Exploration of Engineering Technology, 工程技术探索(20)2023, 5
ISSN:2737-4114(Print) 2705-1242 (Online)

计算机工程的安全隐患及维护方案研究

黄文德

身份证： 440824197011175016 广东 湛江市 524000

【摘 要】当前，我国的经济发展迅速，同时也助推了科学技术的发展，特别是计算机工程的发展。在计算机工程中，涵盖着信息安全技术，无线网络技术以及互联网视觉等领域的内容，发展的速度很快。但在发展过程中，计算机工程的安全也面临着一系列的问题，在如今这个数据时代，保护好计算机工程的安全是非常重要的。文章对计算机工程的安全以及维护计算机安全的意义进行了简要的介绍，着重阐述了目前可采用的维护计算机安全的一些措施。

【关键词】计算机工程；安全隐患；维护方案

在目前的社会发展过程中，计算机在社会的生产生活过程中扮演着重要的角色，计算机工程广泛的应用在金融行业、医疗行业以及教育等等多个行业的发展过程中，因此，计算机工程的安全问题对于社会发展来说非常重要。计算机工程的安全维护是一项比较复杂的工程，在计算机工程施工开始时，就需要对可能存在的安全隐患进行排除，并制定好安全维护方案，确保计算机工程在运行过程中是安全的，同时也能够更好的保障生产效率，使得计算机工程能够更好的服务于社会的发展。

1 计算机工程安全的概念

计算机工程的安全，其实本质上就是指网络安全，在进行维护时，可以通过一些管理方式与相应的技术手段，确保在计算机工程运行过程中所用到的各种资源不会被外界所侵害，能够保障计算机的软件和硬件的安全，从而达到工程中的信息数据，是有绝对的安全性和完整性的。主要包括两个方面的安全，其中一方面就是物理安全，是指计算机的硬件不会受到损伤和破坏，另一方面就是逻辑安全，即计算机内部所涉及到的一些算法、程序以及数据等不会泄露，那么通过一些技术来有针对性的维护计算机工程的物理安全和逻辑安全，就能够极大的避免在计算机的运用过程中出现数据信息被窃取、修改和破坏的情况出现。在数据时代，计算机的安全非常重要，稍有不慎就可能会对用户造成极大的损失。所以要想让计算机发挥其作用，首先就要保障计算机的安全，有了这个基础之后，才能够充分的发挥出计算机的作用，真正的提升生产效率，方便日常生活。

2 维护计算机工程安全的必要性

当前，计算机工程已经广泛的应用在社会的生产过程以及人们的日常生活之中了，计算机安全稳定的运行，能够使得工作生产的效率得到提升，就比如说在医疗行业，原本需要手写的病历单，现在用电子病历单取而代之，同时还能够随时调取出来对病人的既往史进行查看，以便于医生能够更加全面的掌握患者的病情，假如没有计算机的应用，可能还需要对患者进行一系列的询问，带来很多不方便，还有可能因此错过最佳的治疗时间。所以计算机在各个行业的发展过程中都发挥着极其重要的作用，推动了各个行业的发展。在计算机工程的设计和运行过程中，计算机软件是一个非常重要的工具载体，对于这些软件的维护能够更好的满足不同用户的各种需求。

3 计算机工程存在的一些安全隐患

3.1 计算机本身对计算机工程安全的影响

对于计算机系统本身以及其所使用的各种软件来说，都或多或少的存在着一定的漏洞，即便系统一直在进行修复更新，存在的漏洞也不能做到完全消除，而这些计算机本身存在的漏洞，就是病毒或是黑客侵入的大门。比如，一些非法的用户想要通过攻击计算机系统中存在的漏洞来入侵计算机，以达成某种目的，就会通过协议上存在的漏洞来作为突破口，非法获取系统的管理权限，进而窃取计算机系统中的数据等，从而造成破坏。同时黑客还可以借助缓冲区漏洞和口令漏洞对计算机进行攻击，对缓冲区漏洞进行攻击时，其基本的原理是，向计算机本身存在的缓冲区漏洞发送过强的指令，超过计算机的处理极限，使得计算机系统的运行速度变慢，更严重的还会直接使整个计算机系统瘫痪，然后趁虚而入。针对计算机的口令漏洞进行攻击时，则是直接强行的破译计算机的网络口令，完成整个系统的入侵。

