计算机信息管理技术在网络安全中的应用

文 / 张宁

摘要：伴随计算机信息管理技术的普及和快速发展，计算机信息管理技术在网络安全中扮演着越来越重要的角色。虽然网络给人们的生活、工作带来了较多的便利，但是网络优势的背后也存在着不容小觑的隐患，这些隐患对人们的财产安全有着不小的威胁。因此，计算机信息管理技术也就愈发受到外界重视。文章针对计算机信息管理技术在网络安全中的应用进行详细阐述，并提出具体应用措施，以期构建安全网络环境。

关键词：计算机信息管理技术；网络安全；技术应用

在当下的社会中，人们已经愈发离不开网络，网络已经渗透到我们生活中的各种细节中，成为我们生活、工作中不可或缺的一部分，也正由于网络的重要性，网络安全问题也逐渐受到越来越多的重视。网络安全问题的备受关注，也让计算机信息管理技术有了新的发展需求及要求，只有作好发挥计算机信息管理技术在网络安全中的应用，才能构造一个和谐、安全的网络环境，显而易见，这是非常有必要的。

一、网络安全现状及计算机用户需要

当前的网络安全还是主要集中在电脑及手机两个方面，电脑和手机都是人们离不开的通讯、交流工具，与人们的日常生活密不可分，这也就意味着一旦电脑或者手机被黑客攻击，人们的财产安全将被严重威胁，很容易造成的经济损失，更严重者，还有可能在社会上造成严重负面影响，造成人们的恐慌，所以，网络安全始终是互联网环境中一个迫切需要解决的问题。

当前的网络安全状况仍旧不乐观，仍有许多影响、威胁互联网安全的因素存在，主要分为两个大方面：

（一）计算机本身存在的漏洞

在互联网中，计算机本身存在的漏洞可以说是影响网络安全的其中一个因素。造成计算机存在漏洞的原因大多是计算机工程师的最初的设计存在问题，虽然问题不大，但是也容易被黑客盯上，从而进行破坏及渗入。因此，当电脑存在漏洞的时候，用户需要及时进行修补，不给不良分子破坏机会。所以，在关注网络安全的同时，也需要积极完善计算机本身，不给不法分子留有机会。

（二）计算机外部攻击

在网络安全中，重大隐患还是要属外部攻击，黑客利用不正当技术对计算机终端进行攻击，利用计算机存在的漏洞成功盗取用户各方面信息，严重威胁着用户的经济财产安全。由于网络的开放性特点，攻击现象仍是层出不穷，再加上用户防范意识不强，很容易无意间下载木马病毒，这给不法分子提供了可乘之机，也不利于网络安全。

二、计算机信息管理技术在网络安全中的具体应用及用户操作原则

（一）计算机信息管理技术在网络安全中的具体应用

1.防火墙技术

防火墙技术是应对外界攻击及未知病毒的第一道防护屏障，是信息管理技术中的核心技术。防火墙技术可以对外界攻击及时敏锐察觉，帮助用户加以甄别和判断，一定程度上对计算机进行了保护。防火墙还可以对病毒加以筛查，帮助用户判别有害软件，从而杜绝下载程序，保护了计算机内的信息资料。现阶段的防火墙主要有包过滤式、代理式、地址转换式三种方式，主要运行模式是及时切断访问权限，从而杜绝、切断不良分子对计算机的不良企图途径，还可以大大提升网络安全。

2.访问控制技术

访问控制技术主要是在入网环节中进行信息的筛查与剔除，将不良信息与未知风险阻挡在计算机外。现阶段的访问控制技术主要是与身份认证结合在一起，通过这种手段，将不明身份的人杜绝在计算机外，较大程度避免了黑客攻击，也较大程度地避免了网络异常情况出现。

3.安全评估技术

对于计算机网络来说，时时刻刻都有可能受到攻击和威胁，遇到的攻击及威胁类型也不尽相同，需要计算机技术进行多方面的筛查和检测，对未知的危险做到有效评估，安全评估技术也就是在这方面发挥功效的。安全评估技术会将计算机运行状态加以检测和评定，全面分析计算机网络安全状态，还会挖掘出潜在威胁并消除掉，为计算机安全运行提供了有力帮助。像我们常用的 360、金山毒霸等软件，都能对计算机进行实时检测并评价，帮助用户更好地了解计算机运行状态，防止黑客攻

击，切实提高了计算机运行安全性及安全性。

4.追踪技术

在计算机信息管理技术中，追踪技术是其中的亮点，是可以有效追踪攻击来源的有效技术手段。追踪技术可以根据攻击时间、攻击类型等锁定不法分子的 IP 地址，最后寻找到源头，可以破获重大危害网络安全事件。追踪技术分为主动追踪和被动追踪两种方式，用户可以进行相应选择和设定，不管何种形式都大大降低了网络安全风险，大大提高了资料、信息、数据安全性，大大保障与维护了用户权益。

