大数据时代高校数据安全需求与挑战

针对大数据环境下的高校数据安全问题，我们建议在规划、建设、运行过程中，同步考虑“把数据关进笼子，让数据访问在阳光下进行”的数据安全策略。

文 / 朱圣才

高校数据安全需求

大数据时代背景下，高校信息化产生的各类数据成为高校最重要的资产之一。然而，高校的网络信息安全建设工作没有达到银行、证券、金融等行业的高投入和大规模建设，高校的数据安全建设工作在整个网络信息安全建设中没有得到足够的重视，在数据收集、存储、传输和使用过程中缺乏必要的防护措施，使得大量敏感信息、个人信息的安全性无法得到有效保障。高校在推进业务系统整合、数据中心建设、数字校园与智慧校园建设、数据分析与挖掘等大数据建设的同时，必须坚持安全与发展并重的方针，为大数据发展构建安全保障体系，在充分发挥大数据价值的同时，解决面临的数据安全和个人信息保护问题。

如何保障数据的机密性、完整性、可用性，对于教育行业来讲，特别是高校，有着更深层次的意义。高校有着大量的科研成果、学术资料、教职工信息以及海量的学生信息，是数据泄露的相对高发地带。因此，高校需要切实加强安全防护以保障高校数据安全。

当前高校数据安全面临的挑战

老旧系统带来的数据攻击

早期的老旧系统，明文传输、明文存储较为普遍，并且系统漏洞较多，加之无人运维，常见的 SQL 注入漏洞、文件上传漏洞、弱口令、第三方中间件漏洞等这些安全漏洞均会造成服务器权限被获取，数据库被攻击等网络信息安全事件，危害非常之大。从目前教育主管部门的漏洞通报来看，多数安全漏洞及安全事件都发生在老旧系统之中。对于老旧系统的攻击，以及攻击带来的数据安全问题是比较常见的，如何处理好这些老旧系统是关键。通过这些简单的攻击手段就能达到攻击目的的攻击行为基本都是零成本，这种零成本攻击造成数据泄露也是高校最为常见的情况。

大数据带来的数据集中

大数据时代的到来，给数据分析挖掘奠定了丰富的数据基础，这个基础就是数据集中，数据集中是指将数据集中到中心一点以便于数据分析挖掘。这种数据的高度集中在给数据分析挖掘带来效益的同时对数据安全的危害也是可见的。身处大数据时代，高校也在进行一系列的大数据整合工作，建设各自的数据中心，将数据进行集中存储和管控。业务流程的整合实现了各自高校各项业务的优化，优化的本质是数据分析挖掘的结果。这些优化后的成果如果没有得到更好的保护，产生的副作用也是巨大的。

另外，大数据带来的数据集中需要防范 APT 攻击行为，APT 攻击是黑客用客户发动的网络攻击和入侵行为，是一种蓄谋已久的网络攻击行为，APT 攻击以窃取核心数据资料为目的，对大数据应用产生重大安全威胁。APT 攻击具有很强的隐蔽性，传统的防护策略并不能检测到，很难被发现。

云计算带来的数据存储

云计算是一种服务模式，通常被分为包括基础设施即服务、平台即服务、软件即服务三种模式。云计算平台可以分为包括以数据存储为主的存储型、以数据处理为主的计算型、以计算和数据存储处理兼顾的复合型三种类型平台。各高校实际使用情况显示，各高校目前基本都建立了自己的以数据存储为主的私有云平台，但是这种用于数据存储的私有云平台产品基本都是由各厂商提供，并非各高校私有技术，这些用于数据存储的云计算平台的安全性如何未知；抛开这些未知数，目前还有很多高校使用了大量的公有云平台，将各自的业务系统部署在商业的公有云上，数据、应用均在外部云上，这些数据的安全性也有待商榷。

系统外包带来的数据控制权

系统外包在各行各业都有，教育行业、高校也不例外，各式各样的系统通过外包方式进行开发维护，各外包公司掌握着各类系统的应用程序源代码、服务器权限、数据库权限等核心信息。例如高校普遍使用的财务系统、人力资源系统、招生系统、学籍管理系统、科研管理系统等等，多数都使用信息化方式外包或者通过购买产品进行运行，如果对这些信息系统运维外包过程管理不严，极有可能造成重要数据泄露；同时在进行外包运维过程中，运维工程师的技术水平良莠不齐，有可能由于操作不慎造成数据丢失、损坏等。这种过度外包依赖对数据的安全是不可控的，各高校需要自主掌握数据的控制权。

数据资源开放共享与安全保护矛盾

大数据时代智慧校园建设对数据的需求越来越高，需要精准的数据信息作为支撑，例如，可以通过学生的个人消费情况，梳理一些特有的功能进一步优化校园卡服务。然而，数据信息作为一种资源，更是一种资产，需要进行保护，这种对数据信息的挖掘底线需要制定，总之，保护和需求的矛盾越来越显现。

针对大数据环境下的高校数据安全问题，我们建议在规划、建设、运行过程中，同步考虑“把数据关进笼子，让数据访问在阳光下进行”的数据安全策略。

大数据时代，是机遇与挑战并存的时代，高校数据安全防护工作任重道远，需要有效的技术手段和相关政策法规并举才能保障大数据时代的数据安全与个人信息问题，需要技术创新与制度创新才能不断引领大数据时代的安全工作。CEN

（作者单位为华东师范大学）

提升数据安全四大对策

吴海燕
清华大学信息化技术中心

数据安全并非单一技术或者管理措施即可解决的复杂问题，需通过整体的信息安全保障体系的设计与实施，综合考虑技术和管理各方面的措施。

清华大学信息化技术中心吴海燕认为，应从以下几个方面入手解决高校数据安全问题。

第一，建立数据分级防护策略

数据分析防护策略是核心的数据安全策略。建议根据数据的保密性、完整性等安全属性，根据相关法律法规要求，根据数据对于学校的重要程度，对数据进行安全级别划分，使数据能够得到适当的安全防护。建立数据分级策略需要考虑如下几个方面的问题：1. 数据的分级原则，考虑到可操作性，建议高校数据分为三个或四个安全级别，如可划分为公开数据、一般业务数据、内部敏感数据、个人数据四个安全级别；2. 数据管理与操作的各个角色设置；3. 各级别数据的防护措施等方面的内容。对于不同级别的数据，还要明确其在数据访问控制、存储、传输、备份、审计等方面的要求。

第二，严格数据的访问控制

包括通过防火墙实现网络访问控制、通过主机安全加固强化主机访问控制、通过数据库加固限制数据库访问控制，通过 Web 应用的安全设计与开发防止黑客通过 Web 应用漏洞获取敏感数据。

第三，探索尝试数据加密与一致性校验技术

以散列的方式加密存储口令类不需要解密的数据是较成熟的解决方案，但对于敏感数据（如科研经费等数据）的可逆加密目前国内外高校都在探索中。清华大学采用了 PKI 相关的技术实现了对招生数据的数字签名和定时验签，有效地提升了招生数据的完整性。

第四，实施数据库审计

安全审计是通过测试信息系统对一套确定标准的符合程度来评估其安全性的系统方法。安全审计根据一定的安全策略记录和分析历史操作事件及数据，发现能够改进系统性能和安全的地方。对数据库操作进行审计的关键在于审计策略的设定，审计策略设得宽泛会导致审计数据过多，而审计策略设得过为严格则会造成审计数据不全，需要进行适当的平衡。CEN