网络信息安全周报

【2017】第 30 期

党委宣传部
信息网络中心　编　　2017 年 11 月 30 日

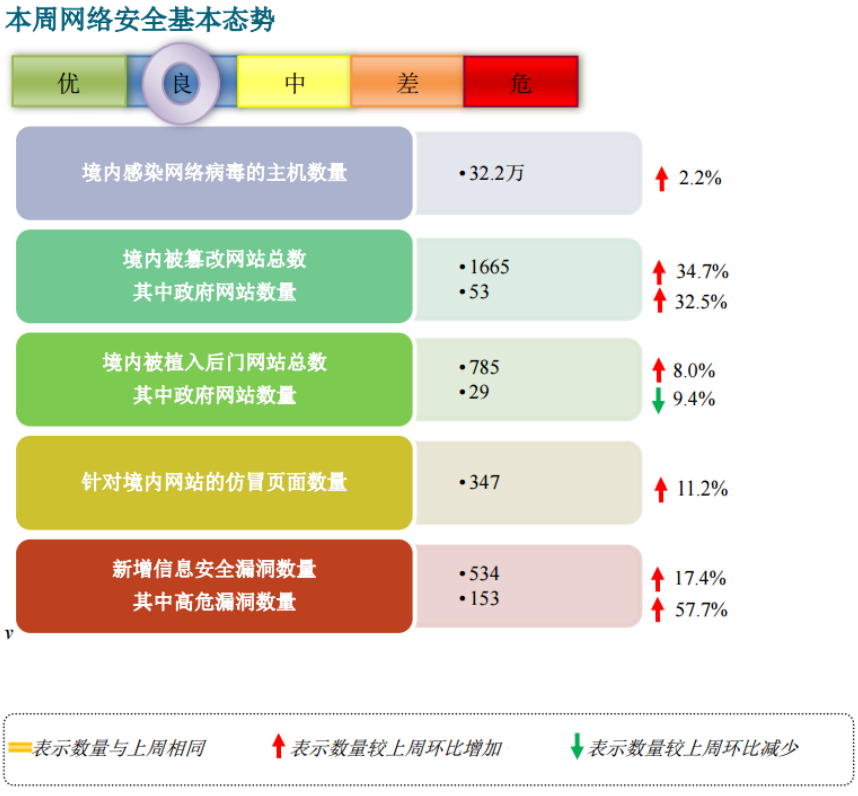
本期要目

- 【权威发布】全国网络安全信息与动态（2017 年 11 月 6 日-11 月 12 日）
- 【城院 IT】综合业务管理平台统计信息(2017 年 11 月 13 日—19 日)
- 【新闻解读】为了咱们的网络安全，国家放过哪些大招？

全国网络安全信息与动态

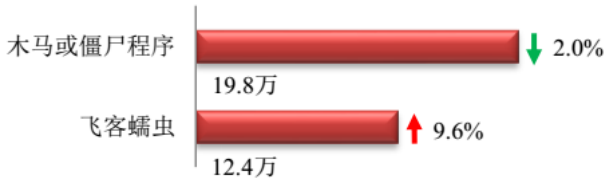
（2017 年 11 月 6 日—11 月 12 日）

根据国家互联网应急中心最新公告数据：



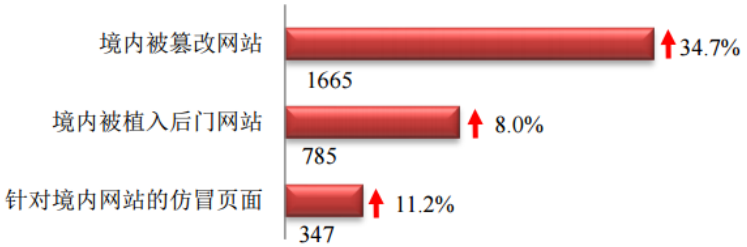
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 32.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.8 万以及境内感染飞客（conficker）蠕虫的主机约 12.4 万。



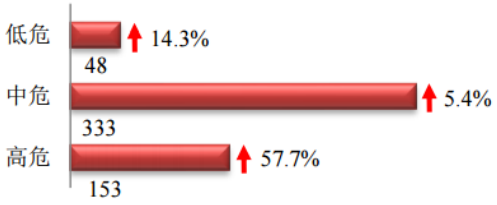
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1665 个；境内被植入后门的网站数量为 785 个；针对境内网站的仿冒页面数量为 347。



