计算机网络安全技术在网络安全维护中的应用

萧世昌
广东培正学院　广东　广州　510830

摘　要：尽管计算机科技带来了方便，但是它的保密性比较差。在实际工作中，由于各种原因，如黑客攻击，病毒攻击，系统存在缺陷等，从而导致系统文件丢失，系统瘫痪等。要想保证计算机网络的安全，就必须将入侵检测技术、防火墙技术和加密技术等技术运用到实际中去，尽量降低其它因素对网络的危害。

关键词：网络安全；安全维护；安全技术；计算机技术

引言：在现代社会，计算机已经成为人类生存和发展的重要工具，它给人类带来了巨大的便利。在科技进步的同时，计算机的安全性与网路的维护性也越来越受到重视。要加大科研力度，做好有关的安全和管理工作，保证计算机网络的正常运转。

1 计算机网络安全技术

1.1 作用

由于我国现代互联网技术的快速发展，网络安全受到了社会各界的广泛关注。对于如何看待和分析问题，不同的人、不同的主体有着不同的视角和思路，因此对网络安全也有不同的看法。用户必须高度重视隐私和安全企业要有效防范欺诈和窃取商业秘密，加强信息安全保护，切实保障信息的完整性和安全性[1]。此外，公安部门的合理做法，一旦信息泄露或丢失，给国家造成巨大的物质和经济损失，甚至造成社会混乱，国家也能有效抵御来自外界的非法入侵。因此，网络安全对于现代社会的发展具有非常重要的价值。

1.2 特点

1.2.1 安全性

通过计算机网络的文件传输比纸质文件传输更依赖于虚拟网络。上传的文件越多，对计算机网络安全的威胁就越大。在使用计算机网络安全技术时，不仅要保证计算机物理设备的安全，还要保证网络文件和数据的安全，以免泄露用户的隐私。

1.2.2 公平性

计算机网络中的文件由虚拟代码组成，在创建和合并过程中会受到大量入侵和威胁，如果文件不完整则无法修复。使用计算机网络安全技术可以保证网络文件和网络数据的完整性，确保文件和数据的完整性。

1.2.3 保密性

保密性不仅是计算机网络安全技术的一个特点，也是使用计算机网络安全技术必须遵循的原则。随着计算机技术的不断发展和网络覆盖范围的扩大，计算机网络已经充斥着人们的生活。例如，早先人们使用纸质文件来存储文本或图像信息，但今天人们使用电子文件来存储信息。计算机网络安全技术中有多种加密方式，人们可以利用加密方式对电子文件进行加密，以保护隐私，防止隐私泄露。

2 网络安全的影响因素

2.1 网络病毒对网络安全的影响

不同种类的网络病毒会对计算机产生不同损害，且入侵方式也存在差异性。蠕虫病毒、木马病毒、脚本病毒是比较常见的网络病毒，以木马病毒为例，它会潜伏在用户的计算机系统中，对用户信息进行复制、篡改和泄露，入侵计算机防火墙系统。如果将木马病毒与其他网络病毒配合使用，非法分子就能够对用户计算机实现远程可视化控制。木马病毒侵入计算机系统后，不法分子会利用木马程序对计算机进行控制，轻松盗取计算机用户的重要资料信息。与其他类型网络病毒相比，计算机中存储的文件不会被木马病毒感染，病毒也不会不断繁殖，但可以隐藏后诱导用户将该病毒下载至计算机中。木马病毒严重占用系统存储空间，使计算机耗能大大增加，最终危害用户的信息安全。信息技术发展革新的同时，网络病毒也在不断发展，其危害性与种类与日俱增，很多网络病毒会极为隐秘地侵入计算机系统，引发严重的后果，给用户造成重大损失[2]。

2.2 网络安全管理对网络安全的影响

除日常开展系统维护外，网络安全管理工作的不断完善也是网络环境安全稳定的重要保障。网络环境具有极高的开放性和复杂性，再加上长期以来很多网络企业用户和个人用户缺乏网络安全意识，网络安全维护投入相对较少，技术人员专业水平有限，使得计算机网络安全问题频频发生。在网络安全管理开展过程中，管理人员专业素养水平有限，操作和管理不规范，甚至会导致

计算机设备损坏，使得信息安全风险进一步提高，用户信息泄露问题不断发生。虽然人们已经越来越重视网络安全，但是在实际安全管理工作中还存在很多问题，对于黑客入侵等危险因素应对不够，导致计算机网络安全水平有限，仍需进一步提升安全管理水平。

