网络信息安全周报

【2018】第 7 期

党委宣传部
信息网络中心 编

2018 年 4 月 19 日

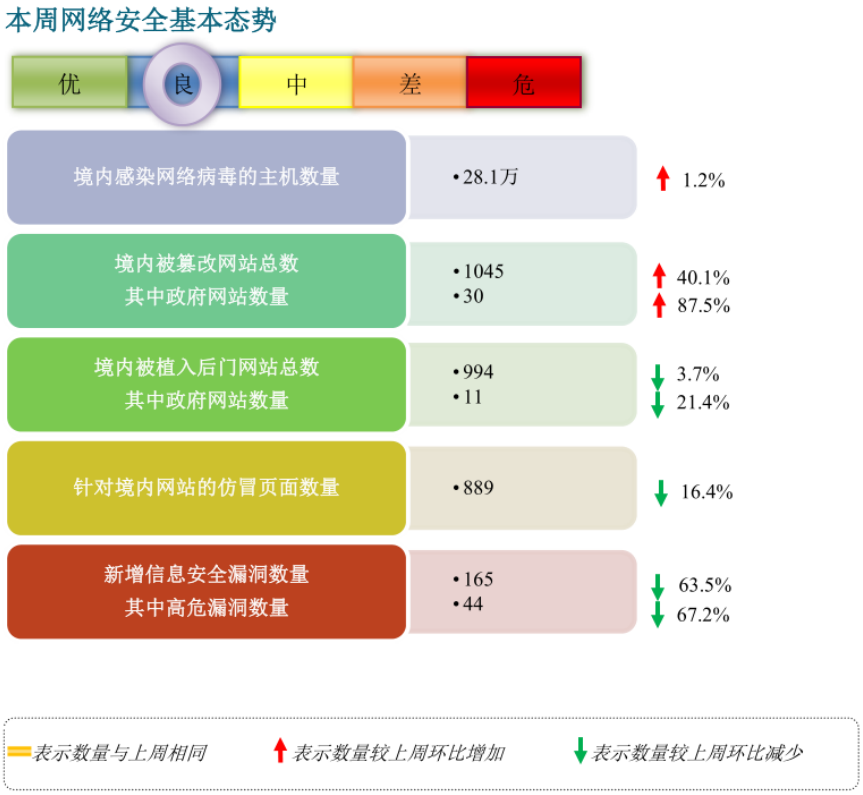
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 4 月 2 日—4 月 8 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 4 月 9 日—4 月 15 日)
- 【安全教育】网络安全保护意识更加全面 关键设施安全不容忽视
- 【安全术语】七大网络安全术语

全国网络安全信息与动态

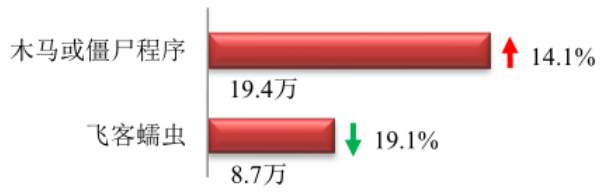
（2018 年 4 月 2 日—4 月 8 日）

根据国家互联网应急中心最新公告数据：



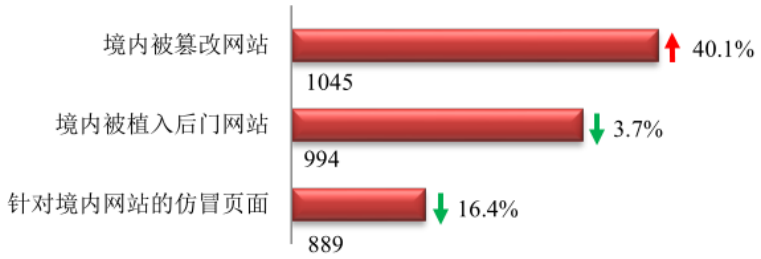
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 28.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.7 万。



