夯实网络安全壁垒 提升金融服务体验

——浅析中国银行金融网络安全架构建设

中国银行数据中心 戴亮 刘洋

随着我国促进互联网金融健康发展等相关政策的深入实施，银行业等传统金融行业的市场化改革加速，竞争日趋激烈。如何通过高效安全的金融网络为客户提供普惠便捷的金融服务，成为银行业探索实践的重要目标，更成为银行业基业之树长青的核心竞争力。

在总行领导关于“担当社会责任，做最好的银行”目标指引下，面对日趋严峻的网络安全形势，为不断夯实金融网络安全架构，中国银行深耕网络安全体系建设，持续探索并积极实践多样化的网络安全技术在金融业务中的深入应用，取得了良好的成效。

一、金融网络安全面临的严峻形势

互联网金融的飞速发展加速了银行业传统柜面业务向网上银行、第三方支付、P2P 等新型服务模式的扩展。但与此同时，新型服务模式也带来诸如服务方式虚拟化、业务边界模糊化、经营环境开放化等特点，使得互联网金融业务面临网络攻击、病毒入侵、非法窃取账户信息、客户信息泄露等信息安全问题。

1、金融机构成为不法分子实施网络攻击的重点目标

近年来，部分不法黑客将攻击重点转移至金融机构。对银行业等金融机构进行攻击，不仅能够直接攫取巨大的经济利益，还能破坏金融秩序，对社会稳定造成极大影响。而对银行来说，将直接造成业务中断和客户流失。

2、业务连续性需求给信息安全风险管理提出更高要求

借助移动互联网技术，银行业可为客户随时随地提供便捷的金融服务，但愈加严格的业务连续性需求也给银行业信息安全风险管理水平提出了更高要求。如何丰富信息安全风险管理手段，优化业务连续性管理体系，提升风险管理体系与业务连续性管理体系的协调性，成为银行业重点关注的领域。

3、网络技术的创新应用给互联网金融带来更大挑战

近几年，“互联网+”和网络新技术的研究方兴未艾，为金融行业创造了巨大的便利和经济效益。与此同时，新技术的成熟度、应用场景和风险管理，也给银行业带来了前所未有的挑战。

二、中国银行金融网络安全部署策略

经过多年的探索与实践，在金融网络安全领域，中国银行逐步建设成一套以“多层次、多样化”为目标的智慧网络安全防护体系。

1、高可用的两地三中心网络架构

目前，中国银行在北京部署生产数据主中心、同城备份中心，在

上海部署异地灾备中心，各中心间通过运营商高速光纤连接，实现业务数据在主中心及备份中心间的传输及同步。

以两地三中心网络架构为依托，中国银行部署互联网出口、外联网、一二级骨干网络、网点接入网，形成了多层次、多功能、跨地域的综合性网络。

2、多层次的网络安全防护策略

在网络安全防护策略上，中国银行采用分层部署、逐级保护的方式。按照“建立网络通信与访问安全策略，隔离不同网络功能区域，采取与其安全级别对应的预防、监测等控制措施”的监管要求，根据网络功能进行区域划分，在功能区边界部署防火墙，建立访问控制、入侵检测、终端准入等多种方式相结合的网络安全防护体系，防范对网络的未授权访问，保证网络通信安全。

3、多样化的网络安全新技术运用

通过网络端口安全和防欺骗等技术实现网络接入安全防护，通过终端入网准入控制实现对入网终端的合法性检查，通过漏洞扫描系统及时发现存在的系统缺陷。

通过部署远程安全漏洞检测系统，实现对操作系统、数据库系统、中间件、应用程序、网络设备和安全设备内嵌系统的安全检测，及时发现安全漏洞和不合规的参数配置，并为缺陷修复和处置提供参考解决方案。

三、中国银行金融网络安全发展目标

面对业务快速扩张、经营压力增大的发展需求，中国银行需要更加健壮、高效、智慧、安全的网络支持。而日趋严峻的互联网安全形势更是对中国银行金融网络安全工作提出了更高的要求。针对未来的网络安全发展趋势，更是要在总体架构、安全防护、新技术应用和应急处理等方面深耕细作。

1、强化两地三中心网络架构，全面推进灾备网络建设

在现有两地三中心的网络架构基础上，加快推进海外分中心及分行灾备网络建设，完善全行范围内的灾备网络架构，确保一级分行和二级分行网络在出现灾难情况仍可支撑核心业务的持续运行。

此外，通过灾备演练检验上百套重要系统灾备恢复方案的有效性，不断贴合真实场景，灾备演练场景和范围覆盖全球多时区、多时段，提升重要业务连续性保障能力，使灾备人员的应急处置能力得到提升。

2、完善网络防护体系，部署多层次的网络安全防护措施

不断优化网络防护架构，通过多层异构防火墙实现外部到生产网络的隔离，通过 IDS、IPS 等工具实现实时的网络入侵检查和防御，通过地址转换实现对内部服务器的隐藏保护。

在关键的骨干传输区域，通过部署流量监控设备和入侵检查设备，实施监控异常流量和网络攻击行为。在终端接入区域综合实施多

种安全策略，通过访问控制和终端入网准入控制实现对入网终端的合法性检查。

3、在新技术领域持续探索创新，加快网络设备国产化进度

积极尝试网络新技术、新工艺、新模式，搭建基于大数据的网络管理平台，持续探索虚拟化和云计算等技术在网络安全领域的实践应用。坚持以客户体验为中心，不断增强适应互联网生态系统构建的新技术运用能力。

进一步加快网络设备的国产化步伐，消除容量瓶颈，不断增强网络基础设施和关键技术的自主可控能力，

4、不断提升应急处理能力，增强网络安全防护水平

持续强化 7×24 小时运维体系，完善跨部门应急协调和“峰值”管理手段，与电信运营商、公安机关和第三方安全机构建立协作机制。从人员技能、管理机制、监控预警、应急预案、有效性评价等方面苦练内功，不断提升。

进一步提高自动化监控预警水平，加强网络攻击事件防范与应急响应能力，最大程度降低网络攻击事件可能造成的损失与影响，确保各信息系统安全稳定运行。

四、总结

面临互联网金融生态的蓬勃发展，以及经济新常态下不断深化国际化战略的发展需求，中国银行深刻地意识到：既要开放怀抱迎接互

联网金融带来的挑战和机遇，更要坚持金融网络安全建设。要以时不我待的紧迫感，持续提升风险管理及防范能力，不断完善技术防护体系，优化网络保护机制，部署多层次的网络安全防护措施，在持续提升用户服务体验的路上砥砺前行。