网络信息安全周报

【2018】第 21 期

党委宣传部
信息网络中心 编

2018 年 9 月 27 日

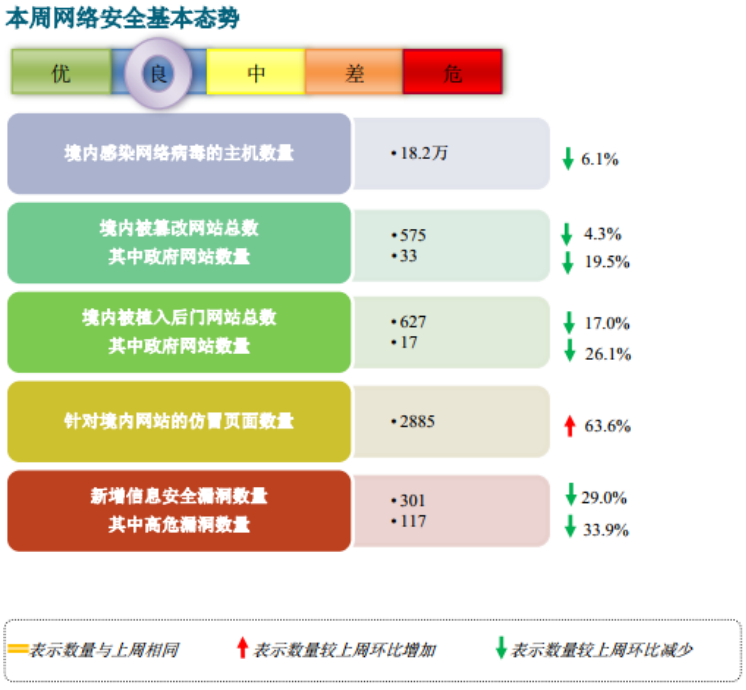
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 9 月 10 日—9 月 16 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 9 月 17 日—9 月 23 日)
- 【城院安全】网站群管理平台统计信息（2018 年 9 月 17 日—9 月 23 日）
- 【网络安全】简单高效的信息安全策略

全国网络安全信息与动态

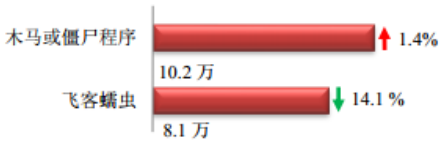
（2018 年 9 月 10 日—9 月 16 日）

根据国家互联网应急中心最新公告数据：



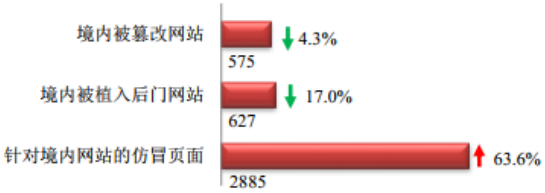
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 18.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.2 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。



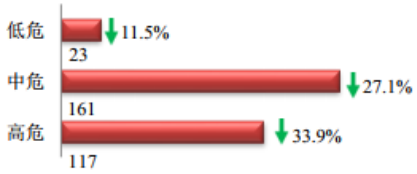
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 575 个；境内被植入后门的网站数量为 627 个；针对境内网站的仿冒页面数量为 2885。



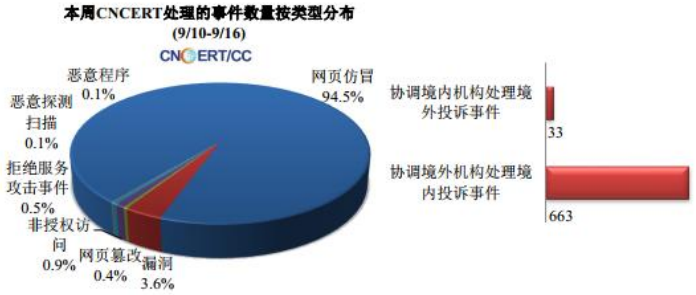
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 301 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 1358 起，其中跨境网络安全事件 696 起。

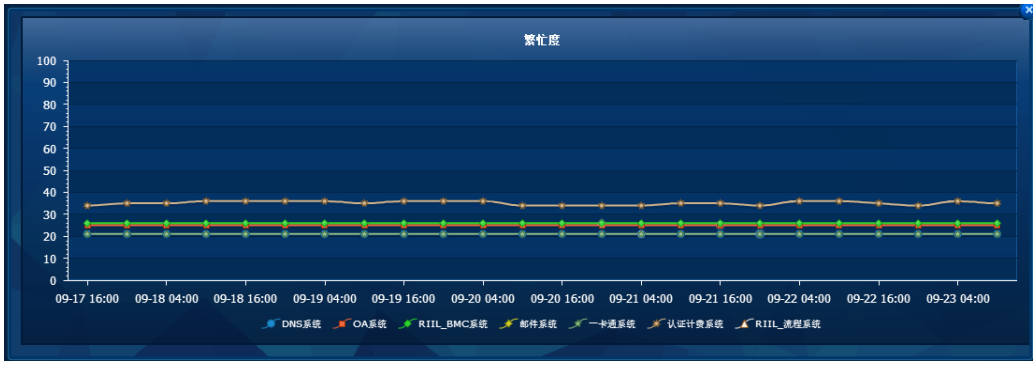


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1276 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1276 起。

