



Challenges of Network Security



Phillip Barker
IT Director, Curry County
BarkerP@co.curry.or.us



Overview

There are many threats to mitigate:

- Physical security, Passwords, Remote Access, Phishing, Network Security, Viruses & Spyware, Hostile email & websites, Laptops, Default passwords, Lack of Awareness, Intruders, Insiders, Network design defects.



Goals

- Security Posture improvement.
- Mitigate or eliminate reachable and exploitable vulnerabilities.
- Use layered security model to build survivable infrastructure.
- Layered defenses increase your chance of detecting a breach.
- Layers are physical, technical and psychological.



Balancing Risk and Security

- Strike a balance between security and usability; the more secure you make it the less useful it is.
- Risk Tolerance: What do you consider a reasonable security posture?



Email Security

- Inspection and screening of all email is critical to defending networks against attack.
- There are now email security appliances from many vendors. Choose one with nothing in common with your internal systems. By doing so you greatly reduce your risk by improving odds for successful detection of hostile content.



Web Security

- Many threats to contain: Hostile website content comes in a wide variety of forms.
- Countermeasures: Secure filtering proxy, Browser security plug-ins from Finjan, Web of Trust, AdBlock, McAfee Site Advisor and others.



A More Secure Environment

A combination of:

- Hardened hosts
- Intrusion detection
- Established procedures
- Dedicated Knowledgeable IT Staff
- Continuous training
- Know thy network!



Training & Awareness

- www.cert.org
- isc.sans.org
- www.giac.org
- www.isc2.org/cissp/default.aspx
- www.infosecinstitute.com

Also from Cisco, IBM, Microsoft.




Links to Tools

- www.nessus.org
- www.eeye.com/Retina/
- www.snort.org
- bro-ids.org
- wireshark.org
- www.cisco.com/web/go/asa



Email security tips

- Drop all SMTP traffic from:
 - * .wireless.isp.com
 - * .cablemodem.homeisp.com
 - * .dhcp.isp.com
 - * .adsl.isp.com
 - * .customer.isp.com
 - * .ppp.isp.com



Things to consider

- Use the same assessment and profiling tools used by hackers to find and remove weak-points before they're exploited.
- Problems: Unpatched, Default, Unfiltered, Unrestricted, Misconfigured, Unaudited.



Things to Consider

- Attack tools are now more widespread and easier to use. No special skills or knowledge required.

www.metasploit.com/

www.insecure.org/



Questions?

- Thanks for taking the time to learn more about network security.
- I'll be happy to answer all your questions.