

安全周报

中国信息安全博士网

七月 第一期

二〇一〇年七月十二日

weekly.secdactor.com

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



SMP-U

国迈移动存储设备管理系统

唯一三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盘什么时间在哪台计算机（包括CPU、IP地址、MAC地址等）违规外联。

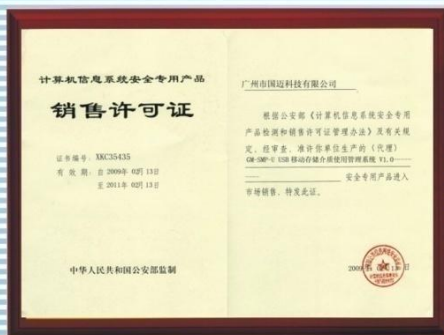
■ 专用安全U盘：

内部U盘、单向导入U盘、单向导出U盘、双向交换U盘。

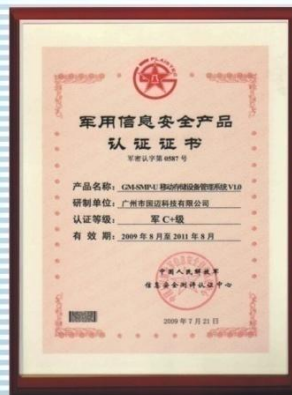
权威认证：



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、某核辐射研究院、山东公安、广东公安、广东国安、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

Guangzhou Goldmessage Technology Co., Ltd.



便携式计算机网络及 移动通信安全隐患展现系统

产品总述:

便携式计算机网络及移动通信安全隐患展现系统是一套能对网络信息系统和移动通信系统的多样化攻击手段、攻击方法、攻击后果、防护策略等进行直观展现的系统。

系统的成果包含当前主流的攻击方式和工具，展示各类网络隐患可能带来的攻击后果，便于系统管理人员、涉密人员及各级领导干部了解和学习各种攻击方式和防护方法，进而达到提高其忧患意识、责任意识和保密意识的目的。

便携式计算机网络及移动通信安全隐患展现系统的主要特性在于：
全部采用便携式设备，方便携带，且配备投影仪，现场展示效果好。
图形化操作界面、简明的操作手册，方便操作，实用性强。

展现的隐患种类较为齐全，功能丰富，更新速度快，新隐患出现后，会随时为用户进行升级和更新，并及时进行技术培训。

服务及时周到：为用户提供全面的技术支持与现场服务。

产品功能:

- 木马植入演示
- 网页篡改攻击演示
- U盘文件窃取演示
- 文件恢复窃取演示
- 网络钓鱼攻击演示
- 手机窃听演示
- 系统漏洞利用

国工信科技发展（北京）有限公司

地址：北京市中东路400号 邮编：102218 电话：8610-64126291 传真：8610-64126291
<http://www.guogongxin.com> email: secdoctor007@163.com



第三届中国信息安全博士论坛

(2010年7月31日-8月1日 宁夏·银川)



宁夏大学

欢迎您!

指导单位: 工业和信息化部信息安全协调司
教育部高教司
教育部高等学校信息安全类专业教学指导委员会

联合主办: 中国电子信息产业发展研究院
宁夏大学
北京电子科技学院

协办单位: 北京信息科技大学
北京交通大学
中国刑事警察学院

承办单位: 《信息安全与技术》杂志社
国工信科技发展(北京)有限公司

官方网站: 中国信息安全博士网 (www.secdactor.com)
第三届中国信息安全博士论坛官网 (meeting.secdactor.com)
教育部高等学校信息安全类专业教学指导委员会 (www.sec-edu.cn)

支持媒体: 中国电子报、中国计算机报、中国电脑教育报、通信产业报、中国经济和信息化、软件和信息服务、网管员世界、赛迪网、宁夏当地多家媒体

会议主题: 信息安全产、学、研的联盟创新与发展

会务组: 010-64126291 13661116129 张鹏飞

电子邮件: secdactor@163.com

会议官网: meeting.secdactor.com

目录

学术会议.....	7
中国信息化与 IT 治理高层研讨会.....	7
2010 中国中小企业信息化与成长力推进高峰论坛.....	9
2010 中国信息安全技术应用展览会.....	10
政府之声.....	10
美国：袭美黑客并非来自朝鲜.....	10
日本首设政府 CIO 推出满足国民信息技术战略.....	11
“网络工商”运营将与公安联网.....	12
印度禁售黑名单一网打尽 25 家中企.....	13
韩国总统府等 5 家网站受到黑客攻击.....	15
个人隐私成社交网站牟利工具.....	16
病毒播报.....	16
一种针对 MSN 和 Windows Live 的新威胁已出现.....	16
51kantv 盗 CNTV 世界杯视频 病毒悄然利用.....	17
网民热议新版红楼梦 黑客借机传病毒.....	18
微软称对 Windows 新漏洞 PC 安全展开调查.....	18
淘宝秒杀器暗藏木马病毒 买家网购需谨慎.....	19
产业动态.....	20
MySQL 开发者上诉欧盟批准甲骨文收购 Sun 决定.....	20
IBM 斥资 4 亿美元收购安全软件厂商 BigFix.....	20
Gartner：今年全球云服务市场将达 680 亿美元.....	21
中移动“扣费门”引发计费系统漏洞之争.....	21
微软向俄安全机关开放 Windows 7 源代码.....	24
全球最大 BT 网站曝安全漏洞.....	24
技术前沿.....	25
Win 7 SP1 包含升级版系统激活技术.....	25
传美国国家安全局开发新系统防御网络攻击.....	25
欧空局拟建造“末日方舟”备世界末日.....	26
黑客攻防.....	27
微软证实黑客已破解 Windows7 无限使用.....	27
网易回应黑客攻击事件：员工电脑被入侵所致.....	27
苹果 iTunes 和 App Store 遭黑客攻击.....	28
黑客攻破 iTunes 网站操纵用户账户购买软件.....	29

淘宝专家：关注网络账户链安全	29
男子散布木马病毒盗取银行卡号诈骗 40 万	30
Skype 安全协议遭破解	31
海外来风	32
Tax credits result in phishing attacks	32
企业推荐	34
北京数字证书认证中心简介	34

学术会议

中国信息化与 IT 治理高层研讨会

来源：CNET 科技资讯网

在今天的商业环境中，IT 已成为企业业务发展和管理不可或缺的重要组成部分，其作用和影响力已扩散到企业的每一个领域。但 IT 给企业带来活力、利润和竞争力的同时，也给企业带来了风险。例如，日益依赖 IT 的企业面临着因信息安全导致的业务灾难风险。因此，如何最大限度地保证信息安全成为每个企业都必须正视的问题。近日在深圳召开的“中国信息化与 IT 治理高层研讨会”上，信息安全架构和 IT 治理成为众多 CIO 关注的热点。会议认为加强信息安全离不开 IT 治理，完善的 IT 治理是信息安全的保障；而建立有效的信息安全架构则是 IT 治理的基石，企业才可以在很大程度上防御 IT 带来的信息安全风险。那么，信息安全架构是什么？为什么没有信息安全架构，IT 治理就容易成为空中楼阁？

一.IT 治理面临的信息安全挑战

在中国经济强劲复苏的背后，企业的业务发展与创新对 IT 的依赖程度越来越高。但任何事物都有它的两面性。正确、恰当地使用 IT 系统能为企业带来飞速的发展，但系统缺陷、人为误操作、系统攻击等不可预料的各种 IT 风险也同样会使企业面临巨大的灾难。长期以来，人们对保障信息安全的手段偏重于依靠技术，例如加密技术、数据备份、防病毒、防火墙等手段。而且在大多数 IT 管理人员的视角中，信息安全也仅仅局限在技术层面的操作，信息安全经常被看作只是一个技术问题，很少认为它是企业必需的并需要优先考虑。事实上，仅仅依靠技术来保障信息安全的愿望往往是难尽人意的，因为面对复杂多变的安全威胁和隐患单靠技术手段是无法消除的。

据实践经验表明，信息安全治理是与 IT 治理密不可分的。假如把信息安全治理比作指引组织进行安全项目的路标，那么信息安全架构的设计便是组织通往信息安全这个目标所用的交通工具。因此，没有了信息安全架构，IT 治理根本无从谈起。信息安全架构是指企业管理层利用它来监督企业在信息安全战略上的过程、结构和联系，以确保 IT 运营处于正确的轨道之上。因此，缺乏良好信息安全架构的企业，就是说缺乏健全的风险控制机制，因而不可能很好的进行信息安全管理，进而也不可能取得 IT 治理的成功；同样，没有信息安全管理体的畅通，IT 治理也只能是一个美好的蓝图，而缺乏实际的内容。

二.为什么信息安全架构是 IT 治理的基石？

(1)IT 治理要以 IT 风险防治为核心

目前，信息系统已在企业和政府组织中得到了广泛的应用，IT 治理成为企业治理越来越关键的一部分。在复杂的现实环境中，不安全因素总是存在的。各种各样的资料都显示着信息安全风险以

及灾难性事件的数量，正随着时间的推移而增加。IT 治理的一个重要内容是估计相关风险对企业的经营收益和 IT 绩效的影响，并有效控制 IT 风险，避免 IT 资产的损失。IT 风险是一种潜在的可能，是指某些威胁将会造成 IT 资产甚至其它相关资产损失或者破坏的潜在可能性。安全从来就不是一种非黑即白的概念。目前的信息安全早已不只是人们传统意义上的安全，即添加防火墙或路由器等简单的设备就可保证安全，而是成为一种系统和全局的观念。信息安全是指使信息避免一系列威胁，保障业务连续性，最大限度地减少业务损失，从而最大限度地获取投资和回报的一种保障机制。

