

# 大数据时代通信网络安全管理模式探索

孙英存

天津市滨海新区公安局

DOI:10.12238/acair.v2i2.7357

**[摘要]** 本文结合大数据应用新生态面临的时代背景,对网络信息安全存在的风险隐患进行分析,就如何通过网络安全意识形态的建设、信息加密方式迭代应用、优化硬件防控措施、提升软件保障能力、健全机制建设、培养信息化专业人才进行深入探索和研究,分析制定网络信息安全保障管理策略,为确保大数据时代信息通信更高效、网络安全更可靠提供思路。

**[关键词]** 大数据应用; 信息通信; 网络安全; 保障策略

**中图分类号:** C37 **文献标识码:** A

## Exploration of Communication Network Security Management Mode in Big Data Era

Yingcun Sun

Tianjin Binhai New Area Public Security Bureau Tianjin Binhai New Area

**[Abstract]** Based on the background of the new ecology of big data application, this paper analyzes the potential risks of network information security, and makes in-depth exploration and research on how to construct network security ideology, iteratively apply information encryption methods, optimize hardware prevention and control measures, improve software support capabilities, improve mechanism construction, and train information professionals, and then analyzes and formulates network information security management strategies to provide ideas for ensuring more efficient information communication and more reliable network security in the era of big data.

**[Key words]** big data application information communication network security strategy

### 引言

大数据是信息时代的一种新的思维方式,大数据时代各种类型的网络服务也开始不断涌现出来,大数据应用及网络通信的不断发展给人们的生产和生活都带来了极大的方便,全面推动了人类社会的进步和发展。我们也同时面临着网络信息及数据的安全问题,我们必须把信息安全当作网络通信发展的核心和关键,切实做好信息安全保护工作,打造安全可靠的网络通信环境,为党的二十大提出的建设中国式现代化提供强有力的保障。

#### 1 正确认识大数据应用新生态

##### 1.1 当前社会大数据应用无处不在

大数据是信息时代背景下所产生的一种新型资源,大数据的应用可为社会发展、人民生活提供服务,可为智能决策提供支撑。对企业而言,大数据可提高工作效率,降低企业成本,为精准营销带来更多客户等。对政府而言,可利用大数据进行统筹分析、提高管理效率、助力打击违法犯罪分子等。对个人而言,可利用大数据更加高效的了解社会、方便生活、利于工作等。大数据应用为促进国家经济提升、社会稳定及国际竞争力提供

了帮助。我国的大数据原始积累、网络技术研发、信息通信能力日新月异,但网络安全隐患不容忽视。

##### 1.2 网络信息安全隐患问题突出

在大数据及信息化时代,各种类型的数据、信息技术呈爆发式增长,人们的生活工作都离不开数据及信息技术的支持,重要的数据都需要通过网络渠道进行分析与传播。因此,网络通信技术具有较强的普遍性与开放性,人人都可以参与到互联网共享平台,互联网的这种开放性特色会给人们的工作和生活带来巨大便利。但一些不法分子也会通过黑客技术、利益交换等方式窃取或篡改用户信息,致使个人隐私、企业商业机密、数据安全等受到威胁,对网络系统安全性造成严重影响,这种网络空间信息安全问题的严重性、迫切性远远超过其他传统性安全问题。

#### 2 筑牢网络安全意识形态建设

##### 2.1 切实提升用户信息安全认知水平

随着我国社会、经济、科技发展水平的不断提高,大数据及网络信息大幅提升了各行各业的效率效益,政府机关、企事业单位甚至个人无不运用网络技术处理工作、生活中的各类事务,

网络成为人们生活中不可或缺的重要工具。同时,网络信息安全风险隐患无处不在,绝大部分用户对网络安全的认知程度有待提升,信息安全意识还没有形成共识,相关职能部门必须加大宣传、培训力度,引导不同层次网络用户加强信息安全防护意识,严防信息丢失或泄露造成不必要的经济损失、安全隐患、信任危机甚至生命危险等社会问题。

## 2.2 筑牢专职人员网络安全防范意识

基于大数据时代发展的特点,网管人员必须全面提升安全防范意识、认真钻研安全防范技术、及时制定安全防范预案,切实做好事前防护、事中处置、事后补救。一要经常性对保护对象进行实时分析,不断对预案内容进行针对性调整,以推动安全管理工作的顺利开展。二要对其可承受的风险进行科学评估,不断对风险管理策略进行优化,为网络通信各项业务的正常开展创造条件。三要制定针对网络运行风险的解决措施,一旦有网络安全事件发生,技术人员需及时处理,确保网络通信整体稳定、数据存储基本安全。

