新形势下计算机通信网络安全隐患及其解决策略探究

关 健
天津市住房公积金管理中心 天津 300000

摘 要：计算机系统通讯网络的安全问题直接影响着计算机系统的正常使用，改善计算机系统安全的一般预防措施，可以减少安全事故的可能性。文章剖析了计算机系统安全的重大意义，总结了目前计算机网络中存在的主要安全问题，并给出了具体的改善方法，以保证计算机与系统间通讯网络的安全性。随着电脑网络安全科技的提高与发达，国内计算机用户数量日益增多，这不但为人民提供了便利，也暴露出不少网络安全问题。所以，人们必须建立一种完善的网络安全防护措施，已保证认识日常生活中的信息安全。本文总结了网络安全防护的方法和策略。

关键词：新形势；计算机；通信网络；安全隐患；对策

引言

当前已步入数字经济大环境，加强计算机通信网络安全既是维护国家安全的重要内容，又是推动我国信息产业发展的必然举措，同时也是维护用户基本权益的关键举措。然而随着信息化建设步伐的加快，计算机通信网络安全问题日益突出。通过对网络运行状态、Web应用、主机、弱密码、中间件等网络安全脆弱点持续监测，以及网络安全风险事件的采集，可为实现数据驱动的网络安全风险事件预测提供相应的数据基础，从而为保证计算机通信网络安全工作的顺利开展保驾护航。

1 计算机通信网络安全概述

目前，有关信息安全方面的系统化概念依旧不够完善，在计算机快速发展的背景之下，人们有了更多的信息交流方式，信息交互速率与速度的不断加快，使得信息泄露风险也进一步加大。为有效应对这种问题，人们进一步加大了信息安全研究力度，因此信息安全这一概念也应运而生。在新形势下，人们针对信息安安投入了更大的研究力度，大量精力的投入使得研究成果越来越丰硕。计算机信息安全的强化能够有效避免信息交互期间由于各种因素而导致的系统破坏、信息破坏、信息泄露以及信息修改等隐患，确保信息稳定、精准且安全地完成交互。计算机通信网络技术的安全问题既包括信息泄露，也包括判断信息是否真实、是否完成了信息加密、是否完成了信息完整性对比等等。

2 新形势下加强计算机通信网络安全的重要性

互联网要用标准协议书与网络联接所形成的非常大的球化网络。该网络包含无线路由器、网络交换机、网络防火墙等网络设备、各种各样联接链接、无数服务器及无数计算机终端设备。计算机网络安全指的是在网络信息的传递和互动过程中，为确保计算机网络硬件配置和管理控制网络软件的安全，避免各种各样破坏的现象，确保网络信息互动的顺利推进所采取的必要对策实践证实，提升计算机通讯网络安全具有关键的事实意义。

2.1 加强计算机通信网络安全管理是维护国家安全的重要内容

新形势下，网络安全与国家安全息息相关。基于网络大国战略的实行保障网络安全已成为现如今国家发展的主要战略之一网络通讯的风险性严重影响国家安全管理。因此，为了避免外界网络的非法侵入，有必要针对网络危险因素采用必要的防御措施。

2.2 加强计算机通信网络安全是推动我国信息产业发展的必然举措

全力发展信息产业早已成为我国经济高质量发展的主要构成部分。信息产业发展前提条件是建立和完善的信息网络系统，确保网络通讯的安全。

2.3 加强计算机通信网络安全是维护用户基本权益的关键举措

在物联网大背景下，互联网早已成为人们生活的主要构成部分，尤其是在现如今环境下。互联网早已成为人们购物、诊疗、教育、外出的关键支撑点载体。在国家对网络安全的有效监管下，网络信息平台的经营愈来愈规范，但网络环境的公开透光性增强了用户信息泄漏的风险。比如，在信息公布过程中，通讯网络安全存在系统漏洞也会导致用户公布的信息被外界盗取，犯罪分子盗取用户个人信息执行网络行骗，给用户带来一定的经济损害。因此，从保护用户信息安全的角度考虑，必须提升计算机通讯网络的安全管理，努力最大程度地清除计算机通讯网络里的安全安全隐患。

3 计算机网络通信中存在的安全隐患分析

3.1 系统方面的安全隐患

我们的计算机是一个相对智能的信息系统。此外，环境温度、湿度、强烈振动和外部自然灾害等环境因素对它的影响也非常微弱。目前，我们使用的计算机和网络设备没有抗冲击性、防水性、防火性、防雷性和抗电磁干扰性。此外，由于缺乏应对自然灾害和事故的能力，未考虑广泛的接地系统。

