计算机网络的数据安全策略重点分析

岑　莉
江西软件职业技术大学　江西南昌　330000

摘　要：随着计算机网络技术的飞速发展，数据安全也存在了较大问题，由于计算机网络系统存在漏洞、群众网络安全意识较为薄弱、专业网络技术人员专业能力较低、存在黑客、木马等入侵等问题的存在，使得个人、企业等的网络数据信息存在泄漏、篡改等风险，对个人、企业等的发展带来较为严重的损害。因此，有关人员要重视网络安全维护工作，要积极地提升人们的网络安全意识，加强对网络行为进行监督，强化个人、企业的数据安全保护，不断地优化和改进网络入侵检测技术，并且还要强化专业技术人才队伍建设，促进网络安全保护技术水平的提升，从而更有效地确保计算机网络的数据安全，营造更加优质的网络运行环境，维护社会各行业的良好发展。

关键词：计算机网络；数据信息安全；防范策略

The key analysis of data security policy of computer network

Li Cen
Jiangxi University of Software Professional Technology, Nanchang 330000, China

Abstract: With the rapid development of computer network technology, there are also big problems in data security. Due to the vulnerability of computer network system, the weak awareness of network security of the masses, the low professional ability of professional network technicians, and the existence of hacking, Trojan horse and other problems, the network data information of individuals and enterprises is exposed to leakage, tampering and other risks. The development of individuals, enterprises and so on has brought more serious damage. Therefore, the relevant personnel should pay attention to the maintenance of network security work, to actively enhance people's awareness of network security, strengthen the supervision of network behavior, strengthen personal and enterprise data security protection, constantly optimize and improve network intrusion detection technology, and also strengthen the construction of professional and technical personnel, promote the promotion of network security protection technology level, Thus, it can ensure the data security of computer network more effectively, create a better network operating environment, and maintain the good development of social industries.

Keywords: Computer network; Data information security; Preventive strategy

引言

由于现代通讯科技的发达，电脑的使用也更加普遍，从计算机网络的兴起到现代计算机网络的发展速度已经很快，现代计算机网络在实际生活中已经给人类带来了大量宝贵的信息资源，在各个领域使用的过程中，不但对互联网自身的稳定性提出了相当高的要求，而且也对现代计算机网络系统管理维护工作有着较高的需求。

一、计算机网络的概念与安全指标

1.概念

计算机及网络安全可以分为两种，一是物理安全，二是逻辑安全。前者是指计算机的硬件安全，即与计算机相关的设备设施的安全，后者主要是指计算机软件系统的安全，即计机软件系统不会遭受恶意侵害，信息不受盗取。

2.网络安全的指标

（1）保密性

有关人员利用加密技术，将未被授权的用户自动过滤出去，不能访问有关页面，只有那些经过授权的用户才能够访问有关页面，进入相应的数据库，通过这种方式，可以有效保证用户信息的安全；

（2）授权性

有关人员依据计算机网络中可以利用的信息数量以及访问的意图给予用户相应的权限。

（3）完整性

计算机网络信息有可能被窃取，也有可能一些非法信息进入其中，破坏其完整性，为此，有关人员通常会利用散列函数保证信息完整，也可以利用加密手段来避免非法信息的侵入；第四，可用性，网络信息系统中所存储的信息必须可用，否则也就失去了价值，但是有些情况，网络信息系统遭受侵害，很有可能信息失效，无法应用，为此，有关人员优化系统设计方案，使其在遭受侵害时，信息也能够自动回复；最后，认证性，所谓计算机网络认证，简单地说就是指保证网络权限的所有者与提供者是相同的人。现阶段计算机系统认证方法有数据源认证，通过信息数据源来对用户进行认证的一种方式，还有一种是实体性认证。无论哪一种认证方式，现阶段都能够应用。

二、计算机网络的数据信息安全问题

1.用户网络安全防护意识不足

计算机网络的数据安全管理工作不仅需要具备良好的网络系统和网络环境，还需要网络使用者能够具备良好的数据安全防范意识，能够掌握更多的网络安全防护知识和技能，能够正确地使用和应用计算机网络技术，规范自身的网络使用行为，从而为自身的数据信息提供良好的保护，尽可能地避免自身的数据信息被滥用。但是，在实际网络使用过程中，较多的用户缺乏良好的数据信息安全保护意识，对计算机网络使用行为的规范性还缺乏全面地掌握，这就容易使得自身的网络使用行为存在安全隐患。目前，较多的网络用户对于计算机网络的使用，往往关注的是网络技术的便利性，借助计算机网络技术实现交流和工作的便利，但是对计算机网络中存在的安全隐患缺乏重视和认识，对一些隐藏病毒、木马等的文件和网站无法有效地识别，这就使得在下载文件、链接或者是浏览陌生网站时会为计算机设备带来病毒，部分用户在使用计算机网络时，往往会由于个人的操作不规范，在一些陌生的网站、链接地址中填写个人信息、下载一些游戏、娱乐软件等，导致个人信息被泄露，为个人带来极大的不便。而且，还有部分计算机网络用户由于缺乏良好的数据信息安全保护意识，则不进行安全认证防护，对于个人的计算机设备缺乏密码设置，个人账号设置的密码则也较为简单，这就使得个人设备以及账号密码更加容易被破解，从而导致自身的数据信息被窃取和泄露，为自身的数据以及财产信息带来了较大的安全隐患。对个人的数据信息的保护力度较低，一些企业在计算机网络使用中，往往缺乏良好的信息安全管理制度，使得企业自身的网络信息系统容易遭到破坏，从而导致企业的财务数据、运营信息等发生泄露，影响企业的良好发展和运作。

