山东省教育行业网络安全形势分析

山东省通信管理局
国家互联网应急技术处理协调中心山东分中心

网络安全形势

教育行业网络安全威胁分析

对策与建议

一，网络安全形势

网络安全形势

世界各国将网络安全提升到国家战略的高度

- 美国：网络安全办公室，对国家安全委员会和总统负责，统筹协调军队、情报部门和政府组织的网络安全事务。
- 英国：协调政府各部门网络安全计划的网络安全办公室、协调政府和民间机构重要信息系统安全保护的网络安全行动中心。
- 法国：网络与信息安全局（FNISA），以监控敏感的政府网络，发现和应对网络攻击。
- 韩国：信息安全司令部，专门应对网络战的威胁。

网络安全形势

- **维护网络安全已成为一种国家行为**
  - 军事组织信息对抗
  - 国家间情报对抗
  - 意识形态对抗
- **维护网络安全受政治利益驱动**
  - 恐怖组织
  - 民族分裂组织
  - 极端宗教组织
  - 受操纵的媒体
  - 有政治目的的黑客群体

网络安全形势

- **网络安全形势日益严峻**
  - 垃圾邮件泛滥成灾
  - 恶意代码形成产业链
  - 网络攻击目的性、针对性更强
  - 网络钓鱼猖獗
  - 安全漏洞频发
  - 域名系统安全性凸现
  - ……

网络安全形势

- 315晚会曝光公共WIFI漏洞
- 水牢漏洞威胁我国十余万家网站
- 20万儿童信息泄露或打包出售
- 徐玉玉案
- Jeep1.5万车主信息遭泄露

网络安全形势

“没有网络安全就没有国家安全”

“中央国家安全委员会”
“网络安全与信息化领导小组”

“网络安全和信息化是相辅相成的。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。”

中华人民共和国网络安全法

二，教育行业网络安全威胁分析

山东省教育行业网络安全形势严峻

国家战略：教育信息化是国家信息化建设的重要组成部分和战略重点。

我省教育信息化应用广泛：近年来，我省教育主管部门及行业信息化应用日益广泛，据不完全统计，我省教育行业共开办网站或系统约5300个，涵盖了教育信息公开、教学科研、招生考试、学生管理等方方面面。

教育信息化形式日益增多

山东省教育行业网络安全形势严峻

教育网络存在较大隐患：由于事关国计民生和公共利益，又承载着大量的敏感信息和隐私数据，已成为网络黑客组织及不法分子攻击的重点。

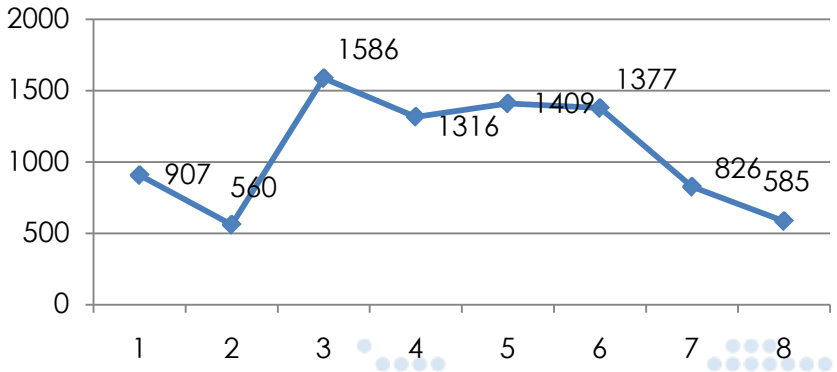
网络安全案件频发：近期，我省相继曝光的包括“徐玉玉案”在内的、多起因盗卖学生个人信息引发的电信网络诈骗案件，凸显了加强教育信息系统运行和数据安全防护的重要性和紧迫性。

电信网络诈骗猖獗

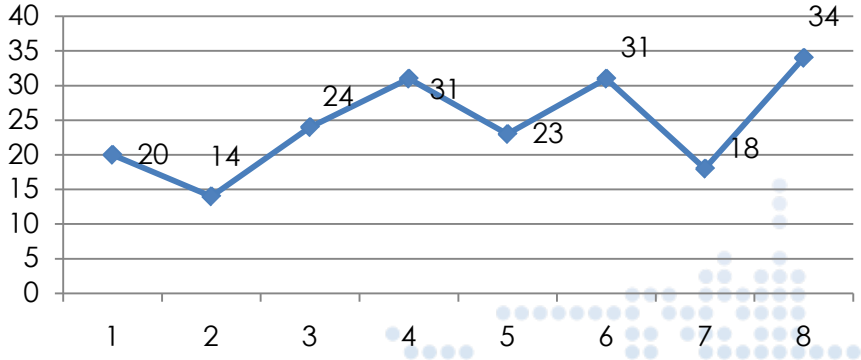
1.针对教育行业的黑客活动日趋活跃

安全形势升级：据不完全监测，今年以来我省共发生针对教育行业的网络安全威胁和事件4304起，其中教育行业终端主机受控事件3929起，占比91.3%；应用系统类事件375起，占比8.7%。终端主机类和应用系统类事件比往年同期均呈上升趋势，教育部门及行业网络面临双重威胁。