传统的信息安全管理基本上是一种静态的、局部的、突击式、事后纠正式的管理方式，导致的结果是不能从根本上避免和降低各类风险，也不能降低信息安全故障导致的综合损失。而基于信息安全架构的思想是一个系统化、程序化和文件化的管理体系，基于系统、全面、科学的安全风险评估，体现预防控制为主的思想，强调遵守有关信息安全的法律法规及要求，强调全过程动态控制，本着控制费用与风险平衡的原则合理选择安全控制方式保护关键信息资产，使信息风险的发生概率和结果降低到可接受水平。COSO(美国内部控制委员会)在最新一期的 IT 治理指南中将 IT 信息安全架构界定为内部控制和风险防范的起点与核心，足以说明 IT 治理应以信息安全的识别和防范为着力点。因此，企业需要建立完善、健全的信息安全架构来规范 IT 治理行为，通过建立详尽的风险控制机制来降低企业的 IT 风险。

(2)信息安全是 IT 治理的基石

信息安全不是一个孤立静止的概念，它是一个多层面、多因素的、综合的、动态的过程。不同的企业对信息安全会有不同的理解，长期以来信息安全被看作是消极因素，不产生价值。然而，全球网络的出现和企业传统边界地的延伸，使其成为价值和机会的创造者，特别在提升 IT 利益各方的信任感方面。因此，信息安全必将成为 IT 治理一个重要且必不可少的部分，忽略信息安全将使 IT 价值的创造无法持久。信息安全的涵义体现在三个方面：一是安全性，是指确保信息仅可让授权的人获取和访问；二是完整性，是指保护信息和处理方法的准确和完善；三是可用性，是指确保授权人需要时可以获取信息和相应的资产。因此，实现信息安全是一个需要完整的体系来保证的持续过程。有效的安全防卫不仅是技术问题，也是一个管理问题。

一般来说，信息安全架构是通过实施一套恰当的控制措施来实现的，该控制措施包括政策、实践、程序、组织结构和工具软件组成。因此，信息安全架构模型和其它模型一样，具有以下几个方面的优点或作用：①信息安全架构模型涉及信息安全和业务需求的各个方面，能以简单方式测定差异，并有助于确定有关安全性方面的相对水平；②信息安全架构成熟度是测量安全管理处理等级的一种方法，这些等级是一个给定的信息安全管理处理的惯例，体现各个成熟层次的典型模式，有助于企业将主要精力投入到关键的管理方面；③信息安全架构模型等级有助于专业人员向管理层解释信息安全管理存在的缺陷，并把组织的控制惯例与最佳惯例对照起来，从而确定企业的未来发展目标。因此，信息安全架构和 IT 治理不但是息息相关的，也是 IT 治理的基石。

2010 中国中小企业信息化与成长力推进高峰论坛

来源：中国信息安全博士网

为落实国务院《关于进一步促进中小企业发展的若干意见》（【2009】国发 36 号文件）精神，贯彻工业和信息化部关于 2010 年促进中小企业发展的工作部署，提升我国中小企业的信息化水平和企业的成长力，中国信息协会决定于今年 7 月 8 日在北京京都信苑饭店举办“2010 中国中小企业信息化与成长力推进高峰论坛”。



中国信息协会会长卢时彻在会上发言

本届高峰论坛创新性地将提升企业成长力，这一企业实现可持续发展的核心命脉，作为新形势下推进中小企业信息化建设的主攻方向，以“抓住两化融合发展契机 以信息化提升中小企业成长力”为主题，围绕“政策环境、管理能力、技术创新、市场开拓、业务流程、成本控制、资源获取、员工素质”等影响企业成长力的各项要素，探讨如何在政府支持和指导下，针对中小企业的实际经营特点和需求，提供能够迅速见效兼顾可持续成长的信息化解决方案。论坛将盛邀政府领导、行业协会领导、专家学者、企业精英等演讲嘉宾，以及中小企业 CEO/CIO/技术主管、银行/投资信贷机构和行业媒体等共 300 余人出席，共商以信息化提升中小企业成长力大计，切实推动中国中小企业快速健康成长，为国民经济的持续稳定发展共同努力。

会上，中国信息协会会长卢时彻和工业和信息化部信息化推进司副司长董宝青就当前中国信息化的现状做了发言，董司长提出中小企业信息化要从细分市场着手，重视专业化和平台化。

会后，评选出“2010 年度中国中小企业信息化最佳××提供商、2010 年度中国中小企业信息化贡献企业奖、2010 年度中国中小企业信息化技术创新奖、2010 年度中国中小企业信息化最佳解决方案奖、2010 年度中国中小企业信息化最佳产品奖”，并举行颁奖仪式，为获奖企业颁发证书及奖牌”。

2010 中国信息安全技术应用展览会

来源：天极网手机频道

上海将举行“2010 中国信息安全技术与应用展览会”及“2010 中国信息安全高峰论坛”。此次活动由全国信息安全行业协会联盟、公安部第三研究所、上海市信息安全行业协会主办。

信息安全行业是上海顺利进行信息化建设的基础。信息安全产业作为新兴产业目前正处于发展的关键时期，了解国际信息安全技术和产业的发展态势，整合上海信息安全产业优势，从战略高度精心规划好上海信息安全产业发展，以市场为导向，集中力量，加速推进产业化，规范和促进我国自主信息安全产业这样一个新兴产业的跨跃式发展，抢占国内外信息安全产业制高点，将对上海信息产业乃至国民经济的建设具有深远的意义。

为了更好的推动信息网络的普及与应用，促进信息安全产业的技术交流，更进一步提高全社会的网络风险防范意识，加强国际、国内信息和网络安全企业更为广泛深入的交流与合作，由上海市网络与信息安全协调小组办公室、全国信息安全行业协会联盟、公安部第三研究所、上海市信息安全行业协会联合主办的“IS-EXPO 2010 中国信息安全技术与应用展览会及 2010 中国信息安全高峰论坛”将于 2010 年 10 月 13-15 日在上海光大会展中心隆重举办。

政府之声

美国：袭美黑客并非来自朝鲜

来源：四川新闻网

在经过近一年的技术分析之后，美国官员与网络专家 3 日说，去年 7 月对美国在韩国多家网站发动大规模攻击的黑客，不大可能来自朝鲜。一些美国专家认为，韩国黑客有可能才是真正的攻击者。这次袭击任务的目的就是“想找一只替罪羊”，是为了加剧南北对抗态势。

朝鲜《劳动新闻》5 日发表评论，谴责韩国参加“防扩散安全倡议”海上拦截演习，称这是挑起朝韩间的军事纠纷、并以此为导火索最终挑起侵朝战争的有目的和有计划的行为。

另据报道，两名朝鲜居民于 6 月 26 日划木船经日本海到韩国寻求庇护，这是自 3 月 26 日韩国“天安舰”沉没以来，朝鲜居民第五次逃到韩国。

日本首设政府 CIO 推出满足国民信息技术战略

来源：博客

日本政府的信息技术战略本部经近一年的工作，已制定出至 2015 年的中长期信息技术发展战略。该战略的正式名称为“i-Japan 战略 2015”。

其要点为大力发展电子政府和电子地方自治体，推动医疗、健康和教育的电子化。该战略本部认为，日本的通信基础设施已在世界领先，然而各公共部门利用信息技术的进程发展缓慢。通过执行该战略，日本的信息技术将真正实现使全体国民的生活更加便利。

战略名称“i-Japan”当中的 i 代表两个意思。一个 i 是指象用水和空气那样的应用信息技术 (inclusion)。另一个 i 是指创新 (innovation)。该“i-Japan”战略是继本世纪初日本政府推出的“e-Japan”战略和“日本信息技术新改革战略”之后的后续发展蓝图，规划了日本全国至 2015 年的信息技术发展之路。

为了体现以人为本，创造使国民安心和有活力的社会，该战略有一个核心内容被称为“国民电子个人文件箱”。其目的是可以让国民自己管理自己的信息资料。即通过互联网安全可靠地完成工资支付等各种手续，对其进行综合管理，使国民享受到一站式的电子政务的服务。这一项目要求 2013 年完成。

日本政府希望，通过执行这一战略，将开拓支持日本中长期经济发展的新产业。日本政府已认识到，目前已进入到了将各种信息和业务通过互联网提供的“云计算”时代。作为信息技术的载体，要大力发展以绿色信息技术为代表的环境技术和智能交通系统等重大项目。

展望世界各国，近一两年纷纷推出了新的信息技术战略。美国奥巴马政府注重各种智能系统和先进通信技术的发展。英国布朗政府也推出了新的信息技术战略。欧洲各国在“框架 7”基础上，信息技术得到蓬勃发展。近年来在达沃斯世界经济论坛上，日本的全球信息技术排名远落后于北欧各国，今年仅仅排在第世界 17 位。对此，日本的有识之士指出，在日本的都会和地方、大企业和中小企业、勇于创新的人与我行我素的人之间，隔开他们的数字鸿沟在不断扩大。特别是，日本与世界在行政、医疗、教育上应用信息技术的差距也在扩大。不甘如此落后的日本政府 2009 年补充拨发了 1 万亿日元预算，用于信息技术的发展。日本政府清楚地认识到，人才是发展信息技术的第一要务。该战略除了提出了培养信息技术人才的具体目标之外，还明确规定，在日本政府层面，首次设立了首席信息技术长官 (CIO，副首相级) 的职位。该 CIO 将监督日本信息技术战略的执行，提高各级领导和具体执行人员对于在行政、医疗和教育的电子化上的认识，推进以国民利用信息技术的便利性为首要战略的新的信息技术计划的落实。

