网络信息安全周报

【2018】第 18 期

党委宣传部
信息网络中心 编　　2018 年 7 月 6 日

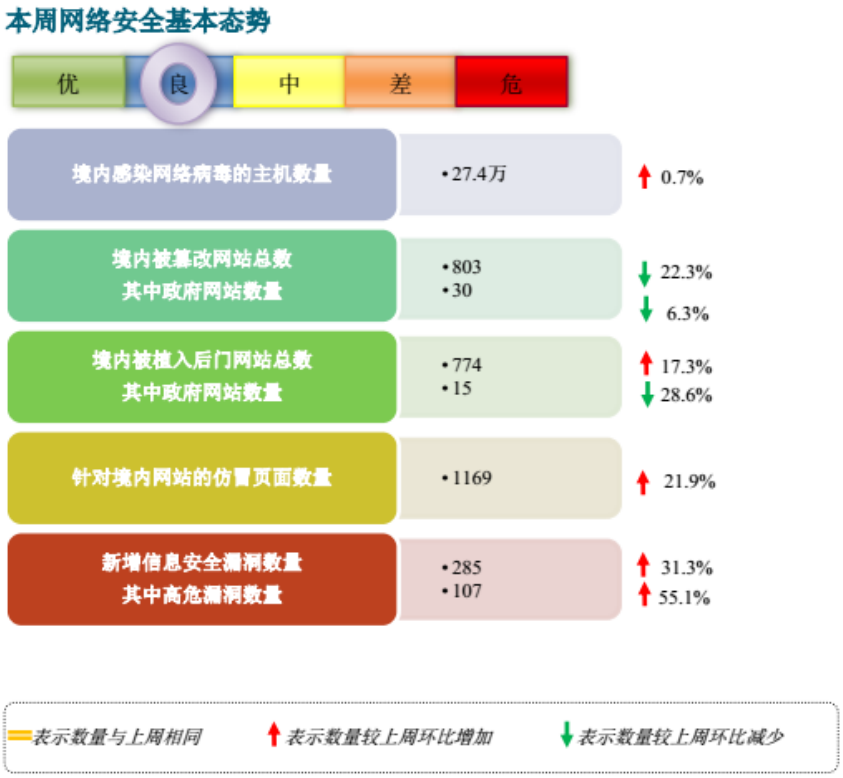
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 6 月 25 日—7 月 1 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 6 月 25 日—7 月 1 日)
- 【城院安全】网站群管理平台统计信息（2018 年 6 月 25 日—7 月 1 日）
- 【网络教育】《关于规范党员干部网络行为的意见》

全国网络安全信息与动态

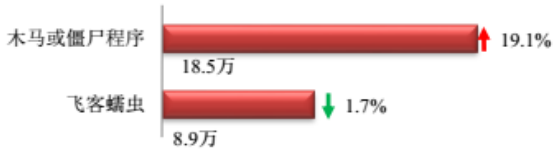
（2018 年 6 月 25 日—7 月 1 日）

根据国家互联网应急中心最新公告数据：



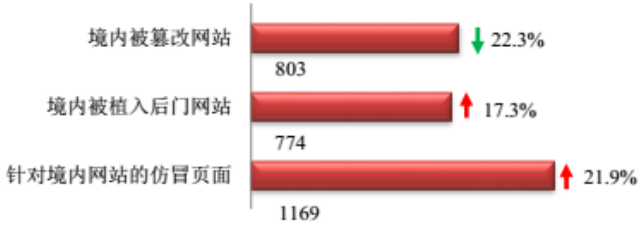
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.9 万。



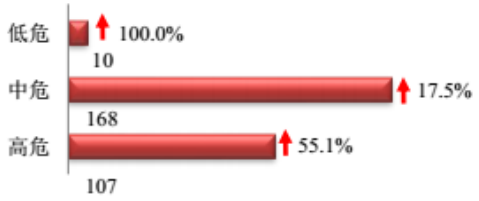
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 803 个；境内被植入后门的网站数量为 774 个；针对境内网站的仿冒页面数量为 1169。



