
Extract from the report

IT security for private users

Analysis of interview meeting with private users as well as recommendations of a working group appointed by The Danish Board of Technology

On the project

This paper is an extract, translated into English, from the Danish report "Brugernes it-sikkerhed", published in April 2008. Excluded from the original Danish report are a presentation of the suggested solutions in the form they were presented to the participants ahead of their interview meeting, as well as the analysis itself of the results of the interview meeting.

IT security is a continually growing challenge to private users. The image of threat is changing currently and contributes to confusion and insecurity in private households. Careless conduct and no knowledge of technological security solutions, firewalls, antivirus, security updates etc. involve a risk to the general Internet security.

Lacking IT security may inflict problems on the user herself. Virus, phishing and hacking may bring the safeguard of personal data at risk, online identity theft, system breakdown and financial loss. Poor or insufficient IT security may also inflict problems on others. An unsafe computer may for instance work as a middle-station of offence against property and attack on other users' computers, homepages etc. If, for instance, the user has a home office, careless conduct in the home may cause problems at the workplace and result in leakage of other people's personal data, system breakdowns, theft of intellectual rights and confidential business data and subsequent financial loss to the workplace.

The responsibility of IT security handling for private users evidently lies with the users themselves, but the software producers, Internet suppliers and the state are also responsible for making security easier to handle by private users. The question is how to distribute the responsibility in the most appropriate and reasonable way.

A survey of the general IT knowledge among the Danish population carried out by The Danish Technological Institute in 2007 concludes that almost 40% are either completely without ICT abilities or only to a limited extent¹. Another survey from The National IT and Telecom Agency of the opinion of the Danish population on IT security points out that the understanding of IT security is considerably low and that this fact should be remembered when defining the future security solutions². A focus group survey from 2002 of the general knowledge, opinion and conduct of the citizens in relation to IT security reveals the widespread opinion among the participants that security is a topic they do not want to give too much thought³. It is difficult to keep oneself updated and to know how to act, and security is a matter that should be obvious without active involvement. If not, the survey shows, people's typical reactions are concern and restraint from accepting certain possibilities on the Internet.

A targeted effort to increase user awareness (the so-called "awareness raising") is of course necessary, but bearing the above surveys in mind it is reasonable to assume that such an effort cannot stand alone. Too many people do not have knowledge of IT security, and even though this group is decreasing, it will always be there. Consequently, there seems to be a need for redistributing some of the responsibility regarding security handling, e.g. through adjustment, co-ordination and automation of the effort.

¹ "Borgernes IKT-færdigheder i Danmark" (The ICT abilities of the Danish population) 2007, published by Teknologisk Institut (The Danish Technological Institute)

² "Undersøgelse af den danske befolknings holdning til it-sikkerhed" (Survey of the opinion of the Danish population on IT security) 2006, published by Parkegaard og Kristensen Sikkerhed (Parkegaard and Kristensen Security)

³ "IT-sikkerhed. Analyse af borgernes viden, holdninger og adfærd" (IT security. Analysis of the knowledge, opinion and conduct of the citizens) 2002, published by PLS Rambøll

A report from 2007 on "Personal Internet Security" from The House of Lords in Great Britain reveals the same viewpoint, and the overall conclusion is that it is neither fair nor reasonable to leave the responsibility of IT security handling to private users in a situation of constantly changing technological development, during which more and more criminals operate on the Internet.⁴

Consequently, The Danish Board of Technology wants to focus on the IT security of private users by identifying efforts to redistribute some of the responsibility of IT security handling thus increasing the general security level. However, there exists no survey of how far private users are willing to go when it comes to leaving IT security handling to others, and it has been the aim of this project to contribute with knowledge of this topic.

A working group appointed by The Danish Board of Technology has been assigned to work out a catalogue of recommended solutions, realistic to carry through, however containing controversial efforts that may put the private users in a dilemma when choosing among them. For when choosing a suggestion that improves security, a price must often be paid, for instance in the shape of reduced control of the user's own computer and access to the Internet.

The catalogue of recommendations has been presented to and evaluated by private users at an interview meeting. On the basis of own belief as well as the user opinions of the suggested solutions, the working group has compiled its recommendations.

The working group includes the following members:

- Susanne Karstoft, Juridisk Institut (School of Law), Aarhus Universitet (The University of Aarhus)
- Per Tejs Knudsen, cBrain
- Nicholai Kramer Pfeiffer, Cybercity
- Birgitte Mikkelsen, Finansrådets it-sikkerhedsgruppe (The Danish Bankers Association, the IT Security group)
- Jakob Illeborg Pagter, Alexandra Instituttet (The Alexandra Institute)
- Steffen Stripp, Dansk Metal (The Danish Metalworkers' Union)

Project management in The Danish Board of Technology:

- Bjørn Bedsted
- Julie Refsgaard Lawaetz

The project has been financed by The Ministry of Science, Technology and Innovation and mainly focuses on the IT technical problem areas and security solutions, according to agreement with The National IT and Telecom Agency. Several security problem areas of a privacy nature have therefore deliberately been excluded. However, the suggested solutions are not consequently less important, and it is the belief of the group that there is a need for a general debate on privacy, e.g. in relation to electronic health records, registres and informed consents.

