2024年云计算顶级威胁

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《2024 年云计算顶级威胁（Top Threats to Cloud Computing 2024）》由 CSA 云安全联盟顶级威胁研究工作组专家编写，并由 CSA 大中华区组组织专家完成翻译并审校。

翻译组成员：

陆　琪　　刘连杰　　刘　刚　　赵晨曦　　卜宋博　　肖文棣

审校组成员：

郭鹏程　　党超辉　　卜宋博

研究协调员：

闭俊林　　易利杰

贡献单位：

爱立信（广州）有限公司　　天翼安全科技有限公司

天翼云科技有限公司　　中国移动香港有限公司

晨星资讯（深圳）有限公司

（以上排名不分先后）

英文版本编写专家

主要作者：

Jon-Michael Brook Alex Getsin

Vic Hargrave Michael Roza

贡献者：

Jon-Michael Brook Randall Brooks Alex Getsin

Vic Hargrave Laura Kenner

Michael Morgenstern Stephen Pieraldi Michael Roza

审校者：

Vishnu Guttha

Yuvaraj Madheswaran

Nishith Sinha

CSA 全球员工：

Sean Heide

Claire Lehnert

Stephen Lumpe

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予改正！ 联系邮箱 research@c-csa.cn；云安全联盟 CSA 公众号。

序言

随着云计算的快速普及，云安全已成为企业数字化转型过程中不可忽视的核心问题。云环境的开放性、多样性和复杂性，给企业带来了前所未有的安全挑战，而其中的威胁正不断演变。为了帮助企业更好地理解并应对这些威胁，云安全联盟（CSA）大中华区发布了《2024 年云计算顶级威胁》。本报告基于 500 多位全球专家的调研与分析，深入剖析了当今企业面临的云安全风险，并为应对这些挑战提供了切实可行的策略建议。

2024 年，云计算领域的安全威胁格局将发生显著变化。我们看到，传统威胁正在逐渐被边缘化，新的风险，如配置错误、身份与访问管理的薄弱、不安全的 API 接口，以及缺乏系统性的云安全策略，正成为核心安全问题。而随着生成式人工智能（如 ChatGPT）的广泛应用，企业在享受技术创新带来效率提升的同时，也面临着更复杂的安全挑战。AI 技术的双刃剑效应，不仅加速了网络攻击的自动化和复杂化，也为云安全防护带来了前所未有的机遇。如何在这个动态的环境中，平衡 AI 技术的应用并最大化其积极效应，成为企业安全策略中至关重要的一环。

展望未来，全球云安全将继续面临愈发复杂的供应链风险、监管环境的不断演变，以及新型攻击手段的层出不穷。企业需要具备前瞻性思维，采用创新的安全架构和技术，尤其是在零信任模型、自动化安全管理、云原生安全工具等方面加大投入，确保其在日益变化的环境中具备强大的应变能力。同时，安全技能的差距也将继续成为企业面临的长期挑战，推动全员持续教育与技能提升是增强组织整体安全韧性的关键。

李雨航 Yale Li

CSA 大中华区主席兼研究院长

目录

摘要

《顶级威胁》报告旨在提高人们对云计算威胁、漏洞和风险的认识。在本次报告中，我们对 500 多位云计算行业的专家进行了调查，深入探讨了云计算领域的安全问题。受访者识别出今年他们的云环境中存在的 11 个重要安全问题。顶级威胁工作组利用调查结果及其专业知识编制了《2024 年云计算顶级威胁》报告。

最新报告重点介绍了 2024 年的顶级威胁。报告中还显示了 2024 年和 2022 年威胁的排名对比。

观察

调查分析显示，由云服务提供商 (CSP) 负责的传统云安全问题在排名中的持续下降。此前报告中提到的拒绝服务攻击、共享技术的漏洞以及云服务提供商 CSP 数据丢失等问题，如今因评级较低而未被纳入本报告。这些问题的消失显示出对云计算的信任感增加；基础设施即服务 (IaaS) 环境中的老旧云安全问题不再那么令人担忧。此外，我们观察到“数据泄露”问题不再占据云计算顶级威胁的主导地位。

随着云商业模式和安全策略的演变，本报告提高了对以下关键安全问题的关注：

- 配置错误与变更控制不足
- 身份和访问管理 (IAM)
- 不安全的接口和 APIs
- 云安全策略缺失

配置错误与变更控制不足：如今位居 2024 年顶级威胁调查首位，相较于 2022 年报告中的第三位有所上升。多年来，配置管理一直是组织能力成熟度的基石。然而，向云计算的过渡加剧了这一挑战，使团队必须采用更强大的云特定配置。由于云服务的持续网络访问和无限容量特性，配置错误可能对整个组织产生广泛影响。

身份和访问管理 (IAM)：曾位居首位，如今降至第二位。云环境中仍存在重放攻击、伪造身份和过度授权等挑战，这与本地设置类似。然而，使用自签名证书和不当的加密管理显著地增加了其安全风险。零信任架构的实施和软件定义边界（SDP）的应用正成为受访者重点关注的问题，反映了这些问题在云安全中的重要性。

不安全的接口和 APIs：从第二位降至第三位，微服务的采用突显了保护接口和 API 的重要性。尽管它们在云服务（包括 SaaS 和 PaaS 产品）中起着关键作用，但由于开发人员的效率不足与云服务所需要的持续在线的要求，保障安全的接口和 API 仍然面临着巨大挑战。

云安全策略缺失：仍位于第四位，这一领域持续关注的问题是：为什么在规划和构

建安全解决方案时仍存在重大挑战？云计算已经是稳定发展的技术，它需要明确的可执行的架构策略。

目标读者

云计算和安全从业者以及爱好者将从本报告中受益。以获取在云安全方面的威胁和挑战的最新见解，了解这些威胁如何影响行业，以及可以采取哪些措施来减轻其后果。同时，本文基于调查的研究将为合规、风险、技术、信息安全人员和高管管理层提供与当前相关的技术趋势和优先考虑的云安全事项。

调查

在创建《2024 年云计算顶级威胁》调查报告时，CSA 顶级威胁工作组分两个阶段进行了研究。这两个阶段均通过调查收集了网络安全专业人士对云计算中最相关的威胁、漏洞和风险问题的看法与意见，最终目的是确定 2024 年的顶级威胁。

在第一阶段研究中，工作组旨在通过面对面调查工作组成员来创建云安全问题的初步清单。工作组从之前的报告（《云计算的 11 类顶级威胁》）中的 11 个顶级威胁（安全问题）开始，通过讨论又增加了 19 个问题。然后，工作组在一系列会议中审查了这 30 个问题，并要求成员根据其所在组织及他们熟悉的组织，评估每个问题的重要性。这最终形成了调查中的 28 个问题。

在研究的第二阶段，工作组的主要目标是通过对 500 多名安全专业人士的在线调查，根据重要性对这 28 个安全问题进行排名。工作组选择了一个以 10 分为满分的评分系统，以反映每个问题的重要性。调查参与者被要求对每个云安全问题进行 1 到 10 的评分，1 表示“不是很重要”，10 表示“最重要”。每个类别的得分被汇总并取平均值，然后根据平均分对安全问题进行排名。最终，工作组确定了以下 11 个顶级威胁。

排名	平均分	威胁
1	8.282331	配置错误与变更控制不足
2	8.070780	身份与访问管理（IAM）
3	7.987272	不安全的接口与APIs
4	7.620689	云安全策略缺失
5	7.582061	不安全的第三方资源
6	7.545801	不安全的软件开发
7	7.506641	意外的数据泄露
8	7.462794	系统漏洞
9	7.389799	云可见性/可观测性不足
10	7.379310	未验证的资源共享
11	7.364326	高级持续性威胁（APT）

在确定了 11 个顶级威胁后，工作组对每个问题进行了分析。每个分析包括对问题的描述、业务影响、关键措施、案例和实际事例，并引用了 CSA《云计算关键领域安全指南 v5》领域指南中的相关章节，以及 CSA《云控制矩阵》（CCM）和 CAIQ v4 控件中的相关缓解控制措施。最后，整体方法代表了 CSA《云审计知识证书学习指南 v1》中提出的顶级威胁方法论。

威胁1
配置错误与变更控制不足

配置错误是指云计算资产的设置不正确或次优，这可能会使它们容易受到意外损坏或外部/内部恶意活动的攻击。缺乏云系统知识或对云安全设置的理解以及恶意意图可能导致配置错误。一些常见的配置错误 [1]包括：1. 密钥管理不当，2. 监控和日志记录被禁用，3. ICMP（互联网控制消息协议）保持开放，4. 不安全的自动备份，5. 存储访问权限，6. 缺乏验证，7. 对非 HTTPS/HTTP 端口的无限制访问，8. 对虚拟机、容器和主机的过度权限（最小权限原则），9. 启用了过多的云访问权限（最小权限原则），10. 子域名劫持，11. 特定的云提供商（如 AWS S3 存储桶）的配置错误。云资源的配置错误是导致云安全问题的主要原因，可能会导致严重的损害，如下所示的业务影响部分所示。[2]

在云环境中，不充分的变更控制实践可能导致未被检测到的不当配置，构成重大安全风险。云环境与传统 IT 基础设施有显著不同，这使得变更控制更具挑战性。传统的变更流程通常涉及多个角色和审批，通常需要几天或几周才能完成，然后才能进入生产环境。另一方面，云计算方法强调自动化、广泛访问和快速变更，通常将静态基础设施元素抽象成代码。此外，使用多个云提供商会进一步增加复杂性，因为它们具有独特的功能和频繁的更新。这种动态环境要求对变更控制和补救措施采取敏捷和积极的方法，许多组织都在努力实现这一点。

商业影响

配置错误/不充分的变更控制对云系统的影响可能非常严重，这取决于配置错误/不当变更的性质以及检测和缓解的速度。以下是云配置错误和不充分变更控制可能导致的影响：

技术影响：

- 数据泄露：未经授权的云访问敏感数据会破坏机密性。
- 数据丢失：从云系统中永久或临时删除关键数据会影响可用性。
- 数据破坏：对云系统中的数据进行物理或逻辑错误会危及完整性。

运营影响：

- 系统性能：云资源性能下降影响用户体验和生产力。
- 系统中断：云服务的完全或部分关闭会扰乱业务运营。

财务影响：

- 赎金要求：可能需要支付费用以恢复被破坏的云数据或系统访问。
- 不合规和罚款：未能遵守监管要求可能导致罚款和处罚。
- 收入损失：由于云服务中断、客户不满或法律行动，可能会发生财务损失。
- 股价下跌：泄露和公开披露可能会损害市场感知和公司的估值。

