

安全周报

中国信息安全博士网

第五期

二〇一〇年五月三日

weekly.secdactor.com

- 学术会议
- 政府之声
- 病毒播报
- 产业动态
- 技术前沿
- 黑客攻防
- 海外来风

浪潮SSR成为

“中华人民共和国第十一届运动会唯一指定服务器操作系统安全加固系统产品”



浪潮 主机安全的领导厂商

浪潮SSR (Server System Reinforcement) 服务器安全加固系统是基于对信息安全等级保护制度及相关标准的深入理解,以构建安全的计算环境为基础,以强制访问控制为主线,结合当前信息安全产业的发展现状而推出的专门针对服务器操作系统的整体安全解决方案。SSR采用先进的ROST技术理论,在操作系统内核层对服务器操作系统进行加固,同时根据信息安全管理中的“三权分立”原则,实现对用户和进程的最小授权,防止对系统文件和重要数据的误操作,从根本上免疫目前针对操作系统的各类攻击行为,彻底防范病毒、蠕虫、黑客攻击等对操作系统和数据库的破坏。这一独到的服务器系统安全解决方案填补了国内在此领域的长期空白,浪潮信息安全被赞誉为“服务器安全专家”,开辟了信息安全产业发展的新方向。

浪潮SSR产品系列

SSR企业版:企业核心主机操作系统免遭受非法攻击的“智能屏障”

SSR网络版:可信服务器安全运维中心

SSR专用版:为您的主机系统量身订做的“安全胃甲”

主要功能

从根本上免疫针对服务器操作系统的攻击

符合国家信息安全等级化保护三级标准

有效防止内、外网针对服务器系统的攻击

保障业务的连续性、稳定性、安全性及可靠性

有效解决了安全体系中系统层的安全问题

从根本上防范冲击波、震荡波等蠕虫类病毒



inspur 浪潮

中华人民共和国第十一届运动会
IT产品与服务合作伙伴

浪潮信息安全事业部

北京办事处:北京市海淀区阜成路73号裕惠大厦1002室 邮编:100142
电话:010-68451517 (总机) 传真:68451517-6688
成都办事处:成都市一环路南一段22号红瓦大厦930 邮编:610041
电话:028-85243518 传真:028-85214223
杭州办事处:杭州文三路478号华星时代广场A楼1507 邮编:310012
电话:0571-88907770 传真:0571-88907772
南京办事处:南京市中山北路45号华美达怡华酒店7层 邮编:210008
传真:025-83308166
安徽办事处:合肥市长江中路436号金城大厦1301室 邮编:230061

广州办事处:广州市天河区北路898号信源大厦17层 邮编:510898
电话:020-38182808-8208 传真:020-38182825
上海办事处:延安西路129号华侨大厦23楼 邮编:200050
传真:021-62485588-9075
太原办事处:太原市平阳路东巷56号7号楼5单元201室 邮编:030012
济南总部:济南市山大路224号1号楼1层东厅 邮编:250013
技术支持热线:0531-85105399 0531-88932888 (总机) 转5399
售后服务热线:0531-85105398 0531-88932888 (总机) 转5398
E-mail: Security@inspur.com

目录

学术会议.....	4
会议提醒：2010 全球宽带通信及物联网高层论坛将召开.....	4
政府之声.....	4
国家保密局：重要涉密场所不能使用 3G 手机.....	4
国资委：电信运营商招标信息为商业秘密.....	5
全国人大通过保密法 网络运营商应配合泄密调查.....	6
2010 信息安全专项项目申报 4 月 30 日截止.....	6
李东荣：谋划金融业“十二五”信息化发展规划 保障金融信息系统安全.....	9
病毒播报.....	11
本周病毒预报（2010.4.24-2010.4.30）.....	11
谷歌再次修复 Chrome 漏洞.....	11
钓鱼网站借玉树地震大发国难财 谨慎捐款.....	12
卡巴斯基揭示网银大盗“宙斯”木马真相.....	14
产业动态.....	16
RSA 大会上的中国企业家身影.....	16
赛门铁克斥资 3.7 亿美元收购两家安全厂商.....	18
新融合时代 信息产业彰显十大趋势.....	18
方正安全构筑安全长城 长城资产管理方案.....	21
惠普收购 McAfee 传闻再起 被投资者看好.....	22
技术前沿.....	23
同洲电子涉窃密：源代码鉴定成案件关键.....	23
云计算火热背后：标准及安全成首要问题.....	24
企事业单位局域网的信息安全技术分析.....	26
JavaScript 大师：网络开发应更重安全.....	28
ISMS 实施过程常见困惑与应对.....	28
黑客攻防.....	32
世界第一黑客十大建议.....	32
破解 iPhone OS 存在诸多安全隐患.....	33
黑客攻破 iPhone 手机 运行 Android 系统.....	34
国家网络入侵防范中心：上周共有漏洞 73 个.....	35
海外来风.....	35
McAfee Apologizes for Update Mess.....	35

学术会议

会议提醒：2010 全球宽带通信及物联网高层论坛将召开

文章来源：新浪科技

2010 年，随着经济形势的进一步好转和技术创新的推进，全球电信业逐渐复苏，步入了良性发展的轨道。当前，各国纷纷把电信业列为国家战略部署的先导领域，物联网、云计算、通信融合的新业务、新产品不断出现，泛在化、宽带化、融合化、智能化已经成为下一代网络发展的热点，发达国家不断地抢占新技术进行开发，新一轮的发展竞争即将展开。在此背景下，经工业和信息化部批准，工业和信息化部电信研究院将于 2010 年 5 月 6 日，在北京鸿翔大厦举办“2010 全球宽带通信及物联网高层论坛”。

本次论坛，以“宽带推动新兴产业模式”为主题，邀请工信部领导和业内专家、国内主要电信运营商、国内外电信企业代表共同探讨下一代宽带通信网络技术和业务创新、物联网技术与产业链建设等 NGN 发展热点问题。通过此次论坛，我们将更加全面、深入地了解国内外宽带和物联网的发展动态和趋势，为我们准确把握现阶段的技术攻关方向，了解由此带来的新兴产业模式提供了翔实有据的参考。

“2010 全球宽带通信及物联网高层论坛”为原“NGN 在中国全球峰会”的品牌延续性活动，迄今为止已经举办了 6 届。本次论坛将再次搭起技术交流与互动的对话平台，携手业界同仁，共同促进中国电信市场中新兴产业的健康发展。

政府之声

国家保密局：重要涉密场所不能使用 3G 手机

文章来源：cismag.com.cn

在上月的科协联组讨论会上，国家保密局总工程师杜虹博士在列席政协联组会议回答政协委员的提问时表示，相关部委制定了 3G 移动终端使用保密管理的规定，指的是在核心涉密场所和重要涉密场所不能使用 3G 手机，并非所有涉密人员都不能使用，普通人使用不会有影响。

此前，有媒体报道，3G 手机强大的视频传输功能，容易导致在使用过程中，将办公环境中的作战地图、文件或军事设施等涉密信息传输出去，相当于给对方来了个视频直播。3G 手机具有照相、大容量存储功能，如果在工作场所拍照并流传出去，同样会在无意中造成泄密隐患。3G 手机具有随时随地上网功能，也必将给安全保密和管理工作带来更大的难度。此外，3G 手机还安装有操作系统、办公文字编辑等软件，不排除黑客使用木马程序控制手机视频、照相功能的可能性。

针对有政协委员表示对有关 3G 手机保密管理规定不太清楚一事，杜虹博士表示，我国目前的保密形势非常严峻，近年窃密、泄密案件呈高发态势，其中最主要的特点就是体现在泄密、窃密案件的高技术上，由于国家秘密不是写在纸上锁在保险柜里，而是通过声光电等形式传输，因此对 3G 的使用提出了要求，虽然 3G 很多方面跟 2G 差不多，但它有高速视频等特点。去年相关部门对 3G 手机的使用发过通知，指的是在核心涉密场所和重要涉密场所禁用，而并非指的是禁用 3G 手机，不是所有的涉密人员都不能使用 3G 手机。

国资委：电信运营商招标信息为商业秘密

文章来源：通信产业报

4 月 26 日，国务院国有资产监督管理委员会（下称国资委）发布了《中央企业商业秘密保护暂行规定》。该规定强调指出，各中央企业要高度重视商业秘密保护工作，加快研究制订相关实施细则，切实保障企业利益不受侵害，促进企业又好又快发展。

据悉，该规定所称的商业秘密，是指不为公众所知悉、能为中央企业带来经济利益、具有实用性并经中央企业采取保密措施的经营信息和技术信息。商业秘密的保护范围主要包括：商业模式、招投标事项、客户信息、并购重组、产权交易等经营信息；设计、程序、产品配方、制作工艺、制作方法、技术诀窍等技术信息。

中央企业商业秘密的密级，根据泄露会使企业的经济利益遭受损害的程度，确定为核心商业秘密、普通商业秘密两级，密级标注统一为“核心商密”、“普通商密”。

规定强调，中央企业在涉及境内外发行证券、上市及上市公司信息披露过程中，要建立和完善商业秘密保密审查程序，规定相关部门、机构、人员的保密义务。

一位不愿具名的电信专家对记者表示，此规定将为中央企业，“尤其是在各大媒体频繁出现的电信运营商套上紧箍咒”。该专家分析指出，规定中所指称的招投标信息、商业模式、客户信息等，都将对电信运营商今后的管理提出更严格的要求。“TD 四期招标即将开闸，整个通信行业都在热炒。现在出台这样一份文件，无异于给业界泼了一盆冷水，中移动很可能对招标结果秘而不宣。”

不过也有运营商人士表示，公众对于手机实名制的非议主要在于客户信息的安全性能否得到保障。“现在国资委出台文件将客户信息定义为商业秘密，也为手机实名制的顺利出台奠定了基础。”

全国人大通过保密法 网络运营商应配合泄密调查

文章来源：中新网

十一届全国人大常委会第十四次会议 29 日下午在北京闭会。会议表决通过了保守国家秘密法。该法明确了定密权限，并规定机关、单位应当定期审核所确定的国家秘密，对在保密期限内因保密事项范围调整不再作为国家秘密事项，或者公开后不会危害国家安全和利益，不需要继续保密的，应当及时解密。

这部法律对国家秘密的范围和密级、保密制度、监督管理、法律责任等作出了规定，规定法律、行政法规规定公开的事项，应当依法公开。该法明确了国家秘密的保密期限，规定“除另有规定外，绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。”

保守国家秘密法规定，国家秘密的密级分为绝密、机密、秘密三级。在定密权限上，法律规定中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市、自治州一级的机关及其授权的机关、单位可以确定机密级和秘密级国家秘密。具体的定密权限、授权范围由国家保密行政管理部门规定。

根据该法的规定，国家秘密的保密期限已满的，自行解密。对需要延长保密期限的，应当在原保密期限届满前重新确定保密期限。

保密法第二十八条规定，互联网及其他公共信息网络运营商、服务商应当配合公安机关、国家安全机关、检察机关对泄密案件进行调查；发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，应当立即停止传输，保存有关记录，向公安机关、国家安全机关或者保密行政管理部门报告；应当根据公安机关、国家安全机关或者保密行政管理部门的要求，删除涉及泄露国家秘密的信息。

保密法规定，互联网及其他公共信息网络运营商、服务商违反本法第二十八条规定的，由公安机关或者国家安全机关、信息产业主管部门按照各自职责分工依法予以处罚。

2010 信息安全专项项目申报 4 月 30 日截止

文章来源：中国信息安全博士网

由国家发改委组织实施的 2010 年信息安全专项项目申报日期将于今日截止。2010 年 2010 年信息安全专项将主要围绕三个方面展开：一、为国家信息化建设提供支撑的信息安全产品产业化，二、为基础信息网络和重要信息系统安全运行提供技术支持的信息安全专业化服务，三、)面向国家信息安全的安全标准体系及重要信息安全产品的关键标准。

