

再谈网络安全服务

赵 粮

Lenovo GIS
2007-11-23

议题 – 再谈网络安全服务

- ❑ 发生了什么事情？
- ❑ 有什么思路？
- ❑ 如何行动？



网络攻击逐渐转向商业利益

Zero-days are sold online

There are... offering zero-days... even have a... it is... are



This [WM]... special... selling this exploit for \$4,000

— Alexander Gostev, senior virus analyst, Kaspersky Labs

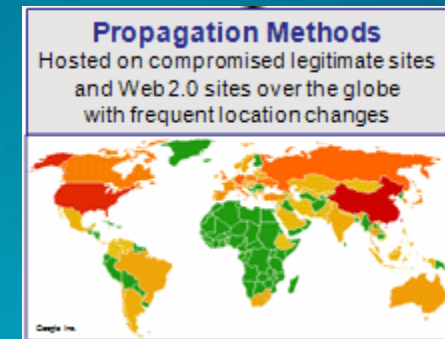
- Windows Vista (-1)-day was available for \$50K before Vista was even released!

<https://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-gutmann.pdf>

利益驱动下的网络地下经济

● 专业人士和Script Kiddies完成的攻击、入侵在工具、复杂性和可检测方面不可同日而语

● 一般商业企业在对付专业攻击和入侵时显得力不从心



Anti-Forensic Methods
Evade signature-based detection by utilizing code obfuscation and controlled exploits visibility in the wild

```
<SCRIPT LANGUAGE="JavaScript">
<!--
xxx=String.fromCharCode(60,79,66,74,69,67,84,32,115,116,121,108,10
61,34,108,111,99,97,116,101,34,32,116,121,112,101,61,34,97,112,11
,99,116,34,32,99,100,97,115,115,105,100,61,34,99,108,115,105,100,
51,55,55,45,48,40,97,97,48,48,51,95,55,97,49,49,34,32,99,111,100,
01,114,115,105,111,110,61,53,44,50,44,51,51,97,48,44,49,49,97,52,
,97,110,100,34,32,118,97,108,117,101,61,34,82,101,108,97,116,101,
82,65,77,32,110,97,109,101,61,34,66,117,116,116,111,110,34,32,118
5,77,32,110,97,109,101,61,34,87,105,110,100,111,119,34,32,118,97,
2,13,10,60,80,65,82,65,77,32,110,97,109,101,61,34,73,116,101,109,
15,45,105,116,115,58,99,58,47,119,105,110,100,111,119,115,47,104,
,97,108,116,95,117,114,108,95,101,110,116,101,114,112,114,105,115
```

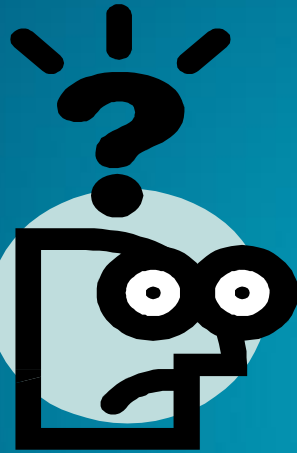
document.write(xxx)

专业人士作案

<http://sbin.cn/blog/2007/11/13/securityethics/>

企业如何获得“安全”？

CISO



Outsourcing

安全产品及服务
安全顾问服务
安全管理服务

预算成本

管理层和企业战略
信息安全使命
KPI / SLA

In sourcing

应用系统开发
数据库和存储
数据中心
服务器
网络和通信
PC和桌面
服务台

我的安全服务观 - 2003

● 《安全服务 - 2003》 - 安全服务的收益

- 节省时间、减小机会成本
- 节省投资、提高产品利用效力和效率
- 提高综合安全水平和应急能力

● 《用专业服务消除隐患》 - 安全风险管理的三个层次

- 快速、大量部署安全产品
- 定期、不定期的风险评估和加固
- 集中统一的安全管理平台

<http://sbin.cn/blog/2003/03/03/professional-security-service/>

我的安全服务观 — 【2004】

Security On-Demand

- Alignment
- Efficient
- Responsive

- 安全是一种服务(业务)
Security is a service
 - 安全与业务紧密对应
Map Security to business
 - 安全像服务一样运行
Run Security as a service
 - 安全“根源分析”
Security Root-cause analysis
- 安全就绪的IT基础架构
Security-ready IT infrastructure
 - 服务知晓的安全
Service-aware security
 - 开放互通集成
- 安全自我管理
Self-managing Security
 - 互操作与自动响应
Auto-response and Interoperability