## 3 实现信息加密方式迭代应用

### 3.1 强化信息传递的准确性

网络信息从一端经若干个节点(如服务器、路由器、交换机等)传递到另一端,技术人员要从发送端开始,实施信息传输全流程保护,确保信息发送与接收保持零失误,避免发生传输错误问题,就要采取差错检验的方式,在信息传输过程中对帧的长度、格式等内容进行优化,从而使链路传输的准确性得到保障。

### 3.2 保护信息应用的安全性

大数据时代网络信息安全防护必须做到全覆盖,特别是针对一些重要的核心机密信息如涉及金融交易、商业机密等信息更要做到重点保护。一要为网络设备添加权限管理,如文件加密、用户名及账户口令、验证码等常见加密技术,提升信息安全防护意识;二要充分利用先进技术和信息设备,如使用加密狗、电子身份证等身份识别设备,防止违法分子利用漏洞窃取重要机密信息;三要及时引入两种安全防护技术,为数据信息安全提供双重保障,使得计算机及其网络设备在加密技术以及身份验证功能的双重加持下,实现更高效的安全保障。

### 3.3 完善信息安全防护策略

信息安全防护可以结合大数据领域、云计算环境、移动网络客户端、信息交换数据库等资源特点,增强对先进技术的研发力度,制定应对隐患冲击的安全策略。如:针对病毒或不法分子通过对用户的IP地址进行截获后,对网络发动入侵,从而盗取用户信息资源的具体操作,用户必须做好自身IP地址的重点保护,并采取绝对保密的策略,使用第二层交换机进行消息传播,通过强化对IP地址的管理,对控制交换机加以防护,达到保护自身IP地址绝对安全的目的。此外,也可以加强对路由器的环境隔离与控制,监视来访IP地址,查看IP地址是否携带病毒或不良信息,发现异常情况则拒绝访问,确保TCP/IP通信协议的安全。

## 4 优化网络安全硬件防控措施

### 4.1 优化防火墙设置

防火墙是行之有效的抗病毒方式之一,为更好地保护网络通信安全,有必要从多个方面加强网络系统防火墙的构建,形成较为严密的防火墙体系,对通过防火墙的数据流加以屏蔽或者过滤,并随时对病毒进行监控,实现对外部用户信息流的实时监控,防止外界对本地服务器的监听、窃取操作,最终实现对内部用户信息的保护。

### 4.2 优化硬件设施环境

硬件设施安全运行受外部环境影响很大,外部环境温度过高、湿度过大或电磁环境转变等,这些都会直接导致硬件设施损坏、数据信息丢失等问题。为防止此类问题发生,相关技术人员要注意硬件设施的安全使用,提升硬件设施的使用效率,要对硬件设施的运行环境定期进行检查,及时更换老旧设备,对可能带来不良影响的各种因素加以管控,增强硬件设施的使用效率和使用寿命,确保整个网络设备处于安全状态。

### 4.3 优化设备维护管理

硬件设备是网络通信安全稳定运行的基础,相关人员必须严格按照管理制度做好设备的维护管理及线路的检测等工作,并对设备运行过程中可能发生的风险进行预测,制定相应的处理预案,以使其长期保持良好的运行状态,避免对网络信息安全造成不良影响。

## 5 提升网络安全软件保障能力

### 5.1 及时处理系统漏洞

通过对大量网络及数据安全问题进行分析,大多数安全风险的起因均是系统存在漏洞。这就要求技术人员必须加强对系统漏洞的防范工作,做好对漏洞的全面分析,明确事故的起因,构建相应的数据模型,为安全防护工作提供依据。技术人员需要对防护工作的覆盖面进行拓展,在做好日常计算机、通信设备等运行状态的检修外,还需要对外部设备加强控制,对文件进行安全监测,避免木马、病毒等入侵系统。技术人员还要充分利用大数据技术的优势,构建事故分析预警系统,对通信网络潜在安全风险进行预测,并制定相应的防范措施,切实保障网络系统稳定运行。

### 5.2 经常开展必要性分析

利用大数据分析技术,数据处理速度更快,能够为网络数据安全提供技术支持,网络数据信息的安全也能得到更好的保障。管理人员利用该技术对数据进行多维关联分析,进而实现对数据信息的实时监测,提高信息通信安全管理质效。例如,网管人员可以利用大数据技术,对网络中的异常访问进行检测,加强对网络攻击及其他恶性事件的防范。研究人员可将网络管理系统与项目管理系统相融合,推动网络接入安防保障系统取得新提升;工作人员可将大数据技术与通信安全管理相融合,推动安管技术研发工作取得新进展。

