OWASP 中国
Open Worldwide Application Security Project

2024 OWASP Top 10
基础设施安全风险

前言

动机 - 为什么《OWASP Top 10 基础设施安全风险》如此重要?

本 OWASP 项目旨在提升人们对基础设施安全风险、威胁与漏洞的意识，并提供高质量的信息。基础设施安全风险在信息安全领域中占据着至关重要的地位。在成功入侵系统后，这些漏洞往往是导致整个企业或组织遭受重大安全破坏的主要因素。尽管这些威胁在网络攻击链中具有重要地位，但由于攻击来源往往是内部而非外部，因此它们常被企业和组织忽视。企业和组织必须认识到，单纯的外部防护措施远远不足够。如果攻击者能够突破或绕过外部防线（例如通过钓鱼攻击），并找到初步的突破点，那么完善的内部防御机制就显得尤为关键。尤其是威胁检测与监控，它们能够及时发现内部攻击和潜在威胁。正是基于这些考虑，我们启动了这一项目，旨在提供实用且高质量的信息，普及这些威胁的认知，从而加强全球企业和组织的内部安全防护。

开放数据征集、下一版本与贡献

为进一步提升《OWASP Top 10 基础设施安全风险》的质量与影响力，我们诚邀您参与 2024 与 2025 年度的开放数据征集活动。在此期间，您可以匿名或公开捐赠数据，贡献给本项目。我们将在 2024 和 2025 年间收集并整理所有数据，进而为 2026 版本的发布做准备。通过这一方式，我们计划在发布《OWASP Top 10 基础设施安全风险 - 2026 版》时，使用更为全面的数据集，以进一步提升其质量与深度。

对于捐赠者与贡献者，我们将在相关项目页面上列出他们的名字作为赞助商（如愿意）。此外，我们还计划对与基础设施安全风险相关的 CVE（公共漏洞与暴露）和 CWE（常见弱点枚举）进行深入研究。欲了解更多详情或参与贡献，请访问我们的相关平台。https://github.com/OWASP/www-project-top-10-infrastructure-security-risks/blob/main/docs/2024/INT_2024-Open_Call_for_Data.md

版本

Edition: 2024 Version: 2024

项目贡献者

项目负责人：Nick Lorenz、Tim Barsch

贡献者：Tobias Neugebauer

中文版项目人员：张坤、刘畅，许天翔，陈殷

审核：陈殷

ISR01:2024_过时的软件

描述

保持软件的及时更新至关重要。因为更新往往包含与安全相关的补丁，如果软件未能保持最新状态，它可能会存在已知的漏洞。这些漏洞通常是公开的，并且可以通过安全扫描工具轻松识别。不幸的是，许多企业和终端用户未能定期更新其软件组件。缺乏有效的更新机制和管理，使得许多软件和底层系统随着时间推移逐渐暴露于风险之中，且随着时间的延续，其危害性也日益加剧。

风险

过时的软件可能引发各种不同的安全漏洞，涵盖从低风险的漏洞到可能导致整个系统被攻陷的严重问题。软件系统中这些漏洞的严重性和数量因具体情况而异。通常，随着时间的推移，漏洞的数量和危害性会逐渐增加，因为新的漏洞不断被发现，系统的安全风险也随之加剧。

整改措施

建议将所有软件组件（包括库文件等）保持在最新、稳定且受支持的版本。应定期检查每个软件及其组成部分的更新和补丁。建议实施更新管理流程，确保不遗漏任何组件，且能及时进行检查。此外，定期访问供应商网站和信息安全平台，关注相关软件的 0day 漏洞信息也是十分重要的。在某些情况下，虽然这些漏洞可能暂时没有官方更新，但企业或个人仍应采取必要的防范措施，以减少漏洞带来的潜在风险或降低其发生的概率。

攻击场景示例

场景#1：过时的 Web 服务器

某公司部署了一个内部网站，供员工访问和获取信息。然而，由于公司缺乏有效的更新管理流程，未能定期检查和更新软件组件，所使用的 Web 服务器已运行过时版本，存在已知漏洞。其中一个漏洞是远程代码执行（RCE）。一名攻击者通过入侵某员工的计算机，获取了对其设备的控制权限，并通过枚举该内部 Web 服务器的版本，迅速发现了与该版本相关的远程代码执行漏洞（CVE）。随后，攻击者找到相应的漏洞利用工具，成功突破安全防线，获取了底层服务器的访问权限。

