面向云攻击的安全防护技术研究

Research on Security Protection Technology for Cloud Attacks

郑 涛[1],郭新海[2,3],丁 攀[2,3],王 戈[2,3],刘 安[2,3](1. 中国联合网络通信集团有限公司,北京 100033;2. 中国联通研究院,北京 100048;3. 下一代互联网宽带业务应用国家工程研究中心,北京 100048)

Zheng Tao[1], Guo Xinhai[2,3], Ding Pan[2,3], Wang Ge[2,3], Liu An[2,3](1. China United Network Communications Group Co., Ltd., Beijing 100033, China; 2. China Unicom Research Institute, Beijing 100048, China; 3. Next Generation Internet Broadband Service Application National Engineering Research Center, Beijing 100048, China)

摘 要:

随着信息技术、数字技术和智能技术的不断演进与发展,云计算已经成为了企业数字化转型所依赖的重要基础设施,并日益发挥出重要作用。如今,云计算已经经历了虚机时代和原生时代,即将进入智能时代。新的时代背景下,云计算将面临更多样、更复杂、更大量的攻击。分析云攻击的特点,并针对云攻击构建相应的安全防护能力,对云的安全发展至关重要。分析了当前云计算的特点和所面临的主要威胁,结合云上攻击行为,研究了新形势下面向云攻击的安全防护能力。

关键词:

云原生;云攻击;云安全;安全防护

doi:10.12045/j.issn.1007-3043.2023.08.006

文章编号:1007-3043(2023)08-0024-05

中图分类号:TN915.08

文献标识码:A

开放科学(资源服务)标识码(OSID):

Abstract:

With the continuous evolution and development of information technology, digital technology and intelligent technology, cloud computing has become an important infrastructure on which enterprises rely for digital transformation, and plays a more important role. Nowadays, cloud computing has gone through the virtual machine era and the native era, and is about to enter the intelligent era. In the new era, cloud computing will face more diverse, complex, and massive attacks. Analyzing the characteristics of cloud attacks and building corresponding security protection capabilities for cloud attacks is crucial for the security development of the cloud. It analyzes the characteristics of current cloud computing and the main threats it faces, and combined with cloud attack behavior, it studies the security protection capabilities of cloud attacks in the new situation.

Keywords:

Cloud native; Cloud attack; Cloud security; Safety protection

引用格式:郑涛,郭新海,丁攀,等. 面向云攻击的安全防护技术研究[J]. 邮电设计技术,2023(8):24-28.

1 背景

近年来,云计算技术一直处于高速发展和广泛应用的过程中,并且随着公有云和私有云的广泛部署,云计算基础设施已经成为了企业部署新业务的首选。“十四五”时期,中国的信息化进入加快数字发展、建设数字中国的新阶段,云计算作为数字中国建设的新型数字基础设施,在推动人工智能、5G、工业互联网、物联网等技术的发展和应用方面发挥着越来越重要的作用。云计算的普遍应用和相关技术发展,使其经历了云计算1.0虚机时代和云计算2.0原生时代,目前正在朝着云计算3.0智能时代迈进[1]。新技术的发展与应用,必然导致新的安全问题,安全技术作为一种伴生技术,需要能够解决新技术所带来的安全问题。但是,目前云安全的发展相较云资源与云能力产品的发展存在一定的滞后,导致面向云资源发起的攻击越来越多,企业需要面临相较于传统计算环境更多的风险暴露面以及更复杂更频繁的攻击行为。

因此,在当前云计算2.0时代,云原生技术日趋成熟,并因ChatGPT的推动助力朝着云计算3.0智能时代

收稿日期:2023-06-01

迈进，分析云计算所面临的主要威胁和攻击者的主要攻击行为，并研究相关的安全防护能力，能够为企业的云安全防护体系的建立提供帮助，保障企业业务和数据更安全的在云上运转[3]。