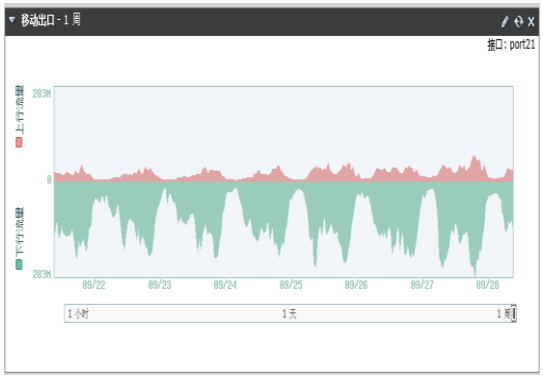
城院 IT 综合业务管理平台统计信息

(2018 年 9 月 17 日—9 月 23 日)

主要业务服务繁忙度



网络出口带宽情况统计

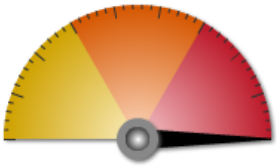


APT统计

防火墙统计	
恶意	115946
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	436197287

【城院安全】网站群管理平台统计信息（2018 年 9 月 17 日—9 月 23 日）

风险趋势

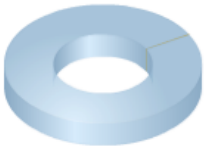


最近一周的全局风险等级为高，
在这段时间里共检测到 443582 次攻击，其中低 72715 次，中 88216 次，高 282651 次 ；在以上统计中由**协议违规、文件限制、SQL注入攻击**产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [**告警日志**] 。

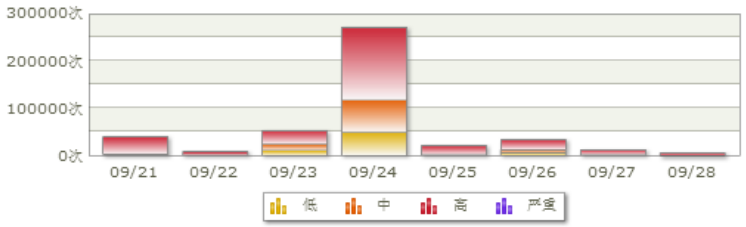
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