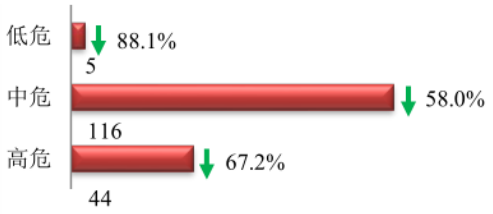
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1045 个；境内被植入后门的网站数量为 994 个；针对境内网站的仿冒页面数量为 889。



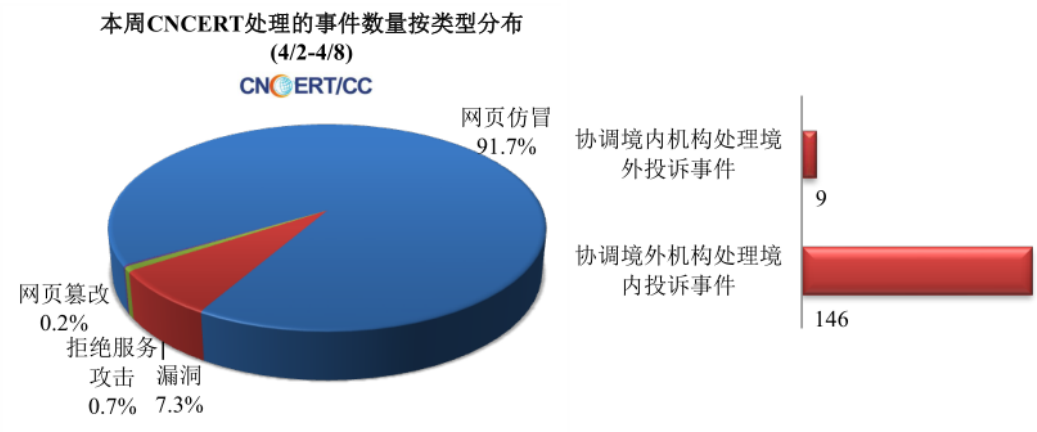
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 165 个，信息安全漏洞威胁整体评价级别为高。



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 424 起，其中跨境网络安全事件 155 起。



城院 IT 综合业务管理平台统计信息

(2018 年 4 月 9 日—4 月 15 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	合计		站点名称	合计
就业服务网	25		化学与环境工程学院	
兰州城市学院	5		机关党委	
马克思主义学院	5		机械工程学院	
甘肃省民族音乐研究中心	4		基本建设处	
国有资产管理处	4		教师发展中心	
旅游学院	4		教务处	
廉政网	3		教学质量监测与评估中心	
电子与信息工程学院	2		卡务中心	
教育学院	2		兰州城市学院校医院	
科学研究处	2		美术与设计学院	
路易艾黎研究中心	1		人事处	
保卫处			膳食处	
财务处			商学院	
财务处旧			审计	
城市社会心理研究中心			石油工程学院	
城市信息与系统科学研究所			实训中心	
传媒学院			数学学院	
创新创业学院			体育学院	
档案馆			团委	
党委（校长）办公室			外国语学院	
党委宣传部			网络报修	
党委学生工作部			文史学院	
党委组织部			心理咨询中心	
地理与城乡规划学院			信息技术教育与应用研究所	
电子信息科学与技术研究所			信息网络中心	
发展规划处			学位办公室	
甘肃省高等学校外语教学指导委员会			音乐学院	
甘肃文化翻译中心			音乐研究中心	
甘肃张芝书法院			幼儿师范学院	
国际交流处			招生网	
后勤管理处			职业技能鉴定所	