2 云计算面临的主要威胁

2023年云安全联盟（CSA）大中华区主席李雨航院士指出，云安全下半场中原生安全是基石、应用安全是核心、数据安全是目标，新时代下云安全的3驾马车即云原生安全、云应用安全和云数据安全。当前，云原生的代表技术容器、容器编排平台、微服务、DevOps、CI/CD和Serverless等在云基础设施和云应用中被大量使用，这些技术的使用为企业的业务应用开发、部署和持续服务带来了极大的便利，但也使企业面临的风险发生了变化，主要表现在以下几个方面。

a）容器技术的使用拓展了企业需要管理的资产。企业在开展网络资产安全管理时不仅要对传统的服务器、网络设备、安全设备、虚拟机和应用程序等资产进行管理，还需要将容器纳入资产的范围。另外，由于容器主要使用镜像构建，而镜像的使用极易导致供应链攻击、恶意镜像传播和敏感信息泄露等风险。

b）容器编排平台作为容器的控制和管理系统，进一步增大了风险攻击面。由于平台不安全的配置，大量攻击通过攻击容器编排平台进一步开展横向渗透。

c）开发运营一体化和持续集成/持续交付为应用业务系统的开发、部署和运营效率提供了保证，但是由于开发人员安全经验的缺乏，也引入了大量系统漏洞。

d）由于微服务和Serverless的使用，业务逻辑缺陷、API滥用、未授权的访问以及敏感数据泄露等也成为了云原生应用所面临的主要风险。

2022年，CSA总结了云计算面临的十一大类主要威胁[2,6]，并给出了云客户和云供应商需要重点关注的主要云安全威胁，如表1所示。

3 面向云计算的攻击分析

在网络安全的攻守博弈过程中，因为攻击方能够随时随地的针对网络的任何薄弱点发起攻击，而防守方需要利用有限的资源构建起全面的安全防御体系，使得防守方一直处于劣势地位。因此，为了解决防守方面临的问题，帮助企业更全面地了解攻击者的攻击特点、攻击战术和攻击技术，需要对攻击者的攻击行为进行分析。

表1　云计算所面临的十一大类主要威胁

类别	详细介绍
不充分的身份、凭据，访问和密钥管理、特权账号管理	由于未进行充分的身份、凭据，访问和密钥管理、特权账号管理造成的漏洞
不安全的接口和API	由于错误的配置、不良的编码习惯、缺乏身份认证和不恰当的授权导致的漏洞
配置不当和变更控制不足	未对系统、应用、容器、平台等进行安全的配置，对云环境中的变更控制不足导致错误配置，并阻碍了纠正错误配置
缺乏云安全架构和战略	由于缺乏云安全架构和战略导致的企业和基础设施安全架构实施被限制
不安全的软件开发	云环境导致的软件开发的复杂性，导致可能出现新的漏洞和错误配置
不安全的第三方资源	来自第三方资源的漏洞，供应链漏洞
系统漏洞	云服务平台中普遍存在的系统漏洞
云计算数据的意外泄露	云错误配置导致的意外数据泄露
无服务器和容器化工作负载的配置不当和利用	应用程序的不合规配置导致的安全缺陷和风险
有组织的犯罪、黑客和APT攻击	高级持续威胁，有组织的犯规和黑客攻击
云存储数据泄露	云中存储的数据可能被组织之外的个人发布、查看、窃取和使用

3.1 云攻防矩阵

为了解决攻守双方实力不对称以及防守方经常处于被动的局面，2013年MITRE公司基于实际发生的安全事件，创建出了ATT&CK（Adversarial Tactics，Techniques，and Common Knowledge）知识库。截至目前，ATT&CK发布的攻防矩阵已经涵盖了企业、移动端、工控系统等方面，其中企业的攻防矩阵包括了PRE、Windows、macOS、Linux、云 、网络和容器。ATT&CK v13版本的云攻防矩阵中涵盖了针对云进行攻击的11项战术和68项技术，分别从初始访问、执行、持久化、特权提升、防御绕过、凭证访问、发现、横向移动、收集、渗透、影响共计11个方面进行了介绍，如图1所示。

