工程技术研究 (3)2020,3
ISSN:2705-0998

通信计算机信息安全问题及解决对策

邓　勇
中移铁通有限公司邢台分公司　河北　邢台　054000

摘　要：伴随时代的快速发展，世界各国已然进入数字化通信时代，人们的生活也无法脱离不同类型的智能电子设备，对通信计算机的依赖性越发严重。如今，计算机普及程度明显提高，且人们运用计算机的频率也相应增加，通信技术安吉为人们正常生活、工作等提供了足够的便利，但同时也产生了许多安全威胁。为此，文章简要分析了通信计算机信息安全的具体定义及其通信安全的重要性，基于此分析诱发通信计算机安全隐患产生的主要问题与原因，并提出加强通信计算机系统安全防护以及采用理想通信计算机防范技术等具体方案，以期为我国通信计算机信息安全保护工作提供相应的参考与帮助。

关键词：计算机；通信信息安全；解决方案

引言

当今社会，互联网技术已发展为人们沟通、交流、获取和分享知识最为重要的一个工具，人们已对于网络技术产生了极大的依赖性。相关数据指出，我国网民总数量已经超出了七亿人。人们在互联网平台上开展线上交易、共享、商务洽谈等各项活动。但是随着网络技术的发展，进而出现了网络安全问题。在运用网络时稍有不慎就会出现一系列问题，包括用户私人信息被泄露、黑客攻击等。而一些企业可能受到网络攻击后丢失重要数据信息，势必影响到企业的进一步发展，这就表明网络防护的强化是必然的发展趋势。网络运用过程中信息化安全管理技术有助于计算机网络安全性的提高，以此对信息管理技术进行大力推广。

1 计算机网络通信安全的重要性

计算机网络术语是一种运用较为广泛的信息传输系统，作为计算机与通信技术的有机融合所形成的重要产物，其安全性自然十分关键与重要。通信网络之中普遍存储了大量的信息数据，计算机通信能够完成对信息以及数据的传送、处理、应用以及分享。计算机网络安全技术便是针对网络产生的安全问题，运用更为有效的方案加以处理，借此保证三级通讯的安全性。伴随计算机通信网络的高速发展，资源共享已然开始向一体化方向发展，计算机通讯对数据以及信息的处理以及传输都为人们的生活提供了便利，人们在享受上述信息革命提供便利的同时，也必须面临计算机通信安全所存在的问题。计算机通信的安全即必须确保信息传输以及存储的安全性，避免受到外界环境的影响或是破坏，确保数据完整性以及真实性。故而，加强对信息数据安全防护工作以及保密工作，对计算机网络通信的现状以及未来发展而言都十分关键。

2 通信计算机中信息安全存在的问题及其成因

2.1 网络木马

互联网和计算机技术都具备共享性和开放性的特点，这些技术将生活便捷提供给人们的同时，也使得网络管理难度得以增大。人们在互联网平台上可以自由沟通和共享数据信息，这使得网络木马的传播更为便利。网络木马实际上就是恶意编制的一种代码程序，并通过隐蔽方式进入到安全性不高的计算机中,以此对计算机使用者的个人信息进行盗取，包括支付信息、身份认证信息等，然后将盗取到的相关信息传回至盗取者。网络木马具有很强的伪装性，再加上目前的检测技术以及查杀手段较为滞后，一般都是在网络木马问题非常严重时，信息管理者才能发现，并通过编制相应代码消除掉网民木马。当计算机中植入了网络木马，会使得计算机中的保密信息以及个人信息暴露给盗窃者。现阶段，网络上出现的用户信息被售卖的现象基本上都归咎为网络木马。

2.2 内部操作方面存在的问题

内部操作方面存在的问题主要体现在因为工作人员操作不当或因为其与原因所引发的计算机突然断电等问题。如果通信计算机突然断电，便会诱发数据丢失问题。若通信服务器的存储介质遭受强烈的冲击以至于损害，服务器存储介质内的全部数据都有可能受到损害。

2.3 门户安全所诱发的问题

部分外部入侵人员并不会直接侵入通信计算机以获取数据，也不会直接控制计算机，但是其会尝试不断瓦解计算机门户的安全性，并尝试为计算机录入一些病毒，而病毒具有潜在的安全隐患，只要通信计算机门户被打开，外部入侵人员便会结合个人实际需要入侵计算机服务器以获取关键的数据。

3 通信计算机安全问题的防护对策

3.1 制定信息安全管理制度

针对病毒的防范往往需要应用相应的数据库，将怀疑为病毒的数据与数据库的内容进行比对，在此基础上实现对病毒数据的判断。为了达到最佳的判断效果，早期数据库的建设至关重要，在建设过程中，需要对已知病毒源代码进行收集，才能顺利实现对病毒数据的识别。需要注意的是，如果早期数据库建设不到位或者数据不完善，当计算机受到

