大数据时代计算机网络安全技术应用探讨

郑明才
江西软件职业技术大学　江西南昌　330041

摘　要：网络信息技术被广泛应用于高新技术产业、军事、国防等各个领域，网络信息在人们的生活中无处不在，随之而来的网络信息安全问题也越来越突出。一旦网络信息安全受到威胁，将会对社会以及大众造成不可挽回的损失。本文通过对当前计算机网络信息安全存在的问题进行了分析，并进一步探讨了网络信息安全技术管理在计算机中的具体应用策略。

关键词：网络信息安全；技术管理；计算机应用

Discussion on the application of Computer Network Security Technology in the era of big data

Mingcai Zheng
Jiangxi University of Software Professional Technology, Nanchang 330041, China

Abstract: Network information technology is widely used in high-tech industry, military, national defense and other fields, network information everywhere in people's life, the ensuing network information security problems are becoming more and more prominent. Once the network information security is threatened, it will cause irreparable loss to the society and the public. This paper analyzes the problems existing in the current computer network information security, and further discusses the specific application strategy of network information security technology management in the computer.

Keywords: Network information security; Technical management; Computer application

引言

计算机网络技术的普及对人们的生活有很大的影响，是不可或缺的一部分。然而，由于黑客入侵和计算机病毒等因素也会对计算机安全构成威胁。因此，采用有效的技术来维护网络安全是非常重要的。然而，网络管理属于一个任务相对较大的项目，需要计算机系统各方面的配合和各种防范措施的实施。只有这样才能维护网络安全，保证人们对计算机的使用。

一、计算机网络安全相关概念

计算机网络技术涵盖的内容较为广阔，不仅有网络技术，还有密码学和数学等领域的知识。计算机网络的保护主要是对整个系统的硬件和软件进行保护。在保护过程中，首先需要对相关数据进行监控，并以此为依据保障数据不受破坏。在数据的安全性得以保障的前提下，相关人员的利益也能够相应得以保障，从而整个系统也具备了一定的安全度与可靠度。在计算机网络的保护工作中，对网络信息安全进行防护是工作的重要内容，也是安全隐患相对较多的领域。网络安全与信息安全并不完全相同，它们有不同的侧重点和发展方向。对于网络安全来说，主要关注的是线路连接和操作系统、管理人员、服务领域等的安全。但信息安全的问题在于计算机中包含的数据的安全性，其侧重点在于数据的可利用性、加密功能与准确度。计算机信息网络安全的影响因素相对复杂，不仅包括自然灾害，也包括系统漏洞与不当操作、恶意攻击、病毒等。而计算机信息网络安防工作则应当对各类因素采取相应手段，使信息网络安全系数有效提升。与此同时，计算机网络安全的维护并非一己之力能够完成，而是需要所有相关人员都加以重视，不仅计算机用户需要有网络安全意识，研发团队也不应忽视网络安全问题 [1]。

二、计算机网络信息安全存在的问题

1. 存在软件漏洞

当前，很多网络信息被盗用或入侵，在很大程度上和系统软件有着直接关系，不法分子通过软件存在的漏洞，进行非法操作，对信息进行篡改。如我们电脑上经常使用的浏览器，便很可能会存在漏洞，在浏览网页时，未屏蔽一些危险网站链接，不小心点进去后，电脑便会被病毒入侵，之后出现蓝屏或者死机等情况，对用户的信息安全以及使用安全造成了极大的影响 [2]。

2. 网络安全意识比较薄弱

随着网络信息技术的不断发展，网络上的信息量也在不断增加，各种新媒体层出不穷，人们可以随时随地传播和获取信息。但是目前很多人安全意识比较薄弱，未充分认识到网络安全的重要意义，在使用计算机过程中，操作也非常的随意，存在诸多网络安全隐患。部分区域对网络安全管理相关措施执行不到位，对于存在的

