

主管部门可组织梳理本行业/领域内主要依靠信息化处理的业务情况,并按照业务承载的社会功能/职能的重要程度、其他行业对其的依赖程度等方面确定本行业/领域内的主要业务。

c) 定级指导

主管部门可组织分析本行业/领域内的主要业务,并根据业务信息重要性和业务服务重要性分析各主要业务的安全保护要求,结合行业/领域自身情况,形成针对主要业务的行业/领域定级指导意见。跨省或者全国统一联网运行的等级保护对象可以由主管部门统一确定安全保护等级。

d) 定级工作部署

主管部门可制定本行业/领域的定级指导意见,并统一部署全行业/领域的定级工作。行业/领域主管部门应对下属单位的定级结果进行审核、批准。

活动输出:行业/领域的业务总体描述文件,行业/领域定级指导意见,行业/领域定级工作部署文件。

5.3 等级保护对象分析

5.3.1 对象重要性分析

活动目标:

通过收集了解有关等级保护对象的信息,并对信息进行综合分析和整理,分析单位的主要社会功能/职能及作用,确定履行主要社会功能/职能所依赖的等级保护对象,整理等级保护对象处理的业务及服务范围,最后依据分析和整理的内容,有行业/领域定级指导意见的还应依据行业/领域定级指导意见,形成单位内等级保护对象的总体描述性文档。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:单位情况说明文档,等级保护对象的立项、建设和管理文档,行业/领域定级指导意见。

活动描述:

本活动主要包括以下子活动内容:

a) 识别单位的基本信息

调查了解等级保护对象所属单位的业务范围、主要社会功能/职能和生产产值等信息,分析主要社会功能/职能在保障国家安全、经济发展、社会秩序、公共服务等方面发挥的重要作用。

b) 识别单位的等级保护对象基本信息

了解单位内主要依靠信息化处理的业务情况,这些业务各自的社会属性和业务内容,确定单位的等级保护对象。并确定等级保护对象的业务范围、地理位置以及其他基本情况,获得等级保护对象的背景信息和联络方式。

c) 识别等级保护对象的管理框架

了解等级保护对象的组织管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责,获得支撑等级保护对象业务运营的管理特征和管理框架方面的信息,从而明确等级保护对象的安全责任主体。

d) 识别等级保护对象的网络及设备部署

了解等级保护对象的物理环境、网络拓扑结构和硬件设备的部署情况,在此基础上明确等级保护对象的边界,即确定等级保护对象及其范围。

e) 识别等级保护对象的业务特性

了解单位内主要依靠信息化处理的各种业务及业务流程,从中明确支撑单位业务运营的等级保护对象的业务特性。

f) 识别等级保护对象处理的信息资产

了解等级保护对象处理的信息资产的类型,这些信息资产在保密性、完整性和可用性等方面的重要

性程度。

g) 识别用户范围和用户类型

根据用户或用户群的分布范围了解等级保护对象的服务范围、作用以及业务连续性方面的要求等。

h) 等级保护对象描述

对收集的信息进行整理、分析,形成对等级保护对象的总体描述文件。一个典型的等级保护对象的总体描述文件应包含以下内容:

- 1) 等级保护对象概述;
- 2) 等级保护对象重要性分析;
- 3) 等级保护对象边界描述;
- 4) 网络拓扑;
- 5) 设备部署;
- 6) 支撑的业务应用的种类和特性;
- 7) 处理的信息资产;
- 8) 用户的范围和用户类型;
- 9) 等级保护对象的管理框架。

活动输出:等级保护对象总体描述文件。

5.3.2 定级对象确定

活动目标:

依据单位的等级保护对象总体描述文件(有行业/领域定级指导意见的还应依据行业/领域定级指导意见),在综合分析的基础上将单位内运行的等级保护对象进行合理分解,确定所包含的定级对象及其个数。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:行业/领域定级指导意见,行业/领域定级工作部署文件,等级保护对象总体描述文件,GB/T 22240。

活动描述:

本活动主要包括以下子活动内容:

a) 划分方法的选择

为了突出重点保护的等级保护原则,运营、使用单位应对大型等级保护对象进行划分,划分的方法可以有多种,可以考虑管理机构、业务类型、物理位置等因素,运营、使用单位应根据本单位的具体情况确定等级保护对象的分解原则。

b) 等级保护对象划分

依据选择的等级保护对象划分原则,参考行业/领域定级指导意见(若有行业/领域定级指导意见),运营、使用单位应将大型等级保护对象进行划分,划分出相对独立的对象作为定级对象,应保证每个相对独立的对象具备定级对象的基本特征。在等级保护对象划分的过程中,应首先考虑组织管理的要素,然后考虑业务类型、物理区域等要素。承载比较单一的业务应用或者承载相对独立的业务应用的对象应作为单独的定级对象。

