新环境下的计算机网络信息安全及其防火墙技术

王 波
（凯里学院信息网络中心 贵州凯里 556011）

【摘 要】网络信息化技术在持续进步，社会各界也愈加的重视网络数据的安全问题，信息化时代的到来，各行各业对信息的需求量也是逐日增多，信息获取最快速的方法便是通过互联网，现在的网络环境复杂且多变，病毒的形态也是各式各样，其侵染所需时间短损坏性极强，对强大的网络信息造成严重的安全威胁，从而影响人们的日常生活。为了确保计算机网络信息的安全，相关工作人员应积极研究防控技术和方法，确保实际网络应用的安全性，在网络信息安全领域防火墙技术是重要的核心技术，不断受到社会的广泛关注，其技术的应用对计算机网络信息安全也带来了正面积极的效果。

【关键词】计算机；网络信息安全；防火墙技术
DOI: 10.18686/jyfzyj.v3i7.47389

随着计算机的发展和普遍使用，人们对计算机也是越发的依附。在未来的科学技术的发展中，计算机的影响很是巨大，但同时也存在各种安全隐患，各类病毒的风险不断在平时的生活中蔓延开来，黑客创造的病毒、软件自身的漏洞和安全意识不足等都是网络信息的主要安全威胁。因此，有必要创建一个足够安全、科学合理的网络使用环境，相关行业需要从技术角度合理实施保护，明晰外网环境和内部系统的关联性，进而高效掌控网络体系。

1、对计算机网络安全造型影响的原因分析

1.1 网络黑客的攻击

当前计算机网络系统中，大量黑客袭击电脑事件出现，电脑网络系统已经成为了那些具有深厚网络技术侵袭者的表演平台，大多数情况下，黑客出现并不是因为有自由入侵的能力，而是因为他们擅长发现网络的破绽并针对它发起攻击，通常黑客采取的侵入行为分为两种，一种是主动型攻击，这种攻击有强大的目的和计划，黑客通过攻击用户可以得到他们想要的数据，但是与此同时，黑客对互联网的主动型攻击也很容易暴露自己，在黑客发现自己被追踪后便开始执行被动型攻击，这是第二种类型的攻击，比如把病毒等低劣的程序和或软件放入隐藏文件中，偷偷地盗取用户的信息和数据，对于计算机网络安全来说，黑客带有目标型的攻击经常会给用户造成非常严重的损失[1]。

1.2 计算机系统存在漏洞

计算机网络系统的管理漏洞也对用户的信息安全造成了一定的影响，当外部网络信息对计算机发起攻击时，工作人员不但需要掌握一定的技术，并且还要对计算机进行正确的管理，一个健全的管理系统可以减少网络信息安全事件发生的频率。除此之外，人们对网络信息安全的重要性的认识也比较匮乏，用户信息保护意识不足等也加大了信息泄露的风险。还有一些比较特殊的情况，某些大公司和企业的计算机网络系统比较庞大，管理系统不完整也会加大网络信息被泄露的可能性，还有某些软件存在“抄近路”的问题，这是由软件设计师和程序员为了自己的方便而设置的，但一旦大家都“抄近路”，所造成的损失将深不可测。

1.3 计算机病毒的侵入

计算机病毒是指一种会对系统软件与硬件造成损害的程序代码，其有着强大的寄生性能、潜伏性能、毁坏性和自我克隆性，再加上互联网络本身就是开放性的，使其成为了当前数据信息的最大安全威胁，病毒一般会依靠电子邮件、附件以及一些不合法的网站来成功侵略电脑的主机系统。近几年，随着云查杀软件和木马检测系统的推广和使用，大量的超级性病毒（一旦运用便能侵染超百万的数据信息的病毒）已经接近绝迹，经国家级电脑病毒应急处理中心合计显示，逻辑炸弹病毒是最常见的恶意程序，他们利用游戏插件、恶意网址、山寨软件和视频等诱人的网络资源，欺骗用户并实现入侵对计算机安全造成严重威胁，它的扩散形态复杂感染速度快破坏性强，完全消除是很困难的，可轻松对硬盘、光驱、主板等造成破坏是目前网络安全的最强大的对手。病毒一旦在网络上传播的话网络将无法正常运转，可见强化人们的计算机数据安全防护意识是多么重要[2]。

