Locking down Exchange Server: E-mail security fundamentals

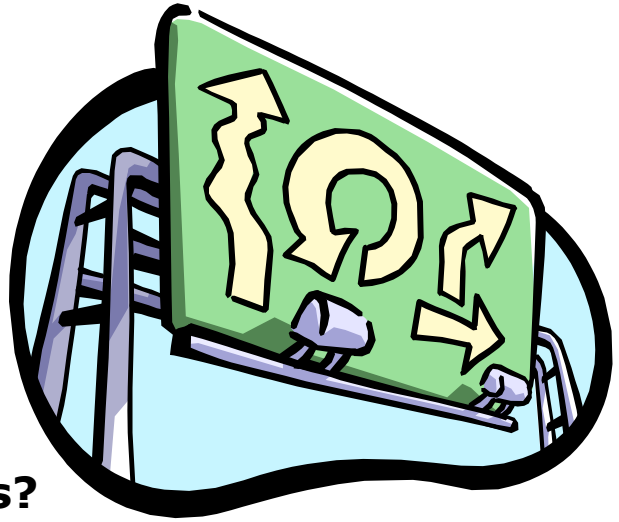
E-mail Security Webcast Series: Part 1 of 5

Speaker: Lee Benjamin

ExchangeGuy

LeeB@ExchangeGuy.com

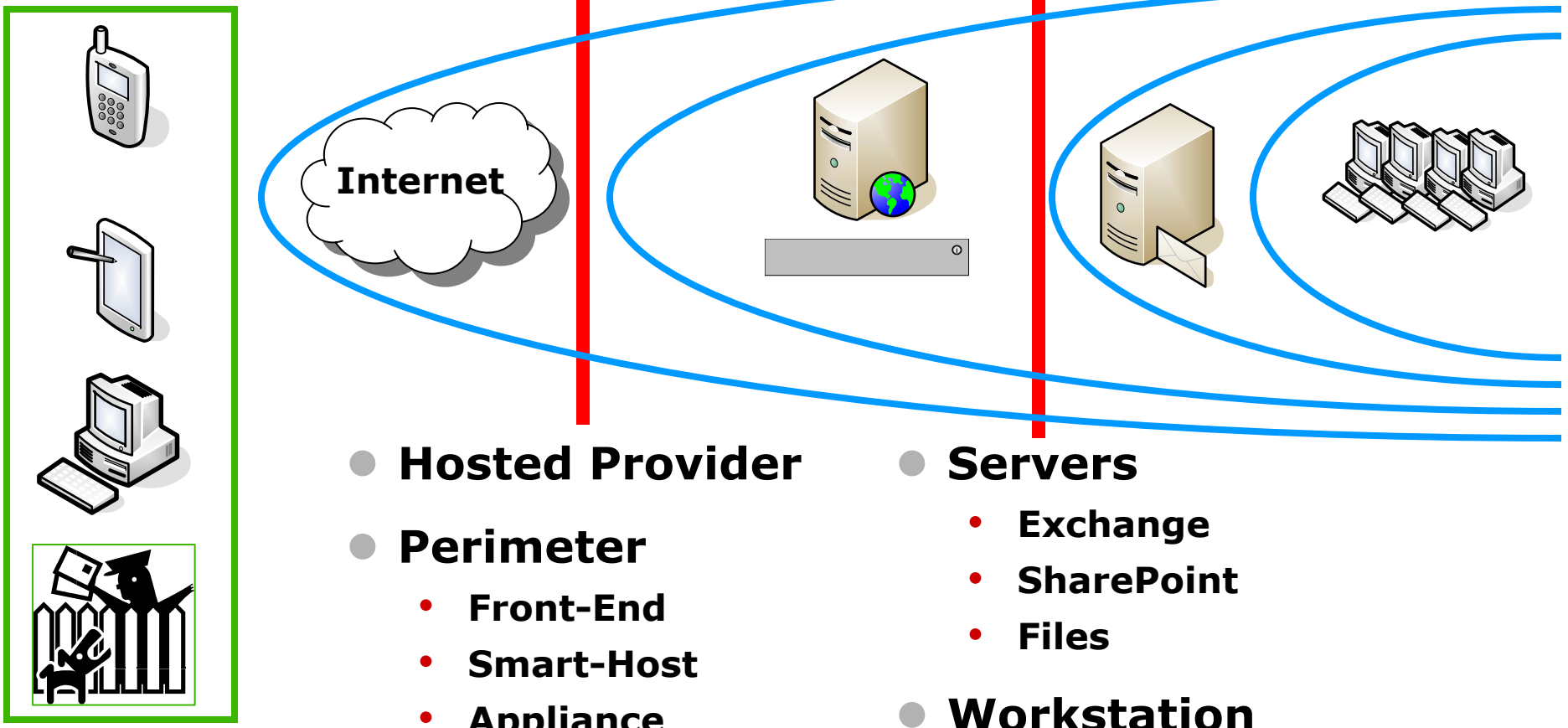
Documentation!



