电信网络安全等级保护的研究

作者：魏薇 来源：泰尔网 发布时间：2008-03-21

摘要：主要研究电信网络安全防护体系中的安全等级保护，重点对安全等级保护的原则、相关角色和职责、安全等级的划分方法、基本过程进行了研究，对安全等级保护与电信网络生命周期的关系进行了阐述。

1、引言

电信网络承担大范围的公众通信，其安全状况对于国家安全、社会秩序、经济建设、公共利益、网络和业务运营商的利益等具有重要意义。通过对电信网络进行安全等级划分，并按照安全等级保护要求进行规划、建设、运维、管理和监督，可以实现对电信网络重点保护和有效保护的目的，增强安全保护的整体性、针对性和实效性，使电信网络的安全建设能够突出重点、统一规范、科学合理。

本文重点研究电信网络安全等级保护的原则、相关角色和职责、安全等级的划分方法、基本过程以及与电信网络生命周期的关系等问题。

2、安全等级保护的原则

2.1 电信网络的安全等级应满足安全防护的总体指导性原则

电信网络安全防护体系包括安全等级保护、安全风险评估、灾难备份及恢复三部分工作，三者之间互为依托、互为补充。作为电信网络安全防护体系中的一个重要组成部分，电信网络的安全等级保护应首先满足安全防护的总体指导性原则：

（1）适度安全原则：安全防护工作的根本性原则，指安全防护工作应根据电信网络的安全等级，平衡效益与成本，采取适度的安全技术和管理措施。

（2）标准性原则：安全防护工作的指导性原则，指电信网络安全防护工作的开展应遵循相关的国家或行业标准。

（3）可控性原则：指电信网络安全防护在人员、工具、过程方面都是可控的，具体包括：

●人员可控性：相关的安全防护工作人员应具备可靠的政治素质、职业素质和专业素质。相关安全防护工作的检测机构应具有主管部门授权的电信网络安全防护检测服务资质。

●工具可控性：要充分了解安全防护工作中所使用的技术工具，并进行一些实验，确保这些技术工具能被正确地使用。

●项目过程可控性：要对整个安全防护项目进行科学的项目管理，实现项目过程的可控性。

（4）完备性原则：安全防护工作应覆盖电信网络的安全范围。

（5）最小影响原则：从项目管理层面和技术管理层面，将安全防护工作对电信网络正常运行的可能影响降低到最低限度。

（6）保密性原则：相关安全防护工作人员应签署协议，承诺对所进行的安全防护工作保密，确保不泄露电信网络安全防护工作的重要和敏感信息。

2.2　电信网络安全等级保护在实施过程中应重点遵循的原则

（1）自主保护原则：在主管部门的监督指导下，各网络和业务运营商应按照相关标准确定其运营的电信网络的安全等级，并对电信网络自主实施安全保护。

（2）同步建设原则：各网络和业务运营商在对电信网络进行新建、改建、扩建时，应当同步规划和设计其安全方案，投入一定比例的资金实施安全方案，保障电信网络与其所属安全等级的要求相适应。

（3）重点保护原则：通过对电信网络划分不同的安全等级，提出不同程度的安全保护要求，实现不同等级的安全保护，集中资源优先保护关键的电信网络。

（4）适当调整原则：跟踪电信网络的变化情况调整其安全等级，并根据安全等级的调整情况及时调整相应的安全保护措施。

3、安全等级保护相关角色和职责

对电信网络实施安全等级保护的过程中涉及到各类组织和人员，不同组织和人员将会参与不同或相同的活动。安全等级保护实施过程中各类角色及其职责如下：

（1）主管部门：其主要职责是监督、指导网络和业务运营商遵照相关标准确定电信网络的安全等级，对网络和业务运营商确定的安全等级进行审批；监督、管理网络和业务运营商遵照相关标准中的等级保护要求对电信网络进行安全等级保护；对网络和业务运营商的安全等级保护工作开展情况进行检查，发现存在安全隐患或未达到安全等级保护要求的，责令其限期整改。