附《国家发展和改革委员会办公厅关于组织实施 2010 年信息安全专项有关事项的通知》。。。。。。教育部、工业和信息化部、公安部、安全部、国家质检总局、中科院、国家密码局、国家保密局办公厅(室)，各省、自治区、直辖市、计划单列市发展改革委：

为了贯彻落实 2006-2020 年国家信息化发展战略和国家信息化“十一五”规划的工作部署，进一步促进我国信息安全产业的发展，提升信息安全专业化服务水平，保障国民经济和社会信息化的健康快速发展，我委决定组织实施 2010 年信息安全专项。现将有关事项通知如下：

一、2010 年信息安全专项重点

专项按照优化产业结构，提高完善产品性能和功能，培育专业化服务，推动标准化建设，扶持骨干重点企业，提升产业竞争力，以及重要信息系统自主可控能力的指导原则，主要围绕以下三个领域展开：

(一)为国家信息化建设提供支撑的信息安全产品产业化

1、重点支持金融、税务、民航、电力、海关、军工和电子政务等领域的专用安全操作系统、专用安全服务器、专用安全数据库、安全中间件、操作系统与数据库安全加固、数据安全存储、容灾备份软件等产品的产业化。

2、重点支持保密移动存储介质管理、安全保密检查与评测、安全审计与追踪、电子数据取证与证据管理、涉密电子文档安全处理与管理软件、防信息泄漏等安全保密类产品的产业化；重点支持网络木马监测与防治、网络反扫描、产品脆弱性扫描分析与风险评估、高速智能化入侵监测、移动和桌面终端与 WEB 服务器安全防护、面向无线网络的安全管理、安全一体化集中管理(SOC)、等级保护综合管理、以及保障云计算安全的安全保护类产品的产业化；重点支持面向数字签名、电子印章等应用安全的数字版权保护类产品的产业化；重点支持视音频监控、网络安全态势分析与预警等监控类安全产品的产业化。

3、重点支持高性能专用安全芯片和专用安全设备、基于自主密码技术的高性能集成应用产品的产业化。重点支持基于国产可信计算芯片的安全应用产品，基于电子身份证的网络身份认证产品的产业化；重点支持安全的 RFID 应用产品以及面向 RFID 的安全产品的产业化。

(二)为基础信息网络和重要信息系统安全运行提供技术支持的信息安全专业化服务

1、重点支持基于介质的数据恢复服务、关键数据的容灾备份服务、网络安全应急支援服务、信息系统安全监控系统的托管服务、基于云计算的安全服务。

2、重点支持信息安全风险评估与咨询服务、信息安全漏洞补丁与咨询服务、无线数据终端的安全检测服务、网络服务软件在线运行适用性及安全性评测服务、RFID 类产品和系统安全性检测服务、密码技术产品测试服务。

3、重点支持面向信息系统的等级保护安全方案设计咨询服务、专用信息系统安全可控性仿真与验证服务。

(三)面向国家信息安全的安全标准体系及重要信息安全产品的关键标准

重点支持信息安全相关标准的制订, 以及验证环境的建设及应用, 主要包括: 终端安全配置、安全审计与取证鉴定、互联网应用服务安全检测、涉密信息系统防护、网络安全风险评估与应急响应、密码算法及其产品检测等安全保护类标准; 安全监控与数据采集、数据灾备、统一威胁管理(UTM)、可信计算产品等安全设备类标准; 安全漏洞与恶意代码、安全服务资质、安全等级保护等安全管理类标准; 网络安全接入、身份管理等安全认证类标准; 面向家庭信息终端、云计算、物联网、三网融合、下一代互联网、工业控制系统等新技术应用安全架构类标准。

二、申报要求

(一)请项目主管部门根据投资体制改革精神和《国家高技术产业发展项目管理暂行办法》的有关规定, 结合本单位、本地区实际情况, 认真做好项目组织和备案工作, 组织编写项目资金申请报告并协调落实项目建设资金、环保等相关建设条件, 同时汇总相关申请材料并报我委。

(二)项目主管部门应对报送的材料(如资金申请报告、银行贷款承诺、自有资金证明、销售许可证明等)进行认真核实, 并负责对其真实性予以确认。

(三)为加强项目管理工作, 本次专项项目采取纸质材料申报和网上申报并行的组织实施方式。请项目主管部门在报送项目纸质申报材料前, 先登录国家发展改革委高技术产业发展项目管理系统 <http://ndrc.jhgl.org/xxhc>, 履行相关网上申报手续, 纸质申报材料的具体报送地点将在网上申报系统首页另行通知。

项目纸质申报材料包括: 项目资金申请报告(达到可行性研究报告深度)、项目简表和项目汇总表, 上述材料一式三份。项目所需备案文件和自有资金情况、投资及信贷承诺等证明资料须提交原件并单独装订。纸质材料和网上申报的项目信息原则上应保持一致(涉密及不宜通过网上申报的项目材料, 可在纸质报件中予以补充), 未履行网上申报手续的项目将不予受理。

(四)信息安全产品产业化类项目的承担单位原则上应为企业法人。申报项目应具备以下条件: (1)按规定在当地政府备案; (2)已落实项目建设资金; (3)采用的科技成果应具有我国自主知识产权, 知识产权归属明晰; (4)项目申报单位必须具有较强的技术开发和项目实施能力, 具备较好的资信等级, 资产负债率在合理范围内; (5)申报产业化的产品应具有公安部门出具的销售许可证明, 如是密码类的产品应具有国家密码局出具的销售许可证明。资金申请报告的具体编制要求请详见附件一。

(五)信息安全服务类项目的承担单位可为企业法人或事业法人。申报项目应具备以下条件: (1)按规定在当地政府备案; (2)已落实项目建设资金; (3)具有较强的技术开发和项目实施能力, 具备较好的资信等级, 资产负债率在合理范围内。资金申请报告具体编制要求请详见附件二。

(六)信息安全标准类项目的承担单位可为企业法人或事业法人。申报的项目应属于国家信息安全标准化“十一五”规划的重点领域, 并已列入国家信息安全标准制修订计划。资金申请报告具体编制要求请详见附件三。

(七)2010 年信息安全专项项目申报日期截止至 2010 年 4 月 30 日, 在经我委组织专家对申报项目进行初选后, 将于 2010 年 5 月中旬组织现场答辩。具体项目答辩名单、答辩时间和地点, 将在专

家初选后另行通知。

李东荣：谋划金融业“十二五”信息化发展规划 保障金融信息系统安全

文章来源：中国信息化

第六届银行业科技工作座谈会最近在广东省中山市召开，中国人民银行党委委员、行长助理李东荣出席会议并致辞。会议回顾了“十一五”金融业信息化建设成果，并对“十二五”信息化发展战略进行了展望。

李东荣表示，金融业信息化为我国金融业平稳安全运营提供了良好的支撑环境，应充分总结金融业“十一五”信息化建设的成就和问题，深入分析金融业信息化建设的经验和教训，积极谋划金融业“十二五”信息化发展规划，全面推进金融业信息化建设，力争金融业信息化工作走在其他行业前列。

新挑战，新机遇建国 60 年来，我国金融业信息化建设的主要成就，体现在以下几个方面——首先是金融信息化技术框架已经建立，信息化的基础设施日趋完善。我国的金融业已经拥有了世界先进的大型计算机、小型计算机、PC 服务器、刀片服务器等各类计算机，开发了大量的金融信息和业务处理系统，形成了比较完整的金融信息基础设施体系。

其次，金融行业数据集中工程基本完成，以国有商业银行为代表的各金融机构实现了业务数据的集中处理，统一规范业务操作规程，重新设计了营运工程，建立了集中式的数据中心，有效提高了数据的处理能力和整体可靠性。为下一步实现经营节约化、管理信息化、决策职能化奠定了基础。

第三，金融核心业务系统成功投产，部分商业银行研制开发了涵盖全行业的处理、经营处理、决策分析和渠道的全功能银行业务系统。部分保险公司陆续启动了财务系统、保险数据系统、保险数据仓库集中的 IT 运行平台和网络安全项目，大大提高了信息系统的整体整合应用能力，为业务发展提供了有力的支撑。

近年来，我国金融业信息化工作经历汶川地震、奥运安保、国际金融危机、国庆 60 周年等重大考验，抗风险能力不断提高，金融信息基础设施正常运转，重要业务系统安全稳定运行，各项金融业务有序开展，为促进我国经济平稳运行发挥了重要作用。

李东荣强调，金融业信息化建设还面临着一些挑战：一是金融业信息化的安全生产能力需再上一个台阶，金融业标准化工作亟需加快推进；二是科技创新有待加强，自主知识产权的软硬件在行业中的利用率、核心竞争力建设等需进一步发展；三是金融业信息化对金融服务、金融调控和金融

监管的支持力度需继续得到改善，金融信息共享需继续推进。

完善金融信息化标准体系 2008 年以来，美国的次贷危机席卷全球，金融系统的风险控制和监管被提到了前所未有的高度。如何利用信息技术的优势加强金融机构的内部风险控制，提高金融监管和服务水平，防范和化解金融风险，促进金融的改革和创新，从而推动我国经济社会的发展，是当前我国金融业信息化建设面临的重大课题。

温家宝总理在 2007 年全国质量工作会议上提出，要及时的跟踪和掌握国外先进标准情况，加快完善国家标准，主要的指标要符合国际标准，要加大金融标准化的工作力度，完善我国金融标准化体系。

我国金融标准化工作近年来得到不断发展与完善，现已基本形成具有中国特色的金融标准化体系。1992 年我国金融业成立了全国金融标准化技术委员会，1996 年人民银行与环球银行金融电信协会，就加强双方在报文信息格式方面的合作签署了协议。1999 年建成了全国的金融认证中心，截止到 2008 年年底，共制定发布 32 项金融国家标准和 58 项金融行业标准。同时，金融业的国际标准采标工作取得了很大工作，修订计划发布了 26 项涉及金融业务的报文、信息安全、金融交易卡等领域的国际标准。

“十二五”期间金融工作将加大金融标准化的工作力度，谁掌握了行业标准，谁就能掌握先机。标准化已成为国际市场竞争的重要工具，标准是否坚定已经成为决定胜负的重要因素，目前我国金融业正逐步进入国际竞争的大环境，提高信息化标准化手段来参与竞争能力，是促进国内金融业健康发展的当务之急。

重视金融信息安全保障我国目前已初步建立起银行的信息安全管理机制，出台了密码体系、电子认证等规范制度，建立健全应急处置和风险防范机制。各大银行正陆续建立灾难备份中心，其中有 13 家全国性的银行已经建成了同城的灾难备份中心。9 家银行已经建成了异地的灾难备份中心，上海证券交易所分别对交易系统在同城和异地建立了实时的灾难备份系统。

“十二五”金融工作必然会考虑到金融信息系统安全问题。现代金融业高度依赖信息技术，信息的安全性、可靠性和有效性直接关系到整个金融业的安全，李东荣指出要高度重视金融信息安全工作，特别是网络安全、网民安全、银行卡安全，各级银行要充分认识到金融信息的安全对整体业务和金融体系，乃至经济体系的影响，要牢固的树立风险防范意识，强调成本可控，把信息科技作为风险管理的重要手段。在借鉴国外先进技术和经验的同时，要按照科学发展观的要求，加强我国金融信息自主知识产权的开发和金融科技队伍的培养。

病毒播报

本周病毒预报（2010.4.24-2010.4.30）

文章来源：Antivirus-china

国家计算机病毒应急处理中心通过对互联网的监测发现，近期出现一种新型恶意木马程序 Trojan_NetsFlt.A。该恶意木马程序通过网页挂马方式进行传播，可以修改受感染操作系统的浏览器 IE 主页，将主页设置为指定的 Web 网站地址。

