

网络安全服务保障

东软网络安全事业部
席斐 高级咨询顾问 CISP

2005年3月

©2003 Neteye. All rights reserved.
Confidential – Do Not Copy or Distribute



安全服务的重要意义

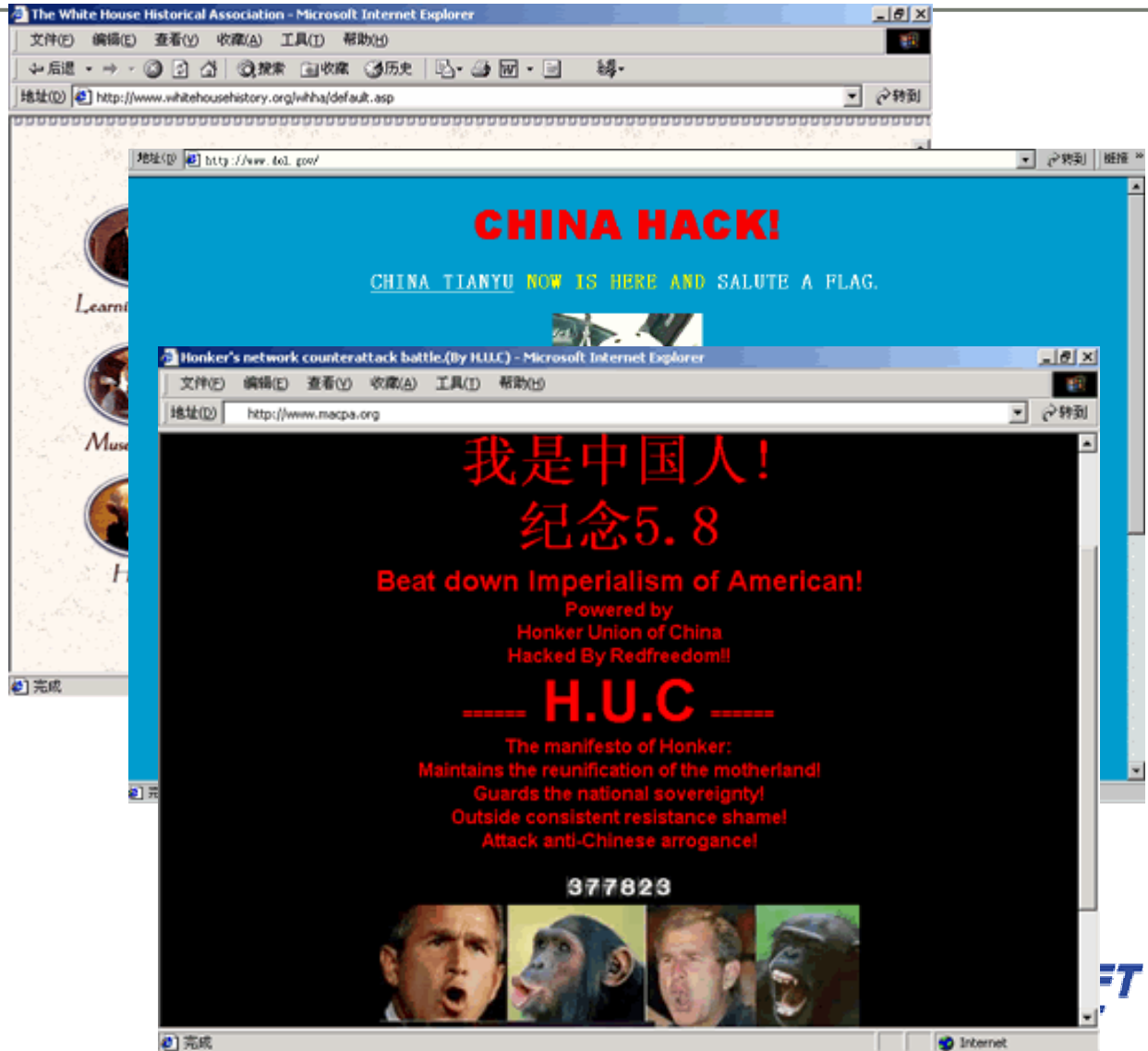
- ▶ 如何使安全产品发挥应有的作用，以及如何评价和验证安全产品的有效性？
- ▶ 安全产品、安全服务、安全管理以及人员教育都是安全体系建设中不可缺一的部分。
- ▶ 安全产品解决不了所有的安全问题。