3.2 自然因素对计算机工程安全的影响

计算机工程能够安全稳定的运行，主要依靠先进的信息化技术，以及智能化的计算机系统，但信息化技术和智能化系统是否能够正常的运行，就取决于组成计算机的一些基础设备，比如说计算机主机，显示屏，硬盘等。这些基础设备在使用过程中，如果外界发生自然灾害，或是因为自然因素导致这些基础设备不能够正常运

行时，同样也会影响到整个计算机工程的安全性。比如说遇到地震、泥石流等自然灾害时，计算机的一些基础设施一定会受到损害，那么就无法支持计算机工程的正常运行，如果长期无法修复，还可能会造成更多无法挽回的损失。所以自然因素通过影响到计算机的基础设施，进而影响到整个计算机工程的安全。

3.3 网络病毒入侵

计算机病毒的类型有很多，同样也可以通过计算机本身存在的一些漏洞进行入侵，导致计算机的软件受到一定的损伤，从而使得整个系统的运行速度提升不上去，出现运行缓慢、卡顿等问题。那么这些网络病毒，可能会在用户下载非正规软件，浏览一些不良网站时进行入侵，对计算机工程的安全带来极大的安全隐患。

3.4 竞争对手恶意破坏

在计算机工程行业的发展过程中，随着社会经济的不断发展，市场的竞争也越来越激烈，会有企业为了追求经济利益不顾竞争规则，对竞争对手的计算机工程进行恶意的破坏，比如，在网络上散布虚假的信息引起恐慌，对网站的信息进行恶意的篡改，以及对信息进行截获等等，严重的影响到了计算机工程的正常运行，使得计算机工程无法确保其运行的安全性，造成了经济上的损失。

4 计算机工程的安全维护措施探讨

4.1 完善计算机病毒防御机制

企业要建立起计算机病毒防御的机制，这是保护计算机工程安全的一道重要的屏障。要在计算机系统中引导用户养成正确上网的习惯，加强对计算机病毒的防范意识，对一些不良的信息网站，拒绝点进去浏览，以免给病毒留下可乘之机。其次，在选择防御软件时，要给用户推送一些正规的杀毒软件和防火墙，对计算机系统定期进行垃圾清理，病毒查杀，以及构建起防御体系等，确保系统能够持续稳定的运行。同时，在一些软件的应用过程中，加强软件应用的规范性，使用户能够进行规范操作，以免病毒入侵，导致数据信息的泄露。

4.2 加强访问控制与数据加密处理

对用户的访问进行控制，就需要对用户的身份进行验证，以此来保障计算机工程的安全，需要注意的是，在对用户进行识别的过程中要讲究识别的准确率和速度，以免影响到用户的体验感。还需要通过访问的控制技术，来对用户的访问权限进行限制，有效避免一些非法用户进入系统对系统内部信息进行访问，这能够在很大程度上保护计算机工程数据信息的安全性和保密性。同时，对于一些关键性的数据，要对其进行加密处理，避免数据在发送过程中，传输过程中或是下载过程中被有心之人窃取，为数据的安全再建立起一道屏障，只有通过正确输入特定的密钥，才能够对数据包进行解密，进而查看具体的数据内容，有力的保障了数据的安全性和保密性。

4.3 减少及优化系统硬盘所存储的程序数量

计算机是应用程序安装运行的重要载体，会影响到系统的软件是否能够正常并安全的运行。如果在计算机的系统硬盘上安装大量的程序，会加重系统运行的负担，导致系统运行的速度降低，出现卡顿、死机的情况。所以，要想保障计算机工程的运行效率，就需要控制在系统硬盘上所安装的程序和软件的数量，为系统的运行留下充足的空间。必要时，还可以进行系统的重装，进一步优化空间，以此来提升计算机的运行速度。