站群系统应用防火墙入侵防护记录

序号	入侵位置	入侵者IP	归属地	详细信息	入侵方式	入侵时间
191731	站点名称：教务处	60.205.212.155	广东省深圳市 英达通信	含有非法请求参数	SQL注入	2018-04-15 04:17:55
191730	站点名称：教务处	60.205.212.155	广东省深圳市 英达通信	含有非法请求参数	SQL注入	2018-04-15 04:17:36
191729	站点名称：教务处	60.205.212.155	广东省深圳市 英达通信	含有非法请求参数	SQL注入	2018-04-15 04:15:44
191728	站点名称：兰州城市学院	60.205.212.155	广东省深圳市 英达通信	含有非法请求参数	SQL注入	2018-04-15 04:09:18
191727	站点名称：兰州城市学院	60.205.212.155	广东省深圳市 英达通信	含有非法请求参数	SQL注入	2018-04-15 04:08:03
191726	站点名称：就业服务网	185.92.73.172	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-15 03:41:44
191725	站点名称：就业服务网	185.92.73.172	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-15 03:41:44
191724	站点名称：就业服务网	185.92.73.172	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-15 03:41:42
191723	站点名称：石油工程学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-12 23:06:30
191722	站点名称：石油工程学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-12 23:06:29
191721	站点名称：石油工程学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-12 23:06:29
191720	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-04-12 02:30:04
191719	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-04-12 02:29:52
191718	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-04-12 02:27:42
191717	站点名称：团委	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-12 02:13:45
191716	站点名称：团委	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-12 02:13:45
191715	站点名称：团委	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-12 02:13:45
191714	管理平台	10.0.65.52	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：lzw	错误帐号或密码	2018-04-11 09:10:02
191713	站点名称：数学学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-10 10:28:49
191712	站点名称：数学学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-10 10:28:49
191711	站点名称：数学学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-10 10:28:48
191710	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 18:30:27
191709	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 18:28:08
191708	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 18:07:03
191707	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 16:24:50
191706	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 16:22:30
191705	站点名称：兰州城市学院	220.181.55.143	北京市 奇虎公司电信互联网数据中心CDN节点	含有非法请求参数	SQL注入	2018-04-09 16:01:09
191704	站点名称：外国语学院	134.73.216.20	北美地区	含有非法请求参数	SQL注入	2018-04-09 14:20:10
191703	站点名称：外国语学院	134.73.216.20	北美地区	含有非法请求参数	SQL注入	2018-04-09 14:20:09
191702	站点名称：外国语学院	134.73.216.20	北美地区	含有非法请求参数	SQL注入	2018-04-09 14:20:09
191701	站点名称：兰州城市学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-09 13:06:45
191700	站点名称：兰州城市学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-09 13:06:44
191699	站点名称：兰州城市学院	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-09 13:06:44
191698	管理平台	10.0.91.70	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：wsxy	错误帐号或密码	2018-04-09 10:46:21

