Internet Security

A Solid Foundation for Sustainable Internet Development

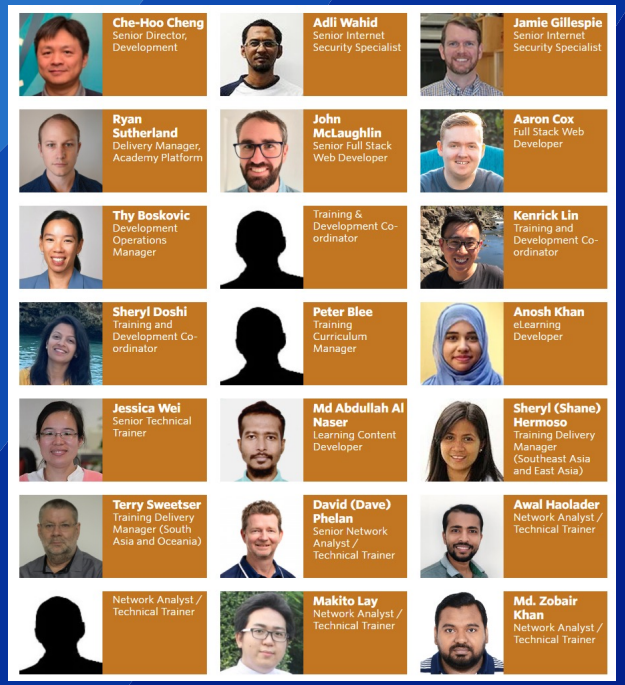
Presenter:

Terry Sweetser

Training Delivery Manager, South Asia & Ocenia
APNIC

Acknowledgements

Che-Hoo & The Team
APNIC Development



Internet Security

- A branch of Computer Security or Cybersecurity
- Encompasses the Internet, browser security, website security, and network security as it applies to other applications or operating systems as a whole
- Objective is to establish rules and measures to use against attacks over the Internet
- Internet is an inherently insecure channel for information exchange, with high risk of intrusion or fraud, such as phishing, online viruses, trojans, ransomware and worms

Source: https://en.wikipedia.org/wiki/Internet_security

Security Breaches Are Public News

- Many countries now have laws requiring security breach notifications
- You don’t need to go far to see examples from all industry sectors
- Check out www.haveibeenpwned.com

Critical Infrastructure

- Critical Infrastructure uses the internet
- Even companies that don't consider themselves to be CI, would be classified as such by the government
  - Food production/delivery
  - Non-hospital health services
  - Manufacturing

Critical Infrastructure

- Many ISPs and data center providers may be hosting CI without even knowing it
  - Do the protection requirements then extend to the ISP or DC?
  - Do your providers know how important your data is?

Infrastructure Critical to Your Business

- Even if a company isn't part of CI, it usually holds valuable information for the operation and existence of that company (and sometimes of the livelihood for their customers)
  - Entire companies have been shut down or lost >10% of their stock price after a data breach
  - Others have exposed financial and personal information for millions of customers, most of which cannot be changed or replaced by the customers so they will live in perpetual fear of their data being misused against them

The Global Village

- The internet is not a local network, attacks can come from anywhere
- While some attacks are very targeted (APT), the majority are completely indiscriminate
  - They don't know who you are, they don't know where you are from, they just want to cause damage and disruption, or to make money.
  - If you are an easy target, you will be found.
  - You may already be compromised. Many organisations don't discover a compromise until months (or even years!) after the initial event.

