大数据时代计算机网络安全体系构建

白永军

（沈阳现代制造服务学校，辽宁 沈阳 110000）

摘要：如今我国已经进入大数据时代，无论是生活还是工作都无法离开计算机信息技术。在大数据为人们生活以及工作带来诸多便利的同时计算机网络安全问题也成了大数据时代急需解决的重要问题之一，这与每位计算机网络用户的切身利益息息相关。因此，本文有必要围绕大数据时代计算机网络安全体系构建展开深入探究与讨论，以期在确保用户安全使用计算机网络的同时对维护社会和谐稳定发挥出积极的重要作用。

关键词：大数据时代；计算机网络；安全体系；构建；有效策略

在大数据浪潮的深刻影响下，人民群众的生活样态、表达习惯、学习方式以及道德观念等都发生着巨大的转变，网络化、自主化以及自由化的特征越来越明显。虽然大数据为人民群众带来了诸多有利影响，但是由此引发的安全隐患接踵而来，不可忽视，因此，构建计算机网络安全体系成为重中之重。在实际工作中，为了顺利达到目的，管理者应从思维、实践等方面着手，引导用户正确理解并且安全使用计算机网络，相信这对提升所有用户的网络安全素养都具有十分重要的意义。

一、大数据时代含义

尤其是近两年，随着互联网经济飞速发展，大数据呈现出来爆炸式、多样化的发展态势，大数据慢慢成为相关人员关注与讨论的中心。从根本上来看，大数据不仅仅体现在数据之大上，其更深层次的内涵在于海量数量的分析、整合、交换以及管理方面，通常其与“大发展”“大利润”“大知识”与“大科技”等关键词有着紧密的内在联系。在大数据时代，人们更加推崇“使用大数据说话”的思维与办事方式，截至目前，大数据已经悄然渗透到医疗、通信、教育、金融等各行各业当中，并且为行业变革与创新带来了崭新的发展机遇。慢慢地，大数据的价值得以彰显，其产生了巨大的社会与经济效应。具体说来，在大数据时代，不管是人或者物都在被数据化，数据呈现出来明显的流动性、开放性与共享性特征，与此同时，越来越多的潜在社会风险慢慢凸显，其中最严重的要数计算机网络安全问题。如何最大限度地发挥出大数据的正面作用，充分利用大数据的思维、技术与方法造福人类，这是当前乃至未来研究的重中之重。

二、大数据时代计算机网络安全概述

当前，网络已经逐步向着大数据时代靠拢，大数据已经在各行各业中发挥出来了独一无二的作用，虽然大数据表现出来了诸多优势，但是其对信息使用埋下的安全隐患仍然不容忽视。尤其随着数据数量的增多，虽然大数据技术能够有效加快信息处理与分析，但是如果没有足够安全的信息防护技术做保障，那么数据泄露的问题可能会频繁发生，最终将对用户隐私造成巨大威胁。由此看来，要想从根本上确保数据信息的准确性，必须制定切实可行的应对方案，尤其应构建完善的计算机网络安全体系。然而，从当前现状出发，现有的网络安全技术难以满足大数据时代的具体要求，特别是目前的互联网安全维护工作还依然存在着诸多不足与漏洞，一方面，这将增加计算机网络的安全风险，另一方面，这也对当前以及未来的计算机网络安全维护工作带来了更大的难度与挑战。因此，结合此种情况，从大数据时代背景出发，做好计算机网络安全设置，构建完善的计算机网络安全体系显得尤为重要。

三、大数据时代计算机网络安全问题分析

（一）计算机网络体系的安全问题

计算机网络具有明显的开放性特征，通常是由 PC、传输介质以及适宜的网络技术协议组合而成。置身于网络中的用户一般都是虚拟且自由的，他们完全可以不使用真实信息，同时，信息内容也不会受到限制。无论是在国内还是国外，计算机网络的连通并不会受到地域的限制，只要有设备，通过协议，便可实现无障碍连通。因此，从以上几点来看，计算机网络体系本身便隐藏着一定的网络安全问题，需要引起重视。

（二）操作系统的安全问题

从本质出发，操作系统属于支撑软件的一种，它的主要作用就是为各种应用系统提供运行环境，一旦操作系统软件在系统开发设计过程中出现不足或者漏洞时便可能会留下潜在的网络安全隐患。以操作系统的网络文件传输为例，如果在远程文件传输时被安装间谍程序，那么用户整个文件传输过程都可能会被黑客监测到，由此引发的一系列问题将会给操作系统带来诸多安全隐患。

