Vulnerability disclosure: ENISA's guide and the Dutch approach

Huge numbers of cyber attacks exploit vulnerabilities in computer-based systems and yet vulnerability disclosure is not a straightforward matter, as the discoverer of a vulnerability could face legal risk if they report that vulnerability. Sofie van der Meulen, Attorney at Law at Axon lawyers in Amsterdam, discusses vulnerability disclosure with a particular focus on ENISA's recent Good Practice Guide on Vulnerability Disclosure and the Dutch approach to this issue.

Vulnerabilities

Vulnerabilities are 'flaws' in computer-based systems that may be exploited to compromise the network and information security of affected systems. Vulnerabilities provide a gateway to exploit a system and as such pose potentially severe security risks. Examples of the exploitation of vulnerabilities include: theft of data, unauthorised remote execution of commands, denial of service attacks ('DDoS') and complete shutdown of systems. Identifying and fixing vulnerabilities is therefore crucial to prevent as much exploitation as possible. The process of disclosing vulnerabilities is vital as this is the starting point of fixing the system and keeping data in cyberspace secure.

Vulnerability disclosure

The European Union Agency for Network and Information Security ('ENISA') Good Practice Guide on Vulnerability Disclosure, which was published in November 2015, underpins the importance of vulnerability disclosure. In this guide, ENISA describes many challenges associated with vulnerability disclosure and identifies a number of good practices.

The media has reported some vulnerabilities, such as Heartbleed[1], POODLE[2], and Shellshock[3]. This manner of disclosure comes with the risk of exploitation of the disclosed vulnerability after the media have increased public awareness of it. Therefore, the right time to go public with vulnerabilities is crucial. But who should report vulnerabilities? And how?

According to the ENISA guide, disclosure of vulnerabilities can occur in three different ways: (i) non-disclosure, (ii) responsible/coordinated disclosure or (iii) full disclosure. Discoverers[4] who consider reporting a detected vulnerability face legal threats when they report the vulnerability. These legal issues range from prosecution under criminal law for hacking, civil liability, breach of contract and copyright issues. Overall, stakeholders in the security community agree that the current legal climate does not favour improved security due to the legal uncertainty surrounding the reporting of vulnerabilities.

Responsible disclosure: the Dutch approach

In January 2013 the National Cyber Security Centre ('NCSC') published its guidelines to stimulate coordinated responsible disclosure[5]. The aim of the guidelines is to provide organisations with essential 'building blocks' for a responsible disclosure policy ('RD policy')[6]. Such RD policy describes how an organisation deals with a reported vulnerability, which serves as clarification for the discoverer. A RD policy can provide the discoverer with sufficient reassurance with regards to legal issues, such as protection from legal actions if the reporting by the discoverer is compliant with the RD policy, and an RD policy also underpins the importance of vulnerability reporting for the organisation as a vulnerability reported in a timely fashion can limit damage for the organisation involved prior to publicly disclosing the vulnerability.

In response to the NCSC guidelines on responsible disclosure, the Dutch Public Prosecutor sent a letter on 18 March 2013 to all its departments informing them about the guidelines and how a RD policy plays a role in the decision as to whether or not to proceed with a prosecution of hacking in certain cases.

Ethical hacking?

Currently, the Dutch Penal Code does not recognise the concept of ethical hacking. Hacking can be prosecuted under Article 138ab of the Dutch Penal Code. However, according to the letter, ethical motives can play a role in the determination as to whether an action constitutes a violation that should be prosecuted or not. First of all, ethical hacking implies prior authorisation by the IT system owner for testing the security. Furthermore, the following questions, based on case law in the Netherlands, are considered with regards to whether to proceed with a prosecution or not:

- Were the suspect's actions necessary within a democratic society, i.e. did they concern an important general interest?
- Did the suspect's conduct involve proportional actions? Were the means chosen in proportion to the goal to be achieved? In other words: how did the hacker gain access to the IT system? If any disproportional actions were carried out for this purpose, this will not constitute 'ethical hacking.'
- Could the discloser/suspect

have taken other possible actions? Was the vulnerability immediately reported to the owner of the IT system or not? Were, for example, tracks erased or manipulated? Was data copied or deleted? If tracks were erased, or data manipulated, copied or deleted, this will not constitute responsible disclosure/'ethical hacking.'

