CLAROTY

TEAM82

Cyberworld

2025 年 CPS 安全状况：楼宇管理系统(BMS)暴露风险

对一些重要行业中楼宇管理与自动化系统所面临的高风险暴露进行分析研究

目录

引言

在以IT为中心的企业里，专门负责制定和执行网络安全策略、管理潜在风险的高级管理人员，被赋予网络化物理系统（Cyber Physical systems, CPS）安全治理职责。因为，众多企业发现网络中有大量物联网（IoT）和运营技术（OT）设备，常见的网络风险源于楼宇管理系统（BMS）和楼宇自动化系统（BAS）。

出于经营战略与经济效益的考虑，BMS和BAS逐渐联网。地产、零售、酒店、数据中心等领域都依赖暖通空调（HVAC）、照明、能源、电梯、安防等系统。以前，这些系统由设施管理部门独立操作。如今，使用先进的BMS和BAS功能进行连接与集成。

BMS 和 BAS 可以连接到设施内的其他智能传感器与设备。这些系统会收集数据，帮助企业分析能耗趋势，同时确保达到环保和可持续发展的监管标准。尤其是有多个站点的企业，使用这些系统不仅能提高效率，还能优化流程，从而降低运营成本，提升整体利润。

术语

Building Management System (BMS)
楼宇管理系统

BMS 是一个集中式平台，可以对多个楼宇自动化子系统进行控制、监察、分析和配置。

请您注意：为了让报告内容保持一致，提及的BMS涵盖本页术语描述的所有相关组件。

Building Automation System (BAS)
楼宇自动化系统

BAS是一种网络系统，通过统一的控制方式，连接、自动化管理、控制楼宇内的各种系统，例如：暖通空调（HVAC）、照明、安防系统。

Building Automation Controller
楼宇自动化控制器

楼宇自动化控制器是一种可编程的控制单元，用于管理楼宇内一个或多个子系统的运行，例如：暖通空调（HVAC）、照明、门禁控制。它会根据传感器的输入信息和用户设置的参数，执行逻辑控制程序，并向现场设备发送指令来实现自动化管理。

Building Automation Device
楼宇自动化设备

楼宇自动化设备是指楼宇自动化系统中执行特定功能的任何物理或逻辑组件，例如：传感、执行、控制、通信。

Building Management Sensor
楼宇管理传感器

楼宇管理传感器是一种现场设备，用于监测和报告对楼宇运营至关重要的环境或系统数据。例如：温度、湿度、占用率、光照水平、空气质量、能耗。这些传感器为自动化控制器或管理系统提供实时数据。

虽然把 OT 和 IoT 设备连接到互联网能带来很多好处，但没有做好安全管理，也会带来网络安全风险。有些用户或供应商在使用这些技术时，可能不了解背后的网络安全问题和必要的防护措施，结果这些设备变成了可以在整个互联网中被发现的资产。这种暴露为潜在攻击打开了大门，可能对企业造成严重影响。常见的安全风险包括：未修补的已知漏洞、默认密码、单因素身份验证、不安全的互联网连接。

这些安全风险可能把楼宇自动化系统中的重要资产暴露给攻击者，让他们有机会植入勒索软件或破坏业务系统。一旦攻击者成功进入网络，他们可能干扰正常运作、破坏物理设备，从而对楼宇内的人员造成潜在伤害。举个例子：如果数据中心的冷却系统或零售仓储的冷藏系统，因网络攻击突然离线，就会带来严重的后果。

虽然连接对于推动业务发展至关重要，但也扩大了攻击者可利用的攻击面。安全团队必须具备风险意识，及时采取措施来防止这些潜在的漏洞被利用。

本报告深入分析各个行业资产密集型企业中 BMS 和 BAS 面临的暴露风险。智能楼宇、零售仓储、数据中心、酒店等领域都高度依赖 BMS 和 BAS 来维持可持续的运营。

