National Cyber Security Centre
Ministry of Security and Justice

Coordinated Vulnerability Disclosure

Jeroen van der Ham

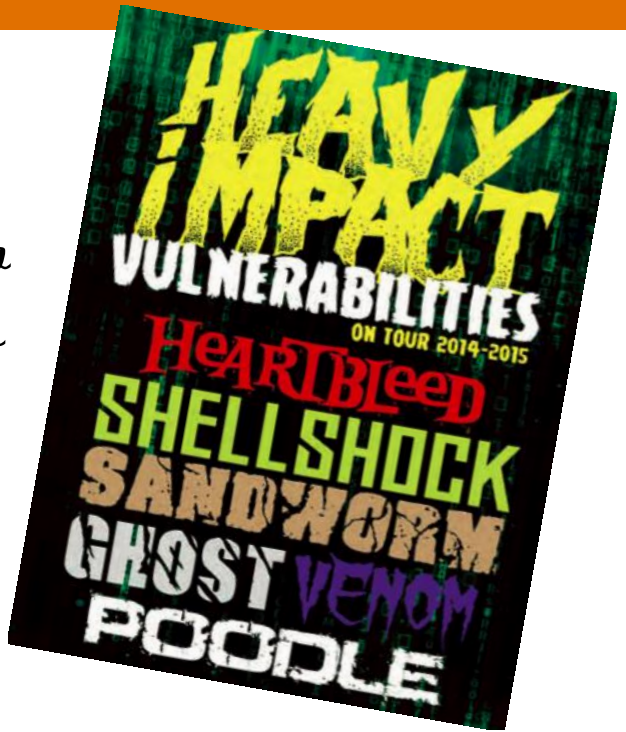
NCSC

Some facts

By Source (WP:NFCC#4), Fair use, Wikipedia.org

Drown

"Everybody has vulnerabilities, being able to receive them and respond to them is what matters"



Source: Cyber Security Assessment Netherlands 2015, image creator Ken Westin

Undesirable situations

159.46.193.36
is vulnerable!

Afraid to report vulnerabilities

Panic
!

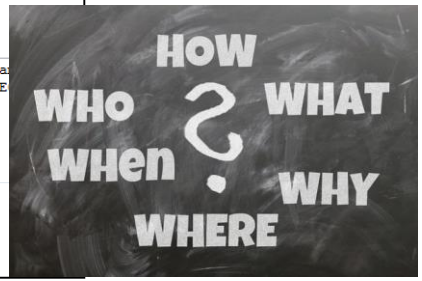
User Name:

E-mail address:

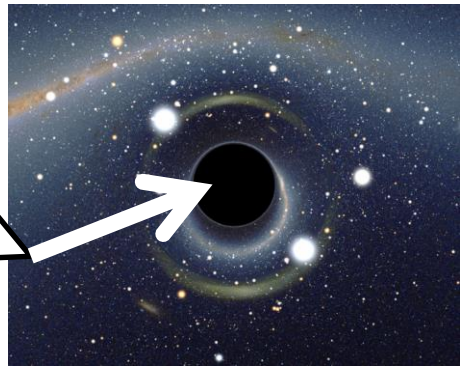
SELECT * FROM users WHERE na
= 'a';DROP TABLE users; SELE
* FROM userinfo WHERE 't' =

Comments:

Submit



I found a vulnerability in your system! Gimme money! Grz H4x0r!



Many international CVD initiatives & guidelines

Initiatives

- Global Forum on Cyber Expertise (GFCE) Cyber Security Coordinated Vulnerability Disclosure Initiative
- USA National Telecommunications & Information Administration (NTIA) Cybersecurity Vulnerabilities Multistakeholder Process

Guidelines

- ENISA Good Practice Guide on Vulnerability Disclosure
- GCCS Best practice guide Responsible Disclosure
- ISO/IEC 29147:2014 and ISO/IEC 30111:2013
- Responsible Disclosure policy guide (NL)

Many parties have implemented the guideline

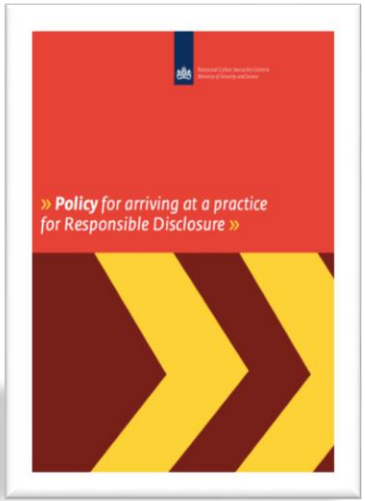
Coordinated Vulnerability Disclosure Manifesto

Palo Alto Networks, Vodafone, Phillips, Honeywell, Rabobank, CIO Platform Nederland, ABN AMRO, CIOforum Belgian Business, Corbion Group Netherlands, Eneco, European Network for Cyber Security, IHC Merwede, ING, KPN, LUMC, NS, NUON, NXP, PostNL, SAAB, Schuberg Phillis, SNS Bank, Stedin, Surfnet, Tennet, TNO and VOICE.