资产
风险
优先级
流程

可度量
可考核
可管理

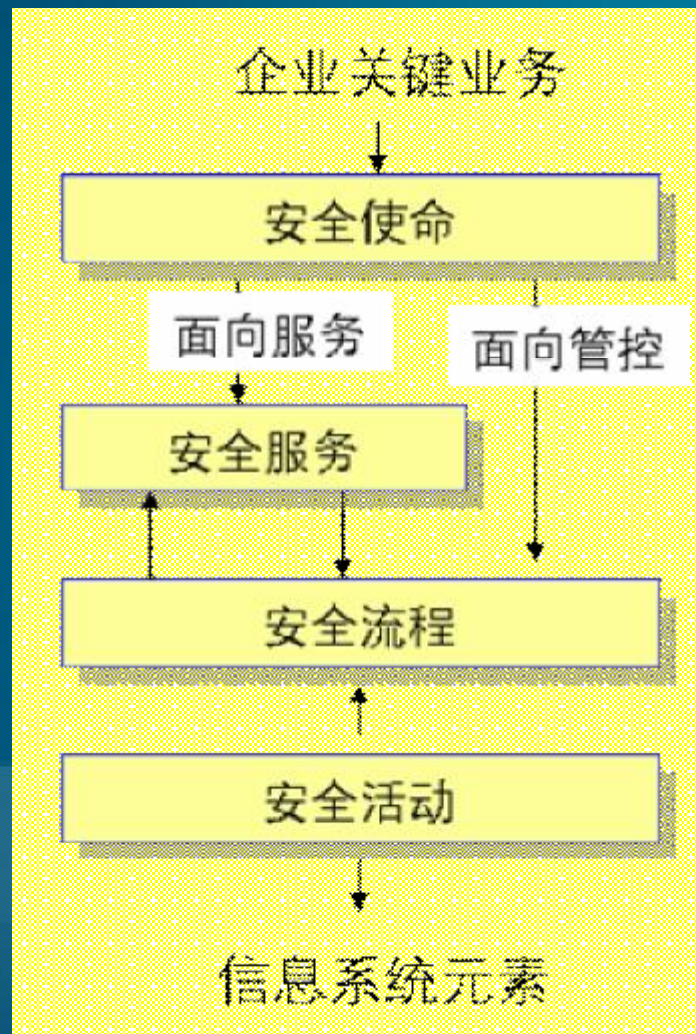
标准化
模块化
集成性

深层防御
面向业务
智能相关

我的安全服务观 — 【2006】



最终用户
其他小组
管理层



企业安全服务是对企业安全管理各种活动的抽象。

企业安全服务概念的提出有利于提高安全管理的成熟度，在实现管控的前提下，提高安全管理的“客户感知”水平，从而推进安全控制措施的效力和效率。

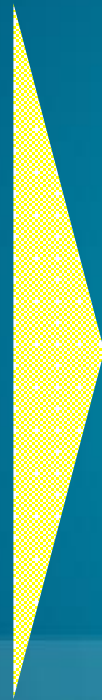
企业“安全服务”是一个过程



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



- 结盟国内外知名、有实力的IT服务厂商和安全设备厂商
- 建设面向客户的IT运行维护平台和安全管理平台
- 建设集中的报表和审计中心
- 拓展设备租赁、代维等服务模式作为增值服务
 - FW/IDS/IPS/UTM/AV 出租和管理
- 建设CERT/SWAT队伍
 - Anti-DoS 和 紧急事件响应服务
 - 预警和补丁服务
 - 教育和培训服务

伙伴共赢



END & DISCUSSION

