网络安全维护的计算机网络安全技术运用思考

郑志超
山东港口科技集团烟台有限公司　山东　烟台　264000

[摘　要]近年来，国家计算机信息技术不断的发展和进步，使得计算机已逐渐进入人们的生活中，并且成为生活中重要组成部分之一。虽然计算机可以为人们的生活以及社会中的企业带来很多便利的因素，但在使用的过程中仍存在一定的安全隐患。科学地使用网络安全技术能够降低网络攻击造成的负面影响。为了有效确保网络安全、提升网络环境的安全性需要有效维护网络的安全运行，避免信息文件泄漏的现象发生，应不断提升信息存储和传递的质量。鉴于此，文章以计算机网络安全技术在网络展开论述，并提出以下几点作为参考。

[关键词]计算机；网络；安全技术；运用
【DOI】10.12252/j.issn.2096-627X.2021.11.338

引言

经济飞速发展，科学技术日新月异，网络技术也取得长足发展，计算机的到来给企业和人们的生活带来很多优势，一方面能够提高企业的工作效率以及质量，另一方面能够为人们的生活提供很多便利的条件。随着计算机不断的应用，同时也出现大量的网络安全隐患，这些隐患会危及到企业和人们的财产，带来一定的影响。如，一些不法分子在网络中使用一些手段盗取企业重要文件或信息等满足自身利益。因此，当下最重要的问题是加强网络安全的监控，通过有效的网络安全技术降低安全隐患，保障企业网络安全。

1.计算机网络安全及其在网络安全维护中的重要性

1.1 计算机网络安全概述

网络安全技术主要在以下方面实现其独特优势，如：可控性，完整性，机密性，可用性和可检查性，有效确保数据传输及数据共享过程的安全。计算机在网络中的所有信息的浏览、存储、运输等，作为计算机用户特定的行为，具有一定的隐私性。当信息被存储在计算机内，或利用计算机存储到网络中，得以实现其完整性，需要确保计算机网络存储的信息和内容不被篡改，计算机网络自身具有一定保护性。当信息内容要被修改时，只能有指定的用户进行完成。为了能够有效防范计算机内部系统遭到病毒的袭击和破坏，需要专业技术工作人员重视计算机网络安全性，通过专业的维护与检修，进一步提高系统安全性，保障能够抵御任何的病毒与风险，使得企业运用计算机网络得以安稳放心。

1.2 重要性

互联网技术逐渐深入社会的各行业中，人们的生活和工作更离不开网络，但在实际生活中，网络也存在一定的风险，如：不法分子借用网络手段实施诈骗等行为，严重制约着民众的财产安全。不少企业采用信息系统共享技术或搭建自己的系统，在这种情况下一旦出现病毒入侵或黑客入侵，企业的信息资料会被盗取，使得自身利益受到损失。因此构建安全、健康的网络具有重要的现实意义。

2.计算机网络安全中存在的问题概述

2.1黑客攻击

虽然计算机的到来给国家带来很大程度的发展，但是计算机自身存在一定的开放性特点，人们能够通过计算机获取自己想要的信息。一般来说，每台电脑都可以受到一些网络技术人员的攻击，攻击源头难以在短时间内确定。而网络中的“黑客”更合适电脑技术人员的顶端，这些人员使用网络技术会对任意一台电脑形成严重的攻击，并从中获取想要的信息以及文件等，使得企业受到严重的经济损失。根据对黑客攻击的了解得知，黑客能够对储存或者传输中的信息实行全面的拦截，同时也会对电脑中内部的文件形成获取，甚至更严重就会导致所有电脑都出现死机的状态，无法继续使用。

2.2系统内部的漏洞

计算机自身的系统是需要不断的升级实现理想的状态，主要是因为计算机自身存在一定漏洞，在研发过程中必须对计算机实行定期的升级，将其中的漏洞全部修复。而且计算机自身内部的漏洞会给不法人员提供有效的途径对其中的文件及信息实行破坏。这些不法人员可以通过计算机自身存在的漏洞进入到网络的内部中心，导致网络系统出现瘫痪。因此，要想保证计算机的安全性，就需要不断的提高安全防护，从根源上加强安全措施，使计算机减少被攻击的概率。

2.3病毒和木马的问题

传播病毒的方法有很多，其中有些人员是通过发送邮件传播病毒。如果人们在使用的过程中下载邮件中的信息，那么直接会对电脑带来木马病毒，使得电脑的系统被破坏。同时还有一些网站当中指导木马病毒，只要下载这些病毒就会立刻进入电脑系统内部进行严重的攻击。这种情况一旦出现，不仅会给人们的财产带来一定的程度损失，还会降低电脑的安全性，使电脑易受到大量病毒的攻击。有些病毒是无法在短时间内发现，会逐渐侵蚀电脑中的重要信息，带来重大的损失。

3.计算机网络安全技术在网络安全维护的运用

3.1加密技术的应用，增强安全性能

由于计算机网络自身存在开放性的特点，相关人员在实行计算机网络安全维护的工作中应该使用加密技术提高计算

机自身的安全性。加密技术的使用将重要的信息全部转换成密文的形式来进行传递，而对方在接受到信息后再运用同样的方法将文件全部还原。同时合理的使用加密技术加强网络自身的安全性能，有效防止不法人员对信息的盗取以及破坏等，还可以预防非本机用户的窃听行为，使信息得到良好的保护。如：在某一企业当中，技术人员在工作中需要将外部网络和局域网络实行分开处理的方式，将企业重要的文件使用局域网络完成传输，对部分软件实施加密技术来加固安全性，使重要文件在传输的过程中始终保持安全，进而将文件顺利传输到接收人员的电脑中。

3.2IDS技术的应用

IDS 技术的有效应用可以对网络中是否存在安全隐患以及恶意文件等实行有效的检测，一旦检测出其中存在问题，可通过有效的技术来处理。其中还包括企业内部人员在工作中非法使用信息以及外部入侵等行为的发生。因此，技术人员在工作中通过使用IDS 技术能够有效地加强网络自身的安全性，使计算机可以始终处于正常的运行状态，从而给使用人员提供良好的环境来确保信息不会受到任何的攻击和破坏。

一般在使用的过程中主要通过以下方面完成操作。需要对使用用户进行操作活动以及系统运行来检测，在检测环节中对用户的操作信息实行全面的跟踪，并做出正确的判断，查看用户是否存在不法行为；对已经发生的不正规操作实施全面的监控，并及时汇报给相关技术人员来进行有效的补救，降低相关人员与企业的损失；技术人员在工作中要对网络中存在的异常现象实行详细的分析，通过有效的方法顺利解决。

3.3防火墙技术的使用

防火墙技术是技术人员在工作中经常使用的一种方法，针对用户在访问计算机过程中执行严格的安全控制，将一些会给计算机内部带来影响的文件以及信息等全部阻隔在外，从根源上提高计算机自身的安全性，有效防止计算机被病毒所攻击。而且操作非常简便，防火墙自身的技术在计算机使用期间会默认开启，为计算机加强安全保障。如：为了防止病毒传播，防火墙会及时扫描在使用计算机查找病毒和特洛伊木马时传输的信息和数据，有效地识别网络黑客的恶意攻击和异常的网络操作问题，识别隐藏的网络安全风险，立即保护计算机网络安全。

3.4使用杀毒软件和漏洞扫描

计算机内部是否存在病毒，可以通过查毒软件来进行全面的查询，然后加强计算机自身的安全性。随着科技不断的发展，现在已经研发出很多杀毒软件来使用，所以用户在使用电脑期间一定要安装杀毒软件来减少病毒的侵袭，来保护用户在使用户过程中的安全。同时，大部分的杀毒软件都可以对计算机系统中的漏洞进行检测和修复，就可以有效的保障计算机使用期间的安全。如：在计算机网络操作系统中处理病毒，需要安装计算机防病毒软件，并使用防病毒软件从计算机网络操作系统中删除病毒。随着科学技术的进步，病毒将继续更新和发展，因此防病毒软件必须不断更新并保持最新状态，以维护网络安全。

如果一些企业自身对网络安全的要求较高，那么可以聘请专业的网络技术人员在工作中进行加密程序的处理。另外，专业的技术人员可以在工作中及时对计算机存在的病毒实行修复，有效地降低其中的损失，有效降低计算机的安全隐患，有效为网络安全提供技术服务。

3.5网络安全教育在计算机网络安全中的应用

网络安全意识的主要体现是员工在使用网络时具有良好的操作习惯，能够及时规避网络的不安全因素并手动清除隐患。因为这要求员工具有一定程度的风险识别能力，并且对网络安全维护有事先的了解，因此，可以将这些项目添加到部门的培训工作中，让全体员工完全理解这些问题，共同维护企业网络安全。

4.结语

计算机网络技术作为现代社会经济发展的重要轴心，企业自身必须不断加强网络安全管理，制定一定的安全的运维计划和相应的规章制度，进一步加强技术保护。随着计算机不断的发展和使用，出现大量的网络安全隐患，给计算的使用带来严重影响，也有必要提高人们对网络安全的认识，加强警惕，注意计算机网络的正常使用，以使罪犯不会侵入，不会造成经济和财产损失。同时尽快加强计算机自身安全性能减少病毒的入侵，不断使用先进的技术和概念有效地确保计算机网络的安全运行，创建有序的网络环境并持续利用便利性，从根源上加强企业计算机的安全管理，从而有效的保护用户财产。

参考文献

[1]高丽.基于网络安全维护的计算机网络安全技术运用[J].信息与电脑，2020.

[2]吴玉梅.基于网络安全维护的计算机网络安全技术运用[J].电子技术与软件工程，2018.

[3]成乐；姜华；王秀燕.计算机网络安全技术在网络安全维护中的运用研究[J].科技经济导刊，2021.

[4]靳舜.计算机网络安全技术在网络安全维护中的运用解读[J].科技创新导报，2020，17.

[5]钱磊.计算机网络安全技术在网络安全维护中的应用思考[J].2018.

[6]张志花.基于网络信息安全技术管理的计算机应用探究[J].网络安全技术与应用，2020.