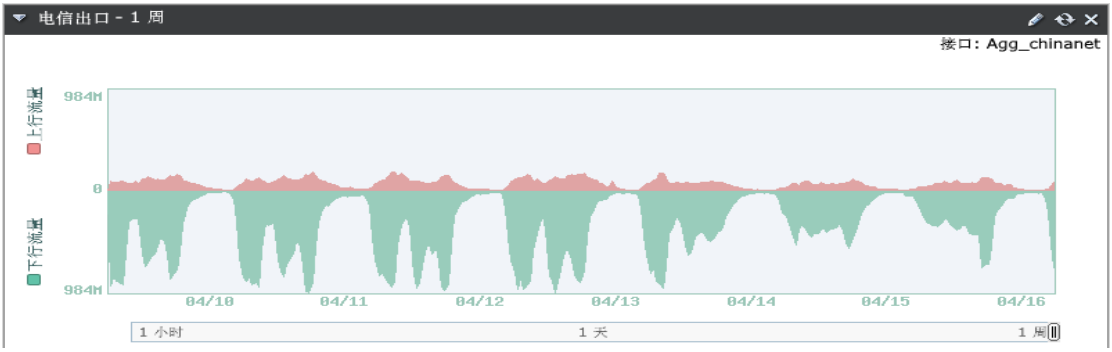
站群系统应用防火墙网站访问 IP 封禁记录

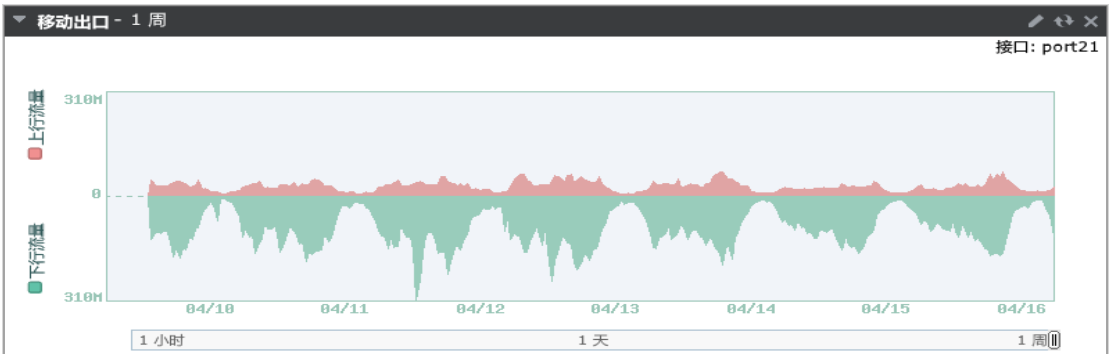
封禁IP	封禁IP归属地	封禁开始时间 ▼	封禁结束时间
60.205.212.155	广东省深圳市 英达通信	2018-04-15 04:17:55	2018-04-15 14:17:55
185.92.73.172	欧洲和中东地区	2018-04-15 03:41:44	2018-04-15 13:41:44
27.255.77.11	韩国 Ehost互联网数据中心	2018-04-12 23:06:30	2018-04-13 09:06:30
94.130.237.171	乌克兰	2018-04-12 02:30:04	2018-04-12 12:30:04
110.87.188.33	福建省福州市 电信	2018-04-12 02:13:45	2018-04-12 12:13:45
110.87.188.33	福建省福州市 电信	2018-04-10 10:28:49	2018-04-10 20:28:49
134.73.216.20	北美地区	2018-04-09 14:20:10	2018-04-10 00:20:10
27.255.77.11	韩国 Ehost互联网数据中心	2018-04-09 13:06:45	2018-04-09 23:06:45

