科教新闻

沈阳分院召开2008年院地合作委员会工作会议

中科院东北振兴科技行动计划项目顺利通过阶段检查


路甬祥会见辽宁省委书记张文岳

沈阳市委书记曾维视察沈阳芯源公司和沈阳新松公司

科教新闻

等级保护：突破网络安全瓶颈（中国科技信息）

发布时间：2007-7-9

防火墙越“砌”越“高”，入侵检测越做越复杂，病毒库越来越庞大，依然无法应对层出不穷的恶意攻击和病毒，尤其是无法禁止已经在电脑硬盘中驻存的一些恶意程序向网络肆意传播。

“堵漏洞、做高墙、防外攻，防不胜防。而等级保护政策的推行是现在信息安全保障的主要环节。”中国工程院院士、国家信息化专家咨询委员会委员沈昌祥这样概括目前信息安全的基本状况。在第八届中国国际计算机网络和信息安全展览会高峰论坛上，已于6月正式全面启动的信息安全等级保护新政策成为专家们讨论的热点。

从终端开始防范

目前，整个信息安全状况存在日趋复杂和混乱的趋向：误报率增大、安全投入不断增加、维护与管理更加复杂和难以实施、信息系统使用效率大大降低、对新的攻击入侵毫无防御能力，尤其是对内部没有任何防范。

沈昌祥指出，目前我国信息与网络安全的防护能力处于发展的初级阶段，许多应用系统处于不设防状态。国防科技大学的一项研究表明，我国与互联网相连的网络管理中心有95%都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是攻击重点。

当前的信息与网络安全研究，处于忙于封堵现有信息系统安全漏洞的阶段。要彻底解决这些迫在眉睫的问题，归根结底取决于信息安全保障体系的建设。　　“目前，我们迫切需要根据国情，从安全体系整体着手，在建立全方位的防护体系的同时，完善法律体系并加强管理体系。只有这样，才能保证国家信息化的健康发展，确保国家安全和社会稳定。”沈昌祥说。

“我们必须控制引发不安全问题的根源。”沈昌祥说。事实上，所有入侵攻击都是从个人电脑终端上发起的，黑客利用被攻击系统的漏洞窃取超级用户权限之后，才大肆进行破坏活动。此外，即使是合法用户也应该纳入严格的访问控制，因为再坚固的堡垒也会从内部被攻破。据2002年美国FBI统计，83%的信息安全事故为内部人员对外勾结所为，这一比例还呈上升趋势。所以，如果合法用户可以进行越权访问，也是一个非常大的安全隐患。

“现在的不安全问题都由PC机结构和操作系统的不安全引起。”沈昌祥说，“如果在终端操作平台实施高等级防范，这些不安全因素将在源头即被控制。恶意攻击手段变化多端，原有应对措施都是采取封堵的办法，捕捉黑客攻击和病毒入侵的特征信息，然而攻击特征都是滞后信息，不能据其科学预测未来的攻击和入侵。”

“这显然不合理，我们要改变思维方式，从终端开始防范攻击。把不同信息系统分成不同的安全级别，然后严格按照安全级别所规定的要求，从事信息活动。目前，我国正积极推动这一信息安全等级保护制度，以最大限度避免系统安全漏洞和低级庸俗内容带来的信息安全风险。”沈昌祥在各种场合这样反复强调。

信息安全重在管理

如何在终端做到安全防范？信息安全等级保护措施的出台也许是一个好消息。信息安全等级保护的试点工作从去年开始在国家各重要部门实施。虽然信息安全等级保护标准和一些相关要求已提出多年，但大部分用户和信息系统管理人员对之了解甚少，这已经成为标准推广的难点之一。

“事实上，信息安全等级保护的核心思想就是根据不同的信息系统保护需求，构建一个完整的信息安全保护体系。分析《计算机信息系统安全保护等级划分准则（GB 17859-1999）》可以看出，信息安全等级保护的重点在于内网安全措施的建设和落实。建立一个完整的内网安全体系，是信息系统在安全等级保护工作中的一个重点。”公安部公共信息网络监察局郭启全说。

据介绍，信息安全等级保护涉及政府机构中多个部门的职能，信息系统安全等级保护监管级别划分为：第一级，自主性保护；第二级，指导性保护；第三级，监督性保护；第四级，强制性保护；第五级，专控性保护。政府信息安全保护职能部门应当逐级加大安全保护力度。系统主管部门也应按级加强自管、自查、自评力度。

专家们认为，分级分类是等级保护的关键。如果信息系统的分级分类不科学，安全保障建设也将事与愿违，甚至可能使我国的基础信息网络和重要信息系统面临严重安全隐患。

“等级保护中的分级实际上涉及两项工作，不能混为一谈。一是如何将信息系统划归到各个安全级别中，二是为每一级的信息系统规定安全要求。”郭启全说。

沈昌祥认为，等级保护应根据信息系统的综合价值、综合能力保证的不同要求以及安全性破坏可能造成的损失来确定相应的保护等级。

“分级更重要的是为信息系统‘对号入座’。现在我国提出五种级别、五种类型，其实各个类型里头也分不同的级别，应该科学考虑。同一个类型也可以采用不同级别的具体措施。像美国的做法是，提出保密性、完整性及可用性三

性，并为每‘性’划出高、中、低三个等级。”沈昌祥说。

郭启全认为，信息安全等级保护制度的制定与实施，将逐步把信息安全等级保护制度落实到信息安全规划、建设、评估、运行维护等环节，使我国信息安全保障状况得到基本改善。同时，信息安全等级保护制度实施后，我国信息安全厂商的相关产品也应针对等级划分进行有针对性的调整，这对整个安全产业的未来发展有重要的指导意义。（摘自中国科技信息网）