PROPOSAL 15.9.2022, CYBER RESILIENCE ACT

The Articles of the Cyber Resilience Act

Annex 1

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Cyber Resilience Act Text 15.9.2022 (https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles_(Proposal_15.9.2022).html)

You may also visit:

NIS 2 Directive (https://www.nis-2-directive.com)

Digital Operational Resilience Act (DORA) (https://www.digital-operational-resilience-act.com)

European Chips Act (https://www.european-chips-act.com)

CONTACT DETAILS

Cyber Risk GmbH, Dammstrasse 16, 8810 Horgen

+41 79 505 89 60

george.lekatis@cyber-risk-gmbh.com (mailto:george.lekatis@cyber-risk-gmbh.com;)

www.cyber-risk-gmbh.com

SUPPORT

Cyber Risk GmbH has been established in Horgen, Switzerland (Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341).

The founder of the firm is George Lekatis. George has provided training

SERVICES

Home (https://www.cyber-risk-gmbh.com)

About (https://www.cyber-

Social Engineering (https://www.cyber-risk-gmbh.com/Social_Engineering.html)

High Value Targets (https://www.cyber-

(https://www.cyber-risk-gmbh.com)	and executive coaching in information security and risk management to many leading global organizations in 36 countries.	risk-gmbh.com/About.html)	risk-gmbh.com/High_Value_Targets.html)
		Training (https://www.cyber-risk-gmbh.com/Training.html)	Reading Room (https://www.cyber-risk-gmbh.com/Reading_Room.html)
		For the Board (https://www.cyber-risk-gmbh.com/Board.html)	Contact (https://www.cyber-risk-gmbh.com/Contact.html)
		Assessment (https://www.cyber-risk-gmbh.com/Assessment.html)	Impressum (https://www.cyber-risk-gmbh.com/Impressum.html)