“网络工商”运营将与公安联网

来源：北京晨报

监管平台即将投入使用 专为虚拟财产维权

1.7亿人在网络游戏世界中消费，国内每年有几十亿虚拟货币交易，当游戏中的“宝石”真能换成几十万元的人民币时，现实中的“贼”瞄准了虚拟世界，行骗、欺诈、纠纷等一样不少地接踵而至。昨天，工商、专家、消协等各方人士聚集一堂，研讨“网游”维权。记者获悉，北京工商网络交易监管平台即将投入使用，“网络工商”能全程监控交易过程，届时虚拟的消费环境也会有实实在在的证据留存。

处理网络投诉最麻烦

石景山工商分局从2008年开始，对受理的网络游戏投诉进行跟踪分析，发现投诉类型主要表现为：游戏玩家被游戏供应商封账号、设备丢失、不能正常上网游戏、不退已经缴纳的游戏费、账号被盗用等导致消费者损失。该局副局长高德友告诉记者，游戏物品被盗投诉处理最麻烦。“游戏玩家将获得的精良装备在现实生活中高价出售，并成为赖以谋生的手段，比如《天龙八部》中八九级的宝石在现实生活中可以折合人民币几十万元，普通的宝石也要上千元，一旦物品丢失，对玩家的打击非常大。”

今后可调取交易记录

“保护虚拟财产是未来网络安全和法制建设的趋势。”目前工商部门已经着手开发网络交易监管平台，将“网络工商”深入到虚拟交易中维权执法。据石景山工商分局消保科科长屈向东介绍，平台设在各个工商分局，将与网络运营商端口对接，交易纠纷发生时，工商部门能调取交易全程记录，在解决取证难的同时，也能相对准确地判定当事人责任。

游戏平台与公安联网

工商总局制定的《网络商品交易及有关服务行为管理暂行办法》和文化部制定的《网络游戏管理暂行办法》分别于今年7月1日和8月1日实施，两部规章中都明确提出“实名制”。特别是后者，还增加了虚拟货币交易服务不得为未成年人提供服务、网游企业应要求玩家使用有效身份证进行实名注册并保存用户信息等。

“《办法》实施后，对于实名制的落实和未成年人保护，网游运营商不能再推卸责任。”高德友明确表示，根据谁获利、谁尽责的原则，运营商应督促游戏参与者实名注册。记者从游戏运营商方面了解到，多个游戏平台已经与公安部联网，玩家上线注册即可实时查询身份。

■专家建言

网络交易进消保体系

《消费者权益保护法》规定消费者是“为生活”需要购买商品和接受服务的自然人，造成工商部门在调解网络游戏消费争议时无法可依。网络游戏玩家是否属于消费者，还需要在法律层面上有

明确的界定。与会专家纷纷建议在修改“消法”时，将网络交易也纳入消保体系。

印度禁售黑名单一网打尽 25 家中企

来源：cnbeta

“印度市场残酷也要去做。”今年 5 月，中兴通讯执行副总裁何士友就印度出口问题曾这样慷慨陈词。两个月后，中兴在内的 25 家中国设备制造企业被印度政府列入“黑名单”。印度《经济时报》披露，印度政府刚刚制定了一份中国和以色列电信设备制造商的禁运名单，在新的网络安全标准实施前，这些厂商将被暂时禁止向印度移动运营商提供设备。该名单由印度情报局制定，共涉及 26 家公司，包括联想、华为、中兴、日海通讯、UT 斯达康、通宇通讯、国人通信、迈普通信等 25 家国内设备厂商，以及以色列电信设备制造商 Com verse。

华为、中兴官方对此均不予回应。据称，中兴今日将召开专门会议应对印度被禁事宜。

450 份订单没着落

印度《经济时报》称，自 2010 年 2 月以来，印度移动运营商已经与这 26 家公司签订了 450 份订单，总值超过 20 亿美元，但这些订单均未交付。目前已经交付的 27 份订单都是与爱立信、诺基亚西门子通信公司以及阿尔卡特朗讯等西方厂商签订的。

据称，印度电信部之所以对这 26 家公司发出暂时禁令，是因为该部门尚未部署必要的手段来监控完整的电信设备供应链，也无法对网络安全进行审查，因此无法对从中国和以色列 OEM 厂商那里进口的电信设备的安全性进行评估。

印度政府此前曾表示，不会针对某个特定国家的电信设备发布进口禁令。印度通信部长派洛特还特地澄清，印度方面并未实施任何禁令，只要能证实无安全隐患，就可以进口。但这份名单显然与此前的表态相悖。

印度通信部在一份内部文件中表示：“根据情报局关于进口电信设备的反应和提案，出于安全原因，不推荐使用中国 OEM 厂商和一家以色列企业的设备。情报局特别强调，不推荐进口中国 OEM 厂商的产品，除非通信部认为对方在供应链中采取的安全措施足够充分。”

印度市场遭遇封锁对中兴华为负面影响极大。相关数据显示，2009 年，中兴全球收入中有 10.10% 来自印度；而印度也是华为在亚太最重要的海外市场。在华为上一财年的全球营收中，印度市场贡献了大约 14 亿美元，比前年增加了一倍以上。

凯基证券之前预计，今年中兴通讯约有 10%-15% 的营业收入来自印度市场；在印度 3G 牌照发放后，印度市场对公司的贡献则有望占到总营收的 20% 以上。但目前来看，不能太过乐观。

里昂更预测，“黑名单”将对中兴今年的收入有 7% 的负面影响，将其目标价由 37.1 港元大降至 22 港元，评级降至“跑输大市”。

“我们没有安装间谍软件”。

印度安全部门坚持认为，中国设备商可能在设备中嵌入间谍技术，从而对国家安全造成威胁。

“我们检查过是否有可能在交换机或在软件中装间谍装置，结果发现我们没可能在其中装间谍软件。”中兴通讯印度公司主席 D.K.G hosh 指出，“印度政府也同意我们的看法，表示‘确实没有在你的设备或者软件中发现间谍软件。’但是出于安全考虑还是要展开安全审查。”

中兴给本报发来的邮件称，“我们愿意按照要求参加并有足够信心通过所有的测试。而在此之前，我们希望能够得到与其他厂家一样的公平待遇。”

为了缓解印度方面的猜疑，华为派驻印度的工作人员现在流行取印度名、着印度服装。华为副总裁姚卫民也取了“拉杰夫(R ajeev)”作为自己的印度名。华为甚至提出，愿意披露其网络系统的源代码，以向印度政府表明，其设备

不会带来安全威胁。

目前，华为印度员工总数已有 5000 多人，并已在班加罗尔建立研发中心。有消息称，华为即将投资 3 亿美元至 5 亿美元，在印度第四大城市金奈附近 修建一座电信设备制造厂，以化解印度方面的安全顾虑。

中兴则向本报透露，公司将进一步加大对印度市场的投入，引进新的生产设备，在原有的投资基础上扩大生产，为 3G 网络建设做好准备。

印度今年 5 月刚刚拍出 3G 牌照，国内设备厂商显然不愿意错过这样的大规模建网机会。中兴通讯执行副总裁 何 士 友 透露，印度市场在为中兴通讯贡献毛利率不到 20%，为中兴通讯全球市场最低，2009 年中兴通讯总利润率为 33%。但何士友强调“印度市场残酷也要去 做。”

“毛利率不高，并非问题所在，庞大的市场空间决定了印度成为全球所有设备供应商的战略市场。”中兴通讯印度公司主席 D.K.G hosh 说。

中国设备商无一通过印度“安全审查”

事实上，在“黑名单”出炉前，印度对我国通信厂商已经接连发难。

去年 11 月，印度政府要求设备商不要从中国公司购买安装在敏感的边境地区的设备。其所谓敏感地区包括印度与中国、孟加拉、缅甸和巴基斯坦接壤的 边境地区。

一个月后，印度政府以存在“安全风险”为由，禁止从中国进口手机，并对华为和中兴通讯等企业生产的同步数字传输设备(SD H)征收反倾销税--其中对华为 SD H 设备征收 50%的临时反倾销税，对中兴通讯和烽火通信的征收比例则高达 236%。

印度国有电信运营商 BSN L 更对华为三次毁约，单方面取消了华为获得的总额 40 亿美元的设备采购订单，分别转给法印合资公司阿尔卡特-IT I 公司和爱立信公司。

今年 5 月，华为和中兴参与印度北区和东区项目的竞标权被剥夺。BSN L 董事长库尔迪普·戈雅尔表示：“与中国厂商的设备相比，西欧厂商的设备确实昂贵，这是不争的事实。但政府指示我们，不得订购中国厂商的设备，尤其是重点 区域内的项目。”

商务部新闻发言人姚坚称，印度有关部门出台的有关电信设备进口安全审查的政策影响到了中国企业，主要是华为和中兴，订单额高达 50 亿美元(约合 人民币 338.8 亿)，而这些订单都是中印企业事先已经签署的订单。

据商务部了解，到目前为止，还没有一家中国企业的产品通过印度政府要求的所谓“安全审查”。

对于印度市场目前是否已经完全对国内设备企业封锁，华为中兴未予回应。

“这已经不是企业与企业之间的问题，而上升到国与国之间。”消息人士透露，商务部已经在与各厂商密切沟通，酝酿统一措施以应对。

韩国总统府等 5 家网站受到黑客攻击

来源：国际在线

国际在线报道：韩国通信委员会 7 号晚透露，包括韩国总统府青瓦台以及外交通商部网站在内的 5 家网站当天受到黑客攻击，但目前尚没有造成重大影响。具体情况，我们来连线国际在线驻韩国记者张玲。张玲，你好。这次网站受黑客攻击的情况怎样？为我们介绍一下。

