第 3 卷◆第 2 期◆版本 1.0◆2020 年
文章类型：论文|刊号（ISSN）：2630-4759 /（中图刊号）：270GL018

计算机网络安全及其防范措施探究

童长卫
中共龙岩市委党校
DOI:10.32629/ej.v3i2.435

[摘　要] 随着我国计算机及网上办公的不断普及,计算机网络随处可见。在单位不但有互联网,还有政务网、办公网、无线网等各类网络。网络成为电力之外,生活、办公不可或缺的基本物质基础。但随之而来的计算机网络安全问题也层出不穷。这其中既有网络技术层面的问题,但更多的是使用者缺乏安全意思所至。本文对计算机网络安全存在的问题,特别是一些人为因素进行分析、讨论并提出自己的一些观点,希望对今后的相关研究起到一定的参考作用。
[关键词] 计算机网络；防范意识；安全隐患；信息安全；等级保护

近些年来,我国计算机应用及电子政务的日趋普及,特别是大数据、云计算机的出现,对网络的要求越来越高,不但是要求方便、快速,而且要求稳定、安全。另一方面,随着国际情形的日趋复杂,网络空间已经成为新的新的主权疆土,网络正面临全新的威胁。既有国家成面的,特别是意识形态的威胁,也有普遍的经济犯罪的威胁。既有来至外部的传统黑客组织的威胁,也有主要来至内部的极端个人的威胁。因此,在当今时代,为保证国家安全、单位信息安全、个人信息安全,应从各个层面加强网络安全。特别是要让用户提高安全意识,增加防范水平。同时在监管方面,相关人员应对网络安全知识的宣传力度进行加强,进而加大环境本身的可靠度和稳定性,使经济良性运行。

1 计算机网络安全中存在的问题

1.1一些计算机系统及网络本身自带的漏洞问题

计算机操作系统目前基本是Microsoft(美国微软公司)的WIN系列一统天下,win系列操作系统由于自身的原因,存在各种漏洞,面临各种威胁。常见的威胁有5类：计算机病毒、逻辑炸弹、特洛伊木马、后门、隐蔽通道。同时,WIN操作系统是一个非开源的操作系统,在国际情势日趋复杂的今天,其安全问题特别值得重视。另一个方面,网络的基本协议TCP/IP也决定了网络的不安全性。一是明文传输给数据安全带来巨大隐患,二是由于TCP采用三次握手来建立一个连接,不可避免的容易探到SYNFlood攻击,三是IP协议是根据IP包中头中的目的地址项来发送IP数据包,这样就不可避免的存在IP欺骗引起的各种攻击。再者,软件开发人员在进行应用系统开发时往往只注重系统功能的实现,偏向于界面设计、功能体验以及响应时间、并发数等方面的性能考虑。对安全方面一般只注重用户名与密码的设计,对系统存在的漏洞,数据传输过程的加密,特别是架构方面的漏洞考虑不全。软件步骤前没有经过严格的安全测评[1]。所有这些都造成了计算机系统、网络及各类运用系统中存在大量的安全隐患。所以我们说没有绝对的安全,关键是建立适合的信息安全策略。

1.2大量病毒存在于计算机及网络之中

由于计算机及网络本身存在各种漏洞,各形黑客(包括个人和组织)出于不同目的,制造了大量的病毒。传统病毒通过移动介质进行传播,防范较为简单容易。随着蠕虫病毒的出现,现在的病毒基本都依靠网络(包括邮件、网页等形式)进行传播,它们传播速度快、传播面广、防范较为困难,危害极大。像永恒之蓝勒索病毒,它通过邮件、网页、木马等形式进行传播,它通过对用户文件的加密阻止用户对文件的访问,一旦感染很难破解,如果没有备份,基本无法恢复受感染文件,只能受其勒索,从而造成极大损失。同时,随着智能手机的普及,出现了大量针对手机的病毒[2]。它主要通过诱导用户打开不明链接的方式进行传播,它会导致用户手机死机、关机、自动发送短信或拨打电话等,严重的可以窃取用户资料,包括用户帐户信息。因此,计算机病毒是网络安全的主要威胁之一,必须重点防范。

1.3用户本身不规范的操作方式

大多数的信息安全事故都是由于人为的疏忽或不规范的操作方式引起的。前面提到的永恒之蓝勒索病毒所造成的损失最严重的单位(企业)互联网,而是与互联网物理隔离的企业局域网。正是由于企业局域网与互联网相隔离,系统升级、补丁较为困难,同时,也造成技术人员思想上的麻痹,认为相对独立的企业局域网是较为安全的。因此,一旦企业局域网感染病毒,会速度全网传播,短时间内造成重大损失。还有,许多同志由于知识结构及年龄等原因,网络知识、操作技能偏差,安全意识不强。例如,在密码设置方面过于简单、密码更换频率低、对个人信息的忧患意识不足等进而部分个人信息被非法应用。有个单位,重要领导在内部OA中的密码从来没有变更过(还是系统启用时默认的8个8),有个内部员工多次冒用领导用户名与密码进入系统,造成重要文件(信息)泄密[3]。

