大数据背景下通信网络安全管理策略研究

吴清云

四川华电木里河水电开发有限公司

摘　要：大数据（Big Data）是20世纪末在计算机领域被首次提出的一项专有名词，随着大数据技术的变革和应用渠道的拓展，现如今，大数据技术已经融入经济、社会、政治甚至文化发展领域中，成为不同领域工作模式变革和数字化发展的关键支持技术。在当前计算机技术的发展与提高下，对数据的存贮率要求愈来愈高，利用大数据不但能够保存大量数据，还可以快速挖掘和定位数据信息，为人们的生活工作提供便利。随着大数据技术的不断发展，其应用渠道和信息来源变得更为广泛。随着信息技术的不断发展，通信网络逐渐成为人们日常生活中不可或缺的重要组成内容。由于通信网络的不断扩大和适用人群数量的不断增加，通信网络的稳定性受到了相应的影响，导致通信网络安全问题更加突出。通信网络安全指的是通信网络中的物理环境、硬件设备、数据安全等各方面的内容，可运用政策、标准、技术以及管理等方式确保通信网络的稳定实施。在大数据背景下，通信网络安全防护工作可以针对性地解决网络中的各项隐患问题，实现安全防护的高效性。

关键词：大数据；通信网络；安全管理；分析

【DOI】10.12252/j.issn.2096-6288.2023.05.221

引言

随着现代通信网络技术的革新和发展，企业与个人的网络通信需求已经得到极大程度的满足，但与此同时，通信网络的广泛应用势必会给通信活动的隐私性和安全性带来更多挑战。大数据是信息化社会的变革动力，大数据技术的优化发展为现代通信网络的构建提供了巨大发展契机，但伴随大数据信息获取和传播能力的提高，网络安全问题也日益严峻。大数据技术，是一种在互联网技术下的大数据存储模式，其使用领域非常广阔，将深刻影响着人类的生活与方式。在大数据时代下，万物互联将成为一大特点，人与物、人与网络平台间的差距也将进一步缩短。大数据最根本的特点即是信息量巨大。但凡事均具有两面性，大数据背景下的社会变革迅速，通信网络的建设已经成为个人生活和企业构建不可缺少的重要环节，个人隐私、商业机密等重要通信内容都需要依赖网络条件进行传达和存储，在此过程中一旦受到不法人员的信息侵袭，通信网络安全就会无法得到保障。因此，探究大数据背景下通信网络安全管理策略就显得极为必要。

一、分析影响网络通信安全的因素

（一）分析网络系统的漏洞

对于网络系统漏洞而言，主要是指网络应用软件或操作系统在被设计和编写中，因为受到技术限制和检验实效等导致其网络系统出现了瘫痪，进而也是为不法分子以及黑客入侵提供出了便利。在网络通信过程中，无论何种信息传递都离不开网络软件和系统的支持，一旦支撑系统出现漏洞，就会成为通信网络安全的重要隐患。虽然随着相关软件的不断开发和系统迭代，相关技术不断发展，我国通信网络安全已经得到基本保障，但根据目前通信网络维护现状来看，系统漏洞仍然是影响通信安全的重要因素，查找与修复漏洞的必要性不言而喻。

（二）分析网络协议以及网络结构的互通性

通信网络是具有一个先天性的要素，那就是交互和反馈的连通性要求，通信是人和人之间的沟通过程，无论是发送或接受信息，都是需要相应的主体进行信息编辑和信息反馈，从而形成一个连贯的通信网络，这种沟通过程强调交互和反馈，这也意味着通信网络需要满足极高的连通性需求，但网络安全强调私密化、阻断化，减少开放的交互需求就能从一定程度上增加网络安全性，因此，两相取舍之下，为了实现通信网络的互联与互通，往往在网络协议与网络结构的建立之初，网络设计与管理者就会被迫牺牲一些网络安全机制，通过增加网络的开放性满足通信需求。

（三）分析用户访问的需要

根据网络使用功能来分析，其本质就是一个开放的信息传递和收集平台，任何一个企业或项目建立起的网站和应用软件或简易程序的目的都不会是简单的自我使用需求，而会将用户捕捉、市场需求和信息交流的要求放在网络平台搭建与使用功能的首位。这种对市场适应