声誉影响：

- 公司声誉：泄露和公开披露可能会损害组织的公众形象和品牌价值。

关键措施

1. 云配置监控、审计和评估 - [3]：通过利用机器学习，组织可以自动化定期检测云系统安全配置错误，减少对手动检查/审计/评估的依赖，提高效率。

2. 云系统、变更管理方法 - [4]：持续不断的业务转型和安全挑战的动态性质要求确保使用实时自动化验证正确进行批准的变更。

案例

近期由于配置错误和不充分的变更控制导致的事件包括：

（2023 年 5 月）据报道，丰田汽车公司承认发生了一起重大的车辆数据泄露事件，影响了日本约 215 万用户。受影响的用户几乎包括了所有注册丰田主要云服务平台 T-Connect 的用户，以及雷克萨斯车主使用的类似服务 G-Link 的用户。这些数据从 2013 年 11 月到 2023 年 4 月中旬公开可访问了十年。此次泄露的原因归咎于人为错误。尽管泄露的数据包括车辆位置和识别号码等详细信息，但尚未报告有恶意使用的情况。针对此事件，丰田已采取措施阻止外部访问数据。该公司已启动对丰田连接公司管理的所有云环境的调查。此外，公司承诺实施审计云设置的系统，建立持续监控程序，并为员工提供关于数据处理规则的全面培训。[5]

（2023 年 9 月）据报道，DarkBeam，一家托管云服务提供商和数字风险保护公司，无意中将一个 Elasticsearch 和 Kibana 界面暴露在外，未受保护，导致报告和未报告的数据泄露记录被泄露。泄露（下载）的数据包括用户的电子邮件和密码，总计超过 38 亿条记录。DarkBeam 一直在收集这些信息，以便在客户发生数据泄露时提醒他们。此事件可能不仅影响 DarkBeam 用户。该漏洞于 9 月 18 日被发现，并在报告后立即关闭。数据泄露通常是由于人为错误造成的，例如在维护后忘记给实例设置密码保护。泄露的数据中包括 16 个名为"email 0-9"和"email A-F"的集合，每个集合包含 2 亿 3963 万 5000 条记

录。这种广泛且有组织的数据处理对那些凭据被披露的个人构成了重大威胁。威胁行为者可能会使用他们的个人信息针对受影响用户发起钓鱼活动。用户必须在在线账户中更改密码，使用强大的密码生成器并启用双因素认证来保护他们的账户。[6]

CSA 云计算关键领域安全指南 5.0

领域 2：云治理

领域 3：风险、审计和合规

领域 5：身份与访问管理

领域 7：基础设施与网络

领域 9：数据安全

领域 10：应用安全

领域 11：事件响应与弹性

CSA 云控制矩阵 v4.0

A&A 审计与保障

A&A-02：独立评估
A&A-03：基于分风险规划评估

AIS 应用程序和接口安全

AIS-02：应用程序安全基线需求
AIS-04：应用程序安全设计和开发
AIS-05：自动应用程序安全测试

BCR 业务连续性管理与配置管理

BCR-02：风险评估和影响分析
BCR-08：备份

GRC 变更控制与配置管理

CCC-02：质量测试
CCC-04：未经授权的变更保护
CCC-09：变更恢复

CEK 密码学、加密和密钥管理

CEK-03：数据加密
CEK-05：加密变更管理

DSP 数据安全与隐私生命周期管理

DSP-07：设计和默认数据保护
DSP-08：设计和默认数据隐私
DSP-17：敏感数据保护

GCR 治理、风险管理和合规

GRC-02：风险管理计划
GRC-05：信息安全计划

HRS 人力资源

HRS-09：人员角色和职责
HRS-11：信息安全意识培训

IAM 身份与访问管理

IAM-03：身份清单
IAM-08：用户访问评审

IVS 基础设施与虚拟化安全

IVS-02：容量与资源计划
IVS-03：网络安全
IVS-04：操作系统加固和基线控制

LOG 日志记录与监控

LOG-03：安全监控与警报
LOG-05：审计日志监控与响应
LOG-12：访问控制日志

SEF 安全事件管理、电子发现与云取证

SEF-03：事件响应计划
SEF-04：事件响应测试
SEF-06：事态分类过程

TVM 威胁、脆弱性管理

TVM-07：脆弱性识别
TVM-08：脆弱性优先级
TVM-09：脆弱性汇报管理

参考链接

1. Common Cloud Misconfigurations and How to Avoid Them 常见的云配置错误及如何避免
   https://www.upguard.com/blog/cloud-misconfiguration

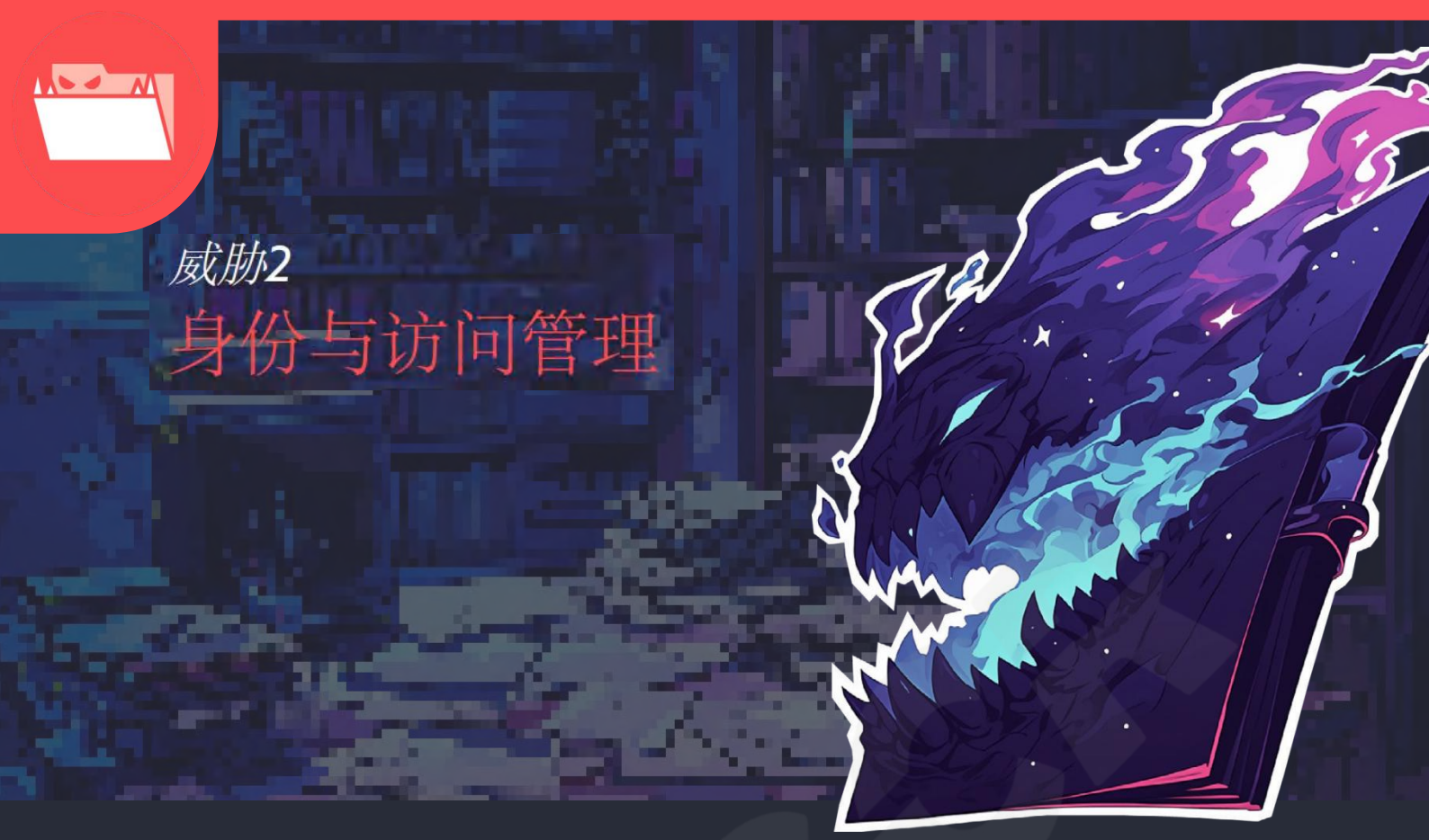
2. 13 Most Common Misconfigurations on the Cloud 云端最常见的13种配置错误
   https://www.clouddefense.ai/common-misconfigurations-on-the-cloud/

3. Safeguarding Against Security Misconfigurations with the Power of Machine Learning 利用机器学习的力量防范安全配置错误
   https://securityboulevard.com/2023/11/safeguarding-against-security-misconfigurations- with-the-power-of-machine-learning/

4. Change execution monitoring 变更执行监控
   https://www.versio.io/solution-change-request-management.html

5. More than 2 million Toyota users face the risk of vehicle data leak in Japan 超过200万丰田用户面临日本车辆数据泄露风险
   https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12/?ref=thestack.technology

6. DarkBeam leaks billions of email and password combinations DarkBeam泄露了数十亿的电子邮件和密码组合
   https://securityaffairs.com/151566/security/darkbeam-data-leak



威胁2

身份与访问管理

身份与访问管理（IAM）确保个体在证明自己的身份后，只能访问他们被授权的资源。这个系统在定义和管理用户角色、访问权限以及分配或撤销这些权限的具体条件下起着关键作用。尽管 IAM 在网络安全中扮演着至关重要的角色，但由于其复杂性以及网络威胁不断演变的特性，IAM 也带来了持续的挑战。用户认证、授权、单点登录（SSO）、多因素认证（MFA）和活动监控等关键组件对 IAM 的有效性至关重要。然而，这些特性的复杂性和动态性可能会引入漏洞，特别是如果没有正确实施、配置、更新和监控的话。随着网络威胁变得更加复杂，保护敏感信息免受未经授权的访问变得越来越困难，这使得强力实施和持续完善 IAM 策略对于加强网络安全防御变得不可或缺。

在云环境中管理身份和访问可能会变得复杂且风险重重。不同的云提供商拥有独特的系统，这可能导致错误和安全漏洞。当用户可以创建和管理自己的账户和资源时，可能会导致过度的权限和配置错误，增加安全风险。每个供应商都结合了不同的 IAM 框架和细致的细粒度权限。如果没有对多个系统的深入理解和管理策略，配置错误和不一致的安全政策的风险就很大。通过集中的 IAM 系统监控，问题响应变得更容易，而不一的政策则进一步复杂化了安全工作。云资源的动态特性，如短期资源和自动扩展，增加了管理的复杂性。将云和本地系统集成可能是一个挑战，尤其是在混合环境中和需要单点登录的情况下。遵守各种法规是另一个障碍。缓解这些风险涉及 1. 采用具有强大认证功能的统一 IAM 解决方案，如单点登录和防钓鱼。2. 实施多因素认证（MFA）。3. 强制执行最小权限原则。4. 自动化配置和去配置流程。5. 开展活动监控。6. 为用户和管理员提供持续的培训和意识提升计划。适当实施和持续完善 IAM 策略可以保护敏感信息并维护网络安全防御的有效性。