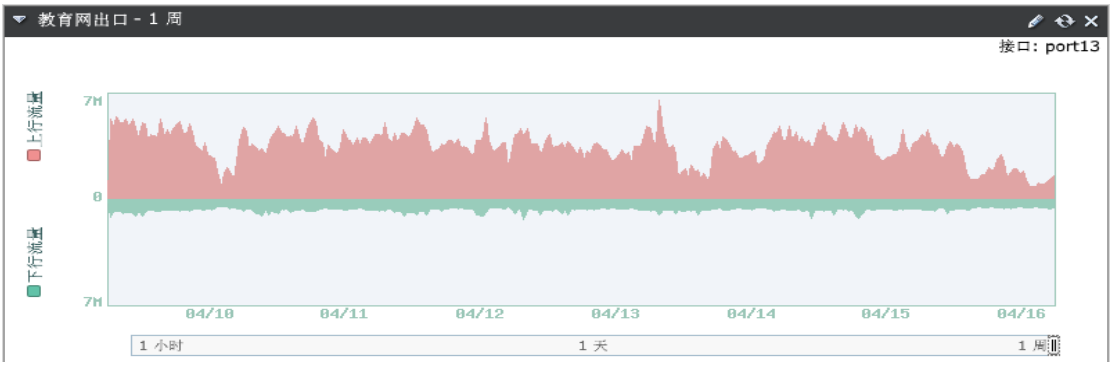
站群系统 4 月份网站累计访问次数

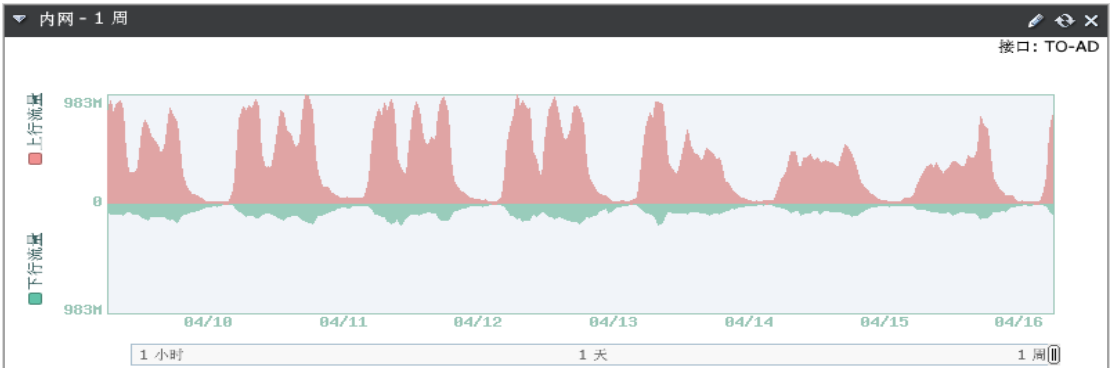
站点名称	访问次数	站点名称	访问次数
兰州城市学院	41999	团委	166
就业服务网	4357	财务处	164
教务处	3391	保卫处	146
化学与环境工程学院	1720	后勤管理处	126
教育学院	1677	甘肃文化翻译中心	115
文史学院	1409	党委宣传部	112
电子与信息工程学院	1409	膳食处	106
机械工程学院	1120	发展规划处	101
人事处	1100	学位办公室	93
地理与城乡规划学院	1097	教师发展中心	90
外国语学院	1078	党委组织部	81
数学学院	1004	信息网络中心	78
音乐学院	963	廉政网	77
旅游学院	957	甘肃省民族音乐研究中心	74
石油工程学院	906	卡务中心	53
美术与设计学院	858	兰州城市学院校医院	53
马克思主义学院	792	信息技术教育与应用研究所	46
幼儿师范学院	760	甘肃张芝书法院	44
商学院	693	心理咨询中心	41
体育学院	617	机关党委	39
传媒学院	477	审计	36
科学研究处	396	基本建设处	29
国有资产管理处	359	城市社会心理研究中心	18
教学质量监测与评估中心	323	实训中心	15
党委学生工作部	244	职业技能鉴定所	10
党委（校长）办公室	216	电子信息科学与技术研究所	10
创新创业学院	191	城市信息与系统科学研究所	8
路易艾黎研究中心	189	国际交流处	1