该木马运行后，会将受感染操作系统浏览器 IE 主页篡改为指定的 Web 网址，并阻止操作系统中防病毒软件的正常升级，使其无法运行。一旦计算机用户找到并手工删除该恶意木马程序释放出来的病毒文件，则会导致操作系统无法正常与互联网络连接。

该恶意木马程序试图通过修改受感染操作系统浏览器 IE 默认首页的方式，提高一些 Web 网站的点击流量，从中谋取非法的经济利益。同时，该木马程序还会通过安装驱动程序来拦截网络数据，使系统中的防病毒软件无法正常进行升级。

另外，该木马程序还迫使受感染操作系统主动连接互联网络中指定的服务器站点，从该 Web 服务器站点接收远程的控制命令，以便对木马程序进行版本的更新或是提高某些广告 Web 网站的点击率等更多的远程操作。

专家提醒：

针对该恶意木马程序，国家计算机病毒应急处理中心建议广大计算机用户采取如下防范措施：

（一）针对已经感染该木马程序的计算机用户，我们建议立即升级系统中的防病毒软件，进行全面杀毒。

（二）针对未感染该木马程序的计算机用户，我们建议打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御，这样可以第一时间监控未知病毒的入侵活动，达到全方位保护计算机系统安全的目的。

谷歌再次修复 Chrome 漏洞

文章来源：赛迪网

据报道，谷歌本周初修复了 Windows 版 Chrome 浏览器的三个安全漏洞。这是谷歌在 4 月份第二次修复 Chrome 浏览器的安全漏洞。

谷歌本周二发布的 Chrome 4.1.249.1064 补丁修复了三个“高”等级的安全漏洞。这是谷歌四级系统中第二严重的安全漏洞。丹麦安全漏洞跟踪公司 Secunia 按照自己的严重等级评级系统把这些安全漏洞列为“非常严重”的安全漏洞。

按照谷歌的做法，安全漏洞的技术细节是不公开的。谷歌采取这种策略是为了防止攻击者在大多数用户没有使用新的补丁之前了解到技术细节。

据研究人员称，报告谷歌修复的两个安全漏洞的安全研究人员获得了谷歌举报安全漏洞奖励计划的奖励。谷歌的这个计划是在今年 1 月推出的。大多数发现安全漏洞的人都获得了 500 美元奖金，但是，安全研究人员 Jordi Chancel 在 Chrome 处理谷歌 URL 方式中发现的跨域绕过安全漏洞获得了 1000 美元奖金。

谷歌这次发布补丁是不到两个星期的时间里第二次为 Chrome 浏览器发布补丁。谷歌在 4 月 20 日还修复了 Windows 版 Chrome 浏览器中的 7 个安全漏洞，其中 4 个安全漏洞的是“高”等级的，3 个安全漏洞是“中等”等级的。这些安全漏洞多数都是谷歌内部安全工程师发现的。但是，谷歌为报告安全漏洞的两位外部研究人员每人发给了 500 美元奖金。

据网络测量公司 NetApplications 最近发布的数据显示，谷歌 Chrome 是全球第三流行的浏览器，占浏览器市场份额的大约 6%。

钓鱼网站借玉树地震大发国难财 谨慎捐款

文章来源：赛迪网

2010 年 4 月 24 日，360 安全中心今日再度发出钓鱼网站安全警示：近期不法分子以玉树赈灾捐款的名义制作了大量钓鱼网站，利用网友爱心大肆诈骗。目前遭仿冒的主要是中华慈善总会、中国红十字基金会等官方网站。360 安全专家石晓虹博士为此提醒广大网民，在网上用网银、第三方支付工具等在线方式捐款一定要慎重，并尽量使用 360 网盾等有效的反钓鱼软件进行自动识别各种钓鱼网站。

360 安全专家石晓虹博士介绍说，捐款类钓鱼网站模仿大家耳熟能详的慈善网站，从网页制作来看，甚至能做到以假乱真，网友从肉眼上很难分辨。但只要保持警惕，还是可以发现一些蛛丝马迹。“比如下面这个利用中国红十字名义捐款的钓鱼网站，其他页面都与百度有啊的捐款页面一模一样，只有域名和捐款账号不同。网友捐款前，一定要仔细核查汇款账号，如果发现开户名是个人而非该慈善机构的单位账号，就应该多留个心眼了。”



图片一：仿冒中国红十字总会的捐款页面，不法分子将捐款账户变成个人账户号

据悉，钓鱼网站除了在论坛、网站、QQ群等给自己打广告之外，还利用“自问自答”的方式推广自己的钓鱼网站。“不法分子现在都成了网络营销高手，他们经常在一些分类信息网站、贴吧、问问等问答网站自己发帖、自己回答，并利用SEO（搜索引擎优化）将这些‘自问自答’顶到搜索结果展示页的前几页。网友不仅很容易搜到，而且十分信赖这类网站的推荐。”360安全专家石晓虹博士说，“在这种情况下，一般网友往往会丧失警惕，所以最简单省心，也是最可靠的方式便是凭借安全软件判断网站是否为钓鱼、欺诈网站，以防上当受骗。”



图片二：钓鱼网站 jk.ez.to 做“自问自答”传播



图片三：360 安全浏览器拦截钓鱼网站

据悉，中国反钓鱼网站联盟近日也发表公告称，联盟已接到多起网民对相关钓鱼网站的投诉。为此，360 安全专家石晓虹博士提醒广大网友，网友可以下载使用 360 安全卫士 7.0 版，其附带的 360 网盾能智能识别、拦截钓鱼、挂马等各类恶意网页；对于那些安全性未知但又不得不浏览的网站，建议用户使用 360 安全浏览器的“隔离模式”，就能放心浏览任意带毒、带木马网页都不会中招。

附：部分利用玉树赈灾诈骗的钓鱼网站

hxxp://cctv-t2.com/jk/index.htm 仿冒中国红十字基金会

hxxp://jk.ez.to 仿冒中国红十字基金会

hxxp://www.688tx.com/ 假冒中华慈善总会

安全小贴士：所谓“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的 URL 地址以及页面内容，或者直接以虚假信息为诱饵，以此来诱使用户输入银行账号信息或直接从汇款方式骗取用户钱财。

卡巴斯基揭示网银大盗“宙斯”木马真相

文章来源：IT168

近日，著名安全厂商卡巴斯基实验室发表了一篇技术分析文章，详细分析了一种名为“宙斯”(Zeus)的木马所引发的互联网疫情。宙斯木马是一种传染性非常强的恶意软件，在全球各地的计算机上都能够看到它的身影。由于 Zeus 木马易于传播，并且能够非常方便地窃取受感染用户的在线数据，尤其是网上银行帐户等信息，这使得 Zeus 木马成为互联网黑市上销售量最高的间谍软件之一。

宙斯木马最早出现于 2007 年,经过多年的发展,已经变得非常强大,它使用简单,且易于盗取在线数据,因此成为了很多网络犯罪分子进行网络犯罪的首选恶意软件。那么此恶意软件具体有何等强大之处呢?我们简要总结如下:

重大危害:

计算机上记录的所有信息都可以被宙斯木马窃取(例如当你选择记住密码时),这些信息包括账号、密码以及其它各种用户在网上键入的信息。

即使用户未选择让计算机自动记住相关信息,木马还会通过记录用户的击键以及输入顺序的方式来获取用户的在线账户信息,并将窃取到的信息发送到僵尸网络控制中心。

为了阻止键盘输入信息被监视,很多网站都采用了特殊的软键盘输入技术。但是,宙斯木马却能够在用户点击鼠标的时候截取屏幕,从而截获用户输入的信息。

宙斯木马能够控制所有通过浏览器传输的数据,如果你试图打开一个已经被宙斯木马控制的网站,木马很可能会在用户看到网页内容之前修改网页代码。修改后,网页上会新出现一个字段,要求用户输入一些个人信息。例如,当用户在访问网上银行网站时,要求用户输入用户名和密码或 PIN 码,由于确信此网站确实是正规的银行网站,用户会毫不犹豫地输入相关个人信息。但是,正规的网站不会向用户索取此类绝密信息,就这样,网络罪犯通过宙斯木马窃取到用户的网银账号。

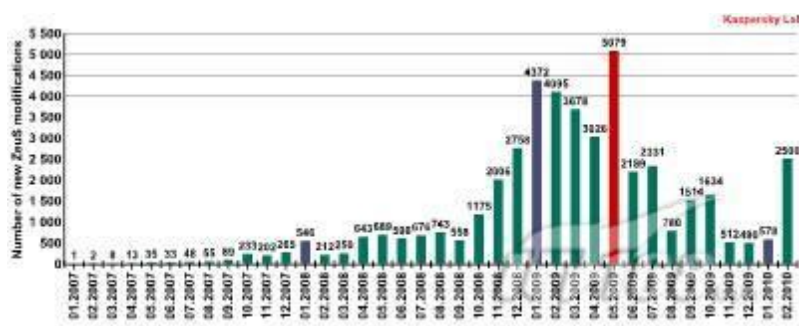
用户在某些网站注册时,会生成一种特殊的电子签名,用户每次访问该网站时都需要验证此签名。如果你的浏览器中不包含此签名,则无法访问网站的全部功能。如果计算机被宙斯木马所感染,木马会自动查找此类签名,将其发送给黑客。

如果黑客想要利用受感染计算机从事其他非法网络活动(例如发送垃圾邮件),可以利用宙斯木马远程安装各类所需的软件。

也就是说,即使用户的计算机目前没有什么值得黑客窃取的数据,网络罪犯也不会轻易放过用户,他们还很可能会利用用户的计算机从事其他网络犯罪活动。受感染的计算机会组成僵尸网络,统一受网络罪犯的控制。普通用户很可能感染此木马几个月,也毫不知情。

定制性强,感染量大

由于宙斯木马能够有效收集个人数据,组成僵尸网络,所以能够被用于多种网络不法行为。几乎所有从事网络犯罪的人都试图获取此木马。此外,对此木马进行定制,适应不同人的需求也并不复杂。网络罪犯还可以轻易将其加密,阻止反病毒软件的检测。网络罪犯甚至可以在购买此木马时,选择定下图是 2007 年至 2010 年 2 月不同月份新出现的宙斯木马新变种数量:



2009 年，美国发表了一篇报告称仅美国就发现有超过 360 万台计算机感染宙斯木马。这还仅仅是一个大概数据，事实上数量应该会更大。而且，确切统计受感染计算机数量也非常困难，因为就算很多家用计算机用户感染了此木马，也浑然不知。最近被检测到的宙斯木马组成的大型僵尸网络名为 Kneber，位于美国，于 2010 年 2 月被确认。经研究发现，此僵尸网络控制的计算机遍布 196 个国家 2,500 个不同组织，总计算机数量大约为 76,000 台。当然，这也仅仅是冰山的一角，还有大量已感染计算机未被确认。这使得此木马在黑市中非常抢手。

产业动态

RSA 大会上的中国企业家身影

文章来源：信息安全与通信保密 作者：穆瑛

2010 年 3 月，美国旧金山。在安全保密业界备受全球瞩目的 RSA 大会上，我们惊喜地看到了中国企业家的身影，这是他们首次联合在 RSA 大会上高调亮相。这种全球视野中的集体出场，本身就意味着一种思想上的开放。全球化在以前意味着某大国化，但现在更多的是指对地球上任何的人、产品和思想的包容与接收。全球化意味着联系性和流动性，从国家、计算机到网络、SNS 或者能源、金融、医疗等行业，都有可能会联系到一起。未来，诸如无线射频识别、全球定位系统等技术的广泛应用，将加速这一趋势更快发展。联系性和流动性越强，透明度和风险性都会增加。

虚拟世界中全球化技术发展的趋势正是“云计算”的来临。

今年的 RSA 大会，作为大会嘉宾，亚瑟·科维洛先生在开幕主题演讲中，鼓励安全界同仁迎接不断壮大的虚拟基础架构带来的挑战和机遇，采取更广阔的安全视野，聚集“云计算”带来的 IT 变革。……他指出，有些事情阻碍了“云”这一愿景的实现，简单地说，那就是“云安全”。2010 年 3

