网络空间资产测绘与攻击面管理的技术研究

梁　群

（中通服创发科技有限责任公司，湖南长沙，410016）

【摘要】随着信息技术的发展，网络安全形势也变得异常复杂，网络空间资产测绘与攻击面管理作为新型网络安全技术已被行业认可。基于对攻击面管理相关技术的学习和研究，提出网络空间资产测绘与攻击面管理平台建设的整体架构，并给出相关的核心业务管理流程以及技术能力要求，在运营商的实际生产环境中得以验证，帮助运营商构建以资产为核心的立体化防御体系，让网络安全防患于未然，做好网络安全保障工作。

【关键词】网络空间资产测绘；攻击面；网络安全；主动防御

【doi:10.3969/j.issn.2095-7661.2022.04.008】

【中图分类号】TP393.08　　【文献标识码】A　　【文章编号】2095-7661（2022）04-0026-04

Technology Research on Cyberspace Asset Survey and Attack Surface Management

LIANG Qun

(CCS Transfar Technology Co. Ltd., Changsha, Hunan, China 410016)

Abstract: Along with the development of information technology(IT), the situation of network security becomes extremely complicated. Cyberspace Asset Survey and Attack Surface Management, as a new type of network security technology, has been widely accepted. This new technology is based on the study and research of ASM technology which brings out the overall platform architecture and provides key service management processes and technological capabilities, and at length has been proved effective at the network service providers' (NSPs) side. To come into a conclusion, this solution is able to help NSPs build a multi-dimensional asset-centered defense system, thus nipping the risks and attacks in the bud, and better assuring network security.

Keywords:cyberspace asset survey; attack surface; network security; active defense

万物互联时代，企业的业务应用云化、移动化、社交化是企业在数字化转型中的必经之路。随着信息技术的发展，网络信息系统带来高效、便利的同时[1]，网络边界逐渐模糊，网络资产爆炸增长，数以万亿的资产攻击面暴露在高阶威胁之下，给企业的网络空间安全带来全新挑战。行业客户在安全运营过程中，常常受困于资产家底的数量不清、类型不清、位置不清、归属不清、风险不清和防护情况不清，导致安全防御如盲人摸象；漏洞、配置错误、弱口令等资产安全问题层出不穷，安全运维人力有限，风险处置往往是力不从心。无论是重保护网还是日常运营，资产安全管理都已成为行业客户的烦恼。如何在网络攻击爆发之前，以攻击者视角绘制完整的资产攻击面[2]，精准、实时、智能地加强网络空间的资产及攻击面管理，提升对未知威胁的主动防御能力，已成为行业共识。

1 攻击面的定义

攻击面是系统相关元素中可被攻击者利用来实施攻击的元素集合[3]，包括：承载业务应用软件的操作系统、中间件、数据库、开源组件以及业务系统自身存在的安全漏洞，系统或软件中的安全控制策略配置错误或缺失，违反安全制度和合规要求的网络配置等。

2021年，Gartner在安全运营曲线（Hype Cycle for Security Operations）中发布了网络资产攻击面管理（Cyber Asset Attack Surface Management）和外

[收稿日期] 2022-07-29

[作者简介] 梁群（1979—），男，湖南衡阳人，中通服创发科技有限责任公司网络信息安全事业部，本科，研究方向：网络安全、软件研发。

部攻击面管理(External Attack Surface Management)新的安全技术理念。国内安全行业权威机构也争先发布网络空间资产测绘与攻击面管理能力指南和技术标准,2021年数世咨询发布《网络空间资产测绘能力指南》,同年《电信网和互联网资产安全管理平台技术要求》行业标准开始实施,毫无疑问,网络空间资产测绘与攻击面管理已成为了新型网络安全技术焦点,为平台建设提供了坚实的安全方法理论支撑。

2 整体架构设计

网络空间资产测绘与攻击面管理旨在通过高精度的资产指纹图谱技术、脆弱性评估与安全威胁检测技术,实现安全资产与攻击面全要素管理,在网络攻击之前发现资产中存在的安全问题,及时整改,构建立体化的主动防御体系。