病毒攻击的时候，数据库往往难以及时准确判别这些病毒数据，导致病毒进入电脑造成严重损失。当前很多病毒数据库建设存在诸多问题，导致针对病毒的防护效果很差，难以实现对计算机的有效保护。为了强化计算机网络安全，有必要建设相应的病毒防御体系，可以安装相应的病毒查杀软件，并定期对计算机内部文件进行扫描，及时清除危及计算机安全的病毒和木马。还要针对计算机系统进行及时升级和维护，提高系统完整性安全性，避免为黑客留下可以利用的漏洞。此外，还要注重做好计算机设备配置的升级，提高计算机运行安全性。还要做好计算机机房的安全防护，要注重做好防火操作，还要规范应用计算机，提高计算机维护效果。

3.2 增强用户安全意识

网络用户必须要树立良好的网络信息安全意识，并针对计算机网络安全形成明确认知，借助于可行性对策阻止黑客、病毒的入侵。要想保证这一目标的实现，就需要用户重视在使用计算机网络时对于资源和信息的共享，不能随意浏览陌生网站，不能点击陌生链接和信息，保证自己使用的计算机软件为正版，不能随意卸载能够保护计算机安全的所有软件。除此之外，相关部门需要加强教育宣传工作，并通过不同渠道进行宣传，有助于网络用户的安全意识得以增强。与此同时，需要合理完善现有的法律制度，严厉惩治不法分子，使得计算机网络侵犯代价得以提高，进而保护计算机网络信息的安全性。

3.3 加强防火墙安全技术

在计算机安全防卫中，防火墙是一种十分普通的系统，主要是对个人计算机进行有效保护，同时拦截外界数据，能够有效剔除具有威胁的数据以及压缩包。另外，在防火墙中，还可以设置计算机访问权限，限制外界计算机访问本计算机，给予计算机一定的保护。针对异常用户，网络防火墙功能中还增加了筛选功能，能有效排查用户来源，拒绝异常用户访问并进行锁定。一定程度上减少了网络安全威胁，提升了计算机以及网络稳定性能。

3.4 安全切换的技术

为了保证终端节点能有效接收信息，需要建设相应的移动性管理方案，还要提供无缝对接等协议服务。在实践过程中，可以结合需要对网络平台等进行切换，切换方案会根据具体特点和要求进行设计，要确保切换时间符合实际需要，减少丢包率提高性能标准。当用户端在不同节点实施切换，相应的接入点节点等需要实现频繁的信息交换。在这个过程中，有必要建设相应的安全手段来确保信息的准确性安全性，满足用户对信息安全性机密性的要求。一般来讲可以引入安全机制，增加切换的延缓，从而提高安全切换的效率；还要按照网络拓扑的特点做好准备，减小切换过程中的处理开销，确保其稳定性。

3.5 加强各种计算机信息技术的使用

信息化时代明确指出了信息数据安全具有的重要性，并对各种计算机信息技术进行研发，以此保护计算机网络信息安全。如数字签名技术以及文件加密技术是在储存、传播信息时进行加密管理，以此提高信息的安全性。在调用这些保密数据时必须对正确口令进行输入才能获得，以此防止网络病毒入侵所造成的信息泄露问题。而生物特征识别技术是将人的声音、虹膜、笔迹以及脸部等作为鉴定标准，只有通过生物特征识别技术的鉴定之后，才能对计算机内部数据信息进行使用，防止网络信息数据被盗取。

结束语

通信计算机信息安全属于现代人们极为关注与重视的问题，保证通信计算机稳定安全的运行，可以使信息安全程度提高，而信息安全程度越高，企业运营的安全性更高。为此，企业、学校等用户，需要通过合理的方式包括采用合理的防范方案以及行之有效的防范技术等，以不断加强通信计算机信息安全性。

参考文献：

[1] 基于大数据时代视域下的计算机信息处理技术研究[J]. 王亮 , 左文涛 . 通讯世界 ,2019(11):145-146.

[2] 徐春凌 . 大数据时代计算机网络信息安全及防护教学研究 [J]. 中国多媒体与网络教学学报 (中旬刊),2019(11):53-54.

[3] 曲丽颖 . 当前通信计算机信息安全问题及解决对策[J]. 计算机产品与流通 ,2018(2):55.

作者简介：邓勇 , 男 , 汉族，1980 年 2 月 13 日，河北省邢台市，中移铁通有限公司邢台分公司，工程师，无，本科，研究方向：通信工程 , 邮箱：15833667598@139.com