场景#2：废弃的旧服务器

某公司拥有一套更新管理流程，旨在确保所有软件组件保持最新。然而，这一流程未能覆盖到一台存储着机密建设计划的旧内部服务器。攻击者成功入侵公司内部网络，发现了这台服务器，并通过枚举其操作系统版本，发现该版本已不再获得厂商支持，且存在多个漏洞，其中包括一些严重的漏洞。攻击者利用公开的漏洞利用工具成功入侵服务器，窃取了公司的商业秘密，并将这些信息出售给了公司的竞争对手。

ISR02:2024_不足的威胁检测

描述

威胁检测在网络安全防御中至关重要。在多数网络攻击中，尤其是内部攻击，威胁行为者的首次被察觉通常为时已晚。大多数网络攻击往往是在威胁行为者执行恶意行为，导致内部流程受到干扰或员工工作受到影响时才被发现。例如，当勒索软件开始加密员工计算机或关键服务器上的数据时，网络攻击的检测通常已经太迟。有效的威胁检测应在威胁行为者和恶意活动造成严重损害之前，及时识别并应对。理想情况下，威胁行为者应在入侵初期阶段就被发现，或者最迟应在其建立控制的命令与控制阶段进行识别。

风险

如果威胁行为者未能在网络攻击初期被及时发现，目标系统很可能陷入无力防御的境地，无法采取有效的应对措施。威胁行为者通常在内部网络中潜伏数周甚至数月，直到他们开始执行明显的恶意操作。不足的威胁检测是复杂网络攻击频繁得逞的主要原因之一。如果没有完善的检测与监控机制，目标系统将无法察觉威胁行为者已进入内部网络并在其中横向移动。

整改措施

为构建高效且有力的威胁检测系统，建议在内部基础设施的多个层面和关键节点上实施不同的流程和机制。安全事件与事件管理（SIEM）系统、防火墙、端点检测与响应（EDR）应用程序以及其他监控活动的工具和软件，构成了威胁检测体系的基础。至关重要的是，在尽可能多的基础设施层面和节点上部署这些传感器与系统，例如计算机、服务器以及网络的不同 ISO/OSI 层级。通过这种方式，能够显著提高网络攻击及其威胁行为者的早期发现率，使得目标能够采取相应措施，及时防御潜在的毁灭性攻击，保护内部基础设施免受损害。

攻击场景示例

场景#1：网络检测不足

某公司拥有内部基础设施，包括员工计算机等端点系统，以及用于承载内部应用的服务器，这些服务器存储着公司关键的业务数据。公司为每台员工设备安装了端点检测与响应（EDR）软件。然而，一名员工不小心下载并执行了恶意软件，却没有意识到其危害。该恶意软件由一个先进持续性威胁（APT）组织所编写，这是一个高度专业化的网络犯罪集团，而 EDR 系统未能识别该恶意软件。结果，恶意软件从员工的受感染计算机入侵到一台内部服务器，并开始横向传播，逐步感染了所有内部服务器。由于缺乏有效的网络威胁检测系统，这一过程未能及时被发现。最终，恶意软件加密了服务器上的所有数据，公司失去了对这些数据的访问，从而无法继续进行正常的业务操作。如果公司当时实施了冗余且全面的威胁检测与监控系统，而不仅仅依赖 EDR 软件，完全可以避免这一惨剧的发生。

场景#2：异常检测不足

某公司为员工提供了内部服务，供其共享重要的数据和文件，并为员工配备了笔记本电脑以及配置好的虚拟私人网络（VPN）软件，以便他们能够在家工作。在一次火车出行中，公司的员工笔记本电脑被一名网络犯罪分子盗取权限，该犯罪分子成功获取了员工的账户信息。随后，犯罪分子访问了公司的内部共享文件，并下载了其中的所有数据。由于公司缺乏有效的异常检测系统，未能及时发现这一数据外泄行为。如果公司部署了异常检测系统，本应能发现这次大量数据传输，或注意到员工通常不访问的共享文件的异常访问。最终，犯罪分子将窃取的数据和文件出售给了竞争公司。

