The Dutch Responsible Disclosure Policy

Tarik El Yassem
Agenda

- Introduction
- Responsible disclosure: what and why
- The Dutch RD guideline
- Intermediary results
- Lessons learned
- The road ahead
- Questions
Introduction

- Tarik El Yassem
- 8 years at GOVCERT.NL/ NCSC.NL
- Msc from University of Amsterdam
- Incident response
- Co-author of Responsible Disclosure guideline
- Implemented it at NCSC, helped others
- Senior security intel analyst at Rabobank Global SOC
Does this look familiar?

- Incidents due to “leaks” in the media
- Inconvenient timing
- Researchers frustrated
- Organization panics
- Business as usual after damage control
  - Org still not listening to security people
  - Not learning
  - No transparency

- Ignore, be vulnerable, fix, repeat
Can't we all just get along?

- Be reachable
- Get time to fix
- Track and follow up
- Appreciate white-hat community
- Don't arrest clumsy teenagers
- Learn from vulnerabilities
RD: what and why
The Dutch RD guideline

- Looked at others (Microsoft, Facebook, Google)
- Looked at standards ISO
- Mostly focused on products
- Needed broader approach
- Had talks with:
  - Hackers, researchers, journalists
  - Banks, telco's, vital infrastructure
  - Law enforcement, lawyers, policy makers
  - Political pressure
Reporter experience

Reporter = researcher, hacker, you, your mom
Reporters: we bring gifts!
Reporters: helpdesk
Reporters: security department?
Reporters: police
Reporters: credits

Information for Security Researchers

If you’re a security researcher, please review our responsible disclosure policy before reporting any vulnerabilities. If you’re not a security researcher, visit the Facebook Security Page for assistance.

If you believe you have found a security vulnerability on Facebook, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to quickly fix the problem.

Responsible Disclosure Policy

If you give us a reasonable time to respond to your report before making any information public and make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our service during your research, we will not bring any lawsuit against you or ask law enforcement to investigate you.

Thanks!

On behalf of our millions of users, we would like to thank the following people for making a responsible disclosure to us:

- Emmanuel Bronshstein (8he3mm2j)
- Matt Evans
- Rohit Mui (Brothtmual)
- Krishna Chatterya Venkatesw
- Armin Razdjo
- Usha Gobejishvili (@khudafagom)
- Luis Delgado (@lidelgado)
- Yue Zhou
- Emilie Balic (@CaminAnem)
- Kelvin Zhang (@x00rS School) (@vertex53.com)
- Abhishek Gut @ (Advisory)
- ChrisY Deven
- Yoji Kogusa
- João Lucas Melo Brasso (whitehat hackers.com.br)
- Steffen Taimoski
- Ben Sheppard (benheppard.net)
- Rakan Alatibbi (@rthelawm)
- Nadia Copperstein
- Oussama Nesara
- James Covernale
- Neelak Sandrewang
- Norio Norura (@horio norura)
- Loget X
- Pratap Gaichate
- Vibhas Chauhan
- Harri Simila
- Andre Nathello
- Joakim Franson
- Sandeep Ramkale (@drSandeepL337)
- Aswin Bahar (@cyber4.com)
- Warren Ho
- Andreas Boll Sauerwein
- Robert Jurgenske
- Brendan Scarvell
- Andrey Lobanets (@Iolcrus)
- Tom Mckay
Reporters: want small reward
Reporters: protect customers
Reporters: they don't give feedback
Reporters: no transparency
Organizations' experience

Banks, telco's, governments, small businesses, vital infrastructure
Organizations: NoOooOOoOo!!!!
Organizations: all criminals!
Organizations: blackmail!
Organizations: cost effective
Organizations: limited sight
Organizations: no budget
Organizations: no policy
Organizations: vague reports

62.100.52.106
Result: policy guidelines

Result: guidelines; not law

- But Ministry of Security and Justice and Public Prosecution Service support and advocate guidelines

  *Public Prosecution Service ultimately still has the discretion to prosecute, for instance when a reporter goes ‘too far’ despite of agreed terms, of course this also holds true for organisations*

- **Policy is an agreement between organisation and reporter**

  *Reporter and organisation agree to adhere to published policy, organisation promises not to file a complaint with the Police*

- **More detailed terms on disclosure, proposed fix and credits are made upon further contact**
Intermediate results
Intermediate results

- Almost zero incidents due to media
- Working with media to disclose
- Better relations with hacker community
- People getting jobs instead of arrests
- Organizations waking up
- More mature, aware and secure society
Reports to the NCSC

- NCSC: 38
- Government: 47
- Other: 28

* From start till June 2014
Intermediate results

T-shirts, tropys, halls of fame, money, diners, tickets to or presenting at conferences, site visits, etc
Lessons learned

- Responsible Disclosure policy since January 2013
- Lots of quality disclosures
- Website vulnerabilities
- Internet Explorer zero day
- Also false-positives from scanning tools
- Fixed quickly but organizations not looking beyond

Worth while and useful
Lessons learned

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
Lessons learned

Creating policies

- Involve hackers & researchers
- Get backup from politicians
- Get backup from public prosecutors
- Develop your own policy
Lessons learned

Implementing policies

- Find a boardroom sponsor
- Discuss responsibilities
- Think about credits and rewards
- Develop a process
- Assign a coordinator
- Learn from disclosures and share
The road ahead

- Evaluation in early 2015 by NCSC
- Revised edition
- International organizations
- We hope others will follow
Conclusion

- Responsible disclosure works!
- Very useful for organizations
- The Netherlands is, who's with us?
More questions?

Questions for me: tarik.el.yassem@rabobank.com
Questions for ncsc.nl: info@ncsc.nl

More information:
http://responsibledisclosure.nl/en/
http://www.ncsc.nl/
Thanks Rabobank, NCSC.NL and you!