News reuschlaw Legal Consultants.

Secure by Design

by Philipp Reusch

Background

Cyber-attacks and security gaps which manifest themselves in devices with an Internet connection are posing a growing risk to users. This in turn represents a major impediment to the ongoing introduction of the Internet of Things (IoT). Whilst so far the EU has not let itself get carried any further than declarations of intent, the 'Department for Digital, Culture, Media & Sport' from Britain has come forward with an actual concept proposal. Above all, that proposal puts responsibility on manufacturers and IoT service providers.

The actual content

The department's proposal consists of thirteen guidelines, geared to some extent toward existing best practice measures. The guidelines are listed in order of importance. (You will find a full list here.) In the area of product liability the concept impinges mainly on manufacturers' obligations relating to design, though their obligations to issue proper instructions and their product surveillance obligations are also strongly affected.

First priority for manufacturers is to ensure that unique passwords are used on all IoT products and that these cannot be reset to a universal default value. Furthermore, manufacturers should make sure that their products receive software updates in due time and securely without any impairment of the functionality of the product. In addition to that, manufacturers must, in an 'end-of-life policy', state the period for which the product is to receive software updates. Last but not least, an obligation to guarantee an encrypted transmission of security-relevant data via the Internet is also incumbent on manufacturers.

Finally, the concept also has a bearing on the obligation of manufacturers to inform. For example, the necessity of each and every update should be made clear to the user, and the user should be enabled to implement it in a user-friendly way. The user should also receive clear instructions on how to delete personal data on the product. Given that instructions for use must – from every point of view – be able to be understood by the least well informed user, there is a very considerable amount of work to be done here in terms of enlightenment and explanation.

As its second most important point, the concept provides for manufacturers to deploy a public contact for the disclosure of weaknesses. Manufacturers not only have to keep an eye on their product with a view to security gaps and necessary updates; they must also be available for a communication process. There are, for example, also obligations on them to notify in respect of risks discovered or attacks to which they may have been exposed.

Summary

The concept provides some explanation of the way risk will be distributed in future laws in the area of cyber security. During the rest of this year, the department will be observing voluntary implementation and its effectiveness. If the guidelines prove effective, the concept will be able to serve as a model all over Europe. In the interests of their own competitiveness and those of a reduced liability risk, manufacturers would be well advised to implement appropriate security standards early on.

reuschlaw Legal Consultants
reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cyber security and data protection, compliance management and contract law. The sectorial focus is on companies in the machine manufacturing and automotive supply industries, the consumer goods industry and manufacturers of medical devices and cosmetic products.

Company contact: Melanie Schuh / Head of Marketing & Communications / T +49 30 2332895-0 / E melanie.schuh@reuschlaw.de