

5. december 2016

DET TALTE ORD GÆLDER

Tak for invitationen til at tale her.

Jeg har i dag to overordnede budskaber:

1. Øget digitalisering er godt nyt for kunder, banker og samfundet.
2. Øget digitalisering gør også sektoren mere sårbar for ødelæggende hackerangreb, men Nationalbanken og sektoren arbejder løbende på at forhindre, at det sker.

Danskerne er digitale – meget digitale. Der er flere mobiltelefoner end indbyggere i Danmark og internet i næsten ethvert hjem. Danskernes digitale parathed er faktisk den højeste i verden. [figur 1]

Den teknologiske udvikling har ændret måden at drive bank på.

Udviklingen har banet vejen for en række tiltag, der har gjort den finansielle sektor mere effektiv. Det er til glæde for sektoren, og det er til glæde for danskerne.

Øget digitalisering muliggør mere automatiserede processer og mere selvbetjening fra kundernes side. Det reducerer også behovet for filialer og antal ansatte – en bevægelse der har været i gang i en del år, som det fremgår af oversigten her. [figur 2]

Udviklingen har gjort digitale løsninger til en konkurrenceparameter, hvor bankerne konkurrerer om at tilbyde kunderne de bedste digitale produkter.

Men udviklingen har også åbnet for øget konkurrence fra helt nye aktører, der får mulighed for at komme ind på områder, som bankerne tidligere har domineret fuldstændigt.

Konkurrence er som bekendt godt, og intet tyder på, at der bliver mindre af den i fremtiden. Forude venter skærpet konkurrence som følge af det nye EU-betalingsdirektiv, der hedder PSD2. Det kan være en "game changer" for finanssektoren.

PSD2 åbner for, at tredjeparter – med en kundes godkendelse – kan få direkte adgang til at foretage transaktioner på kundens bankkonto. En tredjepart kan for eksempel være en kaffekæde, et flyselskab eller en anden bank end dér, hvor kunden har en indlånskonto.

Pointen er, at PSD2 giver nye aktører adgang til at tilbyde betalingstjenester uden at føre indlånskonti. Det giver disse aktører en fod indenfor, som de kan bruge til at formidle andre tjenester, som for eksempel udlån, som bankerne i modsætning til betalingsformidling rent faktisk tjener penge på.

De danske banker har været dygtige til at følge med og udvikle egne digitale løsninger. Et eksempel er mobile betalingsløsninger, der er blevet meget populære blandt danskerne. Løsningerne har været medvirkende til, at aktører fra udlandet endnu ikke har vundet betydelige markedsandele i Danmark. Den begrænsede størrelse af det danske marked spiller selvfølgelig også ind her.

Øget digitalisering stiller betydelige krav til de enkelte banker om at følge med den seneste teknologiske udvikling, hvis de fortsat skal være konkurrencedygtige. Det er dyrt. Det kræver typisk betydelige investeringer, og her vil bankens størrelse komme til at spille en rolle.

De store banker kan bedre stå på egne ben, når det drejer sig om at udvikle nye digitale løsninger. De mindre institutter er til gengæld afhængige af samarbejde med for eksempel en datacenter eller en større bank for at kunne tilbyde de løsninger, som kunderne efterspørger.

Den digitale udvikling kan føre til større spredning mellem de små og store spillere, hvor større banker typisk kan udnytte stordriftsfordele. Øget digitalisering bidrager derfor til, at udviklingen med færre institutter fortsætter. [figur 3]

Den øgede digitalisering indebærer også en sårbarhed. Den finansielle sektor er afhængig af komplekse it-systemer. Næsten 600 mia. kr. skifter konto hver dag via de systemer. Det svarer til over en fjerdedel af det danske bruttonationalprodukt. Og det gør den danske finansielle sektor til et oplagt mål for cyberkriminalitet.

Truslen er derfor anderledes i dag end tidligere. Der findes fortsat Olsen-Banden-typer [figur 4], men nutidens trusler er radikalt anderledes og kan påvirke hele samfundet.

I et historisk perspektiv er det en ny form for kriminalitet, der kan udøves fra Herning, Hongkong eller et helt tredje sted. Vi har allerede set mange angreb på finansielle institutioner rundt om i verden. Angrebet på centralbanken i Bangladesh gav genlyd globalt, og det var en advarsel om, at cyberangreb bliver stadig mere sofistikerede.

