彎曲評論

科技 · 人物 · 潮流

关于中国网络安全的讨论与建议

陈怀临, 弯曲评论创办人
huailin@gmail.com
www.valleytalk.org

讨论范围

国外网络安全发展趋势

我国网络安全工业现状

相应的措施建议与讨论

国外网络安全发展趋势

--具备领先的学术研究和政府资金和政策支持

--具备来自世界(包括中国)一流的工业界人才/团队

--具备完整的产品和解决方案

* 高中底端防火墙
* IDS/IDP，Anti-Virus, APT，Zero-Day Detection
* DDoS产品和解决方案

国外网络安全发展趋势(Cont.)

硅谷网络安全产品研发趋势

--云安全(Cloud Security)

--基于云的新一代DDoS产品和方案CloudFlare et. al.

--下一代APT，WAF产品, CryptDB

--主动防火墙防御(Proactive Defense)

--数据泄露安全防御(Data Leak Protection)

--基于大数据日志和报文流量分析的产品和方案

--云和数据中心网络健康和性能监控产品和方案

国外网络安全发展趋势(Cont.)

硅谷网络安全产品研发趋势

--基于软件的虚拟防火墙，解决公有云，私有云和混合云的安全问题

--基于云的DDoS，解决中小型企业的网络安全问题。

--云和数据中心健康和性能监控和管理系统，解决日益增长的企业和政府的数据和服务都在往云中迁移

--BYOD 移动安全产品和解决方案，解决无线终端接入安全

国内网络安全目前总体现状

--国内学术界具备跟踪和仿制能力，缺乏体系级别的的核心创新能力。

--国内工业界具备跟踪和仿制美国产品能力，但短期不具备超越能力。

--国外安全产品基本覆盖金融，通信业，电力等许多国家关键网络领域。

国内网络安全公司目前现状

--缺乏跟踪国外先进技术的资本实力和技术视野

--商业利益，各自在分割的行业市场，生存艰难

--缺乏和不具备完整解决方案的技术，维护能力

--缺乏对国家级电信，金融和政府大网的理解

国内网络安全厂商简介

--DDoS：绿盟

--上网行为管理:深信服

--传统防火墙：天融信

--IDS:启明星辰

--NGFW：山石网络

--APT：瀚海源

--Anti—Virus：安天网络

注:缺乏整体解决方案的能力.

国内网络安全厂商简介(Cont)

--产品同治化，缺乏创造力的产品。特别是高端产品

--行业垄断和竞争，缺乏健康的生态环境

--单点技术，缺乏完整的产品解决方案

--缺乏高端和国际化视野人才

国内网络安全环境分析

--不是国外反华势力侵袭，更多的是国内自己网络环境恶劣。

--缺乏法律(Law)和相关政策(Regulation)

--缺乏技术手段监控和保护

--金融系统，电商，政府和相关行业网络是最弱的环节

目前我国网络安全产品缺陷(Top 10)

云和数据中心的健康安全监控系统

云／数据中心的安全产品和解决方案

基于大数据分析的行为分析产品

APT／Zero Day的研究

数据加密和防泄露技术的研究

BYOD移动安全

面向金融领域的反欺诈和风控产品

新一代DDoS产品

新一代WAF安全

高性能和完备的Ant-Virus产品

对国家网络安全发展的若干建议

建立完善的国家网络安全的监控系统和反应系统，从而确保DDoS攻击，网络中断等事件的及时反应。

建立国家级别的云数据中心，逐步迁移各个独立的，缺乏信息保护能力的重要部门的数据中心到具有容错，泄洪和抗打击能力的国家级别数据中心。并大量保存有战略价值的冷数据。

加强数据分析水平能力。建立国家级数据分析公司或者通过工业界合作，深度的大数据挖掘，在战略层面保障国家网络和更高层面的信息安全

附录: 相关资料和参考文献

网络安全的趋势:From NGFW to NGTP http://www.valleytalk.org/?p=21192

2014最受关注的10大安全公司 http://www.valleytalk.org/?p=23535

2013－2014 DDoS安全报告 http://www.valleytalk.org/?p=26461

最近DDoS对银行攻击的教训 http://www.valleytalk.org/?p=21274

Advanced Persistent Threat(APT) http://en.wikipedia.org/wiki/Advanced_persistent_threat

Zero-Day Attack

http://en.wikipedia.org/wiki/Zero-day_attack