

OWASP 2013

Responsible Disclosure A Local Perspective

Presenter: Nick von Dadelszen

Date: 12th September 2013

Company: Lateral Security (IT) Services Limited

Company Overview

○ Company

- Lateral Security (IT) Services Limited
- Founded in April 2008 by Nick von Dadelszen and Ratu Mason (Both Directors)
- Staff - Auckland, Wellington, Melbourne (18 staff)

○ Services

- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modelling and risk assessment)
- Regular ongoing technical testing and assurance programs

○ Differentiators

- True vendor independence
- Security testing and advisory are our niche specialties
- Highly experienced and skilled staff

Agenda

- What is responsible disclosure
- Why is it an issue in NZ
- What can we are doing about it
- What you can do right now
- Lets start a discussion

What Is Responsible Disclosure

- Definition:

“Responsible disclosure is revealing ICT vulnerabilities in a responsible manner in joint consultation between discloser and organisation based on a responsible disclosure policy set by organisations.”

- Goal:

“To contribute to the security of ICT systems and control the vulnerabilities in them by reporting those vulnerabilities in a responsible manner and acting on the reports appropriately so as to prevent or limit potential damages to the maximum possible extent.”

Why It Is An Issue

- 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 issues?

“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

NZITF Responsible Disclosure Group

- NZITF has created a working group to create some local responsible disclosure guidelines
- Will include a process for researchers and ICT owners
- We hope to include a third party arbiter to allow anonymous disclosure
- We hope to get buy-in from major NZ organisations and .govt.nz
- First draft for consultation is aimed for before Kiwicon

What You Can Do Right Now - Researchers

- Don't break the law
- Crimes Act 252 - Accessing computer system without authorisation:

“Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.”
- What does that mean for SQL injection or XSS?
- What about direct object reference?

What You Can Do Right Now - Researchers

- Talk directly to the organisation, or to another relevant party
 - Hosting Provider, NCSC ...
- Keep anonymous if preferred
- Give enough details for reproduction of the issue
- Give them a chance to fix it before doing anything else
- If desirable, state intention to publish, but don't blackmail

What You Can Do Right Now - Researchers

- Crimes Act 237 – Blackmail:



“Every one commits blackmail who threatens, expressly or by implication, to make any accusation against any person (whether living or dead), to disclose something about any person (whether living or dead), or to cause serious damage to property or endanger the safety of any person with intent—


- (a) to cause the person to whom the threat is made to act in accordance with the will of the person making the threat; and
- (b) to obtain any benefit or to cause loss to any other person.”

What You Can Do Right Now - Organisations

- Discuss how you would handle a vulnerability disclosure
- Determine who is responsible for response
- Make reporting vulnerabilities easy
 - security@...
 - Publish a disclosure policy on your website
- Act in good faith
 - If they are reporting a vulnerability, they are not the bad guys

Recent NZ Example





[Home](#) [About NZRS](#) [Contact](#) [DNS](#) [FAQs](#) [News](#) [Notices](#) [SRS](#) [WHOIS](#)

- » [About NZRS](#)
- » [Board](#)
- » [Community](#)
- » [Governance documents](#)
- » [Presentations](#)
- » [Team](#)
- » [Vision, Mission, Values and Goals](#)
- » [Vulnerability disclosure policy](#)

YOU ARE HERE: [Home](#) > [About NZRS](#) > Vulnerability Disclosure Policy

Vulnerability Disclosure Policy

NZRS is committed to resolving security vulnerabilities quickly and carefully. If you believe you have discovered a security related issue within our online systems, we appreciate your help in disclosing the issue with us responsibly and confidentially so that we can investigate and respond.

PROCESS

Contact us via email (security@nzrs.net.nz) with a detailed report of the potential vulnerability. If you believe the vulnerability is serious or there is a chance that email is insecure, then please encrypt the message with PGP. Our individual keys are listed on the [team page](#) and we will shortly publish details of our corporate key on this page.

This email should include as much of the following as possible:

- » Type of vulnerability

Registrars

Username: *

Discussion Points

- Should public disclosure be an end-goal when dealing with local websites?
- How can we get local organisations to pick this up, assuming they don't know much about security?
- Are bounties a good or a bad thing?
- What about crowd-sourced security testing of government sites?
- What type of organisation could be an arbiter?

Questions & Contacts



Presentation Download
[www.lateralsecurity.com/
presentations](http://www.lateralsecurity.com/presentations)

Vacancies for 3 more staff

Lateral Security (IT) Services Limited

Wellington

38-42 Waring Taylor Street (level 7, Petherick Tower)

PO Box 8093, Wellington 6143, New Zealand

Phone: +64 4 4999 756

Email: sas@lateralsecurity.com

Auckland

187 Queen Street (level 8, Landmark House)

PO Box 7706, Auckland, New Zealand

Phone: +64 9 3770 700

Email: sas@lateralsecurity.com

Australia - Melbourne

200 Queen Street (level 13)

Melbourne, Australia VIC 3000

Phone: +61 452627779

Email: sas@lateralsecurity.com