对于电信网、广播电视传输网等通信网络设施,应分别依据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。跨省的行业或单位的专用通信网可作为一个整体对象定级,或分区域划分为若干个定级对象。

在云计算环境中,应将云服务客户侧的等级保护对象和云服务商侧的云计算平台/系统分别作为单独的定级对象定级,并根据不同服务模式将云计算平台/系统划分为不同的定级对象。对于大型云计算平台,宜将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

物联网主要包括感知、网络传输和处理应用等特征要素,应将以上要素作为一个整体对象定级,各要素不单独定级。

对于工业控制系统,其一般包含现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中,现场采集/执行、现场控制、过程控制等要素应作为一个整体对象定级,各要素不单独定级;生产管理要素宜单独定级。对于大型工业控制系统,可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

采用移动互联技术的等级保护对象主要包括移动终端、移动应用和无线网络等特征要素,可作为一个整体独立定级或与相关联业务系统一起定级,各要素不单独定级。

c) 定级对象详细描述

在对等级保护对象进行划分并确定定级对象后,应在等级保护对象总体描述文件的基础上,进一步增加定级对象的描述,准确描述一个大型等级保护对象中包括的定级对象的个数。

进一步的定级对象详细描述文件应包含以下内容:

- 1) 相对独立的定级对象列表;
- 2) 每个定级对象的概述;
- 3) 每个定级对象的边界;
- 4) 每个定级对象的设备部署;
- 5) 每个定级对象支撑的业务应用及其处理的信息资产类型;
- 6) 每个定级对象的服务范围和用户类型;
- 7) 其他内容。

活动输出:定级对象详细描述文件。

5.4 安全保护等级确定

5.4.1 定级、审核和批准

活动目标:

按照国家有关管理规范和定级标准,确定定级对象的安全保护等级,并对定级结果进行评审、审核和审查,保证定级结果的准确性。

参与角色:主管部门,运营、使用单位,网络安全服务机构。

活动输入:行业/领域定级指导意见,等级保护对象总体描述文件,定级对象详细描述文件。

活动描述:

本活动主要包括以下子活动内容:

a) 定级对象安全保护等级初步确定

根据国家有关管理规范、行业/领域定级指导意见(若有则作为依据)以及定级方法,运营、使用单位对每个定级对象确定初步的安全保护等级。

b) 定级结果评审

运营、使用单位初步确定了安全保护等级后,必要时可以组织网络安全专家和业务专家对初步定级结果的合理性进行评审,并出具专家评审意见。

c) 定级结果审核、批准

运营、使用单位初步确定了安全保护等级后,有明确主管部门的,应将初步定级结果上报行业/领域主管部门或上级主管部门进行审核、批准。行业/领域主管部门或上级主管部门应对初步定级结果的合理性进行审核,出具审核意见。

运营、使用单位应定期自查等级保护对象等级变化情况以及新建系统定级情况,并及时上报主管部门进行审核、批准。

活动输出:定级结果,主管部门审批意见。

5.4.2 形成定级报告

活动目标:

对定级过程中产生的文档进行整理,形成等级保护对象定级结果报告。

参与角色:主管部门,运营、使用单位。

活动输入:定级对象详细描述文件,定级结果。

活动描述:

对等级保护对象的总体描述文档、详细描述文件、定级结果等内容进行整理,形成文件化的定级结果报告。

定级结果报告可以包含以下内容:

- a) 单位信息化现状概述;
- b) 管理模式;
- c) 定级对象列表;
- d) 每个定级对象的概述;
- e) 每个定级对象的边界;
- f) 每个定级对象的设备部署;
- g) 每个定级对象支撑的业务应用;
- h) 定级对象列表、安全保护等级以及保护要求组合;
- i) 其他内容。

活动输出:安全保护等级定级报告。

5.5 定级结果备案

活动目标:

根据等级保护管理部门对备案的要求,整理相关备案材料,并向受理备案的单位提交备案材料。

参与角色:主管部门,运营、使用单位,等级保护管理部门。

活动输入:定级报告,主管部门审核意见,等级保护对象安全总体方案,安全详细设计方案,安全等级测评报告(第三级及以上等级系统需要提供)。

活动描述:

本活动主要包括以下子活动内容:

- a) 备案材料整理

运营、使用单位在等级保护对象建设之初根据其将要承载的业务信息及系统服务的重要性确定等级保护对象的安全保护等级,并针对备案材料的要求,整理、填写备案材料。

- b) 备案材料提交

根据等级保护管理部门的要求办理定级备案手续,提交备案材料(新建等级保护对象可在等级测评实施完毕补充提交等级测评报告);等级保护管理部门接收备案材料,出具备案证明。

活动输出:备案材料,备案证明。

6 总体安全规划

6.1 总体安全规划阶段的工作流程

总体安全规划阶段的目标是根据等级保护对象的划分情况、等级保护对象的定级情况、等级保护对象承载业务情况,通过分析明确等级保护对象安全需求,设计合理的、满足等级保护要求的总体安全方

案,并制定出安全实施计划,以指导后续的等级保护对象安全建设工程实施。

总体安全规划阶段的工作流程见图 3。

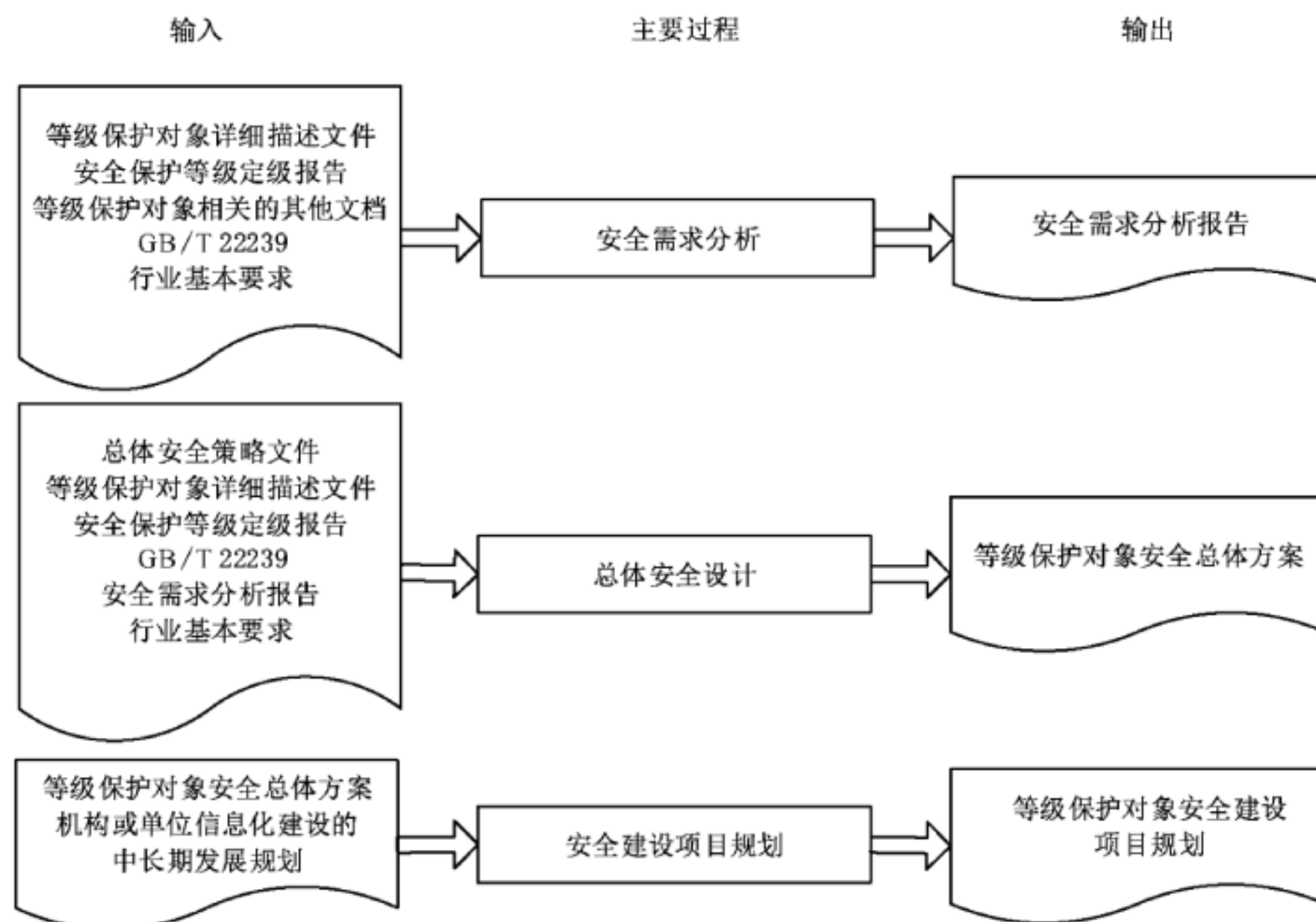


图 3 总体安全规划阶段工作流程

6.2 安全需求分析

6.2.1 基本安全需求的确定

活动目标：

根据等级保护对象的安全保护等级,提出等级保护对象的基本安全保护需求。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:等级保护对象详细描述文件,安全保护等级定级报告,等级保护对象相关的其他文档,GB/T 22239,行业基本要求。

活动描述：

本活动主要包括以下子活动内容：

a) 确定等级保护对象范围和分析对象

明确不同等级的等级保护对象的范围和边界,通过调查或查阅资料的方式,了解等级保护对象的业务应用、业务流程等情况。

b) 形成基本安全需求

根据各个等级保护对象的安全保护等级从 GB/T 22239、行业基本要求中选择相应等级的要求,形成基本安全需求。对于已建等级保护对象,应根据等级测评结果分析整改需求,形成基本安全需求。

活动输出:基本安全需求。

6.2.2 特殊安全需求的确定

活动目标：

通过分析重要资产的特殊保护要求,采用需求分析或风险分析的方法,确定可能的安全风险,判断实施特殊安全措施的必要性,提出等级保护对象的特殊安全保护需求。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:等级保护对象详细描述文件,安全保护等级定级报告,等级保护对象相关的其他文档。

活动描述:

确定特殊安全需求可以采用目前成熟或流行的需求分析或风险分析方法,或者采用下面介绍的活动:

a) 重要资产分析

明确等级保护对象中的重要部件,如边界设备、网关设备、核心网络设备、重要服务器设备、重要应用系统等。

b) 重要资产安全弱点评估

检查或判断上述重要部件可能存在的弱点(包括技术和管理两方面),分析安全弱点被利用的可能性。

