网络信息安全周报

【2017】第 35 期

党委宣传部
信息网络中心 编　　2017 年 12 月 28 日

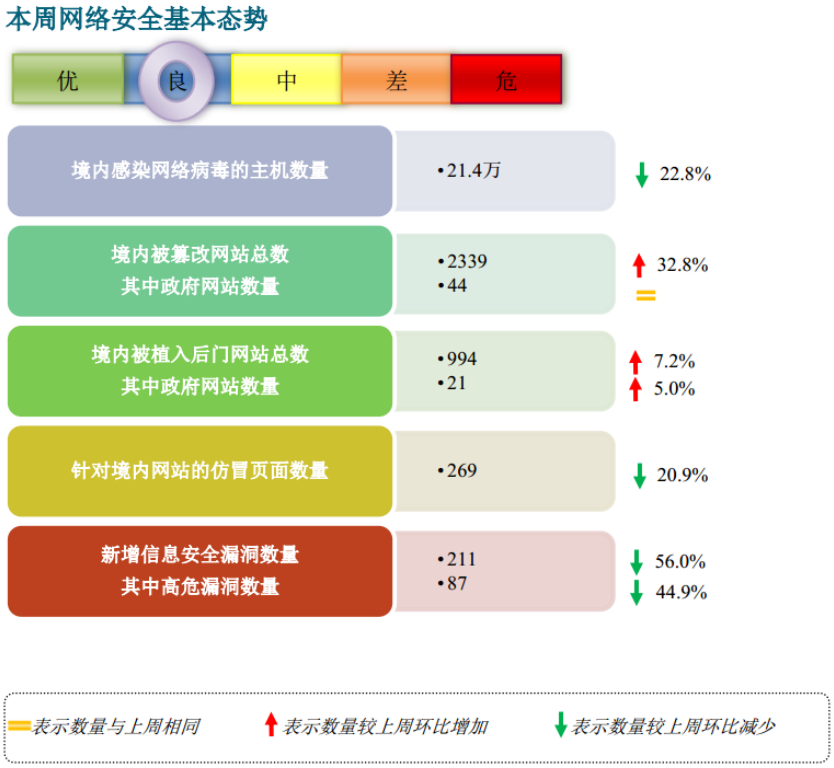
本期要目

- 【权威发布】全国网络安全信息与动态（2017 年 12 月 11 日—17 日）
- 【城院 IT】综合业务管理平台统计信息(2017 年 12 月 18 日—24 日)
- 【学习中国】2018 年网络安全趋势展望：垂直行业成主要目标

全国网络安全信息与动态

（2017 年 12 月 11 日-12 月 17 日）

根据国家互联网应急中心最新公告数据：

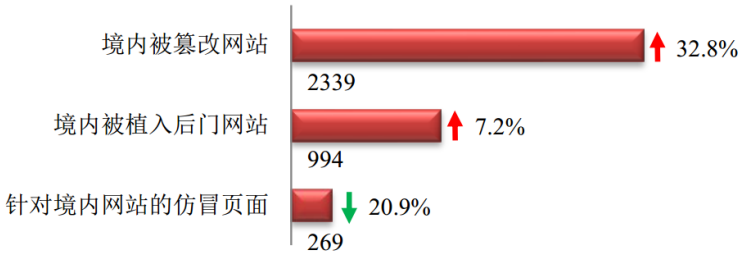


本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 9.3 万以及境内感染飞客（conficker）蠕虫的主机约 12.1 万。

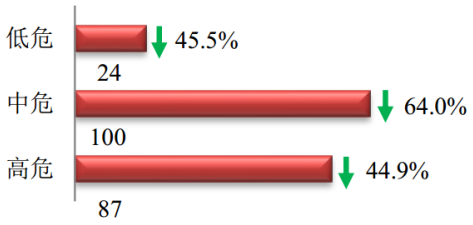
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2339 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 269。