月，RSA 大会再次浓墨重彩了当下几乎时时、处处都在关注的“云计算”和“云安全”。

为期 5 天的 RSA 大会，业界探讨着未来安全保密的发展趋势及应对。可以说，注册参会的两万多人，几乎都是全球安全保密业界的精英。来自全世界顶尖的专家、学者还有企业家，不远万里，赶赴到旧金山，他们在这里交流、对话，碰撞智慧的火花。

这一次，我们看到了中国企业家的身影，他们首次在 RSA 大会上集体高调亮相，搭建展台，亮出了“中国观点”（详见我刊本期报道）。除了 2009 年，往届的 RSA 大会上，几乎看不到一位中国知名企业家的相关报道。而此次他们用一种集体的形式出现在了旧金山 RSA 大会。

如果我们越来越依赖于科技应用，——英国首相戈登·布朗于 3 月 22 日宣布，英国将为每名公民开设个人专属网页，在未来 4 年内建成无纸化社会。科技的应用将极大影响未来和历史此乃大势所趋，——那么我们对科技的方方面面都必须关注和了解，同时，对自己能够驾驭科技的能力要有清醒的认识和准确的判断。

所谓清醒和准确。从“金砖四国”到 G2 峰会，从“世界工厂”到“Made with China”，30 多年来，中国抓住了“全球化”的机会，回到了世界中心，置身在全球热议的“中国崛起”之声中。达沃斯会议上“中国热”；“我们有生之年将遇到的头等大事就是中国的崛起”之类的溢美之词何其多乎；美国前任财长保尔森惊人之语：“中国等新兴市场国家的高储蓄率造成全球经济失衡，导致金融危机。”；美国财长盖特纳指责中国正在“操纵”人民币汇率……无论是敬畏还是责难，无论是喜欢还是疑问，都在导引出一个事实：全世界都在谈论中国，全世界都想读懂中国，全世界都在了解中国。而中国，如何“不以物喜、不以己悲”，在清醒认识自己，修炼内功的同时，真实展现开放、坦荡的自己？

想到了 2009 年年底，王石在哥本哈根参加全球气候会议时，代表 200 多名中国企业家宣读了《中国企业界哥本哈根宣言》，他在微博上如是写道：“人生是大舞台，每个人都在表演，同职业演员不同的是，我们表演的只是我们自己……中国企业家承担环保责任，责任亦是机会，担当越大，机会就会越多。”在应对全球气候变化的战争中，离不开中国企业界的参与。

同样，无论是信息化进程还是产业化进程，都离不开 IT 技术的支持。“云计算”即将带来的 IT 变革——融合（2009 年 RSA 大会主题思想），其中极为迫切需要解决的“云安全”（2010 年 RSA 大会主题思想），更离不开中国企业家的参与。

未来学家奈斯比特因《大趋势》闻名于世。25 年前，他的《大趋势》让我们从另一个全新角度看世界。25 年后，他的《中国大趋势》让我们从世界的角度看中国。

就像水无定型，河岸可以壮丽开阔，也可以污秽拥塞一样，一切都在于人的内心，是万里无云楚天阔，还是死水微澜泛青苔。身处世界热议“中国崛起”的中心，让我们对现在心存宽广，对未知充满敬意，以开放的心态，坦荡的胸襟，更平和更无畏地迎接未来。

赛门铁克斥资 3.7 亿美元收购两家安全厂商

文章来源：新浪科技

今日早间消息，据报道，安全厂商赛门铁克昨日宣布，将分别斥资 3 亿和 7000 万美元收购加密服务提供商 PGP 和终端安全服务厂商 GuardianEdge Technologies。

这两起交易仍有待监管机构的批准，预计将于 6 月完成收购。被收购的两家均为私有公司。赛门铁克表示，这两家公司掌握着电子邮件、文件系统、可移除媒体和智能手机等领域的标准加密技术，将对赛门铁克现有的安全服务提供有力补充。赛门铁克目前提供了网关、终端安全和数据防丢失软件等，对数据进行加密能提供更高级别的安全保护，能更有力地应对数据丢失或是遭窃等情况。

赛门铁克称，将在 PGP 的核心管理平台上对自己现有产品进行标准化，使管理员能集中管理加密任务。同时，PGP 的核心管理平台将整合至赛门铁克保护中心，该保护中心可对赛门铁克旗下所有产品进行集中管理。

GuardianEdge 此前就与赛门铁克展开过业务合作，该公司主要为笔记本、便携式存储设备和智能手机提供安全解决方案。赛门铁克称 GuardianEdge 在政府市场上表现不俗。

收购完成后，PGP 和 GuardianEdge 将并入赛门铁克企业安全集团，由资深副总裁弗朗西斯·德苏扎(Francis deSouza)管理。

新融合时代 信息产业彰显十大趋势

文章来源：中国计算机报

随着计算机和互联网的普及应用，中国信息产业步入发展的快车道。IT、电信、互联网和消费电子产业趋于融合，进入信息产业发展的新融合时代，2010 年中国信息产业发展将呈现以下十大趋势：

一、移动互联网产业用户增长与应用发展齐头并进

随着 3G 网络建设的日益完善以及投资的持续注入，2010 年中国市场移动互联网行业高速增长，根据计世资讯预测，到 2010 年底中国移动互联网用户将达到 2.5 亿。

移动互联网用户活跃度将有较大提升，随着各种应用服务的日渐完善以及基础网络的稳定，用户将对工具性(如移动搜索、手机浏览器)、娱乐性(如手机游戏、手机阅读)的应用服务的使用形成习惯，活跃度大大提升，较高用户粘性的应用业务将为移动互联网盈利模式的展开奠定用户基础。

二、电子商务产业进入深入应用时代

计世资讯数据显示,截止到 2009 年底,国内使用第三方电子商务平台的中小企业用户规模已经突破 1000 万,而中国电子商务用户规模已经突破了 1 亿人。

2010 年,电子商务服务获奖深入覆盖商业经济各个方面:不管是国民经济的制造业领域,还是服务业的流通领域;无论企业应用、个人应用,还是政府采购;无论内贸服务,还是跨国外贸服务;无论是基于联网的电子商务,还是基于移动互联网的电子商务都将呈现高速发展的趋势。

三、中国云计算服务进入蓄势待发阶段

计世资讯数据显示,2009 年中国云计算服务市场将达到 381.5 亿元,与 2008 年相比增长 36.4%。2010 年以前中国的云计算服务市场仍处于市场引入阶段,无论是市场供给的成熟性、丰富性,还是市场需求方的认可程度都处于发展的初期。

而随着云计算各种服务模式的不断丰富和发展,以及宏观经济形势的逐步好转的正面影响下,预计到 2011 年左右云计算市场将进入成长阶段,中国云计算服务市场将呈现加速发展的势头,到 2012 年预计中国整体云计算服务市场规模将达到 750 亿元。云计算在中国市场有着巨大的发展潜力。云模式为企业提供了一种获得 IT 和使用 IT 的更经济的方法,尤其是在经济衰退的情况下。这对中小企业来说非常重要。

四、中国软件运营服务(SaaS)产业链趋于成熟

根据计世资讯数据,到 2011 年,中国软件运营服务产业规模将达到 283 亿元,未来五年的复合增长率达到 33%。管理型软件运营服务产业的增长将非常迅速,未来五年的复合增长高达 83%,2011 年的产业规模将达到 28 亿元,市场发展潜力巨大。

虽然管理型软件运营服务则刚刚开始,但管理型软件运营服务已吸引了国内众多公司的参与。目前主要有五类角色。第一类角色是以中国电信、中国网通、中国移动和中国联通为代表的电信运营商,例如中国电信推出了商务领航业务;第二类角色是以用友、金蝶、金算盘、SAP、Oracle 等为代表的软件提供商,例如用友、金蝶组建了专门的在线事业部,SAP 和 Oracle 也推出了专门的 CRM 服务;第三类是新出现的软件运营商,例如 Salesforce、800CRM、Xtools 等公司;第四类是 IT 服务提供商,例如神州数码专门成立了在线公司来提供软件运营服务;第五类是平台软件提供商,例如微软专门推出了 Live 战略。整个软件运营服务(SaaS)产业链呈现百花齐放的发展趋势。

五、绿色 IT 与节能降耗成为产业发展共识

在全球能源资源日益紧张、气候环境日趋恶化,经济衰退不断加剧的今天,绿色 IT 已经成为传统企业和 IT 企业的共同选择。由于 IT 在成为信息化社会中最重要组成部分的同时,对能源的消耗、环境的压力也不断增加。加之金融危机的深度影响,作为当前中国 IT 产业发展的一股明确趋势,绿色 IT 受到业界高度重视。

企业经营虽然是以利润最大化为前提,但是不能不负责任,不能够不考虑到可持续发展和地球的生存环境。绿色 IT 已经成为中国 IT 企业正在付诸实施的一项新的创新工程。

六、数据集中催生新一代企业级数据中心

计世资讯(CCW Research)认为,在电子政务、企业信息化等领域的逐渐展开,以及基于 WEB 的应用不断普及深入,新一代的企业级数据中心的建设将成为行业信息化的新热点。

计世资讯认为,新一代企业级数据中心的建设过程将是一个融合了数据集中、系统整合、企业网络升级、新型 WEB 应用、安全等内容的系统工程。新一代企业级数据中心将使行业信息化迈入一个更高的层面。在新一代的企业级数据中心的建设热潮中,必将给计算系统、数据存储系统、网络设施、安全和管理等领域的产品和技术带来崭新的机会与挑战。智能化的基础设施、服务器虚拟化技术、存储虚拟化技术、业务连续性保障技术、自主计算、智能化的监测/控制/管理等技术将与新一代企业数据中心的建设密切联系在一起。计世资讯分析认为,新一代企业级数据中心建设的热潮将带来超过 600 亿的市场规模。

七、重构计算机将改写人机交互的新格局

人机交互的风格经历了命令界面、图形界面、多媒体界面等主要发展阶段,目前正向虚拟现实技术和多通道用户界面的方向发展,例如,拥有强大处理功能的笔记本电脑能够像人类一样,用“视觉”准确的辨别出物体及其运动。这些我们认为短期不能实现的技术和应用正向我们走来。

英特尔将在 2010 年初发布的芯片让我们看到,这种原型采用了基于在互联网上建立“云”计算资源的数据中心的结构形式的新一代芯片,使未来的云数据中心将在目前的能效水平上得到数量级的成倍提升,从而节约大量空间资源和电力成本,同时对于推进人机交互发展将发挥巨大的作用,这无疑对目前亟需用户应用动力推进的计算机产业带来巨大的发展机会。

八、中国有线数字交互电视产业高速发展

计世资讯数据显示,2009 年中国有线数字电视产业双向网络市场规模达到 1200 万户,2010 年预计中国有线数字电视产业双向网络市场规模达到 2000 万户,增长速度超过 60%。随着用户的高速增长,预计 2010 年中国有线数字交互电视(ITV)整体市场容量达到 275 亿元。

中国有线数字交互电视产业的发展,将对整个信息产业带来巨大的影响,随着交互电视的发展,视频点播(VOD)、电子节目指南(EPG)、因特网接入、交互式新闻、交互式游戏、交互式电视商务、收发电子邮件、交互式广告、实况聊天等多种增值服务市场将呈现高速发展趋势。

九、4C 融合和终端融合成为发展趋势

随着电信网络、有线电视网络和互联网的发展,计算机(computer)、通信(communication)、消费电子(consumer electronics)、内容服务(content)之间趋于融合。而 4C 的融合也带动了终端之间的融合,也意味着 PC、手机、家电之间的界限越来越模糊。

