CNA Challenges from a National CERT Perspective

Seema Khanum

Mohd Akram Khan, CISSP

Indian Computer Emergency Response Team (CERT-In)

CERT-In,
Responsible Vulnerability Coordination
and
CVE Numbering Authority

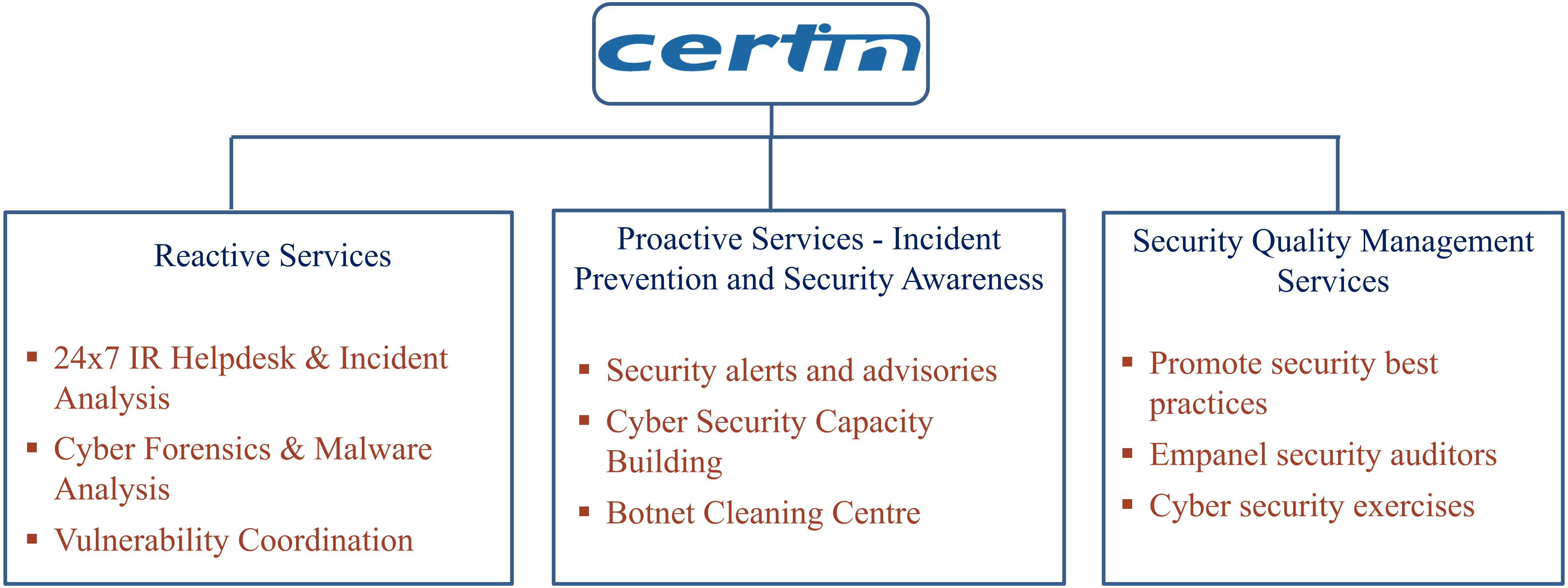
Indian Computer Emergency Response Team

- Established: 2004
- Operating Model – Government funded
- Constituency - Entire Indian Cyber Community (Government, Public, Private and Individuals)
- RFC 2350 - https://cert-in.org.in/PDF/RFC2350.pdf
- Designated as the national agency for specific cyber security functions under Indian IT Laws:

Section 70B of the Information Technology Act 2000 designates CERT-In as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

Indian Computer Emergency Response Team ....contd



certin

Reactive Services

- 24x7 IR Helpdesk & Incident Analysis
- Cyber Forensics & Malware Analysis
- Vulnerability Coordination

Proactive Services - Incident Prevention and Security Awareness

- Security alerts and advisories
- Cyber Security Capacity Building
- Botnet Cleaning Centre

Security Quality Management Services

- Promote security best practices
- Empanel security auditors
- Cyber security exercises

Affiliations

FIRST™ Improving Security Together

APCERT Asia Pacific Computer Emergency Response Team

TF-CSIRT Trusted Introducer

Charter of Trust

Vulnerability Coordination @CERT-In

- Issues requiring actions only by owner / operators
  - Websites, backend application servers, open cloud buckets, old software etc.
  - Remediation to be carried out by owner
    - Code changes, Security controls, system hardening etc.
    - No public announcement – *typically*

- Issues that also require action from customers / clients / users
  - operating Systems, office suits, pdf readers, firmware, Internet browsers etc.
  - i.e. the issues requiring CVE IDs
    - Code changes by vendors / maintainers, patch released
    - Coordinated public announcement
    - Patching to carried out by customers