1.4 钓鱼网站诈骗

钓鱼网站是指效仿真实网站的链接地址或页面内容，或在真实网站程序中插入危险代码，从而不合法的获取电脑所有者的数据信息，由于该网站通常只是普通的假网站模板，因此它们一般没有不良的软件代码，这一特点也就使得利用传统的防病毒引擎很难彻底的消除它们。该网站大多是借助聊天工具、广告、网页、论坛、虚假电子邮件等方式进行廓张的，当前最为常见的体现就是假购物、假赢、假银行网站和假电子商务网站等，从而给人们的银行账户、密码和有关个人信息等构成特定威胁。据有关部门调查合计，近两年内，钓鱼网站给人们带来的威胁已经成为仅次于木马病毒的第二大信息数据安全威胁。

1.5 自然因素

在操作计算机系统时，自然方面的因素给数据信息的安全带来的影响也是不容小觑的，大部分的电脑数据都是保存在外部的设备上的，因此无法保证外部设备长期永久完好无损，然而许多机房都忽视了抗震、防火、防水、放电击等工作，没有充分考虑接地系统，因此对自然灾害的抵抗力还需加强，尤其洪水和火灾都可能会损坏到计算机系统，使得部分电脑上的数据信息遭到破坏，严重的还会消失，进而使得电脑使用者无法正常的使用电脑，造成不必要的麻烦。

2、防火墙技术在计算机网络信息安全保护中的运用

2.1 在内外网构建隔离墙

现如今，对于计算机数据信息安全防护的技术，最常用且最知名的就是防火墙技术，无论什么时间什么地点，它都能充分发挥出保护电脑数据信息安全的作用。防火墙技术的原理是将互联网分为内网和外网两个板块，并在两者之间建立起隔离的屏障，这种隔离屏障就是安全使用互联网的重要保障。基于互联网用户的需求，防火墙对复杂的外部网进行隔离，并在防火墙内构建新的网络环境，对外部网络的行为进行实时监测，从而达到有效阻止外网入侵内网窃取数据和信息的目的，同时，也并不会因为有防火墙而致使用户访问外网时出现无法访问或者访问困难的情况，并且在电脑数据得到了保障的同时，使用者们也获得了想要获取到的信息[3]。

2.2 对信息进行过滤处理

当前，电脑使用者经常用到的防火墙技术主要有两种：信

息过滤技术和代理技术，其中信息过滤技术是类似于人们乘坐高铁前进行安全检查的原理，进入计算机内部网必须先经过防火墙的数据包检测，只有检测合格的数据包才有权利进入计算机系统，任何不符合安全要求的都将被拒绝访问，需要注意的是，信息过滤技术通常只检测头部数据而不是所有的数据包，如果需要检测所有的数据包，需要花费大量的时间并对用户访问效率产生影响，在检查头部数据过程中，过滤技术会根据指示确定恶意和敏感信息并将其提出以保证用户的安全。代理技术是一种双宿主关网，也就是说它包含两个网络接口分别连接到内部网络和外部网络，信息的传输也是由两个网络接口卡之间的一个媒介来完成的，它不仅全面细致地筛选了数据，而且具有信息传输和通信的功能，来自外部网的信息在进入内部网之前必须经过代理（媒介）的全面检查，所以，用户在应用代理技术过程中，就可利用有防火墙的主机，结合主机的实际不足之处来制作出对应的代理软件，使得计算机数据信息得到最大程度上的保护。

