计算机网络工程安全与病毒防护

董子阳
广东创世科技有限公司

[摘　要]计算机工程安全在人们生活中的重要性与日俱增，网络安全问题也引起了人们的关注。如何为人们建立一个安全的网络环境已经成为一个亟待解决的问题。尤其是当前，网络病毒的出现，导致个人信息的泄漏、个人账户的篡改和计算机数据的破坏，给人们的生活以及网络工程的安全带来了极大的威胁。因此，本文的研究主要针对计算机网络常见的病毒特征和计算机网络的工程安全问题，提出有效的防护对策。希望这样可以保证计算机网络的正常使用，避免一些隐藏的问题，防止财产损失和数据泄漏，保证网络的正常运行。

[关键词]计算机网络工程安全；病毒预防；措施
【DOI】10.12252/j.issn.2096-6288.2020.03.417

随着科学技术的快速发展，让人们逐渐进入到信息化时代，而计算机就是信息化时代的产物，它可以提升了人们的生活质量，还可以给人们生活和工作带来了便捷，但在带来便捷的同时也存在一定的问题，尤其是网络工程安全和病毒预防问题，因此就计算机网络工程安全与病毒预防进行讨论，并对计算机网络安全存在的问题提出维护措施，做好计算机网络工程安全与病毒预防工作，促使计算机得到更好的发展和应用。

一、计算机病毒的特点

想要有效的对于计算机的病毒进行防范，先要了解计算机病毒的特征。

1.善于伪装。现如今随着系统的日益更新换代，市面上有很多杀毒软件可以对于软件进行有效检测。虽然说杀毒软件很厉害，但是病毒也随着科技的发展变得更加厉害，具有较强的伪装性和隐蔽性。尤其是趁计算机用户不注意的时候，病毒会潜藏在文件里或链接里，对用户进行文件的破坏或数据的入侵。甚至会伪装成一些计算机的文件，一旦打开文件就会引起病毒入侵，甚至防火墙都无法抵抗了。

2.攻击力强。目前市面上存在的计算机网络病毒攻击力极强，首先会破坏计算机的防御功能，紧接着对于内容进行篡改，导致部分计算机的用户难以招架，甚至会影响计算机的正常使用。从目前来看，计算机进攻领域被广泛出现在金融行业和政府行业不法分子，为了获取利益而窃取相关资料，就是通过病毒的导入来进行资料的窃取。网络的病毒分类有很多种，一般可以分为木马病毒和蠕虫病毒，扩散面积极广，范围极广能在很短的时间内感染局域网之内的所有计算机。而且部分病毒的攻击力甚至无法清楚，很可能一台计算机刚刚清除，另一台瞬间被携带病毒的工作站所感染。

3.潜伏期长，感染范围广。计算机常见的病毒中木马病毒是后门程序会潜伏在系统中，来盗取用户的账号或密码。病毒传播范围广，被利用计算机系统中的漏洞或是程序的漏洞发出攻击，每种病毒都会对计算机进行扫描，一旦传播出去危害性极大，被感染后如同病毒会发放大量的数据包，使得传播速度极广，也会因此导致部分计算机存在CPU或内存占用过高，濒临死机。除此之外，潜伏期较长，且范围较广的病毒还包括邮件性病毒，虽然容易清除，但是会隐藏在附件中，很难察觉。会通过浏览器的漏洞来进行传播，部分用户只是浏览了相应附件，就会使得病毒趁虚而入。最广泛的windows系统中出现的系统病毒是漏洞性病毒，虽然说计算机会有定期的安全补贴和病毒扫描，但不一定能够完全将这些漏洞性病毒进行清杀。例如风靡网络的震荡波病毒，就是感染性强，潜藏隐蔽的病毒，一旦出现就会导致多部网络计算机瘫痪，给使用者带来巨大损失。

二、计算机网络工程安全问题

造成计算机网络的安全因素有很多，最常见的就有计算机系统漏洞、黑客攻击、木马病毒入侵、IP地址被盗等。

1.计算机操作系统漏洞。一直以来计算机网络安全问题中的操作系统的漏洞是无法避免的，每当一个新的系统产生就会带来很多系统漏洞，所以修复漏洞成为了计算机工作人员不可避免的.工作漏洞的产生与黑客分子和不法分子对于人们的系统进行非法攻击破坏有关，部分不法分子为了利益利用病毒，非正常的植入人们的系统，篡改系统中的数据，不仅影响了人们系统的正常运行，还会使部分系统处于瘫痪状态，更严重的会借助病毒盗取用户资料，造成用户使用系统中难以挽回的损失。

2.计算机木马和病毒入侵。常见的计算机用户经常会遇到电脑文件无缘无故被删除、篡改或加密的问题，这种问题均是因为计算机的木马或病毒入侵导致的。例如前段时间较为有名的永恒之蓝的病毒，就对于用户的windows系统进行了攻击和入侵。这是一种恶性的蠕虫代码，通过对于windows网络共享协议的改变，攻击人们的计算机修改数据。想要解除这种病毒需要支付高昂的费用才能缓解。一般来说计算机的病毒木马传播需要通过部分邮件的附件或下载相应的程序，伪装成浏览器的页面，利用安全漏洞进行传播。因此，在日常用户使用过程中，需要对于网站上突出的链接或是不当的链接进行防范。

3.黑客攻击入侵。网络安全威胁不减反增的原因，就是因为近几年的黑客入侵日益频繁，部分不法分子利用不正当的手段盗取人们电脑中的信息或者文件。黑客一词由来已久，部分黑客利用自己高超的编程技术，对于电脑中的系统