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



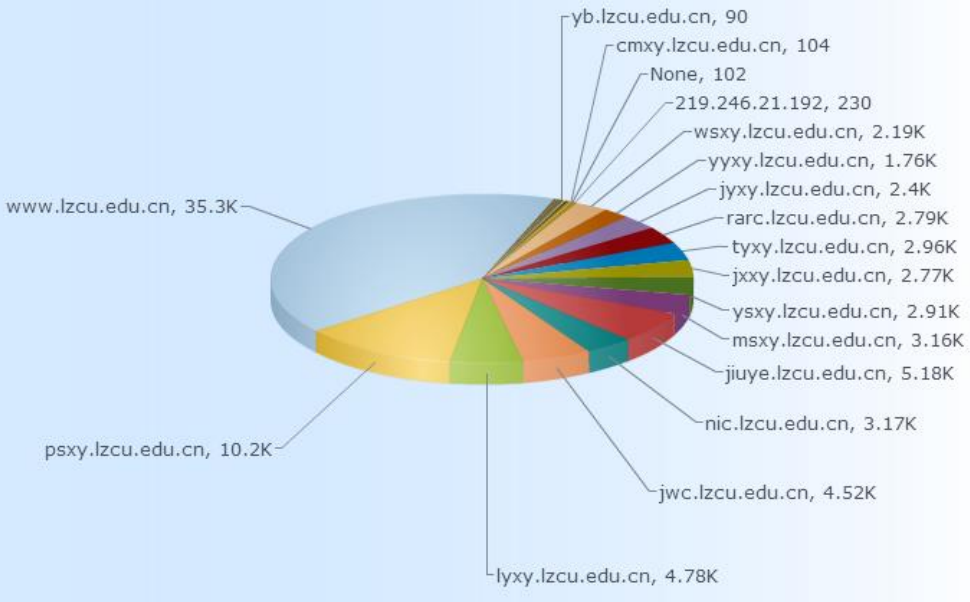
风险趋势图



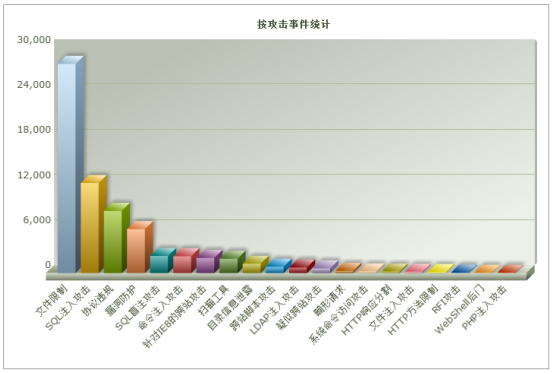
攻击类型统计(TOP)

	全部 ↓	告警	阻断	重定向	放行
协议违规	**144571**	5055	139516	0	0
文件限制	**74523**	42053	32470	0	0
SQL注入攻击	**72869**	5257	67612	0	0
其它	151624	21721	129903	0	0

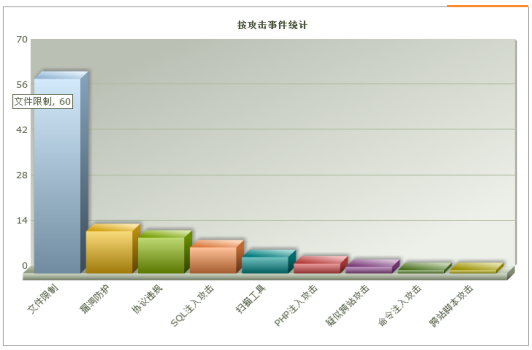
[被阻断]按告警主机名统计



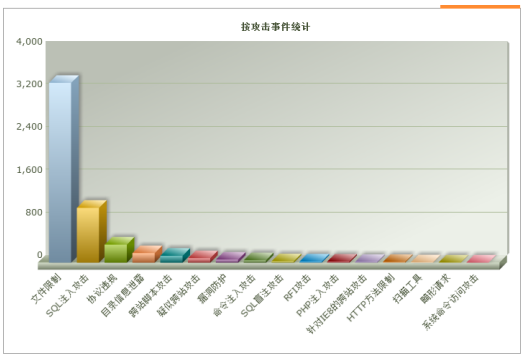
事件	主机名	统计
文件限制	www.lzcu.edu.cn	27795 次
SQL注入攻击	www.lzcu.edu.cn	11960 次
协议违规	www.lzcu.edu.cn	8263 次
漏洞防护	www.lzcu.edu.cn	5827 次
SQL盲注攻击	www.lzcu.edu.cn	2258 次
命令注入攻击	www.lzcu.edu.cn	2228 次
针对IE8的跨站攻击	www.lzcu.edu.cn	1993 次
扫描工具	www.lzcu.edu.cn	1897 次
目录信息泄露	www.lzcu.edu.cn	1232 次
跨站脚本攻击	www.lzcu.edu.cn	843 次
LDAP注入攻击	www.lzcu.edu.cn	743 次
疑似跨站攻击	www.lzcu.edu.cn	621 次
畸形请求	www.lzcu.edu.cn	286 次
系统命令访问攻击	www.lzcu.edu.cn	209 次
HTTP响应分割	www.lzcu.edu.cn	202 次
文件注入攻击	www.lzcu.edu.cn	180 次
HTTP方法限制	www.lzcu.edu.cn	135 次
RFI攻击	www.lzcu.edu.cn	59 次
WebShell后门	www.lzcu.edu.cn	48 次
PHP注入攻击	www.lzcu.edu.cn	41 次



事件	主机名	统计
文件限制	www2.lzcu.edu.cn	60 次
漏洞防护	www2.lzcu.edu.cn	13 次
协议违规	www2.lzcu.edu.cn	11 次
SQL注入攻击	www2.lzcu.edu.cn	8 次
扫描工具	www2.lzcu.edu.cn	5 次
PHP注入攻击	www2.lzcu.edu.cn	3 次
疑似跨站攻击	www2.lzcu.edu.cn	2 次
命令注入攻击	www2.lzcu.edu.cn	1 次
跨站脚本攻击	www2.lzcu.edu.cn	1 次



