2020 年上半年云安全分析报告

– 联合发布 –

CAICT 中国信通院

安恒信息 DAS-Security 安全中国

NSFOCUS

目 录

一、云计算的背景与发展趋势

随着云计算等企业级技术应用的发展普及，产业互联网实际已经在各行各业展开实践。广度上不仅覆盖服务业、工业和农业，还从商业扩展到公益和政府，整个社会走向全面互联网；深度上，从营销服务、生产研发到运营管理，互联网渗透到组织内部的各个环节。数据信息由此实现从消费端到供给端的高效流通，数字产业与传统产业相互协同带动，助推中国经济迈向高质量发展阶段。

在新旧动能接续转换的过程中，传统产业的数字化升级和新兴产业的数字化能力建设，使当前的安全趋势发生了变化。该报告基于互联网、产业互联网及相关领域在上云过程当中面临的安全态势、风险趋势、应对力量以及监管状态等进行梳理，以期为行业提供阶段性的总结和建议，助力云上各方有策略地建立安全能力，更好应对安全风险。

二、国内云平台总体资产情况

2020 年，累计监测发现云平台上中大型单位的（除去大量个人、小型企业等）网站与 WEB 业务系统数量有 6,507,161 个，覆盖单位 604,614 个，主要是阿里云网站和腾讯云网站，分别占比 59.52%和 27.99%，云平台网站数量分布情况如下。

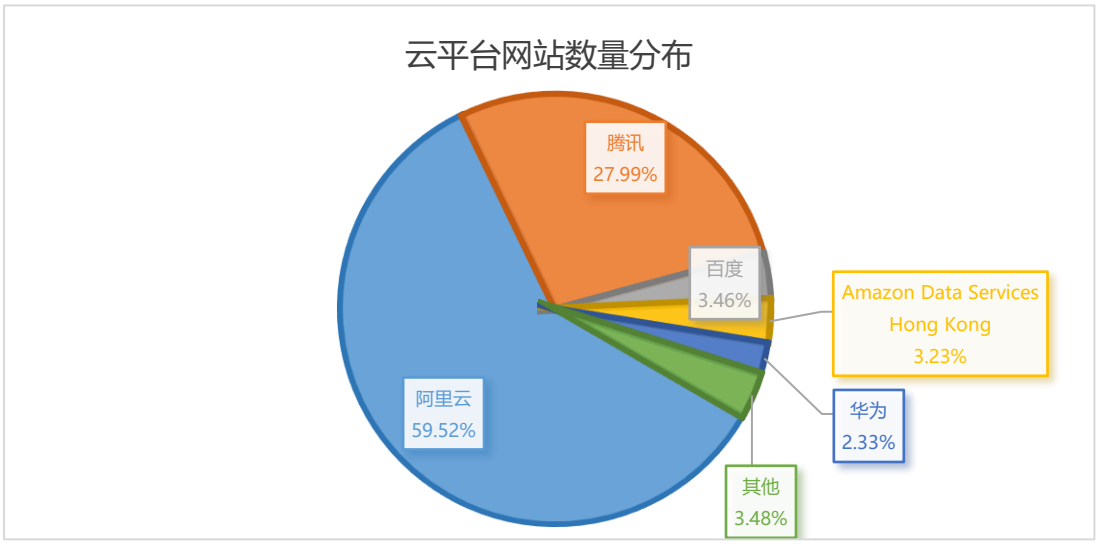

图 1 云平台网站数量分布

根据对云平台网站区域进行分析，发现主要分布在北京、香港、广东等区域。

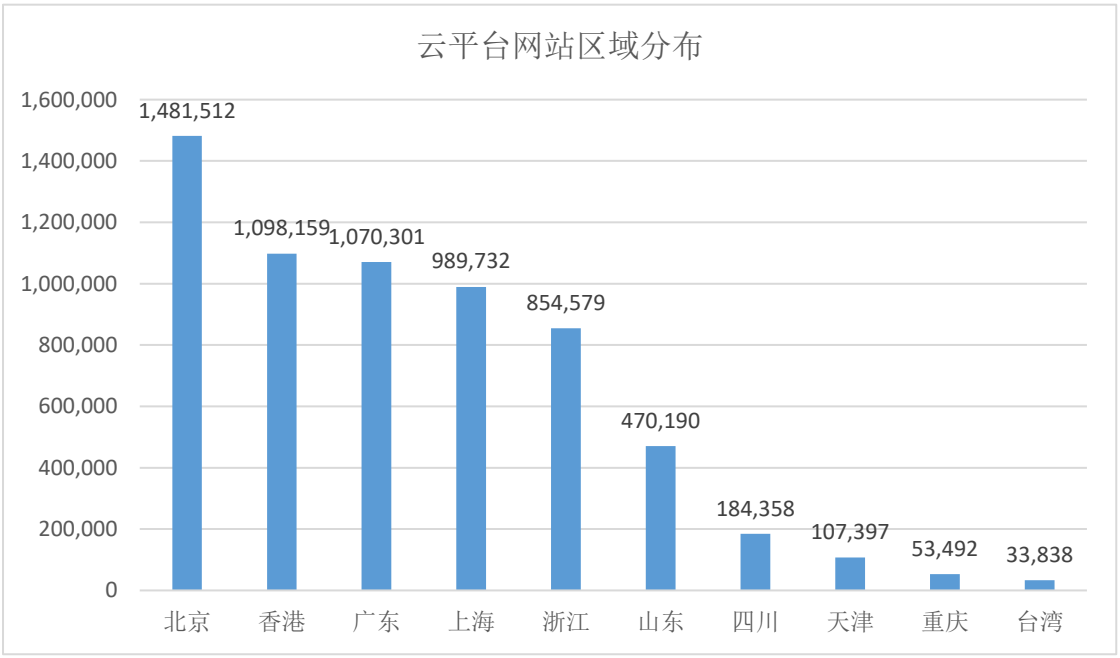

图 2 云平台网站区域分布

全国重要行业网站有 45.9 万，其中在云平台上的重要行业网站有 67,401 个，覆盖单位 18,363 个，重要行业网站上云情况如下。

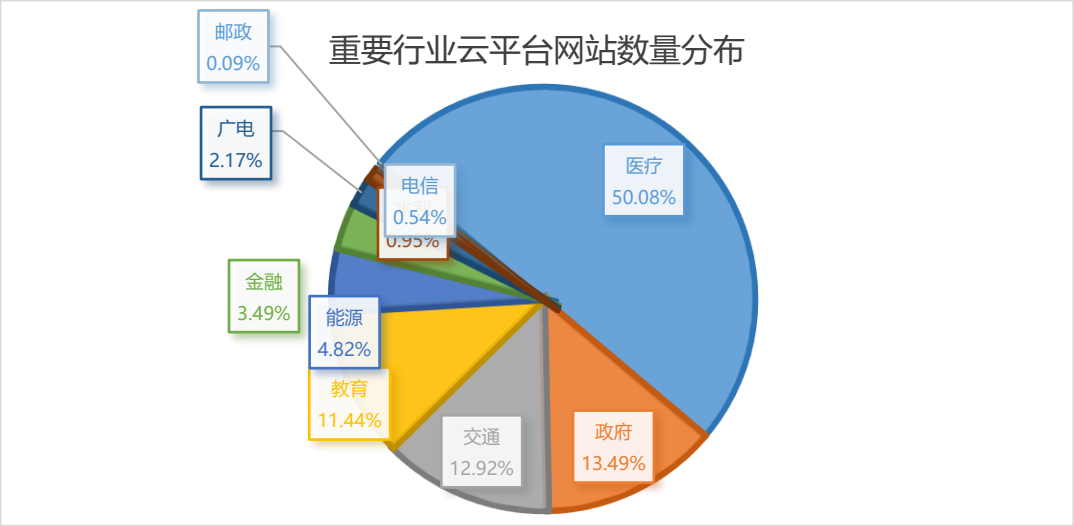

图 3 重要行业云平台网站数量分布

目前国内已有 14.66%的重要行业网站已经上云，并且主要是医疗与政府行业。这一方面是大量互联网医疗等新型医疗企业的开办，另一方面也是由于云资源的便捷性与价格更廉价。

三、云安全面临威胁的总体状况

1. 云平台侧面临的安全威胁

云计算平台安全与传统信息安全并无本质区别，但是云计算大量使用虚拟资源、资源界面不确定、动态数据流等特性，相对于传统信息安全，云计算新的安全威胁主要来自硬件资源、软件资源、基础资源的集中，针对这些庞大的资源无法实现有效保护，例如，云平台使云上用户的重要数据和业务应用都处于云服务提供商或运营建设方的云平台环境中，云服务提供商如何实施严格安全管理和访问控制措施，

避免内部员工或者其他使用云服务的用户、入侵者等对云内数据的窃取及滥用的安全风险。如何实施有效的安全审计、对数据的操作进行安全监控，以及开放环境中如何保证数据连续性，业务不中断等，这些都是需要重点考虑的问题。总体来看，云计算平台侧主要面临以下威胁。

1.1 数据物理集中，安全风险高

云计算平台离不开物理基础设施的建设，云计算数据中心也可归为传统数据中心 IT 机房的范畴。随着大量云计算数据中心的建设，逐步实现了各区域各节点基础设施的集中化管理，由小变大的运营方式带来了比传统 IT 机房环境更多的安全风险:

- 云计算数据中心依然面临传统安全中主要的安全风险威胁，如物理边界安全、非授权访问检测、人员识别和入侵检测响应等
- 云计算数据中心的数据相对集中，更容易遭受地震、水灾、火灾等不可抗拒的自然灾害破坏
- 云计算数据中心面临严峻的安全管理风险，数据中心的存储介质和设备一旦被毁或被盗，将造成信息泄漏及数据丢失事故
- 云计算通过网络传输各类型数据，用户和云服务器一般不在同一个区域，数据传输过程面临被非法窃取、破坏和修改的挑战

1.2 网络隔离和监测非常困难

对于现阶段大型数据中心的云平台，出于操作和安全的原因，将云的网络进行隔离和监控是非常重要的，对于云平台来说，至少要包含以下五个方面的隔离和监测:

- 不同云租户网络之间的隔离和监测
- 同一云租户不同虚拟机之间的隔离和监测
- 虚拟机和互联网边界之间的隔离和监测
- 存储网络与业务网络之间的隔离和监测
- 管理网络和业务网络之间的隔离和监测

而在云平台实际运行过程中，要实现这 5 个部分的隔离和监测还是非常困难，这有些是受制于目前安全技术的发展，也有一些是因为网络设计的限制。比如，传统的网络入侵检测系统（IDS），在传统网络中，是通过交换机镜像的方式采集流量进行监控，但在云环境中，入侵检测系统就非常难采集到流量进行监控，因为虚拟机之间的流量交互可能直接在某个宿主机上就完成了，根本不会到物理交换机上，所以通过传统的镜像方式根本无法监控。

