计算机网络安全技术的影响因素与防范措施

胡晓龙
昆明地铁运营有限公司　云南　昆明　650000

摘　要：在当前网络的广泛应用和计算机的不断高速发展，计算机网络技术已经给我们的日常生活和办公的各个领域都提供了极大的方便，已成为现代社会日常生活的重要一部分。在实际使用计算机网络系统的过程中，通常都会遭遇一些网络安全因素的干扰，这也就很容易使计算机等网络设备面临安全危机，所以计算机网络系统的安全性问题也引起了我们的重视。

关键词：计算机网络；安全技术；影响因素

引言：近些年来，随着中国经济在互联网上的迅速发展，信息不仅仅在普通民众的生活中得到了反映，在各行业的工作中也逐渐进行着渗透，为我国的经济发展与社会进步提供了强大的信息保证。同时，加强对安全研究领域的研究，实现安全的现代化，并逐渐发展成各个方面的重要研究问题，所以，建设出更加完备的计算机安全平台，必须从安全平台中完善并制订出针对性的防范措施，维护着互联网世界的安全。

1 计算机网络安全技术概述

计算机网络安全管理技术，主要是以互联网信息技术为依托而进行的安全措施，通过网络安全技术来对互联网世界当中的信息和互联网数据进行实时维护的技术。计算机网络安全技术主要是以物理安全保护技术和逻辑安全保护技术为基础而实现的。物理安全保护技术通常指的是对任何一种通信系统和其关键基本装置所进行的防护。而计算机系统网络安全技术，主要以物理安全防御和逻辑安全防御技术为核心来实现的。物理安全保护技术，通常指的是对任何一种网络通信装置或者其有关基础装置所进行的防护。其中，逻辑安全保护技术指的是通过保护物理内容和逻辑资料的安全性，提高其可用性和安全性[1]。不过，互联网安全本身就有一定问题和缺陷，在现实运用当中也存在着一定危害因素，面对这一问题就必须采取相应的预防措施，进而才可以使其顺利地运转，使之可以给整个计算机与网络信息技术的使用带来安全保护。

2 计算机网络安全的威胁特点

2.1 潜伏性以及隐蔽性

目前的安全问题与过去的攻击方式已不同，一般都采用隐蔽性很强的病毒，一旦电脑染上病毒，数据发生泄露后，我们一帮很难及时发现，木马和病毒可以在电脑当中潜伏很长，一直待我们寻找适当的机会才对电脑实施侵入。病毒与木马较的潜伏性和隐蔽性给人们的电脑安全管理带来了很大的困难，电脑通常没有发生什么异常，如果发生问题，带来的经济损失是无法挽回的。

2.2 传染性以及突发性

计算机在平时工作中，平时运行中，一般都是连接网络，但有的时候在进入一般的运行中后，如接收电子邮件同时进入了互联网，此时的电脑会给计算机带来严重中毒，有时在毫不知情的状态下由于邮件泄露或各种故障，并不会给予计算机任何的时间和反应时间，计算机被感染病毒，同时如果局域网中的计算机被病毒感染其它计算机也会被病毒感染，很大的机会将病毒经由互联网传播到其它计算机上[2]。

2.3 危害性和破坏性

计算机网络遭到入侵后将会给我们的生活带来极其巨大的冲击。当前，由于计算机网络在我们的工作中扮演着十分关键的角色，而各行各业的许多工作中都离不开计算机网络的支撑，如果出现了严重的攻击行为，将会带来十分重大的社会风险，并造成极大的经济影响。

3 计算机网络安全技术的影响因素

3.1 计算机网络本身存在的问题

平时的电脑应用中，一些安全问题是不可避免的。包括操作系统中出现泄漏、故障不能恢复的现象。计算机和互联网等信息技术的迅速普及给我们带来了便捷业务服务的同时，也同时存在着用户的个人安全性和隐蔽性秘密资料的被泄露，而这种情况下也为犯罪分子故意谋取或者盗窃网络上个人秘密资料提供了可能性，在很大程度上对用户的国家安全和个人利益都造成了不少影响。此外，因为计算机网络传输信道的存在滞后性，导致计算机设备的干扰特性不断减弱，导致使用者的私人资料信息更易被窃取和随意修改，严重影响信息传输的稳定性。最后计算机系统安全程序的泄漏极易导致网络