商业影响

不充分的 IAM 可能导致未经授权的访问、数据泄露和监管不合规，造成重大的财务和声誉损害。有效的 IAM 策略对于保护敏感信息和维护强大的网络安全防御至关重要。

技术影响：

- 系统访问：弱认证可能导致后端系统中的机密数据被利用。
- 数据披露：由于通信弱点、系统访问或凭证重用，外部各方可能访问业务数据。
- 数据丢失：MOVEit 活动展示了如何通过外泄的数据在谈判赎金时提供筹码。

运营影响：

- 系统中断：云服务的完全或部分中断可能会干扰业务运营。
- 功能延迟：由于需要修复软件漏洞，功能更新可能会延迟。

财务影响：

- 收入损失：由于服务中断、服务恢复、客户不满或法律行动，可能会发生财务损失。
- 不合规：未能充分保护身份和访问控制可能导致不遵守监管要求，如 GDPR、CCPA 和特定行业法规如 PCI DSS。监管违规可能导致重大罚款和法律行动。

声誉影响：

- 公司声誉：损害云服务组织的公众形象、业务和品牌价值。
- 客户声誉：依赖安全性较弱的 API 云服务的客户可能会经历数据泄露和服务中断，对他们的声誉产生负面影响。

关键措施

1. 统一 IAM 解决方案：使用提供强大认证、集中管理和跨多个云提供商的可见性的 IAM 解决方案。

2. 遵循最小权限原则：确保用户只拥有执行其任务所需的访问权限。控制影响范围有助于减轻潜在的违规行为。

3. 自动化配置和去配置：实施自动化工具来管理账户和权限的生命周期，确保及时更新和删除不必要的访问权限。

4. 访问评估和监控：实施自动化工具来管理账户和权限的生命周期。

5. 部署工具以检测、警报并防止未经授权的访问尝试，通过持续的安全监控确保及时更新和删除不必要的访问权限。

案例

（2023 年 5 月）MOVEit 活动：一系列与 MOVEit 文件传输工具相关的安全漏洞影响了包括政府机构和医疗保健提供商在内的多个组织。例如，俄勒冈州交通部遭受了一次泄露，影响了大约 350 万人，攻击者由于账户权限过高和职责分离不当而获得了敏感个人信息的访问权限。需要强有力的日志记录、审计和基于流量的异常检测来捕捉账户被入侵后产生的流量。这些事件突显了数据勒索攻击的新兴趋势，网络犯罪分子迫使受害者支付赎金以防止被盗数据的公开，而不是解密数据。[1]

（2023 年 6 月）JumpCloud 数据泄露：JumpCloud 是一家身份和访问公司，由于一个复杂的国家级行为者遭受了一次数据泄露。这次攻击通过向 JumpCloud 的命令框架注入数据，针对特定客户账户。这次泄露最初被追溯到一个钓鱼邮件活动和未失效的凭证，强调了复杂网络攻击带来的风险以及包括凭证强度审查、强制定时重置和日志审查在内的强大安全措施的重要性。

[2]

（2023 年 10 月）Okta 数据泄露：Okta，一家提供身份服务和认证管理的供应商，经历了一次数据泄露，其中一名未经授权的行为者使用被盗的凭证访问了其支持案例管理系统。此事件泄露了客户支持案例信息，突显了在可访问系统中存储服务账户和敏感信息的风险。持续监控和系统性审查流程至关重要。[3]

CSA 云计算关键领域安全指南 5.0

领域 2：云治理

领域 3：风险、审计和合规

领域 5：身份与访问管理

领域 6：安全监控

领域 9：数据安全

领域 10：应用安全

领域 12：相关技术和策略

CSA 云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01: 应用和接口安全策略和规程
AIS-02: 应用程序安全基线需求
AIS-03: 应用程序安全指标

CCC 变更控制和配置管理

CCC-07: 基线偏离检测
CCC-08: 例外管理

DSP 数据安全与隐私生命周期管理

DSP-03: 数据清单
DSP-04: 数据分级分类
DSP-07: 设计和默认数据保护
DSP-17: 敏感数据保护
DSP-19: 数据位置

GRC 治理、风险管理和合规

GRC-02: 风险管理计划
GRC-05: 信息安全计划
GRC-06: 治理责任模型

IAM 身份和访问管理

IAM-01: 身份与访问控制的政策与规程
IAM-03: 身份清单
IAM-05: 最小权限
IAM-08: 用户访问评审

LOG 日志记录和监控

LOG-10: 加密监控与报告

IVS 基础设施与虚拟化安全

IVS-03: 网络安全
IVS-06: 分区与隔离

TVM 威胁和漏洞管理

TVM-08: 脆弱性优先级

参考链接

1. MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023 MOVEit网络攻击：追踪2023年最大的数据盗窃事件 https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government- business

2. JumpCloud: June 20 Incident Details and Remediation JumpCloud：6月20日事件详情及补救措施 https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation

3. Okta hit by third-party data breach exposing employee information Okta遭遇第三方数据泄露，导致员工信息曝光 https://www.bleepingcomputer.com/news/security/okta-hit-by-third-party-data-breach- exposing-employee-information/

4. The 10 Biggest Data Breaches of 2023 (so far) 2023年十大数据泄露事件（截至目前）
https://www.crn.com/news/security/the-10-biggest-data-breaches-of-2023-so-far

5. DOJ-Collected Information Exposed in Data Breach Affecting 340,000 司法部收集的信息在数据泄露事件中曝光，影响34万人
https://www.securityweek.com/doj-collected-information-exposed-in-data-breach- affecting-340000/

威胁3
不安全的接口与APIs

云服务提供商(CSP)、企业供应商和内部开发人员提供机器对机器的应用程序编程接口（API）或完整的人机界面（UI）套件，通常用于系统控制。然而，初始的设计需求往往与长期使用不一致。领导层的变动、企业战略方向的调整或第三方合作伙伴的访问需求，会暴露出潜在风险，并带来快速部署的时间压力。此前的决策、未记录的假设、遗留支持需求、不良的架构设计或本地部署/IaaS/SaaS产品一致性期望，都可能影响企业向云端过渡的进程。

API和UI因多种原因变得容易受到攻击，包括：1. 不充分的认证机制，2. 缺乏加密，3. 不当的会话管理，4. 输入验证不足，5. 糟糕的日志记录和监控，6. 过时或未打补丁的软件，7. 在上云期间假定的保护平等性，8. 过于宽松的访问控制，9. 缺乏速率限制。Akamai 2024年的报告记录了，“在2023年1月至12月的12个月期间，29%的网络攻击针对API，表明API是网络犯罪分子关注的领域。”[1] 人为的门户认证方法增加了风险，例如弱密码或重复使用的密码，这些密码很容易被破坏。攻击者可以利用这些漏洞，造成的影响范围从未经授权的访问、敏感数据盗窃或服务中断。在2023年，OWASP强调了保护接口的重要性，通过新的API安全Top 10增强了他们流行的网络列表。[2]

商业影响

不安全的接口对云系统的影响可能很严重，这取决于系统的性质以及存在的其他安全措施或缓解措施。不安全接口或 API 的风险因 API 的使用情况、与 API 相关联的数据以及漏洞被检测和缓解的速度而异。最常见的商业影响是 API 未安全保护而导致敏感或私密数据的意外暴露。在考虑不安全接口可能造成的影响时，请考虑以下几点:

技术影响：

- 系统访问：认证不充分可能导致后端系统的被利用。
- 数据泄露：由于通信弱点、系统访问或凭证重用，外部方可能访问到业务数据。

运营影响：

- 系统中断：云服务的完全或部分关闭可能会干扰业务运营。
- 功能延迟：由于需要修复软件漏洞，功能更新可能会延迟。

财务影响：

- 收入损失：由于服务中断、服务恢复、客户不满或法律行动，可能会发生财务损失。
- 不合规和罚款：未能遵守漏洞管理的监管要求可能导致受到处罚

声誉影响：

- 公司声誉：云服务组织的公众形象和品牌价值可能受到损害。
- 客户声誉：依赖于安全措施不足的 API 云服务的客户可能会遭遇数据泄露和服务中断，对他们的声誉产生负面影响。

关键措施

1. 应按照最佳实践监控和保护 API 提供的攻击面。

2. 应实施速率限制和节流，以防止拒绝服务（DoS）攻击和凭证填充。
3. 必须更新传统的安全控制方法和变更管理政策，以跟上基于云的 API 增长和变化。检查具有自动基于时间轮换的短时效凭证，而不是持有者令牌或用户名/密码。具有多因素认证（MFA）因素的人类可访问用户界面将提高安全性。所有与认证事件相关的令牌应遵循标准，并能够检查它们发行的时间。
4. 在迁移功能时，确认产品和服务的一致性。供应商本地部署方案的 API 接口与 SaaS 应用之间调用存在较大延时，在不同的超大规模云服务提供商之间迁移时，可能会有很大的不同。
5. 调查凭证生命周期自动化和技术，这些技术不断监控异常 API 流量。整合情报源以增强检测。这些工具可以在接近实时的情况下纠正性地解决问题。

案例

与不安全接口和 APIs 相关的近期问题实例包括：

（2024 年 1 月）安全研究员 Troy Hunt 发现了一个 Twitter 替代品 Spoutible 的 API 漏洞。该漏洞允许通过使用带有 Spoutible 用户名的 API URL 访问用户账户信息，包括电子邮件地址和 bcrypt 哈希密码。这次违规暴露了 207,000 条记录的数据。[3]

（2024 年 1 月）由于一个公开的 API 与现有的电子邮件数据库匹配，导致超过 1500 万个 Trello 账户泄露。此事件凸显了 API 安全不足，并导致用户数据的暴露，这些数据后来在暗网上出售。[4]

（2024 年 1 月）2024 年，梅赛德斯-奔驰的重大 API 泄露让黑客访问了公司的 GitHub 企业版，暴露了源代码、云密钥和内部文件。这次违规被追溯到一名员工的 GitHub 令牌没有时间戳，在一年前被发现在公共仓库中。[5]

（2024 年 2 月）澳大利亚 ISP Tangerine 被入侵，暴露了超过 200,000 条记录。这次违规被追溯到一名承包商的登录凭证。被盗数据包括个人信息，如姓名、出生日期、电话号码和电子邮件地址。[6]

CSA 云计算关键领域安全指南 5.0

领域 3：风险、审计与合规领域

领域 4：组织管理领域

领域 5：身份与访问管理领域

领域 6：安全监控领域

领域 7：基础设施与网络领域

领域 8：云工作负载安全领域

领域 9：数据安全领域

领域 10：应用安全领域

领域 11：事件响应与恢复力领域

CSA 云控制矩阵 v4.0

AIS 应用与接口安全

AIS-01：应用和接口安全策略和规程
AIS-04：应用程序安全设计和开发
AIS-06：自动应程序安全测试

IAM 数据安全与隐私生命周期管理

DSP-01：安全、隐私策略和程序
DSP-03：数据清单
DSP-04：数据分级
DSP-05：数据流文档

CEK 密码学、加密和密钥管理

CEK-03：数据加密
CEK-04：加密算法

IVS 基础设施与虚拟化安全

IVS-03：网络安全
IVS-04：操作系统加固与基线控制
IVS-09：网络防御

CCC 变更控制与配置管理

CCC-01：变更管理策略和规程
CCC-02：质量测试
CCC-05：变更协议

参考链接

1. 2024 State of the Internet Report on API Security: Shining a Light on API Threats 2024年互联网报告API安全：揭示API威胁
https://www.akamai.com/lp/soti/lurking-in-the-shadows

