Conversations with

Udo Helmbrecht

How do you see the nature of the cyber security threat to institutions, businesses, and individual citizens changing?

If you look back over the last five or six years, we have seen many threats from ‘classic’ email viruses such as Trojan horses and worms. We have these with us still, but more recently we have also seen the appearance of drive-by exploits (the injection of malicious code into the HTML of websites that exploit vulnerabilities in browsers), where you download malware (malicious software).

This is a change. And we still have to contend with botnets (malware that allows an attacker to take control over an affected computer, usually part of a network of infected machines). In some member states, good cooperation between governments and telecommunication sectors has provided a lot of help for small and medium-sized companies—and citizens—to detect these new threats, but botnets are still around.

These are the top threats, but we have other challenges such as hardware and software failure—human mistakes that we will always have to cope with.

What is ENISA [European Network and Information Security Agency] doing to foster cooperation between states to protect institutions, security organizations, industry, and individuals from these threats?

In terms of the threat perspective, we try to raise awareness and ensure that people take the appropriate action to protect themselves. We publish each year a ‘threat landscape report,’ an overview of what threats are out there, taking into account the global situation but especially addressing European Union member states.

We also undertake more traditional work to encourage organizations to adopt virus detection programs, firewalls, and the use of encryption for intellectual property communications, and to make sure everyone is careful when surfing sites they don’t know.

Part of the EU initiative is ‘cyber security month,’ working with member states and member states associations, to try to raise awareness of cyber security issues among small to medium-sized companies and citizens.

Have you done any work to quantify the cost of cyber attacks to European organizations, industries, and individuals?

In December 2011 we published a paper on the subject, “The economics of security: facing the challenges.” But there are a lot of shortcomings to quantifying the cost. It’s difficult to define the damage because, unlike [with] insurance, for example, you really cannot measure the damage with any degree of accuracy, or work out the probability of an incident.

For example, if you look at the official statistics around cyber-criminal, you only get statistics for when people report occurrences to the police. These tell you how many incidents are reported, but they do not give you a value on the cost of the damage or tell you how many incidents occur overall. And it’s difficult to define exactly which areas are included—credit card fraud, malware, intellectual property issues, and so on. So any figure is somewhat artificial.

This must be frustrating, but it also shows the nature of the problem. In which sectors does ENISA operate? How far involved are you in issues such as threats to national security, to industry, to aviation infrastructure, such as the air traffic management system?

Our basic objective is to work together with European institutions and member states to increase the level of information technology security, preparedness, and readiness.

What we do is to support member states in building up national or governmental computer emergency response teams, or CERTs, so member states are better prepared. We organize a pan-European exercise where member states, banking, and telecommunications sectors are involved. We try to get together the most important sectors in Europe and work with them to have a better understanding of the threats and the solutions. By working with governments and these companies we can do a lot; in our last exercise in October we had more than 100 telecommunications companies and 100 banks participating.

The first of these events took place in 2010, as a table-top exercise. So step by step we have gradually been involving more industry participants in the events, which take place every two years. The intention is to incorporate more and more sectors, and I expect next time we will have other sectors and all member states.

There are other industries, such as aviation and the automobile sectors, where issues of cyber security remain the concern of safety regulators, national and European. In these areas it concerns are part of the safety culture of the industry. But in other areas, such as financing, banking, energy, telecommunications, these are critical infrastructures where governments have a certain responsibility.

How do you work with other government organizations, in the U.S., for example, to take a joint approach to what has become a global threat?

We have contacts within the U.S. Dept. of Homeland Security, and have been observers to the ‘Cyber Storm’ exercises at a working group level, where we exchange information. How much further we go will depend on the cooperation between EU member...
states. But maybe next year we will hold another EU/U.S. exercise—this is currently being considered.

Do you look at threats from government agencies and individuals?

We examine the threat from the viewpoint of technology, business models, and opportunities. ENISA is a ‘common market’ agency. We take the Lisbon Treaty [signed in December 2009 to address issues such as globalization, climatic and demographic changes, security, and energy] as the basis for our work, and we look at how to build up new business models in a secure way, via cloud computing and social networks, for example. We look at improving service level agreements in cloud computing contracts.

We also look at new technologies—radio frequency identification—and how they can be balanced with concerns around privacy issues. We have developed a very successful impact assessment that is now used by manufacturers in the clothing industry, for example.

Another example is ‘green energy’ and the introduction of smart meters—how we should introduce digital electricity meters that are compliant with privacy and IT security. We look at both upcoming and deployed technologies.

