Source: http://www.bmi.bund.de/cln_183/SharedDocs/Reden/EN/2010/10/bm_isse.html?nn=10 (2010-10-07)

"Understanding the Internet as chance and part of life"

reason: MP for the ISSE conference
Date: 2010.10.05
City: Berlin
Speaker: Dr. Thomas de Maizière, Bundesminister des Innern [Federal Minister of the Interior]

Imagine a world without the Internet.

Imagine a world without e-mail.

Imagine a world without mobile phones.

Some of us here, myself included, would feel as if we were back in the 1980s. We would have no computer virus or Trojan attacks to worry about, our networks wouldn't be clogged with spam, and a pleasant dinner out with friends wouldn't be constantly interrupted by ringing mobile phones.

On the other hand, we would also have no booming Internet industry, no rapid and convenient communication channels, and we might not have been able to plan an evening with friends at short notice anyway, since we wouldn’t have been able to reach them.

If you remember, until a few years ago the Internet was mainly an information platform that at first very few people knew about or had access to. Today, the Internet is an integral part of everyday life. This development has created many new possibilities – for the economy, for society, for our personal lives. Just think of the new business models based on the Internet. Think of the advances for freedom of expression around the world. Or think of parents and grandparents who use the Internet to stay in touch with children and grandchildren far away.

Despite all the positive aspects and opportunities offered by the growing interconnectedness of all areas of life, the economy and public administration via the Internet, this development also has its downside. Our computer networks are increasingly misused by organized international crime. Cyber criminals use highly sophisticated methods to gain financial advantages at the expense of others. Whole new value-added chains have developed around this shadow economy. We are seeing a significant increase in espionage and sabotage activities.

In a recent development, a new and powerful malicious software programme was discovered in early July. Called Stuxnet, this computer worm is the first to attack supervisory control and data acquisition (SCADA) systems, which are used in many key areas of infrastructure. Simply inserting an infected USB stick into a computer is enough to spread the worm.

This incident represents a watershed in IT security management. Even industrial control systems which used to operate in isolation can be affected by future IT attacks like Stuxnet. There has apparently been a gradual trend towards connecting these systems with the Internet. In addition, the use of standard computer operating systems is increasing, resulting in higher risk of attack. This development is a cause for concern, as it allows new possibilities for criminal activity, even if enormous efforts are required to mount such attacks.

Another challenge in the modern computer age is protecting against botnets that take over individual computers without their owners' knowledge and link them into networks. Millions of computers, all of them online at all times, need effective protection against malware and misuse.

We can stay ahead in the endless race against attackers only if industry, the research community and public administration engage in dialogue and cooperate at national and international level on the basis of mutual trust. We must continue and increase our efforts to raise awareness and we must give the issue of IT security high policy priority.

In all of our activity, we must not forget that the point of all our protection and efforts is not the information and communications technologies or the Internet, but the autonomous individual. Rapid technological development and above all the Internet with its seemingly endless opportunities, as well as risks, demand that we protect and help people find their way in this cyber era.

To do so, we must

1. educate,

2. create transparency,

3. and take our govermental responsibility serious.

About my first point, education: Each Internet user must remember one thing: Everyone who goes on the Internet needs basic knowledge and a healthy amount of common sense: Why should I publish intimate details about my private life on the Web that I would otherwise share with only a few close friends? What makes a reliable and secure password? What basic settings do I need to protect my computer against viruses and malware? What security risks must I watch out for when I am online? How do I design my own website so that it can't harm others? This is why my ministry already supports important Internet-education initiatives like "Deutschland sicher im Netz" (Keeping Germany safe on the Web). And we plan to continue.

About my second point, transparency, above all in data processing: Here too there is much to be done.

Businesses can and must use the Internet to tell the public more quickly, simply and comprehensively, in language that all can understand, about what information they collect, what they use it for and who they share it with. Providers would be well advised to work together to formulate standard, legally binding agreements.

And about my third point, adapting the law: Existing legislation already adequately covers many new aspects brought by the Internet and information and communications technology (ICT). And we should always start by seeking an analogy to the "offline world".