Method

The compilation of the suggested solutions is made by the members of the working group based on existing knowledge of the topic. Being developed by the working group does not, however, mean that the working group recommends to implement all the suggestions. The task was primarily to formulate some

⁴ "Personal Internet Security" 2007, published by the Authority of House of Lords

suggestions, from which the users themselves could choose. The general view and final recommendations of the group will be presented in the next section.

The suggested solutions have been presented to a group of private IT users at an interview meeting in Odense 27 November 2007. The Danish Board of Technology has arranged the event and analysed the results.

An interview meeting is a method to make an opinion poll among a group of approx. 25 citizens. The method consists of a combination of group interviews and a questionnaire. A group interview gives a lively debate and provides the participants with the opportunity to add aspects that are not included in the questionnaire. In return, the questionnaire ensures that all participants are heard and that comparable data are created in essential areas.

The 23 citizens who attended in Odense received in advance the suggested solutions presented by the working group. The interview meeting took three hours and started with an introduction to the subject followed by handing out the questionnaires. The participants had a little less than one hour to fill in the questionnaires. Then the participants were split into small groups and interviewed on their opinion on the suggested solutions. The group interviews took a good hour.

The selection of participants was made in steps. At first, 2000 invitations were sent out to citizens in the Municipality of Odense by a random draw from the Danish centralised register of personal information. Among these, 70 citizens gave positive feedback, and 30 citizens among them were chosen to participate in the interview meeting. The group of participants is considerably representative of the distribution in Denmark as to gender, age, education and employment.

Recommendations of the working group

The working group finds that the handling of IT security is today left too much to the individual user. The present situation is neither reasonable nor appropriate considering the need to maintain a desired security level in society as a whole. Therefore, it is the recommendation of the group that the judiciary and the executive authorities will in future think (more) in models providing the private users with easy IT security handling, by moving part of the task closer to the parties who have a genuine possibility to improve the security.

The group has prepared some possible solutions and has aimed to test, how far the users are willing to go to be helped with security. Therefore, the suggested solutions described include some interventions towards the private users that will improve the security level of the private user as well as the general security level. But they are also more intervening than the present arrangements, as they include increased control with and limitation of the user's free conduct on the Internet. The nature of the limitations varies from making actual demands on the users to an actual delegation of responsibility of certain security assignments to other party.

At the interview meeting, there was an expressed wish to obtain help to handle security, and it is the impression of the group that the majority of the users accepted the interventions implied by the suggested solutions, even though not all did, of course. In the following section, the working group commits definitively to the suggested solutions it has worked out and presents its recommendations - based on the reaction of the users, among others - of how to deal with them in future.

Digital identity

The working group recommends the introduction of a digital identity to be used for public as well as private services on the Internet.⁵ The digital identity should be based on hardware or in another way represent a similar security.

The advantage to the users of introducing a digital identity is that a sufficiently safe identification of the individual user can take place, i.e. securing authenticity. The security of the user identification is decisive for which services and utilities will be supplied on the Internet in future. The safer user identification, the smaller risk that sensitive personal information will fall into the wrong hands. In this way, the supply of services that for instance involve information about health, financial matters etc. may be increased. This means that the individual user will have improved access to and knowledge of the information stored about her. The working group finds that mobility and user-friendliness are terms with important influence on how much the public will use the digital identity.

The digital identity should only contain information that identifies the user, and no further personal information such as medical records, where a means of payment has been used and for what etc. If the identity is solemnly established as a method to secure that the user is the one she says she is, then the working group does not share the concern of the users that the suggested solution may provide private companies with the possibility to obtain personal information about their clients at public authorities and vice versa. However, it is necessary to take the general resistance of the users seriously of using the digital identity for both public and private services. This resistance points out the need for a considerable

⁵ The working group has decided to use the term "digital identity" in order to think freely, and not letting its suggested solution be tied up to the Danish digital signature. However, it is emphasised that the elements in the suggestion presented here by the group may be incorporated in a new version of the digital signature.

information effort, if a future digital identity should be used for both private and public services, which the group finds to be a desirable development.

In order to further suppress the threat of recording all traffic on the Internet, it is also important that the users keep having alternative identification possibilities to services that do not require a strong identification such as the digital identity. It could be less critical services or anonymous communication with public authorities, where a strong identification is evidently insignificant.

The working group recommends that the use of digital identity should be compulsory to people who want to use public services on the Internet, to which identification is required today. The fact that IT weak people cannot use a digital identity should not stop the technological development. The working group has not decided, which solutions should be offered this group of people.

