

计算机网络信息管理及其安全研究

方硕伟

大唐河北发电有限公司王快发电分公司 073100

[摘要]在计算机网络技术持续快速发展的过程中,信息管理与安全工作同样具有至关重要的作用。为切实增强计算机网络信息管理实效,也为了更好地夯实计算机网络的安全运用水平,有必要精准全面地把握好计算机信息管理的问题与不足,积极运用科学且精细化的安全防护策略,切实把握好网络破坏的类型,最大程度增强计算机网络的使用安全。

[关键词]计算机网络;信息管理;安全防护;网络破坏

[DOI] 10.12252/j.issn.2096-6261.2021.11.252

伴随着信息技术的持续发展,计算机网络在方便人们生产生活的同时,也因为自身的安全隐患以及信息风险等,极易给人们带来严重的影响。为全面助推计算机网络信息管理实效,也为了精准高效地夯实它的安全管理水平,人们有必要把握好计算机网络信息管理的现状与问题,积极运用精细化的安全防护策略,切实增强计算机网络信息管理水平,更好地增强计算机网络的整体使用成效。

1 计算机网络信息管理的现状与问题

在计算机网络运行发展的过程中,信息管理工作是至关重要的。因计算机系统存在的漏洞与缺陷,因计算机系统存在着不足与问题等,都会影响着计算机网络信息管理实效,也可能会增加一定的信息风险。为此,在计算机网络信息管理的过程中,要精准全面地把握好信息管理的现状与问题,科学全面地运用精细化的防护举措,最大程度增强计算机网络安全运行实效。现阶段,计算机网络信息管理的问题,集中表现在以下几个方面:

1.1 病毒入侵

病毒的传播速度是非常迅猛的,而且它能够破坏计算机的应用程序,给计算机网络用户的信息安全带来直接地影响与威胁。计算机网络系统在运行过程中,它自身是存在着一定的安全漏洞的,再加上用户在计算机网络的使用过程中,明显缺乏科学的使用习惯,也明显缺乏一定的安全意识,这就为病毒入侵提供了可能,也直接威胁着计算机系统的整体安全实效。当用户在使用计算机网络的过程中,当用户计算机被病毒侵袭后,那么计算机就可能被病毒所控制。病毒发布者正是利用这样的方式来实现关键重要信息地窃取,正是利用这样的方式来实现控制用户的计算机,直接威胁着用户计算机的使用安全。特别是在一些存储绝密信息的计算机网络系统,一旦被病毒入侵,那么这些关键信息都有可能被黑客所窃取,严重威胁着信息拥有者以及使用者的合法权益。

1.2 网络入侵

在计算机网络运行实践中,网络入侵的威胁是非常大的。通常情况下,黑客会选择在网络出现问题时进行破坏活动,主要是通过自身具备的高水平计算机技术对一些账号信息、商业文件、政府机密文件等进行非法窃取,继而非法获利,或者实现自身的不良目的。计算机网络并不是“天衣无缝”的,事实上,计算机网络中存在着非常明显的漏洞。对于广大用户而言,他们在利用计算机网络的过程中,可能缺

乏一定的安全认知,可能缺乏必要的安全意识,这些都会为黑客网络入侵提供了可能。

1.3 人为失误

在计算机网络高效且快速运行的过程中,人为方面的失误,也会滋生不同程度的安全隐患,也会造成较为严重的信息安全问题。用户在使用计算机系统的过程中,为有效防范可能遭受的网络攻击或者黑客入侵等,需要定期查杀网络中存在的病毒,也需要下载专门的防火墙。虽然,现阶段的网络攻击等行为不断变化,但防火墙技术的运用,无疑能够在很大程度上保障网络信息的安全。但事实上,很多用户在使用计算机网络系统的过程中,并没有认知到防火墙的重要性。比如部分用户在利用防火墙的过程中,可能被防火墙弹出的拦截信息较为厌烦,所以,他们可能就会主动关闭防火墙,这就使得计算机网络系统的安全风险等级有所增加。

2 安全防护策略研究

在计算机网络系统安全且高效运行的过程中,科学且精细化的安全防护技术,始终发挥着重要的现实作用。为科学全面地提升计算机网络的安全运行实效,也为了全面优化计算机网络的运行环境,人们需要精准全面地把握好计算机网络信息管理问题,充分全面地研判计算机信息安全风险,科学全面地运用高效化的安全防护策略,最大程度增强安全防护水平。

2.1 实现对IP地址的隐藏化处理

为防范黑客对计算机网络系统IP地址的非法入侵,也为有效防范可能出现的不良网络入侵,人们在使用计算机网络系统的过程中,要实现对IP地址的精准隐藏。实践证明,在计算机网络系统科学且高效运行的过程中,人们只有不断提升自身的安全意识,全面增强自身的安全素养,积极实现对IP地址的隐藏化处理,才能够切实提升自身计算机网络系统地安全运行实效,也才能够更好地保障计算机网络系统的科学运行。在计算机网络系统运行实践中,一些技术高超的黑客,往往会利用非法手段来获取用户的IP,并发动如OOB攻击、SSping攻击等各种进攻。在实践过程中,为全面系统地增强网络安全运行实效,也为了切实保护好IP地址,应该运用性能良好的代理服务器把IP地址进行科学且妥善化地处理,这样IP地址就能够得到合理且高效化地隐藏,这样能够在很大程度上提升计算机网络系统地安全运行实效,也能够有效防范可能出现地网络攻击。

2.2 封死黑客的“后门”

