

Det danske betalingsmarkeds robusthed



FINANS
DANMARK

Indholdsfortegnelse

Forord - Betalingsmarkedets robusthed i en ny verdensorden	4
1. Introduktion	6
2. Det danske betalingsmarked er digitalt	8
2.1 Danskernes betalingsvaner	10
2.2 Betalingsmarkedet bygger på en velfungerende teknisk infrastruktur og tæt samarbejde.....	14
2.3 Tiltag der understøtter en høj robusthed på betalingsmarkedet i Danmark.	21
2.4 Alle aktører bør være forberedt på nedbrud og have et effektivt beredskab.	26
3. Identificerede trusler og risici	28
4. Sårbarheder	36
5. Fra analyse til handling	48
5.1 Anbefalinger til at styrke robustheden i betalingsmarkedet på kortere sigt	50
5.2 Fokusområder for robustheden på længere sigt	62

Forord

Samfundets centrale tandhjul – betalingsmarkedets robusthed i en ny verdensorden

I kernen af den moderne finansielle sektor ligger et tandhjul, som ikke bare understøtter bankernes forretning, men hele samfundets økonomiske sammenhængskraft: betalingsinfrastrukturen. Den skal være sikker. Den skal være effektiv. Og vigtigst af alt – den skal skabe tryghed.

Gennem årtier har danske banker investeret massivt i digitalisering. Ikke kun for at styrke deres egne systemer, men også i rollen som en markant bidragsyder til hele samfundets digitale udvikling. Straksbetalinger, Mobile-Pay og MitID er ikke bare teknologiske løsninger – de er symboler på en sektor, der i samarbejde med det øvrige samfund har skabt globalt anerkendte løsninger, som har gjort Danmark til et af verdens mest digitaliserede lande.

Med digitalisering følger kompleksitet. Og med kompleksitet følger sårbarhed. Den digitale finansielle infrastruktur er i dag samfundskritisk, og den skal beskyttes mod cyberangreb, hvidvask og digital svindel. Det er netop, hvad finanssektoren har gjort – med betydelige investeringer og et konstant fokus på sikkerhed.

Men verden har ændret sig. Den russiske invasion af Ukraine, geopolitiske spændinger og opbrud i globale alliancer har skabt et nyt trusselsbillede. Et billede, hvor ikke mindst Europa og Danmark både geografisk og alliancemæssigt er blevet et centralt omdrejningspunkt for nye trusler, og hvor afhængighed af teknologier og leverandører uden for EU pludselig er blevet en strategisk sårbarhed.

Sommeren 2025 mindede os om, hvor skrøbeligt det hele kan være. Et nedbrud i Nets lammede betalingssystemet i Danmark, og i Spanien og Portugal gav et kæmpe strømnedbrud lignende konsekvenser. Det er ikke længere hypotetiske scenarier – det er virkelighed.

Det danske betalingsmarked står stærkt. Men styrke er ikke en garanti for fremtidig robusthed. Derfor er det afgørende, at vi stiller skarpt på, hvordan vi sikrer den kritiske infrastruktur fremover. Det kræver samarbejde på tværs af sektorer, myndigheder og politiske beslutningstagere. Vi skal stille de svære spørgsmål – og forsøge at finde svarene på, hvordan vi håndterer de nye trusler i en ny tid samtidig med, at vi bevarer og styrker de muligheder og fremskridt, som den teknologiske udvikling har givet os.

Denne rapport er finanssektorens systematiske bud på, hvordan vi kan forstå og håndtere de trusler, risici og sårbarheder, der præger betalingsmarkedet. Den indeholder anbefalinger til både kortsigtede og langsigtede tiltag – og den markerer et ønske om et bredt samarbejde på tværs af sektorer for at sikre fremtidens finansielle infrastruktur.

I en verden præget af usikkerhed og uforudsigelighed, er robusthed ikke bare en teknisk disciplin. Det er en nødvendighed for, at vi som samfund kan være trygge, sikre og ikke mindst effektive i en ny virkelighed.

God læselyst.



Michael Rasmussen,
formand
Finans Danmark



Lars Gert Lose,
adm. direktør
Finans Danmark



1. Introduktion

Betalingsmarkedet er afgørende for vitale funktioner

Betalingsområdet har de seneste årtier gennemgået en markant transformation. Fra kontanter og checks til netbank, kort og mobilbetalinger – i dag er 9 ud af 10 betalinger i butikkerne digitale. Denne udvikling har skabt stor værdi for både forbrugere og erhvervsdrivende, men har samtidig introduceret nye risici og afhængigheder, som kræver strategisk opmærksomhed og handling.

Det danske betalingsmarked er et komplekst økosystem med mange aktører og indbyrdes afhængigheder, både nationalt og europæisk. Derfor er det nødvendigt at analysere robustheden bredt og systemisk – ikke kun hos enkeltaktører, men i hele værdikæden.

Denne rapport gennemgår, hvordan betalingsmarkedet i dag er opbygget, og hvordan det bliver brugt af danskerne. Herefter identificerer rapporten en række trusler og risici, som gør det muligt at kortlægge systemernes sårbarheder og robusthed. Begrebet robusthed skal forstås som evnen til at opretholde sikre, effektive og stabile betalingsløsninger – også under pres.

Rapporten bygger på interviews med 11 centrale aktører i betalingsmarkedet samt research og inddragelse af nationale og internationale erfaringer. Den samler konkrete anbefalinger og fremtidige fokusområder, som sigter til at styrke robustheden fremover.

Rapportens afgrænsning

Rapportens primære fokus er dagligdagsbetalinger i Danmark – f.eks. betaling ved køb af mad, medicin og benzin. Disse scenarier forudsætter en velfungerende betalingsinfrastruktur, der kan understøtte forskellige betalingsformer og aktører.

Fokus er på aktører som forbrugere, erhvervsdrivende, tekniske leverandører, banker og myndigheder. Målet er at belyse robustheden i økosystemet som helhed – herunder afhængigheder og koncentrationsrisici – snarere end at evaluere enkeltaktører.

Analysen koncentrerer sig om nedbrud af kortere varighed. Længerevarende nedbrud, der påvirker forsyningskæder og samfundets funktioner bredt, ligger uden for rapportens afgrænsning, men flere af rapportens indsigter vil også være relevante i sådanne scenarier.

Analysen omfatter betalinger, som en forbruger i Danmark foretager. Det er:

- Betalinger via fysiske betalingskort – i fysiske butikker eller online
- Betalinger via wallet- og mobilbetalingsløsninger i fysiske butikker eller online. Det kan være Apple Pay, Google Pay eller MobilePay
- Kontantbetalinger i fysiske butikker
- Mobilbetalinger mellem privatpersoner, primært MobilePay
- Betalinger via net- og mobilbank, hvor forbrugeren laver overførsler til butikker og virksomheder

Disse betalinger er ikke omfattet af analysen:

- Betalinger mellem virksomheder
- Faste betalinger via Betalingsservice
- Løn- og ydelsesudbetalinger via NemKonto
- Forudbetalte kort, kryptoaktiver og betalinger hen over grænser

Rapportens anbefalinger kan dog også have afledte positive effekter for disse betalingstyper.

Analysemetode

Analysen bygger på en flerstrengt metode, der kombinerer:

- **Research** af branchedata, eksisterende analyser og regulatoriske rammer
- **Interviews** med 11 nøgleaktører fra hele betalingsværdikæden
- **Workshops og dialogforløb** for at identificere fælles problemstillinger og løsninger

Interviewene er struktureret omkring konkrete afhængigheder, trusler, beredskabsscenarier og strategiske prioriteringer. Data er analyseret i relation til udvalgte brugerrejser og risici, og hovedkonklusioner er valideret med interne og eksterne eksperter.

Finans Danmark har samlet interessenter fra erhvervsorganisationer, banker og tekniske leverandører for at sikre bred repræsentation og solidt vidensgrundlag.

2.

Det danske betalingsmarked er digitalt



Danskerne har adgang til en række digitale betalingsløsninger, der er nemme og hurtige at anvende, og som stort set alle danskere benytter. 98 pct. af de 16-74-årige benytter således netbank, mobilbank eller MobilePay og over 99,8 pct. har et betalingskort. Bankerne har et bredt produktudbud, og bankerne har udstedt over 10 mio. betalingskort til privatpersoner. Stort set alle tilbyder både Dankort [typisk co-brandede med Visa eller Mastercard] og et rent Visa eller Mastercard til deres kunder.

2.1 Danskernes betalingsvaner

Brugen af digitale betalingsløsninger er udbredt blandt danskerne i hele Danmark og på tværs af aldersgrupper, hvor særligt gruppen over 40 år de seneste år har taget de digitale løsninger til sig. Udviklingen i danskernes digitale betalingsvaner har betydet, at de ressourcer, samfundet bruger på betalinger, er faldet markant. Danskerne skal ikke længere bruge tid på at hæve penge i en pengeautomat, men kan betale i supermarkedet med to klik på telefonen.

På tværs af fysisk handel, internethandel og mellem privatpersoner foretog danskerne 3,8 mia. betalinger i 2023, hvoraf to-tredjedele var baseret på kortbetalinger. Det svarer til, at hver dansker i løbet af året foretager 461 korttransaktioner eller knap 9 kortbetalinger om ugen.

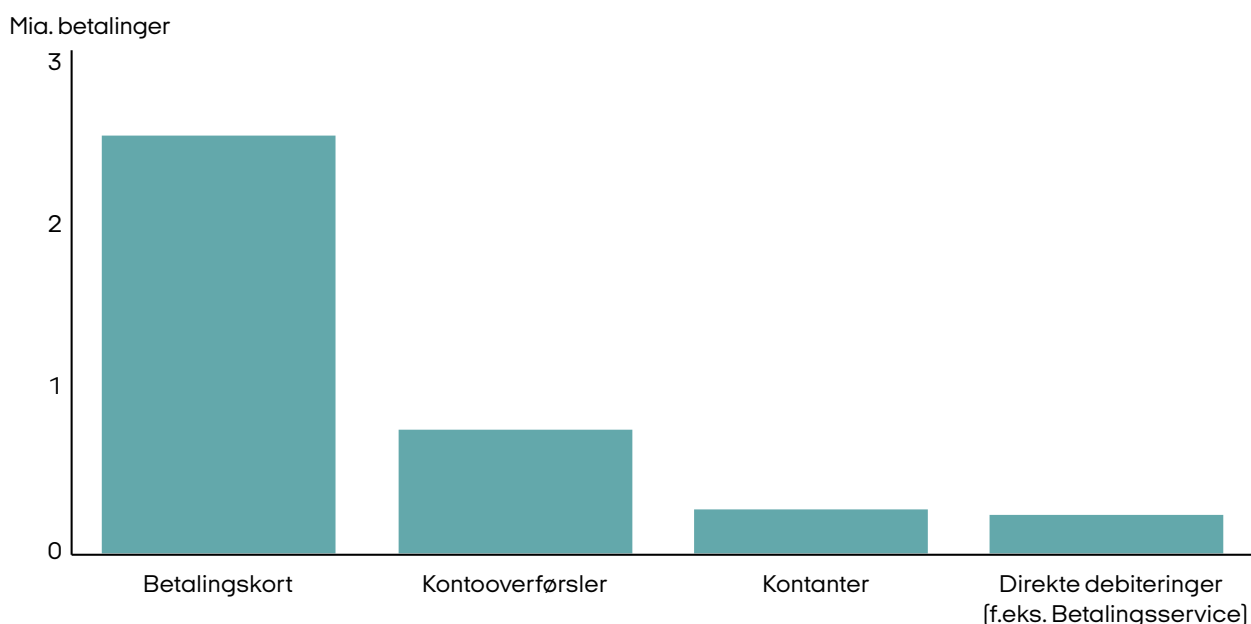
Begreber der bruges om betalinger

Betalingstjenester er den aktivitet, som medvirker til at flytte penge fra en betaler til en betalingsmodtager. Udbyderen af en betalings-tjeneste formidler en betaling imellem to parter, uden at aktøren selv er en del af den aftale, som betalingen beror på. En kontooverførsel og Betalingsservice er eksempler på betalingstjenester.

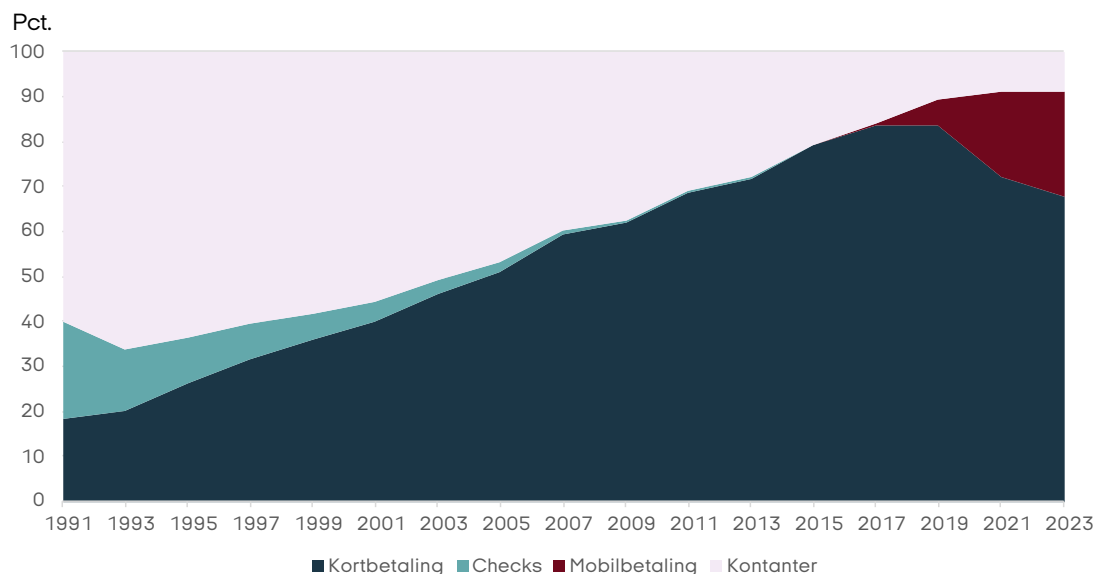
Betalingsinstrumenter giver indehaveren mulighed for at overføre penge til en anden part, f.eks. via et betalingskort eller net- og mobilbank. Digitale betalingsinstrumenter er dermed et redskab, der giver adgang til instrumentholderens betalingskonto i en bank.

Betalingsløsninger bruges i denne rapport som en samlet betegnelse for betalingstjenester, betalingsinstrumenter og teknologi. Eksempler er betalingskort fra Dankort, Mastercard og Visa, wallet-løsninger som Apple Pay og Google Pay samt mobilbetalingsløsninger som MobilePay.

Borgernes samlede betalinger i 2023



Omsætning i fysiske butikker fordelt på betalingsløsninger



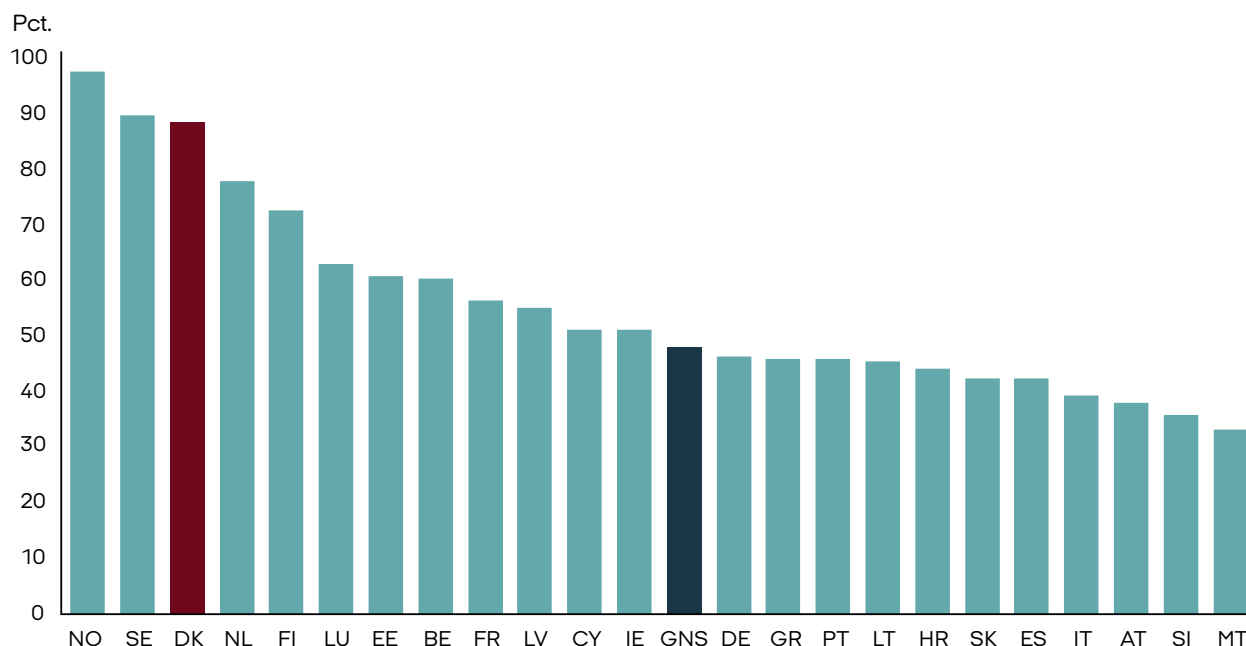
Kilde: Nationalbanken

I den fysiske handel har udviklingen i brugen af betalingsløsninger været kendetegnet ved et skifte fra checks og kontanter til kontaktløse kortbetalinger og mobilbetalinger. I 2023 skete 91 procent af omsætningen i fysiske butikker med digitale betalingsløsninger, mens kun 9 procent foregik med kontant betaling. Butikker i fysisk handel har som udgangspunkt pligt til at tage imod kontanter i dagtimerne, og udviklingen mod færre

kontantbetalinger har derfor været drevet af, at forbrugerne har valgt de digitale løsninger til.