我们的手机可以看电视,手机可以上网,手机可以控制家电,而电视又可以上网和点播增值服务,计算机可以便携和通话,而且内容方面所有的终端都可以共享。这一切都代表着信息产业融合的时代正在我们走来。

十、物联网产业从概念向扎实应用发展

“物联网”概念的问世,打破了之前的传统思维。过去的思路一直是将物理基础设施和 IT 基础

设施分开：一方面是机场、公路、建筑物，而另一方面是数据中心、个人电脑、宽带等。而在“物联网”时代，钢筋混凝土、电缆将与芯片、宽带整合为统一的基础设施，在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。

从计世资讯对物联网领域的典型应用 m2m 来看，全球 M2M 市场 2010 年将超过 7000 亿美元，中国市场也保持 30% 以上的增长速度，物联网应用将和我们的工作生活息息相关。

方正安全构筑安全长城 长城资产管理方案

文章来源：Cbsi 中国 • PChome.net

客户背景与需求

中国长城资产管理公司是国家四大国有资产管理公司之一，肩负着收购、管理和处置国有银行不良资产，防范金融风险的重任。为了完成国家赋予的使命，迫切需要建立安全、高效的、网络化的业务处理和信息化管理系统，为公司依法合规地处置、经营资产和高效科学地管理决策提供基础工具。

然而高速发展的信息化建设虽然为中国长城资产管理公司提供了高性能、大容量的信息通道，但同时也使得中国长城资产管理公司网络面临着新的风险，比如网上流行的恶意病毒、黑客攻击、窃取密码、拒绝服务等，这些风险可能给网络带来诸如数据不能正常传送、信息被破坏等种种损失和不确定性，威胁到网络的正常工作。因此，如何保证网络的正常和安全运行是信息化过程中十分重要的一环。

供应商的选择

继国家交通部、河北承德钢铁、国家外汇管理局、以及中铁六局等国家重点行业用户之后，方正信息安全技术有限公司凭借在技术、产品和服务方面的优势，以及公司提出的“层层设防，集中控管，以防为主、防治结合”的安全策略及相应的整体信息安全解决方案从众多强手中脱颖而出，拿下了该项目。中国长城资产管理公司采纳了方正安全公司的整体信息安全产品，其中包括方正千兆安全网关、方正防火墙、拒绝服务防范系统等产品的整体实施方案。

方正安全网关方案

在关键的 Internet 的入口及核心服务器群前，架设方正安全网关（PAGD）8000 系列产品，监控所有进出内部网络的 HTTP、FTP、IMPA4、NNTP、SMTP 和 POP3 数据，并对上述数据进行病毒过滤，形成对内部网络的第一道病毒防护屏障。

部署方正安全网关 PAGD 解决方案后，在网络防病毒工作上取得了显著的实效，主要体现在以

下几个方面：

1) 实时扫描所有进出网络的数据，保证网络中的用户可以放心地浏览 Internet 网页，下载软件，而且 Lotus Domino 服务器从外部接收的邮件完全无毒，真正从网络入口处就杜绝了病毒的入侵，有效地保护了整个网络的安全。

2) PAGD 的病毒特征文件缺省每日自动更新，有效地保证了它能抵御所有新出现的病毒。

3) 在 PAGD 中记录了所有的病毒事件日志，网络管理员随时可以进行查看，通过总结调整了其中的内容过滤，从而减低了带宽资源的总消耗量，更大地发挥了安全网关的效能。

方正防火墙方案

在关键的 Internet 的入口及核心服务器群前安装方正防火墙系列产品，监控所有进出内部网络的业务数据，并对上述数据进行访问控制和过滤防护，防范拒绝服务攻击，形成对用户和网络的整体防护。

部署方正方正防火墙解决方案后，在网络整体防护工作上取得了显著的实效，主要体现在以下几个方面：

- 1) 网络的防范：有效抵御了来自内部、外部的网络攻击。
- 2) 业务系统的防范：有效保障关键业务数据的访问控制和数据安全。
- 3) 拒绝服务的防范：有效杜绝拒绝服务攻击。

客户反馈

经过一段时间的使用，中国长城资产管理公司的信息化主管领导对于方正安全的整体防病毒安全解决方案、售后服务以及安全响应等都感到十分满意。尤其是在安装实施过程中，方正安全的工程师高度负责的敬业精神更是让用户领导留下了非常深刻的印象。

惠普收购 McAfee 传闻再起 被投资者看好

文章来源：cnBeta

美国投资银行 Friedman Billings Ramsey 近日在报告中称，惠普可能收购互联网安全厂商 McAfee。

Friedman Billings Ramsey 在报告中称：“收购 McAfee 将明显提升惠普在安全市场的竞争力，从而与思科一较高下。” McAfee 是全球第二大安全厂商。

受该报告影响，McAfee 股价周一大涨 1.44 美元，为两个月以来的最大涨幅，收于 41.57 美元。Friedman Billings Ramsey 同时指出，今明两年全球软件市场的并购将十分活跃。

早在 2006 年 8 月，就有分析师预测，惠普可能收购 McAfee 或赛门铁克，以弥补在安全市场的空白。当时，IBM 斥资 13 亿美元收购了安全软件和咨询厂商 Internet Security Systems。

技术前沿

同洲电子涉窃密：源代码鉴定成案件关键

文章来源：信息时报 作者/潘敬文

上周，本报报道了同洲电子因涉嫌窃取宇龙酷派商业机密而引发危机，本周该事件有进一步进展。据记者从各方了解到，目前该案件的焦点集中在源代码鉴定上。

“就跟判断文章是否抄袭一样，对 E89 手机源代码进行鉴定，就是判断同洲是否抄袭的最佳方法。”深圳市同洲电子股份有限公司(002052.SZ，以下简称同洲电子)董事长袁明如此向记者表示。“过了一个月后才上交，天知道源代码是否早已被修改过？”一名宇龙酷派内部人士气愤地反驳。

同洲电子

要求深圳警方比对源代码

上周，本报手机版深入报道了上市公司同洲电子涉嫌窃取宇龙酷派商业秘密，并引发股价下跌危机事件，引起广泛关注。本周记者获悉，该案件有新进展。

据记者了解，同洲电子近日致函深圳警方，要求警方加快组织对该公司被指侵权的 E89 手机源代码进行比对鉴定。同洲在函中表示，正因为没有及时对 E89 手机源代码进行鉴定，才会出现与事实完全不符的报道和解读。

日前，再次接受记者采访的同洲电子董事长袁明表示：“就跟判断文章是否抄袭一样，对 E89 手机源代码进行鉴定是判断同洲是否抄袭的最佳方法。”

指责酷派阻碍源代码鉴定

据同洲电子向媒体披露的信息，案发后同洲电子董事会为配合警方尽快查明案情真相，已于今年 3 月 2 日主动向深圳市公安局经济犯罪侦查局提交涉嫌侵犯商业秘密的 E89 手机的源代码。同时，该公司已经按要求提供该技术的相关说明和支持，并安排高管人员和相关部门的员工接受案情询问。

据披露，尽管针对 E89 手机源代码的鉴定申请已于 4 月 10 日由国家科技部知识产权事务中心受理，但却由于涉案的另一主角——宇龙酷派的“无理阻扰”，致使该鉴定工作至今未能开展。

酷派 质疑源代码已被修改

“我们阻扰？我们怎么会阻扰？鉴定对我们是有利的啊！”面对直指向自己的矛头，一位宇龙酷派内部人士情绪激动。该人士表示，早在去年 5 月，酷派就发现同洲 E89 手机跟酷派相关手机非常相似：“连源代码中的错误都相似。”因此当时酷派就开始收集证据。该人士更表示：“1 月 18 日公

安局开始逮捕行动，而同洲直到 3 月 2 日才上交源代码。谁能保证源代码在长达一个月的时间内没有被粉饰修改？”

而据一位不愿透露姓名的相关人士透露，同洲电子手机部的电脑系统有严格的格式化程序：平均每月均会格式化，因此这无疑给调查带来很大困难。另有人士私下透露，尽管涉案的其中一位主角——同洲电子移动手机部总经理王国军在近日的同洲电子组织的媒体见面会上出现，但依然是“取保候审”身份。“最初逮捕的 7 人中不包括王国军，但其后对这 7 人的审讯中警方获悉，抄袭源代码均为王国军策划。”据透露，王国军最初潜逃，但其后承受不住警方发布通缉令的压力，被迫自首。而对于上述传闻，同洲董事长袁明拒绝评论，并表示一切以公告为准。

云计算火热背后：标准及安全成首要问题

文章来源：飞象网

能迅速扩大服务器能力、提供安全的数据中心、降低企业投资成本等，多种优势让云计算成为下一代互联网的主流方向，也因此得到全球各大 IT 巨头的关注。但随着这一技术的不断市场化，云所存在的标准、安全等问题也越来越被关注。

对此，瞻博(JUNIPER)亚太区企业架构师 Greg Bunt 近日在接受飞象网采访时也给出了他自己的看法。

云计算标准应该开放

目前虽然很多厂商都有云相关产品和解决方案推出，但却缺乏一个统一的云计算标准，各产品在互操作上也难以兼容。

针对这一问题，微软中国研发集团主席张亚勤曾表示，全球应该有一个统一的国际云计算标准，他认为任何企业或者国家如果自己搞一套云计算标准，最后的结果很可能是形成信息孤岛。

对此，Greg Bunt 也持有相同观点，他表示要寻找开放、全面、基于标准互操作的方法来实现安全地扩展。据 Greg Bunt 透露，目前相关行业成员正在就政策、标准和合作研发与政府部门展开合作。

“我们一直倡导一个开放的标准，瞻博也正在和 IEEE 密切合作。对于目前一些竞争对手采取封闭式标准的做法，我个人并不赞成。”

具体到国内，工业化信息化部副部长娄勤俭近期也再次强调，要加强对下一代互联网技术、云计算等的标准研究工作，推进信息网络在各行业的应用。

安全保障成首要挑战

在云计算发展面临的挑战中，安全和隐私排在了首位。

这里的安全性主要包括两个方面，一是自己的信息不会被泄露避免造成不必要的损失，二是自

已在需要时能够保证准确无误地获取这些信息。

Greg Bunt 坦承，安全性是目前云计算最需解决的问题，也是瞻博一直以来重点关注方向。“在传统 IT 领域，瞻博的防火墙产品就占据了非常大的市场份额，而对网络安全厂商 NetScreen 的收购，也是瞻博其安全战略的重要部分。”

据 Greg Bunt 介绍，传统的安全方式是在客户和数据中心之间进行加密，而随着云计算的提出，客户和数据中心往往是在不同的地区，甚至不同的国家，原有模式已很难维系。对此，瞻博采取的解决方式是通过数据中心和数据中心、服务器与服务器之间的加密实现更高的安全架构。

巨头寻求组合应对云大战

“一站式”服务能力现在已经成为 IT 巨头们的竞争利器，为了达到这一目标，众厂商纷纷采取了收购或产业链合作的方式来应对这一市场大战。

2009 年 11 月，思科、EMC 和 VMware 宣布结成虚拟计算环境联盟，这是三大 IT 巨头的首次共同协作。

随后三家公司推出了 Vblock 基础架构包，并成立一个独立的公司 Acadia 来为数据中心提供端到端业务的私有云基础架构建设方案。Vblock 集 EMC 的存储设备、思科虚拟技术服务和网络设备以及 VMWare 的虚拟技术于一体。

瞻博和 IBM 也有着类似的合作关系。据 Greg Bunt 介绍，在和 IBM 的合作中，瞻博主要提供网络架构和操作系统，部分 IBM 产品也由瞻博 OEM 代工，IBM 提供其所擅长的服务器和存储服务。

对于 HP 收购 H3C，Greg Bunt 认为同样是基于互补的需要，HP 看中的正是 H3C 在 IP 网络和数据中心领域的技术优势，能够在未来满足云计算对数据中心的应用需求。

