企业网络信息安全体系建设研究

陆 琦 葛 利

（石家庄星安信息安全测评技术有限公司，河北 石家庄 310053）

摘要：随着信息技术的不断发展，企业网络成为商业活动的重要平台。然而，网络安全问题日益严重、不容忽视，是企业稳定发展的关键影响因素。企业及个人必须认识到信息系统本身有着较强的脆弱性与复杂性，控制好病毒传播、黑客攻击与网络犯罪等安全风险，才能够保护企业信息资产不受到侵害。对此，研究探讨了企业网络面临的安全威胁，进一步提出了一个多层次、全方位的网络信息安全体系建设框架，包括入侵检测系统、防火墙技术和交换机配置等技术措施，并结合制定网络安全愿景、健全安全管理制度等管理策略，助力企业网络信息安全体系建设，推动企业现代化、全面化发展。

关键词：企业网络；信息安全；体系建设；策略

企业网络信息安全体系构建是一项系统性工程，且直接关系到企业的生存与发展。作为企业管理者和员工都应当协同合作、扎实推进网络安全体系建设工作。具体来说，首要任务是提高对网络信息安全的重视程度，逐渐完善管理制度、运营机制与技术设备等。相应人员培训、细节管理、日常监管等一一跟进，从内到外提高企业网络信息安全水平，值得我们深入探索与实践。研究对企业网络信息安全体系的建设进行系统研究，旨在为企业提供指导性的建议，帮助企业提升网络安全管理水平，积极防范和应对网络安全风险。

一、网络安全隐患分析

当今，信息技术迅猛发展，企业网络已成为支撑日常运营的重要基础。然而，伴随网络技术带来的便利，各种网络安全威胁随之增多，给企业带来了诸多潜在的安全隐患。最为紧急的就是病毒、木马、钓鱼网站等，能够窃取一些敏感数据，而影响到企业的正常运营。还有信息技术、计算机的普及，增加了数据泄露的风险，使得传统网络边界防御效果大打折扣。部分企业还面临内部威胁，由于员工失误或故意而为，都会对企业产生负面影响。不仅如此，企业在全球化经营中面临的法律法规和文化差异，也会对网络安全管理造成影响。例如，不同国家和地区对于数据保护有不同的规定，企业需要遵守这些规定，以免引发法律风险和信誉损失。同时，企业在跨境数据传输和处理过程中，也需要考虑到数据加密和隐私保护问题。结合以上，我们看到企业网络信息安全隐患涉及各个领域和方面，是一个多方面、多层次的问题，应当计划有效的干预与管理措施，逐步构建出适应现代企业发展的企业网络信息安全体系。

二、企业网络信息安全体系建设要素

（一）入侵检测系统

入侵检测系统（IDS）是一种安全措施，监控网络和系统的运行状况，也确保其资源的机密性、完整性和可用性。IDS 的目标是尽可能发现各种攻击企图和行为，并采取相应的防护措施。根据入侵检测的手段，IDS 又可以分为基于网络和基于主机两种模型。前者通过分析系统内部的数据来判断恶意活动，关注内存、文件是否发生了变化，数据来源是系统重的审计日志。我们可以看到，它是性价比更高的，且监测更加细致，不需要专门的硬件平台和多么丰富的流量支持。后者通过连接在网络上的站点捕获数据包，并对其进行分析，判断是否具有已知的攻击模式。当发现可疑现象时，系统便会发出警告，并向中心管理站点发出信号。基于网络的模型反应速度快、隐蔽性较好、视野更加宽阔、占资源比较少。总之，入侵检测系统保护网络和信息安全，实际应用中可以根据需要选择适当的模型。

（二）IP 安全策略

IP 安全策略基于通信分析，将通信内容与预设的规则进行比较，如果通信符合规则，则允许传输；否则，拒绝传输，以此实现了更加细致和精确的 TCP/IP 安全控制。配置 IP 安全策略的过程是相对简单的，用户可以根据自己的需求和网络环境来设置相应的规则。用户需要确定哪些通信是需要被允许的，哪些是需要被禁止的。然后，根据这些需求来创建相应的规则。例如，设置规则来允许来自特定 IP 地址的通信，或者禁止来自某些特定端口的通信，还可以设置规则来限制通信的流量，以防止网络拥塞或滥用。一旦规则建立，系统也会自动分析与过滤，同样进行相应的步骤，进行网络信息安全管理，对抗潜在威胁与危险因素。此外，IP 安全策略还支持动态更新规则功能，用户可以自己设置修改，不需要重新启动便完成配置。这无论是对企业还是员工来说，都是一项重要的措施，同样值得我们深入探索与实践。

