COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach

Uldis Ķinis *

Faculty of law, Rīga Stradiņš University, Latvia

Keywords:
Latvia
Cybersecurity
Software
Vulnerability responsible disclosure procedure
Algorithm
Waiver
Policy
Regulation

A B S T R A C T

Cybersecurity is an integral part of security. It plays a tremendous role in modern society. It encompasses technical, organizational and legislative measures created for the purpose of protecting and minimizing impacts from cyber incidents. Any software may contain bugs or security holes. Hackers frequently discover such flaws and, without vendor's consent, disclose step-by-step instructions about vulnerability to the public, disregarding the possible IT security risk. Many vendors already have introduced responsible disclosure policies or "bug bounty" programs. In 2013 the Netherlands launched the first state responsible disclosure Guidelines. Guidelines contain principles, definitions and organizational measures, necessary for responsible disclosure policy as a state policy.

Latvia decided to draft Regulation on responsible disclosure procedure. In March 2016, the Ministry of Defence created a working group. The goal of the drafters was: 1) to prepare amendment to Law on the Security of Information Systems to create legislative framework for responsible vulnerability disclosure process; 2) to draft an amendment to Section 241 (3) of Criminal Law to create a guaranty against prosecution (waiver) for persons who act in accordance with responsible disclosure process. The paper provides an insight into this process, difficulties faced by drafters and presents provisional results of the legislative draft and lessons to be learnt.

© 2017 Uldis Ķinis. Published by Elsevier Ltd. All rights reserved.

1. Introduction

[C]ybersecurity is a 'comprehensive multidimensional, interdisciplinary term', which includes technologies, processes and practices designed to 'protect networks, computers, programs and data from attack, damage or unauthorized access'.[1] In other words, it encompasses technical, organizational, and legislative measures that the State should introduce to minimize the impact of cyber incidents. Section 6 of *Law on Information Technology Security of Latvia* defines a cyber incident as a 'harmful event or offence, which may endanger

[1] Cybersecurity. Whatls.com<http://whatis.techtarget.com/definition/cybersecurity> accessed 1 October 2016.

* Faculty of law, Rīga Stradiņš University, Riga Dzirciema str. 16, LV 1007, Latvia.
E-mail address: uldis.kinis@rsu.lv.

https://doi.org/10.1016/j.clsr.2017.11.003
0267-3649/© 2017 Uldis Ķinis. Published by Elsevier Ltd. All rights reserved.

Please cite this article in press as: Uldis Ķinis, From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.003

integrity, confidentiality, and availability of information technologies'.[2] The Vulnerability is 'cybersecurity term that refers to a flaw in a system that can leave it open to attack'.[3] A flaw in IT systems may be caused by software security holes, because it is impossible to create perfect software.

Responsible disclosure policy (hereinafter – RDP) was designed to make vulnerability disclosure process more effective. RDP generally includes four phases[4]: 1) discovery – a hacker discovers system vulnerability; 2) report to the vendor: 3) the vendors' response; 4) the hacker publishes limited information about the vulnerability, not jeopardizing the vendor's system security. The purpose of RDP is to engage into vulnerability disclosure process the so-called "grey hats" – independent IT researchers, who have agreed to cooperate with vendors in vulnerability disclosure process in good faith. Nowadays RDP experts consider this process as being an effective tool for disclosing the so-called "zero-day" exploits. [P]ublic unaddressed zero-day vulnerabilities are infinitely more dangerous than arcane ones'.[5] Mostly RDP has been introduced as a vulnerability disclosure instrument for IT companies, like Google[6], Facebook[7], and Sophos[8]. Recently numerous credit institutions have also introduced policy like this, for example, Swedbank[9], ABN AMRO Bank,[10] etc.

The first legal research concerning RDP can be found in literature[11] in 2005. The legal debate started, when ISS employee Michael Lynn found vulnerabilities in Cisco's Internet routers, which could seriously affect the infrastructure of the Internet, and was scheduled to speak about the discovered vulnerabilities at Nevada Black Hat Conference. However, due to pressure exerted by Cisco, organizers cancelled Lynn's talk. Moreover, Cisco filed a lawsuit against Lynn. Cisco claimed that Lynn had violated several laws, including, infringement of copyright and disclosure of trade secrets. Professor J.S. Granick[12], who was the defence attorney in this case, from the author's point of view, provided the most comprehensive legal analysis related to legal implications of the disclosure process.

In later years researchers paid more attention to the term and content of responsible disclosure and its compliance with human rights. For example, whether full public disclosure of vulnerability, which may include instructions, on how to fix vulnerability, should be protected under the freedom of expression.[13] Some authors assessed information, which an independent researcher gained during the discovery of the vulnerability, as copyright value.[14] In majority situations, the research included in the papers referred to above was based on analysis of case law, which will be described in the first part of this paper. This research helped companies to launch their bug bounty policies or to create their own RD policies.

