CEPS EVENT REPORT

Thinking ahead for Europe

CEPS Task Force
on
Software Vulnerability Disclosure in Europe
2nd Meeting, 29 November 2017

Background

Launched on 27 September 2017, the CEPS Task Force on Software Vulnerabilities Disclosure focuses on key aspects surrounding the debate on software vulnerability disclosure (SVD) in Europe. The Task Force is exploring ways to arrive at guidelines for governments and businesses to harmonise the process of handling SVD throughout Europe. At its completion, the members will outline specific principles and formulate policy recommendations directed at EU member states and institutions in the development of an effective policy framework for introducing a process of so-called coordinated vulnerability disclosure (CVD) in Europe. For more background information on this initiative, please click here.

2nd meeting of the Task Force

With the recent addition of Kaspersky, the European Data Protection Supervisor and the Center for Democracy & Technology to our ranks, total membership of the Task Force now numbers 17: 9 from the private sector, 6 from the EU institutions and 2 from civil society.

This second meeting was devoted to reports on:

- mapping the CVD models currently in use in Europe,
- evaluating specific best practices (Latvia & Japan)
- the results of an ad hoc analysis of the legal constraints in the implementation of CVD in Europe across member states and
- testing the feasibility of extending the Dutch model of CVD to other European countries.

The activity of the Task Force is very urgent. In November, the White House released a report on Vulnerability Equity Process. This is a welcome initiative and shows that the US is currently ahead of the EU in debating this issue and underlines the urgency of the work of the TF. In this respect, maximum transparency within the EU, the member states (MS) and among other stakeholders is key. In fact, it is the foundation on which both citizens and decision-makers alike will base their trust in the digital economy. It is a shared responsibility among stakeholders to look at how to improve the resilience of our digital infrastructure in order to prevent attacks that could challenge our democracy.

The preliminary mapping exercise shows that the EU needs a united and harmonised policy framework to enhance CVD capability. The Task Force is working on a map of the VD practices in the MS, which should give an idea of the state of the art at national level across the EU. The information is collected directly from the national CSIRTs (Computer Security

Incident Response Teams) and governments' cybersecurity departments. The work will address three fundamental questions:

1) Which MS have established a governance structure on VD and do they have processes in operation?
2) How is the decision-making process on VD structured and how is actual vulnerability disclosed?
3) Which policies for coordination with other institutions and information-sharing mechanisms are in place?

The preliminary analysis presented shows that some MS have taken ad-hoc initiatives (with varying degrees of success) on CVD:

- Belgium: in 2014, the national CERT (computer emergency response team) published a Responsible Disclosure Policy.
- Finland: in 2010, Cybersecurity Centre Finland published a Vulnerability Coordination Policy, which was updated in 2012.
- Lithuania: a VD framework is in place.
- Luxembourg: a responsible vulnerability disclosure process for the private sector is provided, but it is not yet a CVD policy at national level.
- Romania: the national CERT has posted a CVD policy on its website.
- UK: operates an ongoing pilot project on Vulnerability Coordination.
- Latvia: has designed a model but has failed to put it into law.
- The Netherlands: has put in place a more consolidated model of CVD.

Many MS, however, have not yet put a policy in place or have not made any relevant information available. Therefore, the Task Force members have decided to complete the exercise involving a new round of queries, targeted at individuals who are more knowledgeable about these processes.

However, we can clearly state that there are significant differences across MS at the present time.

The experiences of Latvia and Japan

Latvia

In 2016, the CERT of Latvia was planning to put CVD into law, but in the end, the initiative failed. Launched by the Minister of Defence, the initiative led to a proposal that was sent to the cabinet of the Ministers with the aim of transposing the process into law. It was directed to public institutions and municipalities, not to private actors. The process would have started with the researcher finding the vulnerabilities (V) and then informing the CERT within 5 days of his/her discovery. The coordinating body (CERT) would have verified the V and informed the owner of the system, who would have been obliged to fix the V within 3 to 6 months. Subsequently, the system owner would have informed the CERT and the CERT would have informed the researcher, who could have published it. As stated, earlier, however, the initiative failed. The proposal went to the cabinet of the Ministers, where it was approved, but

then objections were raised by the State police. State police insisted on the creation of a register of researchers, which would have eliminated any possibility of anonymity, which is an essential feature of any such scheme. Therefore, it was decided by the authors of the initiative to drop the proposal.

