大数据背景下高校网络信息安全与防护探析

陈平波
（南京邮电大学通达学院，江苏 扬州 225127）

摘要：进入大数据时代，人们的工作和学习越来越多地依赖于网络，这对于网络信息的发展来说是机遇与挑战并存的。高校应充分认识到网络信息面临的安全挑战，通过科学的方式方法进行信息防护，提升其安全性，以避免信息的泄露和损毁问题带来的损失。故而，本人从大数据背景下高校网络信息安全隐患入手，对其防护策略进行探讨，以期为促进网络信息安全略尽绵力。

关键词：大数据背景；高校网络信息；计算机安全与防护

在利益的驱使下，大量的恶意攻击和病毒程序存在于计算机网络之中，它们往往会藏身于文件或者正常的运行程序，随时准备对计算机网络发起攻击。随着计算机的广泛应用，越来越多的人开始习惯于将数据和信息储存于计算机网络，以及通过网络获取信息。大数据背景下，高校网络信息安全隐患呈现出时代特点，那么，校方和教师也应顺应时代发展，在网络信息安全防护方面采取更加积极的措施。

一、大数据背景下高校网络信息安全隐患

（一）用户不规范操作

随着计算机的广泛应用，网络中蕴含着海量的数据和信息，由于其上传和使用者的身份复杂，这些数据和信息的安全性是难以保证的，如果用户自身操作不规范，将会给计算机网络安全造成威胁。在不熟悉计算机网络或者网络完全意识的不强的情况下，用户进行操作时难免会出现失误和违规，这些操作会给某些危险性数据入侵用户计算机可乘之机，从而对用户计算机网络数据的完全性和时效性造成影响。

（二）他人主观恶意攻击

根据攻击方式不同，人们习惯于将这些恶意攻击划分为被动攻击和主动攻击两种类型。在计算机用户不知情的状态下，对其计算机网络信息进行截取、破译，以达到为黑客或者不法分子提供机密信息的恶意攻击，被称为被动攻击。

主动攻击则是指，黑客或者不法分子对计算机网络信息的有效性与完整性有选择地进行破坏，其手段多样，令人防不胜防。他人对计算机网络的主观恶意攻击行为，轻则会影响用户对计算机信息网络的正常使用，重则造成国家机密的丢失和泄露，从而直接或者间接地对国家经济、政治造成不利影响。

（三）计算机病毒攻击

自然界的病毒是人类健康的克星，同样的计算机病毒也是威胁计算机网络完全的重要因素。它可以隐身在正常的程序或者数据文件中，待用户启动该程序或者使用该文件夹时入侵计算机系统，并完成多种预设指令，比如窃取数据、删除数据、破坏数据等等。这些行为会给用户造成不可估量的损失，故而，对于技术人员和用户在防范计算机病毒方面作出了巨大努力，并且还将继续努力下去。

（四）自然条件与灾害的威胁

设计师在设计计算机的时候，已经预想过来自环境和灾害的威胁，并利用最新的科技手段为其增强抵御能力，故而随着计算机的不断更新迭代，其对环境的适应性越来越强，但是性能的提升在自然条件与灾害的威胁面前依然显得无力。在天气比较恶劣的情况下，计算机硬件设备的运行难以正常维持。比如，温度的急剧升高、长期湿度过高造成电路被损害之后，计算机稳定性与高效性将会降低，甚至出现数据丢失和信息传输失败的情况。

二、大数据背景下高校网络信息安全防护措施

（一）防火墙加密

防火墙是常用的阻挡他人恶意攻击的有效工具之一，它位于计算机和网络连接之间，对流经它的网络通信进行过滤。

首先，安装防火墙之后，可以通过对恶意攻击进行过滤，有效地阻挡非法用户的入侵，从而防止其对用户信息进行盗取和破坏。

其次，用户还可以利用防火墙对计算机网络的环境进行监测，以提高计算机信息的安全性。

再次，防火墙可以关闭不适用的端口，对木马程序进行拦截，阻止身份不明入侵者的恶意行为。

根据防火墙技术性的差异，人们将其分为包过滤型、代理型、地址转换型、监测型四类。

包过滤型防火墙可以利用分包传输技术判断数据包的地址信息，排除来自数据包的危险性，如果判定某个数据包为不安全，就会阻止用户的访问与下载行为。

代理型防火墙则会对服务器与客户端的信息交流进行隔离，安装这一防火墙之后，客户端并非直接对服务器发出使用数据的请求，而是会首先将这个请求发送给代理服务器，再由代理服务器获取数据并发送给客户端，代理服务器的参与，使得不法分子难以对用户计算机信息进行非法操作。

地址转换型防火墙可以隐藏用户的真实 IP 地址，令非法分子找不到用户计算机的门牌号，使得其即便想对用户进行针对性攻击，也无从下手。

监测型防火墙会实时、主动对计算机数据进行监测以及安全性分析，这种监测和分析渗透于计算机网络的各层数据，大大提高了高校计算机网络安全性。

（二）数字加密

信息数据包的传输过程，给非法分子进行数据拦截创造了机会。利用这一过程，非法分子能够实现对重要数据的篡改和窃取，从而从中牟利。

为了保护计算机网络信息的完整性和安全性，数字加密技术应运而生，其核心就是密钥和密匙。加密算法和密钥共同组成了对计算机信息的加密过程，其中密钥是参与算法实现过程的关键信息。

有时候，根据算法的不同，秘钥会分为私有密钥和公有秘钥，以满足不同的计算机网络信息安全需求。目前来说，基于字符替换的古典密码（算法）已经很少在实际应用中见到，多采取公开密钥算法和对称算法，以提高文件传输的安全性。

