National Cyber Security Centre
Ministry of Security and Justice

The Dutch experience
Implementing a RD policy

2nd National Cyber Security Strategies Workshop

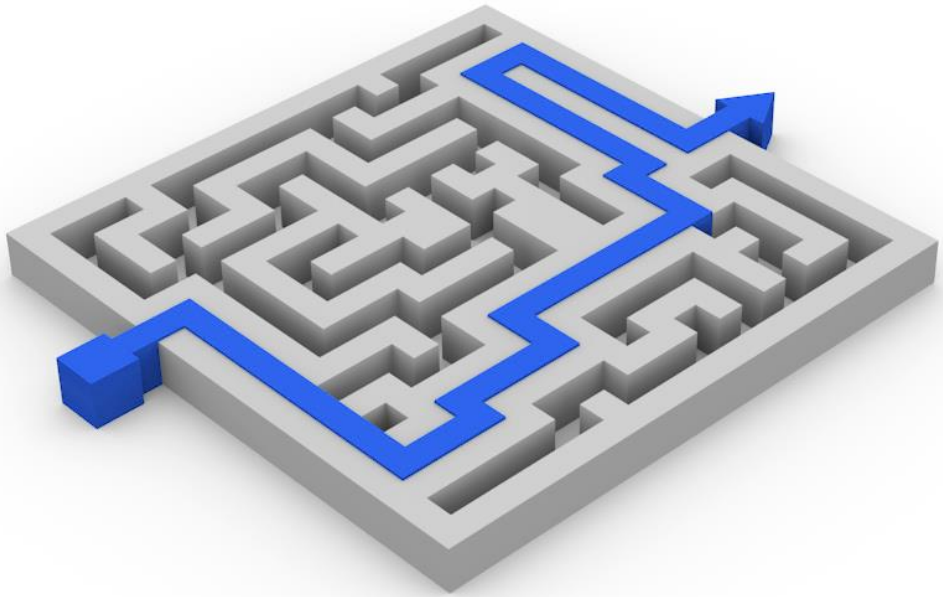
Riga, May 13th 2015

David Willems
Deputy Manager Monitoring and response

Fix a problem

The perspective of a hacker

The perspective of a company/ the government



Published beginning of 2013

What is in the policy? (examples)

Organizations' promises

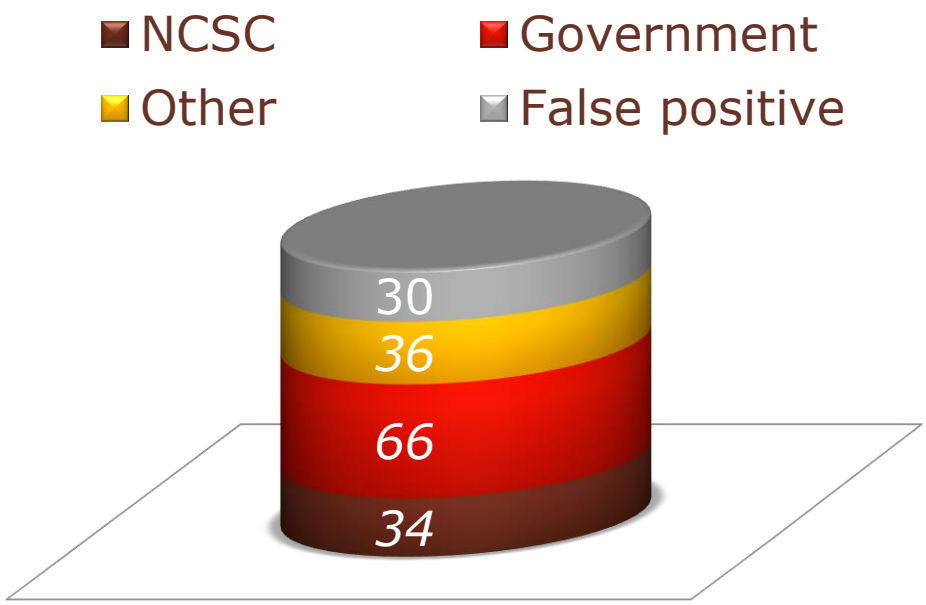
- Take report seriously
- No legal proceedings
- Response time
- How to report
- Disclosure
- Rewards
- …

Reporters’ responsibilities

- Report timely and securely
- Don’t do more than necessary
- Don’t disclose until fixed
- No social engineering
- No DDoS
- Provide detailed report
- …

What is the role of the NCSC?

- Deal with our own Responsible Disclosure reports (of course)
- Intermediary between reporter and organization (when necessary)
- Promote and further develop Responsible Disclosure



** Reports where we have had an active role from start to November 30, 2014*

Public prosecutor guidelines

"Whenever a hacker gets in touch directly and safely with the owner of the IT-system regarding a discovered vulnerability and no data is manipulated or removed then there may be a case of RD. This means there is no reason for a criminal investigation and for a criminal prosecution"

Our experience so far

- Many organizations have published a policy
- Generally good comments from both reporters and organizations
- Many good quality reports
- Mostly website vulnerabilities, but also 0-days
- Reporters getting hired instead of arrested

- Some recurring and bad reports
- False positive reports from scanning tools
- Hard to find responsible department
- Focus on fixing a specific vulnerability, not on the big picture

RESPONSIBLE DISCLOSURE HALL OF FAME

This page contains the 'Hall of Fame, with a (mostly up-to-date) list of all those people that have highlighted security issues to us. It is a direct result of our **responsible disclosure policy**, which we implemented in December 2012, modeled after the work of Floor Terra.

This has directed a lot of eyes towards our infrastructures, which spotted a lot of tiny details we would have otherwise missed. While we regularly scan our own infrastructure using automated tools, there are

The Bug Bounty List

Welcome to Bugcrowd's community powered list of bug bounty programs

Bugcrowd also manages private Bug Bounties for companies who aren't on this list. The details of these bounties are only available to Bugcrowd Ninja's via our Tester portal. Join the Ninjas or find out more information about private bounties.

Products and Services

If you notice something missing, or spot a bounty program which has ceased please tweet to us or email us. We'll update ASAP and credit you for your help!

Bugcrowd - https://portal.bugcrowd.com/user/sign_up

National Cyber Security Center (Netherlands)

Schuberg Philis

LIST FILTER

- Reward Offered
- Swag
- Hall of Fame

Some tips

- Find a boardroom sponsor
- Discuss responsibilities
- Think about credits and rewards
- Develop a process to deal with reports
- Be able to fix things
- Assign a coordinator
- Learn from fixed vulnerabilities
- Be clear about time to fix and your priorities

National Cyber Security Centre
Ministry of Security and Justice

Thank you for your attention

David Willems

Email: david.willems@ncsc.nl