2. OWASP API Security Project OWASP API安全项
https://owasp.org/www-project-api-security/

3. Twitter rival Spoutible alleges smear campaign amid security breach controversy Twitter竞争对手Spoutible在安全漏洞争议中指控抹黑活动
https://techcrunch.com/2024/02/12/twitter-alternative-spoutible-clashes-with-critics-over- security-breach/

4. Massive Trello User Data Leak: Hacker Lists 15 Million Records on a Dark Web Hacking Forum Trello 用户数据大规模泄露：黑客在暗网黑客论坛上列出1500万条记录
https://www.cpomagazine.com/cyber-security/massive-trello-user-data-leak-hacker-lists-15- million-records-on-a-dark-web-hacking-forum/

5. Mercedes Source Code Exposed by Leaked GitHub Token GitHub令牌泄露导致梅赛德斯源代码暴露
https://www.securityweek.com/leaked-github-token-exposed-mercedes-source-code/

6. 230k Individuals Impacted by Data Breach at Australian Telco Tangerine 澳大利亚电信公司Tangerine的数据泄露影响23万人
https://www.securityweek.com/230k-individuals-impacted-by-da

ta-breach-at-australian- telco-tangerine/

威胁4

云安全策略缺失

云安全策略包括考虑外部因素、现有实施情况以及云技术的选择、优先级和趋势，以创建一个高层次的计划或方法。这些见解帮助组织实现云安全目标并支持业务目标。策略可以包括云架构和云部署模型的设计、云服务模型、云服务提供商（CSPs）、服务区域可用区、特定云服务以及一般原则，例如基于影响（国家和环境或社会）对 CSPs 的偏好，或者对按需服务消费和计费模型的容忍或避免。云安全策略制定可能会考虑现有的供应商锁定、业务意图在需要本地数据居住的特定地区扩展，以及全公司对某个 CSP 或模型的偏好。此外，策略可能会影响或决定跨不同云账户、供应商、服务和环境的 IAM、网络和安全控制的前瞻性设计。

策略应当先于设计并指导设计，但常见的情况是云技术要求对规划、战略制定和改进采取渐进和敏捷的方法。健全的云安全策略能够确保云账户、网络和服务中的工作负载安全运行和生产力。此外，这将通过克服（或避免）安全挑战和风险、支持决策制定，并在业务、技术和风险不确定性的情况下获得有意义的利益，为组织服务。

商业影响

缺乏云安全策略和架构会阻碍有效和高效的基础设施安全工作和设计的实施。反复出现的安全失败可以归因于策略和设计的不足，并可能导致各种影响。

技术影响：

- 数据泄露：未能设计或实施健全的云安全策略可能导致反复的安全事件和违规行为，结果出现重大的保密问题。

运营影响：

- 部署：对云安全策略采取不充分的战略方法可能导致工作分配不当、部署和工程的阻碍、重复工作或授权解决方案、范围蔓延以及无效的补丁和修复措施，在这些情况下，设计层面的措施会更有效。

财务影响：

- 财务成本：由于未能设计或实施健全的云安全策略而反复出现安全事件和违规行为可能导致重大的遏制费用。
- 不合规和罚款：由于云安全策略设计和实施不当导致的监管不合规可能导致罚款。

声誉影响：

- 公司声誉：负面媒体报道和口碑是云安全失败的常见结果，即使没有涉及违规或恶意意图。这些将对客户获取、合作和股票估值产生负面影响，特别是在短期内。安全和云供应商特别依赖他们的品牌信任，容易受到安全失败的影响。

关键措施

1. 制定云安全策略或关键指导原则，并定义目标或目的。
2. 在设计和实施云服务和安全措施时，考虑业务目标、风险、效率、安全威胁和法律合规性。
3. 考虑可能的人为错误、持续对抗你的云弹性的威胁行为者，以及在云策略和安全中未能激活核心保护或基线控制（例如，纵深防御、优先考虑配置简洁的云部署模型）。
4. 设计适当的云网络、账户、数据、身份管理和边界保护的最佳实践，专注于策略的落地与执行。

案例

与缺乏云安全架构和策略相关的问题近期实例包括：

（2023 年 6 月）JumpCloud，一家基于云的身份和访问管理（IAM）服务，整合了数万家企业客户的资产和身份系统，经历了一次安全漏洞，涉及通过针对一名工程师的鱼叉式网络钓鱼进行未授权访问。这场高级且持续的攻击以及随后的调查、遏制和违规教训涵盖了 API 密钥、用户意识、源代码管理和集成、服务部署模型和控制、端点和身份安全措施、基础设施和容器技术设计、客户和当局的参与以及沟通。在复杂的基于云的和对安全敏感的技术服务中构建有效的弹性以挫败高级攻击需要能力和毅力。然而，它也需要对安全及相关领域进行前瞻性和深刻的规划和交付考虑。[2]

（2022 年和 2023 年）2022 年 1 月，LAPSUS$黑客组织通过破坏一名第三方客户支持工程师的账户，访问了 Okta 的内部管理系统。攻击者能够浏览 Okta 的系统、客户管理、数据门户和一些机密信息。2023 年，Okta 被几个知名客户，包括 BeyondTrust 和 1Password，告知发生了另一次违规。这第二次违规显示了这家基于云的身份公司的 IAM、检测和整体弹性方面持续存在的差距。[3]

CSA 云计算关键领域安全指南 5.0

领域 1：云计算概念与架构

领域 2：云治理

领域 3：风险、审计与合规

领域 12：相关技术与策略

CSA 云控制矩阵 v4.0

A&A 审计与保障

A&A-03：基于风险的规划评估
A&A-04：符合性需求

BCR 业务连续性管理与运营弹性

BCR-03：业务连续性策略
BCR-04：业务连续性计划

DCS 数据中心安全

DCS-06：资产分类与跟踪

DSP 数据安全与隐私生命周期管理

DSP-01：安全、隐私政策和程序
DSP-03：数据清单
DSP-07：设计和默认数据保护

GRC 治理、风险管理和合规

GRC-02：风险管理计划
GRC-06：治理责任模式
GRC-08：特殊利益团体

HRS 人力资源

HRS-02：可接受使用的技术策略与规程

IAM 身份与访问控制

IAM-01：身份与访问控制的策略与规程
IAM-04：职责分离
IAM-09：特权访问角色的隔离

IPY 互操作性与可移植性

IPY-01：互操作性与可移植性策略与规程

IVS 基础设施与虚拟化安全

IVS-06：分割与隔离
IVS-07：迁移到云环境
IVS-08：网络架构文档

STA 供应链管理、透明度与可核查性

STA-04：共享安全责任模式控制所有权
STA-08：供应链风险管理

TVM 威胁和漏洞管理

TVM-08：漏洞优先级

参考链接

1. IBM Security. (2023). IBM X-Force Cloud Threat Landscape 2023 Report - Section 3, Recommendations and best practices. IBM 安全。（2023年）。IBM X-Force云威胁态势2023报告 - 第三部分，建议和最佳实践。
https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/09/13/x- force-cloud-threat-landscape-2023

2. [Security Update] June 20 Incident Details and Remediation [安全更新] 6月20日事件详情及补救措施
https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation

3. Okta, with a bruised reputation, rethinks security from the Okta 在声誉受损后，从上到下重新审视安全策略top down
https://www.cybersecuritydive.com/news/okta-security-revival/708636/

威胁 5

不安全的第三方资源

云计算的使用正在快速增长，第三方资源可能包括从开源库中提取的外部代码，SaaS 产品，或者像在“威胁 3-不安全接口和 APIs”中所述的那样。来自第三方资源的风险被视为供应链漏洞，因为它们是将你的云服务或应用/业务系统交付给客户的一环。这也称作网络安全供应链风险管理（C-CSRM），主要关注对个人云服务或应用程序带来的供应链网络安全风险。另外，根据科罗拉多州立大学研究显示，三分之二违规行为由于供应商或第三方漏洞引发。[1]

产品或服务是所有其他使用产品或服务的总和，因此任何集成在应用程序内的组件（如一行代码）都可能成为漏洞的起点。对黑客来说，他们只需找到最脆弱的环节作为攻击切入点即可实现目标，而这个最脆弱的环节往往就是大企业中的小型供应商。

商业影响

因使用不安全的第三方资源引发的问题，将对技术、运营、财务和信誉带来商业冲击。以下是思考这些如何影响组织的初始步骤：

技术影响：

- 数据泄露：第三方访问权限被侵犯可能导致敏感数据在云端遭到未授权访问，威胁机密性。
- 数据销毁：错误的代码重构可能导致未经授权访问，危及数据安全。

运营影响：

- 生产系统中断：第三方资源中存在的延迟或漏洞可能对生产系统造成损害。

财务影响：

- 不合规和罚款：若第三方不遵守规定，公司可能需要承担损失、处罚和罚款。

声誉影响：

- 公司信誉：由于不安全的第三方资源导致公开披露的违规行为，客户可能会对公司保护敏感信息能力产生怀疑。

关键措施

1. 软件无法百分之百保证安全，特别是对于您未参与创建的代码或产品。但组织仍可做出明智选择，决定使用哪些产品，并利用官方支持的第三方资源。同时要检查是否有合规认证/资质，评估其在安全工作上的透明度、漏洞奖励计划以及解决安全问题和提供修复措施的责任心。

2. 利用软件成分分析（SCA）工具识别第三方资源，并制定软件物料清单（SBOM）

或SaaS物料清单（SaaSBOM）。

3. 跟踪记录组织正在使用的SBOM、SaaSBOM以及其他第三方资源。组织应避免只有在受害者名单公布后才发现自己一直在使用易被攻击的产品。这包括开源、SaaS产品、云服务提供商和托管服务，以及可能已集成到应用程序中的其他部分。

4. 定期自动化和手动审查第三方资源。如果流程中检测到不需要或存在安全问题且版本过旧的产品，则需通过适当方式进行补救。这包括审查赋予代码库、基础设施或高影响力个人等关键部门访问权限。

5. 与供应商合作，确保他们接受过自动化应用程序安全测试的培训并具备相关工具。

案例

近期与第三方相关的问题包括：

（2024 年 2 月）据 IBM 称，2023 年全球数据泄露的平均成本约为 445 万美元。此外，2023 年 4 月，网络电话公司 3CX 报告了一次针对供应链的攻击事件。网络罪犯目标是一个或多个 3CX 源代码库，并在该公司桌面应用程序中植入恶意软件。[2]