问题无法及时解决，部分企业存在随意浏览网页的情况，导致病毒入侵，密码被盗等问题，导致计算机存在安全隐患 [3]。

3. 恶意攻击

目前，网络存在恶意攻击，通过制造垃圾信息，攻击网络数据信息安全，让网络系统资源处于危险状态，用户主机不能正常连接网络，网络惯犯针对安全性较低的系统，攻击目标系统，造成不同程度危害。计算机网络信息安全是要有相对安全的操作环境的，如果计算机系统遭到破坏，信息传输过程中，自然会存在风险，用户的信息也会被泄露。随着科技的不断更新，计算机软件和硬件也在不断更新，操作系统快速地更新换代，新的操作系统自然也对防御手段提出了更高的要求，以往的屏蔽技术无法满足当前的实际需求，用户信息安全也受到极大影响。计算机的远程操作系统让不法分子有了可乘之机，其通过远程控制侵入系统，窃取用户信息，攻击操作系统，导致信息数据丢失，造成极为严重的后果。计算机病毒也很猖獗，这些病毒具有很强的攻击力，且非常隐秘，除了获取用户登录名和密码等信息之外，还会通过邮件的形式，发送病毒，传播速度快，很容易导致用户系统崩溃，严重威胁计算机网络安全。针对以上情况，必须不断更新与完善防护手段与措施，防治不法分子攻击计算机对计算机系统造成严重破坏，通过升级计算机系统，提升其病毒防御能力，网络管理人员还应当加大监督与管控力度，用户也应当不断强化自身网络信息安全意识，保护好个人信息安全 [4]

三、基于网络行为的计算机网络安全预警系统设计的需求分析

1. 计算机网络安全预警系统设计方案

借助网络计算机可以将不同地方分散的计算机之间建立起相应的通信及网络资源共享。同时，该计算机系统还具备数据吞吐量大、结构复杂、功能繁杂等特点。因此，基于用户的网络行为习惯，对计算机网络安全系统进行研究设计时，需要注意计算机网络安全预警系统是通过对各种设备、工具以及手段的利用，对网上的用户使用行为进行实时的观测与监控。并通过计算机系统中存在的漏洞与病毒等方面的扫描，对系统的数据实施检测审计与评估，从而分析与识别用户自身的使用行为。并针对网络中存在的异常情况或不同的攻击行为做出的及时判断与应急反应。针对计算机网络使用过程中存在异常不安全的行为，可以进行跟踪、记录与分析和捕杀，从而保障计算机网络的安全性与稳定性 [1]。然后，当计算机网络使用过程中存在异常行为之后，通过跟踪使用过程中的记录与行为分析，可以将其攻击特征加入计算机安防系统中，方便后期的查询、分析及统计。在出现不安全的攻击行为后，经过及时的处理，可以对攻击的来源以及病毒根源进行查询。从而维护计算机网络使用的安全，以及对用户使用行为的管控。

2. 系统总体设计目标

基于用户的网络行为所构建的计算机网络安全预警系统，主要是为了给用户网络安全提供更多的保障。同时基于用户的网络使用行为习惯，进行了有效的分析与预测，最后结合分析的结果，向预警系统发送信息，以此来保障计算机网络的安全。因此，计算机网络安全预警系统主要包括以下 6 种功能模块，比如数据采集功能模块、特征值提取功能模块、用户行为分析模块、行为预测模块、预警和响应模块、信息发布模块。

四、计算机信息网络安防工作相关策略

1. 树立计算机信息网络安全防范意识。

据统计，现阶段威胁网络安全的大部分事件都由相关人员安全意识的缺失造成的。为解决此类问题，计算机信息网络使用者应当对网络安全问题加以重视，同时应当加强对网络安全知识的学习，以此提升安全防范能力。在此基础上，政府等各个相关部门也应当对法律法规加以健全，以法律对网络用户行为进行约束，使网络安全程度有效提升。

2. 强化对账户的安全管理。

威胁计算机网络信息安全的方向较为多样化，其中恶意攻击是较为常见的一种，而一般情况下的恶意攻击方式主要是盗取账户的用户名与相应的密码。尤其在互联网技术飞速发展的阶段，各类 APP 浩如烟海，而大部分 APP 在使用初期都需要完成注册，在注册过程中，一旦用户对自身账号与密码设置缺乏难度，则容易被破解，从而导致个人信息泄露情况的发生。而个人信息泄露并非终点，与之相关的各类信息也都容易随之泄露。因此，用户应当加强自身对账户与密码的安全管理意识，可提升密码难度，使其更具独立性与私密性。此外，也可加快更换密码的频率，以此有效防止密码被破解导致的个人信息泄露等问题。

3. 防病毒软件

病毒极具破坏性，同时繁衍速度极快。利用计算机网络传播速度快的特征，病毒通过自我复制并传播，导致整个计算机网络出现故障，从而导致用户存储的信息被干扰和改变。如果情况严重，计算机网络会自动销毁。为了更好地维护计算机网络安全，阻止病毒在计算机扩散传播，我们可以利用防病毒软件来抵制病毒。反病毒软件是一个强大的程序，可以从计算机上清除病毒和木

马。目前，各家庭网络安全使用的杀毒软件主要有金山毒霸、360 杀毒软件等，它主要起到查毒、杀毒、防病毒和修复数据信息的作用。然而，该软件中的病毒预防程序通常是在病毒生成后才开发的，其被动性和滞后性非常强。因此，我们需要依据病毒的发展情况，不断更新防病毒软件系统，确保计算机网络的使用安全性，这也是研究者迫切需要解决的问题。