事件	主机名	统计
文件限制	jwc.lzcu.edu.cn	3360 次
SQL注入攻击	jwc.lzcu.edu.cn	1024 次
协议违规	jwc.lzcu.edu.cn	337 次
目录信息泄露	jwc.lzcu.edu.cn	176 次
跨站脚本攻击	jwc.lzcu.edu.cn	130 次
疑似跨站攻击	jwc.lzcu.edu.cn	83 次
漏洞防护	jwc.lzcu.edu.cn	56 次
命令注入攻击	jwc.lzcu.edu.cn	45 次
SQL盲注攻击	jwc.lzcu.edu.cn	26 次
RFI攻击	jwc.lzcu.edu.cn	22 次
PHP注入攻击	jwc.lzcu.edu.cn	19 次
针对IE8的跨站攻击	jwc.lzcu.edu.cn	14 次
HTTP方法限制	jwc.lzcu.edu.cn	13 次
扫描工具	jwc.lzcu.edu.cn	7 次
畸形请求	jwc.lzcu.edu.cn	3 次
系统命令访问攻击	jwc.lzcu.edu.cn	1 次



威胁	事件	统计
高	文件限制	69400 次
	SQL注入攻击	28594 次
	漏洞防护	7227 次
	目录信息泄露	3277 次
	命令注入攻击	2756 次
	SQL盲注攻击	2676 次
	针对IE8的跨站攻击	2218 次
	跨站脚本攻击	1605 次
	疑似跨站攻击	881 次
	LDAP注入攻击	701 次
	RFI攻击	346 次
	HTTP方法限制	288 次
	系统命令访问攻击	213 次
	HTTP响应分割	210 次
	文件注入攻击	180 次
	PHP注入攻击	101 次
	WebShell后门	48 次
低	协议违规	7446 次
	扫描工具	2181 次
	畸形请求	340 次
	漏洞防护	4 次
中	协议违规	4714 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	2
机械工程学院	8
化学与环境工程学院	13
职业技能鉴定所	
甘肃省民族音乐研究中心	
国际文化翻译学院	18
地理与城乡规划学院	9
心理咨询中心	
商学院	7
甘肃省高等学校外语教学指导委员会	
研究生处	
招生网	
幼儿师范学院	4
机关党委	
传媒学院	4
城市信息与系统科学研究所	
审计	
文史学院	5
马克思主义学院	8
甘肃张芝书法院	
国际交流处	1
科学技术处（社会科学处）	4
信息网络中心	3
兰州城市学院校医院	
兰州城市学院	26
音乐学院	4
就业服务网	23
美术与设计学院	4
保卫处（武装部）	
学报编辑部	

城市社会心理研究中心	
数学学院	3
路易艾黎研究中心	
党委宣传部（新闻中心）	18
体育学院	3
发展规划与合作交流处	2
党委教师工作部（人事处）	
电子信息科学与技术研究所	
饮食服务中心	
基本建设处	
实验设备与国有资产管理处	
学校办公室（校友会办公室）	1
教育学院	
创新创业学院	4
卡务中心	
电子与信息工程学院	9
党委学生工作部（学生工作处）	
甘肃文化翻译中心	
财务处	
后勤管理处	
档案馆	
教务处	
外国语学院	8
教学质量监测与评估中心	10
党委组织部（党委统战部、党校、机关党委）	
旅游学院	7
教师发展中心	
团委	1
实训中心	
石油工程学院	4
廉政网	3