（2024 年 3 月）被标记为 CVE-2024-3094 号的恶意后门在 xz Utils 中被发现，这是一款广泛应用的数据压缩工具。几乎所有 Linux 和 Unix 操作系统都装有此工具。xz Utils 能提供无损压缩功能。其中一位主要开发者（已经为该项目贡献了多年时间。）故意在 5.6.0 和 5.6.1 版本中植入了后门。[3]

（2024 年 4 月）根据 Cyberint 的 2024 最新报告，供应链攻击有多种手法，如盗取证书、篡改软件或固件、窃取数据和发起拒绝服务攻击等。他们注意到近期供应商遭受的侵害事件有所上升。此外，还存在试图通过篡改供应商产品或服务来影响其他组织的情况。[4]

CSA 云计算关键领域安全指南 5.0

领域 1：云计算概念和架构

领域 2：云治理

领域 5：身份与访问管理

领域 7：基础设施与网络

领域 10：应用程序安全

CSA 云控制矩阵 v4.0

BCR 业务连续性管理与运营韧性

BCR-01：业务连续性管理策略和规程
BCR-02：风险评估和影响分析
BCR-03：业务连续性策略

CCC 变更控制和配置管理

CCC-04：非经授权的变更保护
CCC-05：变更协议

DCS 数据中心安全

DCS-05：资产分级
DCS-06：资产分类与跟踪
DCS-07：受控接入点

DSP 数据安全及隐私生命周期管理

DSP-03：数据清单

DSP-05：数据流文档化

DSP-06：数据所有权和管理权

DSP-08：设计和默认数据隐私

DSP-10：敏感数据传输

DSP-16：数据保留和删除

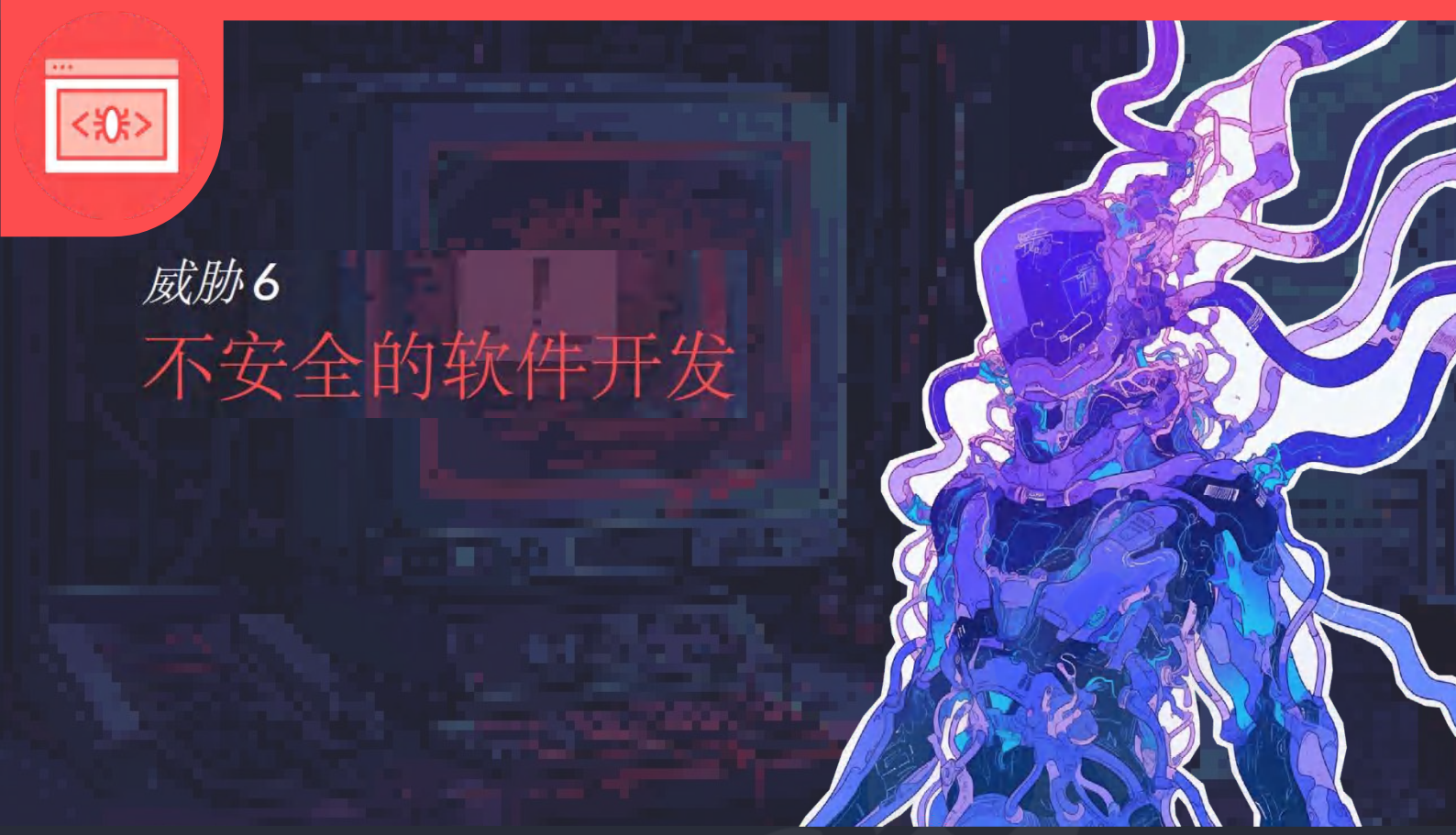
参考链接

1. Hackers Putting Global Supply Chain at Risk 黑客将全球供应链置于风险之中
https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply- chain-at-risk

2. Rising Threat: Understanding Software Supply Chain Cyberattacks And Protecting Against Them 威胁上升：了解软件供应链网络攻击及其防护措施
2.https://www.forbes.com/sites/forbestechcouncil/2024/02/06/rising-threat-understanding-software-supply-chain-cyberattacks-and-protecting-against-them/?sh=4e0f3fd16907

3. Backdoor found in widely used Linux utility targets encrypted SSH connections 在广泛使用的Linux工具中发现后门，针对加密的SSH连接
https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility- breaks-encrypted-ssh-connections/

4. The Weak Link: Recent Supply Chain Attacks Examined 薄弱环节：近期供应链攻击分析
https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/



威胁 6
不安全的软件开发

虽然开发者并未有意制造不安全的软件，但由于软件和云技术的复杂性，可能会无意中产生漏洞。当这类不安全的软件被部署时，威胁行为者可以利用这些弱点破坏云应用程序。通过采取以云为导向的策略，组织能推动 DevOps 流水线的建立，并实现持续集成/持续部署（CI / CD）流程。云服务提供商（CSPs）也可提供如防护或自动化应用程序安全测试等安全开发功能。此外，CSPs 提供 IAM 功能，可在开发环境中执行最小权限原则，并支持拒绝访问。

需要进行持续教育以确保每个开发人员理解公司与 CSP 的共享责任模式。例如，如果某位开发人员的软件出现了零日攻击漏洞，则该开发人员需负责修复问题；反之，如果是 CSP 提供了软件开发或运营环境，则由 CSP 负责实施补丁来修复问题。

拥抱云技术使得公司能专注于其业务特色，并将所有可能商品化的事物交给 CSP 管理和拥有。正如 Cloud Controls Matrix 4.0 所述，组织应："根据自身的安全需求，为应用程序设计、开发、部署和运营定义并实施（安全开发生命周期）SDLC 流程。"通过执行 SDLC，将更加关注于交付更安全的云应用程序。

商业影响

不安全的软件开发会对技术、运营、财务和信誉等产生商业影响。以下是思考这些影响如何作用于组织的初始点:

技术影响：

- 数据泄露：不安全的软件可能会导致敏感数据在云端被未授权访问，从而威胁到信息机密性。
- 数据破坏：由于软件开发的安全问题，可能会引起未经授权的数据访问和损害。

运营影响：

- 功能延迟：不安全的软件开发可能导致功能更新推迟。
- 系统停机：不安全的软件有可能导致云服务部分或全部关闭。

财务影响：

- 不合规和罚款：未遵守监管要求的公司可能需要承担赔偿、处罚和罚款责任。

声誉影响：

- 客户信赖：由于公众对不安全软件开发所暴露出来的漏洞知晓，消费者对公司保护敏感信息能力产生怀疑。

关键措施

1. 制定并执行一个安全开发生命周期（SDLC）流程，包括在设计、开发和运营阶段进行弱点和漏洞扫描。

2. 不存在绝对安全的软件应用程序。组织的开发团队可以利用云技术来打造更为安全的云应用，并采取措施以增强其韧性。

3. 利用云技术能避免重复创造已有解决方案。开发者可通过使用防护栏和其他API专注于处理业务特有问题。

4. 理解共享责任模型，如修补CSP服务或开发者应用中的漏洞等事宜，确保及时进行补救。

5. CSPs高度重视安全，并会提供如“精心构建框架”或安全设计模式等指导，帮助用户安全地实施服务。

案例

近期与账户劫持相关的问题包括：

(2024 年 4 月) WordPress 插件遭受一次漏洞攻击，该漏洞编号为 CVE-2024-27956，CVSS 评分高达 9.9/10（严重级别）。此漏洞使得攻击者能创建具有管理权限的用户账户并植入后门以实现长期访问。其根源在于影响 SQL 的常见弱点，这是一个 SQL 注入问题，对 WP Automatic 3.9.2.0 及之前版本产生影响，并已波及 30,000 个网站。[2]

(2024 年 4 月) 黑客组织 Fancy Bear（也称 APT28）利用 Windows 打印服务程序中的一个漏洞提升权限、获取凭证和窃取数据。他们使用了一个名为 GooseEgg 的未曾公开过的黑客工具，自 2020 年 6 月起至少已经确认 APT28 开始使用 GooseEgg 工具。[3]

(2024 年 4 月) 网络安全研究人员发现 Apache 项目 Cordova App Harness 存在依赖混淆漏洞。此次攻击针对包管理器先检查公共仓库再检查私有注册表的习惯性行为。威胁行动者可以将同名恶意包发布到公共包仓库中去。值得注意的是，依赖性可能成为软件开发工厂的潜在弱点。[4]

CSA 云计算关键领域安全指南 5.0

领域 1：云计算概念与架构

领域 5：身份与访问管理

领域 10：应用程序安全性

领域 11：事件响应与恢复能力

CSA 云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01：应用和接口安全策略和规程
AIS-02：应用程序安全基线需求
AIS-03：应用程序安全标准
AIS-04：应用程序安全设计和开发
AIS-05：自动应用程序安全测试
AIS-06：自动应用程序安全部署
AIS-07： 应用漏洞修复

