信息化摘编 NO.12

2023-04-18 东师信息化办

本期导读

汇 高校信息化新业态

聚 兄弟院校之优长

高校信息化新业态

一．高校智慧校园网络安全管理体系

随着高校智慧校园建设的步伐逐步加快，面临的安全问题也越发严重。当前高校急需建立完善的网络安全管理体系，提升技术管理人员能力，降低网络安全风险。

1．打造网络安全管理体系

江南大学信息化建设与管理中心通过制度建设，四级管理（统筹管理、技术支撑，落实网络安全主体及个体管理职责）建立起了完善的网络安全管理体系。

2．技术赋能，提升网络安全能力

加强网络安全队伍建设，结合网络安全教育培训，形成线上线下相结合、多维度的高校网络安全教育培训体系，提高网络安全意识、网络安全管理能力和专业技能，提升整体网络安全能力。

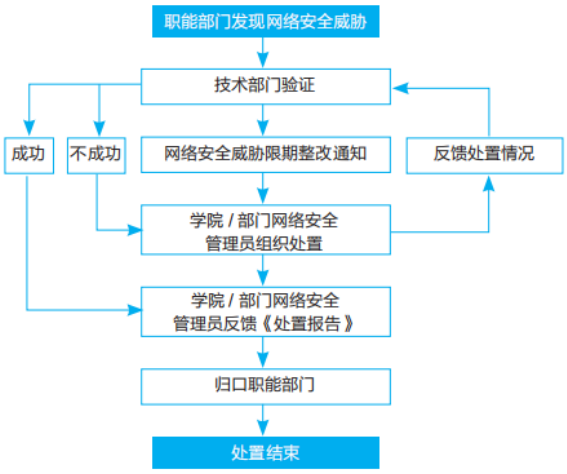
3．技术保障，降低网络安全风险

通过网络安全等级保护，规范信息化的网络安全建设与管理，治理网络安全风险。

第一，等级保护，规范信息化建设与管理。围绕“1 个中心”管理下的“3 重防护”开展网络安全等级保护工作，将网络安全等级保护与智慧校园信息化建设的全生命周期管理相融合，严格按照网络安全等级保护 2.0 的要求进行网络安全建设与管理，保障智慧校园建设。

第二，网络资产治理，提供基础数据。建立网络资产治理平台，实现“资产发现—备案审核—漏洞发现—加固整改—事件处置”安全闭环，形成全校一本账、学院/部门一本账、信息系统责任人一本账的分级管理模式。

第三，风险治理，降低网络安全威胁。高校网络安全风险治理通过网络安全监测、预警、处置等方式，降低网络安全威胁。校内通过漏洞扫描、渗透测试等手段开展自主监测，再结合各级网络安全管理单位的监测成果，多角度保障高校网络安全。同时，依托良好的组织结构和准确的网络资产数据，从“发现、验证、通报、处置、再验证、结束”，形成一套行之有效的网络安全威胁处置流程，见下图：



网络安全威胁处置流程

4．工作宣传，提升网络安全影响

以网络安全工作简报的形式，向学校各级领导定期汇报当前国内外网络安全环境、学校网络安全态势和网络安全工作成果，提升网络安全工作影响力。

（信息来源：https://mp.weixin.qq.com/s/O1K9GDYDNbBxWQk0YaUAnA）

二．如何保障高校虚拟卡的安全应用

随着虚拟卡大规模应用，新一代一卡通系统的信息安全问题已成为重要关注点。

由于虚拟卡系统应用功能相对庞杂，在校园网中与数据中心进行数据交换的同时，通常也会与银行、支付宝、微信等第三方采用不同对接方式，需要一定程度上对互联网开放。其安全防护可根据虚拟卡业务进行功能分类和系统边界设计。虚拟卡安全防护设计的重点可考虑纵深防御和安全强健性两方面：

1.纵深防御

纵深防御在信息安全模型中具有重要意义，保护区域边界、计算环境、网络基础设施等多个重要位置，是安全规范的核心组成部分。主要包括：

①虚拟卡专网物理设备的保护（数据库防护、存储设备防护）

② 虚拟卡系统计算环境防护（虚拟卡应用软件防护、虚拟卡相关 Web 服务防护、数据交换服务防护）

③ 纵深防御（互联网攻击防范、虚拟卡专网防护）

设计在线交易数据传输网络采用 VLAN 隔离，师生 Client 设备直接通过校园网进行，业务请求通过指定服务器入口转发、反馈，以完成交易流程。

VLAN1：虚拟卡服务端集群采用 DMZ 区与后勤消费刷码设备线下设备，利用“虚拟卡专网主干网备用光纤+专网区的交换机”设置隔离端口，整个通讯链路采用新分配 IP 地址段。