中国市场对手很强大

作为一个在中国有超过十年时间的企业，瞻博较早对这一市场进行了布局，而随着国内互联网经济的日渐成熟，中国已逐渐成为瞻博重要战略发展区域。

在说到中国市场的竞争时，Greg Bunt 认为 H3C、华为、中兴都是很优秀的企业，也是瞻博强劲的对手。“但我们也有自己的优势，瞻博除提供网络设备外，还提供安全服务，并且可直接为数据中心最终用户服务。”

据悉，在国内电信行业，瞻博为广东电信、香港电信等提供了数据中心产品服务。

在被问及针对不同客户瞻博是否有不同的产品策略时，Greg Bunt 解释道，除了为大型客户提供高端数据中心产品外，对于一般规模企业，瞻博会有简化版产品，但为了保证产品的互操作和安全性，所有产品都会采用相同的操作系统。

“另外我们还可以提供 SDK(软件开发工具包)，合作伙伴可以根据情况在瞻博产品之上添加自己的标准和需求，达到定制化的目的。”

企事业单位局域网的信息安全技术分析

文章来源：万方数据

随着信息网络的高速发展，企事业单位也不可抗拒的加入到了信息网络时代之中。越来越多的企事业单位都逐步的组建了自己的本地局域网，从而实现了其生产过程自动化和管理水平现代信息化。信息化的实现使企事业单位的工作效率得以极大的提高，因此，信息管理工作在现代的企事业单位中发挥着越来越重要的作用。随着信息技术的广泛、深入的应用，各种先进的局域网给企事业单位办公和管理带来高效率的同时，也带来了新的网络信息安全问题。

一、网络信息安全概述

1.1 安全的含义

网络信息安全涉及到信息的机密性、完整性、可用性、可控性。它为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。随着网络时代的迅速前进，信息安全的含义也在不断的变化发展，单纯的保密和静态的保护已不能适应当今的需要，如今的信息安全已变为了一个信息保障体系系统。信息保障和依赖于人操作和技术实现组织的任务运作，针对技术信息基础设施的管理活动同样依赖于这三个因素，稳健的信息保障状态意味着信息保障和政策、步骤、技术和机制在整个组织的信息基础设施的所有层面上均能得到实施。

1.2 信息安全系统性能

为了对企事业单位的局域网内的计算机进行实时有效的管理，充分发挥信息安全系统的保护和监督作用。根据局域网应用状况和技术水平，信息安全系统应具有以下性能。

①全面性。不仅要知道局域网内的各个机器的使用状况，还要了解客户端的运行信息，实现全面完整的保护。

②实时性。安全系统必须是一个操作系统启动时立即自动运行的程序，所以它必须嵌入在被保护计算机的启动配置文件中。

③操作性。安全系统使用者多是管理人员。他们应用计算机的能力可能不是很强，因此一定要简便好用，图形界面通俗易懂，操作方便简单。

二、企事业单位信息化网络所存在的安全风险分析

2.1 路由/交换设备的安全风险

路由设备负责将网络中的信息传输和交换选择优化路径，由此可见。路由设备在信息网络中的核心地位，路由设备的安全直接影响到整个网络的安全。路由设备的安全风险主要有：

①路由器缺省情况下只使用简单的口令验证用户身份，并且远程 TELNET 登陆时以明文传输口令。一旦口令泄密路由器将失去所有的保护能力。

②路由器口令的弱点没有计数器功能，所以每个人都可以不限次数的尝试登录口令，在口令字典等工具的帮助下很容易破解登录口令。

③每个管理员都可能使用相同的口令，因此，路由器对于谁曾经作过什么修改，系统没有跟踪审计的能力。

④路由器实现的某些动态路由协议存在一定的安全漏洞，有可能被恶意的攻击者利用来破坏网络的路由设置，达到破坏网络或为攻击做准备的目地。

2.2 数据库系统安全风险

数据库系统是局域网络体系里不可缺少的重要组成部分，它负责担负管理和存储网络中数据信息的任务。随着数据库技术的不断发展，一些非法用户也利用先进的技术攻击破坏数据库系统，窃取数据库中的数据，数据库系统的安全风险日益严重。数据库中的安全风险主要表现在两个方面：

①数据库数据的安全，数据库中存放着大量的数据，它应能确保当数据库系统崩溃时，当数据库存储媒体被破坏时以及当数据库用户误操作时，数据库数据信息不致丢失。

②数据库系统的安全，数据库系统应该不被非法用户侵入，应该尽可能的堵住潜在的各种漏洞，防止非法用户利用它们侵入。

三、企事业单位局域网络安全的实施

3.1 建立网络安全管理组织

企事业单位应该建立自己的网络信息安全方面最高权利的管理组织机构，从来负责规划本单位局域网络信息安全有关规划、建设、投资、安全政策等方面的决策和实施；单位建立网络安全管理组织还能确定网络信息安全各岗位人员的职责和权限，建立健全本系统安全规程和制度，做到安全审计跟踪和分析检查，及时发现和处理安全风险隐患。

3.2 建立完善的网络安全体系

3.2.1 建立完善的局域网中心网络安全体系

面对日益复杂的网络入侵技术和网络环境，如何在确保单位内部关键业务信息和生产数据安全的前提下实现信息共享，已经成为突出且尖锐的问题。要较为有效的解决这个问题，企事业单位必须采取一系列的网络安全措施方案，尤其有必要在单位局域网中建立完善的中心网络安全体系。

在企事业单位的局域网内设置中心网络安全体系采用物理隔离的方法实现了将内网间接的与外网相连，大大加强了单位的局域网的信息安全性能。

3.2.2 建立完善的网络安全策略体系

在局域网络信息安全管理中，技术是基础，是科学管理的立足点。但一味依赖技术的安全保证是远远不够的，企业的规章制度保障、组织保障及网络安全教育、人员素质提高等往往成为信息网络安全决定因素。因此，建立相应的科学的网络安全策略体系是局域网信息安全体系的保障。

JavaScript 大师：网络开发应更重安全

文章来源：eNET 硅谷动力

身为 JavaScript 网络技术重要推手的雅虎（Yahoo!）架构设计师 Douglas Crockford 表示，现行网页开发技术思维仍偏重多媒体功能或浏览效能的提升，未来应以网络安全为第一优先。

Crockford 现为 Yahoo! 资深 JavaScript 架构师，负责 YUI（Yahoo! User Interface）的架构设计，并且担任 ECMA JavaScript 2.0 技术委员会成员，为 JavaScript 开发社交网络大师级人物，此次受邀参加 OSDC（Open Source Developer's Conference Taiwan）进行专题演讲，向众多开发者介绍 ECMA JavaScript 的发展。

Crockford 向媒体阐述网络技术发展时指出，当前的网络技术仍然不脱过去的思维，网页开发技术仍以功能强化、浏览网页效能提升为主，虽然强化了网络开发的丰富性，但未将网络安全列为开发优先考虑因素的结果，致使网络安全事件层出不穷。

延续过去网络开发思维的结果，现今网络技术强调强大的互动、多媒体功能，但也让一些攻击手法兴起，以 XSS（Cross-Site Scripting）为例，由于内嵌多个不同来源的指令代码，容易让黑客藉指令集趁虚而入，窃取用户端电脑的资料。

虽然也有新的技术，如 Google 推动的 Caja，用以防范 XSS 跨站攻击手法，但整体技术发展方向仍是朝功能、效能提升前进。

以 HTML 5 技术为例，Crockford 表示，虽然 HTML5 增加了许多功能，但让整个指令代码变得更庞大且复杂，容易产生漏洞遭到攻击；另外，支援存取使用者电脑、手机的终端资料，将资料被窃的安全风险扩大至手机上，而过于庞大复杂的结果，不容易因应日新月异的攻击手法改变，长期而言易形成安全风险。

对于当前浏览器产业形成速度竞赛，纷纷强化 JavaScript 引擎加速网页浏览速度，号称最快的浏览速度，他认为，浏览器加速网页浏览速度虽是好事，但这样改善方式有限，只在 5 至 10% 的终端浏览器部份加速，若能同时改善服务器端，加速的效果更大。

对于制定中的新标准 ECMA Script 5，他乐观预期未来将成为主要的网络开发标准，虽然 Apple、Chrome 还不明确，但包括 IE、FireFox、Opera 都倾向 ECMA Script 5，今年应会看到新的浏览器采用。

ISMS 实施过程常见困惑与应对

文章来源：中国信息安全博士网 作者：谷安天下牛志军

国内从 1999 年，厦门人保获得第一张 ISMS 认证证书至今，通过该项认证的企业为 180 多家，包括华为、中兴、深交所、深圳地铁、平安保险、上海中芯国际、大连华信、上海银行、比亚迪汽车、中国移动（北京、辽宁、天津公司、广东公司）、中国网通（天津、北京公司）、中国电信（上海、北京、广东公司）等企业，主要集中在电信、金融、软件外包开发等行业。与目前国际通过该项认证的企业数量 5200 家相比，中国通过认证的企业数量并不多，但国内按照或参考 ISO27001 或 ISO27002 国际标准，建立健全本企业信息安全管理体系的企业却越来越多，一直以来，在实施信息安全管理体系的实践过程中，无论是企业的管理层人员还是具体实施人员，无论是通过认证企业还是未认证企业，对 ISMS 实施过程都不同程度的存在着一些困惑和误区。

困惑一：想仅仅通过技术和产品，就解决所有的（或主要的）安全问题。很多企业，甚至大型知名企业，上了很多技术和产品，有的企业甚至也建立了很多安全管理制度，甚至做了信息安全管理体系并通过了认证，投入了很多财力人力，但整体信息安全管理水平并没有明显提升，信息安全问题还是层出不穷。根源在于这些企业都存在着一个普遍的问题：相关的管理跟不上，如设备上线了，运行很久了，还存在着很多默认配置、设备的相关策略不完备、长时间不评审不更新、离职人员帐户仍然存在、制度不执行或执行不到位、不彻底。这些问题不能很好地解决，即使有再好的产品、技术或标准，企业的信息安全管理水平也很难从根本上有所提高，上再好的产品、技术和标准最多是升级一下 IT 救火队的装备水平。在信息安全方面，一定要重视“三分管理，七分技术”这一原则，要向管理要安全。技术只是帮助实现管理的手段，就 ISO27001 而言，它的 11 个控制区域中，只有 3 个区域是完全和技术相关，其它 8 个都是要求如何进行信息安全管理，比如物理安全、人力资源安全、业务连续性管理这些都无法纯粹依靠技术来实现，更多的是要靠管理来实现。

困惑二：信息安全与工作效率的关系，做信息安全会不会影响工作效率。业务部门表面上都支持，但实际工作中并不配合。这是很多企业信息安全管理体系推行过程中，具体实施人员最常见的体会和抱怨。业务部门的支持是一个永远的问题。导致这个问题的原因很多，“工作很忙”，“出差刚回来，还要出去，根本没时间看那些什么安全策略”，“不要不相信我，我不会泄密”、“我们工作本来就很忙，拜托别再给我们增加工作了”等等。真的没有时间吗？明显不是，真正的原因是“业务才是最重要的，其它都是次要的”、“我干的这几年，运气不会这么差吧”，对安全风险的严重性认识不足，心存侥幸心理，不仅一般员工如此，有的管理层人员乃至核心管理层人员都不同程度有如此想法。

首先，信息安全负责人员在具体实施过程中，也要考虑统筹安排时间，毕竟企业是以赢利为目的的，业务是很重要的，在具体工作安排上，在不影响工作绩效的前提下，要尽可能以节约业务部门人员的的时间的方式进行，比如安全意识的宣传，不要只是课堂培训一种方式，内部网站、经常性的提示性邮件、宣传小册子、打印机复印机旁的小贴士、台历上的安全小故事都是不错的选择，信息安全宣传方法要灵活，你理解业务部门，业务部门也会欢迎，也会理解你的工作。

