 DOI: https://doi.org/10.12345/gcjsygl.v5i18.8461

# Analysis on the Safe Operation and Protection of the Information Network

**Wei Wu**

Beijing Branch of Hunan CRRC Times Communications Signal Co., Ltd., Beijing, 100070, China

**Abstract**

With the rapid development of the Internet, the network information office is particularly important, but then, the information security problem is increasingly prominent, the network information security boundary defense system with firewall as the core can only meet the general needs of information security construction, but cannot meet the protection problem of the core business. Based on what the author has seen and known in his job, through a simple analysis of the safe operation and protection of information network, this paper points out the problems existing in enterprise information security in the emerging stage, and takes the internal and external network isolation and transformation project as a case to provide some reference for the company.

**Keywords**

information network; network security; network operation protection

# 浅析信息化网络安全运行及防护

吴为

湖南中车时代通信信号有限公司北京分公司，中国·北京 100070

**摘　要**

随着互联网的快速发展，企业的网络信息化办公显得尤为重要，但随之而来的，企业的信息安全问题日益突出，仅仅以防火墙为核心的网络信息安全边界防御体系只能够满足信息化安全建设的一般性需求，却不能满足公司核心业务的保护问题。论文通过笔者在工作岗位上的所见所知，通过对信息网络安全运行及防护进行简单分析，指出现阶段企业信息安全存在的问题，以内外网隔离改造项目为案例，为公司提供一些借鉴和参考。

**关键词**

信息化网络；网络安全；网络运行防护

## 1 引言

网络安全是信息化的基石。没有网络安全，信息化发展得越快，危害的可能性就越大。互联网的发展和应用带来了网络攻击、网络恐怖主义、网络盗窃、网络欺诈等一系列安全问题，尽管不少企业已经建立了完善的安全体系，但是网络在运行过程中会受到各种因素的影响，从而产生更多的安全问题。我们应该深入分析网络运行过程中的潜在问题，采用先进的保护手段，确保网络在运行过程中更加安全高效。

## 2 信息网络安全的定义

网络安全是指保护网络系统中运行和存储的硬件、软件和数据免受因意外或恶意原因造成的损坏、更改、泄露和非法应用，系统能够持续可靠地运行，网络服务不会受到影响，防止异常中断，有效保护网络信息。随着现代信息网络的飞速发展，各行各业都涉及网络安全的问题。根据 360 威胁情报中心的数据，在中国境内发起攻击目标的国际 APT 组织共有 38 个，攻击范围覆盖全国，可以说未来网络空间就是大国博弈的新战场，企业网络安全也成为不可松懈的一部分。

## 3 企业信息安全存在风险

据统计，瑞幸“云安全”系统共截获病毒样本 5000 多万个，病毒感染 29 多亿。而随着企业大量信息的采集和存储以及公共网络通信和传输、信息系统的分析和应用等功能，其涉及的设备和系统越来越多，网络传输压力越来越大，信息集成融合度越来越高，其对外暴露的设备接口、网络设备、通信链路、数据协议等很多方面都缺少安全防护，这大大增加了遭受恶意攻击的风险[1]。攻击者可以通过非法访问设备，非法入侵网络，攻击破坏应用平台，以窃取、篡改、伪造数据等手段入侵设备、网络、系统，从而给企业造成不可估量的损失。

【作者简介】吴为（1985–），中国北京人，本科，从事网络安全研究。

## 4 信息网络安全防护与运行的构建

### 4.1 内外网隔离

笔者所在公司是一家上市公司，集研发、生成、制造、销售等为一体。主要从事轨道交通方面的研究和市场推广，包括轨道交通信号系统、轨道交通列控系统、城际铁路信号系统等。作为中国电气化铁路事业的引领者，公司长期致力于信号系统方面的研发及国产化，掌握的自主核心技术已经大批量投入生产制造，并参与国内及国际竞争，市场份额已达国内占用率的 70%，正在努力实现将中国的铁路带出去，带到世界的各个角落。

