校园网攻击面管理的思考与建议

文 / 郑海山[1] 辛毅[2]

Gartner（美国高德纳咨询公司）将攻击面管理分为外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）和数字风险保护服务（DRPS）三类。其中，EASM是指对组织在互联网上可见的所有数字资产和脆弱性的管理；CAASM是指管理组织能够查看的所有内部和外部的数字资产，主要手段是与现有工具进行集成，整合各类系统的数据；DRPS是指管理组织在互联网甚至深网（Deep Web）里主动或非主动留下的数字痕迹。

外部攻击面管理

EASM通常是指对互联网暴露的数字资产和脆弱性进行管理，但对于高校，更为严重的威胁经常来自校园网内部。高校校园网内有着大量的师生各类终端，在攻防演练时，我们通常均要假设攻击者一定会突破校园网的边界防护进入校园网甚至数据中心内网。

高校一般有校级数据中心，并且要求所有二级单位的服务器均托管在数据中心里。但是各个二级单位还是会有自己其他的一些类似门禁、视频监控、大型仪器、虚拟仿真、物联网等平台，这些平台的系统或服务器的物理位置不在校级数据中心，缺少校级安全设备的防护。所以高校在外部攻击面管理方面，可以将校园网等同于互联网来考虑。在优先做好互联网攻击面梳理的前提下，同步推进校园网内的攻击面管理。

攻击面管理中除了做好资产梳理外，也要进行高频度的脆弱性扫描和安全检查，应定期扫描和评估在互联网上可见的系统和应用程序中的脆弱性，然后通过漏洞优先级技术（VPT）处理漏洞来减少攻击面。

攻击面管理主要是做好暴露面收缩，具体可从以下几个方面展开。

门户等信息发布类网站与信息系统

只有信息发布的网站应统一使用网站群平台发布。制作服务器和发布服务器应当分开部署并且做好静态发布和防篡改保护。应常态化梳理各个网站有发布权限的用户，缩小网站信息发布的攻击面。

高校信息系统往往较多，对于信息系统的防护，可以使用统一的应用交付平台。在应用交付平台完成TLS卸载后再挂接Web应用防火墙和日志审计系统。使用应用交付平台也是对信息系统进行白名单管控的过程，只有通过设置到应用交付平台的信息系统才会被外部访问。通过这个策略，可以大大缩小整体信息系统的暴露面。

使用了应用交付后，通过设置服务器的防火墙使得服务器只对应用交付系统开放权限，可以大大缩小服务器攻击面，将服务器在网络上隐藏起来。

如果应用交付平台支持进行身份认证，可以对部分只有校内师生访问的系统预先进行身份认证，采用零信任架构，这样可以将这些系统的暴露面缩小到只有认证后的用户才能发起恶意攻击。

信息系统资产内比较重要的是API（应用程序编程接口）资产。由于调用JavaScript API通常不会引起URL（统一资源定位符）变化，调试API需要使用一些专门的工具，导致很多开发人员认为API比较隐蔽，被攻击比较难。而且API通常需要使用JavaScript引擎发起调用要求，导致很多脆弱性扫描工具无法扫描API的安全。以往常见的API问题包括：缺乏身份验证机制导致全站API未授权访问；虽然Web界面显示较少字段，但是

EASM通常是指对互联网暴露的数字资产和脆弱性进行管理，但对于高校，更为严重的威胁经常来自校园网内部。

中国知网 https://www.cnki.net

API 返回值包含全部字段，里面可能包含敏感信息；Web 界面有对数据进行分页，但是通过传入一个非常大的页面尺寸可一次性将所有数据全部读出；敏感 API 接口文档工具暴露；老旧的 API 版本未下线导致存在脆弱性问题；等等。API 本质上还是 Web 应用，所以常见的 OWASP（开放式 Web 应用程序安全项目）TOP 10 的安全问题在 API 上也存在。