其次，落实具体控制措施的好处，要向业务部门讲透。向业务部门推行的很多安全控制措施，

如果能够得到良好的落实，对业务部门也是有好处的，有助于降低业务部门及相关人员的风险，业务部门不配合很大程度上是因为他们自己还没有看到这一层，我们的实施人员也没有向业务部门人员点透这一层。大部分情况，在业务部门人员明白这一层后，都会积极配合，也会接受因为控制措施实施导致的工作效率暂时性所受到的影响。

再次，单就实施具体的安全产品（如终端控制软件、使用 CA 证书）而言，在实施初期，由于业务部门人员操作不熟悉，会在一定程度上影响工作效率，但一旦人员操作熟练后，就不存在这个问题了，而且由于安全控制的提高，会降低业务部门的安全风险，减少业务部门人员用于终端或系统故障的时间，提高业务部门的工作效率。

困惑三：安全管理是一阵风，风吹时很猛，但吹过了，也就完了，如何长久保持。其实信息安全管理，特别是信息安全管理体制，要保持信息安全管理体制能够有效长久运行，最重要的是在企业中建立以下三个机制：持续改进机制、信息安全奖惩机制和内部信息安全审计机制。

要在企业文化中不断渗透持续改进的思想和意识，设置配置需要及时更新、安全制度和策略需要及时评审，缺少持续改善机制和文化企业的信息安全管理，无法逃脱“搞运动”的宿命一体系建立时，人人热血沸腾，文档制度一大堆，大家都认真执行，但过了几个月就基本上束之高阁，一切又回到旧轨道上。

“推行管理体系本身就是一件很有难度的事情，再加上奖惩，更不好做了，奖好办，但罚时，该罚谁呢，罚谁谁都会不高兴，会影响到同事关系，信息安全就是得罪人的事，没人愿意做，不好做”，具体实施人员经常有这样的抱怨。其实这个问题很容易解决，第一，明确和高层领导讲，如果想安全管理能够长久化、持续化，必须要有配套的奖惩（不能只奖不罚或只罚不奖）；第二，奖惩的问题本来就不应该是信息安全实施人员的职责，是人力资源部门的事情，不建议信息安全实施人员不要借机“夺权”，在本职工作外，做自己原本不擅长的工作，信息安全实施人员要做的就是把控制措施执行情况的数据交给人力资源部门（很多是和技术相关的，需要实施人员提供）。

定期的信息安全内部审计机制非常重要，只有进行检查（CHECK），并对检查中发现的问题进行的整改（ACTION），整个信息安全管理体制才会形成完整的 PDCA 循环，形成一个闭环。如果因内部人员能力限制，也可以将内部安全审计外包给有资质的安全公司或会计师事务所进行。没有检查机制的安全管理是不可能有效绩的。

困惑四：只是下面的人在忙，老板只是口头上重视。这种现象在一些企业中很明显的存在，结果是具体实施人员也想了很多办法，费了很多力气，但实施效果并不理想。造成这种现象的原因就是缺乏高层真正的支持，包括财务、人力的投入，安全是自上而下的过程，自下而上的进行很难成功，信息安全管理体制的推行需要企业最高管理层的绝对支持和身为表率并持之以恒，最高管理层可能没有时间去一一详细了解每一项安全策略的内容，没有时间去参与具体的每一项实施工作，实践中这也是不可能的也不必要的，但最高管理层必须要很清楚他们的相关言行必须与企业信息安全的终级要求相一致，如果相背离，极有可能会事倍功半、事与愿违。在一个高层管理层人员都为贪

图便利在使用弱口令的企业，却建立起一套良好的信息安全管理机制是不可想象的。

困惑五：忘记安全是一个动态的过程。“信息安全花了这么多钱，为什么还出事”，在企业中，特别是发生重大的信息安全事件后，不时会听到这种声音。出现这种声音，有两种可能，一种是安全没有落实到位，安全最重要的是落实，空中楼阁式的安全管理只是美丽的肥皂泡，结局只能是又获得一次惨痛的教训。在实践中，还有另外一种情况，企业执行力也不错，各项措施也有落实，但还是出现问题了。这时出现这种声音，问题在于持这种说法的人，问题出在他的思维方式上。风险是一个动态的过程，信息安全也是一个动态的过程，产品技术标准不断发展和完善，信息安全威胁也是不断地升级换代，随着企业信息化程度的进一步加深，企业核心业务对 IT 依赖度的进一步加强，信息安全问题会相对越来越多，这是一个不可扭转的趋势和现实。现实的情况是上这些设备，建了这个体系，会减少很多安全问题和风险，但不能完全避免，如果不上这些设备和体系，问题只会更多。这一点是信息安全管理部门和人员最希望得到管理层和业务部门理解的一点。

100%的安全是没有的，也是不可能的，即使是与要时刻核算成本的企业相比，可以“不计成本”投入的安全部门和军队，也做不到 100%的安全，美国的 CIA、FBI 和国防部不也不上一次发生过网页被改，重要机密被泄露的事件吗？美国 SP800 标准中不也是把“绝对安全”改为“相对安全”了吗？

信息安全事件的发生具有一定的必然性，也有偶然性，不能单凭信息安全事件的影响程度和发生与否作为考虑安全管理人员绩效考核的唯一标准。对于管理层而言，重要的是考虑在信息安全方面的投入和风险接受级别间找到一个平衡点

困惑六：其它企业的成功的经验，为什么在我们这里却不行。信息安全管理实施模式切忌生抄照搬，一定要结合自己企业的企业文化和实际情况进行。在执行力强的企业中，很多控制措施可以一步到位，但在执行力稍差的企业中，就是考虑是不是要分步实施；在对大型企业或金融行业，每年有固定的 IT 预算，IT 投入较充裕，一些安全控制手段可能考虑通过技术实现，但在一些小型企业或 IT 投入较小的企业，就要考虑通过管理实现。除此之外，还要考虑企业文化的其它方面，如企业的不同性质、企业领导人的不同风格、企业内部沟通机制、信息安全主导部门和人员在企业中的地位诸多等因素。

另外，在信息安全管理过程中需要以人为本，尊重人性。在企业的信息安全管理中，除了产品和技术外，人员的因素非常重要，人员的无意泄密还可以通过培训提高安全意识来改善；可以通过邮件审计、打印复印控制、USB 控制、硬盘或文件加密等方法，减少泄密的渠道；但对人脑记忆的信息的传播是无法通过技术来控制的，至少目前的技术手段是实现不了的。而且技术手段实现的诸多的监控，更多是为安全事件的留下证据，与之相比，事前预防是最重要的，加强事前预防的最可行和有效的手段就是从管理方面通过包括人性化管理、信息安全奖惩等方法综合运用不断增强员工对企业的认同感、归宿感和忠诚度。

作者简介：牛志军，金融证券期货行业资深信息安全顾问，BS7799LA，国家注册审核员，国内

第一批 ISMS 实施咨询专家；对于信息安全咨询有丰富的理论基础和实施经验，擅长于行业风险评估、IT 审计、ISMS 建设、企业内部控制等领域，曾成功主导多家知名企业信息安全项目的实施工作，发表信息安全论文多篇；对营销管理、战略管理、人力资源管理等有广泛涉猎。

黑客攻防

世界第一黑客十大建议

文章来源：比特网

“电脑与他的灵魂之间似乎有一条脐带相连。这就是为什么只要在计算机面前，他就会成为巨人的原因。”——美国联邦调查局某特工。

凯文·米特尼克，1964 年生于美国加州的洛杉矶。13 岁时他对电脑着了迷，掌握了丰富的计算机知识和高超的操作技能，但却因为用学校的计算机闯入了其他学校的网络而被勒令离校。

15 岁时，米特尼克成功入侵了“北美空中防务指挥系统”的主机，成为黑客史上的一次经典之作。

不久，他又成功破译美国“太平洋电话公司”在南加利福尼亚州通讯网络的“改户密码”。随后，他又进入了美国联邦调查局(FBI)的电脑网络，吃惊地发现 FBI 的特工们正在调查的一名电脑黑客竟然是他自己！他立即施展浑身解数，破译了联邦调查局的“中央电脑系统”密码，每天认真查阅“案情进展情况报告”，并恶作剧地将特工们的资料改成十足的罪犯。不过，特工人员最终还是将米特尼克捕获，法院将他送进了少年犯管教所，米特尼克成为世界上第一个“电脑网络少年犯”。

很快，米特尼克就获得假释。1983 年，他因非法通过 ARPA 网进入五角大楼的电脑网络而被判在青年管教所 6 个月。1988 年因为入侵数字设备公司 DEC 再度被捕。1990 年，他连续进入了世界 5 家大公司美国太阳微系统公司、Novell 网络公司、NEC 公司、诺基亚公司和摩托罗拉公司的网络，修改计算机中的用户资料，然后逃之夭夭。1994 年 12 月 25 日，米特尼克攻击了美国圣迭戈超级计算机中心，因此获得“地狱黑客”的称号。但是，这次攻击激怒了负责该中心计算机数据安全的著名日籍专家下村勉，为挽回损失和教训米特尼克，这位计算机高手利用自己精湛的安全技术，帮助 FBI 将米特尼克捉拿归案。

联邦法院以 25 宗非法窃取电话密码、盗用他人信用证号码和闯入他人网络的罪名起诉米特尼克，而且未经审判就将米特尼克关押了 4 年半，并且不得保释，这是美国司法史上对一名高智商罪犯所采取的最严厉的措施。

2001 年 1 月，米特尼克在认罪后，获得了监视性释放。

“黑客们变得越来越老练和狡猾，他们会想出各种新的花招，利用技术漏洞和人性的弱点来劫持你的计算机系统。”——凯文“米特尼克

获得自由后的米特尼克，目前投身于计算机安全咨询和写作中，他穿梭于世界各地，告诉人们在一个充满工业间谍和众多比他更年轻的黑客世界里，如何保证自己的信息安全。

他在一次转机的间隙，写下了以下十条经验与大家分享。

● 备份资料。记住你的系统永远不会是无懈可击的，灾难性的数据损失会发生在你身上——只需一条虫子或一只木马就已足够。

● 选择很难猜的密码。不要没有脑子地填上几个与你有关的数字，在任何情况下，都要及时修改默认密码。

● 安装防毒

软件，并让它每天更新升级。

● 及时更新操作系统，时刻留意软件制造商发布的各种补丁，并及时安装应用。

● 在 IE 或其它浏览器中会出现一些黑客鱼饵，对此要保持清醒，拒绝点击，同时将电子邮件客户端的自动脚本功能关闭。

● 在发送敏感邮件时使用加密软件，也可用加密软件保护你的硬盘上的数据。

● 安装一个或几个反间谍程序，并且要经常运行检查。

● 使用个人防火墙并正确设置它，阻止其它计算机、网络和网址与你的计算机建立连接，指定哪些程序可以自动连接到网络。

● 关闭所有你不使用的系统服务，特别是那些可以让别人远程控制你的计算机的服务，如 RemoteDesktop、RealVNC 和 NetBIOS 等。

● 保证无线连接的安全。

在家里，可以使用无线保护接入 WPA 和至少 20 个字符的密码。正确设置你的笔记本电脑，不要加入任何网络，除非它使用 WPA。要想在一个充满敌意的因特网世界里保护自己，的确是一件不容易的事。你要时刻想着，在地球另一端的某个角落里，一个或一些毫无道德的人正在刺探你的系统漏洞，并利用它们窃取你最敏感的秘密。希望你不会成为这些网络入侵者的下一个牺牲品。