山东省教育行业主机类事件按月发生频次

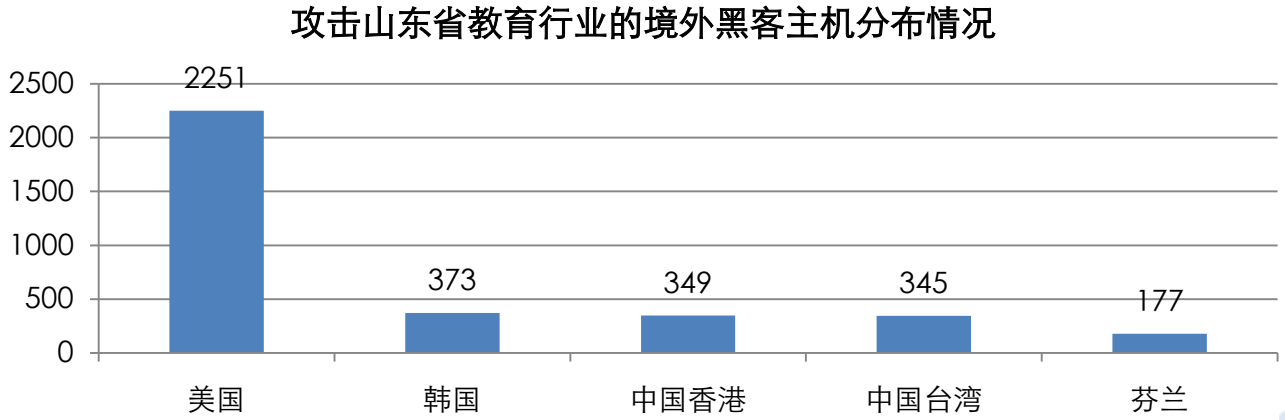


山东省教育行业应用系统类事件按月发生频次



针对教育行业的黑客活动日趋活跃

境外威胁加剧：值得注意的是，境外黑客对我省教育行业攻击活动尤其活跃，占到总攻击次数的80%以上。美国、韩国、香港、台湾成为境外攻击源最多的国家和地区，其中来自美国的控制端主机个数高达2251个。教育行业信息系统涉及国家科研成果、公民个人信息等大量重要情报，一旦被境外组织获取将严重威胁国家安全和社会稳定。

