计算机网络安全技术在网络安全维护中的运用研究

师 伟*
云南电信公众信息产业有限公司，云南 650001

摘 要：时代在不断发展，互联网技术也从未停下革新的脚步，与此同时，互联网技术凭借着自身强大的优势与特点，被广泛应用于各行各业当中，为人们的生活、生产、工作、学习等各方面提供了极大的便捷，并且为人们展示了一种全新的交流方式与平台。但是，计算机在使用的过程中，也会存在安全问题，必须对出现的问题进行科学处理，确保网络系统在稳定、安全的状态下运行。主要对计算机网络安全技术在网络安全维护中的运用进行分析，研究计算机网络安全技术在网络安全维护过程中存在的问题，并提出与之相对应的解决方法与策略。

关键词：计算机网络安全技术；网络安全维护；计算机技术

一、引言

在信息技术及计算机网络技术迅猛发展的背景下，人们对网络安全技术的重视程度不断提升。对此，必须要强化网络安全技术的应用，并加强网络技术设备的维护，依靠专业的计算机网络技术开展网络安全维护，减少系统漏洞、病毒入侵等问题，以此保障计算机网络应用的安全性，保障人们的隐私安全。

二、影响计算机网络安全的重要因素

（一）计算机系统漏洞

对于计算机来说，网络把所有的计算机串联起来，而在这个计算机的网络上，计算机中完整的软件系统和硬件系统便是计算机在网络上的“保护伞”，避免计算机被轻易入侵。对于世界上的计算机系统一般使用的是微软的Windows系列系统和苹果的MacOS系统。这两种系统有着较为丰富的保护经验，且在十几年的发展中，系统的漏洞不断被修补、完善，对于使用者来说都是较为可信的电脑操作系统。但对于网络的来说，未知的网络领域很多，性能出色的计算机可以探索更多的网络范围和领域，同时这些网络的领域的安全性便会更差，拥有更多的漏洞可供黑客进行攻击。黑客对于计算机的入侵便是通过管理员身份对计算机的数据进行篡改和盗取。网络世界错综复杂，各种系统也不能保证绝对的安全，而系统中存在的问题便是漏洞，从而威胁到计算机的安全[1]。

（二）黑客攻击

当前网络信息技术不断普及，黑客技术水平不断提升，黑客攻击会针对计算机系统中的漏洞及网络产生攻击作用，黑客会借助漏洞复制、损坏或者倒卖大量的商户信息，直接导致企业网络平台遭受信誉损失，泄露大量数据信息，影响计算机网络的安全运行。尤其以互联网经济相匹配的网络平台信息泄露情况最为严重，直接会导致企业经济效益损失情况发生，对企业的经营产生不利影响。黑客在进行网络攻击的过程中，会直接对用户信息终端产生攻击，并盗用信息数据，依据信息数据分析结果，选择攻击内容，使得企业遭受巨大的经济损失。黑客对计算机系统攻击的主要形式包括木马病毒安装、病毒植入等方式，也有黑客会依靠交流软件和信息传递等形式对用户的重要信息进行盗用，以此谋取巨大的经济效益。

（三）非法恶意攻击行为

随着信息化时代的到来，电脑黑客的攻击行为和攻击手段也呈现出多样化的趋势，对用户的计算机系统造成了极大的破坏。黑客通常借助计算机系统中存在的漏洞和问题进行攻击，这种非法恶意攻击行为不同于单纯的病毒攻击，它的目的性和专业性更强，对计算机系统造成的破坏程度更大，所以成为构成计算机系统安全威胁的重要因素。黑客常见的非法恶意入侵攻击手段有漏洞入侵、木马入侵等。近年来，计算机用户为了防止黑客利用漏洞对计算机系统造成破坏，所以不少用户给自己的Win2000或是XP系统安装简单易学的IIS，搭建一个不定时开放的ftp或者web站点，从

* **通讯作者：**师伟，1983 年 1 月，男，汉族，云南昆明人，现任云南电信公众信息产业有限公司技术部副经理，高级工程师，大学本科。研究方向：信息安全理论及技术、网络安全、项目管理。

而提高计算机系统的安全性，但是IIS并没有像用户所期待的那样，能够完全阻挡黑客的漏洞入侵，比如黑客利用IIS的WebDAV漏洞进行攻击，给计算机用户信息造成了威胁。