性的考虑并不是一件错事，通信网络正是由于这样的使用策略才得以完善和发展，但凡事均不能只考虑单方面优势，我们仍应该看到加快信息交流、适应市场需求的背后，是通信网络访问用户的不确定性，管理者与经营者也难以确保商业间谍或专业黑客不会混入常规访问用户的队列中。因此，用户访问因素也会给通信网络安全带来巨大隐患。

（四）分析地理位置和地域因素的影响

通信网络的建立和使用是离不开终端数据库和处理中心的技术支持，不管是通信网络基站修建或者是大范围的信息处理系统构建，都需要满足远距离网络传输的要求。对于一般企业和具有通信需求的个体而言，使用网络可以从有线和无线两种方式中进行选择，但无论哪种通信网络建立方式，都会有通信线路建设需要，特别是对于跨国企业来说，跨越省市和国际的网络连接可能会造成过长通信线路建设的负担，过远的地理位置会降低网络通信质量，此时因地理位置因素在信息传输过程中造成的信息缺失，就会给黑客攻击和信息攫取提供便利，由此产生通信网络安全问题。

二、基于大数据的通信网络安全隐患问题分析

（一）分析通信网络内的安全漏洞问题

计算机网络系统具有资源共享的优势，具有自身的交互特征，可以充分的满足不同用户对计算机功能的需要，能够有效的去提高计算机系统的可拓展性，计算机网络系统具备多用户接入和多功能拓展的优势，但是会形成很多安全漏洞，容易遭到恶意攻击。同时，随着计算机网络运行周期的不断延长，长时间使用操作系统会导致漏洞暴露，致使系统遭到破坏，继而形成安全风险。在网络工作开展的过程中，链路是基础性的支持，在系统的交互过程中，系统或文件内部的漏洞会对内部链路形成攻击，继而导致数据缺失，形成漏洞。一旦被不法分子利用，便会导致通信网络的安全受到威胁。

（二）分析通信网络外部破坏的问题

现如今通信网络外部破坏主要是受到两个方面因素的影响，一方面是人为破坏，就算是相关人员在取得计算机通信网络准入权限后，在计算机系统程序中释放病毒等危害较大的数据信息，或者关闭防火墙和杀毒软件等，致使计算机通信网络安全无法得到安全防护工具的保护，降低保护等级，继而影响其安全性。另一方面遭受自然灾害，特别遭遇暴风雨或者其他极端恶劣天气情况，会导致室外公共通信线路遭到破坏，形成短路或者断路故障，继而影响计算机通信网络的稳定运行，会导致数据遗失或者系统瘫痪等问题。

三、分析大数据背景下通信网络安全管理策略

（一）分析人员培训和通信网络安全防护意识的提升

对于信息安全意识而言，是参与信息传播和接受过程中个体思维体现出来的一种安全观念，参与网络通信是由意识的个体，进行信息窃取的不法网络活动分子可能会通过多种方式降低通信个体的安全意识和警戒心，因此提高信息安全意识是保护通信网络安全的关键环节。通信网络安全相关知识培训是提高信息安全意识的常用手段。这里所指的相关知识培训在实际安排过程中应该按照适应情境不同进行划分，并根据相应情境开展适当形式的人员培训。针对每一网络通信个体来说，通信网络安全培训重点应该放在提高信息泄漏关注度和隐私数据合理存取上，而面对企业通信需求，培训重点应该是加强企业员工信息安全教育，利用大数据网络的便捷性特点，对员工实施层级式信息管理，减少机密商业信息的人为泄漏概率。

（二）分析大数据下的通信网络安全技术革新和应用

1. 分析防火墙和加密系统的更新和应用

防火墙在现如今网络防御领域的应用是比较高的，作为一种内部和外部网络、专用、公共网络之间的安全屏障，防火墙可以根据隔离操作和访问控制功能，过滤掉多数不合理的范文要求，控制安全性比较差用户的访问权限，这无疑是给通信安全安装了一道保险门。通信加密是弥补网络漏洞、防止信息泄漏的关键环节，常见有密码加密、扩散加密、物理加密等多种加密形式，与防火墙联用相当于为通信网络安全加上了一把大锁。但是无论再高超的防火墙技术与加密系统，随着时间的推移，职业黑客和信息盗窃不法分子仍然能够找到其中漏洞，这就说明通信网络安全屏障需要不断更新迭代，才能发挥其最大功用。因此，在大数据背景下，通信技术人员应该利用大数据的信息收集能力，提升自身技术上

