计算机网络安全与网络技术研究

施亮
赣州职业技术学院信息工程学院，江西 赣州 341000

摘要：在现代信息技术和通信技术迅猛发展的时代背景下，网络平台成为了人们获取数据信息最重要的来源，同时，数据信息的开放性传递也为人们带来了更加便捷的体验。但网络的开放性和灵活性，让数据在自由流通的同时也面对着不可忽视的安全风险问题。各类型的网络安全隐患与数据传输漏洞，更是为人们敲响了网络安全防护的警钟。本篇文章就是探究了影响网络安全的相关因素，并且就计算机网络安全技术和安全防护措施进行了探究，希望能够为社会发展提供更加安全和良性的网络环境提供有效的参考意见。

关键词：网络安全；技术控制；防护措施

Research on Computer Network Security and Network Technology

Shi,Liang

Ganzhou Vocational and Technical College, Department of information engineering, Ganzhou, Jiangxi, 341000, China

Abstract: In the era of rapid development of modern information technology and communication technology, the online platform has become the most important source for people to obtain data information. At the same time, the open transmission of data information has brought a more convenient experience to people. However, the openness and flexibility of the network expose data to security risks that cannot be ignored during free circulation. Various types of network security hidden dangers and data transmission vulnerabilities have sounded the alarm for network security protection. This article explores the relevant factors affecting network security and delves into computer network security technologies and security protection measures, hoping to provide effective reference for creating a safer and healthier network environment for social development.

Keywords: Network security; Technical control; Protective measures

DOI: 10.62639/sspis12.20240103

数据时代依托网络平台作为信息传递的桥梁，现如今的计算机网络已经与人们的日常生产与生活紧密地连接在了一起，越来越多的用户甚至可以足不出户就获取丰富的外来资源，同时，还能够实现信息的高效传递。然而，人们在享受网络构架带来的开放环境时，网络安全问题也面临着前所未有的挑战与考验[1]。由于黑客入侵、网络病毒影响所引发的数据丢失、系统破坏、机密性文件被盗等多方面的问题，更成为了新时期网络安全防护工作应当关注的重要话题。

一、威胁网络安全的相关因素

（一）自然客观因素

自然客观因素对于网络安全所带来的影响，基本是由于设备的使用寿命、软硬件的老化、不同设备之间密度过大引起的电磁辐射、突发性的外界自然灾害、空间场地使用场景恶劣等问题所引发的，在这些自然客观因素的直接影响或间接作用下，都会对网络运行的安全性带来威胁。

（二）病毒入侵

病毒入侵是目前计算机网络系统在运行过程中最主要的安全影响因素。病毒会附着在外来的文件或以其他渠道进入计算机内部的运行程序中，从而对于软件的正常运行或工作发出破坏性的指令代码。不仅如此，绝大多数的计算机病毒还具有繁殖和复制的能力，在通过各类型途径进入运行程序之后，将会持续地扩展和蔓延。以蠕虫病毒为例，该病毒会着重性地针对计算机的操作系统中存在的 Bug 进行攻击，甚至还可以抓住漏洞主动性地对正在运行的程序发出破坏指令。而蠕虫病毒的蔓延速度也是极快的，可通过网线实现快速传递，且在第一时间并不容易被发现，一旦感染蠕虫病毒甚至可能会破坏铜网线连接区域下的所有软件。不仅如此，很多计算机系统的内存中也存在蠕虫病毒，蠕虫病毒的附着还可以与其他病毒之间相互联合，让病毒的爆发以指数性的破坏性增长[2]。目前，世界范围内流行的计算机安全病毒除蠕虫病毒之外，还有人们熟知的意大利香肠病毒和宏病毒，这些病毒对于网络环境带来的破坏不可小觑。

（三）非授权异常登录

非授权异常登录对网络环境带来的威胁事实上是一种典型的人为威胁因素，在并未获取管理员授权认可的前提条件下，很多黑客分子或不法人员将以非法的形式入侵到机密内部网络，属于

