计算机信息系统维护与网络安全漏洞处理方法

宋国辉
广东培正学院　广东　广州　510830

摘　要：在这个信息爆炸的时代，许多重要的工作都可以通过大数据来完成。然而，它给人们带来了方便，也给人们带来了一些危险。在计算机技术领域中，由于存在着许多的安全隐患，这些隐患的存在，不但会威胁到计算机使用者的信息安全，而且也会给他们带来一些经济上的损失。在这种情况下，有关工作人员必须要强化自己对计算机信息系统的管理，并要对计算机信息系统中存在的网络安全缺陷进行及时的处理，从而保证使用者的人身安全，减少因为这些缺陷而造成的损失。

关键词：计算机；系统维护；网络安全

引言：随着计算机网络技术的发展，信息技术在生产、工作、生活中起到了非常关键的作用，然而，在计算机网络发展的同时，网络安全漏洞问题也对信息数据的安全性造成了很大的影响，不法分子利用这些问题，盗用和损毁用户的信息及数据，给用户带来了很大的损失，在这种情况下，必须加强对网络安全问题的关注，全面考虑计算机网络安全漏洞问题，并对其进行计算机网络信息系统的维护及网络安全漏洞的处理。

1 计算机信息系统维护和安全漏洞管理的必要性

利用计算机信息技术，可以提高人类日常生活的便捷程度，并在一定程度上带动社会生产效益的提高。除此之外，信息技术的使用，也会带动社会企业效益的提高。在人类经济社会各个领域中，运用计算机信息技术可以全面地体现互联网信息技术的优越性，从而更好地配合电子商务和企业电子办公功能建设，推动社会经济的发展进步。当前，社会经济的发展和日常的生产生活都与计算机网络技术密切相关，但是，运用计算机网络技术在给人们提供便利的同时，也严重危害着使用者的切身利益。计算机的开放性较强，使得在计算机的运营过程中，安全漏洞的问题时有发生，如果没有及时解决网络信息泄露问题，将影响计算机内部信息资料的使用安全，甚至造成内部信息系统数据遭到修改或窃取，因此需要采取合理的措施处理内部安全漏洞问题，保证计算机运营的稳定性，保障计算机应用的安全与便捷[1]。

2 安全维护中对计算机安全技术使用的影响因素

2.1 计算机网络因素

首先，内部网络组织因素的影响主要表现在拓扑结构上。在一些企业的日常管理中，内部网络的拓扑结构具有星型、环型和总线型交叉使用的不同特点。为了提高计算机网络不同拓扑结构之间的通信效果，对内部网络安全结构进行了调整，以减少网络安全技术应用的影响。其次，网络协议因素的影响主要体现在网络兼容性上。一些计算机网络使用用户来降低使用网络的成本。通常在已经建成的网络结构中进行互联、互通等操作。基于此，厂商逐渐完善了网络协议的统一运行标准，一方面是为了获取更高的利润空间，另一方面是为了增加保护计算机网络安全的风险。最后，宿主因素的影响主要体现在其成分的多样性上。由于区域内互操作性，主机类型和不同操作系统存在较大差异，很容易加剧内部安全威胁和冲突。

2.2 计算机用户因素

计算机用户因素对网络安全技术使用的影响主要表现在两个方面：一方面，随着社会计算机网络需求的快速增长，网络用户规模和数量不断增加。但是，对用户权益的保护不够，很容易导致网络安全风险增加，对技术的使用产生不利影响。此外，一些互联网用户缺乏安全信息。工业网络管理员的缺失加剧了计算机网络内部用户与安全技术使用之间的矛盾。

2.3 计算机黑客因素

由于现代科学技术的影响，我国出现了各种类型的计算机网络技术病毒。此外，他的攻击隐蔽性还在增加。然而，我国缺乏开发网络安全技术软件的主动性，导致工作效率降低，网络反黑客能力不足，严重限制了我国网络安全技术的应用效果[2]。

3 计算机信息系统维护策略

3.1 信息采集维护

数据收集对于电子计算机非常重要，是系统正常运行的先决条件。如果采集数据有问题，下一步就不正常了，应该改正。数据采集和存储可以提高数据采集的准确性，在一定程度上提高系统维护的效率。当收集到的

信息详细而准确时，维护变得越来越重要。为保证信息的真实性，首先要确定客户的真实身份，以确定信息的来源是否可靠。只有这样才能验证数据本身的安全性，让计算机保持健康。要想提高数据采集过程的效率，就需要提取各种合理的数据信息，去除不必要的数据数据，使计算机更准确、更准确地求解各种数据数据。

