Security Incident Response Capabilities & CSIRTs

Adli Wahid
Security Specialist
adli@apnic.net
Adli Wahid

• Security Specialist @ APNIC
• Board Member @ FIRST.org
• Member of INTERPOL Cyber Crime Expert Group
• Let’s Connect
  • Twitter: @adliwahid
  • Linkedin: Adli Wahid
  • APNIC’s Blog: https://blog.apnic.net
Security Resilience

- Security by Design
- Security in Deployment
- Security in Operation
- Security in Breach
Ecosystem

Network Operators / Service Providers

Law Enforcement / Judiciary

Policy Makers

End Users / Consumers

National CERTs/CSIRTs | Cyber Security Agency

Hardware / Software Vendors
Why?

1. Get notified
2. Reduce Impact of Security Incident
3. Understand the (root) cause
4. Do Something About It
Get Notified

• How can other CERTs/CSIRT contact you?
  o Incidents
  o Source of Security Incidents
  o Suspicious activities
  o Threat Information

• Whois db and other means
  o APNIC’s Whois Accuracy initiative

• Will you do something about it?
  o Awareness
  o Capabilities
  o Policies & Procedures

• All of the above: Preparedness

https://blog.apnic.net/2016/09/27/lea-stakeholders-enter-whois-discussion/
Reduce Potential Impact

• Timeliness

• Security Incidents have affect constituent’s
  • Operation
  • Business
  • Image / Brand
  • Safety

• Understand the (root) cause
  o Advise / Alert the constituents

• Reduce cost required to fix

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Do Something About It

• Remediation
  o Analysis
  o Collaboration
  o Escalation

• DDoS Example
  o Fixing / removing vulnerable hosts
  o Fixing / removing vulnerable services
  o BCP 38 / Source Address Validation
  o Continuous Monitoring

• Join industry-wide initiatives

ShadowServer Foundation
https://www.cybergreen.net
Community of CSIRTs

- Trusted group
- Information Sharing
- Beyond that
  - Lessons Learned
  - Joint Projects (Standards, Tools, Frameworks)
  - Joint Activities (Events, Drills)
  - Resources (Training, Trainers)
  - Mentoring
- Examples:
  - FIRST.org, APCERT, NZITF

https://www.first.org
CERT/CSIRT Activities in AP Region

• Partnerships
  • Collaboration with FIRST.org
  • MoU with Asia Pacific Computer Emergency Response Teams (APCERT)
  • Share resources, promote initiatives

• Activities
  • FIRST Technical Colloquia (Security Track) at APRICOT & APNIC Supported Events
  • Cyber Security Workshops
  • Training / E-Learning

• 2017
  • FIRST-TC @ APRICOT
  • More activities being planned

Tonga CERT Discussion

Security Workshop in Bhutan
Thank You

Adli Wahid

adli@apnic.net