北京理工大学网络信息技术中心

工作简报

（2019.6.1～2019.6.30）

2019 年第 5 期　　网络信息技术中心　2019 年 7 月 1 日

一、校园网建设与运行维护

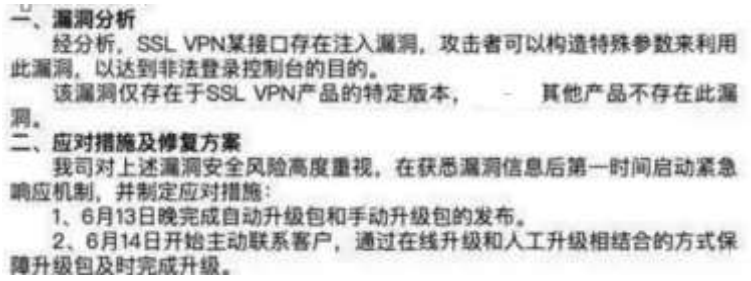
1、校园网日常运行和维护状况：

6 月 5 日，填写《北京理工大学修缮工程项目申请表》，协助西山实验服务中心修复其于五一期间因施工挖断光缆导致的北院 1 号楼网络故障事宜。

6 月 10 日，完成学校正版软件平台卡巴斯基杀毒软件的 license 升级，保证学校师生员工的正常使用。

6 月 11 日，完成学校统一 DHCP 管理平台的升级工作，并将宇航学院楼地址纳入统一管理，解决该楼部分用户无法获得 IP 地址的问题。

6 月 14 日，第一时间联系 VPN 设备厂家，处理其可能存在的 VPN 漏洞导致恶意用户非法登陆控制台。


一、漏洞分析
经分析，SSL VPN某接口存在注入漏洞，攻击者可以构造特殊参数来利用此漏洞，以达到非法登录控制台的目的。
该漏洞仅存在于SSL VPN产品的特定版本，　其他产品不存在此漏洞。
二、应对措施及修复方案
我司对上述漏洞安全风险高度重视，在获悉漏洞信息后第一时间启动紧急响应机制，并制定应对措施：
1、6月13日晚完成自动升级包和手动升级包的发布。
2、6月14日开始主动联系客户，通过在线升级和人工升级相结合的方式保障升级包及时完成升级。

6 月 27 日，完成良乡校区文科楼和 7 号宿舍楼等在建楼宇的现场地勘工作，为下一步配合学校完成相关楼宇网络工程建设做好准备。

2、邮件及计费系统日常配置管理和维护情况：

交流和讨论如何做好邮件安全的溯源和保护工作；完成 2019 年夏季毕业本科生、研究生校园网用户的电子邮件帐号和外网帐号数据整理工作；完成数据库安全审计系统的定期巡检工作；在 A10 设备上为教务部选课系统搭建负载均衡备用方案；为暑期排练学生做外网帐号保留的处理。

二、学校信息化建设

6 月下旬，我中心作为数字离校的技术支持单位，积极配合学校毕业生离校工作安排，认真进行系统数据准备、网络环境测试及使用咨询工作，全面保障离

校系统平稳运行。

三、数据中心的维护和管理

1、网站维护：按照学校要求及时更新校园网主页的相关内容，2019 年 6 月 1 日至 6 月 30 日期间，校园通知公告网共审核及发布“最新通知”116 篇，日常监测二级网站情况。

2、服务器维护：做好虚拟主机系统的日常维护工作，包括上线在役期系列安全产品的日常升级维护和审计分析，防病毒软件的日常维护，跟踪与我校信息系统有关的漏洞平台情报、监测安全设备数据等。2019 年 6 月 1 日至 6 月 30 日期间，处理私有云平台托管主机故障 3 例，架设学工系统云主机 4 台。假设部门内部业务云主机 2 例，架设桌面系统 2 例。日常维护私有云平台、存储系统、数据中心网络以及安全系统。数据中心拦截网络攻击次数情况：