针对 API 资产的防护，可采用独立的 API 安全网关，也可合并在具有 API 网关模块功能的应用交付平台上进行防护。基于 API 网关的能力，做好身份验证、访问控制、权限管理、流量控制、分析、监控和审计等工作。

信息系统中还有一类有终端用户性质的系统，比如虚拟仿真、高性能计算作业提交系统等。这类系统跟其他信息系统不同的是，其他信息系统一般对用户限制比较严格，用户只能在浏览器上，根据信息系统的需求实现受限的功能。但是这些系统通过虚拟化后，用户可以使用 SSH 或者浏览器进入操作系统级别，对系统或者网络环境有较强的控制能力。这类信息系统有很强的终端用户特点，而且用户量大，安全隔离机制不一定完善，所以一旦被攻破，会比较容易进入数据中心内网进行横向渗透。因此，这类系统应当部署在一个独立的安全域，把它等同于终端用户来管理。

服务器

服务器应做好分区分域，使用防火墙或者 ACL（访问控制列表）规则对区域进行分隔。分区分域的粒度应做好平衡，避免太粗导致分区分域失去意义，也要避免太细导致访问规则复杂。

服务器应设置严格的防火墙，服务器的端口开放可以分为 4 种类型：一是管理端口，比如 SSH、RDP、中间件的管理端口，这类端口应当限制只有管理员 IP 或者堡垒机才能访问；二是业务内部端口，比如数据库端口、LDAP 端口、心跳连接端口等，这类应当限制只有相关业务安全域可访问，或者直接限制到具体的服务器 IP；三是业务外部端口，比如 HTTP、HTTPS、SMTP、NTP 等，这类需要对所有用户全部开放；四是其他端口，比如用于监控的 SNMP、Zabbix 端口，这类端口可只信任需要监控的发起者的服务器 IP。

除了因对外提供服务而接受外部连接外，服务器应限制主动对外连接。限制主动对外连接可以减少被攻击后连接 C&C（Command and Control）的风险，实现对服务器和数据更好地隔离和保护，减少数据泄露风险。限制主动对外连接后，一些操作系统、应用程序、安全设备的安全补丁和规则更新可以通过在校内建立补丁服务器来完成，也可通过专门的代理对外连接。如果服务器需要与云服务、外部 API 或第三方服务集成，也应当通过代理完成，并且经常对流量进行审计。

限制主动连接后也应当关注一些不规范的使用方法，比如使用反向连接的工具，走 Web 隧道等方法绕过限制。

做好服务器防火墙后，应当对服务器端口进行常态化检查，查找弱口令、脆弱性、开放的端口和声明不一致、防火墙失效等问题。

账号凭据

高校的人员流动性较大，信息系统运维中也高度依赖第三方开发商提供的服务，各类账户较多，最主要应关注统一身份认证账户、VPN 账户、邮件账户和第三方运维人员账户。

首先，应当排查没有对接统一身份认证的系统，要求进入统一身份认证体系，并且尽量关闭自带的认证，如果无法关闭或者还需保留的，应当做好各项密码安全保护措施。

其次，启用多因素认证可以极大地缩小暴露面。然而需要注意的是，如果电脑被全面控制，即使多因素认证也无法阻止后续攻击。对于社会工程学和钓鱼攻击，一般单位很难完全防范，即使进行了网络安全素养培训或反钓鱼邮件演练，仍然会有部分师生员工成为这类攻击的受害者。

对于第三方运维人员账号的管理，应当要求运维人员拨号 VPN 后再使用堡垒机进行运维，并且禁止第三方运维人员为了方便而使用绕过限制的方式进行运维。

高校应定期主动对以上账户凭据进行扫描，扫描使用的密码字典可使用互联网上的常见弱口令字典、用户已经泄露在各类社会工程学库的密码、用户个人信息（如姓名、身份证号、手机号）等字符或数字组合。扫描可采用效率较高的手段，比如使用 LDAP 或者密码直接导出 Hash 比对。

