

计算机网络中的信息安全因素研究

郑明才

江西软件职业技术大学 江西南昌 330041

摘要: 随着时间的推移,科技水平不断提高,互联网信息时代飞速发展,网络信息资源日趋丰富多彩。人们可以在线查看所需的所有信息,并且可以在线购买所需的一切,足不出户即可赚钱、学习和交流。互联网已经成为人们生活中不可或缺的一部分,人们的生活水平得到了提高。然而,在线操作系统包含的信息量巨大,复杂性高,具有一定的开放性和创新性。因此,在线信息也存在安全风险,作者对影响计算机网络信息安全的因素进行了调查,并提出了预防措施。

关键词: 计算机网络; 信息安全; 因素

Research on information security factors in Computer Network

Mingcai Zheng

Jiangxi University of Software Technology, Nanchang 330041, China

Abstract: With the passage of time,the level of science and technology continues to improve,the Rapid development of the Internet information age, network information resources increasingly rich and colorful.People can see all the information they need and buy everything online, earning, learning and communicating without leaving their homes.The Internet has become an indispensable part of people's life and people's living standard has been improved.However,online operating system contains a large amount of information,strong complexity,has a certain degree of openness and innovation.Therefore,there are security risks in online information. The author investigates the factors affecting the security of computer network information and puts forward some preventive measures.

Keywords: Computer network; Information security; factors

虽然计算机网络的安全运行为社会公众带来了极大便利,但隐藏的风险也带来了一些影响。鉴于现代网络的常见安全问题,可以借助计算机网络技术来解决。而且,在宏观角度方面,可以根据计算机的实际行为,综合考虑各种安全风险,综合应对。控制计划可以做到这一点,从不同角度加强对计算机网络安全管控,灵活运用网络安全防护技术,降低安全风险,为计算机网络安装安全可靠的操作系统。

一、计算机网络信息安全的覆盖范围

信息安全的范围主要包括信息的传输、信息的存储和信息的在线分析,而互联网上的信息安全还包括对用户身份信息的识别和授权。目前,在网络信息系统安全过程中,我们主要遵循以下步骤:(1)根据计算机系统、数据库、邮件电子和计算机系统应用程序的安全

功能,禁止用户访问权限。(2)下载合适的桌面杀毒软件到本地网络。(3)在企业内网与Internet的接口上安装合适的防火墙。(4)在广域网中采用较少位数加密传输关键业务信息。采用上述网络信息安全措施,可以暂时保证计算机网络的运行安全,但保证计算机网络信息系统的安全对于海量数据的研究尤为重要。这远远不能满足要求和标准,我国计算机网络系统的安全性还比较薄弱,广大技术人员应积极采取有效措施,继续加强网络计算机信息安全建设。

二、影响计算机网络信息安全的主要因素分析

1. 安全评估体系较为薄弱

目前,我国主要将黑客防范系统视为分析计算机网络信息安全的系统,评估计算机网络安全存在的问题,从而确定安全因素的高低。但是,这类安全扫描系统相

对简单,可能无法满足计算机网络的基本信息安全要求。另外,我国现有的芯片、数据库保护工具、网关软件保护工具和操作系统保护技术,大部分都是从国外引进的。话说回来,这意味着我国计算机网络信息安全的技术水平相对较低,无法真正满足广大计算机用户的网络信息安全需求^[1]。

2. 计算机病毒的攻击

换句话说,计算机病毒是计算机程序代码和一组指令,这些指令或代码被注入或编译成程序,可以干扰计算机的运行和数据,影响计算机的正常使用。互联网黑客通常寻求从特定计算机上破坏或窃取机密信息,并使用计算机病毒攻击目标计算机。病毒本身具有强大的检测、隐藏、发射、寄生等功能,对计算机网络的信息安全构成极大威胁。抵御计算机病毒,防止病毒对计算机程序和数据的攻击,减少数据和软件的丢失和被盜问题,及时采取预防措施,确保和防止网络系统的正常运行。

3. 计算机系统漏洞造成网络安全问题

计算机网络系统由硬件和软件组成。虽然硬件是软件安装的职业,并且本身就是计算机的组成部分,但软件是使用硬件介质安装在计算机上的,并且可以根据需要进行修改和删除,该软件是压缩的计算机语言代码,通常只有在下载到您的计算机时才可用。然而,在网络化系统中很容易出现逻辑性偏差。在这个阶段,一些恶意软件利用这种情况来攻击网络系统中的薄弱,并利用这些错误来攻击计算机。现实生活中有很多这样的例子,例如下载的软件中绑定的恶意软件,就能通过计算机的漏洞入侵,一些人为设定的木马程序通过路由器等设施入侵计算机等,这些都是计算机漏洞带来的网络安全问题。

连接多台计算机可以创建一个小型局域网。该局域网对维护和管理几乎没有风险和不便。例如,一些公司的内部局域网是通过与其他网络的连接和共享建立的,网络的状态存在安全风险。特别是,广泛的资源共享和便携式设备的频繁使用会威胁到其他计算机的网络安全。

