网络技术

- 卫士通计算机通讯系统常见故
- 建好五本台帐 推进计算机
- 卫士通计算机通讯系统常见故
- 党政机关计算机通信系统的现
- 加强管理维护 确保网络畅
- 浅谈办公自动化建设中的若干
- 计算机泄密的主要途径与防范
- 谈秘书沟通的网络资源
- 党务内网的内部安全隐患与对
- 秘书知识产权网络环境保护之

活动竞赛

- 秘书竞赛领证通知
- 秘书竞赛部分照片
- 竞赛获奖选手晋级核准表
- 竞赛获奖选手办证通知
- 赛前提示
- 竞赛考场安排
- 竞赛赛程
- 职工组竞赛名单
- 学生组竞赛名单
- 有关竞赛事项的调整

办公自动化的网络安全问题及对策探析

作者：翟峰 发表时间：2006-9-2 访问：567次

西方在二十世纪五十年代提出了“ 电子数据设备簿记忆 功能”，六十年代出现了”信息管理系统”，七十年代 ”未来办公室”、”无纸办公”提上了应用发展日程，八十年代”办公自动化”理念基本形成。我国办公自动化工作起源于二十世纪八十年代中后期，是从电子打字机、传真机、复印机、轻印刷系统逐步向计算机及其互连网、移动通信应用过渡的。时光延续到二十一世纪的今天，已发展到了有办公的地方就有办公自动化的运用程度。

可以说，办公自动化确实给我们今天的文秘工作带来了极大的便捷和极高的效率——现在文件打印及存储可以用电脑，资料图片要保存可以用扫描仪将其转化为EDI(电子数据);要获取外界信息可以上互连网 浏览，感兴趣的也可以下载；要传递信息的可以用电子信箱;甚至更先进的电子邮局；企业内部进行沟通与流程操作的可以通过内部网络来完成，既具保密性又很方便;如果配备具有办公室功能的手机的话，则可以在旅途中完成一切文字及图片资料的起草、修改、打印、储存、检索、传递等工作;发传真、打印文件、电话、电脑网络会议，可视对讲，真的是一切尽在掌握中。此外，办公自动化所涉及的范围又很广泛，除上述运用范围外，还可运用电脑网络系统进行档案储存检索管理、日程安排、会议安排、人事行政管理、财务管理等一切涉及信息化办公范畴的运用，客户联络、业务洽谈、合同签约、公共关系及至企业内部运作，都可以借助先进的计算机系统来解决，从而为我们的文秘工作省下了大量的精力和时间，使我们的文秘工作能抽出更多的时间从事更重要的决策性或策划性的工作。

但是，我们在分析办公自动化给我们带来的便捷和效率的同时，也要看

到，由于我们目前的办公自动化所使用的计算机硬件和软件操作系统基本还处于Winlnter(微软、英特尔的合称)之下，而汉字编辑排版（含表格)、图形、图像、声音等应用软件却有多种格式标准，相互间交互使用，通常用"兼容"、"转换"来完成，其最终相容率很难达到百分之百，不能显示图形、图像或显示出的格式不对等现象也时有发生。加之目前我国信息业仍处于发展过程中，安全软件的开发及对计算机病毒和网上黑客的防范措施还不力，故而使我国这些在大规模社会化办公自动化系统中存在的这些隐患还一时难以彻底消除，还需要我们正视这些问题的存在，并据此采取切实有效的防范对策。

鉴于上述，笔者认为，要正视办公自动化方面存在的问题，首先即应对这些问题进行认真探析。归纳起来，办公自动化的安全隐患问题主要有如下几种:

一是“黑客”入侵

"黑客"是英文 "Hacker"的音译，最初是指那些热衷于计算机程序设计的人，现在则专指利用通信软件及联网计算机，通过网络非法进入他人系统，截获或篡改计算机数据，危害信息安全的计算机入侵者。随着计算机技术的飞速进步和互连网的普及，许多"黑客"的活动已开始从寻求刺激、炫耀技能的恶作剧演变为利用网络技术从事经济或政治犯罪活动，其形式也开始由个人行为向有组织方向发展。在网上，"黑客"几乎无处不在，党政机关的核心机密、企业的商业秘密及个人隐私等均在他们窥视之列。"黑客"中有的破坏党政机关及办公机构的网站，使它们突然瘫痪或不能正常工作，有的窃取银行帐号，盗取巨额资金，有的以窃获的文秘机密资料为要挟，进行网上恐怖活动。

与常规犯罪相比，"黑客"犯罪有许多新特点。一是智能性。作案者一般都具有相当高的计算机专业技术知识和娴熟的计算机操作技能，作案前往往经过周密策划，与反"黑客"力量斗智周旋。二是隐蔽性。"黑客"犯罪是在由程序和数据这些无形要素组成的虚拟空间里进行的，往往不受时间、地点限制，因此，难以对作案者进行追踪和监控。三是社会危害性大。大量事实证明，礼会对网络系统的依赖性越大，计算机犯罪的发案率就越高。近些年

来，"黑客"犯罪正在像瘟疫一样迅速波及到计算机网络的每一个角落，给社会造成的危害也越来越大。

二是“病毒”破坏

《中华人民共和国计算机信息系统安全保护管理条例》 (1994年2月18日国务院147号令)对计算机 "病毒"的定义是:"计算机病毒是指编制或者在计算机程序中插入破坏计算机或毁坏数据、影响计算机使用，并能自我复制的一级计算机指令或程序代码"。电脑病毒是计算机独有的一种产物，是一种人为制造的，在计算机运行中对计算机信息或系统起破坏作用的程序，它通常隐蔽在其它程序或文件之中，按照设计者约定的条件引发，按照设计者制定的方式进行破坏。主要有四个特性:(一)寄生性。计算机病毒主要寄生在各类文件之中，并不单独存在，很多病毒将自身整个程序分成若干片断，分别依附在多个文件里达到隐蔽和防杀的目的。(二)破坏性。电脑病毒的设计者虽然心态、技术、目的各不相同，但对他人电脑工作环境的破坏欲却是不约而同的，其破坏作用主要表现在三方面:（１）干扰计算机正常工作;（２）毁坏计算机数据;（３）破坏计算机正常功能。第一方面通常被称为良性病毒，它们主要以恶作剧为目的，对计算机及其存储信息不构成实质性破坏;第二、三方面属于恶性病毒，它们经常造成数据被损、硬件被毁、系统无法恢复工作等恶性事实。(三)潜伏性。很多病毒的发作需要一定引发条件，不具备引发条件时，电脑工作无任何异样，甚至查索软件也无能为力，这一现象非常容易造成操作人员的麻痹大意。如某公司职员将工资表中连续两个月不出现自己的名字设为病毒引发条件（俗称逻辑炸弹)，结果在他被解雇两个月后，公司电脑全部瘫痪，大量数据丢失，而且病毒迅速沿网络蔓延。(四)传染病。病毒通常是靠感染特定的一类或几类文件来传播，并不断按照某种方式进行自我复制和衍出新的变种。如前不久出现的"怕怕 (PAPA)"病毒，在一台电脑上每传播一次（病毒不被清除，就会一次又一次的传播)，就可以感染网络中的60台电脑，这60台电脑又可分别各感染６０台电脑，如此延续，其几何数量级的增长，使传染数量和范围几乎与时间无关，而由单位时间内网上电脑的开机量决定。

三是“网”上泄密

随着电信事业的迅速发展，近年来党政机关单位和企业购买微机的越来越多，不少用户连接“因特网”，上网人数呈上升趋势。微机联网为党政机关

和企业实现办公自动化、了解掌握信息提供了便利条件，但也容易造成“网”上泄密。据报载，1999年5月北约轰炸南联盟期间，四川某国防军工机关文秘工作人员郭某出于爱国热情和对北约暴行的义愤，曾撰写文章在互连网上发表，文章涉及了我空军最新研制的新技术装备等重要机密。文章被国外若干互联网站转载，致使我国防秘密外泄。郭某的行为已构成泄露国家秘密罪。为此，成都市武侯区法院一审判处郭某有期徒刑8个月。

