ISSN:2705-0963（Print）　ISSN:2705-0955（Online）

Pisco Med Publishing

计算机网络安全漏洞及防范措施

付羽冉

黑龙江财经学院　黑龙江　哈尔滨　150000

摘　要：新形势下，计算机网络技术已经在相关领域中得到了相对广泛的应用，但计算机网络安全漏洞却呈现出了愈演愈烈的趋势，因此应当做好相关层面的漏洞防护工作，切实保障计算机用户的信息安全，进而避免其他不必要的损失。其实互联网技术更像是一把双刃剑，它既能够提高用户的工作和学习效率，但又有可能造成其他风险事件。不法分子会利用网络安全漏洞攻击用户的计算机，进而窃取个人用户或企业的隐私信息。此外，遭受过攻击的计算机系统也会遗留下各种安全漏洞，会有可能造成更为严重的损失，因此需要做好相关安全漏洞的防范工作。

关键词：计算机网络；安全漏洞；系统漏洞

进入信息时代，人们的工作以及生活与计算机、网络密切相关，计算机已经成为一项基础性工具。由于当前网络环境开放度较高，加之相关法律法规完善度不足，在计算机应用过程中，信息泄露、篡改等事件时有发生，严重威胁网络安全，甚至还会使单位以及个人蒙受巨大损失，因此，相关工作人员应积极总结以往常见网络安全漏洞，及时采取有效防范措施，提高计算机网络安全。以计算机技术发展作为背景，借助计算机技术，不仅可以有效满足各领域交流沟通，还能够进一步促进我国经济发展，但是与此同时，用户对提高网络安全性的需求也逐渐迫切，相关安全漏洞的出现，将会导致用户使用体验下降显著，并为用户工作以及生活等多个方面带来不便。本文以计算机网络安全作为研究方向，具体对安全漏洞进行分析，并提出相关防范措施，以供参考。

一、网络安全漏洞

在不同原因下，受到多种因素影响，将会引发计算机网络安全问题。总体而言，该问题的出现主要与人为操作、计算机系统自身漏洞以及客观因素有关，导致在实际应用过程中，存在各种各样的计算机网络漏洞，使计算机处于运行异常状态。一旦上述问题没有得到有效解决，将会给予不法分子可乘之机，严重影响用户财产安全。特别是针对计算机自身系统问题，由于难以彻底解决，因此，当这种漏洞出现后，将会给相关企业以及单位造成巨额损失。

二、计算机网络漏洞

（一）系统漏洞

系统漏洞主要与网络协议有关，并且在操控体系具有缺陷的情况下，也会引发系统漏洞。具体而言，在网络协议中，具有较高的开放性，包容性较强，而这一优势也间接增加了网络安全漏洞，导致网络安全受到影响。例如，在 IP 协议存在缺陷的情况下，一些不法分子借助缺陷，能够以用户名义操作用户计算机电脑，盗取相关信息，而这一操作难以被安全防护系统发现。而在系统初始化、服务器文件配置失误的情况下，将会给予不法分子可乘之机，导致计算机系统出现病毒，并且病毒查杀软件无法对该病毒进行识别并拦截，形成计算机安全问题。

（二）病毒入侵

经计算机系统，可完成与外部网络的信息交互，在这一过程中，充分体现了计算机功能的多样性。因为计算机功能处于逐步完善状态，信息交互较为频繁，这也增加了病毒传输的渠道，导致计算机受到外部网络病毒攻击，出现相关用户信息盗取、破坏以及丢失事件。并且在严重的情况下，还会造成系统瘫痪，使计算机无法正常工作，对用户影响严重。病毒入侵属于常见安全漏洞，属性相对复杂，可长期潜伏在系统中，经网络，实现大面积传播，危害较大。并且病毒种类多样，不同种类病毒破坏力、破坏方面也有所不同。近年来，以计算机网络技术发展作为前提，病毒也得到了进一步发展，无论是破坏力，还是复杂性，均得到显著提升，仅仅通过单一使用杀毒软件，难以实现对病毒的彻底查杀。当相关有害程序（特洛伊木马、炸弹、病毒）入侵到计算机中，将会形成相关网络安全漏洞，引发网络安全风险。对于特洛伊木马而言，当其攻击计算机系统后，将会安全防护系统故障，为黑客入侵拖延时间，该木马破坏能力较高，范围较广。与之相比，炸弹扩散范围相对较少，但是同样具有较大的破坏能力，导致网络信息资源被破坏。