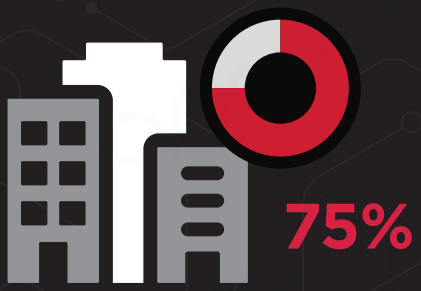
通过分析，找出了企业在已知被利用漏洞（KEV）方面最容易暴露的地方，包括：已知被用于勒索软件和敲诈攻击的KEV、不安全的互联网连接。这些特定的暴露情况构成了高风险的BMS和BAS，这些系统可以被攻击者远程访问，并且包含已在真实环境中被攻击者频繁利用的漏洞。换句话说，这些暴露问题对企业构成真实且迫在眉睫的威胁，应被列为最高优先级进行修复处理。

本报告的分析数据是从那些使用CPS技术的企业中收集，这些企业使用了BMS来管理楼宇的各种系统。

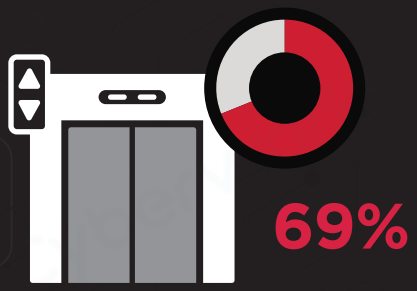
467,000+
BMS

529 家企业

主要发现



75% 的企业有
受到 KEV 影响的 BMS 设备



69% 的企业有 BMS 设备
存在与勒索软件攻击相关的 KEV

51% 的企业有既受到 KEV 影响
又不安全联网的 BMS 设备

楼宇管理系统(BMS)面临的威胁

与大多数OT系统一样，许多BMS在设计之初并未考虑接入互联网，更不用说网络安全支持了。它们通过 BACnet 和 Modbus 等传统协议进行通信，而这些协议本身就不具备加密机制。

2019 年，BACnet 协议新增了一个附加规范，称为 BACnet SecureConnect，它为通信与身份验证提供了传输层安全性（Transport Layer Security，TLS）。此技术确保传输中的数据被加密，可防止数据被篡改，避免对BMS造成干扰或损害。然而，使用BACnet协议进行通信的BMS设备并不强制要求采用SecureConnect。许多企业仍继续使用旧协议，导致系统持续面临暴露风险。

类似的情况也出现在KNX通信协议上。KNX是一种开放协议，可与不同供应商的BMS技术互通，在欧洲BMS中得到广泛应用。虽然该协议的核心部分支持加密和其他安全机制，但这些功能仅通过附加组件 KNX Data Secure 和 KNX IP Secure 提供。因此，必须正确配置这些安全扩展，才能有效防止数据篡改及其他可能影响系统运行的干扰行为。

BMS中的传统技术问题类似于其他OT领域所面临的挑战。除了使用不安全的通信协议，攻击者还可能发现BMS中使用已知的默认或硬编码凭证，从而使未经授权的第三方更容易访问系统。

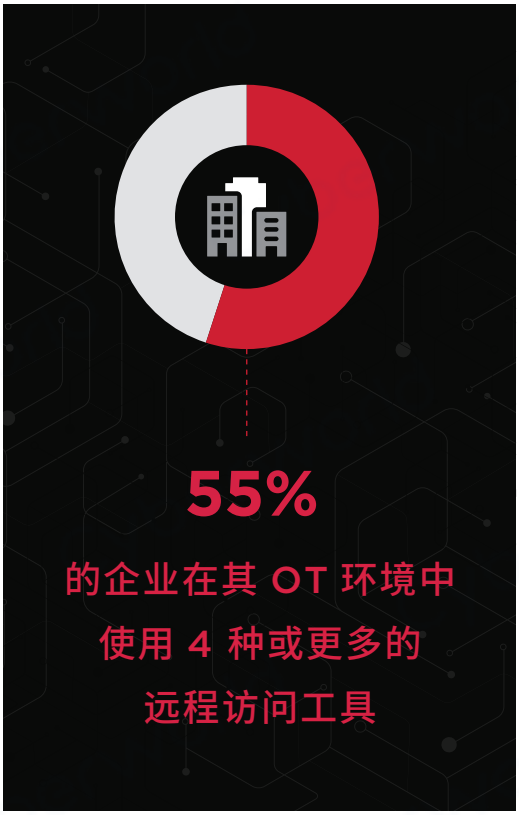
一些BMS设备已经投入使用很长时间，早已不受原供应商支持。这些设备的固件或软件中的一些漏洞未得到修复，原供应商已停止为老旧BMS设备提供安全更新或功能支持。