记者：是这样的。韩国通信委员会 7 号晚介绍说，受到攻击的 5 家网站分别韩国总统府青瓦台网站、韩国外交通商部网站、韩国主要门户网站 NAVER，以及韩国外汇银行和韩国农协银行的网站。攻击发生在韩国当地时间下午 6 点钟左右，与去年 7 月发生的黑客攻击韩国政府网站方式相同，本次黑客采取的攻击方式仍是“大规模分布式拒绝服务”，但攻击的烈度并不高。目前韩国通信委员会专业人士正在分析黑客攻击的来源地。

大规模分布式拒绝服务（DDoS），是指通过感染病毒的电脑向某一特定的目标计算机服务器发动密集式的“拒绝服务”要求，借以把目标计算机的网络资源及系统资源耗尽。主持人。

主持人：我们记得，去年 7 月 7 号起的连续三天，韩国总统府青瓦台、国防部等主要政府部门和银行网站遭到大规模分布式拒绝服务攻击，给韩国带来了严重的影响。那么，这次的黑客攻击从时间上看只是巧合吗？黑客以同样的攻击方式入侵成功，是否说明韩国网络系统存在着一定的安全隐患呢？

记者：是的，从时间上看，两次黑客攻击的时间相隔一年，难免让人产生联想。但是韩国通信委员会目前尚无任何评论，只是表示在就黑客攻击事件进行调查。

2009 年 7 月，包括韩国总统府、韩国国会、韩国国防部、韩国国家情报院等在内的网站以及一些门户网站和商业银行网站先后受到大规模分布式拒绝服务的黑客攻击，导致 20 多家网站瘫痪。此外韩国大量个人电脑先后染上病毒。这一事件给韩国造成了严重的影响。当时，韩国国内舆论也对韩国网络安全的脆弱性提出了猛烈的批评。根据韩国事后的调查，主要怀疑目标还是指向朝鲜，认为是朝鲜通过第三国向韩国的网站发起了黑客攻击。

应该说，韩国是目前在世界上网络用户比例最高的国家之一，约有三分之二的韩国人每天都使用互联网。韩国网络的系统还是非常稳定和安全的。去年 7 月的黑客攻击事件发生后，韩国国防部随即决定成立网络司令部，以提高韩国的网络作战能力，应对网络攻击的威胁并在遭受攻击后实施反击。按照计划，今年 6 月该网络司令部投入运行。此外呢，韩国和美国在打击网络恐怖主义领域也进一步加强了合作并开展联合反黑客演习。

个人隐私成社交网站牟利工具

来源：中国证券报

昨天，中国社会科学院在京发布了《新媒体蓝皮书：中国新媒体发展报告（2010）》。蓝皮书认为，社交网络是中国互联网 2009 年的热点，但是社交网站也容易引发的个人信息安全问题，不容忽视。

蓝皮书认为，通过社交网站，商业公司不但可以收集用户的手机号、MSN 账号等普通信息，还可以通过分析网民发布的博客、帖子、同学群体等，推测出用户的消费倾向（节俭还是奢侈）、个人婚姻情况（单身还是离婚）、工作情况（是否有跳槽意向）等涉及隐私的信息。目前社交网站的隐私泄露、用户个人的安全意识不强等非技术性的因素，已经成为商业公司收集、利用网民隐私的重要来源。网民在社交网站注册个人资料之后，很容易遭遇手机号泄露、MSN 和邮箱账号密码被盗用等安全风险，而利用各种方式骗取网民个人资料用以牟利，已经成为社交网站利润的重要来源。

病毒播报

一种针对 MSN 和 Windows Live 的新威胁已出现

来源：cnbeta

根据安全厂商 G Data 的警告，一种针对 MSN Messenger 和 Windows Live Messenger 的新威胁已经出现。该公司研究发现连接到这两个服务的垃圾邮件和钓鱼网站呈爆发趋势，并且大多以虚假的好友请求出现。安全厂商 Trusteer 说他们已经掌握了一种恶意软件攻击，它可以通过创造虚假的银行登录页面来窃取用户的账号进行转账。该公司提醒英国的银行用户注意这种威胁，它可以通过网站和垃圾邮件中的附件进行传播。

与此同时，赛门铁克公司也发现了一种针对国防承包商的攻击，方式包括黑掉某承包商公司网站来向另一承包商发动恶意软件攻击。这种攻击的灵巧性和复杂性特别值得关注。

另一方面，本周安全部长 Baroness 在 2010 伦敦国土安全会议上称，网络安全和信息保障对于英国经济发展至关重要，并承诺政府将会与私人团体在制定和执行网络安全政策方面开展更密切的合作。

51kantv 盗 CNTV 世界杯视频 病毒悄然利用

来源：赛迪网

近日有些用户求助，发现桌面上有个 51kantv 的图标。经过分析会发现，其中一部分是某些共享软件捆绑安装的播放器插件，但同时发现开始有病毒伪装成 51kantv 模样。病毒除生成一个 51kantv 的图标在桌面，还会弹出广告。另发现，网民在线看世界杯相关视频时，会安装这个 51kantv 插件。

据反映，很多用户是在找世界杯直播地址的时候被安装 51kantv 插件。经了解，原来不少个人网站也要借世界杯赚流量，他们想到一招，是从 CNTV 偷流量，盗播 CNTV 的数据源，需要安装 51kantv 插件。

不明真相的网民若发现自己的桌面多了个 51kantv，不妨去找 C:\Program Files\szPlayer 这个目录，这里面提供了 51kantv 卸载程序。卸载这个东西后，就会影响在电脑上看世界杯。

好在目前假冒 51kavtv 来传播的病毒尚不多见。病毒伪装成 51kantv，在桌面创建异常图标，这和以前遇到的很多桌面图标病毒类似。51kantv 的实现手段是通过篡改注册表新生成的 51kantv 病毒图标，手动操作注册表非常繁琐，所以世界杯期间找球赛直播地址，要非常小心，推荐各位还是用大的门户网站或 cntv 看直播吧。小网站的球赛直播尽量不要去，避免无意中被木马入侵。

正常的 51kantv 文件是无病毒的，如果不喜欢这个东西，可以用资源管理器打开 C:\Program Files\szPlayer 目录，运行其中的卸载程序。

最近非常流行的病毒都有一个共同特征：在桌面生成莫名其妙的桌面快捷方式、篡改浏览器主页、弹出广告。如果用户计算机出现上述奇怪的现象，需要首先考虑是否中招。

网民热议新版红楼梦 黑客借机传病毒

来源：计世网

新版《红楼梦》一经开播，即在网民中引起热议，“新版红楼梦”立刻成为互联网的搜索热词。可牛免费杀毒安全中心发现，大量“新红楼梦”相关网站被挂马或植入病毒，网友上网搜索新红楼梦时，电脑安全将面临着严峻的考验。

新版中李少红采用了其擅长的唯美、空灵风格，充满了《聊斋》般的鬼魅气息。这让不少喜欢李少红影片的人再一次大饱眼福。尽管网上对新版《红楼梦》质疑不断，但是丝毫不影响他们下载收藏的热情。据悉，80%以上的网友不愿在电视上慢慢更新，而选择上网下载“新版红楼梦全集”。然而令许多网友苦恼的是，只要在网上下载影片就无法避免木马的威胁。近日，网友“墨夏”在搜索“新红楼梦全集下载”时，无意点击了一个网页，电脑速度开始变慢，总是会弹出广告消息对话框，桌面上还出现了无法删除的图标。

可牛免费杀毒安全专家表示，每逢新片上映必定引来黑客关注。黑客会借“新红楼梦”爆火之际进行大面积挂马攻击。不少恶意电影网站还会以“新版红楼梦全集观看”等信息诱骗用户下载被捆绑了木马病毒的“专用播放器”。据了解，借“专用播放器”传毒危害最严重的是——快播伪装者木马。该木马不仅会盗取账号、窃取隐私，还会感染系统内所有的可执行文件（exe 文件），非常难以清除，即使重装系统，木马也会借被感染的可执行文件“死灰复燃”。安全专家表示，网友只需开启使用可牛免费杀毒进行全盘扫描，即可彻底清除“快播伪装者”。

在此，可牛免费杀毒安全专家提醒影迷在网上寻找片源时，应开启可牛免费杀毒的实时保护和浏览器保护功能，谨防网页挂马攻击；及时进行系统漏洞修复，并经常使用高效的可牛双引擎查杀功能对系统进行扫描，不给病毒木马可乘之机。

微软称对 Windows 新漏洞 PC 安全展开调查

来源：赛迪网

7 月 7 日消息，据外国媒体报道，微软星期二称，它正在对有关新的 Windows 安全漏洞可能破坏运行老版本 Windows 操作系统的 PC 的安全的报道展开调查。

安全公司 Secunia 在其网站上发表的公告中称，这个安全漏洞是由于 Windows XP 和 Windows 2000 中的一项功能的边界错误引起的。如果利用这个安全漏洞，就能够执行恶意代码。这家安全公司把这个安全漏洞列为“中等严重”的安全漏洞。

微软部门经理 Jerry Bryant 在声明中说，微软正在对 Windows 2000 和 Windows XP 中存在安全漏洞的新的公开的说法展开调查。微软到目前为止还不知道任何利用这个安全漏洞实施的攻击。他在

声明中使用了微软的标准语言，说微软将采取适当的行动，这包括作为补丁星期二的一部分发布一个补丁或者发布一个计划外的补丁。

淘宝秒杀器暗藏木马病毒 买家网购需谨慎

来源：长江网

7 月 7 日消息，可牛免费杀毒安全中心接到大量淘宝用户求助，称因使用了某款“淘宝秒杀器”而导致电脑中毒，淘宝账号被盗。据悉，大部分“淘宝秒杀器”非但不能提升秒杀几率，还捆绑有木马，导致买家财产受到损失。