（三）黑客攻击

对于社会生产、生活而言，计算机属于基础性工具。因此，计算机网络安全与系统运行密切相关，并且还会直接影响用户经济利益。在计算机系统中，黑客攻击主要对象为国家、企业、个人储存的信息数据。黑客能够设计病毒，对私人计算机系统进行攻击，盗取信息、数据，牟取利益，严重损害计算机网络安全，甚至还会直接影响社会利益，威胁国家安全。在黑客攻击的情况下，计算机将会呈现系统瘫痪状态，无法正常投入到工作、生活中，并且黑客还能够监视该计算机系统，盗取相关信息。

（四）浏览器漏洞

在计算机中，浏览器的使用较为常见，不仅能够帮助人们及时、有效获取各类网络信息资源，还具有实时上传、分享各类信息资源的功能。但是受到浏览器自身漏洞影响，在

ISSN:2705-0963（Print） ISSN:2705-0955（Online）

信息上传以及下载过程中，将会出现网络安全风险。基于这一情况，虽然相关工作人员积极编写程序，提升浏览器功能完善性，确保其属性安全，但是由于用户个人操作问题，网络安全风险始终存在。

三、安全漏洞防范对策

（一）技术层面

1. 漏洞扫描

在相关防范措施中，定期漏洞扫描具有较高的直接性，通过扫描计算机运行空间，加以有效分析，能够检查出相关入侵、攻击行为，并进一步对计算机系统中存在的信息进行检测，确保信息合法性、合理性，当发现安全漏洞时，能够及时完成漏洞修补，使相关安全问题得到有效控制。针对计算机系统，需要经服务器、核心硬件，完成数据交换，而在这一过程中，借助漏洞扫描，在安全漏洞检测方面效果显著，并且可以有效对漏洞进行处理，使模拟计算机安全防护中存在的缺陷得到修补。

具体而言，无论是 Ping 扫描技术、端口扫描技术，还是弱点探测技术，均属于漏洞扫描技术。以 Ping 扫描技术为例，借助该技术，能够实现对主机 IP 地址的有效监测，并对计算机端口进行检查，观察其网络状态以及服务条件，以此作为参考，具体分析计算机网络安全情况。结合该技术应用，在定期范围内，应完成技术升级工作，保障技术性能与时俱进性，使各类新型病毒能够被有效识别。同时，在使用过程中，应逐步增加扫描范围，保护计算机环境质量，优化使用安全性。

2. 入侵防御技术

计算机系统信息资源传输、共享的实现主要通过与不同网络结构构建信息交互完成，借助这种信息交互方式，有效摆脱了时间、空间的束缚，提升了信息交流空间的开放性，使其具有更高的灵活性以及便捷性。但是为有效保障信息传输、共享安全性，还需要相关人员加大管控力度，通过使用入侵防御技术，提高信息安全，保护网络安全。就目前而言，在市场中，相关入侵检测软件产品种类较多，但是这些软件多以事后控制为主，只有在计算机受到攻击影响的情况下，才能够发挥作用，同时，该类型软件具有较高的失误率。因此，要求行业应加强事前入侵防御技术研究，总结以往常见网络漏洞，并提出针对性预防措施，将其纳入到总体网络安全风险预防方案中，建立有效计算机网络安全防御体系。经计算机安全防护系统，可有效实现外部入侵预防，使计算机网络能够始终处于安全状态，提升计算机使用稳定性。除此之外，在相关入侵防御软件研究中，应重点突出软件病毒拦截功能以及恶意攻击拦截功能，在计算机系统中，深入挖掘各类潜藏病毒，深度清理各种垃圾邮件。

3. 防火墙安装

分离器、限制器以及分析器共同构成了防火墙，借助防火墙，既能够监督计算机内部网络环境，还能够有效监督计算机外部网络环境，为系统运行安全提供了有效保障。正常而言，防火墙多配备在计算机系统、外部网络中，起到良好的屏障作用。具体而言，基于安全漏洞预防工作，应结合计算机系统实际情况以及运行需求，在合理选择防火墙后，完成相应的安装工作。同时，在固定时间间隔内，应强化防火墙检验工作，并及时对其进行升级，保障防火墙实际功能，确保计算机系统能够始终处于安全防护状态。通过应用防火墙技术，能够实时对各类信息数据进行监护，并且能够监护整个信息传输、共享过程，避免计算机系统受到外部入侵。除此之外，经防火墙扫描，建立在有效检验基础上，能够对计算机通信数据进行判断，在确定其安全性的基础上，方允许后续访问动作。如果使用防火墙为高性能防火墙，还具有病毒过滤功能，当检测出信息存在安全风险后，可及时予以过滤，有效防止病毒入侵。区别于安全防护原理，可具体对防火墙进行技术分类，包括过滤以及互联网服务、检测等。具体分析上文三种技术类型，过滤技术出现时间最早，属于早期防火墙形式了，借助路由器端，以互联网协议、地址作为筛选对象，能够发现不符 IP，并以法律法规作为基础，对相关互联网协议以及地址进行访问，提高计算机网络安全性。