（三）防火墙技术

防火墙技术作为网络安全体系中的不可或缺部分，能够在一定程度上隔离多种病毒、恶意软件、攻击行为等。具体来说，防火墙实现了内外网络不同信任域之间的隔离与访问控制，同时支持单向或双向的控制。不仅增强了网络安全性，还有效记录了网上活动轨迹，为网络安全提供了坚实的防线。首先是对安全性能进行强化，能够对进出数据进行严格检查，过滤可疑访问。其次，它集中管理所有安全软件，实现了经济、高效的安全管理。此外，防火墙监控网络存取和访问，记录详细信息，并在发生异常时及时报警，构成了防火墙在网络安全中的核心地位。除了保护外部威胁，防火墙还关注内部信息的安全，通过对内部网络的划分和隔离，确保局部安全问题不会影响全局网络，体现了防火墙技术在网络安全中的综合价值。总的来说，防火墙技术在网络信心安全中的应用具有积极意义，且经济、有效，是现代企业网络信息安全体系构建的重要基础技术。同时，既是全面安全保护的重要手段，也是企业与个体上网安全的可靠保障。

（四）交换机

交换机在计算机网络中至关重要，在企业网络信息安全工作开展中扮演重要角色。首先，基于交换机的安全体系通过虚拟局域网，能够保证网络的安全性能，实现对不同网络部分的隔离管理。其也能够通过设置控制访问列表，最大限度地禁止非法访问，而加强防火墙功能，提高整个安全体系的过滤能力。此外，在网络端口实施的安全措施，能够确保网络运行的安全性。交换机的主要结构由 MAC 地址和网络交换机端口组成，可以对网络虚拟端口和流量的严格控制，有效提高网络交换机端口的安全性能。而在实际访问过程中，如果主机的 MAC 地址与交换机的信息不符，相应的终端口将自动关闭，以保护网络安全。总之，交换机在计

算机网络中发挥着重要作用，不论是局域网，还是访问控制、端口安全等，都是企业网络信息安全的重要保障，需要各大企业在今后网络安全工作中加强建设。

三、企业网络信息安全体系建设策略

（一）制定网络安全愿景

当今，信息化快速发展，企业网络信息安全是企业发展的重要一部分。制定网络安全愿景是企业对于网络安全的长远规划，包含了企业的核心价值观、技术创新、人才培养等多个方面，以下进行介绍：一是企业要充分重视网络安全工作，并将其列入企业核心价值观之中。企业应将网络安全视为企业战略的一部分，在各个层面强调网络安全的重要性，从高层管理到基层员工，都认识并重视网络安全对企业的重要性。必要的话还应当与企业社会责任、企业建设使命等融为一体，保护用户数据安全、维护互联网络安全，为社会创造更大的财富与价值。二是企业要充分重视技术创新、与时俱进，面对网络威胁与攻击时有足够的“弹药”。企业应关注新兴技术，包括人工智能、大数据等，提高网络安全防护能力。同时，还要进行相关硬件设备、软件更新等工作；更应与科研机构、高校合作，研究网络安全技术，提高企业的研发能力。由此从根本层面增强网络安全防护力，奠定企业网络信息安全的坚实基础。三是企业必须强调合规意识，严格遵守国家和行业的相关法律法规，确保企业的网络信息安全合规；必须关注人才培养与培训，提高员工的网络安全意识和技能，为企业的网络信息安全提供有力支持。总之，制定网络安全愿景至关重要，需要企业在各个方面重视并部署，保证上到企业核心价值观下到企业底层员工都要重视网络信息安全工作，奠定企业长远发展、现代化建设的坚实基础。

（二）健全安全管理制度

要健全安全管理制度，企业首先要明确的就是安全工作的总体目标，与企业业务发展与今后发展息息相关。进一步的，必须制定一系列详尽的安全策略和操作规程，涵盖数据保护、访问控制、身份验证、网络安全监控、事件响应等多个方面，形成一套完整的安全防护体系。在此基础上，企业还需要建立起一套完善的风险评估机制，定期对现有的安全措施进行审查，及时发现潜在的安全漏洞并加以修补。研究认为，还有必要对各部门和员工进行细化责任制度，包括出现问题后的追责制度，以确保人人重视网络信息安全、相关制度与条例执行到位。我们必须指定安全管理人员，专门负责日常的维护工作，还应进行跨部门协作，保证在面对复杂安全威胁时也有人可用、有法可解。此外，安全管理制度建设注重合规性要求，密切关注国内政策、法律法规，及时进行调整优化，确保最新的法律要求能够落实到位，避免企业因为该方面的问题而面临更大的法律风险，避免得不偿失。最后，企业还应将安全管理制度视为动态发展体系，在后续一系列工作中优化完善，扼杀潜在的网络信息安全风险。那么，就要对上述一系列总体目标、操作流程、责任认定、部门协同等优化改进，做好长期的“作战”准备。只有这样，企业员工才能够在整体的带动下关注网络安全工作，意识与技能也不断进步，提高企业整体的安全防护能力。以此构建出完善、合理的企业网络信息安全体系，共同为企业繁荣贡献一份力量，也是企业可持续发展的坚实基础。