Only where there are obvious gaps in existing law should the government examine whether and how to close these gaps. But before passing any new regulation, we should carefully examine whether it suffices to rely on – and if necessary, require – voluntary self-regulation in society and industry. Only where self-regulation does not yield satisfactory solutions, or where strong special interests crowd out the common good must and will government take action.

In other areas, however, we must think more carefully about the possible need for legislative action. For example, how can we make sure that individuals retain control over their sensitive information and personal data, even in the digital age?

To answer this question, we must thoroughly examine our applicable data protection law, which is still largely a product of the analogue age. In doing so, we must pay special attention to the fact that data protection and data security always have a legal, a technical and an international component. All of these must be developed in tandem in order to achieve good results.

As a good example, I would point out the need for trusted online identification and the secure transmission of identifying information. Our De-Mail and new identity card offer technical solutions for both.

Internet-based – and thus technical – data protection applications, known as "privacy apps", could implement existing rights to information or to object simply and cheaply at the click of a mouse. Maybe this conference will inspire ideas for such apps.

Legal and technical solutions must be pursued in tandem also when it comes to control options for individual users. One example might be a digital date of expiry which individuals can use to define how long the information they have put on the Internet should stay there. I am pleased that software companies and research institutions are already working on such approaches, although there are certainly still some technical problems to work out.

The Internet enables globally networked information processing and storage. In cloud computing, for example, data are located in a "virtual cloud" outside one's own infrastructure. On the one hand, this means I can access my data at any time from almost anywhere. On the other hand, however, I have a hard time knowing where exactly my data are stored and who is processing them. This also leads to uncertainty as to which law applies.

Retaining control over sensitive information and personal data is therefore a challenge for the future. In designing data and information security, for identity authentication authorization management (IAA), we will need trusted and internationally interoperable systems and applications.

When talking about legal framework conditions for "clouds" which guarantee data security and data protection, we must think in a European and global context. National, supranational and international arrangements must be developed in concert.

At the national level, we can and will come up with our own strategies for dealing with the Internet and will submit them to the process of building international consensus.

Today, twenty-five years after electronic mail was first introduced, fewer than 5% of e-mails in Germany are sent in encrypted form. The overwhelming majority of e-mails and their attachments can be intercepted, read like a postcard and manipulated. Senders and recipients can therefore never be sure who they are really communicating with and whether the message has been altered. Then there is the problem of never knowing for sure whether an e-mail ever actually reached its intended recipient.

With De-Mail, we are working with the IT industry to achieve a higher level of trust between communication partners. Secure registration procedures and connections between providers prevent messages from being intercepted or manipulated. And De-Mail provides legally binding proof of when the message was received.

In designing De-Mail, we placed high priority on making sure the technology is as simple to use as ordinary e-mail. In this way, we hope to rapidly raise the level of security for electronic messages and make De-Mail part of everyday life.

I also hope the new identity card rapidly becomes part of everyday life online. This new document, which you can apply for starting November 1st, will also enable cardholders to identify themselves on the Internet as easily, conveniently and reliably as in the real world with the conventional identity card.

The online function is optional for cardholders and service providers. It is voluntary, an option for reciprocal, reliable authentication.

If cardholders choose to use this option, the new identity card makes it easier for them to control their information. And when personal data are necessary, cardholders can provide them with greater awareness and in a more targeted way.

Many safeguards ensure that personal information cannot be linked. No one needs to fear becoming a “transparent citizen”.

This is why we concentrated on ensuring a very high level of security for citizens’ data while keeping the card easy to use. This means that the only data that can be read from the card are the data needed in that particular situation.

For example, if you want to order a book online, the online merchant will be able to read your address on the card, but will not have access to your date of birth.

Card users themselves ultimately decide which data can be accessed. And both parties to the transaction must verify their identity: The online merchant who wants to see my identity card must also provide proof of identity. To this end, the government issues authorization certificates that come with strict data protection obligations. Here, government functions as a sovereign guarantor of trust, without however intervening in the communication between users and service providers.

