

安全周报

中国信息安全博士网

十二月 第四期

二〇一〇年十二月二十四日
总第39期

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
- 高端访谈
- 企业推荐

第二届中国信息安全 人才培养与就业工作研讨暨交流会

2011年3月·北京

高端访谈下期预告：
专访中国科学院高能物理研究所计算中心许榕生先生

“云计算国家信息安全战略”举办
IBM将为北约司令部创建云计算系统

年底大回馈！
20篇文章发布
仅需888元

2011年1月24日前预订有效



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。

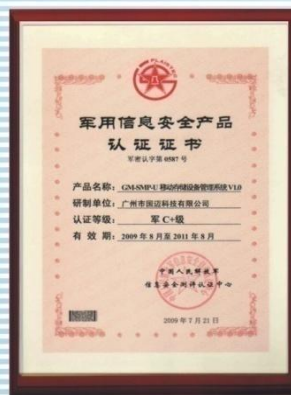
权威认证：



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



第二届中国信息安全 人才培养与就业工作研讨暨交流会

(北京 2011年03月26日)

北京
欢迎您！

指导单位： 教育部高教司
工业和信息化部信息安全协调司
国防科技工业局安全生产与保密司
教育部高等学校信息安全类专业教学指导委员会
全国信息技术人才培养工程

联合主办： 北京理工大学
中国传媒大学
北京邮电大学

协办单位： 北京电子科技学院
中央财经大学
北京信息科技大学
北京交通大学
宁夏大学

承办单位： 中国信息安全人才网
北京艾得威尔信息咨询中心
NSACE网络信息安全项目组

支持媒体： 中华英才网 赛迪网 CIO时代 天极网 e媒网 中国计算机安全网
计世网 中国软件网 中国IT实验室 电脑商情在线 中国经济和信息化
大学生就业网 信息网络安全 计算机安全 信息安全与技术 艾瑞网

会议主题： 新形势下信息技术与信息安全人才需求及就业。

届时，教育部、工业和信息化部领导，国防、军工、IT厂商、
欢迎各界用人单位踊跃报名

会务组：010-64126291 13661116129 刘 晴 张鹏飞

010-62658942 13263364585 陈继霞 李丽曼

电子邮箱：cis-rc@163.com meeting@nasce.org.cn

官方网站：

中国信息安全人才网
www.cis-rc.com

中国信息安全博士网
www.secdocor.com

教育部信息安全教指委官方网站
www.sec-edu.cn

第二届中国信息安全人才培养与就业工作 现场招聘会



第二届中国信息安全人才培养与就业工作研讨暨交流会将于2011年3月在北京隆重召开。本次会议将特邀相关主管部门领导和业界权威专家参加，并集聚了众多信息技术与信息安全人才培养教育机构、人才需求单位以及人才中介机构的众多负责人。

届时，教育部、工信部领导以及国防、军工、金融、银行、电力、证券、IT公司、信息安全厂商、科研院所等用人单位以及全国百余所设有信息技术、信息安全及信息对抗专业的高校师生将齐聚北京，展开一场盛况空前的大型人才招聘盛宴！

联合主办：北京理工大学 中国传媒大学 北京邮电大学

协办单位：北京电子科技学院 中央财经大学 北京信息科技大学

北京交通大学 宁夏大学

会议时间、地点

会议时间： 2011年03月26日

会议地点： 北京

信息技术与信息安全人才的盛会！火热报名中！望各企业积极踊跃参加，莫失良机！

(11月15日之前报名将享有报名优惠!!!)

会务组：010-64126291 13661116129 张鹏飞

电子邮箱：cis-rc@163.com

目录

高端访谈.....	8
高端访谈下期预告：中国科学院高能物理研究所计算中心研究员许榕生	8
学术会议.....	10
第二届中国信息安全人才培养与就业工作研讨暨交流会会议延期通知.....	10
“云计算国家信息安全战略”举办	11
物联网与智慧城市建设高峰论坛举行.....	12
政府之声.....	14
英特尔收购 McAfee 交易遭欧盟严格审查.....	14
印度开展各级政府网站安全审查 漏洞百出	15
IBM 将为北约司令部创建云计算系统.....	15
江西国企建立首席信息官专家库.....	16
工信部：中欧将推进未来互联网和 IPV6 合作.....	16
美国银行的逆袭:终止维基解密业务	17
中国数据泄露防护(DLP)呼唤标准出台	17
病毒播报.....	20
今年手机病毒预计超 2500 种.....	20
交易劫持型木马今年增长最快	21
恶评插件仍猖狂 网民票决坚定整治信心.....	21
产业动态.....	22
方正电脑与国民技术合力打造信息安全之盾	22
联想扬天首次全面预装定制版 360 软件	24
赛门铁克：杀毒免费是不公平的.....	25
美移动安全软件厂商 Lookout 融资 1950 万美元.....	28
摩托罗拉将收购云存储厂商 Zecter.....	29
百度诉 360 不正当竞争一审获赔 38.5 万元.....	30
谷歌搜索新增黑客报警功能.....	31
用友发布云计算战略实施第二次转型.....	31
微软助力企业启动云的力量.....	32
技术前沿.....	34
稳捷网络力推可信第二代 Web 安全新理念.....	34
全面解析 Web 应用防火墙的价值和优越性.....	36
黑客攻防.....	37
清华大学子网站遭黑客入侵并被植入黄色信息.....	37

调查显示：2010 年网络盗窃首超现实盗窃.....	38
警惕黑客 4 种手段攻击无线局域网	39
黑客袭击纽约旅游公司盗 11 万张信用卡信息.....	40
海外来风.....	41
Microsoft confirms IE flaw, not yet being exploited.....	41
企业推荐	43
北京智恒联盟科技有限公司	43

高端访谈

中国信息安全博士网作为中国信息安全行业的高端智库平台，一直在我国信息安全行业发展过程中贡献着自己的力量。作为信息安全博士网的“高端访谈”栏目，我们定期邀请信息安全行业内的顶尖级专家、学者、院士、重要行业用户、以及政府官员和产业精英，通过不同角度的深度剖析，为读者全面展示信息安全各方面、各层次的发展及问题。为行业发展、产业进步提供建议。将客户的相关文字、音频或视频文件放在中国信息安全博士网高端访谈栏目进行宣传。

高端访谈下期预告：中国科学院高能物理研究所计算中心研究员 许榕生



人物简介：

许榕生，男，中国互联网连接世界的推手、曾任国家计算机网络入侵防范中心首席科学家、联合国教科文组织网络工作组中国代表的成员。

1947 年出生，福建省莆田人。1970 年毕业于北京大学数学力学系，1981 年在中国科学院研究生院获硕士学位，1987 年在美国加州大学获博士学位。1993 年，在中国建起了第一条互联网专线，建立了中国第一个 Web 服务器，获得中国科技进步特等奖；1999 年，“黑客入侵防范软件”获中国科学院科技进步一等奖。

曾担任国家 973 网络安全体系研究的“信息获取与分析”子课题项目负责人及中科院知识创新工程重点项目“黑客入侵防范体系研究”的课题负责人。现继续承担网络与信息安全的若干国家研究课题。现任中国科学院高能物理研究所计算中心研究员、博士生导师兼中科院信息办专家组成员。出版著作《电子商务安全与保密》、《黑客攻击技术揭秘》等著作 8 部。

发表有关论文 50 余篇、著作四本。

主要从事：互联网网络工程及网络安全；通过对 TCP/IP 的协议分析，IP 层通讯的硬件化处理及应用层软件的编程加工，针对网络入侵防范的特殊需求，实现各种适合高速网下的网络安全工具的研究与开发等领域的研究工作。他是中国最早向大众传播和介绍互联网知识的人之一，

主持人：今天，我们这一期的“高端访谈”栏目，有幸邀请到了我国国家计算机网络入侵防范中心首席科学家。中国科学院高能物理研究所计算中心研究员、博士生导师兼中科院信息办专家组成员许榕生老师。您好许老师

主持人：首先，许老师，给大家打个招呼。

许老师：.....

主持人：我们知道，您目前正在研究网络入侵取证，请您系统的谈谈这方面的进展情况。

许老师：.....

主持人：计算机取证在近些年来发展很迅速，在今后计算机取证技术的发展和完善路径。您有什么好的见解？

许老师：.....

主持人：美国在网络战这方面比其他任何国家都要超前得多，准备措施比其他国家要充分，而且已经有过几次大的演练或者实战经验。那对于，我国的网络战，在紧急情况下，如何发挥我们自身的网络战对策？如何避免更多的损失？

许老师：.....

主持人：曾经有消息称：“关于您组建反黑客部队的事，当然这也只是误传。”能提出类似“团队”一意，从这些方面，能看的出，您对于研究网络安全方面的技术与人才培养是非常负责、非常重视的，那请您给我们讲讲，您在培养人才方面有哪些好的见解和要求呢？

许老师：.....

主持人：您认为我国信息安全发展方向是什么？国内外有什么好的沟通？

许老师：.....

主持人：今天对许老师的采访是很有意思，真是受益匪浅，很感谢许老师的做客。希望许老师能给我国信息安全方面做出更多的贡献。再次感谢许老师！~

这一期，我们中国信息安全博士网的“高端访谈”就到这里，我是润洁。下一期再见。

详情请登录：<http://www.secdactor.com/html/yingxiangtianxia/>

学术会议

第二届中国信息安全人才培养与就业工作研讨暨交流会会议延期 通知

来源：中国信息安全博士网

尊敬的领导、各位朋友：

大家好！

应各界朋友要求，“第二届中国信息安全人才培养与就业工作研讨暨交流会”会议将由 2010 年 12 月 19 日延期至 2011 年 3 月 26 日（周六）隆重举行，给各位朋友带来不便敬请您见谅！

如有建议及询问参加会议相关事宜请直接联系会务组或查看“中国信息安全博士网”、“中国信息安全人才网”有关本次会议的最新通知，我们将竭诚为您服务，期待与您的美好合作！

会务组联系方式：010-64126291

网站：www.secdactor.com www.cis-rc.com

此致

敬礼

第二届中国信息安全人才培养与就业工作研讨暨交流会组委会

2010-11-19

“云计算国家信息安全战略”举办

来源:中国软件网

12 月 18 日上午,由 CCF 主办的“‘云计算’时代的国家信息安全战略”专题论坛在北京翠宫饭店举行。IT 学术界和企业界的学者专家齐聚一堂,从技术、管理和产业几个方面共同探讨了‘云计算’时代的国家信息安全战略。



中科院软件所研究员、信息安全国家重点实验室主任 冯登国

中科院软件所研究员、信息安全国家重点实验室主任冯登国在会上表示,云计算是信息技术领域的一次巨大变革,它同时带来技术理念、产业发展和安全战略的变革。云计算的出现必然会对现有的安全体系造成一定冲击。

冯登国认为,目前,虽然云计算为用户提供了更廉价、更强大的计算能力,但云计算平台却无法识别用户计算任务的合法性。一旦云服务平台被攻击者控制、安全漏洞被利用或云用户身份被盗用,攻击者将可以利用云服务平台的庞大网络资源、用户身份资源、计算资源组织 DDOS 等类型的更大规模攻击。而由于云服务平台的动态特征,对于此类攻击将更难于确定和追踪,这使得基于云的安全攻击带来连串安全噩梦。

面临严峻的挑战,我们应从基础平台、关键技术、标准规范、监督管理等多方面进行变革,以适应云计算应用于发展的需要,冯登国说。

会上,清华大学计算机系教授、高性能技术研究所所长杨广文先生从技术角度深度分析了云数据中心的安全问题。杨广文说,目前“云”尚未出现一种确切的技术,因此任何系统的建立还是基于传统技术,根据企业自身的需求规划框架,实现安全策略。