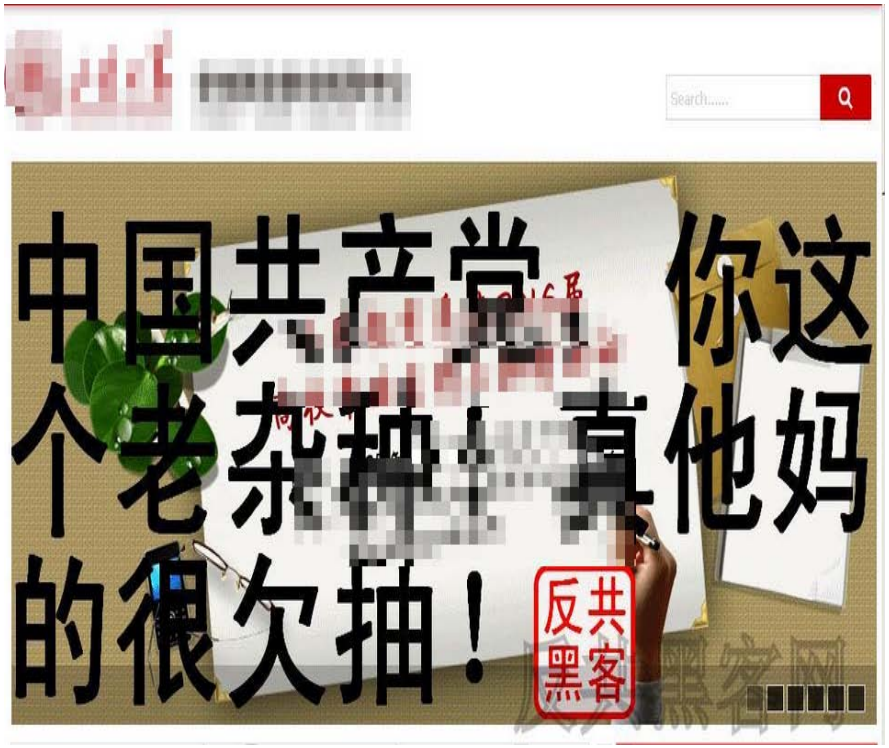


针对教育行业的黑客活动日趋活跃

反动黑客猖獗：专门针对教育行业、具有政治意识形态色彩的浅层攻击行为也日渐增多。

省内某高校就业指导中心网站遭“反共黑客”组织恶意篡改，网站首页被挂上反动宣传标语。随后，省内多个学校网站接连遭该组织攻击。

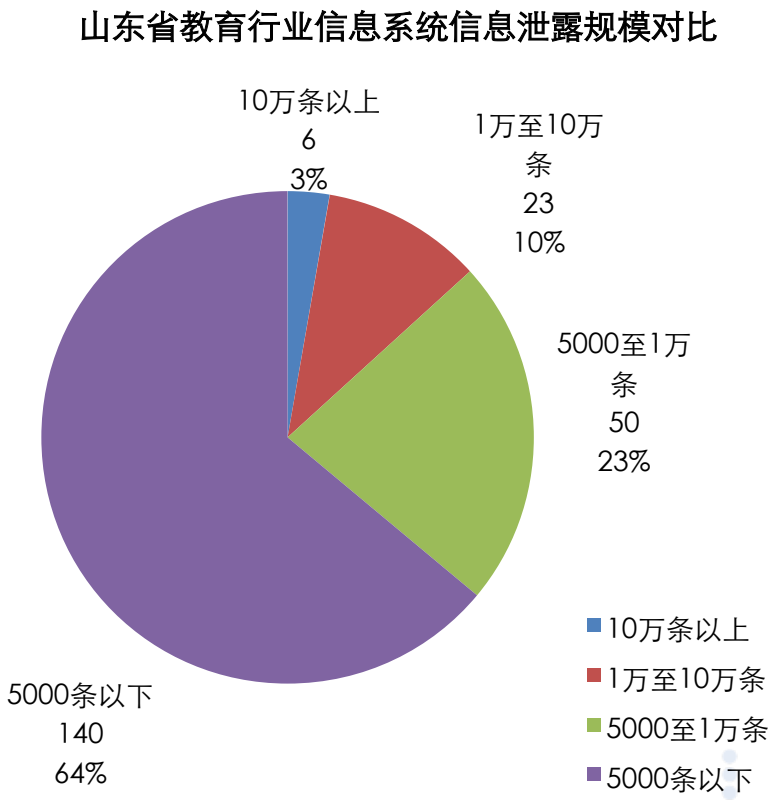
境外组织利用教育行业网站影响面广、管理相对疏松的特点，进行反动宣传和蛊惑，造成极为恶劣的社会影响。



山东某高校遭反动攻击

2 教育行业信息系统已成为个人和组织信息泄露的较大隐患

信息泄露风险上升：2016年以来，我省教育行业信息泄露风险和事件数量大幅增长，共计有195个教育类网站及相关信息系统存在信息泄露隐患，系统的信息数据泄露规模呈上升趋势。有6个信息系统的信息泄露规模在10万条数据以上，1万至10万条数据规模的达23个之多。面向教育政务、教育管理、教学科研等相关信息系统的信息安全防护工作刻不容缓。

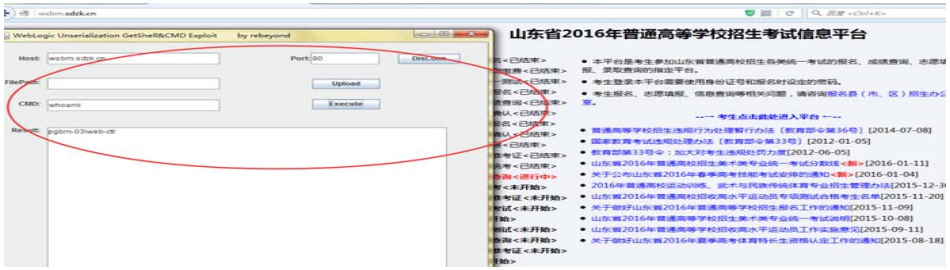


教育行业信息系统已成为个人和组织信息泄露的较大隐患

徐玉玉事件分析：2016年8月，我省临沂市18岁高考女生徐玉玉被诈骗分子以提供助学贷款为由，骗取了全部9900元学费，直接导致该女生两天后不幸猝死。案件调查显示，该案起因是黑客利用漏洞攻击某高考报名信息系统获取考生资料，并通过地下交易链贩卖给诈骗分子，从而帮助犯罪分子实施精准诈骗活动。之后，因网络信息泄露引发的徐玉玉式悲剧接连发生，折射出我省教育行业网络安全防护能力的不足，加强公民教育信息安全保护势在必行。