限，对既往防火墙与加密系统开展研究和更新，建立技术领先意识，将其安全性和使用性能更高的系统合理的应用到通信网络之中。

2.建立起异常通信数据采集和分析系统

大数据技术的一个优点就是信息收集的广泛性和快速性，这个优点应用通信网络安全管理中，可以和通信技术相互配合，建立起具有优秀的发展前景的异常通信数据采集和分析系统，该系统主要包含数据采集和集成分析两个模块，其中数据采集模块是整个系统运行的关键环节。从数据广泛性来看，数据采集工作需要涵盖用户数据、传输数据、流量监测、漏洞更新、事件日志等，从数据抓取过程来看，可靠而稳定的信息抓取设备是数据采集的基础。从数据分析模块来看，大数据技术的应用面非常广泛，采集完成的数据需要经历大数据技术的筛选和挖掘，异常结果需要依靠大数据进行可视化呈现和数据备份。异常通信数据采集与分析系统在企业通信安全管理中的应用价值最高，通过对企业通信网络信息的抓取和分析，许多还未成为高风险的通信安全事件都能够得到提前控制，这对降低企业信息管理成本，能够有效的减少商业信息泄漏概率。

（三）合理的应用SaaS云安全产品发挥出大数据安全管理优势

SaaS（Software as a Service）主要是作为一种云计算的模式，主要是可以为拥有者提供出一种云软件的服务，并不是将软件安装到本地计算机上。首先大数据技术在通信安全管理中的优势主要是可以通过SaaS云安全产品进行体现。其次SaaS云安全产品可以采用大数据技术来提供更加准确的服务和更好的用户体验，这表示着SaaS和大数据之间关系是十分密切的，它们可以相互促进，并共同为企业和个人提供更好的通信安全管理服务。所以SaaS云安全产品可以利用大数据技术，将收集到的结构化或非结构化的海量、高增长率和多样化的通信数据进行处理和分析，使用SaaS提供的数据仓库服务来存储和管理大数据，并对通信敏感信息展开专门的安全管理，例如数据加密、多层密钥应用、设置敏感信息传递令牌等。由此，企业可以检查自己的通信安全堆栈并进行研究，在不牺牲安全性的情况下，SaaS云安全产品提高对自身通信网络安全的管理。

总结

综上所述，大数据背景下的通信网络安全同时面临着机遇和挑战，站在辩证思想角度来说，这样的机遇和挑战是合理的，一种事物想要得到长足发展，必定是在各种挑战中获得经验从而进步。互联网在我国的发展历史虽然不算久远，但已经在近二十年的发展过程中促使我国经济社会发生了几次大变革，并且已明显改变了人们的生活习惯。网络技术与信息技术的深入研究带给社会的价值不可估量。网络联通式通信手段改变了以往人们对信息交流的认知，但同时也为信息泄漏和窃取行为的产生埋下了隐患。因此，对影响通信网络安全的因素进行发掘，对既往安全管理情况进行剖析是提高通信网络安全管理策略的有效性的有力方式，本研究顺着这一分析路径，对通信网络安全管理策略展开了详细讨论，希望能够通过技术革新和人员培训等策略的提出，为我们通信网络安全壁垒的建设添砖加瓦。

参考文献

[1]李永钢.大数据技术在5G通信网络中的应用探析[J].电脑知识与技术，2022，18（27）：56-58.

[2]郭天科.大数据分析在移动通信网络优化中的应用[J].无线互联科技，2022，19（15）：103-105.

[3]刘磊.大数据背景下信息通信网络安全管理管理策略研究[J].网络安全技术与应用，2022（08）：57-59.

[4]谭韶生，夏旭.基于大数据优化神经网络的船舶通信网络干扰信息识别[J].舰船科学技术，2022，44（14）：133-136.

[5]刘国凤.大数据背景下信息通信网络安全管理策略研究[J].中国新通信，2022，24（14）：9-11.

[6]左李景.大数据背景下信息通信网络安全管理策略研究[J].中国新通信，2022，24（14）：107-109.

[7]吕静.通信网络系统中大数据技术问题分析[J].科技创新与应用，2022，12（21）：153-156.

[8]韩春杨.大数据技术在5G通信网络中的网络优化应用[J].电子测试，2022，36（12）：132-134+131.

[9]王素云.试论大数据技术在5G通信网络中的应用[J].电子质量，2022（06）：90-94.

[10]覃光文.大数据分析在移动通信网络优化中的应用[J].数字通信世界，2022（03）：131-133.