KOMMISSIONEN

OBSERVATORIET FÖR
INFORMATIONSSÄKERHET

Grundskydd i datorer och programvaror

PM Observatoriet för Informationssäkerhet 1:2001

Inledning

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 och användningen av Internet.

Säkerhet i form av integritet för individen är det grundläggande kravet, men det kravet måste balanseras mot krav på funktion och transparens i tjänsteutbudet. Systemen ska fortfarande vara lätta att använda, den höjda säkerheten till trots. Andra parametrar är krav från operatörerna på låga kostnader för drift och flexibilitet i kontakter med slutanvändare, vilket bäst tillgodoses genom en hög grad av självadministration från användarens sida.

Ett grundskydd för datorer som motsvarar användarnas krav på leverantörer och återförsäljare av datorutrustning (främst persondatorer) måste specificeras. Information om individsäkerhet, dvs. användarnas möjligheter och ansvar, måste göras enkel, tillgänglig och lättfattlig. Det finns ett stort behov av att höja IT-säkerhetsmedvetandet överlag i det svenska samhället.

I takt med att användaren förstår och lär sig säkerhetsaspekterna kan denne själv öppna och göra funktioner tillgängliga som i högre grad ger andra åtkomst till det egna systemet, men under kontrollerade former.

IT-kommissionen har givit Observatoriet för informationssäkerhet till uppgift att specificera funktioner för att åstadkomma ett grundskydd i persondatorer.

Regeringens IT-proposition

I IT-propositionen (proposition 1999/2000:86) har regeringen prioriterat uppgifter som innebär att staten ökar

- tilliten till IT,
- kompetensen att använda IT samt
- tillgängligheten till informationssamhällets tjänster

med syfte att skapa ett informationssamhälle för alla.

Hemdatorsatsningen

1998 infördes skattelättnader som innebar att man underlättade för arbetsgivare att låta anställda hyra datorer för att utbilda sig och skaffa sig datorvana på fritiden och i sin egen takt. Detta har bidragit till att Sverige snabbt kommit att bli världsledande när det gäller antal datorer per hushåll.

I slutet av 1998 fanns en persondator i mer än 50 % av hushållen. Merparten av dessa maskiner var utrustade med modem och möjligheter till Internetanslutning. En senare undersökning visar att 67 % av hushållen hade persondator vid utgången av 1999. Siffror för år 2000 visar att andelen nu är större än 70 %.

Samtidigt får allt fler hushåll via sitt boende tillgång till fast anslutning till Internet, till en fast och ofta låg kostnad och med relativt hög kapacitet (jämfört med vanlig modemanslutning).

I takt med den tillväxten ökar också mängden samtal med frågor och klagomål från användare som konstaterar att en fast anslutning till nätet, med hög kapacitet, också har gjort dem öppna för åtkomst från andra. Mängden intrång och intrångsförsök ökar.

Under den närmaste tiden kommer en hel del avtal, såväl nya som förnyade, att tecknas om köp av personaldator. Datorleverantörerna ser fram emot en ny PC-boom under 2001 och har förväntningar på att man kommer att sälja omkring 300 000 enheter, till ett värde motsvarande ca 6 miljarder kronor.

Det fast och ständigt uppkopplade hemmet ger stora möjligheter till insyn i människors privatliv (och i värsta fall också företagshemligheter). Kraven på operatörer och leverantörer att leverera produkter och tjänster med hög säkerhet har så här långt inte varit särskilt uttalade. Hos dessa har oftast andra överväganden, som t.ex. att snabbt skaffa marknadsandelar, fått dominera. Olika aktörer konkurrerar om marknadsandelar i huvudsak med pris och tjänsteutbud. En konsekvens av detta är att vi får produkter och tjänster som saknar genomtänkt säkerhet. Säkerhet är ännu inte något försäljningsargument.

Informationssäkerhet är kritiskt

Det är alltid en svår uppgift att i tider av pionjäranda och entreprenörskap lägga sordin på stämningen och tala om säkerhet och integritet. Det finns emellertid en uppenbar risk att om vi inte möter frågeställningarna nu så kommer ingen att efterfråga de tjänster som verkligen kommer att underlätta tillvaron för många av oss.

När bandbredden till och från användarna ökar och datorn ständigt är uppkopplad ökar risken för oupptäckta intrång.

