In the Boxing Ring
2023年12月

Network Box x 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2023年12月份的 In the **Boxing Ring**

节日的问候，节日的祝福！本月，我们将对 "了解公司的安全态势 "系列进行总结。如今，企业越来越依赖技术和数字基础设施。这在带来众多好处的同时，也使企业面临潜在的风险和干扰--任何规模的企业都无法避免网络攻击。因此，确保稳健的安全态势至关重要。在第 2 页至第 3 页，我们将讨论制定灾难恢复计划的重要性，以及为什么您的企业可能成为黑客攻击的目标。

另外，我们很荣幸地宣布，Network Box 新加坡 SOC 现已获得 TÜV SÜD PSB Pte Ltd. 的 ISO 27001 认证，在此向我们的新加坡团队表示热烈祝贺！此外，Network Box 美国与 MSP Toolkit 和 Praxis Data Security 共同举办了现场网络安全活动。最后，Network Box 香港迎来了 Raimondi 学院信息与通信技术系的师生们参加网络安全研讨会/工作坊。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2023

本月摘要:

了解公司的安全态势

(第二部分)

Kseniia Degtiareva
Network Box 网络安全顾问

如今，企业越来越依赖技术和数字基础设施。这在带来众多好处的同时，也使企业面临潜在的风险和干扰。因此，确保稳健的安全态势至关重要。本文是我们安全态势系列的第二部分，我们将讨论制定灾难恢复计划的重要性，以及为什么您的企业可能成为黑客的目标。

为什么需要灾难恢复计划

自然灾害和非自然灾害都会严重影响企业运营。因此，企业必须制定明确的灾难恢复计划，以减轻其负面影响。灾难恢复计划是一套明确的流程和程序，概述了企业如何应对各种灾难并从灾难中恢复。它确保关键业务功能能够快速有效地恢复，最大限度地减少停机时间和经济损失。

以下是企业需要制定灾难恢复计划的一些主要原因：

最大限度地减少停机时间和生产力损失: 灾难会严重干扰企业运营。如果没有适当的恢复计划，企业可能难以回到正轨，导致停机时间延长、生产力损失和潜在的收入损失。准备充分的灾难恢复计划可确保采取必要措施，最大限度地减少停机时间，使企业尽快恢复运营。

保护数据和信息: 数据是当今企业最宝贵的资产之一。数据可能遭到破坏或完全丢失，从而给企业带来严重后果。灾难恢复计划应包括备份和恢复程序，以保护关键数据和信息。从而确保数据可以有效地恢复和访问，以保护业务运营的完整性和连续性。

确保业务连续性: 如果处理不当，灾难会对企业造成长期影响。灾难恢复计划可使企业在灾难发生期间和之后保持业务连续性。它概述了关键步骤，以确保即使在不利情况下也能继续履行基本职能。通过优先考虑业务连续性，企业可以最大限度地减少灾难对其运营的影

满足监管和合规要求:
许多行业对数据保护和业务连续性都有具体的监管和合规要求。强大的灾难恢复计划有助于企业满足这些要求，并遵守适用的法律法规。企业可以通过制定灾难恢复计划来表明其对保护敏感信息和保持业务完整性的承诺。

灾难恢复计划对任何企业的风险管理战略都至关重要。它为减轻灾难的影响提供了路线图，使企业能够迅速有效地恢复。通过投资于精心设计和定期测试的计划，企业可以保护其运营、数据和声誉，确保在不可预测的世界中取得长期成功。

您的企业是黑客攻击的目标吗？

在当今的网络威胁形势下，任何规模的企业都无法幸免于网络攻击。黑客不断在互联网上扫描易受攻击的目标，各种规模的企业都可能成为受害者。以下是黑客将您的企业作为攻击目标的几个原因：

有价值的数据: 获取经济利益的潜力往往是黑客的驱动力。如果您的企业处理客户信息、付款详情或知识产权等有价值的数据，那么您的企业就会成为一个有吸引力的目标。黑客可以利用这些数据达到各种恶意目的，包括身份盗窃、金融欺诈或在暗网上出售。

行业声誉: 特定行业由于掌握着宝贵的信息，更容易受到网络攻击。例如，医疗机构存储敏感的患者数据，金融机构处理大量资金，技术公司拥有宝贵的知识产权。黑客可能会以这些行业的企业为目标，获取有价值的信息，并利用它们的声誉获取经济利益。

安全措施薄弱: 黑客通常会寻找阻力最小的途径。如果企业的安全措施薄弱或过时，就很容易成为攻击目标。这包括使用薄弱的密码、不定期更新软件、缺乏适当的加密或忽视员工网络安全培训。黑客可以利用这些漏洞，在未经授权的情况下访问您的系统和数据。

勒索软件的潜力: 近年来，勒索软件攻击日益猖獗。黑客利用恶意软件对企业数据进行加密，并索要赎金才能释放数据。任何企业都可能成为勒索软件的攻击目标，尤其是拥有宝贵数据且安全措施薄弱的企业。

竞争优势: 在某些情况下，黑客可能会以寻求竞争优势的企业为目标。怀有恶意的竞争对手或个人可能会试图在未经授权的情况下获取企业的专有信息、商业机密或即将推出的产品计划。他们这样做的目的是获得竞争优势或破坏您的业务运营。

企业必须明白，网络攻击威胁是真实存在的，并可能造成严重后果。实施强有力的网络安全措施、定期更新安全补丁以及对员工进行最佳实践教育，可以大大降低成为黑客攻击目标的风险。请记住，网络安全是一项持续的工作。保持警惕，掌握信息，保护您的企业免受不断变化的网络威胁。

Network Box HIGHLIGHTS

Network Box 新加坡
ISO/IEC 27001 : 2013 认证

Network Box 很荣幸地宣布，我们在新加坡的办事处 Network Box (SIN) Pte Ltd 通过了 TÜV SÜD PSB Pte Ltd. 的 ISO 27001 认证。这意味着，Network Box 新加坡安全运营中心已建立并应用信息安全管理系统来安装、配置、监控和支持 Network Box 统一威胁管理设备。

CERT NO.: IS27-2023-0192
ISO/IEC 27001 : 2013

Network Box USA
网络安全现场活动

Network Box USA 与 MSP Toolkit 和 Praxis Data Security 共同举办了题为 "网络安全现状 "的现场活动： 您需要与客户和潜在客户进行的顶级网络安全对话 "的现场活动。活动涵盖的主题包括 合规性、框架、风险、 SASE、XDR、SIEM、AI/ML、边缘防御、IAM、DLP、勒索软件和网络保险。

Network Box 香港
网络安全研讨会

Network Box 香港 欢迎 Raimondi 学院信息和通信技术系的师生。研讨会重点介绍了当前的网络威胁形势和可用于缓解这些威胁的技术。

月刊主办	订阅
Mark Webb-Johnson 主编 **Michael Gazeley** **Kevin Hla** 产品支持 **Network Box HQ** **Network Box USA** 贡献者	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 Jiang