“十二五”将开启云计算的时代,而云计算作为信息技术领域又一次重大变革,将对信息技术及社会进步的方方面面带来深远的影响,对我国而言,应尽量避免再次陷入高墙信息产业被国外垄断的被动局面。同时,云计算也是我国发展信息产业、缩小与美国等发达国家差距、掌握信息技术

发展主动权的重要机遇。

物联网与智慧城市建设高峰论坛举行

来源:科学时报

全球金融危机爆发以来,信息技术产业发展的竞争格局正处于深度调整中。面对新兴的物联网产业,只有审视所处的产业环境,深刻认识产业发展的特点、规律和矛盾,方能更好地推进物联网产业的持续发展。

近日,在由国脉物联网技术研究中心举行的“物联网与智慧城市建设高峰论坛”上,物联网规划与政策专家安筱鹏指出,当前中国物联网产业的发展,有三个主要矛盾需要解决,即物联网应用市场的碎片化需求与规模化供给的矛盾,物联网技术、产品、服务供给的分散化与客户需求一体化的矛盾,及物联网作为一个新兴产业,所必然面临的需求不成熟与技术不成熟的矛盾。

“只有深刻认识产业发展的特点、规律,及所面临的基本矛盾时,我们才能找到产业发展的方向,才能找到工作的重点,形成产业发展正确的思路。”安筱鹏说。

探索新商业模式

国际电信联盟在 2005 年物联网的报告中指出,物联网产业发展的挑战不仅仅在于技术问题,还在于市场的规模化应用。

一方面,规模化行业应用的不足,将成为制约物联网产业形成、核心关键技术突破和标准化的重大瓶颈,从而难以激发产业链各环节的参与和投入热情;另一方面,只有规模化供给才能降低成本,形成产业发展的良性机制,形成市场发展的动力。

安筱鹏表示,互联网、移动通信等传统通信业务在发展过程中,通信终端产品 and 应用服务具有标准化和规模化特征,因此每种终端和增值服务都会形成庞大的消费群体。而物联网应用由于要与具体行业需求相结合,因此其应用在很大程度上是分散化的,很难形成规模化的应用群体。

“物联网产业面对的是多个行业不同需求的、小规模的分细分市场,单一产品和服务在细分市场之间的可通用性和可移植性差,需求呈现碎片化特征。”安筱鹏说。

那么,物联网产业在发展过程中,该如何解决需求碎片化与规模化供给的矛盾呢?对此安筱鹏表示,应探索物联网产业发展的商业模式,将零散应用整合为规模效应,从而实现产业化发展的突破。

“信息产业发展的实践表明,只有建立在成功的商业模式创新基础上的技术创新,才有产业化的坚实基础,只有依托技术创新的商业模式创新,才具有更强大的竞争力。”安筱鹏说。

国脉物联网技术研究中心在此次论坛上独家发布的《中国物联网行业景气及企业家信心指数调查报告》也指出,物联网商业模式的创新与物联网的产业发展阶段密切相关,如何让好的服务与设

施顺畅地向客户传递，如何使客户以最经济、最便捷的方式享受服务，都需要有良好的商业模式作引导。

中国的机会

“目前我国的物联网产业发展仍处于各自发展的起步阶段，从物联网产业的供应来看，我们不仅仅缺乏技术、产品和标准，更缺乏能够整合产业上下游资源集成商，这也将影响产业发展的进程。”安筱鹏说。

在安筱鹏看来，用户看重的不是具体的技术细节，而是集设备、网络、运营、服务于一体的集成化解决方案。这就需要服务提供方具备产业链上下游的资源整合能力。

2008 年，IBM 提出“智慧地球”的战略理念。这一理念是 IBM 继电子商务、“随需而变”等理念之后的新提法，旨在解决系统之系统所面临的复杂问题，与其长期积累的信息技术研发优势，及其在行业应用的系统综合集成能力和客户关系方面的优势，均形成了较好的吻合。

而从国内现状看，提供物联网服务的各方，尚不具备构建这种面向超复杂系统一体化解决方案的实力。

针对国内的现状，安筱鹏指出，应积极培育信息系统的综合集成能力，抢占产业发展新的制高点。

“我们应加快培育和发展集信息化规划、咨询设计、项目实施、系统运维和专业培训为一体的信息技术服务业，支持有条件的企业开展信息技术服务业务剥离重组，推动信息技术及相关服务的社会化、专业化、规模化和市场化。并抓住全球技术和业务流程外包快速发展的机遇，加快外包业务的规模化、高端化。”安筱鹏说。

此外，物联网的感知、网络、应用每一个层面，都可以提供多种技术选择，这种技术的不确定性也引发了相关标准、商业模式、产业组织形态等方面的一系列问题。

在安筱鹏看来，中国具有大国大市场的优势，如果能充分利用好这一优势，加强物联网技术攻关，在一些需求迫切、且市场前景广阔的行业开展应用试点示范，并培育好产业链的整合能力，则将在很大程度上决定我国物联网产业自主发展的能力和水平。

政府之声

英特尔收购 McAfee 交易遭欧盟严格审查

来源:CNET 科技资讯网

12 月 20 日国际报道 英特尔以 76.8 亿美元收购安全软件厂商 McAfee 的计划遭遇欧盟的严格审查,这将至少导致这一收购交易被推迟。

消息人士透露,在对英特尔收购 McAfee 交易初步评估期间,欧盟委员会曾私下表示担忧,这可能导致该交易的审批期限延长。

上述消息人士称,欧盟审批的重点是,英特尔将在处理器芯片中集成安全技术的意向。欧盟担心,如果 McAfee 在使用这些功能方面享有特权,竞争对手将因此处于劣势。

据悉,自英特尔 11 月末正式向欧盟提交审批材料后,欧盟委员会已经多次征询其他安全软件公司的意见。欧盟关注的问题之一是,英特尔如何在芯片中集成安全功能,是否会只向 McAfee 的安全软件开发部分功能。

文档显示,欧盟还担心,英特尔是否会使用 McAfee 的技术判断哪些软件能够在其处理器芯片上运行,利用名为“sleeper agent”的功能显示 McAfee 软件广告窗口,或以牺牲竞争对手软件的性能为代价,为 McAfee 软件预留处理能力。

英特尔发言人未就此置评。英特尔之前曾发表声明称,该公司已经提供相关资料,供监管机构审批用。

英特尔投资者关系副总裁凯文·塞勒斯(Kevin Sellers)说,“我们相信,英特尔和 McAfee 整合对于安全领域的突破性创新是非常重要的,收购交易完成后,我们将发布更详细的产品计划和策略。”

塞勒斯称,英特尔预计这一交易将于 2011 年上半年完成,但表示目前没有消息需要对外公布。英特尔 10 月中曾表示,预计这一交易将于今年年底或明年初完成。

英特尔的全球 PC 处理器市场份额约为 80%,而且已经就反垄断问题与欧盟交过锋。英特尔正在上诉欧盟委员会 2009 年开出的 14.5 亿美元罚单。

英特尔曾表示,该公司没有直接在其芯片中整合 McAfee 产品,使其他安全软件公司处于不利地位的计划,计划为芯片增添能提高所有安全软件,而非仅仅 McAfee 软件性能的电路。

根据欧盟的法律法规,欧盟委员会需要在明年 1 月 12 日就英特尔收购 McAfee 交易做出裁定,或对这一交易进行深入调查。英特尔可以提出修正措施,减轻欧盟的担忧。

印度开展各级政府网站安全审查 漏洞百出

来源: 环球时报

印度媒体称, 由于印度联邦中央调查局 (CBI) 近日遭到黑客攻击, 印度对其所有部级部门的网站和各级政府网站开展了安全审查, 结果发现其中约有 280 个网站容易受到黑客攻击, 许多“至关重要”的政府机构网站也位列其中, 还包括印度海军和印度国家档案馆等部门的网站。

《印度时报》23 日报道称, 印度的网络安全审查发现许多政府网站都面临网络入侵的风险, 而一些印度中央机构网站因为由私人机构负责代理, 更是漏洞百出。

报道指出, 上述网站由于未能定期接受安全审查, 故而面临极高的网络入侵风险。还有消息人士透露, 此前遭到黑客攻击的中央调查局网站从 2007 年起, 就 再也未曾接受过安全审查。不过这起黑客攻击案件也让印度开始警醒, 此后, 印度各级政府网站都被要求严格遵循印度国家信息中心所制定的网络安全准则和规范。同时印度信息产业和工信部还要求印度国家信息中心增加人力, 以保证各级政府网站服务器的安全。

IBM 将为北约司令部创建云计算系统

来源: 赛迪网

12 月 23 日消息, 据国外媒体报道, 全球最大的计算机服务器供应商 IBM 将为 NATO(北大西洋 公约组织, 简称北约)创建云计算系统。IBM 该项目负责人 E.J.Herold 称, 该云计算系统使 NATO 能更快地收集和分析信息, 如阿富汗军事情报。该系统将首先应用于位于弗吉尼亚诺福克的北约司令部, 之后会扩展到其他军事指挥机构。

IBM 为 NATO 其他部门和 28 个成员国建立了类似项目, 已经在 NATO 站稳脚跟。

据悉, IBM 将以私有云模式管理诺福克司令部的军事情报。私有云模式让用户在自己的安全系统上把信息存入服务器, 云计算系统将协助北约司令部把通过雷达系统、照相机或红外线图像所获信息收集到一起。

江西国企建立首席信息官专家库

来源:大江网-信息日报

记者 20 日从省国资委获悉,为建立和完善 CIO(首席信息官)制度建设,发挥专家人才的智慧作用,我省决定建立“江西省国资监管及企业信息化专家库”。

据悉,CIO 入库专家可以是高等院校、科研机构、机关、事业、企业、社会团体等单位的专家学者、业务骨干。CIO 专家建库常年进行,今年首期入库专家推荐材料须于 12 月 30 日前报送省国资委。

工信部: 中欧将推进未来互联网和 IPV6 合作

来源:新华网

北京 12 月 21 日电,工业和信息化部副部长杨学山 21 日表示,中欧将积极推进在未来互联网和下一代互联网协议 IPV6 方面的合作,并将联合发布宣言落实 IPV6 合作。

杨学山是在北京举行的第三次中欧经贸高层对话上作出上述表示的。

IP 地址即互联网地址,是用来唯一标识互联网中计算机的逻辑地址,具有唯一性,相当于生活中家庭地址的门牌号码。IPv4 地址是目前正在广泛使用的 IP 协议,它采用 32 位地址长度,全球可用的 IPv4 地址只有大约 43 亿个,因此全球互联网必须过渡到下一代版本的 IP 地址协议即 IPv6 地址。

杨学山说,工业和信息化部 and 欧盟方面有多个合作机制和渠道,在中小企业、材料、汽车、电信、信息技术、信息化等领域进行不同层次交流。

杨学山介绍,在日前举行的第二次中欧信息技术、电信和信息化对话上,工信部和欧盟信息社会与媒体总司同意进一步拓宽和深化信息技术、电信和信息领域合作。双方将推荐中欧双方专家积极推进未来互联网和下一代互联网协议 IPV6 等方面合作,推动双方有关企业的首席信息官进行互访和交流,并共同探讨有关云计算的研究。

“在全球化深入发展大背景下,双方要进一步发挥中欧信息技术、电信和信息化对话机制的作用,在信息通讯技术创新、信息通讯基础设施构建、信息通讯技术应用、信息产业发展和网络信息安全保障方面进一步开展合作与交流。”杨学山说。

