ISSN:2705-0963（Print）　ISSN:2705-0955（Online）
Pisco Med Publishing

浅析计算机网络安全技术的防范措施

付冬波

广东东软学院

摘　要：在当前社会发展中，人们的生活生产都需要计算机网络技术的帮助，各类活动都需要在网络的基础上来开展。所以，做好计算机网络安全技术应用工作，积极地制订相应管理方案，这对于社会的发展有着非常重要的作用。因此，学生应该要加强自身学习，积极地将自己培养成优秀的计算机网络安全人才，这样才能够制定更加完善的网络安全系统，有效地提高防火墙的性能，最大程度上保证用户使用网络的安全性。对此，本文通过分析计算机网络安全技术的内涵，并探究了影响其安全技术发展的因素，最后再针对其中的问题提出了一些改进策略，希望能够为计算机网络安全技术发展提高一定的理论或实践依据。

关键词：计算机；网络安全技术；防范措施

信息化时代下，人们的交流方法与以往有很大的不同，通过网络交流能够更好地提高效率，也为我国发展提供帮助。但是，在运用计算机网络技术的过程中，也存在着一定的安全问题，这些安全问题会泄漏用户隐私，容易给用户造成经济损失。因此，我们应该要采取一定的措施提高用户的安全防范意识，在日常生活中不浏览风险网页，并定期对计算机进行杀毒，规范自身的上网行为，这样才能够减少网络安全问题的出现，保障自身的信息安全。

一、计算机网络安全技术的内涵

计算机网络安全技术就是在计算机技术的帮助下，来保护计算机网络系统中的信息，避免其受到外部影响，更好地提高计算机网络系统安全水平。计算机网络安全技术能够为人们提供可靠的保护，还能够保障信息的有效传输，能够更好地提高信息共享效率，真正地为网络使用营造一个安全的环境。

二、影响计算机网络安全技术发展的因素

（一）用户意识淡薄

在网络时代发展过程中人们的生活和工作都需要网络为其提供帮助，但是在使用上却没有重视对网络信息安全的关注，缺少相应的安全防范意识。而且，人们更多的是重视网络效应，没有重视网络信息安全，在管理上缺少资金投入，这样就直接影响计算机网络安全技术水平。具体分析，人们对网络安全问题没有关注，缺少积极主动，经常是在出现问题后，才想起采取相应办法来解决，这样就无法从根本上有效地提高网络安全技术，也无法提升人们的网络安全意识。

（二）计算机网络病毒因素

随着计算机网络技术水平的不断提升，病毒技术也在不断提升，这样就直接使得计算机网络安全受到影响。想要更好地解决计算机网络病毒问题，那么就应该积极更新，营造一个良好、安全的环境，让计算机网络能够正常运行。而且，相关部门也应该加以重视，要能够针对具体的网络安全问题来采取相应措施，保障计算机网络的安全和稳定。

（三）人为因素对网络安全造成的问题

在网络信息安全管理中，人为因素是网络安全的主要因素之一，用户的安全防护意识不强，是网络安全面临的主要因素。在网络信息时，没有安全防火墙系统或者杀毒软件，对网络病毒信息进行检测，通过对网络中的信息与病毒库中的信息进行对比分析，然后对异常信息进行主动拦截与杀毒，达到对计算机进行保护的目的。由于网络系统的安全管理工作人员，缺乏必要的技术措施，网络操作能力不足，不能有效地设置网络防火墙、网络数据的管理，对网络数据的密码设置过于简单，或者故意泄露网络信息数据，都会给网络信息数据的安全带来隐患。

三、计算机网络安全技术的防范措施

（一）运用防火墙技术

在构建网络安全系统的过程中，需要用到防火墙，通过对防火墙的利用，来有效地阻隔不良信息，避免计算机中毒。所以，在完善网络安全系统地过程中，就应该积极地利用防火墙技术，要能够将其和计算机系统有效结合，以此来提高防火墙的安全性能。在防火墙的组成中，网络级和应用级网关是中非常重要的内容，通过对应用级网关的有效应用，能够及时检查计算机传输和接收数据的安全性，并且能在网关的帮助下实施备份，通过这一技术更好地保证服务器与客户的有效联系。

（二）运用虚拟网络技术

计算机网络技术发展日新月异，技术更新非常快，不论是硬件或者软件，相对应的产生大量的资金费用，因此，在信息网络技术的应用过程中，需要结合相关的技术要求以及性能来选择相应的设备，采取合理化的举措来减少资金的浪费，减少技术更新对应用产生的影响。在信息网络技术的设计中，要考虑相关的影响因素，保障后续的维修工作顺利开展。基于此，虚拟网络技术的应用应该按照标准来执行，不能对计算机的性能产生影响，始终将服务这一原则放在首要位置。

因此技术人员应对网络信息中的各个环节进行把控，保

ISSN:2705-0963（Print） ISSN:2705-0955（Online）

障技术的安全应用，制定完善的操作流程。其网络体系分别做以下介绍：

首先：虚拟专用网络技术的主要部分是隧道技术，在运行中有很大作用，主要的运行方式是将分散的数据信息重新整合成压缩包或数据包的形式，数据传输市场采用的是数据包或压缩包的形态，将数据打包处理能有效地避免数据丢失，保障数据传输的完整性和可靠性。再次打包整理数据是很关键的，是隧道技术的重要步骤，在当前，在接收与传送邮件的时候都采用的是隧道技术。

其次：加密技术，加密技术在虚拟专用网络的运行中起着重中之重的作用，这一技术是保护网络信息数据传输的关键数据，通过将数据进行乱码编排处理再进行传输，乱码的数据要想变成有用的数据，需要理解密钥知识，网络数据没有使用密钥技术，企业的数据网络很容易土崩瓦解，重要数据会遭到流失或者复制，尤其是网络黑客破坏企业网络数据，影响计算机网络的安全。目前网络犯罪越来越多，由于网络监管的难度比较大，法律上对有些犯罪没有明确的判定，使不法分子游走在法律的边缘，为了保证计算机网络的安全，因此数据加密技术是企业或个人必须要掌握的虚拟专用网络安全技术。

再次：身份认证，身份认证技术在虚拟专用网络技术的应用中主要表现为各个软件 App 注册都要进行实名信息认证，在认证个人信息的过程中要填报本人的各类信息，以及短信验证码，图标数字验证码，只有输入匹配的验证码信息，才能顺利完成注册。在计算机网络信息发展形势下，身份认证这一技术运用的范围越来越广，在维修信息安全的基础上能有效地避免人们的经济损失，身份认证这一技术的运用能极大地方便人们的生活，主要是对查阅资料信息的授权，避免不法分子对个人信息的冒用，有效守护企业信息技术的安全。

最后：ISAKMP 与 SKIP 技术，是主要的管理技术，是使用在密钥上的管理技术。SKIP 技术为不公开的密钥传播技术，ISAKMP 技术为公开的密钥传播技术。在 ISAKMP 技术应用中，所有用户都能通过一定渠道获得密钥，SKIP 技术则无法达到这一操作，所以在实际运用中使用哪一种技术需要对实际情况进行判定，那么网络安全可以使用密钥技术来进行保证，能在发挥密钥技术的安全管理的功能的同时降低在使用的时候会有安全漏洞。

（三）有效使用杀毒软件

在构建网络安全防御中，要与用户的实际体验进行联系。所以，相关单位应该合理地开展网络安全防御工作，不断地提高计算机网络对病毒的防御能力。相关单位要能够积极落实当前的网络安全防御工作，并且从实际情况出发，企业、个人和单位都应该积极对计算机软件进行杀毒，排查病毒，与此同时还应该做好软件的日常更新工作，这样能够及时地修补软件漏洞，更好地提高软件的性能，提高软件的工作效率。此外，相关单位还应该针对具体的计算机网络安全系统来制定应用方法，通过杀毒软件来更好地保护计算机的核心数据，积极地做好备份工作。

（四）其他技术的运用

利用可信访问控制来提高计算机网络的安全性，也是当前计算机网络技术安全常见的问题之一，采用该技术主要是控制非授权用户与非法用户访问资源的权限，限制非法用户对合法数据访问的权限，在一定程度上限制了非法用户访问不同网络的全面，也保证用户的数据不会被窃取，同时还要防止合法用户在未授权的情况下，登录系统访问云平台中其他用户的数据。利用访问控制技术设置用户登录平台的权限，在用户登录系统时，可以自动地记录用户的行为，便于生成平台管理日常，从而能有效地对用户访问日志进行审计，方便管理员对整个计算机网络平台体系进行管理。

四、结语

总之，计算机网络技术的应用，为数据利用提供了便利，还要针对网络安全的问题，采用合理的策略，做好网络安全防护，共同应对网络安全，减少网络中的数据不安全问题，定期对电脑系统进行查毒、杀毒，并设置防火墙、安全防护措施等，还要提高个人信息的安全，养成良好的网络安全保护意识，才能有效的保证网络安全。

参考文献：

［1］王世伟 . 论大数据时代信息安全的新特点与新要求［J］. 图书情报工作，2020（6）：5-14.

［2］邓震林 . “大数据”时代的计算机信息处理技术［J］. 通讯世界，2020（7）：35-36.

［3］黄若莲 . 计算机网络安全技术的影响因素与防范措施分析［J］. 中国新通信，2020，22（5）：124.