ISR03:2024_不安全的配置

描述

不安全的配置是一个严重的安全漏洞类别。这类漏洞通常发生在硬件、软件或网络组件未经过正确设置或配置时，从而使其暴露于潜在的网络威胁。理解并解决不安全配置问题，对提升组织的网络防御能力至关重要。要应对这些漏洞，必须采取积极主动的措施，包括定期进行审计、实施严格的配置管理，并在整个组织范围内遵循安全最佳实践。

风险

IT 系统中不安全配置的风险不容忽视。这类配置为攻击者提供了可利用的漏洞，可能导致数据泄露和横向渗透等安全问题。这些漏洞往往成为攻击者的"优先攻击成果"，为其提供了轻松进入组织网络的机会。为有效应对这一风险，组织必须优先进行正确的配置管理，定期开展安全审计，并严格遵循安全最佳实践，从而缩小攻击面，强化网络防御。

整改措施

定期进行安全审计和正确的配置管理是解决此类漏洞的关键措施。应对措施可能包括但不限于：

- 定期审计与扫描：定期开展安全审计和漏洞评估，以识别不安全的配置。自动化扫描工具可帮助主动发现并修复这些问题。
- 供应商安全建议：大多数供应商会提供有关如何更安全地配置软件的安全建议，或发布系统加固指南。
- 教育与培训：为员工提供网络安全培训与意识提升项目，降低不安全配置的发生风险。不安全配置通常是未落实最佳实践策略的结果。

攻击场景示例

场景#1：缺失安全头部请求包

某公司使用一款内部 Web 应用程序来存储敏感的客户数据。然而，该应用程序未配置必要的安全头部请求包，如内容安全策略（CSP）和 X-Content-Type-Options。一名不满的员工，具备基本的技术知识，发现了这一配置漏洞。该员工利用缺失的安全头部，发起了跨站脚本攻击（XSS），将恶意脚本注入 Web 应用程序中。脚本执行后，便将敏感的客户数据传送到该员工控制的外部服务器。安全头部的缺失使得应用程序容易受到此类客户端攻击，最终导致员工能够窃取客户的敏感数据。

场景#2：缺乏或不足的网络隔离

某医疗服务提供商在单一网络环境下进行行政操作与患者数据管理，且两者之间缺乏必要的网络隔离。一名因工作不满的内部员工，作为系统管理员，决定利用这一网络隔离不足的漏洞。凭借其高权限访问权限，他能够轻松地从行政管理网络区域跳转至患者数据管理区域。随后，他恶意篡改患者记录，造成严重的数据完整性问题，对患者的治疗安全构成了威胁。

ISR04:2024_不安全的资源与用户管理

描述

管理 IT 基础设施中的资源和用户是一个复杂且充满挑战的任务，而确保其安全性则更具难度。有效的资源和访问权限管理至关重要，这包括明确谁可以访问哪些资源以及每个用户应拥有的权限。例如，必须明确哪些数据应如何存储以及存储在何处等关键问题。大多数公司依赖集中式的资源和用户管理工具，如 Active Directory 或 Microsoft Entra ID，但管理这些复杂工具本身就是一项挑战。如果在没有完善安全策略的前提下部署这些工具，往往会导致诸多安全漏洞。此外，权限管理和访问控制常常被忽视，许多用户或技术人员拥有超出实际需求的权限。

风险

不安全的资源与用户管理可能带来诸多安全隐患。例如，用户权限过多时，一旦账户被攻击者窃取，攻击者便可获得更高权限，从而极大地增加发生严重网络攻击的风险。此外，员工离职后，如果未及时撤销其权限或删除其账户，账户的安全性也会受到威胁。如果未能严格执行如密码策略等安全规定，账户的防护将大打折扣。对于数据访问或应用程序访问等资源亦是如此。随着资源和用户数量的增加，管理视角变得愈加模糊，潜在风险也在不知不觉中积累。