4. 数据加密技术

受到数据加密不足影响，将会导致不法分子有漏洞可钻，不利于计算机网络安全。因此，要求相关人员应切实落实数据加密工作，通过提升该项技术先进性，使数据能够始终保持安全状态，进而保障计算机系统安全防御能力。在应用数据加密技术过程中，可进一步配合防火墙，以内、外两个角度出发，严密保护计算机信息安全。总结目前现有数据加密技术，主要类型包括两种，即对称式、非对称式。针对对称式加密技术而言，无论是加密，还是解密，密钥使用具有相同性，该技术在加密速度方面优势显著，可将其应用在硬件系统中，使整个计算机安全性能得到显著提升，整体而言，该技术应用范围相对较广。而针对非对称式加密技术而言，该技术在加密、解密过程中，密钥使用不同，分为公钥、私钥两种，需要在配合使用基础上，实现信息解密。正常而言，公钥、私钥分别为公开状态以及私人保管状态，与对称式加密技术相比，该技术具有更加良好的加密效果，并且不会发生相关窃听情况，信息传输安全性更高。

5. 访问权限管理

以计算机系统实际情况出发，全面落实访问权限管理，有利于构建防控机制，以免出现非法用户入侵情况，防止计算机系统受到外部入侵。针对计算机访问系统，通过借助初级入网系统，能够提供相应的信息支持，便于用户完成相关访问操作，同时，该系统还能够进步控制用户登录操作，约束服务器访问操作，对用户入网时间、操作进行详细记录。当用户需要启动计算机网络系统时，须通过用户信息验证，并正确输入口

ISSN:2705-0963（Print）　　ISSN:2705-0955（Online）

令，才能够进入网络系统，无论是用户信息验证未通过，还是口令输入未通过，均不允许进入到网络系统中。

（二）管理层面

1. 提高风险防范意识

提高风险防范意识主要以用户视角出发，对用户计算机使用行为进行规范。具体而言，作为计算机网络用户，应树立正确的道德观，不随意对他人信息进行泄露，对于来源不明的软件，应谨慎下载，注意查看软件使用权限，禁止盲目开启。网络环境具有较高的开放度，易出现个人隐私泄露情况，因此，用户应提高安全风险防范意识，积极采取有效措施，减少相关安全风险事件出现。同时，应在合理范围内，保护自身权益。而针对企业而言，当发现安全风险后，出现的损失通常较为严重。因此，企业应切实完善管理体系，并将网络安全管理纳入其中，切实完善体系内容，严格限制系统访问权限，以免出现信息数据被盗取情况。

2. 加强网络安全监管手段

以世界经济发展作为背景，在互联网中，信息丰富性得到有效提升。为有效保障网络信息安全，要求相关部门应以该项工作着手，健全相关法律法规，切实落实相应的监督管理工作，经有效筛查，提升用户接收信息的安全性、健康性。同时，要加大惩罚力度，建立在眼里制裁基础上，提高不法分子犯罪成本，严厉打击各类网络违法行为。除此之外，应进一步加大维护网络安全宣传力度，加强知识普及，提高用户操作水平，提高计算机使用规范化，在最大程度上避免相关网络漏洞事件出现，保护个人以及企业切实利益。

四、结语

综上所述，计算机网络技术的飞速发展，为人们提供了一定的便利性，然而也为当前社会带来了一定的不良影响。计算机网络技术本身具有着开放性和共享性，而人们在利用计算机技术保存和获取信息时，往往会导致信息被窃取和篡改的情况，对人们的日常生产生活造成较为严重的影响，因此提升计算机网络安全技术的有效性也就成为了当前技术人员需要重点探讨的问题。技术人员应该不断优化当前的数据安全技术和防护技术，为计算机网络使用的安全性提供全面保障，使其能够更好地满足人们的使用需求，从而推动我国计算机网络安全技术的深入发展。

参考文献：

［1］邓泽 . 计算机网络安全的漏洞及防范措施［J］. 数码世界，2021（03）：256-257.

［2］徐宁，常亮 . 浅谈计算机网络安全漏洞及防范措施［J］. 网络安全技术与应用，2021（02）：160-161.

［3］郭艳光 . 计算机网络安全漏洞分析及防范措施［J］. 电子测试，2020（20）：124-125.

［4］张映红 . 浅谈计算机网络安全漏洞及防范措施［J］. 新课程导学，2020（23）：86-87.