Danmark er sammen med de øvrige nordiske lande i toppen blandt europæiske lande, når det gælder antallet af digitale betalinger i fysisk handel – kun overgået af Norge og Sverige.

Andel af digitale betalinger i fysisk handel



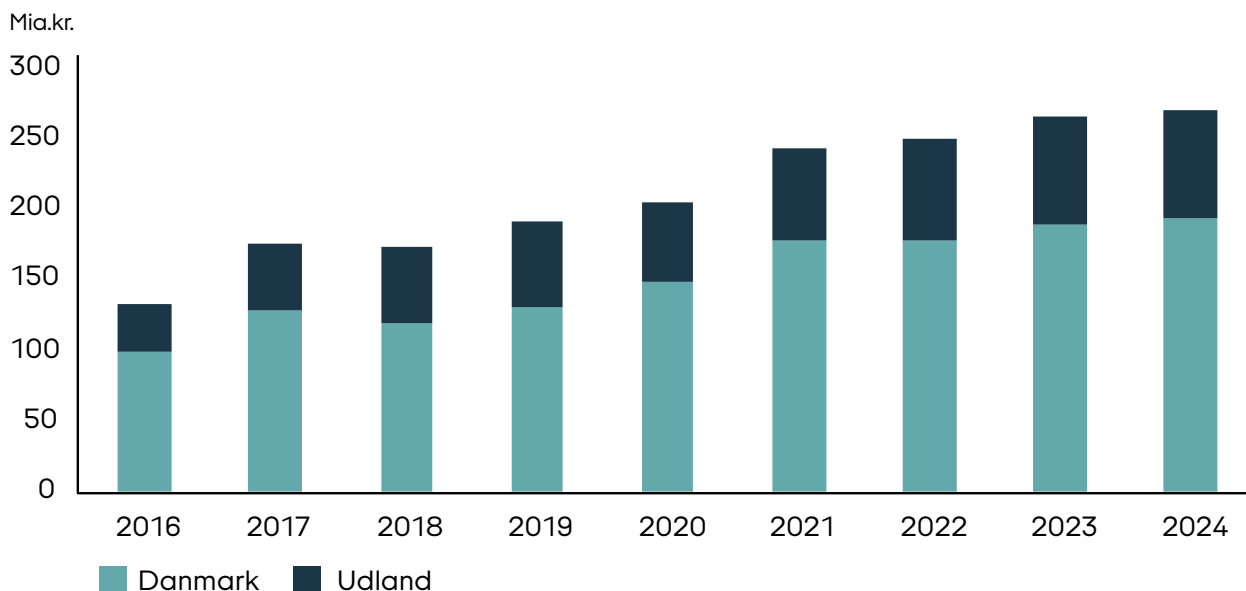
Kilde: Nationalbanken

Langt hovedparten af kortbetalinger i Danmark sker med Dankort (inklusive co-brandede Dankort), Mastercard og Visa. De seneste år har brugen af internationale kort været stigende og udgjorde i 2024 en større andel af den samlede kortomsætning end Dankort. Det skyldes bl.a., at betalinger med Apple Pay og Google Pay indtil nu fortrinsvist er sket ved brug af internationale kort. Ved udgangen af 2024 udgjorde wallet-betalinger i den fysiske handel som Apple Pay, MobilePay og Google Pay

knap 40 pct. af alle kortbetalinger foretaget i den fysiske handel.

Ud over den stigende digitalisering af betalinger i den fysiske handel er der de seneste år sket en betydelig vækst i onlinehandel, hvor betalingen typisk sker med kort. Handlen på nettet udgør en voksende andel af den samlede kortomsætning og var i 2024 på 272 mia. kr., hvilket er mere end en fordobling siden 2016.

Kortomsætning på internettet med brug af betalingskort



Anm: Figuren viser kortomsætningen på internettet med dansk udstedte betalingskort.
Kilde: Nationalbanken

MobilePay blev lanceret i 2013 og siden har det været muligt at anvende mobiltelefonen til at overføre penge til andre privatpersoner og senere også til at betale i butikker og på webshops. Løsningen er populær og over 4,5 millioner brugere, og omkring 200.000 butikker og webshops i Danmark tager imod MobilePay. Betalinger med MobilePay i detailhandelen sker i dag primært ved brug af QR-koder. MobilePay har i november 2025 – i samar-

bejde med bankerne – begyndt udrulningen af kontaktløse betalinger, hvor betalingen sker på samme måde som med kontaktløst kort eller wallets, som f.eks. Apple Pay og Google Pay. Den underliggende gennemførelse af betalingen er i første omgang baseret på et betalingskort, men senere bliver det muligt at gennemføre kontaktløse MobilePay-betalinger som en kontooverførsel.



2.2

Betalingsmarkedet bygger på en velfungerende teknisk infrastruktur og tæt samarbejde

Selvom en digital betaling virker enkel, kræver den en velfungerende teknisk infrastruktur og et tæt samarbejde mellem flere aktører i en nøje koordineret proces. Overførslen er mulig gennem betalingsinfrastrukturen, der består af en kompleks samling af centrale systemer, brugergrænseflader mellem forskellige aktører, omfattende aftaler, regler og tekniske standarder. I det følgende beskrives kortbetalinger, kontooverførelser og kontanter, samt relevante aktører og systemer på betalingsmarkedet.

Kortbetalinger er komplekse og omfatter adskillige aktører

De centrale aktører i forhold til kortbetalinger er kortholder, kortudsteder, kortindløser og betalingsmodtager samt kortselskabet. Hertil kommer en række andre aktører, der leverer den nødvendige teknologi og infrastruktur, der gør det muligt at overføre midler fra betaler til betalingsmodtager via betalingskort. Det er f.eks. terminalleverandører i fysiske butikker og betalingsgateways på internettet samt processorer, som sammen med kortindløser i denne rapport betegnes som "centrale tekniske aktører".

Ud over betalinger med fysiske betalingskort gennemføres betalinger med Apple Pay og Google Pay også som en kortbetaling. Betalinger med MobilePay på internettet sker også typisk ved brug af en kortbetaling.

Roller og aktører på betalingsmarkedet



Centrale aktører i et betalingskortsystem



Kortselskabet ejer kortsystemet og de forbundne rettigheder. De mest kendte kortselskaber i Danmark er Visa, Mastercard og Nets, som ejer Dankortet. Kortselskaberne opstiller de regler, som kortudstedere og -indlødere skal overholde for at være en del af kortsystemet. I tillæg til kortselskabernes regler skal alle, der er i berøring med kortdata, også overholde kravene i Payment Card Industry Data Security Standard [PCI DSS]. Det er sikkerhedsstandarder, der gælder for alle kortbetalinger. Selvom kortmærkerne repræsenterer forskellige netværk og systemer, behandles kortbetalinger i vid udstrækning af de samme aktører. Ligesom de anvender den samme underliggende infrastruktur.



Kortholder er den, som betalingskortet er udstedt til. Kortholder kan benytte kortet til at betale for varer eller tjenester. Kortholder er typisk en almindelig forbruger.



Kortudsteder udsteder betalingskort til kortholder. Kortudsteder indgår en aftale med kortselskabet for at få licens til at udstede kortene fra kortselskaberne. Licensen giver tilladelse til at benytte kortselskabets kortsystem og mærke. Kortudsteder er typisk banker, men de kan også være andre virksomheder.



Kortindløser indgår ligesom kortudstederen en aftale med kortselskabet og opnår derved en licens til at behandle betalinger med kortselskabets betalingskort på vegne af en betalingsmodtager. Det er kortindløseren, der sørger for, at kortbetalinger bliver godkendt på betalingsterminalen, dvs. søger om autorisation og godkendelse af betalingen hos kortholderens kortudstedende bank og kortselskabet, og at pengene fra kortholderens konto i sidste ende bliver overført til betalingsmodtageren. I Danmark er Nets den største kortindløser. Nets er p.t. den eneste kortindløser, som tilbyder indløsning af betalinger med Dankort, mens der findes flere kortindlødere, som tilbyder indløsning af betalinger med internationale betalingskort, som Mastercard og Visa. Det gælder f.eks. Swedbank Pay og Wordline. Den 1. juli 2025 trådte en ændring af lov om betalinger i kraft, der gør det muligt, at der kan komme flere indlødere af Dankortet end Nets.



Betalingsmodtager er en erhvervsdrivende (typisk en forretning), som indgår en indløsningsaftale med en eller flere kortindlødere for at kunne modtage betalinger med betalingskort.



Udbydere af wallet-løsninger gør det muligt, at kortbetalinger kan foretages via mobilen. Det er f.eks. Apple og Google. Når kortholder tilknytter sit betalingskort til en wallet, skabes der en unik kode også kaldet en token, der kan bruges til betaling. En token er en digital og krypteret udgave af betalingskortet, som opbevares i wallet-løsningen, og som er med til at beskytte betalingsoplysningerne. Når wallet-løsningen bruges, sendes token til kortindløseren og kortselskabet. Kortselskabet dekrypterer kortoplysninger fra token og sender informationen til godkendelse hos det kortudstedende pengeinstitut. Men ellers fungerer det på samme måde som betalinger med fysiske kort.



Processorer gennemfører tekniske funktioner i forbindelse med kortbetalinger. Både kortindløser og kortudsteder kan gøre brug af en processor. For kortindløser hjælper processoren med at indsamle og videresende kortoplysningerne i kortnetværket. Det er fx Nets og Swedbank Pay. For kortudsteder bistår processoren blandt andet med sikkerhedstiltag og monitorering af transaktioner. Det er fx Nets og Worldline. Kortudstederen kan f.eks. tillade, at processoren ud fra fastsatte parametre kan godkende korttransaktioner i tilfælde hvor kortudstederens systemer ikke svarer.



Leverandører af kortterminaler og betalingsgateways leverer teknologi og tjenester, der gør det muligt for butikker i fysisk handel og online at modtage kortbetalinger. Dette inkluderer levering af terminaler, teknisk support mv. Betalingsgateways varetager tilsvarende opgaver for butikker ved internethandel, dvs. forbinder webshops med kortindlødere. I Danmark er leverandører af kortterminaler og kortindlødere ofte den samme aktør. Det gælder f.eks. Nets og Verifone.

Mange aktører er involveret i en kortbetaling



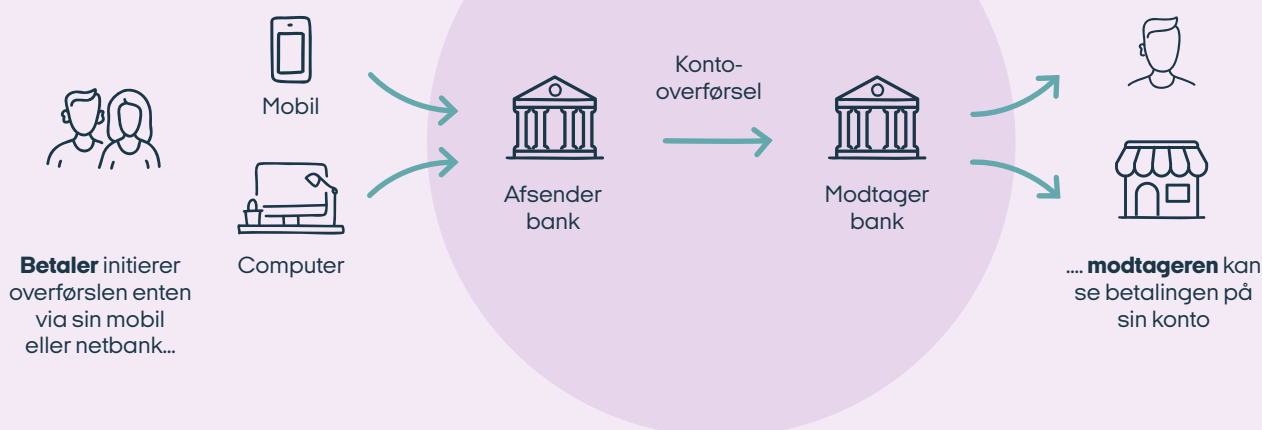
Gennemførelsen af kortbetalinger bliver i vid udstrækning varetaget af de samme aktører. Ved Dankort-betalinger varetager eksempelvis Nets både rollen som terminalleverandør, kortindløser, ejer af Dankort [kortselskab] og processor for både kortindløserne og kortudstedende banker. Nets er p.t. den eneste indløser af Dankort-betalinger og er generelt den største kortindløser med en markedsandel på ca. 75-80 pct. af det samlede antal kortbetalinger indløst i Danmark. Samtidig behandles hovedparten af alle kortbetalinger i Danmark via Nets' systemer. Det sker i deres rolle som processor for både kortindløserne og kortudstedende og er uafhængigt af hvilken kortindløser, der indløser kortbetalingen. Det skyldes, at Nets er den eneste processor af Dankort-betalinger og samtidig er processor for hovedparten af betalinger med internationale kort. Hvis Nets i disse roller rammes af forstyrrelser, vil det kunne have store konsekvenser for kortbetalingsmarkedet. Det er derfor vigtigt at sikre de rigtige rammer for, at både rollen som indløser og processor kan varetages af flere forskellige aktører.

Derudover cleares alle korttransaktioner i samme system, som Mastercard Payment Services ejer og driver. Driftsforstyrrelser i denne del af kortinfrastrukturen vil potentielt påvirke transaktioner med alle de forskellige kortbetalingsmærker, herunder Dankort, Visa og Mastercard, og dermed have vidtrækkende konsekvenser. Hvis imidlertid kun ét kortselskab er ramt af driftsforstyrrelser, vil det stadig være muligt at anvende betalingskort fra de to andre mærker. Tilstedeværelsen af tre udbredte kortmærker fra de forskellige kortselskaber bidrager derfor alt andet lige til øget robusthed af kortbetalingerne i Danmark.

Kontooverførsler benytter en mere enkel infrastruktur med færre aktører

Kontooverførsler anvender en anden infrastruktur end kortbetalinger og involverer færre aktører. En kontooverførsel sker direkte mellem betalers bank til modtagers bank via clearing- og afviklingssystemerne.

Færre aktører er involveret i en kontooverførsel



Infrastrukturen bag kontooverførsler udvikles løbende, og Danmark var et af de første lande i verden til at introducere straksbetalinger i 2014. Straksbetaling betyder, at modtageren får pengene ind på kontoen få sekunder efter overførslen er foretaget og kan foretages døgnet rundt alle årets dage. Straksbetalinger har betydet en klar forbedring af forbrugerne og virksomhedernes mulighed for hurtigt at få betalt deres regninger, overføre penge eller hurtigt dele en regning. Straksbetalinger sker via systemet TIPS-DKK og supplerer overførsler via Intradagclearingen, som sker inden for samme dag eller til næste dag.

I Danmark foretages kontooverførsler primært via netbank eller mobilbank og bruges f.eks. til betaling af regninger og til overførsler mellem privatpersoner. Ved MobilePay-betalinger mellem privatpersoner og til forretninger i den fysiske handel er den underliggende betaling typisk en straksbetaling, som gennemføres med det samme fra betalers bankkonto til modtagers bankkonto. MobilePays nye kontaktløse betalingsløsning i den fysiske handel kan på sigt også anvende kontooverførsler, som den underliggende betalingsinfrastruktur.

Kontooverførsler bruges i mindre omfang til onlinekøb, da f.eks. kortbetalinger her ofte vil være mere brugervenlige og forbundet med andre forbrugerrettigheder. Men kontooverførsler via net- eller mobilbank vil i en nedbruds- eller krisesituation kunne anvendes som supplement, hvis kortbetalinger ikke fungerer. De bidrager også til robustheden, da kontooverførsler som beskrevet ovenfor

kan håndteres via to systemer og har en anden infrastruktur end kortbetalinger. MobilePay-betalinger mellem privatpersoner sker som en kontooverførsel og vil ligeledes være et supplement, f.eks. hvis én privatperson ikke kan anvende sit betalingskort og i stedet overfører et beløb til en anden privatperson, som godt kan anvende sit betalingskort. Derfor indgår begge betalingssituationer i rapportens undersøgelser. En velfungerende, robust og sikker infrastruktur er ligeledes fundamentet for en yderligere udbredelse af mobilbetalingsløsninger baseret på kontooverførsler – både i Danmark, Norden og EU.

Samarbejde mellem europæiske mobilbetalingsløsninger

I september 2025 har en række europæiske mobilbetalingsløsninger, herunder Vipps MobilePay, annonceret et samarbejde om at sikre samspil mellem de forskellige løsninger baseret på europæisk infrastruktur og standarder. Det vil gøre det muligt for brugerne at lave straksbetalinger på tværs af både grænser og de forskellige løsninger. Både når de skal handle i butikker og online samt overføre penge mellem privatpersoner.

Kontanter er et supplerende beredskab

Kontantinfrastrukturen er løbende tilpasset den nedadgående efterspørgsel. Det gælder både i forhold til Nationalbankens produktion af kontanter, kontantselskabernes videreformidling og bankernes udbud af kontant-tjenester. Nationalbanken vurderer, at den nuværende adgang til udbetaling af kontanter er dækkende.

Spørgeundersøgelser fra Nationalbanken viser, at mange borgere lægger vægt på kontanter som et beredskab, hvis andre løsninger ikke virker. Det skal ses i sammenhæng med, at kontanter er fysiske og analoge, og kontantbetalinger dermed kan foretages uden kontakt med bagvedliggende digitale systemer.