2.计算机病毒入侵

在计算机网络的应用中，木马病毒十分常见。这些病毒通常会在系统或操作软件中潜伏，在用户操作中实现相应的信息获取，并造成相应的破坏。在计算机网络安全防护技术的发展中，木马病毒的更新也呈现出了惊人的速度，且具有了越来越强大的隐蔽性和攻击性。如果用户的计算机被木马病毒入侵，其中存储的信息便会受到严重破坏，严重的情况下甚至会导致用户的计算机系统瘫痪，对其正常使用和信息安全造成严重威胁。

3.黑客非法攻击

在当今的信息化时代中，借助于计算机网络，人们可实现所需信息的轻松获取，但是这样的模式也为黑客的非法攻击提供了更多的便利。通常情况下，黑客都具有独特的计算机网络技能，且其攻击一直呈现出一种无差别的状态，也就是任何用户的计算机都有可能受到黑客攻击。在这样的情况下，如果不能做好网络信息安全防护工作，用户的网络信息将会受到严重威胁，甚至会给用户带来重大的经济损失。

4.计算机软件漏洞

在计算机网络的应用过程中，借助于各种计算机软件，用户可获取到各方面的网络信息服务。在计算机网络的不断发展中，越来越多

的计算机软件得到开发并投入应用，从而为用户提供了更多的便利。但是在软件开发中，因内部和外部各种因素的影响，使其本身难免存在一些漏洞。而来自外界的攻击刚好可以对这些软件漏洞加以利用，从而对用户的网络信息进行非法盗取、篡改等操作。这样的情况如果得不到有效防治，用户的信息安全、财产安全乃至于人身安全都会受到严重威胁。

三、计算机网络数据信息安全的有效防护策略

1.加强网络安全防范意识

加强网络安全防范意识，加强计算机用户的个人网络安全意识，加强个人用户账号等信息隐私的防范意识。所有计算机网络共同使用同一个网络资源，因此个人在使用计算机网络过程中，要时刻保持警惕，远离计算机网络中的不稳定因素，远离不法分子和通过计算机诈骗人员的干扰，增加自身网络安全性。设置远程防控权限，增加密码的设置的难度，使用安全绿色的网络地址，有效保管账号信息，下载安全软件。利用安全的大数据技术排除计算机网络中的不稳定因素，及时修补计算机内部存在的漏洞。使用安全规范的网络监控系统。加强个人计算机网络安全的监管，不断完善账号的个人信息，提高个人和企业用户网络信息的隐私权意识，远离不安全的网络程序，处理以谋私利为目的的非法恶意盗用信息的入侵者。对于企业计算机网络用户，要聘用专业的计算机网络安全管理人员对企业的网络进行定期的安全维护，及时发现网络风险，快速高效的发现网络中不稳定及恶意破坏安全系统的信息，及时处理风险。提高计算机网络安全管理人员的专业技能管理技术，其专业素质能够胜任网络安全员的工作，提高计算机网络安全管理人员网络安全意识，关注安全网络管理人员的身心健康，时刻保证计算机网络的安全性。完善企业计算机网络安全法规制定和实施，完善公司内部网络安全部门及职责，保证企业计算机网络安全的运行和使用。定期检查维护企业大数据信息，加大网络安全宣传力度，预防因不正当操作给计算机系统造成的损害，对违规使用恶意软件损害公司网络的行为给予严厉处罚，加大计算机网络隐私使用权和力度，合法使用网络计算机大数据信息。

2.加强对杀毒软件应用的重视

要确保网络的数据信息安全，还需要加强对杀毒软件研发和应用的重视，要更加高效地、全面地利用杀毒软件，更有效地防止病毒和垃圾信息的入侵。因此，个人和企业在应该更加重视杀毒软件的应用，在个人以及企业网络运行中要安装安全管家、金山毒霸等相应的杀毒软件以及防火墙设置，通过二者的相互结合，确保个人以及企业网络系统的安全运行，此外，还要注重定期地对杀毒软件进行更新和升级，确保杀毒软件的作用能够更有效地发挥出来。同时，也可以设置邮件识别系统，更好地过滤一些垃圾邮件，也避免病毒通过邮件进行传递和入侵，确保计算机网络系统的可靠性。

