计算机数据安全的有效防护措施

岳熙恒
（河南经贸职业学院，河南 郑州 450000）

摘 要：计算机技术的不断发展，为了保证计算机数据安全，需要重视结合计算机技术发展实际，科学的制定更加完善的数据安全防护方案，有效的为数据安全管理工作开展提供技术保证。本文在实践研究过程，总结了计算机数据安全的整体情况，分析了安全问题来源与应用对策。

关键词：计算机；数据安全；防护
【DOI】10.12231/j.issn.1000-8772.2021.05.130

1 引言

在计算机数据安全管理过程中，技术人员应深入工作实际，有针对性的制定更加完善的数据安全管理模式，从而全方面加强数据安全防范水平，有效的为数据安全管理工作开展奠定基础。下面结合具体实际，科学的总结提高计算机数据安全的措施。

2 计算机数据安全的整体情况

计算机数据安全与计算机网络紧密关联，计算机网络包含网络硬件、网络操作系统和网络应用程序。数据的载体是计算机的网络硬件，分载体是应用程序，操作系统主要用来实现数据管控。计算机的运行离不开数据传输，数据网络中充斥着大量的数据传输来维持计算机工作。因此，维护计算机的安全，主要是维护网络数据的安全，防止数据被盗用和网络欺诈行为发生，在各个环节都不能放松，有效保障数据安全防护。注重计算机数据安全主要有三个方面：第一，在计算机处于数据处理的阶段，要防止非法程序的入侵，避免计算机本身的硬件故障造成的数据信息损失；第二阶段是数据传输阶段，要保障数据传统的及时性和安全性，使计算机稳定运行，不会出现各项服务中的指定失误，不受外来指令的影响，保证数据本身的准确性和数据的私密性；第三阶段是数据存储阶段，数据被存储在计算机的数据库内，要严格做好保护和保密措施，将数据信息设置成仅被部分用户读取，同时要防止非用户强制解码，进一步做好防护措施。

3 计算机数据安全问题的来源

3.1 计算机网络的安全漏洞

处理数据中的计算机操作系统容量是固定的，因此在对多元和多重数据处理时，鉴于数据本身特点，计算机在根据对应 IP 传输数据的时候，几乎无法一次性管理很多目标，和处理不同路径的数据。算法优化也并不能解决该问题，因此容易出现安全漏洞。这种安全漏洞，就是黑客和不良分子入侵系统毒害系统的契机，同时安全漏洞正是由于数据处理的算法在较多目标数据中产生的，不好规避，因此数据安全问题的一个重要来源就是计算机网络的安全漏洞。

3.2 计算机网络中的各种病毒

木马，我们最初熟知的病毒名词，用户在使用计算机传输和存储数据的过程中极容易代入病毒。由于计算机的各个存储位置数据是可以共享的，因此在传输数据的过程中，很多文件夹因为病毒文件数据携带破坏数据的代码。病毒通过共享通道传播，对计算机中的所有数据造成影响，甚至会导致数据的损坏和丢失。而且不同病毒的查杀情况也不同，有少数即使被清除后仍会留下痕迹的现象。

3.3 计算机故障

如计算机出现硬盘损坏等硬件问题，数据载体设备则无法正常运行。计算机本身电压不稳出现异常，数据系统也会随之受到不同程度的影响。如果非自带电源计算机系统断电，数据也会瞬间丢失。所以计算机本身硬件故障和人员操作故障，都会直接影响计算机数据的安全。

4 计算机数据安全的有效防护措施

4.1 提高控制访问对象的权限

要设置成计算机指定的合格用户使用者才有权访问计算机中的数据，提高控制访问对象的权限。设置成计算机的固定操作用户使用，可以设计计算机用户名基础验证，同时加深优化验证程序，设置多重验证指令和连环验证方式，甚至采用针对个人特殊的验证指令。在用户权限设置程序中，权限的要求也要更加仔细，防止漏洞发生危及数据安全。通常操作最多的方式是在控制面板中设置用户名和密码，虽然防控有限，但能够有效保障计算机基础安全，提高控制访问对象的权限很有必要。

4.2 强化计算机数据加密措施

针对重要性强的数据信息，要强化加密措施，有效保障计算机数据的安全性。计算机数据信息种类繁多，加密方式也要五花八门，才能有效保证数据的高级安全。数据在计算机中是以代码的形式出现的，加密后的数据信息将以二重代码的形式被隐藏，数据文件的职能会被计算机以解码方式来识别，黑客入侵或病毒引入计算机的时候瞬间突破计算机防线，即使接触到保密信息但也实现不了对加密信息的检索，保障数据安全。由于计算机代码和算法的不断发展优化，文件加密技能也得到了一定程度提升，一项重要的加密技术——微机芯片，被普及使用。保障数据安全的重要策略就是要用高科技技术手段强化数据加密措施。

4.3 加设防火墙并使用安全防护系统

在计算机数据安全领域，防火墙是一项十分重要的安全技术，能够提升计算机内存储数据的安全性。计算机防护系统其实有很多，一方面要将病毒隔离在计算机之外，另一方面要利用安全防护系统的软件来实现系统数据处理过程中的修复功能，防止漏洞发生。除此之外，软件还能够对病毒实行查杀监控，提供强大的数据维护功能。计算机的某些端口，用于下载及上传文件，同时也通过各种类型的病毒，安全防护系统能够监测出端口位置并随之关闭，有效阻止病毒对计算机通道的入侵。目前市场上的腾讯管家、360 管家和金山毒霸等大厂家品牌的软件都很强大，对系统的安全防范能力很强，能够全面防护病毒和修复漏洞，还能够清除恶意代码，要合理而有针对性的选用。

4.4 完善计算机数据安全以及网络安全的监督体制

不规范的网站通常携带恶意代码，或者使用计算机人员的操作不当，都有可能为计算机带来病毒。相关部门需要通力配合，来完善计算机安全机制和保障网络安全监督体制，集体和个人都要遵守强有力的监督体制，保障计算机内的数据安全。互联网中恶意植入病毒和窃取信息是违法的，要做到违法必究，严肃对待网络犯罪，严厉打击违法行为。建立完善的监督和惩治体系，降低网络风险带来的数据安全损失。

5 结束语

在计算机领域，数据安全管理工作是提高计算机技术应用水平的重要部分，如何保证数据安全需要结合有效的技术方法，科学的开展数据安全防范工作，从而不断提高计算机数据管理效率，通过以上分析，从多方面进行了实践探索，希望分析能加强研究能力。

参考文献

[1]王淳.计算机办公信息系统中数据加密防范研究[J].湖北农机化，2020(01)：136-137.
[2]蒋燕翔，潘育勤.云计算技术在计算机数据处理中的应用[J].软件，2020,41(01)：255-257.
[3]刘婷婷.计算机数据安全的有效防护措施[J].卫星电视与宽带多媒体，2019(23)：20-21.
[4]袁臣.大数据时代计算机网络安全的有效防护研究[J].现代信息科技，2019,3(20)：164-165.