第42卷 第6A期
2015年6月

计 算 机 科 学
Computer Science

Vol. 42 No. 6A
June 2015

石油企业内网安全隐患及控制策略分析

路坤桥[1] 王金和[2] 邓 涛[2] 李 红[2]

(东北石油大学石油工程学院 大庆 163000)[1] (新疆油田公司采油二厂 克拉玛依 834008)[2]

摘 要 随着信息技术的发展,石油企业内部网络在生产经营活动中起到日益重要的支撑作用,这对网络的承载能力和安全性提出了更高要求。建立一个合格的内网安全系统,保证内部核心数据安全,成为迫切需要解决的问题。以新疆油田采油二厂内网建设和管理为例,分析了内网存在的安全问题和隐患,从优化完善网络架构、部署安全防护系统、建立健全安全保障体系3个方面提出安全控制策略,为油田企业网络安全管理提供参考。

关键词 油田企业,内网,安全隐患,控制策略

中图法分类号 TP393.08 **文献标识码** A

Analysis on Security Risk and Control Strategy of Petroleum Enterprise Internal Network

LU Kun-qiao[1] WANG Jin-he[2] DENG Tao[2] LI Hong[2]

(School of Petroleum Engineering, Northeast Petroleum University, Daqing 163000, China)[1]

(PetroChina Xinjiang Oilfield Company No. 2 Production Plant, Karamay 834008, China)[2]

Abstract With the development of information technology, the internal network of the petroleum enterprise rises to prop up the function increasingly and importantly in produce activity, putting forward the higher request to the loading ability and safety of the network. How to set up an eligible security system, how to guarantee the security core data from enterprise, those are issues need to be solved immediately according to the enterprise pressing requirement. This article takes the internal network security of the Xinjiang oilfield company No. 2 production plant as an example, analyzing existing security risk of internal network, and put forward three control strategy: excellent and perfect network structure, deploying the security protection system, building up the safety guarantee system, to provide the reference for the oil-field enterprise network safety.

Keywords Oilfield enterprise, Internal network, Security risk, Control strategy

1 引言

新疆油田采油二厂在信息化、数字化建设进程中,逐步完善了从生产站区、办公区到油田公司以及关联业务单位的网络覆盖,在此基础上应用信息门户、RTX、电子邮箱、生产管理系统、ERP系统、OA系统等,实现了办公同步、资源共享、信息录入访问及逻辑处理功能,正在进行的智能油田建设将进一步实现井站远程监控、数据智能分析等功能。随着采油厂核心生产技术、经营成本信息、日常生产数据逐步“数字化”和“网络化”,现代油田生产办公对网络、计算机的依赖也越来越高,如果出现网络安全问题,就有可能造成重大损失或灾难性的影响。因此,加强网络安全、防止信息泄露和修改、非法窃取已成为迫切需要解决的问题,及时掌握和控制网络安全隐患十分必要。

2 内网安全和管理概述

一般而言,我们通常以企业局域网的网络边界为限,将企业网络划分为内部网和外部网两个部分。因此,内网安全指的就是企业内部局域网的信息安全。具体地说,就是对企业局域网防火墙以内网络的信息安全综合管理,进一步也包括对局域网终端的综合管理。

按照中国石油统一规划,采油二厂网络在3层架构中处于汇聚层和接入层,通过千兆光纤与油田公司核心层连接。对内,与中国石油各级内部网络互联;对外,通过油田公司统一出口接入Internet网,厂内用户通过油田公司代理服务器与外部网络交互。由油田公司统一架设防火墙、防病毒网关、IDS等网络边界防护系统,过滤防护在外网泛滥的病毒、黑客攻击,采油二厂负责内网中的交换机、服务器、终端、应用系统等网络节点的安全防护。

3 内网安全存在隐患

通过分析石油企业信息内网现状和运行情况,发现其主要存在以下几方面安全隐患。

3.1 部分员工桌面行为不规范

部分员工随意使用游戏软件、即时通讯、炒股软件、迅雷下载等的情况无法控制,严重影响工作效率,占用有限带宽资源,影响正常业务的开展。

对互联网的访问无法控制,部分员工随意访问一些非法

路坤桥(1992—),男,主要研究方向为石油工程,E-mail:ycx@petrochina.com.cn;王金和(1970—),男,工程师,主要研究方向为油气田网络安全;邓 涛(1980—),男,助理工程师,主要研究方向为油气田网络安全;李 红(1969—),女,工程师,主要研究方向为油气田网络安全。