整改措施

为了有效地管理资源与用户并确保其安全，需要采取一系列综合措施。首先，建议制定清晰的战略，明确当前的资源状况及哪些人员需要访问这些资源。其他权限管理同样应遵循这一原则。始终坚持"最小权限原则"，确保用户仅获得完成工作所需的权限。在此基础上，相关策略和方案应广泛应用于基础设施和技术平台，如 Active Directory。随后，必须确保严格的权限限制得以落实，并对使用的工具进行安全配置。为了进一步强化资源与用户管理，建议引入特权访问管理（PAM）等工具、原则与方案。同时，应设立授权管理团队，专

门负责决定用户的权限范围及其有效期。最后，定期更新资源和用户清单也至关重要，例如新增或淘汰服务器时，需同步更新相关记录。

攻击场景示例

场景#1：不安全的权限管理

某公司采用传统的基础设施和多个 IT 系统来管理其生产设施，依赖 Active Directory 管理 IT 资源和用户。所有员工均拥有本地管理员权限，可在自己的设备上安装额外软件。IT 管理员都拥有域管理员权限，凭此可以管理员工设备、提供问题解决支持并维护基础设施。某员工因威胁行为者实施的社会工程学手段，被诱导打开了收到的恶意邮件附件，笔记本电脑因此被感染，但无人察觉。由于该员工拥有本地管理员权限，威胁行为者能够运行 mimikatz 等恶意工具，提取本地系统中的凭证。该系统运行 Windows 操作系统，且会在一定时间内存储用户凭证。几小时前，一名 IT 管理员曾登录该员工的笔记本电脑解决打印机问题，凭证便被存储在员工的本地设备中。威胁行为者利用 mimikatz 和本地管理员权限提取了这些凭证，从而轻松获得了域管理员账户的凭证。作为 Active Directory 中权限最高的账户，域管理员的凭证使得威胁行为者能够控制几乎所有基础设施组件，进而通过攻破单一系统完全入侵了整个公司基础设施。由于缺乏安全的资源和用户管理，以及未遵循最小权限原则来管理特权用户，导致整个公司和基础设施被威胁行为者攻破。

场景#2：过时且不安全的用户账户

某公司拥有一套内部基础设施，并通过中央客户数据管理系统进行管理。然而，公司未在技术层面严格执行密码策略。某员工在咖啡馆远程工作时，暂时离开去洗手间，将上锁的笔记本电脑留在桌上。威胁行为者趁机靠近笔记本，尝试了几个常见密码，成功获得访问权限。他们发现了指向公司客户数据管理系统的链接，通过随身携带的数据线将所有数据传输到手机中。随后，威胁行为者又发现了公司网络中一个包含敏感配置数据的管理员共享目录，并成功窃取。由于公司未能实施有效的资源管理和密码策略，威胁行为者不仅获取了员工日常访问的数据，还顺利窃取了敏感的管理数据。这一事件突显了公司在安全管理上的重大漏洞。

ISR05:2024_不安全的加密使用

描述

加密在网络安全防护中至关重要，尤其在外部应用和系统中已经得到了广泛的关注，但在内部网络和基础设施中的重要性往往被忽视。企业和用户必须意识到，如果在内部网络所使用的系统和协议中未能实施足够的加密措施，威胁行为者可能会通过相邻的方式读取、篡改或注入数据，从而影响通信和系统的安全。加密的缺失可能导致敏感数据泄露和特权账户的泄密。值得注意的是，单纯依赖外部防线并不足以完全保护内部系统。一旦攻击者通过钓鱼等手段突破外部防线并获得内部网络的访问权限，外部防护便失去了作用。因此，企业必须确保内部基础设施的安全性与外部系统同等严密，甚至更加完善。

风险

如果使用了不安全的加密方法或配置，信息泄露和特权账户被泄露的风险会大大增加。这显著提高了发生毁灭性网络攻击及其影响的可能性。例如，如果管理员使用常见的远程访问协议（如远程桌面协议 RDP）连接到内部服务器，而没有启用加密或使用的是不安全的加密方式，则相邻的本地威胁行为者可以从网络中读取这些凭证，并轻松攻破特权账户。同样的风险也适用于通过内部网络传输的敏感信息。公司的内部基础设施通常使用多种协议、工具和系统来传输数据或访问各类组件。每个组件都必须配置使用足够且安全的加密和加密方法，以保护数据和账户的安全。

