计算机网络安全技术在维护网络安全中的应用研究

王琦

（吉林司法警官管职业学院　吉林长春　130062）

摘要：伴随着社会经济的飞速发展，因特网日趋成熟，资讯科技的发展也更加迅速。在信息时代，网络已经渗透到人们的生活中。计算机网络为人们提供了方便，但也存在着不容忽视的风险。所以，我们必须要对计算机网络进行深入的分析与研究，并做好网络的安全维护，比如对计算机的安全系统的功能进行持续的优化，对计算机的脆弱性加强对系统的保护，提高计算机网络的抵抗外部入侵的能力等等。针对这一现状，本文从网络安全技术角度出发，论述了网络安全技术在网络安全维护中的风险，并对其运用策略进行了探讨。

关键词：计算机网络；安全技术；维护

计算机网络技术为我们的日常生活提供了方便，但它所带来的危害也应引起我们的高度关注。网络风险很可能会导致个人隐私的泄漏或财产的损失，比如被黑客攻击，它不仅对公司、对社会都是一种威胁，还会威胁到整个社会的稳定。所以，加强对网络的维护，保证网络的安全，对于整个社会的发展来说，就显得尤为重要。在信息化程度不断提高的情况下，必须加强对网络安全的研究，并采用新的技术来保证网络安全。

1 计算机网络安全和计算机网络安全技术概述

“计算机网络安全指的是运用计算机网络管理技术，对网络展开监视和管理，确保用户的隐私和安全，让每个人都可以在一个安全、稳定的网络环境中使用电脑”[1]。由于计算机在实际运行的过程中，会有一定的风险漏洞，有些不法之徒会利用这个漏洞，对计算机进行攻击，窃取信息，从而获得利润，让人民的生命和财产受到巨大的伤害。为此，我国应加大对网络安全的宣传力度，提高公众对网络安全的认识。在计算机网络被攻击之后，会对网络内外造成严重的破坏，比如重要数据丢失、设备损坏等。归根结底，网络安全的本质就是为了保证我们在网上的信息的安全，它分为安全性和可操纵性两个部分。其中，“安全”的重点在于确保用户的信息安全，而“可操作”是指在确保了信息网络的安全后，仍然具有较强的操作能力。

2. 当前计算机网络安全所面临的风险

2.1 操作自身存在问题

在现实生活中，计算机网络能够给人们带来极大的方便。但与此同时，人们也越来越多地注意到了网络与系统安全问题。然而，在目前的计算机网络中，在一些具体的应用中，存在着一些问题。首先，在电脑发展过程中，电脑与资讯科技是紧密相联的，资讯科技的持续高速发展将推动电脑科技的更新换代。同时，为了适应自己的电脑系统需要，需要对电脑软体进行不断的升级与配置。所以，当计算机与自己的操作系统之间存在着不同步时，不但会被很多病毒所感染，也会使计算机不能安全可靠地工作。其次，虽然从表层来看，我们对电脑网路技术应用的真实进程进行了评价，显示出整体的发展状况还算不错，但还有很多与电脑网路技术有关的技术还在发展之中。所以，该系统在使用上还存在着一些不足之处，但如果能及时加以改进，其发展前景将十分光明。

2.2 系统漏洞风险

系统出现漏洞、计算机受到病毒、黑客攻击，导致信息泄露、信息被篡改、非法信息传播等，是网络安全的风险。从目前的计算机系统发展状况来看，它们或多或少都存在着一定的缺陷，因为网络是虚拟的，所以用户的个人信息很容易被盗取或篡改，这样的情况不但会扰乱网络中的传输信息，还会给用户带来难以估计的损失。软件同样是计算机中的一个重要组成部分，它包括了操作系统、数据库、应用软件、传输控制协议、网络软件和服务、密码设置等。

2.3 计算机病毒风险

“电脑病毒是指对电脑的安全性造成严重威胁，从而使电脑无法正常运作的程式或程式语言”[2]。它具有非常强大的自我复制能力和破坏能力，一旦它侵入了计算机系统，就会对计算机的源程序代码进行破坏，造成计算机瘫痪。不能正确启动。有些隐藏的病毒也是非常危险的，比如特洛伊特洛伊特洛伊。木马病毒并不会迅速地进行自我复制，也不会故意对一些软件造成伤害，而是会以自己的身份进行伪装来吸引使用者下载，当使用者点开相应的链接或程序时，便会对使用者造成持续的伤害，进而开启宿主的“门户”，让使用者彻底失控。黑客们可以肆无忌惮地破坏和窃取重要的资料，甚至是遥控控制。