We have developed and tested the new identity card together with experts. In this way, we were able to create a modern identity card that ensures both the physical security of the card itself and the security of the data stored on the chip. Security mechanisms protect all transmissions of data, so that no one can intercept such transmissions, copy or manipulate the data without explicit authorization. No data can be accessed or sent from the card without the cardholder’s explicit consent. Here too, users must keep their computers’security features up to date in order to prevent misuse.

With the structures of the new identity card, the Federal Government has created a robust foundation for its use, while paying attention to technical, legal and organizational aspects. Now it is up to the service providers on the Internet to take advantage of these structures. This call is addressed both to businesses offering their personalized services on the Internet and to the state and local governments: With the new identity card, they will find it easier to provide their services in a more convenient way, meaning that citizens will have to make fewer trips to government offices.

Within the federal administration too, information technology is vital for ensuring the ability to work and the capacity for action. In both the public and private sectors, mobile telephony and text messaging is an integral part of the daily routine.

But we now know that it is relatively easy to eavesdrop on GSM mobile networks. In concrete terms, this means that mobile phone conversations and text messages need additional encryption for protection.

That is why the Federal Office for Information Security (BSI) developed a new standard for encrypted phone calls and text messages called secure cross-network communication, in German SNS.

Thanks to this new standard, it is possible to make encrypted phone calls and send encrypted text messages between mobile phones made by different manufacturers. The new standard also allows for encrypted connections to TETRA mobile devices used by the police, fire services and other security organizations. The SNS standard is open and allows interested manufacturers to develop and sell products which use this standard.

These and other products based on the SNS standard will make the federal administration's mobile communications more secure.

We want to take full advantage of our possibilities and improve the framework conditions for IT security already during the design phase of new infrastructures. "Security by design" must take the place of the "bolted-on security" often practised in the past.

Neither in economic terms nor in terms of security policy can we afford to wait until long after an infrastructure's functionality has been developed and then expend great efforts to come up with the IT security. This is where the Federal Office for Information Security plays an important role: It is involved early on in the development of infrastructures and new IT-based applications.

The Federal Office's technical guidelines on IT security for specific applications and infrastructures, its certification of products according to defined protection profiles, and its IT security standards set the course for significantly greater IT security.

In this way, we are creating a dependable framework for long-term security of investment in increasingly complex structures. At the same time, by setting standards, the Federal Government provides orientation and promotes future IT innovations.

IT security has long been more than a national issue. Due to the high degree of global interconnectedness in our information systems, incidents in other countries have a growing impact on IT security in our country as well. The division between internal and external security are becoming increasingly blurred.

This is why the Federal Government is working not only at the national but also at the international level to strengthen cross-border IT security.

At European level, our goal for the medium term must be to establish Europe-wide IT security themes, thereby creating a harmonized level of IT security in the EU which all participants can depend on. Founded in 2004, the European Network and Information Security Agency, ENISA, provides important services on the way to achieving this goal.

ENISA's mandate is currently being renegotiated. I would like to see this agency play a greater role in the EU's policy-making process and the implementation of policy decisions in the Member States.

Beyond the EU, we are also working to promote IT security in supranational initiatives and organizations such as the OECD, NATO and the G-8. Here, our immediate goal will be to work towards consolidating international activities which are currently divided into many individual initiatives. We must help existing security standards gain greater acceptance.

Whether national or international, with conferences like this one you are helping make our ideas and actions more transparent. Talking about the challenges the Internet will bring helps all of us create innovative solutions and not immediately call for new regulations.

This ISSE conference has exactly this aim: to provide a forum for new and innovative solutions in Europe. So I urge you: Let us continue to work together creatively, private industry and governments, to increase the potential that lies in today's information and communications technology and create interesting, versatile and above all trusted IT solutions for society.

Imagine a world where the Internet is always safe.

Imagine a world in which mobile communication is easy, safe and reliable for every user.

Imagine a world in which each user has sovereignty over his or her data.

This world may be twenty years in the future, but we must take advantage today of our opportunities to turn visions into reality, so that the blessings of the digital age do not become burdens.

With that in mind, I wish you a successful three days at this conference, with many lively and productive exchanges.