In short: if a person detects a vulnerability and immediately reports this vulnerability to the owner of the IT system, this likely qualifies as 'ethical hacking.' However, if the hacker has 'done more' (copy, manipulate or delete data), a criminal investigation will probably take place. Although the NCSC guidelines do not provide ethical hackers or other discoverers with legal certainty as hacking can always be investigated and prosecuted under the Dutch Penal Code, the letter on behalf of the Dutch Public Prosecutor demonstrates that the Public Prosecutor is seriously thinking about the issue.

Vulnerabilities in Cyber Security Assessment 2015

According to the Cyber Security Assessment Netherlands 2015 ('CSAN 2015')[7] vulnerabilities in software are still the Achilles heel of digital security. Software suppliers released thousands of updates in 2014 in order to repair vulnerabilities in their software. With regards to responsible disclosure, CSAN 2015 mentions that even though ethical hackers sometimes have concerns about responsible disclosure and possible prosecution, the Dutch approach has apparently led to a degree of confidence among ethical hackers and other discoverers in determining how their actions fit within the existing legal framework[8]. The increasing number of reports indicates a growing trust between the IT community, the government and the owners of IT systems. Furthermore, the number of organisations in the Netherlands pursuing a RD policy is still growing. In 2014, the Dutch Public Prosecutor did not prosecute reporters who acted in accordance with the RD policy of the relevant organisations[9].

Ethical motives can play a role in the determination as to whether an action constitutes a violation that should be prosecuted or not

Conclusion on the Dutch approach

As far as I am aware the Dutch approach of the NCSC and the additional clarifications provided in the letter of the Dutch Public Prosecutor are rather unique. On a larger scale, the legal framework is fragmented. Varying requirements and sanctions across jurisdictions create legal uncertainty and do not facilitate or stimulate information security. Creating legal certainty in such a varied legal landscape is not an easy task, and perhaps near impossible considering the wide range of (conflicting) interests of stakeholders. However, transparency on how public prosecutors deal with decision-making surrounding vulnerability disclosure is worth pursuing. It allows ethical hackers and other discoverers to understand the process and possible legal implications become more predictable for them, which results in the required trust that is needed to realise a high level of information security.

Copyright

Possible violation of criminal law is only one of the legal concerns related to vulnerability disclosure. Besides liability under civil (contractual) law, infringement of copyright is another concern. The European Court of Justice ('ECJ') shed some light on this issue in 2012. In November 2009 the SAS Institute filed a lawsuit against World Programming Limited for copyright infringement. SAS Institute argued that copyright protects functions of a computer program and accused World Programming Ltd of copyright infringement by developing a system that copied SAS's manuals. The ECJ ruled that copyright protection does not extend to software functionality, the programming language used and the format of the data files used by the program[10]. It stated that there is no copyright infringement when a company that does not have access to the source code of a program studies, observes and tests that program to create another program with the same functionality. Copyright does not protect software firms against 'reverse engineering.'

Sofie van der Meulen Attorney at Law
Axon Lawyers, Amsterdam
sofie.vandermeulen@axonlawyers.com

1. This vulnerability in OpenSSL allowed attackers to read out the internal memory of systems from a distance.
2. This vulnerability allowed attackers to break into secure connections that used SSLv3.
3. Shellshock, a vulnerability in the Bash shell, allowed attackers to execute commands on infected systems from a distance.
4. 'Discoverer': the individual or organisation that reports vulnerabilities.
5. Guideline available through: https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html
6. The ENISA Good Practice Guide on Vulnerability Disclosure provides a 'Vulnerability disclosure policy template' in Annex E.
7. Report available through: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands
8. See also (in Dutch): https://www.ncsc.nl/actueel/nieuwsberichten/responsible-disclosure-steeds-breder-toegepast.html
9. Letter from Minister of Security and Justice, 17 December 2014: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure
10. European Court of Justice, Case C-406/10 (SAS Institute Inc. v. World Programming Ltd).