3、 新环境下计算机网络信息安全防护策略

3.1 合理利用防火墙技术进行安全管理

一般来说，计算机运行程序使用安全系统和防火墙技术目的就是阻止不良软件和各类病毒的侵扰，防火墙技术有将数据信息分隔开的功效，能够使得恶劣的病毒和内部网络分开，然后将计算机系统内部的文件每隔一段时间对其进行筛查、分类整和保存，同时对那些来自外部的数据信息的安全性进行辨别，最终达到阻止病毒侵入主机系统的目的。目前，不良软件和电脑病毒的数量和类型也在随着科技的进步而不断上升，对计算机网络的信息安全带来了很大的威胁，防火墙系统设计的相关工作人员，必须更加详细地了解各种病毒的特性，并用专业的方法设计安全的系统以保护网络信息的安全，在使用计算机网络的过程中，对于一些比较常见的计算机病毒或恶意软件，通常防火墙技术或网络安全系统都可以轻松拦截，防火墙本身还具有一定的信息分离功能，可以在内部网络和外部网络之间构建屏蔽层，屏蔽外部网络信息，以防止病毒程序入侵。因此，负责防火墙和互联网安全系统设计和使用的工作人员必须不断学习和充分了解各种新病毒的特点，以最大限度地提高网络的信息安全性。

3.2 利用防病毒技术保证网络安全

保护计算机网络信息安全的过程，不仅需要加强技术和硬件的配置，还要注重安全管理问题，加强内部监督和控制，健康的内部网络管理系统可以快速的更新网络检测系统，以避免计算机长期暴露于安全漏洞中，并有效阻碍各类计算机病毒的侵入。与此同时要开展电脑使用方面的安全技能知识教育，并不断强化此类教育，此外还需要定期更新现有的防病毒技术，从而使得网络数据信息能够在最大程度上提升其安全性。总的来说，计算机网络技术的不断进步也创新了相应网络信息安全保护技术。在新时代，为了满足用户日益多变的需求，技术人员需要不断改进和更新防火墙技术，使其成为网络安全的保护屏障[4]。

3.3 定期对计算机进行安全漏洞扫描

漏洞扫描是一种安全检测技术，它可以检测出网络系统的安全漏洞，还可以发现可被病毒攻击的漏洞，通过漏洞扫描可事先发现将被攻击的漏洞链接，然后就能够专注于修补和修复漏洞，从而将信息化网络数据的安全大大提升。有两种主要的扫描执行模式：基于互联网的扫描和基于主要机体的扫描，扫描方法通常是测试和攻击模拟，测试是指与目标主机端口建立连接，并请求远程协助服务，记录主机的响应，收集安全漏洞信息，模拟攻击是指使用模拟方法，如木马、电子邮件等入侵方法对计算机发起攻击，以检测目标系统中可能存在的已知安全漏洞。

3.4 加强用户的防范意识

提高用户的网络信息安全意识与普及计算机安全基础知识是十分必要的，这将提高整个网络的信息安全管理，如面对未知信息、电子邮件等不感兴趣的链接不要因为好奇而随手点开，也不要从互联网上的某些网站下载不规范的软件或文件。另一方面，计算机用户必须学会如何隐藏自己的IP地址，因为隐藏自己的IP地址对于保护网络的信息安全非常重要，病毒常常是在用户不知情的状态下随手安装的，在这种情况下，攻击者如果无法找到用户的IP的便无法对系统发起攻击。因此，隐藏IP地址是非常必要的，此外用户还需要及时更新电脑系统的补丁文件，以保证自己的信息不受黑客软件的攻击。

4、结论

综上所述，如果网络安全得不到充分的保护，随时可能给计算机网络用户带来巨大损失，因此进一步加强网络信息安全的维护很有必要。目前，防火墙技术作为一种简单实用的防护技术，对网络数据信息的保护是非常高效的，其作用意义不容小觑，在保护网络信息安全方面发挥着重要的作用，在全球各国联系不断增强的今天，网络信息安全是中国人的主要关注事项，对所有领域的发展都非常重要，因此了解防火墙技术并合理利用它是确保网络信息安全的最重要方法，对社会的建设和发展有很大影响。

参考文献

[1] 黄建华，刘昕林，黄萍．新环境下的计算机网络信息安全及其防火墙技术[J]. 电子技术与软件工程，2020(01):225-226.

[2] 刘瑜．新环境下的计算机网络信息安全及其防火墙技术应用[J]. 电脑知识与技术，2019,15(21):30-32.

[3] 李文．新环境下的计算机网络信息安全及其防火墙技术应用[J]. 数字技术与应用，2019,36(05):15-17.

[4] 梁立志．新环境下的计算机网络信息安全及其防火墙技术应用[J]. 信息记录材料，2019,19(05):44-46.