改进措施

建议确保所有协议、通信工具、远程访问工具、数据传输工具等都配置为使用安全的加密方法和配置。此外，应该将不支持安全加密的协议迁移至安全的替代方案，例如将 TELNET 替换为 SSH，将 FTP 替换为 SFTP。确保所使用的加密方法和配置足够强大，并遵循最佳实践及官方建议。加密功能不应由公司自行开发或实现，而应使用公开的、知名的加密库。记住，“不要自制加密算法！”

示例攻击场景

场景#1：未加密的远程访问工具

某公司拥有一套常见的内部 IT 基础设施，其中包括多个内部服务器，用于向员工提供各种应用程序服务。公司的一款重要应用是客户关系管理（CRM）系统，其中存储了大量关于客户的敏感数据。威胁行为者通过一个公司因配置错误而暴露在互联网上的未知系统，成功渗透进入公司内部网络。威胁行为者通过监听该系统与内部网络的所有通信流量，获取敏感信息。期间，一名管理员使用 TELNET 远程连接内部文件服务器执行更新操作。由于 TELNET 不具备加密功能，管理员的凭证以明文形式在内部网络上传输。威胁行为者捕获了这一数据包，成功窃取了管理员的登录凭证，并利用这些凭证登录到 CRM 服务器，窃取了所有客户数据，最终将这些信息出售给了竞争公司。

场景#2：加密使用不足

某公司拥有一套内部 IT 基础设施，部署了多个内部应用程序。其中一款应用程序用于为公司客户生成发票。威胁行为者成功渗透到公司的内部网络，并能够监听并注入数据包到内部网络流量中。一名员工连接到发票系统，创建多张客户发票。尽管员工的笔记本与发票服务器之间的通信协议进行了加密，但该加密协议未进行身份验证或完整性校验。威胁行为者利用这一漏洞发起了中间人攻击（MitM），注入并篡改了数据包。攻击者修改了员工发送到发票服务器的数据，将款项从公司账户转移至攻击者控制的账户。当客户按照发票支付款项时，钱款流入了攻击者的账户，而非公司账户。

ISR06:2024_不安全的网络访问管理

描述

网络访问管理是内部基础设施架构和访问控制规定的一个基本方面。

有效的网络访问管理能够防止多种攻击，并减少网络攻击的影响以及威胁行为者在内部基础设施中的横向移动。更为严重和关键的风险是缺乏网络隔离，这将限制内部基础设施各部分之间的访问。通常，企业在攻击者成功获取物理网络端口或附近的 Wi-Fi 访问后，未能阻止威胁行为者访问内部网络。此外，通信路径的流量应该根据应用层的上下文进行监督和调控，以确保只有被允许的通信路径能够通过。

风险

缺乏网络隔离将大幅增加网络攻击在内部基础设施中蔓延的风险，因此增加整个基础设施被妥协的风险，尽管可能只有一个组件受到影响。

如果没有网络访问控制机制，攻击者可以在威胁行为者成功获取物理访问网络组件、诱使员工插入恶意设备或接入附近的 Wi-Fi 时，访问内部网络。

缺乏网络隔离将大幅增加网络攻击在内部基础设施中蔓延的风险，从而增加整个基础设施被攻破的风险，即使只有一个组件被入侵。如果没有网络访问控制措施，攻击者只要能够物理访问网络组件、诱使员工插入恶意设备或接入附近的 Wi-Fi，就能获得对内部网络的访问权限。对基础设施组件的访问控制不充分，或者更准确地说，未能在应用层附近实施网络控制，可能会使威胁行为者滥用常见的通信路径。

整改措施

建议将网络访问控制（NAC）机制作为网络访问管理的一部分进行实施。例如，基于证书的 NAC 技术将确保只有经过批准的设备能够访问公司的网络。理想情况下，网络隔离应在基础设施的架构阶段考虑。与“必

