安恒信息官方微信

聚焦云安全、态势感知、大数据安全、互联网及物联网安全等领域

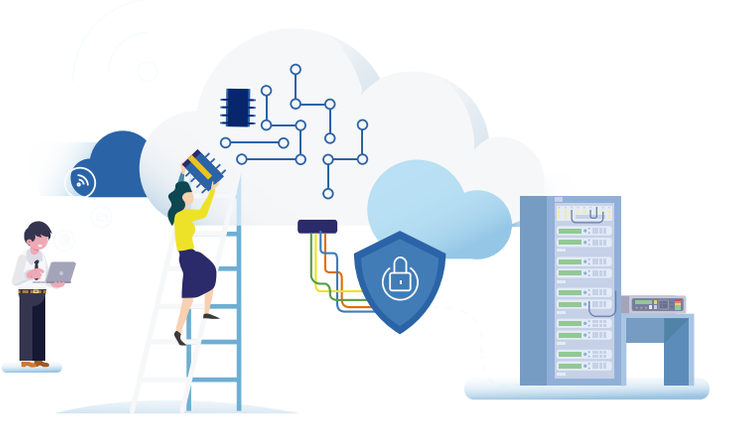
发布国内外网络安全时事热点

网络安全科普手册

党政机关及企事业单位篇

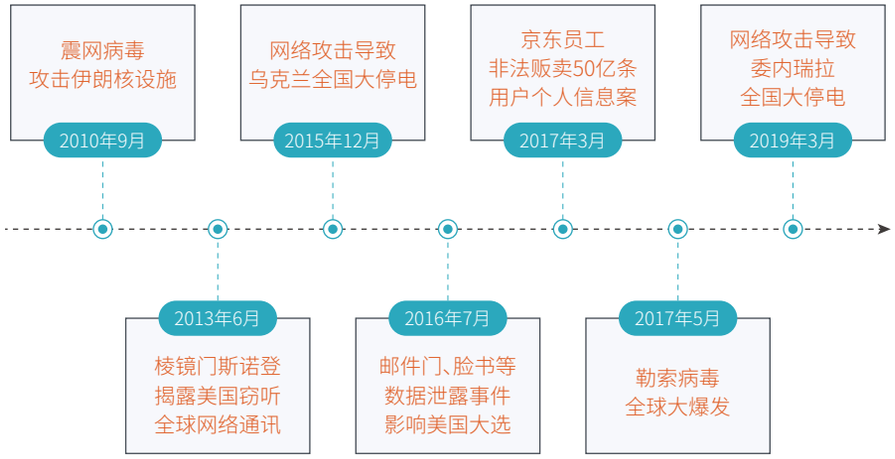
中共浙江省委网络安全和信息化委员会办公室
2019年8月

目录/contents



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。



- 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。
- 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。
- 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。

网络安全需要履行的责任

【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。

网络安全需要履行的责任

【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

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。
- 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。

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。
- 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。
- 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。

网络安全典型事件案例

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。

网络安全典型事件案例

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。

评： 公民个人信息受我国《网络安全法》保护，非法手段窃取公民个人信息属违法犯罪行为，将依法受到公安机关惩处。同时相关部门在信息化建设过程中，应提高公民个人信息保护意识，加强对公民個人信息保护的力度。

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。

关于如何提高政府企事业单位网络安全意识的建议

（一）多形式多举措加强宣传教育

针对信息安全意识、安全技能、热点安全事件组织开展经常性的网络安全教育培训，邀请信息安全领域安全专家进行授课、实战化训练，对全省县（省、区）级以上政法部门进行网络安全业务培训，建立常态化政法工作信息安全人才队伍建设与培养机制，增强网络安全意识和防护水平。

（二）自觉规范网络行为

实践的过程即是安全意识养成的过程，渐渐的你将形成自己的网络安全观。比如将微信、QQ、支付宝、邮箱、论坛等各个网络应用的账号密码有意识的设置成高强度的并且全部不同的字符；将自己重要的文档资料定期进行备份；谨慎下载未知程序；不随意打开广告等弹出式网页；安全防护软件及时更新并查杀病毒；安装APP时仔细查看需要授予的权限等。

（三）加强技术层面建设

加强计算机操作技术、网络安全技术方面的培训，强化计算机操作人员对网络病毒、网络安全的防范意识；加大各政法门户网站安全防护建设投入力度，开展网站安全专项检查；利用系统加固对抗未知漏洞的攻击；构建云安全防护体系，尤其需要重视大数据安全，最终从重边界防护转到云、管、端安全并重。

（四）强化网络安全管理工作

制定并实施完善的网络安全管理体系和制度，如机房出入管理制度、操作规程、系统维护制度、网络安全防范处置预案等，统一进行政法部门网络安全顶层规划设计。

关于如何提高政府企事业单位网络安全意识的建议

（五）加强组织和人员保障

加强部门网络安全组织保障，设置足够的岗位编制，建立网络安全技术运维团队，加大第三方网络安全服务采购投入。

（六）建立网络安全应急保障体系

建立完善的应急处置机制和流程，针对各类网络安全应急事件，制定一体化的应急预案，加强日常应急值守，确保网络安全应急机构24小时在岗值班，做好重大网络安全事件预防防护、应急处置和应急技术支援工作。

（七）开展政法系统“护网演练”