Download the manifesto at www.thegfce.com

Coordinated Vulnerability Disclosure building blocks

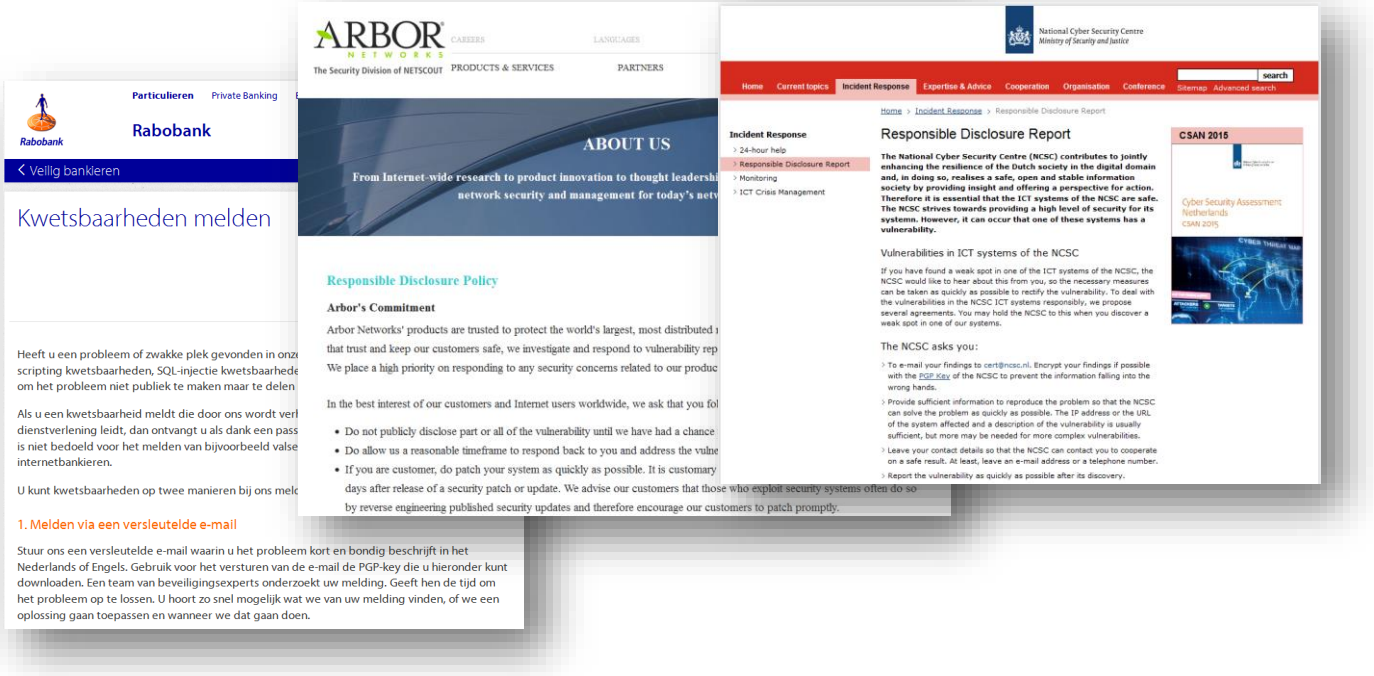
Promises of the organization (CVD policy)



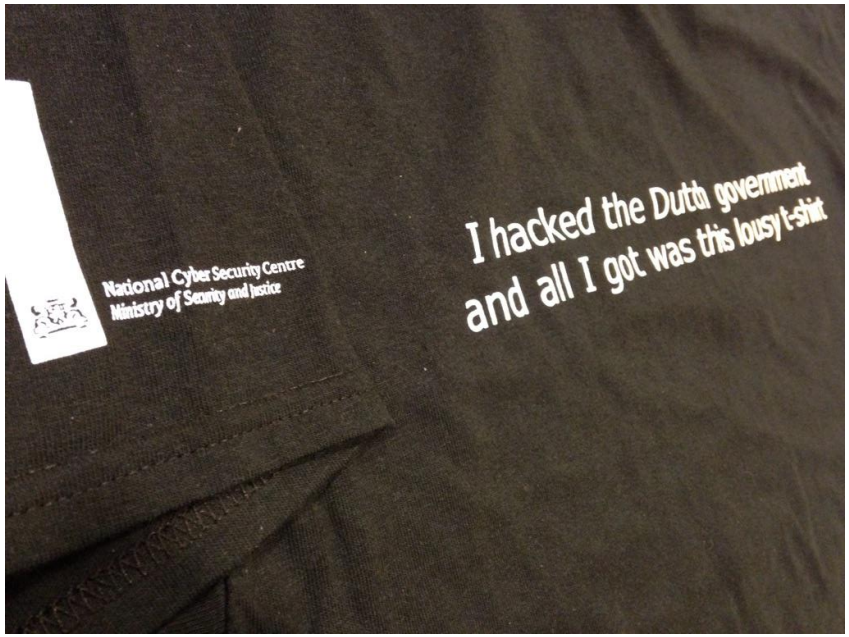
Responsibilities of the researcher or ethical hacker

www.ncsc.nl

Example pages



Example rewards



Or: bug bounties (€)