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 211 个，信息安全漏洞威胁整体评价级别为高。



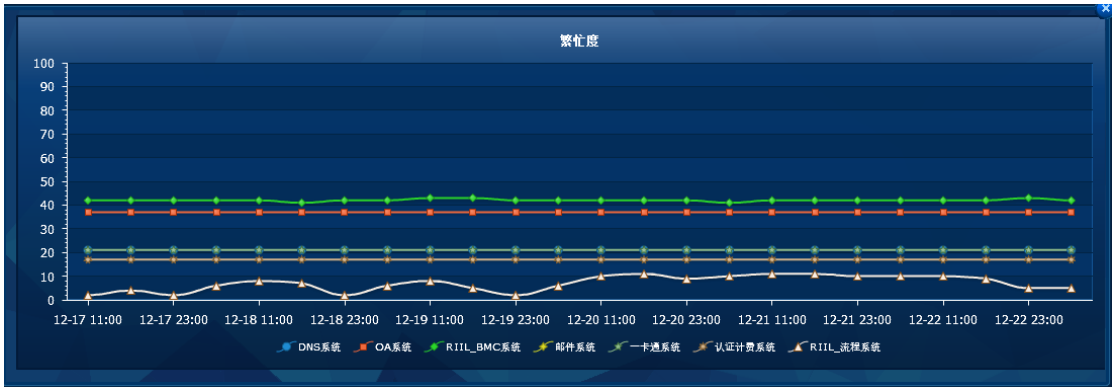
本周事件处理情况

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 1241 起，其中跨境网络安全事件 217 起。

城院 IT 综合业务管理平台统计信息

(2017 年 12 月 18 日—12 月 24 日)

主要业务服务繁忙度



网站集群网页更新情况统计

网站	发布		网站	发布
兰州城市学院	28		党委学生工作部	
教学质量监测与评估中心	14		党委组织部	
旅游学院	9		电子信息科学与技术研究所	
就业服务网	8		发展规划处	
城市社会心理研究中心	7		甘肃省高等学校外语教学指导委员会	
马克思主义学院	6		甘肃张芝书法院	
外国语学院	5		国有资产管理处	
音乐学院	4		后勤管理处	
地理与城乡规划学院	3		化学与环境工程学院	
电子与信息工程学院	2		基本建设处	
廉政网	2		教师发展中心	
传媒学院	1		教务处	
甘肃文化翻译中心	1		卡务中心	
机关党委	1		兰州城市学院校医院	
机械工程学院	1		路易艾黎研究中心	
教育学院	1		美术与设计学院	
科学研究处	1		膳食处	
人事处	1		商学院	
数学学院	1		审计	
体育学院	1		石油工程学院	
信息网络中心	1		实训中心	
幼儿师范学院	1		团委	
保卫处			文史学院	
城市信息与系统科学研究所			心理咨询中心	
创新创业学院			信息技术教育与应用研究所	
档案馆			学位办公室	
党委（校长）办公室			招生网	
党委宣传部			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
191361	站点名称：地理与城乡规划学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-24 00:28:37
191360	站点名称：地理与城乡规划学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-24 00:28:35
191359	站点名称：地理与城乡规划学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-24 00:28:27
191358	站点名称：信息网络中心	180.130.10.79	云南省大理州 联通		SQL注入	2017-12-21 23:49:26
191353	站点名称：膳食处	121.204.107.170	未知国家 未知地区		SQL注入	2017-12-19 15:01:25
191352	站点名称：路易艾黎研究中心	185.92.73.105	欧洲和中东地区	含有非法请求参数	SQL注入	2017-12-19 14:54:20
191351	站点名称：路易艾黎研究中心	185.92.73.105	欧洲和中东地区	含有非法请求参数	SQL注入	2017-12-19 14:54:20
191350	站点名称：路易艾黎研究中心	185.92.73.105	欧洲和中东地区		SQL注入	2017-12-19 14:54:13
191349	站点名称：膳食处	121.204.107.170	未知国家 未知地区	含有非法请求参数	跨站脚本注入	2017-12-19 12:50:10
191348	站点名称：膳食处	121.204.107.170	未知国家 未知地区	含有非法请求参数	跨站脚本注入	2017-12-19 12:50:08
191347	站点名称：膳食处	121.204.107.170	未知国家 未知地区	含有非法请求参数	跨站脚本注入	2017-12-19 12:49:34
191345	管理平台	124.152.99.30	甘肃省 联通	登录位置：网站管理	错误帐号或密码	2017-12-18 19:56:01
191344	管理平台	124.152.99.30	甘肃省 联通	登录位置：网站管理	错误帐号或密码	2017-12-18 19:55:39
191343	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	SQL注入	2017-12-18 11:09:15
191342	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	跨站脚本注入	2017-12-18 11:09:14
191341	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	SQL注入	2017-12-18 11:09:05
191340	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	跨站脚本注入	2017-12-18 11:06:45
191339	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	跨站脚本注入	2017-12-18 11:06:42
191338	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	SQL注入	2017-12-18 09:24:50
191337	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	SQL注入	2017-12-18 09:24:48
191336	站点名称：兰州城市学院	182.118.33.7	河南省郑州市 奇虎360科技联通节点	含有非法请求参数	SQL注入	2017-12-18 09:24:48
191334	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:48
191333	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:48
191332	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:47