通过攻防演练的方式，对政法企事业单位的系统安全防护能力、安全运维能力以及安全事件的监测、响应能力进行全面的检验，最终实现以赛促学，以赛代练，达到增强网络安全意识的目的。

（八）建立网络安全监测预警和信息通报制度

加强网络安全信息收集、分析和通报工作，充分发挥信息通报作用，完善通报机制和平台建设，形成了政法企事业单位网络态势感知能力、通报预警能力、数据分析能力、指挥协同能力和追踪溯源能力。

网络安全意识

网络安全意识——邮件系统安全

【违规现象】
邮箱开启自动转发功能

【措施与建议】
关闭邮箱自动转发功能

【违规现象】
私设外网邮件系统，未使用公司统一外网邮件系统

【措施与建议】
用外网邮箱处理工作文件时应统一使用公司外网邮箱。严禁私设外网邮件系统

【违规现象】
邮件系统未开启收发日志审计和敏感内容拦截策略等功能

【措施与建议】
邮件系统应开启收发日志审计和敏感内容拦截策略等功能

【违规现象】
对外发送敏感内容文件未采取保护措施

【措施与建议】
对外发文件应根据其敏感性采取安全加密、打开次数控制、有效时间控制、打印控制、白名单等措施加强外发文件保护

网络安全意识——桌面终端安全

【违规现象】
移动存储介质未更改初始口令、内部人员口令通用导致信息泄露

【措施与建议】
在第一次使用移动存储介质时应及时修改初始口令，并避免口令在内部人员混用

【违规现象】
个人手机或智能可穿戴设备连接办公计算机

【措施与建议】
严禁内网办公计算机连接个人手机或智能可穿戴设备

【违规现象】
操作系统、数据库系统账号使用8位以下只有数字构成的口令，从未定期修改

【措施与建议】
操作系统和数据库系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同

【违规现象】
未开启桌面终端监控，桌面终端注册率、防病毒软件安装率、保密检测系统安装率未达到100%

【措施与建议】
应严格按照公司要求安装桌面终端管理软件，开启桌面终端监控软件。桌面终端注册率、防病毒软件安装率和保密检测安装率达到100%

网络安全意识——桌面终端安全

【违规现象】
信息内、外网计算机违规存储、处理国家秘密信息
【措施与建议】
定期进行关键字检查，规范员工工作习惯，保证信息内网不存在国家秘密、信息外网不存有国家秘密和企业秘密

【违规现象】
使用企业邮箱或外部邮箱发送含公司敏感信息内容邮件
【措施与建议】
如需使用外部邮箱，应严格按照公司规定使用公司统一邮件系统发送邮件，并且发送内容不得包含公司敏感信息

【违规现象】
将涉及国家秘密的计算机、存储设备与信息内、外网及其他公共信息网络连接
【措施与建议】
定期进行关键字检查，规范员工工作习惯，保证信息内网不存有国家秘密

【违规现象】
普通移动存储介质和扫描仪、打印机等计算机外部设备在信息内部和信息外网交叉使用
【措施与建议】
要建立移动存储介质安全管理制度，严禁普通移动存储设备及其他外部设备在信息内网和信息外网间交叉使用

网络安全意识——信息涉密安全

【违规现象】
员工离职、调动后未注销其在信息系统中所有的账号和访问权限
【措施与建议】
应制定有关管理规范，严格规范员工离岗过程，以及终止离岗员工所有访问权限

【违规现象】
未签署保密协议，重要安全岗位人员离职时未签署保密协议
【措施与建议】
应与员工签署保密协议，重要安全岗位人员离职时应签署保密协议

【违规现象】
新增的公司公共微博、微信账号未备案

【措施与建议】
在公司公共微博、微信账号开通之前应进行安全备案与使用管理

【违规现象】
在公司公共微博、微信上发布未经审核的内容

【措施与建议】
在微博、微信发布内容前，所发布的内容都需进行审查与核实

网络安全意识——内外网安全

【违规现象】
内网办公计算机通过无线上网卡等方式连接互联网

【措施与建议】
禁止内网终端使用智能手机、无线上网卡等无线上网设备连接互联网，对违规外联用户应进行严肃查处

【违规现象】
在公司外网随意用wi-fi组网

【措施与建议】
严格执行公司办公计算机保密制度，wi-fi网络必须具有网络准入、安全审计、用户身份认证等安全防护手段

【违规现象】
通过互联网接入信息内网进行远程维护

【措施与建议】
禁止通过互联网接入信息内网设备和系统的远程维护

【违规现象】
在信息内网使用无线网络组网

【措施与建议】
在信息内网应采用有线网络的形式组网

网络安全意识——内外网安全

【违规现象】
信息内网和信息外网交叉使用

【措施与建议】
严格区分信息内网和信息外网计算机，两者不能混用

【违规现象】
信息内网计算机配置无线设备

【措施与建议】
严禁信息内网计算机配置无线鼠标、无线键盘和无线上网卡等无线设备

【违规现象】
家属区网络违规接入信息内、外网

【措施与建议】
家属区网络应严格按照公司要求进行管理，严禁违规接入信息内、外网

【违规现象】
无线网络未开启网络接入控制和身份认证

【措施与建议】
无线网络应启用认证功能，并设置8位以上数字和字母或特殊字符混合的密码