2019 年 6 月份学校主网站总请求数 23457688，网站总流量 1635.17GB，清洗了 56.99GB 的恶意流量。

总请求数	总流量	Alexa 全球排名
23457688	1635.17GB	9033

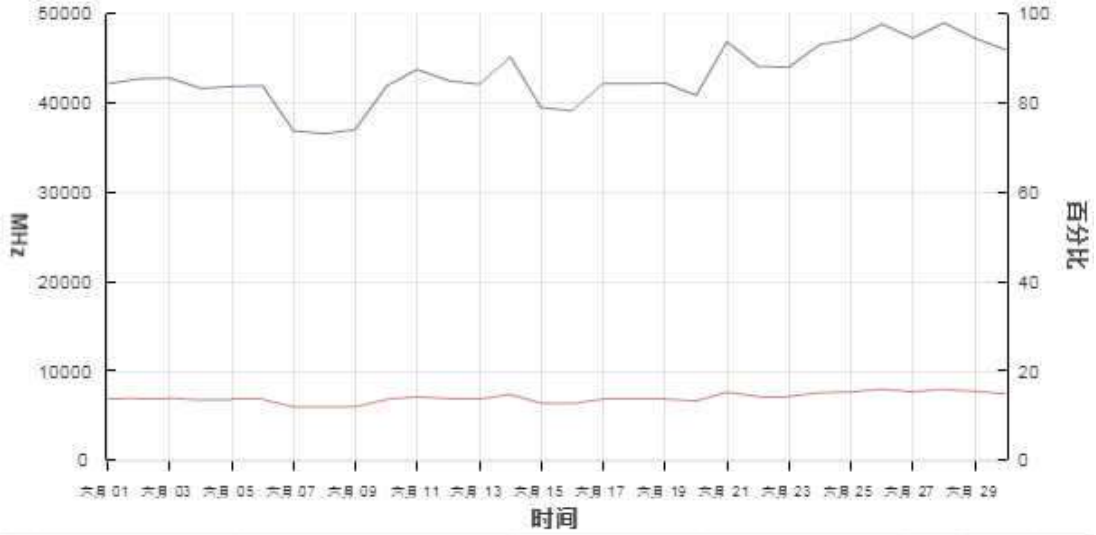
数据中心监测到的攻击数据：

3、云主机运行平台当前状况（2019 年 6 月 30 日）

Production-R710 集群：

总内存资源	1.50TB	总存储资源	50.71TB	主机数	8
虚拟机数量	307	总 CPU 资源	307GHz	CPU 数	128

4、云主机运算平台 CPU 使用情况（2019 年 6 月 1 日至 2019 年 6 月 30 日）：



项	对象	测量	汇总	单位	最新	最高	最低
	production	使用情况(MHz)	平均值	MHz	4...	4...	3...
	production	使用情况	平均值	百分比	1...	1...	11...