相关事件：

5月份，山东分中心发现并预警山东高考报名系统信息泄露漏洞，50万条考生信息泄露

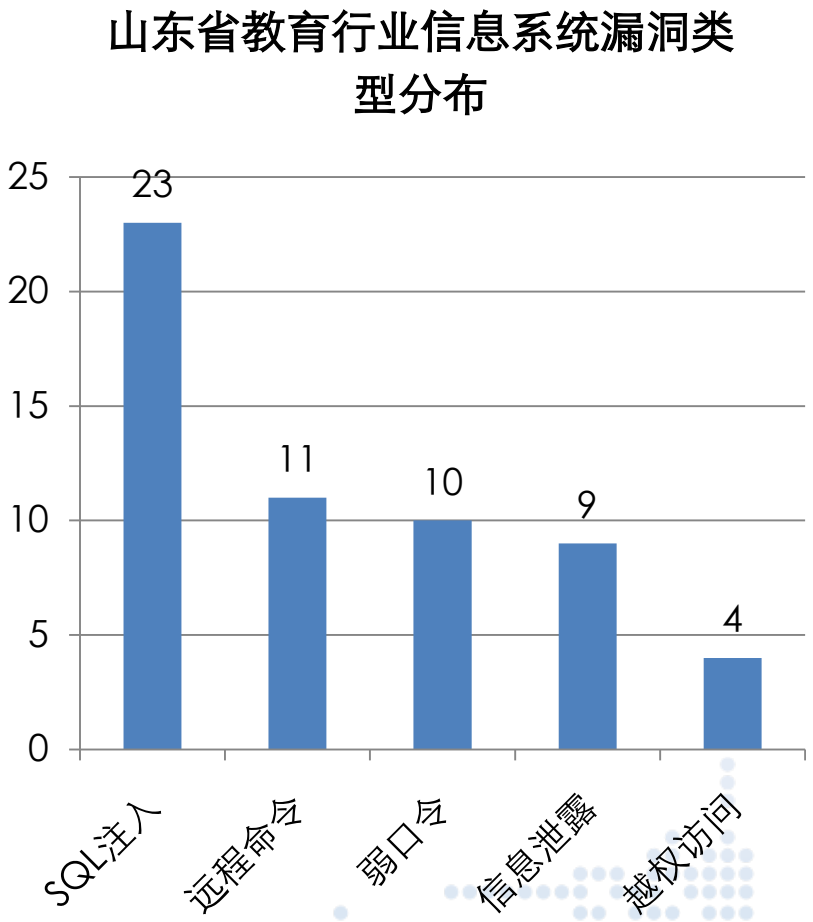


CHAR	CHAR	DATE	VARCHAR2	CHAR	CHAR	CHAR	CHAR
乔光远	1	1998-11-11 00:00:00	371482199811110337	201437148200023067	15053421487	山东省德州市禹城县辉馨佳园6#1单元402	齐鲁中学
赵倩倩	2	1997-03-29 00:00:00	370784199703290543		15163683178	山东省潍坊市安丘市景芝镇保元村	潍坊市体育运动学校
王群	1	1997-08-28 00:00:00	372321199708280250	201337010100033013	13805437967	山东省滨州市惠民县东景委庭5号楼2单元901	山东师范大学第二附属中
周琳玲	2	1997-11-06 00:00:00	370104199711061324	201337010100033021	13953137798	山东省济南市张庄路68号嘉苑城市之家17-1-202	山东省济南市第八中学
徐庆超	1	1994-02-05 00:00:00	372930199402055615	201337172800043070	15865777707	山东省东明县东明集镇团民王庄村468号	东明县东明集镇第二初级
殷新月	2	1997-12-03 00:00:00	372321199712039400	201337162123023022	18366822449	山东省滨州市惠民县大年陈镇于王口村	惠民县大年陈镇中学

KSH CHAR	XM VARCHAR2	SFZH VARCHAR2	KLDM CHAR	KM1 NUMBER	KM2 NUMBER	KM3 NUMBER	KM4 NUMBER	KM5 NUMBER	ZF NUMBER	TZF NUMBE
15370782112834	庄萍萍	370782199610214282	1	127	128	130	218	0	603	0
15370283110095	陶雯雯	370283199611192627	1	127	129	133	214	0	603	0
15370683110554	冠佳宝	370683199608040026	1	126	121	124	232	0	603	0
15371302130179	金童	371322199707070564	3	126	126	122	229	0	603	0
15371322110436	李金泽	220625199709142439	1	126	115	133	229	0	603	0
15370282110282	陈飞燕	370282199610164847	1	126	120	130	227	0	603	0
15371083110135	李宣豐	37108319970123902X	1	126	118	132	227	0	603	0
15370102110104	郑文琦	370112199707286846	1	126	118	132	227	0	603	0