网络出口带宽情况统计









APT统计

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

网站安全检测一（360 网站安全检测）

网站安全漏洞

存在"服务器配置信息泄露"风险，安全性降低5%　漏洞信息已隐藏，只对网站管理员开放 请先验证权限

虚假或欺诈网站监控

正常

挂马或恶意网站监控

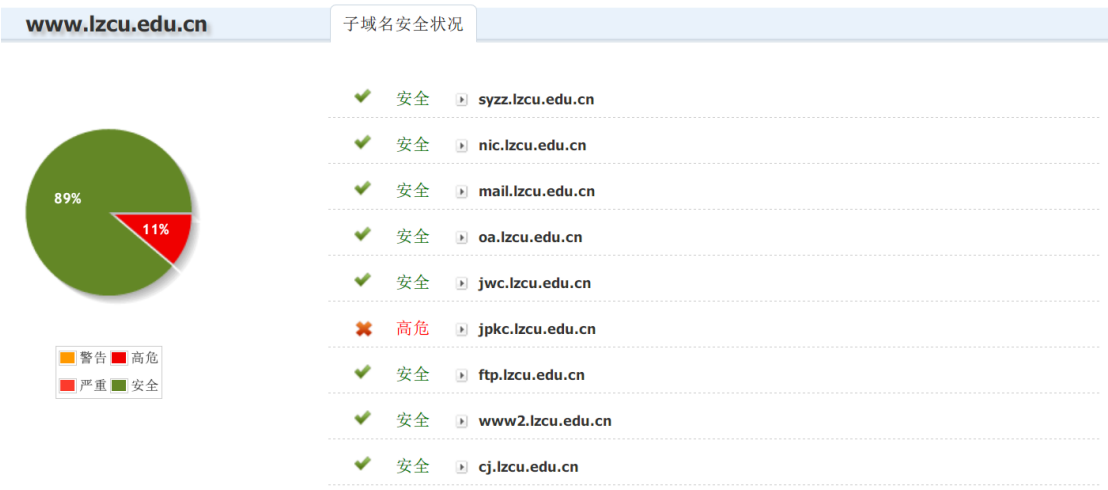
正常

黑客篡改网站监控

正常

网站敏感内容监控

正常



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	586.23 ms	100 %
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	538.53 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	299.3 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	402.31 ms	100 %

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	34 高危	查看详情>>
jpkc2.lzcu.edu.cn	90 良好	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jwc.lzcu.edu.cn	90 良好	查看详情>>
kyc.lzcu.edu.cn	34 高危	查看详情>>

当前 1 / 2 页 首页 上一页 下一页 尾页

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	0 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

【安全教育】网络安全保护意识更加全面 关键设施安全不容忽视

新华网 2018-04-16 07:48:40 来源:法制日报

在蚂蚁金服展台，只要用手机扫一扫就能提示您安全风险。殷立勤 摄

大学生：海量个人信息泄露可能危及国家安全

群众：重要设施数据关键敏感

大数据时代网络安全保护意识更加全面

网络安全，可谓是近年来民众最为关注的焦点问题。

值得注意的是，《法制日报》记者在调查中发现，在不少市民看来，网络安全不仅是个人信息的安全，还涉及到社会及国家的网络安全；不仅是数据安全，还包括电网等基础设施的安全；不仅是网络系统的安全，还包括内容的安全。

个人信息保护日趋严谨

“在大数据时代，个人已经非常透明，只要你使用互联网的服务，无论是聊天搜索还是看视频、阅读，实际上是把自己产生的数据交给互联网公司。”在北京某互联网金融公司上班的李航对《法制日报》记者说。

李航说，这种体会来自社会对互联网金融行业的评价——“这个行业长期以来被视为个人信息泄露的源头之一”。

“互联网金融的发展得益于计算机的普及和现代网络信息技术的突破，后者同时也带来技术漏洞、信息泄露等一系列问题。同时，互联网金融行业对个人信息依赖性极强，但目前我国征信体制不健全，互联网金融平台核实客户信息缺乏有效渠道，有的确认方式比较原始，有的不得不通过线下方式确认，不利于发挥效率优势。”对于行业内部的问题，李航说得很直白。不过，他也认为，近年来，尤其是网络安全法出台后，行业内部对公民个人信息安全更加重视。

“在获得数据后，如何让数据形成关联，在保护消费者权益的基础上形成经济价值、提升社会效益，这是互联网企业在大数据时代面临的极大挑战。”李航说。

对此，李航向记者介绍了一些具体做法：在人员管理上，能够接触到大量用户敏感信息的员工，在入职前都必须经过充分的背景调查，并签署相关保密协议。即便被调离岗位或终止劳动合同，个人信息处理岗位上的相关人员也会被要求继续履行保密义务。