2.3 用户层面因素

用户是计算机网络的使用主体，其安全意识和行为操作对于计算机网络的安全性具有直接性的影响。具体而言，用户层面的影响因素主要体现在两个方面：一方面，用户缺乏良好的计算机网络安全意识，在使用计算机和网络的过程中，未能形成良好的使用习惯，可能发生破坏计算机网络安全的行为。另一方面，网络信息时代背景下，用户使用计算机网络的频率大幅提升，但大部分用户的网络安全素养并没有得到提升，缺少正确使用计算机网络安全技术以及有效保护用户权限的能力，使得计算机网络中的安全风险不断增多，严重影响计算机网路的安全性。

2.4 黑客层面因素

黑客是威胁和破坏计算机网络安全的一个重要因素，其对计算机网络安全性的影响主要有两方面体现：一方面是通过制造和传播计算机病毒来破坏计算机网络的安全性和稳定性。常见的病毒形式有：蠕虫病毒、木马病毒、文件型病毒等。这种危害形式具有传播能力强、不易被发现等体征；另一方面是通过直接入侵或植入间谍软件的方式，对具体目标造成危害。此类破坏形式多以窃取用户信息、机密文件、商业信息为目的[3]。

3 计算机网络中信息系统技术安全维护路径

3.1 安全事件发生前的维护

计算机网络中的信息系统安全维护应着重于防患于未然，维护这一联系可从四个方面着手：

3.1.1 设置网络入侵检测屏障

利用入侵检测技术更好地保障网络通信的安全，预防和控制对网络系统的非法入侵尤为重要。基于保护网络信息安全的需要，可以基于入侵检测方法识别各种网络入侵威胁，并据此提供网络入侵防御和控制的方法和工具。总结目前的情况，可以得出结论，无论是签名分析方法还是统计分析方法都可以用来建立网络入侵检测阈值，具体用来纠正网络偏差，从而准确地达到入侵检测的目的。时间最短。为了按照同步保护方式保证数据处理和数据计算的安全，还需要注意“主动免疫可靠计算”。通过使用代码基因，可以及时识别外来代理，及时发现网络主体中的各种恶意信息，更好的状态测量和内存隐私。

3.1.2 防火墙技术

（1）安全配置中的应用

在网络中，安全配置具有很大的影响，因此，计算机使用者必须对此给予足够的关注，并结合自己的实际需要和使用情况，选择适合自己的安全配置。防火墙技术可以将各种类型的数据按照一定的类别划分出来，从而保证数据的安全性。针对重要地区，采用防火墙技术可以进行专门的保护，从而确保计算机网路的正常运作。要想保护好重要的信息资源，就必须对这类信息进行更高层次的保护，除了使用防火墙技术以外，还必须追踪某些有害信息的IP地址，以便可以在计算机网络中被拦截下来。

（2）在日志监控方面的应用

目前，防火墙技术得到了日益广泛的使用。目前，对数据中心进行接入控制的主要手段有：对数据中心进行接入控制。当计算机发生异常时，防火墙技术会及时提醒用户。随后将会出现一个协定监视，并且该协定的存在性也很有意义。当计算机发生故障时，可以对其进行功能分析，找出故障原因，并提出相应的防护对策，保证计算机的正常运行。在发生问题的时候，协议能够最直观地反应出问题所在，有助于我们找到问题所在，并对问题进行处理，从而可以重建防火墙，对某些危险的程序和病毒进行屏蔽，从而提升防火墙的使用率[4]。

3.1.3 开展业务应用安全检测

网络安全人才短缺现象普遍存在于我国各行各业。许多公司只关注关键业务系统的安全测试，希望用有限的资源解决最严重的问题。但是，从入侵者的角度来看，业务系统中的漏洞是一个严重的问题。因此，组织可以应用IAST灰盒测试和威胁建模等技术，并将它们应用于整个业务开发生命周期，以确保开发、运营和安全团队中的每个人都在做好自己的工作。

3.1.4 强化网络安全建设

以资产为中心的网络安全项目更为常见，这种围绕边界安全保护和威胁检测构建核心安全功能的方式很容易忽视通常对资产本身进行的安全改进。基于公司已知资产，构建网络安全应重点识别公司所有资产和未知资产、公共数据、应用程序、服务、公司等的漏洞。应该分析、监控开放资产和服务变化、威胁监控、合规性检测、检测和其他指标。当工作环境中出现潜在威胁时，应建立针对性的应急机制，在出现网络安全问题时，有效解决相关问题，显着降低网络安全问题的负面影响。