BMS的其他风险包括：缺乏身份验证和访问控制。攻击者可利用 Shodan 或类似的扫描服务，扫描出连接至互联网的 BMS 设备，然后用“暴力破解”或“字典攻击”（brute-force dictionary attacks）的方式，尝试访问这些设备，并试图横向移动到企业网络中。

第三方访问是BMS的另一大风险，需要妥善管理。许多供应商在合作时使用自己的远程访问技术，但这些技术往往不是企业级别的，可能不支持多因素身份验证等安全功能。

Team82 的最新报告指出：远程访问工具的泛滥加剧了问题。55% 的企业在其 OT 环境中使用 4 种或更多的远程访问工具，有些企业多达 16 种工具。

不安全的连接问题，不仅因缺乏安全的远程访问工具，还因通过开放端口和未使用的服务连接BMS而加剧。这些“敞开的门”，往往是简单的配置错误，很容易被攻击者发现并利用，需要通过彻底检查防火墙规则、记录活动、改善网络分段来解决这些问题。



现实中的 BMS 攻击事件

以下为公开报道的重大网络攻击事件，攻击者利用了暴露的 BMS：

欧洲公司的 BMS 被摧毁：2021 年，两家未具名的欧洲工程公司报告称，其 BAS 被攻击者破坏。攻击者利用了 KNX 协议的弱点，成功瘫痪整个系统。KNX 协议广泛用于照明与 HVAC 系统之间的通信。

MGM Resorts（美高梅国际酒店集团）：2023 年，MGM Resorts 遭遇重大网络攻击。攻击者入侵了内部系统，导致旗下 30 多家赌场和酒店业务全面瘫痪。

Omni 酒店：2024 年，Omni 酒店遭受了一次复杂的网络攻击，导致酒店宾客服务严重中断，只能人工办理入住手续、房卡失效、Wi-Fi 无法使用等，攻击者声称窃取了约 350 万名宾客的资料，攻击造成的影响持续了一周以上。

最严重的 BMS 暴露风险是什么？

本报告分析的资产范围包括：楼宇管理系统（BMS）、楼宇自动化设备（包括传感器和执行器）、楼宇自动化控制器。

467,000+
系统和设备

529
家企业

Team82 研究发现，很多企业面临的 BMS 暴露风险：一是系统中存在 KEV，这些漏洞常被黑客用来发动勒索软件攻击；二是 BMS 连接到互联网时缺乏安全保护，容易被攻击。

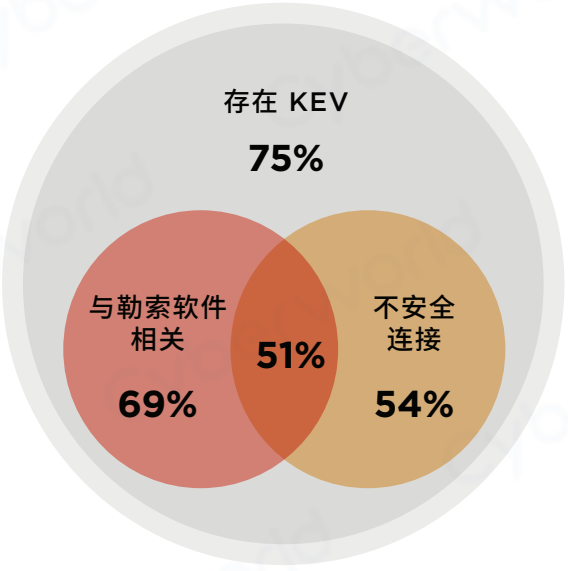
鉴于BMS在商业楼宇、零售仓储设施、其他重要行业设施的正常运营中扮演核心角色，保护这些系统需要赋予更高的优先级。尤其是在这些系统因远程管理、数据分析等业务和运营需求而接入互联网时，强化安全措施变得更加重要。