4. 身份信息检验

目前，大部分的计算机网络在使用时，一般不会进行身份验证，这样也使得网络使用门槛比较低，任何人都可以使用网络。也埋下了信息安全隐患，身份信息验证对用户登录加强管理，从而保障登录使用人员的合法身份，在很大程度上能够保障计算机系统的安全性。其能够确定计算机使用人员的身份信息，其主要是通过检验参数，对所有参数进行全面检测。必要的情况下，还可重复进行验证，确保登录者身份信息真实有效，身份信息检验已经逐渐被应用于现代网络系统当中，其能够有效避免和预防非法入侵网络系统，保障网络信息传播效率与安全性。在具体应用过程中，为了减少参数验证烦琐流程以及重复性，通常计算机会采集用户的部分生理特征与个人信息作为验证时的参数标准，如用户的指纹、虹膜、面部信息等，但是由于技术成本等问题，使得这些暂时并未得到普及，最为常见的验证方法依然是使用密码登录进行身份验证 [5]。

5. 系统网络架构

设计的网络安全预警系统在服务器中创建对应储存列阵和服务器汇集网络程序，在研究过程中重点使用区域网络存储数据。在对数据存储过程中，划分为不同区域进行存储。最后利用集群技术调取，使各个区域中的数据相互作用。主要使用 Web 技术、数据库等类型，并且根据多级冗余方式保证系统能够安全、可靠地运行。在交换机外部对入侵系统和防火墙的检测体制进行明确，从而能够抵御危险。在系统和数据库访问过程中，为了使数据流动，以关键词、时间段等方式得到数据，保证定位和请求能够精准地传递和发送。通过多重相互确认更快地进行访问。为了保证系统的安全性，利用部署信息强隔离装置、入侵检测设备和防火墙等障碍组织外界入侵，及时地发现网络安全威胁并且消除，系统要限制同、个用户在相同时间内登录的次数。如果连续多次的登录失败，系统要自动断开连接，并且在一段时间中用户都无法能继续登录。实施设备特权的用户权限分离，在系统不支持的时候要求部署日志服务器保证管理员操作被审计，网络特权用户管理员不能够操作审计记录。

6. 定期对计算机进行安全扫描。

在一般情况下，计算机在使用过程中容易出现配置问题，导致配置问题的原因往往是外界因素。而配置出现问题后，相关安全问题也极易随之出现。因此，为尽量降低存在安全问题的可能性，则需要计算机网络信息安全相关管理人员对计算机定期进行安全检测，以此方式对各个软件进行扫描，从而能够及时发现其中存在的问题，降低计算机被攻击的概率，提升计算机网络安全性能。计算机网络安全防护在计算机运行过程中发挥了至关重要的作用，因此计算机信息网络安防工作是一项重要工作，在工作过程中，相关人员应当对配置进行及时调整，针对系统漏洞安装补丁，同时及时解决潜在问题，以此将计算机网络安全防护工作落到实处，为计算机网络安全贡献力量。

五、总结

随着计算机网络的快速发展与普及，网络信息安全问题越来越突出，其次，网络的使用门槛也比较低，每个人都可以使用网络，但是很多人信息安全防护意识薄弱，且不具备相应的专业技术能力，因此，加强计算机网络安全防护是非常必要的。通过逐步完善网络信息安全技术手段，制定相应的管理机制，从而最大程度上保障计算机网络信息安全。

参考文献：

[1] 王征，陈晶，王盛 . 基于网络信息安全技术管理的计算机应用思考 [J]. 网络安全技术与应用，2017，21（004）：1-1.

[2] 张子涵 . 基于网络信息安全技术管理的计算机应用问题 [J]. 中小企业管理与科技（下旬刊），2019，32（027）：262-262.

[3] 谢世春，倪培耘，宝磊 . 基于网络信息安全技术管理的计算机应用探讨 [J]. 计算机产品与流通，2019，11（12）：42-42.

[4] 陈亮 . 基于网络信息安全技术管理的计算机应用研究 [J]. 环球人文地理，2017，21（018）：302-303.

[5] 李国盛，张静薇 . 计算机网络管理相关安全技术探析 [J]. 科技创新导报，2013（08）：221.

[6] 王喆 . 计算机网络管理及相关安全技术探索 [J]. 产业与科技论坛，2016，15（5）：36-37.

基金项目：江西省教育厅科学技术研究一般项目“基于区块链协议的云计算 BaaS 架构网络平台应用研究”（课题编号 :GJJ206605）