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 534 个，信息安全漏洞威胁整体评价级别为中。



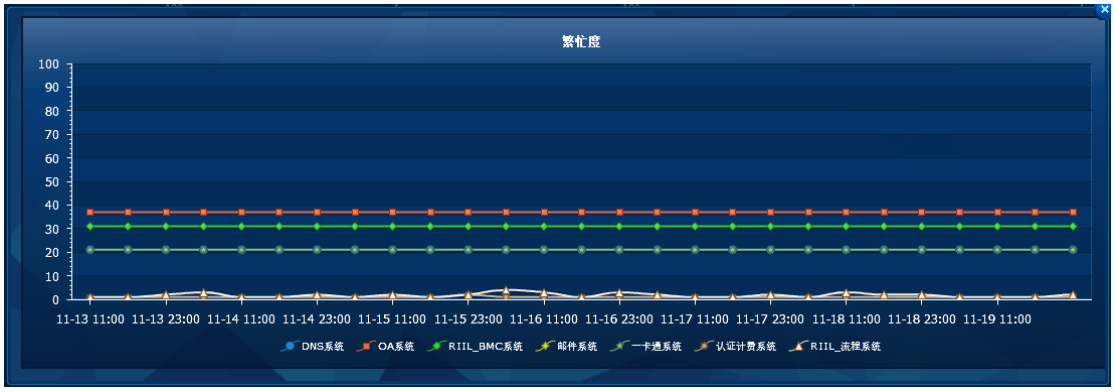
本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 465 起，其中跨境网络安全事件 206 起。

城院 IT 综合业务管理平台统计信息

（2017 年 11 月 13 日—11 月 19 日）

主要业务服务繁忙度



网站集群网页更新情况统计

站点名称	发布		站点名称	发布
兰州城市学院	47		机关党委	
就业服务网	10		城市信息与系统科学研究所	
教学质量监测与评估中心	9		审计处	
外国语学院	7		兰州城市学院教育评估中心	
音乐学院	6		兰州城市学院校医院	
商学院	5		美术与设计学院	
马克思主义学院	4		保卫处	
地理与城乡规划学院	3		城市社会心理研究中心（新）	
传媒学院	3		党委宣传部	
文史学院	3		体育学院	
数学学院	3		发展规划处	
电子与信息工程学院	3		人事处	
幼儿师范学院	2		电子信息科学与技术研究所	
甘肃张芝书法院	2		基本建设处	
教育学院	2		国有资产管理处	
石油工程学院	2		党委（校长）办公室	
化学与环境工程学院	1		创新创业学院	
科学研究处	1		卡务中心	
信息网络中心	1		传媒学院（新）	
路易艾黎研究中心	1		甘肃文化翻译中心	
膳食处	1		城市社会心理研究中心	
党委学生工作部	1		后勤管理处	
旅游学院	1		档案馆	
信息技术教育与应用研究所			教务处	
机械工程学院			党委组织部	
职业技能鉴定所			教师发展中心	
兰州城市学院心理咨询中心			团委	
甘肃省高等学校外语教学指导委员会			实训中心	
学位办公室			廉政网	
招生网				

