Promoting Network Security (A Service Provider Perspective)

“Prevention is the Foundation”

H S Gupta
DGM (Technical)
Data Networks, BSNL
hsgupta@bsnl.co.in

Connecting India

Agenda

- Importance of Network Security for a Service Provider
- Challenges in enhancing security in Service Provider environment
- Various security threats
- Role of Service Provider in enhancing security
- Role of customer in enhancing security
- Ways to minimize Security Threats
- Conclusions

Connecting India

Importance of Network Security for a Service Provider

- Service availability is maintained
- SLAs are maintained and Service degradations are avoided
- Reduction in manpower and other support costs
- Customer satisfaction and confidence is increased
- Public image is maintained
- Revenues are maintained
- Possibilities of getting involved in litigation are reduced

Connecting India

Challenges in Enhancing Security in Service Provider Environment

- Multiple Services
  - Internet [Narrowband, Broadband (DSL, Broadband Loop Carrier), Wireless (Wi-Fi), Leased]
  - PSTN
  - Mobile
  - VPN, Dial VPN
  - Hosting and Colocation
  - & others
- Vast Coverage in terms of Network Elements
- Increase in use of IT for OSS & BSS (Need to maintain Main and DR sites)
- A number of systems from different vendors need to get integrated (Best of breed scenario)

Connecting India

Challenges in Enhancing Security in Service Provider Environment

- Managing multiple vendors (More so in PSU scenario)
- A number of maintenance contracts with different vendors for maintenance of hardware and software
- Systems and Processes need to keep pace with technology
- Rapid Technological Evolution

Connecting India

Challenges in Enhancing Security in Service Provider Environment

- Number of attacks and vulnerabilities continue to grow
- Applications and products continue to be shipped with insecure defaults
- Striking a right balance between Over Protected to Under Protected
- New services and applications are adding to the complexity

Various Security Threats

- Any use of the Internet, be it via broadband or dial-up technology, poses certain security and privacy risks.
- Broadband poses a higher risk than dialup technology because of "Always On" nature and high bandwidth.

Connecting India

Various Security Threats

- Email
- Open Proxies
- Viruses, worms & Trojans
- Open Mail Relay
- Distributed Denial of Service Attacks (Weapons of Mass Disruption)
- Botnets
- Intrusion
- Malicious traffic
- Malicious Code
- Managing Multi Vendor scenario
- Managing multiple hardware & software

Connecting India

Various Security Threats

- Managing multiple services
- Spyware
- Identity Theft and Phishing
- Increase in the use of Internet for criminal & terrorist activities
- Application and OS Vulnerabilities
- Former employees
- Insider threats (current employees, vendors)
- Hackers
- Employee Error
- Social Engineering, Spoofing, Appl embedded attacks, blended attacks

Connecting India

Threats Due to E-mail

- Spam
- Phishing
- Cyber Crime cases (including abusive attacks)
- Forged E-mails

Impact of Spam on Service Provider

- Increase in hardware sizing
- Increase in bandwidth requirement
- Customer quality of service gets impacted
- Cost at Customer side
  - More data to download
  - More time to download
  - Loss of productivity

Back

Connecting India

Consequences of Open Proxy Servers

- Open Proxies allow a third party to exploit the system to send unsolicited emails or carry out illegal activities that get traced to exploited system
- Malicious users cover their tracks by chaining through multiple proxies either manually or using products such as Proxy Chains
- The IP of the organization being blacklisted by various bodies
- The loss of image of the organization and legal ramifications, if misused for illegal activities
- Loss of bandwidth

Back

Hacking of Websites

- Defacement
- Malicious content
- Stealing of information
- Hosting of Phishing Sites
  - Customers even doesn't know that this has been hosted
  - Comes to know when Service Provider tells them
  - Incidents are increasing at an alarming rate
- Reduces confidence for Online Activities

Back

Live Case Studies

- Phishing sites of a number of Banks
- List of Open Proxy Servers
- Nigerian 419 scam
- Lots of defacement of Websites
- Increase in network traffic due to worms like Blaster, Sobig, Nachi
- Increase in CPU utilization due to malicious traffic
- More outbound traffic than inbound
- Connecting insecure PC in the LAN

Connecting India

Different Security Tools

- Policies & Procedures
- Access Control
- Host Intrusion Detection System
- Network Intrusion Detection System
- Firewall
- Intrusion Prevention System
- Anti-Virus
- Anti Spam
- Vulnerability Assessment
- Public Key Infrastructure

Connecting India

Different Security Tools

- Network Baselining
- Out of band Management
- Time Synchronization (NTP)
- Access Control Lists
- Documentation
- Physical Security
  - Bio Metric devices
  - Water Leakage Detection
  - Rodent Repellant System

Connecting India

Role of Service Provider in Enhancing Security

- Protect own infrastructure from customers, employees and outside world
- Help protect other peers
- Make the Customers aware about Internet Security as attacks targeted to a particular customer CAN and DO affect the Service provider infrastructure
- Protect customers from outside world as also from each other

Connecting India

Role of customer in Enhancing Security

- Awareness about Internet Security, viruses, Fraud developments etc.
- Use of Virus Protection software
- Use of Personal Firewall
- Filter E-mail for Spam
  - Most Spam mails contain scam of some sort
  - Delete spam mails from webmail
- Not responding to phishing Emails
- Not sharing the Internet account with anyone.

Role of customer in Enhancing Security

- Restricting access to the Internet leased line or Broadband connection.
- Visiting trusted websites
- Turning off computer when not in use
- Disable non-essential services such as file and printer sharing
- Download and install the patches as needed

Connecting India

Ways to Minimize Security Threats

- Deployment of proper technology
- Increasing customer awareness
- Increasing employee awareness
- Updated Systems & Procedures
- Keeping updated about latest trends in Security

Connecting India

Security…

Not just a Technology Problem

80% of the security risks can be avoided by taking basic precautions

Connecting India

Security Dilemma

- Moore's law in reverse direction- networks are becoming less secure while the cost to defend them is increasing.
- PREVENTION IS THE FOUNDATION

Connecting India

Conclusions

- Security is not to be treated as a mere hardware and software issue
- Static and Passive approach to security is inadequate
- Customer & employee awareness is important
- Point solutions are no good. Holistic approach needs to be taken

Connecting India

Conclusions

- Security needs to kept in mind while designing the network
- Systems and Procedures must be in place to deal with multi-service, multi-vendor, multi-hardware & software network
- Concentrating on Preventive aspects will be cheaper and effective

Thank You

Connecting India