大数据背景下计算机信息安全及防护措施分析

赵大鹏
（河南职业技术学院　河南郑州　450046）

【摘　要】大数据背景下信息技术的发展是非常快的，这使得人们在信息共享以及收集和整合方面获得了较大的便利，信息技术对人们的生活和生产起到了很大的帮助，但是网络技术的普遍应用，也导致出现了很多安全问题。本文对各项网络信息安全存在的问题做了详细分析，并针对这些问题提出了一些安全防护措施的建议。

【关键词】大数据；安全防护；计算机网络；信息通信；措施
DOI: 10.18686/jyyxx.v2i4.33426

大数据背景下，智能技术的快速发展以及计算机技术在各行业领域的普遍应用，使人们的信息传递、共享、收集和获取得到了很大的便利，然而计算机在成为人们较为依赖的生活的一部分的同时，人们储存信息、办公、浏览信息以及查找资料所需的时间更多，留下的个人信息和浏览记录也更多，这些信息一旦被不法分子获取，就会给用户造成很大的财产损失，严重的情况，还会对人身安全造成威胁。因此本文对计算机的各种安全问题进行分析，并对这些问题提出了优化方案，以及能够对用户安全起到帮助。

1 大数据背景下计算机安全防护潜在威胁

在当前的高等院校教学中，计算机安全防护方面的教育教学，在很大程度上受到了大数据时代背景的影响。当前阶段面临的计算机安全威胁较之前有了大幅度增加，给高等院校的计算机安全防护效果带来了不小的挑战。这些挑战通常来自于三个方面：①外部环境方面，一些校内人员由于个人原因，对火灾以及水灾的防范措施没有做到位，导致各种计算机软硬件受到破坏；②计算机自身的系统配置方面，很多高职院校的计算机存在较大的系统漏洞，很容易就会被病毒或者黑客入侵，轻则数据被篡改，重则关健信息被黑客所盗取，威胁到用户安全；③安全意识方面，人们使用计算机已经经历很长时间了，很多高校的管理人员安全意识越来越淡薄，特别是面临大数据时代的挑战，他们大多没有较好的认识，在计算机安全管理过程中没有及时更新观念，没有强化安全防护意识，使当前计算机安全防护能力越来越弱。

2 大数据背景下安全隐患方面的问题

2.1 信息维护意识淡薄

通常在计算机网络的使用过程中，很多人只关心能否能找到自己所需要的网络资源和有效信息，而在查询到信息之后，也不会清理各种浏览痕迹，甚至不会考虑自己计算机中所遗留的身份信息是否具有安全隐患，更不会考虑这些安全隐患是否会对自己的生活和工作造成不利影响。在一些计算机软件的使用过程中，刚刚推出的软件往往会存在一些 BUG。但是大部分人没有足够的计算机知识，很多时候只考虑这些软件能否满足使用需求，而不去考虑自己在输入信息时是否会留下安全隐患。如果这些信息被不法分子获取，就会导致用户在某些方面受到损失。

2.2 信息管理不完善

内部专用网络与公共网络相比，前者具有更高的安全性，然而，这两者都是网络组成的信息系统，通常会存在一些网络漏洞。在实际的计算机使用中，很多人出于对内部网络较为放心的心理，使得在网络使用过程中风险意识较弱，在网络操作的过程中也比较随意，这种心理导致他们在安全隐患方面存在很大的疏忽，会产生很多网络安全问题，从而对自身造成极大损害。内部网络通常包括一些企事业单位、家庭以及院校网络，数据泄露问题非常常见，在利益的驱动下，很多员工违背原则，谋取利益，通过自己的职务之便，对企业的各种重要信息进行盗取，倒卖给其他不法人员，部分员工还会将一些内部网络使用权限出卖给黑客，而黑客一旦获取了这些机密信息，并且将这些信息外泄，就可能给企业造成较大的损失。

2.3 网络信息不完善

当前计算机网络信息各项制度还没有完善，相关的立法体系也并不完整，不法人员抓住这些薄弱环节进行非法操作，很多不法人员还会进行团队作案，在违法犯罪人员被抓之后，又可能会因为相关的管理机制不完善，对他们的处罚没有起到实质性的作用，反而助长了他们的嚣张气焰，使得网络信息犯罪规模和数量都不断提升，极大的危害了社会治安。除了网络制度不完善之外，企业的信息安全管理措施也非常的欠缺，很多企业只注重经济效益的增长，而忽略了自身网络的管理和维护，一旦出现问题，就会给企业带来非常沉重的打击。

2.4 网络防火墙

针对网络安全问题研究的防火墙技术，能够快速识别外界的病毒以及其他的各种黑客攻击，并且能够及时地预防。但是当前的各种网络信息技术具有较快的发展速度，新的娱乐软件大量出现，而传统的防火墙更新速度却非常的缓慢，很多时候它对各种信息的保护隔离效果非常的弱，黑客在各种新型的病毒使用过程中能够对防火墙造成很大的危害，使防火墙瘫痪。