站群系统应用防火墙入侵防护记录

A	B	C	D	E	F
序号	入侵位置	入侵者IP	归属地	入侵方式	入侵时间
191174	管理平台：就业服务网	117.157.64.40	中国 移动	错误帐号或密码	2017-11-17 23:33:35
191173	管理平台：就业服务网	113.200.106.4	陕西省西安市 联通	错误帐号或密码	2017-11-17 23:30:40
191172	管理平台：就业服务网	113.200.106.4	陕西省西安市 联通	错误帐号或密码	2017-11-17 23:25:52
191171	管理平台：就业服务网	117.157.64.40	中国 移动	错误帐号或密码	2017-11-17 23:23:45
191170	站点名称：外国语学院	42.184.185.46	黑龙江省鸡西市 电信	SQL注入	2017-11-17 21:13:12
191164	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	SQL注入	2017-11-16 23:28:36
191163	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	SQL注入	2017-11-16 23:28:35
191162	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	SQL注入	2017-11-16 23:28:32
191160	管理平台：就业服务网	124.152.132.23	甘肃省 联通	错误帐号或密码	2017-11-15 21:59:23
191159	管理平台：就业服务网	42.92.178.156	甘肃省 电信	错误帐号或密码	2017-11-15 10:41:42
191158	站点名称：外国语学院	118.69.29.226	柬埔寨	SQL注入	2017-11-14 19:29:53
191157	站点名称：信息网络中心	118.69.29.226	柬埔寨	SQL注入	2017-11-14 19:29:33
191156	管理平台：就业服务网	117.157.64.233	中国 移动	错误帐号或密码	2017-11-14 19:08:25
191152	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	跨站脚本注入	2017-11-14 10:06:29
191151	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	跨站脚本注入	2017-11-14 10:06:07
191150	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	跨站脚本注入	2017-11-14 10:06:03
191149	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	SQL注入	2017-11-14 08:23:43
191148	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	SQL注入	2017-11-14 08:23:43
191147	站点名称：兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联通节点	SQL注入	2017-11-14 08:23:43
191146	站点名称：兰州城市学院	124.42.13.235	北京市 光环新网	跨站脚本注入	2017-11-13 17:06:36
191145	站点名称：兰州城市学院	124.42.13.235	北京市 光环新网	跨站脚本注入	2017-11-13 17:06:26
191144	站点名称：兰州城市学院	124.42.13.235	北京市 光环新网	跨站脚本注入	2017-11-13 17:06:26

站群系统应用防火墙网站访问 IP 封禁记录

封禁IP	封禁IP归属地	封禁开始时间 ▼
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2017-11-16 23:28:36
182.118.33.6	河南省郑州市 奇虎360科技联通节点	2017-11-14 10:06:29
182.118.33.6	河南省郑州市 奇虎360科技联通节点	2017-11-14 08:23:43
124.42.13.235	北京市 光环新网	2017-11-13 17:06:36
202.200.145.187	陕西省西安市 西安建筑科技大学	2017-11-12 14:19:31
173.208.164.162	美国 密苏里州堪萨斯城WholeSale互联网股份有限公司	2017-11-10 16:26:20
61.178.60.177	甘肃省兰州市 一只船北街万网网吧	2017-11-09 15:29:50
61.178.60.177	甘肃省兰州市 一只船北街万网网吧	2017-11-09 15:28:05
117.22.102.89	陕西省西安市 电信	2017-11-08 19:20:10
61.178.60.177	甘肃省兰州市 一只船北街万网网吧	2017-11-08 16:08:51

站群系统应用防火墙网站危险文件扫描记录

序号	路径	类型
1	E:\VSB9\manager\system_owners\lyxy_webprj\content.jsp	恶意js引用
2	E:\VSB9\manager\system_owners\lzcsxy_webprj\cheng_2.jsp	恶意js引用
3	E:\VSB9\manager\system_owners\lzcsxy_webprj\content.jsp	恶意js引用
4	E:\VSB9\manager\system_owners\lzcsxy_webprj\dh_jianjie.jsp	恶意js引用
5	E:\VSB9\manager\system_owners\lzcsxy_webprj\index.jsp	恶意js引用
6	E:\VSB9\manager\system_owners\lzcsxy_webprj\list.jsp	恶意js引用
7	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_1.jsp	恶意js引用
8	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_2.jsp	恶意js引用
9	E:\VSB9\manager\system_owners\lzcsxy_webprj\new_list_1.jsp	恶意js引用
10	E:\VSB9\manager\system_owners\lzcsxy_webprj\xiaobao.jsp	恶意js引用
11	E:\VSB9\manager\system_owners\lzcsxy_webprj\xinxiang.jsp	恶意js引用
12	E:\VSB9\manager\system_owners\lzcsxy_webprj\xr_lingdao.jsp	恶意js引用
13	E:\VSB9\manager\system_owners\sxy_webprj\index.jsp	恶意js引用
14	E:\VSB9\manager\system_owners\sygcxy_webprj\index.jsp	恶意js引用
15	E:\VSB9\manager\system_owners\zsw_webprj\index.jsp	恶意js引用