但是,与我国目前的情况相比,关于互联网信息安全的相关有效法律法规并没有描述,没有特定的绑定到特定的用户或网络运营商等,因此他们可以在网络上为所欲为,甚至一些黑客攻击计算机窃取机密信息。在没有明确的法律和广泛的网络、复杂的环境和一定的结构的情况下,一些网络犯罪分子不会停止,网络信息安全受到严重威胁^[2]。

4. 网络黑客的攻击

近年来,黑客的攻击方式变化多端,成为对计算机网络安全的最严重威胁。通常,黑客利用计算机病毒攻击个人、公司甚至国家的私人网络空间,以窃取和了解机密信息。随着计算机病毒的快速发展,黑客手段越来越隐蔽,影响用户计算机的正常使用,给国家和个人造成巨大的经济损失。

5. 网络协议的威胁

TCP/IP协议是目前使用最广泛的协议。但是,该协议有几个安全漏洞,为黑客提供了机会。黑客使用缓存窃取用户的敏感信息或向系统资源发送恶意请求。过多的服务器资源使用户难以访问计算机的网络资源,网络变得不可用。攻击网络协议的方法比较隐蔽,不易于察觉,会给计算机用户带来很多麻烦。

6. 用户安全意识有待提升

用户安全措施不足是影响网络信息安全的最重要因素之一。大多数用户没有完全意识到信息安全问题,并且误解了防火墙和防病毒软件等保护措施的存在。这会影响计算机的正常运行,因此不能忽视防火墙设置和防病毒软件的安装。同时,用户在公共场所使用电脑后,经常会忘记清理密码,抹去个人数据,导致机密数据外泄。一般来说,主要原因是用户对信息安全威胁缺乏应有的认识,缺乏正确的计算机使用习惯,导致用户的安全意识低下。

三、加强计算机网络信息安全的防护措施

1. 加强网络立法,健全信息安全法规体系

在运行计算机网络时,一个合适的信息安全系统是最重要的条件,也是保证安全发展的重要因素。因此,有关部门要坚决加强网络安全体系建设,建立有效的信息安全体系。通过这种方式,才能够保证在网络中有法可依、在网络使用中有法必依、在进行督查时执法必严、发现不法分子能够违法必究。为网络安全的发展做出贡献。迄今为止,我国已经制定了各种法律法规来保护互联网的实际使用。它根据互联网和网络安全的实际需要,提供有效的安全保障,保障计算机网络的发展,为计算机网络的安全提供了法律依据^[3]。

2. 加强对不良病毒网站的控制力度

计算机网络中应用程序的技术安全应主要防止恶意网站的恶意入侵。网络攻击是造成计算机损坏和信息丢失的主要原因。解决恶意计算机站点的攻击问题是提高计算机网络应用安全的有效保障。除了改善计算机防火墙设置和系统维护,减少计算机网络用户浏览恶意网站的数量,也是保障计算机用户信息安全的重要途径。此

外, 通过加强对恶意病毒网站的管控, 可以有效防止恶意网页浏览引起的强大病毒攻击感染您的计算机, 能够防止用户信息财产的损失, 也有助于计算机网络数据的安全和有序传达, 进一步高效的便利人们的生活与工作。

3. 注重操作系统与软件的及时更新

选择计算机操作系统和软件, 用户需要选择真实的操作系统和软件, 及时更新系统漏洞和安全设置, 开放和保护网络信息安全。同时, 企业需要将认证技术集成到自己的网络系统中, 对用户进行一致的认证和管理。此外, 要求运营商和管理员通过输入适当的密码并按照其权限合法运行这些应用程序来防止未经授权的用户访问在线资源和数据。

4. 加强防火墙技术的应用

防火墙保障计算机网络信息安全的第一道障碍直接影响计算机网络的实际运行。在某种程度上, 防火墙可以看作是计算机的保护壳。安装防火墙可以通过可以有效隔绝其他用户进入计算机网络系统, 并对内部人员的网络访问权限进行约束, 从而大大降低计算机网络被侵袭的概率。更重要的是, 根据防火墙技术的监控能力, 可以通过日志的形式跟踪和监控您的网络使用习惯。当检测到可疑用户行为时, 及时发出相应的警告信号, 进行有效监控。但是, 我国现有的计算机防火墙的安全级别还比较低, 还不能完全满足网络安全的要求。为此, 我国计算机安全管理部门正在积极开发新型防火墙技术, 有效提高计算机网络安全系统的安全性, 确保计算机网络运行环境健康安全, 真正为广大用户营造一个健康安全的计算机网络运行环境^[4]。

