Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 142 | August 2000

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

Four dictates on data security

The ICT industry needs security regulation, concludes security experts

The telecom sector must meet a number of security requirements, since it delivers services that are vital to society. The same ought to be truer for data service enterprises and suppliers of internet-access. This is the recommendation from an expert panel asked by the Danish Board of Technology to come up with its tenders on the most pressing IT-security problems. The panel also points out that a breakdown in the very large business enterprises can have drastic societal consequences. For this reason, requirements pertinent to their security level ought to be drawn up.
The panel also institutes a search for a far more intensive effort to teach *everybody* – children and adults – about the "rules of conduct" when using IT. Differing security regulations throughout the world render it difficult for smaller Danish concerns, to make good use of the possibilities in the new economy. The panel accordingly encourages the government to press for greater standardization.
Finally, the panel calls for a personal "service card" as the very best solution to the problem of establishing secure identification on the internet

For the coming sessional year of the Danish Parliament, the Danish Board of Technology has asked three of the country's leading experts in data security to come up with their bids on just which IT-security problems the government and the Parliament ought to be directing their attention toward in the approaching assembly.

The three panel members are:
Preben Andersen, CERT-coordinator at UNI-C, Business and Research (CERT, *Computer Emergency Response Team,* is a global cooperation around IT-security). UNI-C is a national enterprise, operating under the auspices of the Ministry of Education, which delivers IT-solutions, primarily to the education-sector. Previously, leader of the National Police's IT-investigation unit. Previously, member of the government's IT-security council.

Agner Mark, administrative director at Dan Net, which delivers data-communication solutions to customers in 60 nations. Dan Net is owned 100 percent by Tele Danmark. Member of the board of the Danish EDI-council. Previously, member of the government's IT-security council.

Jan Carlsen, administrative director at the Institute for Data Security, an information-security concern operating under the auspices of Pricewaterhouse-Coopers. Moreover, Jan Carlsen is a member of the government's IT-security council.

The panel's work took place at the offices of the Danish Board of Technology on August 8, 2000. The proceedings were reported and the discussion subsequently collated by project manager Morten Jastrup, of the Danish Board of Technology's secretariat.

The panel chose to focus on four areas where there are very real problems that ought to be solved.
The four areas are so different in so many ways that it makes no sense to "rank" them in order of importance. However, the members have chosen to name the concentration of data traffic first, especially because this problem will have such far-reaching consequences should the worst-case scenario take place.

Concentration of tasks

Up until a few years ago, the use of IT was a matter of internal affairs for the particular enterprise and the particular institution. However, in recent years, a number of business concerns have emerged which specialize in providing IT-solutions for other firms. Together with internet Service Providers (ISP), these IT-service firms can quickly become crucial to their customers' communications.
The panel sees no reason for questioning the security in the firms that are presently providing IT-solutions. Nonetheless, the panel is of the opinion that these firms' concentration of operation- and service-assignments can potentially lead to a serious security problem.
The firms watch over assignments for their customers, who pose great demands on operational reliability as well as on confidentiality. In this connection, it makes sense to cast a sidelong glance at the telecom sector. This field has been regulated over the course of many years because the services that it provides are of vital importance to the society. Suppliers of access to the internet and appurtenant services occupy a similar position. However, these firms have *not* been subject to the same degree of security requirements.
The panel recommends that a list of minimum requirements for security with respect to these firms be hammered out, in keeping with the style of the requirements that are imposed on the telecom sector.
Furthermore, the panel is of the opinion that certain firms can become such enormous "nodes" that a breakdown would have consequences which would be noticeable on the societal plane. This applies not only to the aforementioned IT-service firms but also to leading firms in other branches. The increasing dependence on information technology entails a risk that a large-scale IT-breakdown in one of the larger "node firms" could simply paralyze parts of the society.
The Parliament's politicians, therefore, ought to consider introducing minimum requirements with respect to IT-security for firms of considerable size.