Hushållen, dvs. användarna, kan inte förväntas bära hela ansvaret för att hantera säkerheten i den egna datorn. Den pågående och allt snabbare datoriseringen av svenska hushåll förstärker säkerhetsproblemen. En persondator med fast anslutning och relativt hög kapacitet får inte bara tillgång till Internet och de tjänster som nätet förmedlar, den görs också tillgänglig utifrån. En av de bakomliggande orsakerna till detta är att de vanligaste operativsystemen ur säkerhetssynpunkt är svaga.

En paradox i sammanhanget är att dagens dator- och Internetanvändare blir allt kunnigare i att använda möjligheterna hos tekniken samtidigt som de blir alltmer ovetande om den bakomliggande tekniken och om hur den egentligen fungerar.

Det finns inte bara en risk för att datorerna och dess innehavare själva attackeras av någon eller något. Den högre bandbredden relativt uppringda anslutningar, medför också en större risk för

att det egna systemet kan utnyttjas för att utgöra en bas för vidare attacker, t.ex. distribuerade dos-attacker (DDOS). (Se Observatorierapport nr 23/2000)

Säkerhetsproblem

Med hemdatorerna följer ett varierande utbud av förinstallerade tillämpningar och programvaror. Dessa levereras ofta utan att man kunnat täppa till olika säkerhetshål, eftersom dessa många gånger upptäcks efter det att installationerna genomförts. Förekomsten av dominerande leverantörer gör att deras produkter också är attraktiva måltavlor för angrepp av olika slag. En orsak till detta är att angrepp som utnyttjar ett säkerhetsproblem i en spridd programvara får mycket stor effekt. Ytterligare ett problem är att gamla versioner av programvaror får vara i bruk för länge, då användaren i dagsläget förväntas att själv kunna ta reda på var rättelser och uppdateringar finns, och hur de ska installeras.

Det finns en rad säkerhetsproblem förknippade med användningen av elektronisk kommunikation, där ett av de grundläggande är att mycket kommunikation sker i klartext. Grovt kan problemen grupperas som:

Avlyssning: Information mellan två kommunicerande datorer kan avlyssnas från en tredje nätverksansluten persondator (t.ex. hos grannen) utan att detta kan upptäckas av sändande eller mottagande system. Risken att bli avlyssnad ökar om näten byggs med fel teknik.
Modifiering av överförd information: En angripare förändrar den information som överförs på nätet utan att detta upptäcks hos den mottagande parten.
Otillbörligt utnyttjande av resurser: I och med att det inte finns något tillräckligt skydd mot att en person på nätet kopplar upp sig mot någon annans system kan det användas för att t.ex. göra dataintrång någon annanstans.

Internet är byggt efter principen ”alla ska kunna nå alla med allt”. Så fort man är ansluten till Internet är man också en del av Internet. Där användaren kan komma åt Internet kan Internet komma åt användaren. Samma teknik och protokoll används både internt i datorn för att kunna dela på skrivare, dokument eller annat och externt vid överföringar på Internet. I många fall finns möjlighet för andra att utnyttja tjänster som användaren kanske inte ens känner till att de existerar och är aktiva, som exempelvis möjligheter till fjärrinloggning.

Nätet förmedlar endast information mellan avsändare och mottagare. Nätet kan inte göra den elektroniska kommunikationen säker, det måste ske i ändarna, i datorerna ute hos varje ansluten användare.

Även om det finns många säkerhetsprodukter att tillgå – olika typer av brandväggar, intrångslarm, antivirusprogram, filterfunktioner – kan det vara ett problem att ju tätare man gör datorer och anslutningar desto mindre tillgängligt blir nätet och tjänsterna och användbarheten går förlorad. Risken är därmed också stor att användarna hoppar över den delen, i synnerhet om de inte får handfast vägledning och blir motiverade till att vidta erforderliga säkerhetsåtgärder.

Därför krävs ett mycket målmedvetet arbete och investeringar för att ge användare möjlighet att skydda sig mot virus, blockering av tjänster, förvanskning och avlyssning av information eller intrång.

Problemen är inte nya, men de har inte uppmärksammats i någon större omfattning då det vanligaste anslutningssättet fortfarande är att ringa upp via modem. Datorer med uppringd förbindelse till Internet tilldelas ett IP-nummer (som är datorns adress på Internet) varje gång man ringer upp. Därför blir också adressen olika för varje gång. Även om någon lyckas göra intrång i en dator under en uppringd session hittar denne någon inte med automatik tillbaka till samma dator nästa gång användaren ringer upp. Oftast varar förbindelsen inte så länge att en angripare hinner åstadkomma något större problem. Dessutom är överföringshastigheten i en uppringd förbindelse så låg att det är tämligen ointressant att angripa datorer anslutna på det sättet.