网站群管理平台应用防火墙入侵防护记录

站点名称：机关党委	110.87.188.33	福建省福州市 电信	含有非法请求参数：-1));select pg_sleep(9); --	尝试SQL注入	2018-09-23 22:08:57
站点名称：机关党委	110.87.188.33	福建省福州市 电信	含有非法请求参数：-1);select pg_sleep(9); --	尝试SQL注入	2018-09-23 22:08:57
站点名称：机关党委	110.87.188.33	福建省福州市 电信	含有非法请求参数：-1;select pg_sleep(9); --	尝试SQL注入	2018-09-23 22:08:57
站点名称：兰州城市学院	42.94.192.32	甘肃省酒泉市 电信	含有非法请求参数：'+convert(int,CHAR(65)+CHAR(90)+CHAR(87)+CHAR(84)+CHAR(83)...	尝试SQL注入	2018-09-21 11:08:31
站点名称：兰州城市学院	42.94.192.32	甘肃省酒泉市 电信	含有非法请求参数：'+convert(int,CHAR(120)+CHAR(73)+CHAR(77)+CHAR(55)+CHAR(85...	尝试SQL注入	2018-09-21 11:08:31
站点名称：兰州城市学院	42.94.192.32	甘肃省酒泉市 电信	含有非法请求参数：'+convert(int,CHAR(65)+CHAR(115)+CHAR(70)+CHAR(101)+CHAR(1...	尝试SQL注入	2018-09-21 11:08:29
站点名称：兰州城市学院	42.94.192.32	甘肃省酒泉市 电信	含有非法请求参数：'+convert(int,CHAR(54)+CHAR(112)+CHAR(52)+CHAR(48)+CHAR(53...	尝试SQL注入	2018-09-21 11:08:29
管理平台	10.0.125.190	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：nicxnl	错误帐号或密码	2018-09-20 11:01:02
管理平台	10.0.125.190	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：nicxnl	错误帐号或密码	2018-09-20 11:00:29
管理平台	10.0.32.38	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：cxgh	错误帐号或密码	2018-09-20 09:45:04
管理平台	10.0.116.40	□□〈	登录位置：网站管理；登录账号：xcbzf	错误帐号或密码	2018-09-20 09:05:43
管理平台	42.91.1.178	甘肃省兰州市 电信	登录位置：网站管理；登录账号：lyxy	错误帐号或密码	2018-09-19 20:51:58
管理平台	42.91.1.178	甘肃省兰州市 电信	登录位置：网站管理；登录账号：lyxy	错误帐号或密码	2018-09-19 20:50:28
站点名称：信息网络中心	220.191.231.98	浙江省金华市 电信电子政府网络	含有非法请求参数：select site_name from siteinfo union select 'testtest' fro...	尝试SQL注入	2018-09-19 17:01:39
管理平台	10.0.27.115	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：szxy	错误帐号或密码	2018-09-19 10:54:18
管理平台	10.0.112.214	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：jxgc	错误帐号或密码	2018-09-19 08:18:40
管理平台	10.0.125.190	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：nicxnl	错误帐号或密码	2018-09-18 14:48:11
管理平台	10.0.112.214	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：jxgc	错误帐号或密码	2018-09-18 13:42:00
管理平台	10.0.112.161	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：wgrxy	错误帐号或密码	2018-09-18 10:53:06
管理平台	10.0.112.161	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：wgrxy	错误帐号或密码	2018-09-18 10:52:56
管理平台	10.0.27.115	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：szxy	错误帐号或密码	2018-09-18 10:47:31
管理平台	10.0.27.115	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：szxy	错误帐号或密码	2018-09-18 09:09:05
站点名称：教育学院	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数：markiframeindex	尝试跨站脚本注入	2018-09-17 15:05:25
站点名称：教育学院	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数：markiframeindex	尝试跨站脚本注入	2018-09-17 15:05:24
站点名称：教育学院	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数：markiframeindex	尝试跨站脚本注入	2018-09-17 15:05:24
管理平台	10.0.50.34	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：dvbgs	错误帐号或密码	2018-09-17 15:01:23
管理平台	10.0.38.150	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：mks	错误帐号或密码	2018-09-17 15:00:15
管理平台	10.0.38.150	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：mks	错误帐号或密码	2018-09-17 14:59:25
管理平台	10.0.112.14	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：tw1	错误帐号或密码	2018-09-17 14:52:33
管理平台	10.4.27.150	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	2018-09-17 08:21:40