Bad habits and naïveté on the internet

Despite the fact that for quite some time now, there has been a great deal of discussion going on about encryption, it is only a very few who actually encrypt their communications as part of standard procedure. Unfortunately, it is far from being so that this is the only instance where we can see that even though security is something we certainly talk about, most of the users let it remain 'all talk and no action'.
The rules of play are vital to any society. We have a new generation of people who are going to be living their lives with the internet and with a host of new technologies that we still don't have any idea about. On the other hand, a considerable part of the parents' generation remains relatively in the dark about many of the things that are happening on the internet.
There have always been gaps of understanding between the generations. But the present-day's young generation is growing up these years with an entirely new world at their feet which a great many people of their parents' generation simply do not understand.
The generation gap, then, is greater than it normally is. For this reason, it is more difficult for parents to teach their children how to make use of the new technology in a prudent fashion. The school system must be invested with the task of teaching children about the basic "rules of the highway" for electronic communications.
There is a need for teaching children, from very early on in the public schools and up through the rest of the school system, about the internet and about how to use it in a sensible way, and especially about the things one should not or must not do.
In much the same way, an internet "driver's license" for adults, conceived along the lines of the personal computer driver's license, would be a good idea. A basic understanding of the internet among the parents would play an important role in breaking down the generation gap.
For this reason, the panel suggests that special materials for teaching people about the traffic rules on the internet be designed – and that it cover all levels, from the public school to adult education.

Shortage of international rules and standards

In many ways, the Danish business structure is quite well suited to a rapidly developing, global economy. The many small and medium-sized firms are flexible and can make use of the possibilities that are emerging on the international markets. But this advantage often gets devoured by difficulties encountered in adapting to local rules and frames. The smaller Danish enterprises do not have the same capacity for becoming completely conversant with all the details of the local legislation to the same degree as the larger foreign companies.
In this vein, encryption is a serious problem. Changing rules about how fully one has to encrypt his/her messages, and especially about American export restrictions, make life unpleasant for many business concerns that have departments situated in several

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm

different nations. Even if one is attentive to matters of security, it might be illegal or impossible to protect oneself when it comes to communications transmitted to other countries. Frequently, the taxation and customs area is more or less an impenetrable jungle in which you can do no more than fumble your way around.
As likely as not, these problems will never be entirely removed. There will always be differences that render it difficult to deal with many countries. However, it is precisely because the Danish business structure is what it is that the panel is encouraging Denmark to put pressure on the European Union, and (operating through the EU) on the WTO to draw up rules that are as elastic as possible. On this point, Denmark has more to lose than most of the other countries.

Secure identification on the internet

One of the fundamental problems about electronic telecommunication is finding out *whom* you are actually in contact with. The technology affords rich possibilities for veiling one's identity. In light of how difficult it is to get most users of the internet to take security seriously, a solution for the security- and identification-problem has to be established which simultaneously is easy to use and embodies distinct advantages for the citizens.
The law about the digital signature, passed in May, is a step in the right direction. But the very best solution, in the opinion of the panel, would be a personal "service card", which refers to a central key-center. A card with a PIN-code, as a security measure, is conceived along the lines of the credit card. According to predictions, in just a few years from now, models with biometric identification, such as iris recognition, will be generally accessible. The panel encourages that the debate about a personal service card be raised and emphasizes that it is crucial that the "service card" takes the form of an offer to the citizens and not something foisted upon them.

Postscript from the panel's participants:
Lack of real knowledge
As a matter of fact, we know very little about the real IT-security problems that Danish businesses, institutions and private citizens are facing. The politicians as well as the practicians are obtaining most of their information through the media, where "IT security-experts" and their companies are frequently the source of the stories. We will permit ourselves the liberty of placing a question mark alongside these sources' motives and alongside their independence. In our opinion, at least, the general impression that viruses, hackers and pedophiles constitute the greatest security problems on the internet simply has no basis in reality. By far, the greatest and most frequently occurring security problems are the everyday occurrences such as cables being disconnected, machines breaking down, human error, etc. These might seem trivial, but they are by far the most frequently occurring problems. And for the business concerns which do get hit by such problems, there are the same serious consequences regardless of whether it is a malicious virus or moisture in the **server-compartment** that shuts down the system on any given day.
The reason that the panel has chosen not to place the lack of real knowledge among the four most pressing problems is that the government's IT-security council is about to start mapping out the real IT-security problems which Danish business enterprises, organizations and institutions are facing. The panel is encouraging the politicians to ensure that ministries and institutions take part in this investigation, which is being conducted anonymously.
Another misapprehension is the belief that "the market" will solve a great part of the security problems in connection with information technology. It is a fallacy to believe that firms and private users are going to purchase the secure products and that through this means, they will bring about a secure exchange of information. Experience has demonstrated, unfortunately, that this has not been so. The market for IT-products and services is so immeasurable that small and medium-sized enterprises and private users have no real chance of orienting themselves and finding secure solutions.
Quite some time ago, a decision was made to set up rules about how electric wiring has to be insulated, about how the electrical outlets have to satisfy certain security requirements and it was stipulated that electric blankets and other electrical appliances must not be dangerous.
In much the same way, there is now need for setting up security requirements pertinent to information technology. It's not enough to say that the users will certainly think twice the next time they get a shock.

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm