

计算机网络安全技术与防范策略探讨

邓映旋

荔浦市公安局互联网信息安全中心 广西 桂林 541000

【摘要】随着科学的进步互联网技术在现代社会迅猛的发展,便利的网络带给了人们很多的方便,但是,也随即产生了网络犯罪,网络犯罪就是不法分子通过网络进行盗取,窃听等不法操作。所以网络安全威胁问题一直都受到社会的重视。如何才能确保网络信息的安全性,尤其是网络上重要的数据的安全性呢?本文从计算机网络的一些常用安全技术简单分析,同时在此基础上,就计算机网络安全防范措施进行了深入探讨,希望能够为创造网络安全运营环境提供一些建议。

【关键词】网络安全;安全性;防范措施

随着计算技术和移动网络的发展,现在人们生活已经离不开网络,最常见的是人们工作网络化和沟通线上化。很多不法人员受利益的驱使进行网络违法行为,导致网络安全受到威胁,面对这种情况,计算机用户应强化安全使用意识,采取有效策略,提高网络使用安全性。

1 计算机网络安全

计算机网络安全的具体含义随着用户的变化而变化。不同的用户对网络安全有不同的需求。从个人用户的角度来看,个人隐私或机密信息在网络上传输时,可能只希望受到保护,以免被窃听、篡改和伪造。简单来说,网络安全包括网络系统的硬件和软件以及网络上信息传输的安全。网络安全既有技术问题,也有管理问题,两者相辅相成。

2 计算机网络安全技术种类

网络安全技术的改进可以保证网络使用的安全。通过对数据信息的预防和控制,可以保证软件不被侵犯。好的技术可以识别网络数据的危害,减少对有害计算机信息的侵犯。网络安全技术有以下几种形式:

2.1 数字签名技术

该技术对数据信息的私钥进行加密,用原始文件传送摘要,接收者用发送者的公钥解密信息,获得信息内容^[1]。

2.2 防火墙技术

防火墙是有效监控计算机用户在使用过程中对网站的访问有无危害,防止不法分子使用互联网进入网络窃取信息。

2.3 数字时间戳技术

该技术是一个加密后的凭证文档,包括需要加时间戳的文件摘要。DTS收到文件的日期时间和数字签名,用户首先将需要加时间的文件用HASH编码加密形成摘要,然后将该摘要发送到DTS,DTS在加入了收到文件摘要的时间日期信息后再对该文件进行数字签名加密操作,最后送回给用户。

2.4 入侵检测技术

该技术对计算机系统中的数据进行分析,总结

入侵的特点,采取有效的预防和控制策略,保证计算机的安全使用。利用入侵检测技术可以检测计算机中的未授权行为,是检测计算机网络中非法行为的主要技术。

2.5 加密技术

通过密码的计算,将重要的文件数据转化为难以识别的数据信息。即使不法分子截获信息,具体内容也无法破解。如果需要,可以使用不同的加密技术来转换数据。

3 计算机网络防范策略

3.1 建立完善的网络安全体系

对于计算机病毒和黑客来说,建立防火墙是主要的对抗手段。在计算机工作中,防火墙会进行实时保护。一旦出现病毒或黑客攻击,第一个障碍就是防火墙。防火墙将发出警报并及时阻止。如果危险数据信息想要传输到计算机,必须与防火墙设置代码相匹配。如果配对不正确,它将立即发出警报。计算机的工作过程就是运行内部程序和软件的过程。一旦遇到不熟悉或无法区分的信息,就需要启动内部防火墙程序,以减少安全风险的发生。如果非法人员未经允许通过网络进入他人账户,系统将自动阻止此行为。用户在使用计算机时,应及时检测和升级防病毒软件和防火墙系统,并更新内部软件。用户下载软件时,应事先确定软件的安全性,然后进行安全管理。出现问题时,用户应快速响应,以确保存储磁盘的安全。

3.2 重视网络安全管理

现如今计算机安全事故频发。网络安全部门应提前采取防范措施,降低网络安全事故发生的概率。一是提高计算机用户的安全防护意识。目前很多用户虽然都知道网络的便利性和危险性,但在实际使用过程中,却没有注意防范计算机病毒和黑客。虽然有些用户想主动预防,但他们不知道如何预防。作为网络安全技术人员,首先要普及安全事故案例,让用户了解网络风险非常普遍,如果不小心,就会发生在自己身上。技术人员讲解网络安全事故的预防和准确操作,演示如何正确使用计算机,帮助用户识别计算机是否安全。二

是采取有效措施,减少计算机风险的发生,设置计算机的访问权限,加密存储在计算机磁盘中的数据,设置重要软件的密码。密码越复杂越好。三是现在许多计算机用户使用路由器进入网络。路由器的不当使用也隐藏着巨大的安全风险。用户需要在计算机上设置权限,以确保路由器仅在固定计算机上执行网络传输。技术人员应保护路由器和计算机中重要文件的传输路径,确保文件的生成和传输严格保密。此外,还要备份重要文件,以防止由于计算机问题而丢失文件。

3.3 提高计算机管理人员的业务素质

为了提高计算机使用的安全性,仅仅依靠用户来提高网络安全意识是远远不够的。计算机管理者需要进行远程安全保护,提高计算机专业知识的利用率和保护策略。管理员在电脑中设置相应的密码,用户进入陌生网站时需要确认密码,再进入网站获取资源。减少电脑用户随意进入病毒网页,不自觉感染病毒、信息泄露等问题。管理者要不断提高专业素质,与时俱进,随时更新知识,更好地为网络安全服务。

3.4 加强杀毒软件的使用

防火墙是控制网络病毒的一种有效的防范系统,但现在许多新病毒很容易越过防火墙,降低计算机的安全性。因

此,除了设置防火墙外,还应安装防病毒软件,以防各种病毒。根据新病毒的特点分析,计算机防病毒软件对病毒的控制有待改进。由于病毒本身具有复制的特性,一旦计算机被复制,就会被杀毒软件检测出来,并采取措施加以防范。研发人员逐步开发出相应的病毒防范方法,为网络安全提供更高更好的安全防护。因此,技术推广人员应推广杀毒软件的使用范围,以确保计算机使用的安全。最后,要合理运用各种策略,例如:访问控制措施、虚拟专用网、虚拟局域网、漏洞扫描等很多种安全技术和措施。只要你根据自身的情况合理的运用相关措施,就能保障计算机的网络安全。

4 结束语

随着互联网技术的不断发展和进步,计算机网络安全以及成为了社会发展的重要保证。虽然目前提高计算机使用安全的技术很多,但是黑客和病毒也在不断的进步,因此我们必须不断完善和创新网络安全防范措施,提高网络安全管理,提高计算机管理人员的素质,减少因为计算机网络安全导致重要信息泄露的發生的事件。

【参考文献】

- [1] 陈焱. 关于计算机网络安全技术的影响因素与防范措施探讨 [J]. 信息记录材料, 2019,20(4):67-68.
- [2] 陆羽翔. 互联网中信息安全技术的重要性及其应用 [J]. 科技创新导报, 2017,(15):167-168.
- [3] 郭黎明. 浅析探析基于网络信息安全技术管理的计算机应用 [J]. 数码世界, 2019,(7):258.

【作者简介】

邓映旋(1988.06-),女,单位:荔浦市公安局互联网信息安全中心,专业:计算机网络技术,研究方向:互联网信息安全。