美国银行的逆袭:终止维基解密业务

来源:cnbeta

美国银行（Bank of America）上周五加入了由其他机构发起的封杀维基解密账户的行动。

美国银行正式发表声明表示，该银行已经加入有由万事达公司，PayPal 公司，Visa 欧洲和其他机构发起的封杀维基解密账户的行动。阿桑奇上月接受《福布斯》杂志访问时，曾表示将于明年初发放有关美国大型银行的密件，外界揣测“维基解密”的主要目标是美国银行。

美国银行发言人表示，这一决定是基于维基解密的行为已经涉及侵犯公司处理付款的内部政策。

维基解密随后在 Twitter 上呼吁其支持者尽快停止使用美国银行的一切服务。该网站还在一个社交媒体上公开表示，要求所有热爱自由的美国银行客户尽快关闭该银行的账号。

维基解密创始人（Julian Assange）朱利安阿桑格本周获得保释并前往英国一乡村房宅度圣诞。阿桑格上周五表示忧虑美国准备引渡及起诉他。

美国司法部长埃里克霍尔德（Eric Holder）表示，美国政府正在考虑以“间谍法”及其他法律控告维基解密以危害美国政府为目的发布政府敏感信息。但过往从未以“间谍法”控告出版媒体，故无先例可循。

中国数据泄露防护(DLP)呼唤标准出台

来源:网界网

众所周知，行业标准、技术标准和产品标准，对于高科技行业来说，具有战略制高点的意义。在国家“核高基”战略和信息安全等级保护制度的大背景下，出台数据安全和数据防泄露产品的标准，对于 DLP 行业的发展具备至关重要的作用。当前，由于标准缺失，中国数据泄露防护行业的发展处于深度困扰和迷茫状态中。为了改变这种现状，一部由中国人首创的数据泄露防护(DLP)标准，亟待相关部门制订出来。

一、为什么要制订数据泄露防护(DLP)标准？

1、数据泄露防护(DLP)具备国家信息安全的战略高度，必须由国家来牵头

政府部门掌握着大量重要甚至核心的机密，已成为各种窃密活动的重点目标。我党政机关和军工单位也是国家秘密非常集中的领域，一直是窃密与反窃密，渗透与反渗透的主战场。据国家有关部门统计，在全国泄密事件中，军工系统占有很大比例。境内外敌对势力和情报机构以我党政军机关和军工单位为主要目标的窃密活动更加突出，渗透与反渗透、窃密与反窃密的斗争更加激烈。由于一些单位涉密信息系统安全保障能力不够、管理不力，导致涉密信息系统泄密案件的比例逐年上升，安全保密形势非常严峻。因此严格按照涉密信息系统分级保护的要求，加强涉密信息系统建设

意义重大。

2、国外 DLP 产品的入侵有霸占中国数据安全市场的危险

自 2007 年以来,赛门铁克、麦咖啡、趋势科技等跨国信息安全巨头,纷纷收购数据泄露防护(DLP)公司、技术和产品,涉足推动数据泄露防护(DLP)领域,在全球推出以内容检测为核心技术、辅以身份认证和访问控制、日志审计等技术的 DLP 产品。于此同时,这些跨国巨头凭借其强大的资金实力和技术背景,其 DLP 产品如同洪水猛兽般向中国涌来,在中国广泛宣传,必将对中国信息安全产品市场造成强大的冲击。

信息安全产品的技术含量非常高,这就要求知识积累一定要充足,才能开发出有竞争力的产品。在中国信息安全市场,尤其在防火墙、防病毒及入侵检测方面,基本上是国外产品一边倒的局面。国内安全产品市场近八成高端用户的首选是国外产品。由于国内产品的技术水平相对于国外的同类产品还比较落后,产业化水平较低。而国内厂商整体上是技术模仿和重复投资的手段争夺区区几亿元的低端市场。

如果任由国外 DLP 厂商圈占和蚕食国内市场,那么在这个相对来说还比较新,国际国内都还有广阔发展前景的领域,必然又将像防火墙、防病毒及入侵检测市场那样,完全沦陷于跨国信息安全巨头的铁蹄之下。长此以往,中国信息安全市场将不再有中国信息安全厂商的生存之地,必将沦为别国厂商的附庸。

3、国内 DLP 正处于高速发展的成长期,需要建立相应成熟的软环境

目前中国信息安全市场已进入成长期,这一时期的特点为:市场增长率很高,需求高速增长,技术渐趋定型,行业竞争状况和用户特点比较明朗,顾客对产品的认知能力迅速提高,产品形成差别化趋势以满足顾客不同的需求,生产能力呈现不足;市场竞争逐渐形成,进入壁垒拔高,企业应付风险的能量得到增强,利润呈加速增长态势。

据权威机构调查数据显示,中国 2010 年数据泄露防护市场容量可达 10 亿元以上。而且也每年 30%的速度上升。其中,北京亿赛通公司的文档安全管理系统、

4、国内 DLP 产品走向国际市场

从全球信息安全发展的历程来看,基本是欧美国家走在前列,不论是防火墙、杀毒软件、IDS/IPS 等传统产品,还是近年来新兴的其他产品,基本都是由少数跨国信息安全巨头主宰着全球信息安全市场。众多发展中国家的信息安全厂家都是在学习和模仿这些巨头的技术,开发适合本地的对应产品,很少有发展中国家有独创产品领先于发达国家产品,并在全球市场推广开来的。

但是,这种局面很可能会有所改变。从传统的经济学理论来说,发展中国家有"后发优势",可以站在巨人的肩上,创造出全新的技术理论体系和产品。这一点在数据泄露防护领域已经有所体现。

北京亿赛通作为中国唯一一家具备开发数据泄露防护体系的信息安全厂商,从 2008 年首创以"透明加密"为核心的数据泄露防护体系。其中,关于文档安全管理系统的"透明加密技术"和针对服务器和数据库加密保护的"文档安全网关技术",在全球均属首创。亿赛通 DLP 体系完全不同于国际上

其他 DLP 产品, 具备开创性的独有优势。如果能进一步得到发展, 将很有可能开辟出一条全新的技术路线, 在全球信息安全领域中占据一席之地。

5、劣质产品充斥市场, 误导用户, 给用户带来损害

当前, 在中国数据泄露防护(DLP)市场上, 充斥着大量的不合格劣质产品。主要有两种表现: 一、部分加密软件功能简单, 性能低下, 运行非常不稳定, 漏洞很多, 完全满足不了电子文档和数据的加密需求; 二、有的信息安全产品主要功能是内网安全管理, 通过 OEM 集成了部分加密功能, 就打着加密软件的旗号, 愚弄和欺骗用户, 这部分产品在功能上就不完善, 完全属于不合格产品。

根据业内资深人士介绍, 作为成熟的文档加密和数据泄露防护产品, 从业者必须经过五年以上加密产品开发经验, 并且有客户终端实施超过 30 万以上。根据中国 ESN 调查机构的报告, 符合这一标准的加密软件厂商仅有北京亿赛通一家而已。

由于不良商家的不规范经营, 市场上产品鱼龙混杂, 概念混乱, 给用户选购产品带来极大的困扰。部分用户在实施不合格产品之后, 往往造成系统瘫痪, 信息保密形同虚设, 根本无法做到数据泄露防护。因此, 广大用户深感困扰, 纷纷呼吁相关部门制订出台相关标准。

二、数据泄露防护(DLP)产品标准的相关依据

制订数据泄露防护(DLP)标准, 其法律依据来自《中华人民共和国标准化法》, 同时还必须参照等级保护和分级保护的相关政策法规。

根据中华人民共和国标准化法的有关规定, "企业生产的产品没有国家标准和行业标准的, 应当制定企业标准, 作为组织主产的依据。企业的产品标准须报当地政府标准化行政主管部门和有关行政主管部门备案。已有国家标准或行业标准的, 国家鼓励企业制定严于国家标准或者行业标准的企业标准, 在企业内部适用。"就我国数据泄露防护(DLP)市场现状来看, 无论是 DLP 产品, 还是加密软件, 都还没有统一的国家标准。为此, 制订 DLP 产品的国家标准, 是当前关于 DLP 领域的重大事件。

1999 年国家发布并于 2001 年 1 月 1 日开始实施 GB17859《计算机信息系统安全保护等级划分准则》。2003 年, 中办、国办转发《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发〔2003〕27 号), 提出实行信息安全等级保护, 建立国家信息安全保障体系的明确要求。2004 年 9 月 17 日, 公安部、国家保密局、国家密码管理委员会办公室、国务院信息办下发了《关于信息安全等级保护工作的实施意见》, 明确了信息安全等级保护的重要意义、原则、基本内容、工作职责分工、要求和实施计划。2006 年 1 月 17 日, 四部门又下发了《信息安全等级保护管理办法(试行)》, 进一步确定职责分工, 明确了公安机关负责全面工作、国家保密工作部门负责涉密信息系统、国家密码管理部门负责密码工作、国务院信息办负责的管理职责和要求。涉及国家秘密的信息系统应当依据国家信息安全等级保护的基本要求, 按照国家保密工作部门涉密信息系统分级保护的管理规定和技术标准, 结合系统实际情况进行保护。

1997 年《中共中央关于加强新形势下保密工作的决定》明确了在新形势下保密工作的指导思想和基本任务, 提出要建立与《保密法》相配套的保密法规体系和执法体系, 建立现代化的保密技术

防范体系。中央保密委员会于 2004 年 12 月 23 日下发了《关于加强信息安全保障工作中保密管理若干意见》明确提出要建立健全涉密信息系统分级保护制度。2005 年 12 月 28 日, 国家保密局下发了《涉及国家秘密的信息系统分级保护管理办法》, 同时, 《保密法》修订草案也增加了网络安全保密管理的条款。随着《保密法》的贯彻实施, 国家已经基本形成了完善的保密法规体系。

三、DLP 产品标准的深远意义

数据泄露防护(DLP)标准的出台, 是一件利国利民的大事, 对于国家管理部门、产品生产厂商和用户都具有重要作用, 对于 DLP 行业的健康、可持续发展具有强大的推动作用。

有利于厂商研发生产标准化 DLP 产品, 使得市场规范化发展。

有利于用户产品选型、实施和测评, 选用优质产品保护数据安全

真正落实国家关于信息安全等级保护和分级保护政策

间接支持国家"核高基"战略实施

病毒播报

今年手机病毒预计超 2500 种

来源:解放日报

北京网秦天下科技有限公司日前发布了《2010 年中国大陆地区手机安全报告》。报告指出, 据网秦“云安全”数据分析中心统计: 截至 2010 年 11 月, 新增手机病毒 1513 个, 累计病毒数量达 2357 个。预计 2010 年手机病毒总数将超过 2500 种, 同比增长 193%, 累计感染手机 800 万部以上。我国广东地区以 21% 的感染比例居首位。北京、上海、福建、江苏等紧随其后。

手机病毒的种类经过不断扩展, 已经从原先较为简单的系统破坏、恶意扣费, 扩展到隐私窃取、金融盗号和窃听监控等方面。专家建议手机用户在网下载软件时, 要选择具有安全验证机制的正规手机软件下载网站, 切勿轻信“破解版”、“完美修正版”等经过二次加工的手机软件、手机游戏、歌曲、音乐、电子书等, 其中可能嵌入手机病毒; 还要不定期备份手机上的重要数据, 例如通讯录, 避免因感染病毒或手机丢失后数据的丢失或隐私泄露; 智能手机如需维修, 最好把 SIM 卡拔出来; 经常查一查话费清单, 看有无流量特别的情况。

