Communication to the Swedish Government from the Swedish ICT Commission Concerning

Basic protection in computer hardware and software

The Observatory for Information Security
PM 1:2002
Basic protection in computer hardware and software

In the wake of the rapid growth in the number of households with computers and access to a “always on” Internet connection, measures are needed to counteract the security hazards which connections of this kind entail. Cogent methods for creating greater awareness of risks and knowledge of protection are needed, or else we will very soon run into problems of IT reliance.

The IT Commission has tasked its Observatory for Information Security with specifying functions for achieving basic protection in personal computers. The enclosed memorandum contains a description of such functions and measures proposed as follows:

Measures proposed

The IT Commission considers it reasonable that all new contracts for personal computers should raise the level of awareness concerning the importance of security issues and the need for a higher level of safety by stipulating that every personal computer delivered under the contracts shall be delivered with:

- all web services shut off, i.e. the computer shall not offer active web services (e.g. printout, file division etc.) as a default setting. This means that no one else will be able to benefit from services which the user does not know about or has not deliberately turned on. The consequence of such services already being turned on at delivery is, for example, that information in the computer is made available to others for whom it is not intended, outside the user’s control.

- web services which are robust and resistant to attacks; the services activated must not be amenable to abuse or manipulation from the web. Otherwise other web users can sabotage a computer from outside, from the web.

- simple functions for activating web services and configuring authorisation for those entitled to use them; failing this there will be a serious risk of the user either not being able to use the services he wants to or of his opening without control and making the computer accessible to others over whom the user has no control.

- the possibility of separating different users; security functions must be viewed in relation to the applications and services used. If access limitations
cannot be based on an individual, i.e. adapted to allow a user to protect personal information, then there is an obvious risk of different members of the family being able to read or destroy each other’s information.

- **anti-virus programs with the possibility of automatic updating;** otherwise there is a serious risk of the computer becoming infected with a virus. New viruses are being developed all the time, and anti-virus programs can only follow hard on the heels of that development, they cannot really anticipate it. Virus attacks can have a number of negative consequences, from completely wrecking the computer to the user, for lack of protection, contributing towards the destruction of other people’s information or computers.

- **applications which will not automatically and without prior warning execute programs which have come in through the web;** in this way it is possible, for example, to prevent a program concealed in an e-mail letter sending itself to all recipients in the user’s address book.

- **back-up functions;** protective measures notwithstanding, it is possible for all information and software in the computer to be lost, e.g. in the event of a hardware fault, virus attack etc. If so, it is important to be able to repair the computer and restore the information.

- **description (and references) so that, from the computer, a user can easily access information about relevant IT security problems;** a measure of this kind will help to create greater awareness of risks and greater knowledge about protection.

**Remit to the Agency for Administrative Development**

The IT Commission finds that the Government should commission the Agency for Administrative Development to formulate and communicate to suppliers demands concerning pre-installed security functions as per the above. At the same time, the need for such functions should be drawn to the attention of everyone responsible for PC procurement in both business enterprise and public administration. Internet operators should also be able to give an account of the functions they can offer to prevent users being affected with such incidents as computer virus, encroachment or other phenomena in connection with the procurement of Internet services.

**eEurope**

The Government should alert the European Commission to the imperative necessity of taking these questions into consideration in the course of work on eEurope and in the ongoing development of the action plan “eEurope2002”.

On behalf of the IT Commission,

Christer Marking
Basic protection in computer hardware and software

- summarised background to the communication to the Swedish Government from the Swedish ICT Commission

Summary

The proposed basic protection in computers should include requirements for suppliers of computer hardware (PCs above all) to deliver them with

1. a function control facility,
2. functional manuals with a warning text,
3. information on security questions,
4. reference to security products.

The question has an EU aspect and should be amenable to discussion within the framework of eEurope.