1.3 宿主机和虚拟机之间存在相互影响

云计算环境下，用户大部分业务的运行载都是云主机，而云主机又运行于宿主机之上，云主机一旦发生安全事故，将会直接或间接地影响到宿主机，如虚拟机逃逸问题，进而

将直接威胁到用户的整个业务系统的安全性，通常云环境下存在以下安全风险:

- 服务器、宿主机、虚拟机的操作系统和数据库被暴力破解、非法访问
- 对服务器、宿主机、虚拟机等进行操作管理时被窃听
- 同一个逻辑卷被多个虚拟机挂载导致逻辑卷上的敏感信息泄漏
- 服务器、宿主机、虚拟机的补丁更新不及时导致的漏洞利用以及不安全的配置和非必要端口的开放导致的非法访问和入侵
- 虚拟机因异常原因产生的资源占用过高而导致宿主机或宿主机下的其他虚拟机的资源不足

1.4 大数据带来了大威胁

数据安全是信息和数据治理的关键。与云安全所有领域一样，由于数据安全并不适合对所有内容提供同等保护，所以应基于风险应用数据安全。

应用数据安全是目前云计算用户最为担心的安全风险，也是用户数据泄漏的重要途径。因此有一些人认为，云安全就是数据安全。

用户数据在云计算环境中进行传输和存储时，用户本身对于自身数据在云中的安全风险并没有实际的控制能力，数据安全完全依赖于服务商，如果服务商本身对于数据安全的

控制存在疏漏，则很可能导致数据泄漏或丢失。现阶段可能导致安全风险的有以下几种典型情况:

- 由于服务器的安全漏洞导致黑客入侵造成的用户数据丢失
- 由于虚拟化软件的安全漏洞造成的用户数据被入侵的风险
- 数据在传输过程中没有进行加密导致信息泄漏
- 加密数据传输但是密钥管理存在缺失导致数据泄漏
- 不同用户的数据传输之间没有进行有效隔离导致数据被窃取
- 用户数据在云中存储没有进行容灾备份等

云计算服务商在对外提供服务的过程中，如果运营商的身份认证管理机制存在缺陷，或者运营商的身份认证管理系统存在安全漏洞，则可能导致企业用户的账号密码被仿冒，从而使得非法用户堂而皇之地对企业数据进行窃取。因此，如何保证不同企业用户的身份认证安全，是保证用户数据安全的第一道屏障。

2. 云租户侧面临的安全威胁

2.1 网络攻击威胁

云环境下，云租户的业务都由云平台承载，而不法分子也会通过对云平台的攻击，对云租户的业务安全造成威胁。

通常云环境下，存在以下威胁:

- 业务高峰时段或遭遇DDoS攻击时的大流量导致网络拥堵或网络瘫痪
- 重要网段暴露导致来自外部的非法访问和入侵
- 单台虚拟机被入侵后对整片虚拟机进行的渗透攻击，并导致病毒等恶意行为在网络内传播蔓延
- 虚拟机之间进行的 ARP 攻击、嗅探
- 云内网络带宽的非法抢占
- 重要的网段、服务器被非法访问、端口扫描、入侵攻击
- 云平台管理员因账号被盗等原因导致的从互联网直接非法访问云资源
- 内部用户或内部网络的非法外联
- 内部用户之间或者虚拟机之间的端口扫描、暴力破解、入侵攻击等

2.2 主机攻击威胁

云环境下，用户的业务都由云主机承载，云主机的安全问题将直接威胁到用户的整个业务系统的安全性，通常云环境下存在以下安全风险:

- 服务器、宿主机、虚拟机的操作系统和数据库被暴力破解、非法访问
- 对服务器、宿主机、虚拟机等进行操作管理时被窃听

- 同一个逻辑卷被多个虚拟机挂载导致逻辑卷上的敏感信息泄露
- 服务器、宿主机、虚拟机的补丁更新不及时导致的漏洞利用以及不安全的配置和非必要端口的开放导致的非法访问和入侵
- 虚拟机因异常原因产生的资源占用过高而导致宿主机或宿主机下的其它虚拟机的资源不足

2.3 应用安全威胁

对于提供各种云服务（IaaS、PaaS、SaaS）的供应商而言，第一，Web 应用安全方面，由于云服务选择将 Web 作为绝大多数应用的入口，因而其面临的各种攻击可能都会转嫁至云应用上；第二，应用内容安全方面，云计算通过互联网提供服务，网络上的信息内容安全问题（恶意邮件、虚假欺诈信息等）将不可避免地影响云服务的信誉；第三，用户管理方面，当前云应用中简单的身份认证和不严格的访问控制给许多黑客提供了可趁之机云环境下。综上而言，用户的云上应用面临各种各样的安全威胁问题:

- Web 应用入侵、上传木马、上传 Webshell 等攻击
- 网页被恶意篡改，展示敏感或不当内容
- 权限认证和访问控制机制缺失，容易渗入云内
- 应用对外接口被利用，对云平台进行攻击
- 应用系统健康状况不明确

2.4 数据安全威胁

在传统环境下，用户的数据和业务系统都位于自己的数据中心，在其直接管理和控制范围之内。但是在云计算环境里，用户的数据和业务系统都迁移到了云上，使得数据的所有权和管理权分离。又由于云计算技术架构在传统服务器设施上，所以传统 IT 架构上的数据安全问题都有可能在云计算中出现，因此，在云环境下，数据生命周期的每个阶段都会出现一系列新的数据安全问题。云上的数据安全通常存在以下风险:

- 数据在传输过程中受到破坏而无法恢复
- 在虚拟环境传输的文件或者数据被监听
- 云用户从虚拟机逃逸后获取镜像文件或其他用户的隐私数据
- 因各种原因或故障导致的数据不可用
- 敏感数据存储漂移导致的不可控
- 数据安全隔离不严格导致恶意用户可以访问其他用户数据

四、上半年云端威胁态势分析

随着云计算的快速发展，越来越多的企事业单位和业务场景向云平台上迁移，大量的应用系统聚集到云平台上。不

少单位认为云服务商提供的基础安全防护策略已经足以应对网络安全，因而疏于本单位的运维管理，甚至部分云网站由于没有管理人员进行运维已经逐渐成为僵尸网站。但实际上，云上网站依旧面临着系统架构、非硬件层的故障、系统性能、数据安全等众多安全问题，各种网页篡改、不良信息等网站入侵问题依旧是无法避免的。本章针对 2020 年云端 DDoS 攻击态势和云端 Web 应用面临的威胁进行分析。

1. 云端 DDoS 攻击态势分析

当前，攻击者使用虚假身份开设云帐户，或者利用漏洞攻陷云端系统发起 DDoS 攻击越来越普遍。今年上半年，来自云端的 DDoS 攻击源占所有攻击源的 14%，占所有流量的 22%。