CVE Numbering Authority (CNA)

- **Inception :** October 2021
- **Scope:** Vulnerability assignments for vulnerabilities impacting all products designed, developed, and manufactured in India
- **CNA Organization Type:** CERT
- **Motivation:** Strengthen trust in “Digital India” and “Make in India”

A Catalyst for Change
From service oriented to global manufacturing hub

TLP:CLEAR

Responsible Vulnerability Disclosure and Coordination Policy

- To encourage responsible vulnerability research in our country
- Enables collaboration with
  - researchers
  - cybersecurity organizations
  - academic institutions
  - vendors/OEMs
  - International CERT's / CNA‘s
- Defines our expectations and what to expect from us
  - Tentative timelines, rewards and a disclaimer

TLP:CLEAR

National CERT - CNA duality

- Coordination is already in the DNA
- Pre-existing trust relationships
- National stature and legal powers help
  - Can urge patience from involved parties
  - Deal with unresponsive OEMs/Vendors
- Quicker public disclosure to constituency
- Promote CVD domestically

- More often need to deal with ‘out-of-scope’ reports
- CVE assignment is not straightforward
  - lacks insight into product (code, libraries etc.)
- Vendors apprehensive of accepting
  - unfounded fear of action
- Situations concerning unmitigated vulnerabilities

TLP:CLEAR

CERT-In's experience with CERT – CNA dual role

Vendor Hesitancy

- CERT-In is federal cyber agency equipped with legal powers to issue directions and initiate legal actions
  - Although rare, OEMs / Vendors mistake our vulnerability notifications as legal notice
- Wary of possible reputational damage
  - Specially smaller OEMs or OEMs into highly competitive markets
  - Competitor might misuse CERT-In's advisory to affect their business prospects
  - Some have even sent written requests
- Some attempt to play down
  - "vulnerability is really not that serious"
- Some delay their responses
  - or worse, become unresponsive

Lack of awareness about CVD

- Some vendors don’t have appropriate security programs
  - Lack of awareness regarding vulnerability handling processes
    - Did not think about it, rarely have to deal with it or don’t have budget for it
  - OEMs supporting exclusive set of entities
  - Need lots of convincing and explaining
- Incomplete remediation
  - Root cause not fixed, improper workarounds – can be bypassed with little efforts
  - Back and forth with reporter and vendor – extends remediation time
  - Reporter may publish negative report

No Point of Contact (PoC)

- CERT-In, being a CERT, coordinates vulnerability reports concerning any Vendor
- Vendors often do not publish PoC for reporting security issues
  - Some vendors do not have appropriate security programs (no surprise!)
  - Most publish sales / customer support contacts
    - tried them and got interesting responses
    - but it works too
- Sometimes researchers report to CERT-In when they can not find proper reporting coordinates
- CERT-In’s existing network, trusted stature and legal authority helped
- Require time and continuous efforts
  - even to the extent of snail mails – rare but still….

Premature public disclosure risk

- Reporter is an important stakeholder
  - CERT-In’s CVD Policy acknowledges
- Impatience about making the issue public
  - A few reporters give their own deadlines - limits mitigation time
  - Some even want the issue to be resolved immediately
- Bounty / rewards expectations
  - Our CVD policy provides for giving recognition and appreciation
  - No provision for monetary reward currently, but Vendor can if they desire

TLP:CLEAR

Other issues worth noting

- A CERT CNA / Third Party CNA often lacks required insight into product
  - Proprietary products
  - Possibility of white labeling of software
  - Assignment becomes complex
    - Coordination begins with a questionnaire
- Situations where owner doesn’t control the code
  - Third party / outsourced code
  - Contract expired or lacks provisions

Conclusion

Meeting constituency's expectations

- CERT-In is the trusted cyber security agency in India
  - Government, public, private sector and individuals refer for services and guidance
  - Must fulfill high expectations
- Good CVD policy is important
  - Timelines, expectations, scope of rights and obligations etc. helps
- But expect disagreements nonetheless
  - "timeline mentioned is too long"
  - "no provision for safe harbor"
  - "issue not fixed immediately, nobody is serious"
  - Significant media interest
- Feedbacks are always welcomed
  - allows us to improve

Key takeaways

- Operating as both CNA and National CERT has its advantages
- National CERTs can raise awareness about importance of CVD
  - clarify doubts and apprehensions
  - help expedite dissemination of vulnerabilities
  - manage everyone's expectations and save negative publicity
- Promote CVE program amongst local vendors
  - bring transparency in vendor vulnerability disclosure
  - ensure proper remediation of issues and save time
- Also appreciate Vendors for their efforts
  - give credit to save their interests
- National CERTs can help deal with unresponsive / uncooperative Vendors

Thank you

www.cert-in.org.in