5. 运用杀毒软件保护用户的信息隐私

计算机网络技术使用安全的一个重要方面是保护用户信息的机密性。生活中最常见的认证方式是短信认证和密码认证, 这种认证方式是基于通信双方的相互识别, 通过密码和短信验证身份, 身份验证是最有效的在线安全形式之一。它可以让人们更安全地浏览网页, 是对个人身份的一种象征。

网络用户应注意计算机网络安全的应用。市场上有许多类型的防病毒程序。安装防病毒软件是任何用户最重要的步骤之一。防病毒软件是保护用户和维护计算机网络的一种手段, 而这些防病毒程序主要是为了保护用户和重要文件的隐私。此外, 通过安装防病毒软件, 用户可以监控其计算机的风险并密切监控其计算机网络的安全性。

6. 入侵检测技术应用

入侵检测技术是一种新型的信息安全防范技术。这项技术涵盖了许多技术, 包括人工智能、统计技术和网络通信技术。该技术的使用可能取决于执行统计分析和签名处理的分析方法, 这些分析方法可以确定计算机的运行状态。在这种情况下, 如果计算机被黑客入侵, 它会警告用户尽快断开网络连接或发出信号。从而保护网络信息安全, 保证计算机系统的正常运行。入侵检测技术的应用简单、高科技、方便、不影响计算机网络的运行。

7. 提升用户安全意识, 做好安全性评估

为了减少人为因素对网络信息安全的影响, 需要提高计算机用户的安全意识, 提高对各种网络保护方法的认识。同时, 要加强信息安全用户教育, 使他们能够从概念层面了解网络信息安全的重要性。

它还安装了强大的网络安全操作系统, 实施了强大的监控系统, 并定义了网络管理员的职责。同时, 管理员应对系统进行定期、全面的安全检查。如有必要, 可以使用各种黑客工具来模拟攻击并找到容易被黑客利用的安全漏洞。修复处理, 为网络系统的安全、可靠、稳定提供重要保障^[5]。

8. 管理计算机内部资料

网络的开放性导致网络数据、信息、资料的流失。许多黑客攻击您的计算机以窃取敏感信息或从您的计算机中删除不正确的信息。在这种情况下, 数据将被备份并存储在其他硬件中, 有效防止数据丢失造成的重大损失。备份数据也可用于在丢失或更改时恢复计算机数据。另外, 还可以对数据进行加密处理。一般来说加密的数据就算流失也不会被盗用, 不法分子窃取加密数据没有解密密钥是根本无法解开的。

9. 高效利用虚拟网络专用技术

目前, 现有的特殊虚拟网络技术主要涉及核心技术、身份验证技术、隧道技术、加密技术等。这些技术在开放的互联网平台中发挥着重要作用, 有效防止了网络资源的涌入和信息, 并且大多数用户可以充分利用专用的虚拟网络技术来保护他们的隐私。例如, 开放互联网平台的用户可以通过支持信息加密技术, 充分再现数据加密的功能。这样可以有效保证互联网上内部数据、文件、密码等动态信息的安全, 以减少内部攻击导致的数据丢失。但是, 用户在设计电脑密码时, 应避免使用简单的姓名首字母、生日、电话号码等容易泄露的信息, 而应使用符号和数字来增加密码的复杂性。另一方面, 用户在浏览某些网站时不应单击“记住密码”对话框或使用

“保存密码”功能。当用户单击保存密码时，很可能使计算机密码永久留存在网络中，甚至被不法分子窃取。最后，用户应刻意频繁更改密码，以有效减少泄露原始密码的影响。基于此，用户在使用公共网络时应注意以上问题。只有在概念层面建立足够的互联网信息保护知识，才能降低个人数据泄露的可能性^[6]。

四、结语

随着新时代计算机网络的快速发展和普及，互联网逐渐开始在人们的日常生活中扮演着不可或缺的角色。但是，在实际工作流程中的计算机网络中，仍然存在各种形式的木马病毒，严重危害计算机网络操作系统的安全，事实上，计算机网络通常具有结构松散、开放性强的缺点。如果计算机网络的安全配置薄弱到用户不注意安全管理，病毒或黑客就可以直接导致对计算机网络的

恶意攻击，确保计算机网络安全措施。

参考文献：

- [1]袁姗姗.计算机网络信息安全影响因素及防范措施研究[J].信息记录材料, 2022, 23(01): 86-88.
- [2]孙璐.计算机网络信息安全影响因素及数据加密技术探讨[J].无线互联科技, 2021, 18(20): 104-105.
- [3]成国名.计算机网络信息安全影响因素及防范措施[J].中国科技信息, 2021(18): 59-60.
- [4]陈翔.计算机网络中的信息安全因素分析[J].集成电路应用, 2021, 38(05): 76-77.
- [5]赵泽阳.计算机网络信息安全影响因素及防范措施探讨[J].科学技术创新, 2019(13): 105-106.
- [6]闫晶.浅析计算机网络信息安全影响因素及防范措施[J].电子元器件与信息技术, 2018, 2(02): 4-8.