网络系统本身的漏洞很多，互联网技术最重要的问题是网络开放性。然而，这种广泛的开放性已经成为安全方面的一个弱点。此外，互联网所依赖的TCP IP协议没有高安全性。实现该协议的网络系统可以执行威胁、攻击、业务中断、数据缩减和数据操作，来防止用户操作错误，加强用户安全意识。计算机病毒是一个可执行程序，能够在可执行程序和数据文件上自由运动。当激活后，就可以运行。病毒同时具备感染性、潜伏性、触发性和破坏力。而计算机病毒则主要经由复制文件、传播文件、可执行程序，以及其他行为传播。垃圾邮件和商业间谍软件，指一些人在商务、宗教、政治以及其他社会活动中，通过在电子邮件地址上的“广告”和商业“传输”，迫使他们“推送”给他们的邮件或进行传播垃圾邮件。不是为了攻击操作系统，只是利用盗取操作系统和应用信息来威胁使用者的隐私权和电脑安全性，操作系统性能可能会受到较小程度的危害。

3.2 人为因素

计算机网络出现安全隐也与人为因素有关，许多计算机用户通过网络获取资源。尽管贮备了资源，可是他们的安全观念还不够，没有采用有效对策设定计算机通讯网络的安全。这给犯罪分子机会，保护计算机免受病毒进攻和非法侵入。新时期下，许多新科技网络黑客在页面中嵌入木马病毒，通过计算机软件系统漏洞将病毒嵌入系统，没经计算机用户许可就轻易控制计算机，盗取和破坏信息这是人为因素造成的安全安全隐患，严重影响计算机的安全运作。此外，在用户使用过程中，假如安全对策落实不到位，会增加被犯罪分子侵入或病毒影响的风险，尤其是对企业计算机而言[1]。如果出现了这种问题，可能会危及企业的核心利益。

3.3 计算机操作系统的漏洞

目前，在用户应用计算机过程中，操作系统是必不可少的，操作系统属于计算机的核心与主体，也可以说计算机的灵魂所在就是操作系统。但是目前我们最常应用的Windows操作系统依旧具有较多的安全隐患。因为微软公司在计算机刚刚萌芽的发展初期便迅速占领了计算机软件这一庞大的市场，因此也致使微软在相当长一段时间内都处于明显的竞争优势地位。因为竞争对手的缺失，再加上微软软件系统一直属于家用这一定位，因此也就致使大部分黑客会首先考虑研究微软这一操作系统，因此做好对微软系统的安全防护工作势在必行。从近些年来的实际情况来看，微软当中也有某些端口出现了漏洞或者被黑客利用的情况，进而致使大部分用户电脑发生数据异常故障。

3.4 用户使用计算机不规范

用户不规范操作是造成计算机通信网络安全隐患的重要因素，主要表现为：第一，用户缺乏安全意识，在使用计算机系统时没有有效保护个人账号密码，导致个人账号信息被外界不法分子所窃取。比如，用户在公共网络环境下登录网上银行导致个人银行账户、密码被窃取；第二，用户操作不规范导致计算机网络发生安全隐患。比如，用户在传输网络信息时，如果没有对传输的信息进行加密处理，容易导致传输的信息被窃取，从而造成网络信息泄漏。

3.5 木马病毒的快速发展

现如今，网络黑客有了越来越多的攻击手段，更新安全系统无法及时且精准地对接下来出现的病毒变化进行预测，只能够对自身存在的漏洞进行不断修复，以求降低网络安全隐患发生的概率。然而不论何种程序，都必定存在各种各样的漏洞，而网络黑客就是要找到这些漏洞，从而进行更加高效的网络入侵活动，从当前的实际情况来看，安全防护工具在更新过程中往往无法满足网络黑客攻击手段的创新与变化。由此可见，网络黑客的入侵在计算机通信网络当中无处不在，无法从根本上将其全面赶尽杀绝，这就要求我们必须提高警惕，尽可能降低网络黑客入侵时带来的损害。同时也应当积极面对木马病毒的快速发展，深入分析各类木马病毒的特性，以求能够及时有效的加以应对[2]。

4 新形势下计算机通信网络安全隐患的解决策略分析

4.1 提高计算机用户安全意识

从计算机通信网络管理层面来看，计算机通信网站软件后台管理者要增强自身的网络通信安全意识，充分认识到计算机通信网络安全的重要性，做好安全教育和培训，提升计算机通信网络管理系统相关人员的安全意识和观念，掌握最新的计算机通信网络安全防护技术和能力，研发应用安全系数更高的网站或软件登录系统，密切监控计算机通信网络中的不安全动向，确保计算机通信网络的安全与稳定。同时，考虑到计算机通信网络环境中人员因素极其复杂，计算机通信设备维护及更新通常由网络工作人员完成，要加强计算机通信网络工作人员的内部管理，避免工作人员获取用户的数据及隐私