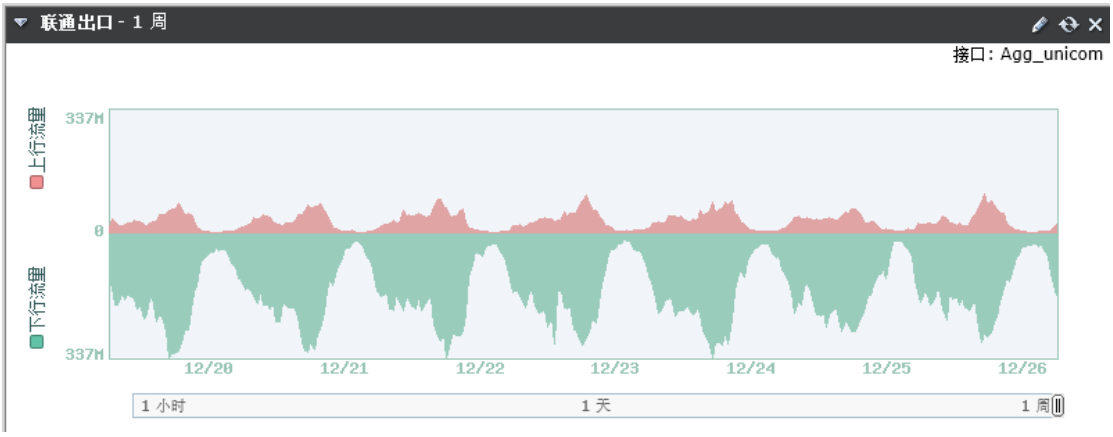
站群系统应用防火墙网站访问 IP 封禁记录

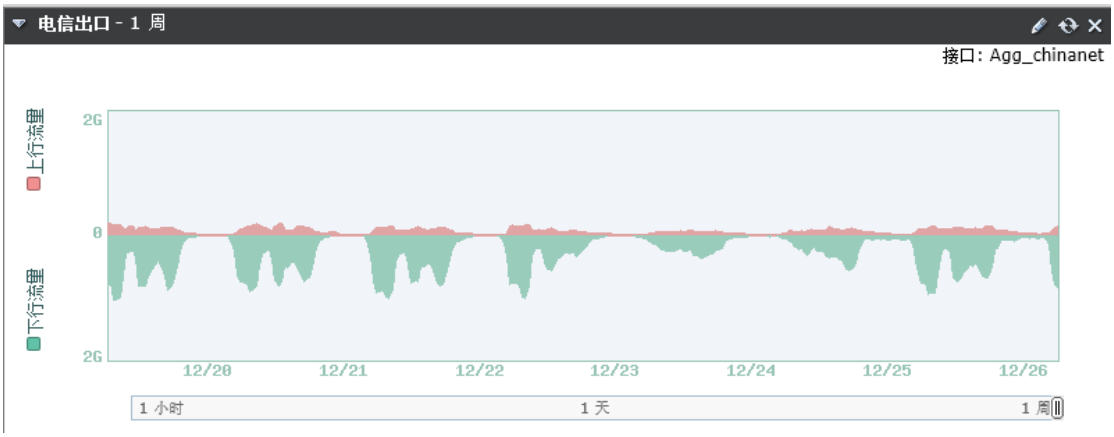
封禁IP	封禁IP归属地	封禁开始时间 ▼
110.87.188.33	福建省福州市 电信	2017-12-24 00:28:37
185.92.73.105	欧洲和中东地区	2017-12-19 14:54:20
121.204.107.170	未知国家 未知地区	2017-12-19 12:50:10
182.118.33.7	河南省郑州市 奇虎360科技联通节点	2017-12-18 11:09:15
182.118.33.7	河南省郑州市 奇虎360科技联通节点	2017-12-18 09:24:50
198.204.225.114	美国	2017-12-18 07:04:48