Nationalbanken vurderer, at kontanter kan fungere som et supplerende beredskab, men ikke et samfunds-dækkende beredskab. For at kontanter kan fungere som et supplerende beredskab ved nedbrud kræver det, at borgerne har dem anskaffet før nedbruddet sker, da de ikke nødvendigvis kan forvente at kunne benytte kontantautomater i en situation, hvor kort- og mobilbetalinger ikke virker. Det er baggrunden for, at Nationalbanken anbefaler, at borgere bør have et mindre beløb i kontanter og angiver et pejlemærke på 250 kr. pr. person i husstanden. Samtidig bør hver husstand vurdere, hvorvidt der er behov for at have et større kontantbeløb til rådighed. Finans Danmark støtter Nationalbankens anbefaling.

Nationalbanken peger på store investeringer, hvis kontanter skal bruges som mere end et supplerende beredskab

Nationalbanken vurderer, at kontanter godt kan fungere som et supplerende beredskab for den enkelte borger, men er i praksis ikke et effektivt betalingsberedskab på et samfundsmæssigt niveau. Det vil kræve betydelige investeringer, hvis kontanter skal løftes til et selvstændigt beredskab i de situationer, hvor de digitale betalingsløsninger ikke fungerer på normal vis. Det indebærer blandt andet en national beredskabsplanlægning, investering i større kontantreserver hos virksomheder, husholdninger, den finansielle sektor og Nationalbanken, ligesom der skal være en ekstra kapacitet hos kontanthåndteringsselskaberne til at transportere kontanterne til og fra butikker, banker, kontantautomater mv. Derudover vil det kræve, at man både udvikler og implementerer offline-funktionalitet i kontantautomater samt øger antallet af kontantautomater, særligt i de større byer.

Nationalbanken vurderer derfor, at omkostningerne til etablering af et samfunds-dækkende kontantberedskab ikke står mål med gevinsterne, set i forhold til, at der er gode forudsætninger for, at danskerne kan foretage offline-betalinger med deres betalingskort, selv hvis betalingssystemerne er forstyrret. Finans Danmark er enig i denne vurdering.

Forskellige centrale systemer håndterer betalingerne

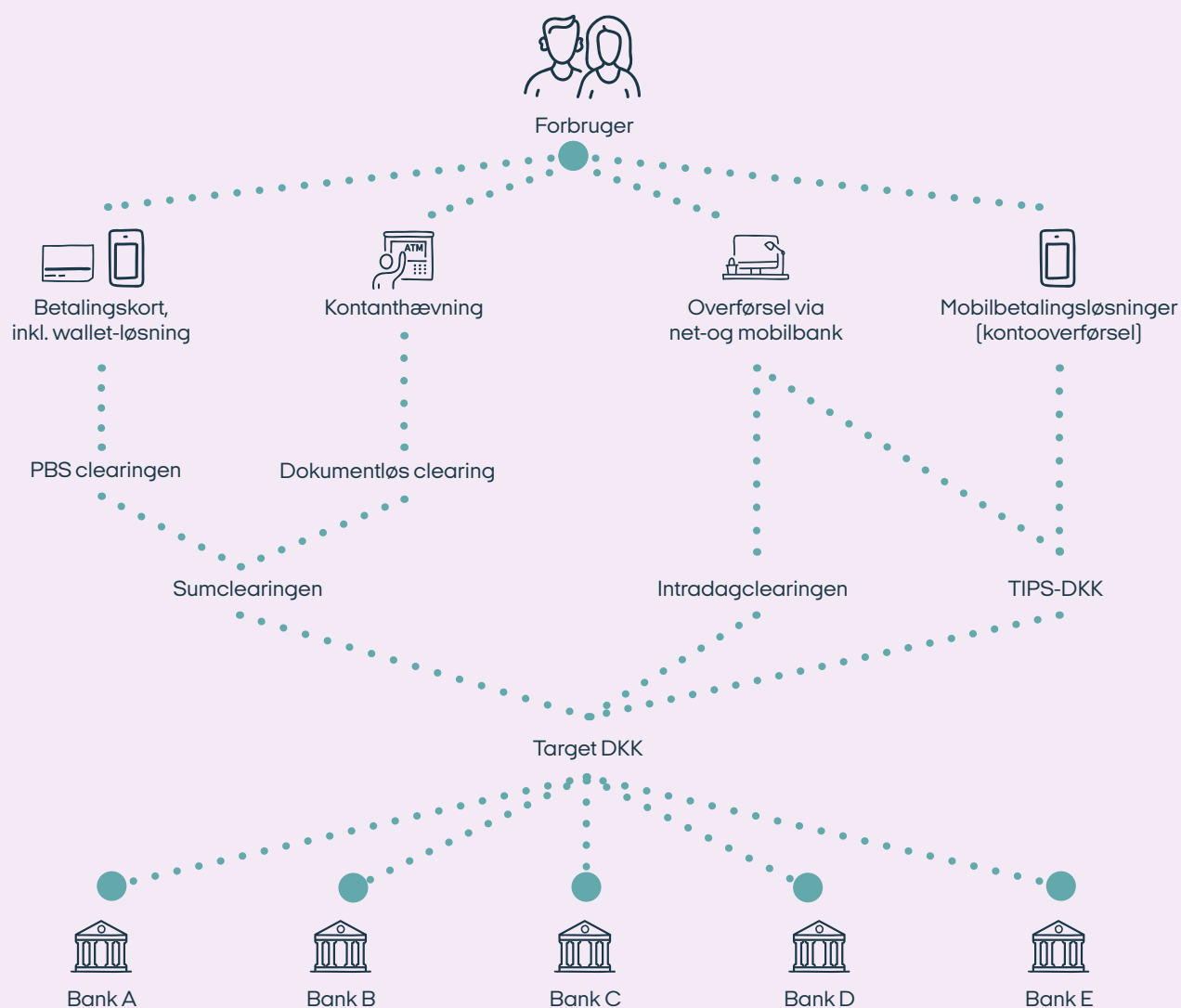
Den valgte betalingsløsning bestemmer, hvilket underliggende betalingssystem, der benyttes. PBS-clearingen bruges blandt andet til betalinger med Dankort, internationale betalingskort og Betalingsservice, mens den dokumentløse clearing blandt andet anvendes til afregning af indbetalingskort og kontanthævninger i pengeautomater. Sumclearingen samler beløb fra den dokumentløse clearing og PBS-clearingen, og Sumclearingen behandler dermed kortbetalinger, wallet-løsninger, og kontanthævninger. Sumclearingen, inkl. den dokumentløse clearing, ejes af Finans Danmark på vegne af de danske banker, mens Mastercard Payment Services ejer PBS clearingen samt er operatør af alle tre systemer.

Intradagclearingen gør det muligt at lave en kontooverførsel inden for samme dag eller til næste dag. Alle transaktioner opgøres og afstemmes flere gange i døgnet. Intradagclearingen ejes ligeledes af Finans Danmark på vegne af de danske banker, og Mastercard Payment Services er operatør af systemet. Som det beskrives nedenfor, er en modernisering af Intradagclearingen samt dele af Sumclearingen igangsat.

Hver eneste straksbetaling afvikles enkeltvis og øjeblikkeligt i TIPS-DKK. Deltagere i TIPS-DKK [typisk banker] overfører likviditet til en konto i TIPS-DKK, hvorfra der sker en overførelse mellem afsenderbank og modtagerbank, hver gang der foretages en straksbetaling. TIPS-DKK er en del TARGET DKK, og Nationalbanken er systemejer for TIPS-DKK.

Nationalbankens afviklingssystem for betalinger og værdipapirhandler samt Nationalbankens system for sikkerhedsstillelse går under betegnelsen TARGET DKK. Afviklingssystemet for betalinger og værdipapirhandler er baseret på den Europæiske Centralbanks fælleseuropæiske platform for afvikling af betalinger og værdipapirhandler, TARGET Services. Når transaktioner er opgjort og afstemt i henholdsvis Sumclearingen og Intradagclearingen, afvikler banker deres indbyrdes mellemværender på konti i TARGET DKK. Nationalbanken er systemejer af TARGET DKK og har indgået aftale med ECB om brugen af TARGET Services.

Overblik om betalingsløsninger og betalingssystemer



Finanssektoren moderniserer betalingsinfrastrukturen

Finans Danmark og bankerne arbejder på en modernisering af Sumclearingen og Intradagclearingen for at understøtte en fortsat robust og sikker infrastruktur. Senest i begyndelsen af 2027 forventes der at blive igangsat en ny clearing til kontooverførsler, som vil være baseret på formater, som også bliver brugt i Norden og i forbindelse med euro-betalinger. Dermed vil betalinger i danske kroner bruge de samme formater som de øvrige nordiske valutaer og euro.

Dette vil give et fælles fundament, som styrker mulighederne for udviklingen af betalingsløsninger.

Som et led i arbejdet er der underskrevet et letter of intent med den europæiske virksomhed EBA CLEARING om et nyt clearingsystem, som afløser for Intradagclearingen. Med den nye løsning vil Intradagclearingen blive løftet til en standard-plattform baseret på europæiske standarder.

2.3

Tiltag der understøtter en høj robusthed på betalingsmarkedet i Danmark

Nationalbanken vurderer, at Danmark har en sikker, effektiv og stabil betalingsinfrastruktur. De enkelte aktører på betalingsmarkedet arbejder både individuelt og sammen om at styrke deres robusthed, herunder mod cyberangreb. Det understøttes både af love, myndigheder samt en række samarbejder og initiativer. Senest har aktørerne implementeret DORA-forordningen, som skal styrke den digitale, operationelle modstandsdygtighed i den finansielle sektor.

Der gælder et overordnet princip om sektorsansvar ved håndteringen af robusthed og forberedelsen af beredskabssituationer i Danmark. Det betyder, at myndigheder fordelt på sektorer selv bærer ansvaret for beredskabet i deres egen sektor. Ved større hændelser kan det nationale krisestyringssystem derudover aktiveres.

For den finansielle sektor er det følgende myndigheder, som løfter sektoransvaret:

Erhvervsministeriet

Ministeriet har det overordnede ansvar for rammevilkårene i den finansielle sektor. Erhvervsministeren har i forbindelse med den politiske aftale om styrkelse af Dankortet fra juni 2025 annonceret, at ministeren inden udgangen af 2026 vil gennemføre en evaluering af den danske betalingsinfrastrukturens robusthed.

Finanstilsynet

Tilsynet er en styrelse under Erhvervsministeriet, som fører tilsyn med, at virksomheder overholder den finansielle lovgivning, herunder DORA, lov om finansiell virksomhed og lov om betalinger. Finanstilsynet gennemfører årligt en undersøgelse af danske finansielle virksomheders opfattelse af aktuelle risici og af deres tillid til det finansielle system i Danmark. Undersøgelsen for 2025 viser, at virksomhederne anser cybertrusler og geopolitiske forhold som de største kilder til risiko for den finansielle stabilitet i Danmark. I 2024 gennemførte Finanstilsynet sammen med syv virksomheder også sin første cyberstresstest med det formål at undersøge virksomhedernes evne til at håndtere omfattende nedbrud.

Nationalbanken

Nationalbanken overvåger de centrale danske betalings- og afviklingssystemer (blandt andet TARGET DKK, Sum- og Intradagclearingen) samt de vigtigste betalingsløsninger (Dankort, Betalingsservice og kontooverførsler). Overvågningen er baseret på internationale standarder og principper og bidrager til at sikre robustheden i betalingsinfrastrukturen. Nationalbanken indsamler også statistik og analyserer løbende strukturerne og dynamikkerne på detailbetalingsmarkedet, herunder udviklingen i borgernes betalingsadfærd og -præferencer.

I tillæg til de finansielle sektormyndigheder er der en række myndigheder med et tværgående ansvar for beredskab i Danmark, som beskrives i boks på side 26.

Love der understøtter høj robusthed og sikre betalingsløsninger

DORA – Forordning om digital operationel modstandsdygtighed

I januar 2025 trådte en ny EU-forordning om digital operationel modstandsdygtighed, DORA, i kraft. DORA har til formål at styrke den digitale, operationelle modstandsdygtighed i den finansielle sektor og stiller blandt andet krav til organisering, risikostyring og kontroller samt test af cybersikkerheden, herunder såkaldte trusselsbaserede tests, og indberetning af it-relaterede hændelser.

Som en del af risikostyringen skal de finansielle institutter beskytte alle relevante fysiske komponenter og infrastrukturer, såsom lokaler og datacentre. De finansielle institutter skal også kortlægge processer og definere hvilke it-systemer, som er vigtige og kritiske, og derudover afdække, hvor hurtigt funktioner skal kunne reetableres efter et nedbrud. Der er samtidig krav om dokumentation og risikostyring af samarbejdspartnere, der leverer kritiske komponenter til de aktører, der er omfattet af DORA.

DORA stiller ikke bare krav til forbedret cyberbeskyttelse og -sikkerhed, men også store krav til operationel modstandsdygtighed når og hvis, hændelser forekommer. For de omfattede finansielle institutter, som blandt andet er kreditinstitutter, betalingsinstitutter og e-pengeinstitutter, kræver DORA dermed investeringer.

Lov om finansiell virksomhed

Lov om finansiell virksomhed stiller blandt andet krav til operatører af finansielle digitale infrastrukturer. Det er eksempelvis IT-operatører af detailbetalingssystemer og virksomheder, der udfører væsentlig drift eller udvikling for den fælles betalingsinfrastruktur. Loven stiller blandt andet krav til styring af it- og cyberrisici, indberetning af it- og cyberhændelser, løbende trusselsbaserede tests og styring af tredjepartsrisici. Finanstilsynet har bl.a. udpeget de tre bankdatacentraler Bankdata, BEC og Net-company Banking Services samt Mastercard Payment Services som operatører af finansiell digital infrastruktur.

Lov om betalinger

Lov om betalinger regulerer udbuddet og brugen af betalingstjenester. Loven indeholder tilladelseskrav til udbydere af betalingstjenester (f.eks. krav om risikovurdering af betalingstjenester), sikkerhedskrav (f.eks. krav om to-faktor godkendelse ved elektroniske betalinger) og forbrugerbeskyttelse (f.eks. ved svindel med betalinger). Kreditinstitutter, betalingsinstitutter og e-pengeinstitutter kan udbyde betalingstjenester.

Loven implementerer 2. betalingstjenestedirektiv (PSD2), men indeholder også en række danske særregler. Det er f.eks. regler om Dankortet, der fastsætter hvor meget en betalingsmodtager i den fysiske handel skal betale for at tage imod betalinger med Dankort. Den 1. juli 2025 trådte en ændring af lov om betalinger i kraft der muliggør, at der kan komme flere indlødere af Dankortet end Nets.





Samarbejde og initiativer, der styrker robustheden

Systemerne på betalingsmarkedet er tæt forbundne, og aktørerne på betalingsmarkedet deltager derfor sammen med andre dele af den finansielle sektor i en række samarbejder, som skal styrke betalingsmarkedets robusthed

Finansielt Sektorforum for Operationel Robusthed

Finansielt Sektorforum for Operationel Robusthed, FSOR, er et offentlig-privat samarbejdsforum i den finansielle sektor. Formålet er at øge den operationelle robusthed på tværs af sektoren, herunder robustheden over for cyberangreb. Der er i FSOR etableret en risikovurdering af relevante tværgående risici i sektoren samt et kriseberedskab på sektorniveau, som supplerer FSOR medlemmernes egne kriseplaner og det nationale kriseberedskab. Formålet med FSOR-kriseberedskabet er at koordinere indsatsen, hvis der opstår en operationel hændelse, der potentielt kan påvirke den finansielle stabilitet. FSOR-kriseberedskabet testes jævnligt for at sikre, at det fungerer i praksis.

FSOR ledes af Nationalbanken og har deltagelse af de væsentligste aktører i den danske finansielle sektor.

TIBER-DK programmet

Siden 2019 har Nationalbanken faciliteret og koordineret trusselsbaserede test under TIBER-DK-programmet. TIBER står for Threat Intelligence-Based Ethical Red-teaming og er udviklet af Den Europæiske Centralbank, ECB. TIBER-DK henviser til den danske nationale implementering. I TIBER-DK-programmet testes de deltagende finansielle virksomheders cyberforsvar med udgangspunkt i virkelige hackergruppers faktiske taktikker, teknikker og procedurer. Formålet er, at virksomhederne bliver klogere på egne styrker og svagheder i deres cyberforsvar, og testene bidrager dermed med vigtig læring om at modstå avancerede cybertrusler. I TIBER-DK er DORA's krav til trusselsbaserede test indbygget.

Nordic Financial CERT

Nordic Financial CERT, forkortet NFCERT, er et samarbejde mellem de nordiske banker, der har til formål at styrke finanssektorens modstandsdygtighed over for cybertrusler og -angreb. CERT er en forkortelse for Computer Emergency Response Team, og NFCERT er en operativ kapacitet i forhold til forsvar mod og bekæmpelse af cybertrusler. NFCERT stiller en platform til rådighed, som gør det muligt for medlemmerne at samarbejde om håndtering af cyberkriminalitet, dele information og reagere på trusler på en koordineret måde.

Cyberalliancen

Cyberalliancen er et samarbejde mellem flere sektorer, herunder Finans Danmark, Teleindustrien, Danske Re-derier, Dansk Energi, DANVA samt Forsikring og Pension. Formålet med Cyberalliancen er at skabe en fælles national indsats for at styrke cyber- og informationssikkerheden samt beredskab i de samfundskritiske sektorer.

Strategi for cybersikkerhed i den finansielle sektor [2022–2025]

Strategien har til formål at beskytte den kritiske IT-infrastruktur i finanssektoren og sikre, at sektoren kan opretholde drift og genoprettes under kriser. Strategien understøtter samarbejdet internt i sektoren og på tværs af samfundsvigtige sektorer og er forankret i Finanstilsynet. Den udspringer af den nationale cyber- og informationssikkerhedsstrategi. Som led i strategien er der etableret en decentral enhed for cyber- og informationssikkerhed i finanssektoren – kaldet DCIS, forankret i Finanstilsynet. DCIS bygger videre på eksisterende samarbejder i Finansielt Sektorforum for Operationel Robusthed [FSOR] og Nordic Financial CERT [NFCERT], som begge bidrager til enhedens opgaveløsning. DCIS samarbejder også med de øvrige 25 samfundsvigtige sektorer, herunder energi, sundhed, transport og tele.