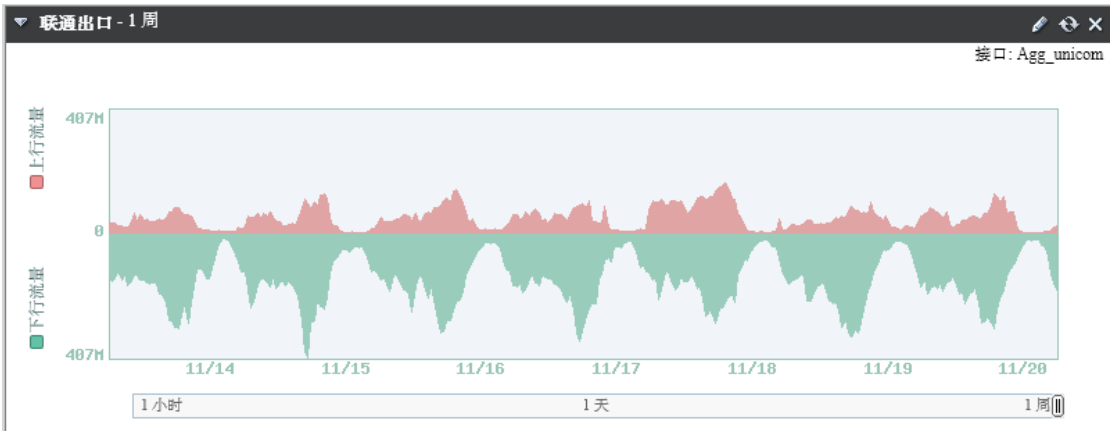
注：文件扫描危险语句记录

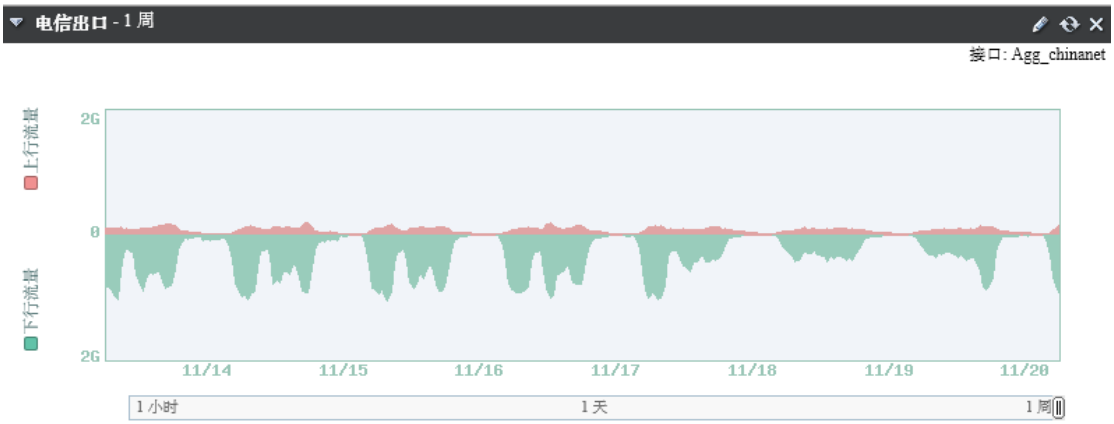
<SCRIPT src="http://bdimg.share.baidu.com/static/api/js/share.js?v=89860593.js?cdnversion=409375">

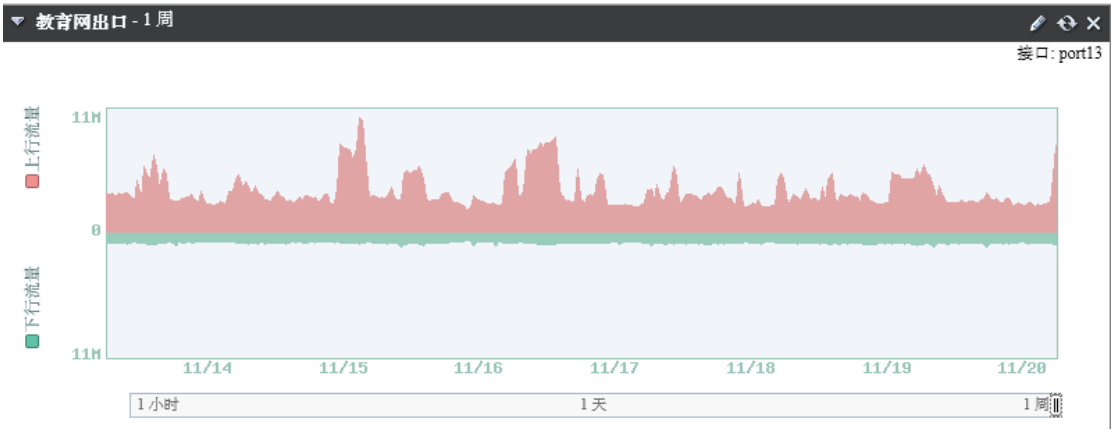
<SCRIPT src="http://bdimg.share.baidu.com/static/api/js/share.js?v=89860593.js?cdnversion=409563">