作为中国铁路信号产业核心研发的研发基地，企业的信息安全能力非常重要，对于拥有核心技术的企业就更为重要。随着信息技术的发展，企业的技术资料存在着很高的安全隐患，一旦丢失，损坏或者被窃都将带来很大的损失，所以为了增强企业核心数据机密的安全性，我们需要对公司的网络进行隔离。如果要解决信息网络安全这一问题，必须将公司的网络进行隔离，划分为双网，将传统意义上的有线传输改为有线和无线隔离传输，有线部分作为公司内网，进行企业办公和核心系统的环境，外网作为对外业务和查询资料的环境，内网和外网物理隔离，在某种意义上这样可以防止外部的入侵，可以很大程序上保证公司网络传输的安全性。将核心业务系统处于内部网络，其余业务处于外部网络，如果需要将信息从内部网络传递到外部网络，必须经过严格的签审流程才可以开放，这样既使得企业的核心技术得到保护，也能解决企业业务信息传递的连续性。通过将内网和外网进行物理隔离，可有效地防止外部非法入侵和病毒感染，防止企业内部数据信息泄露，从而有效保证企业信息安全（如图 1 所示）。

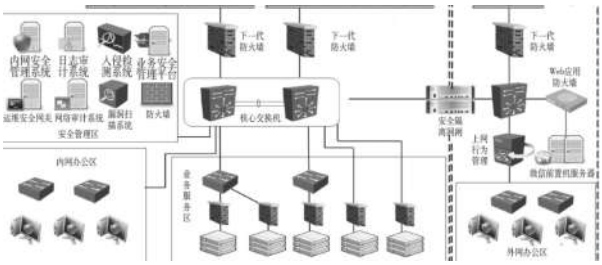

图 1 内外网隔离实施图

### 4.2 建设完善的防御体系

在网络系统安全维护过程中，需要建立完善的防御体系，防范安全威胁。 防御系统主要存在于网络的分离层，用于保护系统结构，提高网络运行的安全系数。 在构建系统网络结构的过程中，可以阻隔外部通信干扰； 员工还可以搭建入侵检测系统，拦截病毒； 很多监控系统都安装在室外，在开放的运行环境中提高了对自身安全等级的要求。为了保证自身的安全，还可以从数据源上加强自身的安全性，从芯片、硬件结构以及操作系统等方面综合采取措施，以提高整体的安全性 [2]（如图 2 所示）。

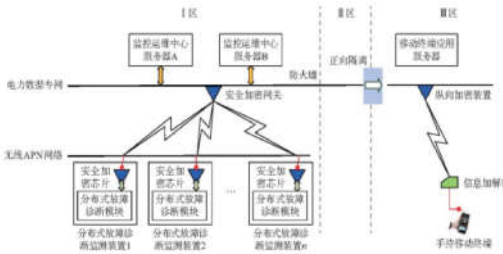

图 2 安全系统整体结构

### 4.3 构建科学合理的管理体制和运行机制

网络信息安全的威胁首先来自人为因素。目前，中国企业在保障体系方面还比较薄弱。一旦出现人为因素造成的网络安全攻击，企业网络信息的隐患就会时刻威胁到网络的生存状态，企业信息安全的隐患就会非常明显。此外，还存在机制不完善、管理层面缺乏监督等问题。网络信息管理是提高网络信息安全的重要手段，可以在一定程度上保证计算机系统中信息的安全。一旦管理出现问题，网络信息的安全就难以保证 [3]。例如，信息系统运营商保密意识薄弱，对重要信息不加密。专业人士可能会利用其职位进入系统窃取信息用于非法目的。

综上可知，必须要建立科学合理的管理体制：①对明确收集使用企业信息的程序和限度提出考验，部门之间可互相监管并制定相应制度；②定时开展培训，培养员工的保密意识；③设置相应的惩罚制度，将保密意识贯穿企业文化当中。

## 5 结语

在信息化时代，加强信息安全防护，需采取行之有效的计算机网络安全防护技术及其措施，创建良好的信息安全环境，加大大数据的应用，只有确保计算机数据信息的安全，才能保证计算机网络持续可靠的运行，才能为企业正常运行保驾护航。

### 参考文献

[1] 彭丽宇,张进川,苟娟琼,等.地方铁路机车智能运维系统信息安全防护体系研究——以朔黄铁路智能运维系统为例[J].北京交通大学学报(社会科学版),2019(3):111-119.

[2] 袁骏毅,潘常青,宓林晖.基于等级保护2.0标准体系的医院信息化安全建设与研究[J].中国医院,2021,25(1):72-73.

[3] 徐玉芬.信息化时代计算机网络安全防护技术研究[J].网络安全技术与应用,2021(5):170-171.