交易劫持型木马今年增长最快

来源:京华时报

昨天,金山网络安全中心发布的《2010 年中国网络购物安全报告》显示,有超过 1 亿用户曾遭遇过网络购物的陷阱,带来直接经济损失将突破 150 亿元,其中专门针对网购的交易劫持型木马是今年增长最快的网络威胁。

据最新统计数据显示,除钓鱼网站外位居第二位的网络威胁是新型交易劫持木马,占有威胁的 16.8%,2010 年交易挟持类木马已经从最初的 1 个,发展为近千个不同种类的木马。

金山网络安全专家李铁军介绍,交易劫持型木马通过在正常的网络购物交易过程中给消费者电脑植入木马,一旦用户电脑被植入木马,这一用户之后所有正常的网购交易都会被劫持。用户付了货款,但店主收不到钱,这些货款被自动打入了木马控制着的账号。

恶评插件仍猖狂 网民票决坚定整治信心

来源: it168 网站

近日,北京市二中院对百度诉 360 将其百度工具栏和百度地址栏两款软件锁定为“恶评插件”进行了一审宣判,使得“恶评插件”再度成为公众关注焦点。

据了解,有些插件却具有恶意行为,如弹出广告、开后门等等。它们严重干扰了正常的网络秩序,使广大网络用户不胜其扰。瑞星称这些软件为“流氓软件”,金山称之为“恶意软件”,而 360 则称其为“恶评插件”。

这些程序共同的特征是未经用户许可强行潜伏到用户电脑中,而且此类程序无卸载程序,无法正常卸载和删除,强行删除后还会自动生成。不仅强迫用户接受阅读广告信息,还会搜集用户敏感信息并向外发送,甚至劫持用户的浏览器,诱导浏览含木马网站,严重影响了互联网的正常秩序。

据悉,“恶评插件”并非 360 公司自己评定,而是通过广大用户对一些软件进行评价和公正的投票,对一些较差的软件或插件,如广告程序、间谍软件、IE 插件等,进行评分和认定,并进而评出“恶评插件”。之后 360 安全卫士和 360 杀毒会对其进行标注和查杀。

显然,清理恶评插件,不仅有利于用户保护自己的信息安全,而且有利于用户对计算机的资源优化,因为这些过多的插件在侵害用户的信息安全的同时,还大量占用系统资源,造成计算机经常不稳定甚至无法使用。

但是,查杀这类软件却让 360 这类专业的互联网安全公司陷入了“无法可依”的“尴尬”境地。由于法律并没有对无论是“流氓软件”还是“恶意软件”抑或是“恶评软件”进行定义,往往让一些安全厂商由此遭受并不公正的诉讼。

比如,清理恶评插件是 360 安全卫士的核心功能,深受用户的喜欢,但也因此给 360 带来了多起诉讼--在百度起诉 360 之前的 2007 年 1 月,同样由北京市第二中级人民法院审理的阿里巴巴诉奇虎 360 将其雅虎助手列入“恶评软件”列表一案,以 360 败诉;而此次,百度诉 360 评为“恶评软件”一案,由于不被法律支持,360 在一审中依然没有胜诉。

由于没有相应法规的支持,360 杀毒与 360 卫士的木马清理功能无法对所有恶评插件进行全部查杀,因此也给用户带了诸多不便。但由于得到了广大用户的拥护与支持,因此,盈科律师事务所合伙人刘永斌律师分析认为,百度诉 360 的判罚结果,估计不会影响 360 继续为网民清理恶评插件的决心。

更有业界人士表示,查杀恶评插件如何规避风险,已是摆在比如 360 这类的互联网安全厂商面前的一道紧迫的命题。而 360 公司通过用户进行评定,并且在对一些恶评插件进行标注后由用户自己选择是卸载还是信任,无疑是一种较好的“网民票决”。

产业动态

方正电脑与国民技术合力打造信息安全之盾

来源:MSN 数码 IT

随着信息技术的高度发展,由终端设备及互联网所连接组成的异构世界变得越来越不可控,从而带来了更多的安全隐患,大到国家军事、政治等机密安全,小到如防范商业企业机密泄露、个人信息泄露等问题,使保证信息的安全性成为当务之急。2005 年 12 月,国家密码管理局颁布了《商用密码产品生产管理规定》(国家密码管理局公告第 5 号),其中,第四条规定,商用密码产品须由国家密码管理局指定的单位生产,其品种和型号须经国家密码管理局批准。由此可见,打造信息安全之盾对任何部门和行业来说都是一个不容忽视的安全战略问题。

从今年 4 月初开始,方正电脑与国民技术在 TCM 安全计算机领域进一步开展了深度的合作。在每台方正具备 TCM 芯片及应用的计算机上,将粘贴国民技术公司提供的 TCM 标贴。标贴上标明了国家密码管理局的认证号,这是国内 TCM 计算机第一次粘贴 TCM 认证标贴,是 PC 应用的 TCM 技术的标志,也表现了方正在 TCM 产业上的决心。此次合作更在产品功能上增加了更多安全要素,在整机产品中,方正电脑整合了 TCM 文件安全共享和 TCM 网络可信安全接入两大功能。

文件安全共享功能,支持用户在拥有 TCM 芯片的计算机群组中共享加密文档,而不具备 TCM 芯片的计算机以及没有通过 TCM 认证的计算机则无法解密文档。该方案无需服务器,不受限于局域网,

可实现更加方便快捷的安全文档共享。在政府、企业的办公环境中，该方案能够有效保护重要文件的扩散范围，防止泄密。

另一功能是 TCM 网络可信安全接入系统，它依赖于 TCM 芯片，可以为用户提供更加安全的接入认证方法。该系统由服务器端、客户端以及管理端三个部分构成：服务器端提供用户身份认证、设备身份认证及策略下发等功能，管理端提供用户身份管理、设备满足身份管理、网络管理及日志管理等功能，客户端收集用户信息及设备信息、发送接入申请。使用 TCM 提供的加密接口，可以提供更安全的终端用户身份识别功能。利用 TCM 芯片，可以为终端提供设备身份识别，禁止非授权设备接入网络。一般来说，TCM 可信计算功能在国内尚处于应用不丰富的时期，方正电脑推出的这两个应用功能，避免了用户采购了 TCM 平台产品后，没有应用可用或还需单独开发应用的麻烦。

作为中国可信计算产业联盟的发起者之一，国民技术自成立以来，在主要产品安全芯片研发和产品化方面一直坚持自主创新的研发道路。其全力打造的网络身份认证芯片，是中国首颗量产的具有全自主知识产权的 32 位 CPU 产品，广泛应用于我国金融、税控、海关、电子政务、数字版权保护等领域。

实际上，方正电脑在 TCM 领域的应用和开拓上已经具有较好的基础。早在 2008 年 9 月，针对行业大客户越来越重视信息安全的问题，方正电脑推出了首款采用 TCM 安全芯片的商用 PC——方正君逸 M580、M530 系列。该机型采用以 TCM 安全芯片为平台的软、硬件结合方式，最大程度保护电脑的安全使用，集高安全性、可管理性、易用性于一身，广泛应用于政府、金融、教育等行业，备受关注。

作为国内 TCM 产业中的领军企业，国民技术在安全存储芯片及其解决方案、可信计算芯片及其解决方案以及移动支付芯片及其解决方案方面均处于国内先进水平。此次方正电脑与其进行深度合作，不仅巩固了双方长期以来建立的良好合作关系，更是通过强强联合，大力助推了 TCM 安全技术的发展。合作双方纷纷表态，在此基础之上将进一步加强双方在技术、应用、产品开发、上下游等方面的深度合作、推陈出新，共同为我国信息安全产业打造强有力的信息安全之盾。

联想扬天首次全面预装定制版 360 软件

来源:it168 网站

2010 年岁末,中国第一大 PC 品牌联想旗下扬天系列和国内最大的安全厂商 360 在京宣布达成全面战略合作。从 12 月起,联想将在扬天系列电脑中预装定制版 360 安全卫士和 360 安全浏览器,这预示着 360 正逐渐开放其软件平台,目标人群将从个人电脑用户扩张到企业用户。同时,更多硬件厂商也将从中受益。

“这次和联想扬天的合作是 360 有史以来与硬件厂商最深入的合作。我们为联想扬天专门定制了扬天版的 360 软件,在保留 360 绝大多数功能的同时,添加了例如联想一键修复、远程帮助等针对联想用户的特定功能。” 360 公司总裁齐向东介绍说。

众所周知,在软件厂商与硬件厂商的合作中,定制软件的成本最高,但与之相伴的是相对紧密的合作关系。为此,360 投入了专门的开发小组建立起联想扬天小团队,专门负责产品的研发和维护,保证定制版 360 在木马、病毒库及产品升级等方面与 360 标准版实时同步。

其实,早在一年前,联想就与 360 达成了首次合作,指定了包括 360 安全卫士和 360 杀毒在内的 360 安全套装为其售后服务与维修的安全工具,在工程师进行售后服务维修时为用户进行电脑体检和查杀木马病毒。“360 是互联网安全领域第一品牌,非常值得信赖,产品也特别简单易用。”联想扬天的负责人说。

业内人士评论,360 最近推出的 360 硬件大师填补了 360 在电脑硬件检测领域的空白,加之此前已经搭建完毕的软件分发、管理平台——360 软件管家,360 在电脑安全与软件管理的一体化整合上已大大领先于国内其他安全厂商,其在硬件厂商心目中的地位也得到了进一步的巩固。预计未来一段时间,与 360 展开深度合作的硬件厂商会越来越多。

赛门铁克：杀毒免费是不公平的

来源:中国经济和信息化

免费杀毒正成为个人用户市场的主流。但赛门铁克认为,这种免费做法的最终受害者还是用户。

今年 IT 界轰轰烈烈的 QQ 大战 360, 一度搅动了整个即时通讯和杀毒软件市场。

随之而来的是面向个人用户的传统杀毒软件厂商纷纷竖起了免费大旗, 卡巴斯基、金山毒霸、可牛杀毒、瑞星杀毒、Avira AntiVir、AVG 杀毒相继推出全免费或免半年、免一年的优惠。

此前, 在桌面安全领域, 付费用户的比例接近 40%。360 的出现, 使得免费杀毒大行其道, 并成了用户的习惯。

360 正是靠着永久免费的策略, 很快就笼络了上亿用户, 到今年 1 月其市场份额已攀升至 33.76%, 成为我国装机量最大的杀毒软件。

据中国互联网络信息中心发布的调查报告显示: 58.6% 的网民愿意使用免费杀毒软件, 而在收费杀毒软件用户中, 35.6% 的用户明确表示到期后不会再续费。

“免费杀毒正成为个人用户市场的主流。”近几个月来, 多份分析报告如是分析。

“对于我们个人来说, 免费是一种涤荡旧有思维的商业体验; 对于互联网领域的企业来说, 免费更多的是一种生存法则, 一种可以改变旧有发展模式而实现脱胎换骨的动力机器。”美国《连线》杂志总编辑克里斯·安德森在其 2009 年畅销书《免费: 商业的未来》中已经明确了互联网的免费趋势。

提供免费, 若找不到清晰的商业模式, 将难破盈利困局; 坚持收费, 意味着市场占有率的不断萎缩——靠出卖许可证赚钱的传统杀毒软件企业陷入空前危机。

虽然大势如此, 但作为全球信息安全大佬的赛门铁克公司仍然坚持收费原则。赛门铁克公司的总裁兼 CEO 恩瑞克·塞伦认为, 免费杀毒软件功能有限, 一分价钱一分货, 有效应对有针对性的攻击才是现阶段信息安全领域最重要的事。

一分价钱一分货

《中国经济和信息化》: 前一阵的 3Q 大战已告一段落, 杀毒软件的免费之风越刮越盛, 你怎么看待免费杀毒?

