网络安全为人民

网络安全靠人民

国家网络安全宣传周
China Cybersecurity Week

国家网络安全宣传周
China Cybersecurity Week

等级保护 知识手册

网警师徒带你了解信息系统安全知识

目 录

网警师徒说

当今社会，互联网应用已经融入到了我们日常生活的方方面面。不同年龄、职业、生活环境的人们，都会随时随地使用手机、电脑进行即时通讯、浏览新闻、生活缴费、股票交易……互联网使我们的生活丰富多彩。

“互联网+”为我们带来方便、快捷生活的同时，也存在诸多安全隐患。如果生活常用信息系统存在安全漏洞，在遭受恶意攻击破坏后，可能出现系统停运、非法入侵等突发问题，对社会秩序和公共利益造成不良影响。

2017年6月1日实施的《中华人民共和国网络安全法》（以下简称《网络安全法》）是网络安全领域的基本法。《网络安全法》第二十一条规定，我国实行网络安全等级保护制度。各行各业通过开展等级保护工作，及时发现网络信息系统与国家安全标准之间存在的差距，排查系统存在的安全隐患，通过安全整改，提高信息系统的安全防护能力，有效降低系统被攻击风险。网络安全等级保护制度为我们建立起安全稳定的网络防护屏障，有效保护人民生活财产安全。

下面，我们将详细讲解等级保护制度的基本内容、典型案例和法律知识，带您更加深入了解等级保护与我们生活的密切关系。

北京市公安局网安总队 欧阳静茜

北京市公安局网安总队 问闻

等级保护制度基本知识

（一）什么是网络安全等级保护

网络安全等级保护是我国网络安全保障的一项基本制度，是国家通过制定统一的网络安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统和载体按照重要性等级分级别进行保护的一项重要工作。

网络安全等级按照系统或信息的重要性和遭受损坏后的危害程度分成五个安全保护等级，第一级安全要求低，第五级安全要求最高，逐级增高。国家针对互联网上为社会大众服务的系统，对应不同等级保护级别提出了不同的安全要求，包括通用安全要求和扩展安全要求，并强制执行。

我们日常生活中使用的水、电、气缴费系统，访问的门户网站等，通常为第二级或第三级系统。银行、金融行业的资产管理系统、支付交割系统、资金账户管理系统等，通常为第三级甚至更高级别。

等级保护制度基本知识

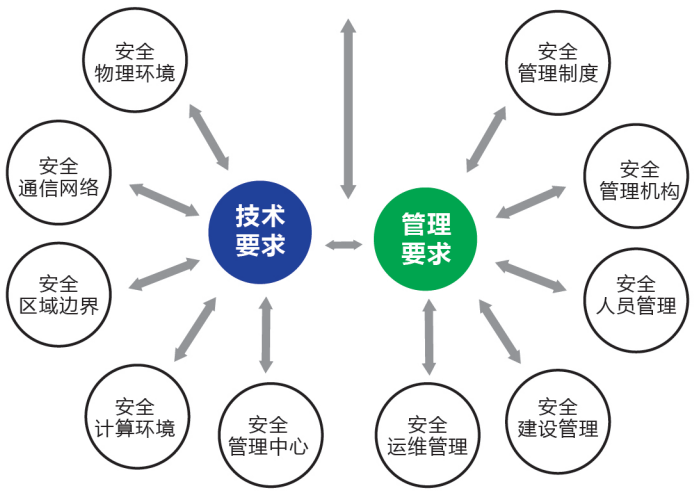
（二）等级保护2.0的主要内容

我国等级保护工作和信息化建设是同步进行的。1994年国务院下发了《中华人民共和国计算机信息系统安全保护条例》（国务院147号令），首次提出信息安全等级保护的概念，并通过二十多年时间建立了配套的法律法规、标准规范和产业体系，用于解决我国党政机关和企事业单位的信息化建设中的信息安全问题。

2017年6月1日，全国人大发布了《中华人民共和国网络安全法》，明确了等级保护的法律地位，并将使用范围扩大至全社会各领域、各行业，这标志着等级制度进入2.0时代。

原有的保护对象主要包括各类重要信息系统和政府网站，保护方法主要是对系统进行定级备案、等级测评、建设整改、监督检查等。在此基础上，等保2.0扩大了保护对象的范围、丰富了保护方法、增加了技术标准。等保2.0将网络基础设施、重要信息系统、大型互联网站、大数据中心、云计算平台、物联网系统、工业控制系统、公众服务平台等全部纳入等级保护对象，并将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置等工作措施全部纳入等级保护制度。