IAM 身份和访问控制

IAM-01：身份与访问控制的策略与规程
IAM-04：职责分离
IAM-05：最小权限
IAM-14 ： 强鉴别
IAM-16 ： 认证机制

CCC 变更控制和配置管理

CCC-02： 质量测试

TVM 威胁、脆弱性管理

TVM-03 ： 脆弱性补救程序

参考链接

1. AWS Well-Architected Framework AWS良好架构框架
   https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html

2. WP Automatic WordPress plugin hit by millions of SQL injection attacks WP Automatic WordPress插件遭遇数百万次SQL注入攻击
   https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by- millions-of-sql-injection-attacks/

3. Microsoft: APT28 hackers exploit Windows flaw reported by NSA 微软：APT28黑客利用NSA报告的Windows漏洞 https://www.bleepingcomputer.com/news/security/microsoft-russian-apt28-hackers-exploit-windows-flaw-reported-by-nsa-using-gooseegg-tool/exploit-windows-flaw-reported-by-nsa-using-gooseegg-tool/

4. Apache Cordova App Harness Targeted in Dependency Confusion Attack Apache Cordova App Harness遭遇依赖混淆攻击 https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html

威胁7

意外的数据泄露

由于配置错误，数据意外泄露的风险每年都在增长。[1] 免费的公共搜索工具可以帮助找到公开的数据仓库。[2] 这些风险存在于亚马逊（S3桶、弹性容器注册表、弹性块存储）、Azure Blob、GCP存储、Docker Hub、Elasticsearch、Redis和GitHub等平台上。[3] 尽管这些问题在过去两年中已被广为知晓和讨论，但Elasticsearch和S3的漏洞通常会在暴露后24小时内发生。2024年4月，云安全联盟发布研究指出21.1%的公共桶含敏感数据。仅过去一年里，除姓名、国籍、生日及性别等基本信息外，还意外披露了大量其他敏感资料如护照信息、密码、学历资料、驾照详情，汽车信息，医疗记录以及生物特征等。这些意外泄露多能预防，并主要由监管不足与控制失当引起。

例如，在创建S3桶时，用户或管理员决定是否启用公共读取权限；添加数据时也给用户同样选择权。默认设置是私有的且需手动更改为公开状态。虽然旧桶中仍有部分历史设置存在，但这个安全问题主要源于选择便利性而忽视了安全性。

商业影响

意外的数据泄露既可能是威胁，也可能是结果 - 这源于内部员工在不考虑安全影响的情况下寻求简化生活。这也是违规行为和其他威胁所导致的后果。其结果明显且每月都有相关新闻报道。

技术影响：

- 数据泄漏：当敏感公司或个人数据因配置错误或其他问题被窃取时，未经授权获取或使用该数据的人将能看到这些信息。

运营影响：

- 业务中断：攻击者可能在几分钟内找到并破坏未加保护的存储和容器，使系统停止运行。

财务影响：

- 不合规：加利福尼亚消费者隐私法案（CCPA）和通用数据保护条例（GDPR）对违规行为设定了严重罚款。

声誉影响：

- 公司信誉：由违规事件引发的公众关注可能会改变消费者和企业对公司诚信度以及治理、控制和管理能力的认知。

关键措施

1. 所有云平台都容易出现配置错误或用户错误，技术解决方案相对有限 - 这些问题通常是流程上的挑战，需要强大的教育计划、IT审计倡议和法律规划等。

2. 一些基本的配置步骤可以显著地减少这个问题中“意外”的部分。确保正确配置

存储桶以最小化访问（维护私人设置，加密内容，并使用多因素认证（MFA）生成强密码）。每个主要的云服务提供商（如Amazon, Google, Microsoft）都提供了安全配置的详细指南。[5]

3. 为了显著降低风险暴露，请实施数据库最小权限身份和访问管理(IAM)策略。确保严格控制并监视此政策的执行情况。禁用/不使用访问控制列表 (ACLs)，而选择IAM以获取更高级别的安全性。持续推进零信任架构。

4. 为了确保合规性，数据所有者必须定期识别和审计数据存储桶及其权限。如果已经进行过相关配置，则云安全态势管理(CSPM)工具可以自动修复问题。

案例

近期各类云数据意外泄露事例包括：

（2023 年 6 月）密码泄露：一个公开链接导致人们可以访问含有 38TB Azure 存储桶的 Microsoft 密码、Teams 消息和文件。亚马逊和 CSA 均强烈反对使用此类链接。[4, 5, 6]

（2023 年 6 月）护照信息泄露：世界棒球软球联合会 S3 存储桶配置错误，导致 48000 条记录被暴露，其中包含 4600 本护照。请参考安全问题 3（配置错误及更改控制不足），以及亚马逊和 CSA 的建议。[4, 5, 7]

（2023 年 5 月）教育数据泄漏：大学招生机构 CaptainU 公开了近 100 万名高中生的学术记录，包括图片和私人信息（涉及 13 至 18 岁学生）。这个案例显示出用户属性不仅被存储并外泄，完整对话、图像等也附加在这些记录上，并一同被存储。[8]

（2023 年 5 月）生物特征数据泄漏：美国政府 AI 承包商 Veritone AI 公开了 550GB 音频、视频以及生物识别图像资料，员工身份信息，警察行车记录仪录像，信息自由法案（FOIA）请求相关文件以及带有授权令牌的系统日志。部分数据可被用于制作深度伪造内容，进一步提高其对欺诈者的价值。[9]

CSA 云计算关键领域安全指南 5.0

领域 2：云治理

领域 5：身份和访问管理

领域 7：基础设施与网络

领域 9：数据安全

领域 10：应用程序安全

CSA 云控制矩阵 v4.0

A&A 应用程序和接口安全

AIS-02：应用程序安全基线需求
AIS-04：应用程序安全设计和开发

BCR 业务连续性管理与运营弹性

BCR-05：文档记录

DSP 数据安全与隐私生命周期管理

DSP-01： 安全、隐私政策和程序
DSP-02： 安全处置
DSP-03： 数据清单
DSP-05： 数据流文档
DSP-06： 数据所有权和管理权
DSP-07： 设计和默认数据保护
DSP-09： 数据保护影响评估
DSP-10： 敏感数据传输
DSP-11： 个人数据访问，撤销，纠正和删除
DSP-13： 个人数据子处理
DPS-14： 披露数据子处理者
DPS-16： 数据保存和删除
DPS-17： 敏感数据保护

IAM 治理、风险管理和合规

GRC-01：治理计划策略和程序
GRC-02：风险管理计划

IAM 身份识别与访问控制

IAM－01：身份与访问控制的策略和规程
IAM－03：身份清单
IAM－05：最小权限

IVS 基础设施与虚拟化安全

IVS－01：基础设施与虚拟化安全策略和程序
IVS－03： 网络安全
IVS－06： 分区与隔离

参考链接

1. Code42 2024年度数据泄露报告
   https://www.code42.com/resources/reports/2024-data-exposure
2. 存储桶搜索工具https://buckets.grayhatwarfare.com/
3. 2023年云端蜜罐陷阱报告
   https://orca.security/resources/blog/2023-honeypotting-in-the-cloud-report/
4. 云安全联盟 - 公开暴露的S3存储桶的危险数据（以及如何补救）
   https://cloudsecurityalliance.org/blog/2023/04/06/the-data-on-the-danger-of-publicly-exposed-s3-buckets
5. 亚马逊S3的安全最佳实践
   https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
6. 微软Azure数据泄露暴露了文件共享链接的危险
   https://www.darkreading.com/cloud-security/microsoft-azure-data-leak-exposes-dangers-of-file-sharing-links
7. 配置错误的WBSC服务器泄露数千本护照
   https://cybernews.com/security/wbsc-data-leak-passports/
8. 大学招生数据库泄露近百万学生的GPA成绩、SAT分数、ID和其他个人数据
   https://cybernews.com/security/college-recruitment-database-leaking-nearly-1-million-students-gpas-sat-scores-ids-and-other-personal-data/
9. 与美国政府有关联的AI公司在数据泄露中暴露了数十亿份文件
   https://www.biometricupdate.com/202405/ai-firm-with-ties-to-u-s-government-exposes-of-billions-of-documents-in-breach

威胁8
系统漏洞

系统漏洞是云服务平台中的缺陷，可用来损害数据的机密性、完整性和可用性，并可能造成服务运营中断。云服务通常由定制软件、第三方库和服务以及操作系统构建。任何这些组件中的漏洞都会使云服务更容易受到网络攻击。系统漏洞主要有四类：

- 配置错误-当使用默认或不正确的配置设置部署云服务时，云服务器会出现漏洞。根据美国国家安全局的说法，云资源配置错误是最普遍的云漏洞。[4] 如前所述，配置错误是本出版物“顶级威胁”调查响应者发现的首要安全问题。
- 零日漏洞-这些漏洞是由威胁行为者发现和利用的，但云服务提供商和软件供应商并不知道这些漏洞。
- 未修补软件-包含已知安全漏洞的软件，尽管有针对这些问题的补丁，但这些漏洞尚未得到修复。
- 弱凭据或默认凭据-缺乏强身份验证会增加威胁行为者未经授权访问敏感数据和系统的机会。

处理系统漏洞需要持续监控系统和网络活动，并定期进行漏洞扫描，以便在黑客发现之前发现安全问题。应定期使用补丁管理系统来查找、获取、测试和部署软件更新或补丁，以修复应用程序和系统中的已知安全漏洞。部署零信任架构可以通过持续身份验证和强制最小权限访问来限制对重要系统资源的访问，从而帮助抵御攻击。

商业影响

系统漏洞以多种方式对云服务的性能和运行产生负面影响。只要系统漏洞没有修补，系统漏洞对云服务的影响就会显现出来。以下是系统漏洞可能造成的一些影响：

技术影响：

- 安全性减弱：未能解决系统漏洞的云服务更容易受到攻击和危害。
- 数据丢失：敏感和关键任务的数据更容易从存在未修补漏洞的系统中盗取或暴露。

运营影响：

- 业务中断：数据丢失会使组织无法履行对合作伙伴和客户的业务承诺。
- 系统性能受损：受到攻击的云服务可能会出现系统性能下降甚至系统中断的情况。

财务影响：

- 收入损失：因服务中断、恢复成本、客户不满或法律诉讼造成的财务损失。
- 不合规和罚款：未能遵守漏洞管理和相关处罚的监管要求而受罚。

声誉影响：

- 公司声誉受损：损害云服务组织的公众形象和品牌价值。
- 客户声誉受损：依赖受损的第三方云服务的客户可能会遭遇数据泄露和服务中断，对其声誉产生负面影响。

关键措施

1. 系统漏洞是云服务中的缺陷，会扩大其攻击面。
2. 美国国家安全局（NSA）和顶级威胁调查的受访者将配置错误确定为最重要的云

服务漏洞。

3. 对系统和网络的持续监控提供了对安全漏洞和其他系统完整性问题的可见性。
4. 定期的补丁管理可确保获取和部署最新的安全补丁，使系统更能抵御网络攻击。
5. 零信任架构可以通过限制对关键云资源的访问来限制零日漏洞的潜在损害。

