European Parliament
2014 - 2019

Committee on Industry, Research and Energy

26/04/2018

AMENDMENTS: 14

Angelika Niebler
Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Proposal for a regulation COM(2017)0477 - C8-0310/2017 – 2017/0225(COD)

Amendments created with

Go to http://www.at4am.ep.parl.union.eu

Amendments per language:

EN: 14

Amendment 1
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 1 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union. Such framework shall apply without prejudice to specific provisions regarding voluntary or mandatory certification in other Union acts.	(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products***, processes*** and services in the Union. Such framework shall apply without prejudice to specific provisions regarding voluntary or mandatory certification in other Union acts.

Or. en

Justification

This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.

Amendment 2
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 2 – paragraph 1 – point 10

Text proposed by the Commission	*Amendment*
(10) 'European cybersecurity certificate' means a document issued by a conformity assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;	(10) 'European cybersecurity certificate' means a document issued by a conformity assessment body attesting that a given ICT product***, process*** or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

Or. en

Justification

This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.

Amendment 3
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 3 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. The Agency shall assist Member States and Union institutions in establishing policies and practices for the responsible management and coordinated disclosure of vulnerabilities in ICT products and services that are not publicly known.

Or. en

Justification

These policies should be consistent with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.

Amendment 4
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 4 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7 a. The Agency shall assist and advise Member States and Union institutions in establishing policies and practices for the

	responsible management and coordinated disclosure of vulnerabilities in ICT products and services that are not publicly known, inter alia by establishing government vulnerability disclosure review processes and coordinated vulnerability disclosure policies.

Or. en

Justification

This task shall be executed in accordance with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.

Amendment 5
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 5 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148, including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;	2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148, including by means of opinions, guidelines, advice and best practices on topics such as ***secure software and systems development,*** risk management, incident reporting and information sharing***, technical and organisational measures, in particular the establishment of coordinated vulnerability disclosure programmes***, as well as facilitating the exchange of best practices between competent authorities in this regard;

Or. en

Justification

The NIS-Directive leaves open the range of measures a company can take in order to ensure compliance as part of the "technical and organisational measures" prescribed in Article 14 of

Directive (EU) 2016/1148. These measures can include the establishment of a coordinated vulnerability programme, and Member states may explicitly consider parameters regarding the establishment of such a programme in transposing the NIS Directive. ENISA can provide guidelines on how to create such a CVD-programme in order to create a consistent European approach to coordinated vulnerability disclosure that is consistent with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.

Amendment 6
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 5 – paragraph 1 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. proposing a blueprint which establishes the roles, responsibilities and legal obligations of vendors, manufacturers, CERTs and CSIRTs, and which further clarifies the legal rights and protections of information security researchers in the context of a coordinated vulnerability disclosure programme, in particular in cases of multi-party vulnerability disclosures that affect multiple vulnerability finders and vendors in different EU Member States

Or. en

Justification

The Meltdown and Spectre vulnerabilities have demonstrated the need for EU-wide coordinated vulnerability disclosure programmes whose scope goes beyond operators of essential services. This blueprint shall be consistent with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111.

Amendment 7
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill

Proposal for a regulation
Article 5 – paragraph 1 – point 4 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	(2 a) the development and promotion of policies that would sustain the general availability or integrity of the public core of the open internet, which provide the essential functionality to the Internet as a whole and which underpin its normal operation, including, but not limited to, the security and stability of key protocols (in particular DNS, BGP, and IPv6), the operation of the Domain Name System (including those of all Top Level Domains), and the operation of the Root Zone

Or. en

Justification

The protection of the public core of the internet is an emerging norm that is supported by the Global Commission on the Stability for Cyberspace, which received its mandate from the conclusions of the 4th Global Conference on CyberSpace (GCCS) held in 2015 in The Hague, as well as the 5th Report of the UN Group of Governmental Experts.

Amendment 8
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 6 – paragraph 1 – point a a (new)

Text proposed by the Commission	*Amendment*
	(a a) Members States and Union institutions in establishing and implementing coordinated vulnerability disclosure policies and government vulnerability disclosure review processes, whose practices and determinations should be transparent and subject to independent oversight.

Or. en

Justification

A government vulnerability disclosure review process involves the management of vulnerabilities discovered by governmental agencies and establishes a process which determines when and how the governmental agency must release the vulnerability in its possession. Ensuring that governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is a critical norm that should be advanced within the EU.

Amendment 9
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 7 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7 a. The Agency shall prepare, together with the EEAS, a regular global Cybersecurity Situational Report on incidents and threats towards individuals, including towards vulnerable users outside the EU such as lawyers, journalists, or human rights defenders, in order to help the Union institutions respond to external needs and uphold its human rights responsibilities abroad

Or. en

Amendment 10
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 7 – paragraph 8 – point e a (new)

Text proposed by the Commission	*Amendment*
	(e a) assisting and advising Member States on establishing and implementing

coordinated vulnerability disclosure policies and government vulnerability disclosure review processes.

Or. en

Justification

This task shall be executed in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111.

Amendment 11
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 8 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) support and promote the development and implementation of coordinated vulnerability disclosure policies and government vulnerability disclosure review processes

Or. en

Amendment 12
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill

Proposal for a regulation
Article 46 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. The methodology to distinghuish between the different assurance levels should be guided by a test which assesses the resistance of the security functionalities against attackers that have significant to unlimited resources.

Or. en

Amendment 13
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 47 – paragraph 1 – point j

Text proposed by the Commission	*Amendment*
(j) rules ***concerning how previously undetected cybersecurity*** vulnerabilities in ICT products and services ***are*** to be reported ***and dealt with;***	(j) rules ***requiring*** vulnerabilities in ICT products and services ***that are not publicly known*** to be reported ***expeditiously by the appropriate authorities to relevant vendors and manufacturers using a coordinated vulnerability disclosure process.***

Or. en

Justification

These state-linked authorities (such as national CERTS) should eventually share vulnerability information off all ICT products and services with affected vendors and manufacturers. This task shall be executed in accordance with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111. State authorities that are 'finders' have very different risk profiles, incentives, obligations, and power vis-a-vis affected vendors and manufacturers compared to individual security researchers.

Amendment 14
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposal for a regulation
Article 47 – paragraph 1 – point m a (new)

Text proposed by the Commission	*Amendment*
	(m a) Rules concerning how and when Member States must inform each other when they acquire knowledge of a vulnerability that is not publicly known in an ICT product or service that is certified under this certification scheme.

Or. en