工程管理
Journal of Project Management
第 6 卷◆第 5 期◆版本 1.0◆2025 年
文章类型：论文| 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

企业网络自动化运维安全解决方案研究

魏昌龙
中国电信武汉分公司
DOI:10.12238/jpm.v6i5.8027

[摘　要] 随着信息技术的飞速发展，网络对于人们的生活和工作已经变得越来越重要。与此同时，网络安全问题也日益突出。虽然网络技术的不断发展为企业和组织提供了更好的运维手段，但是在实践中，网络安全问题依然是制约企业和组织运转的重要因素。为了提高运维效率，越来越多的企业和组织开始使用自动化运维技术。但是，自动化运维技术本身也存在一些安全问题。因此，如何保证网络安全与自动化运维之间的相互匹配，是当前亟待解决的问题。

[关键词] 企业；网络自动化；运维安全

Research on security solutions for enterprise network automation O&M

Wei Changlong
China Telecom Wuhan Branch

[Abstract] With the rapid development of information technology, the network has become more and more important for people's life and work. At the same time, cybersecurity issues are becoming increasingly prominent. Although the continuous development of network technology provides enterprises and organizations with better operation and maintenance methods, in practice, network security issues are still an important factor restricting the operation of enterprises and organizations. In order to improve O&M efficiency, more and more enterprises and organizations are using automated O&M technologies. However, there are some security issues associated with automated O&M technology. Therefore, how to ensure the matching between network security and automated operation and maintenance is an urgent problem to be solved.

[Key words] enterprise; network automation; O&M security

引言

在当前数字化和网络化的商务环境中，企业网络安全防护体系的建立显得至关重要。互联网技术和大数据的快速进步改变了企业的运营和管理模式，使数据和信息转变为企业的关键资源。这种依赖性同时也使企业暴露在严重的网络安全威胁之下，这些威胁可能源自外部黑客的攻击或内部员工的误操作和恶意破坏。一旦企业网络遭遇攻击，可能导致数据泄露、业务中断，严重的话甚至触发法律问题和财务损失。加之，政府对网络安全日益重视，并出台并完善了相关法规政策，企业必须遵从，避免遭遇法律风险。因此，构建全面的网络安全防护体系不仅能提升企业的运营能力，保护企业的数据资产，同时也是企业履行社会责任和遵行法规的重要途径。

1、企业网络安全防护体系构建思路

1.1 企业信息网络安全管理系统总体设计

图 1 中，系统的管理级用密钥管理企业信息安全；应用级和防火墙通信，通过网络攻击入侵检测维护系统安全；端系统级传输信息；子网级配置完全设备；直接链路级和物理层有关，规划网络安全。这 5 个层次分层维护了企业信息系统的安全，效率高、可靠性强、资源消耗少。本文的创新点一在于将随机森林算法融入企业信息网络安全管理中，形成一个强分类器，若决策树过多，模型训练速度慢，会出现过度拟合。针对以上不足，本文对随机森林算法做出改进，运用多层次网络安全态势感知框架，评估出企业目前网络安全的状态。本文的创新点二在于将粒子群算法融入企业的网络入侵检测系统中。该算法通用性强，可调参数少，但存在收敛速度慢的问题，不一定能找到最优解。因此，本文将粒子群算法和支持向量机模型相结

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文| 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

合，构建安全状态检测模型。支持向量机算法适应度好，泛化能力强，在与粒子群算法相结合后，解决了“维数灾”问题，提升了企业网络安全状态检测精度。

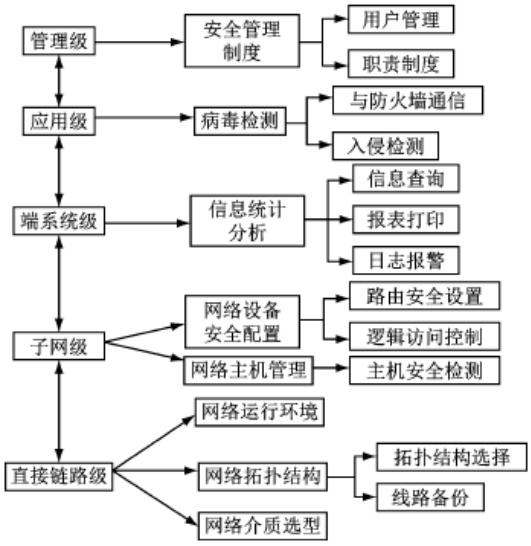

图 1　企业安全管理系统总体框架

1.2 安全策略与管理制度

体系架构设计完成后，接下来就是构建相应的安全策略和管理规程。安全策略描述的是企业在网络安全事件发生时的应对措施，它包括预防、识别、处理和恢复等几个环节。这些都需要根据企业的特定环境，如业务类型、运营规模和可能的威胁等因素来详细制定。同时，管理规程能确保这些安全策略得以有效执行，这涉及员工职责的分配、工作流程的规划、审计监控等方面。这些规程保障了企业网络安全防护体系在其生命周期内，能按照预定的流程和标准运行。