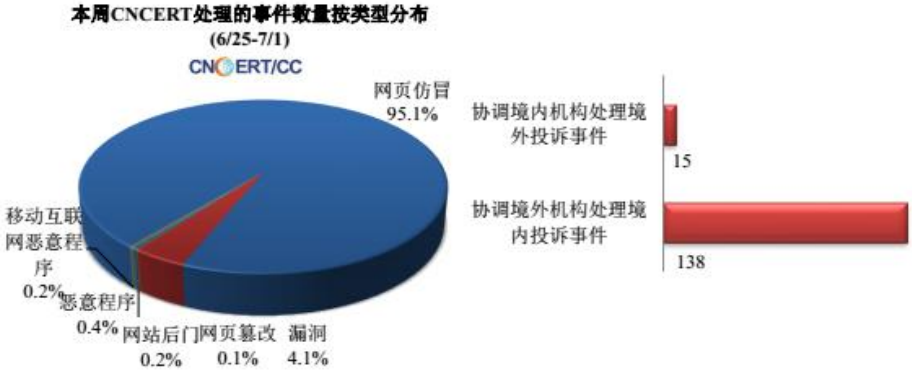
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 285 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

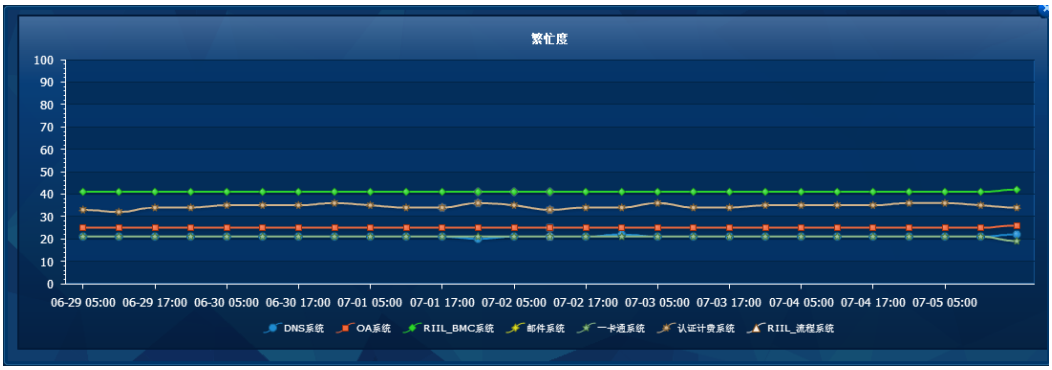
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1072 起，其中跨境网络安全事件 153 起。



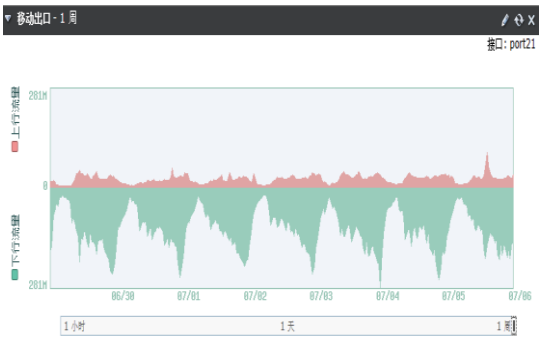
城院 IT 综合业务管理平台统计信息

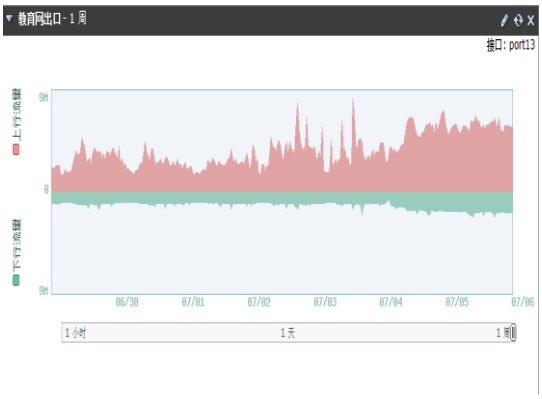
(2018 年 6 月 25 日—7 月 1 日)