Automatic security updates

The working group recommends, in line with more than half of the users, that automatic security updates are encouraged in different ways, for instance that the producers of programs configurate programs in a way that the user must actively refuse updates. The working group is aware that there may be a number of challenges as to convince the program suppliers to prepare their products in such a way, especially as we, to a large extent, deal with international companies. Therefore, this suggestion should be evaluated together with the suggestions of PC inspection and security labeling which will encourage the users and guide them to establish automatic security updates.

Compulsory PC inspection

The recommendation of the working group, corresponding to more than half of the users' own preferences, is to develop and introduce a PC inspection which will in future be required when using public services on the Internet. The PC inspection should monitor the security level of the user and deny access to public services when the level is too low. The recommendation can only be carried through by the participation of public authorities and is estimated to provide a substantial security increase.

There are, however, a number of challenges to be met. These challenges are primarily of a practical and technical nature such as frequency and time of carrying through a PC inspection in such a way that it does not refrain private users from utilising public services on the Internet. As a consequence, it is the recommendation of the working group that the arrangement will start as a voluntary offer which the user will be met with on certain public websites. In this way, it is possible to gain the required experience. Furthermore, the PC inspection was conceived by some of the users at the interview meeting as a limitation of personal freedom and invasion of privacy, as the computers to be inspected may contain photos and other data of a private nature. Therefore, it is important that a future PC inspection is designed in such a way that it does not give access to personal data, but scans exclusively for holes in software programs, malware etc.

It is the conviction of the group, on the basis of the user comments at the interview meeting, that in case the practical problems are solved satisfactorily (e.g. the PC inspection does not take too long) the Danish users will be more positively minded for the introduction of PC inspection as an actual requirement to gain access to public services. The group finds that this acceptance will, however, also to a large extent depend on the fact that the public authorities link the PC inspection with an efficient user guidance as to how to meet the security requirements. The public authorities should provide assistance to the users they require increased security from in a way that the users will conceive the suggestion as a help.

Compulsory mail filtering

The working group recommends, corresponding to the wishes of most users, that Danish mail suppliers introduce a mail filtering system, active as standard, compared to the present situation where the user in some situations should activate it herself.

Security labeling

The working group finds that a trustworthy and successful system of security labeling IT products will increase the general security level and therefore recommends its introduction. The group's recommendation is, among others, justified by the fact that a large part of the users at the interview meeting supported the suggestion and were willing to pay extra for such a labeling system, if it could help them choose safer products.

However, the working group shares some of the concerns of the users, as to how such a system can work in practice. This scepticism concerns, among others, which products should be labeled and how labeling of very dynamic products such as software requiring regular security updates should take place. A trustworthy labeling system should consider that the development within the area of IT goes fast, but the group also believes that this is possible, for instance by providing only software with automatic security updates of high quality and a sufficiently high frequency, with a high score.

Blocking of damaging websites

The working group recommends that the possibility to block the access to damaging websites should be further investigated. A website should of course only be blocked if the site in question without doubt works as an active part of the IT crime, for instance phishing sites and sites from which you may accidentally download malware.

The working group understands that if a blocking should in practice hamper the activities of the IT criminals, then a quick decision process is required. However, the working group also understands that such a quick process will bear the risk of errors and that a number of problems concerning freedom of speech and security of life and property are related to possible blockings. Consequently, there is still a need for more consideration in relation to a possible conduct in the treatment of potential blockings of websites. Therefore, the group cannot at present give a clear recommendation in this matter. The working group has not evaluated who could be responsible for deciding, if a website should be blocked or not, but it seems evident that in case of acceptance it should be made by an authorised party, meaning that it will not be the individual Internet supplier who should make such a decision and bear the corresponding responsibility.

The users at the interview meeting displayed very low tolerance to all types of damaging sites, and the most convincing support was to close down sites with an obviously damaging content such as sites from which malware is downloaded when entering. However, the group notes that more than half of the participants also support a blocking of websites that contain only knowledge of how to construct malware. As mentioned above, the working group has only evaluated blocking of websites that do actively and without doubt represent a security problem to the users of the websites in question. The working group does not find that websites containing only information are damaging to such an extent that a blocking of them is considered, and such websites are not included in the recommendation.

Online data storage

The working group anticipates a situation where the users will increasingly use online services for storage of personal data. There are considerable user advantages in this, as the data will often be better pro-

tected against system breakdown or additional loss of for instance holiday photos. On the other hand, online storage of data provides others with easier access to people's personal data. This risk concerns several of the participants at the interview meeting, whereas others handle it by only storing data on the Internet that others may see. It is the evaluation of the working group that the users lack a genuine understanding of the level of confidentiality and the rights to the data that are stored on the Internet. Especially the rights give concern, and the group recommends to make an effort, in order to inform the users of this matter. It is also recommended that public authorities give the rights, that include data stored on third-party servers, a critical view.