Security is a journey, not a destination

- Having the right staff, with the right skills is important
- Attacks and countermeasures are in constant change/development, so continuing education and information sharing is crucial to stay proactive
- If you don’t hear about your company’s risks and vulnerabilities, you probably need to look harder
- One step at a time

Security Commitments

- People, Process, Technology
  - No Surprise
  - Not Optional
- Security Program with continuous enhancement
- You may not always know what threat actors want
- Technologies aren’t always perfect
  - Vulnerabilities in software & protocols always exist

People

- Knowledge and awareness
- Actual people to lead and do the work
- Dedicated resources to increase capabilities
  - Security consists of multiple domains
  - Specialisation & focus required
- Retaining expertise is not easy
- Your people is the last line of defence

Process

- Documented & Actioned policies, procedures and strategy
- Adopt or follow framework i.e. ISO27001, NIST Cybersecurity Framework
  - Common reference for everyone
  - Bottom line is the same for many frameworks
- Assumed Breach -> Zero Trust Framework
  - Verify before granting access even from internal systems
- Continuous Assessment to validate & remind
  - Audits
  - Table-Top Exercises

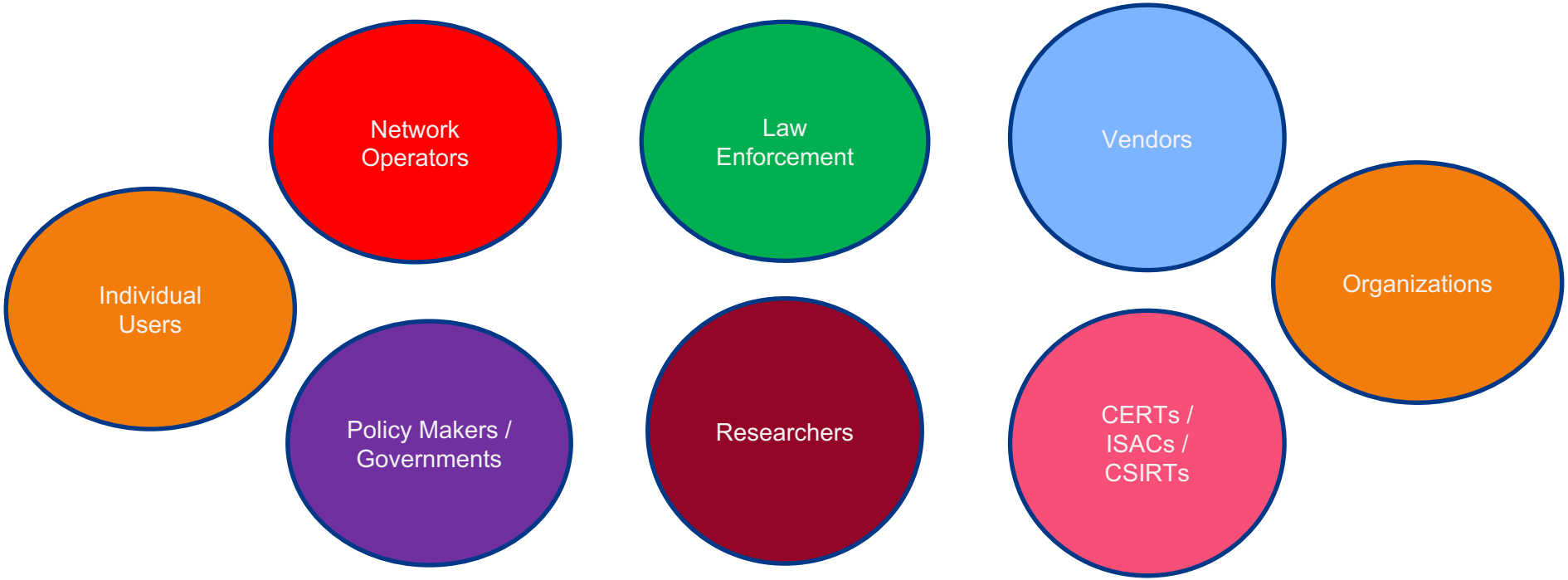
Technology

- Another big area for investment
- Technical Security Controls to protect assets and infrastructure
- Inter-dependencies
  - No single solution or silver bullet
- Cost & Affordability
  - Backup is critical in dealing with ransomware
  - Not enough budget for back-up a big risk
- The most expensive solution is not always effective
  - May consider Free & Open-Source Software