（2）网络和业务运营商：其主要职责是根据相关标准确定其运营的电信网络的安全等级，并分级上报至国家或地区的主管部门审批同意；根据已经确定的安全等级，按照相关标准中的安全等级保护要求对其运营的电信网络实施安全等级保护，包括规划设计、建设施工、运维、废弃等；对安全等级是自主保护级的电信网络，加强其自主保护工作，对安全等级是指导保护级、监督保护级的电信网络，根据主管部门的要求及时上报其等级保护工作的实施情况；定期对其运营的电信网络进行安全状况检查，及时消除安全隐患和漏洞；加强和完善自身安全等级保护制度的建设，制定不同等级安全事件的响应、处置预案，加强电信网络的安全管理。

（3）设备制造商：其主要职责是遵照相关标准中的安全等级保护要求开发安全的网络设备，提交网络设备进行入网测试，并且销售安全的网络设备。

（4）检测机构：必须是由主管部门授权的具有安全防护检测服务资质的机构。检测机构的主要职责是根据主管部门或网络和业务运营商的委托，按照相关标准中的安全等级保护要求对已经完成安全等级保护建设的电信网络进行安全检测。

（5）安全服务商：应按照国家和主管部门的相关规定，在安全等级保护相关标准的指导下，根据网络和业务运营商的要求协助其实施安全等级保护工作。

4、安全等级的划分方法

电信网络安全防护体系中，确定安全等级是进行安全等级保护的前提和基础，直接影响和指导安全防护体系中的安全风险评估和灾难备份及恢复工作。在电信网络中进行安全等级划分的总体原则是：电信网络受到破坏后对国家安全、社会秩序、经济建设、公共利益、网络和业务运营商的损害程度。

4.1　电信网络安全等级的定级要素

电信网络确定安全等级的具体定级要素包括电信网络的社会影响力、所提供服务的重要性、规模和服务范围3个定级要素。

（1）社会影响力：表示电信网络无法提供有效服务对国家安全、社会秩序、经济建设、公共利益的影响程度；

（2）所提供服务的重要性：表示电信网络提供的服务对网络和业务运营商的影响程度；

（3）规模和服务范围：规模表示电信网络服务的用户数多少，服务范围表示电信网络服务的地区范围大小。

4.2　电信网络的安全等级

在确定3个具体定级要素的赋值后，可根据一定的安全等级确定方法得到电信网络的安全等级。安全等级确定可能不是一个过程就可以完成的，而是需要经过定级要素赋值、定级、定级结果调整的循环过程，最终才能确定出较为科学、准确的安全等级。

电信网络可以划分为3个安全等级，分别为自主保护级、指导保护级和监督保护级，其中监督保护级又分为普通监督保护级和重点监督保护级。主管部门对不同级别的电信网络实行不同等级的监管。

（1）第1级：自主保护级

自主保护级是指电信网络遭到破坏后仅对其所有者的利益产生损害，但是不损害国家安全、社会秩序、经济建设、公共利益。本级按照通信行业安全标准进行自主保护。

（2）第2级：指导保护级

指导保护级是指电信网络遭到破坏后对社会秩序、经济建设、公共利益以及网络和业务运营商造成轻微损害。本级在主管部门的指导下，按照通信行业安全标准进行自主保护。

（3）第3级：监督保护级（分普通监督保护级和重点监督保护级两种情况）

普通监督保护级是指电信网络遭到破坏后对国家安全、社会秩序、经济建设、公共利益以及网络和业务运营商造成较大损害。本级按照通信行业安全标准进行自主保护，主管部门对其进行监督、检查。

重点监督保护级是指电信网络遭到破坏后对国家安全、社会秩序、经济建设、公共利益以及网络和业务运营商造成严重损害。本级按照通信行业安全标准进行自主保护，主管部门对其进行重点监督、检查。

5、安全等级保护实施的基本过程

虽然安全等级保护是一个不断循环和提高的过程，但是实施安全等级保护的一次完整过程是可以区分清楚的，包括5个主要阶段：安全等级确定、安全规划设计、安全实施、安全运维、安全资产终止（见图1）。

图1　安全等级保护实施的基本过程

在安全运维阶段，当电信网络因为局部调整等原因导致安全措施变化时，如果不影响其安全等级，应从安全运维阶段进入安全实施阶段，重新调整和实施安全措施，确保满足安全等级保护的要求；当电信网络发生重大变更影响其安全等级时，应从安全运维阶段进入安全等级确定阶段，重新开始一次安全等级保护的实施过程。安全等级保护的5个主要阶段及其主要活动为：