Cybersikkerhedsrådet

Cybersikkerhedsrådet er et offentlig-privat organ, der rådgiver regeringen om, hvordan Danmarks digitale sikkerhed kan styrkes. Rådet bidrager til udviklingen af den nationale cyber- og informationssikkerhedsstrategi, fremmer viden om cybersikkerhed og understøtter videndeling mellem myndigheder, erhvervsliv og forskningsverden. Rådet fungerer også som advisory board for Cybersikkerhedspagten.

Medlemmerne repræsenterer bred faglighed fra både offentlige og private aktører, herunder eksperter fra finanssektoren, energisektoren, telesektoren, IT-branchen, universiteter, kommuner og store virksomheder som Novo Nordisk og TDC.

Cyberpagten

Cyberpagten er et offentligt-privat samarbejde, der skal styrke cybersikkerheden i danske virksomheder – især SMV'er. Den samler aktører som Erhvervsministeriet, Digitaliseringsministeriet, Finans Danmark, Dansk Industri, IT-Branchen og SMVdanmark. Fokus er på kompetenceudvikling, trusselsvarsling og mærkningsordninger som D-mærket.

Erhvervspartnerskabet for beredskab

Under Ministeriet for Samfundssikkerhed og Beredskab er der etableret et erhvervsforum med deltagelse af 21 store virksomheder og organisationer. Formålet er at styrke beredskabet og samfundssikkerheden gennem samarbejde om forsyningssikkerhed, cybersikkerhed og robust infrastruktur. Deltagere inkluderer bl.a. A.P. Møller-Mærsk, Novo Nordisk, Nordea og Finans Danmark.

Operativt Erhvervsnetværk for Samfundssikkerhed

Det Operative erhvervsnetværk for samfundssikkerhed er etableret af Ministeriet for Samfundssikkerhed og Beredskab og ledes af Styrelsen for Samfundssikkerhed. Formålet er at skabe et fortroligt forum, hvor myndigheder og sikkerhedsgodkendte repræsentanter fra erhvervslivet kan dele viden om trusler mod samfundssikkerheden – f.eks. cybertrusler, forsyningssikkerhed og kritisk infrastruktur. Deltagerkredsen forventes at være på plads i starten af 2026.

2.4

Alle aktører bør være forberedt på nedbrud og have et effektivt beredskab

Det er ikke muligt at forhindre alle angreb, selvom der løbende lægges en stor indsats i arbejdet med cybersikkerhed og robusthed. Det er derfor vigtigt, at alle aktører arbejder med beredskaber, der kan håndtere konsekvenserne af eventuelle angreb, der ikke har kunnet afværges. Det gælder både for borgere, erhvervsdrivende, aktører på betalingsmarkedet og myndigheder.

Styrelsen for Samfundssikkerhed har i 2024 udarbejdet pjecen "Forberedt på kriser" med anbefalingen om, at en husstand skal kunne klare sig i tre døgn, hvis en krise rammer, og med råd til hvordan borgerne kan forberede sig på dette. Pjecen indeholder blandt andet råd om, at man bør have et eller flere fysiske betalingskort til brug, hvis internettet er nede, eller det ikke er muligt at betale med mobiltelefonen, og man bør kunne huske sine pinkoder. Det følger også af pjecen, at man bør overveje at have et mindre beløb i mønter og små sedler.

Myndigheder med tværgående ansvar for beredskab i Danmark

Ministeriet for samfundssikkerhed og beredskab

Ministeriet for Samfundssikkerhed og Beredskab (MSSB) blev oprettet i 2024 og har i et tæt samarbejde med de ansvarlige sektorer ansvaret for at forebygge, modstå og håndtere større ulykker, kriser, katastrofer og andre hændelser, der udfordrer samfundets grundlæggende funktioner. Det omfatter også at rådgive og kommunikere til myndigheder, virksomheder og befolkning. Som et eksempel på arbejdet kan nævnes, at ministeren i oktober 2025 inviterede dagligvarebranchen til et dialogmøde om, hvordan branchen og regeringen kan arbejde tættere sammen om bedre adgang til de mest grundlæggende fornødenheder på tværs af landet i krisesituationer, f.eks. i form af beredskabsbutikker.

Styrelsen for Samfundssikkerhed

Styrelsen for Samfundssikkerhed (SAMSIK) er en styrelse under MSSB, som beskæftiger sig med rådgivning og kommunikation til myndigheder, virksomheder og borgere om forebyggelse og håndtering af de trusler, samfundet står over for, herunder på cyber- og informationssikkerhedsområdet. SAMSIK har blandt andet ansvar for den nationale strategi for cyber- og informationssikkerhed, koordination af generel sikkerhed vedrørende kritisk infrastruktur og opgaver vedrørende koordination, herunder Den nationale operative stab (NOST). SAMSIK udgiver løbende trusselvurderinger, både generelle trusselvurderinger af cybertruslen mod Danmark, og trusselvurderinger af specifikke sektorer, som f.eks. finanssektoren.

Den nationale operative stab

Den nationale operative stab (NOST) træder sammen, når der opstår større kriser og hændelser i Danmark. NOST'en træder sammen for at styre og koordinere den operative indsats på tværs af myndigheder, og blev blandt andet samlet, da der i september 2025 var droneaktivitet ved Københavns Lufthavn. Staben ledes af Rigspolitiet og består herudover af SAMSIK, Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste, Forsvarskommandoen, Beredskabsstyrelsen, Udenrigsministeriet, Sundhedsstyrelsen og Trafikstyrelsen. Andre myndigheder kan indkaldes efter behov i forhold til hændelsens karakter, og eksempelvis deltog Nationalbanken på vegne af hele den finansielle sektor og FSOR ved droneaktiviteterne i september 2025.

Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste

Politiets Efterretningstjeneste (PET) indhenter, analyserer og formidler oplysninger om trusler mod Danmark og danske interesser, og PET skal modvirke de trusler, som efterretningsindsatsen identificerer. PET udgiver løbende trusselvurderinger og analyser, f.eks. vurderinger af spionagetruslen og terrortruslen mod Danmark.

Forsvarets efterretningstjeneste (FE) indhenter, analyserer og formidler oplysninger om forhold i udlandet, som har betydning for Danmark og danske interesse. FE udgiver løbende en række uklassificerede rapporter, herunder en årlig efterretningsmæssig risikovurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af Danmarks interesser⁸. FE udarbejder også løbende situations- og trusselvurderinger, som f.eks. en vurdering af den hybride trussel mod Danmark. Vurderingerne gør brug af følgende trusselsniveauer: ingen, lav, middel, høj og meget høj.

Nationalbanken offentliggjorde i oktober 2025 opdaterede anbefalinger til borgerne for et betalingsberedskab samt nye anbefalinger til de erhvervsdrivende i den fysiske handel. Nationalbanken anbefaler, at man som borger har mindst to fysiske betalingskort fra forskellige kortmærker i husstanden, et mindre beløb i kontanter (et pejlemærke er 250 kr. i kontanter pr. person i husstanden) og en mobilbetalingsløsning baseret på kontooverførsler som eksempelvis MobilePay. Endvidere anbefaler Nationalbanken, at de enkelte butikker i den fysiske handel på forhånd har planlagt, hvordan man vil håndtere situationer, hvor en eller flere betalingsløsninger ikke fungerer som normalt. Nationalbanken peger på, at det for mange butikker i den fysiske handel vil det være relevant at modtage offline-kortbetalinger og andre betalingsløsninger end betalingskort og kontanter. Uanset hvad planen er, er det vigtigt, at personalet kender planerne og kan udføre dem.

Kortbetalingsberedskabet

Medlemmerne i Betalingsrådet samarbejder om at sikre et betalingsberedskab med betalingskort i Danmark. Beredskabet skal minimere de samfundsmæssige konsekvenser, hvis det ikke er muligt at betale som normalt, f.eks. hvis en alvorlig hændelse forstyrrer betalingsinfra-

strukturen. I praksis betyder det, at der skal kunne foretages offline-kortbetalinger.

Den aktuelle status er, at mange butikker kan tage mod offline-kortbetalinger, og at mindst 82 pct. af voksne danskere har et fysisk betalingskort, der kan anvendes offline. Målsætningen er, at alle borgere over 18 år med betalingskort fra Dankort, Visa og Mastercard udstedt af en dansk bank skal kunne betale for medicin og dagligvarer i mindst en uge med deres fysiske betalingskort og betalingskort på mobilen, f.eks. via Apple Pay og Google Pay.

Implementeringen af beredskabet er ved at blive færdiggjort i de landsdækkende dagligvarekæder og på apoteker, og de sidste butikker forventes at have implementeret beredskabet senest i midten af 2026.

Kortbetalingsberedskabet skal kunne fungere i alle de nedbrudssituationer, hvor de involverede butikker fortsat sælger varer. Det vil forudsætte, at der er strøm, så butikken kan opretholde basale og praktiske funktioner, såsom at køle varer, benytte kasseapparater, have lys mv.

Betalingsrådet

I Betalingsrådet mødes nogle af de vigtigste aktører på betalingsområdet i Danmark. De udveksler viden og synspunkter om udviklingen i detailbetalinger på det danske betalingsmarked. Det er med til at skabe indsigt og gennemsigtighed i markedet, så forbrugere og virksomheder kan have tillid til, at betalinger foregår hurtigt og sikkert. Betalingsrådet består af 13 medlemmer. Nationalbanken varetager formandskabet for Betalingsrådet og rollen som sekretariat. Finans Danmark repræsenterer bankerne i rådet, som herudover består af repræsentanter fra Copenhagen Fintech, Dansk Erhverv, Dansk Industri, Erhvervsministeriet, Finanstilsynet, Forbrugerrådet Tænk, Mastercard, Nets, SMVDanmark, Vipps MobilePay og Visa.

Det danske betalingsmarked er et kompleks netværk af mange forskellige aktører og systemer, hvor lovgivning og relevante myndigheder sætter rammen for at sikre et robust betalingsmarked. På trods af allerede eksisterende

regler, samarbejder og beredskaber vil der være risiko for nedbrud. Det er naturligt, når vi lever i en digital og foranderlig verden, og næste afsnit identificerer de trusler og risici, som betalingsmarkedet skal forholde sig til.

3.

Identificerede trusler og risici



32 32 133 20 2 2 8 100 0 00 1
1 0 3 9 00 2 35 0 30 1 0 0 1 0 10 0 10
4 48 0 73 1 1 32 1 4 8 20 1 1 1 1 1 1 1 1
3 1 3 29 0 0 1 00 311 33 9 0 0 100 1 10 10
4 4 08 3 9 12 1 1 4 48 0 1 1 1 1 1 1 1 1 1

Aktørerne på betalingsmarkedet skal i stigende grad forholde sig til et trusselsbillede i konstant forandring, og det kan påvirke både den daglige drift og markedets samlede robusthed. Komplexiteten af det samlede økosystem, de mange aktører og deres indbyrdes afhængigheder gør, at det er nødvendigt kontinuerligt at fokusere på den samlede robusthed og om den er tilstrækkelig.

Der kommer der løbende nye trusler og risici til, der blandt andet kan henføres til den sikkerheds- og geopolitiske situation. Det bliver løbende fremhævet i trusselsvurderinger. Det er særligt risikoen for avancerede cyberangreb, stigningen i it-relateret økonomisk kriminalitet samt vejr- og klimaforandringer. Truslerne tager også form som hybride trusler, hvor fjendtlige handlinger ikke alene ses ved cyberangreb og klassiske it-angrebsmetoder, men også mere ukonventionelle handlinger som brandstiftelse, kabeloverskæringer, hærværk og desinformation. Det betyder blandt andet, at betalingsmarkedets aktører løbende også skal forholde sig til den fysiske sikring af bygninger, f.eks. datacentre, for at imødegå de nye trusler og risici.

På den baggrund kan der identificeres flere forskellige årsager til et potentielt nedbrud i betalingsmarkedet. Det ligger uden for denne analyse at undersøge det nærmere trusselsbillede. I stedet fokuseres uagtet trussel eller årsag på den direkte påvirkning af betalingsmarkedet, som disse trusler kan medføre, i form af de risici, som betalingsmarkedet og dets aktører skal forholde sig til. På tværs af forskellige trusler og potentielle nedbruds-scenarier, har denne analyse identificeret fire overordnede kritiske risici, som kan ramme det danske betalingsmarked.

Kritiske risici for betalingsmarkedet



Risiko 1

Strømsvigt

Stabil adgang til elektricitet er en central forudsætning for et velfungerende digitalt betalingsmarked. Det gælder i den konkrete betalingssituation, hvor en butik kun i begrænset omfang kan operere uden adgang til strøm, eller ved den bagvedliggende håndtering af betalingerne, hvor adgang til strøm er afgørende for, at datacentre og kommunikationsnetværk fungerer.

Udfald i strømleverancen kan skyldes alt fra cyberangreb, fysiske angreb på infrastrukturen til fejl i elnettet. Risikoen ses primært ved strømsvigt i større skala, dvs. på nationalt eller regionalt niveau, hvor større dele af det danske betalingsmarked påvirkes. Hvis et mere lokalt strømsvigt påvirker betalingsmarkedet, vil det formentlig være, fordi det rammer en central aktør i markedet, som resulterer i et nedbrud, som udgør en selvstændig risiko for betalingsmarkedet.

Risiko 2

Netværksnedbrud

Det digitaliserede betalingsmarked er afhængigt af adgangen til velfungerende netværk i form af adgang til internet og telenet. Hvis der sker et netværksnedbrud, hvor f.eks. en større teleleverandør er nede, eller hvor central netværksinfrastruktur angribes, udgør det potentielt en udfordring for betalingsmarkedet. Det skyldes, at alle aktører i markedet er afhængige af at kunne kommunikere med hinanden via nødvendige netværk og dataforbindelser. Oftest vil professionelle aktører på markedet dog have ekstra dataforbindelser, så man kan få adgang til netværksoperatører ad en sekundær vej ved nedbrud.

Et netværksnedbrud forhindrer ikke altid betalingers gennemførsel, da en række betalingsmetoder godt kan fungere helt eller delvist, selvom der ikke er internetforbindelse, eller hvis telenettet er nede.

Strømsvigt i Sydeuropa april 2025 lammede store dele af betalingssystemet

Den 28. april 2025 ramte et stort strømsvigt Spanien, Portugal, Andorra og dele af Sydfrankrig, så millioner mistede strøm i op til et døgn. Offentlig transport, hospitaler og betalingssystemer var påvirket, og mange butikker kunne kun tage imod kontanter. Kortbetalinger faldt med over 40 %, e-handelen faldt med mere end 50 %, og det samlede forbrug i Spanien faldt med en tredjedel på en enkelt dag. Panikkøb og tomme hylder var udbredt, og mange betalinger blev forsinket eller afvist. Nedbruddet skyldtes elnetproblemer.

TDC telenedbrud i november 2024 betød, at millioner af danskere ikke kunne ringe

Den 28. november 2024 blev det danske teleselskab TDC ramt af et landsdækkende nedbrud på mobilnetværket, der varede flere timer. Årsagen var en teknisk fejl i forbindelse med en netværksopdatering. Fejlen medførte, at millioner af kunder mistede mulighed for at foretage opkald og bruge mobildata. Situationen gik ud over hele landet, og en væsentlig konsekvens var, at mange hverken kunne ringe til hinanden eller til nødnummeret 112. Myndigheder og politiet måtte derfor udsende patruljer i byerne, så borgere kunne opsøge hjælp fysisk. Samtidigt blev Banedanmark ramt af signalfejl, hvilket ydermere gav transportkaos. TDC fik løst problemet samme aften, men hændelsen viste, hvor sårbart samfundet er ved større tekniske udfald hos centrale infrastrukturselskaber på grund af de gensidige afhængigheder, der er til andre sektorer.

Risiko 3

Tekniske og driftsmæssige nedbrud hos en aktør

En tredje kilde til nedbrud og dermed en vigtig risiko for betalingsmarkedet er tekniske og driftsmæssige nedbrud hos de enkelte aktører, som er en del af en betaling. Mens det for de øvrige risici handler om trusler, som kan ramme betalingsmarkedet bredt, fokuseres der med denne risiko på tilfælde, hvor én enkelt aktør er ramt. Det kan f.eks. skyldes et målrettet cyberangreb, et fjendtligt internt eller eksternt forsøg på sabotage, tekniske fejl hos aktøren selv eller udviklings- eller opdateringsfejl. Konsekvensen ved denne type hændelser er, at én konkret aktør i betalingsmarkedet midlertidigt er ude af stand til at operere, enten helt eller delvist alt efter aktørens organisering og setup. Generelt vil aktørenedbrud naturligt få større konsekvenser for betalingsmarkedet der, hvor enkelte aktører udfylder flere roller, eller hvor én aktør varetager en unik rolle i markedet og derved udgør en koncentrationsrisiko i nedbrudstilfælde.

Cyberangreb mod danske banker i januar 2023 lagde en stribe netbanker ned

Den 10. januar 2023 blev en række danske banker samt Nationalbanken ramt af et koordineret cyberangreb, som førte til, at flere bankers hjemmesider og netbanker var utilgængelige i flere timer. Angrebet blev udført som et DDoS-angreb, hvor tusindvis af forespørgsler overbelastede systemerne. Ifølge sikkerhedsekspert var det den prussiske hackergruppe Killnet, der stod bag angrebet, som havde til formål at skabe frygt og forstyrrelser i den danske finanssektor.

