中央银行的网络风险

作者:Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros, David Whyte

**总结**

**集中**

网络攻击越来越频繁和复杂，公司和决策者将网络风险列为一个主要问题。金融机构和金融市场基础设施尤其面临风险，金融业一直是受攻击最严重的行业之一。尽管已经对私营部门（尤其是金融部门的公司）的网络威胁进行了几次研究和调查，但人们对央行对网络风险的评估知之甚少。

**捐款**

我们利用2021在全球网络弹性小组成员中进行的一项调查，概述了中央银行社区的网络风险。这项调查包含来自世界各地区的21家中央银行的答复。它研究了以下问题：中央银行的主要网络担忧是什么，以及它们如何看待威胁形势？他们采取什么措施来预防或打击网络攻击？他们如何评估整个金融部门的风险和准备程度？

**调查结果**

我们揭示了四个主要见解。首先，发达经济体和新兴市场经济体的央行对不同网络攻击的频率和成本进行了不同的评估。其次，各国央行积极讨论和制定应对网络攻击的政策，并大幅增加了与网络安全相关的投资。第三，各国央行认为，金融领域系统相关网络攻击的潜在损失是巨大的，尤其是如果攻击的目标是提供关键云基础设施的大型科技公司。只有少数几家央行完全同意金融部门为网络攻击做好了充分准备，超过半数的受访者认为金融部门在过去一年中对网络安全的投资不足。第四，各国央行已经在一系列与网络风险相关的议题上进行了广泛合作，例如，在制定健全的网络复原原则、建立专门的知识共享协调中心以及制定共同项目以限制网络威胁等方面。

**摘要**

金融部门网络攻击的不断增加对金融稳定构成威胁，并使网络风险成为决策者的主要担忧。本文介绍了全球网络抵御能力小组成员对网络风险及其对中央银行的挑战的调查结果。调查显示，自2020年以来，各国央行显著增加了网络安全相关投资，优先考虑技术安全控制和恢复能力。各国央行将网络钓鱼和社会工程视为最常见的攻击手段，系统相关网络攻击的潜在损失被认为是巨大的，尤其是如果目标是提供关键云基础设施的大型科技公司。通常，受访者认为金融部门对网络攻击的准备不足。尽管大多数新兴市场经济体的央行为收集金融机构网络攻击信息提供了一个框架，但发达经济体只有不到一半的央行这样做。公共当局之间的合作，尤其是在国际范围内的合作，可以提高中央银行应对网络攻击的能力。

JEL分类：E5、E58、G20、G28。

关键词：网络风险、中央银行、金融机构、云服务、网络监管。

**原文链接:**<https://www.bis.org/publ/work1039.htm>