恩瑞克·塞伦: 一分价钱一分货。免费杀毒软件功能有限, 免费是对不懂安全的业外人士的一种不公平做法, 杀毒软件不是为了防范已有病毒, 而是要针对不同的用户进行防范。

信息安全保护是个严重的问题, 需要保护的不仅是电脑, 而是关键信息, 所以信息安全保护的质量必须要有保证。有效应对有针对性的攻击才是现阶段信息安全领域最重要的事。

上世纪 90 年代只有几百种电脑攻击, 而目前每年就有 300 万种不同形式的攻击, 业界总是有人在散播一种观念, 认为免费的安全软件就够用, 而实际的情况远非如此。这种免费做法的最终受害者还是用户。

《中国经济和信息化》：当今信息安全以及相关产业正经历着重大变化，今后提升信息安全的關鍵是什么？

恩瑞克·塞伦：五大要素正在成为今后提升信息安全的關鍵。

一是身份安全。在未来，人们可以从任何地方简单、安全地访问信息，以实现工作和生活的无缝转换。

二是设备安全。为网络设置防火墙已不够了，取而代之的则是信息和设备两者都必须得到保护。未来，基于信誉的安全是保护重要端点的正确方式。目前包括赛门铁克在内，全球很多行业内公司都在朝这个方向努力。

三是信息保护。在未来，加密技术、数据丢失防护（DLP）和身份保证将实现以信息为中心的安全防护方法，即将所有安全控制工作整合在一起，以确保信息访问是经过授权的。

四是情境与相关性。即在合适的时间为合适的人提供合适的信息。当今所有大型企业都深受非结构化数据的困扰，未来企业必须要建立一个能够理解情境（谁在请求访问信息）以及相关性（哪些信息能够满足该用户的需求）的 IT 架构。

五是云的实现。这个架构将可以根据企业需要提供更高的计算能力、更多的应用和存储。这一点即使是目前规模最大、投资最多的传统网络也无法做到。

数据的隐私保护

《中国经济和信息化》：未来 IT 业界中将有哪些趋势会在全世界产生深远的影响？

恩瑞克·塞伦：首先是消费化。将来，消费者将越来越多地成为新技术早期采纳者，他们会把他们个人的一些工具用到他们的业务当中。

其次是消费者的 IT 化，这是什么意思呢？也就是说很多消费者把技术带回了他们的家中，使他们的家庭变得更加数字化，更加技术化，因为他们有那么多设备，所以他们需要有系统管理员的能力帮助他们。

第三个是移动，今年有 10 亿台移动设备能够移动联网，预计到 2014 年全世界将会有 100 亿台设备能够移动联网。所以，移动是每个人都不能够错过的大趋势。

第四是社交化企业。今天，企业仍然在很大程度上是靠电邮进行合作的，但是我们会看到以全新的方式交互，很好地进行社交化的企业将来能够站在制高点上，他们的战略起点更高，但同时也会有更大的挑战。

第五是虚拟化和数据爆炸性的增长。预计到 2014 年非结构化数据和结构化数据的增长率将达到 400%，而且增速会比今天的速度还要快。

第六是云计算成为最为重要的趋势，在人们讨论云计算会给他们的业务模式带来什么样的影响、加速云计算部署的同时，也必须考虑到云计算带来的挑战。

第七就是威胁情况的变化，今天的威胁更加有针对性，针对个人、针对企业、针对关键基础设施进行攻击。因此需要新技术、新方法来防范这些威胁。

《中国经济和信息化》：从安全角度来说，这些 IT 新趋势对安全行业会带来哪些影响？

恩瑞克·塞伦：在以上的几个趋势中，最核心的是 IT 向云计算方向发展，而云环境则需要新的安全方法，我认为，安全是首要的关注点。

《中国经济和信息化》：云安全是一个很大的概念，一般消费者包括企业用户对其了解还是十分有限，那么你认为对云安全来说目前最大的障碍或者最应该思考的问题是什么？

恩瑞克·塞伦：在云安全方面最容易受到质疑的地方就是数据放在数据中心是否安全，与之相关的一点就是数据的隐私性保护。所以云安全最主要思考的两大问题：一个是数据的隐私性，还有一个就是数据安全的保护。

《中国经济和信息化》：目前赛门铁克在云安全领域并没有完全垄断，包括卡巴斯基、趋势科技以及国内的金山等安全厂商也都推出了类似的计划，而且都宣称自己提供的安全方案最具优势。你对此有何评价？

恩瑞克·塞伦：在云安全方面大家一般都在做三件事情。

首先是通过云来交付服务。通过云来递交以下的服务：电子邮件的过滤、网络流量的过滤以及归档，它们都基于云或者通过云来进行交付的服务。

其次是帮助云服务供应商搭建他们的云安全基础设施。

再次就是参加 CSIA，也就是云安全行业联盟，主要是做一些标准化的工作，通过这种标准化我们就可以更好的和第三方的云服务厂商进行产品技术集成。

云安全是隐患

《中国经济和信息化》：云计算是当前的热门话题，你怎样看待云计算的发展？目前云计算的最大阻碍是什么？

恩瑞克·塞伦：在云计算的应用方面，其实世界各地都一样，都有五个障碍会影响到云。第一个是安全；第二个是可用性；第三个是延迟性，它的反应速度是不是足够的快；第四个是标准问题，是不是能够不断地合规，因为各个政府都有一些监管条例；第五是转换成本，如果你现在对一个服务商不满意，想转到别的地方，这个成本是多少。如果这五点都能很好的得到解决，那么云计算的明天无疑是美好的。

《中国经济和信息化》：安全问题又是云计算的最大隐患，同时现在安全市场每年大概是以两位数的速度在增长，你认为云计算每年能给安全市场带来什么样的增量？

恩瑞克·塞伦：在云计算方面，近五年的复合增长率是 20%。这是全球累计的数据，没有不同的市场的具体数据。上个季度赛门铁克的财报结果非常好，在 DLP 业务和托管、安全服务方面都是双位数的增长。在我看来，对于云计算人们最担心的一点当然就是安全问题，所以安全软件的业务增长会持续下去。

《中国经济和信息化》：从你去年就职以来，赛门铁克就一直受困于存储业务增长缓慢和来自企业安全领域内部与 McAfee 的竞争压力之中。今年 8 月英特尔以 76.8 亿美元收购了赛门铁克的老对

手 McAfee，是否预示着全球安全软件市场将发生变化？

恩瑞克·塞伦：我们不便评价其他公司的做法，但是我认为一家身价 400 亿的公司收购一家身价 20 亿的公司，在专注性上肯定做不过我们。

《中国经济和信息化》：很多软件企业都在向移动领域进军，比如之前 SAP 并购 Sybase，主要目的也是向移动终端方面进军。你对此怎么看？

恩瑞克·塞伦：确实，移动安全是一个非常大的机会，但必须要注意一点，不能认为在 PC 平台上的安全做好了就可以直接搬到移动平台上。移动设备用户有很多其他的需求，比如数据同步的需求、远程数据消灭的需求等等，除此之外还要不断挖掘那些在移动场景之下的客户新需求。

《中国经济和信息化》：独立的软件厂商今后应该如何发展？

恩瑞克·塞伦：当然希望以自己独有的方式展示自己的能力。赛门铁克现在已经创建了一系列的软硬件结合的产品，来服务于存储、备份和安全市场的需求，未来将给市场带来一种软硬件的集成解决方案。

美移动安全软件厂商 Lookout 融资 1950 万美元

来源:新浪科技

北京时间 12 月 23 日午间消息，美国移动设备杀毒软件提供商 Lookout Mobile Security 已经从由 Index Ventures 为首的一个投资者集团获得了 1950 万美元融资，总融资额达到了 3600 万美元。

参与此轮融资的还包括当前投资者 Accel Partners 和 Khosla Ventures。

Lookout Mobile Security 为谷歌 Android 平台、RIM 黑莓平台以及微软的 Windows Phone 手机提供杀毒软件服务。该公司于 2009 年 9 月推出相关产品，目前尚未实现盈利。

Lookout Mobile Security 面临着赛门铁克和其他安全软件厂商的竞争。

摩托罗拉将收购云存储厂商 Zector

来源:新浪科技

北京时间 12 月 22 日上午消息, 据消息人士透露, 摩托罗拉即将收购云存储软件厂商 Zector, 这很可能是该公司明年 1 月拆分前的最后一笔收购。

明年 1 月, 摩托罗拉将分拆为摩托罗拉移动(Motorola Mobility)和摩托罗拉解决方案(Motorola Solutions)两家独立的上市公司, Zector 很可能被纳入摩托罗拉移动旗下。

Zector 是一家由著名风险投资公司 Y Combinator 投资的创业公司, 旗下拥有 ZumoDrive 和 ZumoCast 两款云端存储应用。摩托罗拉之所以收购 Zector, 是因为 Zector 拥有一系列优秀的云端存储产品, 并且已经逐渐获得用户信赖。

比如, ZumoDrive 提供简单的云端存储和同步服务, 并在此基础上加以创新。ZumoDrive 可以让用户的电脑认为存储在云端的文件是本地文件, 从而使用户操作起来更方便。

ZumoDrive 能通过无线使不同设备的播放表实现同步、自动探测文件内容。它还可以自动探测用户电脑上的改动, 并更新到云服务器。ZumoDrive 兼容 iTunes 等媒体应用, 还提供用于 iPhone、Android 和 Palm 等智能手机的移动应用。摩托罗拉有意将 Zector 的存储技术移植到自己生产的手机产品中。

Zector 的另一款云存储应用 ZumoCast, 主要功能是将用户的个人电脑转变为云端存储服务器, 使用户可以通过手机等其它上网设备使用自己电脑上的文件。

随着越来越多用户使用“云”服务, Zector 的 ZumoDrive 已经取得了可观的成绩: 成功融资 1500 万, 并和惠普达成协议, 为其上网本提供云端存储应用。

除 Zector 外, 摩托罗拉在过去的几个月中还收购了家庭软件开发商 4Home、地理定位手机软件创业公司 Aloqa。另据科技界传言, 摩托罗拉已于今年 8 月收购 Web 应用程序开发公司 280 North。

百度诉 360 不正当竞争一审获赔 38.5 万元

来源: 北京晨报

昨天上午, 百度诉 360 不正当竞争一案在北京市二中院有了一审结果。法院一审认定奇智软件(北京)有限公司和北京三际无限网络科技有限公司的行为构成不正当竞争, 判决二公司停止侵权, 刊登声明以消除影响, 赔偿原告北京百度网讯科技有限公司以及百度时代网络技术(北京)有限公司经济损失及诉讼合理支出共计 38.5 万元。

360 “恶评插件” 锁定百度

原告诉称, 今年 3 月初, 两被告在其 360 安全卫士 7.0 软件版本中, 将两原告共同经营的百度工具栏和百度地址栏两款软件定义为“恶评插件”, 并描述为“此类插件具有恶意行为, 可能会危害您的电脑, 建议您立即清理”。按照 360 安全卫士之提示进行操作可以在默认情况下删除该两款软件, 且两被告在 www.360.cn 网站将该软件描述为“具有强制安装, 自身无法正常卸载”。