案例

最近与云中系统漏洞相关的问题示例包括：

（2023 年 1 月）Fortra 披露，有黑客利用了其 GoAnywhere 托管文件传输服务（MFT）中的远程代码执行（RCE）漏洞。该漏洞的漏洞号为 CVE-2023-0669，该漏洞使攻击者能够在某些客户环境中创建未经授权的用户账户，并从 MFT 服务下载文件。[3]

（2023 年 3 月）OpenAI 将其 ChatGPT 服务脱机，以修复该公司在其 Redis 缓存客户端代码中引入的一个错误。Redis 是一个开源系统，ChatGTP 使用 Redis 来缓存用户数据，以最大限度地减少直接数据库访问。该漏洞暴露了用户的聊天记录和新创建的对话中的第一条消息。此外，还暴露了属于 1.2%的 ChatGPT Plus 用户的支付相关信息，包括姓名、电子邮件地址、支付地址、支付卡到期日期以及客户卡号的最后四位数字。[1]

（2023 年 5 月）总部位于俄罗斯的 Clop 勒索软件集团入侵了 MOVEit 的托管文件传输服务（MFT），该组织利用了 MFT 系统中的 4 个 SQL 注入漏洞。这些漏洞分别为 CVE-2023-34362、CVE-2023-35036、CVE-2023-35708 和 CVE-2023-3693X。这些攻击影响了多个 MOVEit 客户，包括美国政府组织和私营部门公司。据估计，有 500 多个组织和 3400 万人受到影响，其中 72%的受害者组织在美国，但许多其他组织在欧洲和亚洲。Clop 勒索软件组织的操作方法已从加密数据转向暴露从目标检索到的敏感数据的威胁。[6]

领域 5：身份和访问管理

领域 6：安全监控

领域 7：基础设施和网络

领域 9：数据安全

领域 10：应用程序安全

领域 11：事件响应和弹性

CSA 云控制矩阵 v4.0

AIS 应用程序和接口安全

AIS-01：应用和接口安全策略和程序

AIS-02：应用程序安全基线需求

AIS-06：自动应用程序安全部署

AIS-07：应用程序漏洞修复

CEK 密码学、加密和密钥管理

CEK-03：数据加密

CEK-04：加密算法

IVS 基础设施与虚拟化安全

IVS-04：操作系统加固与基线控制

TVM 威胁、脆弱性管理

TVM-01：威胁、脆弱性管理策略及规程

TVM-02：恶意软件防护策略和规程

TVM-03：脆弱性补救程序

TVM-04：检测更新

TVM-05：外部库脆弱性

TVM-06：渗透测试

TVM-07：脆弱性识别

TVM-08：脆弱性优先级

TVM-09：脆弱性汇报管理

威胁9

云可见性/可观测性不足

当组织无法有效地可视化和分析云服务的使用是安全的还是恶意的时，有限的云可见性问题就会出现。这个问题包括两个关键挑战：使用未经批准的应用程序和滥用经批准的应用程序。当员工在没有公司 IT 和安全部门的特定许可和支持的情况下使用云应用程序和资源，导致影子 IT 时，就会发生未经批准的应用程序使用。当涉及敏感的公司数据时，这种情况尤其危险。当组织无法监控内部人员如何使用其批准的应用程序或者外部威胁行为者瞄准这些应用程序，就会发生受批准的应用程序的滥用，这些滥用通常是通过凭证盗窃、SQL 注入和 DNS 攻击等方法来进行的。[1, 2, 3]

2023 年，几起重大的云泄露事件突显了缺乏云可见性的挑战。值得注意的例子包括：

- 导致数据泄露的人为错误：泰雷兹（2023）报告称，超过三分之一（39%）的企业在其云环境中经历了数据泄露，其中一半以上（55%）的事件是人为错误造成的。这突显了对提高云环境的可见性和控制力度以防止此类错误的迫切需要。
- 未检测到的安全漏洞：根据 Gigamon（2023）的数据，近三分之一的安全漏洞没有让 IT 和安全专业人员发现。这种缺乏检测突显了感知和实际安全之间的差距，强调了提高可见性和监控工具的必要性。
- 云泄露的成本：Illumio 的研究（2023 年）发现，近一半的数据泄露源于云，每次泄露平均给组织造成 410 万美元的损失。这些漏洞的一个重要原因是对云连接和第三方软件交互的可见性不足。
- 配置错误和访问问题：Expert Insights（2023）报告称，许多云数据泄露是由于访问权限配置错误造成的。大约 83%的组织经历了至少一次与访问相关的云数据泄露的配置错误，许多配置缺乏对用户权限和资源访问的可见性。

组织正在认识到全面监控以及健壮的访问控制[3]并采用零信任分段等高级安全实践的重要性，以降低这些风险并增强整体云安全弹性。[4, 5]

商业影响

有限的云可见性可能会通过各种技术、运营、财务和声誉后果严重影响企业。以下是主要影响：

技术影响：

- 安全性减弱：由于不受监控的漏洞和配置错误，无法缓解可见性问题的云服务更容易受到攻击和损害。
- 数据丢失：APT 攻击通常旨在窃取或暴露敏感和关键任务数据，损害业务信息的完整性和机密性。

运营影响：

- 业务中断：数据丢失可能会使组织无法履行对合作伙伴和客户的业务义务，从而导致重大的运营停滞。
- 系统性能受损：对云服务的攻击会降低系统性能或导致系统中断，影响整体生产力和服务交付。

财务影响：

- 收入损失：服务中断、恢复成本、客户不满或违规后的法律诉讼可能导致财务损失。
- 不合规和罚款：不遵守监管安全要求可能会导致巨额罚款和处罚，这可能会影响组织的财务稳定性。

声誉影响：

- 公司声誉受损：数据泄露会损害云服务提供商的公众形象和品牌价值，使其难以重新获得客户信任。
- 客户声誉受损：依赖受损云服务的客户也可能遭受数据泄露和服务中断，这可能会对客户的声誉和客户关系产生负面影响。

关键措施

1. 开发全面的云可见性：从自上而下的方法开始，让云安全架构师创建一个集成人员、流程和技术的解决方案。
2. 强制全公司培训：确保所有员工都接受过关于公认的云使用政策及其执行的培训。[6]
3. 审查和批准未批准的服务：让云安全架构师或第三方风险管理审查和批准所有未批准的云服务。
4. 投资云访问安全代理（CASB）和零信任安全（ZTS）解决方案：使用这些工具分析出站活动，发现云使用情况，并识别有风险的用户和有资格的员工行为异常。
5. 部署web应用程序防火墙（WAF）：监控所有入站连接的可疑趋势、恶意软件、DDoS和僵尸网络风险。
6. 监控关键企业云应用程序：选择解决方案来控制关键应用程序并减轻可疑行为。
7. 实施零信任模型：在整个组织内采用零信任方法，以确保健壮的安全性。

案例

最近与云可见性有限相关的问题包括：

(2023 年 9 月至 2023 年 10 月）持续约 22 天的 Okta 漏洞是另一个突出云可见性至关重要的例子。Okta 的客户 1Password 首先发现了漏洞，后来 BeyondTrust 证实该漏洞。攻击者通过入侵 Okta 员工的个人谷歌账户获得了访问权限，该账户用于保存 Okta 服务账户凭据。此次数据泄露影响了所有 Okta 员工身份云（WIC）和客户身份解决方案（CIS）客户，但 FedRamp High 和 DoD IL4 环境中的客户除外。包括联邦快递、惠普和 T-Mobile 等大公司在内的数百名 Okta 客户的敏感数据可能遭到泄露。此次数据泄露突显了云服务提供商的漏洞以及此类数据泄露可能带来的广泛影响，引发了人们对 Okta 的安全实践及其保护客户数据能力的担忧。[7, 8]

（2023 年 10 月至 2023 年 12 月）23 日，由于云存储桶配置错误，领先的消费者遗传学公司 Me 遭遇了重大数据泄露。超过 500 万客户的个人基因组数据遭到泄露。这一漏

洞突显了在云环境中保持严格的可见性和访问控制的重要性，特别是那些处理高度敏感信息的环境。此类敏感数据的暴露不仅损害了客户隐私，还引发了人们对公司内部数据安全实践的严重担忧。这一事件清楚地提醒人们，云可见性不足的潜在后果以及需要持续监控和配置管理来保护敏感数据。[9, 10]

CSA 云计算关键领域安全指南 5.0

领域 1：云计算概念和架构

领域 3：风险、审计和合规性

领域 5：身份和访问管理

领域 8：云工作负载安全

领域 9：数据安全

领域 10：应用程序安全

领域 11：事件响应和恢复能力

CSA 云控制矩阵 v4.0

IAM 身份和访问控制

A IAM-03：身份清单

IAM-08：用户访问评审

TVM 威胁、脆弱性管理

TVM-01：威胁、脆弱性管理策略及规程

TVM-02：恶意软件防护策略和规程

TVM-03：脆弱性补救程序

SE 供应链管理、透明性能和可核查性

STA-08：供应链风险管理

参考链接

1. Palo Alto Networks 的 Prisma Cloud：云发现和风险管理
   https://start.paloaltonetworks.com/prisma-cloud-request-a-trial
2. Gigamon：私有云可视性的五大关注点
   https://blog.gigamon.com/2024/03/05/five-top-concerns-in-private-cloud-visibility/
3. 泰雷兹：2023 年云安全研究 - 全球版
   https://cpl.thalesgroup.com/cloud-security-research
4. Illumio：云安全指数：通过零信任分段重新定义云安全
   https://www.illumio.com/resource-center/cloud-security-index-2023
5. CrowdStrike：2023 年云风险报告
   https://www.crowdstrike.com/cloud-risk-report/

6. 2024 年你应该了解的 50 个云安全统计数据
https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/

7. ManageEngine：了解 2023 年的 Okta 供应链攻击：全面分析
https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html

8. BeyondTrust：Okta 支持单元违规更新
https://www.beyondtrust.com/blog/entry/okta-support-unit-breach-update

9. 23andMe 数据被黑客攻击数月未被发现
https://www.engadget.com/23andmes-data-hack-went-unnoticed-for-months-081332978.html

10. 23andMe 证实黑客窃取了 690 万用户的数据
https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9- million-users/

威胁10
未验证的资源共享

认证的云资源共享可能给云服务带来重大的安全风险。云资源可能包括虚拟机、存储桶和数据库，这些资源都包含对业务运营至关重要的敏感数据和应用程序。如果没有适当的用户认证或遵循最小权限原则，云资源就容易被想要窃取公司和个人机密数据的威胁行为者所利用。