（三）数据库的安全问题

很多时候，数据库本身存在着各种各样的漏洞，这也可能对数据库的安全性产生影响，如身份验证不足、备份数据暴露、数据库平台漏洞等。此外，数据库访问者在使用的过程中也可能会引发一系列安全问题，如访问者有意蓄谋出现故意破坏数据库的行为或者未经许可与同意擅自修改或者删除数据库信息等，这些都将对数据库安全造成威胁。

（四）防火墙的安全问题

防火墙是网络的第一道屏障，需要特别强调一点部署了防火墙并不代表着网络绝对安全。尤其处于网络安全漏洞呈现爆炸式增长的今天，如果对防火墙不采取有效的策略，那么其最终很可能成为一种摆设。因此，为了从根本上预防此类问题的发生，网络管理员每当遇到新的网络安全漏洞都应及时更新防火墙安全策略，唯有如此，才能使防火墙的作用最大化。

（五）网络病毒与黑客侵入

网络病毒将会破坏网络数据、用户信息以及网络硬盘，严重时可能会导致系统瘫痪，很多时候，病毒会经过复制之后再次向外传播。黑客会通过向计算机植入黑客程序的方式破坏网络正常通信，以达到窃取信息与入侵系统的目的。不管是网络病毒还是黑客入侵都将对计算网络安全造成严重威胁。

四、大数据时代计算机网络安全体系构建有效策略

（一）加大宣传力度，强化安全防护意识

在大数据时代视域下，之所以诸多计算机网络安全问题显现出来，究其根本原因，主要是因为部分网络管理者或者用户严重

缺乏网络安全防护意识，很多用户在使用网络的过程中并没有进行有效防范，正是因为如此，才让不法分子有了可乘之机。因此，在当前计算机网络安全体系构建的紧要关头，相关人员一定要加大宣传力度，争取让越来越多的网络用户拥有较强的网络安全意识，具体宣传方式可以采用广告、视频、广播等，除了这些传统的宣传方式之外，在大数据时代，相关人员可以充分发挥出来大数据的实际优势以达到宣传的目的。例如，在当前计算机网络使用过程中，从管理者的角度出发，可以依托大数据技术在官方网站或者相关的信息平台上进行网络安全知识的科普，以便让越来越多使用网络的用户深刻认识到安全使用网络的重要性。同时，针对计算机网络的具体使用，随着大数据技术的广泛研发与快速发展，管理人员可以建立对应的安全维护中心。维护中心需要对某一特定区域内计算机网络的使用情况进行追踪与监测，全方位、多角度监测用户使用的某些软件或者系统是否存在一定安全隐患或者问题，这为计算机网络安全体系构建指明了方向，以便制定针对性的防范措施。从网络用户的角度出发，他们在使用计算机网络的过程中能够更好地避免使用外部或者公用网络，以降低安全问题的发生率，也能更好地增强他们安全使用网络的意识。同时，管理者还应不定期地向用户推送与网络安全管理措施以及技术教育相关的内容，用户可以随时随地进行浏览学习，在学习的同时他们的安全意识与防范能力自然而然得以增强。

（二）优化社会环境，加快安全技术研发

在大数据时代背景下，先进的核心技术是法律措施的重要补充。数据服务提供商完全可以充分发挥出现代化科学技术的优势精准识别风险、有效防范网络黑客攻击，以便最大化地提升网络抵御能力。

首先，在国家政策的大力支持下，各类主体需主动积极引进更多在世界范围内享有盛誉的云计算、大数据龙头企业，以便在本土构建完整的大数据产业链，帮助相关企业与产业实现大幅度崛起，刺激其快速发展。其次，引导本科、职业或者其他院校、科研机构、行业协会等积极主动加入大数据产业发展，鼓励技术创新，以制定完善的网络安全使用标准。再次，深化信息安全技术改革，将大数据的先天性优势尽可能发挥出来，以大数据丰富的数据资源为基础，研发设计针对网络黑客攻击的模型与体系，全面提升网络信息安全防御能力。唯有如此，才能适应并且有效应对当今信息安全面临的不断变化的新环境。最后，积极开拓社会组织培育的辅助功能。政府牵头，加强企业、学校、各机构等相关群体的沟通合作，并且定期举行与网络安全相关的丰富多彩的活动，如网络安全知识竞赛、网络安全教育月等，鼓励各类群体积极参加，同时还应鼓励他们积极参与到各类公益活动中，通过分析近几年最新的网络安全风险案例了解更多更细致与网络安全相关的知识与防范手段，将社会补充教育的作用发挥得淋漓尽致。

