政企单位网络安全防护体系的构建与优化研究：新形势下的挑战与对策

刘韬

益阳市消防救援支队，湖南益阳，413000；

摘要：随着数字化转型的深入推进，政企单位的业务运行与网络环境深度融合，网络安全已成为保障其稳定发展的核心要素。然而，新形势下网络攻击手段的迭代升级、内部管理漏洞的凸显以及合规要求的不断提高，使政企单位网络安全面临严峻挑战。本文首先分析新形势下政企单位网络安全面临的外部威胁、内部管理、技术滞后及合规压力等挑战；其次，从技术架构重构、管理机制完善、人员能力提升、合规体系落地四个维度提出网络安全防护体系的构建方案；最后，给出体系实施的保障措施，旨在为政企单位提升网络安全防护能力、实现可持续发展提供理论参考与实践指导。

关键词：政企单位；网络安全；防护体系；数字化转型；零信任架构

DOI：10.69979/3041-0673.26.02.091

引言

随着数字化转型的深入推进，政企单位的业务运行与网络环境深度融合，网络安全已成为保障其稳定发展的核心要素。然而，新形势下网络攻击手段的迭代升级、内部管理漏洞的凸显等问题，使政企单位网络安全面临严峻挑战。本文首先分析新形势下政企单位网络安全面临的外部威胁、内部管理及技术滞后等挑战；其次，从技术架构重构、管理机制完善、人员能力提升三个维度提出网络安全防护体系的构建方案；最后，给出体系实施的保障措施，旨在为政企单位提升网络安全防护能力、实现可持续发展提供理论参考与实践指导。

1 新形势下政企单位网络安全面临的挑战

1.1 外部威胁日益复杂且隐蔽

攻击手段迭代升级：传统的网络攻击以窃取简单信息、破坏网络通断为主，而当前攻击手段呈现出智能化、多样化、产业化的特点。攻击者利用人工智能技术精准定位目标漏洞，通过钓鱼邮件、供应链攻击、物联网设备入侵等方式突破防护边界。其中，供应链攻击通过劫持政企单位依赖的第三方软件、硬件或服务，实现对核心系统的渗透，此类攻击隐蔽性强、影响范围广，凸显了供应链安全的脆弱性。

攻击目标针对性增强：攻击者不再盲目发起攻击，而是针对政企单位的核心业务系统、敏感数据资产制定精准攻击方案。政府单位的政务数据、涉密信息，企业的客户数据、商业机密、财务信息成为攻击重点。APT攻击更是以长期潜伏、持续窃取高价值信息为目标，其攻击周期长、技术难度大，给检测与防御工作带来极大挑战。

1.2 内部管理漏洞凸显风险隐患

安全意识淡薄：部分政企单位员工对网络安全重视不足，存在违规操作行为，如使用弱密码、随意点击不明链接、外接未经授权的存储设备等，这些行为成为网络攻击的重要突破口。实践表明，大量网络安全事件的发生都与内部人员的违规操作或疏忽大意密切相关。

权限管理混乱：部分政企单位未建立完善的权限管理机制，存在权限分配不合理、权限回收不及时等问题。员工可能拥有超出其岗位职责的访问权限，导致数据泄露风险增加。同时，第三方合作机构（如外包服务商、供应商）的权限管理缺乏有效管控，进一步扩大了内部安全风险。

应急响应能力不足：多数政企单位虽制定了网络安全应急预案，但缺乏常态化的应急演练，预案的可操作性与实用性不强。在遭遇网络攻击时，往往出现响应不及时、处置流程混乱、信息上报不规范等问题，导致攻击造成的损失扩大。

1.3 技术防护体系滞后于发展需求

传统边界防护失效：随着云计算、移动办公的普及，政企单位的网络边界从物理边界转向逻辑边界，传统的防火墙、入侵检测系统等边界防护设备难以应对“边界消失”带来的安全挑战。攻击者可通过移动终端、云服务等途径绕过边界防护，直接攻击内部系统。

数据安全防护薄弱：政企单位在数据采集、传输、存储、使用、销毁全生命周期的安全防护存在短板。数据分类分级不明确，核心数据缺乏加密、脱敏等保护措施；数据传输过程中存在泄露风险；数据访问行为缺乏有效监控，难以实现数据泄露的溯源与追责。

