PROGRAM

Responsible Disclosure Expert Meeting
22 - 23 March 2016 in Budapest, Hungary

22 March:

19.30 – 22:00   Participants arriving the day before the Expert Meeting will have the opportunity to meet and network at an informal get-together at the **Novotel Budapest Danube**. This event is offered to you by the Dutch Ministry of Foreign Affairs.

23 March:

08.15 – 09.00   <u>Registration</u>
Please arrive in a timely fashion due to security measures.

09.00 – 09.15   <u>Official welcome and opening</u>
Dr. István Mikola, Minister of State for Security Policy and International Cooperation of Hungary, will open the expert meeting followed by an introduction by **Mr. Hans de Vries**, Deputy Director of the Cyber Security Department at the Dutch Ministry of Security and Justice and initiator of the GFCE.

09.15 – 09.30   <u>Key note speech</u>
Introduction to the GFCE Responsible Disclosure initiative by Mr. Chris van 't Hof, an independent researcher of technology and society. In 2016 he published 'Helpful *Hackers. How the Dutch do Responsible Dislcosure'*, describing 24 case studies of security researchers disclosing vulnerabilities, from the perspective of the media, court, government and the owners and users of the systems involved.

09.30 – 11.00   <u>Policy approaches for responsible disclosure</u>
Exploration of government strategies for promoting cooperation with the research community in the collective pursuit of cybersecurity.

At present multiple governments have a responsible disclosure policy already. During this panel discussion experts will exchange best practices and issues in the field of responsible disclosure policy.

– **Dr. Balázs Bencsik**, Head of the Hungarian National Cyber Security Center
– **Ms. Baiba Kaškina**, Head of the Latvian Computer Emergency Response Team
– **Mr. Hans de Vries**, Deputy Director of the Cybersecurity Department at the Dutch Ministry of Security and Justice

11.00 – 11.30   <u>Networking Break</u>

11.30 – 12.30   <u>Understanding the researcher's mindset</u>
Explanation of the challenges and responsibilities that come with finding a software vulnerability. The independent researchers of **GDI Foundation** have taken time off work for their idealistic project '*366 days of disclosing vulnerabilities*', in which they document their efforts to make networks safer one day at the time.

12.30 – 13.30   <u>Lunch</u>

13.30 – 15.00   <u>Real-world experiences with responsible disclosure</u>
Being informed of a security vulnerability can put your organization on high alert. How to integrate your lessons learned and develop responsible disclosure guidelines?

The development of a responsible disclosure policy helps to mitigate many threats before they become public. Business leaders exchange the real-world best practices that they have developed from their cooperation with the research community with special emphasis of

upcoming threats and the workflow of security operation centers.

- **Ms. Amanda Craig**, Senior Cybersecurity Strategist, Microsoft
- **Mr. Jan van der Sluis**, Security Principal, Hewlett Packard
- **Mr. Ferenc Bíró**, Partner, Fraud Investigations and Dispute Services, Ernst & Young Hungary
- **Mr. Bence D. Horváth**, BAE Systems Applied Intelligence
- **Mr. Paul Samwel**, Lead Security Architect, Rabobank
- **Mr. Ferenc Frész**, CEO and founder of Cyber Services Plc

15.00 – 15.30   <u>Networking Break</u>

15.30 – 17.00   <u>Cybersecurity research in a broader perspective</u>
Analysis of the information security environment. Experts go into the long-term developments in the field of information security. What paths to expect beyond the current policy prospects?

- **Mr. Allan Friedman**, author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*
- **Dr. Levente Buttyán**, Head of CrySys Lab
- **Mr. Ilias Chantzos**, Global CIP and Privacy Advisor at Symantec
- **Prof. Dr. Ferenc Gazdag**, National University of Public Service (TBC)

17.00 – 17.30   <u>Next steps and closing</u>

18.00 – 20:00   <u>Informal dinner</u>