1.3 体系架构设计

在构建企业网络安全防护体系之初，首要任务便是制定体系架构设计。这一设计应根源于企业的业务需求，将企业的运作方式及可能遭遇的潜在威胁纳入考量。在这个阶段，要清晰地识别出防护体系需满足的各项功能，如侵入监测、紧急响应、数据防护等，并对应地设计出各个模块。每个模块应能自主运作，同时与其他模块协同，共同构建起防护网络[1]。

2 企业网络安全存在的问题

一些相关人员缺乏安全意识，不从企业实际发展出发，没有制定科学合理的安全制度，加上企业在网络安全方面的投入不足，没有采取有效的预防措施，相关人员对于网络安全的认识也不足，未能认识到自身行为对网络安全的影响，这种薄弱的员工安全意识也会导致企业的网络系统暴露于潜在的安全风险之下，导致企业的网络安全处于脆弱状态，企业网络安全管理工作难以获得实质性进展。虽然网络技术快速发展，被广泛应用，但网络安全管理却并未得到快速发展与提高，因此导致企业发展受阻。部分企业没有重视网络安全管理，也没有加大这一方面的资金投入，在开展企业网络安全管理工作的过程中未采用先进网络安全管理技术，导致信息安全保护措施和信息维护系统构建的不完善，进而出现信息泄露等事件。当黑客成功入侵企业的网络系统后，通常会全面收集企业的重要的信息数据，并通过植入病毒等手段进行进一步的攻击。这些黑客的主要入侵和攻击手段是在短时间内发送大量邮件，导致企业网络系统崩溃，使得企业员工无法正常使用网络办公，降低了企业的工作质量与效率。

3、企业网络自动化运维安全解决方案研究

3.1 自动化运维技术

（1）自动化运维架构自动化运维架构通常包括以下几个层次：运维自动化平台层、操作系统层、虚拟化层、容器化层、应用层和数据存储层。其中，运维自动化平台层是整个自动化运维架构的核心，包括各种自动化运维工具和技术，提供自动化运维的基础设施和运行环境；操作系统层、虚拟化层、容器化层、应用层和数据存储层是运维自动化的对象和目标，通过运维自动化平台的支持和管理，实现自动化运维的各项任务和操作。（2）自动化运维平台自动化运维平台是自动化运维的基础设施和核心支撑，包括自动化配置管理、自动化部署管理、自动化监控管理、自动化维护管理等模块。自动化运维平台可以提供多种自动化运维技术和工具，如自动化运维脚本、自动化运维工具集、自动化运维 API 和 SDK 等，方便用户进行集成和扩展，实现自动化运维的管控、自动化任务的调度和执行、自动化监控的告警和处理等全面功能。（3）运维自动化工具运维自动化工具是自动化运维平台的核心组成部分，包括自动化配置管理工具、自动化部署管理工具、自动化监控管理工具、自动化维护管理工具等。这些工具可以支持多种自动化运维场景和任务：自动化配置工具可以实现对系统配置的自动化管理；自动化部署工具可以实现对应用程序的自动化部署和升级；自动化监控工具可以实现对系统、应用程序和网络的自动化监控和告警；自动化维护工具可以实现对系统和应用程序的自动化维护和修复。这些工具可以方便用户进行各种自动化运维任务，提高运维效率和减少运维成本[2]。

3.2 严格管理堵塞安全漏洞

有的企业总觉得，现在网络已经达到普及的程度，网络实际上是很简单的事，用不着费太大的精力，交给网管或技术部门就可以了；一般用户认为只要懂得网络就能管理网络安全，这是大错特错的，网络安全管理员一定要经过特殊的培训才能上岗。大量的事实证明，网络出现安全问题都是由于管理不力，用户不会使用或操作不当所造成的。有了网络的基础设施，如果没有相应的配套措施，要避免安全上的问题出现是办不到的，更不能有效地发挥网络的作用，在今后的市场竞争中就不能健康、持续发展。企业信息网络的建立，不是一个单位的事，而是整个信息网络安全的大事，不能因一个单位员工的一个很小的疏忽而影响到整个网络的安全。网络用户间必须要有配合意识，将自己的行为与公司信息网络联系起来，营造一个健康的企业信息网络，需要广大员工的共同努力，安全健康的网络，将对企业办公自动化、数据资源共享等方面产生重大影响[3]。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

3.3 组织管理

企业的安全组织管理必须由上至下，网络安全组织管理架构必须由一把手牵头，并编入各个部门的主要领导。工作组织机构应由主责部门统领，各部门配合，并以安全接口人的方式将工作任务直达各个部门，覆盖所有人员。网络安全管理需要通过制度流程的制定将安全责任落实到各部门，并与各部门绩效挂钩，相关部门各司其职。通过制度流程的实施以及不断完善，规范运营维护人员的运营操作行为。企业安全管理还需要借助安全管理系统（如 SOC）将各系统的安全数据通过安全资产贯穿起来，依照 PDRR 模型，通过工单流转，实现 IT 系统的风险的闭环管控。