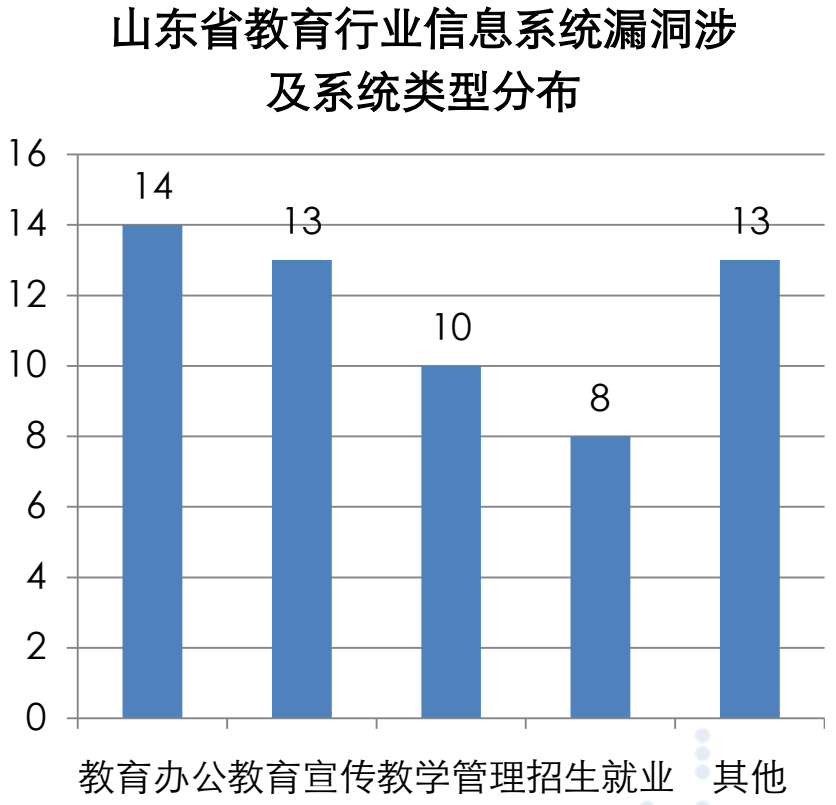
3 教育行业信息系统安全漏洞频发，技术防护能力薄弱

- **什么是漏洞：**漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，是影响信息系统安全的内在原因。经分析发现，前面提到的所有教育网络安全事件均由漏洞引发，无一例外。
- **漏洞问题频发：**2016年至今，我省教育行业网站及信息系统共发现各类安全漏洞59个，SQL注入漏洞、远程命令执行、弱口令等漏洞较多。



教育行业信息系统安全漏洞频发，技术防护能力薄弱

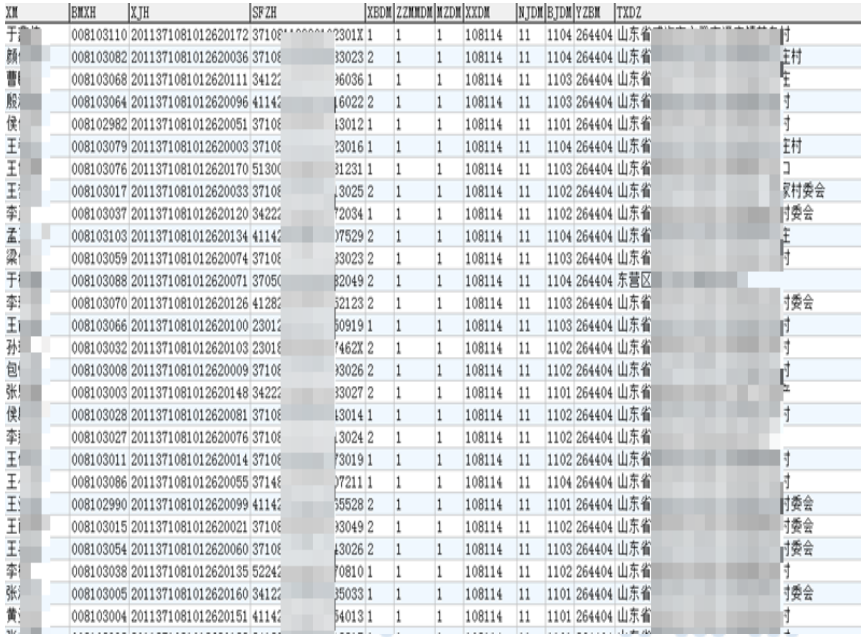
- **漏洞涉及系统类型分布：**按照漏洞存在系统类型来分，各系统存在漏洞情况分布较平均，教育办公类、教育宣传类、教学管理类相关系统存在漏洞较多。系统漏洞安全问题的存在，会造成重要教育数据（如学生个人信息、考试成绩等）被黑客恶意窃取，破坏系统的可用性和稳定性，严重的会危及正常教育教学秩序及社会稳定。



教育行业信息系统安全漏洞频发，技术防护能力薄弱

- **通用软件漏洞危害严重：**特别值得注意的是，一些通用应用系统框架，如Tomcat、OpenSSL、Struts2等，其行业应用多、使用范围广，如漏洞不能被及时发现和修补，将波及大量教育行业信息系统，需引起高度重视。