However, none of the authors referred to above examined RDP as a four-stage legal process. Moreover, none of them even discussed the idea of necessity to create a legal framework for responsible vulnerability disclosure, which is the main novelty and contribution to the research of this paper. Until now, at least according to the author's knowledge, no scholar has provided research concerning the creation of a legal algorithm of responsible vulnerability disclosure process, because no country has had such a law elaborated yet.

The third chapter of this article describes the genesis of countries' attempts to create national responsible disclosure policies. The Netherlands has been the pioneer in Europe in the field of developing Responsible 'Disclosure Policy as an instrument for state the cybersecurity policy'.[15] However, the policy is only guidelines, not a law.

---

[2] Likumi.LV <https://likumi.lv/doc.php?id=220962> accessed 20 March 2016.

[3] Technopedia. Vulnerability <https://www.techopedia.com/definition/13484/vulnerability> accessed 1 October 2016.

[4] IETF Guidelines 2002 Responsible Vulnerability Disclosure listed 7 phases of this process<https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00> accessed 1 October 2016.

[5] Taiwo A. Oriola, 'Bugs for sale: Legal and ethical proprietaries of the market in software vulnerabilities.' John Marshall Journal of computer & information Law, Summer 2011, 1–3. Westlaw. (Thomson Reuters).

[6] Google Application Security <https://google.com/about/appsecurity/reward-program> accessed 18 March 2016.

[7] Facebook bug bounty <www.facebook.com/whitehat> accessed 20 March 2017.

[8] Sophos Responsible disclosure policy <www.sophos.com/legal/sophos-responsible-disclosure-policy.aspx> accessed 21 March 2017.

[9] Swedbank security policy <https://www.swedbank.se/om-swedbank/sakerhet/?contentid=cid_1605327> accessed 23 March 2017.

[10] ABN AMRO Bank 'Reporting weaknesses in our IT system' <https://www.abnamro.com/en/footer/responsible-disclosure.html> accessed 23 March 2017.

[11] To prepare this article, the author examined library resources and online databases, e.g., Westlaw, SSRN, HeinOnline, ProQuest, Science Direct, Scopus and Google Scholar.

[12] See Jennifer Stisa Granick 'The price of restricting vulnerability publications'. International Journal of Communication Law & Policy Vol. 9 Spring, 2005 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=874846> accessed 15.08.2017; Jenniffer Stisa Granick 'Legal and ethics' in Mike Loukides and Collen Gorman (eds) Security Power Tools, O'Reilly, 2007 p 3.

[13] See. Casandra Kirsh 'The grey hat hacker: reconciling cyberspace reality and the law' North Kentucky Law Review, 383, 2014 Westlaw (Thomson Reuters); Andrea M. Matwyshyn 'Hacking Speech: Informational Speech and the First Amendment' Northwest University law review, Winter 2013, Westlaw (Thomson Reuters); Kristin M. Bergman 'A target to the heart of the first amendment: Government endorsement of responsible disclosure as unconstitutional' Northwestern Journal of Technology & Intellectual Property, May 2015, Westlaw (Thompson Reuters); Loren F. Seznick and Carolyn LaMacchiat ' Cybersecurity: should the sec be sticking its nose under this tent?' Journal of Law, Technology & Policy, Vol 2016 pp 35- 70, HeinOnline; Jenniffer M Pacella 'The cybersecurity threat: compliance and role of whistle-blowers' Brooklyn Journal of Corporate, Financial & Commercial Law, Vol. 11, 2006, p. 39, HeinOnline; Dereck E. Bambauer and Oliver Day 'The hacker's aegis'. Emory Law Journal, Vol. 60.p. 1051, 2011 https://ssrn.com/abstract=1561845> accessed 25 April 2017.

[14] See Maylyn Fidler 'Regulating the zero-day Vulnerability trade; a preliminary analysis, I/S: A Journal of Law and Policy for the Information Society, 2015, p 405, HeinOnline; Abdullah M. Algarni, Yashwant K. Malaiya 'Software vulnerability markets: discoverers and byers' World Academy of Science, Engineering and Technology, International Journal of Computers, Electrical, Automation, Control and Information Engineering Vol: 8, No 3, 2014, HeinOnline.

[15] Policy for arriving at a practice for Responsible Disclosure. National Cyber Security Centre. Ministry of Security and Justice, pdf.<https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html> accessed 19 July 2016.

Please cite this article in press as: Uldis Ķinis, From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.003

Download English Version:

https://daneshyari.com/en/article/6890471

Download Persian Version:

https://daneshyari.com/article/6890471

Daneshyari.com