漏洞进行入侵，常常会骗取相关机密文件或盗用相关资料。一般来说部分黑客会经常使用破坏性的攻击或非破坏的攻击，入侵他人系统，攻击他人的服务系统。黑客会破坏被攻击者的系统，从而盗取用户资料和机密文件。

4.IP地址盗用。计算机网络安全中IP地址盗用也是不可忽视的网络安全问题，不法分子借用计算机黑客技术盗取IP地址，给用户带来极大的风险，实施网络犯罪。近一年来，国家就出台了相应的政策来规范和防范IP地址被盗等问题，但是收效甚微。目前Ipv6的地址几乎无穷的，IP地址被分配到全国通用的网络，通过因特网就可以直接查询IP设备，虽然便于访问。但面对非法入侵，例如信息窃听以及数据窃取，就会造成不利的影响。最早Ipv6的设计时，就已经着重于对保护IP的进行了安全协议的设定。但是路由器以及防火墙配置不到位，也会造成IP地址泄漏。

三、计算机网络工程安全威胁的防护对策

针对计算机网络安全问题，各类的威胁与隐患因素，要想确保计算机网络工程安全，就必须要给予针对性的解决办法，尤其是要做好网络病毒的防护。

1.做好防火墙的设置。防火墙的应用在一定程度上能够保护计算机免受外界网络的侵害。这是因为防火墙的应用就相当于在计算机的内网与外网之间建立了一个保护层，隔离内网与外网的同时，也将一些有害的数据、木马、病毒等不安全信息有效的过滤出去，进而达到保护计算机安全的作用。同时，防火墙还可以对计算机端口实施监控，在一定程度上避免木马与病毒通过计算机端口入侵到计算机网络之中。尤其是当人们访问的计算机网络存在木马病毒时，浏览器就会自动提醒人们所访问的网站存在安全问题，是否还需要进行访问，这也有效的避免了不法分子通过网页登录进入到计算机内部网络中，盗取计算机用户信息。所以设置好计算机防火墙，做好计算机防火墙的定期升级则能够在一定程度上有效预防木马与病毒的入侵，保证计算机的网络工程安全。

2.安装防病毒软件。现如今木马病毒的种类与日俱增，严重威胁到计算机网络安全。而防病毒软件作为拦截木马病毒的有效手段，其每天都能够拦截数以万计的木马病毒，拦截有毒的传入文件、拦截伪装网站上的有毒下载程度，并且将威胁文件程度添加到隔离区予以删除。因此在日常计算机使用过程中，就必须要做好防病毒软件的安装工作，及时更新云病毒库，并且还要能够熟悉使用这些软件，且注意不要轻易下载陌生人发过来的文件程度，从而不给木马病毒入侵计算机的机会。

3.加密重要文件和软件。因为病毒的攻击性较强，所以有必要对软件或重要的数据文件进行加密，这样一来即使有病毒成功入侵电脑，但是在获取重要的机密文件时对身份进行验证，病毒就无计可施了。还有一种方法是，加密和隐藏重要的数据信息，用假的信息来覆盖，这样入侵的病毒就无法获得真实的信息。一般来说，学校的教务系统和公司的企业系统都会使用这个方法，对重要信息进行加密，保证其数据文件的安全。那么个人用户也应该注意这方面的措施，加强信息加密意识，定期的对计算机中的重要的信息进行加密，对病毒进行更好的预防。

4.及时修复与升级操作系统。正是因为计算机操作系统漏洞不可避免，且不少木马病毒程序都是依托于操作系统漏洞存在创建的。所以计算机使用者在日常使用过程中发现漏洞问题要第一时间给予修复与升级。为此还可以为计算机安装安全防护软件，通过后台运行及时发现操作系统漏洞进行自动修复，或者是通过定期检查查找漏洞问题，予以及时修复，确保计算机不会轻易受到外界攻击，提升计算机网络安全。

5.操作系统安全漏洞防护。计算机系统中的安全漏洞是非常重要的一个问题，有很多特洛伊木马程序是为了操作漏洞而建设的。所以在日常的计算机使用过程中，需要定期的安装360安全卫士或是电脑管家等相应的防护软件。对于计算机漏洞进行定期的扫描和修复，确保高危漏洞不会威胁人们的电脑使用安全性。另外可以依托这些计算机软件，进行定期的系统升级和修复，查找漏洞的问题，确保计算机不会轻易受到外界攻击。

6.计算机网络工程安全的综合防范。除了上述的计算机网络工程病毒的安全防范之外，管理者和应用者都需要认识到计算机网络工程安全的重要性.因为网络毕竟是具有开放性，对用户的认证在网络安全上显得十分重要，需要通过用户口令密码，实现网络系统权限的分级，增加密码技术的提升，对于不同网络的机密系统或数字签名等方式进行网络加密。包括节点对节点的加密、链路加密方式加强保护机制。同时也要加强防火墙技术中数据包的过滤技术、应用网关技术和代理技术，避免病毒的入侵，为计算机网络的安全提供保障。

总之，计算机病毒是源源不断的，即使一波病毒解决了，也会有下一波新的病毒，科技就是有利有弊，我们接受了其便利的地方，也就要接受其风险。所以计算机主人需要做的就是经常关注计算机，对计算机定期进行全方面的清理和安全检测，建立良好的计算机防火墙系统，及时更新和升级杀毒软件，浏览正规网站，不浏览有风险提示的垃圾网站，做好计算机的网络安全与病毒防护。

参考文献

[1]孙岸文.浅析计算机网络安全的主要隐患及管理措施[J].技术与市场，2016，23（12）：151.

[2]马津伟，郭强.关于计算机网络安全防范技术的研究和应用[J].湖北函授大学学报，2016，29（17）：98-99.