网站群管理平台应用防火墙网站访问 IP 封禁记录

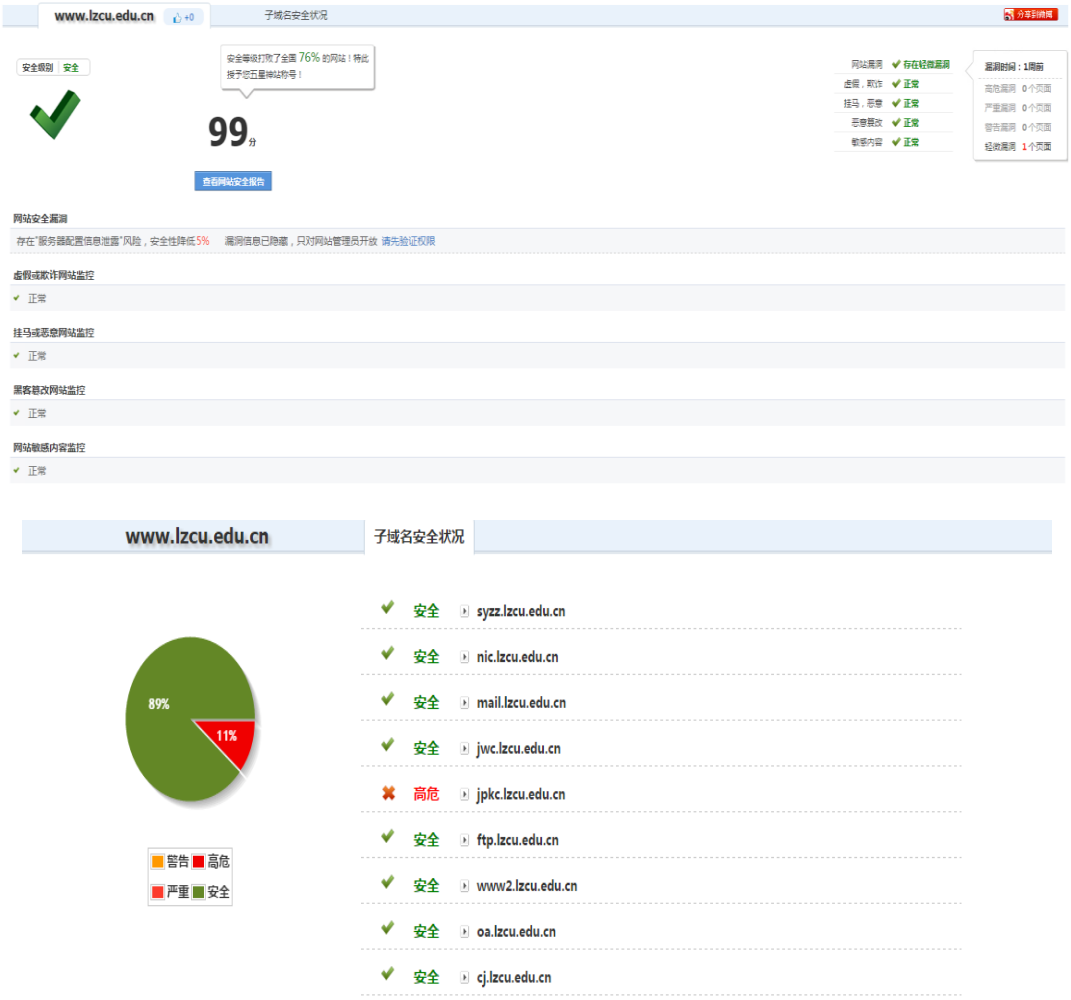
42.94.192.32	甘肃省酒泉市 电信	2018-09-21 11:08:31	2018-09-21 21:08:31	已自动解禁。
42.94.192.32	甘肃省酒泉市 电信	2018-09-21 11:08:31	2018-09-21 21:08:31	已自动解禁。
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2018-09-17 15:05:25	2018-09-18 01:05:25	已自动解禁。

网站群管理平台 9 月份网站累计访问次数

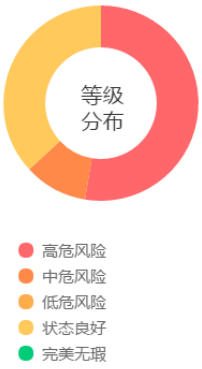
lcsxy	兰州城市学院	155330
jwc	教务处	16732
jyxy2	教育学院	6246
jyfww	就业服务网	6067
wgyxy	外国语学院	4665
sygcxy	石油工程学院	3398
dlyxsghxy	地理与城乡规划学院	3493
wsxy	文史学院	3091
hxyhjgcxy	化学与环境工程学院	2960
cwc	财务处	2755
plgcjsxy	电子与信息工程学院	2641
yyxx	音乐学院	2637
rsc	党委教师工作部（人事处）	2369
lyxy	旅游学院	2198
gjwhfy	国际文化翻译学院	2142
yeafxy	幼儿师范学院	1973
jxxy	机械工程学院	1931
lmsysjxy	美术与设计学院	1843
lmkszyxy	马克思主义学院	1759
sxxy	数学学院	1730
cxcyxy	创新创业学院	1476
cmxy	传媒学院	1470
sxy	商学院	1408
tyxy	体育学院	1311
xxwlzx	信息网络中心	1278
xsc	党委学生工作部（学生工作处）	1189
xzbgs	学校办公室（校友会办公室）	1175
kxyjc	科学技术处（社会科学处）	1171
iec	国际交流处	1033
tw	团委	968
yzzl	教学质量监测与评估中心（弱）	966

yzzl	教学质量监测与评估中心（弱）	966
xlsyz	心理学虚拟仿真实验室	738
hqglc	后勤管理处	549
dwzzb	党委组织部（党委统战部、党校、机关党委	539
xwb	研究生处	469
kwzx	卡务中心	431
gswhfyzx	甘肃文化翻译中心	405
bwc	保卫处（武装部）	367
xjvr	小学教育虚拟仿真实验中心	362
lzw	重勘网	356
jsfzzx	教师发展中心（高等教育研究所）	335
gzc	实验设备与国有资产管理处	315
lyal	路易艾黎研究中心	286
sscc	饮食服务中心	215
xuebao	学报编辑部	210
jbjsc	基本建设处	196
lcsxyxlzxzx	心理咨询中心	172
lcsxyxyy	兰州城市学院校医院	151
fzghc	发展规划与合作交流处	147
xlyjsx	城市社会心理研究中心（弱）	120
dwxcb	党委宣传部（新闻中心）	100
sj	审计	82
zsxfy	甘肃张芝书法院	82
mzyy	甘肃省民族音乐研究中心	80
jyxy	教育学院	74
dzxxkxjsyja	电子信息科学与技术研究所	73
xxjsjy	信息技术教育与应用研究所	70
csxxytkyyja	城市信息与系统科学研究所	32
zyjnjds	职业技能鉴定所	30
jgdw	机关党委	21
gaodeng	甘肃省高等学校外语教学指导委员会	14
lndag	档案馆	1
sxzx	实训中心	1