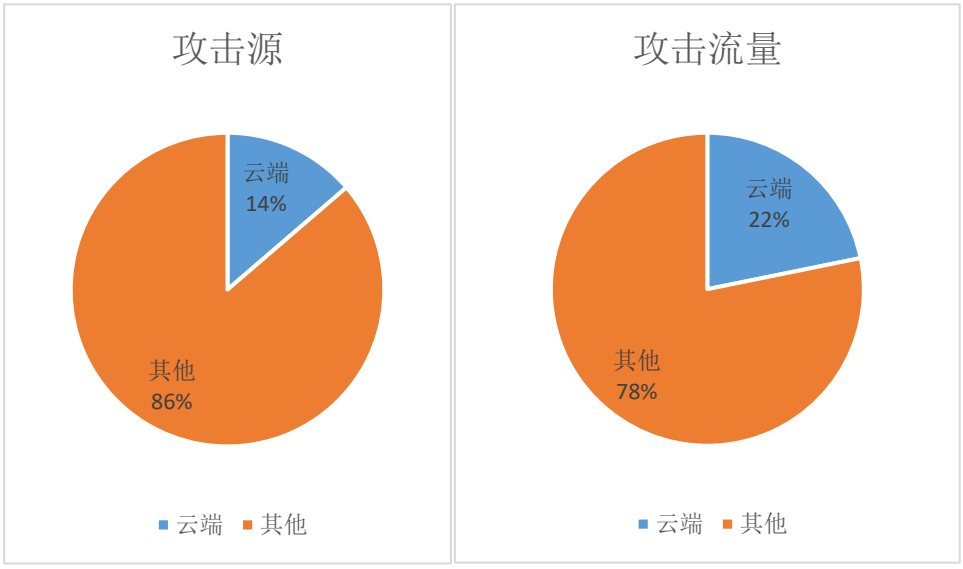

图 4 云端 DDoS 占比

云计算技术的诸多优点使得云服务得以广泛应用，越多来越多的用户将业务迁移至云端，云端的流量也越来越大，

但这也被大流量 DDoS 攻击所利用。从各流量区间分布来看，在大流量攻击中，攻击主力来自云端。

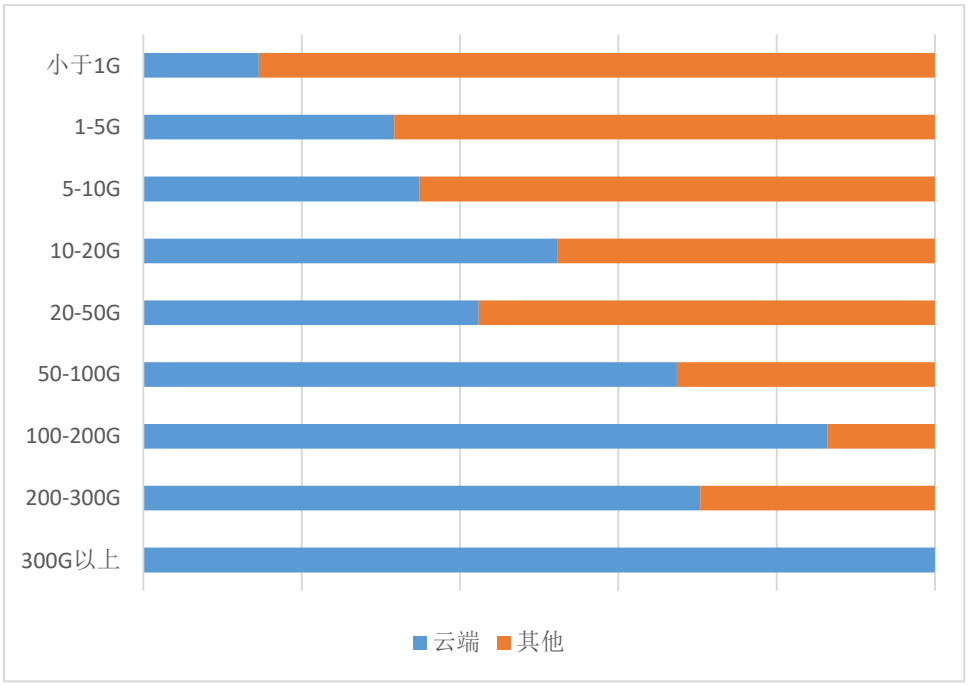

图 5 各流量区间分布

在攻击峰值在 100Gbps 以上的大型攻击中，来自云端的攻击占比 77%。

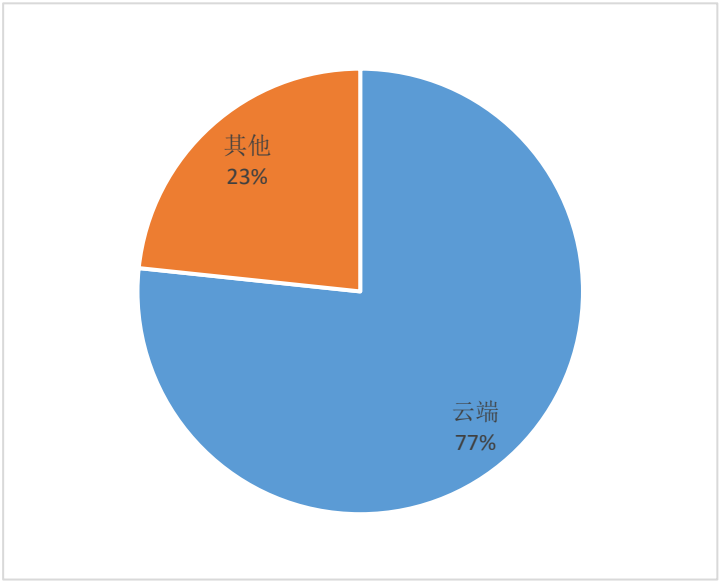

图 6 100Gbps 以上的大型攻击占比

从上半年各月来看，云端攻击源数量逐月上升，从攻击次数来看，三、四月份为云端 DDoS 攻击高峰，从攻击峰值来看，五月峰值最高为 634.6Gbps。

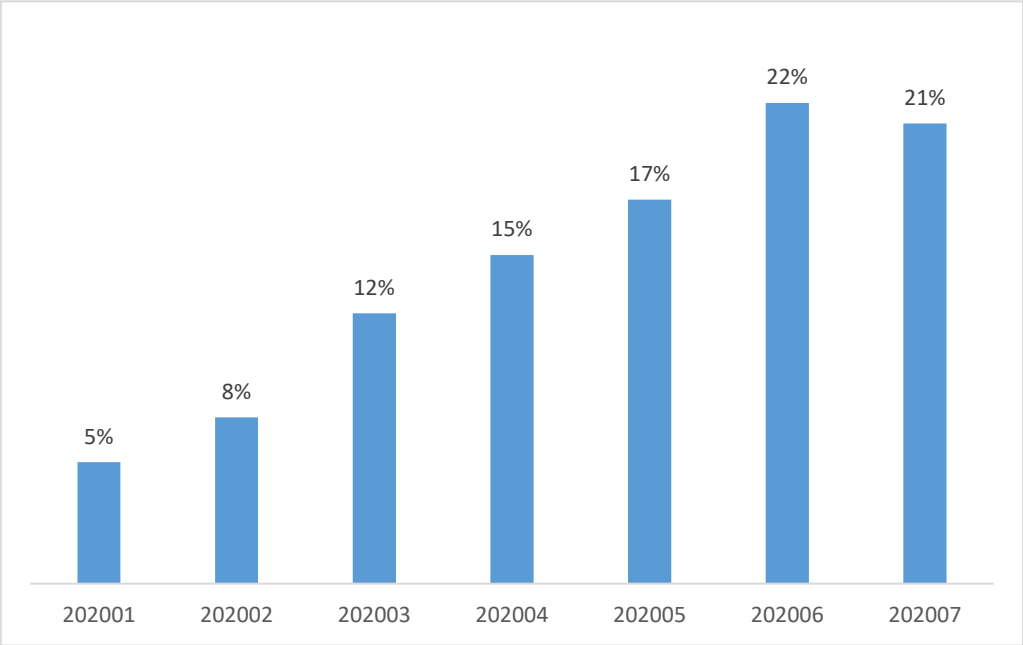

图 7 云端攻击源占比

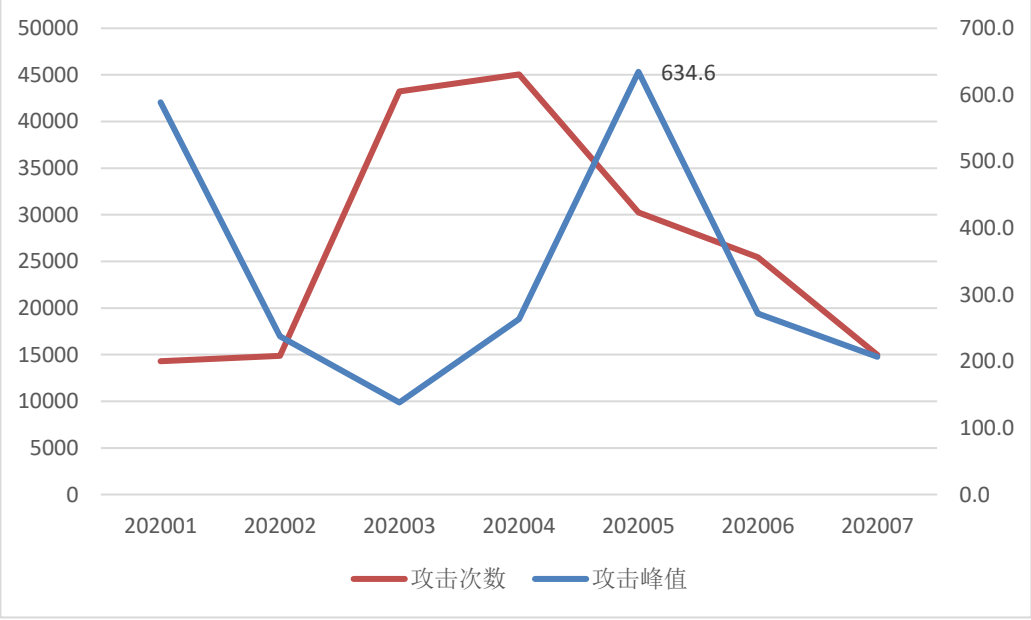

图 8 云端攻击态势

从攻击类型来看，云端 DDoS 主要的攻击类型是 SYN

Flood，占总攻击次数的 37%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 91%。

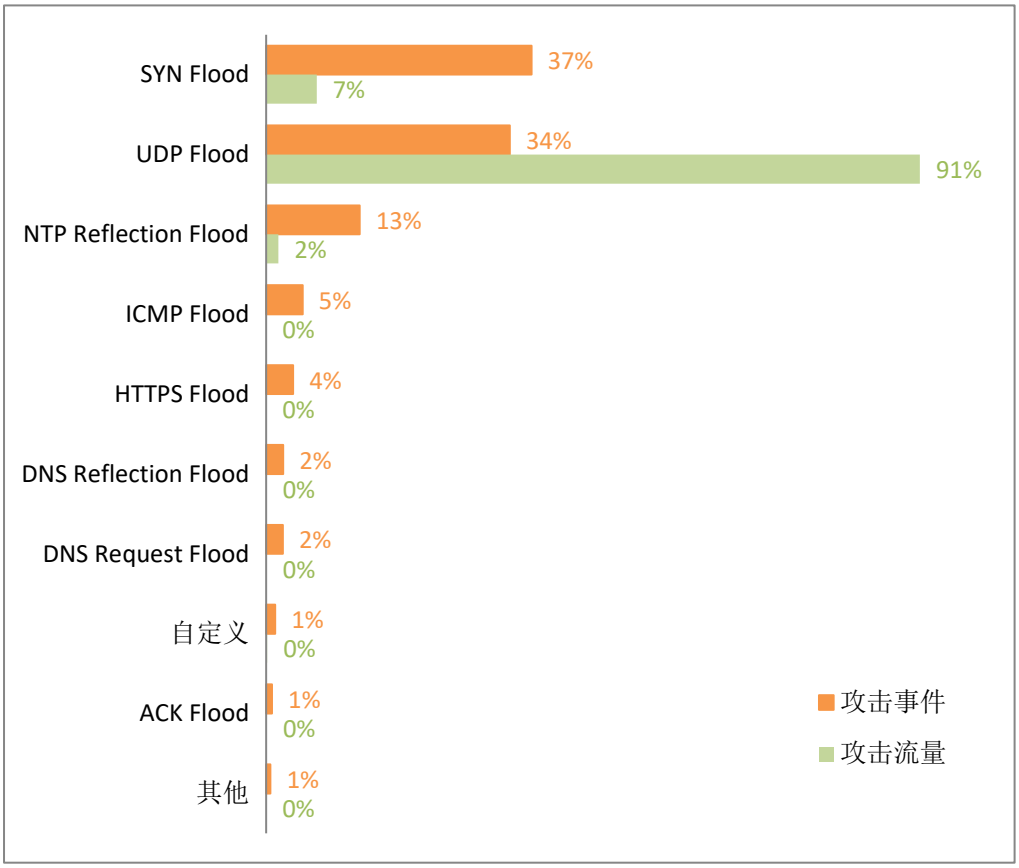

图 9 云端攻击类型

2. 云端 Web 应用威胁分析

2.1 威胁整体概况

2.1.1 安全事件数量趋势

2020 年上半年，主要针对网页篡改、不良信息和僵尸网站等进行监测，累计发现云端 Web 应用安全事件数量 18,257 起，覆盖单位 10,324 个，每个月的安全事件影响单位数情况如下。