Den ökade mängden persondatorer i hemmen och den öppna kommunikationsarkitekturen i kombination med fast anslutning med hög kapacitet skapar en förändrad hotbild. Den nya hotbilden skapar i sin tur behov av ett ökat säkerhetsmedvetande och vissa generella säkerhetslösningar för att undvika att användarnas tillit till IT undergrävs. Detta kommer att ställas på sin spets för den marknad som förväntas komma när det gäller hemmen. Vem ska skydda den dator eller det kylskåp som står i ständig kontakt med nätet? Är det användaren, operatören, datortillverkaren, kylskåpsleverantören eller programtillverkaren?

Svaret på den frågan är att tyngdpunkten i säkerhetstänkandet när det gäller Internet alltid ligger i ändutrustningen, även om en del stöd kan finnas inbyggt i nätet som skyddar mot de mest uppenbara misstagen eller rent oförstånd. Samtidigt är det orealistiskt att tro att vi ska kunna få användare mycket intresserade av säkerhetsfrågor, och framför allt att få dem så intresserade att de lär sig utföra säkerhetsfrämjande åtgärder helt och hållet på eget initiativ. Faktum är att de flesta aldrig kommer att vare sig kunna eller vilja veta tillräckligt mycket om den bakomliggande tekniken för att t.ex. konfigurera ett operativsystem. Det ska inte heller vara nödvändigt. Säkerhetskrav behöver därför formuleras som motsvarar riskbild och skyddsbehov hos ett normalhushåll.

Möjliga lösningar

Kunskapen om den grundläggande Internettekniken är mycket spridd. Det finns ett stort behov av en precisering av hur programvaror och system ska vara beskaffade vid leverans, och att detta också innefattar anvisningar för hur olika funktioner i t.ex. operativsystem ska användas. Det behövs en beskrivning av en standardmiljö för hushållens Internetanslutning med syfte att påvisa och åtgärda säkerhetsfrågorna. Det behövs dessutom verktyg som ger användare säkrare system, och som tillåter en över tiden bibehållen säkerhetsnivå. Dessa åtgärder behöver givetvis också kombineras med ökade kunskaper om risker och skydd.

Ingående komponenter

Komponenter som bör ingå i en standardmiljö är:

- Användaridentifiering och behörighetskontroll
- Brandväggsfunktion och filter
- Funktioner för säkerhetskopiering
- Funktioner för kontroll av åtkomst till nättjänster från datorn
- Virusskydd, och funktioner för uppdatering av virusskydd

Var och en av dessa komponenter beskrivs något utförligare nedan.

Användaridentifiering och behörighetskontroll

Separation av användare och information kan behöva göras även hemma. Åtkomstbegränsningen ska helst vara grundad på individ, dvs. den ska vara lämpad för att tillåta en användare att skydda personlig information och hindra andra från att läsa eller förstöra information. Svårigheten är att detta inte går att implementera i våra vanligaste operativsystem, som inte är utrustade med något system för behörighetskontroll eller filskydd. Funktionen behövs, men det måste finnas något enkelt sätt att realisera den. Ett sätt är att låta förinstallera tilläggsprogram som ger funktioner av typen ”krypterad disk med personlig åtkomst”.

Noteras bör att det kan bli ett växande problem att många använder hemdatorn för åtkomst till sitt arbete. Det är samtidigt svårt att se hur en hemdator skall kunna användas både för roliga applikationer (spel, chatt, etc.) och för att komma åt arbetet, utan att säkerhetsproblem uppstår. Det går inte att lösa genom generella regler. Villkoren och förutsättningarna för hemarbete måste hanteras av varje enskild arbetsgivare.

Vid åtkomst till externa system, finns det ett generellt behov av starkare identitetskontroller än vanliga lösenord, som t.ex. engångslösen, elektroniska certifikat, dosor och liknande lösningar.

Personliga brandväggar

Mot risken för att användarna ska uppfatta säkerhetsåtgärderna som hindrande talar en växande marknad för "personliga brandväggar" (eng.: personal firewall). I dagsläget finns det ett antal användbara produkter. Några av dessa visar faktiskt på att det går att få ett mycket bra skydd (på nätnivå) utan att det behöver bli vare sig jobbigt eller tråkigt att använda Internet.

Rätt använda kan personliga brandväggar lösa följande problem:

- Skydd av TCP/IP-program (själva implementeringen av nättjänster skyddas).