5.1　安全等级确定阶段

安全等级确定阶段主要包括对电信网络的识别、电信网络的划分以及安全等级确定等几个主要安全活动：

（1）电信网络的识别：通过查询相关文档、编制调查表、与有关人员访谈、现场实地观察等多种方式尽可能多地收集、分析和整理电信网络的相关信息，达到对电信网络进行识别的目的。

（2）电信网络的划分：将复杂的电信网络进一步划分为各个相对独立的子网络，例如将固定通信网划分为各个本地网、省内长途网、省际长途网（含国际长途网），并将划分后的子网络作为定级对象。

（3）安全等级确定：根据相关标准中的定级方法科学准确地确定各定级对象的安全等级。

5.2　安全规划设计阶段

安全规划设计阶段主要包括安全需求分析、安全总体设计、安全建设规划等几个主要活动。

（1）安全需求分析：根据国家及企业的安全目标，首先判断电信网络的安全保护现状与安全防护要求中安全等级保护要求之间的差距，这种差距作为初步的安全需求；除上述安全需求外，还要通过风险分析的方法确定额外的安全需求，这种需求反映在对特殊环境和威胁的安全保护要求，或对重要对象的较高保护要求方面。通过现状差距的分析和特殊要求的分析，明确完整的安全需求。

（2）安全总体设计：根据安全需求分析报告和安全等级保护相关要求，设计满足其所属的安全等级要求的安全总体方案，包括安全技术措施和安全管理措施。

（3）安全建设规划：根据安全总体方案，结合企业中长期的发展规划，制定安全建设的实施计划，形成指导今后一段时间内安全建设工作的安全建设规划方案。

5.3　安全实施阶段

安全实施阶段主要包括安全方案详细设计、详细设计方案的实施、安全等级保护检测等几个主要活动。

（1）安全方案详细设计：依据电信网络的安全建设方案，提出本期实施项目的具体实施方案，包括安全等级保护技术实施内容的设计、安全等级保护管理实施内容的设计、实施计划以及经费投入等，以便进行本期安全方案的实施。

（2）详细设计方案实施：包括安全等级保护管理内容的实施和安全等级保护技术内容的实施。安全等级保护管理实施主要是在本期安全详细设计方案的指导下，建立配套的安全管理机构，建立配套的安全管理制度和操作规程，进行人员的安全技能培训等。保证本期安全实施完成后，安全运维有配套的安全管理机制。安全等级保护技术措施实施主要是按照安全详细设计方案，进行安全产品采购、安全控制开发、安全控制集成、测试与验收等主要活动，确保安全技术措施的有效性。

（3）安全等级保护检测：根据主管部门的要求，遵照安全等级保护的管理和技术方面的标准，针对已经实施了安全等级保护的电信网络，检测实施的安全保护措施是否符合相应安全等级的安全保护要求。

5.4　安全运维阶段

安全运维阶段需要进行的安全控制活动很多，我们关注如下安全控制活动：

（1）运行管理和控制：确定电信网络的运行管理职责并对运行管理过程进行控制。

（2）变更管理和控制：分析电信网络的变更需求和影响并对变更过程进行控制。

（3）安全状态监控：确定电信网络的监控对象和工具，监控、分析对象的状态。

（4）安全事件处置和应急预案：对电信网络的安全事件分级，制定应急预案，对安全事件进行处置。

（5）安全检查和持续改进：对电信网络的安全状态进行自查，根据安全检查的结果制定和实施改进方案，确保电信网络的安全保护能力满足相应等级安全要求和自身特殊的安全需求，确保安全等级保护工作的有效性。

（6）安全等级保护检测：根据主管部门的要求，遵照安全等级保护的管理和技术方面的标准，针对正在运营的电信网络，检测实施的安全保护措施是否符合相应安全等级的安全保护要求。

5.5　安全资产终止阶段

安全资产终止阶段的主要活动包括对电信网络中的信息转移、暂存或清除，对设备迁移或废弃，对存储介质的清除或销毁。

（1）信息转移、暂存或清除：识别要转移、暂存和清除的信息资产，制定信息资产的转移、暂存、清除的处理方案，待处理方案审批通过后，根据处理方案对信息资产进行转移、暂存和清除。