要知情"原则类似，网络隔离应尽可能小，并限制这些网络块之间的通信路径数量。虚拟局域网（VLAN）等技术可以帮助实现高效的网络隔离。访问矩阵可以帮助规划网络访问管理结构。接下来建议的步骤是监管和控制"隔离"网络块之间的通信路径。这些桥接或网络过渡应动态调节。根据应用层的上下文，应该允许或拒绝对这些子网络或组件的访问。例如，允许员工远程办公的网络访问，应使用虚拟私人网络（VPN）等安全技术进行。

示例攻击场景

场景#1：网络隔离不足

一家公司拥有一套内部网络基础设施，托管着为其客户提供的不同应用程序。这些应用程序可以通过在线访问，允许客户远程使用服务。公司有多个数据库服务器，用于存储命名应用服务器的数据，以及用于内部应用程序和数据的服务器。一个威胁行为者在其中一台公开可访问的应用服务器中发现了技术漏洞，并完全控制了该服务器。由于缺乏网络隔离，攻击者能够轻松横向移动，攻破所有数据库服务器以及内部应用和数据服务器。该威胁行为者通过仅从一个初始访问点入侵，进一步控制了内部基础设施。后来，窃取的数据被出售给其他网络犯罪分子。

场景#2：弃用的旧服务器

一家公司使用常见的内部基础设施，包括应用服务器和员工文件共享。公司订购了新的网络打印机来替换旧的打印机。一个威胁行为者在新打印机到达公司之前，将恶意硬件注入到这些打印机中。当新网络打印机插入内部网络时，这些恶意硬件（由一台小型计算机组成）也利用网络端口访问内部网络，并且由于没有实施网络访问控制（NAC），因此没有被阻止。然后，它通过互联网连接到一个由威胁行为者控制的远程主机，建立反向连接，并创建一个入侵点进入内部网络，从而可以进行进一步的攻击。

ISR07:2024_不安全的身份验证方法和默认凭据

描述

密码仍然是网络安全的基本组成部分，许多身份与访问管理（IAM）系统依赖于用户名和密码认证。不安全的身份验证方法是网络安全中的常见漏洞，指的是由于密码过于简单、可预测或缺乏复杂性（长度）而容易被猜测或破解的情况。由制造商或供应商在硬件设备或软件应用程序上预配置的默认凭证，往往没有被用户或管理员更改，从而产生了安全漏洞。

风险

凭据是确保只有经过认证和授权的用户才能访问内部资源的关键。弱密码可以通过各种技术轻易被利用，例如暴力破解和字典攻击。然而，默认凭据通常可以在所使用产品的文档中轻易找到。攻击者可以利用未更改的默认设置或被盗的密码来攻击设备或应用程序。这可能导致未经授权的访问、数据泄露以及关键系统的被攻破。

整改措施

组织应强制执行密码复杂度要求以降低风险，实施多因素身份验证（MFA），并教育员工了解使用强密码的重要性。同时，密码管理工具也可以帮助增强安全性。

示例攻击场景

场景#1：打印机

许多网络打印机在出厂时预设了广为人知的默认用户名和密码。攻击者可以利用这一点，访问打印机并查看包含敏感信息的打印任务。为防止这种情况，组织在安装打印机时必须更改默认的凭证，并限制只有授权人员才能访问。

场景#2：用户账户

弱密码或易于猜测的密码是攻击者的主要目标。在攻击场景中，恶意员工可以通过利用弱用户密码，获得对敏感信息或系统的未经授权访问。为应对这一威胁，组织应强制执行密码策略，在多次登录失败后实施账户锁定，并在用户中推广密码最佳实践。

ISR08:2024_信息泄露

描述

信息泄露是指机密或敏感数据在组织内部或外部被无意或恶意地暴露，通常由于安全措施不足或员工疏忽导致。这种泄露可以以多种形式表现出来，例如文件处理不当、网络共享权限配置错误或通信渠道不安全。此外，信息泄露还可能源于内部威胁，其中不满的员工或恶意内部人员故意窃取数据以谋取个人利益或进行破坏。这一威胁需要采取全面的应对措施，包括强有力的访问控制、数据加密、定期审计以及员工安全意识文化的培养。

