高校网站运维队伍建设之道

高等院校在网站安全保障过程中面临安全工作人员少、安全工作可见性差、攻防双方对比不对称、安全工作投入无保障等困境，解决这些困境，管理先行。

文 / 王宇 温占考 吴炜鑫

“技术与管理并重”、“建设与运维并重”是信息安全建设的两个基本原则，强调的是建立和实施安全标准体系，在信息系统建设的全过程中严格按照管理体制执行技术要求。随着信息安全威胁的涉及领域不断扩展和程度不断提升，传统的类似“瀑布模型”层次化的强调“七分管理，三分技术”的信息安全理念已经受到严峻挑战，借鉴信息安全业界以“攻防实战对抗”为核心、以“增加攻击成本”为目的的强调“七分技术，三分管理”的信息安全建设理念成了大势所趋。高等院校在网站安全保障过程中面临安全工作人员少、安全工作可见性差、攻防双方对比不对称、安全工作投入无保障等困境，在立足传统的安全标准体系制度建设的基础上，在现有条件下应该重点借鉴信息安全业界理念和加强自身人员队伍建设。

网站管理组织结构

高等院校所属网站的管理组织结构如图 1 所示，主要由信息管理部门、技术支撑部门和校内业务部门构成。部门分类关注的是承担的具体职能属性，根据部门职能可以在每所高等院校中找到对应的二级部门，参见表 1 示例。

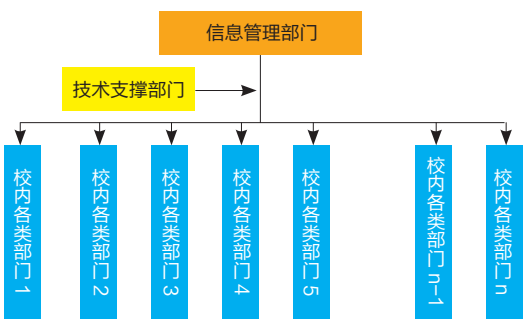

图 1　高等院校所属网站的管理组织结构

信息管理部门，负责制定学校网站建设与管理的相关制度，监督和管理校级别对外信息发布，对学校相关的所有域名和信息系统进行备案和管理，领导和组织网站安全保障工作，领导和组织包括信息安全等级保护的信息安全相关工作。

技术支撑部门，为信息管理部门和校内各类部门提供专业的网站规划、设计、建设和运维的技术支撑，建设和运维门户网站，为校内各类部门提供网站群系统或服务托管环境，组建跨网络管理、信息服务和用户支持的信息安全协调小组统一支持学校网站安全保障，提出和监督实施学校网站安全保障相关技术要求。

校内各类部门，根据学校网站建设与管理制度以及相关安全保障要求，负责本部门相关网站系统的规划、设计、建设和运维。

人员队伍建设建议

网站安全保障相关的人员队伍建设，主要是指学校技术支撑部门的专业信息安全人员队伍的建设，以及校内各类部门的信息安全联系员的组织和培训，重点是前者。对于网站安全保障的人员队伍建设提出以下建议：

1. 技术支撑部门要打破安全工作的部门界限，组建跨网络管理、信息服务和用户支持的信息安全协调小组统一支持学校网站安全保障，确定专职的信息安全负责人，并在内设部门内确定对口安全支援人员。

2. 技术支撑部门内部要将网站安全保障工作作为与网络建设、系统开发、用户服务等同等重要对待，保障资金和项目支持，提供足够的人员保障。

3. 技术支撑部门的安全协调小组要全面指导和协助信息安全工作的各个环节，如帮助用户服务进行用户安全服务与支持，协助设施运维加强数据中心安全建设，协助系统开发规范安全应用开发流程，规范运

行管理交换路由设备安全设置等。

4. 技术支撑部门要组建信息安全应急响应小组，定期对学校相关网站环境进行外部安全检查，跟踪安全业界动态，制定网站安全事件应急响应和处置预案，定期进行应急演练和攻防训练，提升网站安全应急事件处置能力。

5. 技术支撑部门要培养自身安全人员与采购专业安全咨询服务相结合，做好学校顶层设计，规划建设完整的安全保障体系，积极对外参与安全学术交流，加强和国内外安全组织机构的密切联系与合作，充分发挥学生力量辅助学校安全工作。