How far are we from developing a comprehensive European Union cyber security strategy?

In February this year an EU-wide security strategy was published by Commissioners Neelie Kroes [European Commission vice president for the digital agenda], Cecilia Malmström [EU commissioner for home affairs], and Catherine Ashton [high representative of the union for foreign affairs and security policy/vice-president of the commission]. The positive aspect of this is that for the first time we have merged the different political aspects of the ‘digital agenda,’ internal security, and foreign action services together in an integrated strategy.

As a result of this you can expect to see Europe pulling together to work more closely in the cyber-crime area. We now have a joined-up strategy taking into account research initiatives such as the commission’s Horizon 2020 strategic research program and new standards in IT security. It’s a good step forward.

How much work do you do to anticipate future threats, given the knowledge you have accumulated about long-term trends? Is it possible to predict what kind of threats we need to prepare for in the future?

This is like looking into a crystal ball. What we can do is talk to industry about what they are doing. We have an advisory group that includes many of the largest names in the industry—IBM, Microsoft, Intel, for example— and we ask them what is upcoming. They are participating in our studies into areas such as cloud computing, for example.

At the same time, we try to identify the next ‘breakthrough’ technologies, such as smart grids, for example. We know both industry and governments want to push this technology but we also need to discuss the implications of how electricity use behavior can be traced. The question is, what is the social impact of such technologies? This will be difficult to predict before they become market successes.

But overall, and you will see this from our studies, talking to industry gives us a realistic view of what technologies will be employed in the future, what business models will emerge, and where we need to look into the security aspects.

In terms of cloud computing, what would you say are your headline examples—and we ask them what is upcoming. They are participating in our studies into areas such as cloud computing, for example.

Since October 2009, Udo Helmbrecht has served as executive director of the European Union’s European Network and Information Security Agency, based in Heraklion, Crete. ENISA works on behalf of EU organizations and member states to protect institutions, businesses, and individual citizens from the threat of cyber attacks.

Helmbrecht has studied physics, mathematics, and computer science at Ruhr-University, Bochum, and in 1984 was awarded a Ph.D. in theoretical physics. He acquired experience in the field of security through work in a variety of areas, including the energy industry, insurance, engineering, aviation, defense, and the space industries.

During the 1980s and 1990s he held several senior posts at Deutsche Aerospace AG/Messerschmitt-Bölkow-Blohm, including program manager information technology, and before that was head of technical data systems. He became president of the German Federal Office for Information Security in 2003. In 2010 Helmbrecht was appointed honorary professor at the Universität der Bundeswehr Munich, Germany.
Conversations

Concerns, and what initiatives have you begun to identify threats and advise organizations on what they can do to protect their networks?

A big challenge is to look at the terms of reference and the service level agreement (SLA). The problem is if you are a small organization, or a citizen, you cannot negotiate SLAs in the same way that a big company can. You have to depend on your government to determine whether it has a role to play if there are privacy or legal framework issues. If you can't influence the terms of agreement, then perhaps you should look for a local provider.

The second point is about jurisdiction—if you have concerns about protecting your intellectual property rights when your data is in the cloud around the world, then you should look for a cloud provider who can give you the assurance it acts within a legal framework of a member state.

Finally, there's the discussion to be had about a 'European cloud,' a governmental cloud. This is a proposal which would mean national governments only being able to contract from cloud service providers based in that member state, to ensure security of service.

Is there any way we can improve the way governments and industry work together on solving these problems? How do we improve cooperation?

We have some good approaches in terms of public-private partnerships at a European level. If you talk about critical infrastructure industries, we already have good cooperation there—these companies are part of our advisory groups. There is always the question of how to get the small and medium-sized companies involved, because most of the industry input into our work comes from the larger corporations. The difficulty we face is to get more associations representing smaller companies involved; these companies just cannot afford to have representatives traveling around Europe to meetings all the time if the workforce is only 50-100 people.

So the challenge is to get different-sized companies involved.

What's your biggest challenge?

If you look at our critical infrastructures, we have a lot of companies connected to the Internet. Sometimes many of them don't really consider whether they have remote control of the service companies working with them, they don't really ask who has access to their company intranet.

For me, the whole issue of the Stuxnet affair was that it showed how everything is connected today. Stuxnet was about sabotage, but it showed in principle that everything connected to the Internet can be attacked. This is true whether it is criminals or terrorists trying to find a weak point in any of the connected devices. Everyone should be asking themselves: What do I connect to the Internet and who has access to the internal company network?