2016年初，省内某软件公司招生考试软件产品被发现Java反序列化漏洞，全省多个地市招考系统引发严重信息泄露风险，攻击者利用漏洞能够轻易进入招生录取系统内部，可任意下载数十万学生个人资料、考试成绩信息以及真实考卷等敏感数据，甚至具备篡改资料、修改分数等权限，一旦被不法分子利用，极易引发网络诈骗等案件。

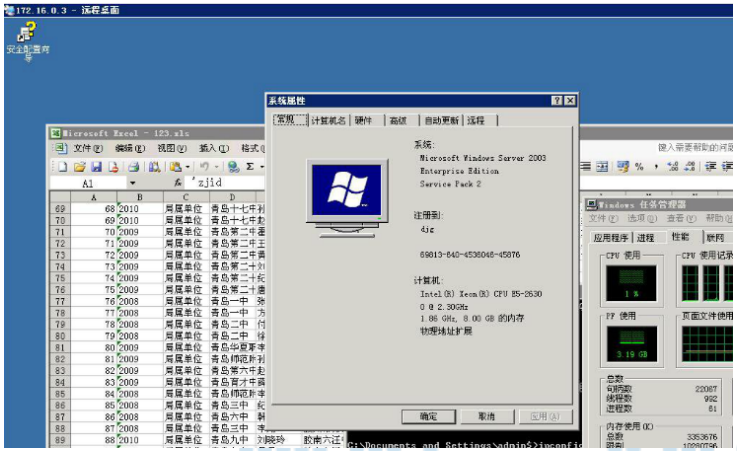


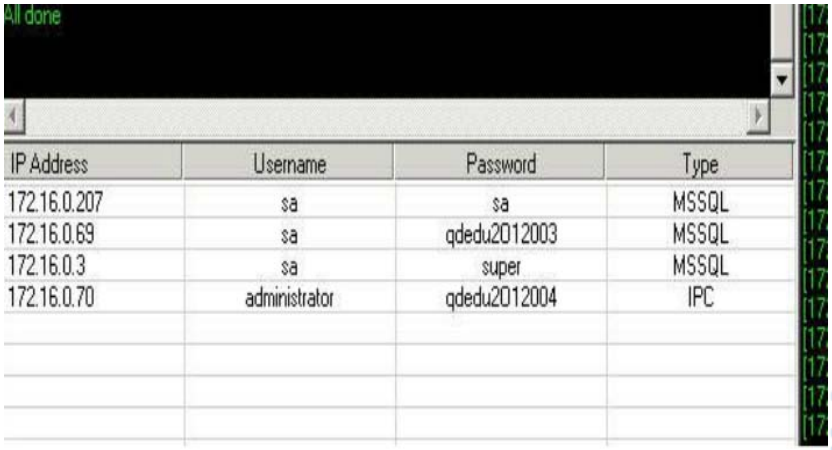
XM	BMXH	XJH	SFZH	XBDM	ZZMMDM	MZDM	XXDM	NJDM	BJDM	YZBM	TXDZ
于	008103110	20113710810126201	37108	1	1	1	108114	11	1104	264404	山东省
颜	008103082	20113710810126200	37108	2	1	1	108114	11	1104	264404	山东省
曹	008103068	20113710810126201	34122	1	1	1	108114	11	1103	264404	山东省
殷	008103064	20113710810126200	41142	1	1	1	108114	11	1103	264404	山东省
侯	008102982	20113710810126200	37108	1	1	1	108114	11	1101	264404	山东省
王	008103079	20113710810126200	37108	1	1	1	108114	11	1104	264404	山东省
王	008103076	20113710810126201	51300	1	1	1	108114	11	1103	264404	山东省
王	008103017	20113710810126200	37108	2	1	1	108114	11	1102	264404	山东省
李	008103037	20113710810126201	34222	1	1	1	108114	11	1102	264404	山东省
孟	008103103	20113710810126201	41142	2	1	1	108114	11	1104	264404	山东省
梁	008103059	20113710810126200	37108	2	1	1	108114	11	1103	264404	山东省
于	008103088	20113710810126200	37050	2	1	1	108114	11	1104	264404	东营区
李	008103070	20113710810126201	41282	2	1	1	108114	11	1103	264404	山东省
王	008103066	20113710810126201	23012	1	1	1	108114	11	1103	264404	山东省
孙	008103032	20113710810126201	23018	2	1	1	108114	11	1102	264404	山东省
包	008103008	20113710810126200	37108	2	1	1	108114	11	1102	264404	山东省
张	008103003	20113710810126201	34222	2	1	1	108114	11	1101	264404	山东省
侯	008103028	20113710810126200	37108	1	1	1	108114	11	1102	264404	山东省
李	008103027	20113710810126200	37108	2	1	1	108114	11	1102	264404	山东省
王	008103011	20113710810126200	37108	1	1	1	108114	11	1102	264404	山东省
王	008103086	20113710810126200	37148	1	1	1	108114	11	1104	264404	山东省
王	008102990	20113710810126200	41142	2	1	1	108114	11	1101	264404	山东省
王	008103015	20113710810126200	37108	2	1	1	108114	11	1102	264404	山东省
王	008103054	20113710810126200	37108	2	1	1	108114	11	1103	264404	山东省
李	008103038	20113710810126201	52242	1	1	1	108114	11	1102	264404	山东省
张	008103005	20113710810126201	34122	1	1	1	108114	11	1101	264404	山东省
黄	008103004	20113710810126201	41142	1	1	1	108114	11	1101	264404	山东省