3 大数据背景下计算机网络信息安全防范措施

3.1 构建完善的安全防护机制

针对当前计算机面临的各种外部威胁，各高等院校需要不断地提升对大数据技术的应用，在对信息数据进行有效处理的基础上，进行动态的计算机安全问题分析，并对相应的安全防护机制进行完善。在实际的工作中，要充分结合高等院校计算机信息安全需求，建设相应的安全管理机制，强化对软硬件设施的安全管理，完善信息的访问控制机制，加强用户的身份验证，尽可能地避免不法分子入侵用户计算机。完善信息安全响应机制，针对各种安全问题，强化身份识别响应和预警，尽可能有效地控制各种不良影响。

3.2 积极引入先进的安全防护技术

技术革新是计算机安全防护中的重点和难点内容，在大数据背景下，高等院校一定要加强自身的技术革新力量，强化安全防护和监管技术的创新，切实做到对计算机信息安全的保护。在对大数据技术的实际应用中，要进行较为彻底的安全隐患排查，充分结合云计算技术的优势，积极全面地查找漏洞，针对各种类型的计算机信息安全漏洞，制定针对性强的补漏措施，消除可能存在的计算机信息安全问题。同时大力引进声音识别等先进计算机识别技术，将这些先进技术运用在计算机的关键信息防护过程中，特别是对用户登录信息以及账户等方面数据的安全防护，一定要提高防护等级。例如，某高职院校通过引进先进安全防范技术，对各种大数据采用分布式处理办法，对高校自身的防护技术进行强化。

3.3 有效组织计算机安全教育培训

计算机工作人员应该不断强化自身的安全防护能力和意识，这对计算机的信息安全保护会产生较为直接的影响。因此高等院校一方面要不断提升信息安全防护人员的专业能力，针对当前院校计算机安全问题存在的各种漏洞进行专业化的处理；另一方面，院校各教育岗位应该普及计算机安全等方面的培训和教育，通过对院校教职工计算机安全教育和计算机素养的不断强化，来提高教职人员的信息安全防范能力和安全意识，积极地引导他们参与到信息安全防护工作中来。例如，在开展网络信息安全教育的培训过程中，可以选取一些大数据背景下具有代表性的网络安全案例。如“网银被盗案件”“停车场收费系统破坏损失”以及“熊猫烧香主犯获刑”等影响较大的网络安全案例，通过对这些案例的宣传和教育，强化全体教职员工的网络安全意识，让他们更加积极主动地去了解和学习安全防护方面的技能和知识，从而强化从业人员的综合素质。

3.4 提高意识，主动安装杀毒软件

很多时候，计算机网络受到攻击是因为不法人员使用了病毒工具，所以用户应自行下载防病毒软件，并且进行及时地消毒、查毒以及封堵的工作。某些个人电脑上安装的防病毒软件，大部分是针对内部的资源进行杀毒，这些软件能够对病毒资源进行扫描，并且对异常情况进行监测和报告，在病毒被检测出来以后又能够自动清除，这是个人电脑查毒的常规流程。然而随着计算机技术的不断更新，病毒也在不断的增多和优化，使得很多的计算机病毒软件必须要进行定期的更新和优化，才能达到有效预防病毒的目的。

3.5 通过虚拟网络技术的使用来维护安全

在网络安全管理方面，可以通过专用的虚拟网络技术，如人脸智能识别、隧道技术、身份认证密钥技术等来围护网络安全，在网络平台中，无论是使用内部网络还是外部网络，系统都是统一开放的，它的开放性使得很多人都可以共享资源和信息，但是这种方式也在很大程度上带来了信息泄露的风险。因此，各相关的企业管理部门和个人应该对数据信息进行加密，设置相应的管理权限，从而降低数据泄露的风险。各部门可以将内部网络进行分散，采用不同的密码权限进行管理，员工和领导者之间的数据权限应该进行明确的划分，以此来有效地增强网络信息安全。此外，企业和个人都可以定期或不定期的更换服务密码，以提高计算机安全，增强对重要数据的保护。

3.6 对防火墙技术进行优化，提升对计算机的保护

防火墙技术，在每个人的电脑中发挥着防病毒攻击的作用，防火墙能够有效拦截一些外界攻击，提高计算机的安全，同时，这项技术还能够对内部人员的行为进行约束，降低信息被盗取的概率，并且能记录相关的计算机操作，并对一些行为进行判断，一旦出现异常，就会进行防护反应。因此应该推广防火墙的应用，各相关的技术和研发应该及时跟进，使防火墙技术能够适应当代网络信息技术发展的需求。

4 结语

计算机网络信息对人们的生活各个领域的影响，越来越普遍和深入，因此我们应该提高安全意识，个人用户应该主动安装杀毒软件，通过各种专用技术来维护网络信息安全，加强防火墙技术，使其起到对用户信息安全管理的作用，通过这些措施降低人们的网络安全隐患发生的概率，促进网络更加快速、安全、稳定地发展。

作者简介：赵大鹏（1977.11—），男，河南商丘人，硕士，讲师，研究方向：计算机。

【参考文献】

[1] 陈玉霞. 关于计算机网络安全防范措施的探讨 [J]. 科技传播，2014，6（17）：210-211.
[2] 罗云. 网络信息安全的法律问题研究 [D]. 重庆大学，2011.
[3] 龙振华. 大数据时代计算机网络信息安全及防护策略 [J]. 中国管理信息化，2019，22（6）：161-162.