如前文所述，BMS 中普遍存在老旧系统，尤其是 Windows 系统，Windows是BMS工作站、SCADA监控系统和人机界面（HMI）中最常用的操作系统，每个月都会出现新的漏洞，企业需要对其进行评估、测试并优先修复。

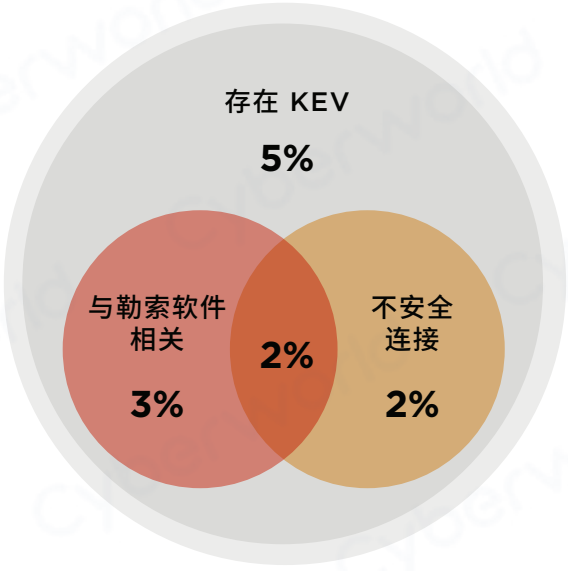
使用未受管理的Windows系统会造成严重的网络安全风险，比如使用 Windows XP 、7 、8 、10 和 Server 2003，这些版本已不再获得微软的安全补丁支持，任何未修复的KEV都将成为永久性漏洞，必须通过补偿性控制措施来缓解，或在发生事件时把 BMS 与企业网络隔离。

以下调研数据表明，75% 的企业使用的 BMS 设备存在 KEV，特别是与勒索软件攻击相关的漏洞，这些漏洞已被攻击者利用过，需要紧急修复。同时，如果BMS的连接方式不安全，风险将进一步加剧，因为攻击者会通过这些漏洞作为突破口进入网络。

企业和设备中的 BMS 暴露情况



企业



设备

BMS 暴露对资产密集型企业的影响

这些暴露数据对资产密集型企业具有深远影响，因为资产密集型企业依赖BMS，BMS不仅关乎效率，还与运营连续性、基本服务、人员安全密切相关。数据中心、零售业、酒店业、智能楼宇（包括写字楼、住宅设施）尤其脆弱，因为它们依赖BMS来调节环境、保护关键基础设施、为顾客和使用者提供流畅体验。

随着 BMS 与 IT 网络和运营技术日益互联，一旦 BMS 遭到攻击，就会在物理和数字层面引发一连串的风险。

在数据中心，BMS控制着关键基础设施，例如：HVAC、配电单元（PDU）、消防系统、备用发电机。一旦遭到针对性攻击，可能会造成环境异常，例如过热或湿度失衡，会威胁到服务器的正常运行、硬件的完整性、与客户签订的SLA。此外，攻击者可能故意触发故障切换、禁用冷却系统、制造虚假警报，导致不必要的停机或支付高昂的调查费用。而且，系统的持续运行对数据中心非常重要，即便是短暂的中断，也可能对整个数字生态系统造成连锁式服务瘫痪。

零售业和酒店业都依赖BMS来控温、照明、节能。在零售业，安全漏洞会导致一系列严重后果，例如：HVAC故障，会干扰销售点（point-of-sale，POS）的正常运行；篡改冷藏控制，会影响食品安全；门禁或紧急系统失灵，会危及顾客人身安全。在酒店业，攻击者会破坏宾客体验，例如：智能客房系统故障、锁住大量房门、制造虚假警报。这些问题会同时影响数十甚至上百家门店，对品牌信誉造成严重打击。