教育行业信息系统安全漏洞频发，技术防护能力薄弱

典型漏洞安全事件

- **事件名：**省内某地教育局网站存在任意文件上传漏洞
- **引发影响：**可上传webshell，并渗透内网，获取十余台服务器权限，大量教师信息、学生学籍信息泄露

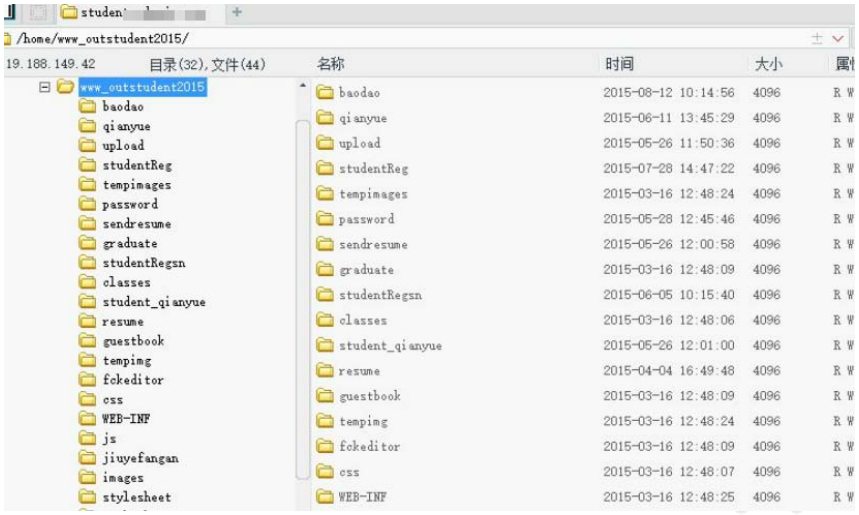




教育行业信息系统安全漏洞频发，技术防护能力薄弱

典型漏洞安全事件

- **事件名：**省内某毕业生就业平台存在弱口令漏洞
- **引发影响：**可利用弱口令登录系统，获取大量学生信息，并可上传webshell



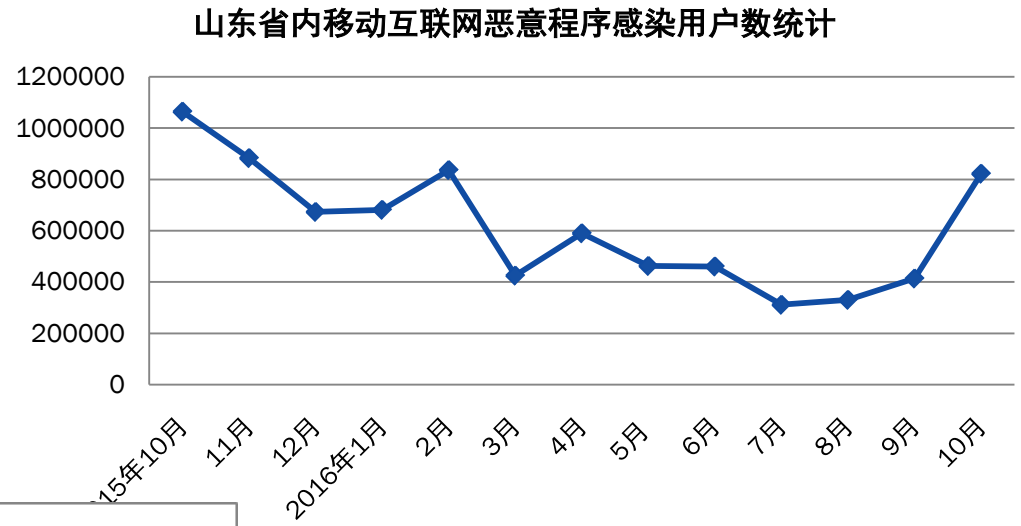
教育行业信息系统安全漏洞频发，技术防护能力薄弱

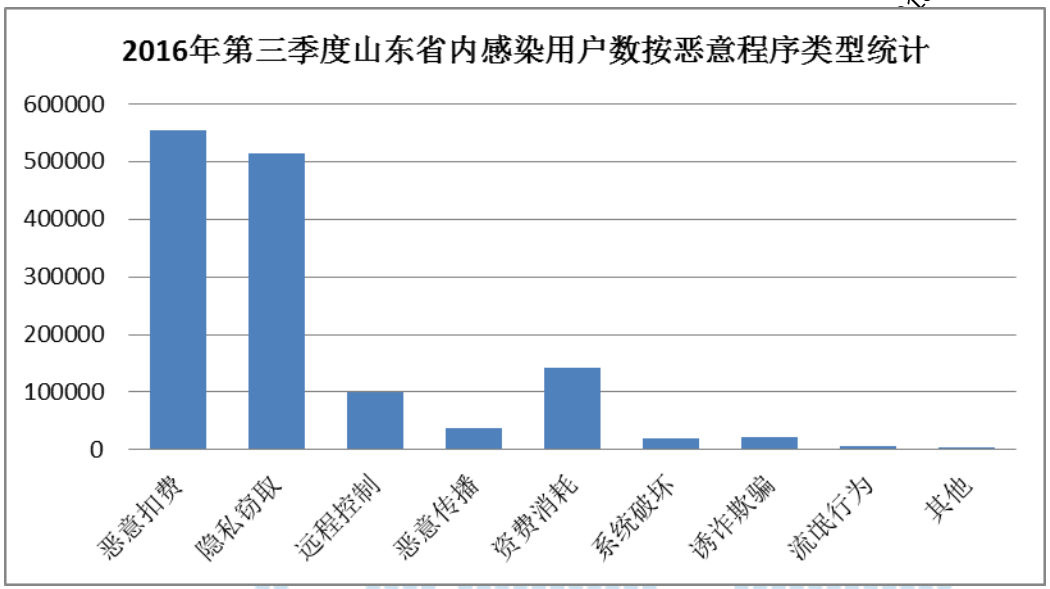
典型漏洞安全事件

- **事件名：**省内某重点高校网站存在信息泄露情况
- **引发影响：**被植入webshell，大量学生信息泄露

移动互联网终端安全

移动互联网终端安全问题





三，对策与建议

对策与建议

- **维护教育网络安全：**教育是立国之本，维护教育行业网络与信息安全，保障全省教育信息系统运行安全、现代化教育健康发展是各相关部门应尽的责任和义务。为了进一步加强教育行业网络信息安全管理，保障人民群众合法权益，亟需针对现状提出解决问题的方法。

对策与建议

1，提高认识，加强管理

有网络的地方，就涉及网络安全；

网络潜在的威胁和危险就在我们身边。

提高认识，加强管理

- 加强内部管理
- 提高网络安全防护能力
- 建立网络安全机构
- 建立健全网络安全工作机制
- 加强网络安全人员的培训教育

对策与建议

2.建立网络安全监测预警和应急协作机制

- **协同应对网络威胁**：教育行业信息化涉及面广、头绪多，网络安全工作艰巨而复杂。建议建立完善行业网络安全监测预警和通报处置工作机制，并与国家相关管理和技术部门沟通协作，实现网络安全威胁信息共享和应急能力联动，有效应对网络攻击行为，促进全省教育行业网络安全和信息化工作协调发展。

建立完善网络安全合作机制

事件监测与处置

SDCERT网络安全监测与分析管理平台

		完整时间	受控IP_点分式	受控端口	控制IP_点分式	控制端口	返回值
	ux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33572	targetHost=9.4.8.355;payload=\01\00\0C