在计算机网络系统科学且高效运行的实践过程中，网络攻击或者非法入侵的存在等，都是基于计算机网络系统自身的漏洞，这是客观因素。当然，也与用户不当的使用习惯等息息相关。为全面有效地增强计算机网络系统的安全运行水平，也为了全面防范可能出现的安全漏洞或者网络风险，人们在使用计算机网络系统的过程中，应该科学且精准化地封死黑客的“后门”。一方面，在利用计算机网络系统的过程中，用户要注重主动关闭“文件和打印共享”的端口。在计算机网络系统的使用过程中，用户可能出于使用习惯，会主动打开这一端口以方便自身的工作，不断提升自身的工作效率。但事实上，这一端口地开启，可能会为用户带来严重的安全风险以及隐患，也会为黑客预留一定的可乘之机。为此，在实践过程中，用户要养成一定的安全习惯，要在不必要的情况下，及时将这一端口予以关闭，并设置相对复杂的密码，以此来全面增强网络安全管理水平，更好地增强网络安全力度。另一方面，用户在利用计算机网络系统的过程中，还应该将不必要的服务及时关闭，以此来防范可能出现的安全风险或者不良入侵。

2.3 科学进行浏览器的安全设置

在计算机网络系统安全且高效运行的过程中，浏览器是重要的输入工具，也是黑客入侵的重要领域。不可否认，现阶段，伴随着计算机网络技术的持续快速发展，人们在利用网络系统的过程中，越来越多地会通过浏览器的方式来进行输入。比如人们可能会在利用浏览器的过程中，设置登陆密码或者设置便捷登陆等，这同样可能为黑客网络入侵提供了渠道。基于此，在计算机网络系统高效运行的过程中，人们应该加强对浏览器的安全设置，应该注重将浏览器的隔离模式及时打开，有效防范可能存在的的社会网络信息。与此同时，隔离模式的运用，还能够防范一些弹窗广告，为用户带来流畅的“冲浪”体验。

2.4 科学安装杀毒软件

在计算机网络系统高效且科学运行的过程中，高效且科学化的杀毒软件，同样具有至关重要的作用。为切实提升计算机网络系统的运行安全，也为了更好地优化计算机网络系统的使用性能，人们在利用计算机网络系统的过程中，要充分结合自身的发展需求，积极安装性能优良的杀毒软件，同时，也要科学安装一些防火墙工具等。实践证明，在预防网络攻击的过程中，这些防火墙技术以及病毒查杀工具，能够将网络病毒进行快速的筛查并精准隔离，以此来保障计算机网络系统的高效且科学化运行。

3 网络破坏类型分析

在计算机网络系统科学运行的过程中，网络破坏类型是非常多元化的。为全面系统地增强信息安全管理，也为了更进一步地优化信息安全，有必要精准全面地把握好网络破坏类型，积极明确网络破坏的防治举措，最大程度增强网络安全成效。在计算机网络系统运行实践中，常见的网络破坏类

型主要包括以下几个方面：

3.1 对互联网进行安全攻击

在全新的信息背景下，互联网在充分满足人们使用需求，在给予人们提供极大便利条件的同时，自身也存在着较大的安全漏洞。黑客在利用计算机网络系统的过程中，正是瞅准了互联网系统的漏洞，所以发起了网络安全攻击，轻则可能会造成重要信息的丢失、篡改，重则可能会造成整个互联网瘫痪。为此，在计算机网络安全运行的过程中，要科学全面地把握这一类型的网络破坏行为，积极运用精细化地防控举措，切实创设科学且良好的网络安全环境，全面保障用户的信息安全。

3.2 木马病毒的植入和窃取

在互联网安全且高效运行的过程中，木马病毒的存在始终具有非常大的威胁。在具体的发展中，木马病毒可能会伪装成其他不同形式，隐藏在网络用户的程序中。作为计算机网络系统的使用主体，用户可能很难发现这一隐藏的信息。木马病毒的存在，会窃取用户的网络信息，比如用户网络账号密码、用户的网络文件等。比如前几年威胁巨大的“熊猫烧香”病毒，就对计算机网络系统用户的信息安全造成了直接的威胁，甚至使得用户的计算机系统出现崩溃和瘫痪问题。

3.3 哄骗式攻击

在计算机网络系统运行实践中，哄骗式攻击的存在同样具有非常大的威胁。这种攻击方式主要是对第三者所拥有的身份进行伪造，主要发生在互联网所规定的服务范围与协议范围内，可以被欺骗的对象包括了DNS服务器、IP地址、X-WINDOW系统和远程调用等。在用户使用计算机网络系统的过程中，若系统存在着较大的风险与隐患，或者系统存在着较大的安全漏洞等，都可能使得计算机网络系统出现不同程度的破坏和影响，都可能会造成计算机网络系统的整体瘫痪。比如IP哄骗式攻击，就是一种对IP进行欺骗的非法行径。基于此，在计算机网络系统安全管理的过程中，人们要多措并举全面防范这一哄骗式攻击，切实增强计算机网络地安全使用成效。

结束语

在计算机网络系统运行发展的过程中，为全面系统的增强信息安全管理成效，也为了全面保障计算机网络系统地高效化运行，用户应该积极运用科学化的安全防护策略，切实增强网络安全防控力度。

参考文献

- [1] 于颖. 计算机网络信息管理及安全防护研究[J]. 农业科技与装备. 2018, (6): 34.
- [2] 赵洪玉. 浅谈计算机网络信息及其安全防护举措[J]. 数字技术与应用. 2018, (3): 192-193.
- [3] 杨凤山. 计算机软件工程的管理和维护研究[J]. 信息通信. 2016, (2): 189-190.