4.4 建立黑客攻击防御措施

对于黑客的攻击，同样需要建立起防御措施，进一步加强防御技术的研究。首先，需要应用的就是过滤技术，对数据的传输过程进行跟踪分析，对数据的危险性进行分析并上报处理，避免出现一些垃圾数据从而影响到整个系统的运行。还有应用代理技术，就是当外界数据进入到系统中时，该技术同样会根据预先设定好的协议内容，对数据的风险性进行评估，以此来判断数据是否有危害，从而确保计算机工程的安全性。还有一项技术就是监视技术，即通过分析一部分数据，对网络通信的不同层次进行检测，来达到有效抵御黑客攻击的效果，降低可能会带来的安全危害，提升计算机网络工程运行的安全与稳定。

4.5 提升相关技术水平

为了进一步提升计算机工程的质量和计算机工程的安全，还需要对计算机工程中所用到的一些技术进一步的进行研究，主要涉及到防火墙技术、VPN 技术以及入侵检测技术等。基本上大部分用户都使用过防火墙技术，该项技术就是借助一些杀毒软件，在使用过程中进行病毒监测，一旦发现有病毒入侵的情况，就可以及时、尽早地发出报警的信号，进而采取相应的措施进行防御或解决已经存在的问题，尽力保障计算机工程的安全。而 VPN 技术的重点就在于对数据的传输进一步的进行加密，保障工程的安全性。

4.6 完善安全管理制度，提升网络管理规范性

要想使得计算机工程的安全得到充分保障就必须要规划制定出科学有效的安全管理制度，安全管理制度

可以让计算机内部持续地进行正常运行，同时规范了计算机管理人员的操作步骤和行为，确保了相关人员可以在规定的情况下进行工作，有利于提高整个计算机工程的效率和安全性。一般来说，相关人员在进行制度建立的时候应当重点关注以下几个方面，首先，设置专业的计算机安全管理单位，计算机的安全管理需要健全和专业的管理单位进行规范化处理，所以说计算机安全管理单位对于整个计算机正常运行起到了十分关键的影响。其次，设置专业知识丰富的监督人员，根据过去的情况来看计算机管理监督方面存在很大的缺陷，同时对于比较危险和长期存在的问题都没有妥善处理，这就会导致很多潜在的风险，所以设置专业人员是十分必要的，可以充分减少不良因素对计算机工程造成的损害，从而提升计算机的运行效率。最后，确立系统管理制度，系统管理制度的目标是使得管理人员和操作人员明确责任划分，提高他们的责任意识，以便于建立良好的工作环境同时做好责任追溯。

4.7 优化升级漏洞扫描技术

一般情况下，安全漏洞问题是网络工程运行安全问题中最为突出的问题，漏洞扫描技术正是解决网络漏洞问题的关键手段，使用这种技术就能够迅速扫描出计算机工程中可能出现的安全漏洞，对网络工程的安全工作做出了重要的保障，有效地降低了计算机被损坏的可能性。漏洞扫描技术的原理主要是对计算机端口进行对比并及时检测出异常的端口，然后进行问题的处理。因此，计算机的维护人员应当按照规定对端口进行检测，充分利用漏洞扫描技术，发现漏洞并及时解决，降低受到损害的风险，维护计算机工程的正常运作。此外，相关人员也需要注意非法入侵的途径，及时发现并拦截。

5 结束语

综上所述，随着时代的不断进步，计算机工程也得到了飞速发展，对于计算机工程的安全维护就显得十分关键。目前，计算机工程还存在着一些安全隐患，当认识到计算机工程对于现代社会的生产生活的重要意义后，就需要采取一些应对措施来进一步的保障计算机工程的安全性，只有不断发展新技术，完善防御措施，才能使得计算机发挥最大作用，在应用过程中能够保证其系统内部数据的安全性，提升生产效率，提高生活水平。

【参考文献】

[1]张杰.试述计算机网络工程存在的安全问题与应对措施[J].赢未来，2017，000（017）：P.372-372.

[2]王喆.计算机软件工程的维护措施和方法研究[J].信息与电脑（理论版），2020，460（18）：94-96.

[3]刘子恒.探究计算机软件工程的维护措施与方法[J].网络安全技术与应用，2020，230（02）：53-54.

[4]王子墨.计算机网络安全管理工作的维护措施探析[J].数码设计.2019，008（013）：P.8-8.