高校网络安全工作四大要点

网络安全是标准的提高，是成本的对抗。在可控的成本下，首先做好安全防护，提高攻击成本。

文 / 郑海山

党委（党组）网络安全工作责任制

2021 年 8 月 4 日，《人民日报》头版发布《中国共产党党内法规体系》一文。同时，《中国共产党党内法规汇编》公开发行，收录了《党委（党组）网络安全工作责任制实施办法》（以下简称《实施办法》）。《实施办法》的公开发布对厘清网络安全责任、落实保障措施、推动网信事业发展产生巨大影响。《实施办法》提到，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。《实施办法》还要求把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度。

高校应当落实党委（党组）网络安全工作责任制，成立网络安全和信息化领导小组，加强对学校网络安全与信息化建设的统筹领导。应当定期举行以领导小组组长和主要成员参与的会议，可按季度召开会议，应每年召开网络安全专题会议。年初应当制定和发布网络安全年度工作要点，年中可配合属地监管部门完成网络安全自查和整改，年末形成网络安全年度工作总结。

高校应当开展监测、预警和通报工作，制定网络安全事件应急预案，开展网络安全事件应急演练，落实网络安全等级保护工作，开展关键基础设施认定工作。

监测工作主要是要利用网络安全设备比如防火墙、WAF、态势感知等安全设备、渗透测试等安全服务、上级主管部门通报的漏洞等发现网站或者信息系统存在的安全隐患，形成通报材料要求二级单位进行整改。

预警工作一般是有重大网络安全隐患或者重要时期保障的时候应当向二级单位发送预警，要求对安全隐患进行自查并整改或者启动重要时期保障值班值守机制。

通报工作一般要求在监测或者预警发现问题后，通过一定的通报手段，及时有效地将信息下发给二级单位，在二级单位未能及时整改时采用技术手段做好保护或者缓解措施。

应急响应工作主要是在网络安全事件出现后，最大限度减少事件对学校业务的损害，保障学校业务正常运行，规范信息系统应急处理流程。学校应当根据国家、教育行业、属地等相关标准和文件，结合学校实际，制定本校的网络安全应急预案，并定期执行演练，以便相关人员熟练掌握，规范处置措施与操作流程，确保预案切实有效，实现网络信息安全事件处置的科学化、规范化。也应督促要求二级单位根据学校的应急响应文件，制定本单位的应急响应机制并上报给学校。

攻防演练

公安部网络安全保卫局一级巡视员、副局长兼总工程师郭启全提出，网络安全防控体系是“打”出来的经验，并且还提出构建国家网络安全综合防控体系的新目标与“三化六防”的新理念。其中，“三化”包括实战化、体系化和常态化，“六防”包括动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控，目的是将国家网络安全综合防御能力和水平上升一个新高度。

在 2019 年 8 月份网络安全大会上，郭启全指出了国内网络安全普遍存在的突出问题，包括重边界防护，轻内部防护，缺乏分区分域和域内防护，一点突破，全网即被突破；部分基层单位对网络安全重视不够，防护措施不到位，成为了网络攻击的突破口等等，这些问题在高校内部也是普遍存在的。

高校应当有针对性地对以上安全问题进行分析并形成应对措施，在事件发生前事先做好准备，常规的安全措施一定要做。在安全事件发生后应当做好应急响应，进行止损，目的在于把事件造成的损失降到最小。

高校基本上都有开展网络安全等级保护制度，等保通过一些规定动作，对策略、制度、规程、台账、基线和设备进行补齐，完成了合规要求。但是等保相对于攻防演练，会更偏向静态。比如一个信息系统即使代码做过审计，所有组件升级到最新，无已知高危漏洞，但是一旦出现一个 0day，整个防护可能就会全线崩溃。当然学校也会有一些纵深防御措施，让 0day 利用起来比较困难，但是从体系上，我们还是需要通过攻防演练来实际验证一下整体的防御体系。