据了解，淘宝秒杀是淘宝商家促销抢购的一种手段。让所有买家在同一时间抢购一些价格超低的商品，整个购物过程基本在 1 秒钟内完成。由于竞争过于激烈，许多淘宝玩家无法及时抢购到心仪的商品，于是淘宝秒杀器应运而生，在百度上随便一搜就会出现大量淘宝秒杀器下载的面页。

最近，淘友小丽连续参加了淘宝网举办的 1 元秒杀比亚迪、宝马等大规模的秒杀活动，并在相关网站购买了一度被淘宝网封杀过的“秒杀器”。然而当输入淘宝账号、密码后，不仅没有实现秒杀功能，账号、密码也被盗了，可谓血本无归。

安全专家介绍，“淘宝秒杀器”属于作弊软件，都是非正规软件厂商（甚至个人）制作，极易被黑客利用。黑客在淘宝秒杀器中捆绑流氓软件或是木马病毒，网民一不小心就中了圈套，轻则电脑被安装了无法清除流氓插件，造成桌面图标无法删除等棘手问题，重则直接被植入远程控制、盗号木马，个人隐私、账户尽在黑客掌握之中。

安全专家提醒广大淘宝买家不要轻信“淘宝秒杀器”。如果在淘宝秒杀过程中不慎点击安装过，请立即进行全面清扫、全盘扫描，保证系统中的木马病毒被及时清理干净。

产业动态

MySQL 开发者上诉欧盟批准甲骨文收购 Sun 决定

来源：互联网

MySQL 联合开发者蒙蒂·维登纽斯(Monty Widenius)周五向欧洲法院上诉了欧盟委员会批准甲骨文收购 Sun 交易的决定。

Sun 2008 年收购了 MySQL。甲骨文 2009 年与 Sun 达成收购协议，并于今年 1 月 27 日完成了收购交易。欧盟委员会 1 月 21 日批准甲骨文收购 Sun 的交易。

维登纽斯的上诉对甲骨文收购 Sun 的交易不会产生任何实质性影响，但会向欧盟委员会施加压力，提高决策过程的透明度。

在对甲骨文收购 Sun 的交易进行调查期间，欧盟委员会曾发表异议声明，担心交易会打压数据库市场上的竞争。MySQL 是三大数据库厂商甲骨文、IBM 和微软的竞争对手之一。欧盟委员会最终决定采信甲骨文确保数据库市场竞争的承诺。甲骨文和 Sun 承诺采取一系列措施，但这一承诺并不具备法律约束力。俄罗斯反垄断机构则要求甲骨文和 Sun 首先采取补救措施，然后才会批准收购交易。

IBM 斥资 4 亿美元收购安全软件厂商 BigFix

来源：新浪科技

据国外媒体报道，IBM 已与安全软件公司 BigFix 达成收购协议。

据知情人士透露，该协议的收购价格约为 4 亿美元。IBM 于周四发表声明称，该公司不会公布协议内容。BigFix 的软件能够即时检测出不符合企业规定的设备，并推荐补丁。

IBM CEO 山姆·帕米沙诺(Sam Palmisano)表示，计划未来五年投入 200 亿美元用于收购。IBM 5 月份曾表示，软件是该公司利润最高的业务，到 2015 年，软件收入将会占到公司总收益的一半。2003 年以来，IBM 软件部门已经完成约 60 起收购。该协议预计于本季度完成。

BigFix 有 200 名员工和 700 家客户，其中包括太阳信托银行(SunTrust Bank)。

Gartner：今年全球云服务市场将达 680 亿美元

来源：人民邮电报

本报讯 全球技术研究和咨询公司 Gartner 指出，2010 年全球云服务收入预计将达到 683 亿美元，与 2009 年 586 亿美元的收入相比增长 16.6%。预计该行业到 2014 年收入将达到 1488 亿美元，呈现出强劲的增长势头。Gartner 研究副总裁 BenPring 表示：“我们看到云计算和云服务在企业中的应用正在加速增长，随着技术提供商开始挖掘利用这个不断增长的商业机会，供应方面也日益活跃。应用部署的规模越来越大，几千席装机量的交易已经十分常见。IT 经理开始用战略性的眼光评估云服务部署，企业开始考虑在一个云服务普及的时代将实施怎样的 IT 运营。这在一年之前是非常罕见的。”

Gartner 预计在未来 5 年内，企业在软件即服务 (SaaS)、平台即服务 (PaaS) 和基础架构即服务 (IaaS) 上的累计花费将达 1120 亿美元。

由于大型内部 IT 团队管理的复杂、定制化的和高成本的解决方案所带来的运营挑战越来越大，这使得云计算变得越来越重要，云计算在应对这些挑战方面的优势将更加突显，将吸引所有类型的企业用户。

从地域上来看，北美和欧洲市场是最大的市场，同时其它地区也呈现增长趋势，但在未来 5 年内，其它地区的增长尚不会动摇成熟市场的地位。

2009 年美国在全球云服务市场中所占的比例为 60%，2010 年将为 58%，到 2014 年，随着其它国家和地区开始更多地采用云服务，这个比例将进一步降低到 50%。2010 年西欧市场在云服务市场所占的比例预计为 23.8%，日本将占 10%。到 2014 年，英国所占的比例预计为 29%，而日本预计为 12%。

从行业方面看，金融服务和制造业是最大也是最早采用云服务的行业。通信和高科技行业对云服务也有大量需求。此外，公共领域显然也对云服务的潜力以及占有整体市场份额颇感兴趣。

中移动“扣费门”引发计费系统漏洞之争

来源：每日经济新闻

各地频繁出现消费者无故被乱扣话费的现象，将中国移动推向了风口浪尖。日前，央视曝光了海南移动因为不规则分割计费导致消费者话费乱扣现象，让运营商计费系统的缺陷暴露于公众面前。据央视报道，黄生精是中国移动海南分公司的手机用户，前不久在查询话费详单时他偶然发现：仅 2 月份的几天时间里，他尾号为 6499 的手机就被多扣了 8 分钟的通话费 2.32 元。

查询了话费详单后黄先生发现，7 个被多收了话费的电话都有一个共同点，那就是每个电话都

被电信运营商分割计费。一个漫游主叫电话，时长是7分59秒，原本应该按8分钟计费，但是，在被分割成5分48秒和2分12秒后，计费时长却变成了9分钟。

针对上述事件，中国移动海南分公司此前承认：发生多收话费的事实系电话交换机计费出现差错造成；超长话单分割计价符合规定，系按漫游当地的标准即每5分钟分割一次。

不过，据央视报道，黄先生的这7个被分割计费的电话也并没有严格按照每5分钟分割计费。一个总时长为50分32秒的通话，如果按5分钟分割计费应该形成10个5分钟和一个32秒的通话计费记录，应为51分钟的话费。然而，话费详单却显示，这次通话被分割成了7个5分钟、1个5分10秒、2个5分零1秒和1个23秒的11个计费话单，计费时长变成了54分钟。

遭遇类似问题的不止黄先生一人。北京华泰律师事务所律师谭光权此前就针对中移动计费差错事件将中移动告上了北京东城区法院。据谭光权介绍，因爱人要出国，在2008年5月7日以他的名义在中国移动公主坟营业厅办理了国际漫游业务，在此期间，双方很少打电话，一般都是发短信，然而在2008年5月13日17时17分16秒时，在其爱人的详单上显示手机号打过谭光权手机号，并且通话时间长达30分22秒（即通话从17时17分16秒-17时47分38秒，总共费用是650元人民币）。但是在谭光权的通信详单上则显示在上述时间，没有接到其爱人的电话，并且在以上时间段内，谭光权还接了两个电话。谭光权指出，该时间并没有收到爱人的来电，而是另一个号码A，然而中国移动辩称A号码就是谭光权爱人使用的。

谭光权对《每日经济新闻》透露，为了调查该事件，他又尝试找了多张移动的卡尝试国际漫游业务，也发现了同样的问题。“近期，我也会针对该事件再次起诉中国移动，其国际漫游计费存在漏洞。”

移动员工写博反击

针对上述事件，中国移动研究院的博客栏目中，一位署名为葛长伟的“关于央视曝光的几起计费差错的分析”博客引发了网友的关注。

在这篇博客中，博主称，这些问题虽然都叫“计费差错”，但其实跟计费系统没有关系，问题根源基本都出在网络设备上。正如任何硬件都避免不了故障、任何软件都避免不了BUG一样，任何运营商的网络都不可能完全杜绝此类问题的出现。

一位移动内部人士在接受《每日经济新闻》采访时表示，碎单与话单分割是完全不同的两个问题，一个是设备差错引发的，一个是运营商设定的。而央视却将碎单问题嫁接成了运营商的话单分割问题，以此暗指运营商不择手段乱收费。

据业内人士透露，目前运营商采取话单分割，主要是为了避免用户恶意欠费，因为每年运营商支付恶意透支的金额就高达几十亿。

上述移动内部人士介绍，为了避免恶意欠费，运营商确实会将一次通话切割成多条话单，这个标准一般是半小时，即1800秒。碎单是指一条短时间的通话因设备方面原因断裂成N条。对于海南为何按照每5分钟分割一次，他表示，各地的规定也不太一样。据《每日经济新闻》了解，目前