公有云上的系统和其他

对于公有云平台上的系统，应做好资产梳理，应采购云平台提供的网络安全组件，比照私有化云平台的其他措施，做好网络安全防护。

针对双非网站，我们应采用管理措施和采购互联网资产梳理服务相结合的方法进行梳理和整改，最终根据政策要求完成整改工作。整改的结果可能包括去除学校相关标识，以及部分或全部迁移至校内进行部署和发布。

对于寄生网站，可从全流量分析平台识别并要求进行整改，应确保所有网站或信息系统都使用标准 HTTP/HTTPS 端口对外提供服务。

针对一些欺诈或仿冒的虚假网站，属于 DRPS 的范畴。对于这类网站，可以通过法律手段来解决。如果这些网站在搜索引擎中排名较高，可以进行举报，请求搜索引擎将虚假网站从搜索结果中移除。另一类 DRPS 相关的可能是在公共存储空间（如代码托管平台、网盘、文库等）位置存储的可能被攻击者利用的各类技术文档（如拓扑图、源代码、培训手册等）。

对于一些厂商在互联网部署的与学校相关的开发测试平台，可通过互联网资产梳理服务得以发现，也应在运维规范内对这种行为进行限制。

对于 SaaS 应用的选购应建立管理规定，应通过管理手段，建立 SaaS 平台准入清单、资格要求等，要求使用单位通

中国知网 https://www.cnki.net

过相关流程进行选用和登记。SaaS 应用需要对接师生数据的，应当进行审查，可不采用全量数据直接导入的方式而使用 CAS（中央认证服务）、OAuth2 等协议或 API 做到数据随用随取，并且不再使用后，要求平台对数据进行删除并给出佐证材料。

物理攻击面，例如数据中心和校园内暴露的设备，需要进行物理攻击防护和设备准入控制。对于外部暴露的设备，应以底线思维来进行防护。例如，对于校园卡的圈存机或监控摄像头等设备，应假设攻击者可以轻易拔插或替换设备并直接进入设备网络。

CAASM 是指管理组织能够查看的所有内部和外部的数字资产，主要手段是与现有工具进行集成，整合各类系统的数据。

网络资产攻击面管理

在 CAASM 的定义中，最重要的关键词就是自动化和数据整合。

自动化

部分高校缺乏资产管理平台，可能会使用离线或在线的类 Excel 工具进行管理。然而，这些方式都是不可取的，因为这些数据的录入和管理都依赖于人工操作。

人工录入容易出现疏漏和错误，导致资产清单不完整或不准确。手动更新资产信息也是一个耗时的过程，手动录入使得工作量加大，导致管理人员产生惰性，容易使资产清单过时。与此同时，人工录入缺乏时效性，无法应对快速变化的威胁环境。一旦资产规模较大，手动录入和维护资产信息几乎是不切实际的。

使用自动化手段能够更可靠、实时地获取和更新资产信息，提高攻击面管理的准确性和效率。而且高校一般会采用校院两级管理，人工维护无法将这些数据向二级单位共享。

数据整合

在信息化领域，一些高校在隐私合规的前提下会做“学生画像”类似的系统。这些系统采集学籍系统、课程管理系统、图书馆系统、体育系统、消费记录、无线网日志等数据，汇总形成学生画像。

攻击面管理方面，我们也需要形成信息系统和服务器等资产的画像。很多资产的属性或者说是指纹信息散落在高校内部各类系统里，可整合这些属性，形成庞大复杂的资产关系表。

采集的数据来源可包括：网络管理系统、网络安全设备 ACL、DNS 系统、VPN、虚拟化平台、应用交付平台、应用发布平台的对接、统一身份认证系统、邮件系统、网站群系统、其他业务系统、共享数据平台对接、云桌面、终端检测与响应（EDR）、堡垒机、蜜罐平台、监控平台、备份设备、扫描设备等。