c) 重要资产面临威胁评估

分析和判断上述重要部件可能面临的威胁,包括外部、内部的威胁,威胁发生的可能性或概率。

d) 综合风险分析

分析威胁利用弱点可能产生的结果,结果产生的可能性或概率,结果造成的损害或影响的大小,以及避免上述结果产生的可能性、必要性和经济性。按照重要资产的排序和风险的排序确定安全保护的要求。

活动输出:重要资产的特殊保护要求。

6.2.3 形成安全需求分析报告

活动目标:

总结基本安全需求和特殊安全需求,形成安全需求分析报告。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:等级保护对象详细描述文件,安全保护等级定级报告,基本安全需求,重要资产的特殊保护要求。

活动描述:

本活动主要的子活动是完成安全需求分析报告。根据基本安全需求和特殊的安全保护需求等形成安全需求分析报告。

安全需求分析报告可以包含以下内容:

a) 等级保护对象描述;

b) 基本安全需求描述;

c) 特殊安全需求描述。

活动输出:安全需求分析报告。

6.3 总体安全设计

6.3.1 总体安全策略设计

活动目标:

形成机构纲领性的安全策略文件,包括确定安全方针,制定安全策略,以便结合等级保护基本要求系列标准、行业基本要求和安全保护特殊要求,构建机构等级保护对象的安全技术体系结构和安全管理体系统结构。对于新建的等级保护对象,应在立项时明确其安全保护等级,并按照相应的保护等级要求进行总体安全策略设计。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:等级保护对象详细描述文件,安全保护等级定级报告,安全需求分析报告。

活动描述：

本活动主要包括以下子活动内容：

a) 确定安全方针

形成机构最高层次的安全方针文件，阐明安全工作的使命和意愿，定义网络安全的总体目标，规定网络安全责任机构和职责，建立安全工作运行模式等。

b) 制定安全策略

形成机构高层次的安全策略文件，说明安全工作的主要策略，包括安全组织机构划分策略、业务系统分级策略、数据信息分级策略、等级保护对象互连策略、信息流控制策略等。

活动输出：总体安全策略文件。

6.3.2 安全技术体系结构设计

活动目标：

根据 GB/T 22239、行业基本要求、安全需求分析报告、机构总体安全策略文件等，提出等级保护对象需要实现的安全技术措施，形成机构特定的等级保护对象安全技术体系结构，用以指导等级保护对象分等级保护的具体实现。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：总体安全策略文件，等级保护对象详细描述文件，安全保护等级定级报告，安全需求分析报告，GB/T 22239，行业基本要求。