Collaboration

- Everybody should play a part and collaborate on Internet security
  - Easier said that done though
- Thinking beyond your own Enterprise / Organisation
  - Help one another and be a good citizen
- Doing security with others in the same sector or with other stakeholders
  - Accelerate learning
  - Create critical mass / pool of security expertise
  - Address gaps in the ecosystem
- Examples
  - Information exchange
  - Capacity development
  - Sharing resources (i.e. awareness materials)

Cyber Security Ecosystem



What Network Operators Care About

- Cost / Performance / Resilience / Interconnections / Efficiency / Scalability / **Security / Stability**
- The market is highly competitive
- All operators are searching for their own niche positions which make them look better than their competitors in order to survive

DDoS Attacks – A Big Headache

- With enhanced Internet infrastructure from backbones to edges, there are more and more large-scale DDoS attacks on Internet of different types
  - DNS Amplification
  - NTP Amplification
  - TCP SYN Flood
  - Random DNS queries on targeted domain names
    - Relevant DNS servers are suffered
- Network operators suffered a lot from time to time
- Network Operators MUST follow the best practices!!!

BGP Prefix Hijacking – Another Big Headache

- Definition:
  - Announcing a more specific path
  - Announcing an address space that is owned by someone else
- Impacts:
  - Rerouting traffic to a malicious network
  - Enabling interception and alteration of sensitive data
  - Causing network unavailability

Source: Williams, R. (2015). street signs being stolen [Image]. https://media.apnarm.net.au/media/images/2015/02/06/IQT_06-02-2015_NEWS_05_STOLENSIGNS1_t1880.jpg

Best Practices for Network Operators

- More like guidelines for engineers
- On technical and operational parts
- Not something very static
- Technologies and the industry are changing very fast
- Engineers should update themselves continuously
- Start from: https://datatracker.ietf.org/doc/bcp
  - There are more than these though…
- End Goal
  - To help make Internet more stable and secure
  - Everyone should do it, together

BCP46 – Recommended ISP Security Services and Procedures

- A good summary as of Year 2000
- Computer Security Incident Response Team (CSIRT)
  - *Abuse / Incident Response Team (IRT) contacts on APNIC database*
- Appropriate Use Policy (AUP)
  - Should be clear in stating what sanctions will be enforced in the event of inappropriate behavior
- Registry Data Maintenance
  - Internet Routing Registry (IRR) and APNIC databases
- Ingress/Egress Filtering on Source Address
- Route Filtering
- Disable Directed Broadcast as default [BCP34]
- No Open Mail Relay [BCP30]
- SMTP Service Extension for Authentication [RFC2554]

BCP38 – Network Ingress Filtering

- Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  - Ingress traffic filtering at the periphery of Internet connected networks will reduce the effectiveness of source address spoofing denial of service attacks
  - Sources of attacks can be traced more easily
  - Reflection type of attacks can be mitigated largely
- Should be done at both the ISPs and edge networks

Packet Filtering Principles

- Filter as close to the edge as possible
- Filter as precisely as possible
- Filter both source and destination where possible

Best Practices for Ingress / Egress Prefix Filtering

- For Ingress Prefix Filtering:
  - Don’t accept RFC1918/RFC6890 prefixes
  - Don’t accept your own prefixes
  - Don’t accept default (unless you need it)
  - Don’t accept prefixes longer than /24
  - Set ingress max prefix limit for peers/IXPs
- For Egress Prefix Filtering:
  - Announce only your own and your customers’ prefixes to your upstream providers and peers/IXPs
    - Don’t announce default, prefixes belonging to upstream providers/peers/IXPs that you directly connect to and all other prefixes!!!
  - You may announce default and/or full routes to your downstream customers (if they need them) but not the others
- http://www.team-cymru.org/Monitoring/BGP/