（稿件编号：IS-24-3-1008）

作者简介：施亮（1986-01），男，汉，江西赣州人，硕士，赣州职业技术学院高级工程师，主要研究方向为计算机网络技术、网络安全、信息化工程、物联网技术应用。

一种典型的违法犯罪和侵权行为。这些黑客分子往往会通过非法入侵内部网络渠道的方式，窃取企业内部以及相关内网的访问权限，并以此作为桥梁，非法入侵企业的其他内部体系，盗取核心机密数据和数据的存储权，甚至对机要数据进行恶意性的破坏与攻击，导致企业内网陷入瘫痪，无法为企业的正常运转提供正常的服务。

二、网络安全技术的类型与应用

（一）防火墙技术

防火墙技术是最古老也是网络系统安全保障中最为常见的技术之一。尽管近年来，市场上各类型的虚拟网络安全技术层出不穷，但防火墙技术在网络安全保护中的地位仍然不可撼动。防火墙体系也是网络系统中安全构架的一部分，防火墙既可以以软件的形式存在，也可以以硬件设备的形式存在，甚至还可以设置芯片级别的防火墙。防火墙大多处在被保护网络与外网的边界区域，能够有效地审查并控制出入被保护网络的数据流和访问申请。不仅如此，防火墙还可以根据不同网络系统的实际需求，设置与之相匹配的访问防控方式，从而将一些不法入侵或存在威胁的申请过滤掉，也可以通过一些其他的特殊操作方式，抵御屏障风险。目前，防火墙系统在应用的过程中，不仅能够确保为保护网络体系中的资源不受到外部往来引发的资源盗取或侵入现象，甚至还能够主动性地拦截被保护网络向外界传递机要信息。其具体的应用大致可以分为以下三种类型：

第一，软件防火墙系统。软件防火墙通常指令操作于一些特定的计算机系统上，需要用户提前安装好软件操作的支持系统。而安装防火墙的计算机设备也被称为整个网络系统的网关，在个人的 PC 端就被称为个人防火墙。这种软件防火墙就类似于应用软件 APP，通过提前安装或设置才能够使用。但需要操作管理人员对所保护的系统平台较为熟悉，才能让 Checkpoint 防火墙发挥有效的作用价值。第二，硬件防火墙。硬件防火墙主要作用于一些专门性的硬件平台，目前，在市场中绝大多数企业采用的防火墙都是这类型硬件防火墙。硬件防火墙基于 PC 端的构架，但事实上，它与普通家庭所用的 PC 电脑并没有过大的区别。目前，在 PC 端口，经过简化的操作系统之后，最常见的硬件防火墙主要有 Unix、Linux、FreeBSD 系统三种类型。但需要注意的是，这类型硬件防火墙系统会受到电脑本身 OS 操作系统所带来的影响[3]。第三，芯片级防火墙。芯片级防火墙作用于更多的专业硬件平台，它没有复杂的操作系统，而是通过专业的 ASIC 芯片更快地识别风险。芯片级防火墙对于入侵或病毒的处理速度更快，防护的能力也更强。目前，市面上的芯片级防火墙生产厂商主要包括 Fortinet、NetScreen、Cisco 等等。芯片级防火墙需要搭配应用专业的操作系统，防火墙本身相比于软硬件防火墙来说漏洞更少，但应用的成本也相对较高。