造成“网”上泄密的原因，一方面是由于少数文秘工作者缺乏保密观念和警惕意识，辨别是非能力弱，导致过失泄密;另一方面是由于有关部门严格审查和检查监督不力，导致境内外某些反动势力或个人有机可乘，利用“因特网”加强非法联系，并泄露国家机密。公安部近日破获一批“法轮功”组织及其人员非法获取、泄露党政机关秘密文件和案件中，有相当一部分是通过互联网发往国外的，给党、国家和人民造成了极大的危害。当然，我们分析办公自动化的安全隐患问题，其目的还在于更好的防范。而要防范，即应拿出切实有效的对策。

对此，笔者在深入探析的基础上，特提出解决办公自动化网络安全问题的八大对策:

其一，教育防范。一是要加强网络道德教育非常关键，要让那些具有计算机才能的人特别是青少年通过正当途径发挥自己的才能，不要成为人人喊打的黑客，甚至堕落为网络罪犯。即使是在网络这一虚拟的空间，人们也希望能拥有一片洁净的蓝天;二是要帮助“换脑筋”。引导党政机关和企业文秘人员看清形势，即要让他们知道，随着国门大开，国外情报间谍机构可以借机进入他们以前难以进人的产业和领域，搜集情报的活动更加广泛和方便，由于科学技术的迅猛发展，人才争夺和市场竞争日趋激烈，经济科技情报受到空前重视。如果“太平思想”严重，不注意保密和自我保护，党政机关的机密文件就会在网上泄露，企业在激烈竞争中就有被淘汰出局的危险。

其二，保密防范。一是要建立网上保密工作机构。即大中机关或厂矿企业都要建立保密工作领导小组，具体负责领导本单位本部门的保密工作。各级保密委员会或保密领导小组都要及时制定年度保密工作计划和保密中长期规划，认真贯彻实施，并经常(每季度至少一次)研究保密工作，解决实际问题。二是要严格按国家规定，党政机关在建设信息网络系统时，必须同步建设安全保密体系，包括物理级、网络级、系统级、应用级四个层面，具体包

括网络隔离、加密、安全检测与监控、防黑客、防病毒、访问控制、身份认证、安全管理等几十项内容。三是要尽快建立我国政务信息化标准体系;不失时机地建立国家和省区市两级政务信息化数据中心，集中管理，减少维护费用;确保"三网一库"安全，提高安全意识，落实安全措施，从源头上抓安全防范。

其三，制度防范。一是要建立健全信息防御法规制度，严格信息安全管理工作。信息安全离不开严密的法规制度和综合管理，任何一个环节上出现问题都有可能造成泄密。因此，制定和完善有关法规和制度，并严格加强统一管理，做到有章可循、依法办事，在网络内部筑起一道由法规制度铸就的"防火墙"。二是单位上网实行上网前申报和上网后审查制度，加强对上网人员的监督，减少泄密人员上网的机会，防止过失泄密。三是规范秩序，加强对单位上网进行管理，认真按照《中华人民共和国计算机信息网络国际联网管理暂行规定》，严格审查和控制，并采取有关技术防范措施，堵塞有害信息传播和泄密渠道。四是加大检查监督力度，严厉打击网络违法犯罪活动，减少和防止 "网"上泄密事件的发生。

其四，黑客防范。目前网络安全的防护措施多数是采用网络防火墙软件，监视和预防黑客程序的入侵，并在受到入侵时预告报警。该方式只能抵御约30%的黑客渗透，最根本的方法还是人工技术性防御。如今年5月8日后，美国对我国部分网站进行狙击，其中新浪网站、中文热讯网站的管理员(简称网管)防卫得当，网页岿然未动，而上海网盛站点 (http:www.netsh.com)不幸被击中，被迫关闭数日。有人预言，网络带来了一个纯技术的世界，这对当今和未来的现实对党政机关上网(广域网和专线网)的防范黑客入侵的安全与保密工作提出了严肃而沉重的课题。