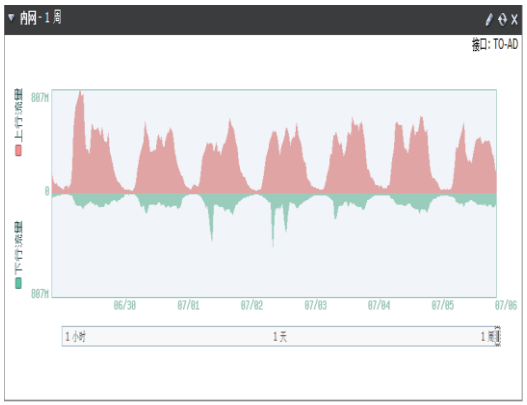
主要业务服务繁忙度



网络出口带宽情况统计





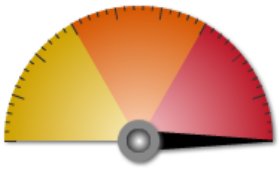


APT统计

防火墙统计	
恶意	58561
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	831727123

【城院安全】网站群管理平台统计信息（2018 年 6 月 25 日—7 月 1 日）

风险趋势

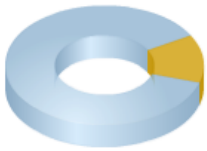


最近一周的全局风险等级为高，
在这段时间里共检测到 1210745 次攻击，其中低 60849 次，中 67801 次，高 1082095 次 ；
在以上统计中由**命令注入攻击、文件限制、头部字段限制**产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [**告警日志**] 。

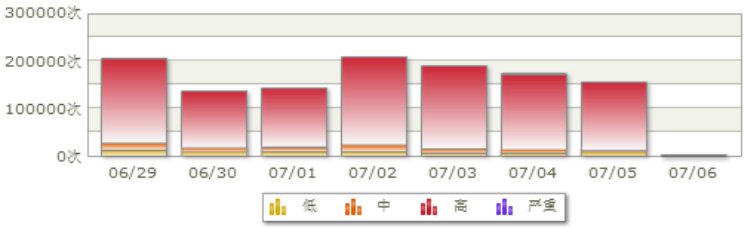
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

时间范围： 最近一周 ▼ 保护站点： 全局 ▼ 危险等级： 全部 ▼ 动作： 全部 ▼ 详细

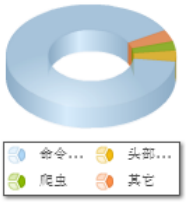
保护站点攻击次数对比



风险趋势图

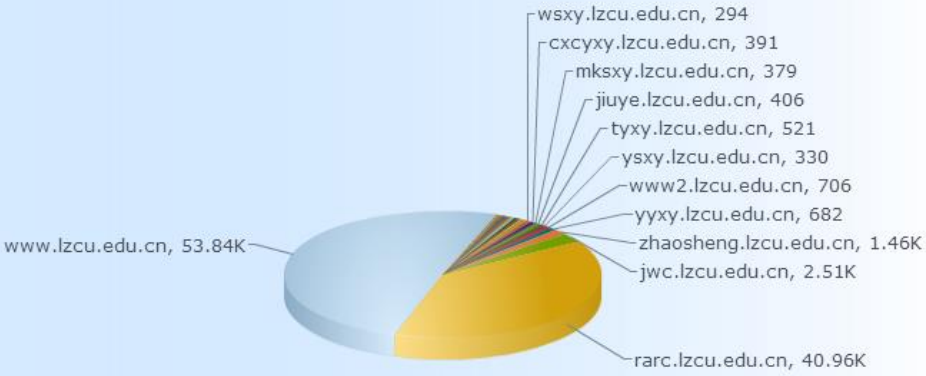


攻击类型统计(TOP)