安全产生一定的不稳定因素，为不法分子盗取数据信息提供便利[3]。

3.2 网络运行机制欠缺监管

互联网首先是一种可以储存大量丰富资料供使用者方便地进行信息检索服务的综合性网络平台，具有极大的开放性，也就是说每个使用者都可以在互联网上实现一些与自己行为相关f的交互，虽然网上的信息共享给人们的工作模式带来了非常强大的优化作用，但对于同时共享的社会环境来说，并无法得到有效而系统性的监控，在目前的互联网环境当中正是因为这样，在许多情况下我们所进行的共享性行为都无法进行有效的控制，而这样固然有利于我们的工作交流活动但那却也同样给了犯罪分子可乘之机[4]。在安全技术方面，必须要建立一种更加高效完善的技术手段，以及一个体系，但是由于网络自身的大体容量，并无法进行更加高效的监控整个网络，进而产生一些网络安全漏洞。对网络科技来说，必须要有一个高效完整的技术手段，以及监管体系，这才能够有效对抗犯罪分子的一些不法行为，进而确保客户和公司的信息f没有发生泄露的风险。

3.3 黑客恶意攻击系统

由于科技不断发展，计算机网络能力日益提高，有些计算机隐藏病毒，骇客通过这种隐藏的病毒对网络实施监控，计算机网络防御能力在日益增强的同时，黑客攻击网络的方式也将日益发生变化。计算机网络系统中黑客通过获取数据，对目标系统漏洞进行检测，并设置相应的模拟条件，采用网络入侵的方法，寻找入侵系统的最好方案，按照规划系统进行入侵。黑客在恶意入侵网络系统过程中，与病毒入侵系统具有明显区别，利用互联网可以对所有电脑终端实施监控，也因此具有终端主导权，同时骇客更具有专业化以及针对性，对计算机系统的入侵成本更高，这也是利用计算机网络过程中所面临的主要安全隐患。

3.4 用户安全意识淡薄

随着当前科学技术水平的日益提高，数字化社会的来临，现代人的娱乐与工作越来越远离互联网。不过，由于一般来说网络本身并无保证安全的能力，同时使用者对互联网发展状况又缺乏很深刻的认识，再加上自身的安全意识不足，因此很容易导致互联网存在着很大的安全危险。由于很多互联网运营机构以及使用者单纯的关注应用功能，忽略互联网数据的安全，很多网络使用者的心里都有着一定的侥幸心理，以为数据被盗或者黑客攻击的现象不会出现在自己身边，这就导致计算机互联网技术的作用没有得以发挥，给不法分子带来了可乘之机[5]。

4 计算机网络安全技术问题的防范措施

4.1 加强网络安全管理

网络相当复杂，许多不法分子都是利用网络的虚拟性、开放性和共享性的特点来进行互联网犯罪活动，通过一些病毒来窃取客户数据，所以有关人员必须通过各种技术手段来提高对互联网的安全控制。对消费者而言，在我们应用计算机网络的过程当中，要强化自身的网络安全意识，定经常对计算机进行杀毒，对杀毒软件进行更新，保证不访问不正常的站点。对监管单位而言，应做好监管工作，强化对上网场所的监管，强化了对有关上网犯罪案件的监督管理，切实地严厉打击相关违法犯罪，以维护计算机及网络平台的安全[1]。对企业而言，必须设置自己的网络安全防护系统，这相当于企业的内部网，把企业的网络环境与外部网络环境有机分隔起来，避免外部的非法侵犯，同时对关键信息必须实行保密管理，避免外部的非法使用，同时针对关键信息可以进行保密管理，防止这些信息可以被通过互联网存取。公司还能够建立一定的授权机构，不同的员工享有不同的授权，这就可以保证不同等级的员工能够读写不同的信息，以此保证信息的安全与准确性。同时公司针对不同等级的信息要求建立不同的信息保密等级，以此更好地保证较高级别信息的安全。

4.2 防火墙技术

计算机中的防火墙技术，是管理着企业内网络和在外界互联网之间的连通状态，并通过企业在内部所建立的安全防御措施对在的局域网信息实施了防护，来防范在外界互联网上传播的病毒进入企业内上网，而防火墙技术则主要包含了在软与硬两方面，对企业在的局域网中的信息进行了监控，以防止非法入侵、恶意代码的进入，并以此来保护内部网络信息的安全，而防火墙在对内部网络上一般都具备了安全报警、设置或者修改内部网络地址信息的能力，同时通常还具有了对内部网络的工作状况进行监控，并且对安全数据信息进行保存的能力，由此实现了改善内部安全性的作用，同时也具有了控制内存应用和控制外部网络、站点使用情况的能力，对于改善的内部安全性也具有着十分重要的作用，不过因为防火墙的技术特点众多，所以需要按照具体的工作环境进行选择，在通常情况下，建议可以选用很多种的防火墙技术，对整个网络实施保护[2]。同时也能够根据内外的要求，对整个互联网上的流量情况实施检测，同时也对互联网中的流量数据进行集中控制与管理，改动将某个软件集中存储到防火墙中，从而集中对整个网络上

