Universe Scientific Publishing
工程技术与发展
第 1 卷◆第 3 期◆2019 年 6 月
刊号：2661-3492 (纸质) 2661-3506 (电子)

A preliminary study on the Application of computer Network Security Technology in big data's era

Chenglong Du

Abstract

computer network technology has triggered a profound change of the times, people can obtain a large amount of information on electronic devices through a very short period of time without leaving their homes. Big data, as a revolutionary technology after "Internet of things, cloud computing", has a very important impact on the development of social industries and people's lives, and has brought people into the "data age". Therefore, under the background of big data's era, it is very important to discuss computer network security technology. Based on the concept of computer network security, this paper analyzes the hidden dangers of computer network security under the background of big data's era, and finally analyzes the security of computer network. The full maintenance technology is discussed.

Keywords

computer network; big data; security technology

大数据时代的计算机网络安全技术应用初探

杜成龙

广东科技学院 广东 东莞 523083

[摘　要] 计算机网络技术引发了一场深刻的时代变革，人们足不出户就可在电子设备上通过极短的时间，获取海量的资讯。而大数据作为“物联网、云计算”后的一项革命性技术，对于社会各行业发展以及人们生活有着极为重要的影响，将人们带入了“数据时代”。因此，在大数据时代背景下，探讨计算机网络安全技术，就显得极为重要。本文从计算机网络安全概念出发，然后对大数据时代背景下计算机网络安全隐患进行了分析，最后对计算机网络安全维护技术进行了探讨。

[关键词] 计算机网络；大数据；安全技术

[DOI] 10.18686/gcjsfz.v1i3.490

目前，计算机网络技术、信息技术越发成熟，已经真正成为了人们生活中的一部分，但是这些技术在为人们生活提供便利的同时，也带来了相应的安全隐患。互联网具有较强的开放性，人们在网络上交流、沟通，就有可能被他人获取私人信息，同时用户在电子设备上储存的关键信息也有可能被不法分子所窃取。而大数据技术，则让各项数据内容呈现出了更高的价值。故，在大数据时代，人们越发关注计算机网络安全，并且已经成为了当前社会需要迫切解决的现实问题。

一、计算机网络安全概念

本文主要立足在大数据技术背景下，对计算机网络安全概念进行阐述。计算机网络安全主要可从保密、安全、完整三个方面来分析。首先，计算机网络可高效传输数据内容，已经成为现代信息传递的重要媒介，而保证信息传递的保密性，则是计算机网络安全的重要内容；其次，计算机网络安全主要可分为内部安全以及外部安全，所谓内部安全主要是指电子设备的安全性；外部安全则主要是指操作计算机网络使用者在接触敏感信息时，是否能够抵御敏感信息影响而获得正确的信息内容；最后，完整主要是指计算机数据的完整性、计算机网络的完整性、计算机系统的完整性，而这些因素的完整与否，直接决定了计算机网络对黑客攻击的抵御能力[1]。

二、大数据时代背景下计算机网络安全隐患

大数据是一种集成移动计算、分布式计算的技术，大数据信息处理速度非常快，并且该技术的应用范围较为广泛，其中多数信息和较高安全级别的信息有着一定的内在联系，因此必须对大数据时代计算机网络安全隐患进行分析。

（一）攻击技术发展

在分布式计算、云计算、移动计算不断发展、应用、普及的背景下，这些技术不仅仅提高了人们利用信息数据的效率，同时也在一定程度上为不法分子提供了便利，木马病毒共计更加智能化，网络攻击更具有针对性[2]。

（二）安全意识缺失

目前，多数用户都没有经过专业化的计算机操作培训，对计算机网络安全没有足够的了解，在访问网络的过程中，经常不按照正确规程访问网络，随意使用来源不明的移动储存设备传输文件，这就会导致木马病毒逐步在设备终端中发展蔓延。

三、大数据背景下的计算机网络安全维护技术

（一）系统需求

本文以某单位计算机网络安全防御系统构建为例，单位网络中主要包括：身份认证系统、系统关机还原；各部门子网络相互连接；入侵检测、安全访问。三个方面的安全建设需求，其网络规划可见图 1。