信息进行非法牟利。

从计算机通信网络用户的层面来看，还需增强计算机通信网络用户的安全意识，要求计算机通信网络用户掌握常见的互联网通信防御措施和步骤，了解简单的密码登录、访问控制手段等内容，通过密码登录设定私密的明文密码，有效保护计算机通信网络信息的安全；通过访问控制手段防御非法黑客入侵，使特定用户登录计算机的相关权限。

4.2 对信息加密技术和访问权限的应用

在新形势之下，往往无法确保操作系统安全性。因此部分重要信息也能够在其他系统当中得到有效存放，比如常见的Linux系统。在该系统当中，大部分用户信息与权限都属于被直接加密的，如果用户想要获取与应用这些软件与数据，就必须要输入具体的密码才能够进行后续操作。除了加密用户信息与软件之外，还应当要求用户及时查看自身的网络信号访问协议，确保自己目前所应用的网络协议是合理合法的。为更好应对网络黑客等不法分子的入侵，导致计算机硬件与软件出现严重故障，要求用户可以通过解调器的调制或者设置路由器等方式，对相关工作人员的应用权限进行进一步明确，同时有效制约除了这些人员之外的各种应用人员[3]。

4.3 防火墙的建立

建立防火墙的主要作用就是减少系统内外部的直接交流，对安全信息进行自动化的识别，并有效过滤部分不安全类型的信息。防火墙可以结合用户设置对网络黑客进行自动阻拦，避免他们随意篡改或破坏用户信息。同时还能够有效减少网络当中存在的各种不安全因素，防止其扩散到更多的局域网当中。同时防火墙软件还能够有效确保信息安全，防火墙的安装能够提高计算机网络的隐蔽性，从而在极大程度上降低网络黑客的入侵概率，确保计算机用户信息安全，在用户进行信息交互过程中，构建起一道更加安全的屏障。总的来说，建立一个有效的防火墙，能够大大减少计算机通信网络运行过程中的安全问题，从而为用户提供更加优质的计算机网络应用体验[4]。

4.4 加强用户账号的安全

提高使用帐号的安全，包括系统登录帐号、电子邮件账号、网络银行帐号,以及其他的应用程序账号。而获取合法帐号和密码则是渗透网络的最常用方法。（1）设置系统登陆帐号的复杂密码；（2）不要设置同一或相似的帐号。试着用数字、字母和特殊符号组合设置自己的帐号和密码。设定长密码，并定时更新。

防止客人帐户攻击，客人帐号就是所谓的客户帐号。它也能够登陆电脑,但这能力是很有限的。最遗憾的是，客人们将会开启黑客的大门，所以最好完全停用或取消Geest帐号[5]。但是，如果客户帐户需要高级帐户，就必须尽快通过渠道使用高级帐户。首先，为客户端设置一个复杂的密码，并将对客户端帐户的访问设置为物理路径，堵住黑客的后门。由于黑客可以进入，我们的系统必须为他们打开一扇“后门”。

4.5 关闭一些不常用的服务和端口

从计算机系统安全保护概念的观点出发，计算机系统拥有更多的服务接口和更安全的操作系统。这用于在配置操作系统时设置不必要的服务功能和接口，特别是在个人使用计算机时。一些常见的服务功能还包括一个未使用的TCP接口。此外，用户还可验证是否配置了接口监视器，以便掌握接口的实际使用状况[6]。如果病毒进入计算机，监视器将会自动产生警告，并部分地区自动关闭接口功能，以避免黑客的进入。

正确隐藏计算机的IP地址，黑客们主要通过网络技术获取目标用户的IP地址，并利用网络测试技术检查主机信号。

结束语：综上所述，计算机通信网络具有明显的开放性和复杂性，数据安全问题尤其突显，成为当前不容忽视的重要研究课题。针对计算机通信网络安全问题，要全面深入地分析影响计算机通信网络安全的相关因素，构建计算机通信网络安全防护体系，从不同角度提出合理可行的计算机通信网络安全防护策略，有效保证计算机通信网络系统数据的安全与完整。

参考文献：

[1]尹茜茜.新形势下计算机通信网络安全隐患及其对策探讨[J].信息通信，2019（11）：178-179.

[2]李林凡.物联网在计算机通信网络发展过程中的应用[J].数字技术与应用，2021（12）：86-88.

[3]宋鹏.浅析数据通信网络维护与网络安全问题[J].电子元器件与信息技术，2021（9）：243-244.

[4]袁捷.新形势下计算机通信网络安全隐患及对策探讨[J].技术与市场,2019(5):219.

[5]尹茜茜.新形势下计算机通信网络安全隐患及其对策探讨[J].信息通信,2020(11):178-179.

[6]刘小锦.关于计算机通信网络安全与防护策略的几点思考[J].现代经济信息,2020(24):363.