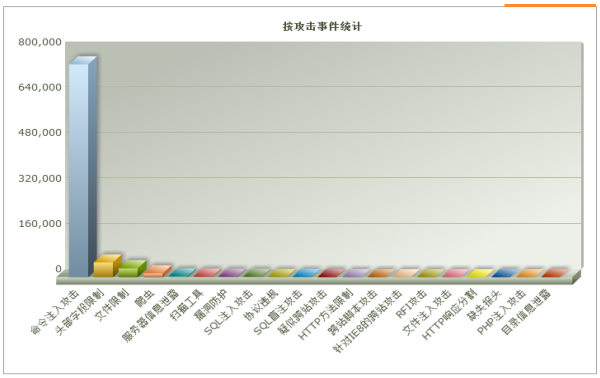


	全部 ↓	告警	阻断	重定向	放行
命令注入攻击	**1537615**	1537568	47	0	0
头部字段限制	**58539**	932	57607	0	0
爬虫	**52026**	51972	54	0	0
其它	63021	54363	8658	0	0

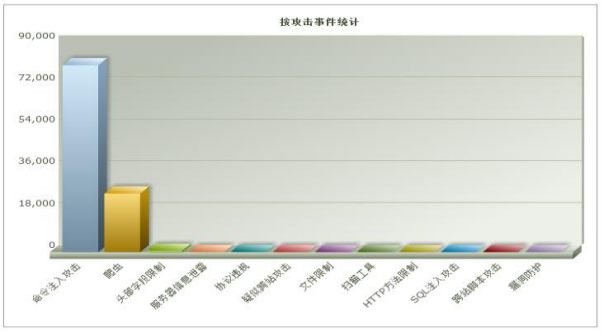
[被阻断]按告警主机名统计



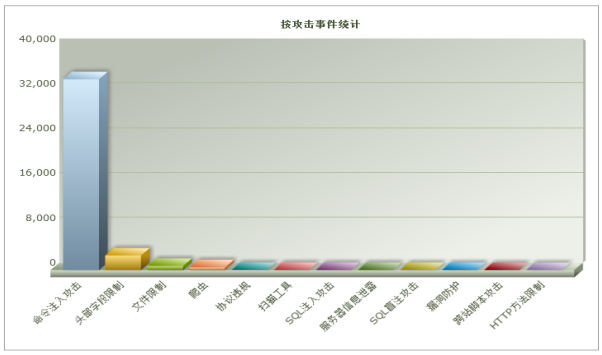
主机名	事件	统计
www.lzcu.edu.cn	头部字段限制	47924 次
	服务器信息泄露	2548 次
	扫描工具	1511 次
	SQL盲注攻击	582 次
	SQL注入攻击	415 次
	文件限制	273 次
	协议违规	210 次
	疑似跨站攻击	151 次
	HTTP方法限制	77 次
	漏洞防护	51 次
	跨站脚本攻击	46 次
	针对IE8的跨站攻击	31 次
	文件注入攻击	8 次
	命令注入攻击	6 次
	爬虫	5 次
	缺失报头	2 次
	目录信息泄露	1 次
	PHP注入攻击	1 次



www2.lzcu.edu.cn	头部字段限制	556 次
	服务器信息泄露	75 次
	疑似跨站攻击	29 次
	协议违规	26 次
	文件限制	7 次
	扫描工具	6 次
	HTTP方法限制	5 次
	跨站脚本攻击	1 次
	漏洞防护	1 次



jwc.lzcu.edu.cn	头部字段限制	2464 次
	扫描工具	12 次
	SQL盲注攻击	9 次
	服务器信息泄露	8 次
	漏洞防护	6 次
	文件限制	4 次
	协议违规	3 次
	跨站脚本攻击	2 次
	命令注入攻击	2 次
	HTTP方法限制	2 次



