 DOI: https://doi.org/10.12349/iser.v5i6.2951

The Construction and Operation and Maintenance Countermeasures of Enterprise Information Network Security Management Are Discussed

Bin Yuan

Air China Changchun Control Technology Co., Ltd., Changchun, Jilin, 130000, China

Abstract

With the rapid development of China's social economy, all walks of life have obtained certain opportunities for development, under the influence of the current era, enterprises should keep up with the pace of development of The Times, use modern information technology to carry out the actual operation work. However, from the current actual situation, there are still many problems to be solved. Based on this, this paper mainly analyzes the construction of the enterprise information network security management method, from the perspective of operations, gives some targeted information network security control, and in the process, the network maintenance control in the actual situation, so as to help further reduce the security problems in the network operation.

Keywords

information network; security management; construction and operation and maintenance; countermeasure analysis

刍议企业信息网络安全管理的建设与运维对策

袁彬

中国航发长春控制科技有限公司，中国 · 吉林 长春 130000

摘　要

随着中国社会经济的飞速发展，各行各业都从中得到了一定的发展机遇，在当前时代的影响下，企业应紧跟时代发展步伐，使用现代化信息技术开展实际运营工作。但是，从当前实际情况上看，此项工作还有诸多问题有待解决。基于此，论文主要分析了企业信息网络安全管理中的建设办法，从运维的角度出发，给出了一些针对性强的信息网络安全管控意见，并在这个过程中，对网络运行维护管控中实际情况进行探讨，从而协助进一步降低网络运行中的安全问题。

关键词

信息网络；安全管理；建设与运维；对策分析

1 引言

在现代科技高速发展的今天，信息技术网络已逐渐渗透到国民的日常工作与生活中。信息化时代对中国社会经济的发展起到了巨大的推动作用，但其内在问题也给企业的日常运营活动带去了诸多的隐患和问题。基于此，企业必须不断强化信息网络安全管控工作，营造一个良好、健康、和谐的网络环境，以此让中国经济与社会得到更加持续的发展 [1]。

2 企业信息网络安全管理的建设与运维的重要性

在当前时代的影响下，企业在实际运营过程中，应全面使用现代化信息技术，从而让企业自身得到更宽广的发展空间。企业的运营设计、生产流程等方面的工作，是其内部人员长时间工作所得到的结晶。所以，在运营工作中融入信息化网络技术，能够为企业提供针对性的发展指导，给员工供给源源不断的工作动力。但是，若网络平台中的数据被泄露出去，则会给企业带去巨大经济损失的同时，也会让其失去市场竞争力，甚至还会导致企业破产问题的出现。从当前实际情况上看，由于网络环境的变化，各种商业信息泄露问题屡见不鲜，所以信息网络安全管控工作逐渐成为企业内部管理人员的关注重点，更是当前企业发展过程中的重要课题，由此可以看，企业信息网络安全管控建设与运维的影响和意义，见表 1。

【作者简介】袁彬（1989–），男，中国吉林榆树人，本科，工程师，从事网络安全研究。

表 1 网络设备安全

物理设备安全	企业应加强网络设备的物理安全措施，如实施门禁措施、安装摄像头等，防止未经授权的人员进入设备。此外，钥匙设备还应配备密码锁或闪光锁等防护措施
配置管理	确保网络设备配置信息的安全，防止非法人员修改配置。使用 ACL（Access Control List）等配置管理工具限制设备访问，防止非法修改
固件和软件升级	定期升级网络设备的固件和软件，修复已知的安全漏洞和缺陷。及时安装厂商发布的安全更新，避免已知攻击
访问控制	采用严格的访问控制策略，对不同的用户进行权限管理，确保只有授权的人员才能访问敏感数据和系统。此外，应定期审查和更新权限设置，以避免滥用或泄漏权限
数据备份与恢复	建立完善的数据备份恢复机制，保护企业重要数据不丢失。定期备份数据，保证备份的安全性和可靠性。它可以在数据丢失或系统崩溃的情况下快速恢复

