

电信网络安全的价值

赵粮

Lenovo GIS
2006-11-22

议题 – 电信网络安全的价值

- ❑ 发生了什么事情？
- ❑ 我们要怎样作？
- ❑ 还要考虑什么？



电信业在安全上的探索



The sky isn't falling...

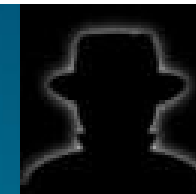
it fell a few years ago...

Roger A. Grimes
Foundstone Ultimate Hacking instructor/consultant
Roger-grimes@infoworld.com

电信业的探索，敢为天下先的精神，许许多多最新的安全产品和技术都是在电信业得到实践

安全服务 ⇒ IDS ⇒ SOC ⇒ AAAA ⇒
桌面安全 ⇒ 行为审计 ⇒ 符合性

SANS Top-20 Internet Security Attack Targets (2006 Annual Update)



Operating Systems

- W1. Internet Explorer
- W2. Windows Libraries
- W3. Microsoft Office
- W4. Windows Services
- W5. Windows Configuration Weaknesses
- M1. Mac OS X
- U1. UNIX Configuration Weaknesses

Security Policy and Personnel

- H1. Excessive User Rights and Unauthorized Devices
- H2. Users (Phishing/Spear Phishing)

Special Section

- Z1. Zero Day Attacks and Prevention Strategies

Cross-Platform Applications

- C1 Web Applications
- C2. Database Software
- C3. P2P File Sharing Applications
- C4 Instant Messaging
- C5. Media Players
- C6. DNS Servers
- C7. Backup Software
- C8. Security, Enterprise, and Directory Management Servers

Network Devices

- N1. VoIP Servers and Phones**
- N2. Network and Other Devices Common Configuration Weaknesses

Security 2.0? Security 1.0 SP2? ...



● 如果我们按照安全历史的发展，做下面的定义：

- 将“安全就是反病毒”定为 安全 Security 0.1，
- 将“安全就是PDR，where P是防火墙、D是IDS、R是安全应急服务”定为安全 Security 1.0

Security 1.0 SP2: ?

● 那么现在我们进入了Security2.0时代

- 关注点从简单的防止攻击和入侵，发展到应用和数据安全，以及内部控制
- 安全体系从“老三样”发展到基于AAAA的综合防御体系，强调安全管理的“内功”
- 安全管理和技术更加强调信息交互、以及相关、挖掘和展现，强调信息的易用性，强调“用户”的感受和使用效果