在物流仓储环境，BMS负责控温、通风、进出控制、传送设备的正常运作。

如果攻击者入侵系统，可能会：锁住卸货码头，阻碍货物进出；停止通风，影响需要控温的货物；错误启动消防系统，造成不必要的混乱。

由此造成的干扰可能延误履行周期、导致库存损坏、降低供应链的可靠性。特别在物流高峰季，当系统运行时间和环境控制对产出至关重要时，这种影响尤为显著。

房地产投资信托（Real Estate Investment Trust, REIT）与智能楼宇运营商日益依赖BMS平台，监控和优化多租户写字楼、住宅小区、混合用途物业。

如果系统遭到破坏，攻击者可能操纵整栋楼宇的系统：HVAC、电梯、照明、门禁，进而引发使用者不满、法律责任风险或监管审查。若多个物业遭遇协调性破坏，特别在停机时间较长、恰逢极端天气及大量人员使用时，会造成大规模的运营和声誉风险。

建议

对于那些依赖 BMS 的企业来说，在应对安全风险时，不能只使用传统的漏洞管理方法。常见的安全框架，比如根据 CVSS（通用漏洞评分系统）评分的优先级排序，有时会忽略一些实际中更严重的漏洞。另外，这些情况也会带来高风险：使用 EoL 的软件和固件、操作设备直接连接互联网、访问权限控制不严。

这种传统方法也忽略了业务影响和运营关键性，如果企业缺乏这些相关信息，就有可能错误分配人力资源和修复工作。

BMS与其他CPS一样，需要一种动态的风险降低方法，而这种方法应基于持续威胁暴露管理（Continuous Threat Exposure Management, CTEM）计划。Gartner 将 CTEM 计划定义为："它是一套流程和功能，让企业能够持续、一致地评估其数字和物理资产的可访问性、暴露程度、漏洞的可利用性。"[1]

如今，楼宇逐步智能化，楼宇管理和自动化系统会更常联网。然而，许多此类系统不具备网络安全功能，直接连接到企业内部网络或公共互联网，会给企业带来新的风险。

建议采取以下五步行动，这是一个优于传统漏洞管理的战略框架，为网络安全决策者和资产所有者提供真实的安全态势评估，并为风险管理团队制定可执行的修复方案，也易于企业高层理解和采纳。

1. **界定范围（Scoping）：**根据设备类型和所属部门，梳理所有重要的业务流程
2. **发现（Discovery）：**识别所有设备、详细属性、通信方式
3. **优先级排序（Prioritization）：**遵循网络安全框架，考虑漏洞的可利用性、暴露对业务的影响
4. **验证（Validation）：**验证各种漏洞是否真实存在，是否可以被外部访问
5. **动员（Mobilization）：**通过可执行的缓解和修复措施，降低风险，保障运营安全

这项行动是一种有针对性的方法，适用于依赖 BMS 的企业，用来制定暴露风险管理计划。
这种方法有助于实现三个核心目标，可降低风险并减轻对业务的影响：

1. **识别CPS风险：**全面了解所有资产及其暴露情况，涵盖IoT、OT、BMS。这个基础步骤有助于发现潜在风险和盲点，否则这些问题可能长期未被察觉。
2. **以业务为中心的风险评估：**依据业务流程的关键性及其对业务连续性的潜在影响，评估暴露风险，而不只是看它们在技术层面有多严重。
3. **优先级排序与可执行的修复措施：**为安全和运营团队提供经过验证、具有背景依据的分析结果，在不中断业务的情况下，大规模、切实可行地降低风险。

以下是若干重要事项，用于指导您的暴露风险管理计划，并确保其与上述目标保持一致。

1. 识别重要流程

暴露风险管理一开始要找出那些对业务非常关键的BMS，像是保障楼宇安全、舒适、运作高效、业务不中断的系统。

第一步是绘制重要的工作流程，看哪些 BMS 支持这些流程。

接着，要根据业务影响大小来给这些流程排优先顺序，比如考虑是否会造成经济损失、停工、声誉下降、违反规定或安全问题。

为了系统性地进行评估，应开展业务影响评估（Business Impact Assessment，BIA），根据中断的严重程度将流程分类（例如，高、中、低）。与重要服务或合规性相关的流程应优先受到保护。

