MINISTRY OF FOREIGN AFFAIRS AND TRADE OF HUNGARY

MINISTRY OF FOREIGN AFFAIRS

Ministry of Foreign Affairs of the Netherlands

GFCE
Global Forum on Cyber Expertise

Report Expert Meeting on Responsible Disclosure

23 March 2016, Budapest Hungary

Summary of the GFCE expert meeting on responsible disclosure that took place March 23rd 2016 in Budapest, Hungary. The initiative for the expert meeting was taken by Hungary, Romania, the Netherlands, and Hewlett Packard Enterprise (the Netherlands). A broad range of about 50 participants represented governments, business, academia, and the technical community.

Participants were welcomed by Mr. István Íjgyártó (Minister of State at the Ministry of Foreign Affairs and Trade of Hungary) and Mr. Hans de Vries (Deputy Director of the Cyber Security Department at the Dutch Ministry of Security and Justice and initiator of the GFCE), who emphasized the urgency of this topic in the broader cybersecurity agenda.
The key note speech was delivered by Mr. Chris van 't Hof (an independent researcher of technology and society), drawing from his experience with security researchers and their distinct incentives for disclosing vulnerabilities. His book *"Helpful hackers, how the Dutch do responsible disclosure*" details these stories and was distributed amongst the participants.
Mr. van 't Hof suggested that proper attribution of disclosers in an online "wall of fame" should be considered in concert with other instruments such as bounty programs to account for these varying incentives.

1. Policy approaches for responsible disclosure

Government representatives offered achievements and challenges in the practice of responsible disclosure.

Competency issues amongst national institutions were highlighted by Mr. Illés Solt (Technical leader of the Hungarian National Cyber Security Center). He asserted that CERT's without task timeline or specific budget allocation may gain legitimacy by showing commitment to their goal of improving cybersecurity.

Ms. Baiba Kaškina (Head of the Latvian Computer Emergency Response Team) addressed the complexity different legal systems for the work of white hat hackers. She summarized how Latvia is currently in the process of amending criminal law and IT security laws in order to create an exemption for professional risk for security researchers, and to establish a national CERT and its responsibilities, respectively.

Mr. Hans de Vries (Deputy Director of the Cybersecurity Department at the Dutch Ministry of Security and Justice) presented guidelines for arriving at a responsible disclosure policy that may be used by organizations and governments alike. Mr. de Vries considered it an urgent responsibility of national CERT's to promote the win-win effects of entering into a dialogue about vulnerable systems.
Dr. Allan Friedman (U.S. National Telecommunications and Information Administration) proposed the point that nearly every organization is now in the business of developing software, indicating that existing best practices such as the FTC's *fair information practices* must now be built into law.

The Indian Ministry of Home Affairs reported on good progress in implementing national responsible disclosure policies during the discussion that followed and Japanese members of government expressed interest.

In response to a question by the Spanish Ministry of Foreign Affairs, participants supported Latvia's view that improving cybersecurity is a global issue and concluded that cooperation is crucial. Overall, the importance of responsible disclosure policy for a free, open and secure internet was widely acknowledged.

2. Understanding the researcher's mindset

The security researchers of GDI Foundation balanced the attempts at governance, risk analysis, and control of technology against their daily experiences with careless systems administration, providing numerous examples of potential data-leaks and abuse of critical systems.
In GDI's 'project 366' vulnerabilities have been disclosed for every day of 2016 thus far.
On the topic of policy development by organizations, Mr. Victor Gevers of GDI stated: 'If you have a responsible disclosure policy, you are in control of the process'. 'A clear guideline really helps us to understand what is legally acceptable and where to stop our investigations', Mr. Vincent Toms added.
In a later discussion, a representative of Cisco Systems shared his belief that organizations like GDI have an important control function in the rapidly growing market for vulnerabilities, stating that GDI's idealistic motivations prevent companies from being held at ransom by keeping the price of vulnerabilities in check.

3. Real-world experiences with responsible disclosure

Mr. Paul Samwel (Lead Security Architect, Rabobank) introduced a Coordinated Vulnerability Disclosure Manifesto and called for support from organizations that are willing to raise awareness for the important role of security researchers. He was joined by Mr. Jan van der Sluis (Security Principal, Hewlett Packard Enterprise), who stated: 'There is always a business case for responsible disclosure'.

Mr. Jan van der Sluis articulated the benefits of having a "Responsible Disclosure Life Cycle" approach being part of an organization's Security Policy.

The ability of organizations to implement guidelines as a useful and necessary first step on the way to formal legal measures was examined by the next panel, consisting of Mr. Samwel, Mr. van der Sluis, Ms. Amanda Craig (Senior Cybersecurity Strategist, Microsoft), Mr. Ferenc Biró (Partner, Fraud Investigations and Dispute Services, Ernst & Young Hungary), Mr. Bence D. Horváth (BAE Systems Applied Intelligence), and Mr. Ferenc Frész, (CEO and founder of Cyber Services Plc).

However, it is imperative to build trust by staying true to promises made. As Mr. de Vries (Deputy Director of the Cybersecurity Department at the Dutch Ministry of Security and Justice) noted: 'Trust comes by foot and leaves by horse'.

In response to a question about dilemma's relating to the interest of states in unreleased vulnerabilities, Ms. Craig noted that anytime Microsoft witnesses a vulnerability being exploited in the wild they would disclose this, whether publicly or to a targeted group of researchers.

Ms. Craig observed that the term 'coordinated vulnerability disclosure' is preferable to 'ethical hackers' or 'responsible disclosure' in an international context, as it makes clear what the ethical and responsible behavior consists of. This rings true and will be taken on board by the GFCE in the development of this initiative.

4. Cybersecurity research in a broader perspective

Dr. Boldizsár Bencsáth (Assistant Professor, CrySys Lab) shared the perspective of research labs in researching and disclosing vulnerabilities, revealing to the participants several examples of what uncoordinated disclosures may lead to.

Amongst other questions, Dr. Allan Friedman raised the issue of what would happen to the quality of vulnerability reports when responsible disclosure would become the norm.

5. Conclusions and next steps

After taking stock of current developments and challenges, the participants and members of the GFCE agreed that responsible disclosure can fulfill an important role in improving cybersecurity.

The urgency of improving opportunities for responsible disclosure was acknowledged. Opportunities to achieve this were examined, including creating policy at both the organizational and government level. The process of creating policy may be aided by the guidelines such as those presented in session 1 and the manifesto for organizations that was introduced in session 3. Both documents are enclosed. Participants agreed that some legal systems currently form barriers for security researchers to conduct responsible disclosure.

Hungary, Romania, the Netherlands, and Hewlett Packard Enterprise (the Netherlands) have committed to further partnership in the field of responsible disclosure. A set of good practices based on the first expert meeting will be released for comment to the participants of the meeting.

Romania announced that the next expert meeting will take place in Bucharest in the fall of 2016. It will build on the work already done and establish the set of good practices. New efforts will focus on removing legal obstacles for responsible disclosure.