我们在应对攻防演练的时候，应当有一个底线思维。坚持底线思维要求我们凡事从坏处准备，努力争取最好的结果。“假

定泄露”是零信任的一个理念，跟底线思维理念实际上是相通的，我们一定要假定，在攻防演练中，红队一定会突破边界，进入学校校园网甚至业务内网。

因为从多次攻防演练来看，随着防守方的防护水平提高，正面突破会比较难，红队已经开始大量使用社工手段，比如使用一些方法拿到师生 VPN 账户、通过抵近攻击在校园内接入 WiFi、发送钓鱼邮件、进入学生交流群私聊甚至直接在大群扔木马、在多个校内系统进行水坑攻击等。由于高校一般师生和信息系统众多，总有一些师生网络安全素养不高、信息系统保护较弱的情况出现，形成了网络攻击的突破口，这些都要求我们的防护一定要以“红队一定会突破边界”为前提来实施，具体的安全防护思路如图 1 所示。

图 1 安全防护思路

反钓鱼邮件演练

高校应当定期举行反钓鱼邮件的演练，可以根据学校实际，通过采购外包或者自行搭建系统完成常态化、全覆盖的反钓鱼邮件演练。如果是自行完成，则需要准备以下步骤：

1. 前期准备：撰写培训材料、编撰自测题、先礼后兵举行演练通告、跟演练发件人业务部门沟通、报告监管部门等。

2. 搭建钓鱼邮件平台：搭建开源钓鱼邮件平台、搭建发件服务器、测试邮件服务器白名单和安全规则绕过配置、拷贝钓鱼页面、设计中招页面、导入邮件列表、开始演练。

3. 最后总结：群发通报举行巩固和形成闭环、通知可能会继续常态化钓鱼。

常用的开源钓鱼邮件平台 Gophish 虽然功能齐全，但是也存在一些小问题，比如无法发送带个性化信息的更高级的钓鱼邮件，邮件模板可替换变量较少，无法发送带跟踪链接的 Word 附件，无法对发送的二维码进行自定义。带个性化信息的钓鱼邮件是指，如果我们可以设计一个沉浸式非常高的场景，比如给一位老师发送他在科研系统内的课题结项要求，列出他的所有课题列表，引导他去点击一个恶意链接，这个钓鱼邮件的隐蔽性非常高，而且是可能发生的。

网站内容错敏词检查

国家对网站内容有一些政策法规要求，比如 2019 年 10 月 31 日的《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》，2019 年 12 月 15 日的《网络信息内容生态治理规定》，2021 年 9 月 15 日的《关于进一步压实网站平台信息内容主体责任的意见》等等。新华社也会定期发布《新华社新闻信息报道中的禁用词和慎用词（最新修订）》，公布一些禁用词、规范用语。

以上法规都对高校网站内容提出了要求，高校应当采取措施对网站内容的表述错误、暗链、黑链、个人信息泄露、失效链接等内容进行相应的整治，加强网站的传播力、影响力和公信力。

我们认为高校网站内容问题的产生，既存在一些客观因素，也有一些主观原因。比如，错别字一般是因为输入法或者编辑文字功底不扎实造成的；不规范用语主要是由于编辑人员责任意识不强、学习不到位等；个人信息泄露等问题主要是一些人员安全意识不足；暗链和黑链的出现，有一部分是由于原先网站被黑，即使迁移到安全性更高的网站群，原先被黑的内容也原样迁移到网站群，这主要是迁移后检查不全面的问题，还有一部分是客观原因，比如原先一个站点的新闻，在当时发布的时候，可能会链接到一个正常的网站，但是随着时间的推移，这个正常的网站可能在过期后网站域名被黑产接管，导致学校网站链接到一个不正常的网站；失效链接的主要原因是，原链接网站关闭，或网站改版导致链接失效，源站反爬机制导致监测误判等。

高校应当采取技术措施，联合宣传部等职能部门对网站内容进行监测整改，并应当把监测左移，做好前置培训和检查，争取在源头上解决网站内容错误问题，并通过定期的后期技术手段监测，形成完善的网站内容安全机制。

对于监测的技术手段，比如爬虫和中文分词，技术上较为成熟，也比较简单，对于错别字的检查，Python 有类库 PyCorrector 可以实现音似、形似、笔画五笔编辑距离特征、语言模型困惑度特征等进行错别字检查，但是误判比较多。而对于规范用语、敏感内容、暗链黑链来说，则需要有情报库。对于失效链接的检查也较为简单，有成熟免费的软件可以做检查。最后，所有的这些都应当有人工进行复核，减少整改人员。整体评估以后建议高校应当采取采购云检测平台的服务加上自行修改云平台不足的模式，完成全校的网站内容整改。CEN（责编：高明）

（作者单位为厦门大学信息与网络中心）