在保护云资源的最佳实践中，至少需要进行基本的身份验证，如输入密码。然而，每年都会有大量数据泄露事件发生，原因是云存储和数据库系统没有密码保护。在当今互联网的海量数据中，找到未受保护的云资源似乎是一项挑战，但实际情况恰恰相反。多年来，像 Shodan、Binary Edge 和 Gravhat Warfare 这样的公共可用物联网（IoT）搜索工具一直存在，很容易发现未受保护的数据存储库。

- 除了密码保护之外，还可以采取其他安全措施来保护关键数据：
- 多因素认证（MFA）：当尝试访问数据时，MFA 要求用户通过二次验证来验证其身份，如一次性访问代码或生物识别验证。
- 第三方认证平台：使用专门用于验证用户身份的服务可以帮助组织可靠地管理用户认证，并提供诸如一键或触式授权的认证方案。

一旦发现漏洞，就可以在网络犯罪分子发现并利用它们之前进行修复。

商业影响

以下是未验证云资源可能导致的一些负面影响：

技术影响：

- 数据泄露：未经授权的威胁行为者可能窃取或暴露敏感和关键任务数据。
- 数据丢失：对数据的无限制访问可能导致部分或全部数据被破坏。

运营影响：

- 业务中断：数据丢失可能阻止组织履行对合作伙伴和客户的业务义务。

财务影响：

- 收入损失：由于服务中断、服务恢复、客户不满或法律行动导致的财务损失。
- 不合规和罚款：未能遵守漏洞管理的监管要求及相关处罚。

声誉影响：

- 公司声誉：损害云服务组织的公众形象和品牌价值。
- 客户声誉：依赖受损第三方云服务的客户可能会经历数据泄露和服务中断，对他们的声誉产生负面影响。

关键措施

1. 云存储和数据库设施有时没有密码保护，任何人都可以轻易利用。对云资源的访问进行限制，实施基本的用户认证和密码强制是必不可少的。
2. 通过部署多因素认证（MFA）和使用第三方授权服务，可以进一步改进认证。
3. 持续监控用户可以帮助确定他们的行为是合法的还是恶意的。

案例

（2023 年 9 月）KidSecurity 是一个广泛使用的家长控制应用程序，父母可以用它来追踪自己的孩子、听孩子的声音和设定游戏时间限制。研究人员发现该公司未能保护其服务使用的 Elasticsearch 和 Logstash 集合，暴露了用户的私有数据。KidSecurity 的日志对互联网上的任何人开放了一个多月。超过 3 亿条记录的私有用户数据被暴露，包括 21,000 个电话号码和 31,000 个电子邮件地址。该应用程序还暴露了用户的支付信息，透露了信用卡号码的前六位和后四位、有效期月份和年份，以及发卡银行。[2,4]

（2023 年 10 月）印度国有的 National Logistics Portal-Marine 网站由于配置错误的 Amazon S3 存储桶而暴露了敏感和私有数据。该网站还传递了一个包含登录凭证的 Javascript 文件给浏览器。暴露的数据包括全名、国籍、出生日期、性别、护照号码、护照签发机构、船舶和其他船员提交的旅行信息的到期日期。发票、航运订单和货物账单也是敏感数据。[3]

（2024 年 1 月）研究人员发现，Tunefab 转换器（用于从 Spotify、亚马逊的 Audible 和苹果音乐等流媒体系统转换音乐）暴露了用户的私有数据。该平台暴露了超过 1.51 亿条记录，包含用户的 IP 地址、地区、ID、电子邮件地址和设备信息。数据泄露是由于配置错误的 MongoDB 数据库造成的，该数据库没有密码保护的访问权限，并出现在公共互联网上。该数据库于 9 月 26 日被发现在一个公共可用的物联网搜索引擎上。[4,5]

CSA 云计算关键领域安全指南 5.0

领域 3：风险、审计和合规

领域 5：身份与访问管理

领域 6：安全监控

领域 9：数据安全

领域 10：应用安全

CSA 云控制矩阵 v4.0

A&A 审计与保证

A&A-04：符合性需求

A&A-05：审计管理过程

DSP 数据安全与隐私生命周期管理

DSP-07：设计和默认数据保护

DSP-17：敏感数据保护

IAM 身份和访问控制

IAM-01：身份与访问控制策略与规程

IAM-02：强密码的策略与规程

IAM-07：用户访问变更和撤销

IAM-08：用户访问评审

IAM-14：强鉴别

IAM-15：密码管理

LOG 日志记录与监控

LOG-05：审计日志监控与响应

LOG-12：访问控制日志

TVM 安全事件管理、电子发现及云取证

TVM-06：渗透测试

威胁 11
高级持续性威胁 (APT)

高级持续性威胁（APT）对云安全构成重大风险。这些复杂的对手，包括国家级行为者和有组织的犯罪团伙，他们拥有资源和专业知识来开展长期攻击活动，目标是云中的敏感数据和资源。

在 2022-2023 年，APT 活动通过各种战术显著威胁了云环境，包括勒索软件和敲诈、利用零日漏洞、网络钓鱼和凭证盗窃、破坏性擦除数据攻击以及供应链破坏。 这些方法突显了 APT 的持续性，需要强有力的安全措施来保护云基础设施免受这些高级威胁的侵害。

为了在云中防御 APT，组织应该监控网络威胁情报，以了解最相关的 APT 组织及其战术、技术和程序（TTP）。红队演习可以帮助测试和提高对模拟 APT 攻击的检测和响应能力。在云环境中进行威胁狩猎行动对于识别 APT 隐蔽而持久的存在也至关重要。多层次的云安全策略，包括强大的访问控制、加密、监控和事件响应，对于对抗这些高级对手是必不可少的。

商业影响

APT 可以通过多种渠道严重影响企业，导致技术、运营、财务和声誉方面的后果。

技术影响：

- 安全性减弱：未能解决 APT 漏洞的云服务更容易受到攻击和破坏。
- 数据丢失：APT 攻击通常旨在窃取或暴露敏感和关键任务数据，损害商业信息的完整性和机密性。

运营影响：

- 业务中断：数据丢失可能阻碍组织履行对合作伙伴和客户的业务义务，导致运营停滞。
- 系统性能：对云服务的攻击可能会降低系统性能或导致系统停机，影响整体生产力和服务交付。

财务影响：

- 收入损失：服务中断、恢复成本、客户不满或违规后法律行动可能导致的财务损失。
- 不合规和罚款：未能遵守监管安全要求可能导致巨额罚款和处罚，这可能影响组织的财务稳定。

声誉影响：

- 公司声誉：高级持续性威胁（APT）可能会损害云服务提供商的公众形象和品牌价值，难以重新获得客户信任。
- 客户声誉：依赖受损云服务的客户也可能遭受数据泄露和服务中断，这可能对他们的声誉和客户关系产生负面影响。

关键措施

1. 业务影响分析：定期分析业务影响，以识别和了解组织的关键信息资产和潜在漏洞。这将有助于优先考虑安全工作和资源分配，以保护最有价值数据免受 APT 威胁。

2. 网络安全信息共享：参与网络安全信息共享组和论坛，了解最活跃的 APT 组织及其战术、技术和程序（TTPs）。通过这些集体知识，可以增强企业的防御和响应能力。
3. 攻击性安全演习：通过红队演习和威胁狩猎活动定期模拟 APT 的战术、技术和程序（TTPs）。这些攻击性安全演习有助于测试和提高您的检测和响应能力，确保您的安全措施能够有效应对复杂的威胁。

CSA 云计算关键领域安全指南 5.0

领域 1：云计算概念和架构

领域 3：风险、审计和合规

领域 5：身份与访问管理

领域 8：云工作负载安全

领域 9：数据安全

领域 10：应用安全

领域 11：事件响应和弹性

CSA 云控制矩阵 v4.0

IAM 身份和访问控制

A IAM-03：身份清单

IAM-08：用户访问评审

LOG 日志记录和监控

LOG-03：安全监控与警报

LOG-05：审计日志监控和响应

SEF 安全事件管理、电子发现及云取证

SEF-03：事件响应计划

STA 供应链管理、透明性能和可核查

STA-08：供应链风险管理

TVM 威胁、脆弱性管理

TVM-01：威胁、脆弱性管理策略及规程

TVM-02：恶意软件防护策略和规程

TVM-03：脆弱性补救程序

TVM-04：检测更新

TVM-05：外部库脆弱性

TVM-06：渗透测试

TVM-07：脆弱性识别

TVM-08：脆弱性优先级

TVM-09：脆弱性汇报管理

TVM-10：脆弱性管理指标

结论和未来展望

本报告分析了云安全威胁的演变态势，重点关注了配置错误、IAM（身份和访问管理）弱点、不安全的 API 以及缺乏全面安全策略的持续性问题。虽然这些威胁与 2022 年报告中识别的相同，但它们的持续存在突显了其关键性。

一些趋势可能会塑造云安全威胁的未来。组织必须保持信息灵通并适应这些趋势，以维护安全的云环境。

关键趋势包括：

- 攻击复杂性的增加：攻击者将继续开发更复杂的技术，包括通过人工智能技术利用云环境中的漏洞。这些新技术将需要具有持续监控和威胁狩猎能力的主动安全姿态。
- 供应链风险：云生态系统的日益复杂将增加供应链漏洞的攻击面。组织需要将其安全措施扩展到其供应商和合作伙伴。
- 不断演变的监管环境：监管机构可能会实施更严格的数据隐私和安全法规，要求组织适应其云安全实践。
- 勒索软件即服务（RaaS）的兴起：RaaS 将使技术不熟练的参与者更容易对云环境发起复杂的勒索软件攻击。组织将需要强大的数据备份和恢复解决方案以及严格的访问控制。

一些关键的缓解策略包括：

- 在整个软件开发生命周期（SDLC）中集成 AI：利用 AI 进行代码审查和早期开发中的自动漏洞扫描等任务，将有助于在代码投入生产之前识别和解决安全问题。
- 使用 AI 驱动的进攻性安全工具：这些工具模拟攻击者行为，以发现云配置、IAM 协议和 API 中的漏洞。这种主动方法有助于组织领先于潜在威胁。
- 云原生安全工具：组织将越来越多地采用专为云环境设计的云原生安全工具。与传统安全解决方案相比，这些工具提供更好的可见性和控制。
- 零信任安全模型：零信任模型强调持续验证和最小权限访问，已成为云安全的

标准。

- 自动化和编排：自动化安全流程和工作流程对于管理云安全复杂性至关重要。
- 安全技能差距：网络安全技能差距将继续是一个挑战。组织需要重视和投入预算用于培训和发展计划，为员工提供持续教育，不断提升员工的安全专业技能和安全意识。

组织可以通过采用这些策略并保持对不断演变的威胁的警惕，来构建安全和弹性的云环境。然而，网络安全格局在不断变化。持续适应和投资于尖端安全解决方案，如云安全态势管理（CSPM）或端点检测和响应（EDR）工具，对于保持领先地位和减轻与云安全漏洞相关的财务和声誉风险至关重要。

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905