Interview – Giles Hogben

ENISA expert, Giles Hogben is the editor of the ENISA report *Web 2.0 Security and privacy*, which was put together by a group of industry, academic and government experts. In conjunction with this study, ENISA conducted a survey of 1,500 end users of Web 2.0 sites and applications.

Giles, why did ENISA conduct this report now and what were some of your findings?
One of the primary reasons for conducting this report is the huge increase in malware from compromised web sites – one report cites an increase of 407% in the year to May 2008. An important reason for this is that Web 2.0 involves a lot of so-called "user-generated content" – opportunities for ordinary users to contribute material to what is available on a web server - this which create a lot of what we call "injection points" - security loopholes for attackers.

The intention with the report is to provide an overview of Web 2.0 vulnerabilities, the key threats and risks to the security of users of Web 2.0 and, most importantly, recommendations for actions and best practices, which mitigate those risks.

The rapid increase in so-called "drive-by" malware infections requires no intervention or awareness on the part of the end-user and is often installed through Web 2.0 applications.

An example issue is that there are problems with the "Same-origin"-policy, which is the method of controlling access between applications served by different providers. There are many techniques for circumventing this policy for illegitimate purposes. Another threat in a Web 2.0 context is misuse of personal data by peers – for example indiscriminate tagging of images without consent. In addition to this there are very few developers with security training.

What do you hope to achieve with this report?
There are a lot of initiatives going on which are trying to improve Web 2.0 security, but there is no comprehensive approach. The rapid development of Web 2.0 has led to many security threats and vulnerabilities, which have not yet been addressed. A useful outcome of this report is that it presents a comprehensive approach. By the adoption

of a comprehensive set of measures aimed at addressing these vulnerabilities by governments, service-providers, standardization bodies and developers, the threats presented by the current wave of Malware 2.0 and other Web 2.0 related problems can be significantly reduced in order to realize the full benefits of this new technology.

Is there anything that ordinary citizens/everyday users need to know or think about?
The report highlights the need for awareness raising of the Web 2.0 security threats. One issue is that personal data is not only collected by service providers anymore, but there is now an additional component where people can post data about each other. Although it is only a research idea at the moment, one way of dealing with this in the future might be that you can actually license your own personal data in the same way as you license a piece of software, which might help in a social networking context.

For full report:
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_web2.pdf

For press release:
http://www.enisa.europa.eu/pages/02_01_press_2008_12_10_web2.html

For FAQ:
http://www.enisa.europa.eu/pdf/faq_web_2.pdf