Bug Bounty programs in Switzerland?

Florian Badertscher, 04.10.2016
C1 - public
About me

• Security Analyst at Swisscom CSIRT, since 2015
  – Incident handling
  – Develop monitoring infrastructure
  – Security initiatives and projects

• Background as pen tester and IT security consultant / teacher
Agenda

- Part 1: Bug Bounty @ Swisscom
- Part 2: Situation in Switzerland
Bug Bounty @ Swisscom

Part 1
Why do we have a Bug Bounty program?

• There was an incident...
• 2 options:
  – Going public with a press release
  – De-escalate the situation using a Bug Bounty program
The basic idea behind our program

**Goals**
- Central point of contact
- Streamlined process to handle vulnerability notifications
- Set the rules
- Create incentives
- Create transparency about security issues

**Scope**
- All our services and products
- We expect from the researcher to identify the system properly

**Bounties**
- Risk based approach
- CHF 150 – CHF 10’000
Legal questions

Current situation
• Enable the payout of bounties
• All test-activities have to be within the bounds of the law
  – No permit to perform all kind of tests on our systems

• And in reality..?

Payout
• Comply with sanctions / embargos
  – Identify the researcher and check all the lists
• Our approach: leave it to the bank
  – No PayPal
How do you start it?

- You probably won’t announce it with a big bang
- Simple page on the website
- Page on HackerOne
Results

Facts
• 200 submissions per year
• 75% web-related
• 50kCHF bounties per year

What works well?
• Quality of the reports
• Some high-risk findings

Where are our difficulties?
• Find the owner of the system X with IP Y out of 3.4 Mio.
• Convince the (external) dev/ops team to address the issue fast
More results

- Clear guidelines about publishing advisories
- Measure the effectiveness of the education
  - Internal developed code has much less vulnerabilities
- Spot your weak points
  - It shows you very clearly, where you’re good and where not
Return on investment

- Learn about vulnerabilities
- Gain insights into the situation at the frontlines
  - All the low-impact submissions are useful as well
- Clean-up old stuff
- Create awareness for security
- Secure software development and Bug Bounty programs complement each other perfectly
- Push agile approaches
What we are working on

• Include the program in our contracts
• Create awareness in the important departments
• Improve the handling / tracking
• Assign some more manpower
Example: CPE

- **Affected devices:**
  - Centro Grande / Centro Business

- **Vulnerability:**
  - Chain of vulnerabilities
  - Remote root access
  - Precondition: remote administration enabled / CSRF
Example: CPE

Swisscom devices are managed

- HDM (Home Device Manager) / ACS (Auto Configuration Server)
- TR-069 or CPE WAN Management Protocol (CWMP)
- It is the responsibility of Swisscom to update the devices
Example: CPE

• **Challenges**
  – Update = replace the firmware
  – Many ISP’s use the software

• **Mitigation**
  – Deploy a quick fix
  – Prepare and test the proper fix
  – Coordinate with the vendor

• **For the technical details:**
  – Visit the talk of SCRT@CYBSEC 16
Example: website

- An old marketing page
  - No sensitive data
  - No connections to internal systems
- Forgotten
- Abandoned
- Hosted abroad
- No contacts
- Compromised through some old PHP crap

- With a Swisscom subdomain
- With a www.swisscom.ch/xyz redirect
Conclusion

**Important points**
- Get top management support
- Know your systems and contacts
- Be ready to handle the workload
- Integrate it in the contracts with suppliers
Situation in Switzerland

Part 2
Some questions

• Experiences from other Bug Bounty programs?

• Requirements of / expectations to a Bug Bounty program?
  – What kind of information?
  – Bounty range?

• How does your responsible disclosure work?
  – Are there any company guidelines?
Limitations

• The legal framework
  – No legal action can not be guaranteed, even with the researcher following all precautions and all the rules
  – The researcher bears the risk
    (you are not allowed to look for vulnerabilities, but if you have found one, you can submit it and even get money for it...)
    – Exception: apps and devices you own

• The Dutch approach?
  – If you follow the rules, the authorities guarantee not to take any action against you
Thank you!
Contact information / Links

Links

- https://hackerone.com/swisscom/

Swisscom (Schweiz) AG
GSE-MON
Florian Badertscher
Postfach
3050 Bern

florian.badertscher@swisscom.com