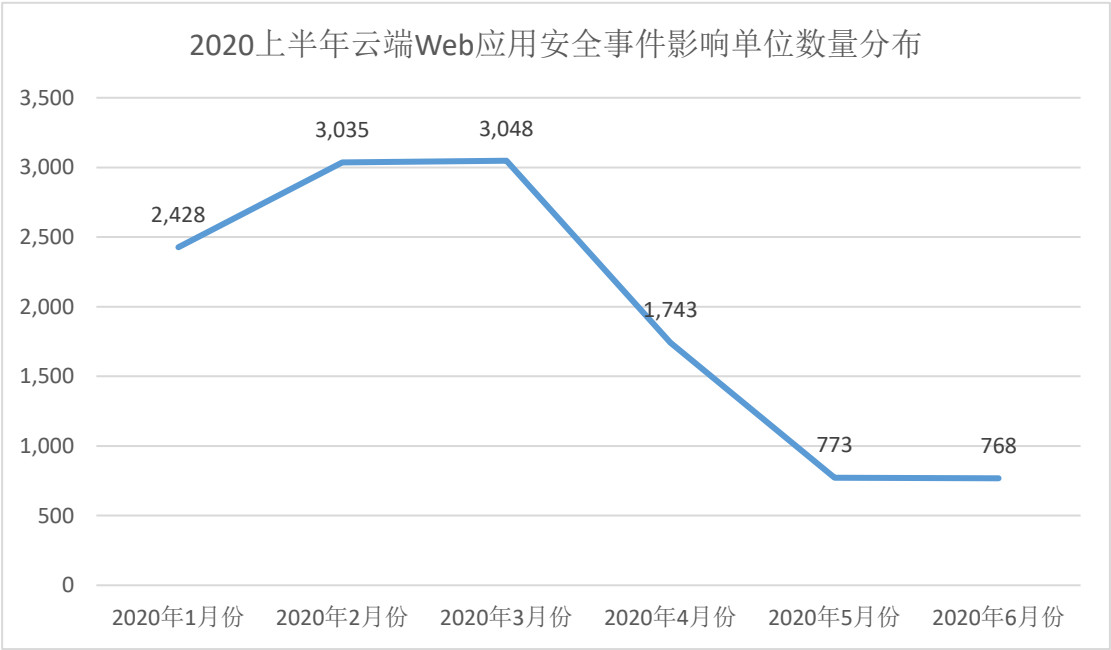

图 10 安全事件影响单位数情况

总体来看，从 1 月份开始云端 Web 应用安全事件呈上升趋势，在 2-3 月份安全事件数量达到高峰，随后逐步下降，整体攻击趋势与疫情发展情况存在一定的同步。

2.1.2 安全事件类型分布

对云端 Web 应用存在的安全事件类型进行统计，主要是以僵尸网站为主，其次不良信息类资产（黄赌毒类站点）与网页篡改均占有较大比重。

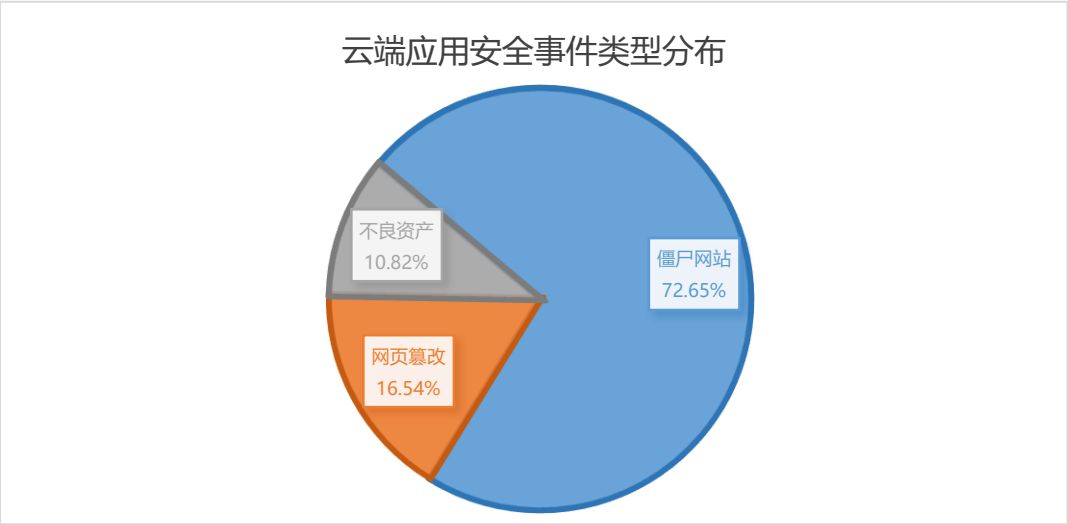

图 11 云端 Web 应用存在的安全事件类型

分析发现云端 Web 应用存在大量的僵尸网站情况，僵尸网站的存在往往是网站所属单位疏于对网站的管理，网站无法提供有效的服务信息，此类站点无人运营，漏洞修复不及时，防护措施不到位，容易产生安全事件，需要尽快整治。