和不健康的网站，可能会导致木马等病毒被非法下载至企业局域网内部，严重危害油田网络安全。

部分员工对信息安全认识程度不高，缺乏防护意识，系统账户长期使用弱口令，增加了受到网络黑客攻击的风险。

3.2 移动介质不能有效管理

企业合作和外协单位的工作人员来厂交流，由于不能及时对相关人员的计算机设备进行检查，木马等病毒很容易被其计算机设备带入内部网络。

部分员工缺乏安全防范意识，未经杀毒处理就直接将u盘、储存卡、光盘等存储介质以及存在安全隐患的个人电脑、手机等终端接入内网，导致木马等病毒程序快速传播，从而感染其他计算机。

3.3 终端安全防护不达标

根据油田公司的统一规划，计算机必须安装统一的Symantec防病毒软件并及时升级更新病毒库。由于计算机数量庞大、用户水平参差不齐，部分计算机未安装防病毒软件或安装了不符合要求的防病毒软件(如瑞星、360、卡巴斯基等)。缺乏有效的措施安装更新病毒防护系统，管理员无法监控客户端防病毒软件是否处于正常运行状态。

系统安全漏洞的修补工作繁重，补丁的下载和安装需要大量的人工参与，且存在安装率不高、及时性不高、完整性不高等缺点。缺乏有效的措施统一升级和更新补丁，管理员无法监控补丁更新情况。

3.4 缺乏有效的故障定位解决手段

当网络出现病毒等安全问题后，被感染终端成为了网络内部的传染源，使得更多的终端遭到木马和蠕虫等病毒侵袭。网络管理人员由于技术手段不足，不能做到对安全事件源的实时、快速、精确定位以及远程阻断隔离。

4 内网安全控制策略

针对油田企业内网存在的安全隐患，采油二厂通过优化完善网络架构、部署内网安全系统、建立健全安全保障体系3个安全控制策略，构建起内网安全整体解决方案。

4.1 优化完善网络架构

通过建设智能网络机房、服务器虚拟化应用、建立灾备系统等策略，建立具有高性能和高可靠性的信息化基础网络设施，使网络达到最佳运行状态，实现企业信息化的物理安全和网络安全。

(1)智能网络机房建设。集成了机房环境及动力设备监控系统、供配电系统、UPS不间断电源、精密空调系统、漏水检测系统、消防系统等，可以对机房主要设备的运行状态、温度、湿度、供电的电流电压频率、配电系统的开关状态、测漏系统等进行实时监控、声光报警并记录历史曲线数据，为机房高效的管理和安全运营提供有力的保证。

(2)服务器虚拟化应用。以VMware Infrastructure套件为软件平台，4台IBM HS系列刀片服务器和1台IBM DS3512高速存储为硬件平台，构建虚拟化群集应用环境，实现了高可用性、分布式资源管理、动态迁移等功能。有42套应用系统整合到虚拟化平台中，在确保系统可用、减少系统中断时间方面发挥了较好的作用，同时解决了系统不兼容导致的服务器低负荷运转和硬件资源紧张的问题。

(3)建立灾备系统。根据公司数据集中规划，采油厂生产Oracle数据库已统一集中到油田公司，采油厂主要对应用服务器的程序和数据进行备份。经多方案对比，采用业内领先的Veritas NetBackup作为备份软件平台，DELL PowerVault MD1000存储作为硬件平台，构建网络数据存储备份系统，实现了网络数据自动化集中式备份，具有高可靠性、易管理、低成本的特点。当面对系统硬件故障、人为操作失误或是黑客的攻击时，依然能切实保证数据的完整性。

4.2 部署内网安全系统

在整个内网中，终端计算机占了网络节点的90%以上，显然是安全管理的重点和难点。通过部署桌面安全系统、病毒防护系统、身份认证系统等措施，将终端计算机全部保护起来，以保障网络安全和信息安全。

