Cyber security by design – new UK guidance and EU certification schemes

13 June 2019

What does 'good' cyber security look like? In this briefing we look at how guidance recently published by the UK's NCSC, and a new cyber certification scheme at EU level, may help organisations answer this question.

Most UK and EU law relating to cyber security is technology neutral, focussing on organisations having 'appropriate technical and organisational measures' in place. However, there is a growing list of resources available which aim to provide more certainty to the market regarding what this means in practice. In this briefing we look at two recent examples of this – at UK level the National Cyber Security Centre (NCSC) has recently published new Cyber security design principles for the design of cyber secure systems, and at EU level the new Cyber Security Act, which comes into force later this month, establishes a Europe wide cyber certification scheme.

NCSC Cyber security design principles

The NCSC published cyber security design principles to help ensure that the 'networks and technologies which underpin modern life are designed and built securely.' The design principles are built around five categories, loosely aligned with stages at which an attack can be mitigated:

1. **Establishing the context:** determine all the elements which compose your system, so your defensive measures will have no blind spots. This will involve, for example, understanding the threat model for your system, which risks are acceptable and what role suppliers play in establishing and maintaining your system. You should also be clear about how you govern security risks.

2. **Making compromise difficult:** an attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible, treat any external data with suspicion and make it easy for users to do the right thing (to prevent them developing workarounds which create security risks).

3. **Making disruption difficult:** design a system that is resilient to denial of service attacks and usage spikes and, where availability depends on a third party, plan for the failure of that third party.

4. **Making compromise detection easier:** design your system so you can spot suspicious activity as it happens and take necessary action.

5. **Reducing the impact of compromise:** if an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible. For example, avoid unnecessary caches of data and anonymise data when it is exported to reporting tools.

The NCSC have also published a set of 6 security architecture 'anti-patterns' - common system design flaws – that they have witnessed over the last decade.

Although the NCSC's guidance is aimed at people who design systems, it is important that those advising on cyber risk management and technology procurement understand the guidance that is available, and consequently what regulators will expect, in this area.

EU Cyber certification

While guidance can help organisations understand how to design secure systems, certification schemes provide them with comfort that the information and communications technology (ICT) products or services they buy (or sell) have been designed with security in mind. The EU Regulation on ENISA and Cyber Security Certification (also referred to as the Cyber Security Act), which comes into force across the EU on 27th June, aims to harmonise the EU's approach to cyber security schemes.

As well as clarifying ENISA's role as the EU's Agency for cyber security, the Regulation sets up a framework to govern voluntary European cyber security certification schemes. Its intention is to increase trust and security of ICT products and services (its recitals discuss 'security by design'), and to address the current fragmentation which exists regarding certification schemes.

The Regulation does not introduce directly operational certification schemes. Rather it creates a system which allows schemes to be established and recognised across the EU. For example, it:

- provides for a rolling work programme to be established which will identify strategic priorities for the schemes and include a list of ICT products, services and processes capable of benefitting from being included in the scope of a European cyber security certification scheme. The first rolling work programme is due to be published by next May;

- enables schemes to specify one or more of three assurance levels of certification – basic, substantial and high and states that schemes may also allow for self-assessment by manufacturers or providers in certain low risk situations; and

- confirms that national cyber security schemes that are not covered by a European cyber security certifications scheme shall continue to exist.

Although the schemes are voluntary, the Commission must regularly assess whether any schemes should be made mandatory and the first assessment must be carried out by the end of December 2023. The Regulation also confirms that the Commission will focus 'as a priority' on the sectors listed in the NIS Directive (for more information on the NIS regime, see our NIS briefing), which must be assessed 'at the latest' two years after the adoption of the first scheme.

Comment

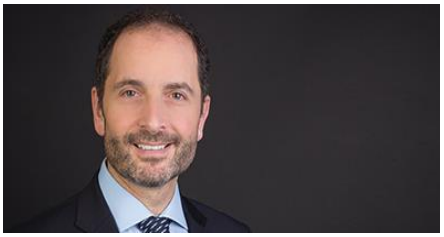
It can be difficult for organisations to know if they have sufficient (or appropriate) processes and measures in place to mitigate a growing cyber risk. The publication of guidance and principles is helpful. However, the volume at which these are being produced means it can sometimes be difficult for organisations to keep pace.

One way in which legislators and regulators can help organisations ensure that the ICT products and services they buy and sell are 'secure by design' is to introduce trusted certification and kitemark schemes. The GDPR already enables this for data protection (no schemes yet exist, but EDPB certification guidelines and annexes have recently been published) and it is encouraging that ENISA will establish EU wide schemes for cyber. Cyber certification schemes do currently exist, for example the UK Cyber Essentials Scheme has been running for 5 years now. However, an EU wide scheme which aims to combat fragmentation of certification at EU level is particularly welcome. While its impact on any UK schemes (given Brexit) may be limited, the Regulation (in its recitals) does include conditions for the mutual recognition of schemes with third countries.

This article was written by Rob Sumroy and Natalie Donovan of Slaughter and May's Cyber Advisory Team.

Our Cyber Advisory team can help your business plan for and manage your cyber risk, working closely with you to develop tailored cyber risk management frameworks and training and response plans, providing hands-on support to your internal stakeholders in the event of a cyber attack, and helping you to mitigate cyber risk generally in your business.

For more information, please contact Rob, Natalie or your usual Slaughter and May contact.



Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com