18/03/2009

Steve Purser, new Head of Technical Department at ENISA

As the new Head of Technical Department at ENISA, Steve Purser was asked to give us some of his views on ENISA's role in the changing European information society, what the current main challenges and the priorities for addressing these challenges are.

Prior to joining ENISA, Steve has been working in the IT sector since 1985, first as a software developer and project manager, then as a consultant. Since 1993, Steve has occupied the role of information security manager for a number of companies in the financial sector. He believes that his experience as a security officer, which involved both strategic and operational tasks, will be extremely useful at ENISA.

What are the main challenges for the future in the area of NIS?
Steve thinks that the main challenge for the future is to ensure that the European approach to NIS is both coherent across Member States and consistent in time. Coherence is necessary to avoid the creation of a weakest link and is compatible with the idea of building 'defence in depth' and consistency is necessary in order to progress to greater levels of maturity over time. Whilst this is the most fundamental challenge, the number one priority for action is the establishment of a proactive and knowledgeable community. He remarks that people currently behave differently in the electronic world to the way in which they behave in the real world and thinks that it will be necessary for everyone to develop a sort of 'electronic common sense' if they are to remain secure on the Future Internet. ENISA's role in making this happen is to support Member States and the Commission in identifying and implementing suitable policies and action plans. This will typically involve studying the current situation, identifying initiatives that have been successful to date and encouraging Member States to adopt similar initiatives. In its role as an information broker, ENISA is also ideally situated to spot opportunities and synergies with existing programs (such as the e-inclusion initiative) and to bring these to the attention of the different actors.

Of course, this cannot happen in a vacuum and any viable approach to improving NIS must take account of the speed with which technology is evolving and being adopted. Mobile computing continues to be highly challenging in this regard and the likely widespread adoption of RFID technology (as typified by the Internet of Things) and similarly highly-distributed technologies will have a major impact on the way in which we secure infrastructure and applications. Steve believes that the security models of the future will give a much more prevalent role to concepts such as trust and behaviour and will also be much more challenging in terms of managing identity and private data.

Finally, the approach to NIS must be economically viable both from a macroeconomic and microeconomic standpoint. People and organisations are unlikely to adopt measures and practices that carry a financial penalty.

What needs to be done to achieve this coherency and consistency?
Meeting these challenges clearly requires a strategic approach. The challenge is to help Member States achieve a suitable balance between national priorities and European priorities so that they can collectively commit to common goals. ENISA plays it's part in this by collecting and analysing data across Member States and by making recommendations based on the input of its stakeholders, which include representatives of both the public and private sectors.

What are the main priorities for addressing the evolving challenges to NIS?
Steve points out that the priorities reflect the challenges, as one would expect. The number one challenge is the creation of a knowledgeable and proactive community and a key idea is to move beyond the requirement for awareness. Awareness is a good first step, but does not contribute anything if it is not translated into concrete action at some point.

ENISA is currently working very closely with DGINFSO in the European Commission in the area of Critical Infrastructure and this is a very important stream of work. From a personal perspective, Steve comments that the current work could be complemented by looking into architectural approaches that place more emphasis on the security of the end-points in the network – the end-user workstation being particularly challenging here. He explains that this point of view is motivated by the number of attacks that have their origin at infected PCs and is substantiated by the rapid rise of botnets in the last few years. One idea here would be to identify practical methods for building architectures that enforce true End-to-End (E2E) security and to encourage their deployment. In the long term however, Steve believes that the industry as a whole will need to steadily improve methods for designing, developing and deploying secure systems.

The third priority is in the area of identity, privacy and trust. To understand this, it is helpful to try to imagine where personal data is being stored these days for the average citizen. Mobile computing has resulted in storage of personal data on a variety of portable devices, such as smart phones, personal computers, USB sticks and a number of other devices and the latest trend of social networking on the Internet encourages people to deposit snippets of information about themselves on several different sites. It is clear that managing multiple identities and private data in this environment is going to be extremely challenging. On the positive side, there are a

18/03/2009

number of interesting developments in the way we protect ourselves also. In particular, the increasing role of trust is becoming increasingly important, as exemplified by reputational based protection models such as one line auctioning and P2P protocols.

Finally, there is still work to be done to align security practices with the modern business model and the expectations of the average end user. In particular, current methods for managing and administering security on a day-to-day basis are limited to the extent to which they can cope with changes in scale of operations and/or operating conditions. We need to adopt approaches that are capable of providing short-term results without sacrificing strategic goals.

Could you explain what 'secure infrastructure' means?
- The information systems today are highly complex, they evolve rapidly and they are easy targets. Future infrastructure therefore must be capable of offering true end-to-end security including end user equipment. Ways in which this can be achieved include agreements on an architectural approach combining network security and end point security and also to reduce the delay between identifying emerging risks and availability of the definitive solution, which can be done through a faster deployment of research results.

What about the end-users?
- As already mentioned it is important to encourage electronic common sense among the Member States' citizens, the end-users. In reality, this means encouraging users to adopt the electronic world the same sort of intuitive risk-management techniques that they use in other areas of life. Most people would be cautious if they were approached by a complete stranger on the street asking them for personal information, whereas this doesn't necessarily seem to be so in the electronic world for instance. One way of dealing with this is to target the end-users with EU-wide information campaigns. It is clearly not the role of ENISA to carry out such campaigns, but it is our role to identify initiatives that already exist and to see to what extent they can be used to further this objective.
Getting back to the priorities already mentioned, Steve continues that one of the main considerations is to put people first, i.e. technology will only achieve its goal if it is used willingly and appropriately.

The notion of identity in global networks is, according to Steve, evolving rapidly and considerable scope for abuse/inappropriate use of personal information exists. In order to achieve trust among the citizens for using electronic networks there are several issues that have to be addressed. Some of the ways in which this challenge may be met are related to privacy-enhancing technologies and the development of guidelines for legislation.

18/03/2009

What do you think is the key to staying up to date with the latest security information?

- First of all this depends on who you are, whether you are a person, organisation or Member State. The information security arena is enormous and one of the real keys to getting the appropriate information is to know what you are looking for. In other words, asking the right questions is absolutely vital. Once the questions are known, it is very easy to become overwhelmed with details, but quite often these details are not necessary. A good rule of thumb is to seek to understand the information to the level required to make the decision that needs to be made. The idea of best practicesis quite interesting here. Interpreted correctly, it works well. However, there is an enormous amount of contextual information that is important in security and people and organisations need to think of how they can use these practices to protect their particular assets. Best practice for a butcher is not the same as best practice for a brain surgeon...

How will ENISA work to further promote risk assessment and risk management methods to the European society?

- ENISA has done a lot of work in the area of risk management and there is an entire Multi-Annual Thematic Program dedicated to emerging risk. In addition, we are continuously working on raising awareness to further enhance the development of the information society and to promote trust in online services and there will be a continued dialogue with the Member States and stakeholders. Passing of information and best practices are only some of the ways in which the awareness raising will continue. It is also important to bear in mind that there are different needs and interests in terms of NIS and these needs to be approached with different messages through different channels.

Risk management is of tremendous importance in terms of NIS, but according to Steve one thing that people sometimes forget when talking about risks is to also look for opportunities related to these risks. Indeed, it is difficult o discuss risks without taking into account the opportunities – people do not take risks for no reason. It is the balance between the opportunity and the risk, which decides the course of action.

- By closely following emerging risks, aligning research with these risks, and deploying research results faster, we will be able to securely leverage new technologies earlier.

For full CV of Steve Purser, new Head of Technical Department see:
http://www.enisa.europa.eu/pages/Structure_Head%20of%20Technical%20Department.htm