(1)桌面安全系统

按照中国石油统一规划，部署应用了北信源VRV内网安全系统，主要包括软硬件资产管理、终端安全加固、补丁分发管理、用户行为监控审计等功能。详述如下：

.软硬件资产管理

通过强化用户的入网注册机制、IP和MAC网络地址管理、网卡管理等功能，有效地规范了网内终端注册管理机制。系统能实现包括外设在内的硬件状态信息、软件状态信息(客户端补丁安装情况、应用软件等)、连网情况信息、资产信息的追踪与报警等管理。

.终端桌面安全加固

对客户终端安全软件资源进行统一监控，网络管理员可根据条件查询指定软件和违规软件的安装情况，对违反规定而致安全防护措施薄弱的客户端进行提示和断网等处理，以此提醒或者切断可能成为传染源的主机，防患于未然。特别地，系统支持对防病毒软件安装及版本的检查，了解网络中的杀毒软件安装状况，必要时通过此系统强制为客户端安装防病毒程序，恶意软件免疫功能则通过插件安装的统一安全设置而保护主机免受潜在威胁的侵害。

.补丁分发管理

集补丁安全认证、补丁测试、补丁分发安装等功能于一体，实现补丁测试、认证、分发综合管理等功能，将认证后的补丁通过统一管理平台向用户网络终端进行配送，确保用户最终应用补丁的安全性，逐步形成统一、稳定、及时的补丁分发机制，避免由于终端脆弱性而导致的恶意入侵及病毒传播，同时合理控制网络流量防范拥塞，有效保障内网的正常稳定运行。

.用户行为监控审计

将安全防范的重点从设备本身转移到设备的使用者——终端用户行为上，通过技术手段使各种管理条例落实，增强用户的安全和保密意识，保护内部信息不外泄。系统通过对用户上网访问行为、各种文件操作、网络文件输出等行为进行监控，并对审计结果形成了翔实的报表，有效地保障信息安全，规范人员安全行为，强化安全意识。

.报警和报表管理

针对内网终端数目庞大、类型复杂的特点，提供了软硬件资产、报警、状态及其他情况汇总报表，有效地提升了管理效能，方便网络管理人员掌握网络情况，对网络运维情况和违规行为等做到了有据可查，及时处理出现的问题。

(下转第478页)

好地实现了原子情感对象的扩展。本文方法在 NLP&CC2013 中文微博评测中获得了优于评测平均水平的结果，证明了该方法的有效性。

本文下一步的工作包括：研究建立完善的句法依存规则集，研究适合的指代消解策略。

参 考 文 献

[1] 宋双永，李秋丹，路冬媛. 面向微博客的热点事件情感分析方法[J]. 计算机科学，2012，6(39)：226-228

[2] Thelwall M，Buckley K，Paltoglou G. Sentiment in Twitter events[J]. Journal of the American society for Information Science and Technology，2011，62(2)：406-418

[3] 姚天昉，程希文，徐飞玉，等. 文本意见挖掘综述[J]. 中文信息学报，2008，5(22)：71-79

[4] 杨亮，潘凤鸣，林鸿飞. 基于组块分析的评价对象识别及其应[J]. 广西师范大学学报：自然科学版，2011，3(29)：151-156

[5] 宋晓雷，王素格，李红霞. 面向特定领域的产品评价对象自动识别研究[J]. 中文信息学报，2010，1(24)：89-93

[6] 王卫平，孟翠翠. 基于句法分析与依存分析的评价对象抽取[J]. 计算机系统应用，2011，20(8)：52-57

[7] 谢丽星，周明，孙茂松. 基于层次结构的多策略中文微博情感分析和特征抽取[J]. 中文信息学报，2012，1(26)：73-82

[8] 知网[EB/OL]. [2009-03-12]. http://www.keenage.com

[9] 王卫平，孟翠翠. 基于句法分析与依存分析的评价对象抽取[J]. 计算机系统应用，2011，20(8)：52-57

(上接第 452 页)

(2)病毒防护系统

按照中国石油统一规划，部署应用了赛门铁克终端防护系统 SEP11(Symantec Endpoint Protection)，集成了防病毒、反间谍软件、防火墙、基于主机和网络的入侵防护方案以及应用和设备控制，易于部署和管理，实现全面、强健的端点防护。主要包括以下技术：

