大数据背景下高校网络安全研究及对策

Research and Countermeasures of University Network Security Under the Background of Big Data

王益忠

Yizhong Wang

潍坊科技学院

中国·山东 潍坊 262700

Weifang University of Science and Technology, Weifang, Shandong, 262700, China

【摘　要】在大数据的背景下，很多企业乃至各大高校都有着比较严密的大数据系统。更重要的是，现代教育的发展、高科技技术日益占据着现代教学的重要地位，从而保证学生们对于信息的提取和吸收，以及对于知识兴趣的提升。论文将对大数据下高校的网络安全进行论述，以便鼓励人们更好地去探索相关对策。

【Abstract】In the context of large data, many enterprises and even major universities have relatively rigorous large data systems. More importantly, the development of modern education and high-tech technology are increasingly occupying an important position in modern teaching, so as to ensure that students can extract and absorb information and enhance their interest in knowledge. This paper will discuss the network security of colleges and universities under the big data, in order to encourage people to explore the countermeasures.

【关键词】大数据；高校网络安全；研究和对策

【Keywords】big data; university network security; research and countermeasures

【DOI】10.36012/peti.v1i2.840

1 引言

在当代大数据的背景下，高校的网络安全越来越重要。每个高校都有自己核心的网络技术和教学方法。同样的，每个高校也都会担心本校的网络安全。尤其是当代信息化高速发展，而且由于信息公开和透明化的需要，高校的网络安全成为人们重点研究的现状。中国高校仍旧存在技术不足和核心硬件不足的问题，这些技术的改变刻不容缓。

2 大数据的基本概念

“大数据”这个词的字面意思是拥有大量的数据信息，大数据时代下，数据还具有价值密度低的实际特点，社会上的各种数据信息和各种样本信息种类繁多，使得每一项信息所占的比重也持续降低，甚至会出现数据信息不真实的现象发生，使得大数据信息价值整体相对较低。随着网络信息技术的发展，大数据具有更详细的含义，即强调将单个数据信息集成到系统化和多样化的信息集中。

3 大数据时代中的不安全因素

3.1 自然类灾害

通常人们生活中使用的计算机，都是由各种零件和设备组装成的，但是缺少一定的防御能力，所以在进行运用的过程中，是很容易被一些外部的因素影响，从而导致计算机设备受损[1]。例如，计算机在自然灾害面前是完全没有抵抗力的，同样会出现碰撞、污染等各种情况，如果要是设备不慎进水或者遭遇雷电打击，那么就会被损毁。所以说，计算机设备在大自然面前是非常脆弱的，同时，这也是对信息安全影响的一个重要因素。

3.2 网络的开放性

计算机网络在实际应用中具有开放性的特点，表明计算机网络系统在某种程度上不稳定和脆弱[2]。同时，在网络的开放使用过程中，互联网环境中的 TCP/IP 协议无法反映其自身的安全性，导致网络基础设施设备的安全性不足。结果，在操作期间网络系统的数据处理功能丢失，这将导致计算机网络中出现安全问题。

3.3 黑客攻击

黑客攻击通常是主动的，并且通过以计划的方式攻击目标，目标信息被破坏，失去效果，然后窃取所需的信息，对被攻击方造成伤害。黑客攻击是非常具有破坏性的，将给社会经济带来巨大损失。

3.4 网络操作系统的漏洞和设计的缺陷

操作系统漏洞是指计算机操作系统本身存在的问题或技术缺陷。由于网络协议实现的复杂性，确定操作系统必须具有

各种缺陷和漏洞。网络设计是指拓扑的设计和各种网络设备的选择。网络设备、网络协议、网络操作系统等都直接带来安全风险。

3.5 安全系统缺乏身份认证

对于现代网络安全系统，身份认证是更好地加强自卫能力的最重要的解决方案和技术之一。但是，由于具体技术水平的限制，现有的身份认证系统仍存在许多不确定性和缺陷。因此，丢失数据、信息等的可能性仍然很高。一些网络黑客利用他们的云平台管理器在他们进行恶意攻击时窃取他人的信息，然后使用这些信息登录到其他人的云平台。非法读取和使用数据会导致其他用户丢失信息，最终导致用户严重损失。