2.4 网络黑客入侵风险

网络黑客以其高超的编程技巧，可以破译各种商务软件，侵入网站，对网络实施攻击。这类人员可以敏锐地察觉到计算机系统的漏洞和缺陷，并可以针对其弱点进行攻击，并制作虚假的网络信息，导致严重的网络安全问题。使用挂马式网址，通过其它恶意程序散布木马。在木马被广泛传播之后，专业的黑客们就能够通过它来获得用户的关键信息，而且，黑客们经常会通过链接的方式，在软件中植入木马，来破坏软件，来实现对软件的远程控制。当病毒侵入电脑时，电脑拒绝服务，并消耗使用者的通信，造成电脑整体瘫痪或系统死机。使用第三方的弱点来进行攻击。随着人们对系统补丁的理解越来越深刻，他们在使用网络的时候，也在不断地提高自己的电脑系统的安全和防御能力，因此，黑客利用系统漏洞来进行网络攻击的可能性也就越来越小。但是，黑客们为了达到他们的不正当目的，就把他们的攻击对象转向了第三方软件，他们利用一些人们经常使用和需要的流行软件，比如一些视频软件、文字处理软件等，来对用户的电脑进行入侵。通过网游窃取账号，窃取用户财物。网络游戏作为一种十分普遍的网络娱乐活动，它的流行特征为网络黑客提供了可乘之机。玩家想要玩游戏，必须要用游戏币来支付，所以玩家要承担一定的财产风险。因为在虚拟的游戏世界中，在玩家的认知中，人物和装备都是稀缺的，因此，玩家们在游戏中进行了大量的投资，因此，游戏资产市场变得异常活跃。于是，黑客们开始盗取账号，进行账号的买卖，主要是游戏账号，密码，虚拟货币，虚拟装备。黑客窃取帐号后，再通过正常的交易网站进行交易，将虚拟货币转化为真实的货币，这其实就是窃取使用者的私有财产。网络钓鱼的手段是通过制作假网址来欺骗用户。在现代社会，电子商务这种新的商业模式得到了很大的发展，因此，网上结算、网上银行等各种网络支付和交易方式都与网络紧密地结合在了一起。这样

的交易方式也给了网络黑客机会，他们会通过伪造的网址，欺骗浏览网址的人，让他们交出银行卡帐号、密码等详细的个人资料，这在金融业非常普遍，而且对于黑客而言，建立一个钓鱼网址并不是什么难事。

3 计算机网络安全技术在维护网络安全中的应用策略

3.1 应用防火墙技术维护网络安全

过滤型防火墙。顾名思义，就是一种用于对数据信息进行过滤的防火墙。按照预先设定好的指导原则，对流入到网络中的信息进行筛选，通过的信息被“放行”，不通过的信息要么被清理，要么被删除。在实际使用中，它是一种构造简单、造价低廉的新型防火墙技术。防火墙是目前应用最广泛的一种计算机网络安全技术，它能对计算机所处理的数据进行监控，并对其进行有效的拦截和处置。在应用层防火墙中，以服务器为核心，对服务器接收到的各种数据进行扫描，并对其进行实时监控和清除。

3.2 使用入侵检测技术维护网络安全

这种保护技术主要应用于计算机软件和硬件设备中，从多个角度对计算机内部的整个各个系统的工作情况进行检查，并对网络系统中的正常使用和危险行为进行合理的区分，从而从根本上提升电子设备运行的安全保障。它可以精确地甄别和标注重要的使用者资料，当资料有变动时，会立即察觉到并上报系统的异常状况，并采取相应的验证措施，并提醒有关人士，防止资料外泄。它是一项全方位的电脑网路安全性测试技术，在这项技术运用的过程中，将收集到的资料进行比对，并将其储存到电脑中。这样，通过入侵检测技术，用户就能够追踪和管理操作系统，识别出用户的正常网络行为，从而确保数据文件的完整性以及计算机网络的安全。

3.3 运用信息加密技术维护网络安全

“计算机信息加密技术主要是为了保护用户的隐私和隐私，对一些重要的文件进行加密”[3]。计算机密钥，保密通信，防拷贝等都是信息加密的一种。通常情况下，在数字通信中，会使用改变负载信息结构的方法，使用加密法对计算机进行加密，对计算机的保护主要是以软件加密为主要手段，有些情况下，为了增强机密性，加密软件还会使用硬件加密、加密软盘等方法，只有使用对应的密钥才能打开加密的数据文件，阻止来自外界的传送或入侵的数据，确保数据不会被泄露，从而对计算机网络的安全性起到更好的保护作用。