Risiko 4

Teknologi-afhængighed

Den fjerde type af risici omfatter potentielle trusler, som opstår ved, at betalingsmarkedet og dets aktører er afhængige af faktorer uden for betalingsmarkedet. Her ses især risici som følger af afhængigheden af virksomheder og tekniske løsninger, som er etableret og udviklet uden for Danmark, Norden eller EU. På grund af den geopolitiske udvikling, handelshindringer eller leveranceproblemer kan der opstå situationer, hvor de dele af betalingsmarkedet, som er særligt afhængig af ikke-europæisk teknologi, er i risiko for at blive påvirket og opleve et nedbrud. Teknologifafhængighed er dermed et vigtigt emne at forholde sig til i arbejdet med at sikre strategisk autonomi og robusthed på det danske betalingsmarked.

Amazon Web Services-nedbrud i oktober 2025 ramte virksomheder og myndigheder globalt

Den 20. oktober 2025 oplevede Amazon Web Services [AWS] et omfattende nedbrud i et af sine datacentre i Virginia, USA. Nedbruddet varede op til 15 timer og ramte tusindvis af virksomheder og myndigheder globalt – herunder banker, betalingsløsninger, kommunikationsplatforme og offentlige tjenester. Blandt de ramte var Lloyds Bank, kryptobørser, betalingsapps og flere europæiske institutioner, som mistede adgang til data og ikke kunne fungere.

Microsoft-nedbrud i oktober 2025 lagde Outlook og hjemmesider ned i timevis

Den 29. oktober 2025 oplevede Microsoft et omfattende globalt nedbrud relateret til Microsofts cloud-platform Azure. Nedbruddet varede ca. 8 timer og medførte forstyrrelser i adgangen til hjemmesider, apps og mailtjenester som Outlook. Både offentlige myndigheder og private virksomheder var påvirket.

Nedbrudslængde

Varigheden af et nedbrud med et af risikoscenarierne er desuden vigtig for analysen af, hvordan robustheden kan styrkes. Nedbrudslængden har således en væsentlig indflydelse på både konsekvenser og det nødvendige niveau af krisehåndtering i betalingsmarkedet. Korte nedbrud, hvor der f.eks. i et par timer er manglende eller begrænset adgang til kortbetalinger, opleves som forstyrrende, men kan oftest håndteres inden for rammerne af eksisterende beredskabsplaner og ved aktivering af alternative betalingsformer.

Når et nedbrud derimod strækker sig over længere tid, intensiveres presset på betalingsmarkedet, og udfordringerne bliver markant større. Langvarige nedbrud kan hurtigt lamme forsyningskæder og øvrig infrastruktur, og forbrugernes adgang til basale varer og tjenester risikerer at blive væsentligt begrænset.

Det kræver forskellige løsninger alt efter hvor længe et nedbrud varer, og derfor skelnes der i analysen mellem nedbrudslængder. Med det afsæt defineres nedenstående fire faser for nedbrud til brug for den videre analyse.

I analysen fokuseres der primært på nedbrud, som varer indtil 7 dage, mens længerevarende nedbrud er uden for scope. Det skyldes især, at øvrige dele af samfundet også påvirkes ved nedbrud af længere varighed end dette, f.eks. ved strøm- eller netværksnedbrud, hvilket forventeligt påvirker forsyningskæder og samfundets almindelige tilstand. Ved langvarige bredere nedbrud er betalingsrobustheden derfor ikke så afgørende som ved kortere nedbrud, hvor øvrige dele af samfundet formentlig godt kan fungere og understøtte købs- og betalings-situationer.

Analysen arbejder med de fire overordnede kritiske risici, som kan ramme det danske betalingsmarked. Sårbarheder i det danske betalingsmarked viser sig, når de identificerede risici i sjældne tilfælde, materialiserer sig i praksis. Næste afsnit handler om de sårbarheder, som vurderes at kunne påvirke det danske betalingsmarked i praksis.

Nedbrud opdelt i fire faser



4.

Sårbarheder



Danmark har generelt et sikkert, effektivt og stabilt betalingsmarked og -infrastruktur. Som beskrevet tidligere er betalingsmarkedet komplekst og står over for et stadig mere udfordrende trusselsbillede, hvor hybride trusler, avancerede cyberangreb og en afhængighed af global teknologi og leverandører i høj grad præger billedet.

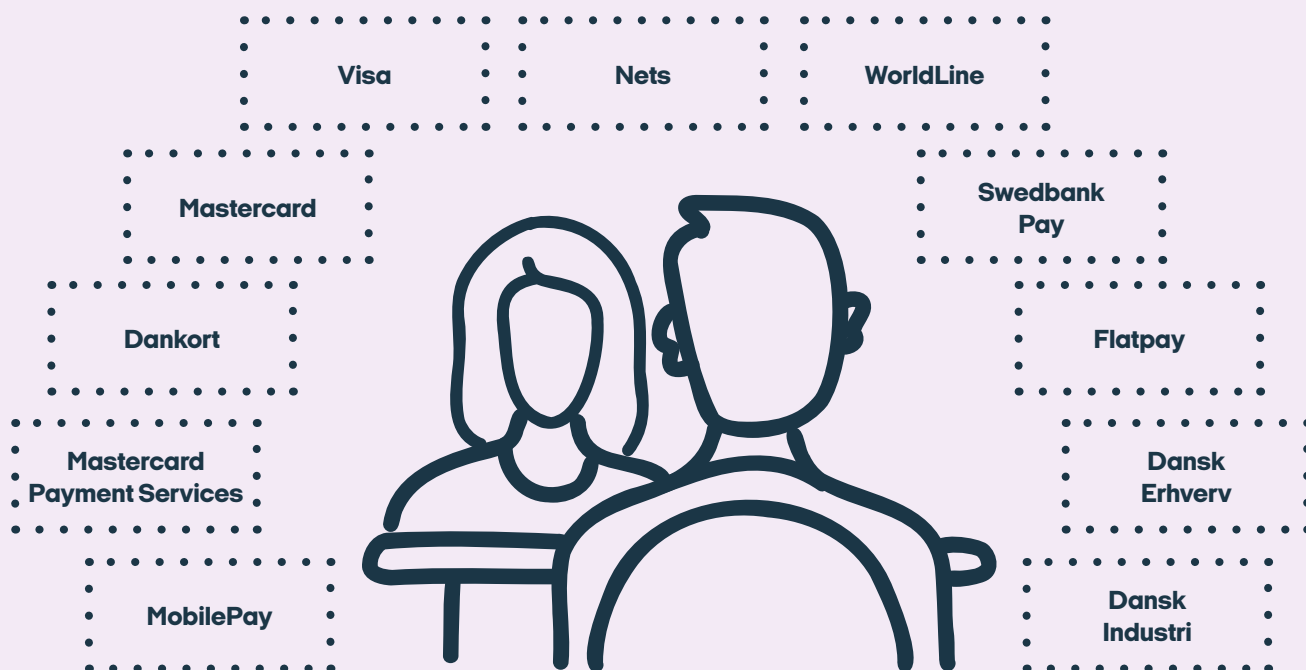
De seneste år har vist, at hændelser, der enten direkte eller indirekte kan ramme betalingsmarkedet, ikke er hypotetiske. Det er derimod reelle risici, der har ført til konkrete og mærkbare hændelser i både Danmark og resten af Europa. Strømsvigt, tekniske og driftsmæssige fejl samt netværksnedbrud har alle testet markedets robusthed, og konsekvenserne har været mærkbare for forbrugere rundt omkring i verden.

Sårbarheder i det danske betalingsmarked viser sig, når de identificerede risici fører til kritiske hændelser i praksis. Aktørerne i markedet har generelt gode risikostyringsprocesser og afprøvede beredskabsplaner. De bidrager til, at de fleste risici ikke fører til egentlige hændelser eller nedbrud, der påvirker muligheden for at betale. Men der er også potentiale for forbedring. Når

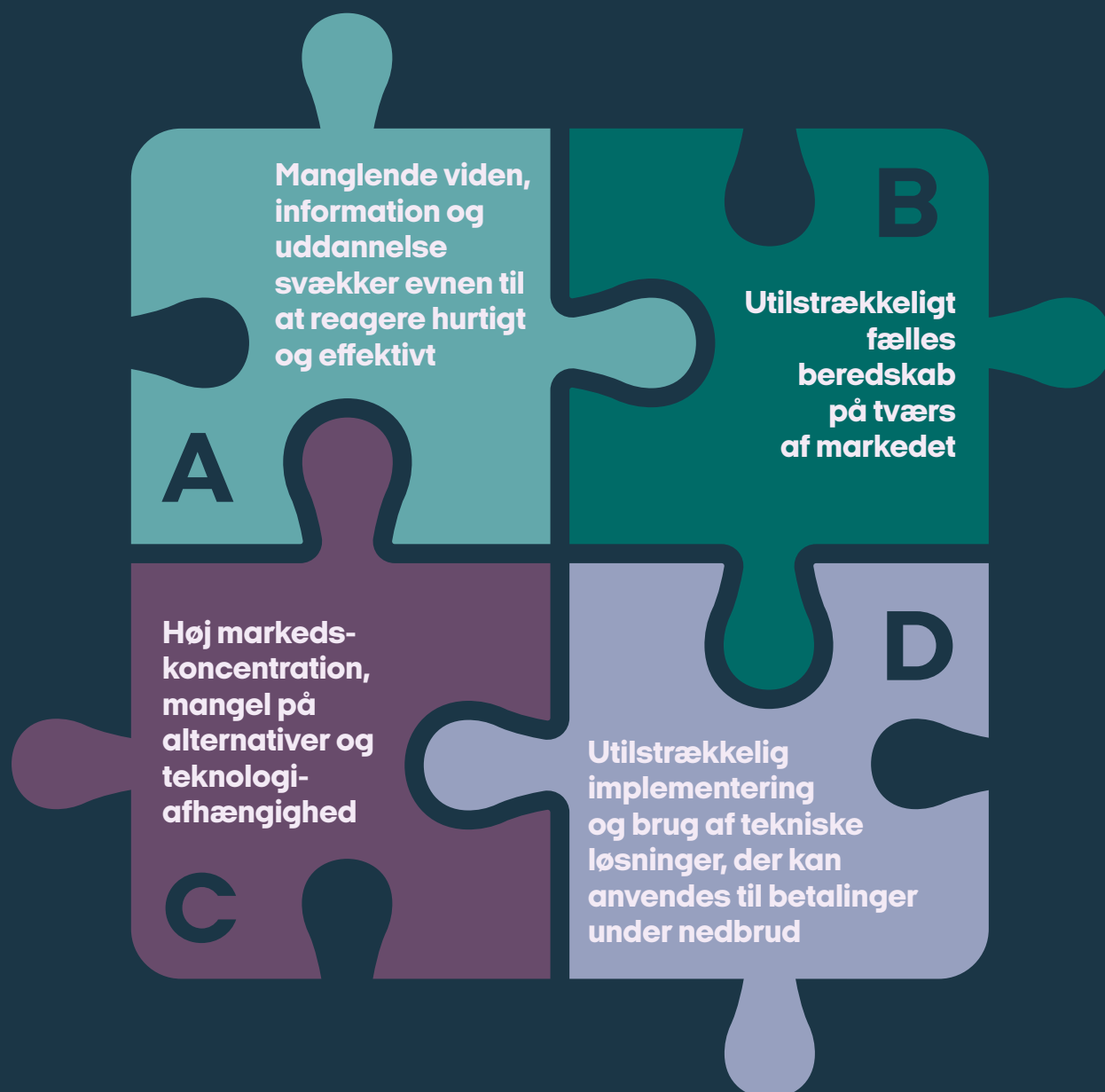
centrale aktører eller dele af betalingsinfrastrukturen al ligevel rammes af nedbrud eller kriser, har det direkte og vidtrækkende konsekvenser for forbrugernes muligheder for at betale. Både i fysiske butikker, online og mellem privatpersoner. Hvilke betalingsmetoder, der påvirkes hos forbrugerne, afhænger i høj grad af hvor i værdikæden, hændelsen slår igennem. Nedbrud hos centrale tekniske aktører eller i den kritiske betalingsinfrastruktur rammer bredt og kan lamme flere betalingsformer samtidig, mens lokale eller sektorbestemte hændelser typisk har mere begrænsede effekter. Konsekvenserne af et nedbrud vil også være forskellige alt efter hvilke butikkers betalinger, der er forstyrret. Sårbarhederne vil således særligt vise sig for butikker med vigtige samfundsfunktioner som eksempelvis butikker med salg af dagligvarer og medicin samt transport og broer.

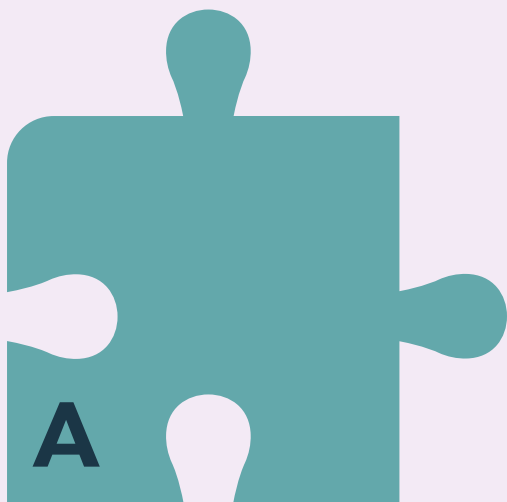
Analysen af det danske betalingsmarked er lavet gennem interviews med nøgleaktører og ved en systematisk gennemgang af betalingsløsninger. Her er der identificeret en række konkrete risici og udfordringer for robustheden, som kan sammenfattes i fire typer af sårbarheder, som præsenteres og diskuteres i det følgende afsnit.

Dem har vi talt med – interviewdeltagere i analysen



Sårbarheder i det danske betalingsmarked





Sårbarhed A

Manglende viden, information og uddannelse svækker evnen til at reagere hurtigt og effektivt

Et robust betalingsmarked forudsætter, at alle aktører har adgang til relevant viden og løbende uddannelse om betalingsløsninger, backup-løsninger og håndtering af nedbrud og krisesituationer. Det drejer sig om både forbrugere og erhvervsdrivende samt centrale tekniske aktører, banker og myndigheder. Flere aktører i de gennemførte interviews peger på, at manglende viden, information og uddannelse er en grundlæggende sårbarhed, der svækker aktørernes og forbrugernes evne til at reagere hurtigt og effektivt, når betalingsmarkedet udfordres af nedbrud. Det gælder særligt blandt butikkernes personale og hos forbrugerne, som ofte vil være de første, der mærker effekterne af forstyrrelser på betalingsmarkedet.

Centralt er, at både forbrugere og butikker ofte har begrænset viden om, hvordan de ved nedbrud tager alternative betalingsløsninger og back-up løsninger i brug. Det gør det danske betalingsmarked sårbart over for de risici, der i praksis kan vise sig. Sårbarheden forstærkes yderligere af, at ca. 40 pct. af alle kortbetalinger i fysiske butikker nu foretages via wallet-løsninger på mobilen. Denne præference kan gøre forbrugerne udsatte under nedbrud, hvis ikke butikken har implementeret offline-løsninger, der understøtter denne betalingsmetode, eller hvis ikke der kan anvendes alternative betalingsmetoder. Manglende forståelse for betydningen af at kunne skifte til offline-kortbetalingsløsninger eller mellem betalingsløsninger kan resultere i, at betalinger afvises under nedbrud og forstyrrelser.

Flere interviewede aktører indikerer, at mange butikker mangler interne rutiner, uddannelse og klare beredskabsplaner. Hvis medarbejdere står uden instruks og træning i krisehåndtering, når de primære betalingsløsninger rammes af forstyrrelser, kan det bremse salget og skabe usikkerhed blandt kunderne. Der findes allerede relevante back-up løsninger, herunder offline-kortbetalinger, men for at disse skal have mest mulig effekt som robusthedsværn kræver det, at butikspersonalet er fortrolige med løsningerne og kan aktivere dem korrekt.



Nets nedbrud i juli 2025 skabte kaos ved festivaler og i butikker

Den 19. juli 2025 oplevede betalingsvirksomheden Nets et omfattende nedbrud, der varede omkring tre timer. Årsagen var en intern systemfejl, der satte Nets' infrastruktur for kortbetalinger ud af drift. Det betød, at mange forbrugere pludselig ikke kunne betale med kort, hverken i fysiske butikker eller online. Nedbruddet medførte omfattende driftsforstyrrelser, og mange festivaler, butikker og caféer oplevede lange køer, frustrerede kunder og tabt omsætning, da digitale betalinger blev afvist og alternativer ofte ikke var tilgængelige.

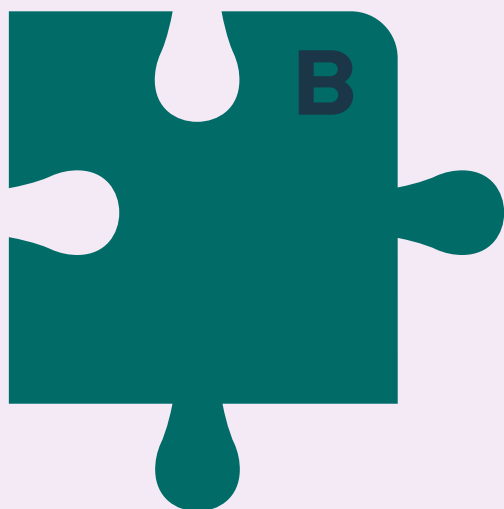
Finanstilsynet vurderede efterfølgende, at Nets' kommunikationsstrategi ikke havde været tilstrækkelig, da Nets i forbindelse med hændelsen ikke kommunikerede klart til alle kunder og samarbejdspartnere eller til offentligheden generelt om hændelsen og dens konsekvenser. DORA stiller blandt andet krav om, at finansielle virksomheder skal have en kommunikationsplan i forbindelse med it-hændelser. Nets har efterfølgende iværksat en række tiltag for både at øge robustheden og for at adressere påbuddet.