3.2 攻击方式分析

通过分析ATT&CK的云攻防矩阵可以看出，云计算所面临的攻击行为多从身份认证、配置缺陷、公网暴露面发起，在取得突破后进入内网进行横向移动和提权，从而获得对内网的控制。云上的攻击方式和传统计算中心的攻击方式发生了很大的变化，传统的数据中心中因为存在大量违规开放的端口、补丁不及时应用、错误配置的中间件、未升级的操作系统以及混乱的网络隔离策略等问题，使得操作系统、中间件、软件应用程序、对外服务端口等都成为了攻击者的攻击入口，但是在云上由于IaaS、PaaS和SaaS等服务模式

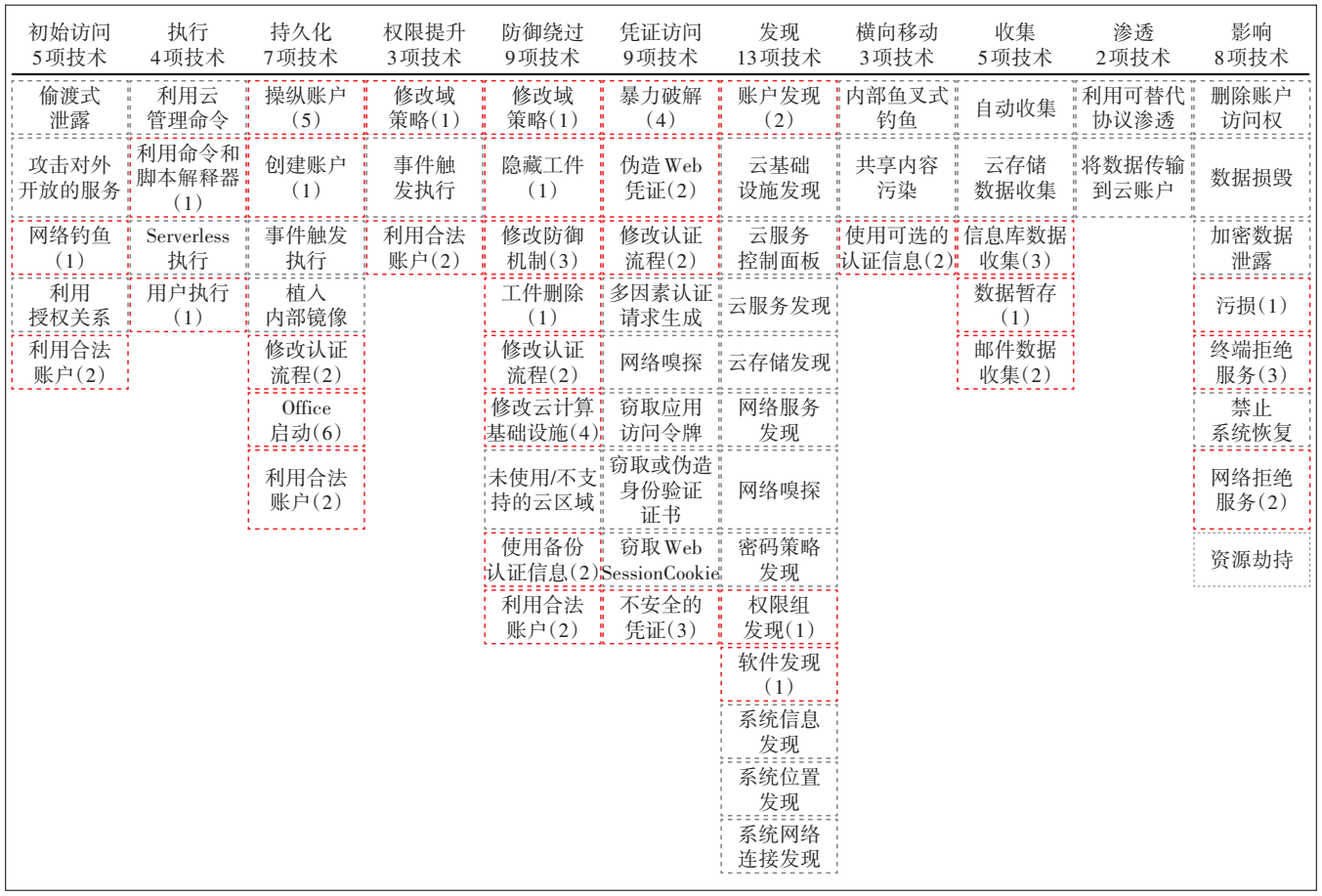

图1 ATT&CK 云攻防矩阵

的不同,产生的安全漏洞和风险暴露面也不同。相对于传统环境来说,云上环境的改变使得攻击者的攻击方式发生了变化。

如图2所示,不同的云服务模式使得攻击者面临的风险暴露面和安全漏洞产生了区别,因此攻击者需要采用针对云环境的攻击方式才能成功渗透到内网,目前云上攻击主要采用纵向突破和横向移动的方式来开展云攻击,常见的云上攻击场景如表2所示。

4 安全防护能力研究

云环境的应用使得企业业务和网络的边界逐渐模糊,安全防护难度加大,风险扩散速度加快,越来越多的攻击者开始利用虚拟机、K8S、容器和云基础架构的配置错误和漏洞进行攻击。因此,为了应对云安全发展进程中存在的困难,需要新的安全防护能力。

4.1 攻击面管理能力