Visst skydd av tillämpningar kan åstadkommas i och med att dessa inte är direkt åtkomliga från nätet. Vanligtvis kan en brandvägg emellertid inte skydda själva tillämpningsprotokollet, så det stora hotet finns kvar, som t.ex. att e-postklienten under vissa förutsättningar automatiskt startar en exekverbar bilaga. Detta kan en brandvägg påverka endast till en viss del. En brandvägg kan inte heller hantera trafik över krypterade kanaler.

Användaren kan välja vilken typ av tjänster denne vill att brandväggen ska släppa igenom och dessutom låta filtret slå larm om något oväntat eller misstänkt inträffar, enligt de regler som användaren själv matar in.

Generellt kan en personlig brandvägg ge **en viss del** av det skydd som behövs. Genom att förhindra generell åtkomst till maskinen, samt kontrollera också utgående trafik, skapas en form av grundskydd på nätverks-/sessionsnivå, vilket i alla fall utgör en hygglig bas.

Behovet av brandväggar bottnar i att det finns brister i de program vi använder. Om alla tjänster på alla datorer utförde tillräckliga kontroller och var korrekt implementerade så skulle det inte behövas brandväggar.

Funktioner för säkerhetskopiering

Funktioner för säkerhetskopiering är något som måste ingå i grundsäkerheten, tillsammans med funktioner för att återskapa data från en kopia, och en exakt beskrivning av hur detta går till (behöver man installera om operativsystemet, hur säkerhetskopior förvaras, etc.). Det går inte att helt försäkra sig mot att det inträffar något som gör den egna informationen otillgänglig eller opålitlig på ett eller annat sätt. Endast genom att ha tagit regelbundna säkerhetskopior kan man återskapa informationen så nära identisk som möjligt med hur den såg ut vid tiden för en händelse.

Funktioner för kontroll av åtkomst till nättjänster från datorn

Datorn ska levereras så att det inte finns några nättjänster påslagna från början (utgående tjänster, servertjänster, osv.). Givetvis finns det både behov och intresse av att köra sådana tjänster, t.ex. för att publicera egna bilder och för att andra ska kunna komma åt information lagrad på den egna datorn (förmodligen efter krav på identifiering). När användaren exempelvis aktiverar tjänster som http-server, exportera (dela) mapp eller något annat ska det finnas något konkret och lättfattligt sätt att specificera vilka som ska kunna göra vad, som t.ex. ”information som kan publiceras utan restriktioner”, ”information läsbar för följande personer”.

Virusskydd och funktioner för uppdatering av virusskydd

Med tanke på att risken för att smittas av datavirus är överhängande, och med tanke på det besvär datavirus kan ställa till med så bör man försöka förhindra att den egna datorn blir smittad.

När det gäller skydd är det fråga om

- att förebygga att datorn över huvud taget blir smittad,
- att upptäcka ett datavirus och förhindra smittspridning,
- att återställa ett smittat system.

Det effektivaste är förstås att undvika att bli smittad och det är därför främst de förebyggande åtgärderna som ska prioriteras. Men ibland hjälper inte det, och då måste man också ha en plan för hur man ska gå tillväga om olyckan skulle vara framme.

I det sammanhang vi nu talar om, grundsäkerhet i persondatorer, är det ett krav att varje persondator ska vara utrustad med ett installerat och aktiverat virusskydd som uppdateras kontinuerligt och automatiskt.

Upplysning om risker och IT-säkerhet

Vad behöver användaren känna till och varför? IT-kommissionens uppfattning är att det behövs allmänt formulerade råd i säkerhetsfrågor till alla som använder datorer och Internet. Exempelvis bör man undvika att hämta program eller filer från okända platser på Internet, man bör ha minst 8 tecken i lösenordet och man bör undvika lösenord som är lätta att gissa eller som kan finnas med i ordböcker. Användarna bör känna till att all e-posttrafik kan avlyssnas, att de inte bör skicka information utan kryptering, att själv signera och kräva signatur på information som man vill förvissa sig om inte kan förvanskas utan att det upptäcks, osv.

En sådan enkel handbok bör vara tillgänglig elektroniskt och följa med varje dator eller Internetuppkoppling. Det kan givetvis inte ställas några krav på att den ska vara heltäckande, men den bör vara tillräckligt informativ och vara försedd med referenser till andra källor för mer information.

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 om hem-PC ska levereras med:

- **samtliga nättjänster avstängda;** dvs. datorn ska inte ha nätverkstjänster (t.ex. utskrift, fildelning, m.m.) aktiva 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 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.

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 de 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.

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