等级保护2.0基本要求

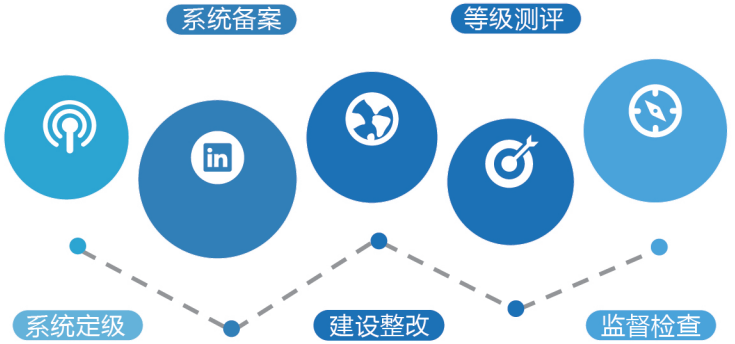


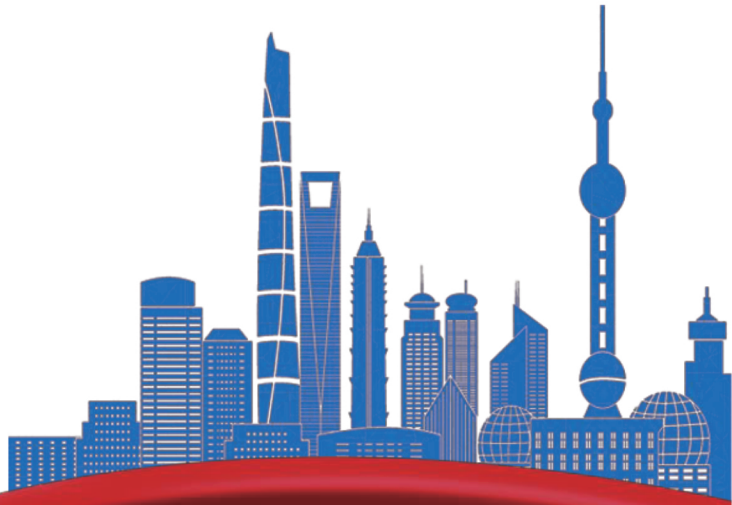
等级保护制度基本知识

（三）网络安全等级保护的基本流程

国家通过制定统一的管理规范和技术标准，组织行政机关、法人、其他组织和公民根据信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。

公安机关是网络安全等级保护制度的执法机构，重要工作包括五个环节：系统定级、系统备案、建设整改、等级测评、监督检查。具体内容为：网络运营者及主管部门在建设规划阶段结合专家评审准确定级，再到县级以上公安机关进行备案。网络运营者对照安全保护等级具体要求进行安全保护建设与整改，系统运营使用单位与测评机构定期开展网络安全等级测评工作，公安机关负责开展相应监督检查工作，保证安全整改措施落实到位。





案　例

（一）宜宾某网站因存在高危漏洞遭入侵被处罚

2017年7月22日，四川省宜宾市翠屏区“教师发展平台”网站因网络安全防护工作落实不到位，导致网站存在高危漏洞，造成网站发生被黑客攻击入侵的网络安全事件。宜宾网安部门在对事件进行调查时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。根据《网络安全法》第五十九条第一款之规定，决定给予翠屏区教师培训与教育研究中心和直接负责的主管人员法人代表唐某某行政处罚决定，对翠屏区教师培训与教育研究中心处一万元罚款，对法人代表唐某某处五千元罚款。

网警提示

（二）汕头某公司未履行网络安全义务被警告

2017年7月20日，广东汕头网警支队在对该市网络安全等级保护重点单位进行执法检查时发现，汕头市某信息科技有限公司于2015年11月向公安机关报备的信息系统安全等级为第三级,经测评合格后投入使用，但2016年至今未按规定定期开展等级测评。

该公司之行为已违反《信息安全等级保护管理办法》第十四条第一款和网络安全法第二十一条第（五）项规定，未按规定履行网络安全等级测评义务。根据《网络安全法》第五十九条规定，广东汕头网警支队依法对该单位给予警告处罚并责令其改正。