其五，病毒防范。亡羊补牢不如未雨绸缪，对付电脑病毒最好的方法是拒其于电脑之外，主要防范方法有:1，不使用非正版软件。2，对外来软盘、光盘 (包括正版软件)首先进行检毒和杀毒。3，装入正版防毒软件，并启动其监控功能。4，同时使用两种以上防毒软件，经常检测磁盘和光盘。5，杀毒软件至少每月升级一次，了解到新病毒出现的消息，立即向有关网站(如上提供)寻找防御和杀灭方法。6，不在网络中胡乱交往，拒收来历不明的电子邮件。7，不进入内容繁杂的民间网站或主页，不下载与工作无关的软件。

其六，密码防范。现在的一些黑客软件，能在ISP(网络服务商)的主机上

根据你的用户名来破译上网密码。因此，最好经常修改密码，并且长度不少于8位，如含有控制码、大小写字母则更为理想。要做到密码防范，还应注意不要把自己的生日当作密码，把自己的电话号码当作密码，把自己的身高体重当作密码。就好像过去人们常把存折塞在床铺底下，藏在柜子顶上一样。可是，黑客也是居家过日子过来的，但凡有点儿蛛丝马迹，无疑就成了他们破解密码的钥匙。尤其须注意，不要向任何人透露密码。一些 "小人"常常冒充你的ISP，编出一些诸如由于系统更新，需要你的密码之类的谎话。千万不要上当。ISP是不会向你询问密码的。

其七，产品防范。一是要加强网络安全建设，就应研究和建立我国自主的网络信息安全平台产品及其标准体系已成为当务之急。二是要搞好我国网络系统的软硬件的开发。三是要认真研制先进的信息防护技术，尤其是特别重视自主开发党政机关系统内部的综合性信息技术，以提高防范能力和信息检查水平。

其八，技术防范。一是要加强网络防御，阻止未经授权非合法用户进入系统，最可靠的方法是对计算机进行物理隔绝。自理机密信息的计算机不能与同一地点的低级计算机连接;也不应连接因特网或可能使其它不可靠系统联网的调制解调器。二是要让电脑网络具有时实监控、即时杀灭、联网自动升级等功能。为此，操作者对所使用的电脑要有一定熟悉程度和感知能力。如对软盘存取异常、系统起动超时、软件运行过缓、无故读写硬盘等变化要有所体会，引起警觉，及时作出相应反应，并善于运用各网站提供的在线杀毒功能，进入相关站点对电脑进行查毒和杀毒。三是要注意E—mail附件。即当收到的电子邮件中带有附件（特别是可执行文件），千万别轻易打开，除非有把握，知道是谁特意寄给你的。因为，现在有很多病毒都是通过电子邮件的附件传播的。像前一段时期的"美丽莎"病毒、"Happy99"病毒、"PaPa"病毒等。一旦运行了这些附件，病毒就会感染你的电脑，并且通过你发送的电子邮件感染你的电脑。另外，网上还有一些居心叵测的人，喜欢通过电子邮件附件发送一些黑客程序。一旦执行了这些程序，上网后你电脑的控制权就落入他们手中，他们可以随意操纵你的电脑，盗取你的上网密码，安装和删除你电脑中的文件。

上一篇： 没有相关信息

下一篇： 没有相关信息

发表评论

用户名：

密　码：

验证码： 7683

发表我的评论

最新相关评论

暂无评论

友情链接：环球政务网 中华秘书网 四川秘书网

博客友情链接：潜人才BLOG

湖南省秘书学会 联系电话：0731-2215063 传真号码：0731-2218084

湖南师大文学院考培中心 联系电话：0731-8644039

湘ICP备06013617号 长沙智诚网络提供技术支持