3 企业信息网络安全管理中的现存问题

3.1 防火墙

防火墙是企业信息网络中的重要防线，防火墙作为一种隔离装置，它可以高效分离内网与外网中的信息，并在两网间构建存取权限。防火前不但能够预防外界对企业内部系统的侵扰，而且还能够对黑客起到一定的抵御作用。由此也可以看出，防火墙具有安全性高、稳定性好、管控便捷等方面的特点，可是其自身也存在一些问题，比如：防火墙无法较好地解决网络病毒以及计算机系统等。基于此，防火墙并不是万能，它在企业信息网络运行与管控活动中也有一定的缺陷。

3.2 病毒侵入

随着时代的发展，计算机网络逐渐被企业所普及，它不但让国民的生活更加充实，而且也大大提高了企业的生产力。但是，随着计算机网络的应用和普及，电脑病毒也随之泛滥，这严重威胁了企业信息网络的安全性。电脑病毒作为一种由人员编写的，能够破坏电脑资料的一种系统，它能够影响计算机的正常工作，以及其指令的有序传达。由于电脑病毒是高度隐秘的，所以一般难以察觉，而且传染力极强，病毒能够在网络上迅速蔓延，有关工作人员很难对其进行有效的管控。现在电脑病毒的种类越发多样化，一些病毒占用了计算机中的大量内存，而另一些则是以损坏系统的资料为主。不管是何种病毒，它都会对计算机的正常工作造成影响，并且会对企业信息网络的正常运营与管控造成一定威胁。

3.3 系统的运作

在计算机网络平台中，操作系统是电脑的“心脏”与“灵魂”，所以其安全问题非常重要。操作系统在不同计算机中是不一样的，当操作系统发生故障时，会导致大量命令不能被正确执行，这不仅会降低整个系统的工作效率，而且还会对信息网络的运行与管控产生影响 [2]。

3.4 缺乏有效的安全管理手段

随着信息化时代的发展，各类信息技术得到了快速的应用，但是许多企业对信息网络运营和管控工作的方式却没有做到及时更新，从而让其不能满足当前时代的发展需要。其中既有资金上的原因，也有技术支撑、安全管控机制不健全等方面的原因。现阶段，企业信息安全管控模式仍停留在过去固有的工作模式中，已无法满足新形势下的企业信息安全管控工作的需要。比如：目前网络安全管控办法都是以事后管控为主，缺少对突发问题的早期监察与预警，从而让有关工作人员难以对信息网络安全管控质量进行有效的保障。

3.5 体制上的缺陷

现阶段，在企业信息网络安全管控工作中，存在着信息不对称等方面的问题，这就需要有关工作人员必须不停健全和完善现有的信息网络安全管控体系，从而提高信息网络运维与管控工作的可靠性。受各种因素的影响，此项工作仍缺少专业化的技术支持，也没有针对性的制度保障，从而让实际工作中的各类问题很难在第一时间被发现，这种情况会严重影响到企业信息网络安全管控工作的落实和开展。

3.6 工作人员的安全意识淡薄

在当今社会，现代化信息技术已渗透到各个领域。但是，有些工作人员对互联网的性质还不甚了解，在企业信息网络应用方面，由于其自身安全观念不强，极易出现操作失误、系统失效等方面的问题，从而给信息网络安全管控工作带来了很大的隐患。另外，由于人员欠缺电脑防病毒意识，致使计算机系统中存有大量的病毒，这给计算机的有序运行带来了极大的安全风险。

4 企业信息网络安全管理建设与运维的举措

4.1 加速企业间的联网隔离

由于现代化信息平台不受空间等方面的限制，其使用范围非常灵活，所以企业可构建一个较大的网络结构，并根据结构层级来落实和传达各类信息资料。在这个过程中，有关工作人员应不断提高自身的信息传输安全观念，并且还应对此项工作进行实时监察，从而确保各类信息数据的传输过程中不会受到影响，在确保信息网络运维和管控工作稳定性的同时，提高企业自身的信息网络运维品质。