同年 7 月, 原告又收到网民举报, 两被告在其最新升级后的 360 安全卫士 7.3beta 版不但继续对百度工具栏和地址栏进行恶意贬损和诋毁行为, 而且在“360 杀毒”和“查杀木马”功能中, 将该两款软件作为“病毒查杀”, 并描述两款软件对用户电脑构成“安全威胁”, 用户按照 360 杀毒默认设置, 即可卸载百度工具栏和地址栏软件。

百度起诉 360 索赔千万

原告认为, 两被告打着安全检测的幌子, 肆意篡改百度搜索页面结果, 借助百度知名度为其 www.360.cn 网站非法攫取流量, 并且对百度工具栏和百度地址栏两软件进行恶意贬损, 阻碍该两款软件的传播和运行, 以期通过这种非法手段抢夺原告用户, 已构成不正当竞争并索赔 1000 万元。

奇智软件公司和三际无限公司答辩称, 公司与百度网讯公司和百度时代公司不构成竞争关系, 并不存在百度网讯公司和百度时代公司指控的各项不正当竞争行为。

负面介绍属不正当竞争

法院认为, 奇智软件公司在其所有的 360 安全卫士软件、三际无限公司所有的 360 安全中心网站中将百度工具栏和百度地址栏软件称为“恶评插件”和“恶评软件”的行为; 奇智软件公司所有的 360 安全卫士软件在查杀病毒、木马时将上述两款涉案软件标识出来并进行虚假描述诱导用户删除的行为, 以及三际无限公司经营的 360 安全中心网站中无依据地对上述两款涉案软件进行负面介绍的行为, 均构成不正当竞争。

关于两被告指控二原告人为操纵网络用户对于上述两款涉案软件的投票结果的主张, 以及关于三际无限公司故意删除网络用户对于上述两款涉案软件的好评, 构成不正当竞争的主张, 法院认为证据不足, 不予支持。

谷歌搜索新增黑客报警功能

来源:赛迪网

12 月 21 日消息,据国外媒体报道,谷歌公司正在竭尽所能地为用户创造一个安全的上网环境。上周五谷歌搜索新增一项功能,在其搜索结果中提醒用户防范已被黑客攻破的网站。

专家指出恶意软件已经遍布整个互联网,每个用户都存在被其攻击的危险。

谷歌最新推荐的一项功能是,如果谷歌检测到某个网站已被黑客攻破和修改,就会在关于该网站的搜索结果中弹出警告:“该网站可能已经被黑。”如果用户点击这条信息,就会跳转到谷歌的帮助中心,以查看相关信息,只有用户点击接受才会继续访问该网站。

谷歌使用各种自动化方法收集被黑网站的普遍特征。如果检测出某网站可能被黑,谷歌会即时与网站管理员取得联系。

如果问题解决,网站管理员可以申请尽快对其网站进行评估,以减少访问量的流失。一旦谷歌验证这些问题已经修复,谷歌将停止显示该网站的警告。

谷歌公司并不是唯一关注黑客恶意攻击网站问题的高科技公司。其竞争对手微软公司将发布的 Internet Explorer 9 可以高效地检测出黑客攻击的信息并加以防范。NSS 实验室的一项报告指出,正处于 Beta 测试阶段的 IE9 是最安全的浏览器,其安全系数比第二位的 Mozilla Firefox 浏览器高出 5 倍。

用友发布云计算战略实施第二次转型

来源:新浪科技

12 月 23 日下午消息,管理软件厂商用友集团今日正式发布其云计算战略。继从财务软件向管理软件完成第一次转型之后,用友未来几年将进行向云服务的第二次战略转型。

用友公司董事长兼总裁王文京透露,用友将实施软件+云服务的策略,迈向“云端企业”,希望在 2015 年成为亚洲最大、全球领先的企业云服务提供商。

据了解,用友将向客户提供 4 大类型 9 种云服务解决方案。

第一为企业云,包括支持大型企业用户的用友 NC 集团企业云、支持中型企业用户的用友 U8/U9 中型企业云、面向小型企业的畅捷通云;

第二为行业云,包括面向医疗卫生企事业单位的用友健康云、面对电子政务市场的用友政务云、面向整个汽车行业生态圈和汽车产品的用友汽车云;

第三为领域云,包括面向客户提供数据分析服务的用友 BQ 分析云;

第四为云服务,包括可为 100 多万家客户提供用友云支持服务、在线学习平台用友云学习服务。

此外，用友还同步推出了七大云商业模式，包括 SaaS(软件即服务)服务模式、托管服务模式、远程管理服务模式、云支持服务模式、云学习服务模式、PaaS(平台即服务)生态链合作模式、IaaS 供应商合作模式。

在用友的云战略中，SaaS 定位为自主开发应用服务，集成第三方伙伴应用服务，自主运营；PaaS 定位为自主建构，自主运营，并利用 PaaS 平台，打造产业链；IaaS 定位为与基础架构运营商合作。

微软助力企业启动云的力量

来源:和讯科技

为把微软领先的云计算技术、服务、解决方案带给更多中国用户与合作伙伴，微软已经面向中国市场正式拉开了“启动云的力量”系列市场活动的帷幕。在这场市场攻势中，微软制定了“动、酝、耘、会”宣传口号，这四个富含中国文化特色的文字，每一个都包含“云”的元素，分别从四个方面深刻诠释了微软在云计算领域的决心、能力及承诺。

微软大中华区总裁兼首席执行官梁念坚先生曾在多个场合公开表示，全球 IT 产业发展推动云计算成为未来产业发展的趋势，而微软以 15 年的经验和持续不断的研发创新继续引领 IT 产业的发展。在中国，建设创新型国家的宏观目标指引下，政府高度重视云计算产业的建设和扶持，而微软中国的目标和使命就是帮助中国政府、企业、消费者充分体验到云计算带来的好处。

云计算产业方兴未艾

作为当今 IT 产业快速发展的重要推动力，云计算技术已受到越来越多技术决策者的关注。根据 11 月 29 日赛迪顾问发布的《云计算产业发展白皮书》显示，当前，中国云计算产业正处于导入和准备阶段，处在大规模爆发的前夜。未来 3 年，云计算应用将以政府、电信、教育、医疗、金融、石油石化和电力等行业为重点，在中国市场逐步被越来越多的企业和机构采用，市场规模也将从 2009 年的 92.23 亿元增长到 2012 年的 606.78 亿元，年均复合增长率达 87.4%。

2010 年 9 月 8 日，国务院审议并原则通过《国务院关于加快培育和发展战略性新兴产业的决定》，确定了战略性新兴产业发展的重点方向和政策，这七大战略性新兴产业包括：节能环保、新一代信息技术、生物、高端装备制造、新能源、新材料和新能源汽车七个产业，并决定集中力量，加快推进。这些战略性新兴产业将替代传统产业成为经济先导产业。

另据国家发展改革委、工业和信息化部于 2010 年 10 月下达的通知，为加强我国云计算创新发展顶层设计和科学布局，推进云计算中心(平台)建设，将在北京、上海、深圳、杭州、无锡等五个城市先行开展云计算创新发展试点示范工作。

政策的鼎力支持、产业的持续发展推动云计算成为引领 IT 业未来发展的重要力量。

微软助力企业启动云的力量

微软不仅拥有 15 年以上运营云计算服务的丰富经验，也是唯一一家 IT 企业能凭借可靠性、安全性和全球影响力，为企业提供一整套云服务。正如微软大中华区副总裁兼市场战略部总经理孙建东所说，微软拥有最全面的企业级云计算产品、技术和基础设施，并致力于通过系列云计算技术和解决方案、Hyper-V 虚拟化技术等实现“IT 即服务”愿景，帮助企业减少 IT 基础设施投入，从而专注于核心业务研发。

在国内，微软致力于与合作伙伴携手开发适合不同行业特性的解决方案，帮助行业用户实现创新，创造商业价值。

西门子公司是微软全球也是在中国的重要客户之一。近年来，随着西门子业务的持续扩展，对内部 IT 的业务需求以及 IT 服务品质的要求也在日益增强，这给内部服务集团和 Intranet 平台提出了众多挑战：设备更新需求、IT 环境空前庞大复杂、高服务品质与绿色 IT 需求等。西门子 IT 解决方案和服务集团希望通过部署 IT 虚拟化技术来解决目前所面临的种种挑战，并通过详细评估最终采用了微软虚拟化解决方案。

西门子 IT 解决方案和服务集团东北亚区副总裁李佳表示：“在西门子集团内部业务应用平台上，通过部署微软解决方案，西门子 IT 解决方案和服务集团实现了新旧服务器的无缝迁移，在降低成本的同时提高了服务品质保障协议(SLA)，并达到构建‘可持续性 IT’的绿色 IT 环境的目的。微软 Hyper-V 虚拟化技术可以很好的与西门子现有的基础架构相集成，此外微软服务团队有力的支持也使得我们可以更有效率地将虚拟化技术部署到生产环境中。”

成都云计算中心是国内首家商业运营的规模化云计算中心，在 2009 年底建成并投入运营，“猪肉质量安全溯源监管系统”则是第一个基于该平台成功部署的电子政务应用。该系统是成都市政府为保障老百姓食用猪肉的质量安全，借助微软的云计算技术，实现有效的数据跟踪和实时监管决策的一个服务于民的项目。

通过采用微软的私有云解决方案，成都云计算中心将曙光高性能硬件服务器平台、微软高性能计算平台 Windows HPC Server、数据库服务平台 SQL Server 2008 以及虚拟化技术(Hyper-V)有机的融合在一起，成功构建出成都云计算服务平台。并通过微软 System Center 实现了对整个私有云平台和动态数据中心的基础架构、应用的管理，涵盖了从物理与虚拟的各种资源全面的监控与端到端的运营管理。借助这一强大的平台和海量数据的处理能力，成都云计算中心实现了对猪肉安全质量溯源监管系统的数据库支持。

孙建东表示：“从成都云计算中心开建之初，微软就和成都市经济和信息化委员会以及云计算中心全面积极配合，把影响到民生的猪肉质量安全溯源监管系统首次在国内以云计算的方式应用起来。微软希望这样的应用也能在国内其他城市推广，让云计算从天上落到地上，真正地服务于公众。”

“酝、耘、动、会”四字方针寓意深刻

为了帮助企业用户和合作伙伴深入了解云计算技术和产业趋势，微软(中国)最新掀起的“启动云的力量”系列活动将从线上、线下以丰富多样的形式进行推广，旨在进一步帮助企业、合作伙伴、

消费者全面了解微软云计算。概括起来,‘酝、耘、动、会’这四字方针蕴含了极其深刻的意义:

- 动: 启动 - 启动并发挥云计算的力量, 帮助企业提升竞争力
- 耘: 潜心耕耘 - 凭借 15 年运营云服务的成功经验, 微软承诺将全力以赴, 与合作伙伴及客户一起迎接云计算浪潮。
- 酝: 精心酝酿 - 微软及合作伙伴向客户提供全面的云计算解决方案
- 会: 悉心融会 - 微软是业界唯一一家可以帮助企业从现有 IT 基础设施无缝、平滑过渡到云计算的厂商

孙建东进一步强调到:“微软将携手合作伙伴, 帮助企业平滑过渡到云计算时代, 迎接云计算浪潮, 进一步提升竞争力。”

技术前沿

稳捷网络力推可信第二代 Web 安全新理念

来源:中国信息安全博士网

安全大趋势看好

长期以来,信息安全市场一直是全球 IT 市场中的明星,其复合增长率一度超过 140%,IDC、Gartner、Frost 等市场分析公司频频对安全市场抛出橄榄枝。近期,根据全球信息安全市场的格局,稳捷网络公司提出目前全球安全发展的五大趋势。