“目前，在一些互联网金融企业，数据会按照敏感信息和非敏感信息进行分类和存储。其中，个人财产信息属于机密数据，个人生物识别信息、个人身份信息、网络身份标识信息等为保密数据。而系统日志、业务日志等内部数据也在敏感信息范畴内。”李航向记者介绍说，如需提取这些敏感数据，业务部门需要进行安全备案，同时还有数量限制和时间控制，“比如一个人在一段时间内只能查询三条”。

发帖留言也关乎网络安全

去年 4 月，《法制日报》记者曾就网络安全意识做过调查。当时，90%的受访者认为，网络安全就是防止个人信息泄露；仅有 10%的受访者注意到，网络安全还涉及打击网络犯罪，还涉及核心数据安全，还涉及基础设施的安全。

某高校大学生林峰就曾是 90%受访者之一。如今，他对记者说，经过一年的学习，他认识到，网络安全不仅是个人信息保护，还要注意不能在网上发表不实言论，以免产生恶意舆论危害国家政治安全。

在北京一所高校上大三的胡天奇对记者说，学校社团曾专门举办辩论会，“大家通过讨论得出一个结论：单一的个人信息泄露会影响个人隐私、社会交往和经济利益；局部性、群体性的个人信息泄露有可能导致网络犯罪和社会问题；大规模的个人信息泄露会引起公众恐慌，危及社会稳定；敏感的、跨境的个人信息泄露更会关乎国家发展和安全利益”。

“我们老师还特别就此问题请教了国防大学的老师，之后向我们讲解说，不管是平时还是战时，如果一个国家很多人的个人信息被有组织、有预谋地收集到一起，那么大到国家的一举一动、小到个人的一言一行都可能暴露在对方的视野下。个人的网上留言等信息通过大数据分析，就会得出个人的政治倾向等信息；更多人的信息汇总到一起，通过分析加工，会对国家发展、国防安全等造成巨大威胁。”胡天奇对《法制日报》记者说。

关键设施安全不容忽视

在网络安全中，关键信息基础设施的安全不容小觑。

何为关键信息基础设施？2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》，其中规定：国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。

李航在入职现在的互联网金融企业前，曾是某银行信用贷款审批人员。他告诉记者，银行内部会经常发放关于网络安全的文件，最主要是不能泄露客户信息、审批流程，还会有一些使用互联网的注意事项，会有定期的网络系统和安全系统的扫描。

“目前，银行系统很少遭到破坏。不过，我知道，如果银行系统遭到黑客攻击，影响会很大，银行的信誉、业务会受到破坏，客户的信息可能会泄露，严重的话对国家经济也会有影响。”李航说。

家住北京市海淀区的张洁给记者讲述了一件发生在她身边的事情。

“我曾经在电网某单位实习，因为这家单位有一些机密数据，所以我在开始实习时就签了保密协议，每次进单位也都要经过安检。有一天，1 名男子想去有大数据的资料室，找不到地方就问工作人员。当时，工作人员觉得这名男子非常面生，于是向保卫部门举报。经核实，此人真的是外来人员，接着就被押到了保卫部。我当时就想知道后续结果，于是四处打听，但一起工作的同事都是讳莫如深的样子。第二天，单位领导把我们的门禁卡都给换了。我感觉，这个人混进来并且想进入大数据资料室，肯定是有目的的。”张洁说。

张洁坦言，在这件事发生之前，她了解电网数据的重要性，但没想到涉及这些数据的问题会如此敏感。

对此，中国人民公安大学教授王大伟说：“心防要高于技防。每个公民要不断强化国家安全意识，使心中的警惕级别高于国家强调的级别，要时时对自己的行为把关。这包括发布微信微博时要注意对时间、地点和照片做模糊化处理，出现不相关的人一定要删掉，牵扯到关键敏感信息时要尤为谨慎。”记者 赵丽

【安全术语】七大网络安全术语

一、协议

接入网络的计算机都可以通过彼此之间的物理设备进行数据交换，这种物理设备包括最常见的电缆、光缆、无线 WAP 和微波等；而协议是为数据交换而建立的规则、标准或约定的集合。