4.2 对终端入网进行标准化、统一化管控

为提高企业信息网络安全管理建设与运维工作的安全性，有关工作人员可使用身份验证软件对各端口开展身份验证活动，从而预防外界信息的入侵。技术人员应明确基线，并监察终端平台，从而确保网络信息平台的可靠性。在这个过程中，企业还应施行运营管控人员实名登记，实时掌握使用人员的动态记录，从而让日后的问责活动更加便捷。

4.3 增强使用者的安全保护意识

现阶段，企业内部各部门应不断加强使用者口令管控，以此提高信息网络的运维和管控工作的可靠性。需要注意的是，信息网络密码不应设定得太过简单，而且还应定期对其进行更改。此外，信息网络运维管控工作人员还应使用用户权限设定，对各层级的用户开展相应的限制，从而规避潜藏问题的出现。同时，由于企业信息网络自身的问题，导致其时常被黑客所利用，所以为保障系统的安全性，有关工作人员有权强制关闭掉相应的业务，可只保留必需的工作接口。

4.4 对各类网络基础建设进行持续改进

在企业信息网络安全管理建设与运维工作中，企业要想做到真正意义上的安全管控，就应在现有的工作基础上，对各类基础设备开展优化和完善，从而提升信息网络的安全防控水准。比如：在网络信息平台中设置避险装置，并安排专人对其进行严密的监测，从而确保物理环境不会对其产生影响，以此提高其物理可靠性[3]。此外，技术人员还应不断提高对核心领域的安全管控，对个别安全等级较高的用户，可使用远程监管的方式，来提高其身份验证和使用安全性，以此保证企业内部各类数据的管控效果。

4.5 采用分布式的监测与管理方式开展工作

随着中国社会经济的飞速发展，现阶段，在分布式监测与管控平台能够在保证系统稳定工作的前提下，可有效增强信息网络运维工作的安全性。在监控工作期间，技术工作人员可作为防火墙或利用监控软件来执行监控任务。同时，也可使用加强网络安全侦测的方式，有规律地辨识出各类安全隐患，并以此为基础，构成相应的安全运营报表。此外，经过使用直观的操作界面，可实现作业人员的安全作业，从而将危险因子划分为不同危险程度的同时，大幅提升了企业的安全风险管控水平。

4.6 构建完善的安保制度

为了不断提高企业信息网络安全管理建设与运维水平，有关工作人员持续优化信息网络平台安全防控体系，加强对终端设备的管控。在健全安全预警机制的基础上，企业内部工作人员必须加强对病毒的监察与管控，定期对信息网络平台进行病毒筛查工作，并以此为基础，对系统中的问题和漏洞进行及时、有效的修补。此外，企业还应经过建立防火墙等举措，有效管控因网络问题而导致的各类风险问题，以此协助企业削弱信息网络风险，让其能为企业的常态化发展保驾护航[4]。

5 结语

综上所述，随着中国现代化信息技术的飞速发展，在当前时代的影响下，企业内部工作人员必须不断优化完善现有的网络设备，提高信息网络运维和管控工作的质量，以此保证此项工作的安全性和可靠性。在这个过程中，企业还应主动使用分布式监测管控等方式，建立一个适合自己发展的安全预防体系，从而在不断提高现有信息网络运维和管控安全系数的同时，协助企业在激烈的市场竞争中获得更大的发展空间和机遇。

参考文献

[1] 杨战武.刍议高校网络安全现状及风险策略[J].网络安全技术与应用,2023(10):85-87.

[2] 樊海峰,余坤.刍议如何加强企业网络安全管理[J].通讯世界,2020,27(8):99-100.

[3] 何敏.电力企业信息网络安全刍议[J].华东电力,2002,30(10):28-29.

[4] 王东方,李峥,郭伟.刍议网络安全分析中的大数据技术应用[J].电脑知识与技术,2018,14(24):24-25.