安全技术整合不足：部分政企单位引入了多种安全技术与产品，但各产品之间缺乏有效联动与数据共享，形成“安全孤岛”。安全管理平台无法实现对全网安全态势的实时感知、分析与预警，难以做到对网络攻击的精准识别与快速处置。

1.4 合规压力不断增大

近年来，行业监管部门制定了相应的网络安全标准和规范。政企单位如果无法满足合规要求，将会面临行政处罚、声誉损害等风险。不过，部分政企单位对合规要求理解不够深入，合规体系建设迟缓，难以实现合规管理与业务发展的同步推进。

2 政企单位网络安全防护体系的构建方案

2.1 重构技术防护架构，强化全方位安全防御

引入零信任架构：基于“永不信任，始终验证”的核心原则，构建零信任安全架构。通过身份认证、权限最小化、持续验证、微隔离等技术手段，实现对用户、设备、应用、数据的全方位管控。建立统一的身份认证与权限管理平台，实现用户身份的集中管理与动态授权；采用微隔离技术划分网络区域，限制不同区域之间的横向访问，防止攻击扩散；对用户的访问行为进行持续监控与风险评估，一旦发现异常行为立即阻断。

完善数据全生命周期安全防护：首先，建立数据分类分级机制，根据数据的敏感程度将数据划分为不同级别，针对不同级别数据制定差异化的保护策略。其次，在数据采集阶段，对数据来源进行合法性验证，确保数据采集合规；传输阶段，采用加密传输技术保障数据传输安全；存储阶段，运用加密存储、数据备份与恢复技术，防止数据丢失与泄露；使用阶段，通过数据脱敏、访问控制等手段，限制数据的使用范围；销毁阶段，采用安全销毁技术，确保数据无法被恢复。最后，部署数据泄露检测与溯源系统，实时监控数据访问与传输行为，实现数据泄露事件的快速发现与溯源。

构建安全态势感知与应急响应平台：整合防火墙、入侵检测系统、日志审计系统等安全设备的日志数据，搭建安全态势感知平台。利用大数据与人工智能技术，对全网安全数据进行分析与挖掘，实现对网络攻击、漏洞隐患、异常行为的实时感知与预警。同时，基于态势感知平台构建应急响应系统，制定标准化的应急响应流程，实现从攻击预警、事件研判、应急处置到事后复盘的全流程管理。定期开展应急演练，提升应急响应团队的实战能力。

加强供应链安全管理：建立第三方供应商安全评估机制，在选择供应商前，对其网络安全资质、技术能力、安全管理制度进行全面评估；在合作过程中，定期对供应商的安全状况进行审计与监督，要求供应商遵守政企单位的网络安全管理规定。同时，建立供应链安全应急方案，当供应商出现安全问题时，能够快速启动替代方案，降低供应链攻击带来的影响。

2.2 完善管理机制，夯实安全防护基础

落实网络安全责任制：明确“一把手”为网络安全第一责任人，建立从单位领导到部门负责人再到基层员工的网络安全责任体系，将网络安全责任层层分解、落实到人。制定网络安全责任追究制度，对因失职渎职导致网络安全事件的人员进行严肃追责，形成有效的责任约束机制。

建立常态化风险评估机制：定期开展网络安全风险评估工作，全面排查网络系统、应用程序、数据资产存在的安全漏洞与风险隐患。风险评估应涵盖外部威胁、内部管理、技术防护等多个维度，形成风险评估报告，提出针对性的风险整改措施，并跟踪整改落实情况。同时，结合业务发展与技术变革，动态调整风险评估指标与范围，确保风险评估的时效性与全面性。

规范第三方合作管理：制定第三方合作网络安全管理办法，明确第三方合作的准入条件、安全责任、管理流程。与第三方合作机构签订详细的安全协议，明确双方的安全义务与违约责任。加强对第三方人员的安全培训与管理，对第三方人员的访问权限进行严格控制，定期审查第三方人员的操作日志。

2.3 提升人员能力，强化安全意识

开展分层分类安全培训：根据员工的岗位特点与职责需求，制定分层分类的网络安全培训计划。对普通员工，重点开展网络安全基础知识、安全操作规范、应急处置流程等方面的培训，提升其安全意识与防范能力；对技术人员，开展前沿安全技术、漏洞挖掘与修复、应急响应实战等专业培训，提升其技术防护水平；对管理人员，开展网络安全法律法规、风险管理、合规管理等方面的培训，提升其决策与管理能力。培训方式可采用线上课程、线下讲座、实战演练等多种形式，增强培训效果。