的数据进行安全保护。通过防火墙还能够对整个网络的安全情况进行数据统计、分析，并可以对每日的网络流量状态进行统计分析和汇总，以便能够在最大范围内防止网络黑客、病毒访问互联网内的电脑或者服务器。

4.3 优化运行环境

外界条件与计算机的安全使用有关，用户应注意对工作条件做出相应的调整，防止因为环境因素而危及应用安全。首先，保持机器工作场所的清洁和干净，减少空气潮湿和灰尘，确保地面清洁，一旦空气相对湿度很大，应采用降湿设施保持空气干燥；其次，雷击会对计算机硬件产生损伤，用户应进行防雷保护措施；最后，对房间温度控制做好管理，假如房间温度控制过高则会降低电脑散热，需要采取合理的降温措施。

4.4 实现计算机网络技术人员综合素质的提升

计算机从业人员在日常工作过程中需要严格按照要求进行作业，在企业有不安全的上网作业情况后必须进行制止，避免造成严重的后果。此外，企业还应该加大力度地推动计算机及网络信息技术的改革和开发，对计算机及网络工作者进行全面培训，不仅提高企业自身信息技术素质的提升，还深入了解新型信息技术，为计算机系统安全性提供有力保障。另外，企业管理者也需要提高加强日常网络安全管理工作的意识，通过定期检查防火墙的运行状态，以形成正确的计算机应用方法，并做好相应的安全措施，从而对于未来计算机网络的安全应用打下了更加坚实的技术基础。

4.5 提升安全防范意识

在计算机的网络安全技术中，使用者安全防范能力对其作用尤其重要，所以，在计算机网络安全的研究领域，就需要使广大网络用户提高了对网络的认识和重视，并以此来判断安全等级。首先，在软件的开发环境中，大量采用网络安全技术，同时利用多媒体使用户更充分地意识到网络防护的重要地位，促进用户对建立安全网络、防范病毒的合理认识[3]。例如，用户在网络安全期间切莫随意登陆钓鱼网站，对带有敏感内容的图片、视频等网站也切勿进行浏览，及时进行杀毒、清除垃圾，以保证电脑的安全系数在合理范围以内。另外，软件开发企业也应经常向使用者发布与杀毒相关的资讯，包括病毒查杀提示、垃圾清理提示等，以让用户在潜移默化中养成定期杀毒、清理垃圾的好习惯，从而降低网络危险。最后，使用者应配置市场上使用的专业杀毒软件，进行更新和查杀病毒，启动抗病毒效果入侵功能，减少木马病毒侵入的可能性，增强防范能力。在收集和传输重要资料信息中，要设定加密，防止信息被截获或者被窃取。

4.6 风险评估和风险管理

对于计算机网络来说，对其进行风险评估的最大意义就是要规避掉可能存在的安全风险，这是保证互联网风险的必要条件[4]。但针对风险管理来说，技术的关键作用就是通过与脆弱度分析、攻击图研究等相结合的手段，来防止网络安全隐患的出现，而网络扫描技术就是利用这一技术为基础，通过对互联网上的脆弱点、以及安全隐患进行查找，可以全方位的确保每个存在的安全隐患都得到了合理的分析与管理。

结语

综上所述，相关机构要进行计算机安全技术的基础研发工作，并通过科研培养专业化的计算机及网络人才，以逐步构建安全可靠的计算机网络系统，同时通过增强计算机杀毒、防火墙的安全功能和做好计算机网络保护工作，以保证用户的生活工作安全。除此之外，必须全面提高广大计算机用户的安全防范能力，科学的利用计算机，完善其网络行为，如此才能降低计算机和安全隐患带来的风险。

参考文献

[1]於肇鹏.计算机网络安全技术的影响因素与防范策略分析[J].无线互联科技，2021，18(20):21-22.

[2]吴晖.计算机网络安全技术的影响因素探索[J].无线互联科技，2021，18(20):78-79.

[3]雍岐剑.关于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(06):150-151.

[4]荀莎莎.计算机网络安全技术的影响因素与防范措施[J].科技资讯，2021，19(13):32-34.DOI:10.16661/j.cnki.1672-3791.2104-5042-8917.

[5]段聪影.计算机网络安全技术的影响因素与防范措施[J].信息记录材料，2021，22(05):60-61.DOI:10.16009/j.cnki.cn13-1295/tq.2021.05.032.