Mulige indsatser

Flere aktører spiller en central rolle i at udbrede information og viden om betalingsløsninger og nedbrudsscenarioer, så markedet bedre kan håndtere forskellige nedbrud og risici. For at løfte butikkernes viden kan centrale tekniske aktører, leverandører af betalingsløsninger og brancheorganisationer med fordel udarbejde og distribuere let tilgængelige vejledninger, så der er kendskab til betalingsløsninger samt eksisterende og nye nedbrudsprocedurer, f.eks. aktivering af offline-kortbetalinger. Nets-nedbruddet i sommeren 2025 understreger også behovet for tydelig og formaliseret kommunikation ved nedbrud, og dermed betydningen af DORA's krav om kommunikationsplaner i tilfælde af it-hændelser og nedbrud.

Det er desuden vigtigt, at forbrugerne får mere viden om deres betalingsløsninger, vigtigheden i at have flere betalingsløsninger, samt mulighederne for at anvende forskellige typer af betalingsløsninger under forskellige nedbrudsscenarioer. Det kan f.eks. ske ved nationale informationskampagner, som pjecen "Forberedt på kriser" fra Styrelsen for Samfundssikkerhed, der indeholder råd om, at alle borgere bør have et mindre beløb i kontanter i tilfælde af kriser, eller Nationalbankens seneste anbefalinger til borgere om at have flere betalingsløsninger og et mindre beløb i kontanter (pejlemærket er 250 kr. pr. person i husstanden). Finans Danmark støtter disse råd og anbefalinger.

Det kan også ske ved, at banker sørger for målrettet og løbende kommunikation til deres kunder om de forskellige løsningsmuligheder, samt hvordan de kan anvendes i forskellige nedbrudsscenarioer.



Sårbarhed B

Utilstrækkeligt fælles beredskab på tværs af markedet

Et robust betalingsmarked forudsætter, at der på tværs af myndigheder, centrale tekniske aktører, banker og erhvervsdrivende er tydelige og koordinerede beredskabsplaner og klar governance.

Medlemmerne i Betalingsrådet arbejder sammen om at sikre et længerevarende kortbetalingsberedskab baseret på offline-kortbetalinger. Som led i det beredskab er de landsdækkende dagligvarekæder og apotekere i gang med at implementere offline-kortbetalingsløsninger ude i butikkerne, og de sidste butikker forventes at have færdiggjort implementeringen i midten af 2026.

Flere peger i de gennemførte interviews på, at der stadig mangler en fælles planlægning og en mere systematisk håndtering af nedbrud. Det skyldes særligt de afhængigheder, der er mellem aktørerne på det danske betalingsmarked. Derudover er yderligere samarbejde afgørende for at kunne håndtere uforudsete hændelser mere effektivt og sikre mulighed for at kunne betale, uanset hvor i værdikæden et nedbrud opstår.

Når aktører efterlyser et stærkere fælles beredskab på tværs af betalingsmarkedet, udgør det en sårbarhed, fordi mangel på koordination, faste procedurer og rollefordeling gør markedet mindre modstandsdygtigt ved alvorlige nedbrud. Det kan også påvirke aktørernes mulighed for at aktivere egne beredskabsplaner. Dermed kan aktørernes egne indsatser blive fragmenteret og ineffektiv, når kriser rammer. Særligt i et marked med høj afhængighed af digitale betalingsløsninger og en infrastruktur med relativt få aktører er konsekvenserne alvorlige, når nedbruddet rammer bredt og på tværs af flere centrale roller.

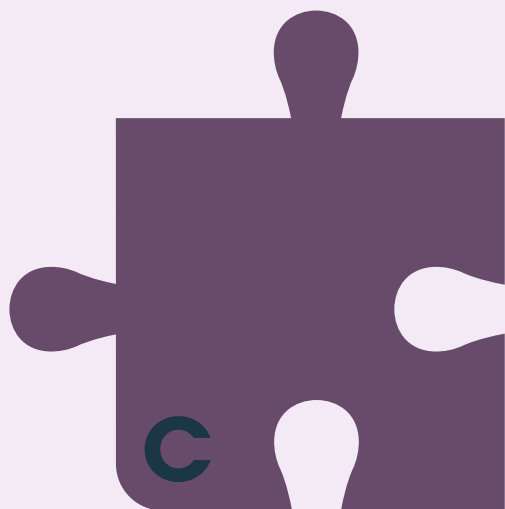
Flere tilkendegiver tilkendegiver i interviews, at denne sårbarhed ikke kun udspiller sig under langvarige eller omfattende hændelser. Selv et tre timers nedbrud, som Nets-nedbruddet i sommeren 2025, kan hurtigt eskalere, hvis beredskab og kommunikation ikke koordineres på tværs af markedet. Nets-nedbruddet illustrerede, hvordan manglende information på tværs af markedet gjorde det svært for aktører at handle effektivt. Længere nedbrud vil kunne forstærke denne effekt yderligere, og føre til økonomiske tab og usikkerhed blandt forbrugere, butikker og aktører i betalingsmarkedet.



Mulige indsatser

Betalingsmarkedets forskellige aktører og myndigheder har alle et fælles ansvar for at sikre, at beredskab og krisekoordination er på plads og let kan aktiveres ved større nedbrud. Men det er afgørende, at det er klart defineret, hvem der har ansvaret for at koordinere indsatsen på området, ligesom det er vigtigt at vide, hvem der står med ansvaret i konkrete nedbrudsscenarier, som går på tværs af betalingsmarkedet. Derudover kan det være nyttigt med en klar og fælles definition af, hvornår der er tale om et nedbrud, hvilke tiltag, der skal iværksættes og hvornår en situation eskaleres til egentlig krisestyring. Det kan f.eks. være i form af en standardplan for krisehåndtering.

En mulig løsning kan f.eks. være at identificere faste procedurer for krisekoordination og tydelig rollefordeling, så beslutninger og kommunikation flyder hurtigt og sikkert mellem alle relevante parter. Driftstest af tekniske løsninger, fælles fora for hændeshåndtering, regelmæssige øvelser og løbende evalueringer af markedets robusthed kan desuden bidrage til, at hele værdikæden er forberedt og kan håndtere uventede hændelser. En klar ansvarsfordeling og koordination på tværs af hele betalingsmarkedet er i den forstand nødvendig for at sikre robust og effektiv krisestyring.



Sårbarhed C

Høj markeds- koncentration, mangel på alternativer og teknologiafhængighed

Som beskrevet i afsnit 4 er det danske betalingsmarked er karakteriseret ved stor afhængighed af få aktører, nationale såvel som internationale, og store dele af infrastrukturen og betalingsløsningerne samlet omkring enkelte systemer og leverandører. Der er samtidig risici tilknyttet afhængigheden af virksomheder og tekniske løsninger, som er etableret og udviklet uden for Danmark, Norden eller EU. Det kan betyde, at hele markedet kan rammes på tværs, hvis en central aktør oplever nedbrud, eller hvis man af geopolitiske eller handelspolitiske årsager pludselig afskæres fra at bruge konkrete løsninger. Teknologiafhængigheden kan dermed også udfordre den strategiske autonomi.

Mastercard og Visa's fokus på europæisk forankring

Som en konsekvens af blandt andet den geopolitiske udvikling har både Mastercard og Visa med offentlige udmeldinger i løbet af efteråret 2025 understreget deres fokus på fortsat europæisk forankring.

Mastercard har blandt andet annonceret nye europæiske datacentre og prioritering af europæisk governance gennem en uafhængig europæisk bestyrelse og samarbejde med europæiske myndigheder og tilsyn.

Visa har tilkendegivet deres fortsatte ønske om europæisk tilstedeværelse gennem blandt andet beskyttelse af europæiske personoplysninger, brug af datacentre placeret i Europa og samarbejde med europæiske myndigheder.

Høj markedsconcentration, begrænsede alternativer og teknologiafhængighed gør dermed det danske betalingsmarked sårbart, når en central aktør eller løsning rammes af nedbrud. Mange butikker benytter kun én indløser, hvilket betyder, at et nedbrud hurtigt kan forplante sig. Effekten på tværs af markedet kan forstærkes, hvis der er tale om en indløser med en høj markedsandel. Manglende alternative betalingskanaler forstærker risikoen for slet ikke at kunne modtage betalinger. Et nedbrud kan dermed ramme butikkerne hårdt, og de kan i praksis blive nødt til at afvise kunder, lukke salget eller overgå til kontant betaling. Denne sårbarhed blev tydelig under Nets-nedbruddet i sommeren 2025, hvor mange butikker og betalingsmodtagere blev påvirket. Mange steder blev kunder sendt hjem uden varer eller bedt om at vende tilbage med kontanter, som flere steder var det eneste alternativ sammen med MobilePay. Her blev denne sårbarhed yderligere forstærket, da butikspersonalet mange steder ikke havde den nødvendige viden eller uddannelse i at aktivere tilgængelige offline-kortbetalingsløsninger. Dermed blev konsekvenserne af nedbruddet yderligere forstærket.



7-Eleven ransomware-angreb i august 2022 lukkede kædens 176 butikker

Den 8. august 2022 blev 7-Eleven i Danmark ramt af et alvorligt ransomware-angreb, som betød, at kassesystemerne ikke længere virkede, og kædens 176 butikker måtte indledningsvist holde lukket.

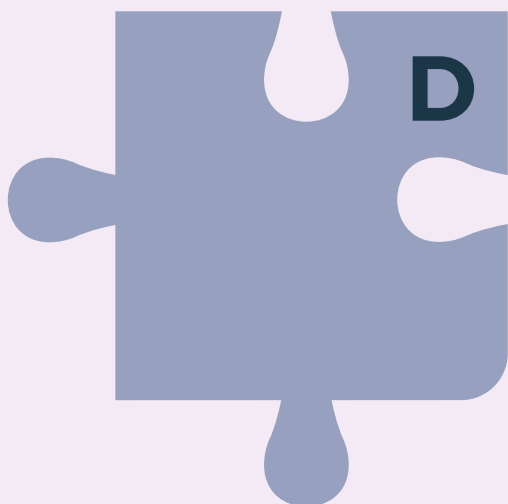
7-Eleven bekræftede selv, at de havde været udsat for et angreb, hvor hackeren via en virus tvang sig adgang til netværket, låste systemerne og forsøgt at afpresse 7-Eleven for at genetablere adgangen. 7-Eleven fik idriftsat et back-up system, som gjorde det muligt for kunder at betale med MobilePay og kontanter. 7-Eleven tog også mobilbaserede terminaler [Soft POS] i brug, som gjorde det muligt at gennemføre kortbetalinger uden om kassesystemerne og de fysiske terminaler, der var ramt af angrebet. Dagen efter kunne 5 butikker genåbne, herefter kom 100 butikker tilbage i stabil drift og efter 72 timer var alle 176 butikker tilbage i stabil drift. De systemer der blev ramt, blev løbende genetableret.

Mulige indsatser

Et robust betalingsmarked kræver adgang til flere forskellige betalingsløsninger, adgang til backup løsninger og teknisk samspil mellem aktørerne både til daglig drift og ved nedbrud. Markedet kan styrkes ved at tilbyde flere forskellige betalingsløsninger og betalingssystemer, der baserer sig på forskellige teknologier, som både kommer fra nationale, europæiske og internationale leverandører.

Robustheden kan styrkes ved at flere – særligt større – butikker overvejer at indgå aftale med flere indløsere, og anskaffe sig mobilbaserede terminaler – også kendt som Soft POS. De kan være backup-løsninger og understøtte driftssikkerheden. Man kan potentielt også løbende analysere markedsconcentration og robusthed for at undgå afhængighed af enkelte aktører.

Brancheorganisationer for butikker og betalingsmodtagere kan med fordel rådgive deres medlemmer om fordelene ved at have mere end én indløser og anvende mobilbaserede terminaler. Hvad der er de rigtige løsninger vil variere fra butik til butik og afhænger bl.a. af butikkens størrelse, hvilke varer butikken sælger og hvilke løsninger, butikkens kunder foretrækker at betale med. Denne viden er nødvendig for at butikker kan afveje omkostning og risiko ved forskellige løsninger. For nogle butikker vil MobilePay, kontanter og relevante offline-kortbetalingsløsninger være tilstrækkelig backup.



Sårbarhed D

Utilstrækkelig implementering og brug af tekniske løsninger, der kan anvendes til betalinger under nedbrud

Sikre velfungerende tekniske løsninger, der ikke kræver forbindelse til betalingssystemerne i betalingsøjeblikket, er afgørende for robustheden i betalingsmarkedet. Tekniske løsninger skal være tilgængelige og operationelle, så betalinger kan gennemføres selv ved netværksnedbrud eller tekniske fejl et sted i betalingskæden. Et robust beredskab forudsætter, at løsningerne løbende tilpasses udviklingen, og at særligt butikker ved, hvordan disse alternativer anvendes. Hvis løsningerne derimod ikke i tilstrækkelig grad er implementeret, vil betalingsmarkedet være sårbart ved nedbrud.

Flere interviewede aktører peger på, at mange butikker og betalingsmodtagere særligt i den fysiske handel ikke er fortrolige med de tekniske løsninger, der kan anvendes til betalinger ved nedbrud, og der mangler klare procedurer for aktivering og ansvar. Manglende viden om løsningerne betyder, at de enten ikke tages i brug af butikkerne eller kun fungerer som begrænset værn. Det betyder, at markedet hurtigt oplever udfordringer med betalinger, økonomiske tab og forsyningsusikkerhed ved længerevarende nedbrud. Det vil især være tilfældet, hvis ikke andre alternative betalingsløsninger (f.eks. MobilePay og kontanter) hurtigt bringes i spil, ligesom f.eks. offline kortbetalingsløsninger mister deres vigtige funktion. Af samme grund er det essentielt, at de tekniske og forretningsmæssige rammer for løsningerne indarbejdes i fælles beredskabsplaner, så aktørerne forstår, hvornår disse er effektive og hvornår andre backupløsninger skal tages i brug.

Mulige indsatser

Mulige indsatser til at imødegå denne sårbarhed er en bredere implementering af offline-kortbetalinger med udskudt autorisation og mere formaliseret viden om, hvornår både offline-kortbetalinger med lokal autorisation og offline-kortbetalinger med udskudt autorisation bør tages i brug. Særligt centrale tekniske leverandører, og eventuelt erhvervsorganisationer, bør hjælpe de erhvervsdrivende med viden, lettilgængelige guides og evt. driftstest og øvelser for at sikre, at funktionerne fungerer i praksis. Der er her en sammenhæng til butikernes viden om brugen af alternative betalingsmidler. Tilsammen skal det understøtte butikkerne i en risikoafvejning mellem omkostninger og robusthed, så de kan vælge den løsning, der bedst afspejler deres behov. Det er centralt, at de erhvervsdrivende i deres beredskabsplanlægning har klare retningslinjer for, hvornår og hvordan løsningerne tages i brug.

Offline-kortbetalingsløsningerne suppleres af Stand-in Processing, STIP, som muliggør, at et kortselskab eller en processor, på vegne af en bank, kan godkende korttransaktioner, hvis bankernes systemer ikke svarer. Det sker ud fra nogle parametre fastsat af banken, f.eks. beløb og antal transaktioner.

Bankerne kan sammen med deres tekniske leverandører med fordel løbende vedligeholde STIP-løsningerne, så kunder har adgang til tilstrækkelige midler til at dække basale indkøb under nedbrud. STIP-løsninger virker på baggrund af parametre, som bankerne har opsat sammen med henholdsvis kortselskaber og bankernes processorer. De er dermed ikke en løsning, som kræver en aktiv handling fra butikkerne ved et nedbrud. Løsningerne fjerner dermed noget af kompleksiteten fra butikkerne og er med til at understøtte robustheden i flere led af en kortbetaling. STIP kan både iværksættes hos kortselskaber og bankernes processorer på vegne af bankerne.

Centrale løsninger, der kan anvendes til betalinger under nedbrud

Offline-kortbetalinger med lokal autorisation:

Terminalen kontrollerer de indbyggede forbrugsgrænser i betalingskortets chip og godkender transaktionen uden direkte involvering af banken. Når forbrugsgrænserne er nået, så afvises den næste betaling. Den løsning virker alene for fysiske betalingskort.

Offline- kortbetalinger med udskudt autorisation (deferred authorisation):

Transaktionen godkendes ikke i betalingsøjeblikket, men lagres i stedet i terminalen. Når betalingsterminalen har genetableret forbindelse til betalingssystemerne, sendes transaktionen til betalingssystemerne for at blive autoriseret. Ved denne løsning er der ikke fastsat forbrugsgrænse, og butikker kan derved risikere tab, hvis der ikke er dækning på kundens konto. Løsningen forudsætter også, at butikkerne har betalingsterminaler, der har lagringskapacitet nok til, at de kan lagre transaktionerne i en længerevarende periode. Løsningen understøtter alle betalingskort, dvs. både fysiske kort og wallet -løsninger.

5.

Fra analyse til handling





Analysen i denne rapport peger på fire overordnede sårbarheder: A) manglende viden, information og uddannelse, B) utilstrækkeligt fælles beredskab på tværs af markedet, C) høj markedsconcentration, mangel på alternativer og teknologiafhængighed, samt D) utilstrækkelig implementering og brug af tekniske løsninger, der kan anvendes til betalinger under nedbrud.