结合多年在网络信息安全方面的实战经验,网络空间资产测绘与攻击面管理平台的整体架构建设蓝图设计如图1所示。

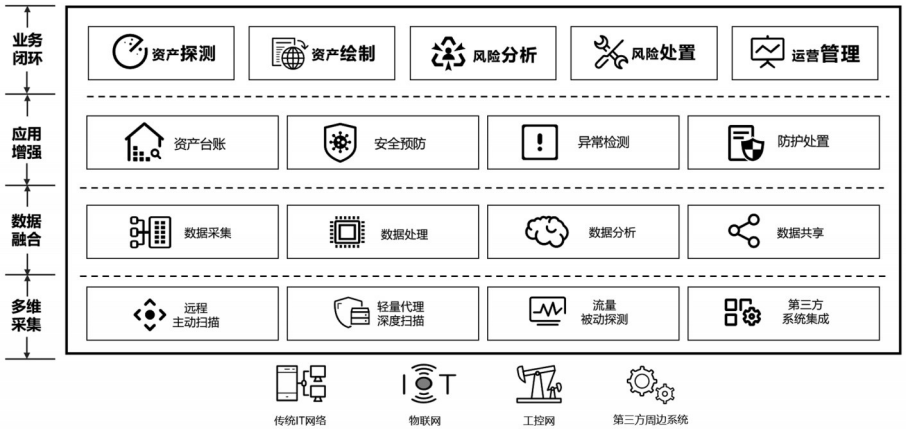

图1　平台整体架构图

平台主要划分为如下几个层级来进行建设,具体的能力描述如下:

多维采集:支持远程主动扫描、轻量代理深度扫描、流量被动探测、第三方系统集成等多种资产数据采集的手段,多维度、深层次地全面采集资产安全管理要素信息。

数据融合:建立资产安全数据模型,支持多源、异构的各类资产数据汇聚、处理以及分析,支持标准化的资产数据对外赋能共享。

应用增强:提供集约化的资产台账管理能力,支持漏洞、弱口令、异常进程、基线配置核查等多种脆弱性问题分析和检测能力,具备一定的安全防护处置能力。

业务闭环:运用可视化技术,支撑安全运维人员开展安全运营管理工作,实现全生命周期的业务端到端技术支撑。

3 核心业务流程

习近平总书记在2016年4月的网络安全和信息化工作座谈会上提出:“要全面加强网络安全检查,摸清家底,认清风险,找出漏洞,通报结果,督促整改。”[4]网络空间资产测绘与攻击面管理的核心业务流程采用“五步法”来提升客户的网络安全主动防御能力,具体的工作流程如图2所示。

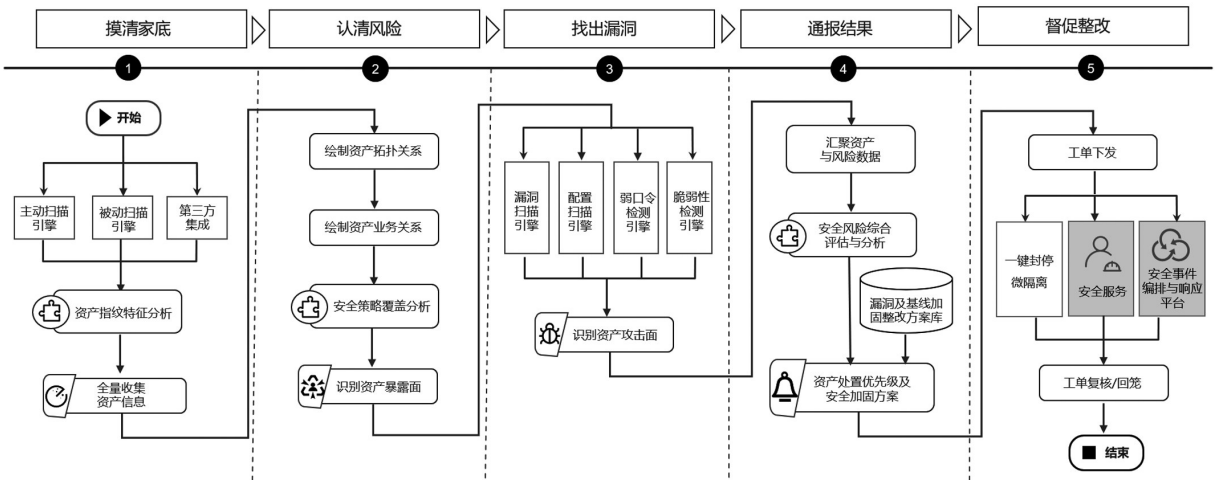

图2　网络空间资产测绘与攻击面管理核心业务流程图

1）摸清家底，是要全面、实时、持续地发现和梳理企业内部和外部的资产，通过资产指纹特征和责任主体指纹等技术，识别通信网、互联网、物联网、工控网中的各类资产，做到资产心中有数。

2）认清风险，是要识别可能有安全风险的资产，梳理资产与资产之间的关系，绘制出资产的网络拓扑与业务拓扑关系图，结合EDR、FW、WAF、NAT等安全策略覆盖情况，识别出可能暴露给攻击者的危险资产。