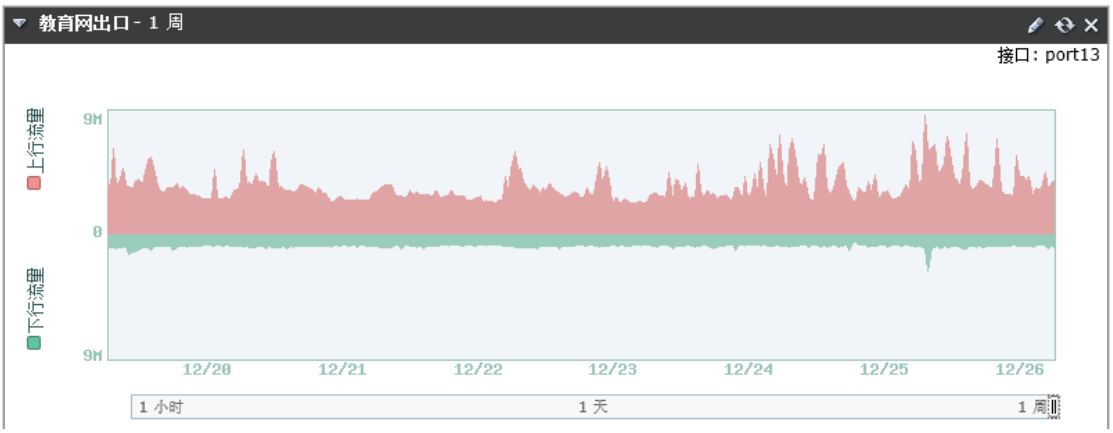
站群系统应用防火墙网站危险文件扫描记录

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

网络出口带宽情况统计



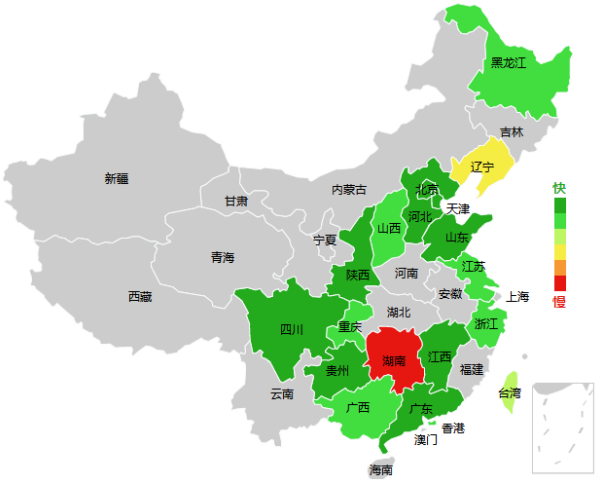




APT统计

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	1,084.44
2	山西	540.22
3	北京	492.65

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	电信	202.77	27.8	34	140.98

360 网站评分（http://www.lzcu.edu.cn）

总分: 81

用户输入URL：	http://www.lzcu.edu.cn
实际检测URL：	http://www.lzcu.edu.cn/
请求总次数：	61 次
文件总大小：	4,345,339 B
检测时间：	2017-12-26 09:48:27

