现代计算机技术与应用
2021 年 11 月第 3 卷第 4 期

影响计算机网络安全的因素与应对措施

张　戈

华中师范大学计算机学院，武汉

摘　要 | 当前，计算机网络快速发展，成为重要的交流工具，在社会各方面发挥着重要作用，但它在给人们的生活、工作等带来便利的同时，也带来了一系列的网络安全问题，这给计算机网络安全带来诸多挑战。本文主要从分析影响计算机网络安全的因素入手，探讨计算机网络安全的应对措施。

关键词 | 计算机网络安全；影响因素；对策

随着计算机网络的迅猛发展，网络已渗透到人们生活的方方面面，给人们的工作、生活、学习等带来极大的便利。但与此同时，网络不法分子的侵入手段也越来越高明，给网络安全带来极大的隐患，因此研究计算机网络安全问题具有十分重要的意义。计算机网络安全是指利用网络管理措施，在网络环境中确保数据不被破坏。计算机网络安全主要包括物理安全与逻辑安全两方面，也就是硬件安全与软件安全。物理安全是指计算机不会因为自然或人为的原因而遭到破坏，引发网络的不稳定，确保网络连接的畅通。逻辑安全是指确保信息

作者简介：张戈，华中师范大学计算机学院，硕士。
文章引用：张戈. “影响计算机网络安全的因素与应对措施［J］. 现代计算机技术与应用，2021，3（4）：94–100.
https://doi.org/10.35534/mcta.0304019c

的保密性、完整性、可用性。计算机网络资源在传递的过程中确保信息的完整与真实，不会发生篡改现象。计算机网络安全涵盖的范围比较广，目前，越来越多的人认识到网络安全的重要性。虽然我们在计算机网络安全方面已取得了一定的成效，但还存在诸多问题函待改进。因此非常有必要探讨影响计算机网络安全的因素，并提出针对性的改进策略。本文主要从分析影响计算机网络安全的因素入手，探讨计算机网络安全的应对措施。

1 影响计算机网络安全的因素

随着计算机网络应用范围的不断扩大，计算机网络安全问题越来越凸显，我们要解决这些问题必须分析影响计算机网络安全的因素。影响计算机网络安全的因素既有人为因素，又有自然因素，必须针对这些因素采取应对侧落实。

1.1 病毒因素

计算机病毒是指编制或在计算机程序中加入的破坏计算机功能和数据，影响计算机使用并能自我复制的遗嘱程序代码。计算机病毒具有隐蔽性、破坏性、复制性等特点，感染病毒的计算机能通过网络进行繁殖传播，在短时间内分布在各个网络的结点里，造成网络瘫痪。如曾经轰动全国的“熊猫烧香”病毒，通过下载文档的方法传播病毒，给计算机系统带来很大的破坏，让计算机网络用户体会到了病毒的巨大破坏力。计算机病毒传播速度快，造成的损失难以估计，计算机感染上病毒，轻则造成工作效率下降，重则造成计算机瘫痪、死机。计算机常见的病毒类型有引导区病毒、文件型病毒、宏病毒、蠕虫病毒、特洛伊木马等。引导区病毒是指通过感染软盘的引导扇区进行病毒传播文件型病毒是将攻击代码插入到可执行文件内传播病毒宏病毒是使用宏语言编写，可以在数据处理系统中运行，通过宏语言将自己复制并繁殖到其他数据文档内蠕虫病毒是通过网络漏洞自主传播，它是一种通过网络传播的恶性病毒特洛伊木马的隐蔽性较强，利用系统漏洞引入用户电脑。木马进入用户电脑后就隐藏在系统目录内，通过修改注册表等进行病毒传播。计算机病毒更新速度快，破坏力大，是影响计算机网络安全的重要因素，必须切实防范计算机病毒。