趋势一,硬件安全领域经过三年的发展,目前已经深入人心,以前总觉得防火墙是硬件,其余用软件替代。这个是以前的状况,但是近几年的发展表明,用户对硬件安全已经有很高的认识,超过 50%以上的用户认可硬件安全设备。

趋势二,传统安全设备向交换机中集成。目前明显的一点,大量跟网络物理层相关的设备,很可能会集成到交换机里面去,主要是指四层以下的安全硬件往交换机中集成趋势明显,成为一种普通的安全模块,比如防火墙、入侵检测、流控、负载均衡、甚至一些网络管理都加入到交换机中。因为这些功能主要是跟硬件打交道,不看网络内容。

趋势三,应用安全设备大发展,这里面的应用安全设备主要是指跟内容打交道的产品,保护服务器与企业 Web 应用为主,比如 Web 安全网关、WAF、上网行为管理、垃圾邮件、DLP 都是跟内容相关的七层设备,这些设备比较难做到网络设备中去。因为内容千变万化,就像常见的协议、P2P、IM 等端口都是飘逸的,很难从设备底层控制,这部分安全领域就是以深度内容检测 DCI 为基础发展

下去。

趋势四，管理类设备稳定增长。对安全而言，四层以下设备和四层以上设备都是实时处理的，但是管理类设备不是，比如认证、用户管理、漏洞扫描、报表日志、监控分析、策略发布、中央控制、数据挖掘等，这些设备对性能的要求不高，从而构成一块专门的市场，比如 SOC 就发展的很特殊。这类安全设备与用户的使用联系更加密切。

趋势五，数据安全设备。数据安全设备综合了很多技术，但是其核心内容就是保护企业的数据库，这块市场属于安全厂商和数据库厂商和存储厂商结合起来做。

稳捷力推第二代 Web 安全

稳捷网络大中国区总经理彭朝晖表示，在目前安全五大趋势之中，应用安全设备的大发展最为引人注目。比如 Web 安全网关已经在全球的电信运营商市场取得了突破，特别是随着稳捷网络推出全球首台万兆 Web 安全网关 BeSecure 2080 之后，Web 安全已经从效果和性能两方面赢得了市场的信心。

与此同时，稳捷网络大中国区市场经理赵晓涛向媒体表示，根据 Gartner 的分析报告，其明确定位 Web 安全网关(SWG)包括两大部分：第一，对来自 Web 的内容进行控制，其中特别强调在企业用户使用的时候进行实时安全控制。第二，从 Web 内容的角度保证安全传输，其寓意是需要保证 Web 内容的安全传递。

谈道这里，有必要提一下目前大红大紫的 WAF 产品。WAF 目前市场是典型的鱼龙混杂状态，很多产品为了实现“网站不被黑”的噱头，使用了很多白名单的方式，有些甚至是静态缓存对比的方式来实现所谓的“网站监控”，对此稳捷网络大中国区市场经理赵晓涛表示，这仅仅是一种讨巧但是极不彻底的“对付”手段。

“真实可靠的 Web 安全，必须内在是聪明且可信的，换言之企业用户需要保护的网站内容，就像是放在一个保险箱内，内部是干净的内容。只有使用这样的内容安全理念去开发产品，才能从源头上确保用户的 Web 安全。” 稳捷网络大中国区市场经理赵晓涛如是说。

稳捷网络大中国区总经理彭朝晖表示，为了能帮助用户实现可信的安全，稳捷网络公司专门推出了 Wedge Trust Content(WTC)模块，利用稳捷网络遍布全球的分层次的可信内容云安全技术，从内容的源头对各种威胁开展零延时防护。

据悉，WTC 利用遍布全球的蜜罐、爬虫、用户递交、云网络等各种技术，将全球 Web 内容进行分类打分并进行积累与内容扫描，依靠分布全球运营商网络的 Web 安全网关设备，主动出击进行信息抓取，积累性的实现全球内容安全资源的共享与增量，而这也标志着全球 Web 安全发展的全新阶段已经到来。

全面解析 Web 应用防火墙的价值和优越性

来源: it168 网站

WEB 应用的重要性

随着互联网技术的发展, WEB 应用越来越受到业务系统的重视, WEB 应用已经与我们的核心业务系统密不可分。如今的电子政务、电子商务、网上银业、网上营业厅等均以 WEB 为载体。WEB 也由原来的网站浏览的代名词转变为诸如网上报名、网上交易、网上报税等多种业务应用系统。

WAF 的价值

WEB 价值重点体现在门户网站的时代时, 我们所面临的安全威胁主要源自网站被黑或者网站被篡改, 因此网页防篡改技术得到成长并大量使用。应用推运系统架构革新, 而系统架构的和革新推动安全技术的发展。WEB 应用防火墙也不例外, 也是在现有 WEB 防护技术力日益无法满足业务的新需求时诞生的。

如果说防篡改软件是一种基于文件管理的被动办法, 那么 WAF 则是从安全的本质出发, 对威胁进行主动防御, 并对 WEB 应用进行性能优化的最佳方案。简单将防篡改软件理解为是文件恢复管理, 而 WAF 则是分析处理不安全的访问行为, 这些不安全的行为包括网页篡改事件、信息泄漏事件、信息窃取事件、信息失效事件等。在中国 WEB 应用环境下的 WAF 通常也会具有网页防篡改的客户端, 功能和市面的网页防篡改软件几乎相同。

WAF 以独立的硬件网关存在, 其部署和使用过程中不需要对原有的 WEB 服务器作任何的调整, 并且 WAF 本身支持多种部署方式, 例如透明网桥模式的部署不需对网络进行任何调整。

与 IPS 相比 WEB 应用防火墙可谓是专注于 WEB 应用的 IPS, 与传统的 IPS 不同, WEB 应用防火墙在特征匹配方面的粒度更细, 至少可以精确到如下几个节点:

对协议的全面理解以及协议规范性检查

请求头关键字段的识别和特征匹配, 从而降低误判

响应头敏感信息的处理防止服务器指纹泄露

响应体特征匹配, 屏蔽敏感信息泄露

针对单个请求, 基于单个 URL 的匹配最大程度确认业务系统的可用性

WAF 的优越性

WEB 应用防火墙技术架构上最佳方案是采用代理技术实现, 然而标准的代理技术应用到 WEB 应用防火墙时却存在一个先天的不足。代理技术会中断业务请求, 因此部署 WEB 应用防火墙需要调整现有业务架构或网络数据走向。另一方面代理技术存在性能瓶颈, 难在胜任大型的业务系统。

安恒信息采用内核级代理技术解决了部署全透明和性能两个技术瓶颈, 是国内首创的全透明 WEB 应用防火墙, 并成功应用于诸多网上银行、运营商 BOSS 系统、电子政务等核心业务系统。

WEB 应用防火墙采用基于特征库的防御技术进行防护, 而特征库技术只能解决通用的, 已知的

攻击行为。而 WEB 应用系统千差万别，仅采用通用特征库不仅防护效果不佳，而且可能会因为代码的原因导致误判，从而影响业务系统的可用性。因此安恒 WEB 应用防火墙中加入了异常检测引擎用于提高防护能力，降低误判率。异常检测技术可以用一个下面这个例子进行说明：

安全检测好比闭路电视监控系统，基于特征的检测技术即通过行人的身高、体重、外貌进行检测，然后通过 X 光机检测身上是否带了已知的不安全装备。而异常检测则是通过对人的行为特征进行分析，例如一个人进门时身带了一个手拎包，而走到大厅后将手拎包放下，人离开。针对这种特为将为触发报警动作。

异常检测到 WEB 安全检测中主要用于补偿特征库的短板，可以有效的防御未知攻击、盗链行为、应用 DDOS 攻击等。

黑客攻防

清华大学子网站遭黑客入侵并被植入黄色信息

来源:新京报

12 月 17 日，黑客入侵清华大学子网站并植入黄色信息。此次攻击对清华大学首页无影响，只是生成了以该网站子网站为域名的黄色网页。清华大学已发现并关闭网站，初步查明为黑客所为。

黄色网页借清华域名

17 日晚，互联网从业者刘先生在对他所在公司的服务器进行情况抽查时，发现他们网站的首页被篡改。经查看被篡改的代码，刘先生发现一个以“www.rccm.tsinghua.edu.cn”开头的网址，点击进入后，发现里面全是黄色信息。

刘先生怀疑黑客同时攻击了清华大学的网站。他解释说，“www.rccm.tsinghua.edu.cn”为“清华大学现代管理研究中心”首页，是清华大学网站二级域名。正常情况下，只有清华大学能申请以“www.rccm.tsinghua.edu.cn”开头的域名。

校方查明黑客所为

记者登录清华大学及现代管理研究中心网页，均无法发现该黄色网页，在各大搜索引擎搜索也没有搜到这个网页。“由于我发现得比较及时，搜索引擎还没有来得及抓取到，因为一般情况下至少 1 个星期才会被收录。”刘先生说。

黑客为何没有把黄色网页放在被入侵网站的首页入口？刘先生解释说，“这就是黑客的狡猾之处。”这样避免了被清华大学发现，从而长期存在，而且可借清华大学的影响力，被搜索引擎更多抓

取。

通过对 IP 地址等信息的查询,刘先生发现是位于辽宁省大连市的黑客对位于清华大学经管学院伟伦楼内的服务器进行的攻击。

清华大学宣传部负责人表示,清华大学经管学院已发现现代管理研究中心网站异常,并关闭该网站,初步查明为黑客所为。

调查显示: 2010 年网络盗窃首超现实盗窃

来源:IT168

根据近日公布的调查数据显示,对全球公司信息和电子数据的盗窃首次超过了现实世界中的盗窃事故数量。

全球风险咨询企业 Kroll 近日公布的 2010~2011 年度《全球欺诈年度报告》显示,在过去的 12 个月中,企业因欺诈而损失的金额从每十亿销售额的损失 140 万美元上升到 170 万美元,上升了 20 个百分点。

这项调查是由 Kroll 委托且由经济学人情报部执行的,对来自世界各地的 800 多名高级行政人员进行了调查。

虽然在去年的《全球欺诈年度报告》中,现金、资产和存货的现实世界盗窃是排名第一的盗窃行为,但从今年的调查结果来看,在过去的 12 个月中,27.3%的企业报告了信息或资产的盗窃,而 2009 年同期仅为 18%。与此同时,对物理资产或者存货的盗窃事故则略有下降,从 2009 年的 28% 下降到今年的 27.2%。

根据 2010 年调查显示,88%的企业表示他们在过去的一年中至少遭遇过一种类型的欺诈。而在分析各个国家的情况时发现,98%的中国被调查企业在去年至少遭受过一次欺诈行为,中国已经超越 2009 年位居榜首的巴西,成为企业遭受欺诈行为最多的国家。哥伦比亚以 94%的欺诈事故而位居第二,而巴西则以 90%畏惧第三。

“对机密信息的盗窃行为日益增加,是因为数据变得越来越‘便携式’,肇事者(通常是离职员工或者心怀不满的员工)可以轻易地移除数据,而不被发现,企业在这方面缺乏足够的控制,” Kroll 公司美洲区副总裁 Robert Brenner 表示,“与此同时,盗贼们逐渐意识到企业的知识产权的不断增长的真实价值。”

“这项调查的结果并没有表明其他类型的欺诈行为正在减少,而只是知识产权盗窃的升幅原因超过了其他保持不变的欺诈行为,企业需要定期对他们是如何控制对信息的方法进行评估。”