Disse sårbarheder viser, at robusthed ikke alene handler om teknisk driftssikkerhed, men om samspillet mellem teknologi, organisering og adfærd på tværs af hele betalingsmarkedets værdikæde. Dette afsnit omsætter derfor analysen til handling gennem både konkrete anbefalinger, der kan styrke robustheden på betalingsmarkedet på kort sigt, og fokusområder for samfundets robusthed på længere sigt. Fokusområderne går på tværs af de samfundskritiske sektorer, og fordrer derfor en fælles tilgang. Samlet set udgør dette en helhedsorienteret robusthedsstrategi, som både handler om at håndtere kriser samt forhindre, at de opstår.

5.1

Anbefalinger til at styrke robustheden i betalingsmarkedet på kortere sigt

På baggrund af analysen af sårbarheder og mulige indsatser, samt indsigter fra de gennemførte interviews, præsenteres i dette afsnit de anbefalinger, som vil kunne styrke robustheden i det danske betalingsmarked på kortere sigt.

Formålet er at identificere de initiativer, der kan omsættes til handling, og som kan skabe mærkbare effekter og styrke samspillet mellem aktørerne på tværs af betalingsmarkedet.

Anbefalingerne supplerer de lovgivningsmæssige krav, som allerede gælder for sektoren, og fokuserer på praktiske og samarbejdsbaserede tiltag, der kan iværksættes inden for de eksisterende rammer.

De valgte anbefalinger er målrettet de mest kritiske faser under et nedbrud. Som tidligere beskrevet omfatter dette akutfasen [0–4 timer], den tidlige nedbrudsfase [4–24 timer] og det vedvarende nedbrud [1–7 dage]. Formålet er at styrke aktørernes evne til hurtigt at genoprette betalinger, koordinere kommunikationen og sikre, at nøglefunktioner fortsat fungerer selv under pres.

De 10 anbefalinger, som præsenteres i dette afsnit, er således konkrete tiltag, der allerede på kortere sigt skal reducere sårbarheder, øge modstandskraften og styrke tilliden til betalingsmarkedets daglige drift.



Anbefaling 1

Erhvervsdrivende bør have beredskabsplaner og uddanne personale til at håndtere nedbrudssituationer



Effekt på robusthed



Problem

- Ved nedbrud har erhvervsdrivende og deres medarbejdere ikke altid tilstrækkelig viden om, hvordan man bedst forholder sig eller hvordan betalinger fortsat kan gennemføres under et konkret nedbrud.
- Der er brug for en tydeligere plan for, hvad der skal se ved et nedbrud, hvor muligheden for at gennemføre betalinger er helt eller delvist påvirket

Målgruppe og ansvar

- Erhvervsdrivende og erhvervsorganisationer. Anbefalingen retter sig især mod erhvervsdrivende med vigtige samfundsfunktioner. Det er særligt butikker med salg af dagligvarer og medicin samt transport og anden infrastruktur.

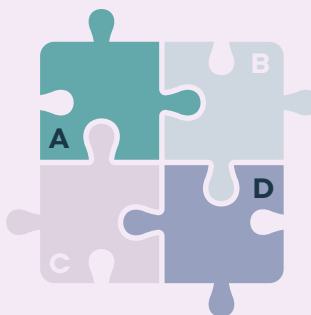
Anbefaling

- Erhvervsdrivende bør udarbejde beredskabsplaner, som forholder sig til forskellige typer af nedbrud, der påvirker evnen til at gennemføre betalinger.
- Beredskabsplanerne skal sikre, at de erhvervsdrivende ved, hvordan de under forskellige nedbrudsscenarier kan holde åbent, servicere deres kunder samt modtage betalinger. Beredskabsplanerne skal testes, og medarbejderne skal uddannes i planen og de løsninger, som sikrer, at betalinger fortsat kan fungere i nedbrudssituationer. Det kunne for eksempel være skift til offline-kortbetalinger, håndtering af mobilbetalinger eller aktivering af back up terminaler.
- Erhvervsorganisationer opfordres til at styrke deres hjælp til medlemmer med vejledning i udviklingen og brugen af beredskabsplaner, ligesom de bør understrege behovet for, at erhvervsdrivende har forholdt sig til muligheden for at kunne modtage betalinger i forskellige nedbrudsscenarier.

Nedbrudsfase

- Det vil være relevant at have en beredskabsplan samt sikre uddannelse og viden i forhold til at håndtere alle nedbrudsfaser. Formentlig vil det især være nyttigt med konkrete og praktiske instrukser i de tidlige nedbrudsfaser, hvor det kan være den enkelte medarbejders ansvar at kende til og kunne håndtere en nedbrudssituation. Ved de længerevarende nedbrud vil krisestyringen formentlig være på ledelsesniveau, hvor den erhvervsdrivende er i dialog med de leverandører, som kan være med til at håndtere betalinger under et nedbrud.

Mitigerede sårbarheder



Anbefaling 2

Nationalbanken skal have ansvar for et samlet betalingsberedskab



Effekt på robusthed

Problem

- Et robust betalingsmarked forudsætter, at der på tværs af myndigheder, centrale tekniske aktører, banker og butikker er tydelige og koordinerede beredskabsplaner og klar governance. Nationalbanken har især en central rolle gennem FSOR og Betalingsrådet, som sikrer et godt udgangspunkt for planlægning, dialog og beredskabsstyring.
- Centrale aktører peger imidlertid på, at der stadig mangler fælles planlægning og et bredere, systematisk betalingsberedskab, som er afgørende for at kunne håndtere uforudsete hændelser effektivt, uanset hvor i værdikæden et nedbrud opstår.

Målgruppe og ansvar

- Anbefalingen retter sig mod Nationalbanken. Anbefalingen kræver, at betalingsmarkedets aktører bakker op og deltager i arbejdet med et betalingsberedskab og ved konkrete hændelser.

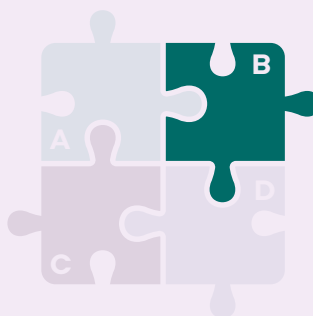
Nedbrudsfase

- Et tydeligere betalingsberedskab med Nationalbanken som hovedansvarlig vil styrke planlægningen og forberedelsen af beredskabs-situationer i alle nedbrudsfaser og sikre tydelige roller og ansvar i de forskellige nedbrudsfaser.

Anbefaling

- Det anbefales, at Nationalbanken får ansvar for at etablere og drive et samlet betalingsberedskab med bred inddragelse af betalingsmarkedets aktører. Det kunne være gennem Betalingsrådet.
- Her skal de forskellige beredskabsindsatser, der i dag foregår på tværs af betalingsløsninger og -systemer, samles. Det er f.eks. test og håndtering af konkrete nedbrud under kortbetalingsberedskabet, som de enkelte aktører på kortbetalingsmarkedet i dag selv koordinerer.
- Et robust betalingsberedskab skal koordineres, testes og videreudvikles, så det tilpasses den løbende udvikling i trusselsbilledet. Det kræver en tydelig forankring hos en myndighed, som har de efterretningsmæssige indsigter og et tilstrækkeligt tydeligt mandat, som er nødvendigt for at få alle aktører i markedet til at bidrage til beredskabet. Det bør som en del af et samlet betalingsberedskab også være klart defineret, hvornår der er tale om en krise eller et nedbrud, der aktiverer betalingsberedskabet og hvilke tiltag, der skal iværksættes.
- Det anbefales desuden, at Nationalbanken hvert andet år skal evaluere robustheden på det danske betalingsmarked og drøfte mulige tiltag med Betalingsrådet.

Mitigerede sårbarheder



Anbefaling 3

Ejerne af de danske clearing- og afviklingssystemer skal vurdere behovet for at styrke den strategiske autonomi i betalingssystemerne



Effekt på robusthed



Problem

I lyset af den øgede geopolitiske usikkerhed er der et øget fokus på strategisk autonomi på betalingsmarkedet. Det vil sige, at et givent land eller regions afhængighed af andre lande og eksterne leverandørers teknologi skal mindskes, så landet styrker kontrollen over egen kritiske infrastruktur. Det handler ikke om isolation, men om robusthed, modstandsdygtighed og suveræn beslutningskraft i krise eller konfliktsituationer.

Den strategiske autonomi er særlig vigtig i den del af betalingskæden, hvor redundansen er mindst. Den er derfor vigtigere i forhold til clearing- og afviklingssystemerne end i forhold til enkelte betalingsløsninger, hvor der er flere parallelle betalingsmuligheder, der kan tage over for hinanden ved nedbrud.

Målgruppe og ansvar

Anbefalingen retter sig mod Nationalbanken, banker og Mastercard Payment Services.

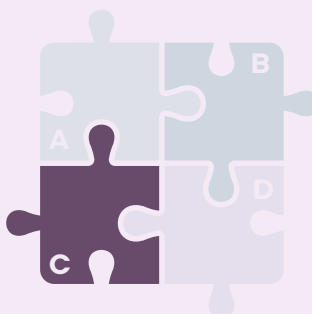
Nedbrudsfase

Anbefalingen vil kunne have en effekt ved alle nedbrudsfaser. Den generelle robusthed kan blive styrket ved at have fokus på den strategiske autonomi i valget af leverandører af clearing- og afviklingssystemer.

Mitigerede sårbarheder

Anbefaling

Det anbefales, at ejerne af clearing- og afviklingssystemerne for detailbetalinger i Danmark – Nationalbanken, banker og Mastercard Payment Services – vurderer og adresserer behovet for at styrke den strategiske autonomi, når systemerne vedligeholdes og moderniseres. Samtidig bør ejerne undersøge muligheden for i større omfang at etablere løsninger med større europæisk, nordisk eller nationalt tilhørsforhold.



Anbefaling 4

Bankerne skal sikre løbende gennemgang og vedligeholdelse af STIP-løsninger



Effekt på robusthed

Problem

- Stand-In Processing [STIP] giver mulighed for at et kortselskab eller en processor kan gennemføre kortbetalinger på vegne af den kortudstedende bank, hvis bankens systemer ikke svarer f.eks. ved et nedbrud. Der er dog behov for at løbende at gennemgå og vedligeholde STIP-løsningerne for at sikre, at de modsvarer det eksisterende risikobillede og for at kunne understøtte forbrugernes nødvendige køb under nedbrud af forskellig varighed.

Anbefaling

- Det anbefales, at alle banker minimum én gang årligt foretager en gennemgang og eventuel opdatering af deres STIP-løsninger. Bankerne skal gennemgå parametre og forbrugsgrænser, så forbrugerne kan dække basale indkøb, også ved længerevarende nedbrud. Samtidig skal bankerne vurdere, om ny teknologi kan bidrage til mere robuste STIP-løsninger.

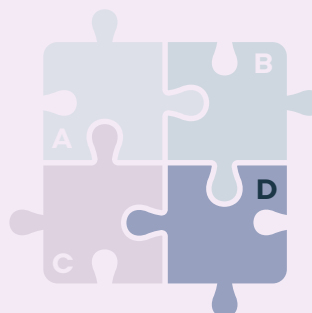
Målgruppe og ansvar

- Anbefalingen er primært rettet mod banker. Anbefalingen kræver samarbejde med kortselskaber og processorer, som skal sikre effektiv implementering, drift og justering af STIP-løsninger.

Nedbrudsfase

- Vedligeholdte STIP-løsninger vil være særlig relevante i akutfasen og den tidlige nedbrudsfase, så forbrugerne kan foretage nødvendige køb, mens butikkerne er åbne. Løsningerne vil dog også kunne anvendes under længerevarende nedbrud.

Mitigerede sårbarheder



Anbefaling 5

Erhvervsdrivende bør modtage et bredt udvalg af betalingsløsninger



Effekt på robusthed

Problem

I Danmark er der tre betalingsløsninger. Kontanter, betalingskort og kontooverførsler. De benyttes som udgangspunkt forskellige infrastrukturer og kan derfor i de fleste situationer benyttes uafhængigt af hinanden. Hvis en erhvervsdrivende ikke giver mulighed for, at kunderne kan benytte sig af forskellige betalingsløsninger, kan der opstå problemer med at betale ved et nedbrud.

Anbefaling

Det anbefales, at den erhvervsdrivende vurderer behovet for at modtage betaling på flere forskellige måder. Det betyder, at den erhvervsdrivende – i tillæg til kontanter – skal overveje at modtage både kortbetalinger samt løsninger, som benytter kontooverførsler. Den erhvervsdrivende bør desuden vurdere behovet for at kunne modtage offline-kortbetalinger, hvis den tilbyder kunder at betale med kort. Overvejelserne bør indgå i de erhvervsdrivendes generelle beredskabsplanlægning og i en risikoafvejning mellem omkostninger og robusthed, så erhvervsdrivende kan vælge den løsning, der bedst afspejler deres behov.

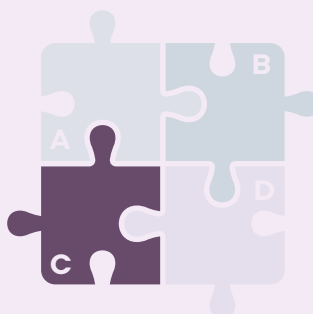
Målgruppe og ansvar

Anbefalingen retter sig mod erhvervsdrivende. De erhvervsdrivende kan via særligt indlødere og terminalleverandører få mere viden om mulighederne for at modtage et bredt udvalg af betalingsløsninger.

Nedbrudsfasen

Et større udbud af betalingsløsninger ved nedbrud er relevant i alle nedbrudsfasen.

Mitigerede sårbarheder



Anbefaling 6

Myndighederne skal følge op på lovændring, der giver mulighed for flere indlødere af Dankort



Effekt på robusthed

Problem

- Det danske betalingsmarked er karakteriseret ved stor afhængighed af få centrale tekniske aktører, og store dele af infrastrukturen og betalingsløsningerne er samlet omkring enkelte leverandører. Det betyder, at hele markedet kan rammes på tværs, hvis en central aktør oplever nedbrud, eller hvis man af geopolitiske eller handelspolitiske årsager pludselig afskæres fra at bruge konkrete løsninger. Den 1. juli 2025 trådte en ændring af lov om betalinger i kraft. Den gør det muligt, at der kan komme flere indlødere af Dankortet. Formålet med ændringen er at styrke konkurrencen på betalingsmarkedet, men det kan også have en afledt effekt på markedets robusthed.

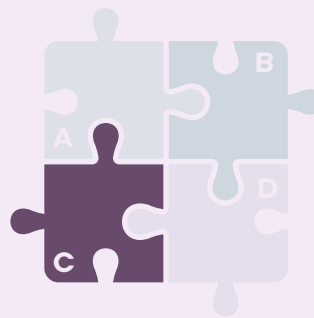
Målgruppe og ansvar

- Anbefalingen er målrettet Erhvervsministeriet og Konkurrence- og Forbrugerstyrelsen. Myndighederne bør inddrage relevante markedsaktører i opfølgningen.

Nedbrudsfase

- Det vil give de enkelte erhvervsdrivende bedre mulighed for at lave aftaler med flere indlødere, som de vil kunne skifte mellem under et nedbrud. Anbefalingen er dermed relevant for alle nedbrudsfaser.

Mitigerede sårbarheder



Anbefaling

- Det anbefales, at myndighederne sikrer, at lovændringen reelt kan anvendes og samtidig evaluere effekten af ændringen. På den korte bane bør myndigheder aktivt sikre, at reglen kan anvendes i praksis, og at potentielt nye indlødere af Dankortet får tilbudt adgang på objektive, ikke-diskriminerende og proportionale vilkår. På den længere bane bør myndighederne evaluere effekten af lovændringen, herunder om der er behov for yderligere tiltag.

Anbefaling 7

Betalingsrådet skal afdække, om mobilbetalingsløsninger baseret på kontooverførsler i højere grad kan udbredes på betalingsmarkedet



Effekt på robusthed



Problem

Betalinger hos erhvervsdrivende i den fysiske handel og på nettet sker traditionelt via kortbetalinger. Et vigtigt supplement til kortbetalinger kan udgøres af mobilbetalingsløsninger, som baserer sig på kontooverførsler. Kontooverførsler anvendes i begrænset omfang i dag og kun ca. 5 pct. af betalingerne i den fysiske handel i 2024 blev gennemført med mobilbetalingsløsninger, som anvender kontooverførsler.

Målgruppe og ansvar

Betalingsrådet, herunder Nationalbanken, som er sekretariat for Betalingsrådet.

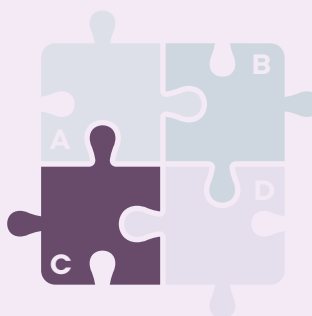
Anbefaling

I den kommende tid lanceres kontaktløse mobilbetalingsløsninger i fysiske forretninger i Danmark. Disse vil også kunne anvende konto-til-kontooverførsler. Det anbefales, at Betalingsrådet undersøger, om mobilbetalingsløsninger baseret på konto-til-kontobetalinger kan udbredes på betalingsmarkedet. Det indbefatter bl.a. en vurdering af, om der er markeds-, infrastruktur- og lovgivningsmæssige barrierer for en større udbredelse på det danske betalingsmarked. Analysens resultater og konklusioner vil kunne bruges som input til Erhvervsministerens evaluering af den danske betalingsinfrastrukturens robusthed, som skal gennemføres inden udgangen af 2026. Resultaterne vil potentielt også kunne understøtte arbejdet med at gøre det muligt, at nationale mobilbetalingsløsninger baseret på konto-til-kontobetalinger kan anvendes på tværs af EU-lande.

Nedbrudsfase

En større udbredelse af mobilbaserede kontooverførsler vil hjælpe i alle faser, men kan især være relevante som et reelt alternativ ved længerevarende nedbrud, når beløbsgrænser på terminaler og offline-værktøjer er nede. Mobilbaserede kontooverførsler vil dog også fungere i akut- og tidlig nedbrudsfase i lighed med øvrige løsninger.

