安全小课堂第111期【网络安全等级保护】

京东安全应急响应中心 9月17日

《网络安全法》第二十一条规定国家实行网络安全等级保护制度，等级保护经过十年的发展已经进入2.0时代，除了传统信息系统，云计算、移动互联、物联网、工业控制系统也被纳入了等级保护的范围。本次分享主要对等保政策、如何定级、等级工作如何开展进行简要的介绍。

JSRC **安全小课堂第111期**，邀请到来自湖南金盾技术部经理**熊璐**作为讲师就**网络安全等级保护**为大家进行分享。同时感谢各位小伙伴们的精彩讨论

什么是等级保护？等级保护2.0在这基础之上有啥变化？

京安小妹

熊璐：

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护.

简单而言，就是将全国的信息系统（包括网络）按照重要性和受破坏后的危害性分成五个安全保护等级（从第一级到第五级逐级增高），定级后第二级以上信息系统到公安机关备案，公安机关对备案材料审核合格后颁发备案证明；各单位各部门根据系统等级按照国家标准进行安全建设整改，备案单位聘请符合国家规定的等级测评机构进行等级测评（第二级系统备案前要进行一次测评、第三级系统每年要进行一次测评）；公安机关对第二级信息系统进行指导，对第三级、第四级信息系统定期开展监督、检查。

等保2.0在1.0的基础上四个大的变化，一个是名称的变化，二是范围的变化，三是定级的变化，四是内容的变化。

名称信息系统等级保护改为了网络安全等级保护

范围

原来只是信息系统要做等保。2.0把云计算、移动互联、物联网、工业控制系统也被纳入了等级保护的范围。

定级：

1、等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，原来定为二级，2.0后改为三级。

2、原来是用户自主定级，2.0在定级流程上加入了主管部门审核、专家评审环节，也就是不完全是自主定级了。

内容

2.0新标准针对云计算、移动互联、物联网、工业控制系统提出了安全扩展要求。传统信息系统需要满足安全通用要求，云计算、移动互联、物联网、工业控制系统在安全通用要求的基础上还需要实现安全扩展要求。原来针对传统信息系统的标准也进行了更新。

讲师

信息安全等级保护的等级划分原则是什么,是如何划分的？

京安小妹

熊璐：

信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

按照公安部《网络安全保护等级定级指南》的要求，非涉密信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成特别严重损害，对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

讲师

等级保护测评主要测试哪些呢？

京安小妹

熊璐：

等级保护测评包括技术测评和管理测评2个部分。技术测评主要包括物理环境安全（机房）、网络通信安全（网络结构）、区域边界安全（边界安全防护措施）、计算环境安全（包括网络设备、安全设备、操作系统、数据库、应用软件、中间件、数据）、安全管理中心（安全管理中心仅三级及以上要求）五个层面，还需进行工具测试和渗透测试（如有特殊原因，客户可以选择不进行，但需签署自愿放弃验证声明）。管理测评主要包括安全策略和管理制度、安全管理机构和人员、安全建设管理和安全运维管理四个层面。

讲师

等级保护测评流程是什么，对公司人员要求是什么？？

京安小妹

熊璐：

信息安全等级保护工作包括定级（用户自主定级）、备案（到公安机关备案）、安全建设和整改、等级测评（根据定级报告中的级别测评看是否达到该级别应达到的要求）、监督检查五个环节。等级测评前需对系统进行定级和备案，等级测评流程分为项目准备阶段、方案编制阶段、现场测评阶段和报告编制阶段四个阶段。为避免测评结论为不符合且能获得较高分数，等级测评前建议公司人员先对系统进行基础加固和整改，其中包括机房整改、网络结构调整、安全设备部署、网络设备和服务器操作系统、数据库、中间件的策略加固、应用整改和漏洞修复等。

讲师

等级保护对于企业中的意义在哪里？？

京安小妹

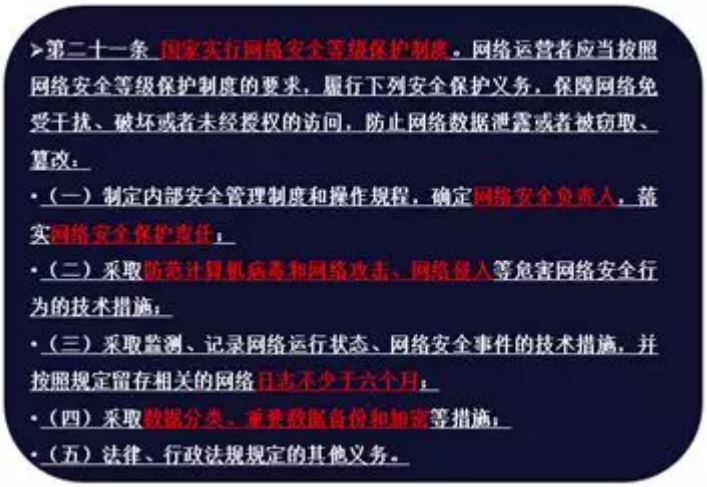
熊璐：

等级保护对企业的意义在于：

一是政策合规，等级保护是我国关于信息安全的基本政策，《网络安全法》第二十一条明确规定：国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。网络运营者不履行第二十一条规定的网络安全保护义务的，可以由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

二是满足自身业务安全需求，互联网企业包括电商、金融、旅游、医疗、教育、媒体等，业务系统中大多承载了大量用户信息、业务信息，其中电商和金融系统还包括交付功能，如未开展等级保护，这些系统的安全问题不会被提前发现，一旦被不法分子利用，将可能造成服务器被控制、用户不需付钱就可支付，用户信息泄露、重要数据泄露和新闻数据被篡改等严重后果。通过等级测评工作可以提前信息系统存在的安全隐患和不足，进行安全整改之后，提高信息系统的信息安全防护能力，降低系统被攻击的风险，维护单位良好的形象。

三是落实个人及单位的网络安全保护义务，合理规避风险。



讲师

互动问答环节：

1. 从技术人员转向等保合规需要什么证书或者技能么？

讲师:

转为测评师需要考取测评师证，分初、中、高级,测评师在公安部考取。

如果是协助过等保，就是等保咨询，这个没有明确的咨询要求，熟悉标准就行

2. 等保合规现在全国有统一标准么？目前似乎还是要按照当地机构要求进行相关工作？

讲师:

等保是有标准的，《信息安全技术 信息系统安全等级保护基本要求》（GB-T 22239-2008）

这是等保1.0的标准，2.0现在在报批稿阶段了，应该很快就会发布，名称改为了《信息安全技术 网络安全等级保护基本要求》

3. ISO27000这些标准，在国内的认可程度如何？

讲师:

国内还是等保为主，ISO27000在一些外企用得多一点，而且ISO27000是偏管理的。

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。