云计算技术的使用重塑了企业的IT架构,使企业的网络资产类型和数量大幅度增加,相应的攻击面也急剧增大。美国NIST给出了攻击面的定义,即未经授权即能访问和利用的企业数字资产的所有潜在入口的综合,并非所有的资产暴露面都可以成为攻击面,但是当暴露面和攻击向量叠加后就会形成攻击面。在传统的数据中心中,攻击面可以很好地被控制,但是如今随着企业的业务上云,云控制平台、身份认证系统、影子资产、SaaS应用以及API接口等,都为企业增加了新的攻击面,导致企业想全面控制自己的攻击面非常困难。因此,开展攻击面管理能够立足于攻击者的视角,结合攻击行为的特点,在攻击发生之前发现和修复攻击面,防止可能发生的攻击行为。

在开展云安全攻击面管理的过程中资产发现是基础,在资产发现的基础上检测资产存在的攻击面,并进一步开展攻击面分析、验证和修复能够实现攻击面的闭环处置,保证攻击面的常态化运营管理,如图3所示。

4.2 原生的安全防护能力

云计算的新时代,云安全不再是单纯的云安全资

图2　云攻击与传统攻击的区别

表2　典型云上攻击场景

攻击方向	攻击场景
利用公有云上租户的不安全的应用与服务配置为突破口	云服务认证Key泄露
	云上租户的云服务不安全配置
	云上的Web应用漏洞
利用公有云本身的服务（IaaS、PaaS、SaaS）问题为突破口	云服务自身功能缺陷导致代码执行
	云服务公开API利用
	云服务第三方软件漏洞利用
	云服务私有或者公开API漏洞挖掘与利用
	容器逃逸
	虚拟机逃逸
	云服务管理面网络入侵