（三）强化员工安全意识

上述制定网络安全愿景、健全安全管理制度中均有员工培训一项，本质目的就是提高广大员工的安全意识。但这些远远不够，对员工的培训和后续教育也应当日益完善、建成体系，为共建企业网络信息安全体系做出更大贡献。首先，员工是企业信息安全的第一责任人，只有员工细心、耐心，发现该方面的问题并及时解决，才能够保证企业网络安全系统正常运行，且达到优良效果。在日常工作中，员工往往是企业信息系统的直接使用者，其操作行为直接影响到系统的安全状态。一个不经意的点击，可能就会触发恶意软件的执行；一次不慎的信息泄露，可能导致重要数据的丢失。因此，培养员工对网络安全的认识，使他们能够识别潜在的安全风险，避免不安全的行为，对企业来说是一项重要投资。其次，员工还是企业文化的具象体验，提高其潜在警觉性与意识技能，就是企业整体水平提升与文化塑造的作用显现。当安全意识深入人心，员工在日常工作中自然而然地采取安全措施，这种自觉的安全行为比任何强制性的规章制度都更加有效。再加上一些奖励、激励，相信有更多员工能够自觉遵守规章制度，保持良好的职业素养，坚固企业网络信息安全防线。今后，企业也应当定期进行宣教和培训，模拟攻击演练、安全知识讲座、在线安全课程等，使员工了解最新的网络安全动态，掌握必要的安全防护技能，增强他们的责任意识。

（四）建立应急响应机制

应急响应机制是企业网络信息安全体系中的重要一环，企业应定期进行网络安全风险评估，识别可能存在的安全威胁和薄弱环节，以此为基础制定出针对性的应急预案。以此对网络安全威胁的识别、评估等进行充分响应，明确发生时、发生后的各类处理办法，面对真实网络安全威胁时有可靠的方案进行处理。企业还应当建立一套完善的监控方案，跟进网络运行状态，及时发现异常。同时，快速定位问题情况，配合专业的网络安全队伍抵御外部攻击、共同面对威胁，或是找准问题后一击而中，在第一时间内对安全事件进行分析判断，采取有效的应对措施。最后，应急响应机制的建设也需要得到企业文化的支持，企业应倡导安全文化，提高员工的安全意识，使他们明白网络安全的重要性，了解应急响应的必要性，积极参与到应急响应的工作中来。总的来说，建立应急响应机制同样十分重要，是各大企业应当重视管理的部分，来保障企业的正常运营。

四、结束语

综上所述，企业网络信息安全体系是一个复杂工程，涉及技术、管理、人员多个方面。企业只有部署安全设备、软件，在管理上细化制度条例，在员工培训与应急预案等方面下功夫，才能够保证企业网络信息的安全。今后，企业应当充分认识网络信息安全的重要性，投入必要的资源与精力支持，不断创新信息安全技术、管理模式，建立起适宜自身发展需要的网络信息安全体系。尤其要以网络信息安全保证自身的市场竞争优势，在现代化背景下不断创新、持续发展，奠定企业长久发展的基石。

参考文献：

[1] 董金玉，肖汉，刘石 . 大数据背景下石油企业网络信息安全管理策略研究 [J]. 中国管理信息化，2023，26（10）：94-96.

[2] 曾莎莉 . 新常态下数智化转型企业网络信息安全体系建设策略 [J]. 信息系统工程，2022（09）：111-114.

[3] 靳峰 . 大数据时代背景下企业网络信息安全问题及防护探讨 [J]. 现代工业经济和信息化，2022，12（02）：124-125+129.

[4] 林琳，刘力华，谢娟 . 油气企业网络信息安全的人因失误分析及对策建议 [J]. 信息与电脑（理论版），2021，33（23）：222-224.

[5] 刘文亮 . 网络信息安全对电网企业数据保护作用的应用研究 [J]. 长江信息通信，2021，34（05）：118-120.

[6] 虞宏烨 . 基于大数据背景下企业网络信息安全技术体系分析 [J]. 网络安全技术与应用，2021（02）：102-103.