IN BRIEF

OVERSIGHT OF THE FINANCIAL INFRASTRUCTURE 2016

FOCUS ON CYBERATTACKS AND CROSS-SYSTEM RISKS

The financial systems in Denmark are safe, stable and efficient but should take a more methodical approach to protection against cross-system risks and defence against cyberattacks.

Those are the main messages in Danmarks Nationalbank's publication *Oversight of the Financial Infrastructure 2016*, an annual publication containing an assessment of the systems underlying settlement of payments and financial transactions in Denmark.

The systems reviewed are those behind e.g. purchases of securities, interbank payments, online bank transactions and transfers via MobilePay and Swipp. The key issues are whether the systems are efficient (ensure rapid settlement, for example), stable (downtime is low) and safe, so that people can trust that payments will be effected as agreed.

The overall conclusion to the most recent review is that all systems (see Box 1) have proved to be safe, stable and efficient. All systems have experienced problems over the last year – such as short periods of downtime for one reason or another. But in the assessment of Danmarks Nationalbank these problems have been small and the system owners have taken satisfactory action in response to the problems. At the same time, the incidence of fraudulent use of payment instruments (e.g. in connection with online shopping) is low, which underpins confidence in the system.

However, in order to observe new international standards the systems should strengthen awareness of two issues relating to safety. One is cross-system risks, the other is cyberattacks.

Oversight by Danmarks Nationalbank Box 1

Danmarks Nationalbank oversees that the exchange of money and securities in Denmark takes place in a safe, stable and efficient manner.

More specifically, Danmarks Nationalbank oversees the systems behind three payment types:

1. Payments between consumers, firms and authorities. Settlement of retail payments takes place via the Sumclearing, the Intradagclearing and the Straksclearing. These systems are owned by the Danish Bankers Association. At the same time, the most important payment instruments are overseen, e.g. the Dankort, which is owned by Nets.
2. Interbank payments. These take place in Danmarks Nationalbank's own system, Kronos.
3. Securities transactions. These take place in the VP settlement system, which is owned by VP Securities A/S (VP).

CYBERATTACKS

These years there is considerable international focus on the risk of cyberattacks on payment and settlement systems.

The Committee on Payments and Market Infrastructures of the International Organization of

Securities Commissions, CPMI-IOSCO, is finalising its guidance on cyber resilience. This guidance should be observed in Denmark.

There is no doubt that outsiders want to gain access to the systems of public authorities and private firms in Denmark. According to the cyber security centre of the Danish Defence Intelligence Service, DDIS, the risk of both cyber espionage and cybercrime is very high. According to DDIS, such espionage is conducted primarily by state and state-supported groups using increasingly sophisticated techniques to try to gain access.

Cyberattacks – whether for the purpose of espionage, crime, activism or terrorism – differ from other risks in several respects. You could be infected without knowing it, an attack can be persistent, and there are many potential points of entry, including business partners who are unaware that they are hosting an attack.

Hence it is important that cyber resilience is a key issue for the boards of directors and managements of the respective systems. Focus must be on identification of risks and protection against – and detection of – attacks. In addition, it must be possible to restore operations rapidly after an attack. And it is important regularly to test system resilience and to keep abreast of developments within the area.

CROSS-SYSTEM RISKS

In future, the system owners – the Danish Bankers Association, VP and Danmarks Nationalbank – should enter into more formalised collaboration with a view to reducing cross-system risks. This applies to the risk of cyberattacks, as well as all other major and minor risks, e.g. incidents that may lead to brief or prolonged periods of IT system failure. This could be a severed cable, a bug in a system update, problems with Internet access, power outages or unauthorised access to data.

If something goes wrong in one system, all systems may be affected. For example, the banks settle retail payments by borrowing money from Danmarks Nationalbank. This is only possible if securities deposited at VP are pledged as collateral. So all three systems must be functioning if a transaction is to be executed. If just one link in the chain is broken, all systems have a problem.

This will come as no surprise to the participants in the process. They have had bilateral discussions. They have agreements, they have procedures, they perform tests. But this is done on a case-by-case basis. The new element is that in future system owners must get together and analyse the whole range of potential problems more methodically.

For further information, see the publication 'Oversight of the Financial Infrastructure 2016'

DANMARKS NATIONALBANK

IN BRIEF
PUBLICATION, DESIGN AND LAYOUT:
DANMARKS NATIONALBANK

DANMARKS NATIONALBANK
HAVNEGADE 5
DK-1093 COPENHAGEN K
WWW.NATIONALBANKEN.DK