In the Boxing Ring
2026年2月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2026年2月份的 In the **Boxing Ring**

本月，Network Box 董事总经理 Michael Gazeley 探讨了“网络安全自满的荒谬性”。在当今的数字化环境中，网络威胁已不再是偶发性的干扰，而是持续不断、日益复杂的攻击，针对各类规模与行业的组织发起。然而，尽管风险显而易见，许多 IT 管理者仍然采取相对被动的态度，寄希望于侥幸，而非未雨绸缪。

在第 2 至第 3 页中，我们将深入分析这种自满为何在逻辑上极具危险性，探讨勒索软件、供应链攻击等不断演变的威胁形态，并阐述为何主动防御如今必须被视为企业的核心优先事项。

在第 4 页中，我们重点介绍了本月 **周二补丁** 将发布的针对 Network Box 8 及其云服务的一系列功能增强与问题修复。

在其他消息方面，Network Box 已顺利完成与 THEi 的培训项目，使相关教授获得网络安全运营授权培训提供方认证。这一举措进一步强化了 THEi 的网络安全课程体系，并确保学生能够掌握 Network Box SOC 运营的实务技能。

此外，作为年终特别内容，Network Box 还将多篇 “In the Boxing Ring” 栏目精选文章汇编，推出《Network Box 技术评论 2025 年版》。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2026

本月摘要

网络安全
自满的荒谬性

Michael Gazeley
Managing Director
Network Box Corporation Limited

当今数字环境比以往任何时候都更加严峻。网络威胁已从零星事件演变为持续不断的攻击浪潮，针对各类规模与行业的组织发起冲击。然而，尽管这一威胁显而易见且迫在眉睫，仍有相当数量的 IT 管理者采取被动应对的态度。“观望等待”的策略不仅已经过时，更在逻辑上极具危险性。

网络安全已不再是小众关注的问题——它已经成为企业至关重要的核心议题。黑客、恶意软件，尤其是勒索软件，已成为日常威胁。相关数据触目惊心：每天都有成千上万的组织遭受攻击，数据被窃取、系统被瘫痪、声誉被严重损害。尽管如此，仍有许多人选择寄希望于侥幸。这并非谨慎，而是失职。

勒索软件已发生了极其危险的演变。它不再只是加密文件并索要赎金。现代变种会窃取机密数据，并将其发布在公开网络甚至暗网之上；同时还会破坏备份，使恢复变得不可能。有些甚至会对受害者网络发起分布式拒绝服务（DDoS）攻击，进一步加剧混乱。其造成的损害不仅仅是经济层面的，更涉及运营、声誉，甚至在某些情况下关乎企业的生存。

威胁格局正在迅速扩展。物联网（IoT）设备在家庭和企业中大量普及，但往往缺乏足够的安全防护措施，每一台设备都可能成为攻击者的入口。人工智能（AI）在诸多领域前景广阔，但同时也带来了新的风险——它可能被武器化，用于自动化攻击、绕过防御以及操控数据。社会工程学仍然是黑客武器库中的重要手段：钓鱼邮件、语音伪造以及身份冒充等策略，依然能够欺骗甚至经验丰富的专业人士。

关键基础设施正面临严峻威胁。电网、供水系统、交通网络以及医疗体系正日益成为攻击目标。一旦其中任何一个遭受成功攻击，都可能带来灾难性后果。美国的 Colonial Pipeline 事件 曾敲响警钟，但类似的安全隐患在全球范围内依然存在。金融机构、教育机构以及政府部门，无一不处于攻击者的瞄准之中。

风险清单既漫长且仍在不断扩大。供应链攻击利用供应商与客户之间的信任关系发起渗透；云配置错误可能导致敏感数据暴露；内部威胁，无论是恶意还是无意，始终是持续存在的挑战。移动设备这一常被忽视的环节，实际上也是通往企业网络的重要入口。而在许多组织中仍在使用的遗留系统，则缺乏抵御现代威胁所需的韧性。

尽管如此，整体应对仍显得乏力。预算限制常被用作理由，同时也存在一种观点，认为自身组织规模较小或影响有限，不太可能成为攻击目标。这些假设不仅错误，而且具有危险性。网络攻击者并不挑剔目标，他们追逐的是机会，而非声望。在许多情况下，规模较小的组织由于防御较弱，反而更容易成为攻击对象。