（二）数据加密技术

在网络信息传递的过程中，为保障数据信息传输和接收的安全性，加密技术就成为了最为常见的数据保护方式，同时也是一种主观性的信息安全防护方法。加密技术是所有网络安全防护技术最为基础的条件，所谓数据加密，就是通过采用应用代码或设置密码的方式，将一些价值较高的信息与数据从原本容易理解的明文形式过渡到复杂混乱的密文形式，这也就是对数据的加密。这种乱码的传输形式，能够让电子信息和数据在传输以及存储的过程中得到有效地保障，也是抵御信息外露和盗取的第一道屏障，确保了数据信息的基础安全。目前，在网络平台中数据加密的方法种类众多，最为常见的就是加密算法。算法功能可以将信息中最有价值的核心部分进行加密，二，算法加密也逐步经历了古典密码、对称密钥以及公开密钥这三大发展阶段。其中，古典密钥包括了算法主要有替代加密、置换加密两种形式。而对称算法和非对称算法加密的种类更多。其中，非对称算法包含了背包密码、椭圆曲线等类型。目前，世界平台中最广为应用的对称算法就是 DES 加密算法，而非对称的加密算法中，RSA 算法最为常见。随着数据加密技术的持续发展，数据加密正在与芯片技术之间相互融合，通过二者之间的融合应用逐步形成了密码专用芯片以及量子加密技术，实现了对数据信息更高程度的安全防护。

（三）入侵检测技术

入侵监测技术也被称为网络动态实时监控技术。这项技术在网络平台中的应用，主要是通过软硬件系统对流通网络上的数据进行动态性的查验，并且与数据库中的历史入侵数据进行比较，从中挖掘具有攻击倾向或携带攻击倾向的数据流。一旦发现系统存在被攻击的可能，就会以最快的方式快速做出反馈，这种方式大多数都是被用户自定义的动作反应。比如，有些用户定义一旦发现攻击倾向就断开所有内网连接，避免病毒的进一步拓展和蔓延[4]。而另外一些用户则选择发现被攻击迹象时，快速地对防火墙软硬件系统发出通知，从而让防火墙对访问权限和访问方式进行调节，并且快速过滤掉入侵的数据流。由此不难看出，入侵检测技术与防火墙技术是一对绝佳搭档，入侵检测技术可以作为防火墙技术的补充与升级，同时，也能够在系统运行的过程中，在不影响任何操作的前提条件下，对网络环境进行动态化的监控，有效地针对来自内部以及外部的攻击迹象进行防范，是提升网络安全性的一道屏障之一。

（四）网络安全扫描技术

网络安全扫描技术是近年来我国网络安全领域在发展过程中最突出和重要的成果。通过网络安全扫描，网络管理员能够在第一时间快速地掌握网络的安全配置等级以及运行过程中的相关应用服务，在及时排查的情况下，可以随时随地地找到安全运行存在的漏洞，并以客观的角度针对目前的网络风险防范等级进行评估。网络安全扫

描技术主要是针对局域范围内的网络系统、Web网络站点、主机挂靠的操作系统、防火墙系统中存在的漏点和盲点进行补充，属于服务于这些系统的安全防范措施。网络安全扫描技术可通过实时性的检测，快速地排查操作系统中可能存在的被攻击、拒绝服务攻击的安全性漏洞。甚至，他还能够排查操作者的主机系统中存在的一些窃听程序，也是检验防火墙系统漏洞的一道屏障。

三、网络安全发展策略

近年来，随着网络攻击技术的日新月异，原本的普通网络病毒和简单的入侵手段也开始逐步趋于更加多元化的攻击手段，甚至还会通过多种手段相融合的方式向系统发出综合性的攻击。这也意味着，现如今的网络安全平台面临着的挑战与日俱增，推动网络安全技术的发展迫在眉睫。在这样的背景下，网络安全防护工作也应当从过去单一的防护功能向多维度结合的防护功能转变，坚持遵循以防御为主、综合利用防范的发展原则，采用多种信息安全技术相结合的方式，构建起更加全面和多维度的保护屏障，才能更好地确保用户的用网环境。