3）找出漏洞，是要充分发现和挖掘资产可能存在的攻击面问题，通过轻量代理发现资产中存在的配置不合规、弱口令等相关资产脆弱性问题，通过集成漏洞扫描引擎扫描资产中存在的安全漏洞。根据信息系统的安全危害程度[5]，评估漏洞的影响范围和处置的优先级。

4）通报结果，是建立基于资产的重要等级、暴露风险系统、脆弱性问题以及安全策略覆盖等维度的资产风险评估模型，实现资产安全风险度量指标，输出资产风险评估报告。

5）督促整改，是通过工单的形式，实现安全风险的闭环处置，通过人工安全服务对安全问题进行修复，同时还可以通过平台内置的一键关停、微隔离等技术手段，实现资产攻击面的快速收敛。

4 关键技术与核心能力说明

4.1 多样资产探测手段融合

为弥补各项探测技术的局限性，平台采用多种探测技术引擎来相互补充，确保资产信息采集的全面性。具体采用的各项技术方式的核心作用、要求及缺点分析如表1所示。

表1 资产探测技术手段汇总表

技术方式	核心作用	技术要求	缺点
远程扫描	在网络可达的情况下快速地收集资产信息	支持分布式子网探测，能够识别150+协议，支持资产指纹特征管理	依赖指纹准确度，采集到的资产信息不全面
轻量代理	精准、深度地采集资产各类信息，并可实现资产安全事件处置	支持主流操作系统，内存占用<40 M，CPU占用<4%，支持基线核查规则，自主式调节，支持一键关停、微隔离等处置能力	需要常驻操作系统的主机中，代理的稳定性要求极高
流量识别	通过旁路网络流量实时动态地采集资产信息，持续跟踪资产变更	支持从流量中对资产的识别，流量解析处理能力>1 Gbps	由于没有流量等一些僵死资产，采集到的资产不全面
第三方集成	与网管平台、SOC平台、CMDB等平台对接，实现资产数据的联动	支持多协议适配，包括Kafka、FTP、数据库等接口方式，预置常见功能接口	依赖第三方资产信息的准确度，安全视角的数据缺失

4.2 五维一体的资产指纹图谱

平台从五个维度构建全要素的资产指纹图谱，更精准地识别资产，具体各类型指纹的核心作用如表2所示。

表2 五维一体的资产指纹表

指纹特征域	核心作用
管理域	描述资产的管理属性，支持网络设备、安全设备、应用系统、Web组件等16个大类，158个小类的资产，详细记录资产版本、端口、服务、框架、设备类型、厂商、管理员等特征，支持自定义扩展属性
业务域	描述资产的业务属性，支持对资产的地域、环境、系统、角色进行业务分域，快速划分资产的责任归属、重要程度及风险等级
拓扑域	描述资产之间的关系，采集资产的邻近信息，实现网络拓扑和业务拓扑半自动化测绘能力，支持企业内组网情况进行详细展示，并运用大数据分析手段，从邻近相似资产中识别资产的归属，发现企业遗漏资产
风险域	描述资产的风险属性，全面采集资产的漏洞、安全基线、异常账号等风险情况，并结合资产重要等级、所属业务系统阶段进行资产风险评估，快速识别和定位高风险资产和业务系统
时间域	描述资产全生命周期的资产属性，基于时间维度，实现对资产的异动情况持续监控

4.3 多维度资产风险评估模型

平台同时构建资产价值、暴露情况、脆弱性、安全策略覆盖等多维度的资产安全风险评估矩阵模型，具体见表3，实现资产攻击面安全风险的可评价、可度量。

表3 资产风险评估模型表

风险评估维度	核心评估要素
资产价值评估	按照业务系统重要性、资产角色重要性、业务归属重要性等对资产重要等级进行评估
暴露属性评估	通过互联网暴露、企业网暴露、数据中心暴露、业务域暴露等评估资产暴露风险系数
资产脆弱性评估	以脆弱性基础评分、脆弱性级别、出现次数、当前状态等评估资产脆弱性风险
安全策略覆盖评估	从EDR覆盖情况、WAF覆盖情况、防火墙访问策略等方面完成安全策略覆盖率评估