威胁	事件	统计
高	命令注入攻击	1247183 次
	文件限制	43261 次
	SQL注入攻击	7528 次
	SQL盲注攻击	6753 次
	LDAP注入攻击	2062 次
	漏洞防护	1998 次
	疑似跨站攻击	810 次
	HTTP方法限制	320 次
	跨站脚本攻击	147 次
	针对IE8的跨站攻击	145 次
	RFI攻击	21 次
	PHP注入攻击	10 次
	文件注入攻击	9 次
	HTTP响应分割	8 次
	缺失报头	3 次
	目录信息泄露	1 次
中	头部字段限制	58380 次
	协议违规	15554 次
	服务器信息泄露	3734 次
低	爬虫	43491 次
	协议违规	8794 次
	头部字段限制	4907 次
	扫描工具	4030 次
	畸形请求	30 次
	缺失报头	10 次

网站群管理平台网页更新情况统计

信息技术教育与应用研究所		城市社会心理研究中心	
机械工程学院		数学学院	2
化学与环境工程学院	7	路易艾黎研究中心	
职业技能鉴定所		党委宣传部	14
甘肃省民族音乐研究中心		体育学院	1
国际文化翻译学院		发展规划处	
地理与城乡规划学院		人事处	3
心理咨询中心		电子信息科学与技术研究所	
商学院	3	饮食服务中心	
甘肃省高等学校外语教学指导委员会		基本建设处	
学位办公室		国有资产管理处	
招生网		党委（校长）办公室	
幼儿师范学院	2	教育学院	
机关党委		创新创业学院	
传媒学院	2	卡务中心	
城市信息与系统科学研究所		电子与信息工程学院	
审计		党委学生工作部	4
文史学院	2	甘肃文化翻译中心	
马克思主义学院	3	财务处	
甘肃张芝书法院		后勤管理处	
国际交流处		档案馆	
科学研究处		教务处	5
信息网络中心	1	外国语学院	
兰州城市学院校医院		教学质量监测与评估中心	1
兰州城市学院	38	党委组织部	
音乐学院	2	旅游学院	
就业服务网	5	教师发展中心	2
美术与设计学院		团委	
保卫处		实训中心	
学报编辑部	1	石油工程学院	
		廉政网	

网站群管理平台应用防火墙入侵防护记录

管理平台	10.0.120.189	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	xcb0nly	错误帐号或密码	2018-06-29 17:46:12
管理平台	10.0.120.189	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	xcb0nly	错误帐号或密码	2018-06-29 17:45:36
管理平台	10.0.65.253	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	nks	错误帐号或密码	2018-06-29 10:51:22
管理平台	117.157.64.181	中国 移动	登录位置：网站管理；登录账号：	jyfw	错误帐号或密码	2018-06-28 17:50:05
管理平台	10.0.124.83	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	hjgc	错误帐号或密码	2018-06-28 15:38:57
管理平台	10.0.24.229	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	gswhfy	错误帐号或密码	2018-06-28 12:23:32
管理平台	10.0.24.229	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	gswhfy	错误帐号或密码	2018-06-28 12:23:03
管理平台	10.0.24.229	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	gswhfy	错误帐号或密码	2018-06-28 12:20:38
站点名称：路易艾黎研究中心	36.110.42.168	浙江省 电信	含有非法请求参数：	-1; waitfor delay '0:0:6' --	尝试SQL注入	2018-06-28 04:08:01
站点名称：路易艾黎研究中心	36.110.42.168	浙江省 电信	含有非法请求参数：	(select(0)from(select(sleep(6)))v)/*'+(select(0)from(selec...	尝试SQL注入	2018-06-28 04:08:01
站点名称：路易艾黎研究中心	36.110.42.168	浙江省 电信	含有非法请求参数：	if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sl...	尝试SQL注入	2018-06-28 04:08:01
管理平台	203.186.123.61	香港 城市电讯有限公司	登录位置：站群管理；登录账号：	admin	错误帐号或密码	2018-06-27 23:43:37
管理平台	10.0.66.3	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	jwc_zhk	错误帐号或密码	2018-06-26 16:13:51
管理平台	10.0.66.3	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	jwc_zhk	错误帐号或密码	2018-06-26 16:13:26
管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	rsc	错误帐号或密码	2018-06-25 16:04:58
管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	rsc	错误帐号或密码	2018-06-25 16:04:24
管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	rsc	错误帐号或密码	2018-06-25 16:03:35
管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	rsc	错误帐号或密码	2018-06-25 16:03:23
管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理；登录账号：	rsc	错误帐号或密码	2018-06-25 16:02:50