CVD building blocks (responsibilities of researcher / ethical hacker)

Timely disclosure

Confidentiality

Proportionate

Least invasive method

No brute forcing

No backdoors

No malware

No alteration of data

No social engineering

Case: Groene Hart Hospital

Source: www.ghz.nl

Groene Hart (ECLI:NL:RBDHA:2014:15611)

Case details

- Dutch public hospital with vulnerable FTP server with easily brute forceable administrator credentials (password: groen2000)
- Hacker finds the vulnerability and informs a journalist
- Journalist informs the hospital at 10:00 and publishes the story at 15:00
- The hospital reports the case to the police
- The hacker used a port scan tool (Nessus) for two weeks (using VPN)
- The hacker probably retrieved the password hashes used by the FTP-server and bruteforced them
- The hacker shares the credentials with other persons
- The hacker installed malware on the server, using his own IP
- The hacker downloaded multiple medical files, including those of famous people
- The hacker sent screenshots of those files to a journalist
- The hacker states that its actions were in the public interest

Groene Hart Hospital

Outcomes:

- Public Prosecutor Service has discretion to prosecute. Judge will have to judge whether the actions of the ethical hacker were proportionate and subsidiary.
- Judge emphasizes that revealing security vulnerabilities can be in the public interest, especially when sensitive (medical) files are at stake.
- The judge finds that there were no other ways for the hacker to discover the vulnerability (least invasive)
- The judge finds that installing the malware was necessary to show that the network of the hospital had weak security.
- However, the hacker accessed the server and downloaded data multiple times, including data about famous people. This was not necessary to proof the vulnerability.
- **Sentence: 120 hours of community service**

Case: KPN

KPN

Case details:

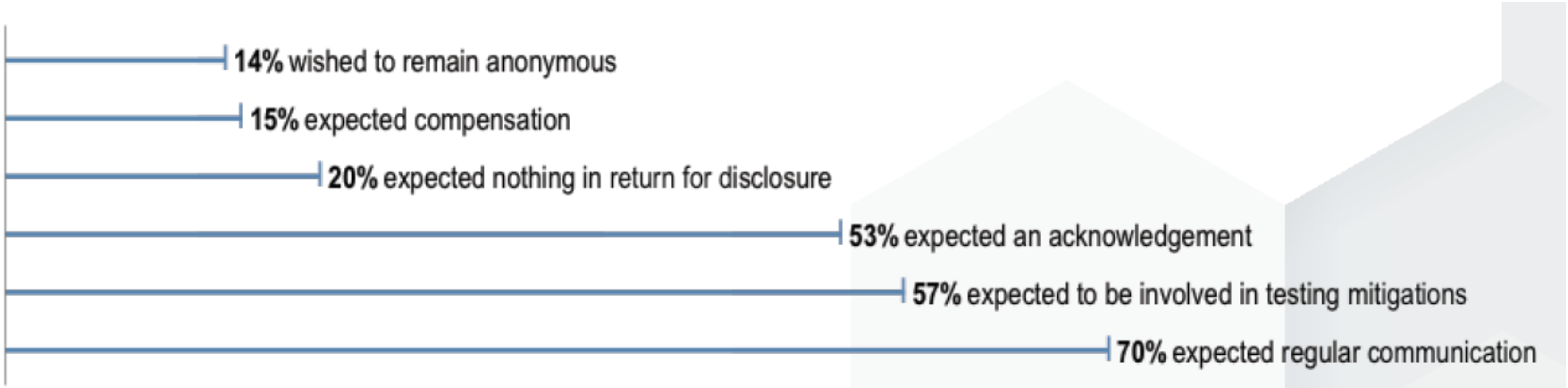
- Two ethical hackers find vulnerabilities in modems
- The modems are widely used by KPN and its customers
- The vulnerabilities give complete remote access to modems
- The vulnerability can be misused for DDoS attacks and to intercept data
- Hackers tested the vulnerabilities against their own modems
- The ethical hackers reported the vulnerabilities to KPN

KPN

Case outcome:

- CERT of KPN takes up the report
- KPN invites the ethical hackers to its office to show and explain their findings
- The vulnerabilities get fixed within a short amount of time
- The ethical hackers are rewarded with KPN ‘goodies’ and are allowed to present their findings at a congress
- KPN uses the case to show that it takes the security of its customers and network very seriously
- KPN releases a press statement on its website and creates an informative video to promote its CVD policy and cooperation with ethical hackers

Researcher motivation



Source: NTIA report: Vulnerability Disclosure Attitudes and Actions
https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

Key takeaways

- Secure software does not exist, receiving and responding to vulnerabilities is what matters
- Coordinated Vulnerability Disclosure policy does not give hackers a carte blanche
- Appreciate and cherish involvement of the ethical hackers and security research community