Routing Security with RPKI

- RPKI deployment has 2 phases
- ROA is just the beginning

RPKI
robust security framework for verifying the association between resource holders and their Internet number resources

Phase 1: ROA (Signing origin)
Resource holders must create their ROA objects, which gets published to the RPKI repo

Phase 2: ROV (Validating origin)
Routers are validating route entries against the RPKI cache

BCP185 – RPKI-based Route Origin Validation

- Origin validation needs to be done only by an AS's border routers
- Operators should be aware that accepting Invalid announcements, no matter how de-preferenced, will often be the equivalent of treating them as fully Valid
- Operator's policy should not be overly strict and should prefer Valid announcements; it should attach a lower preference to, but still use, NotFound announcements, and drop or give a very low preference to Invalid announcements
  - Announcements with Invalid origins SHOULD NOT be used, but may be used to meet special operational needs
- Operators SHOULD use "minimal ROAs" that authorize only those IP prefixes that are actually originated in BGP

AS0 ROAs

- ROA with origin AS0 instead of a real ASN
  - Routes will be RPKI-invalid when they would otherwise be RPKI-unknown.
- Why use it?
  - Prevent unused delegations from being hijacked
  - Mitigate leakage of private-use public address space
- AS0 will never appear as a functional origin in a ROA (see RFC7607)

Ex: For the following VRPs

VRPs
2.0.0.0/16-16, AS0
3.0.0.0/22-24, AS0
4.0.0.0/24-24, AS0
4.0.0.0/24-24, AS1234

With Origin Validation, these BGP routes will have an RPKI state as follows:

ASN	Prefix	RPKI State
1234	1.0.0.0/24	NOT FOUND
1234	2.0.0.0/16	INVALID
1234	2.0.0.0/24	INVALID
1234	3.0.0.0/16	NOT FOUND
1234	4.0.0.0/24	VALID

IPv6 Security

- The worldwide IPv6 capability is at 39.37%. With nearly 40% of network traffic using IPv6, protecting your IPv6 network is very important.
- Common misconceptions:
  - IPv6 is secure by default,
  - IPv6 is too large to scan
  - No NAT makes IPv6 insecure
- The key lessons are:
  - Don’t underestimate the scale of the differences between IPv6 and IPv4.
  - Your IPv4 networks need to be secured against IPv6 vulnerabilities.
  - Your network and security staff need to be competent in IPv6 and in IPv6 security features.
  - How IPv6 is deployed will influence how secure it is in practice.

IPv6 Security Practices

- Filtering ICMPv6 is not straightforward
  - **RFC4890**: “ICMPv6 Filtering Recommendations”
- Filter IPv6 bogons
  - Bogons are commonly found as source addresses of DDoS packets
  - Craft prefix filters from bogons list
- IPv6 DDoS
  - IPv6 introduces a new attack vector with larger potential attack volume.
  - Apply ingress/egress filtering and rate limiting
  - Don’t forget **BCP38**

MANRS

- Mutually Agreed Norms for Routing Security (MANRS)
- A global initiative to improve security of the Internet's routing system and reduce the risk of routing-related incidents
- Outlines specific actions that organisations can take (filtering, anti-spoofing, coordination) to contribute to a more secure and reliable internet infrastructure

https://manrs.org/

DNS Best Practices

- Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS)
- ICANN-supported program that promotes operational best practices for DNS security
- Implementation guidelines https://kindns.org/guidelines/

Good read: KINDNS initiative to improve mutual understanding and security of DNS among operators

DNS Security

- Data exchange or transactions => TSIG, SIG0
- Data accuracy from the right source => DNSSEC
- DNS transport security or privacy => DoH, DoT
- Access to legitimate sites/content => DNS Filtering
- Availability of DNS service => DNS Resiliency

DNSSEC Best Practices

- ICANN DNSSEC Guidebook for ccTLDs
  - https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