<SCRIPT id="gjzonedword20150522" charset="UTF-8" src="http://s.pc.qq.com/pcmgr/zonedword/gjzonedword20150522.js" gjguid="e837c6dd9465d4cffea8a4fca6d80b9f" bid="1" sename="百度搜索" seurl="https://www.baidu.com/s?wd=%s&tn=98012088_5_dg&ch=11">

网络出口带宽情况统计



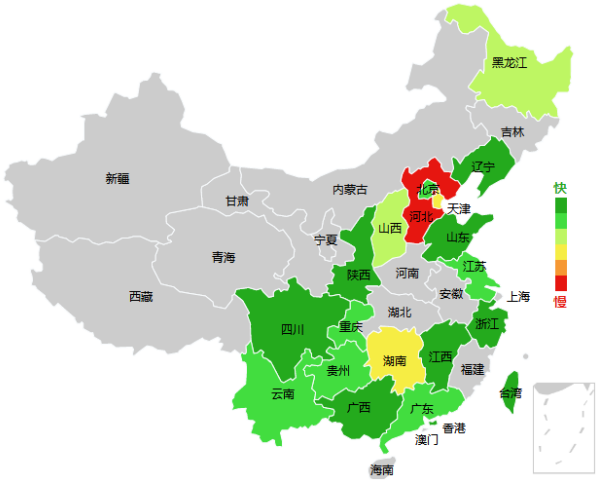




APT统计

防火墙统计	
恶意	2401
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	81447468

360 网站测速（http://www.lzcu.edu.cn）



平均速度排行		
名次	省份	平均速度(KB/s)
1	陕西	1,109.33
2	山西	552.03
3	山东	361.62

北京					
监测点	运营商	总耗时/ms	解析时间/ms	连接时间/ms	下载时间/ms
北京市	联通	387.9	84.68	50.9	252.32
	电信	2473.59	58.68	134.39	2280.52

360 网站评分（http://www.lzcu.edu.cn）

360 网站 DNS 检测（http://www.lzcu.edu.cn）

输入源IP	归属地
219.246.21.192	甘肃兰州教育网

解析结果IP	所用DNS	所属运营商
219.246.21.192	114.114.114.114(114DNS.COM114DNS.COM)	其他
	101.226.4.6(上海电信)	电信
	123.125.81.6(北京联通)	联通
	8.8.8.8(GOOGLE.COMGOOGLE.COMlevel3.com)	其他
	121.28.148.33(河北石家庄联通)	联通
	168.95.1.1(台湾cht.com.tw)	其他
	125.71.5.51(四川成都电信)	电信

网站安全检测一（360 网站安全检测）

注：存在“服务器配置信息泄露”风险，“发现 robots.txt 文件”。

监控对象	类型	监测点	响应时间	访问成功率	
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	4	469.75 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	4	479.95 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	3	216.8 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	3	361.11 ms	100 %	详情

昨日百度中国互联网安全指数上限为100点，距离完美还差49.93点。全行业的网站安全等级偏低。（每日指数上限随观测站点变化而变化）

所有观测站点中，63255个为完美等级站点，751348个为良好等级站点，2168869个为低危等级站点，1157211个为中危等级站点，2491126个为高危等级站点。