建立安全考核与激励机制：将网络安全培训效果、安全操作规范执行情况纳入员工绩效考核体系，对表现优秀的员工给予表彰与奖励，对违反安全规定的员工进行批评教育与处罚。通过考核与激励机制，调动员工参与网络安全工作的积极性与主动性，形成“人人重视安全、人人参与安全”的良好氛围。

2.4 落地合规体系，实现合规与业务协同

建立合规管理框架：深入研究网络安全相关法律法规与行业标准，结合单位实际情况，建立涵盖合规识别、合规评估、合规整改、合规监督的合规管理框架。明确合规管理部门的职责与权限，配备专业的合规管理人员，负责统筹推进合规体系建设。

开展合规自查与审计：定期开展合规自查工作，对照法律法规与标准规范，排查合规风险点，形成合规自查报告。聘请第三方机构开展合规审计，客观评估合规体系的有效性，提出合规改进建议。根据自查与审计结果，制定合规整改计划，明确整改时限与责任主体，确保合规风险及时消除。

推动合规与业务融合：将合规要求融入业务流程的各个环节，在业务规划、系统建设、项目实施等阶段开展合规评估，确保业务发展符合合规要求。同时，利用合规管理提升业务管理水平，通过合规风险防控降低业务运营风险，实现合规管理与业务发展的协同共进。

3 网络安全防护体系实施的保障措施

3.1 组织保障

成立网络安全工作领导小组，由单位主要领导担任组长，统筹协调网络安全防护体系建设工作。明确领导小组、业务部门、技术部门、合规部门在网络安全工作中的职责分工，建立跨部门协同工作机制，加强各部门之间的沟通与协作，形成工作合力。

3.2 资源保障

加大网络安全资源投入，合理安排网络安全建设、运维、培训等方面的资金预算，确保安全技术产品的升级迭代、安全人员的培养引进、应急演练的开展等工作顺利推进。同时，加强与网络安全服务机构、科研院校的合作，引进先进的安全技术与管理经验，提升网络安全防护体系的科学性与先进性。

3.3 技术保障

建立技术迭代机制，跟踪网络安全技术发展趋势，定期评估现有安全技术与产品的适用性，及时引入符合单位需求的新兴安全技术（如人工智能安全、区块链安全等）。加强安全技术团队建设，通过招聘、培训等方式提升技术人员的专业能力，确保安全技术的有效落地与运行维护。

3.4 监督评估

建立网络安全防护体系监督评估机制，制定科学的评估指标体系，定期对体系的运行效果、防护能力、合规情况进行评估。评估结果作为优化体系、调整策略、落实责任的重要依据。同时，建立持续改进机制，根据评估结果与实际运行情况，及时发现体系存在的问题，不断优化完善防护体系，提升网络安全防护能力。

4 结论

新形势下，政企单位网络安全面临的挑战复杂多变，构建与优化网络安全防护体系是一项系统且长期的任务。政企单位应充分认识到网络安全的重要性与紧迫性，从技术架构、管理机制、人员能力、合规体系四个维度入手，构建全方位、多层次、立体化的网络安全防护体系。同时，通过组织、资源、技术、监督等方面的保障措施，确保防护体系有效落地与持续优化。只有不断提升网络安全防护能力，才能有效应对各类网络安全威胁，保障业务的稳定运行，为数字经济的健康发展提供坚实的安全保障。未来，随着技术的不断发展，政企单位还需持续关注网络安全新态势、新问题，推动网络安全防护体系向智能化、动态化、协同化方向发展，实现网络安全与业务发展的深度融合。

参考文献

[1]齐向东.数字时代的网络安全突围重塑内生安全体系[J].投资北京,2025(8).
[2]大卫·辛普森.政企联合治理网络空间[J].信息安全与通信保密,2017(10):1.
[3]马浩.基于大数据的网络安全防御系统研究与设计[J].网络安全技术与应用,2019(4):2.DOI:CNKI:SUN:WLAQ.0.2019-04-024.
[4]宋金金,朱啟凡,顾国武.基于纵深防御的网络安全防护体系[J].无线互联科技,2023,20(8):154-157.
[5]None.全国政协委员肖新光:帮扶政企单位提升安全能力[J].网络传播,2019(4):1.

作者简介：刘韬（1987.12-），男，汉族，籍贯：湖南省浏阳市，学历：本科，职称：中级专业技术，研究方向：信息通信与网络安全。