注意：本检测是通过模拟浏览器请求得到并进行评分，并不能完全说明网站的优劣。

评分	指标
51	减少请求次数
3	使用长连接 (keep alive)
0	设置页面内容具有缓存性
100	开启GZIP压缩
100	把JS置于底部
40	精简CSS和JS文件
100	避免404错误
100	减小Cookie体积
2	使用CDN(外链)

哈哈，您的网站还不赖噢，快看看评价，做的更棒吧！

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	101.226.4.6(上海电信) 114.114.114.114(114DNS.COM114DNS.COM) 8.8.8.8(GOOGLE.COMGOOGLE.COMlevel3.com) 121.28.148.33(河北石家庄联通) 168.95.1.1(台湾cht.com.tw) 125.71.5.51(四川成都电信)	电信 其他 其他 联通 其他 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	3 1	435.2 ms	75 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	3 1	417.5 ms	75 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	133.23 ms	66.67 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	285.12 ms	66.67 %	详情

查看更多 >>

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2017-12-24 20:30:43

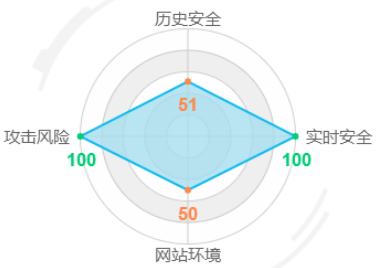
指数评价

80.2

所属行业：教育培训

53.32%↑

战胜了全国 **0.00%** 的网站



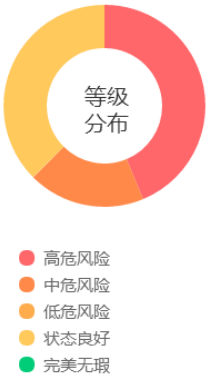
关联网站安全

关联网站数　16

最低指数评价　4.0 高危

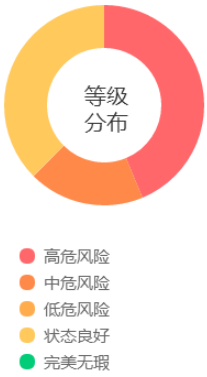
查看更多>>

该网站安全指数评价 良好 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	54.8 中危	查看详情>>
ecard.lzcu.edu.cn	41.2 中危	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jpkc2.lzcu.edu.cn	90 良好	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>>

当前 1 / 2 页　首页　上一页　下一页　尾页



域名	指数评价	操作
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	10 高危	查看详情>>
smtp.lzcu.edu.cn	10 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

【学习中国】2018 年网络安全趋势展望：垂直行业成主要目标

E 安全 2017-12-24 14:05:33

E 安全 12 月 24 日讯 在 2018 年，安全漏洞应被视为不可避免的威胁——而非完全可以避免的风险。

2018 网络安全趋势展望

第四次工业革命（工业 4.0）带来了前所未有的商机，但同时亦增加了网络攻击的必然性——企业自然需要为此做好准备。这不仅要求企业自起步阶段就将安全措施融入技术中，还需要将安全意识切实引入企业文化当中，同时辅以重要的资金投入。Gartner 公司最新预测数据显示，2018 年全球信息安全产品与服务支出总额将增长到 930 亿美元。

结合 2018 年可能出现的一些广泛性网络安全趋势与企业当前安全状况，可以提前对企业未来规划进行考量：

一、网络安全技能不断演进

随着技术的进步，处理网络安全工作所需要的技能正在发生变化。目前我们面临的挑战在于培养网络安全专业人员，使其能够尽快应对威胁，同时根据需要调整自身技能。美国投资咨询机构 Cyber-seucurity Ventures 公司发布报告预测，到 2021 年网络安全领域的人才缺口将达到 350 万。这一巨大的技能差距无疑须要各国政府、高校、学校以及企业协同合作来解决问题。

二、从预防转向应对

2018 年，安全违规事故应被认为不可避免的威胁，而非完全可以避免的风险。网络安全工作从被动的防御转向主动应对。企业必须公开讨论安全漏洞，提高安全意识与问责制度。当前以预防为重点的资源需要重新进行部署，以及时发现并应对潜在的安全隐患。