3.2 信息处理维护

信息处理接口是信息系统的基础。计算机可以广泛应用于生活的各个领域，最主要的是它自身的数据处理功能。它们能够以人脑无法比拟的极高处理速度处理和加工不同类型的信息。提高计算机的处理速度对于维护和改进信息处理电路尤为重要。信息处理对所有系统软件都有非常重要的影响。因此，如果采取有效措施提高其性能，数据处理就会容易得多。信息处理的关键是个体数据的收集和整合，必须使用编程语言进行，编程语言本身必须保证严格稳定的语言表达[3]。

3.3 维护信息储存

计算机有很强的存储能力，计算机把资料资料存入记忆体，记忆体的种类可划分为唯读记忆体与读取记忆体。所谓唯读存储器，就是只能读取存储器中的数据信息，不能将数据信息写入存储器中的存储装置。“读/写内存”意味着内存不但可以从内存中读出，而且可以向内存中写入。ROM与 ROM以其储存的能力而区分，二者都有各自的优点。

3.4 维护信息传输

在计算机信息系统运作的过程中，信息传输是非常关键的一个步骤，在传递信息时，会受到网络状况的影响，因此，网络信号的稳定程度可以在一定程度上对信息传递的精度产生影响，因此，有关工作人员要对计算机信息系统的传输功能进行维护。互联网的主要形态有两种：局域网和广域网，互联网为计算机的资讯传递提供了便利，没有一个稳固的网路，计算机的资讯传递就会变得不顺畅。

4 主要的计算机网络安全漏洞

众所周知，互联网是一个没有任何控制机构的开放的平台，因此，黑客往往会入侵到互联网上的计算机系统，而黑客的入侵不仅会偷走保密资料，侵犯权限，还会对重要资料造成损坏，严重的话，还会导致计算机系统不能正常工作，最终导致计算机系统瘫痪。此外，目前互联网上的数据传送都是以TCP/IP通讯为基础的，而在TCP/IP通讯中又缺少相应的防护机制。另外，互联网上大部分的通讯服务都是基于Unix的，其所具有的显著的安全性缺陷将会对网络的安全性提供直接的影响。以“永恒之蓝”为媒介的黑客程序，不但扩散迅速，而且主动，可以自动搜索并感染存在安全缺陷的计算机，使其自动感染；如今的网络攻击已经不仅仅局限于广域网，而是在一个相对密闭的区域内进行二次传播。在信息技术日益普及和普及的今天，信息技术的应用越来越多，信息技术的应用越来越广泛，信息技术的应用越来越广泛。这次敲诈勒索的大范围暴发，也给网民们敲响了警钟，不仅要给自己的计算机操作系统打上了一个“补丁”，还要提高自己对互联网的保护和保护的认识。根据有关报告，现在中国的互联网用户数量已经突破了九亿，而在这些用户中，青少年用户占了近五分之一。网络借贷，相亲诈骗，过度打赏，对未成年人和他们的家人造成了极大的伤害。有关部门要强化对互联网信息、网络服务提供商的监管力度，还应该积极地指导行业自律，主动地履行自己的社会责任，创造一个安全网络环境[4]。

5 降低计算机网络安全漏洞的对策

5.1 系统补丁的安装

在防止计算机系统出现安全问题时，加载补丁是一种行之有效的方法。计算机用户可以在自己的计算机上打上补丁，这样的方法在防止计算机受到攻击方面具有很大的实用价值。但是在安装系统补丁的时候，要注意及时的升级系统补丁的版本，一旦发现了新的系统漏洞，就可以使用安全杀毒软件进行安装。从而可以有效地防止计算机网路中的安全性缺陷的产生。

5.2 加强计算机网络访问控制管理

建立起一套科学的计算机网路存取控制系统，可以有效地避免计算机网路的存取控制系统。在阅读材料之前，需要登陆进入系统，并填写相关的账户和密码，在经过了材料审核之后，才可以进入。目前，在计算机网络信息操作的环境中，存在着相对较高的复杂性，因此，在进行相关的计算机网络访问控制工作时，需要采取如下措施，首先要建立一套对计算机网路存取管制的科学体系。其次，在登陆该系统时，需要工作人员先登记登陆帐号，然后进行相关的设定。

5.3 系统与防火墙

因为计算机系统本身就有升级的能力，所以可以根据使用者所设置的时间来进行自我检测，并对是否有必要进行升级进行分析，如果有必要的话，那么系统就会自动地下载补丁，并进行升级和安装，从而对系统中的缺陷进行修补。防火墙是一种非常重要的计算机安全保护手段，它会对外界的访问进行控制，当外界的网络对主系统进行访问时，它会自动关闭其它的系统，使计