	ux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33564	targetHost=9.4.8.355;payload=\01\00\0C
	ux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33576	targetHost=9.4.8.355;payload=\01\00\0C
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33603	targetHost=9.4.8.355;payload=\01\00\0C
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	221.0.90.204	3063	23.234.29.99	12214	targetHost=117.21.219.74;payload=\01\0
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33560	targetHost=9.4.8.355;payload=\01\00\0C
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33589	targetHost=9.4.8.355;payload=\01\00\0C
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33590	targetHost=9.4.8.355;payload=\01\00\0C
	僵尸网络-其他协议-DDoS.Linux.BillGates-攻击包	2016-10-31 23:59:59	122.224.50.154	13313	123.234.47.9	33549	targetHost=9.4.8.355;payload=\01\00\0C

CERT综合监测平台

共同建立合作机制:

- 事件通报机制
- 网络安全预警机制
- 事件处置机制
- 网络应急响应机制

促进整个教育行业的网络安全工作健康稳步发展

“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。面对当前我省教育系统复杂严峻的网络安全形势，我们要保持清醒头脑，进一步增强责任感和使命感，采取有效措施，维护好我省教育行业网络信息安全，促进教育事业持续健康发展。”

谢　　谢！

宋江静
18653196827
sdcert@cert.org.cn