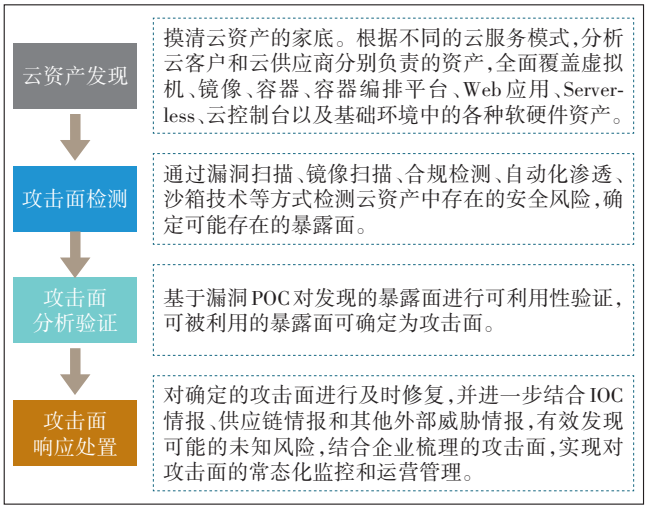

图3　攻击面管理

源池，本质上云安全资源池只是传统安全产品的虚拟化，不能解决当前云计算容器、镜像、容器编排平台等的安全问题。因此，为了能有效应对当前的云攻击行为，需要研究原生的安全防护能力，并以DevSecOps和云原生的安全理念[4]，构建涵盖云业务应用和新型基础设施的全方位安全检测与防护能力，有效保证从底层环境到上层应用的安全[5]。对云应用提供覆盖设计、编码、构建、测试、部署、运营完整生命周期的安全保障能力，对云基础设施提供资产管理、安全配置核查及管理、权限管理和策略管理等方面的能力，安全能力架构如图4所示。

打造云原生安全能力能够有效促进安全左移，提升云应用和基础设施的原生安全水平。同时，能够收敛攻击面，提升对云资产的安全管理能力，在运行阶段为API、容器等资产提供全面的安全检测与防护能力，更加有效地应对攻击者发起的攻击行为。

4.3 智能的安全防护能力

ChatGPT的推出和使用将人工智能推向了新的热潮，2023年中国产业互联网发展联盟和腾讯研究院联合发布的《2023年产业互联网安全十大趋势》，将“云原生安全一体化将大幅提升企业的安全水平”和“ChatGPT大模型AI计算广泛应用安全领域，攻防进入智能化时代”列入在内。如今，网络攻击者已经开始采用人工智能技术发起网络攻击，尤其是利用ChatGPT的代码编写能力，可以大大提升攻击者的进攻效率。另外，由于云上应用生命周期长、资产种类繁多、攻击面大以及云内可观测性不足等问题，又导致了防守者难以高效应对智能化、自动化的攻击行为。因此，在打造云原生安全防护能力的基础上，需要进一步开展人工智能技术研究，利用人工智能技术提升云上网络安全防护能力。

传统的安全检测与防护能力，基本都是利用行为规则库和风险库匹配的方式来确定攻击行为和漏洞，这种方式能在一定程度上发现已知的攻击行为和已知漏洞，但是对于未知攻击的防御以及未知漏洞的检测则显得无能为力。因此，打造智能的安全防护能力