The problem

Within the near future, quite a number of contracts, both new and renewed, will be signed for purchases of home PCs in Sweden. Households/users cannot normally bear the full responsibility for security management within their own computer. The ongoing and accelerating computerisation of Swedish households is accentuating the problems of security. A personal computer that is always connected and has a relatively high capacity not only has access to the Internet and the services it provides but is also made accessible from outside. One of the underlying reasons for this is the weakness, in security terms, of the most widely used operative systems.

There is not only a risk of the hardware itself being attacked by someone or something. The greater band breadth in relation to “dial up” connections also entails a greater risk of one’s own system becoming a base for further attacks – distributed DOS attacks (DDOS), for example.

Various parts of this cause problems:

Pre-installed applications and software are today being delivered with known security flaws. Microsoft’s dominance on the product side makes its product attractive targets for a variety of attacks. Old software is allowed to live too long, and the user is expected to find out where patches and updates are available and how to install them. There are many security products available – such as fire
walls, intruder alarms, anti-virus protection and filter functions but the potential problem is that the more impermeable you make them, the less accessible the web and its services become. That ruins all the fun and implies a serious risk of users ignoring the security side of things.

Possible solutions

The risk of users regarding security measures as a hindrance, however, is contradicted by a growing market for personal firewalls and the existence today of a number of really serviceable products (PGP, Norton, Zone Alarm etc.). Some of these have in fact shown that very good protection (at web level) can be obtained without being difficult or tedious to use.

Personal firewalls, properly used, can solve the following problems:

- Protection of IP stacks (protecting the actual implementation of networks).

- Some protection of applications, in that these are not directly accessible from the web. Usually, though, a firewall cannot protect the application protocol itself, and so the major threat remains, e.g. that of the e-mail client Outlook automatically starting an executable enclosure under certain conditions. A firewall can only affect this to a certain extent. Nor can a firewall handle traffic through encrypted channels.

A personal firewall can, generally speaking, provide a certain portion of the protection that is needed. By preventing general access to the hardware and also controlling outgoing traffic, we create a form of basic protection at network/session level, which at all events is a decent base.

Knowledge of the basic Internet technology is very widespread. There is a great need for norms concerning the characteristics which software and systems are to have when delivered, and also for these norms to include directions on the use of different functions, e.g. operative systems. A description of a standard environment for domestic Internet connections may be needed, with a view to indicating and tackling security questions. In addition, general knowledge is needed concerning risks and protection, as well as tools giving the user support for upgrading system security and permitting the maintenance of a level of security. This works up to a certain level.

It is unrealistic, however, to suppose that we will be able to get users very interested in security issues generally and, above all, get them sufficiently interested to learn to carry out security promotion measures themselves. The fact is that the majority will never understand enough to be able to configure an operative system.

A security plan is needed which will correspond to the risk panorama and protection needs of a normal household.
Components included

Components which should be included are specifications for:

- User identification and authorisation control. Separation of users and information is also needed in the home, especially if the home computer is sometimes used in connection with work.

- Access restriction ought preferably to be based on the individual, i.e. suitable for allowing a user to protect personal information and for preventing others from reading or destroying information. The difficulty is that this cannot be implemented with operative systems like Windows 95/98, which do not have any system of authorisation control or file protection. This is a basic requirement, but there must be some way of realising it. One way is to have supplementary software pre-installed to give functions like “encrypted disk with personal access”.

- Note. A growing problem, it should be noted, is that many people use the home computer for accessing work. At the same time it is hard to see how a home computer can be used both for mobile applications (games, chat etc.) and for getting at one’s work without major security problems occurring. This, however, is a problem for the enterprise/organisation concerned and nothing that can be built in or made a subject of general rules.

- Firewall function and filter, in keeping with the description of personal firewalls, above.

- Back-up functions must be included, together with functions for restoring data from a copy and an exact description of how this is done (whether one needs to re-install the operative system, how back-up copies are stored etc.).

- Functions for checking access to web services from the computer.

- Virus protection and functions for updating it.

- Access to external systems generally calls for stronger identity controls than ordinary passwords such as one-off passwords, certificates or key pads of the type now mostly used by banks.