二、服务器与客户端

最简单的网络服务形式是：若干台电脑做为客户端，使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端电脑。例如我们平时接触的电子邮件服务器、网站服务器、聊天室服务器等都属于这种类型。

另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端电脑进行连接，也就是说每一台电脑都既是服务器、又是客户端，它们之间具有相同的功能，对等的完成连接和信息交换工作。

从此看出，客户端和服务器分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，都是操作着自己的电脑（客户端），且向网络服务器发出常规请求完成诸如浏览网页、收发电子邮件等动作的

三、系统

电脑要运作必须安装操作系统，如今流行的操作系统主要由 UNIX、Linux、Mac、Win10、Windows7 等，这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制，在网络上，既可以作为服务器、也可以作为客户端被使用者操作，它们之间通过“协议”来完成信息的交换工作。

四、IP 地址和端口

我们上网，可能会同时浏览网页、收发电子邮件、进行语音聊天……如此多的网络服务项目，都是通过不同的协议完成的，然而网络如此之大，我们的电脑怎么能够找到服务项目所需要的电脑？如何在一台电脑上同时完成如此多的工作的呢？这里就要介绍到 IP 地址了。

每一台上网的电脑都具有独一无二的 IP 地址，这个地址类似于生活中人们的家庭地址，通过网络路由器等多种物理设备，网络可以完成从一个电脑到另一个电脑之间的信息交换工作，因为他们的 IP 地址不同，所以不会出现找不到目标的混乱局面。

一台电脑上为什么能同时使用多种网络服务。不同的协议体现在不同的网络服务上，而不同的网络服务则会在客户端电脑上开辟不同的端口来完成它的信息传送工作。当然，如果一台网络服务器同时开放了多种网络服务，那么它也要开放多个不同的端口来接纳不同的客户端请求。

网络上经常听到的“后门”就是这个意思，黑客通过特殊机能在服务器上开辟了一个网络服务，这个服务可以用来专门完成黑客的目的，那么服务器上就会被打开一个新的端口来完成这种服务，因为这个端口是供黑客使用的，因而轻易不会被一般上网用户和网络管理员发现，即“隐藏的端口”，故“后门”。

每一台电脑都可以打开 65535 个端口，因而理论上我们可以开发出至少 65535 种不同的网络服务，然而实际上这个数字非常大，网络经常用到的服务协议不过几十个，例如浏览网页客户端和服务端都使用的是 80 号端口，进行 IRC 聊天则在服务端使用 6667 端口、客户端使用 1026 端口等。

五、漏洞

漏洞就是程序中没有考虑到的情况。就是程序设计上的人为疏忽，列如“溢出”漏洞则属于当初设计系统或者程序的时候，没有预先保留出足够的资源，而在日后使用程序是造成的资源不足。漏洞在任何程序中都无法绝对避免，黑客常常就是沉迷在阅读他人的程序并力图找到其中的漏洞。

六、加密

某种意义上说所有上网者都能参与信息共享，因而对某些商业、个人隐私在网络上的传送，数据就会暴露在众目睽睽之下，我们的信用卡、个人电子邮件等信息都可以被截取到，如何才能让这些信息安全呢？通过加密处理的信息在网络上传送，无论谁拿到了这份文件，只要没有“密码薄”仍然是白费力气的。

网络上最常使用的是设置个人密码、使用 DES 加密锁，这两种加密方式分别可以完成用户登陆系统、网站、电子邮件信箱和保护信息包的工作。

七、特洛伊木马

特洛伊木马是一个程序，目前一般可理解为“为进行非法目的的计算机病毒”，在电脑中潜伏，以达到黑客目的。现在有的病毒伪装成一个实用工具、一个可爱的游戏、一个位图文件、甚至系统文件等等，诱使用户将其安装在 PC 端或者服务器上，从而秘密获取信息。

抄送：校领导