2.1.3 安全事件区域分布

根据对存在安全事件的云端 Web 应用 IP 所在区域进行分析，发现主要分布在北京、浙江、广东等区域。

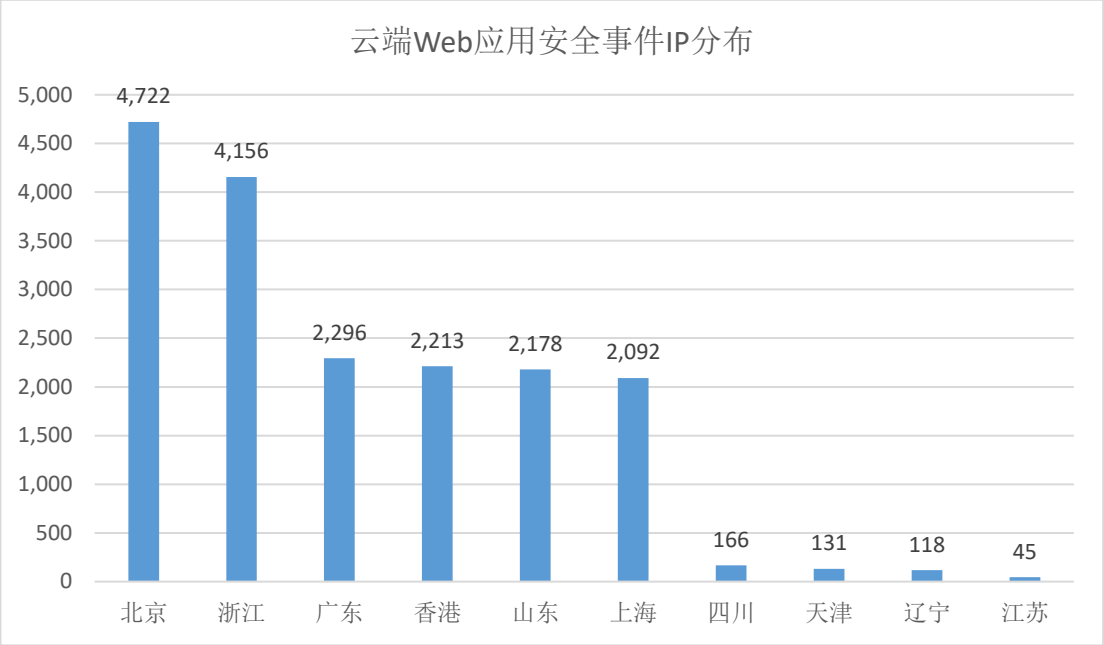

图 12 云端 Web 应用安全事件 IP 分布

2.2 安全事件重点行业情况

2.2.1 安全事件行业分布

存在安全事件的云平台网站中，有 1033 个为重要行业网站，重要行业云平台网站安全事件情况如下。

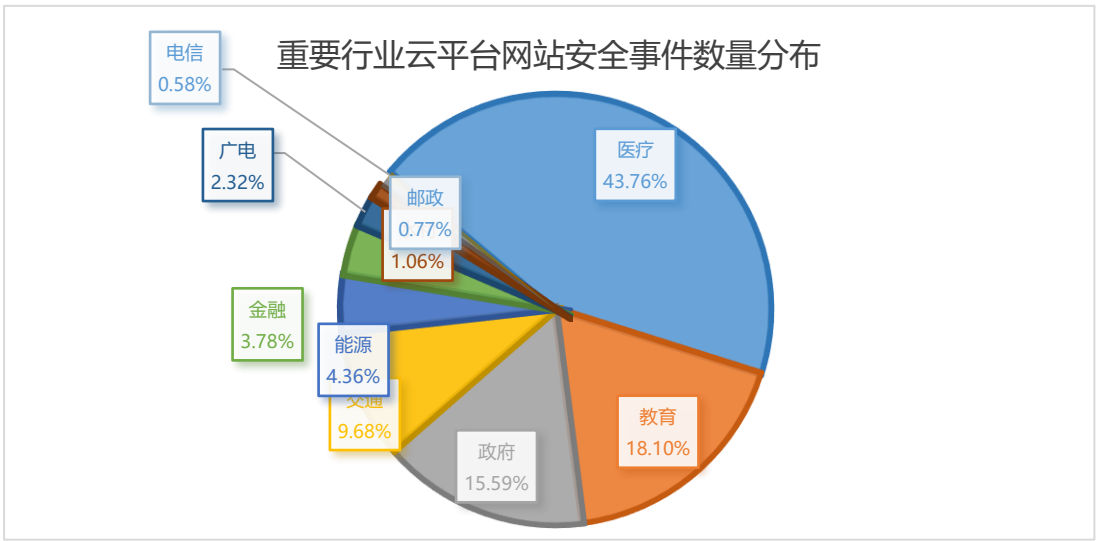

图 13 重要行业云平台网站安全事件数量分布

分析发现，主要受影响的重要行业为医疗，占比 43.76%，

此外教育和政府行业也有一定的影响。

2.2.2 医疗行业受影响情况

2020 年上半年，监测发现医疗行业云端 Web 应用安全事件数量有 452 起，覆盖单位 257 个，每个月的安全事件影响医疗行业单位数情况如下。

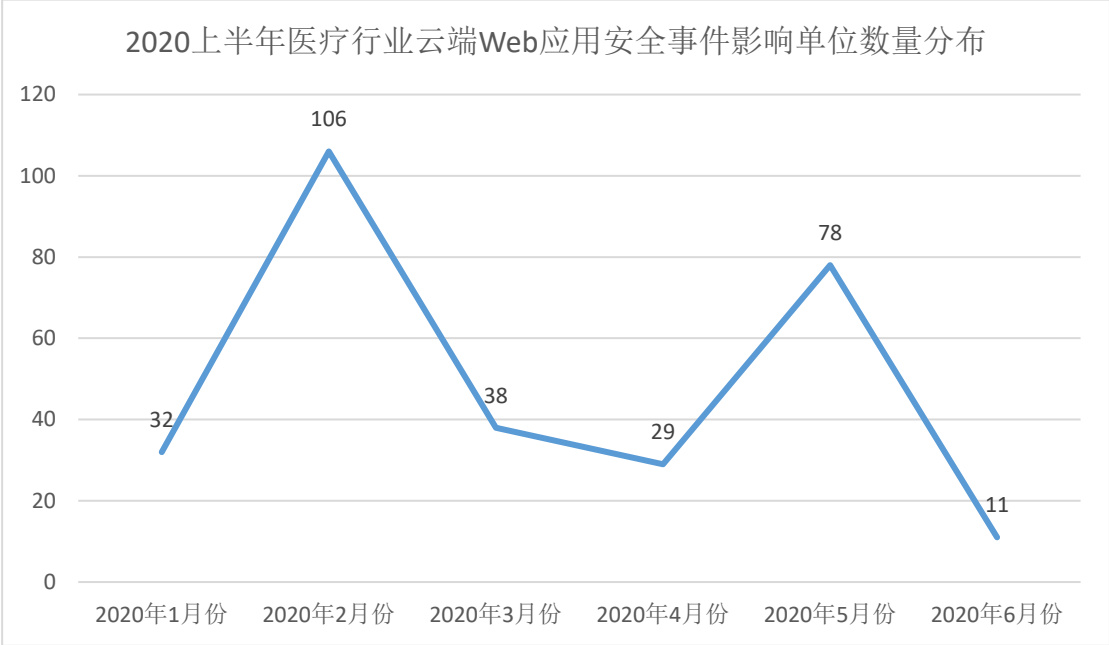

图 14 医疗行业云端 Web 应用安全事件影响单位数量

总体来看，从 1 月份开始云端 Web 应用安全事件呈上升趋势，在 2 月份安全事件数量达到高峰，随后逐步下降，在 5 月份有一定回弹。

根据对存在安全事件的云端 Web 应用 IP 所在区域进行分析，发现主要分布在北京、广东、浙江等区域，与整体安全事件情况基本吻合。

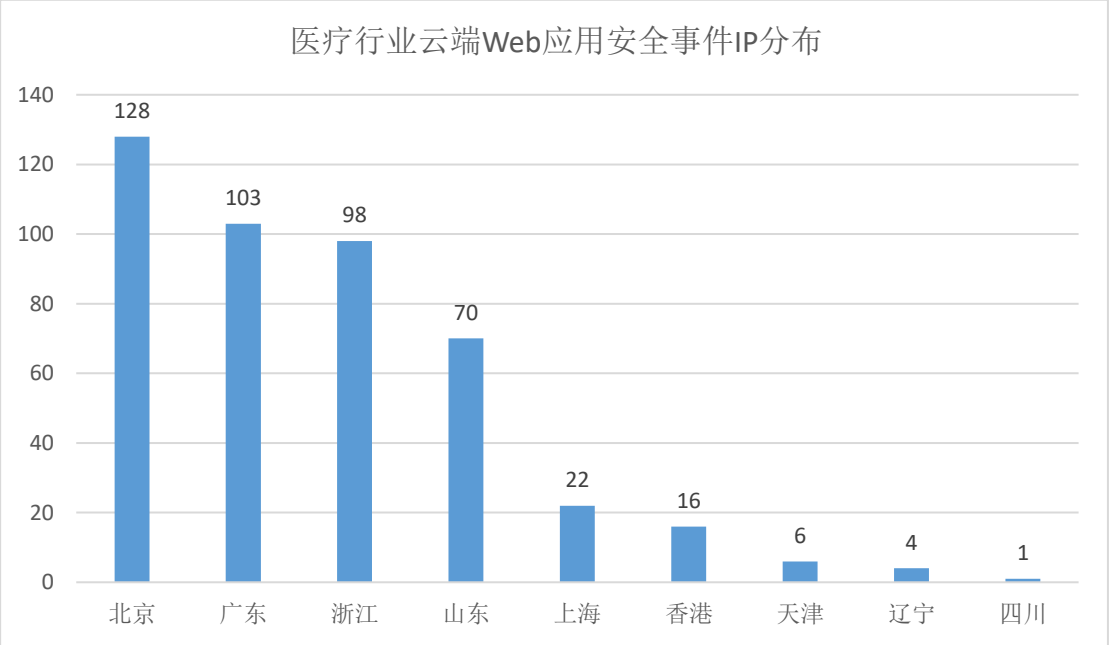

图 15 医疗行业云端 Web 应用安全事件 IP 分布

对医疗行业云端 Web 应用存在的安全事件类型进行统计，主要以网页篡改为主，其次为僵尸网站。

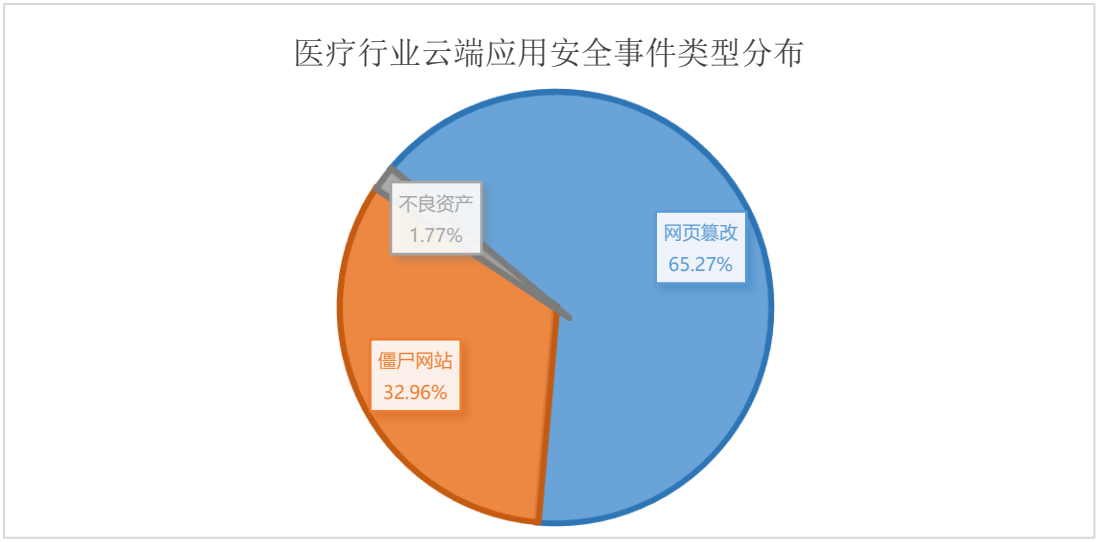

图 16 医疗行业云端 Web 应用安全事件类型分布

网页篡改往往是由于黑客利用网站存在的漏洞或对网页内容进行恶意破坏，插入非正常网页内容，建议网站管理单位对安全事件再次确认，并进行溯源分析，由专业安全公司做一次攻击渗透测试后再重新上线，同时需要加强网站的