The report on Latvia also mentioned that its CERT receives reports mostly from and within Latvia, with little cross-border exchange. Furthermore, the country's coordination on vulnerabilities with other national CERTs is effective. On the issue of coordination, it was suggested that ENISA might work with vendors in a common forum. An EU CERT, however, would not be the solution. In 1999, there was an attempt to create an EU CERT, but it never scaled up. However, ENISA could coordinate the various national responses whenever the national CERTS discover a vulnerability in a product that is used throughout the EU. An alternative solution could be that ENISA would provide guidelines on the reporting process.

Japan

The vulnerability disclosure process in Japan is jointly managed by an independent, non-profit organisation called the JPCERT/CC, funded by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA), a policy implementation agency under the jurisdiction of METI. It focuses on the coordination of vulnerabilities between researchers and vendors through a standardised process (handling and disclosure). All vulnerabilities reported must be coordinated by the JPCERT/CC with a vendor until the vendor provides a fix to the problem and an advisory on Japan Vulnerability Notes (JVN) is published. Within this framework, a case is not officially closed until it is publicly announced on JVN. At the present time, some processes need to be simplified/automated in order to speed up to process of making vulnerability reports available to the vendors so that the vulnerabilities can be addressed in a timely fashion. For such a coordination framework to function as intended, it is best to provide the proper incentives to both reporters and vendors. Third-party coordinators could offer a good solution in circumstances in which multiple parties need to be urgently contacted at the same time.

Legal constraints on the implementation of a CVD across MS in Europe

Among the many challenges to address in implementing a vulnerability disclosure process across EU member states is the relationship of this process to criminal law. Two critical issues need to be considered: 1) When would vulnerabilities search and sharing be considered a criminal offence? 2) In the event that a vulnerability serach is considered a criminal offence, under which circumstances can it be prosecuted? There are three relevant EU legislative instruments for dealing with hacking as a criminal offence: 1) the 2001 Council of Europe Convention on Cybercrime, 2) Directive 2013/40/EU on attacks against information systems and 3) national legislation. The problem, however, is that there is no single interpretation of what constitutes hacking across member states. A possibly solution to this problem is to use prosecutorial discretion when it exists (like in the Netherlands) or to find other ways such as

the 'médiation pénale' as is in France. The fundamental issue is to provide more legal certainty to the CVD process, also through ad-hoc legislation. The discussion suggested the need to work on designing a set of potential vehicles to help circumvent these obstacles.

Evaluating the feasibility of extending the Dutch model of CVD to other European countries

The key to the success of the CVD process adopted in the Netherlands was the creation of a common space in which researchers and organisations could work out problems, without involvement of the government or law enforcement authorities. The guidelines for this process are written in such a way that other organisations (including government organisations) can use them as building blocks for creating their own policy and/or guidelines. The model attempts to create a basis for solid cooperation between organisations and reporters, without having to create specific laws and/or exemptions. The Dutch legal system has the flexibility to make this possible, but, as it turns out, communication is the key issue. Organisations should realise that their internal processes are not immediately or easily evident to the security researcher. Indeed, the latter are most often motivated by recognition. Regular updates from an organisation on the process will prevent a lot of frustration. On the other hand, it is hard for security researchers to strike the right tone towards an organisation and to clearly explain what is happening.

Next Steps of the CEPS SVD Task Force

- Complete the **mapping of the CVD models** currently in use in Europe
- Design a **set of potential vehicles** to manage the current legal constraints
- Prepare a **draft of the first part of the final report** on CVD for discussion at the next meeting on January 31st
- Start the analysis and discussion of the **Vulnerability Equity process** on January 31st
- Discuss plans for organising an **event at the European Parliament** to present the final report of the TF by the end of February

Lorenzo Pupillo
Afonso Ferreira
Gianluca Varisco
Antonella Zarra
Brussels, 23 December 2017