三、计算机网络技术在网络安全维护中的应用

（一）树立正确、科学的网络安全维护意识

树立正确、科学的网络安全维护意识是计算机网络安全应用在网络安全维护过程中的重点与要点，同时也可以说是前提。首先，需要相关部门加大网络安全维护宣传的力度，让每一位用户都能够真正认识到网络安全维护的重要性和意义。其次，各单位与企业中的相关工作人员需要第一时间对于企业员工在运用计算机网络过程中所出现的错误操作进行制止与指导，并定时、定期、有计划地展开计算机安全技术培训课程，让企业中的每一位工作人员都能够具备安全网络维护意识，促进企业网络稳定、安全地运行。

（二）招聘与引进网络安全技术复合型人才

任何工作都离不开人才的帮助与支持，将计算机网络安全技术应用到网络安全维护过程当中，更是需要人才所给予的极大帮助。

首先，相关部门需要加大引进网络安全技术复合型人才的力度，还要不断地对相关的技术进行优化与革新，解决网络安全维护过程中所出现的技术难题。其次，各企业与部门需要制定出健全、完善的人才引进方法与策略，例如，增加薪酬激励方案和福利待遇等，以这样的方法来吸引更多的计算机网络人才加入到自身的企业和部门当中，促进企业网络安全维护质量得到进一步提升。最后，社会要将自己的作用全部发挥出来，运用多形式、多样化的方法让更多的人参与到培训当中来，为网络安全维护提供源源不断的计算机网络安全技术人才。

（三）防火墙技术的应用

防火墙技术自发明以来就受到了计算机用户的喜爱，防火墙技术的应用可以使计算机系统快速识别计算机下载软件和文件中可能携带的病毒，并将其阻挡在计算机系统之外，这样不仅提升了计算机信息的安全性，而且推动了网络安全事业发展。防火墙技术主要是有两种形式对计算机系统进行保护，首先应用级防火墙，它的主要特点是增强输入验证，比如在电脑系统中安装了应用级防火墙，它能够有效地避免网页被黑客篡改，也能够防止木马病毒的入侵，而且它可以对计算机终端服务器内部的处理内容进行实时的检测和扫描，一旦发现电脑系统中出现安全隐患，它会立即断开代理服务器和内容服务器之间的传输渠道，防止不良的病毒和系统攻击电脑系统。其次是包过滤防火墙，包过滤防火墙的工作原理是利用一台路由器或一台主机，根据过滤的规则决定对数据包的取舍，普通的路由器只检查数据包的目标地址，但是过滤路由器处除了决定是否有到达目标地址的路径以外，还会仔细检查数据包，并决定是否发送数据包[2]。

（四）身份认证技术

用户访问数据库时得到相应的限制是利用计算机网络访问数据库的用户身份认证技术，这项技术有利于提高数据库的安全性。访问控制分为强制访问控制和自主访问控制。在强制访问的控制下，用户访问自主性较低，在大多数情况下，系统会限制用户的访问，一般不能访问数据库。而自主访问限制性较低，用户不仅可以自由进入数据库进行访问，还可以将访问权限授予他人。为保证数据库安全的情况，计算机最好设置强制访问控制来控制用户对数据库的访问，这样只有有权限的用户才能进行访问，对数据库的保护起到更好的作用。

（五）入侵检测技术

在计算机网络系统中应用入侵监测技术，可对计算机系统中的入侵行为进行分析。一旦发现计算机系统被入侵，就及时发出报警，对不安全因素的入侵行为进行有效地控制。依靠入侵检测技术，可最大限度对计算机系统中的数据信息进行检验，实现计算机网络安全防护，保障计算机网络顺利应用。入侵检测技术主要由历史审计信息和主机系统两部分组成，其检测质量较高，具有较高的可行性，可全方位对计算机网络系统中的漏洞信息进行检测。依靠入侵检测技术可以有效实现计算机异常检测和误用检测。在开展误用检测的过程中，入侵检测技术可对入侵行为进行有效的检测，检验效率高，极小概率会产生错误判断。但是，这一形式的检验工作所消耗的时间较长，工作量较大。另外，入侵检测技术还可对计算机网络中的异常应用情况及用户开展有效监测，可对计算机整个体系进行规范化扫描，其所消耗的时间比较长。在开展入侵监测的过程中，必须合理应用入侵检测技术，提高计算机网络维护应用的效率。

四、结束语

为了保证计算机网络用户数据安全、保密的需求，可以合理地应用上文中提出的数据加密、防火墙、攻击检测等网络数据库安全管理技术，同时要充分认识各种安全管理技术的应用能力和实用性，为我国营造安全的计算机网络环境提供强有力的技术保障。

参考文献：

[1]崔娟.网络维护中计算机网络安全技术的应用探讨[J].电脑编程技巧与维护,2021(4):164-166.

[2]舒豫,杨林.入侵检测技术在计算机网络安全维护中的应用[J].电子技术与软件工程,2021(8):251-252.