4 网络信息安全防护策略

4.1 物理防护

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、故意破坏和线路攻击；加强内部网络管理员和用户的安全意识，这是最简单、最经济的抗病毒方法之一。网络管理员和终端运营商根据自己的职责和权限选择不同的密码，对应用数据进行合法操作，防止用户访问数据和使用网络资源。确保计算机系统具有良好的电磁兼容性工作环境；建立完整的安全管理体系，防止非法进入计算机控制室和各种盗窃和破坏活动。物理安全策略还包括加强网络安全管理，制订相关规章制度，对确保网络安全可靠运行起到非常有效的作用。网络安全管理策略包括：确定安全管理水平和安全管理范围；制订使用网络操作和人员访问计算机房管理系统的规则；制订网络系统的维护系统和应急措施[2]。

4.2 加强防火墙技术科学应用

在大数据时代，应该从基本的保护技术层面考虑计算机网络信息的安全保护，防火墙技术的应用可以有效隔离内部网络和外部网络，并在两个网络之间建立虚拟围栏。它保证了内部网络运行的安全性，可以有效地防止外部网络的入侵。它根据一定的安全策略对两个或多个网络之间传输的数据包（如链路模式）进行检查，以确定是否允许网络之间的通信，并监控网络运行状态。虽然防火墙是目前保护网络免受黑客攻击的有效手段。在防火墙技术的应用下，它可以抵御未知的入侵和非法攻击，并结合计算机网络安全策略，提高整个计算机网络的安全性。计算机网络内部网安全控制，最重要的是通过数据信息的限制，在屏蔽和隔离安全风险信息方面发挥重要作用。防火墙技术的应用也以这种方式使用，以通过隔离和限制来确保内部网的安全性。但也有明显不足：无法通过除防火墙之外的其他方式防范攻击，并且无法阻止来自内部背叛和临时用户的威胁。它也不能完全阻止受感染软件或文件的传输，也无法防止数据驱动的攻击。

4.3 对网络病毒加强防御

网络病毒的征服已逐渐成为现阶段计算机网络安全发展中不可忽视的部分之一。网络病毒在计算机系统中表现出不同的发展特征，病毒甚至可能变异，在入侵阶段甚至难以被完全治愈。在预防网络病毒方面，防御系统的建立逐渐受到关注。计算机系统可以建立安全管理系统，注意病毒预防的各个过程，提高病毒防治质量。控制计算机病毒管理的软件和编码的合理使用可以实现病毒软件产品的刻板印象。为了有效提高病毒防治质量，可以合理地应用和优化计算机病毒控制软件。可以对病毒管理的各种信息资源进行统计，从而提高计算机病毒的防范性能。

4.4 安全加密技术

因为网络入侵者通常会仔细查看并等待目标计算机中的文件或文件夹来存储密码，然后使用专用的破解加密算法程序来解析密码。因此，管理员应养成定期更改密码的习惯，并使用密码破解程序检查存储密码的文件是否安全等，以确保密码在内部网络中的安全性。加密技术的出现保证了全球电子商务的发展，使得基于互联网的电子交易系统成为可能。对称加密是一种传统的基于密码的技术，其中相同的密钥用于加密和解密操作。非对称加密，即加密密钥与解密密钥不同。

4.5 全面了解用户安全和预防

在加强计算机网络安全的过程中，最基本的安全保护措施是系统身份认证，这是网络安全防范的第一道重要防线。不被第三方和黑客识别的用户在其入侵行为中造成了重要障碍。在此基础上，还要培养相关用户防范计算机安全的意识，确保其实施和实施的深度。高级保护关键计算机网络数据和信息的机密性、完整性和一致性，在真正意义上，实现未经授权，非法访问、使用和传播行为，并实施严格的监控措施，以避免过程中可能发生的危害和影响，并在特定的网络环境下实现安全监督。

5 结语

在大数据的背景下，人们必须做好保护网络安全的工作。尤其是对于高校来说，他们的网络安全代表了中国的教育核心思想，所以他们的网络安全防护更是重中之重。人们要做好安全防护这个大的保护罩，才能不断精进技术，促进中国大数据技术的发展，促进高校教育的现代化建设。

参考文献

[1]张涵,孟令涛,杨艳春.大数据背景下大学生网络安全意识现状研究及对策分析——以长清大学城为例[J].无线互联科技,2018(1):33-34.

[2]杨一名.大数据背景下的网络安全与隐私保护研究[J].电脑迷,2017(2):133-134.