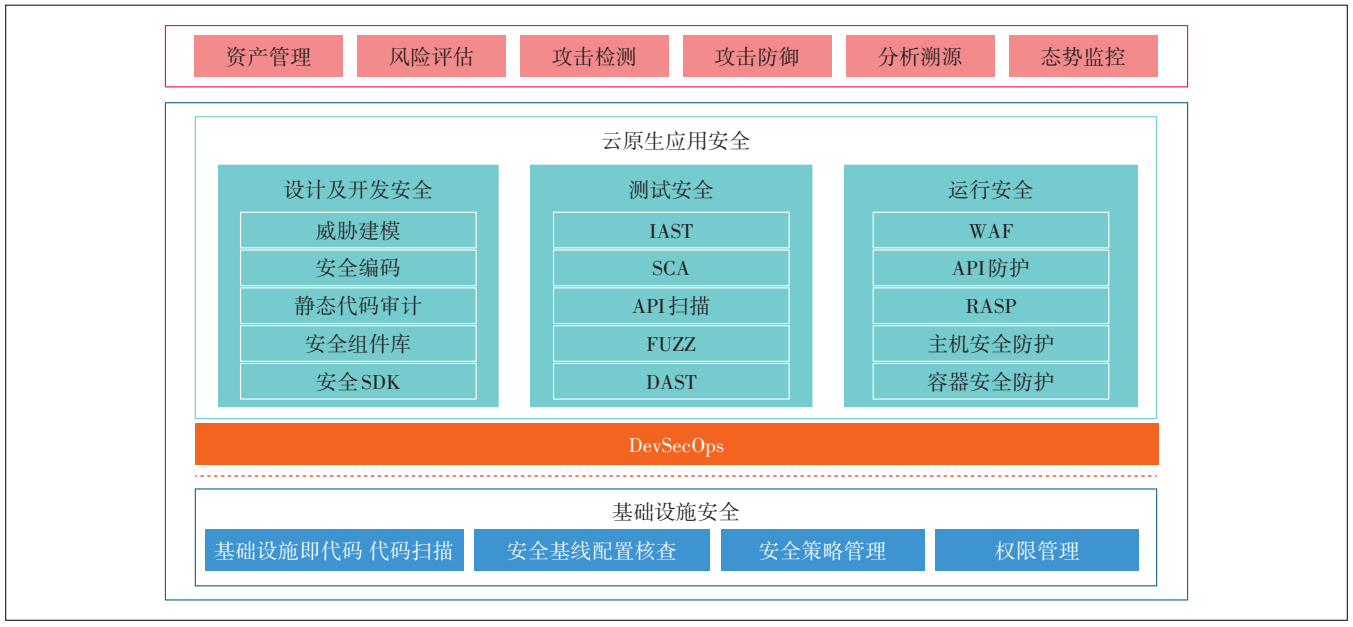

图4　云原生安全能力

可以从如下3个方面着手。

a）高效、自主、精准识别攻击的能力。利用现有网络中广泛收集的行为、漏洞和风险信息，通过人工智能技术对信息进行深度挖掘和关联分析，挖掘正常行为和异常行为，结合态势感知，构建能够开展持续安全监测、安全事件分析、安全威胁预测和安全防御响应的动态、精准、高效主动防御体系。

b）基于人工智能的威胁情报。为进一步完善威胁情报，从而使威胁情报更高效地赋能安全系统，需要基于人工智能技术提升威胁情报的生产和管理效率，并充分利用威胁情报进一步优化安全检测与防御策略，提升安全防护系统的自适应安全能力和主动防御能力。

c）利用人工智能提升安全治理效能。利用人工智能技术结合安全防御体系对攻击行为进行分析，结合网络安全人员的相关经验，提升对攻击事件处理和安全漏洞修复的效率，使网络安全感知与防御体系自动化水平显著提高。

5 总结

网络安全的本质在对抗，对抗的本质在攻防两端的能力较量。如今，云计算已经在各行各业的IT基础设施中广泛应用，成为了国家重要的关键信息基础设施，针对云计算发起的攻击行为也越来越复杂。为了保障云计算的安全，本文结合当前云计算的主要特点，分析了当前云计算中面临的主要威胁，并根据主要威胁分析了攻击者发起攻击行为的主要方式，最终根据攻击行为的特点给出了企业在云安全中需要建设的安全防护能力。通过相应的能力建设能更全面、更有效、更智能地为云计算提供安全防护，助力企业的数字化发展安全推进。

参考文献：

[1] 李雨航，郭鹏程. 云安全的发展与未来趋势[J]. 中国信息安全，2022(5)：39-42.
[2] 郑禄鑫，张健. 云安全面临的威胁和未来发展趋势[J]. 信息网络安全，2021，21(10)：17-24.
[3] 宋胜攀，刘振慧，庄东燃. 云原生应用安全防护技术研究[J]. 保密科学技术，2022(12)：45-51.
[4] 袁曙光. 云安全的未来是云原生安全[J]. 中国信息安全，2022(5)：43-47.
[5] 何宝宏. 云与安全深度融合推动原生云安全发展[J]. 中国信息安全，2022(5)：30-33.
[6] 云安全联盟大中华区. 云计算的11类顶级威胁[R/OL]. [2023-04-15]. https://c-csa.cn/u_file/photo/20230516/7249fd5c67.pdf.

作者简介：
郑涛，工程师，硕士，主要从事网络与信息安全管理工作；郭新海，工程师，硕士，主要从事网络与信息安全研究工作；丁攀，工程师，硕士，主要从事网络与信息安全研究工作；王戈，工程师，硕士，主要从事网络与信息安全研究工作；刘安，工程师，硕士，主要从事网络与信息安全研究工作。