## 6 建立健全网络安全体制机制建设

### 6.1 完善网络安全风险防控机制

由于网络安全风险存在多样化、风险程度高等特点,相关专业部门应当构建完善的网络安全风险防控机制,全面提升对信

息安全的重视程度,针对通信网络用户数量不断增加、传统网络风险分析工具缺陷、行业风险评估与实际情况存在较大偏差、黑客给网络信息安全带来较大威胁等实际情况,指导各级管理人员有针对性地开展防范工作、对相关预防技术进行深入研发、拓展安全防护手段,对网络数据进行有效监控、修补系统漏洞、阻隔病毒入侵、规避黑客攻击、防范和打击违法行为等,严防系统受到威胁、信息发生泄漏。

#### 6.2 完善网络安全管理规章制度

随着大数据时代的来临,各级主管单位亟需加强与相关业务部门的交流,结合各业务系统的特点,对现行网络安全管理制度进行完善和优化设计,制定完善的管理制度和健全的法律法规体系,对违反规定故意制作传播计算机病毒以及其他破坏性程序或者对未经允许即对信息网络中存储、处理或者传输的数据和应用程序进行删除、修改、增减或者进行危害国家安全、损害国家利益、侵犯个人隐私、扰乱社会秩序的违法违规行为作出相应处罚规定并严格执行,对网络信息安全形成有效的防护系统,确保网络数据信息安全可靠、业务系统运行安全稳定。

#### 7 注重网络安全专业人才培养

##### 7.1 组建专业化网络信息安全技术团队

国家领导人指出:“没有网络安全就没有国家安全,就没有经济社会稳定运行,广大人民群众利益也难以得到保障。”在大数据时代,各行各业都离不开网络信息的支撑,维护网络空间安全,必须着力培养熟练掌握信息系统安全知识、网络基础设施安全知识且具有较强实践和创新能力的专业团队。同时,在制度设计、人才选拔、能力培养等多方面给予政策支持,将其培养成一支靠得住、本领强、打得赢的网络安全专业力量,使其既会用群众听得懂的语言讲述网络安全风险,也要善于用专业手段和技术实力化解网络安全风险,通过专业团队与广大用户共同携手,打造安全可靠、清风正气的网络通信环境。

##### 7.2 多措并举拓展技术人才培养范畴

网络安全形势无时无刻不在变化,网络安全专业团队要具备对网络信息安全保障技术研究和创新的敏感性。通过政府、高校、企业、社会等相关行业、组织建立多层次、多渠道的网

络安全人才培养体系,保持与具有先进技术能力专家的交流 and 沟通,营造良好的培训学习环境,紧密结合软、硬件的功能属性,提升网络信息安全技术人才的专业水平和实践经验,建设一支“专兼结合”“新老互补”的高质量网络信息安全管理队伍。同时,加大实践环节的训练强度,锻炼其快速应变和专业技术维护能力,使其在遇到安全问题和不法行为时能够快速发现、及时处置,充分发挥其对网络信息安全保障的关键性作用。

#### 8 结束语

保障网络安全需要全社会的共同努力,政府职能部门要对相关网络安全案例进行归纳总结,对可能引发的各类社会问题做好应对预案及防护策略,要提高政治站位及网络安全防范意识,有针对性的建立和健全完善管理制度,引导全社会各行各业严格遵守国家网络安全相关法律法规。专业职能部门要对通信行业中存在的安全风险进行实时分析研判,通过信息加密、硬件防护、软件保障及专业人才的技术支持等共同发力,为大数据时代信息通信安全营造良好的网络环境,让大数据精准惠及人民大众,为中国式现代化发展提供大数据支撑及安全高效的网络保障。

#### 【参考文献】

- [1]石书红.大数据背景下计算机网络信息安全管理及防范措施[J].普洱学院学报,2020,36(06):15-17.
- [2]张建生,张小红,彭林华.大数据背景下计算机网络信息安全及防护对策[J].信息与电脑(理论版),2018,(20):198-200.
- [3]朱光军,孟子栋.基于大数据时代背景下的网络信息安全及防护策略研究[J].中国新通信,2018,20(02):63-64.
- [4]司瑾.大数据时代背景下的计算机网络与信息安全防范策略浅析[J].数码设计,2017,6(10):9-10.
- [5]洪宇.网络通信中信息安全的保障策略探讨[J].信息与电脑(理论版),2018,(08):182-184.

#### 作者简介:

孙英存(1972--),男,汉族,天津市滨海新区人,本科理学学士,副高,研究方向:计算机与网络通信。