在信息安全领域中，数字加密技术发挥着重要作用，它将计算机网络完全保护分为个小目标："进不来""拿不走""看不懂"。高校计算机网络采用数字加密技术，可以在进行信息传输时，利用密匙对其进行数字打码，之后会自动形成密文。当数据被传输到指定的 IP 之后，则可以通过秘钥对密文进行解码，还原出原文信息。

采用这种数字加密技术进行文件传输，能够有效防止非法分子对重要信息的窃取和篡改，因为没有秘钥的帮助，即便他们截取了信息，也没有办法打开密文，强行打开仅能获得一堆乱码，而无法破译出原文信息。

（三）更新病毒库

在防火墙和杀毒软件的共同保卫下，可以更大限度地避免不法分子通过计算机病毒的攻击，窃取资料以及给用户信息造成损害。专业的杀毒软件会在用户获取到数据库信息之前，对其进行扫描，以对计算机病毒进行辨识，对非法访问进行阻隔。

当前常见的计算机病毒一般为木马病毒，根据其核心代码的特点，杀毒软件可以在扫描到靶向程序之后，对用户发出警告，以及将该软件进行隔离处理。通过在计算机连接至网络过程中形成的闲置段端口，同样可以接入计算机进行信息的上传和下载。

故而，如果这些端口如果被劫持，可能会发生信息遭到篡改和盗窃的情况。防火墙与杀毒软件的联合使用，能够对这些闲置端口起到管理作用、对非法访问和计算机病毒起到阻隔作用，从而提高计算机系统的安全性。

（四）防范黑客攻击

黑客可以通过计算机病毒对用户计算机的入侵，实现利益目的。比如，著名的"比特币勒索病毒"就是俄罗斯黑客所制造的一种通过锁定重要文件，威胁用户在规定时间内支付比特币的计算机病毒。如果用户没有在其指定的时间内完成支付，这些被病毒锁定的文件就会被删除掉。无论是哪种选择，都给感染这种病毒的计算机用户带来巨大的损失。

虽然，各大计算机相关的企业和机构，针对该病毒采取了多种积极措施，但是最终只能选择通过修补计算机漏洞的方式防止用户遭受攻击。受到利益的引诱，黑客对计算机的攻击将会持续下去。虽然我们仍然对于高级病毒没有较好的破解办法，但是通过一些安全防范措施，可以抵御 95% 以上的病毒攻击。

目前常用的阻隔黑客攻击的方法有漏洞修复、访问控制、设置防火墙等，这些对计算机网络的保护措施，能够帮助用户有效地降低遭受攻击的频率。对于内部侵袭，高校计算机则可以采用杀毒软件对计算机实际运行情况进行监听和分析，以揪出潜藏在文件和运行程序中的病毒。

（五）优化信息储存环境

随着网络信息问题的日益突出，人们在网络信息储存安全方面的研究投入了大量精力和财力。新型计算机网络信息储存安全技术的推广，对高校网络安全程度的提升起到了促进作用。

管理者可以利用先进的数据储存安全技术，提高网络信息安全系数，防止用户信息被窃取和篡改。例如，利用加密技术可以对信息进行处理，令非法访问的用户即便能够入侵用户计算机窃取数据，也无法获得原文件信息。

其次，高校还可以通过科学防护制度的建立，优化信息的储存环境。在制度层面上，高校可以采取完善网络信息安全管理制度、建立网络信息监督和排查机制、将网络信息责任落实到个人等三个方面措施。

（六）完善设施，提高等级保护级别

为了提升高校网络信息等级保护级别，保障网络系统的软件、硬件、数据的安全性，可以通过完善设施，促进计算机的物理安全、网络拓扑结构安全、系统完全。

首先，在物理安全方面，应根据相应的标准划分安全等级，以及采取相应的安全措施，以保证场地和机房的安全性、防止计算机设备被盗以及被损毁、媒体本身和数据的安全。在整个信息安全系统中，物理安全处于基础地位，高校应努力提升计算机设备和相关设施抵御地震、火灾、水灾、电磁污染等方面的能力，以及减少人为操作失误、错误对计算机物理安全的破坏。

其次，高校还应完善计算机的软件设施，安装防火墙、防毒系统，并将不同的信息集成在同一个安全平台上实行统一管理，从而为网络信息筑起安全屏障，进而提高网络拓扑结构和系统的安全等级。为了确保信息安全等级保护的科学进行，高校可以请具有保测资质的公司，每年为本校计算机进行测评一次，根据专业人士的评估建议进行整改，以保证整改措施的有效进行，切实保证网络信息安全性。

三、结语

总之，大数据背景下，人们在高校网络信息安全方面作出了很多努力。黑客是绝大多数计算机病毒的制造者，对于黑客的防范是高校计算机网络安全保护工作的重中之重。针对计算机病毒的威胁，高校计算机系统可以及时安装和升级杀毒软件，通过更新病毒库，防范新型计算机病毒的入侵，同时在人们使用计算机网络过程中，到处涉及数字加密技术，其最后一道防线——"看不懂"，更是对信息安全的直接保护。

参考文献：

[1] 王晓静 . 大数据下高校网络信息安全与防护 [J]. 电子技术与软件工程，2020（12）.

[2] 付钰，俞艺涵，吴晓平 . 大数据环境下差分隐私保护技术及应用 [J]. 通信学报，2019（10）.

[3] 陈建学，宋维焕 . 大数据下计算机网络信息安全与防护分析 [J]. 信息技术与信息化，2018（05）.

作者简介：陈平波（1976–），男，江苏靖江人，南京邮电大学通达学院保卫处处长兼后勤保卫党支部书记，硕士，助理研究员，研究方向为就业与创业教育研究、安全管理、信息安全、军事教育。