比如，网络管理系统会有 IP 静态或动态分配列表，可获取 IP 段与二级单位或者区域的映射关系。可从动态分配获知该 IP 应当只是客户端 IP 段，在攻防演练分析中，可知该资产重要性程度。

从 DNS 记录可获取域名真实对应的 IP 地址、别名、申请单位等信息。通过 DNS 记录，也可识别有特殊记录的 DNS，比如是否提供 MX 记录可知是否存在邮件服务。

统一身份认证系统和应用发布平台方面，因为一般只有信息系统才会对接这两个系统，所以就可以判断哪些 Web 应用是一个简单的纯新闻发布系统还是一个复杂的信息系统。

在信息化领域，数据天然是要共享的，所以很多高校会去推动这项工作，学生画像会有比较大的实施基础。但是在网络安全方面，数据的集中只是用来做安全分析，所以很多高校忽略了这项工作的重要性。

数据整合难度有时比较大，有些公司担心开放 API 会增加潜在的攻击面，有些公司没有考虑到要跟其他系统进行集成，开发这些功能导致成本增加，有些公司基于商业策略的考虑，希望保持封闭的生态系统。这些都导致市面上的系统和安全设备开放度普遍不高，从而影响对接。

如同信息化数据治理，整合过程中需要对数据的权威性进行识别。比如一个 IP 如果是从虚拟化平台获得的，那这个 IP 一定是这台服务器的真实 IP，而如果一个 IP 是从 IP 分配表获得的，可认为这个 IP 与这台服务器的对应关系较弱。

整合过程也需要对数据进行梳理。一个信息资产，在不同的系统可能有不同的名字，同一个 IP 地址，可能会配置在不同的资产里，所以应当做好映射关系。例如，可通过一定的规则约束，要求各类系统使用统一的编码规则，或者为了减少工作量，可采用柔性的映射方法或者不映射，依赖查询者自行做好映射。

中国知网 https://www.cnki.net

资产管理平台

通过以上自动化和数据整合的分析，可知高校应当有一个资产管理平台。这个平台，输入 URL 或者 IP 地址，可以立刻展示资产的所有“画像”。这在攻防演练场景下也是非常基础的数据支撑。

在攻防演练场景中，我们如果识别到一个内部 IP 或者 URL 正在被攻击，就需要尽快知道这个资产的相关信息，并做出准确判断，比如是否是重要资产？是否是误报？判断之后才能决定下一步是继续跟踪还是忽略。如果决定跟踪，也需要使用这个系统及时联系到对应责任人。

通过资产管理平台，我们可以识别一个攻击情报是否误报，如果是一个 ASP.NET 的网站，那攻击者采取 PHP 的攻击方式则无效。如果一个资产历史上存在这方面的脆弱性，那再次被攻击的概率也会比较大，需要尽快进行隔离。

如果获取到一个威胁情报，也需要尽快知道哪些系统或服务器使用该组件并受影响。

建立资产管理平台后，也可监测资产的合规性情况。这个合规不一定是法律法规的合规，而是单位内部制定的一些合规规则，比如是否安装恶意软件识别工具？是否做好防火墙配置？是否有使用堡垒机运维？通过识别出不合规问题并向资产管理平台关联的所有联系人发出通知，可以加强单位的攻击面防护，及时弥补安全漏洞。

“画像”对信息系统的全生命周期管理也是非常有必要的。以一个信息系统下线为例，需要回收 IP、域名和虚拟机，撤销反向代理、统一身份认证对接、API 对接、数据库对接、VPN、堡垒机等配置，删除一些 ACL 和安全设备规则配置等操作。通过“画像”，才能确保所有相关资源已经全部释放。

比如一种新的云抢占攻击，一般云平台的 IP 分配是动态的，当学校的某个云平台下线后，释放的云平台 IP 地址有可能被后面申请的其他组织获得，如果 DNS 记录还是指向旧的 IP 地址，有可能导致域名被滥用。

