning. Internetoperatörer bör också kunna redogöra för vilka funktioner de kan erbjuda för att motverka att användare drabbas av incidenter som t.ex. datavirus, intrång eller andra företeelser vid upphandling av Internettjänster.

eEurope

Regeringen bör uppmärksamma den europeiska kommissionen på att man måste beakta dessa frågor i arbetet med eEurope och i den fortsatta utvecklingen av åtgärdsplanen ”eEurope2002”.

För IT-kommissionen

Christer Marking

Kopia till Näringsdepartementet