3.4 运营管理

安全运营是企业安全策略落地的主要手段。以前的安全运营是以问题管理为导向，等待问题出了再进行弥补，这种亡羊补牢式的管理方式，是以损失为前提，安全人员疲于救火，缺乏前瞻性，不能保证网络安全管理的效率与效果和投入产出比。目前业内的认可的管理方式是系统运营风险管理。该管理方式是先进行风险评估，再科学计算网络安全投入，通过风险管控保障系统业务运营目标的实现。安全运营工作通常包括系统安全评估、漏洞加固、安全监控、安全审计、容灾备份，安全态势感知、安全运营分析、策略改进、网络空间测绘、安全规划、统筹建设等。通常以定期与不定期结合开展，定期可以根据系统安全保障级别需要进行，如每天执行容灾备份；每周开展安全审计；每月全面开展一次系统漏洞扫描风险评估和安全加固、由公司组织开展安全态势和安全运营分析以及对应的工作策略改进；每季度进行一次安全资产探测核对和通行字安全检查；每半年开展一次网络安全基线检查和暴露面核查，开展安全演练验证处置能力；每年开展一次网络安全规划和统筹建设。

3.5 加密技术应用

在信息系统中，数字加密技术使用电子密钥将信息转换为密文，以避免信息在传输过程中被窃取。数字加密技术是一种网络安全保护技术。在应用数字加密技术时，信息经过加密、传递、解密三个环节，保证信息传输的保密性和安全性。加密技术分为对称加密技术和不对称加密技术。但是因为双方使用同一密钥，所以会有泄漏的风险。不对称加密技术则采用两个独立的密钥，加密算法比较复杂。近年来，由于各种密码技术的发展，出现了对称加密与不对称加密相结合的方法，即“混合加密技术”。该方法吸取上述两种技术的优点，在保障信息安全方面有着更大的优势。数字签名与数字证书也是数字加密技术的一种。数字签名使用公开密钥加密系统进行信息保密。例如，为了保证数据的安全性，网上银行利用私有密钥和数字签名来对信息进行加密。该方法可以有效避免数据伪造、篡改等，因而被广泛地应用于银行等行业。数字证书则是对使用者进行认证，以确保使用者信息与资料的安全性。电子凭证一般包含用户姓名、身份证号码等，其格式规范以 CCITTX.509 为代表。

3.6 用户身份安全验证

网络通信常依赖用户账户名和密码进行登录验证，然而这一验证方式掩盖了一定的风险。一旦犯罪分子通过非法途径获取到用户名和密码，便能轻易地从计算机中获取信息。随着科技的不断进步，现今涌现出多种验证、识别和加密方法。密码的随机生成是最常见的网络安全审查手段之一。然而，为了更有效地增强网络通信的安全性，可以考虑采用加密的量子密码作为集成密码，并对整个系统状态进行解密，从而提升在线交流的安全性。量子密码作为一种高度安全的加密技术，利用量子力学原理进行信息传输和加密，具备难以破解的特性。采用两字密码作为聚合密码，结合系统整体解密操作，能够极大地提高信息传输的安全性和稳定性。

3.7 健全内部安全防御能力

结合企业实际情况，制定了网络安全使用的相关管理制度，从根本上消除了网络安全危害因素，避免因人为因素导致企业网络系统崩溃，工作效率与质量受到影响；建立科学合理的奖惩制度。企业需要科学合理地选择考核评价指标，建立一支由各个部门主要领导与管理员组成的高质量专业网络安全队伍，对企业相关人员进行定期检查，及时了解员工在开展工作的过程中存在的问题，并详细记录员工的实际考核评价结果，将管理目标和责任落实到个人，实行岗位的责任机制。此外，企业应该根据网络的使用情况对相关人员进行奖励，以充分激发他们的工作兴趣和积极性。虽然所有的信息防护软件都有可能被破解，但主要软件的安全系数越高，破解难度也会随之加大，企业选择合适的软件就能加大防护力度，确保企业的业务活动开展环境始终安全可靠，有效减少网络威胁，促进企业高质量发展。

结束语

总之，计算机技术、网络技术的发展非常迅速，网络信息的对抗技术水平也在提高，系统的安全防护措施无疑也应与时俱进，才有可能确保网络系统和网络信息的安全，才能在企业发展、市场竞争中立于不败之地。技术永远不是解决网络安全问题的唯一手段。要营造安全、实用、稳定、永久的企业信息网络，消除网络中的漏洞，解决网络运行中的安全与防护问题，一靠技术，二靠管理。

[参考文献]

[1]李大玮，刘鹏，王璐.基于大数据的网络安全态势感知系统在网络安全管理中的应用[J].中国新通信.2019，24（2）.DOI：10.3969/j.issn.1673-4866.2019.02.061.

[2]周娟.基于大数据的网络安全态势感知关键技术研究[J].电脑知识与技术.2019，17（31）.

[3]王明芬.网络运维信息可视化系统设计[J].电信快报.2019，（7）.DOI：10.3969/j.issn.1006-1339.2019.07.009.

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.