https://doi.org/10.35534/mcta.0304019c

1.2 黑客因素

网络是开放的，常受到外界的攻击。相对于计算机病毒来说，黑客对计算机网络安全的危害程度更重，黑客是世界上计算机网络安全面临的最大威胁之一。黑客主要是人为因素，一些专门研究计算机网络漏洞的计算机爱好者，利用计算机网络存在的漏洞进行攻击。现在黑客已成为那些专门利用计算机进行非法破坏或入侵他人的代名词。黑客攻击分为破坏性攻击和非破坏性攻击，破坏性攻击会带来非常严重的后果。目前黑客攻击网络的问题很严重，他们常非法侵入重要信息系统，窃听、攻击侵入网络的有关敏感性重要信息，并篡改数据，破坏硬件设施，使网络无法正常使用，从而造成数据丢失，甚至引发系统瘫痪，给用户带来极大的损失。黑客的存在并不是说黑客能制造机会，而是他们善于发现漏洞，这是因为网络自身存在缺陷，使之成为被攻击的目标。随着计算机技术的发展，黑客技术也在不断的更新，因此防止网络黑客的攻击，已成为摆在每个国家面前的重要问题。

1.3 系统因素

计算机操作系统是一种支撑软件，它是使程序或者其他的系统得以运行的一个环境，是计算机运行的基础，由此可见其重要性。但操作系统自身存在不安全因素，它有一些漏洞与不安全性，为计算机网络安全带来诸多问题。操作系统存在结构上的不足，它包括管理、内存管理及外设管理，任何一个管理都涉及很多模块以及程序，一旦这些程序出现问题，很可能导致整个计算机网络的瘫痪，所以黑客常针对系统本身的缺陷进行攻击。网络系统本身的安全问题主要有系统漏洞和移动存储介质，系统漏洞对网络安全的威胁是不可估量的。同时由于价格问题，很多用户使用的电脑操作系统是盗版的，安装使用时不按照系统的配置要求进行安装，导致系统运行时出现诸多问题。其实，操作系统都有漏洞，并且发现这个漏洞到修复需要一定时间，这是一个漫长而具有技术性的工作。正是因为系统存在漏洞问题，黑客经常扫描漏洞，一旦发现漏洞，黑客就会通过技术手段达到控制计算机的目的。同时计算机操作系统允许在计算机网络上传送文件或者安装程序，这也会对计算机

网络安全带来威胁。

1.4 软件因素

软件是计算机运行必不可少的组成部分，有些软件在开发过程中，由于开发者的不注意或者技术所限解决不了，导致软件自身存在一些隐患，一旦这些软件遭受到病毒入侵或者黑客控制，会对计算机网络安全带来威胁。软件带来的网络安全问题很严重，比较常见的是缓冲区溢出遭受攻击，这是一种恶性攻击行为，这是因为在缓冲区没有相应的防范限制，会导致程序的堆栈被破坏，它能使所有数据具有启动程序的功能，进而导致系统崩溃。

1.5 安全意识因素

要全面保证计算机网络的安全，紧靠技术层面是远远不够的，还要加强管理人员及网络用户的安全意识。计算机网络安全防护中，管理人员如果具有较高的技术能力和较强的防范意识，能使网络安全工作达到事半功倍的效果。计算机网络安全人为方面的隐患主要体现在人为泄露，这主要是计算机操作人员的安全意识差，设置计算机口令时过简单，很容易被人识破，或者没有基本的安全意识，随意的把口令告诉别人等，这都会对计算机网络安全造成威胁，造成保密性信息的流失。由于用户安全意识淡薄，使用公共计算机时会留下个人信息，或者随意的把个人信息告知他人，设置的账号密码过于简单等，都会造成个人信息的泄露，不仅会给个人财产带来随时，还会威胁到计算机网络的安全。

2 计算机网络安全的应对措施

2.1 提高技术

为了保证计算机网络安全，网络安全技术是非常重要的，主要包括密码技术、防火墙技术、入侵监测技术等。数据加密技术是网络安全的核心和关键，是对信息重新编码，使非法用户无法获得真实信息的一种技术手段。数据加

https://doi.org/10.35534/mcta.0304019c

密技术的目的是提高信息、数据的安全性，这是防止外界非法用户获取信息的主要手段之一。防火墙技术是网络安全的第一道屏障，是一种隔离技术，一般来说保障网络安全的首选举措就是安装防火墙。防火墙技术能在某机构的网络与不安全网络之间设置屏障，防止对信息资源的非法访问。企业为了保障内部信息的安全，在企业网与网络之间设立防火墙，入侵者必须穿过防火墙的安全防线，才能接触计算机。防火墙比较简单实用，可以在不修改原有网络系统的情祝下，达到一定的安全要求，因此得到了广泛应用。入侵检测技术是对计算机网络资源恶意使用进行识别和检测的一项网络安全技术，检测的目的是发现潜在的攻击行为并采取针对性的防范措施，从而确保计算机网络安全。