破解 iPhone OS 存在诸多安全隐患

文章来源：IT 世界

苹果表示，越狱 iPhone、iPod、iPad 会导致服务中断和其它一些安全问题，未经授权对 iPhone OS

进行修改是导致机器不稳定的主要原因。

越狱机器的危害主要有以下几方面：

- 1.设备和应用不稳定：系统频繁崩溃，内置应用程序被冻结，甚至第三方应用程序和数据丢失。
- 2.语音和数据连接问题：经常掉线、数据连接不可靠，定位数据延迟或不准确。
- 3.服务中断：可视化语音信箱、YouTube、天气和股票很有可能会被破解操作破坏而不能正常工作；第三方推送通知的应用程序可能会遇到同步问题。
- 4.危及个人资料安全：越狱可能导致个人信息流失，黑客有可能以内置木马或病毒窃取个人资料。
- 5.缩短电池寿命：黑客软件会使电池消耗加速，使电池充电周期缩短。
- 6.应用软件无法更新：未经授权的修改造成的对 iPhone 操作系统和机器硬件的损害，苹果将不予质保，并且不能更新到最新的系统。

黑客攻破 iPhone 手机 运行 Android 系统

文章来源：CNET 科技资讯网

4 月 26 日国际报道 在苹果 iPhone 手机上执行 Google 的 Android 操作系统？这听起来不可思议的事，黑客办到了！

David Wang 是破解 iPhone 的黑客团体 iPhone 开发团队(iPhone Dev Team)的成员，他上周贴出一部视频，示范如何在 iPhone 上使用 Android。

视频中显示完整的开机过程--可见到 Tux Linux 吉祥物--以及 Wang 如何用 Android 浏览、接收短信、接电话、播放音乐。这部 iPhone 被他设定成双重开机模式，而视频一开始时的确显示手机执行的是 iPhone OS。

Wang 在视频里说：这还不到可以生产的品质，现在只能说是 alpha 品质。但几乎各项功能都可运作。

让 iPhone 跑 Android，可说是黑客的一大技术壮举，虽然不可能改变整个产业或主流消费者的使用习惯，但显示即便苹果极力维持自家手机的封闭性，仍阻挡不了黑客的破解。

根据他的博客，Wang 自从 2008 年以来就设法在 iPhone 上用 Linux 开机。视频中使用的是第一代的 iPhone，但相同的作法应该也可套用在较新的机型上，例如 iPhone 3G，只是可能需要多费一些功夫。

他说：希望打下基础后，我们可以让 Android 真正成为 iPhone 使用者的替代或补充的选择。也许我们终于能用 Flash 了。

国家网络入侵防范中心：上周共有漏洞 73 个

文章来源：新华网

国家计算机网络入侵防范中心发布安全漏洞周报说，4 月 19 日至 25 日一周内共发现安全漏洞 73 个，其中高危漏洞 27 个，中等威胁漏洞 45 个，低威胁漏洞 1 个，安全漏洞总量相比前一周有所下降。

这些安全漏洞中对我国用户影响较大的有 IBM Cognos 8 商业智能系统未知漏洞、RIM BlackBerry 手机附件服务组件 PDF distiller 多个未知漏洞。攻击者利用这些漏洞可导致远程执行任意代码、影响信息机密性、完整性、可用性或引起拒绝服务攻击等。

国家计算机网络入侵防范中心常务副主任张玉清说，在本周安全漏洞中，最值得关注的是 IBM Cognos 8 商业智能系统未知漏洞。该商业智能系统能支持业务部门制作复杂的合作报表，帮助业务部门更加准确灵活地做好数据分析和信息共享。IBM Cognos 8 商业智能系统存在未知漏洞，攻击者通过攻击向量利用该漏洞可能造成未知影响，截至目前还没有发现利用该漏洞进行的攻击行为，针对该漏洞厂商已发布更新，建议用户及时下载更新，防患于未然。

此外，RIM BlackBerry 手机附件服务组件 PDF distiller 多个未知漏洞也值得关注。RIM 公司的黑莓企业服务器软件及专业版软件附件服务组件中的 PDF distiller 没有正确处理特制的 PDF 文件，如果用户打开包含恶意 PDF 文件的邮件，则可能导致攻击者利用该漏洞执行任意代码或引起拒绝服务攻击。RIM 公司已针对这种攻击发布升级补丁，建议用户尽快安装。

海外来风

McAfee Apologizes for Update Mess

CIO Zone by Mel Duvall

Antivirus software vendor McAfee issued a formal apology for the mess it created when a software update it released crippled thousands of computers around the globe.

In the first public apology issued since problems surfaced earlier this week, McAfee blamed the issue

on inadequate software quality assurance.

"As you know, McAfee on [April 21] released a faulty signature update file (DAT) that caused problems for a number of our customers," said Barry McPherson, McAfee's vice president of support and customer service. "First off, I want to apologize on behalf of McAfee and say that we're extremely sorry for any impact the faulty signature file may have caused you and your organizations."

It is difficult to get a handle on how much damage the update caused as some organizations suffered complete meltdowns while many others reported no effects. Only machines running Windows XP Service Pack 3 were affected. Those running earlier service packs for Windows XP, including SP1 and SP2, were not affected. Nor were computers running Windows 2000, Vista, or the latest Microsoft operating system, Windows 7.

A Gartner analyst estimated about 10 percent of corporate desktops were hit by the glitch and news reports indicated a wide range of businesses, government agencies, hospitals and schools were affected by the faulty update. MSNBC reported that about one-third of the hospitals in Rhode Island had to postpone elective surgeries and stop treating patients without traumas in emergency rooms on Wednesday as a result of the glitch.

McAfee's McPherson said the company was able to publish a SuperDAT remediation tool early Thursday morning to help customers fix affected systems. The tool suppresses a driver causing the problem, restores the original Windows file, and then quarantines the file creating the issue.

"Of course many of you are asking how the faulty DAT made it past our quality assurance checks," McPherson said. "The problem arose during the testing process for this DAT file. We recently made a change to our QA environment that resulted in a faulty DAT making its way out of our test environment and onto customers systems."

"To prevent this from happening again, we are implementing additional QA protocols for any releases that directly impact critical system files," he added. "In addition, we plan to add capabilities to our cloud-based Artemis system that will provide an additional level of protection against false positives by leveraging an expansive whitelist of critical system files."

Judging by some of the comments posted on McPherson's blog, customers were not in a forgiving mood.

"First of all let me say I am glad we have switched nearly 75 percent of our clients away from your product prior to this happening," wrote a poster identifying himself as Charles. "I can't imagine the chaos if we hadn't. It was chaos enough for us running all over town and billing our client's for a software glitch on a program that we recommended to them."

McAfee 为软件升级混乱致歉（中文）

文章来源：ICO Zone 作者：Mel Duvall

杀毒软件供应商 McAfee 针对某款已发布的软件升级时导致全球成千上万台电脑瘫痪做出正式道歉。

自本周早些时候问题被曝光后，McAfee 在首次公开道歉中指责了软件质量保证的不足问题。

“正如你们所知，McAfee 在 4 月 21 日已发布了导致许多客户由错误的署名更新文件（DAT）引起的问题，” McAfee 售后服务与支持副总裁 Barry McPherson 说，“首先，我代表 McAfee 公司表示道歉，对由错误署名文件给您或您的公司所带来的任何影响表示诚挚的歉意！”

由更新所引起的破坏程度是难以掌握的，因为一些机构遭受了彻底的损害而另一些机构却表示没有反应。只有运行 windows XP 服务包 3 的机器才受到影响。那些运行 windows XP 早期服务包包括 SP1 和 SP2 的机器，以及运行 windows 2000、Vista 或者做新的微软操作系统 windows 7 的机器均未受到影响。

一位 Gartner 公司的分析师估算，约有 10% 的公司的计算机被小故障攻击，一份新闻报道表明大范围商业、政府机关、医院和学校受到错误更新的影响。微软全国有线电视公司报道：由于该故障，美国罗德岛州约有 1/3 的医院推迟了常规手术，并在周三停止接待急诊室的外伤病人。

迈克菲公司的 McPherson 表示，公司会在周四早上早些时候发布超级 DAT 修补工具，来帮助客户修复受到影响的系统。该工具将抑制启动程序引起问题，还原原始的 windows 文件，并隔离文件生成问题。

“当然，你们中的很多人会问到，错误的 DAT 是如何通过我们的质量检测的呢？” McPherson 解释，“问题是在检测这个错误 DAT 的过程中引起的。最近，我们更改了我们的质量测试环境，这导致错误的 DAT 可以逃脱我们的测试环境，映射到客户的系统上。”

“为防止该意外再次发生，我们执行另外的质量检测协议，任一版本直接影响决定性的系统档案，”他补充到，“另外，我们计划给我们的以云为基础的 Artemis 系统增加功能，该功能将提供额外等级的保护来阻止决定性的系统档案扩张的黑名单引起的误报。”

从发表在 McPherson 博客上的一些评论判断，客户对此无法原谅。

“首先，我要说，很高兴我们已经在此次意外发生之前扭转了几乎 75% 的客户远离你们的产品，”该消息是由自称为 Charles 的人发布的，“如果我们不阻止，混乱是无法想象的。这些混乱足以使我们满城跑并为我们的客户使用我们向他们推荐的软件的程序的故障开账单。”



SMP-U



国迈移动存储设备管理系统

三证齐全的移动存储设备管理系统

U盘系统核心功能：

- 杜绝U盘泄密事件
- U盘使用权限控制
- 防止U盘交叉使用
- U盘病毒主动防御
- U盘使用日志审计
- 适用于单机/网络

● 功能描述：

全国唯一三证齐全的U盘管理系统，通过国家保密局、解放军保密委、公安部三重权威认证。全网Internet告警中心+专用安全U盘+U盘管理系统“三合一”，对U盘、移动硬盘、手机存储、数码相机、MP3、MP4、各种CF/MD/SD卡/各类FlashDisk等移动存储介质进行分级注册，灵活控制U盘使用权限，防止信息泄密，记录使用日志，主动防御U盘病毒。杜绝因移动存储介质丢失、被盗用等造成的泄密事件。

■ Internet告警中心：

如涉密U盘违规外联到Internet，告警中心自动发出告警信息，并可查询到谁的U盘什么时间在哪个计算机（包括CPU、IP地址、MAC地址等）违规外联。

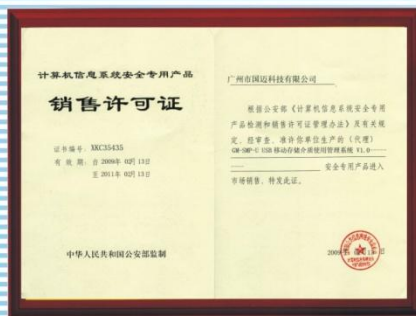
■ 六类专用安全U盘：

安全U盘、增强型安全U盘、单向导入U盘、单向导出U盘、双向交换U盘、外部受限使用U盘

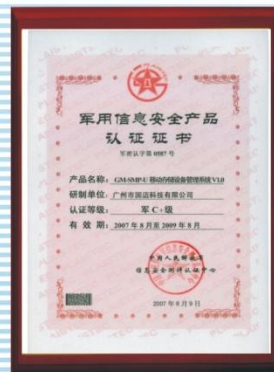
权威认证：



国家保密局认证证书
ISSTEC2008YT0618



公安部认证证书
XKC35435



解放军保密委认证证书
军密认字第0587号

成功案例：北京奥组委、解放军保密委、中国移动、中国边检、中国边防、某军工集团信息中心、总装某局、某卫星发射基地、中国兵器某研究所、中船舶某所、中国航天某设计院、核工业某研究院、山东公安、广东公安、河北检察院、广东省文化厅、洛阳有色金属设计院、机械工业四院、商丘电力、广东省第二人民医院、珠江医院、普利斯通、深圳电器、长丰集团、泰豪集团、汕头海关、北京大唐微电子、上海百联集团、深圳广前电力、河北建筑设计院、达尔嘉（亚洲）等。

防信息泄密，找国迈科技，要找就找最专业的！
更多信息，请登陆www.goldmsg.com