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2017-11-19 11:55:06

指数评价

34.0

所属行业：教育培训

29.36% ↓

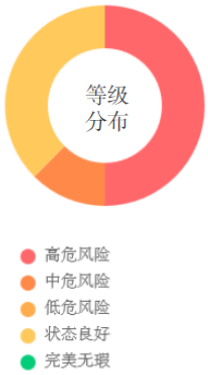
战胜了全国 **0.00%** 的网站

关联网站安全

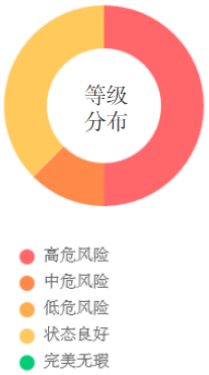
关联网站数	最低指数评价
16	4.0 高危

查看更多>>

该网站安全指数评价 高危 但是仍存在改进空间。建议 开启云观测服务>> ，查看评价详情，获取最新网站安全报警，及时修复以免被搜索引擎风险标识或降权。



域名	指数评价	操作
alumni.lzcu.edu.cn	80 良好	查看详情>>
bf.lzcu.edu.cn	4 高危	查看详情>>
cj.lzcu.edu.cn	49 中危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jpkc2.lzcu.edu.cn	90 良好	查看详情>>
jpkc.lzcu.edu.cn	12 高危	查看详情>>
jwc.lzcu.edu.cn	34 高危	查看详情>>
lzcu.edu.cn	80 良好	查看详情>>
nic.lzcu.edu.cn	90 良好	查看详情>>
oa.lzcu.edu.cn	84 良好	查看详情>>



域名	指数评价	操作
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	4 高危	查看详情>>
smtp.lzcu.edu.cn	4 高危	查看详情>>
syzz.lzcu.edu.cn	4 高危	查看详情>>
test.lzcu.edu.cn	84 良好	查看详情>>
www2.lzcu.edu.cn	4 高危	查看详情>>

当前 2 / 2 页　首页　上一页　下一页　尾页

【新闻解读】为了咱们的网络安全，国家放过哪些大招？

2017-02-08 新华社

网络空间正全面改变人们的生产生活方式，但安全问题不容忽视。除了正在征求意见的“网络产品和服务安全审查办法”外，我国近年来出台不少法律法规和文件，放出大招，打造安全稳定的网络空间。

国家安全法：建设网络与信息安全保障体系

2015 年 7 月通过的国家安全法明确规定：国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

网络安全法：网络领域的基础性法律

2016 年 11 月通过的网络安全法是我国网络领域的基础性法律，明确加强对个人信息保护，打击网络诈骗。该法将于今年 6 月 1 日起施行。

针对个人信息泄露问题，网络安全法规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

针对网络诈骗多发态势，网络安全法规定，任何个人和组织不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

>>中华人民共和国网络安全法
>>专家解读《网络安全法》 具有六大突出亮点
>>网络安全法获表决通过
>>网络安全法获通过 网络运营者不得泄露其收集的个人信息
>>织就网络安全的“法网”——网络安全法六大看点解析
>>聚焦网络安全法遏制网络诈骗四大焦点
>>《网络安全法》解读
>>为《网络安全法》出台点赞
>>《网络安全法》释放了哪些重要信号
>>中国《网络安全法》公布 具有六大突出亮点

《国家网络空间安全战略》：保障网络空间安全的“防火墙”

2016 年 12 月，国家互联网信息办公室发布《国家网络空间安全战略》。这一指导国家网络安全工作的纲领性文件，将为保障我国网络空间安全铸造一道“防火墙”。

战略提出，健全网络安全法律法规体系；加快对现行法律的修订和解释，使之适用于网络空间；加快构建法律规范、行政监管、行业自律、技术保障、公众

监督、社会教育相结合的网络治理体系；鼓励社会组织等参与网络治理；鼓励网民举报网络违法行为和不良信息。

同时，我国将采取包括经济、政治、科技、军事等一切措施，坚定不移地维护我国网络空间主权。加强网络反恐、反间谍、反窃密能力建设，严厉打击网络恐怖和网络间谍活动；严厉打击贩枪贩毒、传播淫秽色情、黑客攻击等违法犯罪行为。

>>网信办发布《国家网络空间安全战略》 提出捍卫网络空间主权等任务

>>《国家网络空间安全战略》全文

>>《国家网络空间安全战略》发布

最新政策：

>>中国发布《网络空间国际合作战略》

>>网络空间国际合作战略（全文）

抄送：校领导