信息泄露是指机密或敏感数据无意或恶意地暴露，无论是在组织内部还是外部，通常是由于安全措施不足或人员疏忽造成的。这种泄露可能以多种形式出现，例如文件处理不当、网络共享的权限配置错误，或通信渠道不安全。此外，信息泄露还可能源于内部威胁， disgruntled 员工或恶意内部人员故意窃取数据以谋取个人利益或进行破坏。这一威胁需要采取全面的方法，包括强有力的访问控制、数据加密、定期审计和员工安全意识文化的培养。

风险

信息泄露的风险在很大程度上取决于泄露的信息种类。内部 IP 地址的泄露可能暴露出网络中的新目标，但个人身份信息或其他受保护数据的泄露可能导致欺诈、身份盗窃或市场上的竞争劣势。此外，信息泄露还可能使组织面临来自恶意行为者的勒索威胁。累积风险突显了实施严格网络安全措施、持续监控以及培养一支知识丰富的员工队伍的必要性，以降低信息泄露及其潜在后果的风险。

整改措施

应对信息泄露的对策需要技术解决方案、政策和培训的结合。采用加密技术可以确保在数据被截获或未经授权访问时，数据保持不可读。此外，实施严格的访问控制措施确保只有授权人员才能访问敏感信息。定期进行安全审计和网络监控对于识别和修复系统中潜在的漏洞至关重要。在人力方面，开展全面的安全培训和意识提升项目，能帮助员工具备识别和防止潜在数据泄露场景的必要知识。此外，培养问责文化和快速的事件报告机制可以显著减少信息泄露发生后的损害。制定明确的数据处理政策并确保遵守监管合规性，进一步加强组织防范信息泄露的能力，使其成为难以突破的堡垒。

示例攻击场景

场景#1：所有员工均可访问客户数据

在一家企业中，由于系统配置错误，所有员工突然获得对包含敏感客户信息的数据库的无限制访问权限。由于不了解数据访问协议，一名好奇的员工在使用公共网络工作时浏览了该数据库，并无意中将一些客户数据外泄。同时，一名恶意内部人员利用这一机会，提取并将数据出售至暗网。情况迅速恶化，当客户报告欺诈活动并追溯到数据泄露时，事件已经给该公司在财务、法律和声誉上造成重大损害，突显了实施强有力访问控制措施以防止信息泄露的重要性。

ISR09:2024_不安全的资源访问和管理组件

描述

缺乏适当的访问控制和权限管理使得未经授权的个人或程序能够访问敏感数据、系统或物理位置。这种漏洞表现为访问政策配置错误、过于宽松的设置或不当的认证机制。

风险

该风险是多方面的，可能对公司安全性和运营完整性产生深远的影响：

- 它使得关键数据、敏感信息和专有资源暴露给未经授权的访问，从而导致数据泄露、知识产权盗窃和机密信息的泄露。
- 未经授权的系统和配置操作可能导致恶意员工（或通过已被攻破客户端的外部攻击者）扰乱关键服务、操控网络流量或注入恶意代码，进而导致系统宕机和业务中断。
- 管理组件被攻破可能为攻击者在组织的基础设施中提供立足点，使其能够转移攻击方向并扩大访问范围。

除了直接的安全影响外，这些漏洞还可能损害组织声誉、导致监管合规性违规，并因应急响应、修复和潜在法律后果的成本而造成财务损失。因此，解决不安全的资源访问和管理组件的风险对于确保组织 IT 基础设施的整体韧性和安全性至关重要。

整改措施

在整个基础设施中实施强有力的访问控制机制，遵循最小权限原则，仅授予用户和系统完成任务所需的最低权限。定期审查、审计并更新访问权限，确保基于"知情必要"原则授予访问权限。该原则规定每位员工仅应获得完成工作所必需的权限，而不是获取超出这一任务所需的额外信息。采用强认证和授权协议，包括多

因素认证，以防止未经授权的访问。员工的安全意识培训对于减少无意中的访问配置错误至关重要。保持所有管理组件（包括硬件和软件）及时更新安全补丁和配置，以维持对攻击的强大防御能力，防止被恶意利用。