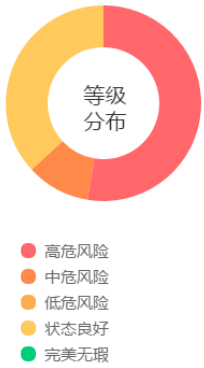
网站安全检测一（360 网站安全检测）



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	19 高危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jiuye.lzcu.edu.cn	19 高危	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	85.6 良好	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】简单高效的信息安全策略

信息安全工作的首要目标是确保高校核心业务系统与主要信息发布平台的正常运作

随着高校信息化建设的迅速发展，高校信息化建设已经渗透到日常学习、科研、管理、服务的方方面面。建设时期不可避免的重建设发展，轻运维安全，使得高校在信息系统安全方面基础薄弱。与此同时，高校还必须面对日益严峻的安全形势，面对来自各相关部门越来越高的安全工作要求，挑战与压力都是巨大的。在有限的人力物力和急迫的网络安全需求下，应对高校的信息安全工作设立清晰务实的工作目标，执行简明高效的安全措施。

信息安全措施无法做到绝对性的安全，一旦网站页面篡改事件真的发生，应第一时间阻断外界对网站页面的访问。可在各个层面做好“一键断网”的预案。

工作目标

确保核心业务系统与主要信息发布平台正常运作

高校师生的日常工作、学习、科研已经高度依赖于各业务信息系统与信息发布平台的正常运作，如果核心业务信息系统与主要信息发布平台停止运作，将导致高校日常工作的中断与信息不能传达的严重后果，同时信息安全工作也就失去了存在的意义，所以信息安全工作的首要目标是确保高校核心业务系统与主要信息发布平台的正常运作。

确保敏感业务数据不被窃取

教育相关的业务数据泄露曾造成过严重的后果，如 2016 年 8 月，山东省临沂市高考录取新生徐玉玉被不法分子冒充教育、财政部门工作人员诈骗 9900 元，并导致猝死。该案件中罪犯掌握的受害者大量个人信息正是黑客利用技术手段攻击了“山东省 2016 高考网上报

名信息系统”盗取并出售给诈骗团伙的。确保高校信息系统中的敏感业务数据不被滥用和窃取，是高校信息安全工作的重要目标。

确保展示度高的系统不被篡改内容

高校近年面临的一大安全挑战是面向公众的网站和各类应用系统迅速增多，黑客通过官方网站或应用系统界面达到非法目的，使得高校遭受巨大损失。近年某境外黑客组织更是以事业单位和高校的对外网站为主要篡改攻击对象，造成了一系列严重后果。确保高校网站和主要应用系统的用户界面不被非法篡改，是高校信息安全工作中不可或缺的一环。

总之，在保证网络安全的前提下尽可能保障师生的网络应用需求。

值得注意的是，各种信息网络安全措施的落实，不可避免会给高校师生的信息网络应用带来额外的不便。各种应用已经是师生工作生活中不可或缺的一部分，需要在保证信息网络安全的前提下尽可能地保障师生的网络应用需求。