爱因斯坦曾说，疯狂的定义就是反复做同一件事，却期待不同的结果。这句话在网络安全领域尤为贴切。持续忽视威胁、延迟升级、对防御投入不足，无异于为灾难埋下伏笔。丘吉尔也曾提出发人深省的观点：“那些不从历史中吸取教训的人，注定会重蹈覆辙。”网络攻击的历史充满了教训，现在正是认真汲取这些教训的时候。

主动防御措施至关重要。定期安全审计、员工培训、完善的备份策略以及应急响应预案，应当成为标准实践。多因素认证、加密技术和网络分段并非可选项，而是必不可少的安全措施。威胁情报必须融入日常运营，漏洞管理也应是持续进行的，而非周期性的工作。

董事会和高层管理者必须在这一使命上给予 IT 管理者充分支持。网络安全不仅仅是技术问题，更是战略重点。预防的成本始终低于事后恢复的代价。保险或许可以弥补部分损失，但无法恢复信任，也无法消除声誉受损的影响。客户、合作伙伴及监管机构都期望企业尽到应有的责任，任何低于这一标准的表现都是不可接受的。

对风险掉以轻心的荒谬必须终结。代价过于高昂，威胁真实存在，现在正是采取行动的时刻。IT 管理者必须走在前列，而不是被动跟随；必须提前预判，而不是事后反应；必须主动防护，而不是寄希望于侥幸。

网络安全是一段旅程，而非终点。它需要持续的警觉性、适应能力与长期投入。数字战场从不宽容，唯有做好准备者才能胜出，其余的只会成为下一份安全事件报告中的统计数字。

归根结底，忽视网络威胁的非理性行为，已不再只是职业上的失误，而是一种失职。黑客、恶意软件以及勒索软件所造成的损害巨大且仍在不断扩大。防御这些威胁的手段其实已经存在，所缺乏的只是付诸行动的决心。

让 2026 年成为改变的一年——让理性战胜自满，让网络安全真正被所有人严肃对待。

Network Box 8 新特性
2026年2月

2026 年 2 月 3 日（星期二），Network Box 将发布本月的 周二补丁 功能增强与问题修复。各区域 SOC 将在接下来的 14 天内分阶段部署这些新功能

本月针对 Network Box 8 的更新包括：

NBRS-8

- **配置历史修复**
  解决了在使用“last month” 时间范围时无法显示结果的问题。
- **增强的 TLS 安全性**
  优化了 TLS 1.3 的 SSL 加密套件顺序，在提升安全性的同时增强兼容性。
- **更智能的垃圾邮件过滤**
  更新垃圾邮件检测机制，不再对回环地址或私有 IP 地址执行实时黑名单列表（RBL）查询。
- **更可靠的特征库更新**
  改进特征库下载机制，在高错误率的网络环境下提供更稳定的更新体验。

在大多数情况下，以上更改不会影响正在运行的服务或要求设备重启。然而，在某些情况下（取决于配置），可能需要设备重启。如果需要，您的本地SOC将与您联系安排此事。

如果您需要关于上述任何内容的更多信息，请联系您的本地SOC。他们将安排部署和联络。

Network Box HIGHLIGHTS

Network Box 香港
THEi 安全运营培训

在与香港高等教育科技学院（THEi）的合作下，Network Box 已成功为相关教授完成培训，并授予其网络安全运营授权培训提供方认证。该认证表明其已具备在 Network Box 安全运营中心（SOC） 体系下开展教学的资质，从而进一步强化了 THEi 的网络安全课程体系，确保未来毕业生能够获得实践能力与行业经验。
Network Box 首席技术官 Mark Webb-Johnson 出席并为获证人员颁发了认证。

Network Box
技术评论 2025

作为年终特别回顾，Network Box 汇编了 2025 年 “In the Boxing Ring” 栏目的重点技术新闻、专题与文章：

- NBSIEM+ 事件工单的自动化建议
- 分类归档（Pigeonholing）
- Box Mail - Network Box 邮件门户系统
- 威胁物理安全的关键网络漏洞
- 法律行业的网络安全关键要务
- 为何真正的 24×7×365 安全运营中心（SOC）对企业网络安全至关重要
- 强化网络安全：管理员最佳实践
- 为何 IT 管理者必须实施外部视角扫描与最佳实践报告建议
- 理解量子密码学：IT 管理员指南
- 安全启动期限：为何 IT 团队必须立即行动以防止系统故障
- 人类防火墙：为何网络安全仍离不开人的参与
- NBSIEM+ 与移动应用

LINK:
https://mcdn.network-box.com/ItBR/2025/Technology_Review_2025.pdf

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581

www.network-box.cn

翻译：Jason