KORT FORTALT

OVERVÅGNING AF DEN FINANSIELLE INFRASTRUKTUR 2016:

FOKUS PÅ CYBERANGREB OG RISICI PÅ TVÆRS AF SYSTEMER

De finansielle systemer i Danmark er sikre, stabile og effektive, men de skal mere metodisk sikre sig mod risici på tværs af systemer og ruste sig mod cyberangreb.

Det er hovedbudskaberne i Nationalbankens publikation *Overvågning af den finansielle infrastruktur 2016*. En gang om året udgives en sådan publikation, som gennemgår de systemer, der ligger bag betalinger og finansielle transaktioner i Danmark.

De undersøgte systemer er dem, der ligger bag fx køb af værdipapirer, bankers betalinger til hinanden, transaktioner via netbank eller overførsler med MobilePay og Swipp. Det centrale er, om systemerne er effektive (fx afvikler hurtigt), stabile (sjældent går ned) og sikre, hvilket betyder, at man kan have tillid til, at en betaling finder sted som aftalt.

Den overordnede konklusion på den seneste gennemgang er, at alle systemer (se boks 1) har vist sig både sikre, stabile og effektive. I alle systemer har der i løbet af året været problemer – fx små tidsrum, hvor systemet af den ene eller anden grund var nede. Men problemerne vurderes af Nationalbanken som værende små, og systemejerne har handlet tilfredsstillende i forlængelse af problemerne. Samtidig er der kun et lille misbrug af betalingsløsninger (fx ved internethandel), hvilket er vigtigt for, at man kan have tillid til systemet.

For at leve op til nye internationale standarder, er der dog behov for, at man i systemerne styrker opmærksomheden mod to områder, som begge handler om sikkerhed. Det ene område er risici på tværs af systemerne, det andet er cyberangreb.

Derfor overvåger Nationalbanken Boks 1

Nationalbanken skal overvåge, om udveksling af penge og værdipapirer i Danmark sker sikkert, stabilt og effektivt.

Konkret overvåger Nationalbanken de systemer, der ligger bag tre typer betalinger:

1. Betalinger imellem borgere, virksomheder og myndigheder. Afvikling af detailbetalinger sker via systemerne Sum-, Intradag- og Straksclearingen. Systemerne ejes af Finansrådet. Samtidig overvåges de vigtigste betalingsløsninger, fx Dankort, der ejes af Nets.
2. Bankers betalinger til hinanden. Det sker i Nationalbankens eget system, Kronos.
3. Handel med værdipapirer. Det sker i VP-afviklingen, som ejes af VP Securities A/S (VP).

CYBERANGREB

Internationalt er der i disse år meget fokus på risikoen for cyberangreb på betalings- og afviklingssystemer.

Den internationale organisation for centralbanker og finanstilsyn, kaldet CPMI-IOSCO, er

ved at lægge sidste hånd på retningslinjer for, hvordan man bedst beskytter sig mod cyberangreb. Disse retningslinjer bør følges i Danmark.

Der er ingen tvivl om, at nogen ønsker at trænge ind hos både offentlige myndigheder og private virksomheder i Danmark. Ifølge Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste (FE) er risikoen for både cyberspionage og -kriminalitet meget høj. Ifølge FE udføres spionagen primært af statslige og statsstøttede grupper, der med stadig mere avancerede teknikker forsøger at komme indenfor.

Cyberangreb adskiller sig – uanset om der er tale om spionage, kriminalitet, aktivisme eller terror – på flere måder fra andre risici. Man kan være inficeret uden at vide det, et angreb kan stå på over lang tid, og man kan blive angrebet alle steder fra, fx fra samarbejdspartnere, der ikke ved, at de lægger system til et angreb.

Derfor er det vigtigt, at cyberrobusthed er et centralt anliggende hos både bestyrelser og ledelser af de respektive systemer. Der skal være fokus på at identificere risici og på at beskytte sig mod – og opdage – angreb. Derudover skal driften kunne genetableres hurtigt efter et angreb. Og man skal løbende både teste robustheden mod og holde sig opdateret med nyeste viden på området.

RISICI PÅ TVÆRS

Systemejerne – Finansrådet, VP og Nationalbanken – bør fremover arbejde mere formaliseret sammen om at reducere risici på tværs af systemerne. Det gælder både risikoen for cyberangreb og i forhold til alle andre store og små risici, fx begivenheder, der kan føre til kortere eller længere it-nedbrud. Det kan være brud på et kabel, en fejlbehæftet systemopdatering, problemer med netadgang, strømnedbrud, eller at de forkerte mennesker får adgang til data.

Går noget galt ét sted, kan det skabe problemer i alle systemer. Fx afvikler banker borgernes betaling ved at låne penge i Nationalbanken. Det er penge, som de kun kan låne, hvis værdipapirer hos VP stilles som sikkerhed. De tre systemer skal alle fungere, for at en sådan transaktion kan gennemføres. Glipper bare et af leddene i denne kæde, så har alle systemerne et problem.

At det forholder sig sådan er ingen overraskelse for de deltagende parter. De har talt sammen bilateralt. De har aftaler, de har procedurer, de tester. Men det sker fra sag til sag. Det nye er, at systemejerne fremover skal sætte sig sammen og analysere hele paletten af potentielle problemer mere metodisk.

Læs mere i publikationen 'Overvågning af den finansielle infrastruktur 2016'

DANMARKS NATIONALBANK

KORT FORTALT
UDGIVELSE, DESIGN OG LAYOUT:
DANMARKS NATIONALBANK

DANMARKS NATIONALBANK
HAVNEGADE 5
1093 KØBENHAVN K
WWW.NATIONALBANKEN.DK