2 在计算机网络领域中应使用的安全防护方式

2.1加强教育与培训

第一,提高用户的安全意识,特别是单位领导和重要岗位人员的安全意识。要让他们了解网络安全威胁的严重性。制定完善的安全策略并始终贯彻。第二,加强安全技能培训。针对单位特殊人群要制定特殊的培训方法。第三,加强网络安全规章制度的建立。对各种网络行为做出规定。第四,定期检查。针对特殊人群的电脑要有专人负责。包括杀毒软件的安装、密码强度、补丁等。

2.2网络信息安全等级建设

《中华人民共和国网络安全法》由全国人民代表大会常务委员会于2016年11月7日发布,自2017年6月1日起施行。网络安全法明确规定必须按等级保护要求对信息系统进行安全保护。网络安全等级保护制度新标准(2.0)从2019年12月1日正式实施。等级保护建设一般需要：

①定级。各单位首先必须根据单位性质、相关文件规定,确定本单位等级保护级别。编写定级报告。《GB/T22239-2019》规定了第一级到第四级等级保护对象的安全要求,每个级别的安全要求均由安全通用要求和安全扩展要求构成。

②备案。准备备案材料向当地网安部门备案。

③建设整改。对照标准,找出本单位的不足,制定方案,进行整改。包括技术安全和管理体系两方面。增加必须的安全产品和服务,如防火墙、入侵检测、堡垒机、网页防篡改、安全审计等软硬件。

④等级测评。准备和接受测评机构的测评。

⑤监督检查。接受当地网安部门的定期检查。

2.3同步建设

过去由于资金等原因,各单位在信息化建设中,往往采用分步走的方式,把安全建设与应用分开,首先考虑的是应用建设,再考虑安全建设。这种建设思路与方式违背了网络信息保护建设必须与应用同步规划、同步建设、同步运行的要求。在进行新系统设计、预算时必须同步考虑信息安全建设。

2.4数据加密技术的应用

在开放的网络环境之下,数据加密技术可以有效的保证数据传输的安全,增强数据保密性。除此之外,其不仅可以较大程度的预防被动式的攻击行为,进而对计算机系统的安全性进行更深层次的提高。值得注意的是,数据加密技术可分为对称式和非对称式加密两种类型。其中,对称式加密技术形式较为简单,其加密与解密的密匙一一对应即可有效的保障交互信息的隐秘程度；非对称式加密技术由解密与加密两部分组成,加密是以某种特殊的算法改变原有的信息数据,使得未授权的用户即使获得了已加密的信息,但因不知解密的方法,仍然无法了解信息的内容；解密则将密码转变成简明文本的过程。

2.5加大对VLAN网络技术的普及

VLAN的中文名为虚拟局域网,VLAN是一种比较新的技术,工作在OSI参考模型的第2层和第3层,凭借这一特点可以将同一局域网络的直接通信变为现实,更进一步的达到数据的融合共享。除此之外,VLAN有着传统局域网无法达到的灵活性,并且还能够节约管理成本以及有效的抵制恶意攻击,进而使计算机网络的稳定与安全得到进一步的提高。

2.6加大对生物识别技术的使用

在网络环境中专门的管理人员一般凭借系统及程序的重要生物特征进行验证工作,从而防止黑客对系统的关键功能造成损伤。由于生物特征存在一定的不可复制性,因此其安全防护上较密码身份验证等更加可靠安全。这样,指纹、面部识别等验证方式可以更好的帮助管理人员维护网络环境的安全。

2.7安全服务外包

网络安全涉及面很广,专业性很强。大多数中小企业(单位)不具备这方面的专业人材。近年来,不少企业(单位)都将信息化服务特别是安全服务外包,取得了较好的效果。信息安全服务外包具有以下优势：

①技术优势。专业的安全公司具有专业的安全团队,一般是安全产品生产厂家或得到厂家的全面支持,能提供全面的安全服务。

②反应更及时,服务更全面。安全公司拥有一套较为完美的安全服务体系,能提供24×7的服务,包括网络安全监测。一旦出现安全问题能快速响应并解决。

③更低的成本。相比较企业自己聘用高水平的安全专家,将服务外包成本更低。当然信息服务外包也存在一些风险,如信认风险、依赖风险等,如何避免这些风险,选择一家具有相应安全资质,服务周到的公司是关键。

3 结论

综上所述,怎样对计算机网络安全进行有效管理,如何为用户提供一个安全、可靠、便杰的网络环境是当今时代的一大焦点话题。一方面要对用户加强管理、教育、培训,增强自我安全防护意识,规避网络风险。另一方面,要通过技术的、管理的、法律的各种手段完善计算机网络安全环境,从而使计算机网络技术的潜在价值得到进一步的开发,使我国社会发展得到进一步的提升。

[参考文献]

[1]李泰.计算机网络安全问题及其防范措施研究[J].通讯世界,2019,26(09):183-184.

[2]赵晓松.浅析计算机网络安全问题及其防范措施[J].湖北开放职业学院学报,2019,32(13):109-110.

[3]朱慧超,谢新屋.计算机网络安全问题及其防范措施研究[J].信息与电脑(理论版),2019,(12):225-226.