浙江、福建移动均采用 1800 秒的分割标准。

该人士指出，央视曝光的案例，达不到话单切割的标准，是碎单问题，而碎单问题根源在网络设备上。

据《每日经济新闻》了解，由于中国移动各地运营商采用的网络设备不统一，所以也造成了网络设备在一定程度上会出现一些系统不协调、不兼容的情况。

“超短话单是最为严重的碎单问题，目前运营商采取的措施有两个：一是删除 3 秒以内的超短话单；二是合并时间连续的话单。”上述移动内部人士表示，删除超短话单很容易实现，但合并连续话单却很难实现，且就算实现了，效果也不理想。合并话单的功能只有在所有碎单都在同一个文件时才能发挥作用，其他情况下都无法实现，这就导致碎单问题还是会体现在用户账单上。除此之外，参数配置的问题也是运营商出现差错的原因。由于用户选择多种套餐，各种套餐数据或许存在冲突，也会出现暂时的错误，但是，只要发现问题，修改参数就可以马上解决了。

针对谭光权所指的国际漫游问题，据中国移动内部人士透露，目前国际漫游业务都是由外国运营商负责将账单反馈给中国移动，对于外国运营商如何设定计费，中国移动也并不知情。

该人士指出，运营商无论开展什么业务，都离不开计费系统的支持。上亿的通话单，经过数据处理，工作量也非常大，出现小概率的错误也难以避免。目前各省市均采用不同的计费系统，这也增加了运营商计费的复杂性。

据中国电信内部人士表示，运营商计费工作是非常海量的，加上这几年计费系统越来越复杂，难免会有一些问题。电信在承接 C 网之初，也有些错误计费，运营商都在努力改正，出现错漏确实是技术原因。

业内呼吁加强计费监管

工业和信息化部网站关于电信服务质量的通告显示，今年一季度工信部以及各地电信用户申诉受理机构，关于电信服务的申诉超过了 1.9 万人次，40%以上都是收费方面的申诉，中国移动以 4566 人次申诉量，成为被投诉收费问题最多的电信运营商。

中消协的一份投诉分析报告显示，今年一季度，移动电话和电信的投诉已经位居投诉量第二。

对此，中消协律师团团长邱宝昌在接受《每日经济新闻》采访时表示，运营商属于垄断行业，由于信息的不对称，计费的数据掌握在运营商手里，运营商既是运动员，又是裁判员，这在一定的程度上损害了消费者的知情权和公平交易权。

“对于像通信这样的垄断行业，政府应该加强第三方的监管工作，对于违规行为，给予惩罚措施。”邱宝昌表示。

针对此事件，中国移动对外表示，中国移动已在第一时间展开内部调查，并将对外公布调查结果。对客户计费确有误差的，中国移动将按照“话费误差，双倍返还”的承诺，对客户进行双倍返还。

微软向俄安全机关开放 Windows 7 源代码

来源：互联网

据《俄罗斯新闻报》报道，为了更好地向俄罗斯国家机关出售软件，美国微软公司同意与俄安全部门分享微软 Windows 7 操作系统原始代码和 Office 2010 等软件。

微软公司代表普里亚尼什尼科夫称，他们与隶属俄罗斯通讯与大众传媒部信息保护系统研究中心的“地图册”科技中心签署了一份补充协议。

普里亚尼什尼科夫介绍说，“地图册”中心可为微软最新产品设置带密码的防护系统，为这些软件开通通向国家机构的路径。对俄罗斯方面来说，最重要的是确信微软软件能够保证在国家机构的使用符合安全部门的要求。

目前，国家订单为微软公司带来俄罗斯市场大约 10% 的销售额。

全球最大 BT 网站曝安全漏洞

来源：互联网

7 月 9 日消息 据外电媒体报道，知情人士透露，全球最大 BT 网站海盗湾(Pirate Bay)服务器存在安全漏洞，导致 400 多万用户的个人信息被泄露。

该外电消息称，海盗湾因服务器存在漏洞被黑客攻击，同时黑客表示已可入侵用户信息的数据库。

阿根廷黑客查·卢索(Ch Russo)，他和另外两名同事发现了多个 SQL 注入漏洞，允许黑客访问海盗湾的用户数据库。之后，黑客可以创建、删除、修改或查看所有用户的信息，包括用户名、电子邮件、用户上传的种子，以及正在下载的用户数量和名称等。

卢索和他的同事已经成功侵入数据库，并提出了截屏。卢索表示，他们并未删除或修改数据库中的数据，但承认曾短暂想过是否将这些数据出售给美国唱片协会或美国电影协会等部门。

最后，卢索及其同事并未出售这些数据，只是把安全漏洞公之于众，旨在提醒用户他们的个人信息并不安全。

显然，海盗湾对该安全漏洞十分重视，因为网站目前已经无法正常访问，页面提示：“网站升级，数据库正在备份，将很快恢复正常。”

技术前沿

Win 7 SP1 包含升级版系统激活技术

来源：驱动之家

作为 Windows 7 的第一个服务升级包，SP1 不仅完善了性能，还加强了对盗版的防御，设置了重重屏障阻止黑客们非法破解 Windows 激活机制。Windows 7 SP1 将默认采用一种升级版的系统激活技术，不过这一技术并不是首次出现，微软早在今年年初就曾提供给 Windows 7 用户下载。

专为 Windows 7 开发的升级版 Windows 激活技术可以检测 70 多个已知的或是潜在的激活破解程序，帮助用户确定安装的 Windows 7 是否为正版，而且它还保证了关键系统文件的完整无损，更好地保护用户的安全。

除了通过 Windows Update 自动升级推送（KB971033）之外，微软还在 Windows 正版网站和下载中心上提供升级版 Windows 激活技术的下载。

微软已经在上月末向首要测试人员提供了 Windows 7 SP1 的 Beta 版本，并将在本月底公开发布。测试人员表示，Windows 7 SP1 Build 7601.16562.100603-1800 中已经包括 KB971033，也就是说系统默认安装了升级版 Windows 激活技术。毫无疑问，正式版中同样会包括这个“破解杀手”。

传美国国家安全局开发新系统防御网络攻击

来源：新浪科技

北京时间 7 月 8 日上午消息，据国外媒体今日报道，消息人士透露，美国国家安全局正在开发一个全新的安全系统，希望借此防御针对美国关键基础设施发动的网络攻击。

消息人士表示，该系统将对电网和核电站等重要基础设施的运营企业和政府机构进行监测，一旦电脑网络内的传感器探测到有网络攻击的迹象，便会激活相应的活动。

据悉，雷神公司(Raytheon)已经获得了该项目的一期订单，总值为 1 亿美元。

美国国家安全局和雷神公司均拒绝对此置评。

欧空局拟建造“末日方舟”备世界末日

来源：搜狐 it

据国外媒体报道，欧空局目前正在制定一项“末日方舟”月球信息库计划，以防人类遭遇毁灭性的大灾难后，可以重新在再生和延续。如果地球上发生宇宙小行星碰撞或者核战争爆发等灭顶之灾，那么“末日方舟”将自动被激活，帮助幸存下来的人类重新繁衍和建设新家园。

六月份，科学家在法国斯特拉斯堡（Strasbourg）开会讨论建设“末日方舟”月球信息库的可能性及实施方法。该信息库将成为在地球灾难中幸存下来的人类提供远程信息供给帮助。

在这个“末日方舟”月球信息库上所储存的基本信息包括：DNA 序列、金属冶炼方法、及植物种植方法等。在大灾难来临之前，科学家会在月球地面以下建设合适的储藏地窖，而“末日方舟”信息硬盘就将存放在这个地窖中。在人类灭绝以前，会在地球上放置数个受良好保护的信息接收器，如果不幸所有的接收器也在大灾难中被摧毁，“末日方舟”会不间断的发送信息，直到幸存的人类重新制造接收器接收完毕信息为止。

为防止大灾难之后的地球不再适合人类生存这一更为恶劣的情况发生，科学家还计划向月球地窖中存放诸如微生物、动物胚胎、职务种子等天然物质。另外，在这个地窖中或许还会存放一些各国博物馆中多余的文物。

另外，为了探测活的有机体是否可以在月球上生存，科学家计划未来十年内首先在月球上实施郁金香种植试验。欧空局研究部门首席科学家伯纳德·弗英（Bernard Foing）宣称，欧空局将在 2012 年或 2015 年开始在月球上种植第一批郁金香或拟南芥（arabidopsis）。

科学家之所以选择郁金香作为第一批在月球上种植的实验性植物，其主要原因在于郁金香的拥有极强的生存能力，并可以经过冷冻、长时间运输后，在恶劣条件下存活。科学家计划利用郁金香、海藻、密闭的人造大气环境、及经化学物质改良后的月球土壤建设出基本的生态系统。

而第一批种植郁金香的实验将在混合有模拟地球大气层气体的透明生物圈中进行。科学家计划通过腐烂植物释放出的 CO₂ 养活海藻，而海藻在光和作用下，会生成人类生命所必须的氧气。

最初在月球上建设的“末日方舟”月球信息库将由机器人管理，并通过无线电和地球指挥中心保持数据传输。另外，科学家还计划在本世纪末之前在月球上完成第一个人类生存基站建设。

鉴于目前月球上存在冷热极端气温、辐射及真空等可能对“末日方舟”月球信息库造成损伤的大自然环境因素，科学家认为将该信息库储存在月球岩石层以下的地表中才会相对安全。并且科学家将该信息库运行的主要动力来源设计为太阳能。

科学家预计，将在 2020 年以前将第一批实验性信息库送往月球，这批实验性信息库的使用寿命被初定为 30 年。随后将在 2035 年以前将完整版的信息库送往月球。完整版的信息库中所容载的信息将包括汉语、阿拉伯语、英语、法语、俄语、西班牙语等不同语种版本。该信息库将和地球上建造的 4000 余座“大灾难避难所”相链接。在这些“大灾难避难所”中将为大灾难中幸免于难的人们