如何才能提供“端到端”的、“面向客户”的服务产品



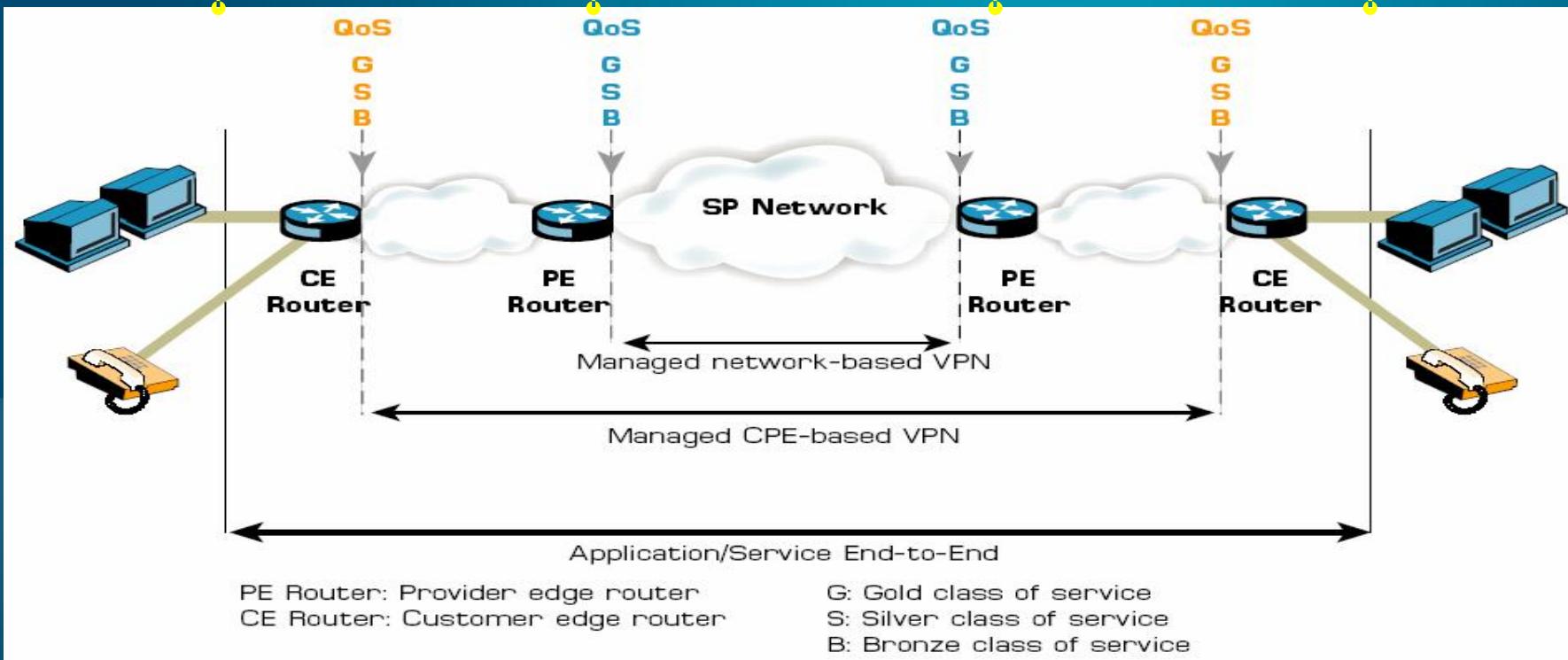
国际领先电信运营商早已先行

- AOL
- ATT
- MCI
- BT
- ...

MSS :: Managed Security Service
PSS :: Professional Security Service

价值链的延伸

当前的电信网络安全边界



电信增值安全服务



【MSS】



管理防病毒服务、管理防火墙服务、管理IDS和IPS服务



WAN防御：即大网上的拒绝服务防御Anti-DDoS



PKI管理服务等



【PSS】



安全风险评估（技术层面发现漏洞和威胁，并分析，推荐解决方案）



安全风险评估（策略和架构方面调研分析，推荐解决方案）



应用生命周期的安全顾问（和顾客一道针对应用开发周期的各个环节进行安全加强）



安全预警服务（帮助监视相关IT系统的安全漏洞和威胁态势，及时发出预警和安全建议）

运营商建设SOC的目的决不应该仅仅限于管理自身的安全设备，而是应该着眼于锤炼自身安全运营能力，时刻准备着走向增值服务。这也是SOC本来和未来最重要的使命！

现代电信运营商要求整合上下游资源，明晰价值链关系

与客户交流互动增加方向



安全作为服务的必经之路



How to Deliver Security As Services ?

- 建设基于ITIL国际最佳实践的流程和指标体系，提高流程成熟度
- 推行SLA/OLA，提高管理活动规范性和透明度
- 提高安全控制和审计能力

HBA 基于主机和应用的审计

- 深入系统、应用和业务
- 不受网络通信协议的影响

NBA 基于网络的审计

- 全面、忠实的操作回放
- 快速低成本部署
- 不容易被篡改和绕过
- 不影响关键应用的性能
- 不会带来兼容风险

- 协议覆盖的全面性，应该可以审计SSH/RDP等加密协议和数据库等
- 部署的灵活性，应该支持分布式部署和集中管理
- 性能和高可用性，应该支持千兆
- 提供灵活的报表和开放数据接口

END & DISCUSSION