几个关键点

Network-网络层面

在网络层面，需要注意的是：

1.在校园网中区隔用户网络和数据中心网络，并在数据中心网络中进一步实施业务分区；

2.策略性关闭校园网边界的部分端口，限制外网对校园网的 SSH/Telnet/Ftp 及常见远程控制端口；

3.设立高安全性、多因素认证的可信用户内网，构建特殊业务系统访问 VPN、堡垒机等通道；

4.在数据中心的边缘部署 IPS/IDS 与防火墙，对服务器网络执行比用户网络更高的网络安全策略；

5.由于极易通过无线监听与 MAC 伪造技术非法冒用身份登录，应逐步关闭基于 MAC 匹配的无线网无感知认证，采用安全性较高的 802.1x 接入认证。

IAAS-虚拟机层面

在网络层面，需要注意的是：

1.应在虚拟机层面利用虚拟网络的软件定义特性实施比数据中心边界更精细的网络访问控制策略来提高安全能力；

2.应在虚拟机层面部署比操作系统更底层的反病毒反恶意代码安全产品，实现高效的全局安全控制；

3.应充分利用虚拟机层面的资源，使用统计数据进行安全预警和判断。

OS-操作系统层面

在操作系统层面，需要注意的是：

1.应做好操作系统尤其是服务器操作系统的补丁控管策略，及时升级修补操作系统漏洞；

2.应减少操作系统多样性，尽量安装统一的操作系统，便于安全漏洞的统一管理，简化安全工作；

3.在操作系统层面应安装资源监控 Agent，及时发现资源的异常使用是发现信息安全威胁的重要手段；

4.在操作系统层面设置缺省部署的安全访问策略，遵循最小开放原则以最大化安全能力。

Web 网站层面

在网站系统层面，需要注意的是：

1.应执行网站最小开放规则，关闭所有可以关闭的网站 B/S 业务；

2.对必须对外开放的网站站点进行重点安全强化，包括但不限于静态化、防篡改、全新部署等手段；并最小化网站的可访问范围；

3.高校二级单位自主建设的网站安全能力参差不齐，网络地址分散各处，难以集中保护，存在极大的安全风险，也一直是黑客攻陷的重灾区，集中规范化建设的站群系统能极大地提升网站的安全性；

4.应对高校的主要网站做定期的主动漏洞扫描，并对其出入流量进行被动 IDS 分析，以及时发现安全风险。

重大保障期间的特别举措

重保期间指重大活动网络安保期间。高校由于其特殊性，在国家重大活动期间往往需要暂时性地特别提升信息网络安全的防御能力，需要执行一系列特别举措。包括：

重要服务器的重新部署

对重要服务器应该完全从操作系统开始重新部署，防止存在可能的历史黑客留下的潜在后门。对于高校而言，DNS 系统相关服务器、主页相关服务器属于重要的高危服务器，应酌情重新部署。可以使用例如 Ansible 这样的服务器部署工具进行批量系统配置、批量程序部署、批量运行命令，实现配置的标准化和自动化。

重要服务器的安全强化

对于重要服务器应进行安全策略的强化保护，使用漏洞扫描工具可以主动发现潜在的安全问题，采用站群模式部署可以有效提高二级单位网站的安全水平，采用网站静态化手段则可以最大化地减少安全风险。网站静态化的本质是简化与减少信息产生与传输的环节，减少被攻击的位点，非静态网站有 SQL 注入、权限绕过、XSS、CSRF 等安全风险。但是没有交互性并不等同于静态网站：引用了第三方图片、JS 脚本、类库、样式表等资源，第三方一旦被篡改将被连带篡改。彻底的静态化则对所有第三方内容均在可信源上下载到本地固化，甚至完全图片化。

应急预案

信息安全措施无法做到绝对性的安全，一旦网站页面篡改事件真的发生，应第一时间阻断外界对网站页面的访问。可在各个层面做好“一键断网”的预案。在操作系统层面，可以预制防火墙规则在需要时生效，或是直接进行系统关机操作；在 Web 服务器层面，可以设定访问某个开关页面关停 Web 服务；在虚拟机层面，可以关闭虚拟机网络或虚拟机本身；在实体机层面，可以直接拔出网线甚至电源；在数据中心网络边界，可以预制 WAF、IPS、FW 的阻断规则；在接入网络层面，可以在出口网关上预制 ACL 规则、在路由器拔出上联网线乃至电源。

这些手段分别适用于不同专业的工作人员，在应急值班期间可以因人施用，在不同层面第一时间阻断访问。

攻击溯源

在信息安全攻击事件发生后，为了给下一次工作积累经验，也为了固定证据，应当做好攻击溯源工作，相关的日志应当写入专门的远程日志服务器，并可使用虚拟机快照等手段对重要服务器做到分钟级别的远端备份以防止攻击者擦除攻击痕迹。

网站关闭的通知页面

对于一些存在安全隐患而被暂时性下线的网站，可使用应用交付设备或者将 DNS 导入到一个特定的通知页面，以最小化网站下线对用户带来的负面影响。为避免临时性替换网站页面内容导致搜索引擎删除原有网站信息，通知页面应当返回 503 HTTP 状态码，也可根据恢复时间指定 Retry-After 返回值。

重保时期的帮助站点与客户服务

重保时期执行的各种信息安全管理策略无可避免将影响用户使用体验，原有系统的帮助页面被基于最小开放原则关闭将极大地增加客服部门工作量，应针对重保时期的信息系统客服服务特点预先设计特殊时期的帮助站点与客户服务方案。

最小化不可控风险的负面影响

针对非主观措施可以防止的上级 DNS、CDN 篡改、甚至伪造页面截图的假攻击也应做好应对预案，如发现被攻击，应当及时下线，并执行检查，如果确定非自身因素则应当及时恢复上线，并在页面上显著位置公布以消除不良影响，在条件允许的情况下建立自动刷新页面的第三方录像存证。

抄送：校领导