2.2 防治病毒

随着计算机技术的发展，病毒也变得越来越复杂，对计算机网络安全带来威胁。计算机病毒可以说无孔不入，因此计算机要防治病毒。病毒查杀可以及时发现恶意攻击行为，确保计算机网络安全。当前计算机网络病毒形式多样，传播途径也不断的发生变化，由于病毒具有危害大、传播快的特点，给计算机网络安全带来极大挑战。现在防治病毒的措施主要是安装杀毒软件，并不断的进行软件升级，更新病毒库等。从功能上说，防病毒软件可以分为网络防病毒软件和单机防病毒软件，网络防病毒软件主要防治网络病毒，一旦病毒入侵网络，网络防病毒软件会立即检测到并删除单击防病毒软件。

2.3 加强管理

计算机网络安全问题是不可避免的，必须加强安全管理。网络安全管理是一项综合管理，不仅仅是简单的技术问题。人们常说网络安全是七分管理三分技术，这说明了管理在计算机网络安全中所起的重要作用。计算机网络安全管理不仅要加强防范，还要加大所采取的管理措施。计算机网络安全主要包括计算机安全意识教育、维护和保养计算机网络的相关知识、计算机网络安全机构建设，并且要建立完善的安全管理体制，网络管理人员要尽一切可能将不安全

因素降到最低。同时加强计算机网络安全的规范化管理，强化管理人员的安全意识。

2.4 访问控制

访问控制是计算机网络安全防范的主要策略，主要是保障信息资源不被非法访问。访问控制主要采用认证系统、访问控制网关、防火墙等方式，在网络资源边界处设置控制网关，这样用户要使用网络资源，只有通过身份认证才能进入，确保用户信息的有效性，如果出现问题就进行追查。同时访问控制还能合理分配网络地址的流量，结合用户需求进行访问限制。另外网络还对访问者进行审核，如果非指定工作站入网访问或者多次口令输入错误，系统都会默认为是非法用户，拒绝继续登录。

2.5 数据备份

为了确保计算机网络安全，用户可以将数据进行备份。数据备份是将有用的文件、数据拷贝到另外的地方，即进行数据备份，即使计算机遭到攻击破坏，也不用担心数据丢失。所以，做好数据备份是保障计算机网络安全的最有效措施之一。数据备份主要是针对计算机网络安全隐患的，如人为损坏、硬件损坏、自然灾害等，同时也能确保数据的完整性。总之，当前计算机网络安全问题越来越受到人们的重视，这不仅仅是技术问题，还是一个管理、使用问题。随着计算机网络技术的快速发展与应用的深入，计算机网络安全技术也应不断发展，从而尽可能提高计算机网络的安全性。

参考文献

[1] 荀迈华. 计算机网络安全问题及防范策略 [J]. 软件，2013.
[2] 栾好利. 浅谈计算机网络安全的对策 [J]. 山东省青年管理干部学院学报：青年工作论坛，2001（1）：73.
[3] 李青春，张肇欣. 浅谈计算机网络的安全问题与防范 [J]. 科学技术创新，2015，（24）：175.

https://doi.org/10.35534/mcta.0304019c

Factors Affecting Computer Network Security and Countermeasures

Zhang Ge

School of Computer science, Central China Normal University, Wuhan

Abstract: At present, the rapid development of computer network, become an important communication tool, plays an important role in all aspects of society, but it brings convenience to people's life, work and so on at the same time, also brings a series of network security problems, which brings many challenges to computer network security. This paper analyzes the factors affecting computer network security and discusses the countermeasures of computer network security.

Key words: Computer network security; Influencing factors; Countermeasures