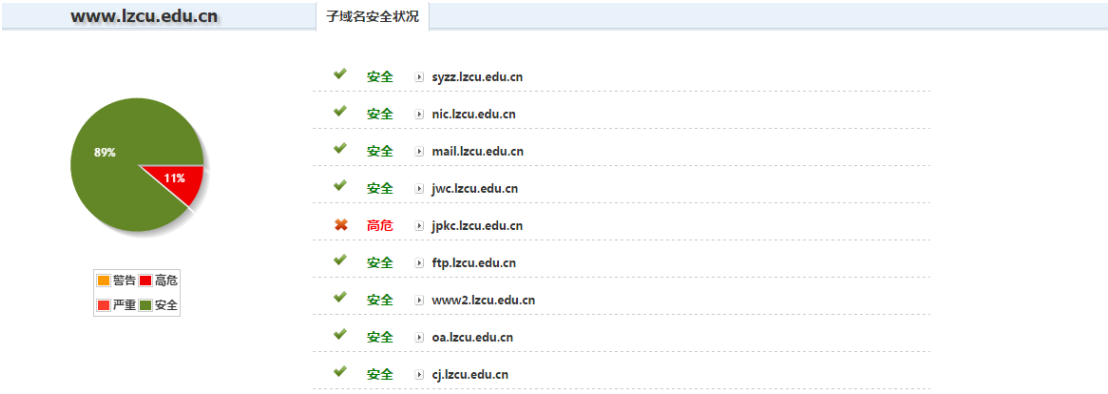
网站群管理平台应用防火墙网站访问 IP 封禁记录

封禁IP	封禁IP归属地	封禁开始时间▼	封禁结束时间
36.110.42.168	浙江省 电信	2018-06-28 04:08:01	2018-06-28 14:08:01

网站群管理平台 6 月份网站累计访问次数

站点名称	访问次数
兰州城市学院	148387
教务处	14675
就业服务网	6556
教育学院	5568
文史学院	4193
教育学院	4054
化学与环境工程学院	3924
音乐学院	3690
电子与信息工程学院	3556
地理与城乡规划学院	3341
外国语学院	3237
人事处	3128
机械工程学院	3001
幼儿师范学院	2851
石油工程学院	2795
旅游学院	2758
数学学院	2659
传媒学院	2447
体育学院	2295
马克思主义学院	2294
美术与设计学院	2281
财务处	2245
商学院	2176
国际交流处	1310
党委学生工作部	1116
科学研究处	1042
创新创业学院	820
路易艾黎研究中心	810
国际文化翻译学院	808
学位办公室	723
教学质量监测与评估中心（新）	656
廉政网	601
教师发展中心	593
国有资产管理处	554
保卫处	498
后勤管理处	497
党委宣传部	473
学校办公室	456
基本建设处	442
饮食服务中心	442
党委组织部	424
兰州城市学院校医院	416
团委	322
卡务中心	256
信息网络中心	245
甘肃文化翻译中心	236
审计	231
心理咨询中心	198
发展规划处	186
学报编辑部	139
城市社会心理研究中心（新）	134
甘肃省民族音乐研究中心	92
电子信息科学与技术研究所	73
甘肃张芝书法院	51
信息技术教育与应用研究所	46
城市信息与系统科学研究所	42
职业技能鉴定所	28
机关党委	20
甘肃省高等学校外语教学指导委员会	13
实训中心	7

网站安全检测一（360 网站安全检测）



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	2	492.42 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	489.42 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	363.84 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	549.07 ms	100 %	详情