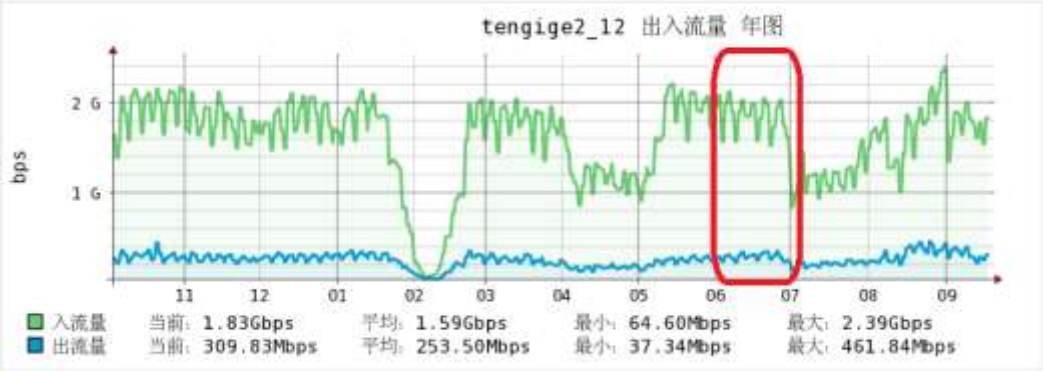
四、校园网基本运行情况

1、网络流量

计费出口-1

计费出口-2

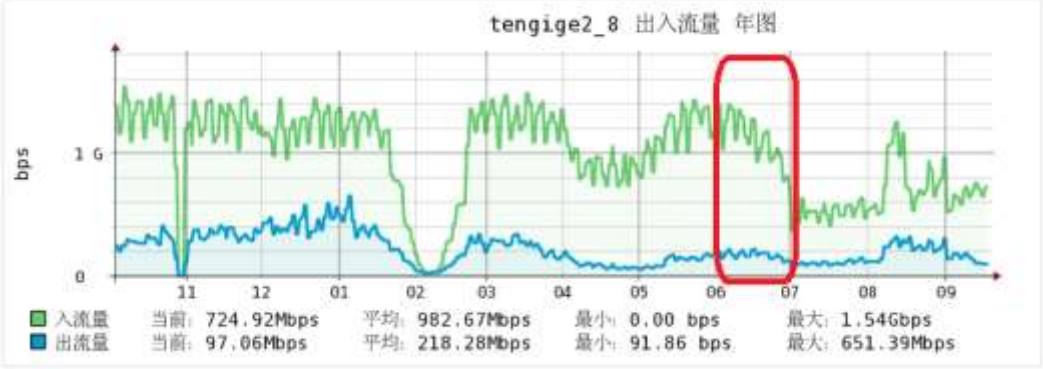
IPV4 电信网出口流量曲线



IPV4 教育网出口流量曲线

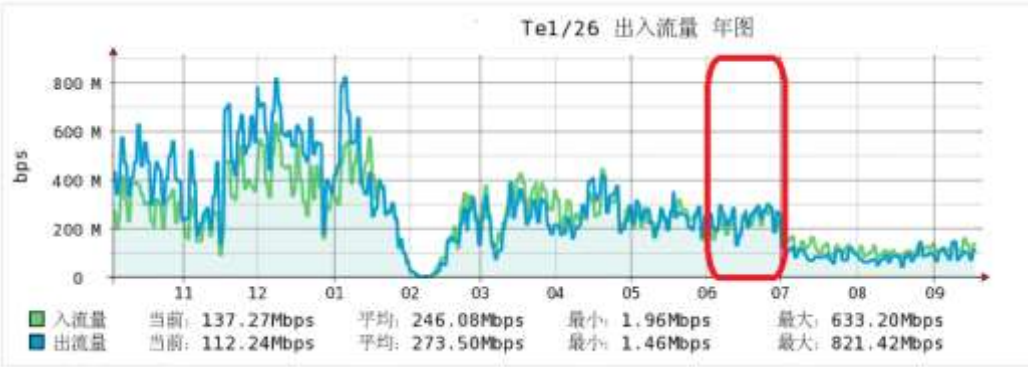
IPV4 联通出口流量曲线

IPV4 移动出口流量曲线

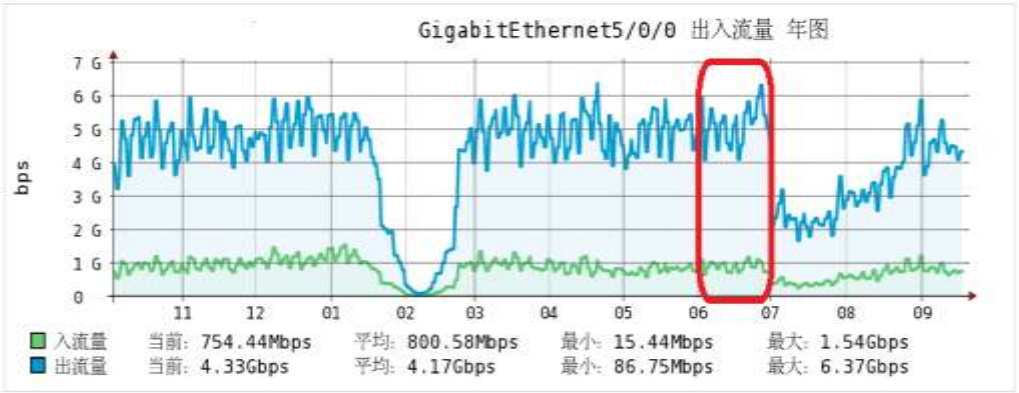


IPV6 北大万兆出口流量曲线

IPV6 政法大学出口流量曲线



全网无线网使用情况



3、垃圾病毒邮件过滤（2019 年 6 月 1 日至 2019 年 6 月 30 日）

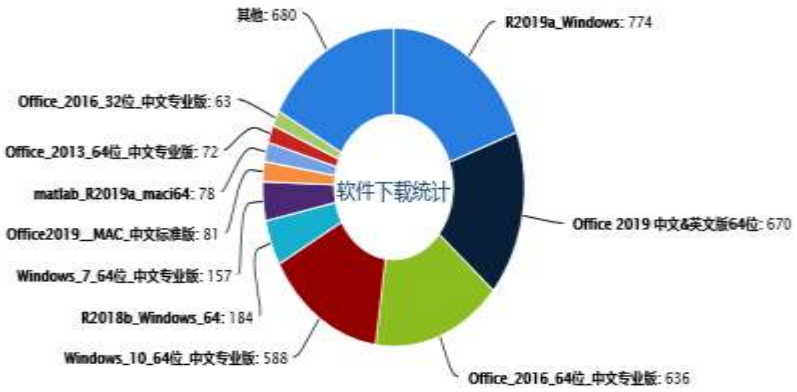
系统统计信息

(从 2019 年 06 月 01 日 到 2019 年 06 月 30 日) 查询

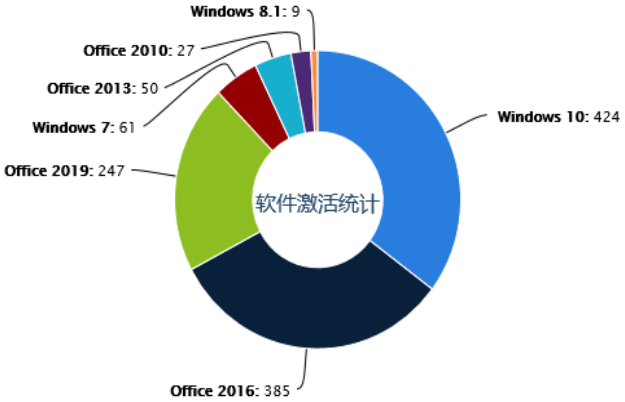
网络层统计	系统网络连接数	5423258次		
	正常连接数	1958039次		36.1%
	被拒连接数	3465219次		63.9%
应用层统计	系统总收邮件(90.21%)			
	系统总收邮件	1684046封	555893.77MB	
	正常邮件	367530封	408134.71MB	21.82%
	拦截邮件	1316516封	147759.06MB	78.18%
	病毒邮件	294封	155.1MB	0.02%