2001年“中美黑客大战”

白宫历史协会

美国劳工部

美国马里兰州执业会计师协会

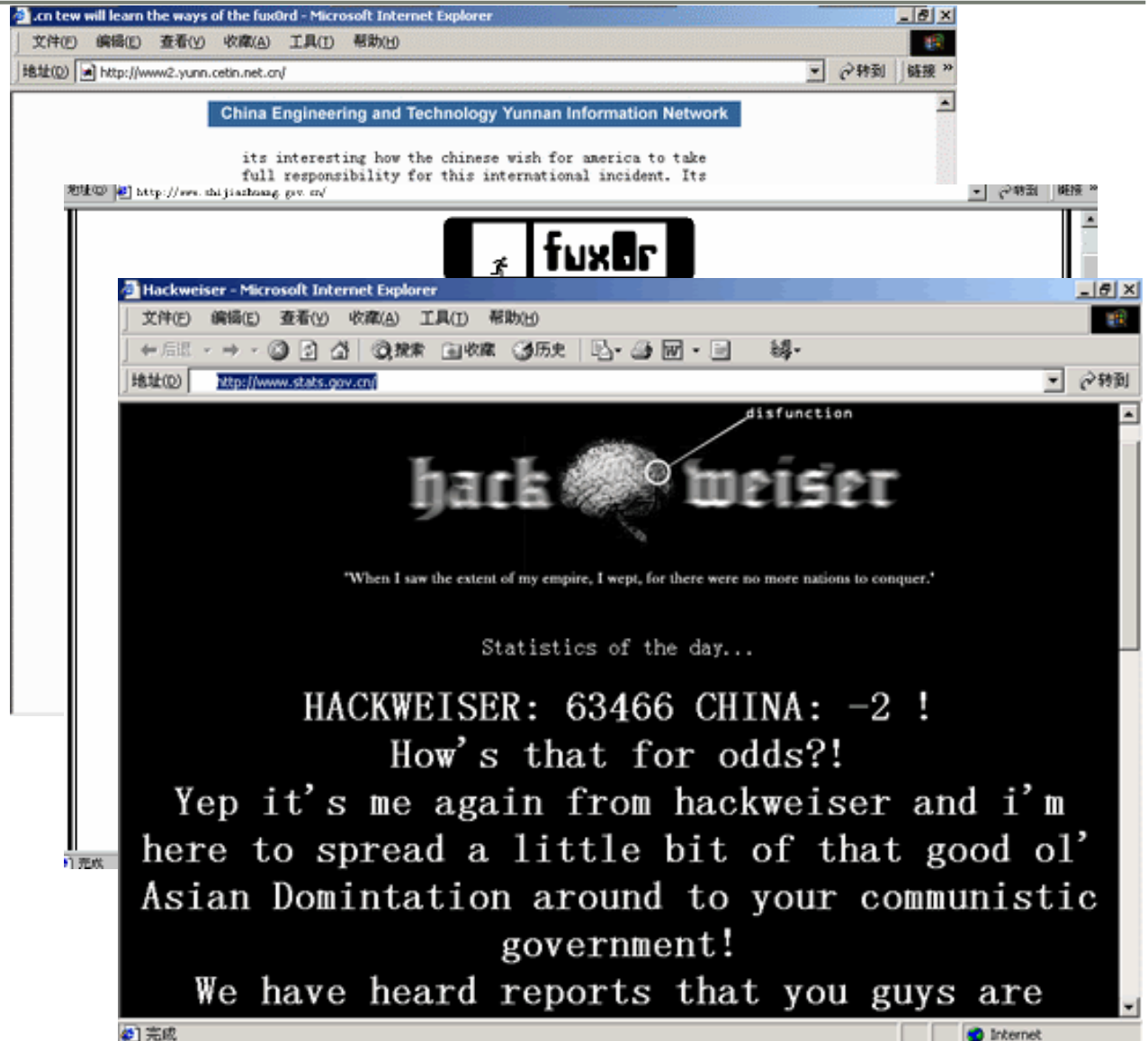


2001年“中美黑客大战”