资产梳理和整合的具体做法

市面上如果已经存在符合单位需求的可用成品软件，可直接采购，也可自行通过一些脚本语言比如 Python 等使用主动和被动流量或日志分析完成。由于各类资产和资产属性是动态的，所以可将主动或被动分析得到的数据保存到有时间戳的时序数据库内，通过对时间进行切片获得某段时间内资产的具体“画像”。如同数据治理，数据的获取和整合的工作量可能较大，单位可以采取逐步推进的策略，一步步完善资产“画像”。

其中，主动获取数据的方式包括：**第一，主动对资产进行扫描。**在主动扫描的过程中，分为两种，一种是为了发现资产，一种是已知资产，扫描更多指纹和脆弱性。扫描可以使用一些类似 Nmap 的开源软件进行，也可采购商业的资产管理产品进行扫描，并让其扫描结果作为一个信息来源进入平台。

第二，使用 API、数据库、自定义脚本、离线文件导入导出等对接。如果需要对接的系统有 API 是最为简单的；如果没有，可尝试使用数据库的方式，也可以使用爬虫框架从 Web 层面获取数据，使用 Shell 脚本从 SSH 获取数据。如果这些都没有，对于一些变化不大的，可手工采用导入导出的方式获得对接系统的数据。

第三，获取互联网平台数据。Shodan、Censys、ZoomEye 等互联网网络空间节点搜索引擎会包含单位对外公开暴露的服务器和网络设备、脆弱性和指纹信息，可通过注册会员使用 API 获取与单位相关的信息。这些信息也是很多攻击者关注的。单位应以攻击者思维对这些信息进行一次梳理，也可通过购买网络安全资产梳理服务，通过一次性或者定期服务，对各类资产进行识别后导入系统。

被动获取数据的方式为：**第一，全流量检测。**全流量检测在攻击面管理层面可以发现一些寄生网站，也可以识别出存在弱口令的系统和账户，还可以检测出 API 资产等。

第二，从应用交付平台等日志系统获取。应用交付平台类似全流量分析，但是是专注于特定资产比如 Web 资产等。应用交付平台通常没有专门的分析能力，但是其留存了所有 Web 的访问日志信息，可获取这些信息进行过滤汇总后获得 Web 资产的一些指纹信息。

攻击面的混淆

一旦做好了攻击面的管理，缩小了暴露面，就可以考虑再使用蜜罐等手段对攻击面进行混淆。如果前面都是在做减法，那这里就是在做加法。

蜜罐应密集部署。“密集”可以从数量、形态和部署区域来展开。数量上，应在内网各个区域部署蜜罐，将没有使用的 IP 使用蜜罐填满。在形态上，可以部署不同厂商的蜜罐，可以部署高交互、低交互和无交互蜜罐。在部署区域上，可使用以下措施：在服务器开端口蜜罐，将文件诱饵发布到尽可能多的服务器或重要用户桌面，将邮件诱饵发布到重要用户邮箱，在 URL 二级目录将流量引向蜜罐，在统一身份认证、VPN、邮件等系统开蜜罐账户，在各个安全域部署蜜罐系统。

蜜罐引入一定也会对高校自己的资产管理造成混乱。所以，蜜罐的资产也要做好梳理，并定期进行轮替增加被识别的难度。

在当今互联网环境下，各种网络威胁层出不穷，而相应的防护手段也是多种多样的。攻击面管理不仅是保护高校网络安全的第一步，也是最为关键的一步。高校通过将校园网等同于互联网来梳理资产分类后，对相应资产类别进行不同方式的攻击面收敛，同时对各类系统属性进行获取和整合，能够全面了解和把握其资产和攻击面情况，从而更有效地保障高校网络安全。CEN（责编：陈永杰）

（作者 1 单位为厦门大学信息与网络中心，作者 2 单位为哈尔滨工业大学网络安全和信息化办公室）

基金项目：中国教育技术协会网络安全专业委员会 2023 年网络安全专项课题（2023CAET1004）。

中国知网 https://www.cnki.net