- APNIC DNSSEC Policy and Practice Statement (DPS)
  - https://www.apnic.net/wp-content/uploads/2016/11/DNSSEC_DPS_210616v1.pdf

BCP16 – Selection and Operation of Secondary DNS Servers

- Authoritative Servers
  - Usually one primary/master server and multiple secondary/slave servers
  - Which one is the real master may not be known externally
  - *Using stealth/hidden master is recommended*
- Servers should be placed at both topologically and geographically dispersed locations on the Internet
- *Using anycast for DNS is becoming the norm*
  - *Not just for root or TLDs but also for individual domain names which have high demands*
  - *Not just globally but also locally*
- *Do not forget about reserved zones*

BCP126 – Operation of Anycast Services

- Multiple nodes sharing the same IP address
  - Coarse distribution of load across nodes
  - Mitigate non-distributed DoS attacks by localizing damage
  - Constraint of DDoS attacks
  - Improve query response time
  - Good for serving DNS queries
- Routing to determine which node to use
- Local scope anycast vs global scope anycast

RFC140 – Preventing Use of Recursive Nameservers in Reflector Attacks

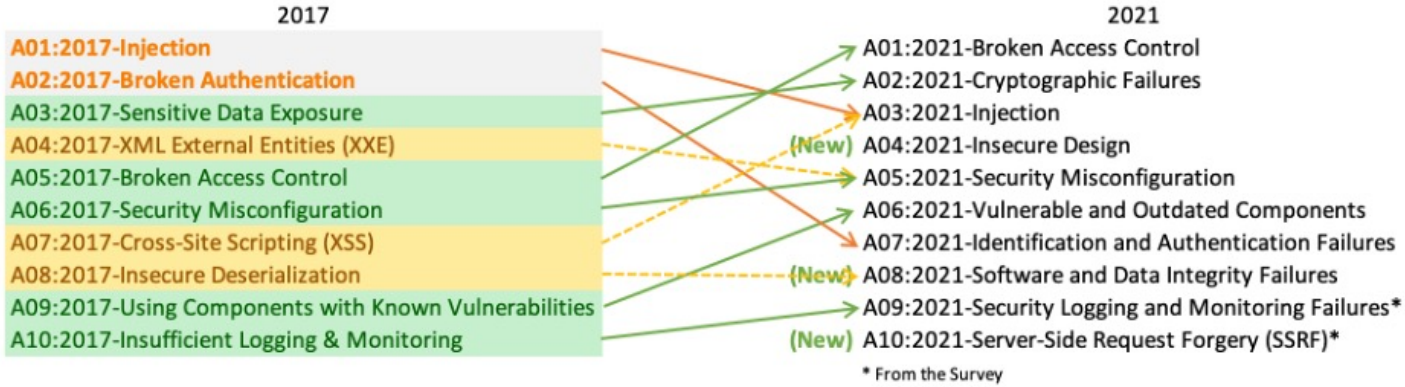
- Due to small query-large response potential of the DNS system, it is easy to yield great amplification of the source traffic as reflected traffic towards the victims
- Amplification factor (response packet size / query packet size) could be up to 100
- Nameserver operators to provide recursive name lookup service to only the intended clients:
  - Disable Open Recursive Servers!!!
  - IP address based authorization
  - Incoming interface based selection
- **Turn recursion off complete on Authoritative Servers!!!**
  - **Keep recursive and authoritative services separate as much as practical**

BCP162 – Logging Recommendations for Internet-Facing Servers

- NAT is being used widely to preserve IPv4 addresses
  - Multiple nodes sharing one IPv4 address
- Still need to support abuse mitigation or public safety requests under such scenarios
- It is RECOMMENDED that Internet-facing servers logging incoming IP addresses from inbound IP traffic also log:
  - The source port number
  - A timestamp, RECOMMENDED in UTC, accurate to the second, from a traceable time source (e.g., NTP [RFC5905])
  - The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports

