PacNOG14 Conference

Responsible Disclosure

Dean Pemberton

Who am I?

- Dean Pemberton
  - NSRC
  - NZNOG (New Zealand Network Operator Group)
  - NZITF (New Zealand Internet Task Force)
  - InternetNZ
  - other

Who am I?

- Professional Sports Photographer
  - Photos removed due to licencing requirements – but they show All Black Sevens team winning!

What we're going to cover

- What is responsible disclosure
- Why is this an issue for security researchers?
- Why is it an issue for operators?
- A look at the NZITF responsible disclosure guidelines
- A look at the New Zealand Registry Services vulnerability disclosure statement

What is responsible disclosure?

- Definition:

"Responsible disclosure is identifying and then revealing ICT vulnerabilities within the bounds of the law and as a collaborative process between the discloser and organisation based on common practice and policy set by organisations."

- Goals:
  - protect the public from security vulnerabilities
  - vulnerability finders should be acknowledged for their actions and in particular, for their responsible approach
  - organisations should be given an opportunity to respond to vulnerabilities in a controlled fashion before they are made public.

Why is this an issue for security researchers?

“The ministry and I do not deal with hackers and we do not deal with burglars.”

Hon JUDITH COLLINS

Current state of play in NZ

- If you report a security vulnerability to a New Zealand website today you probably have a 50% chance of being reported to the police
- The other 50% you spend a large amount of time trying to explain why it is an issue
- This means that while vulnerabilities are being found every day, they are never being reported or fixed
- We can do better than this – we need to be doing better than this

Why is this an issue for operators?

- Many international software companies have responsible disclosure policies and bug bounties in place
  - Microsoft, Google, Facebook, Paypal …

- There is now a vulnerability market for zero-day software exploits
  - Vupen, ZDI, iDefence, .gov …

This covers major software vulnerabilities, but what about local software or website issues? What about .govt.nz & .co.nz issues?

New Zealand Internet Task Force Responsible Disclosure Working Group

- The working group is tasked with producing guidelines on responsible disclosure.
  - Set norms and expectations for both researchers & organisations
  - Create rules of the road

NZITF Draft RD guidelines

NZRS Vulnerability Disclosure Statement

What's next

Process:

- Draft guidelines up on our website for 6 weeks
- **`nzitf.org.nz`**
- Analyse submissions
- Redraft, review & refine.
- Working group meeting in Feb to adopt final
- Launch final guidelines.