日常安全管理工作。

对医疗行业云端 Web 应用安全事件所属云服务厂商进行统计分析，87.39%为阿里云的网站。

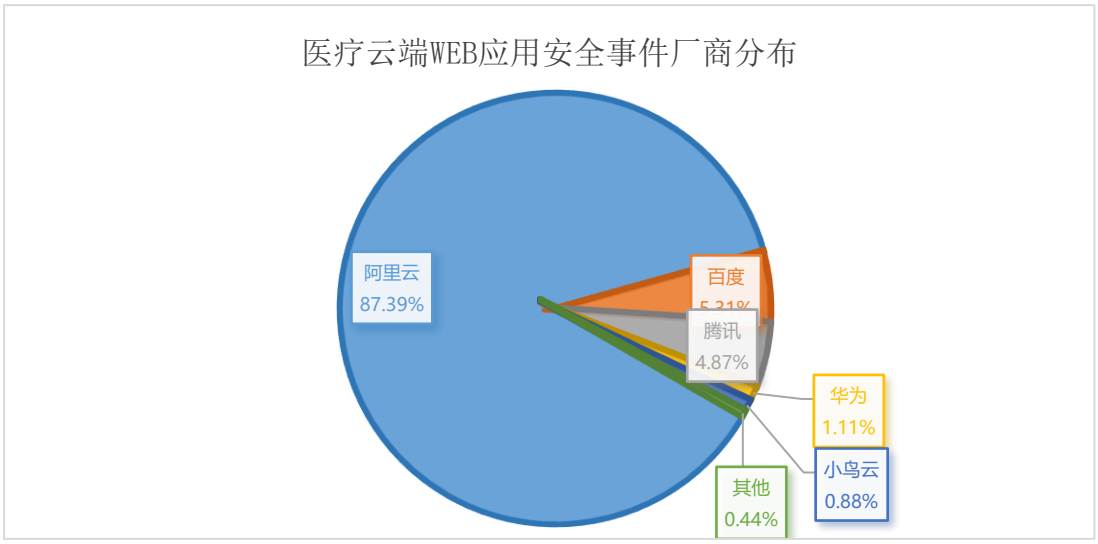

图 17 医疗行业云端 Web 应用安全事件厂商分布

2.2.3 教育行业受影响情况

2020 年上半年，监测发现教育行业云端 Web 应用安全事件数量有 186 起，覆盖单位 134 个，每个月的安全事件影响教育行业单位数情况如下。

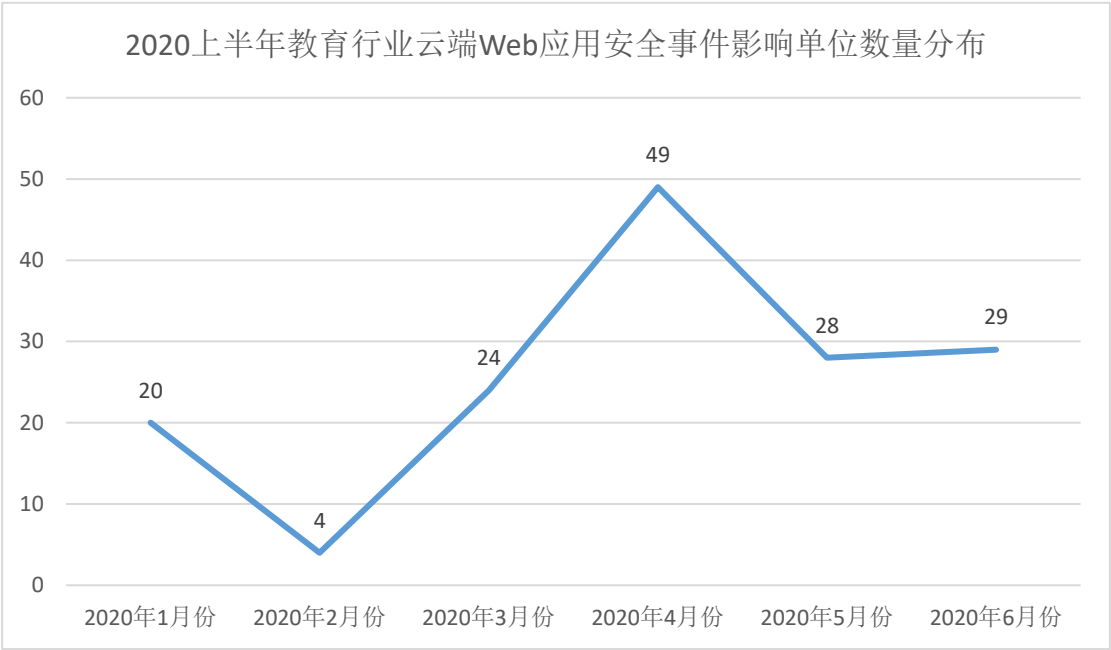

图 18 教育行业云端 Web 应用安全事件影响单位数量分布

根据对存在安全事件的云端 Web 应用 IP 所在区域进行分析，发现主要分布在北京、山东、浙江等区域。

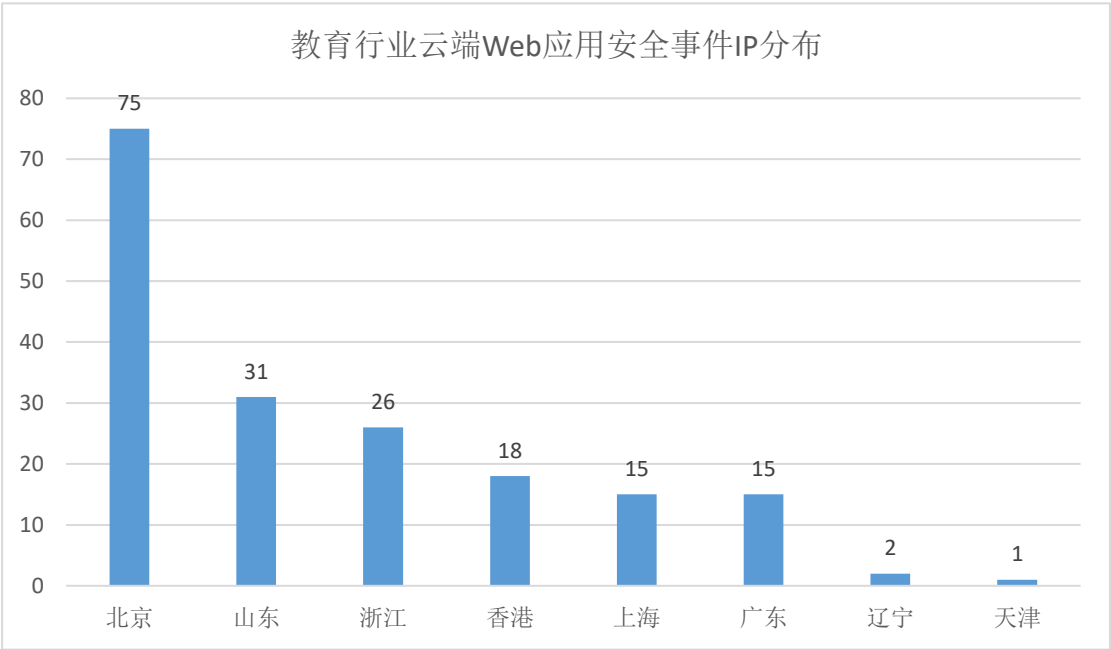

图 19 教育行业云端 Web 应用安全事件 IP 分布

对教育行业云端 Web 应用存在的安全事件类型进行统计，主要以网页篡改为主，其次为僵尸网站。

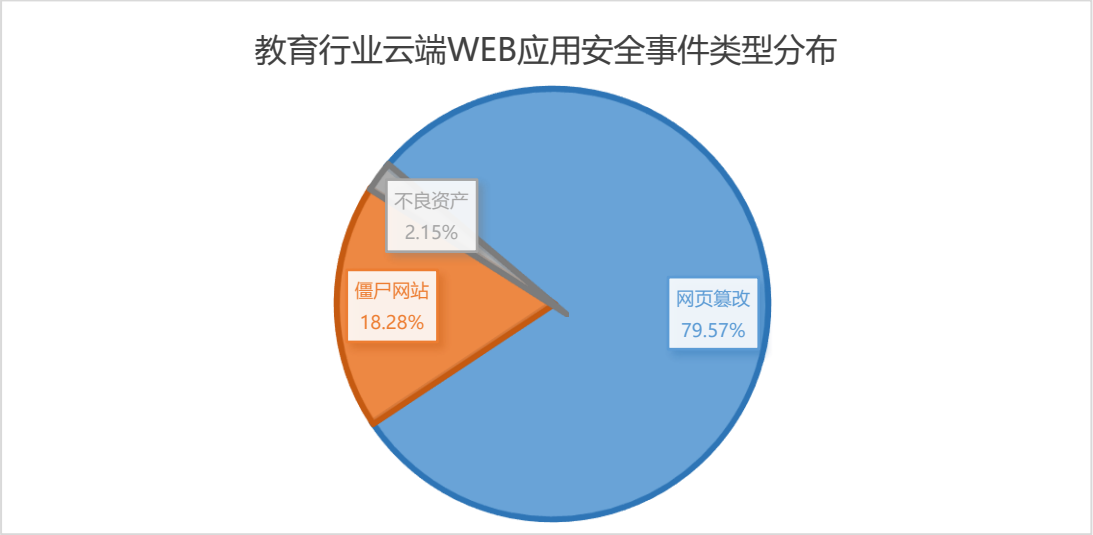

图 20 教育行业云端 Web 应用安全事件类型分布

网页篡改往往是由于黑客利用网站存在的漏洞或对网页内容进行恶意破坏，插入非正常网页内容，建议网站管理单位对安全事件再次确认，并进行溯源分析，由专业安全公司做一次攻击渗透测试后再重新上线，同时需要加强网站的日常安全管理工作。