．增强型防病毒和反间谍软件

提供优化的实时恶意软件检测，对其加以拦截并修复。它的主要特征包括性能优化和来自 Veritas 的新型深度扫描技术，从而可以发现并移除经常逃避检测的 rootkit。

．新型主动威胁防护

通过利用基于行为的扫描，抵御未知或零时差攻击的威胁。通过设定检测所有行为的运算法则，大幅减少了误报的发生。根据指定的安全策略，设备控制可帮助用户严格限制设备访问权，包括 USB 存储、备份驱动等，从而降低数据丢失的风险。

．新型网络威胁防护

整合了 Generic Exploit Blocking，利用独特的基于漏洞的 IPS 技术。由于这种 IPS 技术是嵌入在网络层级，因此可以在恶意软件进入系统之前加以拦截。

．网络访问控制

对试图接入网络的用户终端进行安全检查，强制用户终端进行防病毒、操作系统补丁等企业定义的安全策略检查，防止非法用户和不符合企业安全策略的终端接入网络，降低蠕虫等病毒在企业扩散的风险。

(3)身份认证系统

通过中国石油电子邮件系统的绑定认证，为应用系统和基础平台提供统一的用户管理、认证服务和权限管理，实现各应用系统的“集中认证”、“统一授权”，提高信息和系统的安全性。

对于勘探与生产 ERP 系统、健康安全环保系统等重点应用系统，基于严谨的加密算法与密钥管理机制，采用高安全性的 USBKey 数字证书认证方式，保障办公自动化流程，控制对敏感信息的访问。

4.3 建立健全安全保障体系

建立健全针对信息化安全管理的整套体制，包括管理组织、制度、措施等，保障物理安全、网络安全和信息安全。

(1)建立健全安全管理组织。成立以信息主管领导、网络管理员、兼职计算机管理员等组成的多级安全管理体系，信息主管领导负责安全体系的规划以及部门间的协调工作，网络管理员负责制定安全策略和组织技术实施，兼职计算机管理员负责安全措施的具体实施。

(2)建立健全安全管理制度。我厂相继发布了《采油二厂计算机信息网络管理规定》、《采油二厂重要生产岗位计算机使用管理规定》、《采油二厂门户网站运行维护管理实施细则》、《采油二厂新闻宣传保密审核有关规定》等多项安全保密规定。

(3)制定完善应急处置预案。严重的网络安全问题(如系统设备故障或大范围病毒感染等)处理起来会特别复杂，针对特定的安全问题，制定了《信息化业务应急处置预案》，包括网络应急处置预案、信息门户应急处置预案、应用服务器应急处置预案 3 部分。每年定期进行应急处置预案模拟演练，既提高了网络管理人员的应急响应能力，又使应急预案本身得到了检验和完善。

(4)加强网络日常管理。定期进行操作系统安全策略的维护和检查、系统和数据的备份、分析网络安全事件日志、设备和系统的日常维护等工作。通过加强网络管理，保证了网络的安全可靠运行。

(5)开展网络安全教育。采取多种形式(如网络安全知识培训、签订保密承诺书、保密专项检查等)，对员工开展网络信息安全教育，普及安全知识、小窍门，让员工自觉地参与到安全保护中来，认真执行安全策略，减少安全漏洞，避免内部泄密和攻击等安全事故的发生。

结束语　内网安全是一个系统工程，“三分技术，七分管理”，管理是内网安全的核心，技术是安全管理的保证，任何单一的技术或产品都无法满足网络对安全的要求。我们必须从内网安全管理的全局视角出发，全面整合利用准入控制、网络监控、权限管理、身份加密等多种手段，将管理、技术、人员进行有机结合，在企业内部构建一个立体化的整体安全网络，才能实现真正意义上的内网安全，降低信息泄漏风险，确保各项业务工作正常有序运行。

参 考 文 献

[1] 杨义先，钮新忻. 网络安全理论与技术[M]. 北京：人民邮电出版社，2003

[2] McCarthy L. 信息安全：企业抵御风险之道[M]. 北京：清华大学出版社，2003

[3] 方晨. 计算机病毒与防治[M]. 上海：上海科学普及出版社，2005