Mitigerede sårbarheder



Anbefaling 8

Bankerne skal gennemføre en forstærket oplysnings- og vejledningsindsats overfor kunderne om, hvordan betalingsløsningerne kan bruges



Effekt på robusthed

Problem

- Hvis kunderne ikke har den nødvendige viden om, hvordan de forskellige betalingsløsninger kan bruges, kan det betyde, at de ikke kan betale, hvis en eller flere betalingsløsninger ikke fungerer normalt.
- Derudover vil mere viden også kunne få flere til at anskaffe sig flere forskellige betalingsløsninger.

Anbefaling

- Det anbefales, at bankerne løbende oplyser og vejleder kunderne om de forskellige betalingsløsninger, der tilbydes. Bankerne skal både vejlede om, hvordan de bruges og om behovet for at have adgang til et bredt udvalg af betalingsløsninger, som øger kundernes mulighed for at kunne betale under et nedbrud. Bankerne bør så vidt muligt også sikre sig, at kunderne modtager relevant information under et større nedbrud, f.eks. via net- eller mobilbank eller sms.

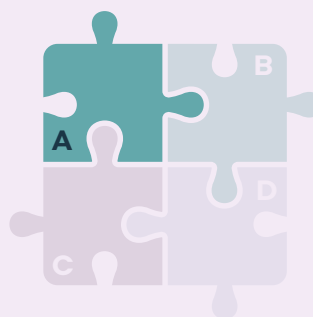
Målgruppe og ansvar

- Anbefalingen rettet sig mod bankerne.

Nedbrudsfase

- Forskellige betalingsløsninger vil især hjælpe i akutfasen og den tidlige nedbrudsfase, hvor kunderne kan være usikre på hvorfor deres betalingsløsning ikke virker som normalt. Men generelt gælder, at det er positivt i alle faser af et nedbrud, at kunderne er informerede om effekterne af hændelsen og hvornår den kan forventes at være løst.

Mitigerede sårbarheder



Anbefaling 9

Erhvervsdrivende bør overveje at anvende flere indlødere samt have backup-terminaler



Effekt på robusthed



Problem

Det kan være sårbart for den enkelte erhvervsdrivende at være afhængig af en enkelt indløser, og det kan være sårbart for betalingsmarkedet som helhed, hvis en indløser med en høj markedsandel, har et nedbrud. Det kan desuden være et problem under et nedbrud, hvis betalingsterminalerne ikke har lagringskapacitet nok til, at de kan lagre transaktionerne i en længerevarende periode.

Målgruppe og ansvar

Anbefalingen retter sig mod erhvervsdrivende. De erhvervsdrivende kan via særligt indlødere og terminalleverandører få mere viden om mulighederne for at anvende flere indlødere og have backup-terminaler.

Anbefaling

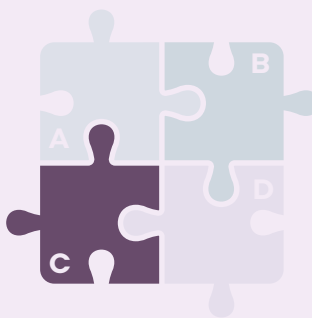
Det anbefales, at større erhvervsdrivende (med mange daglige betalinger eller høj omsætning) overvejer at benytte flere indlødere for at mindske konsekvenserne af nedbrud hos en enkelt indløser. Det kan både være relevant for fysiske butikker og webshops og særligt for butikker med salg af dagligvarer og medicin samt transport og anden infrastruktur.

Derudover anbefales det, at erhvervsdrivende overvejer at etablere backups til sit faste kasseapparat og betalingsterminal. Det kan f.eks. være håndholdte terminaler eller Soft POS-løsninger, der gør det muligt at modtage kortbetalinger direkte på en smartphone eller tablet uden brug af en traditionel betalingsterminal. Overvejelserne bør indgå i de erhvervsdrivendes generelle beredskabsplanlægning og i en risikoafvejning mellem omkostninger og robusthed, så erhvervsdrivende kan vælge den løsning, der bedst afspejler deres behov.

Nedbrudsfase

Muligheden for at kunne skifte mellem flere indlødere eller at kunne skifte til backup-terminaler vil være relevant i alle nedbrudsfaser.

Mitigerede sårbarheder



Anbefaling 10

Centrale tekniske aktører skal hjælpe erhvervsdrivende med indsigt i betalingsløsninger, der kan bruges under nedbrud



Effekt på robusthed

Problem

- Det er allerede i dag muligt at anvende offline-kort-betalinger med hhv. lokal autorisation og udskudt autorisation. Men nylige nedbrud viser, at løsninger ikke enten ikke er implementeret hos eksempelvis dagligvarebutikkerne, eller at mange ansatte mangler viden om, hvordan disse muligheder aktiveres og benyttes i praksis. Det kan resultere i, at løsninger ikke udnyttes fuldt ud, hvilket skaber unødige afvisninger og afbrudte betalinger ved nedbrud.

Anbefaling

- Det anbefales, at centrale tekniske aktører løbende uddanner og fortæller de erhvervsdrivende om løsninger, der kan anvendes under nedbrud. Det er særligt vigtigt, at de erhvervsdrivende ved, hvordan løsninger aktiveres og benyttes i praksis samt hvilke risici, der kan være forbundet med det. De centrale tekniske aktører kan bidrage med information løbende i eksisterende kundeforhold, ved genforhandling af eksisterende kundeforhold eller ved indgåelse af nye kundeforhold. Informationen vil kunne være et input og supplement til de erhvervsdrivende egne beredskabsplaner og understøtte dem i en risikoafvejning mellem omkostninger og robusthed, så de kan vælge den løsning, der bedst afspejler deres behov.

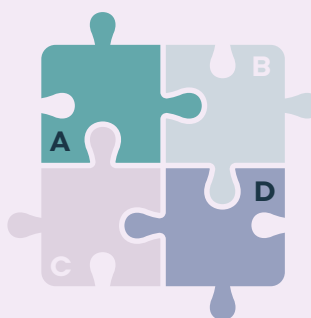
Målgruppe og ansvar

- Anbefalingen retter sig mod centrale tekniske aktører, særligt indlødere og terminalleverandører, der sælger betalingsløsninger direkte til erhvervsdrivende og øvrige betalingsmodtagere.

Nedbrudsfase

- Det er relevant med viden om håndtering af betalinger ved nedbrud i alle nedbrudsfaser. Formentlig vil det især være nyttigt med konkret og praktisk viden om offline-muligheder i de tidlige nedbrudsfaser, hvor det kan være den enkelte medarbejders ansvar at kende til og kunne håndtere offline-betalinger. Ved de længerevarende nedbrud vil der formentlig vil være behov for særskilt dialog mellem betalingsmodtageren og den tekniske leverandør.

Mitigerede sårbarheder



5.2

Fokusområder for robustheden på længere sigt

Anbefalingerne i det foregående afsnit ser på en række af de sårbarheder, der i dag præger det danske betalingsmarked. Disse tiltag styrker den operationelle robusthed på kortere sigt.

Fremtidens robusthed afhænger dog også af, hvordan Danmark håndterer de langsigtede trusler, som kan opstå i samspillet mellem teknologi, geopolitik og samfundsmæssige forandringer. Kriser, konflikter og ny teknologi vil fortsat kunne udfordre både tilgængeligheden og stabiliteten af betalinger. Robusthed handler ikke alene om at reagere på hændelser. Det handler også om at forebygge dem gennem langsigtet planlægning, samarbejde, investering i modstandskraft og fokus på de gensidige afhængigheder til særligt tele- og energisektoren.

Dette afsnit peger på en række fokusområder, som går på tværs af sektorer, og som ser på de underliggende og potentielle årsager til de identificerede risici og sårbarheder. Fokusområderne dækker både teknologiske, organisatoriske og samfundsmæssige dimensioner og fokuserer på at styrke Danmarks samlede robusthed i en mere uforudsigelig, digital virkelighed.

Finans Danmark vil fremover arbejde ad to spor i forhold til nedenstående fokusområder. I det første spor bliver der arbejdet med fokusområder, der er specifikke for

betalinger. Her tegner der sig et billede af et omskifteligt og innovativt betalingsmarked, hvor der er brug for fælles drøftelser af udviklingens konsekvenser for robustheden. Finans Danmark vil arbejde for, at disse fokusområder præger de kommende års drøftelser i Betalingsrådet, som allerede i dag fungerer som en god og konstruktiv ramme om dialog mellem myndigheder, banker og øvrige aktører på betalingsmarkedet.

I det andet spor tages der sammen med energisektoren og telesektoren initiativ til en robusthedskoalition, der skal stille skarpt på samfundsrobustheden i lyset af den geopolitiske og teknologiske udvikling. Der er brug for at skabe rammerne for drøftelser af den udvikling, som præger vores tid. Det kan opnås med en ny robusthedskoalition, hvor de centrale sektorer med de største afhængigheder går sammen. Det vil give en fast struktur for samarbejde på tværs og sikre, at strategi omsættes til konkrete resultater. Ministeriet for Samfundssikkerhed og Beredskab har allerede opsat en struktur for drøftelser om samfundssikkerhed på tværs af offentlige og private aktører, og koalitionen fokusområder spiller ind i dette arbejde. Samtidig skal koalitionen fungere som et fælles referencepunkt for dialog, prioritering og udvikling af nye løsninger. Dermed bliver robusthed ikke blot en teknisk disciplin, men et strategisk ledelsesansvar for de samfundskritiske sektorer.

Fokusområder for Betalingsrådet



Nye former for digitale penge kan give forbrugere og virksomheder nye muligheder for at betale, men kan også medføre finansiell ustabilitet

I løbet af de senere år har en række centralbanker undersøgt muligheder og udfordringer ved at udstede digitale centralbankpenge til forbrugere og virksomheder. Ingen sammenlignelige lande har endnu udstedt digitale centralbankpenge, og Nationalbanken ser ikke noget behov for en digital krone i Danmark på nuværende tidspunkt. På europæisk plan arbejdes der hen mod at kunne udstede en digital euro i 2029-30. Argumentet er, at det kan styrke robustheden af betalingssystemet og mindske afhængigheden af ikke-europæiske kort- og betalingsudbydere. Der kan dog være andre og mere effektive veje at gå for at styrke robustheden. Det skal endvidere sikres, at introduktionen af digitale centralbankpenge ikke bidrager til finansiell ustabilitet, f.eks. i form af bank-runs.

En anden form for digitale penge er stablecoins. Det er digitale aktiver udstedt på blockchains, der søger at opretholde en stabil værdi mod et traditionelt aktiv – typisk en valuta. Det kan ifølge Den Europæiske Centralbank potentielt flytte store mængder af kontant- og korttransaktioner uden for det traditionelle finansielle system og udgøre en risiko for den finansielle stabilitet. Nye former for digitale penge indebærer derfor nye muligheder, men medfører også en række problemstillinger, der kan have betydning for forbrugere, virksomheder og den finansielle stabilitet.

Nye aktørtyper ændrer det finansielle marked og kræver lige vilkår for alle udbydere

Betalingsløsninger udbydes i stigende grad af nye aktører som store tech-platformer og mindre FinTechs. Det ændrer det finansielle marked og er helt generelt til gavn for forbrugerne og virksomhederne. Det kræver rammevilkår, der sikrer lige vilkår for alle udbydere, og samtidig skal forbrugerbeskyttelsen og tilliden bevares. Den stigende kompleksitet stiller samtidig krav til koordinering, standardisering og stærk cybersikkerhed.

Fokusområder for Robusthedskoalitionen



Teknologifhængigheden kan udfordre den strategiske autonomi

Det er afgørende for samfundet som helhed at forholde sig til den afhængighed, der er bygget op omkring den teknologi og de digitale løsninger, som anvendes på tværs af sektorer. I en tid uden handelsbarrierer og geopolitiske spændinger har udbredelsen af global teknologi bidraget til bedre, enklere og billigere løsninger. Men en ny virkelighed kan risikere at blokere for de leverancer og teknologier, der kommer fra lande uden for Danmark, Norden og EU, og som mange sektorer i vid udstrækning baserer sig på. Dette rejser spørgsmålet om strategisk autonomi, og hvordan Danmark og Europa kan sikre, at kritiske funktioner, data og driftskapacitet forbliver tilgængelige under kriser og geopolitiske spændinger. Det bliver dermed også en vigtig faktor for både vækst og konkurrenceevne i Europa.

Regeringen har i den forbindelse i august 2025 også annonceret, at der afsættes 80 millioner kroner i perioden 2026-2029 til at lave en handlingsplan for digital suverænitæt.

Den geopolitiske udvikling kalder på fælles europæiske perspektiver

Balancen mellem nationale løsninger og behovet for fælles europæiske initiativer ændres i takt med, at samfundet bliver stadig mere digitalt, globalt og sammenkoblet. Den teknologiske udvikling, nye markedsaktører, sikkerhed og ikke mindst robusthed, skaber et behov for tættere samarbejde på tværs af sektorer og landegrænser.

For at bevare robustheden i den samfundskritiske infrastruktur og samtidig fremme innovation er det nødvendigt at arbejde med fælles standarder og øget samarbejde mellem systemer, platforme og løsninger. En koordineret og harmoniseret tilgang på tværs af lande og sektorer i Europa kan sikre, at nye teknologier og forretningsmodeller bliver udviklet og implementeret på en måde, der både understøtter åben konkurrence og styrker den samlede robusthed.

Udviklingen af fælles nordiske og europæiske tekniske standarder og samarbejde på tværs spiller her en central rolle. Den bidrager til at sikre lige adgang til infrastruktur, styrker den strategiske autonomi og skaber et solidt grundlag for fremtidens digitale samfund. En robust, sammenhængende og fremtidssikker infrastruktur er afgørende for at kunne håndtere øget kompleksitet og nye risici.

Nye teknologier har potentiale til at øge robustheden, men kan også skabe nye risici og sårbarheder

Den teknologiske udvikling går hurtigt. Blockchain, kunstig intelligens og kvantecomputere er eksempler på teknologier, som allerede bruges på tværs af sektorer. Det er teknologier, som kan styrke robustheden, f.eks. ved at effektivisere manuelle processer og analysere store mængder data. Det kan give mulighed for at handle hurtigere på mulige trusler. Omvendt kan teknologien misbruges af kriminelle til f.eks. mere avancerede cyberangreb samt svindel og manipulation af processer. Det er derfor vigtigt at drøfte, hvordan de samfundskritiske sektorer adresserer potentielle risici, men også fortsat drager nytte af de nye muligheder, som de nye teknologier fører med sig.

Hybride trusler kræver ny sikkerhedsforståelse

Cyberangreb, hybride trusler og forsyningssvigt kan ramme på tværs af sektorer, og betydningen af samarbejde på tværs af sektorer vokser derfor. Her er særligt finans-, energi- og telesektoren gensidigt afhængige. Det er derfor afgørende, at sektorerne forholder sig indgående til deres afhængigheder samt de nye trusler, som opstår. Det kan f.eks. være risikoen for hybridangreb, kabelødelæggelser, droneoverflyvninger og lign. Det skal naturligvis ske i tæt samarbejde med myndighederne.

Forandret trusselsbillede kræver nyt fokus på afhængigheder og koordination af beredskab på samfundsniveau

Det forandrede trusselsbillede stiller nye krav til fokus på afhængigheder mellem samfundskritiske sektorer. Det skaber også et behov for en højere grad af koordination af beredskaber på samfundsniveau. Og der er behov for at gennemføre grundige, nationale analyser og øvelser på tværs af de samfundskritiske sektorer for at identificere og træne håndtering af kritiske afhængigheder og svagheder.

Komplekse trusler fordrer et tættere efterretningsmæssigt offentligt-privat samarbejde

De komplekse trusler er i høj grad påvirket af faktorer, som sektorerne har tiltagende svært ved at styre alene. Det kræver et tættere samarbejde på tværs af samfundet, hvor offentlige og private aktører koordinerer aktiviteter, deler trusselsbillede og efterretninger, samt styrer og prioriterer de vigtigste samfundsmæssige indsatser.

Udvikling af talent og kompetencer som grundlæggende forudsætning for robusthed

Robusthed og fortsat innovation er i høj grad afhængig af adgangen til talent, kompetencer og evnen til at omsætte ny teknologi til praktisk drift, sikkerhed og værdiskabelse. I takt med at nye teknologier som kunstig intelligens, blockchain og kvantecomputing får stigende betydning, ændres kravene til arbejdsstyrken også fundamentalt. Manglen på kvalificerede it- og cybersikkerhedsspecialister er en stor udfordring i samfundet og kan dermed også udgøre en trussel for samfundets sikkerhed og robusthed. Og problemet bliver kun større i fremtiden, efterhånden som digitaliseringen øges og behovet for at styrke vores sikkerhed vokser.

Kilder

Her følger en oversigt over de væsentligste kilder anvendt til at beskrive betalingsmarkedet og det aktuelle trusselsbillede:

Betalingsrådet [2024], Status på kortbetalingsberedskabet i Danmark.

Danmarks Nationalbank [2023], Kontanternes rolle i et samfund med lavt brug af kontanter.

Danmarks Nationalbank [2025], Markedet for digitale detailbetalinger er under forandring.

Danmarks Nationalbank [2025], Overvågning af den finansielle infrastruktur 2024.

Danmarks Nationalbank [2025], Robuste betalinger i Danmark.

Center for Cybersikkerhed [2024], Cybertruslen mod Danmark.

Forsvarets Efterretningstjeneste [2024], Udsyn 2024.

Forsvarets Efterretningstjeneste [2025], Vurdering af den hybride trussel mod Danmark.

Styrelsen for Samfundssikkerhed [2024], Cybertruslen mod finanssektoren.

—