VLAN2：虚拟卡服务端集群采用 DMZ 区内部隔离，聚合支付平台和虚拟卡系统之间相互隔离。

VLAN3：财务数据流部分，聚合支平台与支付宝、微信、银行采用不同对方式和聚合支付平台对接，校外及校内第三方应用与虚拟卡平台等相互逻辑隔离。

④虚拟卡系统对外服务接口安全防范

虚拟卡接口对与一卡通业务无关的通路直接关闭。

在线交易接口：第三方应用与虚拟卡平台通过 HTTP 方式进行通讯，以 POST 方式发起服务调用，一卡通平台接收到请求后，进行相应的业务逻辑判断，通过 HTTPS 中的 response 参数返回。

交易接口加密：采用 CA 中心签发的证书，增强客户账户安全性，并对不同用户给予不同资源访问权限。

数字证书以网络数字加密传输电子凭证的方式有效地对账户使用者进行确认，帮助新一代一卡通确认使用者是否合法。

在密码技术方面，实现支持 SSL 加密传输技术，对用户的关键信息进行加密，防止木马程序截取键盘记录。

2.安全强健性

针对虚拟卡系统的高价值特征，需要加强安全强健性，重点对如下四个层次进行防护：

① 虚拟卡系统难攻破。通过利用防火墙、WAF、操作系统安全配置，结合访问源接入控制，落实尽可能小的开放原则，并对行为进行控制。利用网安设备拦截典型攻击行为，并利用大数据算法进行交易日志、访问日志特征提取，进一步提升虚拟卡系统安全性，实现难以攻破的目的。

② 交易数据难窃取。数据库文件的保护，禁止数据文件直接放在 Web 目录；防止拖库，由于各种 Web 应用漏洞，特别是发生高危的零日漏洞时，Web 应用很容易遭到拖库的危险；Web 服务器保护，由 Web 服务器的操作系统安全设置来实现；数据库保护，合理设置数据库 Schema、表空间管理、读写权限设计等。

③ 敏感数据难利用。通过密钥管理体系分发设备密钥，后台选择加密算法对敏感数据加密，使得攻击者即便获取数据也难以利用。需要重点对交易数据传输加密以及数据库敏感字段加密。

④ 业务数据难篡改。通过增加数据库审计功能，业务层、数据保护（业务数据保护），设置合理数据库全备期限，以及一卡通专用交易审计软件，来发现篡改行为，保留篡改证据。同时还需要考虑 CDP（Continuous Data Protection）来解决非法的删改数据问题。为应对数据篡改难以及时发现的问题，通过自动备份方式每天增量数据备份并历史存档。

由于虚拟卡系统相对开放的特征，面临各种隐患与风险，通过梳理虚拟卡系统需要保护的资源，确定重点防范边界，设计合理的纵深防御方案，评估反馈安全强健性，防范数据泄露与篡改行为 等，能较好地保障虚拟卡系统的信息安全和稳定运行。

（信息来源：https://mp.weixin.qq.com/s/j-5FAhy3DS6Spr96NgaB0A）

兄弟院校之优长

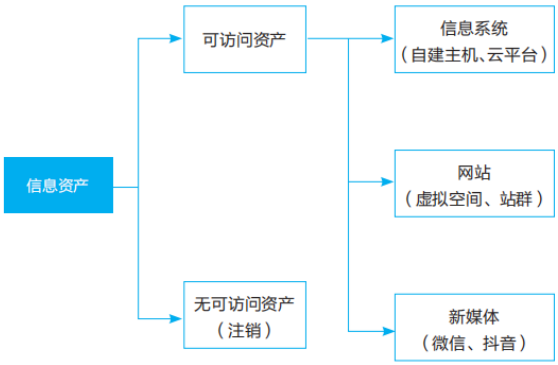
一. 高校数据安全防护实践

在高校信息化建设和发展过程中，业务系统和数据中心汇聚了大量数据，并在多个部门和多个系统之间流通、共享和分析，导致高校数据资产不清晰，给数据安全管控和防护工作带来困难。本文结合武汉大学的数据安全实践，对敏感数据安全防护和动态脱敏提出了一套可行的解决方案。

1. 信息资产梳理

武汉大学信息资产主要包括校内网站、信息系统和新媒体平台，这些资产以域名、IP 和新媒体平台账号的形式记录备案，各类网站和信息系统，均是由学校各院系、职能部门、研究机构等自行建设开发，并提交纸质备案资料，经学校宣传部和信息中心分别审批后上线。