把暴露风险管理和业务影响联系起来，企业能够确保最重要的运营和其背后的资产获得所需的关注与资源配置。

现实案例：某个零售配送中心依赖BMS来控制两个仓储区域，一个是冷藏仓库，另一个是常温储存区。虽然两者都使用环境监测系统，但冷藏仓库的温度控制非常重要，一旦故障，可能导致产品变质并造成严重的经济损失。相比之下，常温储存区的中断可能带来的风险较小。

这个案例说明了为什么在暴露风险优先级排序时，应以业务影响为导向，而不仅仅看BMS的技术属性。将资产与业务结果相挂钩，有助于企业把保护资源集中在最重要的地方。

2. 主动发现资产和暴露风险

在通过BIA绘制重要流程后，下一步是全面了解支持这些流程的楼宇系统。像温度控制、照明、物理安全等系统，虽然与IT基础设施协同运作，但安全团队往往难以全面了解它们的运行状况。如果没有完整且内容丰富的资产清单，就很难有效评估风险或优先处理最严重的暴露问题。

传统上，被动网络监察（Passive Network Monitoring）一直是发现CPS资产的默认方法。但用于发现BMS时，这种方法扩展性不佳，它需要昂贵的专用硬件、漫长的部署时间、耗时的学习周期，这会延迟获得洞察。对于拥有数十甚至数百栋分布式楼宇的企业来说，这种方法不仅成本高昂，还难以快速带来价值。

一个更实际的替代方案是采用无需硬件的主动发现（Active Discovery）技术。这种方法可在楼宇管理环境中提供快速、可扩展的可视化，不需要流量学习（traffic learning），也不需资源密集的设备部署。它可以让安全团队在几分钟内深入掌握资产状况以及相关的业务背景。

一旦建立了完整且集中的资产清单，接下来的重要步骤就是发现那些传统漏洞管理经常忽略的暴露风险。主动发现技术，比如安全查询（Safe Queries），提供了一种独特、无干扰的方法，可获取有价值的暴露风险数据，例如：

- **验证漏洞的可利用性：**某个资产可能存在CVE，CVSS评为“严重（Critical）”，但漏洞管理团队仍需确认该资产是否真的会被利用。主动发现技术可以验证资产的补丁情况，协助安全团队判断其是否仍然存在风险。
- **EoL资产指标：**BMS通常包含不再接收安全补丁的EoL资产。主动发现技术可以识别EoL资产，使团队能够确认是否需要采取替代控制措施，以防止这些无法修补的系统引发意外停机。

- **开放端口：**主动发现技术可以验证源设备与目标设备之间的开放网络路径，从而提供对潜在访问点的可视化。这有助于识别异常或恶意连接，否则它们可能不会被察觉。
- **主机设备上安装的应用程序：**在运行Windows操作系统的设备上，主动发现技术可以揭示已安装的应用程序，提供更深入的软件清单可视化，从而识别可能引发的风险或合规问题。

3. 暴露风险的优先级排序

在建立了全面的楼宇管理资产清单并识别相关风险后，下一步就是进行优先级排序。

与其仅依据技术严重程度评分，安全团队更应根据风险对业务的影响进行评估。这意味着要利用之前开展的BIA，了解哪些流程一旦受损，会带来严重后果，比如财务损失、运营停机、安全事件或合规问题。以这种视角对暴露风险进行优先级排序，可以确保修复工作集中在能够最大程度降低风险和提升业务价值的地方。

为强化这种基于风险的管理方法，外部威胁情报可以提供有价值的相关信息。

美国网络安全和基础设施安全局（CISA）的KEV目录列出了目前在现实中被频繁利用的漏洞，提示哪些问题构成直接且真实的威胁。与此同时，漏洞利用预测评分系统（Exploit Prediction Scoring System，EPSS）则评估某个漏洞在近期被利用的可能性，为暴露风险的优先级排序提供预测维度。将内部流程的重要程度与外部威胁数据结合，企业可以构建一个既贴近实际运营又能响应不断演变的威胁形势的优先级排序框架。

4. 验证攻击路径

许多安全团队仍采用“清单式(Checklist)”的漏洞排查方法，但攻击者的思维方式不同，他们关注的是攻击路径，绘制出网络中潜在的通道，以达到高价值目标。了解并模拟这些攻击路径，可以帮助安全团队主动发现并封锁横向移动通道。