	垃圾邮件	1316222封	147603.96MB	78.16%
	系统总发邮件(9.79%)			
	系统总发邮件	182800封	165377.63MB	
	正常邮件	182663封	163762.54MB	99.93%
	拦截邮件	137封	1615.09MB	0.07%
	病毒邮件	16封	3.6MB	0.01%
	垃圾邮件	121封	1611.49MB	0.07%

4、正版化软件下载与激活情况

平台共下载 3983 次， Windows 10 下载 586 次，Windows 7 下载 157 次，Office 2016 下载 699 次数，Office 2013 下载 72 次，具体产品下载详情见下图。



平台共激活 764 次，Windows 10 激活 424 次，Windows 7 激活 61 次，Office 2016 激活 385 次，Office 2013 激活 50 次，Office2010 激活 27 次，具体产品下载详情见右图。



常见激活问题统计

错误代码	是否平台登记/解决办法
0x803F7001	系统版本不对，需要装入 GVLK 密钥或者通过平台下载操作系统安装介质
0xC004C003	平台登记
0xC004F017	系统版本不对，需要装入 GVLK 密钥或者通过平台下载操作系统安装介质
0xC004F035	平台登记
0xC004F074	平台登记
未检测到 IP 地址	注入“修改值”注册表文件
链接服务器失败	注入“修改值”注册表文件

主题词：北理工 网络 信息化 教育技术 安全

编辑：朱丽洁　　数据统计：卢肖 唐凯 杨德全 屈少杰 武波等　　审核：陈朔鹰

网络信息技术中心　　二零一九年七月一日印发