储存一定量的食物、淡水、及信息接收器。幸存下来的人们可以根据接收到的信息完成家园重建及种性繁衍的任务。

黑客攻防

微软证实黑客已破解 Windows7 无限使用

来源：互联网

据国外媒体报道，有黑客日前表示，已经发现一种可以绕过 Windows7 激活程序的方法，从而无限期使用 Windows7。

一般情况下，用户可以安装试用 windows7 操作系统 30 天，之后必须要按照激活流程进行激活然后才能正常使用，否则 windows7 操作系统会在超过限定期后向用户不断发出提示，虽然不再采取之前颇受争议的“黑屏”方式。但近日被人在网上公开了绕开 windows7 激活机制而无限期使用 windows7 操作系统的方法，这样即使超过微软规定的期限也不会有任何警告提示出现。

微软一位发言人称：“我们已经意识到可绕过 windows7 激活程序的问题，我们正处理此事。”另外还表示，普通用户如果使用黑客发布的破解程序有可能会感染恶意软件的危险，微软目前正在研究对策以屏蔽此类技术。

网易回应黑客攻击事件：员工电脑被入侵所致

来源：cnbeta

针对旗下四大邮箱遭黑客入侵一事，网易向腾讯科技发来声明，称事故是因负责静态页面文件更新工作的员工电脑被入侵，导致 ftp 账号密码泄露所致。目前，该事件对网易邮箱服务并未造成任何影响。今日下午，有大量网友在论坛爆料称，网易的 163 邮箱、126 邮箱、yeah 和 188 邮箱等全都遭遇到了黑客的入侵，黑客在网易邮箱服务器上留言文本都一个是 hack.txt，文档中写着“hacked by hacker just a joke”，意思是“黑客成功入侵，只是个玩笑。”

网易方面表示，黑客在 ftp 服务 器上传了 6 个 txt 文件，并未能侵入数据库等核心系统，也未造成任何用户资料、邮件的泄露。

关于黑客入侵网易邮箱事件的声明

2010 年 7 月 3 日下午，有论坛陆续贴出黑客入侵网易邮箱的消息，随后有网站对事件进行了转载。为免外界误传造成不必要的猜测，网易邮件中心就此事发布声明如下：

网易邮件中心工作人员在 14:00 发现黑客入侵，立即进行了紧急处理，事件对网易邮箱服务并未造成任何影响。据查，事故起因因为负责静态页面文件更新工作的员工电脑被入侵，导致 ftp 账号密码泄露，黑客在对应 ftp 服务器上传了 6 个 txt 文件，并未能侵入数据库等核心系统，也未造成任何用户资料、邮件的泄露。上述文件为静态文本文件，且仅在网易服务器存在了很短时间，不会对信息安全及邮箱服务造成影响。

网易邮件中心一直把用户利益及使用体验放在第一位，发现各类安全问题均会第一时间处理解决，感谢广大用户及各界 12 年来对网易邮箱的关心和爱护，网易邮件中心会进一步加强信息安全管理，保障用户通信安全，一如既往地为一位邮箱用户提供安全优质的电子邮件服务！

苹果 iTunes 和 App Store 遭黑客攻击

来源：新浪

据国外媒体报道，多家科技博客报道称，一些 iTunes 用户的帐户遭到黑客攻击，其中的账户余额被用于购买苹果 App Store 应用商店中的应用。

周日上午，瘾科技报道称，由名为 Thuat Nguyen 的开发者开发的电子书应用销售量大增。在 App Store 的电子书频道内，按营收计算，销售量前 50 的电子书中有 42 个都是由 Thuat Nguyen 开发的。多名用户报告称，“多达数百美元的资金在不知情的情况下被用于购买这些电子书”。

另一家科技博客 TNW Apple 则报道称，这一事件并不局限在某一名开发者开发的应用中，并且全球各地的用户都受到影响。该博客援引一名用户的说法称：“昨天我的信用卡公司联系我，称我的贷记卡出现了可疑的活动。最终确定，我的信用卡在 iTunes 中出现了超过 10 笔额度在 40 至 50 美元的交易，交易总额达到 558 美元。”

苹果目前尚未对此做出回应。苹果近期正遭遇麻烦，其最新推出的 iPhone 4 手机出现了信号接收问题，而苹果对于该问题的回应则遭到外界的讽刺。

黑客攻破 iTunes 网站操纵用户账户购买软件

来源：赛迪网

7 月 6 日消息，有报道称，一位名为 **Thuat Nguyen** 的越南流氓软件开发人员攻破了苹果 iTunes 在线商店的账户，修改了苹果应用程序商店的图书类别，人为提高他自己的图书应用程序的评级和销售排名。**Next Web** 和 **Engadget** 这两个网站星期日报道称，**Nguyen** 的应用程序在 iTunes 应用程序商店图书部分按销售收入排名前 50 位的图书中占了 42 个。

一个用户在 **MacRumors** 网站论坛上抱怨说，他看到许多无法解释的 iTunes 商店的收费，总数超过了 500 美元。两位 iPhone 应用程序开发人员 **Alex Brie** 和 **Patrick Thomson** 注意到了这个越南人的图书排名上升的可疑情况。他们收到了自己的应用程序排名下降和 **Nguyen** 的应用程序排名上升的报警。

有两个用户指出，在 **Nguyen** 的应用程序排名上升的同时，他们的 iTunes 账户被黑了，并且代表他们购买了这些应用程序。这些被黑的账户最多用 200 美元购买 **Nguyen** 的应用程序。

苹果对于这个黑客攻击没有发表官方的声明。但是，**Nguyen** 的应用程序现在已经从苹果商店消失了。**Alex Brie** 在自己的博客中指出，他向苹果报告了这个问题。苹果的一个团队正在对这个问题进行调查。

淘宝专家：关注网络账户链安全

来源：深圳特区报

网上逗留的时间越长，就会留下越多的“足迹”，如果稍不小心，这些足迹就会出卖你。支付宝网络专家表示，当前网上信息尤其是网络账户链的安全尚未得到人们重视，不少用户因此蒙受损失，提醒消费者要高度关注网络账户链安全。

专家分析，一方面很多网民在多个网站注册了账户，但出于方便的考虑，这些账户多数雷同。但另一方面，这些无意中形成的网络账户链却非常脆弱；账户链中的一个环节遭到利用，都可能让一个看似无懈可击的安全账户被轻而易举入侵。

如何才能保管好自己的网络帐户安全呢？支付宝安全专家建议：首先，支付宝账户有双重密码——登录密码和支付密码，两个密码一定要设置不同。其次，对于一些不熟悉的网站，填写信息一定要谨慎。因为在越多的网站注册，则账户信息泄露的风险越大，用户应善于保护自己。第三，在不同网站的注册信息要保持变化，例如账号与密码、安全提问的回答等不要千篇一律。此外，信息不保存在上网的电脑中，尤其是账户与密码切记不可记在同一个文件内，实在记不住就记在手写小本子上，因为一旦电脑中木马后容易导致网络账户被“一锅端”。还有，涉及到网上资金的账户和密

码（如支付宝账号、网银账号）更是要高度重视，建议用与其他账户关联度较小的邮箱或手机号注册。

男子散布木马病毒盗取银行卡号诈骗 40 万

来源：红网

长沙人彭某，家住汽车南站附近，虽然才初中学历，却是附近居民人人羡慕的电脑高手。才 23 岁的他已经为自己买了两辆奥迪和丰田的二手高级轿车，还有一个穿金戴银的漂亮女友。这些让邻居们羡慕不已，可邻居们不知道的是，外表帅气的彭某竟然是个“网银大盗”，他的这些钱全是利用电脑木马病毒，盗取银行卡号后诈骗得来的。

上周，雨花区法院开庭审理了这起信用卡诈骗案件。彭某两年半来通过诈骗所得金额高达 402400 元，法官判处其有期徒刑 6 年零 6 个月，并处罚金人民币 20 万元。

U 盘里他人的银行卡信息有 13 页

彭某从小不爱读书，初中毕业后，除了打工，他把其他时间都花在了电脑上。2006 年 10 月的一天，没钱用的彭某无意中得知有的木马病毒可以盗取市民的账户、密码及身份证信息。于是，他抱着试一试的心态，利用网络传播病毒，入侵了一位市民田某的电脑，获取其银行卡信息后，再利用木马程序远程操作，将田某卡中的十万元钱转走。谨慎的彭某还特地跑到湖北开了个账户转钱，躲避追查。这成为了彭某的“第一桶金”。

第一次成功后，彭某便开始苦心钻研木马程序。2008 年初，彭某觉得一个个入侵太麻烦、耗时间，钱也来得慢，为了一次性获得大量信息，彭某开始雇佣他人来帮忙。彭某雇人将其设置好的木马程序放在任意的网站上，他人登录这些网站后再去进行网上交易时，彭某就可以远程窃取其银行卡号的信息，然后他再通过网上下载他人的身份证号，用生日来套取密码。在庭上，彭某表示，正是因为许多市民习惯用生日做银行卡密码，他才这么容易得逞。

2008 年底，彭某觉得以前迂回的方法来钱还是不够快，他便在网上租了一个 IP 地址，并从网上购得一些木马病毒，将病毒放在租用的服务器上。之后，彭某便装作普通市民，窜至长沙几家银行大厅，利用银行的自助电脑下载并安装木马病毒。市民在使用该自助电脑后，木马病毒就会自动将用户的身份证号、银行卡账号、密码等信息转送到彭某租用的服务器上。被捕时，彭某 U 盘中银行卡号等信息长达 13 页。