对教育行业云端 Web 应用安全事件所属云服务厂商进行统计分析，69.89%为阿里云的网站。

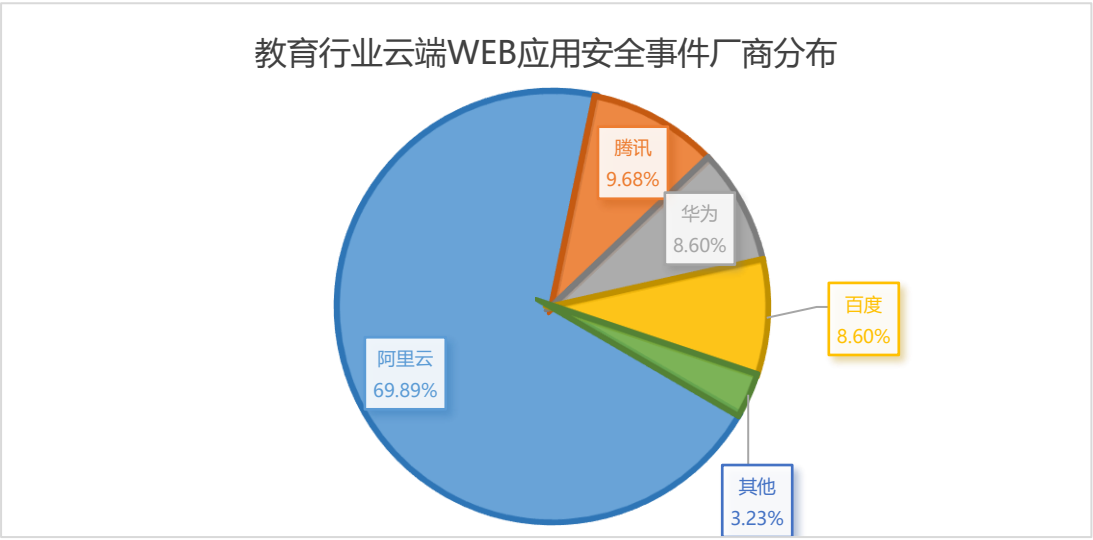

图 21 教育行业云端 Web 应用安全事件厂商分布

2.2.4 政府行业受影响情况

2020 年上半年，监测发现政府行业云端 Web 应用安全事件数量有 161 起，覆盖单位 97 个，每个月的安全事件影响政府行业单位数情况如下。

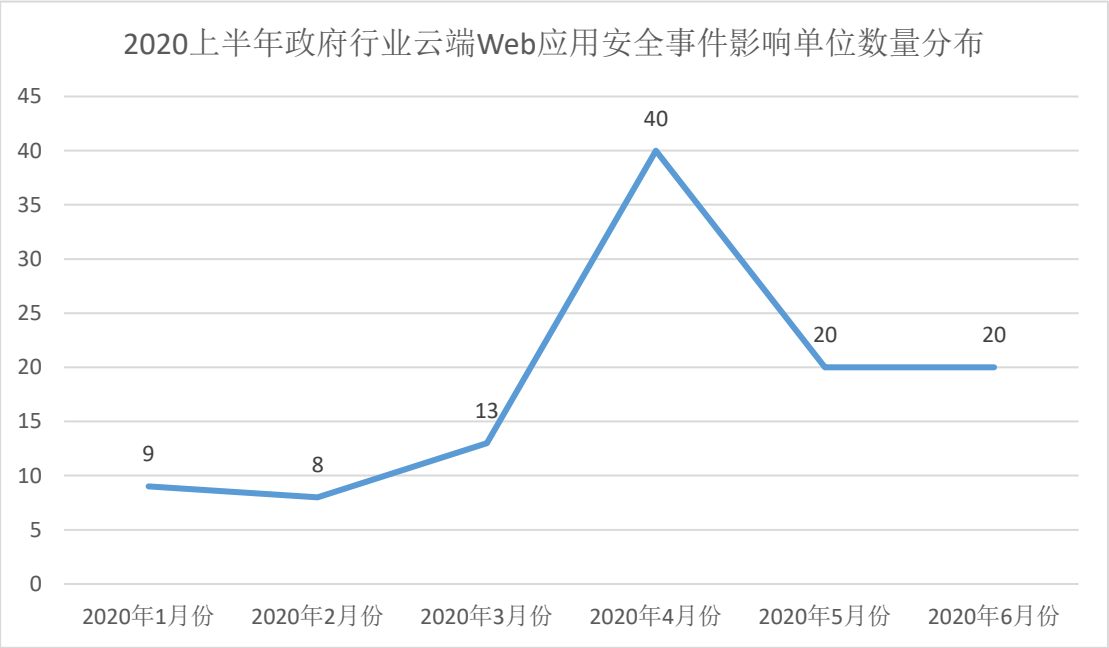

图 22 政府行业云端 Web 应用安全事件影响单位数量分布

根据对存在安全事件的云端 Web 应用 IP 所在区域进行分析，发现主要分布在浙江、山东、北京等区域。

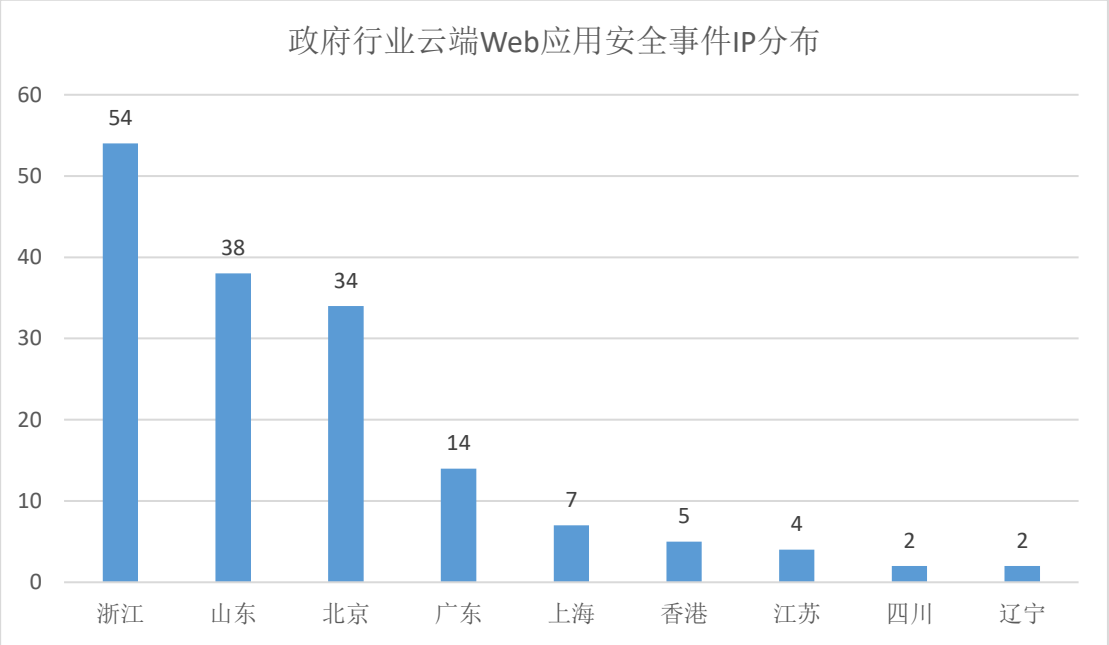

图 23 政府行业云端 Web 应用安全事件 IP 分布

对政府行业云端 Web 应用存在的安全事件类型进行统计，主要以网页篡改为主，其次为僵尸网站。

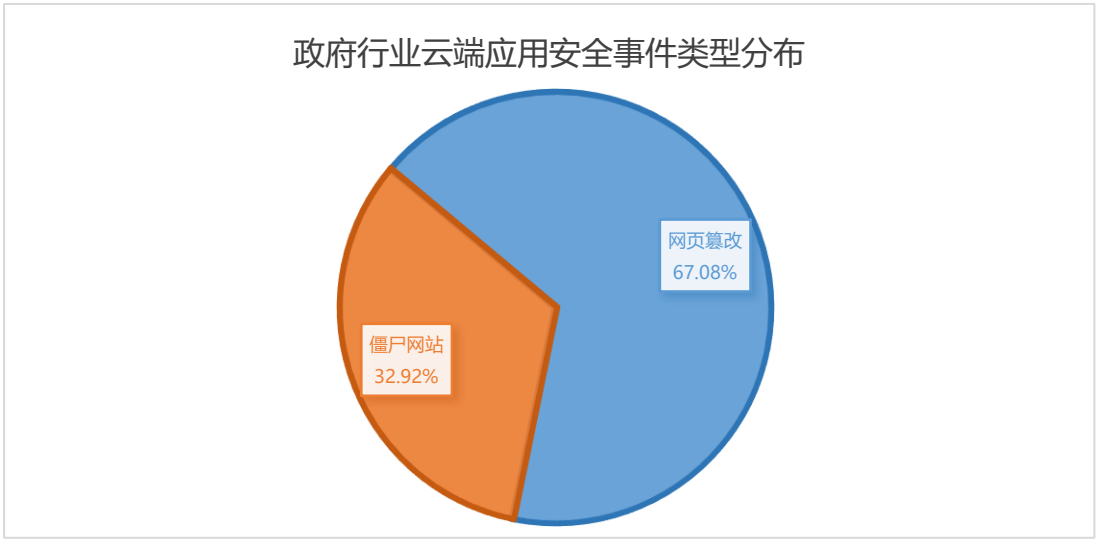

图 24 政府行业云端 Web 应用安全事件类型分布

对政府行业云端 Web 应用安全事件所属云服务厂商进行统计分析，79.50%为阿里云的网站。

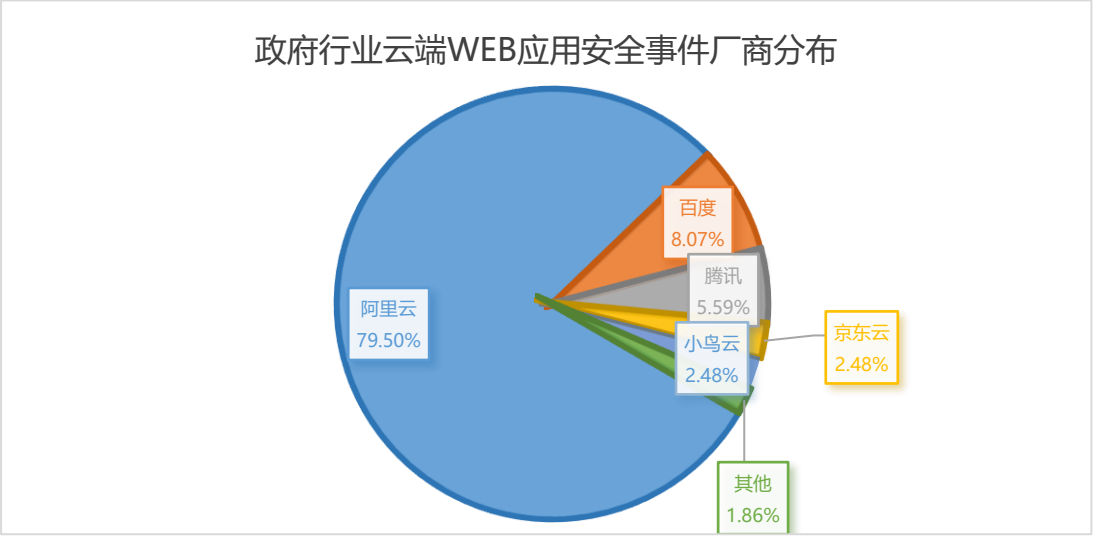

图 25 政府行业云端 Web 应用安全事件厂商分布

五、未来云安全面临的挑战

IDC 以及业界多位专家对未来的云计算发展趋势进行了评估预测，研究表明，多云及混合云模式将逐渐成为主导。云计算的不可知论将在 2020 年继续增长。根据企业的技术和业务需求，企业将针对不同的应用工作负载使用多个公有云和私有云，并将公有云与内部部署基础设施结合使用，同时考虑许多其他因素。这其中的关键是，整合多云基础设施，使其能够无缝协作。

市场上云服务厂商众多，用户往往将业务部署在多个云平台上，多云和混合云的场景逐渐成为云计算行业应用的发展趋势，并且在国内市场上将会长期存在。因此，多云或混合云环境下的云安全管理和云安全攻击风险将成为未来云安全领域面临的新挑战。

1. 云安全管理风险和挑战

对于云平台而言，云安全产品和云安全管理相当于其左膀右臂。在传统的信息服务平台中，安全管理主要负责监视和记录系统中的服务器、网络设备以及所有应用系统的安全状况。和传统平台相比，云安全管理需要进行的监管范围更大，所需要的监管力度也更强，它需要负责监视和记录云平台中重要的服务器、网络设备及所有应用的安全情况，也需要对所涉及的计算机、网络以及应用系统的安全机制实施统一管理、统一监控、协同防护，从而发挥安全机制的整体作用。

1.1 多云环境无法有效管理

现阶段，政务云的建设过程中，每个云服务商往往会为政府单位量身打造政务云平台，在实际使用时，多云之间的壁垒问题十分严重，多云难以实现真正的连通，无法通过统一视角对多云环境及多云的资源进行有效的可视化管理。

1.2 多云安全运维管理困难

传统环境下，大部分安全产品以硬件的形式交付给客户，安全产品也是采用分散管理的形式，而在多云环境下，存在着成千上万的云上资产，对于运维人员来说是十分大的挑战和考验，传统的运维方式效率低且容易出错，难以适应多云的环境。

1.3 多云平台建设成本高

多个云服务商基于自身提供的云平台共同打造一朵具有特色的政务云，但多云的环境存在大量云基础设施重复性投资建设，建设成本较高，且资源无法实现共享和高效利用。

1.4 安全责任界定不清

传统模式下，信息系统通常遵照谁主管谁负责、谁运行谁负责的原则，信息安全责任相对清晰。在云计算模式下，云计算平台的管理和运行主体（云服务提供方）与云端信息系统及数据的责任主体（云租户）不同，相互之间的责任难以界定，服务模式的改变、部署模式的差异、云计算环境的复杂性都增加了界定云服务提供方与云租户之间责任的难度。

1.5 需求不确定性问题

云环境下，云平台管理者在云平台建设初期一般不清楚各个云租户的业务规模，也不清楚各个租户的安全需求。因此管理者很难精确的判断采购的安全产品种类、安全产品数量和安全产品性能，安全建设规划困难。

2. 云安全攻击风险和挑战

2.1 AI 致使云安全黑灰化

近几年，由于人工智能等技术的快速发展，深度学习神经网络日趋成熟， AI 逐步开始替代许多劳动密集型工作，

与此同时，全球针对云计算的黑灰产也日渐活跃。研究表明，通过云端提供的 GPU 高智能高密度智能服务结合智能算法来训练恶意攻击模型的事例越来越多。可以预见，未来一到两年云安全领域将不得不面临如何和 AI 斗智斗勇的问题。

2.2 未知风险漏洞风险周期变短

互联网存在大量已知漏洞，软硬件也不可避免存在些许 Bug，由于黑客技术手段的不断完善，针对新漏洞的探测和利用周期正在逐渐变短。过去针对新漏洞的大规模扫描需要过几天才会出现，而现在往往在新漏洞被发现的第一时间，就会已经爆发安全事故，导致企业的开发和安全运维人员几乎无法在合理的短时间内完成打补丁操作来应对安全威胁。

2.3 网络犯罪国际化

东南亚、欧美等地区的部分国家渐渐成为赌博、诈骗类犯罪的温床，例如曾出现的“东南亚杀猪盘”诈骗，以情感欺诈为切入口，再利用云上的博彩、非法交易等形式，诱骗对方充值，一旦对方被骗，网站会自动销毁。对云服务商来说，如何监管并减少用户在线运营非法业务，也是一场持久战。