4.4 多场景安全事件响应与处置

基于多年的重保支撑、应急演练、日常运维等多种场景下的实战经验，平台提供面向多场景安全事件处置技术手段来提高安全事件的处置效率，具体如表4所示。

表4 安全事件处置技术手段表

技术手段	主要功能
微隔离	自动采集业务网络中的流量信息，分析并固化业务之间的调用关系，识别出资产与资产间异常流量情况，支持通过预警和阻断等多种方式实现异常流量的快速隔离
一键封停	通过主机代理，快速地对主机上的异常进程或服务下达指令，关闭或停止有安全风险的资产或服务
一键派单	通过接口将安全事件派发给其他周边安全事件处置系统（如：安全运营管理平台SOC、安全事件编排与响应平台SOAR等），完成安全事件的闭环处置

5 实战应用案例

由于资产管理涉及的部门多、分布广、变化快，部分资产老旧和历史原因，很难通过管理手段做到100%准确，长久以来对于变化的资产管理及“三无七边”管理工作一直是运营商在安全运营过程中的核心痛点。

网络空间资产测绘与攻击面管理平台在运营商的大网环境中充分进行了能力验证。在某省级运营商项目实战中，采用主被动融合探测技术，构建了全面、准确、动态的资产测绘能力，资产覆盖度超过98%；结合运营商的海量数据，平台积累了10万+的资产指纹数据和2万+的企业指纹数据，通过运用智能化的指纹识别引擎，资产识别准确率94.6%；平台对授权资产围绕漏洞、安全基线、异常账号等脆弱性，开展风险自动化持续监测，累计了1200多项行业基线核查数据和1万+安全加固解决方案库；在实际的安全运营支撑中，并非所有漏洞都需要解决，有些漏洞无论如何都会持续存在[6]，通过评估漏洞确定漏洞处置的优先级，辅助安全运营工作有序、高效地开展，抓住关键，用20%的时间解决80%的网络安全风险；另外，针对不同的应用场景，平台还提供了多种快速安全事件处置手段，提升安全运营效率，帮助该省级运营商实现了安全运营从“被动防御”向“主动防御”进阶。

6 结束语

网络空间资产测绘与攻击面管理为企业内IT基础设施中的资产与安全风险提供持续的从发现、梳理、监控到治理一站式的管理能力，要求比攻击者更快获悉安全风险，让安全主动防御体系具有敏锐的感知力、精准的预判力、对网络攻击的及时阻断力和对攻击处置后的可追溯力[7]。虽然本研究在网络空间资产测绘与攻击面管理上积累了一定的技术和业务能力，但针对IPv6的海量地址的资产探测、数据资产的测绘等一些新领域上仍存在不小的挑战，这也将会是网络空间资产测绘与攻击面管理下阶段持续研究的方向。

【参考文献】

[1]廉新科，闫卿.基于攻击面的安全评估体系研究[J].通信技术，2020(10):2567-2572.

[2]沈传宝.从漏洞管理到攻击面管理[J].中国信息安全,2022(6):60-62.

[3]黄康宇,杨林,徐伟光,张涛,李华波.软件系统攻击面研究综述[J].小型微型计算机系统,2018(8):1765-1773.

[4]新华社.习近平：在网络安全和信息化工作座谈会上的讲话 [EB/OL]. http://www. gov. cn/xinwen/2016-04/25/content_5067705.htm，2016-04-25.

[5]张人杰,曾振,肖玮.网络安全实战攻防演练部署研究[J].湖南邮电职业技术学院学报,2019(3):23-25.

[6]段铁兴.企业攻击面管理的7个实践[J].计算机与网络，2021(13):50-51.

[7]赵姗.网络安全主动防御体系浅析[J].网络安全技术与应用,2022(4):4-5.

（上接第8页）

【参考文献】

[1]张敏，高科，杨凌云.5G网络分流比提升研究[J].湖南邮电职业技术学院学报，2022(1)：1-4.

[2]舒培炼，刘正兴，史大军，张敏.VoLTE丢包分析与特性参数优化研究[J].湖南邮电职业技术学院学报，2020(2)：8-12.

[3]胡漾.基于模糊理论的5G异构网络切换算法研究[J].湖南邮电职业技术学院学报，2021(2)：13-17.

[4]上海大唐移动通信设备有限公司.基于随机森林分析VoLTE网络故障原因的方法及装置：CN201810444550.0[P].2018-05-10.

[5]徐运武.5G CQI指标优化方案的应用研究[J].湖南邮电职业技术学院学报，2022(3)：8-12.

[6]张文刚.基于深度学习的交通预测技术及其在通信中的应用研究[D].成都：西南交通大学,2018.

[7]中国移动通信集团浙江有限公司.VoLTE网络故障检测方法及系统:201810981353.2[P].2018-08-25.

[8]康丁文.5G通信系统中高效LDPC译码技术研究[D].西安：西安电子科技大学,2019.