买了两辆二手高级轿车与不少首饰

2 年半诈骗 40 多万，彭某从打工仔摇身一变成了大老板，他不仅给自己购买了两辆奥迪和丰田的二手轿车，还交了个漂亮的女朋友，为其添置了不少首饰。

法庭上的彭某平头，高个子，看上去很聪明，回答法官提问时条理清楚、口齿伶俐，若不是戴

上手铐，谁也不会相信这个年纪轻轻的小伙子居然诈骗了这么多钱。

当法官要他陈述作案经过时，彭某想了想，只说出了一部分，“太多了，不记得，很多都只有几百块钱，印象最深的是转走了林某的 100500 元，因为我就是拿着这笔钱买的二手奥迪车。”彭某说，就在去年 2 月份，他在网吧上网时查到一个账号和密码信息、手机号，发现那张卡里有十多万。接着他又抱着试一试的态度，用银行卡密码套手机密码，谁知竟套开了。他赶紧去办了张假身份证，前往株洲某银行，用手头上的信息将这笔钱取了出来，拿着钱跑到湖北买了车。

[法官提醒]

网银卡不要存大量现金

彭某因犯信用卡诈骗罪，现已判刑，部分赃款已被追回。法官表示，关于银行卡的盗窃、诈骗案件时有发生，他们都是利用市民的一些生活习惯与一时大意钻了空子，彭某就是其中的典型。法官提醒，要预防银行卡信息被盗用，市民切记不要用生日做密码，在外上网时尽量不要使用网上银行交易，防止木马病毒盗取信息，家用电脑也要定期进行病毒查杀。同时，开通网上银行的卡不要长期存放大量现金，宁愿麻烦些，用多少就临时存多少最保险。

Skype 安全协议遭破解

来源：互联网

美国科技博客 TechCrunch 表示，有人宣称已利用反向工程技术破解 Skype 专有加密协议。若该消息得到证实，这意味着 Skype 悉心构筑的安全措施将变得无效。

Skype 系统被入侵后发生的情况尚不得而知，但最坏的情况是，黑客可以利用反向工程获知更多信息，并知道如何利用这些信息。需要澄清一点，在问题得到确认之前还无需担忧。

Skype 表示，目前根本不存在安全问题，加密协议被破解事件正处在调查当中。

海外来风

Tax credits result in phishing attacks

来源: Infosecurity 杂志

Web browser security firm, Trusteer, has warned that the end of July deadline for filing/updating tax credits is resulting in a raft of phishing emails from hackers.

Coupled with the fact that the 31st of July is also an important date for the payment of income tax, Trusteer says that many parents will now be filing in the hope of an extra tax credit.

The danger now, says Trusteer, is that tax credit filers will click on unsolicited emails that look as though they might have been sent by HMRC, and in doing so, may end up infecting their home or office computers.

"Back in February we warned online banking users of phishing and malware infections stemming from emails offering internet users a tax refund. And given that such phishing emails are twice as successful as bank phishing attacks, cybercriminals have realised that an email with HMRC in its message header is a lot more attractive to recipients", said Mickey Boodaei, Trusteer's CEO.

In addition, he says, it's likely that hackers will exploit this interest in tax credits and tax refunds generally, with a rash of infected emails and/or messages with links to infected websites.

"In a recent analysis by Trusteer of a UK specific botnet containing the details of over 10,000 people, we discovered that the botnet operators are actively looking for login information for the HMRC website, as the information found to have been collected by the criminals included HMRC logon credentials and passwords", he said.

"There are various tax and VAT-related scams that fraudsters can run against you once they have access to your HMRC login information", he added.

According to Trusteer, whose browser plug-in software is offered for free by a number of UK online banks, the Rapport software can report attack vectors to subscribing banks, as well as being capable of monitoring attack trends and informing banks of the main threats their customers are facing over time.

Boodaei says that tax credit and HMRC refund phishing emails dangle the 'carrot' of free cash at internet users, and persuade them to lower their normal credulity guard.

Then, when they see a choice of bank sites from the 'HMRC landing page', they click on the link and immediately start entering their bank and other personal details.

The net result of this is not, he says, a credit to the recipient's bank account, but usually a fraudulent

debit, or series of debits, that empty the account by cybercriminals.

税收抵免导致钓鱼攻击

来源: Infosecurity 杂志

——中国信息安全博士网翻译

Web 浏览器安全公司, Trusteer 发出警告: 截止七月底, 是申请/更新税积分的最后期限。小心黑客发送大量的钓鱼邮件。

同时七月三十一号也是纳税收入的重要日期。Trusteer 说: “现在很多家长希望抵免额外税收”。

Trusteer 说: “现在的危险是税收信贷档案库管理者, 点击看起来像来自于海关总署的邮件, 这样做, 最终可能感染其家中或办公室的计算机”。

“早在 2 月, 我们警告说, 网络钓鱼和恶意软件从互联网用户接收退税电子邮件感染银行用户。并且这种网络钓鱼电子邮件是钓鱼攻击成功的两倍, 网络犯罪分子已经意识到税务及海关总署的邮件里面的信息是非常吸引收件人”, 说米奇 Boodaei, Trusteer 的首席执行官。

此外, 他还说, 黑客很可能会利用银行用户感兴趣的税收抵免和一般退税, 与受感染的电子邮件或受感染网站连接信息在一起。

Trusteer 最近分析在英国僵尸网络其中包含了超过 10000 个人的资料。“我们发现那僵尸网络的经营者正在积极的寻找登录税务及海关总署网站信息。犯罪分子已经收集了包括税务及海关总署登录凭据和密码”, 他说。

他补充说: “有很多税和增值税有关的诈骗, 不法之徒可以针对你一旦登陆, 他们就可以访问您的税务及海关总署的资料”。

据 Trusteer, 银行可以订阅浏览器插件软件, 它是免费提供给英国网上银行的。Rapport 的软件可以报告攻击, 以及攻击的趋势, 并且可以随着时间通知银行, 他们的客户所面临的主要威胁。

Boodaei 说, 税收信贷和税务及海关总署退款钓鱼电子邮件就好比在互联网用户面前晃动着免费‘胡萝卜’, 并引诱他们降低防卫。

然后, 当他们看到一个网站‘税务及海关总署登陆页面’他们点击链接, 并立即开始输入自己的银行及其他个人资料。

这个结果对不对, 他说, 一个信用卡人的银行帐户, 通常是欺诈性扣款, 或扣款系列, 即通过网络罪犯盗取帐户的资金。

这个结果对不对, 他说, “网络犯罪分子通过欺诈性扣款或扣款系列, 盗取信用卡人帐户的资金”。

企业推荐

北京数字证书认证中心简介

北京数字证书认证中心（简称 BJCA）成立于 2001 年 2 月，是北京市国有资产经营公司控股的国有企业，也是首批获得工业与信息化部电子认证服务许可资质的电子认证服务商和具有国家涉密集成资质和信息安全服务安全工程类一级资质的信息安全服务商。

作为权威的电子认证服务机构，BJCA 遵照《中华人民共和国电子签名法》的要求和相关管理规定，向客户提供“政务通”、“信天行”等系列品牌的数字证书服务，旨在提供高品质信息安全服务，帮助用户创造安全可信的网络空间。

BJCA 遵循现代服务业的要求和电子认证服务的行业特点，在全国率先开展了以客户需求为导向的新型电子认证服务体系建设探索。BJCA 不断完善运营规范和服务体系建设，将服务宗旨落实到电子认证服务的各个环节，全面提升了客户价值。

BJCA 通过以客户为中心的新型电子认证服务体系、自主知识产权的应用软件产品和专业定制的安全解决方案，为电子政务、电子商务、企业信息化发展等领域的客户构建了安全、可靠的信任环境。

作为以技术为先导的现代服务企业和行业方向的引导者，BJCA 肩负起社会赋予的责任和使命，不仅参与行业规划，还承担行业标准制定和国家课题研究攻关。并当选为全国信息安全标准化技术委员会成员和中国 PKI 论坛理事单位，被指定为国家信息安全风险评估、信息安全管理体系建设试点技术支持单位。

作为专业的信息安全服务商，BJCA 拥有国内一流的信息安全专家和专业的安全服务队伍，紧跟信息安全领域发展动态，熟悉各种信息安全政策、标准、指南和要求，遵循“分域防护、深层防御；分级保护、动态防范”原则，根据客户信息系统生命周期的不同阶段的相应需求，利用科学的手段和方法，有效开展安全需求分析、安全风险评估；协助客户确定安全等级；制定安全策略；设计安全方案；组织实施安全建设或改造；协助客户制定安全管理制度；提供安全维护和应急响应服务；保障方便获取全方位、专业性、持续性和个性化的安全技术支持与服务。

奥运期间，BJCA 发挥技术优势，为涉及成功举办奥运和城市正常运行的重要信息系统提供安全保障，为平安奥运做出了贡献，受到北京市奥运会残奥会运行指挥部、北京市奥组委、北京市国资委等机构表彰。

经过几年的高速发展，通过营造良好的企业文化，提供广阔的发展空间，BJCA 建立了一支分布于产品设计、技术研发、工程实施、市场营销、经营管理和运行服务等岗位的 300 余人的员工

队伍，已经成为人才荟萃、朝气蓬勃的创新型高科技企业。BJCA 将继续践行“以人为本，追求卓越，求实创新，和谐共生”的企业理念，实现客户满意、企业发展、员工进步。

公司资质

电子认证服务许可证

国家信息安全测评信息安全服务资质（安全工程类一级）

北京市信息安全服务能力等级证书

涉及国家秘密的计算机信息系统集成资质证书（乙级）

涉及国家秘密的计算机信息系统集成资质证书（单项/软件开发）

人防信息系统建设保密项目设计（施工）资质（正本）

电子认证服务使用密码许可证

商用密码销售许可证

高新技术企业认定证书

软件企业认定证书

质量管理体系认证证书

中华人民共和国电信与信息服务业务经营许可证

高新技术企业

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:510698

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