异常发生时间	监控对象	监控类型	当前状态	事件信息	持续时间
2018-05-25 00:29:35	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时3分钟
2018-05-25 00:29:34	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时1分钟
2018-05-25 00:25:35	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时4分钟
2018-05-25 00:17:00	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时19分钟
2018-05-23 11:59:25	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时36分钟
2018-05-23 11:59:25	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时31分钟
2018-05-23 11:49:10	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时48分钟
2018-05-23 11:49:10	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时48分钟
2018-05-10 13:55:48	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	7分钟
2018-05-10 13:52:13	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	11分钟

网站安全检测二（百度云观测）

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	90 良好	查看详情>>
dwxcb.lzcu.edu.cn	34 高危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jiuye.lzcu.edu.cn	49 中危	查看详情>>
jpkc2.lzcu.edu.cn	49 中危	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jwc.lzcu.edu.cn	19 高危	查看详情>>
kyc.lzcu.edu.cn	19 高危	查看详情>>

域名	指数评价	操作
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>>
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	0 高危	查看详情>>
smtp.lzcu.edu.cn	15 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>>

【网络安全】《关于规范党员干部网络行为的意见》

中共中央宣传部、中共中央组织部、中央网信办联合印发

《关于规范党员干部网络行为的意见》

关于规范党员干部网络行为的意见

网络行为是党员干部言行的重要组成部分。党员干部要发挥模范带头作用，走好网上群众路线，规范网络行为，促进形成健康向上、风清气正的网络环境。

一、党员干部在网络上要严守政治纪律和政治规矩。必须牢固树立政治意识、大局意识、核心意识、看齐意识，坚决维护党中央权威，在思想上政治上行动上始终同以习近平同志为核心的党中央保持高度一致。严格遵守党规党纪，模范遵守国家法律法规，在网络行为中坚持正确政治方向，自觉宣传党的理论和路线方针政策，积极践行社会主义核心价值观，传播正能量、弘扬主旋律，共筑网上网下同心圆。

二、党员干部不准参与以下网络传播行为：发表违背党的基本路线，否定四项基本原则，歪曲党的政策，或者其他有严重政治问题的文章、演说、宣言、声明等；妄议中央大政方针，破坏党的集中统一；丑化党和国家形象，诋毁、污蔑党和国家领导人，歪曲党史、国史、军史，抹黑革命先烈和英雄模范；制造、传播各类谣言特别是政治类谣言，散布所谓“内部”消息和小道消息；出版、购买、传播非法出版物；宣扬封建迷信、淫秽色情；制作、传播其他有严重问题的文章、言论、音视频等信息内容。

三、党员干部不得参加以下网络活动：组织、参加反对党的理论和路线方针政策的网络论坛、群组、直播等活动；通过网络组党结社，参与和动员不法串联、联署、集会等网上非法组织、非法活动；参与网上宗教活动、邪教活动，纵容和支持宗教极端势力、民族分裂势力、暴力恐怖势力及其活动；利用网络泄露党和国家秘密；浏览、访问非法和反动网站等。

四、严格规范党员干部在网络平台以职务身份注册账号行为。党员干部以职务身份在微博、微信、网络直播、论坛社区等境内外网络平台上注册账号、建立群组的，**应当向所在党组织报告。**

五、党员干部应当履行举报监督的义务。发现网上违法违规违纪信息、活动的，及时主动向有关部门、网络平台等举报，积极提供线索，协助有关方面处置。

六、切实加强对党员干部网络行为的教育、引导和管理。各级党组织要认真贯彻落实《党委（党组）意识形态工作责任制实施办法》以及《党委（党组）网络意识形态工作责任制实施细则》。对在网络活动中以身作则、表现突出的党员干部，要充分肯定、热情鼓励；对坚持正确立场、传播正能量而遭到围攻的党员干部，要旗帜鲜明地给予保护和支持；**对党员干部违反本意见规定的，要依据党纪和国家法规进行严肃查处。**

抄送：校领导