网络安全宣传手册

（党政机关及企事业单位篇）

中共浙江省委网络安全和信息化委员会办公室

2019年8月

目录

网络安全形势日益严峻 1

网络安全已成国家战略 2

网络安全需要科学的观念 3

网络安全需要履行的责任 4

网络安全典型事件案例 9

**网络安全形势日益严峻**

当前，我国网络安全面临的形势异常严峻、复杂，网络空间的政治战、舆论战、信息战和技术战日趋激烈、公开化，政府网站及金融、能源、电力、通信、交通等领域关键信息基础设施已经成为网络攻击的重点目标，主权国家、恐怖组织、黑客团伙、经济犯罪等各种威胁源头相互交织，呈现出多元复杂的态势，网络安全造成的影响和范围越来越大，损害程度越来越严重。



1.2019年3月，委内瑞拉多次发生大规模停电事件，据报道系美国针对其国内水电站发动了网络攻击，利用恶意程序侵入委内瑞拉电网造成大规模停电。

2、2015年5月至今，勒索病毒不断升级变种持续袭击党政、教育、卫生、科研等部门，造成重要数据被加密、系统瘫痪，严重影响正常生产生活开展。

3、自2012年开始，境外“反共”黑客组织每3天攻击境内网站并张贴反动标语。

**网络安全已成国家战略**

2014年2月27日，中央网络安全和信息化领导小组成立，统筹协调涉及各个领域的网络安全和信息化问题，习近平总书记担任组长，这标志着网络安全提升至国家战略层面。

2016至2019年，习近平总书记每年在网络安全和信息化专门会议上发表重要讲话：树立正确的网络安全观、加快构建关键信息基础设施安全保障机制、全天候全方位感知网络安全态势、加速推动信息领域核心技术突破、增强网络安全防御能力和威慑能力。

**网络安全需要科学的观念**

统筹管理的总体安全观：整合相关机构职能，统筹协调涉及政治、经济等各个领域的网络安全和信息化重大问题。

网络强国的目标愿景观：网络安全和信息化，要从国际国内形势出发，总体布局、统筹各方、创新发展，努力把我国建设成为网络强国。

科学辩证的安全认知观：网络安全和信息化是一体之两翼、驱动之双轮，处理好安全和发展的关系，安全是发展前提、发展是安全的保障，安全与发展同步推进。

协调规范的综合治理观：提高网络综合治理能力，形成党委领导、政府管理、企业履职、社会监督、网民自律等多主体参与，经济、法律、技术等多手段结合的综合治网格局。

不拘一格的专业人才观：突出专业性、创新性、实用性，制定吸引人才、培养人才、留住人才的办法，建立适应网信特点的人才评价机制。

携手应对的合作共赢观：在核心技术研发上，推动强强联合，协同攻关，尽快突破。

**网络安全需要履行的责任**

【履行党委（党组）网络安全工作责任制】

按照谁主管谁负责、属地管理的原则，各地各部门党委（党组）对本地本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人，认真贯彻落实网络安全工作方针政策、法律法规，明确保护工作主要目标、基本要求、工作任务、保护措施，提供人财物保障。

网络安全党委责任制落实情况已纳入省委省政府重点督查项目，网络安全工作也已纳入平安建设考核。各级党委（党组）违反或者未能正确履行职责造成重大影响，将按照《浙江省党委（党组）网络安全工作责任制实施细则》追究当事人、网络安全负责人直至主要负责人责任。

【落实网络安全等级保护制度】

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。

工作要求。网络运营者应对本单位的等级保护对象（网络和信息系统）落实网络安全等级保护制度，组织开展定级、备案、安全建设、等级测评（委托有资质的第三方测评机构开展）、监督检查等工作。

【履行关键信息基础设施保护义务】国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

落实“三同步”原则。安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

实施重点保护。在落实网络安全等级保护的基础上，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

工作要求。1、**运营者**每年至少自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险进行一次检测评估。2、**运营者**要及时处置并报告发生的重大网络安全事件和发现的重大网络安全隐患。3、**行业主管部门**要定期组织开展本行业、本领域关键信息基础设施的安全检测和风险评估。4、**行业主管部门**要建立健全本行业、本领域关键信息基础设施网络安全监测预警平台和通报预警制度。5、**行业主管部门**建立健全本行业、本领域关键信息基础设施网络安全应急预案，每年组织开展应急演练。

**网络安全典型事件案例**

**1.某国企子公司网站被篡改并张贴反动标语被问责。**该单位网站存在高危安全漏洞，被反共黑客攻击并张贴政治类标语。该网站自上线运行以来，未进行安全检测，未落实网络安全等级保护制度，未履行网络安全责任。网信部门责成该国企启动内部问责程序。

评：一些高危安全漏洞如Strus2漏洞、管理账户使用弱口令等，技术门槛很低，被是反共黑客等低水平攻击者的常用攻击手段。

**2.某省直事业单位网站不履行网络安全保护义务被处罚。**某省直事业单位网站存在SQL注入漏洞，严重威胁网站信息安全，连续被网信部门和公安机关通报要求整改而没有整改，且未按规定定期开展等级测评，被公安机关依法给予行政处罚。

评：等级保护制度是我国网络安全保护的基本制度。区县级重要的信息系统，地市级和省级的一般信息系统，一般定为二级，需要定期开展等级保护评测。

**3.某市多家医院因感染勒索病毒导致无法正常就医。**近期，某地级事多家医院信息系统因没有及时整改安全隐患而感染勒索病毒、数据被加密、系统瘫痪，导致百姓无法正常就医。部分医院因数据没有备份，只能通过向黑客支付赎金方式恢复数据。

评：数据备份是网络安全的生命线，重要数据必须做好备份确保安全可靠。同时，要开展经常性的应急演练提升应急处置能力。



**4.某市级部门网站被黑客攻击并植入后门软件。**经技术分析，黑客由境外跳转至香港IP对该网站实施攻击，并上传了网页木马。利用该网页木马，黑客可以随时控制网站，窃取信息，篡改内容。

评：后门软件是一种恶意软件，长期潜伏在信息系统中，可能随时发动攻击。网络安全软件要经常更新、升级，具备查杀主流恶意软件的能力。

**5.信息技术服务外包商窃取公民个人信息。**杭州滨江区某科技公司利用承接省内某疾病预防控制部门信息化建设项目机会，窃取该部门300余万条接种疫苗的儿童及家长个人信息，随后将获取的数据贩卖获利，被公安机关查处。

**6.省民政厅及时排查婚姻登记数据异常访问事件。**省民政厅安全员发现有内部人员通过存在弱口令的账号登录省婚姻登记系统，进行较大数量的婚姻状况查询。对此，省民政厅立即排查相关账号和查询人，排除了数据进一步泄露的风险。

评：近年来，我省已发现多起内部账号、运维账号非法访问或窃取数据的行为。除了按照《浙江省信息技术服务外包网络安全管理规定》加强管理外，配备先进的日志审计系统也是网络安全建设的重要内容。