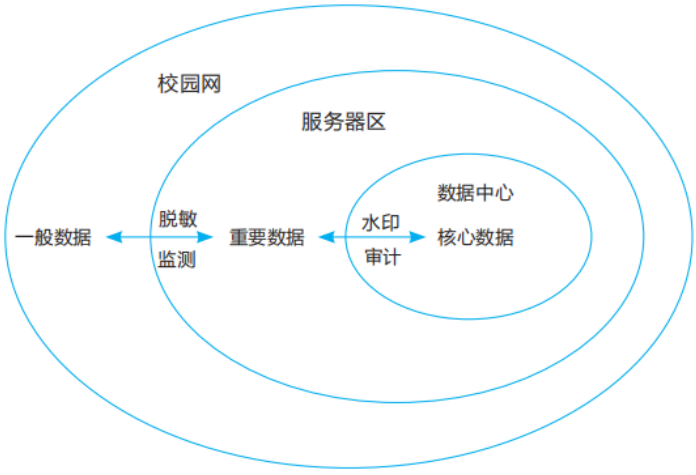
信息资产梳理流程图如下：



2. 数据资产分类分级

①根据网络边界分类保护

高校各业务系统的核心数据集中于信息化职能部门的数据中心平台，随着机房的升级和云平台的部署，一般会形成集中的服务器区，各单位和业务部门则在校园网管理信息系统。可根据网络边界可以划分核心数据、重要数据和一般数据 3 个区域。对于数据中心的核心数据，通过部署数据库防火墙、静态脱敏或水印等技术手段来严格保护；对于服务器区可识别的重要数据，利用数据泄露防护 DLP（Data Leakage Prevention）系统检测出对应的 IP 地址和域名，然后根据信息资产管理数据确定对应的系统，反向代理部署数据脱敏系统 DMS（Data Masking System）进行重点保护，网络边界分类保护示意图如下：



②根据系统等保护定级分级保护

高校信息系统分为校务管理、教学科研、招生就业、综合服务，4 大类 23 种具体业务类型。其中建议安全保护等级定为三级的有 6 种业务类型，其余为二级。6 种具体业务类型主要涵盖科研、招生、门户、一卡通等方面。结合高校实际情况，可以将校园一卡通、科研管理系统、财务管理系统的数据严格保护，通过部署或限制在校园内网。

3．数据安全防护策略

①数据中心部署数据库防火墙

②利用数据泄露防护（DLP）系统

武汉大学大多数学院和单位的业务系统都集中在信息中心服务器区，对服务器区中的重要数据，利用数据泄露防护（DLP）系统采集可检测敏感数据的位置。

以武汉大学部署的数据泄露防护系统为例，制定策略采集外传敏感信息系统的步骤如下：

首先将银行账号、身份证号、手机号这 3 类方便识别的敏感数据设置为监测对象，然后根据泄露条目数量分为低、中、高 3 类告警事件，9 种数据对象，数据对象分类参见下表：

分类名称	分类说明
身份证号低危	身份证号出现次数小于 5 次
银行卡号低危	银行卡号出现次数小于 5 次
手机号低危	手机号出现次数小于 5 次
身份证号中危	身份证号出现次数大于等于 5 次，小于 20 次
银行卡号中危	银行卡号出现次数大于等于 5 次，小于 20 次
手机号中危	手机号出现次数大于等于 5 次，小于 20 次
身份证号高危	身份证号出现次数大于等于 20 次
银行卡号高危	银行卡号出现次数大于等于 20 次
手机号高危	手机卡号出现次数大于等于 20 次

其次，根据上述分类数据对象制定相应的安全策略，如审计或邮件报警。

③部署数据脱敏系统（DMS）

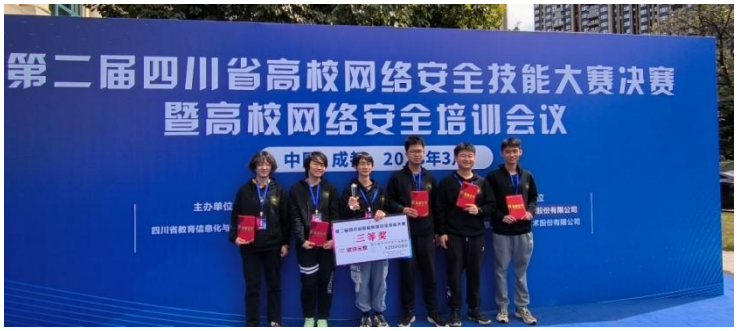
重点关注对敏感数据外传进行精确的动态脱敏。通过数据泄露防护（DLP）系统获取服务器 IP、URI，利用反向代理部署网页动态脱敏系统，网页动态脱敏支持按用户、菜单、URI、API 接口制定策略，无需安装客户端而且不影响数据库，在监测到敏感数据后进行实时的动态脱敏，从而解决高校用户和管理员随意下载敏感数据，运维和外包人员恶意盗取敏感数据的安全隐患。

高校信息化管理部门在制定数据防护策略的同时，需加强宣传，提高师生的数据安全保护意识，共筑数据安全防线。

（信息来源：https://mp.weixin.qq.com/s/jsbk5Df6xaTgeVwZmy6I1w）

二．电子科技大学信息中心带队参加第二届四川省高校网络安全技能大赛决赛并获奖

3 月 23-24 日，四川省教育厅在成都举办了第二届四川省高校网络安全技能大赛决赛暨高校网络安全培训会议。电子科技大学信息中心老师带领的 CNSS 战队在网络安全技能大赛（本科组）决赛中名列第六，获得三等奖。



（信息来源：https://info.uestc.edu.cn/info/1014/2954.htm）

策划：李向龙　　摘编：刘玉燕　　微信发布：张丽丽　　网站发布：郭思佳