3.4 隧道技术

隧道技术是一种基于海量数据来传输因特网上各种类型数据的技术。如果你仔细研究一下，就会发现，所谓的通道技术，就是将所有的数据，重新整合在一起。从总体上看，从业者要根据实际情况对数据系统进行整理，将可用的数据用于加快网络和各类相关的部件，在非真实互联网中的传播，信息隧道就是一种可以采用的整理方式。

3.5 数据加密技术

在计算机网络安全维护中，可以灵活地利用加密技术，实现用户计算机软件和重要的信息数据加密管理的应用目的，将原来的文字和信息数据转化为密文，若要恢复原来的内容，则必须使用与之相符的密钥，从而增强了计算机系统中数据传输和保存的安全性。在网络信息的发展和信息数据的传输过程中，应灵活使用信息数据的加密技术，对信息数据的传输系统进行改进，确保传输的安全性，提升网络环境的安全性。“根据实际了解互联网技术的发展情况，在发展互联网加密技术的过程中，应当划分为数据保存、数据传导与数据分辨”[4]。在资料传送的加密上，可藉由多种科技手段，深化网路工作的执行。比如目前美国的新 DES 技术、欧洲的 IDEA 技术，在全球都处于领先地位。在当今的网络安全技术中，加密技术是不可或缺的一环，它不仅可以有效地防御非法入侵，还可以驳斥恶意病毒等。

3.6 杀毒软件

反病毒软体是侦测，侦测，并清除电脑上的病毒。另外，有些防毒软件也可以用来还原被病毒侵入的资料和档案。而在国内，防毒软件的发展方向也是在不断地向着可以对被病毒侵入的数据以及有关的文件进行恢复的方向发展。总体来说，我们国家的防毒软件能识别和清除超过 9%的计算机病毒，保证了我们的计算机能正常的安全运行。就国内现有的杀毒软件来说，以金山毒霸，瑞星为代表的杀毒软件是主流。

3.7 加大计算机尖端人才的培养力度

网络信息安全问题不但在中国，而且在全世界都是一个很大的问题。不仅是中国的问题，网络安全的问题也出现在世界各地。另外，对军队来说，网络安全的问题也在不断地恶化。一个国家的军用网络如果没有足够的安全性，那么它将不能保障国家的安全，也将威胁到整个世界的安全。例如，美国的卫星通讯，远程录像服务，以及军用网络都受到了攻击，这些攻击会造成一些卫星的减速或者相撞，而另一些卫星也会因此而停止运转。所以，“对一个国家来说，对其进行全面、系统地培训是十分必要的，它直接关系到一个国家的军事力量”[5]。为此，我国教育机构应加大对计算机专业人才的培养力度。

4. 结语

伴随着信息技术的持续创新和发展，我们国家的网络技术取得了不可思议的进展，如今网络技术已经渗透到世界的每一个角落，给我们的生活带来了极大的便利。然而，需要指出的是，我们国家的电子网络的安全性还需要进一步提升，当我们在使用联网的电子设备的时候，一定要注意设置防火墙以及其它的一些系统，以保证我们的设备的安全，并将它们隔离开来，让我们的计算机处在一个绿色安全的环境中，这样才能更有效地使用我们的电子设备。在目前信息化社会的发展过程中，计算机网络安全是人们所面临的一个问题。互联网已经变成了人们生活中不可或缺的一部分，所以，人们必须要对网络安全给予足够的关注，而且要根据未来多样化的时代发展趋势，持续研发出与时代发展需求相适应的计算机网络安全技术。增强他们的安全意识，使他们对网络安全技术有一定的认识，从而在社会上形成一个由社会各方共同努力来维护网络安全的新局面。只有这样，才能让人们在享受到科技带来的方便的同时，也能保证他们的信息安全，从而让他们更好地享受到科技进步所带来的成果。

参考文献：

[1]陈铭.基于网络安全维护的企业计算机网络安全技术应用探讨[J].通讯世界,2018(10):109-110.

[2]张磊.计算机网络安全技术在网络安全维护中的应用[J].电子技术与软件工程,2020(07):237-238.

[3]孙一蓬.网络维护中应用计算机网络安全技术的策略探究[J].信息记录材料,2021,22(10):82-83.

[4]刘雯怡.计算机网络安全技术在维护网络安全中的应用研究[J].网络安全技术与应用,2022(04):168-169.

[5]徐晨.计算机网络安全技术在网络安全维护中的应用分析[J].中国管理信息化,2022,25(08):189-191.

作者简介：王琦，1981.01，吉林长春人，男，汉族硕士，实验师，研究方向：软件工程。