- **Draw a Picture**
- **More Complex Today Than Ever**
  - **Where is your External DNS Hosted?**
  - **External MX Record Points To?**
    - **Do You Have a Secondary MX Record?**
  - **Hosted Services for Anti-Spam/Anti-Virus?**
  - **One or Two Firewalls? ISA Server?**
  - **Perimeter Appliance?**
  - **Exchange Front-End Server?**
    - **Or Smart Host (MS Way of Saying Unix/Linux Box)**
  - **Exchange Gateway/Hub Servers**
  - **Messaging Hygiene Server**
  - **Exchange Mailbox Servers (finally)**

Defense In Depth

Quarantine **Hosted** **Perimeter** **Servers** **Workstation**



- **Hosted Provider**
- **Perimeter**
  - **Front-End**
  - **Smart-Host**
  - **Appliance**
- **Servers**
  - **Exchange**
  - **SharePoint**
  - **Files**
- **Workstation**

Exchange and Anti-Virus

- **Must Have**
- **Most Exchange Shops Use Top 4-6 Vendors**
- **On Your Exchange Servers**
  - **Note: Different Version for File Servers**
  - **Do NOT Scan Exchange Directories with File Anti-Virus**
- **Also Anti-Virus on Perimeter, Perhaps External**
- **Microsoft Purchased Sybari**
  - **Multiple AV Scan Engines, Anti-Spam Add-on**
  - **Antigen for Exchange, Separate Solution For Now**
  - **Also Antigen for Domino/Notes and SharePoint**

Patch Management

- **Install Security Patches With a Few Days**
  - **Exploits Exist Before They Are Released!**
- **Hot Fixes Only If You Need Them**
  - **Call - Support Charges Waived**
- **Rollups**
  - **Yes, They've Been Tested**
- **Service Packs**
  - **Listen To The Chatter (NewsGroups, Blogs, etc.)**
- **Patch Distribution**
  - **Exchange Patches Now Available Thru Microsoft Update (MU) and Windows Server Update Services (WSUS)**

Reduce Attack Surfaces

- **POP3 and IMAP4**
  - **Off By Default in Exchange 2003**
- **NNTP**
  - **Yes, NewsGroups In Exchange Server**
  - **Turn NNTP Service Off After Install**
  - **Exchange Roles**
- **Exchange Roles**
  - **Front-End / Back-End**
  - **Do You Need SMTP, Information Store, etc.**
  - **Exchange Security Templates**
    - **Exchange 2003 Backend Security.inf**
    - **Exchange 2003 Front Security.inf**

Exchange Best Practices Analyzer and Security

- **GREAT Tools To Analyze Your Exchange Environment!**
- **Security Items…**
  - **Recent Changes**
  - **Global Message Size Limits Set**
  - **UCE (Spam) Thresholds**
  - **Latest Service Pack and Patches**
    - **Not Replacement for Microsoft Baseline Security Analyzer (MBSA)**
  - **DNS, Kerberos Configuration**
  - **TCP/IP Ports, Protocols, Suppress OOF to DL's, Exchange Journal (Archive) Settings**
  - **Anti-Virus Installed, Recent Signatures, Symantec, McAfee, Sybari**
  - **Hot Fixes (Windows and Exchange)**

Resources

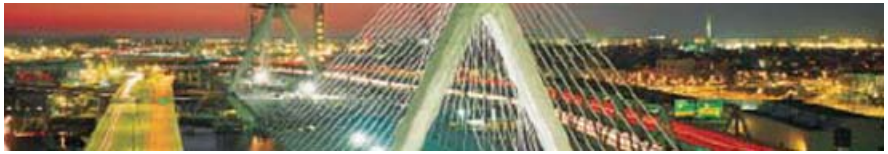
- **Exchange Team Blog**
  - http://blogs.technet.com/exchange
- **Exchange Best Practices Analyzer**
  - http://www.exbpa.com
- **Exchange Server 2003 Technical Documentation Library**
  - http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.mspx
  - **Message Security Guide for Exchange Server 2003**
  - **Ten Additional Exchange Security Documents**
- **Exchange Virtual Labs**
  - **Web-based Access To Labs**
- **Utilities and Add-On Products**
  - http://www.Slipstick.com
- **TechTarget Articles**
  - http://www.SearchExchange.com

Thanks!

ExchangeGuy

LeeB@ExchangeGuy.com

www.ExchangeGuy.com



www.ExchangeServerBoston.com