CEPS EVENT REPORT
Thinking ahead for Europe

CEPS Task Force
on
Software Vulnerability Disclosure in Europe
Kick-off meeting, 27 September 2017

Introduction

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

The new group is composed of the following members:

- Chair: Marietje Schaake, Member of the European Parliament
- Task Force Coordinator: Lorenzo Pupillo, Associate Senior Research Fellow and Head of Cybersecurity Policy, CEPS
- Representatives of the private sector: Airbus, Cloudflare, Enter, ETNO, ICANN, Mozilla, Microsoft and SAP
- Representatives of the EU institutions: Council of the European Union, DG Connect, DG Home Affairs and JRC European Commission
- Representative of European government: Dutch National Cyber Security Centre
- Representative of Civil Society: Access Now
- Advisory Committee: Ross Anderson, Cambridge University; Michael Daniel, Cyber Threat Alliance; Allan Friedman, NTIA; Andriani Ferti, Karatzas & Partners Law Firm; Trey Herr, Belfer Center, Harvard University; and Tim Watson, Warwick University
- Rapporteurs: Afonso Ferreira, Directeur de Recherche CNRS; Gianluca Varisco, Cybersecurity Expert, Italian Digital Transformation Team; and Romain Bosc, Research Assistant, CEPS

This inaugural meeting was devoted to setting the scene and organising the workflow for the activities of the Task Force. This report offers some takeaways from the first meeting.

The activity of the Task Force is very timely.

The recently released new EU Cybersecurity Strategy underlines the need to create the necessary enabling conditions to implement coordinated vulnerability disclosure across member states. In a context in which the EU pledges to reinforce its cyber capabilities and resilience, the Council has announced a joint EU diplomatic response to cybercrime and malicious activities, as illustrated by its so-called cyber-diplomacy toolbox, designed in response to the recent large-scale attacks.

The aim of the Task Force is to provide inputs to policymakers involved in setting up a European Coordinated Vulnerability Disclosure (CVD) model, aimed at serving the interests of all stakeholders involved.

The EU needs a harmonised policy framework to enhance CVD capability

National cybersecurity agencies are taking measures to ensure the proper handling of vulnerabilities within their organisations, in coordination with third parties. They are also raising awareness within the private sector on what companies should do to implement proper vulnerability-handling processes with a view to creating a more secure business environment.

The Dutch National Cyber Security Centre (NCSC) is showing the way forward. With its Global Forum on Cyber Expertise (GFCE), the Netherlands has been the first country in Europe to organise such an inclusive programme in cooperation with other governments and private partners.

The French national cybersecurity agency, ANSSI (Agence nationale de la sécurité des systèmes d'information), has also engaged in discussions in view of the proposed Loi Numérique, mostly exploring ways to protect 'white hats', a reference to ethical hackers who discover and report security breaches and vulnerabilities. The bill also suggests that ANSSI would play a role as a platform for security breaches and vulnerabilities reporting.

Last March, the National Cyber Security Centre in the UK also set up a "Vulnerability Coordination Pilot project".

Most of these initiatives are rooted in international standards such as ISO 29147 for external processes relating to coordination between finders and vendors, and ISO 30111 for vendors' internal processes of investigating, diagnosing and patching. Governments and companies have been applying those norms in very different ways, however, if at all. For instance, not all vendors have robust patch management processes in place in the event an incident occurs.

Another aspect is that current policy frameworks and practices in place so far also need to be reconsidered in light of the development of future technologies and market trends, such as the internet of things (IoT), autonomous vehicles and artificial intelligence.

Public- and private-sector cooperation should make safety and security principles go hand-in-hand

With the growing integration of cyber physical systems (CPS) into industrial and civil environments, safety and security rationales must converge: "Phones and laptops don't kill many people directly: cars and medical devices do..."[1]

In an environment where items collect and exchange data with each other, the attack surface tremendously expands due to the countless access points adding on the network. This also makes malware transmission possible simply from systems to systems without being connected to the public internet.

This context presents engineers, researchers and regulators with numerous new challenges, such as embedding security and safety into technical standards, e.g. based on security-by-design and security-by-default principles. However, ensuring sustainability in software and in the supporting tool-chains is proving more challenging than one might expect: "How do we write code for which security patches must be made available for the next 30 years?" Furthermore, liability and privacy policies must be carefully reconsidered.

Public intervention is needed but the adequate legal response remains unclear

The Dutch government has been at the forefront on this matter, with the Ministry of Security and Justice and Public Prosecution Services advocating soft law and self-regulatory solutions. In 2013, the NCSC introduced guidelines for responsible disclosure, addressing the technical and legal barriers in implementing a proper CVD policy and providing practical solutions for organisations to help integrate diligent vulnerability handling processes and disclosure management into their business practices.

In the US, a new bill, Protecting Our Ability to Counter Hacking Act (or PATCH Act), was introduced with the aim of enshrining their so-called vulnerability equities process (VEP) into law. Such a policy specifies how vulnerabilities should be reported to vendors.

One critical aspect of disclosing vulnerabilities are the legal issues that individuals face when searching and reporting on security flaws. The legal implications are broad, touching on civil and criminal laws, but also contract law, licensing, patent law and other types of legislation, e.g. export controls and trade agreements.

Governments must provide more guidance about what constitutes an offense and must give vulnerability finders and reporters a clear pathway to lawfully point to vulnerabilities and breaches that might be further exploited.

Unauthorised access to information systems is considered a crime in most countries, but the discretion for prosecution (and sanctions) largely varies across the EU, especially depending on the national legal traditions, either based on Common Law or Civil Law. Moreover, there are also implications regarding privacy laws, where the EU's General Data Protection Regulation (GDPR) also significantly impacts the disclosure process.

[1] "Standardisation and Certification in the 'Internet of Things'", Éireann Leverett, Richard Clayton and Ross Anderson, PPT presentation, WEIS, 26 June 2017.

The Task Force aims to investigate the many legal and technical issues surrounding this matter and also to shed light and raise awareness concerning good practices for implementing a mature and robust policy model throughout the EU.

Next Steps

- Implement a **mapping of the CVD models** currently in use in Europe.
- Given the importance of understanding the current legal constraints in the implementation of a CVD in Europe, the Task Force will undertake an **ad hoc analysis of the legal constraints across member states.**
- **Test the feasibility of extending** the Dutch model of CVD to other European countries. The Dutch National Cyber Security Centre could lead this exercise.
- The importance of developing an **effective communication** on the activity and results of the Task Force (TF) has been emphasised. Therefore, as a first initiative, we will **organise an event at the European Parliament, in which TF participants will showcase their own practices on software vulnerability disclosure** (tentatively to take place in the second half of November).
- Involve other national computer emergency response teams in the work of the Task Force.
- Dates of the next meetings: **November 29th and January 31st.**

Lorenzo Pupillo
Afonso Ferreira
Gianluca Varisco
Romain Bosc
Brussels, 10 October 2017