算机中的病毒运转变得更小，如果有一些特别的访问需要，它会进行自动的拦截，从而减少非法的入侵。依赖于数据包信息过滤的方法，对信息和数据包进行了界定，并根据有关规则，对数据包能否进入进行了分析，如果数据包的内容不符合规则，那么就会被自动抛弃。此外，该系统与该防火墙也会在某种程度上对该内部与该外部的资源的存取加以限制[5]。

5.4 目录级与属性

目录级控制是一种对用户的访问进行控制的方法，它可以让用户根据目录来对文件的使用权限进行限制，从而保证了访问的安全，当用户打开了权限之后，他可以通过任何一种形式来访问目标的内容，从而保证了工作的高效，同时还可以在这个过程中对资源的访问进行控制，保证了网络系统的安全。属性安全控制是以用户应用文件为基础，有条理地对资源接入属性产生权限效果，并对其进行分配。这种方法具有很好的完整性和机密性，具有很高的安全性。

5.5 设置不同的密码

密码技术可对数据信息进行密码管理，有效控制了应用的登录权限，并促进了安全性的提高。使用者将重要个人信息进行秘密设置，并设定必须在获得访问授权后才可使用，能有效减少个人信息的泄露概率。许多人在进行计算机密码设定时，其密码往往比较简单，而即使计算机密码设置得较为复杂，但没有养成定时修改计算机密码的习惯，这导致计算机问题和安全隐患越来越多。一般情况下，使用者在设定计算机密码时，可选择字母与数字相结合的方式，不建议选择简单的字母或者数字设置计算机密码。在日常的生产生活工作中，一些威胁者往往会使用各类技术手段破解计算机密码，而计算机使用者更要想办法对此类现象的出现做出合理的规避，通常可以通过提高密码设定的复杂度并对计算机密码定期定时修改来实现。如此，即使计算机系统遭到攻击者的破解入侵或是计算机系统信息被泄露，对计算机用户造成的损失也十分有限。

5.6 数据备份

在新时代下，人们的工作、生活方式都有了很大的改变，依靠网络办公是一种习惯，把工作材料、学习材料存放在计算机上，可以减轻文字存储的负担。为避免用户的关键信息被删除，计算机会让使用者对关键的数据信息进行备份，对关键的文件进行备份，在被病毒攻击时，可以让计算机重新设置系统，对先前的备份的数据信息进行还原，唯有如此，才能将损害降低到最低程度。假如没有对计算机进行数据备份，那么当计算机被病毒的攻击后，就会导致整个系统陷入瘫痪状态，当系统处于瘫痪状态，不能运行的时候，所有的数据信息都会被失去，即使是现在重装的系统数据信息也不能进行恢复，所以，使用者要对数据备份的重要性给予足够的重视。计算机工程师可以开发一种资料备份系统，指导使用者做资料备份，使资料备份变成一种习惯，不再是一种负担。可能一些使用者会认为，数据备份会增加计算机的存储负荷，但事实上，数据备份所占据的计算机的空间非常少，而且对计算机的操作并不会造成任何影响，因此，使用者应当权衡一下数据备份的利害关系，最终可以发现，进行数据备份的益处要远大于弊端[6]。

6 结束语

总之，在网络的安全性保护中，合理地使用计算机安全技术，可以改善网络的安全性；同时也帮助业内有关人士对企业的安全工作进行了优化；同时，也是对计算机科技进行长期、可持续发展的战略规划。上述文章也将从企业在进行网络安全维修时所面临的计算机网络安全问题入手，针对实际情况和需求进行更加细致的分析。从企业内部网络安全审计自动化，杀毒软件，企业信息加密技术，黑客攻防术等四个角度，论述了计算机网络安全技术的具体运用方法。

参考文献

[1]任高明.计算机信息系统维护与网络安全漏洞处理方法[J].信息记录材料,2020,21(07):183-184.

[2]王懿嘉.计算机信息系统维护与网络安全漏洞处理策略分析[J].无线互联科技,2020,17(10):20-21.

[3]徐磊.医院信息管理系统中的网络安全管理与维护策略[J].网络安全技术与应用,2020(02):111-112.

[4]于志刚.网络安全对公共安全、国家安全的嵌入态势和应对策略[J].法学论坛,2020,29(06):5-19.

[5]计算技术与计算机及网络设备[J].电子科技文摘,2020,(06):86-149.

[6]张莎莉，洪月，韩柳.计算机信息管理技术在维护网络安全中的应用策略探究[J].中国新通信，2020，021（008）：144-145.