（一）物理安全策略

所谓物理安全的防护策略主要是针对一些客观性的自然因素采用的，防护工作的主要目的就是有效地避免计算机系统、硬件设备、网络服务器、打印机实体、通信线路链条受到威胁。目前，在日常的办公场所以及服务站中，可能会由于应用场景的恶劣、外部自然灾害带来的影响、人为力学影响、线路空间布局不恰当等因素导致网络安全受到物理威胁。而通过物理类的安全防护策略，首先，能够确保计算机系统具备良好的工作场景。比如，可以通过构建一个电磁兼容的工作环境，避免在网络硬件设备和系统运作的过程中受到电磁辐射所带来的影响[5]。再比如，需要通过定期地清理灰尘、设备所在区域做好通风措施等方式，尽可能让设备处在温湿度环境合理的状况下，延长设备的使用寿命。其次，通过制度的构建，避免主观性的人为伤害。比如，进入机房的操作人员必须通过密钥才能进入机房，这样就能够有效地避免越权操作等行为，也能够防止非法入侵引发的数据盗窃以及数据破坏活动。

（二）政策类保护

目前，我国针对网络安全的政策法规已经基本形成了框架体系，网络安全政策法规框架也被称为“四梁八柱”。其中，以最基础的《网络安全法》作为根本，又延伸出了《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等相关法律法规，同时，针对国家网络基础设施的安全防护、云计算线上服务的安全评估、数据出入境的安全防护控制和网络安全服务也分别出台了一系列的政策法规。希望能够有效提升互联网络的安全防控水平。而这些政策法规面对目前主要存在的黑客攻击、恶意软件病毒、网络钓鱼、DDos攻击、数据泄露、敏感信息的非法获取基本可以实现全覆盖。但针对个别漏网之鱼还需要通过落实国家网络安全保护机制，针对防火墙以及入侵检测的系统进行定期的更新升级和软件补丁，加强用户对于网络安全防护的认知，建立网络安全防护应急响应机制等方式，才能从根源上避免网络病毒的攻击和非法入侵。而作为互联网平台的运营者来说，更应当建立起与数据相关联的平台规则体系，同时，针对用户的隐私数据也应当构建隐私政策和算法策略的披露机制，及时披露制定程序、算法裁决程序，从而确保平台数据信息在存储以及传递过程中的运行规则，保障算法应用的公平公正性。作为个人来说，在日常的生活以及工作中，也应当谨慎地选择相关的应用产品与服务，尤其是要对个人的有效信息做好保护。同时，官方也应当加强对于APP授权的审核，用户也应当针对APP申请的授权内容谨慎处理。针对银行卡、手机账号等相关的重要信息做好加密保护工作，同时在户外，不要随意连接免费的热点，也不要访问非法的陌生网站，更不要随意在公共社交平台上发布关于身份证、户口本、家庭住址以及车票机票和个人影像等相关资料，在尊重他人隐私的同时，也不随意披露个人的隐私信息，加大对于随意披露他人隐私信息的执法力度。

四、结语

综上所述，营造健康与安全的网络环境，是确保我国网络事业长足发展最基础的条件，同时也是保障企业单位、个人用户网络信息系统平稳运行的基石，也是国家信息安全战略落地的关键途径。而针对目前网络安全防护中存在的黑客入侵、非法盗取、病毒携带等各类型的安全问题，更应当敲响网络安全防护的警钟，通过应用多元化数据加密技术、防火墙技术、网络安全扫描技术等构建起全维度的网络安全防护框架，更好地抵御外来风险入侵系统，并及时根据网络安全形态调节安全管理政策，推动我国网络安全工程的建设步入新的发展里程碑。

参考文献：

[1] 唐浩．云计算技术在计算机网络安全存储中的运用分析[J]．网络安全技术与应用，2023，(11)：76-78.
[2] 张伟．计算机网络安全技术发展趋势思考——评《计算机网络管理与安全技术研究》[J]．安全与环境学报，2024，24（09）：3705.
[3] 宋阳，果福明．计算机网络中数据加密技术应用[J]．集成电路应用，2023，40（11）：100-101.
[4] 胡仕川．新工科背景下计算机网络安全课程教学发展路径[J]．网络安全技术与应用，2023，(11)：93-95.
[5] 郝博麟．物联网在提升网络安全技术中的应用分析[J]．网络安全技术与应用，2023，(11)：6-7.