OWASP Top 10

- Open Web Application Security Project (OWASP) presents the most critical security risks to web applications
- OWASP Top 10 2025 will be released in early 2025



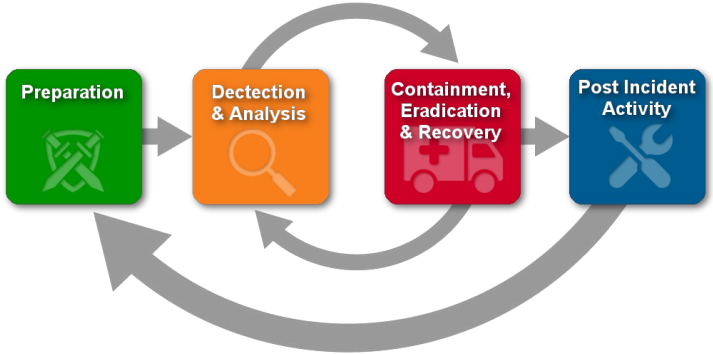
https://owasp.org/www-project-top-ten/

Zero Trust

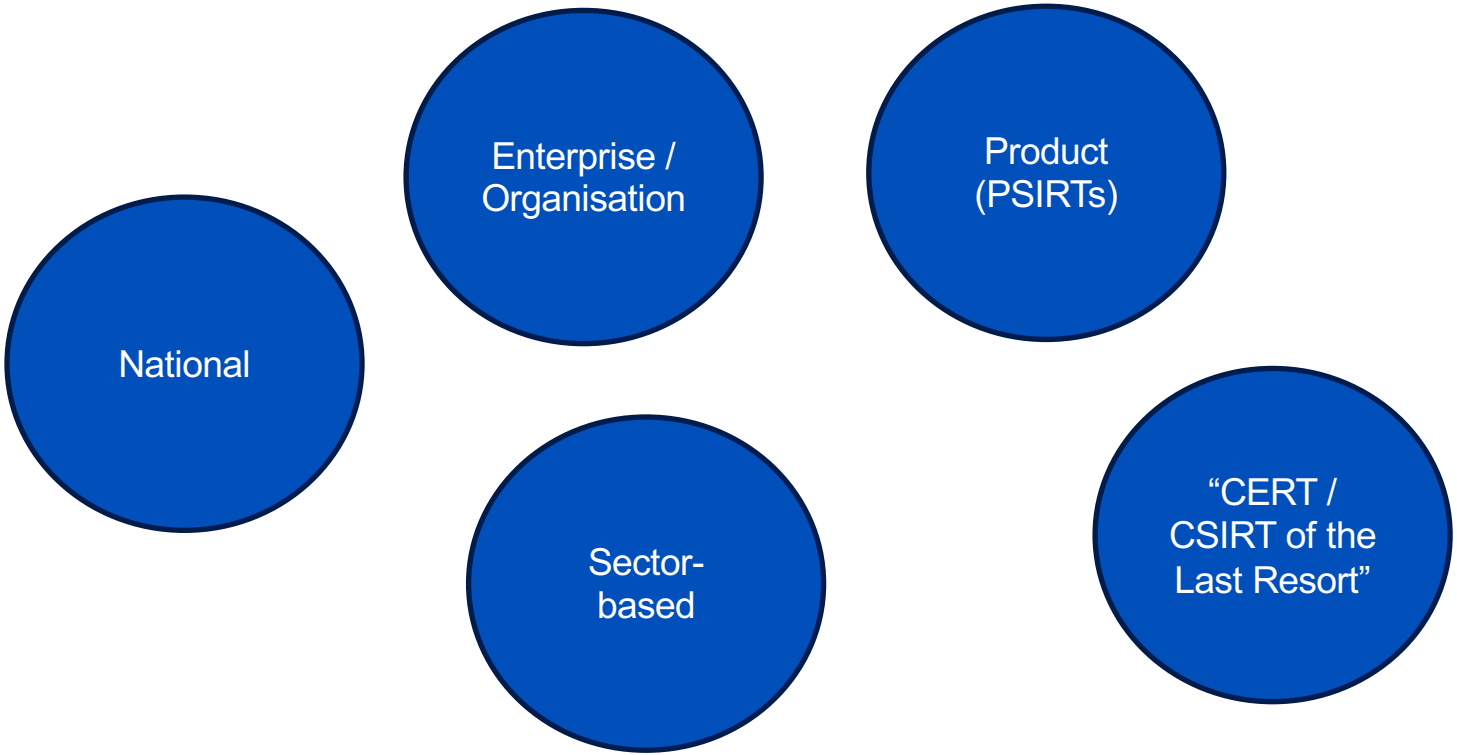
- Zero trust is a security model that assumes that any device can be compromised.
- This is a shift from the traditional approach of securing the network perimeter to one that verifies and authorizes every access, regardless of origin
- Key principles:
  - Least privilege access, Segmentation, Continuous monitoring