（三）增加资金投入，完善网络安全体系

构建完善的计算机网络安全体系，资金是重要支撑。之前很多管理者并没有重视资金在构建计算机网络安全体系当中的投入，导致很多问题并没有从根本上得到有效解决。因此，到了大数据时代，从网络管理者的角度出发他们的首要任务就是从根本上转变自身的固有观念，尤其表现在实际工作过程当中应加大资金投入，一部分用来购买高端的计算机设备，以便从设备或者系统出发增强安全抵御系数，在计算机设备上安装较强的病毒防杀系统，目的是能够集中且有效处理在计算机操作过程中存在的一系列安全问题。另一部分资金可以用来聘请专业且具有丰富经验的网络安全工程师或者引进其他方面的专业人才。在构建计算机网络安全体系的过程中，管理者应引导相关技术人员合理分配资金并且在预算合理范围内购置更多优质的计算机网络系统，在计算机内部安装专业且强悍的病毒查杀软件，以便计算机在面临外部病毒时拥有较强的抵御与抵抗能力，从根本上减少病毒对计算机造成的实际危害。

（四）招揽专业人员，选择有效防护技术

有效的防护技术是计算机网络安全工作得以顺利展开的基础，也是构建计算机网络安全体系的重中之重。当前机构组织面临的主要问题是缺乏专业的技术人员，以致在遇到具体问题的时候难以顺利解决。因此，为了从根本上解决这一问题，整体提升计算机网络安全管理质量，管理者应充分发挥出大数据的优势在转换思路的同时积极主动招揽更多综合实力强、水平高的计算机网络管理与维护人员。这类人员主要负责在固定时间对职责范围内的计算机设备进行日常检查、维修、更新等，唯有如此，才能为构建完善的计算机网络安全体系奠定坚实的基础。与此同时，政府或者机构、企业、学校等应为技术人员组织多样化的专业培训，使其一边学习一边了解到更多有效且最新的现代防护技术。当然，技术人员应发挥出主观能动性对防火墙或者病毒库的实际更新变化进行全面且深入的研究，结合先进的大数据技术或者人工智能技术全方位优化传统的防护模式。通过类似的方式尽可能丰富计算机网络安全体系组成，强化体系功能，增强其安全防护效果，有效防止有不断演变和进化的病毒或黑客侵入。

（五）强化管控力度，制定严格管理措施

为了尽可能规避计算机网络信息出现泄露或者被损害的风险，关键在规范并且完善管理制度。尤其计算机网络用户种类繁杂，数量众多，既涉及了个体单位，又涵盖政府、企业等类别，因此，为了全面保障所有网络用户切身的利益，有效提升用户的信息安全，管理者有责任也有义务制定严格的管理措施，组建专业的网络监管部门，以便及时解决用户在使用计算机网络的过程中出现的一系列问题，从根本上很好地抵御黑客攻击系统，基本保障所有用户的信息安全。首先，建立服务器管理制度，由专门人员负责记录每天服务器的各种操作，网络管理人员应及时做好服务器各种账号以及重要数据的保密工作。同时，技术人员应定期安装或者升级最新的安全补丁，弥补系统漏洞，并且及时检测病毒以及木马，按照规定升级病毒库。其次，建立计算机岗位制度，计算机原则上应由专人复杂操作维护，非专业人员不可对设备、网线、光纤等进行任何调试，以免发生故障，给不法人员带来可乘之机。

五、结语

总而言之，要想确保大数据时代健康、稳定、长远发展，计算机网络安全体系构建是基础也是前提。唯有如此，才能在保证计算机网络信息安全的同时为所有用户营造出来一个更安全、更稳定的上网环境，才能保证大数据技术发挥出最大功效，才能从根本上避免用户信息泄露或者其利益遭受损害。因此，相关人员可以从人才培养、技术创新、强化管控等多方面着手，以便真正在大数据时代背景下构建更安全的计算机网络体系。

参考文献：

[1] 龚旭 . 大数据时代计算机网络安全体系构建 [J].IT 经理世界，2020，23（1）：59.

[2] 龙广明 . 大数据时代计算机网络安全体系构建 [J]. 互动软件，2021（12）：3246-3247.