

A Comparative Study between Japan and the European Union on Software Vulnerability Public Policies

Authors : Stefano Fantin

Abstract : The present analysis outcomes from the research undertaken in the course of the European-funded project EUNITY, which targets the gaps in research and development on cybersecurity and privacy between Europe and Japan. Under these auspices, the research presents a study on the policy approach of Japan, the EU and a number of Member States of the Union with regard to the handling and discovery of software vulnerabilities, with the aim of identifying methodological differences and similarities. This research builds upon a functional comparative analysis of both public policies and legal instruments from the identified jurisdictions. The result of this analysis is based on semi-structured interviews with EUNITY partners, as well as by the participation of the researcher to a recent report from the Center for EU Policy Study on software vulnerability. The European Union presents a rather fragmented legal framework on software vulnerabilities. The presence of a number of different legislations at the EU level (including Network and Information Security Directive, Critical Infrastructure Directive, Directive on the Attacks at Information Systems and the Proposal for a Cybersecurity Act) with no clear focus on such a subject makes it difficult for both national governments and end-users (software owners, researchers and private citizens) to gain a clear understanding of the Union's approach. Additionally, the current data protection reform package (general data protection regulation), seems to create legal uncertainty around security research. To date, at the member states level, a few efforts towards transparent practices have been made, namely by the Netherlands, France, and Latvia. This research will explain what policy approach such countries have taken. Japan has started implementing a coordinated vulnerability disclosure policy in 2004. To date, two amendments can be registered on the framework (2014 and 2017). The framework is furthermore complemented by a series of instruments allowing researchers to disclose responsibly any new discovery. However, the policy has started to lose its efficiency due to a significant increase in reports made to the authority in charge. To conclude, the research conducted reveals two asymmetric policy approaches, time-wise and content-wise. The analysis therein will, therefore, conclude with a series of policy recommendations based on the lessons learned from both regions, towards a common approach to the security of European and Japanese markets, industries and citizens.

Keywords : cybersecurity, vulnerability, European Union, Japan

Conference Title : ICCIS 2019 : International Conference on Cyber Crime and Information Security

Conference Location : Tokyo, Japan

Conference Dates : April 22-23, 2019