中国工程技术
云南信息网

石家庄市人民
政府新闻网

中国统计信息网



网络安全服务保障

对安全事件的处理不能只靠事后处理（应急响应），而应该做到预先防御和保障。

6步走原则：

网络安全服务保障

1、借用安全评估服务帮助我们了解自身安全性

安全评估的检查点

- 网络基础环境与结构
- 网络应用系统
 - ◆ 服务器、工作站
 - ◆ 网络设备
 - ◆ 应用服务
 - ◆ 数据库
- 信息资产的分类与控制
- 数据通讯与存储状况
- 组织在信息安全管理方面的政策与制度
- 安全策略实施与应用状况

事件举例

评估服务还可以发现隐蔽的安全事件

××省财政系统案例

网络安全服务保障

2、采用安全加固服务来增强信息系统的自身安全性

什么是安全加固服务？

- 利用多种技术手段对网络信息系统中的操作系统平台和重要的网络设备提供安全加固和配置优化。
- 安全产品只能从表面上隐蔽安全隐患，而安全加固服务则可以从本质上清除安全隐患。
- 购买和部署安全产品从广义上讲也应归属于安全加固服务中的一个应用手段。

安全加固服务内容

- 操作系统安全修补、加固和优化
- 应用服务安全修补、加固和优化
- 网络设备安全修补、加固和优化
- 现有安全制度与策略的改进和完善
 - 1、机房管理 2、办公环境管理 3、主机系统管理
 - 4、数据管理 5、用户管理 6、安全设备管理
 - 7、物理设备管理 8、网络应用管理 9、应用业务系统管理
 - 10、数据库管理

3、部署专用安全系统和设备提升安全保护等级

安全技术及产品

面对企业级的安全保护需求，我们可以借助目前成熟的安全技术和产品来帮助我们提升整体安全保护等级。目前适合企业级的成熟的安全技术和产品有：

- ◆ Firewall防火墙（首选网络版，备选单机版）
- ◆ IDS入侵检测（首选网络版，备选单机版）
- ◆ VPN虚拟专用网（首选IPSEC版，备选SSL版）
- ◆ PKI/CA
- ◆ 防杀病毒（网关型、服务器型、桌面型）
- ◆

网络安全服务保障

4、加强安全教育培训来减少和避免安全事件的发生

安全培训的重要性

在整个安全体系建设中，人是最重要的因素。

安全培训体系

1. 《黑客攻击与防御技术》
2. 《网络应用系统安全》
(网络设备、操作系统、应用服务)
3. 《安全产品技术与应用》
4. 《信息安全管理体制》
5. 《信息安全整体解决方案》

5、引入应急响应服务及时有效的处理重大安全事件

安全应急响应服务的特点

- ▶ 技术复杂性与专业性

各种硬件平台、操作系统、应用软件

- ▶ 知识经验的依赖性

由计算机安全事件应急小组CSIRT（Computer Security Incident Response Team）中的人提供服务，而不是一个硬件或软件产品

- ▶ 突发性和时效性强

- ▶ 需要广泛的协调与合作

东软应急响应服务介绍

作为一个专业的网络安全服务提供商，东软拥有一整套应急响应机制，同时也具备可以处理各种紧急事件的众多安全服务工程师。我们可以为客户处理的紧急事件包括：

- ◆ 大规模病毒爆发
- ◆ 网络入侵事件
- ◆ 拒绝服务攻击
- ◆ 主机或网络异常事件

东软应急响应服务内容

1. 协助恢复系统到正常工作状态
2. 协助检查入侵来源、时间、方法等
3. 对网络进行评估，找出其他网络安全隐患
4. 作出事故分析报告
5. 跟踪用户运营情况

事件举例

××运营商应急处理案例

6、借助安全通告服务对安全威胁提前预警

安全信息通告

- 紧急事件通告
- 业界动态
- 最新技术发展
- 国家安全政策及法律法规

总结

- 1、借用安全评估服务帮助我们了解自身安全性
- 2、采用安全加固服务来增强信息系统的自身安全性
- 3、部署专用安全系统和设备提升安全保护等级
- 4、加强安全教育培训来减少和避免安全事件的发生
- 5、引入应急响应服务及时有效的处理重大安全事件
- 6、采用安全通告服务来对安全威胁提前预警

只有积极主动的建立起一套完备的安全服务保障体系，才能够真正有效的解决安全问题，而不是紧紧依靠事后处理（应急响应）。

NetEye—值得您信赖的品牌！

信赖缔造姻缘
安全成就百年