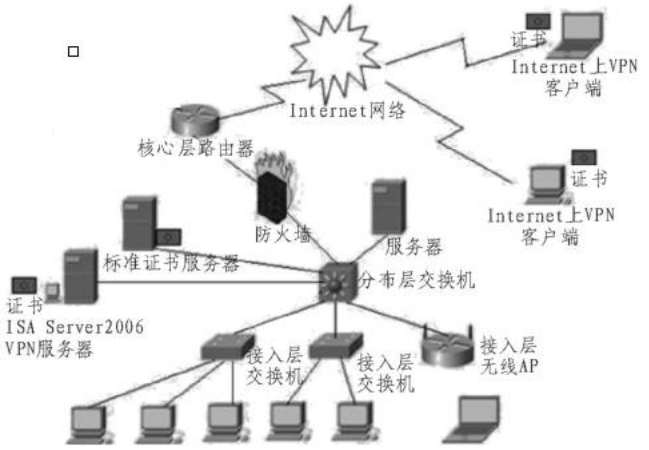

图 1.网络规划

图 1 中网络防火墙主要划分单位内部网络、外部网络，网络区域主要包括对外访问服务的子网络，单位内办公、行政所用子网络。通过分析现代化计算机网络系统需求、网络信息系统安全系统可发现，计算机网络安全防御主要体现在：病毒防护、桌边系统安全、身份识别、访问控制、信息数据加密、安全审计、入侵检测、系统漏洞检测、安全管理、实体安全管理等方面。

（二）网络安全体系结构

网络安全防御体系结构的构建，需要充分考虑到计算机网络系统、信息、数据库、信息传递介质、病毒防治等等内容，该单位网络安全体系构建以信息安全为中心，综合考虑到信息服务以及操作系统，详细结构可见图 2。

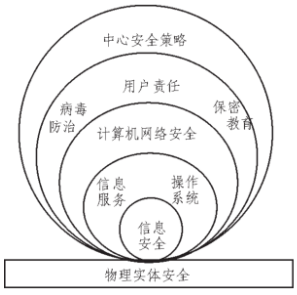

图 2.网络安全体系结构

（三）网络安全体系层次模型

该单位网络安全体系层次构建 OSI 模型，网络安全建设贯穿在这 6 个层次中，采用 TCP/IP 协议。主要分为物理层、链路层、网络层、会话层、应用层（应用系统、应用平台），其中主要考虑到物理层信息安全、链路安全、安全路由访问机制、会话安全、应用安全[3]。物理层信息安全主要是避免硬件设备损坏，避免硬件设备被窃听、攻击等；链路层主要是要保证信息数据传输安全，采取局域网划分、加密通讯等措施；网络层安全主要是通过实现网络授权客户服务，以此来保证网络路由的正确性，避免网络被拦截或者被监控。

（四）网络安全系统设计

1、安全防御功能

大数据在获取数据的过程中，有可能受到来源于多个渠道的攻击，并且黑客病毒可在移动终端、计算机等等多个渠道传播，而木马病毒的潜伏周期普遍比较长，所以在大数据时代背景下，黑客攻击范围在一定程度上被扩大，为有效提高大数据技术应用中心安全防控能力，可构建主动防御系统。主动防御系统主要包括：用户管理、系统配置管理、安全策略管理、网络状态监控、网络运行日志记录、网络运行报表编制。

2、安全预警功能

计算机网络中有着海量的异构应用软件，这些软件使用不同的开发语言、环境、结构，但是在实现集成的过程中，为实现接口相互通信，故存在诸多漏洞，这就降低了计算机网络安全水平。安全预警功能能够体现存在的漏洞，然后就可采取相应的安全防控措施。抵御外来风险（安全预警模块构建可见图 3）。

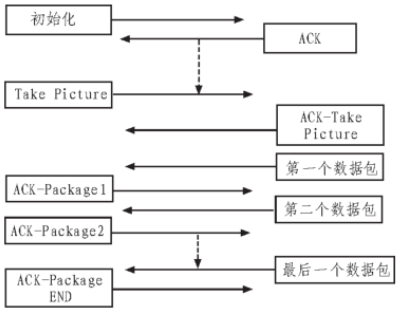

图 3.安全预警模块构建

3、安全保护功能

目前，多数计算机都是通过杀毒软件、防火墙来实现安全保护，而多数杀毒软件都是集成部署的，在大数据技术不断普及的背景下，单一的杀毒软件、防火墙已经不能够满足安全防控需求。故要构建相应的安全保护功能，利用数字签名防御技术来提高计算机网络安全水平。同时，现代计算机网络可利用入侵检测、流量抓包技术来获取实时网络流量，然后通过相应的软件来深入挖掘相关安全信息，实现安全响应，消除安全隐患。