活动描述：

本活动主要包括以下子活动内容：

a) 设计安全技术体系架构

根据机构总体安全策略文件、GB/T 22239、行业基本要求和安全需求，设计安全技术体系架构。安全技术防护体系由从外到内的“纵深防御”体系构成，“物理环境安全防护”保护服务器、网络设备以及其他设备设施免遭地震、火灾、水灾、盗窃等事故导致的破坏，“通信网络安全防护”保护暴露于外部的通信线路和通信设备，“网络边界安全防护”对等级保护对象实施边界安全防护，内部不同级别定级对象尽量分别部署在相应保护等级的内部安全区域，低级别定级对象部署在高等级安全区域时应遵循“就高保护”原则，内部安全区域即“计算环境安全防护”将实施“主机设备安全防护”和“应用和数据安全防护”“安全管理中心”对整个等级保护对象实施统一的安全技术管理。

等级保护对象的安全技术体系架构见图 4。

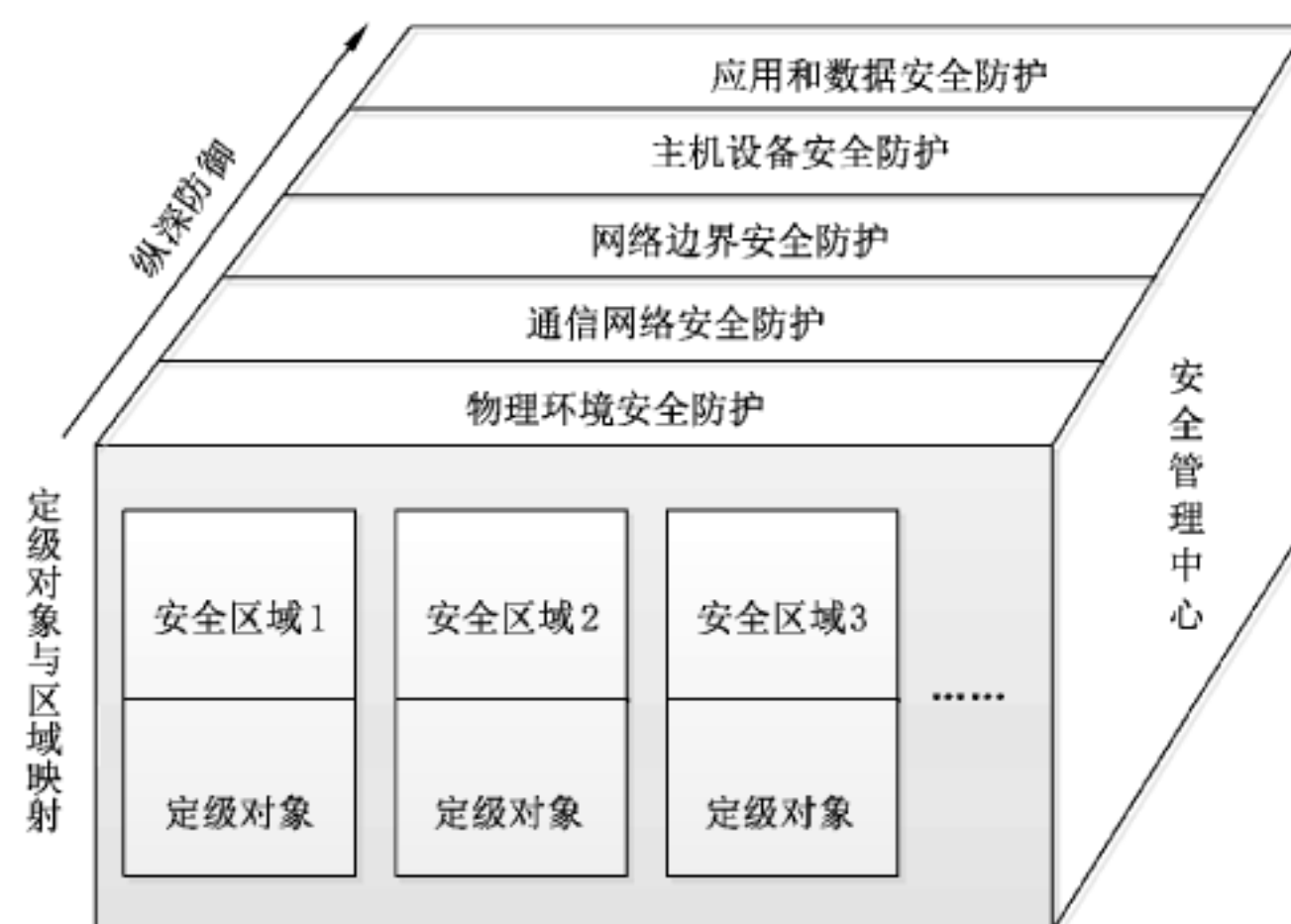


图 4 等级保护对象的安全技术体系架构

b) 规定不同级别定级对象物理环境的安全保护技术措施

根据机构总体安全策略文件、等级保护基本要求和安全需求,提出不同级别定级对象物理环境的安全保护策略和安全技术措施。定级对象物理环境安全保护策略和安全技术措施提出时应考虑不同级别的定级对象共享物理环境的情况,如果不同级别的定级对象共享同一物理环境,物理环境的安全保护策略和安全技术措施应满足最高级别定级对象的等级保护基本要求。

c) 规定通信网络的安全保护技术措施

根据机构总体安全策略文件、等级保护基本要求和安全需求,提出通信网络的安全保护策略和安全技术措施。通信网络的安全保护策略和安全技术措施提出时应考虑网络线路和网络设备共享的情况,如果不同级别的定级对象通过通信网络的同一线路和设备传输数据,线路和设备的安全保护策略和安全技术措施应满足最高级别定级对象的等级保护基本要求。

d) 规定不同级别定级对象的边界保护技术措施

根据机构总体安全策略文件、等级保护基本要求和安全需求,提出不同级别定级对象边界的安全保护策略和安全技术措施。如果不同级别的定级对象共享同一设备进行边界保护,则该边界设备的安全保护策略和安全技术措施应满足最高级别定级对象的等级保护基本要求。