若要有效验证潜在的攻击路径，必须了解网络中各楼宇管理资产之间的通信方式，尤其要识别它们不应该通信的地方。一种有效的方法是利用网络保护工具，这些工具用于控制、监察和分段通信路径。

用于验证攻击路径的网络保护工具：

- **防火墙：**控制网段之间以及与外部的通信流量。如果配置得当，防火墙能有效阻止横向移动，并强制执行网络区域分段。
- **网络访问控制(NAC)：**自动控制哪些设备可以连接到网络。尤其适用于 IT、OT 和 IoT 设备的混合环境，NAC 有助于确保设备之间只进行授权通信。

在智能楼宇中，模拟防火墙区域规则可能揭示出会议室区域与楼宇管理区域之间的异常流量，提示存在潜在的横向移动路径，应当加以封锁。根据实际通信行为验证并优化防火墙规则，可以更有效地实施网络分段，从而减少攻击面。

5. 动员修复

暴露风险管理的最后一步是“动员”，把洞察转化为实际措施。
高效的执行需具备把风险修复工作“业务化”的能力，使其既能符合企业的运作约束，又能带来可衡量的成果。

要成功动员 CPS 暴露风险管理计划，请考虑以下几点：

- **整合工作流程：**把暴露风险数据整合到现有的IT和安全工作流程中，以便团队使用熟悉的工具快速采取行动。
- **OEM协作：**选择与原始设备制造商（OEM）有合作关系的CPS安全供应商，便于现场修复，尤其是在更新或配置影响旧设备系统时。
- **停机计划：**把修复工作安排在维护时段或运营计划之外，尽可能减少对重要流程的干扰。
- **项目价值追踪：**建立明确的关键绩效指标（KPI）和报告机制，展示风险降低情况，并验证CPS安全工作的长期投资回报（ROI）。

如果缺乏上述动员，即使做了最全面的风险暴露评估，也可能停滞不前，严重风险得不到解决，企业仍会处于脆弱状态。

总结

当今，BMS在CPS基础设施中发挥重要作用，企业急需从被动应对转向主动防护。如果企业不采用全面的资产管理方法来发现网络中的每一台设备，关键资产的漏洞和风险就可能隐藏在视线之外。Team82建议依照本报告中提出的详细行动计划，以确保安全、合规、全面保护，免受不断加剧的威胁形势的影响。

参考来源：

[1] Gartner 于 2023 年 10 月 11 日发布的《Implement a Continuous Threat Exposure Management (CTEM) Program》，作者：Jeremy D’Hoinne、Pete Shoard、Mitchell Schneider。
GARTNER 是 Gartner, Inc. 及其在美国和国际上的关联公司的注册商标与服务标志，在此经许可使用，保留所有权利。

关于 Claroty

Claroty 凭借无与伦比的、以工业为主的平台重新定义了网络化物理系统 (Cyber Physical Systems, CPS) 防护。Claroty 平台旨在保护关键任务型基础设施，提供市场上最深入的资产可视化、最广泛的 CPS 安全解决方案，涵盖了风险管理、网络保护、安全访问、威胁检测，可以在云端使用 Claroty xDome，也可以在本地部署 Claroty CTD。Claroty 平台以屡获殊荣的威胁研究和技术联盟为后盾，帮助企业有效降低 CPS 风险，提供最快的价值实现时间 (TTV) 和更低的总拥有成本 (TCO) 。在全球范围内，已有数百家企业在数千个站点部署了Claroty。

关于 Team82

Team82 是 Claroty 的研究团队，曾多次获奖，以研究威胁、分析 OT 和医疗协议、发现与披露工业、医疗、商业漏洞而闻名。Team82 致力于提升 CPS 网络安全，拥有业内规模最大的测试实验室，并与行业领先的供应商紧密合作，评估其产品的安全性。截至 2025 年 3 月，Team82 已披露了 650 个漏洞。

Cyberworld
广州科明大同科技有限公司
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

扫一扫
关注公众号