三、数字化系统驱动下一代安全机制

随着智能技术与物联网的逐步普及，客户数据的保护工作显得愈发重要。敏感信息数据的泄露可能产生直接物理影响，各类组织机构需要为用户及受影响的个人安全承担起责任。问责机制是一大关键挑战，意味着技术企业必须保护其设备、服务与软件以保证用户具备一定的安全可靠性。

四、威胁规模更大、复杂程度更高

时至今日，高达 70%的电子邮件为垃圾邮件，其中绝大部分涉及网络钓鱼。其它常见的黑客威胁还包括勒索软件、恶意软件以及分布式拒绝服务攻击（DDoS）等，此类攻击都曾在最近几个月内曾造成较为严重的危害，并有可能导致企业及客户的数据受到网络犯罪分子的入侵与窥探。美国无限公司 Verizon 最近发布的一份报告显示，93%的数据泄露事件背后存在经济驱动性因素。黑客们的目标自然是以最低投入获取最高回报，因此安全能力较低的小型企业往往成为其首选攻击对象。

五、新兴技术是把双刃剑

新兴技术使得网络犯罪分子能够利用愈发复杂的方法发动攻击，而这些创新成果同时也可帮助我们强化对黑客活动的防御能力。例如，人工智能（AI）型攻击带来的威胁正持续升级，但人工智能亦有助于加快潜在风险的识别过程。据某安全公司发布的预测：人工智能在未来的安全体系中将扮演不可或缺的作用，到 2023 年，全球人工智能安全市场的总体价值将达到 182 亿美元。

垂直行业成主要目标

尽管网络威胁值得各个行业的从业企业加以关注，但以下行业的安全形势显得尤为关键：

银行业、金融服务业与保险业:

这一行业正面临着越来越大的压力，即要求其更新遗留系统，并与新的精通数字化技术的对手开展竞争。消费者日趋青睐便捷且个性化的服务，金融行业所持有的客户数据的价值也在不断增长。不过信任是决定一切的关键——在最近的一项研究当中，有 50%的客户会考虑在遭受网络攻击后转而选择其它银行，而 47%的客户表示此类状况会导致其对银行“完全失去信任”。

医疗卫生行业:

患者记录的数字化彻底改变了整个医疗世界。可穿戴式设备与各类应用则为健康监测带来了进一步改善空间。此外，包括人工智能与物联网在内的新兴技术正被用于加速诊断并改善患者护理效果。然而，所涉及数据的敏感性与更高的连通性也引发了新的风险。

零售行业:

网络购物与数据分析的出现帮助零售商为客户打造更为便捷且个性化的体验。然而，这亦要求其肩负起对应的责任，即保护好所持有的数据（包括客户的购物偏好、登录凭证、银行信息、家庭住址等）。

电信行业:

作为互联网数据的载体，电信企业面临着巨大的网络安全风险，亦承担着可观的安全责任。服务供应商需要将网络安全措施整合至网络硬件、软件、应用程序以及最终用户设备当中，从而最大限度减少严重数据泄露的发生风险，最终切实保护客户证书与通信流量免受入侵。

制造业:

根据 IBM 公司的研究结果，制造业在黑客们最感兴趣的行业当中排名第三。出于经济驱动，这一领域的黑客主要倾向于实施工业间谍活动，包括入侵连接程度日益提升的机器人与 3D 打印生产线等。相关安全漏洞允许黑客访问产品设计蓝图，甚至能够通过变更设备配置破坏生产流程。这种违规行为不但会造成重大的经济损失，同时亦可能危及工作人员的生命安全。

政府机构:

任何组织机构面对数据泄露问题都不可能高枕无忧，政府机构自然也不例外。政府部门所掌握的各类信息——从选民资料到军事防卫计划数据——往往非常敏感，因此亦成为黑客攻击活动的主要针对目标。尽管世界各国政府都在逐步增加网络安全领域的支出额度，并努力实施应对计划以解决一切安全漏洞，但必须承认政府网络安全保障的发展道路还相当漫长。

抄送：校领导