3.2 数据加密技术

灵活运用数据加密技术完成网络安全，管理数据加

密，将明文数据转换为密文，保护网络软件和用户数据。使用正确的密钥可以最大限度地减少数据从网络泄漏的可能性。在信息及信息传输网络发展过程中，增加数据加密技术的使用频率，优化数据传输系统，增加数据传输的安全性，营造优质的传输环境或数据创意。详细了解网络技术的实际状态，完善网络加密技术，如数据存储加密技术、数据传输加密技术、数据识别加密技术等。在数据传输中实施加密应遵循多样化的原则，即针对不同的数据传输需求提供不同的支持，增加数据在网络中传输的安全性，包括美国NewDES技术、欧洲IDEA技术为超前技术。此外，数据加密技术也是网络安全技术体系的重要组成部分，采用该技术可以有效降低非法入侵和病毒入侵的可能性。有证据证明，数据加密技术比加密算法更安全，可以帮助员工更好地维护网络安全工作[5]。

3.3 杀毒软件

杀毒软件是一种特殊类型的软件，可以检测、挖掘和删除软件。在保护网络安全方面，杀毒软件可以恢复被病毒破坏的文件，现阶段我国杀毒软件的发展趋势是恢复被病毒破坏的数据和文件。综合分析我国使用的杀毒软件，我国使用的杀毒软件可以清除9%以上的计算机病毒，提高网络安全。但需要注意的是，杀毒软件的使用会影响网络系统的性能，因此广大网民应该摒弃错误的心态，正视杀毒软件能否正常工作的重要性，提高杀毒软件稳定性和网络质量。

3.4 入侵检测技术

在保障计算机网络安全方面，入侵检测技术还可以用来彻底检查被蓄意入侵或利用的计算机和网络，及时妥善地解决问题，防止不法分子获取非法信息进行干预或入侵。该技术主要用于计算机网络用户检测网络安全漏洞，应用在以下几个方面：（1）应用入侵检测技术进行系统维护，可以实时监控系统运行情况。安全有效地防范病毒，最终形成智能化的网络监控系统，在计算机网络系统受到入侵后，可以准确定位不法分子的位置，从而保证计算机使用的安全。（2）网络滥用统计分析，数据精准管控，及时预警，有效管控。（3）除了检测计算机的操作系统外，还可以监测用户的操作系统，准确识别用户的错误操作，并发出警报。

目前，网络入侵检测技术应用广泛，但仍存在传输速度慢、误报和漏报等诸多缺点。因此，在使用入侵检测技术时应考虑以下几点：一是信息收集。采用目标连接法结合对计算机网络系统内部结构的分析，在使用交换节点连接法时，应事先准备好基本方案，并做好调试和安装工作。系统可以完全连接，所有端口都连接。此外，进入和离开计算机系统的数据应在安装前仔细记录，以尽量减少系统入侵的可能性。二是数据分析。在计算机网络安全防护方面，通过对各种数据的深入分析，结合对比，发现系统中潜在的安全威胁，并第一时间将信息发送至管理服务器。TCP/IP计算机网络的入侵检测本质上是基于具有传感器能力的检测引擎，尤其是在检测计算机系统内部信息时，可以根据检测结果制定安全管理和维护措施。综合信息数据传送至控制中心，提醒用户，减少损失。三是信息响应。在实施入侵检测技术时，还需要考虑数据响应的多样性，如网络引擎告警、SNMPtrap、实时会话查看等，深入分析研究应用价值。拦截技术，监控并完成计算机网络系统维护连接的各个环节，让各个业务系统都处于一个相对安全稳定的环境中，同时记录工作过程，让整个通话过程的数据保持原样，使计算机可能处于最佳保护状态。

4 结束语

总之，计算机科学技术的发展必然会面临越来越多的问题，计算机网络技术在人们的生活和国民经济发展中占有不可低估的地位，计算机网络技术也为我国经济的发展做出了贡献。尽管计算机进步的道路上有许多障碍，但人们必须共同努力克服这些障碍，才能实现计算机网络的健康发展，更好地服务于人民生活和社会经济的发展。

参考文献

[1]崔娟.网络维护中计算机网络安全技术的应用探讨[J].计算机编程技巧与维护，2021（4）：164-166.

[2]饶国勇.探究计算机网络安全技术在网络安全维护中的应用[J].计算机产品与流通，2020（10）：100.

[3]赵宇飞.计算机网络安全及防火墙技术分析[J].智慧中国,2022(1):90-91.

[4]谭祥明,杜守红.计算机网络安全技术的影响因素与防范措施[J].网络安全技术与应用,2021(12):167-168.

[5]谢远福.入侵检测技术在计算机网络安全维护中的应用[J].信息与计算机(理论版),2022,34(12):225-227.