6. 技术支撑部门要配合信息管理部门和校内各类部门，组建信息安全联系员队伍，并提供足够的网站信息安全知识培训和流程支持。CEN

（作者单位为东北大学网络中心）

表 1 高等院校网站管理组织结构示例

部门类型	职能属性	高等院校部门示例
信息管理部门	负责制定学校网站建设与管理的相关制度	信息化建设办公室、宣传部
	监督和管理校级别对外信息发布	党办、校办、宣传部
	对学校相关的所有域名和信息系统进行备案和管理	信息化建设办公室、宣传部
	领导和组织网站安全保障工作	党办、信息化建设办公室
	领导和组织包括信息安全等级保护的信息安全相关工作	党办、保密办、信息化建设办公室
技术支撑部门	为信息管理部门和校内各类部门提供专业的网站规划、设计、建设和运维的技术支撑	网络信息技术部门（如网络中心、信息中心、网络信息中心、计算中心、现代教育技术中心等）
	建设和运维门户网站	
	为校内各类部门提供网站群系统或服务托管环境	
	组建跨网络管理、信息服务和用户支持的信息安全协调小组统一支持学校网站安全保障	
	提出和监督实施学校网站安全保障相关技术要求	
校内各类部门	根据学校网站建设与管理制度以及相关安全保障要求，负责本部门相关网站系统的规划、设计、建设和运维	学院、部处、教学科研组织等

网络可用性和可靠性

在每一次故障发生的时候，其实都是伤害了我们的用户，内部的表述就是可用性或者质量。因此我们必须要足够的重视，那到底什么是可用性和可靠性？影响可用性的因素有哪些？

可靠性是在给定的时间间隔和给定条件下，系统能正确执行其功能的概率。可用性是指系统在执行任务的任意时刻能正常工作的概率。先来看一些指标定义：

1. MTBF——全称是 Mean Time Between Failure，即平均无故障工作时间。就是从新的产品在规定的工作环境条件下开始工作到出现第一个故障的时间的平均值。MTBF 越长表示可靠性越高，正确工作能力越强 。

2. MTTR——全称是 Mean Time To Repair，即平均修复时间。是指可修复产品的平均修复时间，就是从出现故障到修复中间的这段时间。MTTR 越短表示易恢复性越好。

3. MTTF——全称是 Mean Time To Failure，即平均失效时间。系统平均能够正常运行多长时间，才发生一次故障。系统的可靠性越高，平均无故障时间越长。

可用性 Availability = MTBF / (MTBF + MTTR)，一般我们都是用 N 个 9 来表达系统可用性，用宕机时长来说更好理解，如果以全年为周期（24 × 365=8760 个小时），3 个 9(99.9%) 就意味着全年宕机时长是 525.6 分钟，4 个 9(99.99%) 是

52.6 分钟，5 个 9（99.999%）是 5 分钟。

影响可用性的因素非常的多，但是可以从几个维度去看，人与组织、流程、技术和业务管理等四个维度。

1. 人与组织

领导是否重视 IT？是否重视运维？组织是否已经认识 IT 带来的价值，把 IT 当作自己的一个核心能力来看待？是否把面向用户的业务能力和 IT 能力很好的对接？是否建立起用户质量的组织文化？等等。

2. 流程

流程是梳理多个角色自己的关系和职责。我们第一要去看流程在面对故障的是否起到了积极的作用，比如说能够确保故障信息的准确送达，同时保证处理人的角色和职责是清晰的。其次不断去检查流程是否可以自动化驱动，而非人为驱动。我们最终希望形成一个自动化、标准化的流程，这样的流程不容易被异化，且能保证预期执行结果一致。

3. 技术

很多时候大家看到的技术是运维技术，其实对于互联网业务来说，对其高可用的影响，必然是业务 IT 技术架构，因此在其中需要遵循很多原则，有一些原则需要有普适的参考价值。比如说服务降级、灰度发布、过载保护、服务公共化等等。这些方法论是否已经融入到研发和运维的架构设计哲学之中？现实是产品功能需求优先，而非可运维性优先，可运维性最终就是业务的质量。

4. 业务管理

把 IT 能力最终都业务能力看板化，转换成多个业务指标，比如说质量、可用性、用户体验、用户满意度、成本等等，有了这些业务导向性指标，才能把 IT 能力和业务更好地对接起来。否则很容易在组织内，形成“IT 是支撑部门”认识，而非创造价值部门。这一点还有一个重要性，就是让 IT 部门也要足够地认识到，他们的能力直接和业务相关，需要增强业务敏感度。