案　例

（三）山西忻州市某省直事业单位未履行网络安全保护义务被处罚

2017年6月至7月间，山西忻州市某省直事业单位由于法律意识淡薄，疏于管理导致网站存在SQL注入漏洞，严重威胁网站信息安全，连续被国家网络与信息安全信息通报中心通报。根据《网络安全法》第二十一条第二款之规定，网络运营者应当按照网络安全等级保护制度的要求，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；第五十九条第一款之规定，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，由有关主管部门责令改正，依法予以处置。该单位行为已违反《网络安全法》相关规定，当地公安机关网安部门对该单位进行了现场执法检查，依法给予行政警告处罚并责令其改正。

（四）宿迁网警成功查处全省首例违反《网络安全法》接入违规网站案

江苏省宿迁市某科技有限公司服务器内接入一违法网站被发现，民警对服务器进行勘验取证后，立即就此事约谈相关负责人，开展调查。要求对服务器内涉及法律、行政法规禁止传输的信息，立即采取停止传输 、消除等处置措施，保存有关记录，根据《网络安全法》规定，给予上述公司警告处罚并要求其立即整改。

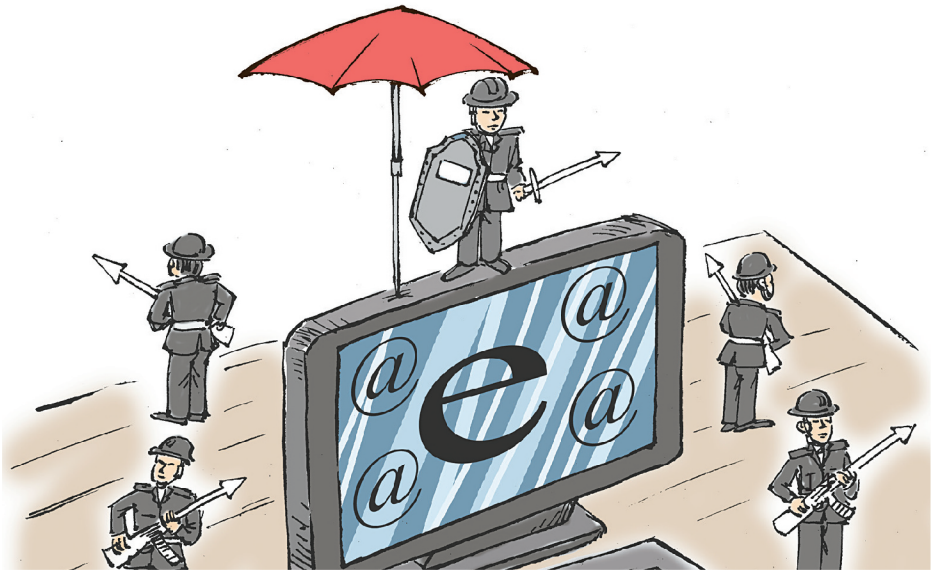
案　例

（五）淮南某高校系统漏洞导致学生身份信息泄露

淮南市公安局网安支队接到国家网络与信息安全信息通报中心通报：淮南某技术学院系统存在高危漏洞，招生信息管理系统中存储的4000余名学生身份信息被泄露。根据现场勘验和调查取证工作情况，淮南市公安局网安支队依法就此事约谈学院相关负责人进行调查。经查，确认该学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的4353名学生的身份信息遭到泄露。淮南市公安局网安支队依法对淮南职业技术学院处以立即整改和行政警告的处罚措施。

（六）蚌埠怀远县某学校未落实网络安全防护和等级保护制度被处罚

2017年8月12日，蚌埠怀远县某学校网站因网络安全防护及等级保护制度落实不到位，遭黑客攻击入侵。蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。2017年8月16日，安徽省公安厅网络安全保卫总队约谈该学校法定代表人、怀远县人民政府分管副县长。蚌埠市局网安支队依法对网络运营单位处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。



您需要了解的法律知识

《中华人民共和国网络安全法》

第十二条 规定：国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第二十一条 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，履行下列安全保护义务，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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十七条 规定：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

您需要了解的法律知识

第四十一条 规定：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十三条 规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第六十四条 规定：网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

首都网警微博

首都网警微信

首都网警今日头条

更多的网络安全知识
请您关注
“首都网警”
相关账号

技术支持单位：深信服科技股份有限公司