Encouraging responsible vulnerabilities disclosure

OECD Global Forum on Digital Security for Prosperity
14 December - Paris

Lorenzo Pupillo, Associate Senior Research Fellow and Head of the Cybersecurity@CEPS Initiative
Centre for European Policy Studies (CEPS)

About CEPS

CEPS is one of Europe's leading independent think tanks providing a:

- Central and neutral forum for debate among all stakeholders in the EU policy process.
- Important contributions to the policymaking process thanks to a strong in-house research capacity combined to an extensive network of partner institutes throughout the world

SVD in the EU

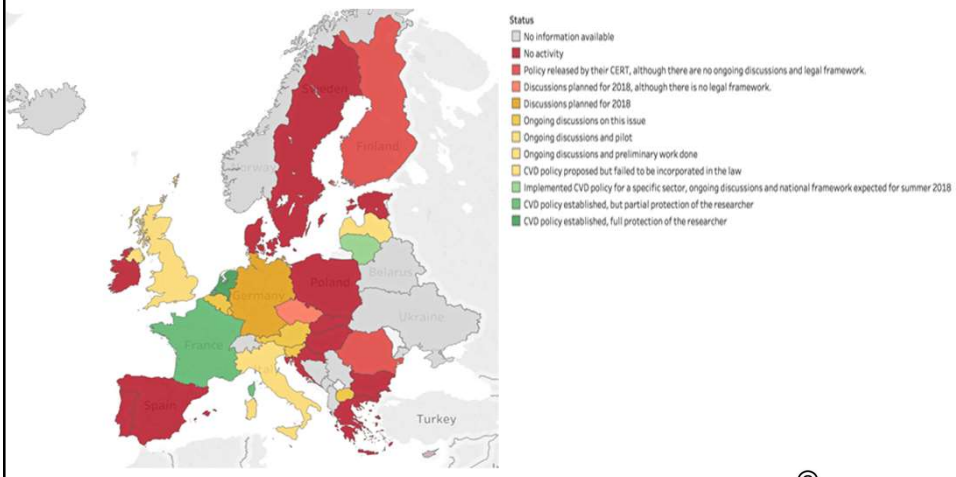
- In 2016, the European Union Agency for Network and Information Security (ENISA) published a report on "Good Practice Guide on Vulnerability Disclosure"

- The Joint Research Centre of the European Commission, and in particular the Cyber and Digital Citizens' Security Unit, carried out research on the vulnerability disclosure process. In the first quarter of 2017, it organised a workshop on zero-day vulnerabilities with representatives from academia, industry and government. The main conclusions were:
  - Research should be the main driver for discovery,
  - An EU-wide independent third party should act as coordinator and
  - A pilot EU vulnerability management centre should serve as a test-bed platform for responsible and coordinated vulnerability disclosure.

- The joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to the European Parliament and the Council of September 2017, mentioned the "important role of third party security researchers in discovering vulnerabilities in existing products and services need to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practices and relevant standards".

- THE BRAHAM PRECISION LOCK FOR A BOX (1784)

A mapping of the state of play, by country



How did the Dutch prosecutor ensure compliance with criminal law?

- Establish *unlawfulness/lawfulness* of the act – three principles
  - Motives
    - What are the ethical motives of the hacker?
  - Subsidiarity
    - If once a hacker discovers a vulnerability, he discloses this to the system owner → ethical hacking
  - Proportionality
    - If he ***does more*** than that (intentionally or unintentionally), the prosecutor will probably launch a criminal investigation
    - *E.g.*, copying of sensitive data or personally identifying information

POLICY IMPLICATIONS

- The Task Force calls upon the European Commission and the member states to collectively draft a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure.
- The National Cyber Security Centre (NCSC) in the Netherlands has published a general guideline for responsible disclosure, which can serve as a useful model that EU member states can follow in drafting their own responsible disclosure policy. In addition, it gives reporters guidance on how to act in finding and reporting a vulnerability.
- The Coordinated Vulnerability Disclosure Template from the NTIA
- It's also worth mentioning that the Cybersecurity Unit, Computer Crime and Intellectual Property Section Criminal Division of the U.S. Department of Justice, in July 2017 released the first version of the framework for a "Vulnerability Disclosure Program for Online Systems" that EU member states could examine as a possible model.

Steps for implementing coordinated vulnerability disclosure processes in Europe 1/ 2

- ***Private sector***
- The private sector could take the lead in implementing coordinated vulnerability disclosure defining and publishing on companies' website public reporting mechanisms on vulnerabilities disclosure according to the ISO standards.
- ***CERTs***
- CERTs should help in putting in place a framework to implement coordinated vulnerability disclosure processes playing the role of thrusted third party and coordination center in this process.

Steps for implementing coordinated vulnerability disclosure processes in Europe 2/ 2

- ***Member states***
- Member states should act in creating the necessary legal certainty for security researchers involved in vulnerability discovery, changing national legislation to allow for the recognition of ethical hacking.
- ***EU***
- The EU should change the European legislation to allow for legal certainty for security researchers involved in vulnerability discovery and to allow for the definition of common rules and procedures across member states to allow for a common process of software coordinated vulnerability disclosure in Europe.

GDDP : Government Disclosure Decision Process

- INCLUSIVE PROCESS: All relevant ministries, including those with missions for user, business, and government security, should participate in the GDDP and participants should work together using a standard set of criteria to ensure all risks and interests are considered.
- The policies, practices, and determinations of the GDPP should be subject to independent oversight and transparency.
- The executive secretariat of the GDPP should be housed within a civilian agency with expertise in existing coordinated vulnerability disclosure.
- The GDDP should be codified in law or other legally binding policy to ensure compliance and permanence.
- The default policy should be to disclose vulnerabilities immediately to the affected vendor(s) so they can be patched.
- Where the vulnerability potentially affects the safety of regulated products (such as cars, medical devices or railway signals, the relevant EU safety and standards bodies should be involved in the GDDP.

Down load the Report

- https://www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges
- lorenzo.pupillo@ceps.eu