5、系统恢复

目前，多数计算机网络访问用户都未经历过专业化培训，对计算机网络正确访问规程没有足够认识，在实际操作中极其容易受到相应的安全威胁，如若计算机服务器受到威胁，那么就能够使用相应的系统恢复技术让系统恢复到正常状态，这对公共计算机的使用来说有着至关重要的意义，可有效避免计算机网络受到攻击，消除安全隐患。故，要结合

实际情况，设置系统恢复模块，所有公共计算机设备在使用关机后，要能够完成网络初始化、任务初始化、协议栈初始化、全局变量初始化。

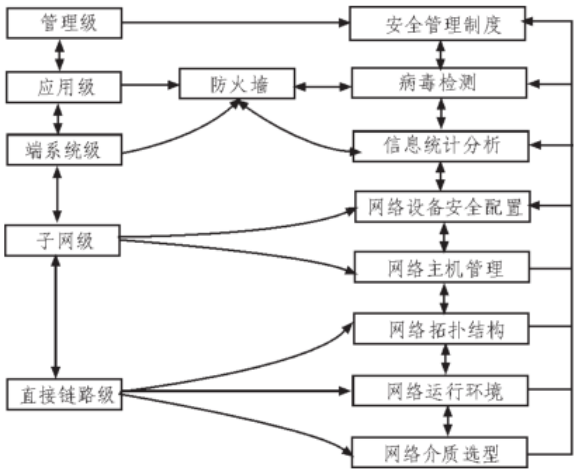

图 4.安全保护模块

本文所列举的计算机网络安全技术，利用漏洞扫描技术以及扫描设备的联动部署，能够有效保证单位内网安全。在规划的过程中，综合考虑到各个部门网络配置的统一性，为各个部门以及网络管理应用服务的进一步配置提供基础，从而保证单位内所有部门的网络安全。经过实践测试表明，计算机网络能够及时发现存在的漏洞以及隐患，并且可在较短的时间内完成补丁，不仅提升了网络安全性，同时还在一定程度上提高了网络运作效率。

结束语：

随着大数据的不断发展，网络攻击方式、网络攻击渠道也在不断变化，并且网络攻击潜伏周期比较长，安全隐患感染传播速度比较快，对大数据技术的正常应用造成了极大影响，故要针对当下计算机网络安全隐患特征，采取相应的安全防范技术，才能提高计算机网络安全防范能力。笔者在文中仅对大数据时代的计算机网络安全技术进行了简单阐述，更为深入的问题还需要广大从业者进一步探讨。

参考文献：

[1]肖霞. 基于大数据时代计算机网络安全技术应用研究[J]. 辽宁高职学报, 2018.

[2]王鑫. 计算机网络安全技术在大数据时代的探讨[J]. 科技创新与应用, 2017(12):102-102.

[3]周小健，鲁梁梁. 大数据时代背景下计算机网络安全防范应用与运行[J]. 网络安全技术与应用, 2017(5).

稿件信息：

收稿日期：2019 年 5 月 22 日；录用日期：2019 年 6 月 8 日；发布日期：2019 年 6 月 20 日

文章引文：杜成龙. 大数据时代的计算机网络安全技术应用初探[J]. 工程技术与发展.2019,1(3).

http://dx.doi.org/10.18686/gcjsfz.v1i3.

知网检索的两种方式

1.打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD 下拉列表框选择：[ISSN]，输入期刊 例如：ISSN：2661-3506/2661-3492，即可查询

2.打开知网首页 http://cnki.net/ 左侧“国际文献总库”进入，输入文章标题，即可查询 投稿请点击：

http://cn.usp-pl.com/index.php/gcjsfz/login 期刊邮箱：xueshu@usp-pl.com