示例攻击场景

场景 #1：文件共享访问

攻击者可能会利用文件共享上的不安全访问控制，未经授权访问敏感文档。导致此类攻击的常见原因是未按照"知情必要"原则管理访问权限。为应对这一威胁，组织应细致地配置文件共享的访问权限，实施严格的权限管理，并更新服务器管理组件，确保强访问控制和认证措施到位。

场景 #2：网络设备管理

网络设备管理组件（如路由器、交换机和防火墙）存在不安全访问的重大威胁。例如，内部攻击者如果访问到路由器管理界面，可能会修改路由表、拦截网络流量，甚至发起拒绝服务攻击。为应对这一风险，组织应通过强认证和访问控制措施来保护网络设备管理接口，确保设备固件及时更新，并通过网络隔离技术将管理流量与公共网络隔离开。定期监控和记录网络设备活动，对于快速检测和响应任何可疑的访问或配置变更至关重要。

ISR10:2024_资产管理和文档记录不足

描述

资产管理不足是指组织在准确识别、跟踪和记录所有硬件和软件资产，以及相关配置、依赖关系和生命周期方面的不足。它包括缺乏有序和最新的 IT 资产清单，而这一清单对有效的安全性、合规性和运营效率至关重要。有效的资产管理可以帮助组织快速且准确地映射受影响的资源，并为事件响应提供支持。

风险

准确的资产清单和相关文档对整体安全至关重要。缺乏文档记录会增加网络中未经授权或未管理的设备和软件的可能性，使得有效地执行安全政策和监控漏洞变得更加困难。其次，它削弱了事件响应能力，因为组织可能难以识别安全事件或漏洞的范围和影响。遵守行业法规和内部政策也变得更加具有挑战性，从而可能将组织面临法律和财务责任。最后，这导致资源配置效率低下，往往导致对冗余资产的过度支出或对关键 IT 基础设施的投资不足。资产管理和文档记录不足会显著威胁到组织的安全性、合规性、成本效益和运营韧性。

整改措施

为降低风险，组织应实施一个全面的资产管理计划。该计划应包括以下关键组成部分：

1. 资产清单：建立并维护完整的硬件和软件资产清单，包括服务器、工作站、移动设备、应用程序和网络设备。持续更新该清单，以反映环境中的变化。

2. 资产分类：根据资产的关键性和功能进行分类。这种分类有助于优先采取安全措施和资源配置。

3. 生命周期管理：实施系统化的资产生命周期管理方法，包括采购、部署、维护和处置。确保淘汰或换代的资产被安全地换代或更新，以避免其成为安全风险。

4. 定期审计：定期进行审计和资产清单的对账，以识别差异并确保准确性。这还包括定期的漏洞扫描周期，以检测受影响的资产并缓解安全风险。

5. 流程、责任和实施文档：提供准确的文档清单，描述所有 IT 和业务流程、相应的责任以及技术细节。

通过建立健全的资产管理程序，组织可以增强其安全防护能力，改善合规性，优化资源配置，并简化运营，从而最终降低整体风险。

示例攻击场景

场景 #1：未检测到的漏洞

随着时间的推移，组织积累了庞大而复杂的 IT 基础设施，包括服务器、网络设备和大量的软件应用程序。由于缺乏系统化的漏洞扫描和资产管理，IT 团队未能意识到其环境中日益累积的安全漏洞。这一疏忽使公司面临潜在的网络威胁，因为攻击者可以利用这些未被检测到的漏洞进行未授权访问、破坏运营或窃取敏感数据。随着组织的发展，这些未检测漏洞的风险也在增长，凸显了实施全面漏洞管理程序的紧迫性，以主动识别、优先处理并修复这些漏洞。

场景 #2：应急响应

应急响应团队遇到了一次严重的安全漏洞。攻击者成功利用公司平台中一个未披露的软件漏洞，导致了重大服务中断。调查发现，攻击者入侵了平台的 Web 服务器，创建了进入内部网络的入口点。为了防止对公司价值造成进一步损害，应急响应团队专注于通过资产管理系统轻松识别的关键资产。凭借准确且最新的文档记录，所有关键系统的漏洞得以快速识别并进行防御，从而避免了重大数据泄露和系统损坏重建。