网络安全管理与网络安全等级保护制度的研究

秦志超

（黑龙江省万文信息安全测评有限公司　黑龙江　哈尔滨　150000）

[摘　要]在网络安全等级保护制度的规范和指引下开展网络安全管理及网络安全等级保护工作，可以进一步规范网络安全管理工作的行为准则，强化网络安全管理工作的有效性和实效性。网络安全等级保护制度有效规范的开展网络安全管理工作，可强化网络安全管理工作实效性。通过严格的等级划分，监督管理等措施的实施，贯彻落实网络安全管理，促进网络安全等级保护工作的顺利开展和升级，营造良好安全的网络运行环境。在此大背景下，本文就网络安全管理与网络安全等级保护制度的相关内容展开分析研讨，可供参阅。

[关键词]网络安全；管理；等级保护；制度

【DOI】10.12252/j.issn.2096-6288.2021.05.182

1.等级保护制度的主要内容

1.1等级的划分

通常，划分计算机信息系统安全保护等级时，划分的依据是，在计算机信息系统遭到破坏后，所带来不同程度的后果。对于国家安全、社会秩序、和公共利益带来的侵害程度越大，其具有的系统安全保护等级就越高。例如某医疗单位的计算机信息系统受到侵害后，会对社会秩序及公共利益造成非常严重的损坏，其系统安全保护等级会被定级为第三级以上，但是这种等级划分的标准无法量化。

1.2工作的原则

中华人民共和国网络安全等级保护制度贯彻原则为“自主定级、自主保护”。对计算机信息系统进行分等级保护，参照相应标准进行建设、运维、管理、升级、改造和监督。各企事业单位在建立计算机系统后，应参照系统信息安全性、重要性以及与公共利益、其他合法组织等的权益间相关联的情况，自主定级、自主保护，以满足国家相关网络安全等级保护制度的具体要求。

1.3监督管理

根据相关法律规定，我国网络安全等级保护监督与管理工作主要由国务院电信主管部门、国家网信部门以及各级公安部门负责。同时，上述几个部门也是我国网络安全等级保护制度的主要监管部门。

2.构建等级安全管理系统模型

2.1安全计算环境层面的实施

在网络安全等级保护技术要求中，安全计算环境层面主要是针对计算机网络安全等级保护系统实施控制，通过对信息的处理以及采取安全策略等措施，整体了解信息系统的重要核心情况。针对信息系统网络环境进行安全计算环境保护工作的开展，可对系统本身的越权访问及威胁行为进行有效的管理和控制。信息系统网络在安全计算环境层面的防护范围内，能够拒绝外界的部分威胁及越权访问。因此安全计算机环境是对信息系统网络安全防护整体进行改造，最大限度地降低因自身安全漏洞引发的安全风险。

2.2安全网络环境层面的实施

网络架构的作用是既可以在系统内部实现，同时也可以在系统外部实现。网络中在传输数据时，会通过部分安全性未知的网络环境。因此在进行网络环境安全工作的同时，还需要确保整个网络架构中网络安全设备的安全运行，需对这些网络设备的日常运行开展定期或不定期的维护，降低设备受攻击的威胁。提高数据传输过程中的安全性，并在此基础上提高数据传输的保密性及完整性。因为系统网络本身具备保密性的安全需求，所以应该对其加密，使其可以和信息系统本身结合，实现第三级信息系统的安全保护要求。

2.3安全区域边界层面的实施

信息系统的安全边界区域实施保护是指对信息系统业务流程进行划分，根据划分结果确定安全区域边界，和数据信息安全域有很大区别。一般信息系统的边界安全防护，主要根据隔离设备及防护技术完成，然后对信息系统进行安全防护。其主要工作是实现越权控制访问和网络区域隔离。对区域边界的威胁进行详细检测，后将检测信息传递给边界防护体系，这样可以降低内部工作人员故意或非故意的越界行为，从而进一步造成网络安全攻击事件或敏感信息泄漏。

2.4安全管理中心层面的实施

安全管理中心是网络安全的核心，对整个系统的安全管理起到决定性作用，也是整个信息安全管理系统中的核心。可以实现对传输及存储的数据信息进行有效管理，保证数据信息在传输过程中的安全性。整合安全机制，提高管理的效率。统一调度，实现所有用户之间能够便于访问、用户可以实现操作和访问，进而对可能存在的漏洞及风险进行合理管控。

3.基于信息等级安全系统的网络安全管理对策

3.1系统定级实现

在构建完成计算机信息系统以后，相关网络运营者应根据其系统识别以及相关描述，全面评估网络信息安全风险，明确网络信息安全等级，起草、上交定级报告，开展定级备案。根据相关规定，二级及二级以上的计算机系统运营者或者主管部门，应在确定安全保护等级后30日内，到相关公安机关网监部门进行网络安全保护等级备案工作；而对于新建的二级及二级以上的网络信息系统，则应在正式运营后，到相关公安机关网监部门进行备案工作，备案时间仍以30日为限。

3.2整体的安全建设规划

安全建设整体规划是以信息系统作为整体规划的基础，针对具体业务进行整体安全风险评估分析，对具体的结构进行确定，根据实践中遇到的安全风险信息结合系统的安全要求，汇总规划出有针对性的安全管理计划，对系统安全建设提供参照和指引。

3.3安全实施与维护

制定网络安全管理方案，执行逐级安全保护责任制，细化网络使用部门、运行部门以及安全管理部门的权责，做到“有法可依、有章可循、违法必究”；加强网络安全知识的推广与宣传，对关键岗位人员进行定期培训，并将培训纳入绩效考核范畴；引入先进科学的网络安全保护技术，制定科学的应急预案。

4.结语

总而言之，网络安全等保制度与网络安全管理是相辅相成的，网络安全管理是提高国家网络安全环境的关键。不管用于办公、生产的网络信息系统，还是各类服务、贸易平台，都应基于网络安全等级保护制度，加强网络安全管理，维护网络空间主权以及发展利益。特别是对安全等级保护在三级及以上的网络信息系统或者关键基础设施单位，更应对其实施重点保护。

参考文献

[1]徐慧姣.网络安全等级保护与其实施策略[J].通讯世界，2019，26（3）：86.

[2]任智敏.基于等级保护的网络安全技术的应用[J].科技创新导报，2018，15（25）：172-173.

[3]李欣，厚佳琪.网络安全等级保护工作的创新发展[J].中国信息安全，2018（8）：33-34.