3.提高安全审计信息的透明度

在互联网条件下，云计算服务应用将越来越安全可靠，并且互联网和云计算服务的安全应用需求将完全升级。平台开发者在提供客户服务以前，应该先通过我们国内有关机构的严密检测。当国内云计算网络平台完成运营的时候，其稳定性和数据安全将得以真正保障和应用。同样，云开发者应该经常向客户尽快传递审计后的资源，确保客户足够的信息安全。一旦在外包完全开启期间云计算数据泄漏，协议中会明确规定服务供应商要为客户的损失承担责任，而一旦业务后期发生的问题也应该由自己担当。另外，国家大数据服务平台云计算的领导将在平台建设过程中做出相应报告，并且对云计算的系统建设实施有效监管，还要求进一步加大对国家的有关部委的监管。并通过系统加强、自我认证和备案，以避免客户身份被盗和客户身份信息的丢失。

4.及时做好漏洞修补工作

用户在实际使用计算机过程中，必然会遇到系统漏洞问题，为避免遭受不法分子的攻击，作为用户应该及时做好漏洞方面的扫描以及修补工作。具体做法如下：

（1）对于系统官方提示的漏洞修补问题应该及时响应。

（2）在发现计算机存在漏洞问题时，应该及时安装及合理运行一些正规安全的漏洞补丁程序，从而促使计算机的网络运行足够安全。

（3）有必要结合现有的一系列高端计算机网络技术合理有效地设计较为完善且有效的计算机保护程序，这样可以对计算机漏洞开展更

为精确的扫描以及修复工作。

（4）对于网络安全管理人员来讲，平时应该积极收集有关计算机入侵方面的信息，并作出统筹分析工作，然后借助分析结果采取具有针对性的防范措施进行应对。对于个人如果技术经验丰富也应做到如此，若是经验技术不足，可及时收集问题，并向有关人员进行请教，或者是找专业人士进行处理。

5.加强对网络行为的规范和监督

在计算机网络应用过程中，存在一些不法分子利用网络技术进行数据信息盗取和滥用，对人们的网络数据信息安全造成威胁。在这种情况下，要更好地保障计算机网络的数据安全，就需要加强对网络行为进行规范和监督。一方面，国家有关部门要完善相关的法律法规，针对网络违法行为制定合理的、有效的规章制度和惩处要求，要加大对网络违法行为的惩处力度，增加利用网络散播谣言、制造和传播网络病毒等不法行为的违法成本，增加规章制度的威慑力，促使人们自觉地遵守网络管理制度，降低网络不法行为的发生概率。另一方面，则要加强对网络使用行为的监管力度，可以通过成立专门的网络监管部门、在各企业、政府部门内部设置网络安全监管中心等方式，对网络系统的运行进行监管，确保网络系统的安全、良好运行，也可以引导广大群众积极地参与网络监督工作中，引导群众对周围的不良网络行为进行举报，拓宽群众举报的途径和渠道，然后对举报的情况进行核实，对于举报属实的群众给予相应的奖励，从而更高效地规范和监督人们的网络使用行为，也营造更加健康的网络环境。

四、结束语

随着计算机网络技术的发展，人们获取数据信息的渠道更加广泛，信息传递与交流也更加便利，计算机网络为社会各行业的发展提供了强有力的帮助，有助于社会的高效发展。但是信息技术的发展也带来了显著的数据安全问题，一些不法分子也会利用计算机网络技术攻击他人的网络系统、窃取个人数据信息等，导致个人或企业的数据信息被泄露、被篡改等，对个人、企业的发展带来较为严重的损害，甚至也会对国家安全产生威胁，破坏良好的网络环境。因此，加强对计算机网络数据安全进行保护具有重要的意义，也是网络建设工作的重要内容和要求，需要有关人员强化对该项工作的重视，充分掌握网络运作中的具体数据安全问题，并且针对性地开展数据安全保障工作，提高计算机网络安全维护技术，确保网络环境的安全性。

参考文献：

[1]付鹏.大数据背景下计算机网络安全及防范措施分析[J].科技创新与应用，2022(1).

[2]王梁.计算机网络安全及防火墙技术分析[J].中国管理信息化，2021(12).

[3]朱亚兵.计算机网络安全问题及防范策略[J].产业与科技论坛，2021(10).

[4]陶丽.大数据背景下计算机网络安全问题初步探讨[J].网络安全技术与应用，2022(1).

[5]董满，罗志坚.大数据时代计算机网络安全管理策略探究[J].网络安全技术与应用，2022(1).

[6]李思慧.大数据时代的计算机网络安全及防范分析[J].数码设计（下），2021,10(1):16.

[7]黄启波.大数据时代的计算机网络安全技术及防范探讨[J].科技创新与应用，2021,11(24):150-152.