Truslen kan meget vel være endnu større, hvis vi taler om organiseret hacktivism, terrorisme eller egentlige statssponsorerede angreb.

Et omfattende angreb, der rammer flere kritiske aktører eller systemer i for eksempel betalingsinfrastrukturen, har potentiale til at sætte hele eller væsentlige dele af sektoren ud af drift i en periode. Indbrud i computere i den finansielle sektor kan derfor have karakter af at være en systemisk risiko og i sidste ende være en trussel mod den finansielle stabilitet.

Selv mindre alvorlige angreb kan – hvis de sker gentagne gange – svække tilliden til det finansielle system.

Det vil være særligt kritisk, hvis det sker på et tidspunkt, hvor sektoren allerede er i knæ – som for eksempel i efteråret 2008.

Det er den systemiske vinkel, der gør cybertruslen til et anliggende for Nationalbanken.

Den systemiske risiko er blandt andet et resultat af, at landets penge- og realkreditinstitutter er tæt knyttet sammen via betalingssystemer og afviklingssystemer, hvor der flyttes store værdier. Dertil kommer, at institutterne benytter de samme datacentraler, netværksleverandører osv. Det betyder, at vi har brug for, at alle centrale led i kæden er meget stærke.

Finanstilsynet og Nationalbanken har undersøgt cyberrobustheden hos 15 af de største og vigtigste aktører i den finansielle sektor.

På trods af de forbehold, der nødvendigvis må være ved sådan en undersøgelse, kan jeg sige, at cyberrobustheden helt overordnet er på et fornuftigt niveau – men der er også plads til forbedringer.

Indbrud i eller sabotage af vigtige it-systemer stiller særlige krav til it-sikkerheden, som der tidligere måske ikke var så meget fokus på.

Traditionelt har fokus været på overrevne kabler, strømsvigt eller fejl i softwaren. Det skal der også garderes imod, men cyberkriminalitet stiller andre spørgsmål og kræver derfor også andre svar.

Det er vigtigt at holde sig for øje, at et angreb på computersystemerne ikke er en utilsigtet hændelse. Der står kriminelle bag, og de udvikler og forfiner deres metoder hele tiden. Dermed ændrer truslerne sig løbende. Det betyder, at et angreb i virkeligheden kan være vanskeligt at opdage i tide.

Vores undersøgelse viser, at de enkelte aktører arbejder med disse udfordringer, men den viser også, at sikkerheden og beskyttelsen mod cyberangreb generelt er mest veludviklet i de organisationer, der har en cyberstrategi, der er godkendt af bestyrelsen.

Det fortæller os, at en strategi udstukket af den øverste ledelse har været med til at sikre fokus i hele organisationen og målrette indsatsen.

Forbundetheden og dermed den gensidige afhængighed mellem snart sagt alle aktørerne i sektoren betyder, at deling af viden og samarbejde er helt afgørende for at dæmme op for de angreb, der givet vil komme i fremtiden.

Først og fremmest vil jeg understrege, at samarbejdet er nødvendigt – specielt i situationer, hvor der kan være en trussel mod den finansielle stabilitet.

Det er baggrunden for, at vi har etableret FSOR – et Finansielt Sektorforum for Operationel Robusthed.

Der er tale om et samarbejde mellem myndigheder og alle de vigtige aktører i den finansielle sektor [figur 5]. FSOR skal gennemføre fælles tiltag for at øge robustheden, som det hedder. Fokus er både på at undgå nedbrud og på at håndtere dem, hvis de alligevel sker.

Den ambitiøse vision for samarbejdet er, at vi skal være "best in class" i Europa, når det drejer sig om at imødegå truslen fra cyberkriminalitet.

Det første konkrete tiltag var den store test af kriseberedskabet i den finansielle sektor, som vi gennemførte i forrige uge. Der blev evnen til at samarbejde og koordinere indsatsen i tilfælde af et omfattende cyberangreb på kritiske systemer sat på prøve.

Det var lærerigt. Alle blev klogere, og alle tog hjem med erfaringer, der kan arbejdes videre med. Det var heldigvis blot en test. Men hvis det bliver nødvendigt, så er vi klar. Vi vil hellere aktivere beredskabet en gang for meget end en gang for lidt.

Nationalbanken arbejder for en robust økonomi i Danmark. Et vigtigt element er en robust finansiell sektor med en robust infrastruktur.

Forude venter yderligere arbejde for alle i sektoren, men den primære indsats skal foregå hos de enkelte aktører.

Tak for opmærksomheden.