2.4 云内的针对性勒索愈演愈烈

自 2017 年“永恒之蓝”漏洞曝光伊始，勒索病毒开始了 3 年的黄金期，大量云平台上的资产或服务都遭遇过恶意

勒索。从 2020 上半年发展趋势来看，除了广撒网式的勒索之外，针对性勒索也逐渐增多。黑客通过主动渗透方式针对云内资产尤其是云内东西向进行恶意软件传播，肆意蔓延，加密数据并勒索高额赎金，对云内的资产及服务影响严重。针对性勒索未来可能占比更大。

六、云安全防范措施及建议

1. 不同云服务模式下的云安全建设

无论是云服务的 IaaS、PaaS，还是 SaaS 模式，安全责任总是分为两部分，一部分是由云计算服务提供商承担，另一部分则由云上客户来承担。由于云服务模式的局限性，操作系统、应用和数据在预设场景下是无法管控的，所以云上的用户需要与云服务提供商和安全厂商协同作战。

对 IaaS 服务来说，云服务商保障物理环境、网络环境等基础设施的安全和虚拟化层面的安全，而云上用户主要负责保障操作系统、应用程序和数据的安全;

对 PaaS 服务来说，底层基础设施安全和操作系统安全归云服务商负责，云上用户只需要负责应用程序和数据安全;

对 SaaS 服务来说，云上用户主要负责自身的应用安全和数据安全，而其他的所有部分都是由云服务商来保障。

综上所述，根据安全责任模型和云计算服务模型，云安全大致可分为云平台安全和云上安全两部分，具体如下。

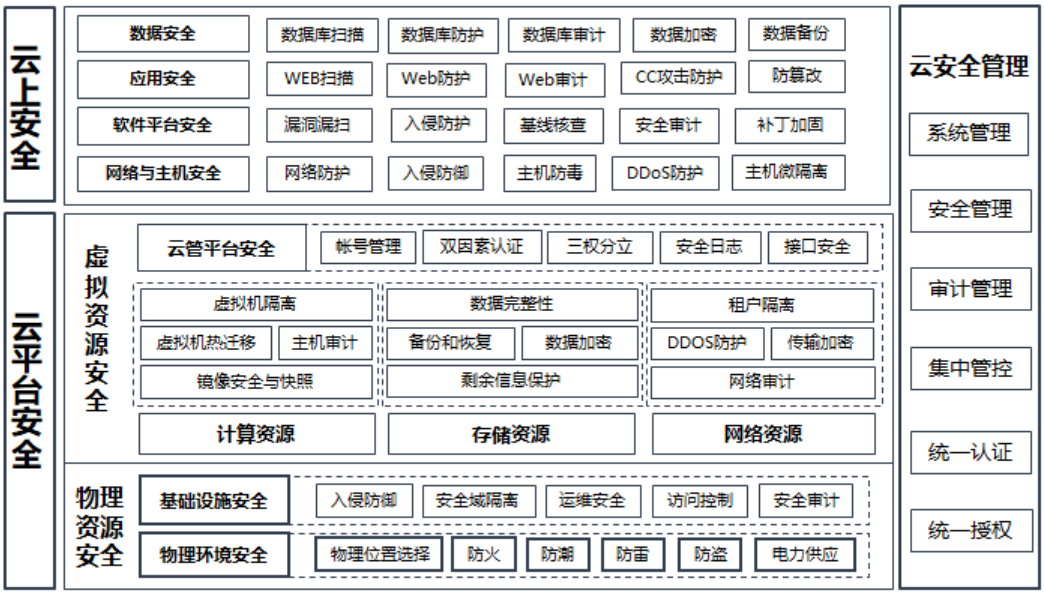

图 26 云安全体系架构

基于这样一个综合的云安全架构，从云平台安全和云上安全两大方面进行说明。云平台安全主要指云平台自身基础设施及软件的相关安全，主要涉及物理资源安全和虚拟资源安全，物理资源安全又包括物理环境完全和基础设施安全等，虚拟资源安全包括计算资源、存储资源及网络资源的安全以及云管平台的安全。而云上安全则是匹配云上业务的最佳安全体系架构。云上安全包括云上网络与主机安全、云上软件平台安全、云上应用安全和云上数据安全。此外，云安全管理部分涵盖了对整个平台体系的集中管控，包括安全管理、系统管理、审计管理、统一认证和统一授权等，是智慧城市的云安全体系架构中必不可少的部分。

1.1 云平台自身安全建设要体系化

云服务商应提供如虚拟机隔离、租户隔离、虚拟机迁移安全、数据完整性保护和备份与恢复等手段措施保证云平台系统自身的安全，在此基础上，还应建立健全云数据中心边界安全防护体系，通过下一代防火墙、访问控制、DDoS 防护及 WEB 应用防火墙等安全能力，对云平台边界的进出总流量进行持续地检测与防护，防止从外部发起的针对云平台环境的恶意攻击，切实提升云平台环境的整体安全性。

1.2 云上业务安全建设要全面

云上安全建设建议：基于云平台之上搭建的业务系统安全，主要由安全厂商来负责。提供诸如云安全资源池这样的云安全产品及整体防护方案，通过云安全资源池中网络安全、主机安全、应用安全及数据安全等安全能力的加持，构建业务安全监测体系、业务安全防御体系与业务审计体系，涵盖云安全能力的事前监测、事中防御和事后审计全生命周期，并互相协同工作，形成一个完整的云内安全事件响应闭环。

1.3 云安全管理建设全局化

为保障云平台信息安全及云上业务安全而采取的一系列管理措施的总和，主要由运营方自行负责。通过建立健全组织机构规范、安全规章制度，对已有的安全能力统一管控

以及通过人员安全管理、安全教育与培训和各项管理制度的有效执行，来落实人员职责，确定行为规范，切实保障云平台基础安全和云上业务系统安全的技术措施真正发挥效用。

2. 企业或个人的安全建设不可少

2.1 云上业务接入访问要可信

云计算模式下，对于企业来说，难免存在员工通过账号登录，获取相应权限，由互联网访问内网业务的过程，员工可能存在使用不安全终端或处于不可信环境下办公的情况，并且远程访问通道的开放，也增加云内核心业务系统遭受恶意攻击的风险。此外，也会存在员工身份鉴别不准确、账号权限控制不足、远程网络链路不安全等问题。在这种情况下，对员工身份的认证管理、账号权限的最小化控制和建立安全的传输通道尤为关键。

建议：通过建立健全零信任安全体系架构，辅以 VPN 和主机安全（EDR）等专有安全措施，对远程接入终端和环境的进行安全检测和评估，对存在安全风险的终端系统进行病毒查杀和加固，不可信的终端（如安全分值低于 80 分值）将不允许远程接入办公系统。从整体上加强对接入访问用户的全生命周期管理和最小化权限控制，动态生成用户的接入访问和行为模式，保证终端的安全可信，保证数据在传输过程中不被第三方窃取。

2.2 未知风险漏洞风险周期变短

互联网存在大量已知漏洞，软硬件也不可避免存在些许Bug，由于黑客技术手段的不断完善，针对新漏洞的探测和利用周期正在逐渐变短。过去针对新漏洞的大规模扫描需要过几天才会出现，而现在往往在新漏洞被发现的第一时间，就会已经爆发安全事故，导致企业的开发和安全运维人员几乎无法在合理的短时间内完成打补丁操作来应对安全威胁。

2.2 云环境及云上业务系统内生安全要可靠

云平台内部的办公业务系统及相应资产数众多，需要满足多种情况下的办公业务需求，可能会导致云内系统由于外部因素出现新的薄弱点，从而被黑客攻击者恶意利用发起攻击，因此，加强云内的整体安全建设势在必行。

建议：通过云防火墙防护引擎、云Web防护引擎、云入侵防御引擎、云漏洞扫描引擎、云主机安全管理引擎等安全措施，对云平台内部与外部的南北向流量和云内东西向流量等进行深度的检测与防护，防止从外部和内部发起的恶意攻击。持续地对云内的重要资产进行安全监测，为资产定期“量体温”，及时发现云内环境及资产的风险并自动进行隔离处置，同时，安全加固云内资产，如主机、操作系统、数据库等。加强对云内核心Web应用系统的保护，全方位从云监测到云防护全面提升云平台环境及云内业务系统的整体安全

性。

2.3 云上业务系统运维与行为审计要细致

公有云服务模式下，对云内系统的远程访问源分布广、变化快，对云内业务系统的操作频繁复杂，常规的操作日志排查很难适应现阶段灵活复杂的操作，远程对云内业务系统及核心资产的重要操作若是不可控制将会大大增加安全风险性，因此，对云内的详细操作安全审计变得尤为敏感和关键。

建议：通过运维审计、日志审计和数据库审计等安全工具措施，针对性审计远程用户访问业务系统的行为操作，对敏感高危操作及时作出告警处置，保证发生数据泄露等事故后可溯源定位分析，全面保障运维安全合规，审计不间断，让接入访问者在云内的一切操作可管、可控、可回溯分析。

2.4 云上安全态势及运营要明晰

随着业务系统上云的进程加快，云安全事件逐渐呈现出黑灰产化，在云平台虚拟环境中，尤其是混合多云的复杂环境中，租户数量多、资产数量多、业务系统繁杂，加之传统安全建设方式无法适用于云计算的复杂环境，IT 安全管理人员常常无法掌控云平台的整体安全情况。因此，能够简单掌控云平台内部的整体安全态势，及时作出安全决策是当下云安全建设的根本。

建议：通过云安全管理平台相关服务或云安全 SaaS 化服务等方式，实时了解和掌控云平台内部环境、业务系统及重要资产的安全态势情况及威胁风险感知情况，对潜在的安全风险及时发现和预警，结合运营分析作出合理化的处置建议，实现云安全问题全方位闭环，真正地让云平台安全无忧。

2.5 建立完善的安全管理体系

按照信息安全等级保护中安全管理部分的要求，参考 ISO 27000 系列标准的控制域和控制项，结合行业最佳实践和监管要求，需要基于自身业务情况和特点建立一套符合其状况的安全管理体系，具体包括以下几个方面:

- 制定安全策略，并根据策略完善相关制度体系
- 建立信息安全管理体系（ISMS），提升总体安全管理水平
- 参照行业监管机构的相关规定和指引，并结合 ISO 27000 体系文件，实现 ISMS 落地实施
- 建立安全运营管理体系
- 结合信息安全建设规划进行实施
- 结合安全域划分进行实施
- 结合等级保护相关内容进行实施

信息安全管理体系的主要任务是了解信息安全现状，确定安全方针和目标，汇总现有制度体系，分析各项差异性，设计适合自身的信息科技风险状况、技术水平以及管理体

系，并辅助实施。