（二）计算机用户操作原则

为了避免外界攻击、内部病毒对计算机造成的危害，计算机用户也需要遵循一定操作原则，切实避免计算机资料信息被盗。

1.时刻保持安全防护观念原则

想要构建安全网络环境，首先需要用户提高防范意识，加强防范措施，时刻将防范观念记心头。具体可以是不浏览非法网页、未知网页，虽然网络中的信息丰富多彩，还是需要用户加强自身约束，抑制住打开未知网站的好奇心，尽量不打开拿不准的链接，很多的链接背后是病毒，所以，树立安全防护观念是非常有必要的。除了克制住好奇心与冲动打开一些不确定网页，还需要用户及时下载杀毒软件进行预防工作，如我们熟知的 360 杀毒软件、金山毒霸软件、电脑管家等都可以选择及下载，计算机用户还需要定期对电脑展开修复及筛查，对电脑漏洞要及时修复，还可以开启杀毒软件 24 小时安全防护，防止电脑运行中受到外界攻击，保证电脑可以长时间平稳、安全运行。

2.充分利用好计算机防护功能原则

除了一些杀毒软件的协助，计算机本身也是具有一定排查风险，控制隐患的功能存在的，用户需要及时打开防火墙、及时采用访问控制技术等，充分发挥计算机本身防护功能，杜绝外界不良信息及不良干扰。计算机用户还可根据计算机本身提示，设置开机使用密码。密码设定要尽量复杂，切实杜绝电脑丢失或不经意间不相关人员动用电脑盗取信息等现象，切实避免电脑资料的丢失现象发生。此外，还需要用户及时修复计算机漏洞，及时安装补丁，以此来减少计算机受到的攻击，确保网络系统的安全性。

三、借助计算机信息管理技术提高网络安全的具体措施

（一）加强操作系统的安全防护

对于计算机本身而言，应具备高、精、尖的设备，也需要用专业扫描软件来检验系统本身是否存在漏洞，一旦发现问题，就需要有效地对漏洞及问题进行分析、查验，找出问题源头，提出有效的解决方案，切实解决存在的一切问题。此外，还需要严格限制文件浏览及使用权限，加强身份认证，可以开拓用户瞳孔、指纹等验证通道，设置多层关卡供用户选择，还要制定全新补丁，将网络安全风险降到最低。

（二）加强信息加密算法的应用

众所周知，计算机信息加密依靠的是各类密码算法，没有密码算法的加持，加密系统将失去安全防护意义。传统的加密方式组成结构单一，采用同一密匙，安全系数较低，所以我们应加强信息加密算法应用，及时采用最新加密算法，像 PGP 混合加密算法、RSA 公开密钥密码技术算法等都是现在常用的加密算法。加密算法方面要及时跟进科研成果，做到与时俱进，做到比黑客技术更具先进性、前沿性。

（三）加强外联网络安全防护

外联的方式有很多，有蓝牙系统、有线网卡、USB 端口等等，人们经常用这些外联传输文件及资料，应该对这些终端进行有效管控，切实阻断终端带来的危害。因此，应当屏蔽不明渠道、不明用途端口，并对计算机安全管理进行设定，一旦发现不明来源终端试图连接网络，应及时切断途径。对此，也可以成立一套身份认证系统，进而提高筛查用户身份效率，进而提高网络安全系数。

（四）制度视角下加强计算机技术网络安全管理

第一，专门成立一个计算机技术网络安全小组，将提高网络安全作为最终工作目标，切实发挥计算机信息技术功效，构建计算机安全管理体系。

第二，在网络改造升级工作中，要严格按照相关规范做好管理网段与业务网段分离。

第三，全面淘汰市面上落后计算机，普及性能好的计算机，避免计算机因使用寿命及使用隐患造成的重大损失。

四、结语

当前，我国的计算机信息管理技术还处于初级阶段，网络安全也还有较长的路要走。在此期间，需要充分结合计算机信息管理技术与网络安全，将计算机信息管理技术充分应用，还需要不断提高技术应用水平、不断研发新技术，以此来应对未来更多网络安全风险与隐患，让网络环境更加和谐、安全。

参考文献：

[1]凌征.计算机信息管理技术在网络安全应用中的探析[J].计算机产品与流通,2019(10):4.

[2]赵霖卿.探析计算机信息管理技术在网络安全中的应用[J].电脑编程技巧与维护,2019(8):156-157,160.

[3]张爱玲.浅谈计算机信息管理技术在维护网络安全中的应用[J].信息记录材料,2019(8):47-48.

[4]毛立钢.物联网背景下计算机信息技术在网络数据管理中的应用[J].信息通信,2018(7):135-136.

[5]龙华彬.计算机应用技术与信息管理的整合解析[J].科技经济导刊,2018,26(19):30,55.

作者单位：

江苏联合职业技术学院南京工程分院