（2）设备迁移或废弃：识别要迁移或废弃的设备，制定设备的迁移或废弃的处理方案，待处理方案审批通过后，根据处理方案对设备进行迁移或废弃。

（3）存储介质的清除或销毁：识别要清除或销毁的存储介质，制定存储介质的清除或销毁的处理方案，待处理方案审批通过后，根据处理方案对存储介质进行清除或销毁。

6、安全等级保护与电信网络生命周期的关系

电信网络的生命周期包括5个阶段，即启动阶段、设计阶段、实施阶段、运维阶段和废弃阶段。电信网络的安全等级保护工作将贯穿其生命周期的各个阶段。安全等级保护工作可分为：对新建电信网络的安全等级保护和对已建电信网络的安全等级保护，两者在电信网络生命周期中的切入点是不同的，但是安全等级保护工作的主要活动基本相同，其安全等级保

护过程与电信网络生命周期的关系如图2所示。

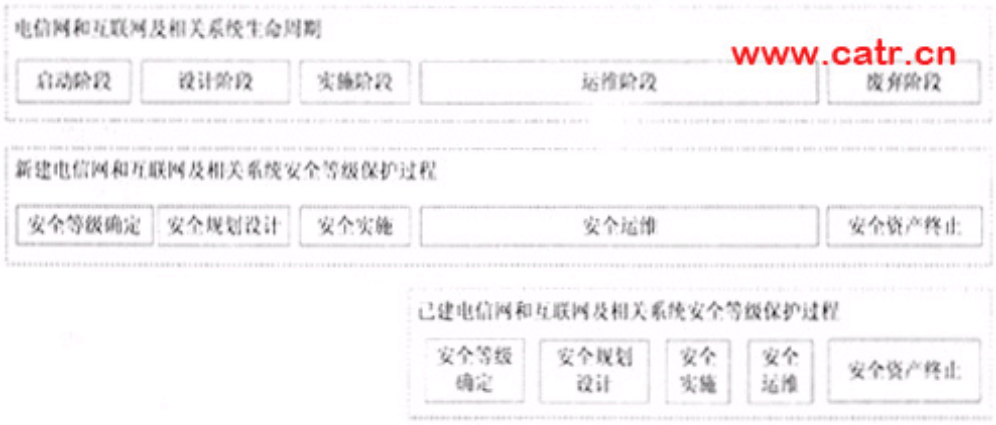

图2　安全等级保护过程与电信网络生命周期的关系

新建的电信网络在生命周期中的各个阶段应同步考虑安全等级保护的主要活动。在启动阶段，应该仔细分析和合理划分各个电信网络，确定各个电信网络的安全等级，定级过程也可能在设计阶段；在设计阶段，应该根据各个电信网络的安全等级，进行安全规划设计；在实施阶段，应在电信网络建设的同时，同步进行安全措施的实施；在运维阶段，应按照相关标准中安全等级保护的要求进行安全运维；在废弃阶段，应对废弃的设备、信息或存储介质等资产进行有效的安全管理。

已建的电信网络通常处于运维阶段，由于在启动阶段、设计阶段和实施阶段可能没有同步考虑安全等级保护的要求或者对安全等级保护的要求考虑不足，因此应在运维阶段启动安全等级保护工作，安全等级保护过程中的安全等级确定、安全规划设计、安全实施的主要活动都将在生命周期的运维阶段完成。由于是已经存在的电信网络，工作的重点是在现有网络的基础上，根据安全等级保护要求，在安全规划设计阶段如何制定满足要求的补充的安全建设方案，在安全实施阶段如何保证在不影响现有业务/应用的情况下，分步骤分阶段分目标地使各类安全补救措施可以顺利落实。

在已建的电信网络基础上进行扩容的安全等级保护工作，扩容部分应与新建的电信网络的安全等级保护过程一致。

7、结束语

本文主要介绍了电信网络安全等级保护的原则、相关角色和职责、安全等级的划分方法、基本过程、与生命周期的关系等内容。

在整个安全防护体系的框架下，安全等级保护如何与安全风险评估、灾难备份及恢复协调配合，以及安全等级保护中采用的定级方法、与安全等级相对应的电信网络技术和管理要求等还需要进一步研究。