从报告中来看,在过去 12 个月中,信息化行业是信息和电子数据事故发生率最高的行业,这些包括金融服务(2010 年为 42%,2009 年为 24%),专业服务(2010 年为 40%,2009 年为 27%),以及技

术、媒体和电信(2010 年为 37%，2009 年为 29%)。

而根据受访者表示，技术发展的速度给打击欺诈行为访问带来新的调查，将近三分之一(28%)的受访者认为信息基础架构复杂性是他们成为欺诈攻击目标的最重要的因素。然而，尽管风险增加，只有百分之 48 的企业表示正在计划在未来 12 个月内将花费更多的资金来加强信息安全，该数据低于去年的 51%。

调查显示，在受访的企业中，对欺诈行为的恐惧让接近一半的企业停止了进一步全球化的脚步。48%的受访者表示，对欺诈行为的顾虑让他们至少放弃了一个外国国家的商业机会。最大的影响在于对新兴经济体的影响，欺诈行为阻止了 11%在中国的业务运行，11%在非洲的业务运营，以及 10%在拉丁美洲的运营。受访者表示，他们设法避免这些国家的地区风险，即使这些国家可能会提供更有吸引力的投资机会。

另外，调查显示，外国腐败行为法案的增加条款和对英国新的行贿法案的引入给这些企业带来新的挑战。将近有三分之二(63%)在美国或者英国运营的企业认为，这些法律并不适用于他们或者不确定是否适用。

结果就是，很多公司都没有准备好处理与欺诈行为有关的监管风险：少于一半(47%)的受访者表示他们有信心部署有效控制来预防在运营各个级别的贿赂行为，而另外 42%表示他们已经评估了风险，并且部署了必要的监控和报告程序。对于那些在过去一年中已经遭受欺诈行为的公司，初级员工和高级管理层最有可能成为肇事者，分别为 22%，而代理人或者其他中介机构则为 11%，Kroll 公司的调查显示。由这些员工执行的欺诈行为比例在北美、欧洲和亚太地区介于 50%到 60 之间，而在中东地区和非洲地区则为 71%。

警惕黑客 4 种手段攻击无线局域网

来源:ZDnet

最近国外专业媒体有人撰文指出，无线宽频上网在美国和欧洲越来越流行，不但许多办公室、机场、咖啡店、饭店等都开始提供无线上网服务，甚至许多家庭用户也有无线宽频上网功能。不过一些国外专家最近指出，许多无线网络并没有采取安全防护措施，不但易遭黑客入侵，甚至连事后要追查元凶都有困难。

专家提醒，黑客入侵无线网络主要常用以下四种主要手法：

方法一：现成的开放网络

过程：黑客扫描所有开放型无线存取点(Access Point)，其中，部分网络的确是专供大众使用，但多数则是因为使用者没有做好设定。

企图：免费上网、透过你的网络攻击第三方、探索其它人的网络。

方法二：侦测入侵无线存取设备

过程：黑客先在某一企图网络或公共地点设置一个伪装的无线存取设备，好让受害者误以为该处有无线网络可使用。若黑客的伪装设备讯号强过真正无线存取设备的讯号，受害者计算机便会选择讯号较强的伪装设备连上网络。此时，黑客便可等着收取受害者键入的密码，或将病毒码输入受害者计算机中。

企图：不肖侦测入侵、盗取密码或身份，取得网络权限。

方法三：WEP 加密攻击

过程：黑客侦测 WEP 安全协议漏洞，破解无线存取设备与客户之间的通讯。若黑客只是采监视方式的被动式攻击，可能得花上好几天的时间才能破解，但有些主动式的攻击手法只需数小时便可破解。

企图：非法侦测入侵、盗取密码或身份，取得网络权限。

方法四：偷天换日攻击

过程：跟第二种方式类似，黑客架设一个伪装的无线存取设备，以及与企图网络相同的及虚拟私人网络(VPN)服务器(如 SSH)。若受害者要连接服务器时，冒牌服务器会送出响应讯息，使得受害者连上冒牌的服务器。

企图：非法侦测入侵、盗取密码或身份，取得网络权限。

黑客袭击纽约旅游公司盗 11 万张信用卡信息

来源:cnbeta

黑客闯进了纽约旅游公司 CitySights NY 的网站，并盗取了 11 万张银行卡号码。

CitySights NY 发言人表示，黑客使用 SQL 注入方式袭击网站服务器，获取了姓名、地址、电子邮件地址、信用卡账号、到期信息和信用卡验证码等信息。这些信息足以用于使用信用卡网上购物。

CitySights NY 是纽约知名的旅游巴士公司。该公司于两周前通知客户该黑客袭击事件，并为客户免费提供一年的信用卡监测服务和公司的优惠券。

CitySights NY 的母公司 Twin America 表示，该公司已经使用了几项重要的措施来提高数据的安全性，目前已经封锁了该服务器的访问权并安装了防火墙，提高系统的反黑能力。

海外来风

Microsoft confirms IE flaw, not yet being exploited

来源: scmagazineus 杂志

Microsoft has confirmed the presence of an unpatched vulnerability in all supported versions of its Internet Explorer (IE) browser.

The software giant on Tuesday evening EST released a security advisory, acknowledging the flaw that, if exploited, could result in the execution of remote code. The bug impacts IE versions 6, 7 and 8.

"The vulnerability exists due to the creation of uninitialized memory during a CSS [style sheets] function within Internet Explorer," the advisory said. Users can be exploited if they visit a web page hosting the exploit.

Microsoft is not aware of any in-the-wild attacks targeting the vulnerability or of any affected customers, Carlene Chmaj, senior response communications manager for Microsoft's Trustworthy Computing group, said in a blog post.

But proof-of-concept code exists. A video demonstrating code execution was posted Monday by Offensive Security, a provider of security tools and training. And on Wednesday, exploit code was published as part of the open-source Metasploit hacking toolkit.

Although the flaw is able to bypass two built-in Windows security features, Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), IE Protected Mode for Vista and subsequent versions of Windows "helps to limit the impact of currently known proof-of-concept exploits," Chmaj wrote.

Microsoft is next due to release security fixes on Jan. 11. As of now, the company has no plans to issue an out-of-cycle patch for this vulnerability.

"However, we are monitoring the threat landscape very closely," Chmaj wrote.

微软证实 IE 浏览器漏洞，尚未被利用

来源：scmagazineus 杂志

——中国信息安全博士网翻译

微软已经确认在其互联网浏览器（IE）的所有受支持的浏览器版本中存在一个未修补的漏洞。

美国东部时间周二晚上，软件巨头发布了一个安全公告，承认该漏洞，如果被利用可能会导致远程代码执行。该缺陷影响 IE 浏览器版本 6，7 和 8。

“由于该漏洞存在未初始化的内存中，并且在 Internet Explorer 的功能中创建一个 CSS[样式表]，”咨询师说。用户可以利用，打开一个网页托管这个漏洞。

微软可信赖计算集团经理卡莱娜 Chmaj，在一篇博客文章中表示，微软还没有收到任何关于该漏洞而受到攻击的报道或者受影响的客户。

但是代码证明了它的存在，一个提供安全的厂商和培训机构在周一，一个视频上演示了执行代码，而在周三，Metasploit 也把该漏洞作为黑客工具包一部分而发布。

虽然这个安全漏洞能够绕过两个内置的 Windows 安全功能，数据执行保护（DEP）和地址空间布局随机化（ASLR），但是 Vista 和 Windows 的保护模式在目前的攻击中限制了该漏洞的影响，Chmaj 写道。

微软在下一个周期 1 月 11 日发布安全补丁。截至目前，该公司还没有计划打破原有的周期为这个漏洞发布补丁程序。

“不过，我们正在非常密切的监视这个漏洞所带的威胁”，Chmaj 写道。

企业推荐

北京智恒联盟科技有限公司

北京智恒联盟科技有限公司成立于 2006 年，是国内专注于 web 安全研究开发以及数据保密安全的领军企业，下设十多个分支机构，截止目前，全国拥有 120 多人服务团队，90%本科以上学历，15%硕士以上学历。基于多年的持续安全技术研究，尤其在网站防篡改技术、黑客攻击及防御技术、信息数据销毁、深度木马检测、服务器安全防护以及应用层深度威胁检测等领域积累了丰富的经验，国内最早专注于研究开发第三代网页防篡改防护系统；公司的产品和技术研究成过近四年来得到了全国众多用户的青睐和支持，尤其在国家部级机关等重要领域得到了高度认可。据权威机构调研，WebGuard 荣获 2008 年-2010 度“网管员最喜爱的网页防护系统”奖、“最值得信赖品牌奖”、WebPecker 网站安全扫描系统荣获“绿色 IT 产品推荐”奖以及 2010 年软件国际博览会“最佳创新奖”等等，在我国奥运举办和“神七”发射期间，公司产品在部分重要领域作出了突出贡献。

大多客户在业务应用方面集中精力持续关注，在信息安全技术方面由于技术发展迅速，往往难以熟练掌握相关技术进行完善的自我保护。智恒联盟全力打造业界“最易用”的软件系统，经过多年精心研发，推出一系列针对网站安全产品和安全保密产品。智恒联盟的安全产品包括：WebGuard 网页防篡改保护系统、WebPecker 网站安全统一监控系统、WebGuard-WAF 综合安全应用网关系统、TrojanChecker 恶意程序辅助检测系统、DataGuard 电子文档保护系统、SecureWipe 移动介质信息消除工具等。其中多项安全技术弥补了国内技术空白，公司以强大的售后支持和极具实用价值的独家功能得到了广泛赞誉，尤其在政府、金融、电信运营商、军工、大中型企业、能源、教育、医疗、电子商务等领域得到广泛应用。公司除产品外，还为客户提供全面的风险评估、安全运维、安全加固、安全管理策略制定等专业安全服务。

北京智恒联盟科技有限公司研发团队由国内众多顶尖级研发人员组成，领先的技术和持续不断的创新精神是企业前进的动力，公司与国内多个著名高校建立了长期深入技术合作，我们将不断努力，研发出更多先进、易用的软件系统！

公司愿景：安全创造价值。

公司使命：成为用户身边最值得信赖的信息安全产品和服务提供商。

公司战略：通过持续不断的技术创新为用户提供最佳安全实践。

公司价值观：以专业的精神，向客户提供最具竞争力的产品和服务，尽心尽责。

中国信息安全博士网

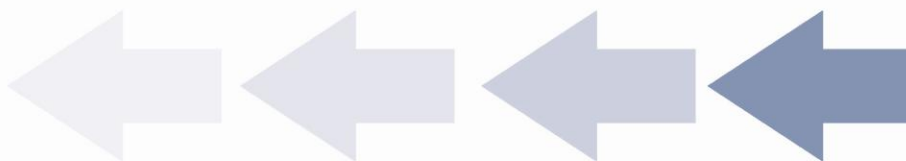
www.secdactor.com



高端访谈

聆听信息安全 访谈高端人物

中国信息安全博士网作为中国信息安全行业的高端智库平台，一直在我国信息安全行业发展过程中贡献着自己的力量。智慧的对话，思想的交锋。政府官员、专家学者、社会名人、国际友人做客中国访谈，解读政策法规，阐释新闻热点，讲述世界风云，倾诉人生故事。秉承权威、人文、开放、深入的原则，为网友展现不同人生的精彩历程。为行业发展、产业进步提供建议。将客户的相关文字、音频或视频文件放在中国信息安全博士网高端访谈栏目进行宣传。



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