Security Preparedness, Response & CERTs/CSIRTs

- Security incidents can cause disruption, destruction & affect reputation
- Need to be prepared & have a response plan
- Computer Emergency Response Teams / Computer Incident Response Teams (CSIRTs) are dedicated resources for responding to security incidents
- Co-ordination at the National Level
  - Internally with other agencies & enterprise CSIRTs
  - International organisations
- Check out APCERT.org & FIRST.org



CERTs/CSIRTs - Different Responsibilities / Constituencies



NOGs

- Network Operators' Groups (NOGs) are being established everywhere in Asia Pacific
  - To create a community of engineers working for different companies / organisations
  - To exchange knowledge and information
    - Best practices, new trends and so on
    - Share repository of useful information such as useful tips and trouble-shooting tools
  - To enhance overall quality of Internet infrastructure
    - Performance, security, stability and so on
  - May help do trouble-shooting and solve problems together when needed
  - Collaboration among people working for competitors!!!
- Regional NOGs
  - NANOG, APRICOT, SANOG, PacNOG, MENOG
- Local NOGs
  - JANOG, HKNOG, AusNOG, NZNOG, MYNOG, SGNOG, IDNOG, PHNOG, BDNOG, and many other NOGs
  - No exclusivity though
- TWNOG revived but more collaboration needed continuously

APNIC's Vision & Mission

- Vision:
  - "A global, open, stable, and secure Internet"
- Mission:
  - To provide essential services as a Regional Internet Registry, and **to support Internet development in the Asia Pacific region**

Internet Development Work at APNIC

- Human Resource Development / Capacity Building
  - Training (APNIC Academy), Technical Assistance & Deployment Support on Internet infrastructure, Operations & Security covering best current practices
- Technical / Security Community Support & Engagement
  - NOGs, Peering Forums, NRENs/RENs & CERTs/CSIRTs
  - LEA/PS Engagement
- Internet Infrastructure Support
  - IXPs, Root Servers, Honeynet & RIPE Atlas

APNIC Academy

- **Resource for Learning Internet Infrastructure, Operations & Security**

- **What It Offers:**

Self-Paced Online Courses

Hands-On Virtual Labs

Access to eduroam

Technical Assistance for Members

Face-to-face Training

Comprehensive Course Material

Explore APNIC Academy's most popular courses!

APRICOT 2025 – CfP open now

- The PC is looking for content for the conference and tutorial sessions and Peering Forum
- Deadline for submissions 27 Jan 2025

https://2025.apricot.net/programme/callforpresentations

Final Remarks

- Take security seriously
- Don’t wait for a data breach before implementing basic best practices
- Hire good people and listen to them
- While it may sound bad, it will only get worse, so make positive changes now
- Let’s work together to make Internet more stable and secure!

Thank You!


Questions