COMMENTARY

Thinking ahead for Europe

31 July 2017

Software Vulnerabilities Disclosure: The European landscape

Lorenzo Pupillo

Software is nearly everywhere today: in our smartphones, our cars, our offices and our homes. But it has been estimated that the average programme has at least 14 separate points of vulnerability. Each of those weaknesses could permit an attacker to compromise the integrity of the product and potentially make an illicit entry. What can we do to protect ourselves? Who should look for vulnerabilities and should the vendors or the users be informed about them?

The debate on how to handle the disclosure of insecurities pre-dates software security. It can be traced back to the locksmiths and lock-picking in England in the 1850s. In his book *The Rudimentary Treatise on the Construction of Locks*, locksmith Alfred Hobbes argued that "it is to the interest of honest persons to know about [insecurities], because the dishonest are tolerably certain to be the first to apply the knowledge practically". And for decades now, this issue has been the subject of broad debate in the information security arena.

Recent events, however, have created a new sense of urgency on this issue. The ransomware attacks from Wannacry took advantage of a vulnerability in Microsoft software discovered by the National Security Agency (NSA) and leaked by a group of hackers called Shadow Brokers. Such incidents focus critical attention on the widespread activity of stockpiling vulnerabilities by national intelligence agencies around the world. Moreover, with the development of the Internet of Things and billions of devices connected to the internet, the attack surface is becoming broader and the impact of vulnerabilities will be even greater, thereby increasing the risks to critical infrastructure.

'Vulnerability disclosure' is the process by which someone shares information about a security vulnerability so that it can be mitigated or fixed. Particularly critical are the zero-day vulnerabilities, which are undisclosed software *vulnerabilities* that hackers can exploit to adversely affect computer programmes, data, additional computers or a network – and for which patches or mitigation do not yet exist.

Lorenzo Pupillo is Associate Senior Research Fellow and Head of the Cybersecurity@CEPS Initiative. He has more than 30 years of experience in ICT policy in the private sector, international organisations and academia. He is also Affiliated Researcher at the Columbia Institute for Tele-Information at the Columbia Business School.

The way to handle this process has generated four types of vulnerability disclosure: full disclosure, responsible disclosure, coordinated vulnerability disclosure and no disclosure. While full disclosure consists of a public release of all the details of the vulnerabilities, quite often without any mitigation measures to protect users, the no disclosure approach represents a way for governments or vendors to acquire vulnerabilities for exploitation or advantage at a later stage. Both the responsible disclosure and the coordinated vulnerability disclosure aim at sharing vulnerabilities information with vendors, but they differ on the degree of the coordination process to protect users. Discussants at a recent CEPS cyber event[1]in Brussels emphasised the importance of introducing a coordinated vulnerability disclosure (CVD) process in Europe, in which finders– individuals or organisations that identify a potential vulnerability in a product or online service – share vulnerability information with vendors, and stakeholders focus on ways to protect users.

EU member states have only begun the practical implementation of this process. The Dutch government is leading the way with a Coordinated Vulnerability Disclosure Initiative, through the Global Forum on Cyber Expertise. The French agency ASSI is also actively participating. Other countries like Italy are catching up in this process through the initiative of the Digital Transformation Team. There is a real need for better harmonisation of vulnerabilities disclosure and handling the process at the national level, for which the international standards ISO/IEC 30111:2013 on vulnerability handling processes and 29147:2014 on vulnerability disclosure can be useful as a starting point.

The policy framework that is already developed, however, may also need to be updated in view of future technologies such as the Internet of Things. The Joint Research Centre of the European Commission has extensively studied these issues and suggests that research should be the main driver for vulnerabilities discovery, while the creation of an EU pilot vulnerability management centre, serving as a test-bed platform, could act as an independent third party in this process. We suggest that this role could be effectively performed by ENISA, the European Union's Agency for Network and Information Security, which is expected to have a stronger and more focused function in European cybersecurity policy under the new Cybersecurity Strategies to be announced in the autumn.

But there is quite a lot of ground yet to be covered, especially for the role that governments should play in resolving the dilemma between disclosing zero-day vulnerabilities and retaining them for intelligence purposes. Only recently has the US government created a vulnerability equity process (VEP), which focuses on explaining how the government determines whether to release or retain a zero-day vulnerability through a structured policy process. Participants at the CEPS event called upon the EU to outline in its forthcoming revised Cybersecurity Strategy specific principles for member states to follow in developing a European vulnerability equity process with clear priority given to reporting vulnerabilities to vendors. This essential step would take the EU far towards a more future-proofed cybersecurity strategy and a more holistic cybersecurity ecosystem in Europe.

[1] Download the programme and the speakers' presentations here.