e) 规定定级对象之间互联的安全技术措施

根据机构总体安全策略文件、等级保护基本要求和安全需求,提出跨局域网互联的定级对象之间的信息传输保护策略要求和具体的安全技术措施,包括同级互联的策略、不同级别互联的策略等;提出局域网内部互联的定级对象之间的信息传输保护策略要求和具体的安全技术保护措施,包括同级互联的策略、不同级别互联的策略等。

f) 规定不同级别定级对象内部的安全保护技术措施

根据机构总体安全策略文件、等级保护基本要求和安全需求,提出不同级别定级对象内部网络平台、系统平台、业务应用和数据的安全保护策略和安全技术保护措施。如果低级别定级对象部署在高级别定级对象的网络区域,则低级别定级对象的系统平台、业务应用和数据的安全保护策略和安全技术措施应满足高级别定级对象的等级保护基本要求。

g) 规定云计算、移动互联等新技术的安全保护技术措施

根据机构总体安全策略文件、等级保护基本要求、行业基本要求和安全需求,提出云计算、移动互联等新技术的安全保护策略和安全技术措施。云计算平台应至少满足其承载的最高级别定级对象的等级保护基本要求。

h) 形成等级保护对象安全技术体系结构

将骨干网或城域网、通过骨干网或城域网的定级对象互联、局域网内部的定级对象互联、定级对象的边界、定级对象内部各类平台、机房以及其他方面的安全保护策略和安全技术措施进行整理、汇总,形成等级保护对象的安全技术体系结构。

活动输出:等级保护对象安全技术体系结构。

6.3.3 整体安全管理体系结构设计

活动目标:

根据等级保护基本要求系列标准、行业基本要求、安全需求分析报告、机构总体安全策略文件等,调整原有管理模式和管理策略,既从全局高度考虑为每个等级的定级对象制定统一的安全管理策略,又从每个定级对象的实际需求出发,选择和调整具体的安全管理措施,最后形成统一的整体安全管理体系结构。

参与角色:运营、使用单位,网络安全服务机构。

活动输入:总体安全策略文件,等级保护对象详细描述文件,安全保护等级定级报告,安全需求分析报告,GB/T 22239,行业基本要求。