Cyber risk in central banking

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

Date:2022-09-14

Keyword:central banks, financial institutions, cyber risk, cloud services, cyber regulation

Attachment:[Link](https://www.bis.org/publ/work1039.pdf)

From:[BIS-working\_paper](https://www.bis.org/publ/work1039.htm)

总结  
集中  
网络攻击变得越来越频繁和复杂，公司和决策者将网络风险列为主要关注点。金融机构和金融市场基础设施尤其面临风险，金融行业一直是受攻击最严重的行业之一。虽然已经对私营部门，特别是金融部门的公司的网络威胁进行了几项研究和调查，但对中央银行的网络风险评估知之甚少。  
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。该调查包含来自世界各地21家央行的回应。它研究了以下问题：央行的主要网络担忧是什么，以及它们如何看待威胁前景？他们采取了哪些措施来预防或反击网络攻击？他们如何评估整个金融部门的风险和准备情况？  
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中央银行对不同网络攻击的频率和成本进行了不同的评估。其次，各国央行积极讨论并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，金融部门系统相关网络攻击的潜在损失很大，尤其是如果攻击的目标是提供关键云基础设施的大型技术。只有少数央行完全同意，金融部门已为网络攻击做好充分准备，超过一半的受访者认为，过去一年，金融部门在网络安全方面的投资不足。第四，中央银行已经在一系列与网络风险相关的主题上广泛合作，例如制定网络恢复力的合理原则，创建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。  
摘要  
金融部门网络攻击的数量不断增加，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弹性小组成员关于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与网络安全相关的投资，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方法，系统相关网络攻击的潜在损失被认为是巨大的，尤其是当目标是提供关键云基础设施的大型技术时。一般来说，受访者认为金融部门对网络攻击的准备不足。虽然大多数新兴市场经济体的中央银行提供了一个收集金融机构网络攻击信息的框架，但发达经济体中只有不到一半的中央银行这样做。公共当局之间的合作，尤其是在国际背景下，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